

DIGITAL FORENSIC

Practical Guidelines for Computer Investigation

Muhammad Nuh Al-Azhar

Jakarta, 2012

DIGITAL FORENSIC

Practical Guidelines for Computer Investigation

Muhammad Nuh Al-Azhar

Jakarta, 2012

Buku ini didedikasikan untuk

Yang tercinta dan tersayang

Istriku Dea dan

Anak-anakku Zhafa, Zimam, Ghaisan dan Ghaliah

I love you all very much more than you can imagine

You all are the source of my inspiration and motivation

RIWAYAT SINGKAT PENULIS



Penulis merupakan anggota Polri yang saat ini berpangkat Komisaris Polisi dan salah satu perintis pengembangan kemampuan digital forensik di Puslabfor Mabes Polri sejak tahun 2000, dan sekarang menjabat sebagai Ketua *Digital Forensic Analyst Team* (DFAT) Puslabfor sejak Januari 2010 yang bertanggungjawab terhadap pemeriksaan dan analisa barang bukti elektronik dan digital yang berasal dari kasus *computer crime* dan/atau *computer-related crime*. Di tahun 2010, penulis beserta tim DFAT berhasil melakukan pemeriksaan dan analisa barang bukti elektronik berjumlah 214 item yang berasal dari 52 kasus, di mana sebagian besar barang bukti tersebut berupa *handphone* dan *harddisk* komputer. Dilanjutkan di tahun 2011 berhasil menganalisa lebih dari 400 item barang bukti elektronik yang berasal dari 55 kasus, dan itu belum termasuk barang bukti elektronik yang diperiksa dan dianalisa dalam tahap penyelidikan. Di samping itu, penulis juga memberikan kontribusi dasar digital forensik berupa SOP-SOP (*Standard Operating Procedure*) yang dibutuhkan dalam pemeriksaan dan analisa digital forensik, mulai dari prosedur pemeriksaan, penerimaan dan penyerahan barang bukti elektronik hingga pemeriksaan komputer, *handphone*, audio forensik dan lain-lain.

Penulis yang pernah mendapat *professional commendation* bidang *crime scene management* dari *senior investigator* New York *State Police* di tahun 2004 adalah lulusan terbaik bidang akademik Selapa (Sekolah Lanjutan Perwira) Polri tahun 2006, penerima *award* dari EC-Council yang merupakan lembaga sertifikasi internasional kompetensi bidang ilmu pengetahuan dan teknologi komputer berupa *Computer Hacking Forensic Inevstigator* (CHFI) tahun 2007 di India dan *Certified EC-Council Instructor* (CEI) tahun 2008 di Jakarta, penerima beasiswa Chevening tahun 2008/2009 dari *Foreign and Commonwealth Office* (FCO) pemerintahan Inggris, lulusan **MSc bidang *Forensic Informatics* dari *University of* Strathclyde, Inggris tahun 2009** dengan nilai *distinction* untuk disertasi yang membahas tentang *Steganography Forensic*, penerima *professional certification* di bidang *audio forensic* dari *Regional Manager* – Asia, Cedar Cambridge

Inggris di tahun 2010, dan penerima *award* dari *British Council* – Indonesia sebagai *Super Six UK Alumni* tahun 2010/2011 bersama-sama dengan Bapak Marty Natalegawa (Menlu R. I.), Riri Riza (sutradara film), Arif Suditomo (Programming Director RCTI), Mimi Mariani Lusli (pendiri Mimi Institute) dan Alexander Sriewijono (pendiri TALK-inc).

Di samping menjadi saksi ahli di beberapa persidangan, penulis juga aktif menjadi instruktur pada pelatihan-pelatihan di bidang digital forensik dan *information security*, antara lain yang diselenggarakan oleh Puslabfor Bareskrim Polri (Pusat Laboratorium Forensik), Kantor Atase Pertahanan KBRI (Kedubes R. I.) di London, UNODC (*United Nations Office on Drugs and Crime*), EC-Council dan Lemdikpol Mabes Polri (Lembaga Pendidikan Kepolisian) yang bekerjasama dengan Politieacademie Belanda; juga menjadi pembicara pada seminar/talkshow/kuliah umum yang membahas tentang *computer crime*, *digital forensic*, *social networking* dan *information security*, antara lain yang diselenggarakan oleh *University of* Strathclyde, Inggris, Universitas Indonesia, Universitas Krida Wacana, Universitas Paramadina, KPK (Komisi Pemberantasan Korupsi), dan Badiklat Kejagung (Badan Pendidikan Pelatihan Kejaksaan Agung).

KEPALA KEPOLISIAN NEGARA REPUBLIK INDONESIA

KATA SAMBUTAN

Assalamu'alaikum Wr. Wb.

Salam sejahtera bagi kita sekalian.



Mengawali sambutan ini, marilah kita panjatkan puji dan syukur ke hadirat Tuhan Yang Maha Pengasih atas segala rahmat dan ridho-Nya sehingga buku dengan judul '*Digital Forensic: Practical Guidelines for Computer Investigation*' karya Komisaris Polisi Muhammad Nuh Al-Azhar, MSc. dari Puslabfor Bareskrim Polri, dapat diterbitkan sebagai sumbangsih penulis untuk perkembangan dunia digital forensik di Indonesia, khususnya Polri dan aparat penegak hukum lainnya dalam rangka mendukung secara ilmiah teknis investigasi barang bukti elektronik yang bertambah setiap tahunnya.

Banyaknya jumlah barang bukti elektronik sebenarnya mencerminkan tantangan yang dihadapi Polri dan aparat penegak hukum lain saat ini, yaitu makin banyaknya kasus-kasus kejahatan komputer (*computer crime*) dan kejahatan yang berkaitan dengan komputer (*computer-related crime*) seperti pembunuhan, perampokan, korupsi, narkotika dan lain-lain yang berkaitan dengan peralatan teknologi tinggi berupa komputer dan handphone sebagai salah satu media yang digunakan pelaku kejahatan dalam melakukan aksinya. Jika barang bukti elektronik ini tidak disentuh dengan baik dan prosedural, maka informasi yang mungkin tersimpan di peralatan canggih tersebut yang dapat membuka kasus kejahatan tersebut akan terabaikan, bahkan kasus kejahatan tersebut bisa jadi tidak terungkap karena tidak cukupnya bukti yang kuat.

Hadirnya buku ini diharapkan dapat membantu Polri dan aparat penegak hukum lainnya bagaimana untuk mendapatkan bukti-bukti digital secara ilmiah dan prosedural yang berasal dari barang bukti elektronik dari kasus-kasus kejahatan tersebut. Dengan adanya bukti digital yang kuat secara teknis dan hukum, maka proses investigasi hingga penuntutan dapat terlaksana dengan baik dan terarah untuk menjerat pelaku kejahatan secara ilmiah. Saya menyambut baik dengan komprehensifnya buku ini yang menjelaskan teknik-teknik untuk mendapatkan bukti-bukti digital tersebut secara cepat dan benar.

Saya selaku pimpinan di Polri menyampaikan apresiasi dan ucapan terima kasih kepada penulis atas inisiatif dan kontribusi yang diberikan dalam penulisan buku ini. Harapan saya, semoga buku ini dapat bermanfaat bagi berbagai kalangan, khususnya Polri dan aparat penegak hukum lainnya, sebagai tambahan wawasan dan pengetahuan serta mampu mengaplikasikan teknik-teknik digital forensik di buku ini, di samping menumbuhkan sikap dan kepedulian tentang arti pentingnya digital forensik untuk mendapatkan bukti-bukti digital yang kuat secara teknis dan hukum.

Sekian dan terima kasih.

Wassalamu'alaikum Wr. Wb.

Jakarta, Februari 2012

KEPALA KEPOLISIAN NEGARA REPUBLIK INDONESIA

Drs. TIMUR PRADOPO
JENDERAL POLISI

KEPALA PUSAT LABORATORIUM FORENSIK

BARESKRIM POLRI

KATA SAMBUTAN

Assalamu'alaikum Wr. Wb.

Salam sejahtera bagi kita sekalian.



Dengan mengucapkan syukur Alhamdulillah ke hadirat Tuhan Yang Maha Esa atas berkat limpahan rahmat dan ridho-Nya sehingga buku berjudul '*Digital Forensic: Practical Guidelines for Computer Investigation*' yang ditulis oleh Komisaris Polisi Muhammad Nuh Al-Azhar, MSc., dapat diselesaikan dan diterbitkan sebagai wujud kepedulian penulis dalam dunia digital forensik di Indonesia, khususnya penanganan barang bukti elektronik dan digital secara ilmiah di lingkungan Polri serta aparat penegak hukum yang lain.

Dalam dunia digital forensik secara teoritis dan praktis, penulis merupakan salah satu kader potensial di lingkungan Puslabfor. Ini dibuktikan dengan tingginya kreatifitas dan motivasinya untuk mengembangkan kemampuan digital forensik dimulai dari tahun 2000 hingga saat ini. Di tataran teoritis penulis merupakan satu-satunya personil Polri yang mendapatkan MSc di bidang digital forensik di Inggris melalui beasiswa Chevening pada tahun 2008/2009, sedangkan di tataran praktis, telah dibuktikan dengan banyaknya jumlah barang bukti elektronik dan digital yang telah dianalisa secara forensik oleh penulis beserta tim DFAT (*Digital Forensic Analyst Team*) Puslabfor di mana di tahun 2010 lalu berjumlah 214 item sedangkan di tahun 2011 sebanyak lebih dari 400 item. Di samping itu, penulis juga berhasil mengembangkan beberapa SOP (*Standard Operating Procedure*) yang dibutuhkan dalam pemeriksaan dan analisa digital forensik.

Saya menyambut baik terbitnya buku ini yang mengupas secara teknis apa dan bagaimana wajah digital forensik yang dapat digunakan untuk melakukan pemeriksaan dan analisa terhadap barang bukti elektronik dalam rangka mencari dan menemukan bukti-bukti digital yang kuat secara ilmiah untuk mengungkap kasus dan menjerat pelaku kejahatan. Pembahasan di dalam buku ini cukup komprehensif mulai dari Undang-undang ITE (Informasi dan Transaksi Elektronik) hingga sisi-sisi teknis pemeriksaan forensik seperti *triage forensic*, *mobile forensic*, *files recovery*, *audio forensic*, *video forensic* dan *image forensic*. Untuk itu buku ini layak menjadi panduan dan pegangan bagi siapapun, khususnya Polri dan aparat penegak hukum lain yang ingin mengetahui dan mendalami dunia digital forensik.

Saya selaku pimpinan di Puslabfor memberikan apresiasi yang tinggi atas usaha penulis untuk membuat dan menerbitkan buku ini. Semoga karya intelektual ini dapat bermanfaat bagi pengembangan dunia digital forensik di Indonesia, khususnya bagi pelaksanaan investigasi kasus-kasus yang berkaitan dengan bukti elektronik dan digital.

Sekian dan terima kasih.

Wassalamu'alaikum Wr. Wb.

Jakarta, Januari 2012

KEPALA PUSAT LABORATORIUM FORENSIK POLRI

Drs. ANDAYONO
BRIGADIR JENDERAL POLISI

KATA PENGANTAR

Alhamdulillah penulis bersyukur kepada Allah Yang Maha Kuasa, dengan rahmat-Nya setelah melalui perjalanan yang panjang dan berliku, penulis akhirnya dapat menyelesaikan penulisan buku yang mengupas tentang Digital Forensik secara komprehensif. Buku ini dibuat sejatinya atas dasar desakan teman-teman di lingkungan Polri, baik dari Puslabfor (Pusat Laboratorium Forensik), Bareskrim (Badan Reserse Kriminal), Lemdikpol (Lembaga Pendidikan Kepolisian) maupun kepolisian wilayah, juga teman-teman dari Kejaksaan dan kampus-kampus seperti Universitas Indonesia dan Universitas Paramadina, serta lembaga lain seperti UNODC (*United Nations Office for Drugs and Crime*) dan EC-Council. Setelah menyelesaikan program pasca sarjana **MSc di bidang *Forensic Informatics* di *University of* Strathclyde, Inggris di tahun 2009**, desakan tersebut semakin menguat, namun dikarenakan kesibukan menangani pemeriksaan dan analisa barang bukti elektronik dan digital di samping melaksanakan penelitian dan memberikan pengajaran di beberapa tempat, desakan tersebut mau tidak mau masih terabaikan hingga di awal tahun 2011. Baru kemudian menjelang pertengahan tahun 2011, penulis paksakan diri untuk memulai menulis buku ini. Setelah berjalan beberapa waktu, penulisan buku ini terhenti juga dikarenakan kesibukan-kesibukan seperti tersebut di atas. Akhirnya di awal Desember 2011, penulis menyentuh kembali penulisan buku ini dan *Alhamdulillah* terselesaikan di akhir Desember 2011.

Untuk terselesainya penulisan buku ini, penulis ingin memberikan kredit poin dan ucapan terima kasih sebesar-besarnya kepada keluarga penulis (istri dan anak-anak) yang mendukung penuh penulis untuk memulai, menyambung dan menyelesaikan penulisan ini. Di samping itu, penulis juga mengucapkan terima kasih kepada pimpinan Puslabfor beserta jajarannya, yaitu Kapuslabfor Brigjen Pol. Drs Andayono dan Kabid Fisika dan Komputer Forensik, Kombes Pol Drs. Agus Irianto, serta rekan kerja di DFAT (*Digital Forensic Analyst Team*) Puslabfor, yaitu Hasta Saputra, Ahmad Pahmi dan Sukendar, juga pihak-pihak lain yang tidak dapat disebutkan satu per satu, yang telah membantu penulis secara teknis dan moral untuk terselesainya buku ini.

Penulis mencoba untuk membuat suatu buku yang nantinya bisa menjadi panduan dan pegangan secara umum dan teknis bagi aparat penegak hukum, dosen, mahasiswa, perusahaan swasta, manajer IT (*Information Technology*), atau siapapun yang ingin mengenal, memahami dan mendalami tentang dunia digital forensik. Untuk itu, buku ini didesain untuk mengupas dan membahas tentang digital forensik secara menyeluruh, mulai dari undang-undang, prinsip dasar, prosedur hingga ke sisi-sisi teknis dari digital forensik itu sendiri seperti *triage forensic* (penanganan awal barang bukti komputer di TKP), *forensic imaging* (penggandaan secara *physical* sektor per sektor), analisa *file system* dari Microsoft Windows, *files recovery* (mencari dan memunculkan *file* walaupun sudah dihapus dan di-*format* sekalipun), *mobile forensic* (analisa *handphone*), *audio forensic* (analisa rekaman suara), *video forensic* (analisa rekaman video) dan *image forensic* (analisa gambar digital).

Meskipun sebagian buku ini mengupas sisi-sisi teknis dari digital forensik, buku ini masih bisa dibaca dan dicerna oleh orang-orang umum yang ingin mengetahui apa dan bagaimana tentang digital forensik. Seperti pada Bab I, II dan III yang masing-masing membahas tentang pendahuluan digital forensik, prinsip-prinsip dasar dan prosedur digital forensik, serta tinjauan perspektif dan forensik tentang Undang-Undang ITE (Informasi dan Transaksi Elektronik). Pada bab-bab tersebut, sebagian menggunakan kosa kata umum yang mudah dipahami. Beranjak memasuki Bab IV, sebagian besar sudah menggunakan kosa kata digital forensik. Pada bab ini, penulis menekankan pentingnya penanganan awal barang bukti di TKP yang dikenal dengan istilah *triage forensic*. Pada penanganan awal ini juga diberikan contoh-contoh *tool* yang biasa digunakan oleh *investigator* di seluruh dunia berikut hasil yang nantinya bisa didapatkan untuk membantu percepatan investigasi.

Untuk Bab V tentang analisa *file system* dari sistem operasi Microsoft Windows dan Bab VIII tentang teori dan analisa *audio forensic*, penulis menganggap bab-bab ini lebih kompleks pembahasannya dibandingkan dengan bab-bab yang lain. Penulis mencoba membahas topik-topik tersebut secara detil di sisi teknisnya, namun akibatnya mungkin sebagian istilah digital forensik agak sulit dipahami. Untuk itu penulis menyarankan untuk membaca bab-bab ini secara perlahan dan tidak melompat-lompat langsung ke sub-bab tertentu agar didapat pemahaman yang utuh.

Penulis juga memberikan pembahasan yang termasuk salah satu paling sering dicari dan dibicarakan oleh masyarakat yaitu tentang bagaimana melakukan proses *recovery* (mencari dan memunculkan kembali) *file-file* yang sudah dihapus (*deleted*) atau bahkan yang sudah di-*format* sekalipun. Pembahasan ini dijelaskan di Bab VI. Pada bab ini juga diberikan cara-cara dengan syarat-syarat teknis tertentu untuk melakukan proses *recovery* tersebut secara benar.

Pada bab-bab selanjutnya, yaitu Bab VII, IX dan X yang masing-masing membahas tentang teori dan analisa *mobile forensic*, *video forensic* dan *image forensic*, penulis mencoba memberikan gambaran yang umum dan khusus mengenai topik-topik tersebut. Misalnya di Bab VII yang menjelaskan mekanisme kerja telekomunikasi mulai dari jenis-jenis jaringan radio yang diberikan oleh *provider* (penyedia jasa) seluler, hingga stuktur kerja BTS (*Base Transceiver Station*), BSC (*Base Station Controller*) dan MSC (*Mobile Switching Centre*), di samping mekanisme penyimpanan data di *handphone* dan *simcard*, serta pemeriksaan secara forensik terhadap peralatan telekomunikasi tersebut. Sedangkan di Bab IX, penulis menjelaskan jenis-jenis analisa forensik yang bisa digunakan untuk menganalisis dan menguji rekaman video seperti menelusuri historis, keaslian dan pembesaran objek yang ada di dalam rekaman tersebut. Adapun di Bab X, penulis mencoba mengupas jenis-jenis format yang biasa digunakan di dalam gambar digital, termasuk penjelasan tentang *pixel* dan metadata exif (*exchangeable image file format*) di samping teknik-teknik untuk menguji keaslian suatu gambar digital.

Akhir kata, tiada gading yang tak retak, begitu juga isi dari buku ini, penulis terbuka menerima saran dan kritik untuk memperbaiki dan meningkatkan kualitas dari isi buku ini. Semoga buku ini dapat bermanfaat bagi berkembangnya dunia digital forensik di Indonesia.

Jakarta, Desember 2011

Penulis,

Komisaris Polisi Muhammad Nuh Al-Azhar, MSc., CHFI, CEI

DAFTAR ISI

RIWAYAT SINGKAT PENULIS i
KATA SAMBUTAN KAPOLRI iii
KATA SAMBUTAN KAPUSLABFOR v
KATA PENGANTAR vii
DAFTAR ISI x

Bab I 1
PENDAHULUAN DIGITAL FORENSIK 1
Latar belakang digital forensik 1
Sejarah berdirinya DFAT (Digital Forensic Analyst Team) 9
Kinerja tahun 2010-2011 14
Faktor-faktor yang mempengaruhi 16

Bab II 23
DIGITAL FORENSIC: Principles and Procedures 23
Prinsip-prinsip Dasar Digital Forensik 25
Klasifikasi Digital Forensik 33
Klasifikasi Barang Bukti 36
Prosedur penanganan awal di TKP 41
Prosedur penanganan di laboratorium 48
Bibliography 59

Bab III 61
UU ITE : Tinjauan Perspektif Forensik dan Hukum 61
Pengertian Informasi Elektronik dan Dokumen Elektronik 62
Alat Bukti Hukum 66
Investigasi 68
Tindak Pidana Teknologi Informasi dan Transaksi Elektronik 69
Saksi Ahli 73
Bibliography 76

Bab IV 78
TRIAGE FORENSIC: First Response Procedure 78
Prosedur penanganan awal komputer dalam keadaan off (mati) 79
Prosedur penanganan awal komputer dalam keadaan on (hidup) 80
Triage tools 80
Pencarian file enkripsi 99
Bibliography 101

Bab V 103
WINDOWS FORENSIC: File System Analysis 103
Struktur *har*ddisk : track, sektor, head dan cylinde*r* 105
Pengalokasian data : clusters dan slacks 109
File system FAT: struktur dan boot sector 117
File system NTFS: struktur MFT dan boot sector 124
Analisa registry 136
Bibliography 148

Bab VI 150
FILES RECOVERY 150
Logical files recovery 151
Deleted files recovery 158
Lost files recovery 163
Low level recovery 168
Bibliography 171
Bab VII 173
MOBILE FORENSIC: Theory and Analysis 173
Mekanisme kerja 174
Mekanisme penyimpanan data 179
Pemeriksaan forensik 187
Bibliography 195

Bab VIII 197
AUDIO FORENSIC: Theory and Analysis 197
Teori Suara 198
Komponen Suara 199
Prosedur Audio Forensic 202
Sampling Suara Pembanding 206
Sampling dan Analysis dengan Praat 207
Analisa Statistik Pitch 213
Analisa Statistik Formant dan Bandwidth 217
Analisa Graphical Distribution 225
Analisa Spectrogram 231
Penarikan Kesimpulan 235
Bibliography 237

Bab IX 238
VIDEO FORENSIC: Theory and Analysis 238
Analisa Hash 239
Analisa metadata 244
Analisa frame 250
Bibliography 257

Bab X 259
IMAGE FORENSIC: Theory and Analysis 259
Format gambar digital 260
Pixel 263
Metadata EXIF 267
Keaslian gambar digital 270
Bibliography 277

Bab I

PENDAHULUAN DIGITAL FORENSIK

Latar belakang digital forensik

Ilmu pengetahuan dan teknologi komputer termasuk salah satu bidang ilmu pengetahuan dan teknologi yang pesat perkembangannya, terutama dalam beberapa dekade terakhir, sehingga komputer sudah masuk ke dalam banyak lini kehidupan manusia, mulai dari bidang kesehatan, sosial kemasyarakatan, bisnis, pendidikan, komunikasi, rancang bangun gedung/jembatan, produk industri, teknologi luar angkasa dan lain-lain. Komputer memiliki banyak kegunaan bagi umat manusia dan oleh karenanya banyak orang ingin mempelajari ilmu pengetahuan dan teknologi komputer agar komputer dapat lebih berguna bagi kehidupan dan pekerjaannya secara pribadi atau juga untuk orang lain.

Ketika teknologi komputer masuk ke Indonesia dan mulai dikenal luas di tahun 1980-an, banyak orang pada saat itu ingin menjadi seorang ahli *programming* (bahasa pemrograman komputer) yang menguasai beberapa bahasa seperti Basic, Fortran, Pascal dan lain sebagainya. Dengan menjadi seorang *programming*, maka ia bisa membuat komputer bekerja seperti yang diinginkan dan pada akhirnya hasil dari *programming* tersebut menjadikan komputer dapat mempercepat pekerjaannya atau orang lain. Output dari *programming* biasanya berupa *software-software* yang didesain untuk kegunaan tertentu, misalnya untuk pendidikan, bisnis, desain industri dan lain-lain. Bahkan output dari *programming* juga bisa bernilai negatif ketika ia diimplementasikan untuk kejahatan seperti pembuatan virus komputer yang akan menginfeksi komputer-komputer dan/atau media penyimpanan digital seperti harddisk, flashdisk termasuk juga file-file. Hal tersebut dapat menimbulkan kerugian yang cukup besar secara materi dan non-materi.

Dengan menguasai *programming* juga, seseorang atau secara bersama-sama dapat membuat dari bahasa program komputer untuk mengembangkan sistem operasi yang merupakan pijakan dasar dalam menjalankan sebuah komputer, baik

sistem operasi yang berupa *closed-source* seperti Microsoft Windows dan Macintosh, maupun yang *open-source* seperti Linux. Oleh karenanya *programming* dapat dianggap sebagai salah satu bentuk spesialisasi yang pertama di bidang ilmu pengetahuan komputer.

Seriring bertambahnya waktu, orang semakin banyak paham tentang tata cara penggunaan komputer dan nilai manfaatnya bagi mereka. Mereka juga ingin bisa menghubungkan komputer yang satu dengan yang lain agar lebih bermanfaat bagi pekerjaan-pekerjaan tertentu yang meminta mereka untuk berbagi *file* (berkas dokumen) atau informasi. Dengan adanya jaringan internet (*inter network*) yang makin mendunia, komputer-komputer yang saling terhubung melalui jaringan-jaringan jadi semakin banyak. Hal ini menjadikan banyak orang ingin mempelajari bagaimana mengatur sistem jaringan komputer dengan baik, untuk itu mereka pun banyak yang akhirnya ingin menjadi ahli *networking*. Dengan memahami ilmu *networking*, mereka mampu mendesain jaringan komputer yang baik dan memiliki tingkat pengamanan yang lumayan tinggi, sehingga sistem jaringan komputer mereka sulit untuk disusupi oleh pihak luar atau yang tidak berkepentingan. Dengan jaringan komputer yang aman, maka orang-orang yang menggunakan jaringan tersebut juga merasa lebih aman dalam bertukar informasi dan berbisnis misalnya penggunaan situs *e-commerce* (situs yang melayani jual beli secara *online*) dengan perlindungan SSL (*Secure Soctket Layer*). *Networking* sendiri juga sering dikaitkan dengan bidang spesialisasi yang lain, yaitu *website developing* karena pada beberapa hal kedua bidang spesialisasi ini saling terkait dalam pembangunan jaringan dan situs yang aman. Oleh karenanya, *networking* dan *website developing* juga dianggap sebagai salah satu bentuk spesialisasi yang lain di samping *programming*.

Di dalam ilmu *networking*, terdapat komputer yang digunakan sebagai *server* dan ada juga komputer yang dikenal dengan istilah *client*. Komputer *server* biasanya menyimpan *database*, sedangkan komputer *client* digunakan oleh pengguna jaringan untuk mengakses komputer *server*. Dikarenakan komputer *server* menyimpan *database* yang memiliki informasi-informasi yang signifikan, maka komputer *client* senantiasa mengakses *server* untuk mendapatkan informasi-informasi yang berguna dan yang lebih baru (*updated*). *Database* yang ada di

server harus dikelola dengan baik, agar setiap saat dapat menyajikan informasi-informasi yang diinginkan oleh komputer *client* secara cepat dan tepat. Untuk itu, pengaturan *database* secara benar sangat diperlukan di dalam sistem *server*. Untuk mencapai hal tersebut diperlukanlah bentuk spesialisasi komputer yang lain, yaitu *information management*. Dengan bidang spesialisasi ini, masing-masing informasi dapat saling terhubung dan dijalin dengan rapi dan aman, sehingga dapat diakses kapanpun secara cepat dan tepat. Bidang spesialisasi *information management* ini seringkali dikaitkan dengan bidang spesialisasi *information security*, karena *information security* diperlukan untuk mengamankan berbagai macam informasi penting dan berharga yang tersimpan di dalam suatu komputer, khususnya *server*. Artinya hanya orang-orang yang memiliki hak-hak tertentu yang boleh mengakses data-data tertentu. Tidak diperbolehkan adanya akses ilegal terhadap suatu data. Dalam implementasinya untuk kejahatan, teknik-teknik di dalam *information security* ini seperti *cryptography* dan *steganography* juga dikenal sebagai *anti-forensic* (teknik yang digunakan untuk merintangi kinerja digital forensik). Misalnya, ketika teknik *cryptography* digunakan oleh pelaku kejahatan untuk menyembunyikan data kejahatannya, maka sangat sulit bagi digital forensik untuk mendapatkan data tersebut.

Biasanya terhadap *database-database* yang berharga dan tersimpan di dalam komputer *server* tersebut, dilakukan pengetesan level keamanan sebelum *server* tersebut di-*launching* (dipublikasikan secara resmi). Pengetesan ini biasanya dikenal dengan istilah Pentest (*penetration testing*). Dengan pentest ini, kekuatan dan keamanan dari suatu *database* dapat terukur dan juga diketahui titik-titik kelemahan yang mungkin dapat dieksploitasi oleh *hacker*/*cracker*. Sebelum di-*launching*, titik-titik kelemahan ini sebisa mungkin ditutup (*patched*) dengan rapi sehingga tidak dapat digunakan untuk masuk ke dalam sistem *database*. Karena pentingnya pentest ini, banyak orang atau perusahaan berusaha mendalami bidang ini. Pentest dalam tahapan selanjutnya juga dianggap sebagai salah satu bentuk spesialisasi dalam ilmu pengetahuan dan teknologi komputer. Dalam praktiknya, pentest ini sering berkaitan dengan spesialisasi-spesialisasi yang lain seperti *programming*, *networking* dan *information management* sperti yang dijelaskan di atas. Pentest sangat membutuhkan ketiga spesialisasi tersebut

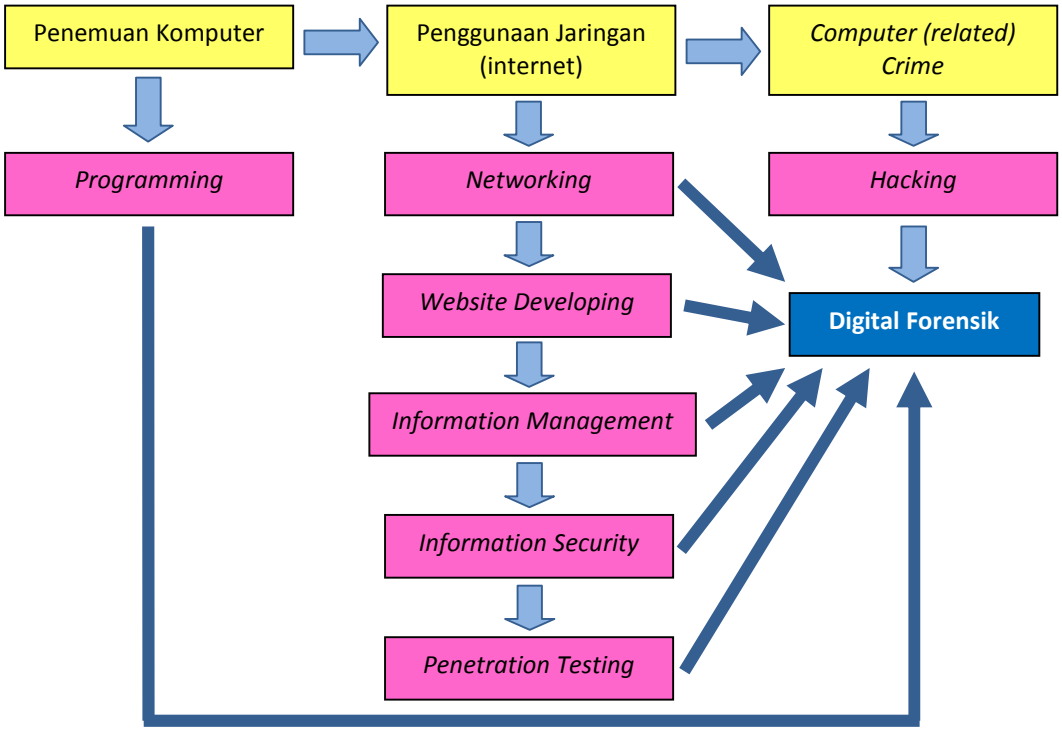
dalam rangka menjalankan tugas pengetesan dengan benar dan menambal lubang-lubang kelemahan (*vulnerability*) juga dengan benar.

Ketika *database-database* yang ada di *server* menyimpan banyak informasi yang penting dan berharga, hal tersebut juga mengundang pelaku kejahatan, yaitu *cracker*. Dalam pengimplementasiannya, *hacker* dan *cracker* sebenarnya merupakan dua sebutan yang berbeda. *Hacker* dan *cracker* adalah orang yang memiliki keahlian di bidang pentest dan menggunakan keahliannya tersebut untuk mencari titik-titik *vulnerability* dari suatu sistem, namun *hacker* menggunakannya (biasanya) secara resmi demi perbaikan dari sistem tersebut, sedangkan *cracker* menggunakannya untuk mengeksploitasi lebih dalam lagi untuk mencari keuntungan pribadi dan kelompok tertentu secara ilegal. Mereka berusaha untuk dapat masuk dan menyusup ke dalam sistem *database* dengan teknik-teknik *hacking* dan mencuri informasi-informasi yang berharga tersebut atau bahkan merusaknya sehingga tidak dapat diakses lagi. Kejahatan yang dikategorikan sebagai *computer crime* atau *high-tech crime* ini menimbulkan kerugian yang cukup besar baik materi maupun non-materi, khususnya masalah *untrust* (ketidakpercayaan) bagi *customer* terhadap dunia perbankan, jika hal tersebut terjadi di *server* suatu bank. *Hacking* yang menjadi basis dari *computer crime* juga dianggap sebagai salah satu bentuk spesialisasi ilmu pengetahuan dan teknologi komputer. Untuk menelusuri dan mengungkap kejahatan tersebut diperlukanlah bentuk spesialisasi komputer yang lain, yaitu komputer forensik atau digital forensik.

Komputer/digital forensik merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum (*pro justice*), yang dalam hal ini adalah untuk membuktikan kejahatan berteknologi tinggi atau *computer crime* secara *scientific* (ilmiah) hingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut. Pencarian bukti-bukti digital untuk menjerat pelaku seringkali merupakan pekerjaan yang sangat kompleks di mana seorang *digital forensic analyst/investigator* harus mengikuti prosedur-prosedur yang diakui secara hukum baik nasional maupun internasional, termasuk juga mereka harus memahami secara teoritis hal-hal yang berkaitan dengan bukti digital yang

ditemukan, di samping juga memahami bagaimana penggunaan *software-software* forensik untuk mencari bukti-bukti digital tersebut dengan benar. Seringkali pula bukti-bukti digital tersebut sudah dihapus oleh pelaku untuk menghilangkan jejaknya. Di sinilah tantangan bagi seorang *analyst/investigator* untuk menelusuri kembali bukti digital yang sudah hilang tersebut, bahkan mereka harus mampu untuk me-*recover*-nya kembali. *Digital forensic analyst/investigator* juga sering dipanggil ke persidangan sebagai saksi ahli untuk menjelaskan proses dan temuan dari bukti-bukti digital tersebut, dimulai dari temuan barang bukti elektronik di TKP, penerimaan barang bukti di laboratorium, pemeriksaan secara ilmiah dan analisa laboratoris kriminalistik hingga pembuatan laporannya. Karena pentingnya digital forensik dalam pengungkapan kasus kejahatan komputer dan *computer-related crime* untuk penegakan hukum di suatu negara termasuk Indonesia, maka digital forensik haruslah senantiasa dikembangkan mengikuti perkembangan ilmu pengetahuan dan teknologi komputer. Digital forensik seharusnya dapat berada satu langkah di depan *computer crime* dan *computer-related crime*. Meskipun begitu seringkali *digital forensic analyst/investigator* mendapatkan temuan atau modus baru dari kejahatan tersebut. Hal ini sering disebut sebagai *learning by crime*.

Dari Gambar I.1. di bawah tentang flowchart perkembangan bentuk-bentuk spesialisasi bidang ilmu pengetahuan dan komputer, dapat diketahui bahwa digital forensik sebaiknya didukung oleh bidang-bidang spesialisasi yang lain seperti *programming*, *networking*, *website developing*, *information management*, *information security*, *penetration testing* dan *hacking*. Hal ini diperlukan karena ketika seorang *digital forensic analyst/investigator* berhubungan dengan *computer crime* dan/atau *computer-related crime*, maka mereka sebenarnya akan berhadapan dengan berbagai macam modus operandi yang dilakukan oleh pelaku yang cerdas (*smart criminals*) dengan memanfaatkan ilmu pengetahuan dan teknologi komputer. Semakin banyak *analyst/investigator* memahami bidang-bidang spesialisasi yang lain, maka pemeriksaan dan analisa barang bukti elektronik dapat dilakukan secara komprehensif. Dengan sudut pandang yang menyeluruh, maka output dari pemeriksaan dan analisa akan lebih maksimal untuk mendapatkan bukti-bukti digital.



Gambar I.1. *Flowchart* bentuk-bentuk spesialisasi di bidang ilmu pengetahuan dan teknologi komputer yang berkaitan dengan digital forensik.

Digital forensik termasuk bidang spesialisasi komputer yang baru, dan oleh karenanya tidak banyak universitas di luar negeri yang menyelenggarakannya, di samping sulit untuk mendapatkan ahli di bidang tersebut untuk menjadi dosen pengajarnya. Misalnya pada tahun 2008/2009 di Inggris, hanya beberapa universitas yang menyelenggaran program pasca sarjana MSc di bidang digital forensik, antara lain *University of* Strathclyde dan *University of* Glasgow. Hal ini berbeda dengan keadaan di tahun 2011 di mana sudah bertambah beberapa universitas yang menyelenggarakan program pasca sarjana tersebut, misalnya Middlesex *University*, Abertay *University*, *University of* Derby, *University of* Portsmouth dan lain-lain. Bahkan di Indonesia sendiri, belum ada satupun universitas yang menyelenggarakan komputer/digital forensik sebagai salah satu mata kuliah, apalagi sebagai salah satu program pasca sarjana. Padahal tantangan ke depan, ahli-ahli komputer akan banyak berhubungan dengan jenis kejahatan komputer dan/atau *computer-related crime* ini, mereka akan sering diminta

bantuannya untuk mengungkap kejahatan ini secara ilmiah. Permasalahan akan muncul ketika permintaan untuk ahli digital forensik semakin meningkat seiring dengan semakin banyaknya penyelahgunaan komputer, *handphone* dan peralatan elektronik lainnya untuk kejahatan, namun orang yang ahli di bidang tersebut masih sangat minim. Hal tersebut akan memaksa perusahaan atau lembaga penegak hukum untuk menggunakan orang-orang yang paham ilmu pengetahuan dan teknologi komputer secara umum atau memiliki spesialisai komputer yang lain seperti *programming*, *networking*, *website developing*, *information management*, *penetration testing* atau *hacking*, namun mereka tidak paham dan tidak memiliki keahlian di bidang digital forensik. Masalah besar yang muncul adalah mereka meng-*handle* barang bukti elektronik yang berasal dari kejahatan tersebut dengan tidak mengikuti kaidah prinsip-prinsip dasar dan prosedur digital forensik yang diakui secara internasional. Dikhawatirkan output dari pekerjaan mereka tidak dapat diterima di persidangan sebagai salah satu alat bukti hukum yang syah. Jika ini sampai terjadi maka pelaku kejahatan komputer dan/atau *computer-related crime* akan dimungkinkan dapat bebas demi hukum.

Analogi dari hal tersebut adalah pemeriksaan secara ilmiah terhadap barang bukti berupa mayat yang ditemukan di TKP. Untuk melakukan pemeriksaan tersebut dibutuhkan seorang dokter yang memiliki kemampuan dan keahlian di bidang spesialisasi kedokteran forensik, bukan bidang-bidang spesialisasi kedokteran yang lain. Begitu juga dengan temuan barang bukti elektronik di TKP, seharusnya barang bukti tersebut diperiksa secara ilmiah oleh ahli di bidang spesialisasi digital forensik, bukan bidang-bidang spesialisasi komputer yang lain.

Oleh karena jumlah ahli di bidang digital forensic ini sangatlah terbatas, baik skala nasional maupun internasional, maka orang-orang yang memiliki keahlian di bidang ini dihargai dengan mahal. Misalnya lowongan pekerjaan sebagai *forensic senior manager* yang berbasis di London, Inggris yang diiklankan lewat situs www.forensicfocus.com per tanggal 2 Desember 2011 seperti pada Gambar I.2. di bawah ini.



Gambar I.2. Lowongan pekerjaan sebagai *digital forensic senior manager* di London dengan gaji yang ditawarkan sebesar 90.000 poundsterling.

Lowongan ini mebutuhkan *skills* kunci tentang komputer forensik, investigasi kebocoran atau pencurian data dan pengembangan bisnis, untuk itu kandidat harus memiliki pengalaman dan keahlian di bidang investigasi forensik lapangan, investigasi *network intrusion* (penyusupan ke dalam jaringan komputer) dan/atau *e-discovery* (pencarian dan *recovery* data-data digital). Di samping mendapatkan mobil dan bonus, gaji yang akan diterima dalam 1 tahun kontrak kerja sebesar 90.000 poundsterling atau setara dengan Rp. 1,2 milyar di mana 1 poundsterling dianggap sekitar Rp. 14.000,- per 17 Desember 2011 di situs http://themoneyconverter.com dan http://www.exchange-rates.org.

Ada juga lowongan pekerjaan di Inggris sebagai *computer forensic analyst* yang juga diiklankan lewat situs www.forensicfocus.com per tanggal 29 November 2011. Lowongan dari perusahaan swasta IntaForensics ini ini lebih ditujukan untuk mahasiswa yang baru lulus dengan pengalaman kerja yang minim, yaitu 2 tahun di bidang *digital forensic*. Adapun gaji yang ditawarkan minimal 30.000 poundsterling atau setara Rp. 422 juta, dan gaji ini bisa naik disesuaikan dengan lamanya pengalaman kerja.

Dari berbagai iklan lowongan pekerjaan sebagai *digital forensic analyst*, dapat diketahui bahwa permintaan pasar untuk ahli di bidang spesialisasi ini sangatlah besar. Oleh karena itu, sebaiknya kampus-kampus pendidikan di Indonesia dapat memasukkan bidang spesialisasi digital forensik ini ke dalam mata kuliah S1 atau program pasca sarjana. Ke depannya makin banyak lulusan sarjana Indonesia yang menguasai dan menjadi ahli di bidang digital forensik ini. Paling tidak permintaan

pasar dalam negeri untuk kebutuhan seorang *digital forensic analyst/investigator* dapat terpenuhi oleh sarjana-sarjana Indonesia, tidak diisi oleh ahli dari luar. Keinginan penulis, kita menjadi tuan rumah di negeri sendiri dan kalau bisa kita juga dapat mensuplai ahli-ahli digital forensik yang diakui bagi pasar di luar negeri. Menurut pendapat penulis, semakin cepat universitas-universitas di Indonesia menyelenggarakan mata kuliah secara umum atau program pasca sarjana secara khusus akan semakin baik bagi perkembangan digital forensik di tanah air.

Sejarah berdirinya DFAT (Digital Forensic Analyst Team)

Di awal tahun 2000an, melihat perkembangan penggunaan teknologi komputer dan *handphone*, penulis memprediksi bahwa 10 tahun ke depan, yaitu di sekitar tahun 2010 akan sangat mungkin terjadi *booming* (ledakan) barang bukti elektronik. Pada tahun 2000an memang penggunaan perangkat komputer untuk kegiatan kantor sehari-hari dan *handphone* untuk kemudahan telekomunikasi belum begitu menyentuh sebagian besar masyarakat Indonesia, dikarenakan harga kedua perangkat tersebut masih relatif mahal dan hanya bisa dijangkau oleh masyarakat yang berpenghasilan tinggi. Kedua perangkat tersebut hanya bisa dinikmati oleh orang-orang berduit dan menjadi *prestige* (nilai tambah) bagi yang memiliki dan menggunakannya dalam kehidupan sosial masyarakat.

Seiring dengan makin banyaknya jumlah produksi komputer dan handphone yang masuk dan beredar di Indonesia sehingga menyebabkan makin lama harga kedua perangkat tadi menjadi semakin lebih murah, banyak masyrakat Indonesia akhirnya mampu unutk membeli dan menggunakan komputer dan/atau *handphone*. Bahkan banyak orang di Indonesia yang memiliki lebih dari satu handphone. Komputer pun tidak lagi menjadi barang mahal seiring dengan kehadiran komputer jenis *netbook*. Bahkan banyak harga *handphone* ternyata pada saat ini lebih mahal dibandingkan dengan harga *netbook*. Hampir setiap orang, baik pelajar maupun dewasa sudah memiliki *handphone*, baik itu *handphone* lokal maupun yang *branded*.

Dengan makin banyaknya masyarakat Indonesia yang memiliki dan menggunakan komputer dan *handphone*, maka akan semakin banyak barang bukti elektronik yang akan dihadapi oleh *investigator* di dalam menangani suatu kasus kejahatan. Barang bukti elektronik berupa komputer dan/atau *handphone* tersebut bisa berasal dari tersangka maupun saksi. Barang bukti tersebut juga bisa berasal dari *computer crime* maupun *computer-related crime*. *Computer crime* merupakan kejahatan yang menggunakan komputer sebagai alat utama untuk melakukan aksi kejahatannya, misalnya *defacement* (pengubahan halaman-halaman suatu situs secara ilegal), *denial distributed of service* (membuat suatu sistem tidak berjalan atau berfungsi sebagaimana mestinya setelah dibanjiri data oleh sekian banyak komputer yang telah terinfeksi dan menjadi *robot network*), *keylogging* (merekam setiap aktifitas pengetikkan di *keyboard* dan aplikasi yang tertampil di layar), *identity theft* (pencurian data-data penting dari orang-orang yang menjadi target), *intrusion* (masuk secara ilegal ke dalam suatu sistem), dan lain-lain. Sedangkan *computer-related crime* adalah segala jenis macam kejahatan tradisional seperti pencurian, pornografi, perampokan, pembunuhan, korupsi, narkoba dan lain-lain di mana di dalam kejahatan tersebut terdapat barang bukti elektronik seperti komputer dan *handphone* yang digunakan oleh pelaku untuk saling berkomunikasi dengan yang lain, atau menyimpan data-data yang berkaitan dengan perencanaan, proses dan hasil kejahatannya.

Seperti yang telah dijelaskan sebelumnya bahwa untuk menangani barang bukti elektronik tersebut dibutuhkan bentuk spesialisasi komputer forensik. Di awal tahun 2000an, penulis sempat kesulitan untuk mendalami bidang ini dikarenakan tidak satupun universitas di Indonesia yang menyelenggarakan mata kuliah ataupun program pasca sarjana di bidang ini, bahkan hingga saat ini. Satu-satunya cara pada saat itu adalah belajar secara otodidak melalui internet dan buku-buku berbahasa Inggris yang penulis beli ketika ada beberapa kali kesempatan ke luar negeri, serta bertanya kepada orang yang memahami bidang ini. Permasalahan yang juga dihadapi penulis saat itu adalah sulitnya untuk mendapatkan orang yang benar-benar memahami digital forensik secara teoritis dan praktis. Di Puslabfor Bareskrim Polri (Pusat Laboratorium Forensik), penulis sering berdiskusi pada tataran teoritis dengan pimpinan yang kebetulan juga mengetahui tentang

digital forensik, yaitu Kombes Pol Saman Azhari, ST., Msi. Selanjutnya penulis mempersiapkan diri sendiri secara teoritis dan praktis di bidang ini, termasuk memahami prinsip-prinsip dasar dan prosedur pelaksanaan digital forensik, karena yang terpenting dalam digital forensik itu adalah prinsip dasar dan prosedur, baru kemudian *hardware* (perangkat keras) dan *software* (perangkat lunak) yang dibutuhkan. *Hardware/software* hanyalah sekedar *tool* (alat) untuk memeriksa barang bukti elektronik, namun inti pemeriksaan itu sendiri adalah prosedur yang benar dan sesuai dengan prinsip dasar dan kaidah internasional.

Pada tahun 2006, akhirnya untuk pertama kali penulis memberanikan diri untuk menerima pemeriksaan barang bukti elektronik dari 3 kasus *computer-related crime* antara lain kasus korupsi, dilanjutkan di tahun 2007 juga sebanyak 3 kasus, antara lain kasus *computer crime*, yaitu penyadapan *email* (surat elektronik) di hotel bintang lima di Jakarta dan kasus ancaman bom di situs pemerintah propinsi D. I. Yogyakarta. Pada tahun ini, penulis akhirnya memutuskan untuk mengambil sertifikasi komptensi internasional di bidang digital forensik, yaitu *Computer Hacking Forensic Investigator* (CHFI) dari EC-Council, yang merupakan lembaga sertifikasi internasional untuk kompetensi dan profesionalitas di bidang ilmu pengetahuan dan teknologi komputer. EC-Council yang berbasis di Amerika Serikat ini juga memiliki program pasca sarjana MSS, yaitu *Master of Security Science* di EC-Council *University*. CHFI merupakan sertifikasi bidang digital forensik yang diakui oleh dunia internasional. Untuk mendapatkan sertifikasi tersebut, harus mengikuti pelatihan yang bersifat *advanced* (level lanjutan) selama 5 hari, kemudian mengikuti ujian *online* dan harus lulus dari ujian *online* tersebut dengan nilai minimal 70. Jika di bawah nilai tersebut, maka gagal untuk mendapatkan sertifikat CHFI.

Dengan adanya CHFI, penulis mendapatkan pengakuan akademik internasional di bidang digital forensik dan *hacking* sehingga lebih dapat diterima di persidangan sebagai saksi ahli. Analogi terhadap hal ini adalah seorang sopir bus angkutan umum yang ahli membawa bus, namun tidak memiliki SIM (surat ijin mengemudi). Ketika dalam suatu razia resmi, ia diberhentikan oleh petugas polisi pengatur lalu lintas, maka akan sangat mungkin ia akan ditilang oleh polisi tersebut dikarenakan tidak memiliki SIM. Begitu juga bagi ahli digital forensik

yang tidak memiliki sertifikasi resmi bidang digital forensik akan sangat mungkin tidak dapat diterima pembuktiannya secara hukum di persidangan.

Di tahun 2008 jumlah kasus yang ditangani meningkat menjadi 7 kasus antara lain *computer-related crime* yaitu kasus pornografi di Bukit Tinggi dan demonstrasi anarkis di Jakarta. Di tahun ini juga, penulis mendapatkan sertifikasi CEI (*Certified EC-Council Instructor*) dan kemudian berhasil melakukan pengkaderan *digital forensic analyst/investigator* di lingkungan Puslabfor dan Labfor Cabang se Indonesia. Penulis menjadi instruktur pada kelas CHFI untuk Labfor dan berhasil meluluskan 8 orang untuk mendapatkan sertifikat CHFI. Di bulan September 2008, penulis berangkat ke Inggris untuk mengambil program pasca sarjana MSc di bidang *Forensic Informatics* dari *University of* Strathclyde. Penulis mengambil program tersebut setelah berhasil lulus seleksi beasiswa Chevening yang berasal dari *Foreign and Commonwealth Office* (FCO) pemerintahan Inggris. Pada program pasca sarjana ini, penulis banyak mendalami digital forensik melalui pendekatan *platform* Linux, di samping *anti-forensic* seperti *cryptography* dan *steganography*. Bahkan penulis mendapatkan nilai *distinction* untuk disertasi yang mengupas tentang *steganography forensic* dengan pendekatan analisa metada untuk deteksi file-file steganography.

Setelah menyelesaikan program master di tahun 2009, penulis kembali ke Indonesia walaupun pada saat itu ada beberapa tawaran untuk bekerja sebagai sen*ior digital forensic analyst* di London dengan gaji yang menggiurkan. Penulis berkeinginan untuk mengembangkan digital forensik di Indonesia, tidak hanya di lingkungan penegak hukum, namun juga di kampus-kampus dan lembaga-lembaga lain di luar Polri. Pada tahun ini, jumlah kasus yang ditangani meningkat menjadi 15 kasus, antara lain *computer-related crime*, yaitu kasus pembunuhan dan jaringan narkoba.

Akhirnya pada tanggal 18 Januari 2010, terbentuklah DFAT (*Digital Forensic Analyst Team*) di Puslabfor melalui surat perintah Kepala Puslabfor sebagai wadah fungsional untuk pemeriksaan digital forensik. DFAT yang berada di bawah Departemen Fisika dan Komputer Forensik merupakan tim kecil yang kemudian keanggotaannya diperbaharui kembali di tahun 2011. DFAT dipimpin oleh penulis sejak awal berdiri dengan anggotanya adalah Donny Zulianto, Hasta Saputra dan

Ahmad Pahmi yang merupakan orang-orang yang memiliki hobi komputer dan kepedulian yang sama untuk pengembangan digital forensik di Labfor. Pada tahun 2010, jumlah kasus yang diperiksa oleh DFAT meningkat sangat signifikan menjadi 52 kasus dengan barang bukti elektronik berjumlah 214 item. Sebagian besar dari barang bukti elektronik tersebut adalah *handphone* dan komputer. Dari 52 kasus tersebut, kasus-kasus nasional yang ditangani adalah kasus pembajakan CD/DVD di Tangerang, pembobolan kartu ATM di Bali dan Jakarta, judi online internet di Jakarta, penyuapan di Jakarta dan video porno yang melibatkan selebriti papan atas di Jakarta.

Selain melakukan pemeriksaan dan analisa barang bukti elektronik di tahun 2010, penulis beserta tim DFAT juga melaksanakan kegiatan penelitian di bidang audio forensik dengan fokus penelitian tentang *voice recognition* untuk kasus *pitch shift*. Di samping itu, penulis juga beberapa kali hadir di persidangan sebagai saksi ahli untuk menjelaskan proses pemeriksaan digital forensik beserta hasilnya dari kasus-kasus yang ditangani.

Pada tahun 2011, kembali terjadi peningkatan jumlah barang bukti elektronik yang diperiksa dan dianalisa menjadi lebih dari 250 item yang berasal dari 56 kasus sampai di akhir Desember 2011. Masih sama seperti di tahun 2010, sebagian besar barang bukti elektronik yang diperiksa berupa *handphone* dan komputer. Adapun kasus-kasus nasional yang sempat ditangani adalah kasus pencurian identitas di Jakarta, kekerasan di Pandeglang, pemalsuan surat di Jakarta dan kasus narkoba di Jakarta. Kesibukan penulis juga semakin bertambah dengan banyaknya permintaan untuk *sharing* (berbagi) ilmu dan pengalaman di bidang digital forensik, misalnya dari UNODC (*United Nations Office on Drugs and Crime*), EC-Council, KPK (Komisi Pemberantasan Korupsi), Badiklat Kejagung (Badan Pendidikan dan Pelatihan Kejaksaan Agung), Universitas Paramadina dan Universitas Indonesia. Malah di Universitas Indonesia, penulis diminta oleh Prof. Adrianus Meliala untuk menjadi dosen yang mengajar mata juliah *Cryptography* dan *Information Security*.

Kinerja tahun 2010-2011

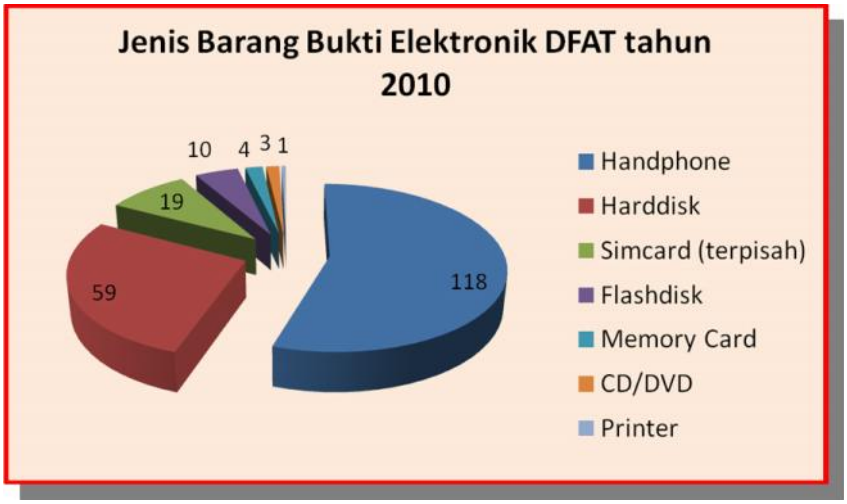
Seperti yang telah dijelaskan sebelumnya bahwa ada peningkatan jumlah kasus dan barang bukti elektronik yang ditangani oleh penulis beserta tim DFAT. Mulai hanya 3 kasus di tahun 2006 dan 2007, kemudian merangkak naik menjadi 7 dan 15 kasus di tahun 2008 dan 2009. Di tahun 2010 terjadi peningkatan yang sangat signifikan baik jumlah kasus maupun barang bukti elektronik, yaitu menjadi 52 kasus dengan total barang bukti 214 item. Hal ini berlanjut di tahun 2011, di mana barang bukti elektronik yang diperiksa dan dianalisa hingga di awal Desember 2011 berjumlah lebih dari 400 item yang berasal dari 55 kasus. Menariknya dari sebagian besar kasus-kasus besar yang diekspos oleh media secara nasional, barang bukti elektroniknya diperiksa di DFAT. Ini menunjukkan adanya pengakuan secara teoritis dan praktis DFAT di bidang investigasi digital forensik, yaitu melakukan pemeriksaan dan analisa barang bukti elektronik untuk mendapatkan bukti-bukti digital yang diakui secara hukum untuk menjerat pelaku. Gambar berikut menunjukkan kinerja DFAT di tahun 2010.



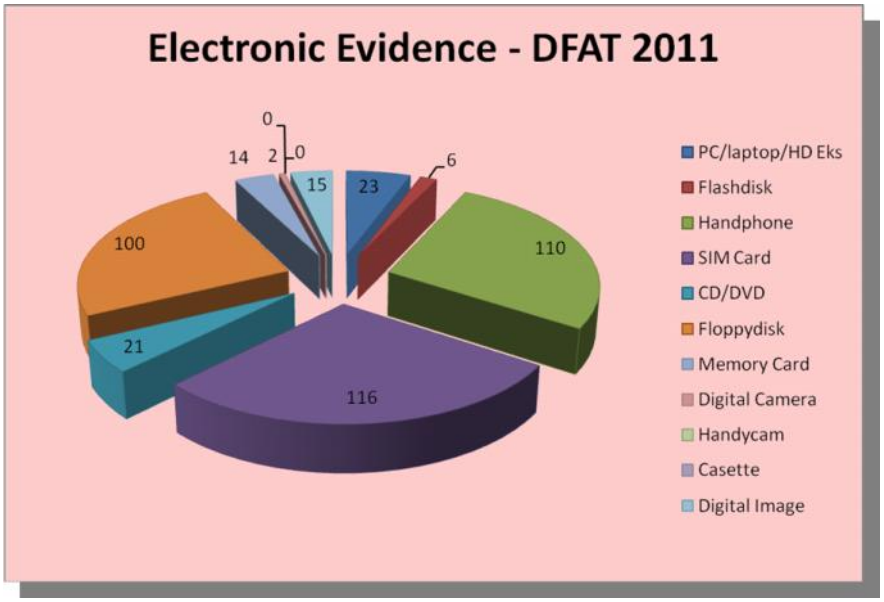
Gambar I.3. Jumlah kasus yang ditangani DFAT Puslabfor mulai dari tahun 2006 hingga 2011 dengan peningkatan yang signifikan di tahun 2010 yang kemudian diikuti di tahun 2011.

Jenis-jenis barang bukti elektronik yang diperiksa di tahun 2011 hampir sama seperti di tahun 2010 seperti yang terlihat di Gambar I.4 dan I.5, di mana porsi terbesarnya berupa *handphone* dan komputer, yang dalam hal ini adalah *harddisk*.

Namun ada juga item barang bukti yang jumlahnya lumayan signifikan yang ditahun-tahun sebelumnya tidak ada, yaitu *floppy disk*. Menariknya *floppy disk* tersebut hanya berasal dari satu kasus nasional, yaitu kasus korupsi.



Gambar I.4. Jenis-jenis barang bukti elektronik yang ditangani DFAT di tahun 2010 dengan porsi terbesarnya adalah *handphone* dan harddisk komputer.



Gambar I.5. Jenis barang bukti elektronik yang diperiksa dan dianalisa oleh tim DFAT di tahun 2011

Di tahun 2011, terdapat lebih bervariasinya jenis barang bukti digital yang diperiksa dan dianalisa yaitu adanya rekaman suara, video dan gambar digital. Barang bukti file rekaman suara berasal dari alat perekam digital dan hasil

penyadapan telepon, sedangkan rekaman video berasal dari kamera cctv, *handphone* dan *handycam*. Adapun file gambar digital barang bukti berasal dari internet.

Di samping pemeriksaan dan analisa barang bukti elektronik dan digital, penulis seringkali mendapatkan panggilan sebagai saksi ahli dipersidangan di tahun 2010 dan 2011 dibandingkan dengan tahun-tahun sebelumnya. Semakin seringnya dipanggil sebagai saksi ahli, secara tidak langsung akan berdampak semakin banyak hakim yang dapat memahami pentingnya keberadaan bukti digital yang akhirnya nanti dapat diterima sebagai alat bukti hukum yang syah.

Faktor-faktor yang mempengaruhi

Dari penjelasan di atas, diketahui bahwa digital forensik merupakan salah bidang spesialisasi ilmu pengetahuan dan teknologi komputer yang memiliki posisi signifikan untuk melakukan investigasi kasus-kasus *computer crime* dan/atau *computer-related crime*. Digital forensik juga harus didukung oleh bidang-bidang spesialisasi yang lain seperti *programming*, *networking*, *information management*, *information security*, *penetration testing* dan *hacking* agar pengimplementasian digital forensik dalam suatu investigasi dapat dilaksanakan secara komprehensif. Digital forensik sebaiknya mengikuti perkembangan ilmu pengetahuan dan teknologi informasi dan komputer, agar digital forensik selalu *updated*, tidak ketinggalan zaman. Untuk tumbuh-kembangnya digital forensik dapat berjalan dengan baik seperti yang diharapkan, maka beberapa faktor yang mempengaruhinya harus juga ikut didesain untuk mendukung digital forensik. Secara umum ada 4 faktor utama yang mempengaruhi perkembangan digital forensik, yaitu :

1. **Manajemen**

   Yang paling utama dari semua faktor tersebut adalah manajemen. Dalam hal ini, manajemen berkaitan dengan pimpinan perusahaan atau lembaga penegak hukum. Dibutuhkan pimpinan yang memiliki keinginan kuat untuk memajukan digital forensik di tempatnya masing-masing. Tidak hanya sekedar

retorika, namun semua hal yang dibutuhkan di dalam perkembangan digital forensik seperti penyiapan kualitas sumber daya manusia dan pengadaan *hardware/software* yang sering berbiaya mahal dapat diimplementasikan.

Manajemen memegang peranan penting yang kedua dikarenakan dengan manajemen yang baiklah, seorang *forensic analyst* dapat lebih fokus dan memaksimalkan kemampuannya untuk melakukan pemeriksaan dan analisa digital forensik. Jika manajemen yang ada tidak mendukung, maka hal ini akan menyulitkan seorang *forensic analyst* untuk mengembangkan kemampuan dan potensi dirinya di bidang digital forensik. Misalnya untuk mengikuti pelatihan-pelatihan yang bersifat *professional certification* yang mahal di mana hal ini tidak didukung oleh manajemen, maka *forensic analyst* akan mendapatkan kesulitan, atau bahkan tidak dapat mengikuti pelatihan tersebut. Jika ini terjadi, maka amat disayangkan, karena ujung tombak dari digital forensik itu adalah sumber daya manusianya yang harus selalu meng-*update* dirinya dengan kemajuan dan perkembangan teknologi komputer.

Hal yang sama ketika membahas *hardware/software* yang lumayan mahal untuk kegiatan pemeriksaan dan analisa digital forensik. Jika ini juga tidak didukung oleh manajemen, artinya *forensic analyst* terpaksa menggunakan hardware/software seadanya atau bahkan ketinggalan zaman, maka hasil pemeriksaan dan analisa bisa dipastikan tidak dapat maksimal (tidak efektif) dan berjalan lebih lambat (tidak efisien).

Berdasarkan penjelasan di atas, berkembangnya kemampuan digital forensik tidak terlepas dari peranan manajemen yang mengatur dan menyediakan pelatihan/pendidikan dan *hardware/software* yang memadai dan sesuai dengan perkembangan ilmu pengetahuan dan teknologi komputer. Di samping itu, manajemen juga sebaiknya memiliki perencanaan strategis untuk perkembangan digital forensik ke depannya, misalnya perencanaan tahunan, 5 tahun dan 10 tahun, sehingga digital forensik yang dipimpinnya senantiasa dapat mengikuti perkembangan zaman. Di dalam perencanaan tersebut, manajemen sudah bisa memprediksi apa yang terjadi ke depannya, dan apa yang harus dilakukan untuk menyikapi perkembangan tersebut dengan meningkatkan atau melakukan perubahan sumber daya yang ada.

2. Prosedur

Faktor penting yang kedua adalah prosedur pemeriksaan dan analisa digital forensik yang mengikuti dan mengacu kepada prinsip-prinsip dasar dan *guidelines* (petunjuk) internasional, misalnya *Good Practice Guide for Computer-Based Electronic Evidence*, yang dikeluarkan oleh ACPO (*Association of Chief Police Officers*) yang bekerjasama dengan 7Safe dan *Forensic Examination of Digital Evidence: Guide for Law Enforcement*, yang dikeluarkan oleh *National Institute of Justice* yang berada di bawah US *Department of Justice.*

Pentingnya prosedur yang dibakukan ke dalam *Standard Operating Procedure* (SOP) adalah untuk memastikan bahwa proses pemeriksaan dan analisa barang bukti elektronik dan digital sudah sesuai dengan prinsip-prinsip dasar digital forensik secara internasional sehingga output pemeriksaan yang berupa temuan-temuan digital dapat diterima sebagai alat bukti hukum yang syah di persidangangan. Jangan sampai pemeriksaan dan analisa sudah dilaksanakan dan memakan waktu yang cukup lama, namun ternyata temuan digital yang dihasilkan tidak dapat diterima oleh majelis hakim di persidangan dikarenakan tidak memenuhi prinsip-prinsip dasar tersebut.

Prosedur ini juga berkaitan dengan Undang-Undang yang berlaku di suatu negara, misalnya di Indonesia, ada Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Di dalam Undang-Undang ini dijelaskan dalam pasal 5 bahwa *informasi elektronik dan dokumen elektronik merupakan alat bukti hukum yang syah*, namun juga dijelaskan bahwa informasi elektronik dan dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini. Di pasal 6 juga dijelaskan bahwa informasi elektronik dan dokumen elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan. Prosedur yang diterapkan di bidang digital forensik oleh *forensic analyst* di Indonesia juga seharusnya mengikuti ketentuan di Undang-Undang ini yang

mensyaratkan bahwa data digital yang menjadi barang bukti digital yang berasal dari barang bukti elektronik harus dapat diakses, ditampilkan, dijamin keutuhannya dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan. Jadi menurut Undang-Undang ini, ada 4 (empat) syarat untuk diterimanya data digital sebagai alat bukti hukum yang syah, yaitu :

1) Dapat diakses
2) Dapat ditampilkan
3) Dijamin keutuhannya
4) Dapat dipertanggungjawabkan

Prosedur dari SOP digital forensik yang dijalankan di Indonesia haruslah dapat memenuhi keempat syarat tersebut untuk data digital yang dihasilkannya.

3. Sumber daya manusia

Ada filosofi lama yang senantiasa cocok dengan perkembangan zaman, yaitu '*THE MAN BEHIND THE GUN*'. Artinya sumber daya manusia didahulukan dibandingkan dengan peralatan atau persenjataannya. Peralatan yang canggih, misalnya komputer digital forensik yang lengkap tidak akan berarti atau banyak manfaatnya jika petugasnya tidak mampu dan menguasai peralatn itu dengan baik, sehingga jadilah peralatan yang canggih dan mahal tersebut menjadi sia-sia. Sebaliknya dengan peralatan yang cukup dan terbatas, namun jika itu digawangi oleh petugas yang professional dan memiliki kompetensi yang tinggi, maka peralatan tersebut dapat berdaya guna lebih maksimal dibandingkan yang pertama.

Untuk mendapatkan kualitas sumber daya manusia yang professional, maka petugas tersebut harus mendapatkan pelatihan-pelatihan (yang bersifat *professional certification* seperti yang dijelaskan sebelumnya) yang selalu kontinu di bidang digital forensik, atau bahkan mengambil pendidikan formal di bidang ilmu komputer, teknologi informasi atau digital forensik, baik di strata satu (S1), maupun pasca sarjana (S2 dan S3). Diharapkan melalui pelatihan-pelatihan *professional certification* dan pendidikan-pendidikan formal tersebut, petugas tersebut memiliki kompetensi dan professional yang jelas untuk menjadi seorang *forensic analyst* yang dapat diandalkan. Ketika di

dalam pemeriksaan dan analisa barang bukti elektronik mengalami kendala atau permasalahan, maka ia dapat menjelaskannya secara ilmiah dan mencari solusi untuk mengatasinya dengan metode yang dapat dipertanggungjawabkan. Arti yang lain adalah seorang *forensic analyst* tidak hanya sekadar operator *hardware/software*, namun ia memiliki posisi lebih dari itu. Ia menguasai ilmu pengetahuan dan teknologi di bidang digital forensik, baik secara teori dan praktis, sehingga ketika nanti ia diminta untuk mempertanggungjawabkan hasil pemeriksaan dan analisa di depan pengadilan, ia mampu melakukannya dengan baik.

4. Hardware/software

Hardware/software merupakan alat yang dibutuhkan oleh *forensic analyst* dan *investigator* dalam melaksanakan tugasnya untuk memeriksa dan menganalisa barang bukti elektronik/digital. Jika *hardware/software* yang digunakan adalah versi yang terkini dan sesuai dengan peruntukannya, maka hasil pemeriksaan dan analisa dapat lebih maksimal, apalagi kalau itu digunakan oleh petugas yang *professional* dan lebih terlatih (*well-trained* dan *well-educated*). Untuk itu, seorang *forensic analyst sebaiknya* tidak tergantung pada *hardware/software* tertentu, karena jika itu dilakukan, kemudian *hardware/software* tersebut terdapat masalah, maka dapat dipastikan *forensic analyst* tersebut tidak dapat menjalankan tugasnya dengan baik untuk memeriksa dan menganalisa barang bukti elektronik/digital.

Ada filosofi teknis yang berkaitan dengan *hardware/software*, yaitu '*NO SYSTEM IS PERFECT*', artinya tidak ada sistem, dalam hal ini adalah *hardware/software* yang sempurna. Semua aplikasi memiliki kelebihan dan kekurangan masing-masing, oleh karena itu *forensic analyst* dan *investigator* sebaiknya memiliki banyak aplikasi yang dapat digunakan untuk pemeriksaan dan analisa. Jika pada aplikasi yang satu, ia tidak mendapatkan hasil yang diinginkan, maka ia bisa mencoba menggunakan aplikasi yang lain hingga mendapatkan data digital yang diharapkan. Untuk itu, *forensic analyst* dan *investigator* seharusnya memiliki aplikasi-aplikasi yang berjalan di *platform* yang berbeda, misalnya sistem operasi Microsoft Windows dan Linux

(misalnya *distro* Ubuntu). Pada beberapa hal, *forensic analyst* dan *investigator* dapat menggunakan aplikasi-aplikasi digital forensik yang berbasis Windows, namun pada beberapa kesempatan yang lain, ia seharusnya juga mampu menggunakan aplikasi-aplikasi forensik yang berbasis Linux. Masing-masing *platform* memiliki kelebihan dan kekurangannya masing-masing, sehingga berefek kepada aplikasi-aplikasi yang dipakai.

Berikut antara lain aplikasi yang berbasis Windows yang digunakan untuk kepentingan digital forensik :

1) EnCase dari *Guidance Software* yang dapat diakses di www.guidancesoftware.com, untuk *forensic imaging* dan analisa data digital yang komprehensif, termasuk *lost file recovery*.
2) *Forensic Toolkit* (FTK) dari AccessData yang dapat diakses di www.accessdata.com, untuk analisa data digital yang komprehensif, termasuk *lost file recovery*.
3) FTK *Imager* dari AccessData, untuk *forensic imaging* dan *logical preview/mounting* terhadap *image file*.
4) WinHex dari X-Ways yang dapat diakses di www.x-ways.net, untuk *forensic imaging*, *logical preview/mounting* terhadap *image file*, *keyword searching* berbasis sektor (*low level recovery*) dan *lost file recovery*.
5) Mobiledit *Forensic* dari Compelson yang dapat diakses di www.mobiledit.com, untuk memeriksa dan menganalisa *handphone*/*smartphone* secara mobile forensik.
6) *Mount Image Pro* dari GetData yang dapat diakses di www.getdata.com, untuk melakukan proses *mounting* (me-*restore*) terhadap *image file* secara *logical* dan *physical*.
7) *Recover My Files* dari GetData, untuk *files recovery*, baik *logical* (untuk *deleted files*), maupun *physical* (untuk *lost files*), termasuk juga partisi.

   Sebagian besar aplikasi-aplikasi yang berbasis Windows merupakan aplikasi berbayar dan menampilkan GUI (*Graphical User Interface*) yang menarik dan mudah untuk digunakan.

Berikut adalah aplikasi-aplikasi berbasis Linux, dalam hal ini adalah *distro* Ubuntu yang dapat digunakan untuk kegiatan digital forensik :

1) *The* Sleuthkit (TSK), untuk analisa komprehensif terhadap suatu *image file*, termasuk *deleted files recovery* dan pencarian konten per sektor.
2) Autopsy, merupakan GUI berbasis *browser* dari The Sleuthkit.
3) dcfldd, untuk *forensic imaging* sekaligus proses *hashing*
4) dd, untuk proses *forensic imaging*
5) guymager, untuk *forensic imaging* sekaligus proses *hashing* dan verifikasi.
6) foremost, untuk *files recovery* termasuk *deleted* dan *lost files*, yang berbasis *sector scanning* dengan melihat *signature* dari masing-masing format *file*.
7) Phatch, untuk melihat metadata exif (*Exchangeable Image File Format*) dari file foto, bahkan mampu untuk digunakan proses editing data exif tersebut.
8) exiftool, untuk me-*recover* data exif dari suatu file fotografi.

Hampir semua aplikasi-aplikasi berbasis Linux merupakan perintah *command line* yang dijalankan lewat terminal, dan bersifat *open source* yang *freeware* (tidak berbayar).

Satu hal yang pasti, sebelum menggunakan aplikasi forensik, sebaiknya *forensic analyst* dan *investigator* sudah memahami cara kerja dan output yang dihasilkan dari aplikasi itu. Di samping itu, aplikasi tersebut sebaiknya juga diakui oleh dunia internasional dan dapat diterima eksistensinya secara hukum di pengadilan.

Bab II

DIGITAL FORENSIC: Principles and Procedures

Seperti yang telah dijelaskan pada bab sebelumnya bahwa salah satu bidang ilmu pengetahuan yang berkembang dengan sangat pesat adalah bidang komputer di mana dalam hitungan hari, minggu, bulan atau tahun status ilmu pengetahuan dan teknologi komputer akan menampilkan wajah yang berbeda dengan sebelumnya. Perkembangan ini menghasilkan dua wajah yang juga berbeda tergantung pemanfaatannya, yaitu sisi positif dan sisi negatif. Untuk sisi positif, kemajuan terseebut digunakan untuk membantu kehidupan manusia agar lebih interaktif, efisien dan efektif dengan dukungan teknologi komputer yang canggih, sedangkan untuk sisi negatif, kemajuan tersebut dapat disalahgunakan untuk berbuat kejahatan yang juga semakin canggih. Ketika pelaku kejahatan memiliki level pemahaman ilmu pengetahuan dan teknologi di bidang komputer yang cukup tinggi, maka ia akan semakin mudah untuk mencari kelemahan-kelemahan dari suatu sistem elektronik ataupun non-elektronik dikarenakan tidak ada sistem yang sempurna (*NO SYSTEM IS PERFECT*), untuk kemudian dieksploitasi oleh dirinya atau kelompoknya dalam rangka melakukan kejahatan yang bisa bermotif keuntungan finansial, politik, keamanan dan lain-lain. Kejahatan ini dikenal dengan istilah *computer crime* seperti yang sempat disinggung pada Bab I. Semakin canggih teknologi yang diimplementasikan dalam kejahatan ini, maka efek kejahatannya seperti tingkat kerugian baik waktu, uang dan fasilitas lain akan semakin besar, bahkan akan semakin sulit bagi para penegak hukum untuk melakukan investigasi kejahatan tersebut atau melacak keberadaan pelakunya, atau bahkan kejahatan tersebut akan menjadi *The X Files*, artinya kasus-kasus yang sulit untuk diungkap.

Agar dapat melakukan investigasi yang benar terhadap *computer crime* tersebut, sehingga kejahatan tersebut dapat terungkap, maka diperlukan sisi positif dari kemajuan bidang komputer, yaitu aplikasi ilmu pengetahuan dan teknologi komputer untuk memeriksa dan menganalisa setiap barang bukti elektronik dan barang bukti digital dalam rangka melihat keterkaitan antara bukti digital yang satu dengan yang lain, sehingga kejahatan tersebut dapat menjadi terang dan keberadaan pelaku dapat dilacak

untuk kemudian ditangkap untuk mempertanggungjawabkan kejahatannya. Aplikasi tersebut dikenal dengan istilah digital forensik seperti yang telah dijelaskan pada bab sebelumnya. Ada juga istilah lain yang pengrtiannya tidak jauh berbeda yaitu *computer forensic* dan informatika forensik.

Digital forensik ini merupakan salah satu bidang spesialisasi dari pemahaman komputer yang sangat luas. Tidak ada seorang ahli komputer pun yang dapat memahami bidang komputer secara detil dari A sampai Z (*NOBODY IS PERFECT*), karena bidang komputer ini sangat luas. Untuk itu diperlukan adanya spesialisasi-spesialisasi di bidang komputer ini. Seperti yang dijelaskan di Bab I, spesialisasi-spesialisasi tersebut dapat dikategorikan, antara lain sebagai berikut :

1. *Programming*
2. *Networking*
3. *Website Developing*
4. *Information Management*
5. *Information Security*
6. *Penetration Testing*
7. *Hacking*
8. Digital Forensik

Oleh karena itu, sebaiknya seorang ahli di bidang komputer mengambil satu atau beberapa bentuk spesialisasi agar dirinya dapat lebih fokus dalam aplikasi ilmu pengetahuan dan komputer. Bentuk spesialisasi yang cocok dalam melakukan investigasi kejahatan komputer atau kejahatan yang berkaitan dengan komputer (*computer-related crime*) adalah digital forensik. Digital forensik ini akan memeriksa setiap barang bukti elektronik dalam rangka mencari keping-keping data digital yang mengkaitkan kejahatan tersebut dengan pelakunya. Untuk itu, seorang ahli digital forensik sebaiknya juga paham meskipun tidak detil mengenai bidang-bidang spesialisasi yang lain, misalnya *networking*, *information security* dan *hacking* dalam rangka mendukung kegiatan pemeriksaan dan analisa digital forensik secara komprehensif.

Tulisan ini akan membahas digital forensik secara umum. Hal ini dimaksudkan agar seorang yang ingin terjun menjadi ahli digital forensik dapat memahami dengan jelas apa dan bagaimana tentang digital forensik. Mereka diharapkan tidak hanya menjadi

operator *software/hardware* di level aplikasi, namun juga paham level dasar dari digital forensik itu sendiri, yaitu prinsip dasar dan prosedur.

Prinsip dasar dan prosedur dalam digital forensik memegang peranan penting untuk mengarahkan pemeriksaan digital forensik untuk tetap berada pada jalur yang benar. Memiliki *hardware/software* forensik, namun tidak memahami tentang prinsip dasar dan prosedur digital forensik, maka bisa jadi ia akan melangkah ke arah yang salah dalam pemeriksaan digital forensik itu sendiri. Analogi untuk hal ini adalah penggunaan senjata. Seseorang memiliki senjata yang canggih, namun ia tidak paham prosedur bagaimana cara menggunakannya dengan benar, maka ia tidak akan maksimal menggunakannya, malah bisa jadi senjata itu akan mencelakakan dirinya atau orang lain. Hal ini diharapkan tidak terjadi di dalam dunia digital forensik. Untuk itu bab ini sebagian akan membahas prinsip dasar dan prosedur yang berkaitan dengan digital forensik.

Prinsip-prinsip Dasar Digital Forensik

Hal yang sangat mendasar untuk dipahami oleh seorang ahli digital forensik adalah prinsip-prinsip dasar digital forensik itu sendiri. Ada banyak *guidelines* di dunia internasional yang membahas ini, yang kebanyakan di antara mereka disponsori oleh pemerintah, dalam hal ini penegak hukum sebagai acuan bagi aparatnya di dalam bertindak yang benar dan prosedural di dalam melakukan investigasi *computer crime* dan *computer-related crime*, serta memeriksa dan menganalisa barang bukti. Di antara sekian banyak *guidelines* tersebut, ada beberapa yang sering menjadi acuan para profesional digital forensik karena lebih diterima dan aplikatif, yaitu :

1. *Good Practice Guide for Computer-Based Electronic Evidence*, yang dikeluarkan oleh ACPO (*Association of Chief Police Officers*) yang merupakan asosiasi para pimpinan kepolisian di Inggris, yang bekerjasama dengan 7Safe.
2. *Forensic Examination of Digital Evidence: Guide for Law Enforcement*, yang dikeluarkan oleh *National Institute of Justice* yang berada di bawah *US Department of Justice.*

3. *Electronic Crime Scene Investigation: A Guide for First Responders*, yang juga dikeluarkan oleh *National Institute of Justice* yang berada di bawah *US Department of Justice.*

Menurut pendapat penulis, ACPO termasuk lembaga pemerintah di bidang penegakan hukum yang sangat jelas menyatakan prinsip-prinsip dasar digital forensik seperti yang dikutip dari *guidelines* di atas, sebagai berikut (ACPO, p4) :

1. *No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court*.
2. *In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions*.
3. *An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result*.
4. *The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to*.

Penjelasan prinsip dasar no. 1 :

Sebuah lembaga penegak hukum dan/atau petugasnya dilarang mengubah data digital yang tersimpan dalam suatu media penyimpanan elektronik yang selanjutnya akan dibawa dan dipertanggungjawabkan di pengadilan.

Sebuah media penyimpanan seperti *harddisk*, *floppy disk* dan *flashdisk* yang merupakan barang bukti harus dijaga keutuhannya sesuai dengan prinsip *chain of custody*. Ini dimaksudkan agar informasi digital yang tersimpan di media tersebut tetap ada dan terjaga keutuhannya hingga ia bisa dibawa ke pengadilan, serta bisa dipertanggungjawabkan asal-usulnya, khususnya dari kemungkinan adanya rekayasa data digital.

Seperti diketahui data digital bersifat *volatile*, artinya mudah sekali hilang atau rusak. Jika penanganan terhadap media penyimpanan tersebut tidak benar, maka data digital yang *volatile* sangat dimungkinkan akan hilang. Jika data yang sangat penting tersebut hilang dan bahkan tidak bisa di-*recovery* (dimunculkan kembali), maka aparat penegak hukum akan kesulitan untuk mengungkap kasus tersebut atau melacak dan menangkap pelaku. Karena sangat pentingnya setiap keping data digital yang ada, untuk itu lembaga penegak hukum dan petugasnya dilarang untuk mengubah data digital yang sudah tersimpan di media penyimpanan.

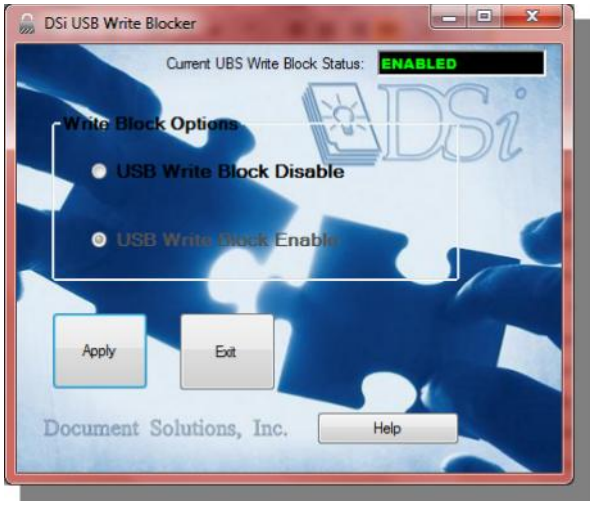
Untuk itu, seorang petugas penegak hukum, baik *investigator* maupun *forensic analyst* harus paham apa yang harus dilakukan dan urutan kerjanya ketika menemukan barang bukti elektronik pertama kali di TKP, maupun ketika dilakukan pemeriksaan lanjutan di laboratorium forensik. Diharapkan dengan terjaganya keutuhan barang bukti media penyimpanan secara digital dalam artian isi dari media penyimpanan tidak berubah, maka data digital yang dicari dan dapat mengungkap kejahatan dan keterlibatan pelaku tetap masih ada di dalam media penyimpanan tersebut.

Seiring dengan perkembangan ilmu pengetahuan dan teknologi komputer khususnya dalam hal anti-forensik seperti *cryptography* (yaitu suatu cabang dari ilmu pengetahuan komputer yang mendalami teknik-teknik penyandian/*encryption* dalam rangka pengamanan data-data digital dengan menggunakan algoritma matematika yang kompleks dan level *bit* yang tinggi), maka penanganan awal barang bukti komputer di TKP ketika ditemukan dalam keadaan hidup, investigator dan forensic analyst dapat diijinkan untuk melakukan *Triage* Forensik dalam rangka mendapatkan informasi digital yang penting dari barang bukti komputer tersebut seperti *encrypted container/files* yang dalam keadaan *decrypted*. Mengenai *Triage* Forensik akan dibahas detil pada Bab IV.

Bentuk implementasi lain dari prinsip dasar ini adalah penggunaan *write protect*, yaitu suatu metode forensik untuk mencegah terjadinya proses penulisan pada barang bukti elektronik ketika diakuisisi. Yang diizinkan terhadap akses barang bukti tersebut adalah proses membaca (*read-only*), sehingga apapun yang dilakukan oleh *forensic analyst* dan *investigator* terhadap barang bukti tersebut tidak akan mengubah isinya. Keutuhan isi dari barang bukti elektronik terjamin,

mulai dari proses *acquisition* (akuisisi) yang menghasilkan *image file* hingga proses pemeriksaan dan analisa secara langsung. *Write protect* ini dapat berbentuk *hardware* maupun *software*. Sebelum menggunakannya, *forensic analyst* sebaiknya sudah mencobanya terlebih dahulu untuk memastikan bahwa *write protect* yang diimplementasikan terhadap barang bukti benar-benar bersifat *forensically sound write protect*. *Forensically sound write protect* ini benar-benar penting karena hasil pemeriksaan/analisa yang berasal dari hal ini dapat diterima di sisi hukum.

Salah satu aplikasi *write protect* yang berbasis Windows dan sering digunakan oleh *forensic analyst* dan *investigator* adalah USB (*Universal Serial Bus*) *Write Blocker* dari *Document Solutions*. Aplikasi ini juga dapat diakses lewat situs *Forensic Focus*, yaitu suatu lembaga yang terkenal di dunia internasional yang membahas hal-hal yang berkaitan dengan digital forensik.



Gambar II. 1. *Screenshot* USB *Write Blocker* dari *Document Solutions*.

Aplikasi ini didesain untuk memproteksi *port* USB suatu komputer dari proses penulisan terhadap media penyimpanan seperti *harddisk* atau *flashdisk* yang terpasang pada *port* USB tersebut. Ini artinya media penyimpanan tersebut akan bersifat *read-only* ketika diakses, baik pada proses *acquisition* (yaitu akuisisi dengan metode *forensic imaging* yang menghasilkan *image file*) maupun pada proses pemeriksaan dan analisa, sehingga isi dari media penyimpanan tersebut

tidak akan berubah selama proses-proses tersebut. Ini sesuai dengan prinsip dasar digital forensik yang pertama.

Aplikasi ini berjalan di sistem *registry* dari sistem operasi Microsoft Windows dengan *support* (dukungan teknis) dari dotNet *Framework*, oleh karena itu jika aplikasi ini dijalankan di Windows XP, maka haruslah di-*install* terlebih dahulu dotNet *Framework* untuk menjalankan aplikasi ini di sistem operasi tersebut. Sedangkan untuk Windows Vista dan 7 yang sudah ada dotNet *Framework* secara *default*, maka aplikasi ini bisa langsung dijalankan.

Penjelasan prinsip dasar no. 2 :

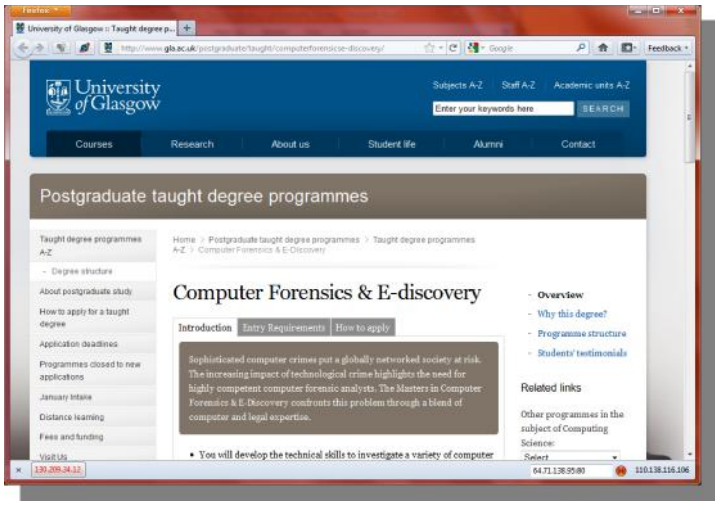
Untuk seseorang yang merasa perlu untuk mengakses data-data digital yang tersimpan di media penyimpanan barang bukti, maka orang tersebut harus benar-benar jelas kompetensinya dan dapat menjelaskan relevansi dan implikasi dari tindakan-tindakan yang ia lakukan selama pemeriksaan dan analisa barang bukti tersebut.

Ini menjelaskan bahwa *investigator* dan *forensic analyst* yang akan memeriksa dan menganalisa media penyimpanan barang bukti harus memiliki kompetensi yang jelas. Kompetensi ini bisa dimiliki oleh *investigator* dan *forensic analyst* lewat baik jalur formal maupun non-formal. Formal di sini adalah mereka harus mengikuti jalur pendidikan yang jelas di universitas seperti pendidikan strata satu (S1) bidang ilmu pengetahuan komputer dan/atau pasca sarjana (S2 dan S3) di bidang komputer yang lebih spesifik seperti MSc di bidang *Forensic Informatics* dari *University of* Strathclyde di Inggris atau MSc di bidang *Computer Forensics and E-discovery* dari *University of* Glasgow, Inggris. Pendidikan formal pasca sarjana yang fokus di bidang digital forensik ini sangat sedikit dibandingkan bidang-bidang spesialisasi komputer yang lain. Di Indonesia sendiri, sampai saat ini belum ada program pasca sarjana yang diselenggarakan universitas-universitas di Indonesia yang fokus di bidang digital forensik ini. Sedangkan non-formal maksudnya adalah lewat jalur kursus-kursus singkat yang bersifat *professional certification* yang di akhir kursus tersebut ada ujian yang biasanya berupa *online exam* di mana peserta kursus wajib lulus dari ujian tersebut untuk dapat meraih sertifikasi professional yang diinginkan, misalnya CHFI (*Computer Hacking*

Forensic Investigator) dari EC-Council, suatu lembaga internasional di bidang sertifikasi kompetensi komputer.



Gambar II. 2. *Screenshot* situs www.eccouncil.org yang menyediakan *professional certifications* CHFI (*Computer Hacking Forensic Investigator*).



Gambar II. 3. *Screenshot* situs *University of* Glasgow, Inggris di www.gla.ac.uk yang menyediakan program pasca sarjana MSc di bidang *Computer Forensics and E-discovery*.

Dengan jelasnya status kompetensi mereka, diharapkan mereka dapat menjelaskan, baik secara teknis maupun praktis alasan-alasan mereka dalam melakukan tindakan-tindakan terhadap media penyimpanan barang bukti. Jika mereka mengambil tindakan, misalnya A, maka mereka harus dapat menjelaskan secara forensik mengapa tindakan A harus dilakukan dan apa hasilnya. Jika

mereka tidak dapat menjelaskan dengan benar mengenai hal tersebut, maka sangat memungkinkan hasil dari pemeriksaan dan analisa yang mereka lakukan terhadap media penyimpanan barang bukti tersebut tidak dapat diterima oleh pihak lain, khususnya lembaga peradilan, dan ini sangat membahayakan, dalam artian hal ini bisa menyebabkan hilangnya alat bukti hukum yang syah yang dapat berimplikasi bebasnya pelaku kejahatan dari dakwaannya.

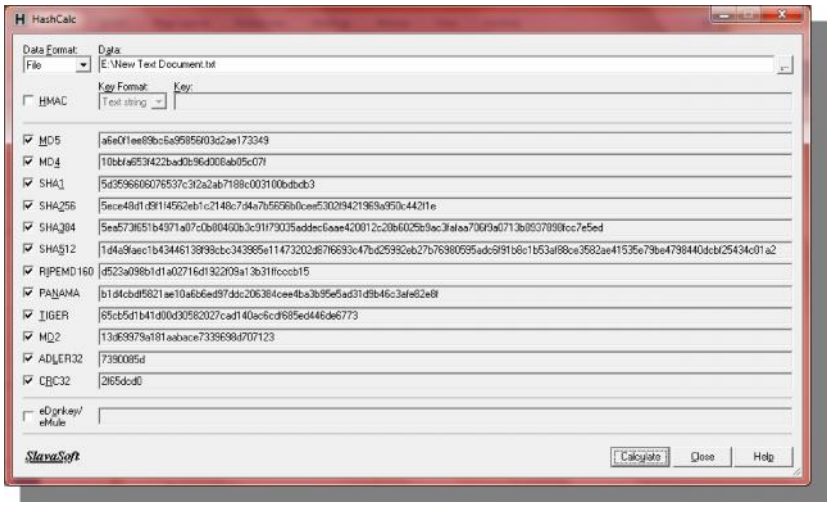
Penjelasan prinsip dasar no. 3 :

Seharusnya ada catatan teknis dan praktis terhadap langkah-langkah yang diterapkan terhadap media penyimpanan barang bukti selama pemeriksaan dan analisa berlangsung, sehingga ketika barang bukti tersebut diperiksa oleh pihak ketiga, maka seharusnya pihak ketiga tersebut akan mendapatkan hasil yang sama dengan hasil yang telah dilakukan oleh *investigator/forensic analyst* sebelumnya.

Ketika seseorang mengakses media penyimpanan barang bukti dalam rangka memeriksa dan menganalisanya untuk mendapatkan data-data digital yang berkaitan dengan investigasi suatu kejahatan, maka ia harus melakukannya dengan benar dan prosedural, serta harus berani untuk diperiksa kembali hasilnya oleh pihak ketiga yang independen. Karena tidak tertutup kemungkinan, majelis hakim dalam persidangan dalam rangka penuntutan atau *criminal investigator* dalam rangka investigasi meminta *second opinion* dari pihak ketiga untuk memastikan hasil pemeriksaan sebelumnya. Nantinya pihak ketiga ini akan menapaktilasi langkah-langkah yang sudah diaplikasikan pada pemeriksaan sebelumnya. Diharapkan hasil yang didapat pihak ketiga ini adalah sama dengan hasil yang diperoleh dalam pemeriksaan sebelumnya. Jika ternyata hasil di antara mereka berbeda, maka perlu dilakukan pemeriksaan ulang oleh pihak keempat dengan mengecek lebih detil tahapan-tahapan yang telah dilakukan sebelumnya untuk mencari langkah-langkah mana yang lebih prosedural dan sesuai dengan prinsip-prinsip digital forensik.

Untuk itu, dalam pemeriksaan awal maupun lanjutan, perlu adanya persepsi di kalangan *investigator/forensic analyst* mengenai keutuhan barang bukti sebelum dilakukan tahapan yang lebih spesifik. Untuk mengukur keutuhan barang bukti

sehingga tahapan-tahapan yang dilakukan dapat diterima, maka digunakanlah sistem *hashing*, yaitu suatu sistem pengecekan otentikasi isi dari suatu file, baik *image/evidence file* maupun *file-file logical* dengan menggunakan algoritma matematika tertentu seperti MD5, SHA1 dan lain-lain sehingga dihasilkan suatu deret nilai yang unik yang berbeda dengan yang lain. Salah satu aplikasi *hashing* yang berjalan di *platform* Windows adalah HashCalc yang menyediakan berbagai algoritma *hashing* seperti MD5, SHA1, SHA256, SHA512, CRC32 dan lain-lain.



Gambar II. 4. *Screenshot* aplikasi HashClac yang menyediakan berbagai algoritma yang dapat dapat digunakan untuk proses *hashing*.

Nilai *hash* ini perlu didapat sebelum melakukan tahapan yang lebih spesifik untuk menggambarkan keutuhan barang bukti dan sesudah tahapan dilakukan untuk menjelaskan data-data digital yang didapat. Ini nantinya dapat digunakan untuk mempertanggungjawabkan tahapan-tahapan yang telah dilakukan.

Penjelasan prinsip dasar no. 4 :

Seseorang yang bertanggungjawab terhadap investigasi kasus maupun pemeriksaan dan analisa barang bukti elektronik harus dapat memastikan bahwa proses yang berlangsung sesuai dengan hukum yang berlaku dan prinsip-prinsip dasar sebelumnya, yaitu prinsip dasar no. 1, 2 dan 3 dapat diaplikasikan dengan baik.

Ini dimaksudkan agar hasil pemeriksaan dan analisa terhadap media penyimpanan barang bukti elektronik yang berupa data-data digital tidak bertentangan dengan hukum positif yang berlaku sehingga dapat diterima secara teknis dan hukum oleh majelis hakim di persidangan. Jangan sampai, pemeriksaan dan analisa yang dilakukan yang telah memakan waktu yang lama ternyata tidak dapat diterima di persidangan dikarenakan tidak sesuai dengan kaidah-kaidah hukum yang berlaku. Di Indonesia, ada undang-undang yang secara khusus membahas secara detil tentang kejahatan-kejahatan komputer dan bagaimana melakukan investigasinya secara benar sehingga hasil pemeriksaan dan analisa secara digital forensik yang diterapkan pada kasus kejahatan tersebut dapat diterima sebagai alat bukti hukum yang syah. Undang-undang tersebut adalah UU no. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Pembahasan tentang undang-undang tersebut akan dilakukan secara detil pada Bab III.

Selain itu, orang yang bertanggungjawab terhadap proses investigasi, pemeriksaan maupun analisa harus dapat memastikan bahwa prinsip-prinsip dasar no. 1, 2 dan 3 yang dibahas di atas dapat diterapkan dengan baik, sehingga hasil pemeriksaan dan analisa yang didapat bersifat kredibel dan dapat dipertanggungjawabkan, baik secara teori, teknis maupun praktis, baik ketika masih di dalam penyidikan itu sendiri maupun di persidangan nantinya. Artinya ketiga prinsip dasar tersebut harus dapat diimplementasikan, dan tidak boleh ada prinsip dasar yang dilanggar. Orang yang bertanggungjawab yang biasanya merupakan ketua tim harus dapat memastikan hal tersebut.

Klasifikasi Digital Forensik

Dikarenakan spesialisasi digital forensik ini memiliki cakupan yang cukup luas, maka terhadap spesialisasi ini dilakukan kategorisasi yang didasarkan pada bentuk fisik maupun *logical* dari barang bukti yang diperiksa/dianalisa, yaitu :

1. **Komputer Forensik**

   Ini berkaitan dengan pemeriksaan dan analisa barang bukti elektronik berupa komputer PC (*Personal Computer*), *laptop/notebook*, *netbook* dan

tablet. Pemeriksaan terhadap jenis barang bukti ini biasanya berkaitan dengan files *recovery*, yaitu suatu metode untuk mengambil *file logical* atau memunculkan kembali file yang sudah dihapus (*deleted*) maupun hilang (*lost*) dikarenakan tidak tercatat lagi di file system. *File-file* tersebut diperlukan untuk membuktikan kejahatan yang terjadi dan menghubungkannya dengan pelaku. Pembahasan mengenai *files recovery* ini ada di Bab VI.

2. *Mobile* Forensik

Mobile forensik ini berhubungan dengan jenis barang bukti elektronik yang berupa *handphone* dan *smartphone*. Pemeriksaan ini biasanya berkaitan dengan informasi digital yang tersimpan di barang bukti tersebut. Informasi yang penting ini seperti *call logs* seperti panggilan *incoming* (masuk), *outgoing* (keluar) dan *missed* (tidak terjawab), SMS (*short message service*) yaitu pesan *inbox* (masuk), *sent* (keluar), dan *draft* (rancangan), *email*, foto (gambar digital), video dan lain-lain diperlukan untuk mengetahui komunikasi di antara pelaku kejahatan, atau pemetaan apa yang telah dilakukan para pelaku yang berkaitan dengan kejahatannya. Ini biasanya pada kasus-kasus narkotika. *Mobile* forensik ini dibahas secara tersendiri pada Bab VII.

3. Audio Forensik

Ini berkaitan dengan rekaman suara yang berhubungan dengan pelaku kejahatan. Rekaman suara ini biasanya diperiksa untuk kepentingan *voice recognition*, yaitu memeriksa dan menganalisa suara yang ada di rekaman barang bukti (dikenal sebagai *unknown samples*), untuk kemudian dibandingkan suara pembanding (*known samples*) dalam rangka untuk mengetahui apakah suara *unknown* adalah identik atau tidak identik dengan suara *known*. Jika identik, maka suara barang bukti berasal dari subyek pembanding, sebaliknya jika tidak identik, maka suara barang bukti tidak berasal dari subyek pembanding. Untuk audio forensik ini ada tahapan-tahapan analisanya, yaitu *acquisition* (yaitu akuisisi file rekaman

suara), audio *enchancement* (peningkatan kualitas rekaman dengan melakukan *noise filtering*), *decoding* (pembuatan transkrip dari suara percakapan yang jelas), *voice recognition* dan kesimpulan. Tahapan-tahapan ini dibahas secara detil pada Bab VIII.

4. Video Forensik

Pemeriksaan dan analisa yang berkaitan dengan video forensik ini adalah barang bukti berupa rekaman video, yang biasanya berasal dari kamera cctv (*closed circuit tv*). Rekaman cctv ini diperiksa berkaitan dengan kegiatan pelaku kejahatan yang sempat terekam di kamera cctv tersebut. Rekaman ini kemudian dianalisa untuk mengambil *screenshot* dari wajah pelaku atau pelat nomor polisi dari mobil yang dicurigai. Permasalahan yang timbul yang berkaitan dengan rekaman cctv ini adalah resolusi video yang rendah dan kualitas kamera yang tidak bagus, sehingga ketika rekaman cctv ini dianalisa, hasilnya tidak bisa maksimal. Selain permasalahn resolusi, ada faktor-faktor lain yang ikut mempengaruhi bisa tidaknya pembesaran secara maksimal terhadap obyek yang diinginkan pada rekaman, yaitu jarak kamera dengan obyek, dimensi ukuran obyek dan tingkat pencahayaan di sekitar obyek. Pembahasan yang lebih detil mengenai video forensik ini dibahas secara tersendiri pada Bab IX.

5. *Image* (gambar digital) Forensik

Ini berkaitan dengan jenis barang bukti digital yang berupa *file-file* gambar digital yang sering diperiksa dan dianalisa untuk mengetahui peralatan kamera digital yang digunakan untuk mengambil gambar tersebut, termasuk waktu pengambilannya. Di samping itu, analisa *image* forensik terhadap *file-file* gambar digital juga sering dilakukan untuk mengetahui keaslian suatu *file* gambar, apakah *file* gambar digital ini masih asli, atau sudah direkayasa dengan menggunakan aplikasi photoshop. Untuk menguji keaslian ini, diperlukan analisa yang komprehensif, di antaranya adalah analisa metadata, analisa pixel dan analisa moment. Pembahasan

tentang analisa gambar digital secara forensik ini juga dibahas tersendiri pada Bab IX dan X.

6. ***Cyber* Forensik**

   Ini berkaitan dengan pemeriksaan dan analisa kasus-kasus yang berhubungan dengan internet atau jaringan komputer seperti LAN (*local area network*), oleh karena itu *cyber* forensic banyak sekali membahas *log files* (*file-file* yang merekam aktivitas komputer pada *session-sesion* tertentu), khususnya dari *network log* yang merekam segala aktivitas alamat IP (*Internet Protocol*) yang mengakses *server* yang menjadi barang bukti. *Log files* tersebut perlu diperiksa dan dianalisa dengan cermat untuk memastikan IP mana yang melakukan kejahatan terhadap *server* tersebut, walaupun kegiatan tersebut memakan waktu yang cukup lama. Untuk mendapatkan *log files* tersebut, *forensic analyst* dan *investigator* perlu bekerja sama dengan *administrator* (orang yang memiliki hak penguasaan tertinggi) dari *server* tersebut. Di samping itu, *cyber* forensik juga menganalisa *email* dan peralatan *network* seperti *router*, *switch* dan lain-lain. Tidak tertutup juga, *forensic analyst* akan melakukan investigasi terhadap kasus-kasus yang berkaitan dengan situs-situs *social networking* seperti *facebook* yang digunakan untuk melakukan kejahatan penipuan atau pencemaran nama baik. Dikarenakan *cyber* forensik ini memiliki cakupan yang cukup luas, maka pembahasan tentang topik ini akan diberikan secara detil pada buku tersendiri nantinya.

Klasifikasi Barang Bukti

Keberadaan barang bukti sangat penting dalam investigasi kasus-kasus *computer crime* maupun *computer-related crime* karena dengan barang bukti inilah *investigator* dan *forensic analyst* dapat mengungkap kasus-kasus tersebut dengan kronologis yang lengkap, untuk kemudian melacak keberadaan pelaku dan menangkapnya. Oleh karena posisi barang bukti ini sangat strategis, *investigator* dan *forensic analyst* harus paham jenis-jenis barang bukti. Diharapkan ketika ia

datang ke TKP yang berhubungan dengan kasus *computer crime* dan *computer-related crime*, ia dapat mengenali keberadaan barang bukti tersebut untuk kemudian diperiksa dan dianalisa lebih lanjut. Adapun klasifikasi barang bukti digital forensik terbagi atas :

a. Barang bukti elektronik

Barang bukti ini bersifat fisik dan dapat dikenali secara visual, oleh karena itu *investigator* dan *forensic analyst* harus sudah memahami untuk kemudian dapat mengenali masing-masing barang bukti elektronik ini ketika sedang melakukan proses *searching* (pencarian) barang bukti di TKP. Jenis-jenis barang bukti elektronik adalah sebagai berikut :

1) Komputer PC, *laptop/notebook*, *netbook*, *tablet*
2) *Handphone*, *smartphone*
3) *Flashdisk/thumb drive*
4) *Floppydisk*
5) *Harddisk*
6) CD/DVD
7) *Router*, *switch*, *hub*
8) Kamera video, cctv
9) Kamera digital
10) *Digital recorder*
11) *Music/video player*, dan lain-lain

b. Barang bukti digital

Barang bukti ini bersifat digital yang diekstrak atau di-*recover* dari barang bukti elektronik. Barang bukti ini di dalam Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dikenal dengan istilah *informasi elektronik dan dokumen elektronik* yang dibahas lebih detil pada Bab III. Jenis barang bukti inilah yang harus dicari oleh *forensic analyst* untuk kemudian dianalisa secara teliti keterkaitan masing-masing *file* dalam rangka mengungkap kasus kejahatan yang berkaitan dengan barang bukti elektronik. Berikut adalah contoh-contoh barang bukti digital.

1) *Logical file*, yaitu *file-file* yang masih ada dan tercatat di *file system* yang sedang berjalan (*running*) di suatu partisi. *File-file* tersebut bisa berupa *file-file* aplikasi, *library*, *office*, *logs*, multi media dan lain-lain.
2) *Deleted file*, dikenal juga dengan istilah *unallocated cluster* yang merujuk kepada *cluster* dan sektor tempat penyimpanan *file* yang sudah terhapus dan tidak teralokasikan lagi untuk *file* tersebut dengan ditandai di *file system* sebagai area yang dapat digunakan lagi untuk penyimpanan *file-file* yang baru. Artinya *file* yang sudah terhapus tersebut masih tetap berada di *cluster* atau sektor tempat penyimpanannya sampai tertimpa (*overwritten*) oleh *file-file* yang baru pada *cluster* atau sektor tersebut. Pada kondisi di mana *deleted file* tersebut belum tertimpa, maka proses *recovery* secara utuh terhadap file tersebut sangat memungkinkan terjadi.
3) *Lost file*, yaitu *file* yang sudah tidak tercatat lagi di *file system* yang sedang berjalan (*running*) dari suatu partisi, namun *file* tersebut masih ada di sektor sektor penyimpanannya. Ini bisa terjadi ketika misalnya suatu *flashdisk* atau *harddisk* maupun partisinya dilakukan proses *re-format* yang menghasilkan *file system* yang baru, sehingga *file-file* yang sudah ada sebelumnya menjadi tidak tercatat lagi di *file system* yang baru. Untuk proses *recovery*-nya didasarkan pada *signature* dari *header* maupun *footer* yang tergantung pada jenis format *file* tersebut.
4) *File slack*, yaitu sektor penyimpanan yang berada di antara *End of File* (EoF) dengan *End of Cluster* (EoC). Wilayah ini sangat memungkinkan terdapat informasi yang mungkin penting dari *file-file* yang sebelumnya sudah dihapus (*deleted*).
5) *Log file*, yaitu *file-file* yang merekam aktivitas (*logging*) dari suatu keadaan tertentu, misalnya *log* dari sistem operasi, *internet browser*, aplikasi, *internet traffic*, dan lain-lain.
6) *Encrypted file*, yaitu *file* yang isinya sudah dilakukan enkripsi dengan menggunakan algoritma *cryptography* yang compleks,

sehingga tidak bisa dibaca atau dilihat secara normal. Satu-satunya cara untuk membaca atau melihatnya kembali adalah dengan melakukan dekripsi terhadap *file* tersebut dengan menggunakan algoritma yang sama. Ini biasa digunakan dalam dunia *digital information security* untuk mengamankan informasi yang penting. Ini juga merupakan salah satu bentuk dari *Anti-Forensic*, yaitu suatu metode untuk mempersulit *forensic analyst* atau *investigator* mendapatkan informasi mengenai jejak-jejak kejahatan.

7) *Steganography file*, yaitu *file* yang berisikan informasi rahasia yang disisipkan ke *file* lain, biasanya berbentuk *file* gambar, video atau audio, sehingga *file-file* yang bersifat *carrier* (pembawa pesan rahasia) tersebut terlihat normal dan wajar bagi orang lain, namun bagi orang yang tahu metodologinya, file-file tersebut memiliki makna yang dalam dari informasi rahasianya tersebut. Ini juga dianggap sebagai salah satu bentuk dari *Anti-Forensic*.
8) *Office file*, yaitu *file-file* yang merupakan produk dari aplikasi *Office*, seperti Microsoft Office, Open Office dan sebagainya. Ini biasanya berbentuk *file-file* dokumen, *spreadsheet*, *database*, teks, dan presentasi.
9) *Audio file*, yaitu *file* yang berisikan suara, musik dan lain-lain, yang biasanya berformat wav, mp3 dan lain-lain. *File* audio yang berisikan rekaman suara percakapan orang ini biasanya menjadi penting dalam investigasi ketika suara di dalam *file* audio tersebut perlu diperiksa dana dianalisa secara audio forensik untuk memastikan suara tersebut apakah sama dengan suara pelaku kejahatan.
10) *Video file*, yaitu *file* yang memuat rekaman video, baik dari kamera digital, *handphone*, *handycam* maupun cctv. File video ini sangat memungkinkan memuat wajah pelaku kejahatan sehingga *file* ini perlu dianalisa secara detil untuk memastikan bahwa yang ada di *file* tersebut adalah pelaku kejahatan.

11) *Image file*, yaitu *file* gambar digital yang sangat memungkinkan memuat informasi-informasi penting yang berkaitan dengan kamera dan waktu pembuatannya (*time stamps*). Data-data ini dikenal dengan istilah metadata exif (*exchangeable image file*). Meskipun begitu metadata exif ini bisa dimanipulasi, sehingga *forensic analyst* atau *investigator* harus hati-hati ketika memeriksa dan menganalisa metadata dari *file* tersebut.
12) *Email*, merupakan singkatan dari *electronic mail*, yaitu surat berbasis sistem elektronik yang menggunakan sistem jaringan *online* untuk mengirimkannya atau menerimanya. *Email* menjadi penting di dalam investigasi khususnya *phishing* (yaitu kejahatan yang menggunakan *email* palsu dilengkapi dengan identitas palsu untuk menipu si penerima). *Email* berisikan *header* yang memuat informasi penting jalur distribusi pengiriman *email* mulai dari *sender* (pengirim) sampai di *recipient* (penerima), oleh karena itu data di *header* inilah yang sering dianalisa secara teliti untuk memastikan lokasi si pengirim yang didasarkan pada alamat IP. Meskipun begitu, data-data di *header* juga sangat dimungkinkan untuk dimanipulasi. Untuk itu pemeriksaan *header* dari *email* harus dilakukan secara hati-hati dan komprehensif.
13) *User* ID dan *password*, merupakan syarat untuk masuk ke suatu *account* secara *online*. Jika salah satunya salah, maka akses untuk masuk ke *account* tersebut akan ditolak.
14) SMS (*Short Message Service*), yaitu pelayanan pengiriman dan penerimaan pesan pendek yang diberikan oleh operator seluler terhadap pelanggannya. SMS-SMS yang bisa berupa SMS *inbox* (masuk), *sent* (keluar), dan *draft* (rancangan) dapat menjadi petunjuk dalam investigasi untuk mengetahui keterkaitan antara pelaku yang satu dengan yang lain.
15) MMS (*Multimedia Message Service*), merupakan jasa layanan yang diberikan oleh operator seluler berupa pengiriman dan

penerimaan pesan multimedia yang bisa berbentuk suara, gambar atau video.

16) *Call logs*, dan lain-lain, yaitu catatan panggilan yang terekam pada suatu nomor panggilan seluler. Panggilan ini bisa berupa *incoming* (panggilan masuk), *outgoing* (panggilan keluar), dan *missed* (panggilan tak terjawab).

Berdasarkan penjelasan di atas, dapat diketahui bahwa ada perbedaan antara barang bukti elektronik dengan barang bukti digital. Yang pertama bersifat bentuk fisik, sementara yang kedua memiliki isi yang bersifat digital. Ini harus dapat dipahami dengan jelas oleh *forensic analyst* dan *investigator* ketika mereka melakukan pencarian barang bukti elektronik di TKP (Tempat Kejadian Perkara), untuk kemudian membawanya ke laboratorium dan menganalisanya dengan tepat dan prosedural, sehingga menghasilkan barang bukti digital seperti yang diharapkan.

Prosedur penanganan awal di TKP

Penanganan awal barang bukti elektronik di TKP memegang peranan yang sangat penting dan krusial, dikarenakan sifat *volatility* (mudah berubah, hilang atau rusak) dari barang bukti digital. Jika penanganan awal barang bukti elektronik tersebut di TKP adalah keliru dan tidak prosedural, maka sangat dimungkinkan barang bukti digital yang penting dan semestinya ada menjadi berubah, atau bahkan hilang. Untuk itu *forensic analyst* dan *investigator* harus mampu memahami prosedur penanganan barang bukti elektronik, yang dalam hal ini adalah komputer dengan benar.

a. Persiapan

Sebelum berangkat ke TKP untuk melaksanakan penggeledahan kasus yang berkaitan dengan barang bukti elektronik, *forensic analyst* dan *investigator* sudah mempersiapkan terlebih dahulu hal-hal atau peralatan yang nantinya dibutuhkan selama proses penggeledahan di TKP. Berikut

adalah hal-hal yang harus dipersiapkan dan dimiliki oleh *forensic analyst* dan *investigator* :

1) Administrasi penyidikan, seperti surat perintah penggeledahan dan surat perintah penyitaan.
2) Kamera digital, digunakan untuk memotret TKP dan barang bukti secara fotografi forensik, yaitu foto umum, menengah dan *close up*.
3) Peralatan tulis, untuk mencatat antara lain spesifikasi teknis komputer dan keterangan para saksi.
4) Nomor, skala ukur dan label lembaga serta *sticker label* kosong, digunakan untuk menandai masing-masing barang bukti elektronik yang ditemukan di TKP.
5) Formulir penerimaan barang bukti, digunakan untuk kepentingan *chain of custody*, yaitu metodologi untuk menjaga keutuhan barang bukti dimulai dari TKP.
6) *Triage tools*, digunakan untuk kegiatan *triage* forensik terhadap barang bukti komputer yang ditemukan dalam keadaan hidup (*on*).

b. Ketika komputer dalam keadaan off (mati)

Berikut adalah tahapan-tahapan yang dikerjakan ketika *forensic analyst* atau *investigator* mendapati barang bukti komputer dalam keadaan mati (*off*) di TKP :

1) Pastikan komputer tersebut dalam keadaan mati, yaitu dengan cara menggeser *mouse* sedikit atau melihat lampu indikator *power*. Ini dilakukan untuk memastikan bahwa komputer tersebut tidak dalam keadaan *stand-by* atau hibernasi.
2) Catat spesifikasi teknis dari barang bukti komputer, yaitu : merk, model, dan *serial number* (S/N) atau *product number* (P/N).
3) Lakukan fotografi forensik terhadap barang bukti komputer tersebut, dilengkapi dengan nomor, skala ukur dan label. Fotografi forensik ini mencakup foto umum (yaitu menjelaskan TKP secara

keseluruhan), menengah (yaitu menjelaskan hubungan barang bukti elektronik dengan benda-benda di sekitarnya), dan *close up* (yaitu foto khusus terhadap barang bukti tersebut). Foto-foto tersebut diusahakan diambil dari 4 (empat) arah yang berbeda. Untuk foto *close up*, juga lakukan fotografi terhadap *name plate* yang biasanya berada di sisi bawah atau belakang.

4) Catat keterangan saksi mengenai hal-hal yang berhubungan dengan barang bukti komputer tersebut.
5) Bungkus barang bukti komputer tersebut, kemudian beri catatan di sisi luarnya untuk menandakan jenis komputer yang berada di dalam bungkusan tersebut. Untuk hal-hal yang sifatnya mendesak, bisa saja barang bukti komputer tersebut tidak dibungkus, namun tetap diberi catatan di sisi *casing* luarnya dengan menggunakan *sticker label* kosong.
6) Isi formulir penerimaan barang bukti. Tulis dengan jelas tanggal dan tempat TKP serta spesifikasi teknis dari masing-masing barang bukti elektronik dan ditandatangani oleh *investigator* dan *forensic analyst*.
7) Bawa barang bukti komputer tersebut berikut catatan-catatannya dan foto-fotonya ke laboratorium untuk pemeriksaan dan analisa lebih lanjut.
8) Catatan Penting : jangan pernah menghidupkan kembali barang bukti komputer yang ditemukan dalam keadaan sudah mati (*off*) ! karena jika hal tersebut dilakukan, sama saja *investigator/analyst* melakukan kontaminasi terhadap isi *harddisk* dari komputer tersebut.

c. Ketika komputer dalam keadaan on (hidup)

Berikut adalah kegiatan-kegiatan yang semestinya dilakukan oleh *forensic analyst* dan *investigator* ketika menemukan barang bukti komputer dalam keadaan hidup (*on*) di TKP. Prinsip dari kegiatan ini adalah berusaha untuk mendapatkan data-data investigatif (yang berkaitan dengan kejahatan)

seefisien mungkin (cepat dan tepat) dengan kemungkinan perubahan isi *harddisk* seminimum mungkin.

1) Catat apa yang sedang *running* dan tertampil di layar monitor dari barang bukti komputer.
2) Catat spesifikasi teknis dari barang bukti komputer tersebut seperti penjelasan sebelumnya, termasuk juga dicatat tanggal/waktu dari komputer tersebut yang biasanya berada di pojok kanan bawah, kemudian bandingkan dengan tanggal/waktu lokal yang sebenarnya.
3) Lakukan fotografi forensik seperti yang telah dijelaskan sebelumnya. Ditambahkan untuk melakukan fotografi tanggal/waktu dari komputer tersebut disandingkan dengan jam yang menunjukkan waktu lokal yang sebenarnya. Ini sangat dibutuhkan untuk menunjukkan seberapa jauh perbedaan antara tanggal/waktu komputer dengan tanggal/waktu yang sebenarnya. Ini sangat erat kaitannya dengan *time stamps* dari suatu file yang menjadi temuan digitalnya. *Time stamps* tersebut berupa *created date* (yaitu tanggal pertama kali file tersebut dibuat dan tercatat di file system yang sedang berjalan), *modified date* (yaitu tanggal terakhir kali file tersebut dimodifikasi, dan tercatat, bisa di *file system* sebelumnya atau yang sedang berjalan), dan *accessed date* (yaitu tanggal terakhir kali *file* diakses dan tercatat di *file system* yang sedang berjalan).
4) Catat keterangan saksi-saksi yang menjelaskan hal-hal yang berkaitan dengan barang bukti komputer tersebut.
5) Lakukan *triage* forensik dengan bantuan *triage tools* yang sudah disiapkan sebelumnya. Pada tahapan *triage* ini, *forensic analyst* dan *investigator* sangat memungkinkan untuk mendapatkan banyak data secara cepat yang berkaitan dengan investigasi kasus *computer crime* atau *computer-related crime*, sehingga dengan cepat pula, *investigator* dapat menentukan tahapan investigasi lebih lanjut dengan benar.

Salah satu tahapan *triage* yang sangat penting yang seharusnya dilakukan oleh *forensic analyst* atau *investigator* adalah melakukan RAM *imaging*, yaitu suatu proses *forensic imaging* (penggandaan secara *physical bit per bit*) terhadap RAM (*Random Access Memory*) dari barang bukti komputer yang dalam keadaan *on*. RAM ini menyimpan banyak informasi dari semua proses dan aplikasi yang sedang *running* (berjalan) sejak komputer dihidupkan. Informasi ini bisa jadi sangat dibutuhkan oleh *investigator* untuk bahan investigasi lebih lanjut.

Selain RAM *imaging*, *forensic analyst* dan *investigator* bisa mendapatkan data-data yang masih tersimpan di komputer tersebut secara cepat, misalnya :

a) *Encrypted files*, yaitu mencari *file-file* enkripsi, yang mungkin dalam keadaan sudah di-dekripsi oleh pelaku. Jika ini terjadi, maka inilah kesempatan yang sangat baik dan tepat bagi *forensic analyst* dan *investigator* untuk mendapatkan isi dari *file-file* enkripsi tersebut.
b) Informasi sistem, seperti jenis sistem operasi, *processor*, ukuran RAM, tanggal/waktu, merk, model, *serial number*, aplikasi-aplikasi yang ter-*install*, proses-proses yang sedang berjalan dan lain-lain.
c) *File history*, seperti *recent files* (yaitu *file-file* yang diakses beberapa waktu terakhir) dan *opened files* (yaitu *file-file* yang diakses mulai dari selesainya instalasi sistem operasi hingga saat terkini).
d) *Internet browser history*, yaitu rekaman/catatan ketika sedang *surfing* (bermain) di internet dari *browser*, seperti Internet *Explorer*, Firefox, Safari dan Opera.
e) *On/Off History*, yaitu rekaman/catatan kapan komputer tersebut *on* dan *off*.
f) *Contents Searching*, yaitu melakukan pencarian terhadap isi dari suatu *file* tertentu secara cepat.

g) RAM *mapping*, yaitu melihat pemetaan RAM yang dialokasikan untuk proses-proses atau aplikasi yang sedang *running*.

h) USB *history*, yaitu rekaman/catatan penggunaan *port* USB (*Universal Serial Bus*) yang digunakan untuk mengakses media penyimpanan data seperti *flashdisk*, *harddisk*, *memory card* (lewat *card reader*), atau bahkan *handphone*/*smartphone*.

i) *Password dumping*, yaitu mendapatkan *password* dari *internet browser* yang digunakan untuk memasukkan *user* ID dan *password* secara *online* dan tersimpan di *browser*.

Kegiatan-kegiatan *triage* di atas harus dipahami oleh *forensic analyst* dan *investigator* bahwa hal tersebut sangat mungkin merubah isi dari *harddisk* barang bukti komputer, oleh karena itu pelaksanaan *triage* harus dilakukan secara hati-hati dan harus mampu memahami apa saja dari isi *harddisk* yang mungkin akan berubah ketika dilakukkan proses *triage*. Untuk itu, semestinya *forensic analyst* dan *investigator* harus memahami dulu secara detil dan jelas mengenai *triage* sebelum melakukannya. Sepanjang *forensic analyst/inevstigator* memahami perubahan dan alasan untuk melakukan *triage* yang dapat dibenarkan secara teori dan praktis, maka pelaksanaan *triage* dapat dibenarkan. Pembahasan lebih detil mengenai *triage* forensik dibahas pada Bab IV.

6) Setelah proses *triage* forensik selesai, maka barang bukti komputer harus dimatikan secara kasar, artinya tidak lewat prosedur *shut down*, namun dimatikan dengan cara memutus aliran listriknya secara langsung. Ini dimaksudkan untuk menjaga keutuhan dari *page file* (yaitu *space*/ruang *harddisk* yang digunakan sebagai *memory* sementara ketika komputer dalam keadaan hidup yang mana *page file* ini menyimpan proses-proses atau aplikasi-aplikasi yang sedang *running*).

Untuk komputer PC, cabut ujung kabel *power* yang berada di belakang *casing* CPU (*Central Processing U*nit), kemudian dilanjutkan di ujung lainnya yang terpasang di stop kontak. Ini dimaksudkan agar jika ada UPS (*Uninterruptible Power Supply*) yang berada di antara CPU dengan *power*, maka ia tidak akan aktif. Sementara itu, untuk komputer berupa *laptop* atau *netbook*, maka cabut batere secara langsung yang berada di posisi belakang atau bawah.

Untuk komputer yang digunakan sebagai *server* yang bisa dilihat dari sistem operasi yang terinstall, misalnya Windows 2000 Server, Windows 2003 Server, maka gunakan prosedur *shutdown* secara normal. Ini dimaksudkan untuk menjaga keutuhan *database* dari *server* dari kemungkinan besar rusak jika dimatikan secara kasar. *Database* ini sangat memungkinkan dibutuhkan oleh *forensic analyst* dan *investigator* untuk investigasi lebih lanjut. Hal yang sama juga berlaku untuk komputer berbasis Linux. Prosedur *shutdown* juga bisa dilakukan lewat terminal dengan mengetikkan *'shutdown –h now'* dalam posisi sebagai *root*. Hal yang sama juga diberlakukan untuk komputer Macintosh yang difungsikan sebagai *server*, namun jika komputer Macintosh tersebut bukan *server*, maka ia dimatikan secara kasar seperti yang dijelaskan di atas.

7) Bungkus barang bukti komputer tersebut, kemudian beri catatan di sisi luarnya untuk menandakan jenis komputer yang berada di dalam bungkusan tersebut. Untuk hal-hal yang sifatnya mendesak, bisa saja barang bukti komputer tersebut tidak dibungkus, namun tetap diberi catatan di sisi *casing* luarnya dengan menggunakan *sticker label* kosong.
8) Isi formulir penerimaan barang bukti. Tulis dengan jelas tanggal dan tempat TKP serta spesifikasi teknis dari masing-masing barang bukti elektronik dan ditandatangani oleh *investigator* dan *forensic analyst*.

9) Bawa barang bukti komputer tersebut berikut catatan-catatannya dan foto-fotonya ke laboratorium untuk pemeriksaan dan analisa lebih lanjut.

Prosedur penanganan di laboratorium

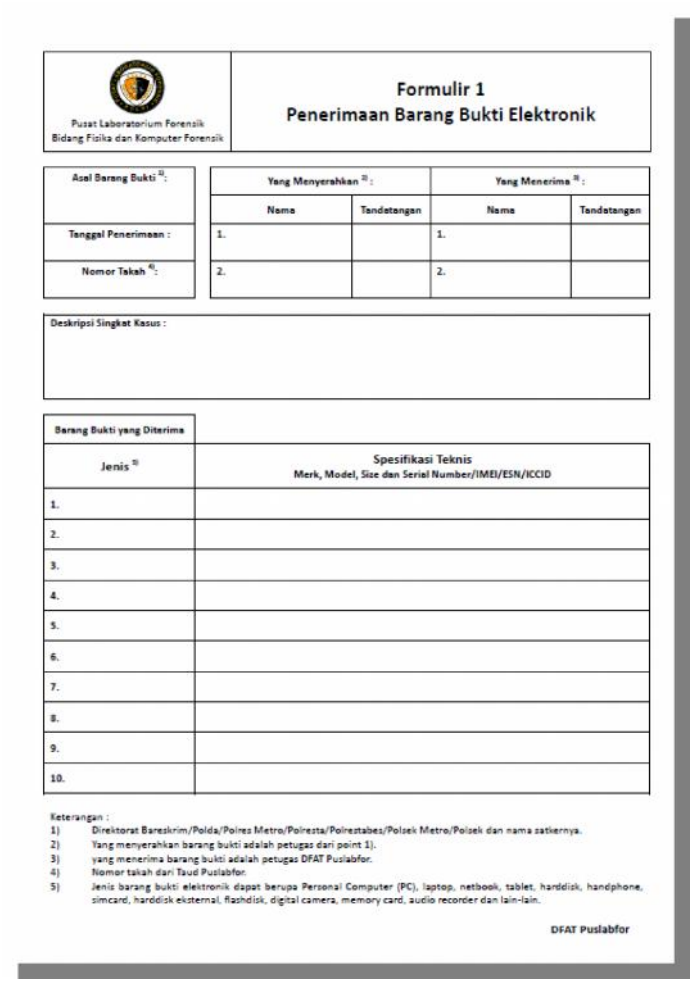
Setelah penanganan awal di TKP berjalan dengan baik dan prosedural, kemudian barang bukti elektronik dibawa ke laboratorium untuk pemeriksaan dan analisa lebih detil, selanjutnya barang bukti tersebut ditangani dengan baik dan prosedural juga sehingga hasil berupa data-data digital yang diharapkan dapat lebih maksimal dan dapat dipertanggungjawabkan secara hukum hingga di persidangan. Berikut adalah tahapan-tahapan secara garis besar penanganan barang bukti elektronik di laboratorium :

a. Administrasi penerimaan

Pada tahapan ini, barang bukti komputer yang masuk dan diterima petugas laboratorium, yang dalam hal ini *forensic analyst* harus dicatat secara detil di dalam *log book*, di samping di formulir penerimaan. Di bawah ini antara lain data-data yang harus dicatat adalah sebagai berikut :

1) Nama lembaga pengirim barang bukti elektronik.
2) Nama petugas pengirim barang bukti elektronik, termasuk identitasnya secara lengkap.
3) Tanggal penerimaan.
4) Jumlah barang bukti elektronik yang diterima, dilengkapi dengan spesifikasi teknisnya seperti merk, model dan *serial/product number* serta ukuran (*size*).
5) Tanda tangan petugas yang menyerahkan dan yang menerima.

Di bawah ini adalah contoh formulir penerimaan barang bukti elektronik yang digunakan oleh DFAT (*Digital Forensic Analyst Team*) Puslabfor.



Pusat Laboratorium Forensik
Bidang Fisika dan Komputer Forensik

Formulir 1
Penerimaan Barang Bukti Elektronik

Asal Barang Bukti [1]:	Yang Menyerahkan [2]:		Yang Menerima [3]:	
	Nama	Tandatangan	Nama	Tandatangan
Tanggal Penerimaan :	1.		1.	
Nomor Takah [4]:	2.		2.	

Deskripsi Singkat Kasus :

Barang Bukti yang Diterima

Jenis [5]	Spesifikasi Teknis Merk, Model, Size dan Serial Number/IMEI/ESN/ICCID
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

Keterangan :
1) Direktorat Bareskrim/Polda/Polres Metro/Polresta/Polrestabes/Polsek Metro/Polsek dan nama satkernya.
2) Yang menyerahkan barang bukti adalah petugas dari point 1).
3) yang menerima barang bukti adalah petugas DFAT Puslabfor.
4) Nomor takah dari Tausi Puslabfor.
5) Jenis barang bukti elektronik dapat berupa Personal Computer (PC), laptop, netbook, tablet, harddisk, handphone, simcard, harddisk eksternal, flashdisk, digital camera, memory card, audio recorder dan lain-lain.

DFAT Puslabfor

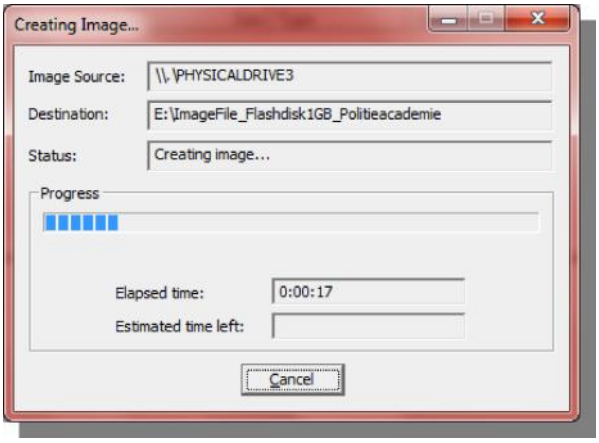
Gambar II. 5. *Screenshot* formulir penerimaan barang bukti elektronik yang digunakan oleh DFAT Puslabfor.

b. Akuisisi

Pada tahapan ini, barang bukti elektronik seperti komputer, diambil *harddisk*-nya yang berfungsi sebagai media penyimpanan untuk selanjutnya dilakukan proses akuisisi. Sebelum dilakukan proses tersebut, komputer yang digunakan untuk kegiatan tersebut harus sudah dilengkapi dengan *write protect* sebelumnya. Ini dimaksudkan untuk menjaga keutuhan isi dari barang bukti, yaitu mencegah terjadinya proses penulisan terhadap barang bukti elektronik. Diharapkan isi barang bukti tidak mengalami perubahan sama sekali. Setelah itu dilanjutkan dengan proses *forensic imaging*, yaitu menggandakan isi dari barang bukti *harddisk* tersebut secara *physical* (sektor per sektor, atau *bit-stream copy*) sehingga hasil *imaging* akan sama persis dengan barang bukti secara

physical. Derajat kesamaan ini dapat dipastikan melalui proses *hashing* yang diterapkan pada keduanya. Jika nilai *hash* antara hasil *imaging* dengan barang bukti adalah sama, maka dapat dipastikan bahwa keduanya adalah identik dan hasil *imaging* bersifat forensik, yang artinya dapat dipertanggungjawabkan secara ilmiah dan hukum, untuk selanjutnya hasil *imaging* ini dapat digunakan untuk pemeriksaaan dan analisa lebih lanjut. Sebaliknya, jika nilai *hash* antara keduanya berbeda, maka proses *forensic imaging* harus diulang sampai mendapatkan nilai *hash* yang sama.

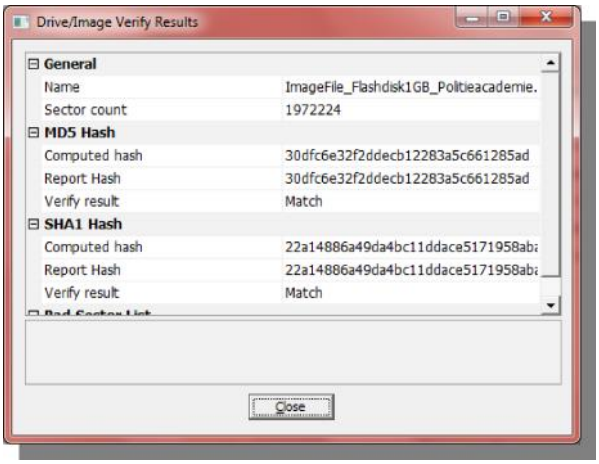
Proses *hashing* ini menggunakan banyak algoritma matematika yang kompleks, namun yang paling sering digunakan untuk kegiatan digital forensik, antara lain adalah MD5, SHA1 dan SHA256. Proses *hashing* ini juga dikenal dengan istilah *digital fingerprint* (sidik jari digital), yang biasa digunakan untuk membuktikan secara pasti apakah kedua file yang dipertanyakan adalah sama atau berbeda.



Gambar II.6. Aplikasi FTK (*Forensic Toolkit*) *Imager* sedang melakukan *forensic imaging bit per bit* (*bit sream copy*) dengan menggunakan metode *disk to image file*.

Untuk proses *forensic imaging*, ada 2 (dua) metode, yaitu *disk to disk* (artinya hasil *imaging* akan berupa *harddisk*), dan *disk to file* (artinya hasil *imaging* akan berwujud *image file*) seperti pada Gambar II.6 di atas. Dari kedua metode ini, metode yang kedua yang lebih sering digunakan oleh

forensic analyst saat ini dikarenakan metode kedua ini lebih fleksibel, efisien dan *integrity* dapat lebih terjamin. Permasalahan menggunakan metode yang pertama adalah ketika kasus yang diinvestigasi memiliki banyak *harddisk* yang harus di-*imaging*. Jika menggunakan metode *disk to disk*, maka *forensic analyst* dan *investigator* harus menyediakan banyak *blank harddisk* (*harddisk* kosong) sebagai target dari proses *forensic imaging*, dan ini pada banyak kasus, sangat tidak fleksibel dan malah memperlambat investigasi itu sendiri. Kalaupun mampu untuk menyediakan banyak *blank harddisk* sebagai target dari *imaging*, itupun akan memakan banyak biaya lebih mahal dan tidak efisien. Permasalahan yang kedua adalah *integrity*. Dikarenakan target *forensic imaging* berupa harddisk, maka ada kemungkinan *harddisk* hasil *imaging* ini akan rusak sektornya (*bad sector*) selama pemeriksaan, analisa atau penyimpanannya. Bila hal ini terjadi maka nilai *hash harddisk* ini akan berubah dari nilai *hash* aslinya. Ini akan menjadi masalah di kemudian hari untuk *integrity* isi dari *harddisk* barang bukti.



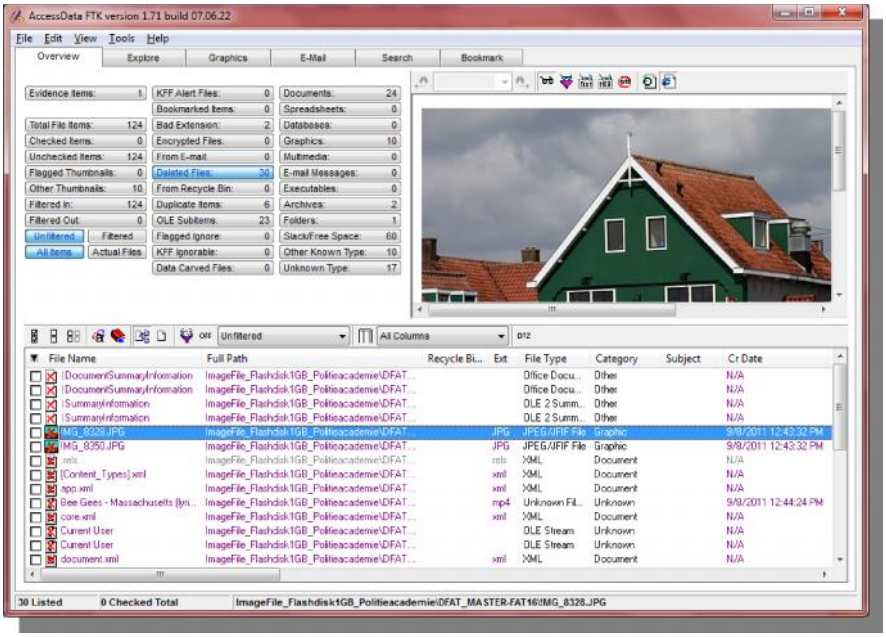
Gambar II.7. Hasil *forensic imaging* dengan menggunakan FTK *Imager* menunjukkan nilai *hash* MD5 dan SHA1 antara sumber (barang bukti media penyimpanan) dengan *image file*.

Setelah selesai proses *forensic imaging* yang menghasilkan *image file*, seperti disinggung di atas, *forensic analyst* dan *investigator* harus mengecek terlebih dahulu nilai *hash* MD5 dan SHA1 antara barang bukti

media penyimpanan dengan *image file*. Jika nilai dari keduanya adalah sama, maka itu artinya *forensic imaging* sukses, sebaliknya jika tidak, maka proses *forensic imaging* harus diulangi. Setelah itu (*forensic imaging* sukses) *harddisk* dari barang bukti komputer disimpan atau dimasukkan kembali pada tempatnya, sedangkan *image file*-nya bisa digunakan untuk tahapan pemeriksaan.

c. Pemeriksaan

Pada tahapan ini, terhadap *image file* dilakukan pemeriksaan secara komprehensif dengan maksud untuk mendapatkan data-data digital yang sesuai dengan investigasi. Ini artinya *forensic analyst* harus mendapatkan gambaran fakta kasus yang lengkap dari *investigator*, sehingga apa yang dicari dan akhirnya ditemukan oleh *forensic analyst* sama (*matching*) seperti yang diharapkan oleh *investigator* untuk pengembangan investigasinya. Setelah mendapatkan gambaran fakta kasusnya, kemudian *forensic analyst* melakukan *searching* (pencarian) terhadap isi *image file* untuk mendapatkan *file* atau data yang diinginkan.



Gambar II.8. Aplikasi FTK digunakan untuk memeriksa *image file* dari barang bukti media penyimpanan di mana aplikasi ini menunjukkan file-file yang sudah dihapus (*deleted*) dari barang bukti tersebut.

Proses *searching* ini bisa jadi akan memakan waktu yang cukup lama, tergantung seberapa besar jumlah *file* dan ukuran dari *image file* tersebut. Untuk mempersingkat waktu yang dibutukan dalam proses *searching* ini, dapat digunakan teknik *filtering* yang akan memfilter hal-hal yang langsung berkaitan dengan yang dicari. Salah satu bentuk *filtering* ini adalah *keywords* yang sesuai dengan fakta kasusnya. Teknik *filtering* yang lain adalah *grouping*, artinya *file-file* yang isinya sedang dicari dikelompokkan, antara lain berdasarkan tipe formatnya, misalnya doc, xls dan lain-lain, selanjutnya baru dilakukan proses *keyword searching* terhadap *file-file* tersebut.

Di samping kedua teknik di atas, proses *searching* dapat langsung ke jenis barang bukti digital yang diinginkan seperti yang dibahas sebelumnya, yaitu langung melakukan *file recovery* seperti yang diinginkan, yaitu mengekstrak dan mengekspor *file-file* seperti *deleted file* (seperti pada Gambar II.8 di atas), *lost file*, *file slack*, *log file*, *encrypted file*, *steganography file* dan lain-lain. Setelah itu dilanjutkan dengan pencarian data digital yang berkaitan fakta kasus.

Ada juga teknik *recovery* lain yang sangat dasar, sehingga dikenal dengan istilah *low-level recovery*, yaitu proses *recovery* yang didasarkan pada *keyword searching* langsung ke sektor per sektor penyimpanan. Untuk data-data digital yang dicari berupa teks, maka teknik ini sangat tajam untuk mendapatkan teks digital tersebut, meskipun proses ini akan memakan waktu yang lebih lama karena ia melakukan *sector scanning* untuk pencariannya. Setelah didapat *hits* (jumlah temuan yang *matching* dengan *keywords*), selanjutnya *hits* tersebut dicek satu per satu untuk memastikan *hits* mana yang sesuai dengan fakta kasus.

Metode pemeriksaan bersifat fleksibel disesuaikan dengan kasus yang sedang diinvestigasi, oleh karena itu *forensic analyst* dapat menerapkan banyak metode untuk proses ini sampai ia mendapatkan bukti digital yang diinginkan.

d. Analisa

Setelah mendapatkan *file-file* atau data-data digital yang diinginkan dari proses pemeriksaan di atas, selanjutnya data-data tersebut dianalisa secara detil dan komprehensif untuk dapat membuktikan kejahatan apa yang terjadi dan kaitannya pelaku dengan kejahatan tersebut. Hasil analisa terhadap data-data digital tadi selanjutnya disebut sebagai barang bukti digital yang harus dapat dipertanggungjawabkan secara teknis keilmiahan dan hukum di depan pengadilan.

Selama proses analisa berlangsung, *forensic analyst* harus selalu berdiskusi dengan *investigator* mengenai data-data digital yang nantinya menjadi barang bukti digital dalam rangka mengkonfirmasi data-data tersebut sesuai dengan fakta kasus dari kasus kejahatan yang sedang diinvestigasi. Ini dimaksudkan agar apa yang dihasilkan pada proses ini *matching* (sama) seperti yang diharapkan oleh tim *investigator*, sehingga proses pemeriksaan dan analisa tidak menjadi sia-sia.

Ketika data-data digital tersebut menjadi barang bukti digital yang mendukung investigasi, maka data-data tersebut harus dilengkapi dengan *properties* teknis dari data-data tersebut seperti nilai *hash* (misalnya nilai MD5 atau SHA1 yang sering digunakan) dan *time stamps* (yaitu *created*, *modified* dan *accessed date*). Untuk *time stamps* ini, yang sering digunakan adalah *created* dan *modified date*, sedangkan *accessed date* jarang dipakai. Hal ini dikarenakan *accessed date* bisa berubah mengikuti proses *scaning* (pengecekan secara keseluruhan proses dan *file*) anti virus, sehingga beum tentu menunjukkan tanggal/waktu yang sebenarnya ketika *file* tersebut terakhir kali diakses. Untuk data digital berupa *file* multi media seperti *file* audio, video dan gambar digital, maka metadata dari *file* tersebut seharusnya juga dilihat, untuk kemudian dianalisa secara komprehensif dan hasilnya ditampilkan di dalam laporan bersama-sama dengan nilai *hash* dan *time stamps*.

Dalam proses analisa metadata, hal tersebut harus dilakukan dengan cermat dikarenakan metadata bersifat *volatile*, bahkan mudah dirubah dengan teknik *hacking* sehingga metadata palsu kelihatan seolah-olah

metadata asli. Jika ini terjadi, *forensic analyst* mendapatkan kesulitan untuk melakukan *recovery* medata yang asli. Teknik hacking yang digunakan untuk mempersulit kinerja *forensic analyst* juga digolongkan sebagai *anti-forensic*. Untuk data digital berupa file foto digital yang di-*download* dari internet, biasanya sangat sulit untuk mendapatkan data exif yang memuat data-data yang berkaitan dengan peralatan pemotretan seperti dijelaskan sebelumnya. Sebagian besar file gambar digital yang berasal dari internet sudah tidak ada lagi data exif yang mengenai tanggal/waktu kapan foto tersebut diambil dan dengan peralatan apa pemotretan dilakukan. Hal yang sama juga terjadi pada data-data digital berupa *file* audio dan video yang berasal dari internet. Ini terjadi dikarenakan pada proses *uploading* ke suatu *website* atau *server*, biasanya terdapat protokol yang akan menghilangkan metadata asli dan menggantinya dengan metadata yang sesuai dengan protokol dari *website* tersebut.

e. Laporan

Setelah didapat barang bukti digital dari proses pemeriksaan dan analisa di atas yang sesuai dengan investigasi, selanjutnya data-data mengenai barang bukti digital tersebut dimasukkan ke dalam laporan teknis. Laporan ini secara umum dibagi menjadi beberapa bab penjelasan, yaitu :

1) Judul, memuat judul pemeriksaan yang dilengkapi dengan nomor pemeriksaan di laboratorium.
2) Pendahuluan, memuat nama-nama *forensic analyst* yang melakukan pemeriksaan dan analisa secara digital forensik terhadap barang bukti elektronik. Di samping itu, bab ini juga memuat tanggal/waktu pemeriksaan.
3) Barang bukti, memuat jumlah dan jenis barang bukti elektronik yang diterima untuk dilakukan pemeriksaan dan analisa. Ini juga termasuk data-data tentang spesifikasi teknis dari barang bukti tersebut seperti merk, model dan *serial/product number*, serta ukuran kapasitas (*size*) dari media penyimpanan seperti *harddisk*

dan *flashdisk*. Untuk barang bukti berupa *handphone*/*smartphone*, juga dicantumkan data nomor IMEI (*International Mobile Equipment Identity*) yang terdiri dari sejumlah digit yang unik sebagai penanda mesin handphone secara internasional, sedangkan untuk *simcard*, dilengkapi dengan data nomor ICCID (*Integrated Circuit Card* ID) yang merupakan data administrasi yang berasal dari provider seluler.

4) Maksud pemeriksaan, memuat nama lembaga pengirim barang bukti elektronik berikut surat tertulis yang berisikan maksud permintaan untuk pemeriksaan dan analisa barang bukti tersebut secara digital forensik. Maksud permintaan ini harus dimintakan kembali penjelasan secara detil oleh *forensic analyst* kepada *investigator*, sekaligus *forensic analyst* meminta *investigator* untuk memaparkan secara singkat dan jelas fakta-fakta kasus yang sedang diinvestigasi.
5) Prosedur pemeriksaan, menjelaskan tahapan-tahapan yang dilakukan selama proses pemeriksaan dan analisa terhadap barang bukti tersebut. Sebaiknya penjelasan mengenai tahapan-tahapan tersebut yang akan panjang kalau dituliskan dalam laporan, diringkas menjadi SOP (*Standard Operating Procedure*) yang baku dan lengkap. Misalnya DFAT (*Digital Forensic Analyst Team*) Puslabfor Bareskrim Polri memiliki sejumlah SOP, antara lain :

   SOP 1 tentang Prosedur Pemeriksaan Digital Forensik
   SOP 2 tentang Komitmen Jam Kerja
   SOP 3 tentang Pelaporan Hasil Pemeriksaan Digital Forensik
   SOP 4 tentang Penerimaan Barang Bukti Elektronik
   SOP 5 tentang Penyerahan Barang Bukti Elektronik
   SOP 6 tentang Triage Forensik
   SOP 7 tentang Akuisisi Langsung Komputer
   SOP 8 tentang Akuisisi Harddisk, Flashdisk dan Memory Card
   SOP 9 tentang Analisa Harddisk, Flashdisk dan Memory Card
   SOP 10 tentang Akuisisi Handphone dan Simcard

SOP 11 tentang Analisa Handphone dan Simcard

SOP 12 tentang Analisa Audio Forensik

Untuk itu pada bab ini, hanya dituliskan bahwa tahapan-tahapan yang digunakan adalah sesuai dengan SOP, misalnya SOP 1, 2 dan lain sebagainya.

Pada bab ini juga dicantumkan nilai *hash* dari masing-masing *image file* (bersifat *physical*) atau *backup file* (bersifat *logical*) hasil *forensic imaging* terhadap barang bukti elektronik sebelumnya.

6) Hasil pemeriksaan, memuat data-data digital yang berhasil di-*recovery* dari *image file* yang kemudian dianalisa lebih detil dan dikonfirmasi dengan *investigator* untuk memastikan sesuai dengan investigasi yang sedang berlangsung. Untuk data-data digital yang ditampilkan harus dilengkapi dengan nilai *hash*, *time stamps* dan metadata (untuk *file* audio, video atau foto digital), serta *path* (alamat direktori dari *file* tersebut di dalam partisinya).

   Jika data digital tersebut berasal dari hasil *low-level recovery* seperti yang dijelaskan di atas, maka sebaiknya ditampilkan *screenshot* (rekaman *monitor* berupa gambar) *hits* yang memuat data digital-nya yang dilengkapi dengan nomor *offset* (yaitu penomoran masing-masing *byte*/karakter yang didasarkan pada sistem heksadesimal).

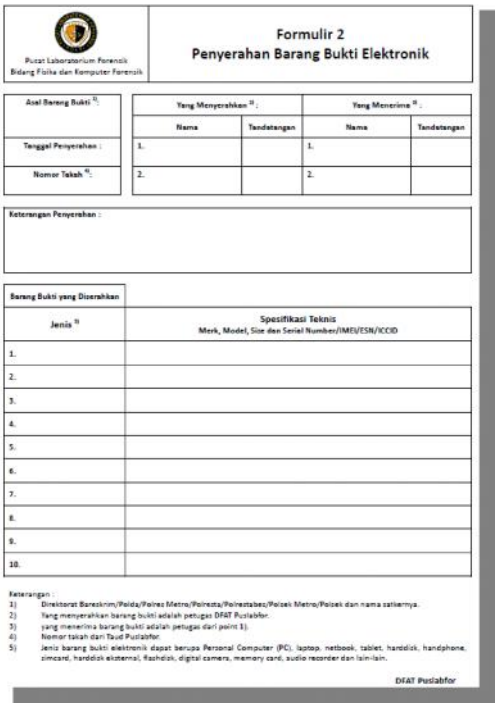
   Jika data digital tersebut berupa gambar/foto atau video, maka sebaiknya ditampilkan juga *screenshot*-nya, dan jika data digital tersebut merupakan gambar yang memuat konten pornograpfi, maka bagian-bagian yang mengandung unsur pornografi tersebut harus ditutupi dengan warna hitam.

7) Kesimpulan, memuat ringkasan yang disimpulkan dari hasil pemeriksaan di atas. Diusahakan kesimpulan berupa kalimat-kalimat yang tidak panjang dan cantumkan di akhir poin kesimpulan bahwa untuk melihat detilnya, bisa dilihat di bab Hasil Pemeriksaan.

8) Pembungkusan dan Penyegelan Barang Bukti, memuat proses pembungkusan dan penyegelan barang bukti elektronik setelah selesai diperiksa dan dianalisa secara digital forensik, untuk kemudian diserahkan kembali ke lembaga yang mengirimnya. Bungkusan barang bukti tersebut dilengkapi dengan label yang menjelaskan jumlah dan spesifikasi teknis barang bukti elektronik yang ada di dalam bungkusan tersebut, di samping nomor pemeriksaan dan nama lembaga asal barang bukti tersebut.
9) Penutup, menjelaskan bahwa proses pemeriksaan dan analisa dilakukan dengan sebenar-benarnya tanpa ada rekayasa dan dapat dipertanggungjawabkan secara ilmiah. Bab ini dilengkapi dengan tanda tangan forensic analyst yang melakukan pemeriksaan dan analisa secara digital forensik.

f. Administrasi penyerahan

Gambar di bawah ini adalah formulir penyerahan barang bukti elektronik yang digunakan oleh DFAT Puslabfor.



Pusat Laboratorium Forensik
Bidang Fisika dan Komputer Forensik

Formulir 2
Penyerahan Barang Bukti Elektronik

Asal Barang Bukti [1] :	Yang Menyerahkan [2] :		Yang Menerima [3] :	
	Nama	Tandatangan	Nama	Tandatangan
Tanggal Penyerahan :	1.		1.	
Nomor Takah [4] :	2.		2.	

Keterangan Penyerahan :

Barang Bukti yang Diserahkan	
Jenis [5]	Spesifikasi Teknis Merk, Model, Size dan Serial Number/IMEI/ESN/ICCID
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

Keterangan :
1) Direktorat Bareskrim/Polda/Polres Metro/Polresta/Polrestabes/Polsek Metro/Polsek dan nama satkernya.
2) Yang menyerahkan barang bukti adalah petugas DFAT Puslabfor.
3) yang menerima barang bukti adalah petugas dari point 1).
4) Nomor takah dari Taud Puslabfor.
5) Jenis barang bukti elektronik dapat berupa Personal Computer (PC), laptop, netbook, tablet, harddisk, handphone, simcard, harddisk eksternal, flashdisk, digital camera, memory card, audio recorder dan lain-lain.

DFAT Puslabfor

Gambar II. 9. *Screenshot* formulir penyerahan barang bukti elektronik yang digunakan oleh DFAT Puslabfor.

Setelah semua proses di atas selesai dengan baik dan prosedural, selanjutnya laporan hasil pemeriksaan secara digital forensik berikut barang bukti elektronik-nya diserahkan kembali kepada *investigator* atau lembaga pengirimnya. Pada tahapan ini, proses serah terima barang bukti harus dicatat di *log book* dan formulir penyerahan barang bukti yang dilengkapi dengan identitas jelas dan tanda tangan petugas dari perwakilan lembaga yang menerima kembali barang bukti dan petugas yang menyerahkannya, di samping tanggal/waktu serah terima dan jumlah serta spesifikasi teknis barang bukti tersebut.

Bibliography

1. ACPO, 7Safe (2008). *Good Practice Guide for Computer-Based Electronic Evidence*. UK ACPO and 7Safe.
2. Al-Azhar, M.N. (2010). *Standard Operating Procedure (SOP) 1 : Prosedur Pemeriksaan Digital Forensik*. DFAT Puslabfor.
3. Carrier, B. (2002). *Open Source Digital Forensic Tools: The Legal Argument.* @stake.
4. Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Elsevier Academic Press.
5. Cox, I. J. et al. (2008). *Digital Watermarking and Steganography*. Morgan Kaufmann
6. Johnson, T. A. (2005). *Forensic Computer Crime Investigation*. Taylor & Francis.
7. Konheim, A. G. (2007). *Computer Security and Cryptography*. Wiley
8. Middleton, B. (2002). *Cyber Crime Field Handbook*. CRC Press
9. National Institute of Justice (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. US National Institute of Justice
10. National Institute of Justice (2001). *Electronic Crime Scene Investigation: A Guide for First Responder*. US National Institute of Justice.

11. Sammes, T. and Jenkinson, B. (2007). *Forensic Computing: A Practitioner's Guide*. Springer.
12. Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Bab III

UU ITE : Tinjauan Perspektif Forensik dan Hukum

Hukum sangat dibutuhkan untuk membuat hal-hal yang diatur di dalam masyarakat menjadi tertata dan saling menghargai antara pihak yang satu dengan pihak yang lain di dalam koridor hukum tersebut, termasuk yang berkenaan dengan perkembangan ilmu pengetahuan dan teknologi komputer. Seperti diketahui perkembangan tersebut sangatlah pesat dan memiliki 2 (dua) wajah yang berbeda dalam hal pemanfaatannya, bisa berwajah positif (yaitu digunakan untuk kepentingan membantu masyarakat banyak) atau berwajah negatif (yaitu digunakan untuk melakukan kejahatan). Kondisi seperti inilah yang akhirnya memaksa masyarakat dan pemerintah untuk membuat suatu produk hukum yang dapat mengatur hubungan yang baik untuk sisi positifnya dan penegakan serta sangsi hukum untuk sisi negatifnya. Ini dimaksudkan agar semua pihak bisa memahami posisinya masing-masing untuk hubungan yang baik antara pihak yang satu dengan pihak yang lain, dan jika ada pihak yang merugikan pihak yang lain, maka hukum dapat mengatur langkah-langkah yang harus ditempuh untuk penegakan hukum dengan melakukan investigasi terhadap hal tersebut.

Investigasi dilakukan juga untuk mengetahui sejauh mana kerusakan atau kerugian yang ditimbulkan oleh pelaku kejahatan yang dialami oleh pihak yang merasa dirugikan. Sangsi hukum yang akan diberikan tentunya harus melihat sejauh mana efek dari tindakan pelaku terhadap korban yang memanfaatkan kemajuan ilmu pengetahuan dan teknologi komputer. Oleh karena kejahatan yang dilakukan berhubungan dengan teknologi komputer maka hukum yang ada juga seharusnya mengatur sejauh mana batasan-batasan yang berkaitan dengan teknologi tersebut. Untuk itu pada tahun 2008 dikeluarkanlah secara resmi Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, yang biasa disebut dengan Undang-Undang ITE. Batasan-batasan pengertian dan pelanggaran serta investigasi dinyatakan dengan jelas menurut kaidah dan bahasa hukum sehingga pelaksanaan penegakan hukum dapat berlangusng secara benar dan dapat hasil investigasinya nanti dapat dipertanggungjawabkan secara hukum di depan pengadilan.

Agar dapat memahami batasan-batasan tersebut, maka pada bab ini akan dibahas Undang-Undang tersebut dari tinjauan perspektif forensik dan hukum. Dengan sudut pandang ini, diharapkan pengertian-pengertian teknis yang berkaitan dengan ilmu pengetahuan dan teknologi komputer dapat dipahami dengan benar dan digunakan sesuai jalurnya (*on the track*) oleh *investigator* dan *forensic analyst* untuk mencari dan memberikan bukti-bukti digital yang diharapkan dapat mengungkap suatu kasus kejahatan dan menangkap serta menghukum pelakunya sesuai dengan tingkatan kejahatan yang dilakukannya. Dengan adanya Undang-Undang ini, aparat penegak hukum seperti *investigator* dan *forensic analyst* akhirnya memiliki pijakan hukum yang kuat untuk memberikan data-data digital yang bisa diakui sebagi alat bukti hukum yang syah untuk membuktikan keterlibatan pelaku dalam kejahatannya.

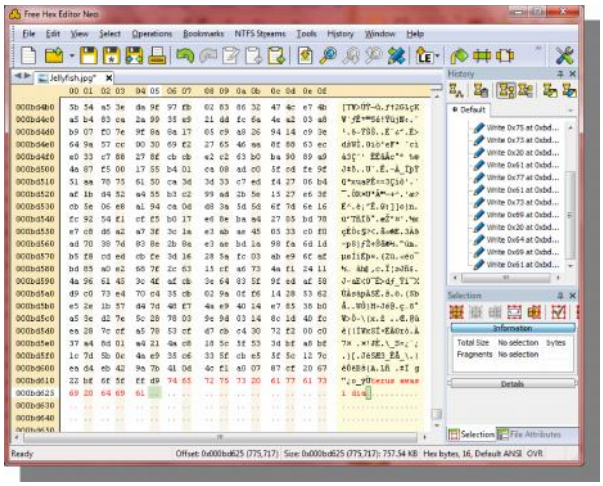
Pengertian Informasi Elektronik dan Dokumen Elektronik

Di Undang-Undang ITE, pasal 1 menjelaskan bahwa yang dimaksud dengan :

Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

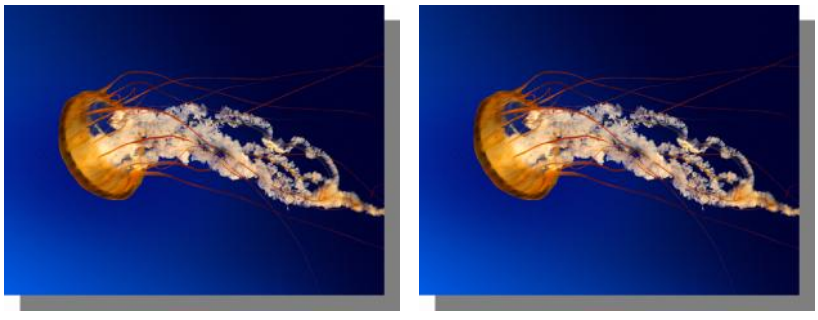
Dari pengertian di atas, syarat utama agar sesuatu digolongkan sebagai informasi elektronik adalah ia harus merupakan satu atau sekumpulan data elektronik yang telah diolah dan memiliki arti. Data elektronik adalah data digital yang bersumber dari perangkat elektronik yang berbasis komputasi. Data elektronik ini bersifat sangat luas, bisa berarti data-data dalam bahasa *binary* (berjumlah 8 *bit* yang terdiri dari 0 dan 1), heksadesimal (berjumlah 16 *bit* yang terdiri dari 0, 1, 2, 3, …s/d 9, a, b, …s/d f), teks (misalnya dengan bahasa *Unicode*, yaitu suatu bahasa pengkodean yang bersifat universal yang memetakan karakter-karakter yang umum dan khusus dalam bilangan heksadesimal), dan/atau berwujud data aplikasi (misalnya *office file*, *audio file*, *image file*, dan lain-lain).

Sebagai contoh, terdapat pesan rahasia yang terdiri dari beberapa kata yang disisipkan ke dalam *file* gambar berformat jpg dengan menggunakan teknik *steganography* yang *simple*. Teknik ini menggunakan aplikasi hex *editor* seperti *Free Hex Editor* Neo yang dikembangkan oleh HHD *Software*. Pada contoh ini, pesan rahasia tersebut berupa kalimat 'terus awasi dia' yang disisipkan di akhir dari *file* tersebut seperti pada gambar di bawah ini.



Gambar III.1. Penyisipan pesan rahasia di akhir dari *file* jpg dengan menggunakan *Hex Editor* Neo.

Penyisipan pesan dengan metode *steganography* tersebut secara umum tidak membawa efek yang berarti terhadap keutuhan gambar ketika ditampilkan seperti yang terlihat di bawah ini.



(i) (ii)

Gambar III.2. Gambar (i) adalah kondisi sebelum penyisipan, sedangkan gambar (ii) sesudah disisipkan pesan rahasia.

Jika *forensic analyst* dan *investigator* memeriksa dan menganalisa hanya didasarkan pada tampilan dari *file* jpg tersebut, maka pesan rahasia yang sangat penting yang dapat menunjukkan adanya komunikasi di antara pelaku dapat dipastikan tidak dapat diketahui. Untuk itu *forensic analyst* dan *investigator* di dalam menganalisa suatu gambar digital yang berasal dari barang bukti komputer pelaku harus melakukannya dengan teliti termasuk melihat isi *file* gambar tersebut dengan aplikasi *hex editor*. Aplikasi ini sangat baik untuk melihat isi dari suatu *file* secara lengkap termasuk data-data yang tidak tertampil ketika *file* tersebut diakses secara normal.

Ketika pesan rahasia tersebut dapat diketahui, maka pesan berupa kata-kata tersebut dapat digolongkan sebagai informasi elektronik karena memenuhi syarat seperti yang dijelaskan sebelumnya, yaitu :

1. Data elektronik. Pesan tersebut berupa tulisan atau kumpulan teks yang merupakan bahasa *Unicode* yang juga bisa dikonversikan ke dalam bahasa heksadesimal.
2. Yang telah diolah. Pesan tersebut telah melalui proses penyisipan dengan menggunakan metode *steganography* yang memakai aplikasi *hex editor*.
3. Yang memiliki arti. Pesan tersebut memiliki makna untuk memerintahkan si penerima pesan untuk mengerjakan sesuatu.
4. Termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi. Pesan tersebut termasuk pada bentuk kumpulan huruf-huruf/tanda.

Untuk *file* gambar yang merupakan *carrier* (yaitu *file* yang yang disisipkan/membawa pesan), ia dapat digolongkan sebagai informasi elektronik, karena ia juga memilik arti yang khusus, bukan sekedar tampilan gambar yang normal. Oleh karena itu, untuk contoh *file* jpg yang kedua ini, terdapat 2 (dua) informasi elektronik, yaitu pesan rahasia dan *carrier file* itu sendiri.

Pasal 1 juga memberikan pengertian tentang dokumen elektronik secara teknis. **Dokumen Elektronik** adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital,

elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Dari pengertian ini, sesuatu digolongkan menjadi dokumen elektronik jika ia memenuhi syarat :

1. Merupakan informasi elektronik.
2. Yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya.
3. Yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik.
4. Termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi.
5. Yang memiliki makna/arti.

Untuk contoh *carrier file* di atas, maka ia juga dapat digolongkan sebagai dokumen elektronik karena telah memenuhi syarat-syarat yang disebutkan di atas.

Berpijak pada penjelasan di atas, maka dapat disimpulkan bahwa setiap dokumen elektronik sudah pasti informasi elektronik, namun informasi elektronik belum tentu dokumen elektronik.

Di samping informasi elektronik dan dokumen elektronik, pasal 1 juga memberikan pengertian tentang **Sistem Elektronik**, yaitu serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik. Maksud dari pengertian ini adalah peralatan komputer yang telah dilengkapi dengan sistem operasi dan aplikasi, sehingga dapat digunakan untuk mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.

Alat Bukti Hukum

Berdasarkan penjelasan di atas mengenai informasi elektronik dan dokumen elektronik, maka ketika pesan rahasia berikut *file carrier*-nya tersebut menjadi bukti digital, maka keduanya yang dapat digolongkan menjadi informasi elektronik dan dokumen elektronik ini bisa menjadi alat bukti hukum yang syah di depan hukum/pengadilan. Hal ini tertuang pada pasal 5 Undang-Undang ITE. Pasal 5 ayat (1) berbunyi : **Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah**. Pasal ini di mata penulis sangatlah fenomenal, dalam artian aparat penegak hukum tidak lagi secara kaku menyandarkan alat bukti yang syah yang berjumlah 5 (lima) item sesuai Pasal 184 KUHAP (Kitab Undang-undang Hukum Acara Pidana) untuk temuan-temuan yang berupa data digital/elektronik.

Pasal 5 ini sudah mengakomodasi informasi dan dokumen elektronik tersebut sebagai alat bukti hukum yang syah, terlepas dari pasal 184 KUHAP yang membuat penggolongan alat bukti yang syah, yaitu keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa. Ini dijelaskan di ayat (2) bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. Hal ini juga diperkuat pada pasal 44 huruf b bahwa informasi elektronik dan dokumen elektronik merupakan alat bukti lain, selain alat bukti yang sebagaimana dimaksud dalam ketentuan perundang-undangan yang sudah ada.

Meskipun begitu, informasi dan dokumen elektronik juga harus memenuhi syarat-syarat seperti yang dijelaskan di Pasal 6 agar dianggap syah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan. Dari penjelasan ini, ada 4 (empat) syarat yang harus dipenuhi agar data digital yang ditemukan dapat dianggap sebagai oleh informasi dan dokumen elektronik, yaitu :

1. **Dapat diakses.**

   Ini maksudnya adalah data digital yang ditemukan dapat diakses oleh sistem elektronik.

2. **Dapat ditampilkan**

   Ini maksudnya adalah data digital tersebut dapat ditampilkan oleh sistem elektronik.

3. **Dijamin keutuhannya.**

   Ini maksudnya adalah bukti digital yang dihasilkan proses pemeriksaan dan analisa harus utuh isinya. Tidak hanya di kedua proses tersebut, namun ketika suatu barang bukti elektronik diakses pertama kali untuk proses akuisisi yang menghasilkan *image file*, isi dari barang bukti elektronik dan *image file* tersebut harus utuh, tidak boleh berubah, dan jikapun ada perubahan selama proses digital forensik berlangsung, *forensic analyst* dan *investigator* harus bisa menjelaskan apa yang berubah, dan tindakan apa yang dilakukan hingga itu berubah, serta alasan teknisnya. Keutuhan barang bukti elektronik, *image file* dan bukti digital dapat diukur dengan nilai *hash*, misalnya MD5 atau SHA1 yang didapat dari proses *hashing*.

   Di samping nilai *hash*, juga dibutuhkan adanya *time stamps* (*created* dan *modified date*) dari bukti digital untuk memastikan ada tidaknya modifikasi dan kapan pembuatannya pertama kali.

4. **Dapat dipertanggungjawabkan**

   Ini maksudnya adalah apa yang dihasilkan mulai dari proses akuisisi hingga analisa di dalam kegitan digital forensik dapat dipertanggungjawabkan, baik secara teknis keilmiahan maupun secara hukum.

   Untuk yang pertama, harus ada SOP yang disebutkan di dalam laporan pemeriksaan yang memuat tahapan-tahapan yang dikerjakan, sehingga ketika hasil yang ada di laporan tersebut dipertanyakan dan diuji ulang oleh pihak ketiga yang independen, seharusnya didapat hasil yang sama dengan menggunakan SOP yang sama.

   Untuk yang kedua yang menyangkut hukum, harus jelas level kompetensi dari *forensic analyst* dan *investigator* yang melakukan kegiatan digital forensik tersebut, sehingga bukti digital yang didapatkan dapat dianggap sebagai informasi elektronik dan/atau dokumen elektronik yang nantinya dapat diterima di depan pengadilan.

Investigasi

Undang-Undang ITE juga memuat hal-hal yang berkaitan dengan investigasi agar tahapan-tahapan investigasi yang dilakukan dapat diterima secara hukum, sehingga produk yang dihasilkan seperti bukti digital yang berasal dari barang bukti elektronik juga dapat diterima secara hukum. Beberapa hal mengenai investigasi yang diatur di dalam Undang-Undang ini adalah sebagai berikut :

1. **Penyidikan.**

   Yang diizinkan secara hukum untuk melakukan penyidikan tindak pidana teknologi informasi dan transaksi elektronik yang diatur di dalam Undang-Undang ini adalah penyidik Polri dan PNS yang lingkup tugas dan tanggungjawabnya di bidang tersebut. Hal ini disebutkan di dalam pasal 43 ayat (1).

   Di pasal 43 ayat (2) juga menjelaskan bahwa proses penyidikan di bidang tersebut haruslah memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data atau keutuhan data. Ini artinya keempat poin ini haruslah tetap diperhatikan selama proses penyidikan berlangsung. Jangan sampai proses penyidikan yang dilakukan malah membuat pelayanan publik menjadi terganggu atau sesuatu/informasi yang menyangkut privasi seseorang menjadi terbuka dan membuat malu orang tersebut.

   Di samping itu keutuhan data selama proses penyidikan memang harus diutamakan, sejak dimulai dari proses akuisisi hingga selesainya proses analisa yang menghasilkan bukti digital. Keutuhan *image file* dan bukti digital ini harus dapat ditunjukkan dengan nilai *hash* MD5 atau SHA1 dan *time stamps*-nya. Untuk mendapatkan nilai *hash* ini, dapat digunakan aplikasi-aplikasi, baik yang berbasis Windows seperti HashClac, maupun yang berbasis Linux, seperti md5sum.

2. **Penggeledahan dan penyitaan**

   Di pasal 43 ayat (3) disebutkan bahwa penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat.

3. **Penangkapan dan penahanan**

   Di pasal 43 ayat (6) juga dijelaskan bahwa dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam.

Tindak Pidana Teknologi Informasi dan Transaksi Elektronik

Tindak pidana teknologi informasi dan transaksi elektronik yang dimaksud di dalam undang-undang ini adalah antara lain mengenai perbuatan-perbuatan yang dilarang mulai dari pasal 27 hingga pasal 37. Tidak hanya mengatur perbuatan-perbuatan yang dianggap sebagai tindak pidana, undang-undang ini juga menjelaskan ancaman hukuman untuk tiap-tiap tindak pidana tersebut seperti yang ada di pasal 45 hingga pasal 51. Berikut penjelasan untuk masing-masing jenis tindak pidana berikut ancaman hukumannya.

Tindak Pidana	Ancaman Hukuman
Pasal 27 ayat (1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar *kesusilaan*. **Pasal 27 ayat (2)** Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan *perjudian*.	**Pasal 45 ayat (1)** Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah).

Pasal 27 ayat (3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau *pencemaran nama baik*. **Pasal 27 ayat (4)** Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan *pemerasan* dan/atau *pengancaman*.	
Pasal 28 ayat (1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan *berita bohong* dan *menyesatkan* yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik. **Pasal 28 ayat (2)** Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (*SARA*).	**Pasal 45 ayat (2)** Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah).
Pasal 29 Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi *ancaman kekerasan* atau menakut-nakuti yang ditujukan secara pribadi	**Pasal 45 ayat (3)** Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah).
Pasal 30 ayat (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum *mengakses* Komputer dan/atau Sistem Elektronik *milik Orang lain* dengan cara apa pun.	**Pasal 46 ayat (1)** Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah).

Pasal 30 ayat (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum *mengakses* Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk *memperoleh* Informasi Elektronik dan/atau Dokumen Elektronik. **Pasal 30 ayat (3)** Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum *mengakses* Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan *melanggar*, *menerobos*, *melampaui*, atau *menjebol sistem pengamanan*.	**Pasal 46 ayat (2)** Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 700.000.000,00 (tujuh ratus juta rupiah). **Pasal 46 ayat (3)** Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah).
Pasal 31 ayat (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan *intersepsi* atau *penyadapan* atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu *milik Orang lain*.	**Pasal 47** Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah).
Pasal 32 ayat (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun *mengubah*, *menambah*, *mengurangi*, *melakukan transmisi*, *merusak*, *menghilangkan*, *memindahkan*, *menyembunyikan* suatu Informasi Elektronik dan/atau Dokumen Elektronik *milik Orang lain* atau milik publik. **Pasal 32 ayat (2)** Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun *memindahkan* atau *mentransfer* Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik *Orang lain yang tidak berhak*.	**Pasal 48 ayat (1)** Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah). **Pasal 48 ayat (2)** Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp. 3.000.000.000,00 (tiga miliar rupiah).

Pasal 32 ayat (3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan *terbukanya* suatu Informasi Elektronik dan/atau Dokumen Elektronik yang *bersifat rahasia* menjadi dapat *diakses oleh publik* dengan keutuhan data yang tidak sebagaimana mestinya.	**Pasal 48 ayat (3)** Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 5.000.000.000,00 (lima miliar rupiah).
Pasal 33 Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat *terganggunya* Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi *tidak bekerja* sebagaimana mestinya.	**Pasal 49** Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 10.000.000.000,00 (sepuluh miliar rupiah).
Pasal 35 Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan *manipulasi*, *penciptaan*, *perubahan*, *penghilangan*, *pengrusakan* Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap *seolah-olah data yang otentik*.	**Pasal 51 ayat (1)** Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 12.000.000.000,00 (dua belas miliar rupiah).

Tabel III.1. Tabulasi tindak pidana teknologi informasi dan transaksi elektronik berikut ketentuan pidana yang memuat ancaman hukumannya.

Dari tabel di atas, dapat dilihat bahwa undang-undang ITE ini banyak memberikan penjelasan perbuatan atau pelanggaran yang berkaitan dengan informasi elektronik, dokumen elektronik dan/atau sistem elektronik, yang dapat digolongkan sebagai tindak pidana informasi dan transaksi elektronik, antara lain perbuatan tanpa hak :

1. Yang memiliki muatan yang melanggar kesusilaan
2. Yang memiliki muatan perjudian
3. Yang memiliki muatan pencemaran nama baik
4. Yang memiliki muatan pemerasan
5. Yang menyebarkan berita bohong
6. Yang menyebarkan informasi kebencian SARA
7. Yang berisi ancaman kekerasan secara pribadi

8. Yang mengakses sistem elektronik orang lain
9. Yang menjebol sistem pengaman dari sistem elektronik
10. Yang melakukan penyadapan
11. Yang mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik
12. Yang memindahkan infomasi dan/atau dokumen elektronik ke orang lain
13. Yang mengakibatkan terbukanya informasi dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik
14. Yang berakibat terganggunya sistem elektronik
15. Yang melakukan manipulasi informasi dan/atau dokumen elektronik seolah-olah data yang otentik

Perbuatan-perbuatan di atas yang dianggap sebagai tindak pidana teknologi informasi dan transaksi elektronik sebenarnya juga diatur di dalam undang-undang lain seperti KUHP (Kitab Undang-undang Hukum Pidana), oleh karena itu pelaksanaan penyidikan kasus yang berhubungan dengan perbuatan/pelanggaran ini sebaiknya memperhatikan secara komprehensif semua undang-undang yang berkaitan dengan hal tersebut.

Saksi Ahli

Dalam penyidikan tindak pidana teknologi informasi dan transaksi elektronik, penyidik harus bekerjasama dengan seseorang atau tim yang memiliki level kompetensi dan profesionalitas yang jelas di bidang digital forensik. Seseorang atau tim ini nantinya akan berhubungan dengan barang bukti elektronik, baik dimulai di TKP hingga di laboratorium. Hasil akhir dari kegiatan mereka diharapkan dapat menemukan bukti digital yang dapat digolongkan sebagai informasi elektronik dan/atau dokumen elektronik menurut undang-undang ITE, sehingga bukti digital ini dapat diterima sebagai alat bukti hukum yang syah oleh pengadilan. Untuk itu peranan mereka sangat signifikan sekali untuk membuat terang suatu kasus pidana teknologi informasi dan transaksi elektronik dan dapat

menghubungkan/mengkaitkan kasus tersebut dengan pelakunya secara ilmiah. Seseorang atau tim ini digolongkan sebagai ahli digital forensik.

Meskipun begitu ada syarat-syarat yang harus dipenuhi oleh seseorang agar ia dapat dikategorikan sebagai ahli. Menurut penjelasan Pasal 43 ayat (5) huruf h disebutkan bahwa YANG dimaksud dengan "**AHLI**" adalah seseorang yang memiliki keahlian khusus di bidang Teknologi Informasi yang dapat dipertanggungjawabkan secara akademis maupun praktis mengenai pengetahuannya tersebut. Ini artinya ada 2 (dua) syarat mutlak untuk menjadi ahli, yaitu :

1. **Syarat akademis**

   Ini maksudnya adalah ahli tersebut memiliki pendidikan formal, baik strata satu (S1) maupun pasca sarjana (S2 atau S3) di bidang ilmu pengetahuan komputer dan teknologi informasi, lebih baik lagi jika ia memiliki pendidikan formal khusus di bidang digital forensik. Untuk saat ini, pendidikan formal ini bisa didapat dari universitas-universitas di Indonesia untuk S1, dan di luar negeri untuk program pasca sarjana di bidang digital forensik.

   Selain pendidikan formal tersebut, syarat akademis tersebut juga dapat berupa *professional certification* seperti CHFI (*Computer Hacking Forensic Investigator*) dari EC-Council yang juga memiliki EC-Council *University* di Amerika Serikat. *Professional certification* ini berupa kursus singkat yang materinya bersifat komprehensif dan memiliki ujian di akhir kursus yang harus dilewati oleh peserta untuk dapat dinyatakan lulus dan berhak mendapatkan sertifikasi tersebut.

   Syarat akademis ini dimaksudkan agar ahli di dalam persidangan dapat memberikan pendapat-pendapat ilimiah secara teori dan praktis dengan benar dan bersifat independen, di samping dapat mempertanggungjawabkan bukti digital hasil pemeriksaan dan analisa digital forensik yang ia lakukan.

2. Syarat praktis

Syarat praktis di sini berkaitan dengan level pengimplementasian bidang digital forensik dari teori menjadi praktek. Teori dan praktek merupakan 2 (dua) hal yang berbeda, namun memiliki hubungan yang erat. Jika seseorang memiliki ilmu yang tinggi namun ia tidak pernah praktek sekalipun, maka ia tidak akan dapat mengimplementasikan ilmu teorinya dengan baik dan benar. Misalnya seseorang yang paham secara mendalam tentang teori berenang, namun ia sendiri tidak pernah mempraktekkan cara-cara berenangnya. Jika orang tersebut ketika nantinya dihadapkan pada kenyataan yang sesungguhnya, yaitu praktek berenang, maka dapat dipastikan ia tidak akan mampu berenang dengan baik, malah bisa jadi ia akan tenggelam. Analogi ini juga dapat digunakan untuk bidang digital forensik. Seseorang dianggap ahli di bidang digital forensik jika ia mampu memahami teori ilmu digital forensik dengan baik dan mampu mempraktekkannya juga dengan baik. Untuk itu syarat praktis di sini sangat mutlak diperlukan.

Syarat praktis secara umum dipengaruhi oleh 2 (dua) faktor, yaitu :

a. Lamanya waktu

   Seseorang yang berpengalaman di bidang digital forensik selama 5 tahun, pasti akan berbeda dengan seseorang yang memiliki 2 tahun pengalaman di bidang yang sama. Artinya semakin lama seseorang berkecimpung di bidang digital forensik, maka ia akan semakin berpengalaman secara praktis di bidang tersebut.

b. Jumlah kasus atau barang bukti

   Lamanya waktu sebenarnya tidak bersifat mutlak untuk menilai level pengalaman seseorang. Jumlah kasus atau barang bukti yang diperiksa dan dianalisa juga ikut mempengaruhi tingkat praktis seseorang di bidang digital forensik. Misalnya seseorang memiliki pengalaman 5 tahun dengan jumlah kasus yang diperiksa hanya 10 kasus, sedangkan di pihak lain ada seseorang yang memliki pengalaman Cuma 2 tahun, namun sudah memeriksa kasus sebanyak 50 kasus. Jika ini terjadi, maka dapat dilihat bahwa yang

junior (yang memiliki 2 tahun pengalaman) sebenarnya lebih berpengalaman di bidang digital forensik dibandingkan dengan yang senior (yang berpengalaman 5 tahun), karena si junior memiliki kasus yang diperiksa dan dianalisa lebih banyak dibandingkan si senior.

Syarat akademis dan praktis seperti yang dijelaskan di atas sangat mutlak diperlukan oleh seseorang untuk dapat dikategorikan sebagai ahli menurut Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Jika ia tidak memenuhi salah satu di antara keduanya, maka ia tidak dapat menjadi ahli di bidang teknologi informasi dan/atau digital forensik. Undang-undang mensyaratkan kedua hal tersebut karena ahli akan berhubungan dengan barang bukti elektronik dan digital yang sifatnya krusial dan penting karena dapat digunakan untuk mengungkap suatu kasus pidana secara ilmiah, artinya benar secara teori dan praktis dan prosedural secara aturan dan hukum.

Bibliography

1. ACPO, 7Safe (2008). *Good Practice Guide for Computer-Based Electronic Evidence*. UK ACPO and 7Safe.
2. Al-Azhar, M.N. (2010). *Standard Operating Procedure (SOP) 1 : Prosedur Pemeriksaan Digital Forensik*. DFAT Puslabfor.
3. Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Elsevier Academic Press.
4. Cox, I. J. et al. (2008). *Digital Watermarking and Steganography*. Morgan Kaufmann
5. Johnson, T. A. (2005). *Forensic Computer Crime Investigation*. Taylor & Francis.
6. Middleton, B. (2002). *Cyber Crime Field Handbook*. CRC Press
7. National Institute of Justice (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. US National Institute of Justice
8. National Institute of Justice (2001). *Electronic Crime Scene Investigation: A Guide for First Responder*. US National Institute of Justice.

9. Sammes, T. and Jenkinson, B. (2007). *Forensic Computing: A Practitioner's Guide*. Springer.
10. Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Bab IV

TRIAGE FORENSIC: First Response Procedure

Barang bukti elektronik seperti yang telah dijelaskan pada bab sebelumnya (misalnya komputer PC, *laptop/notebook*, *netbook*, *tablet*, *harddisk*, *flashdisk* dan lain-lain) sangat penting kedudukannya untuk dapat mengungkap suatu kasus *computer crime* (kejahatan komputer) maupun *computer-related crime* (kejahatan yang berhubungan dengan komputer sebagai salah satu barang buktinya), karena dari barang bukti elektronik inilah nantinya setelah melalui proses akuisisi, pemeriksaan dan analisa akan didapat barang bukti digital yang dapat membuat terang kasus kejahatan tersebut dan mengkaitkannya dengan pelaku. Namun barang bukti elektronik dan digital tersebut juga bersifat *volatile*, artinya mudah sekali berubah, rusak atau hilang baik oleh kegiatan yang disengaja maupun tidak disengaja. Jika penanganan barang bukti tersebut dilakukan secara tidak prosedural dan oleh orang yang tidak memiliki level kompetensi yang cukup di bidang digital forensik, maka sangat memungkinkan bukti digital yang sebelumnya ada tersimpan di dalam barang bukti elektronik dapat berubah, rusak atau bahkan hilang sehingga tidak dapat di-*recover* kembali. Jika ini terjadi, maka kesempatan *investigator* untuk mengungkap kasus tersebut menjadi sulit, atau bahkan kasus tersebut menjadi gelap (*The X File*).

Forensic analyst dan *investigator* tidak menginginkan hal ini terjadi, oleh karena itu dibuatlah suatu prosedur penanganan awal barang bukti elektronik di TKP yang menjadi panduan bagi siapapun, khususnya aparat penegak hukum untuk dapat melaksanakan kegiatan penanganan tersebut secara prosedural. Prosedur tersebut dikenal dengan istilah *Triage* Forensik. Istilah ini sejatinya mengambil kosa kata ilmu kesehatan, yaitu *triage* yang berarti tata cara penanganan pasien untuk pertama kali dalam berbagai kondisi, misalnya pasien pingsan, luka memar, luka bakar akibat panas api, selamat dari tenggelam dan lain-lain. Dengan *triage* ini, diharapkan tenaga paramedis atau masyarakat umum yang paham triage dapat membantu, atau bahkan menyelamatkan nyawa pasien di saat-saat kritis. Istilah ini kemudian diadopsi di bidang digital forensik

menjadi *triage* forensik dengan objek perlakuan adalah berupa barang bukti elektronik dengan tujuan untuk menyelamatkan bukti-bukti digital yang penting untuk investigasi.

Triage forensik juga memiliki tujuan untuk mendapatkan data-data digital secara cepat dari barang bukti elektronik. Ini dimaksudkan agar investigator dapat menentukan langkah investigasi lanjutan dengan benar dan secara cepat dapat melacak keberadaan pelaku dan menangkapnya. Seperti diketahui bahwa proses digital forensik, mulai dari tahapan penerimaan barang bukti elektronik, akuisisi, pemeriksaan, analisa, laporan hingga penyerahan kembali barang bukti tersebut, memakan waktu yang cukup lama. Hal ini berimbas pada kecepatan investigator yang menjadi lambat untuk menentukan tahap investigasi selanjutnya, yang bisa jadi mungkin akan memberikan waktu yang cukup bagi pelaku untuk menghilangkan jejak kejahatannya atau bahkan melarikan diri.

Berdasarkan penjelasan di atas, *triage* forensik memiliki 2 (dua) tujuan akhir yang penting, yaitu :

1. Menyelamatkan bukti digital yang bersifat *volatile*
2. Memberikan bukti digital secara cepat kepada *investigator* dan *forensic analyst*

Meskipun begitu, *triage* forensik dalam prakteknya tetap harus memperhatikan prinsip-prinsip digital forensik seperti yang dijelaskan pada bab sebelumnya.

Prosedur penanganan awal komputer dalam keadaan off (mati)

Prosedur penanganan pertama kali terhadap barang bukti elektronik berupa komputer dalam keadaan *off* (mati) pada prinsipnya sama seperti yang telah dijelaskan sebelumnya di Bab II. Tahapan-tahapan yang telah dijelaskan di bab tersebut harus dipatuhi dan diikuti oleh *forensic analyst* dan *investigator* untuk menjaga keutuhan isi digital dari barang bukti komputer tersebut. Satu hal yang kembali ditekankan di sini adalah 'JANGAN PERNAH MENGHIDUPKAN KEMBALI BARANG BUKTI KOMPUTER YANG DITEMUKAN DALAM KEADAAN SUDAH MATI (*OFF*)'. Karena jika ini dilakukan, maka itu berarti akan mengubah isi *harddisk* dari barang bukti komputer tersebut, dan hal ini bertentangan dengan prinsip pertama digital forensik.

Prosedur penanganan awal komputer dalam keadaan on (hidup)

Untuk barang bukti elektronik berupa komputer yang ditemukan dalam keadaan masih hidup (*on*), prosedur penanganannya pada prinsipnya juga sama dengan tahapan-tahapan yang telah dijelaskan sebelumnya di Bab II. Meskipun begitu ada 2 (dua) hal yang kembali ditekankan di sini, yaitu :

1. Penggunaan *triage tools* sebenarnya dapat mengubah sebagian kecil isi dari *harddisk* barang bukti komputer tersebut. Untuk itu, *forensic analyst* dan *investigator* harus tahu apa saja yang mungkin berubah dan mampu menjelaskan bahwa perubahan tersebut tidak berpengaruh kepada informasi lain atau bukti digital yang sedang dicari. Misalnya ketika *forensic analyst* dan *investigator* menghubungkan *flashdisk* ke *port* USB barang bukti komputer dalam rangka untuk menyimpan hasil dari proses triage, maka hal tersebut sebenarnya mengubah sedikit informasi dari sistem *registry* komputer tersebut. Hal ini masih diperkenankan karena diperkirakan tidak akan banyak merubah data-data digital yang lain.
2. Penggunaan *triage tools* harus dilakukan secara ketat. Artinya tidak boleh mengakses isi *harddisk* secara tidak prosedural, misalnya membuka jendela *windows explorer* pada komputer yang berbasis Windows, kemudian membuka *file-file* secara normal. Ini dapat mengakibatkan banyak perubahan pada isi *harddisk*. Dan ini tidak diperbolehkan. Membuka *file* hanya boleh dilakukan setelah *file* tersebut sudah di-ekspor ke tempat lain.

Triage tools

Setelah memahami esensi dari *triage*, maka penggunaan *triage tools* diharapkan dapat memberikan banyak data digital secara cepat kepada *forensic analyst* dan *investigator*, tanpa banyak melakukan perubahan isi dari *harddisk* komputer tersebut.

Ada beberapa *triage tools* yang sering digunakan oleh forensic professional secara internasional, yaitu :

1. **Helix *Forensic*** dari e-fense, yang bisa diakses di www.e-fense.com.

   Helix memiliki 2 (dua) wajah yang diperuntukkan sesuai dengan *platform*-nya, yaitu :

   a. Wajah berbasis Windows, yang dapat digunakan untuk kegiatan *triage* terhadap barang bukti komputer yang memiliki sistem operasi Windows.

   b. Wajah berbasis Linux, yang bersifat *bootable* sehingga dapat digunakan untuk menjalankan *platform* Linux secara *live* di *analysis workstation* (yaitu komputer yang difungsikan untuk menganalisa barang bukti).



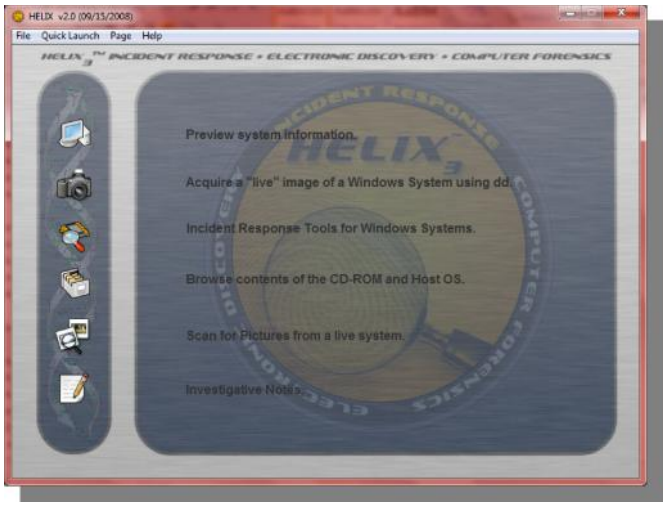
Gambar IV.1. *Screenshot* situs e-fense yang menyediakan aplikasi Helix *Forensic*.

Berikut adalah prosedur *triage* dengan menggunakan Helix Forensic :

a. Siapkan Helix *Forensic* dalam wujud CD atau *flashdisk*.

b. Masukkan CD Helix tersebut ke CD *drive* dari barang bukti komputer yang sedang on, sedangkan *flashdisk* Helix dipasangkan di *port* USB.

c. Jalankan *file* helix.exe untuk masuk ke aplikasi Helix berbasis Windows seperti gambar di bawah ini.



Gambar IV.2. *Screenshot* Helix v2.0 yang diluncurkan pada 15 September 2008, sedangkan saat ini sudah ada Helix v3.0.

d. Ada 6 (enam) *icon* yang disesuaikan dengan peruntukannya masing-masing, yaitu :
    1) *Peview system information*, untuk melihat informasi yang berkaitan dengan sistem yang sedang *running* di barang bukti komputer, seperti jenis sistem operasi, *file system*, partisi dan lain-lain.
    2) *Live acquisition*, untuk melakukan *forensic imaging* terhadap *harddisk* atau partisi, bahkan RAM dari komputer tersebut.
    3) *Incident response*, antara lain untuk *disk preview* (melihat isi *harddisk*), *snapshot* (melihat kondisi *live* komputer, misalnya proses, *services*, *network devices*, *user accounts*, *installed software*, *processors*, *physical disks* dan lain-lain), RAM *imaging*, *backup event logs* (seperti aplikasi, sekuriti dan sistem), *file recovery* (untuk *deleted files*), *on/off time* (memuat historis penggunaan komputer *on/off*, khususnya dalam rentang 3 minggu terakhir), USB *deview* (memuat historis penggunaan *port* USB untuk akses media

penyimpanan seperti *flashdisk*, *harddisk*, atau bahkan *handphone/smartphone* yang memiliki *memory card*).

Ada juga untuk melihat historis penggunaan *internet browser* seperti *Internet Explorer* dan Firefox, namun historis Firefox tidak bisa digunakan untuk Firefox v4 dan v5 karena hanya bisa akses untuk Firefox v3.

4) *Browse contents*, untuk melihat isi *harddisk* atau masing-masing partisi di mana masing-masing *file* dilengkapi dengan *time stamps* (*created*, *modified* and *accessed date*) dan nilai *hash* CRC dan MD5.
5) *Pictures scanning*, untuk mendapatkan gambar-gambar yang ada di *harddisk* komputer, meskipun ada gambar yang *hidden* (tersembunyi). Hal ini penting untuk kasus yang berkaitan dengan pornografi. Teknik ini akan mempercepat pencarian gambar-gambar yang memuat konten tersebut, sehingga *forensic analyst* dan *investigator* dapat dengan cepat memutuskan langkah investigasi lebih lanjut terhadap pemilik komputer.
6) *Investigative notes*, untuk memberikan catatan-catatan penting yang terkait dengan barang bukti komputer yang sedang dianalisa.

2. **COFEE (*Computer Online Forensic Evidence Extractor*)** dari Microsoft, yang bisa diakses di http://www.microsoft.com/industry/government/solutions/cofee/default.aspx.

COFEE untuk kegiatan *triage* dijalankan lewat *flashdisk*, untuk itu melalui COFEE, dipersiapkan *flashdisk* yang nantinya akan di-install aplikasi-aplikasi *triage* (jumlah total aplikasi adalah 154) sesuai dengan *mode*-nya (misalnya *Fast* dengan 71 aplikasi, *Mini-incident response* dengan 30 aplikasi, Normal dengan 125 aplikasi dan *Custom*).



Gambar IV.3. *Screenshot* situs Microsoft yang menyediakan COFEE yang disediakan khusus untuk aparat penegak hukum di seluruh dunia.

Berikut antara lain aplikasi-aplikasi yang disediakan oleh COFEE :

a. mem.exe, untuk menampilkan penggunaan memori.
b. smbios.exe, untuk mengumpulkan data tentang BIOS (*Basic Input Output System*), misalnya *processor*, RAM, tanggal/waktu dan lain-lain.
c. CacheDump.exe, untuk melihat historis penggunaan *Internet Explorer*.
d. ipconfig.exe, untuk mendapatkan data tentang konfigurasi jaringan.
e. net.exe, untuk melihat informasi *network user accounts* dan *administrator*.
f. LastLogon.exe, untuk mendapatkan informasi *logon* terakhir.
g. whoami.exe, untuk menampilkan informasi *user* saat ini.
h. pslist.exe, untuk melihat daftar proses-proses yang sedang *running*.
i. sclist.exe, untuk mendapatkan daftar *service-service* yang sedang jalan.
j. drivers.exe, untuk melihat *driver-driver* yang sudah ter-*install*.
k. reg.exe, untuk mendapatkan data-data *registry*, antara lain tentang URL-URL (*Uniform Resource Locator*) situs yang sudah diketikkan,

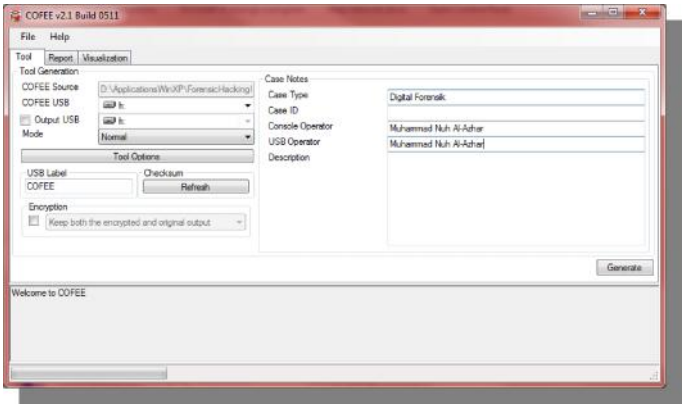
LastSave (yang disimpan terakhir), parameter dari TCP/IP (*Transmission Control Protocol/Internet Protocol*), media-media penyimpanan yang di-*mounting* pada *port* USB, dan lain-lain.

l. psloglist.exe, untuk menampilkan *log-log* yang merekam kejadian (*events*) pada sistem, aplikasi dan sekuriti).

m. extractusb.exe, untuk meng-ekstrak informasi yang berkaitan dengan *device* (peralatan) yang ter-*mounting* pada port USB.

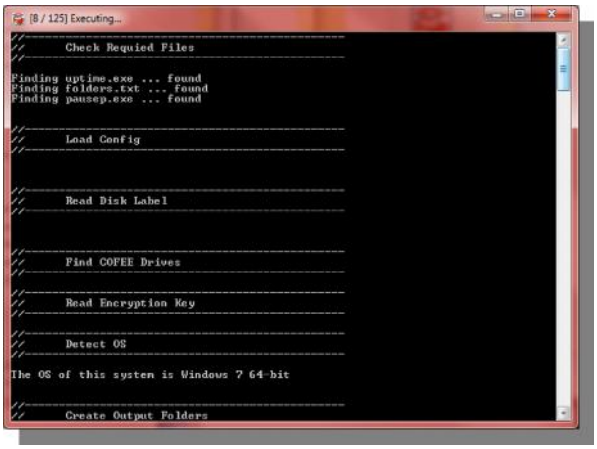
n. ports.exe, untuk mendapatkan daftar *port-port* berikut program yang menggunakannya.

o. vdd.exe, untuk mendeteksi keberadaan *virtual disk* yang biasa digunakan sebagai *virtual system*.



Gambar IV.4. Persiapan untuk meng-*install* aplikasi COFEE dengan *mode* Normal.

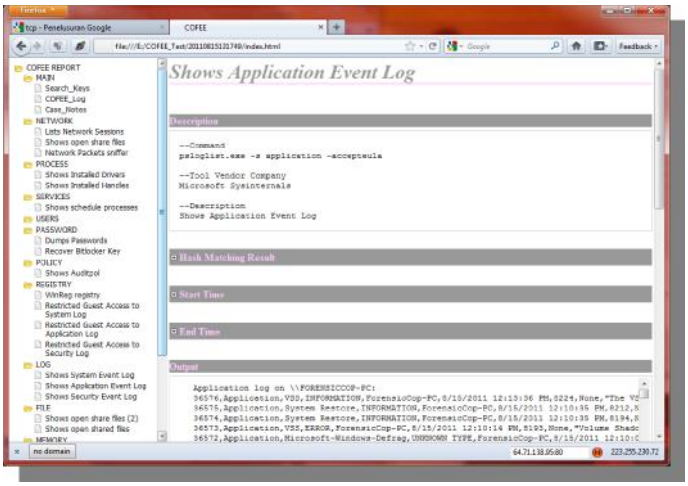
Setelah proses instalasi COFEE selesai, maka akan didapat *flashdisk* yang bisa digunakan untuk kegiatan *triage*, yaitu dengan me-*mounting* (memasangkan) *flashdisk* tersebut ke *port* USB dari barang bukti komputer, kemudian jalankan COFEEUSB.exe untuk membukan jendela terminal yang secara otomatis menampilkan proses-proses yang sedang berlangsung.



Gambar IV.5. Terminal yang menunjukkan aplikasi COFEE yang sedang *running*, yang dalam contoh ini adalah COFEE dengan *mode* Normal.

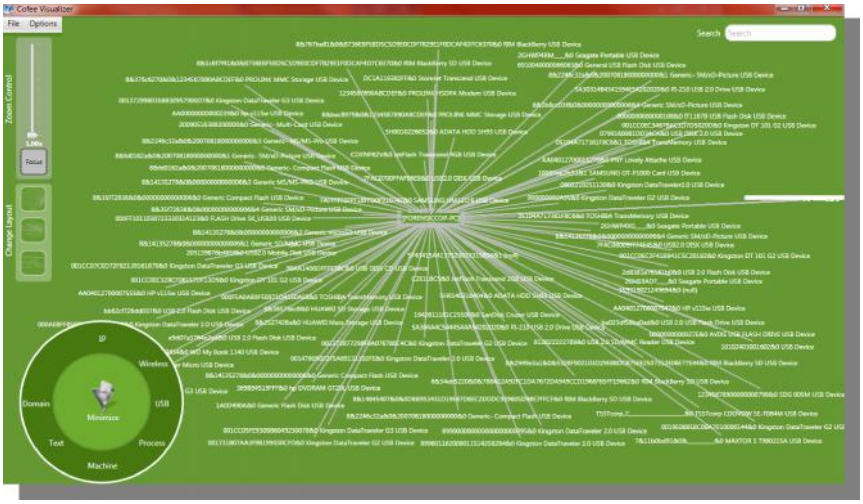
Setelah proses *triage* dengan COFEE selesai, maka jendela terminal akan hilang dengan sendirinya dan di dalam *flashdisk* COFEE akan dihasilkan satu *folder* baru dengan penamaan *folder* berdasarkan nama komputer yang dianalisa dan tanggal/waktu proses *triage* dilakukan.

Untuk melihat hasil proses triage yang dilakukan terhadap barang bukti komputer tersebut, *flashdisk* COFEE tersebut di-*mounting* di *analysis workstation*, kemudian jalankan aplikasi COFEE, dan pilih *tab Report* dengan *input folder* yang dihasilkan dari proses *triage*. Setelah proses *generation* selesai, maka laporan hasil proses *triage* dari barang bukti komputer dapat dilihat untuk dianalisa lebih lanjut oleh *forensic analyst* dan *investigator*.



Gambar IV.6. Laporan hasil *triage* yang dilakukan dengan COFEE.

COFEE juga memberikan suatu *feature* (kelebihan), yaitu adanya bentuk visualisasi yang menghubungkan barang bukti komputer yang satu dengan yang lain untuk hal-hal yang spesifik, misalnya IP *address*, *domain* (nama situs), USB, *wireless* dan *specific words* (kata-kata yang sama). Dengan visualisasi ini, *forensic analyst* dan *investigator* akan lebih mudah dan cepat untuk mencari keterkaitan antar barang bukti komputer dan mengkerucutkannya ke hal yang lebih khusus seperti yang disebutkan di atas.



Gambar IV.7. Bentuk visualisasi COFEE untuk pencarian media penyimpanan yang pernah ter-*mounting* di *port* USB dari barang bukti komputer.

3. **FieldSearch dari Justnet** yang berada di bawah NIJ (*National Institute of Justice*), yang bisa diakses di http://www.justnet.org/Pages/fieldsearch.aspx, yang dikembangkan oleh PMInvestigations bekerja sama dengan KBSolutions.

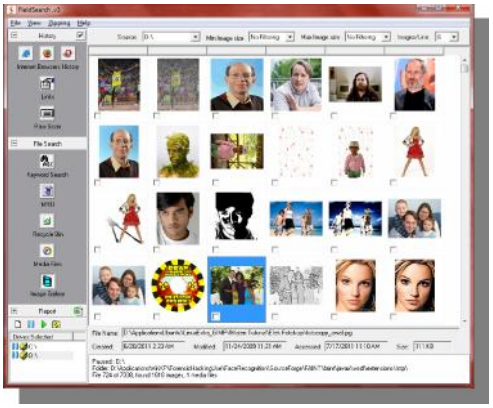
   FieldSearch adalah aplikasi *triage* yang lebih memfokuskan untuk pencarian data digital secara cepat pada *file-file* multimedia (seperti gambar dan video) dari barang bukti komputer yang sedang *on*. Di samping itu FieldSearch juga dapat digunakan untuk mencari data yang terkait dengan historis penggunaan *internet browser* (seperti *Internet*

Explorer, Firefox dan Opera) dan MRU (*Most Recent Use*), yaitu *file-file* yang terakhir kali diakses, serta analisa *Recycle Bin* (tempat penampungan sementara *file-file* yang sudah dihapus). Jika melihat *layout* dan *feature* dari aplikasi ini, FieldSearch sangat baik sekali digunakan untuk proses *triage* barang bukti komputer yang berisikan *file-file* multimedia yang berkonten pornografi.

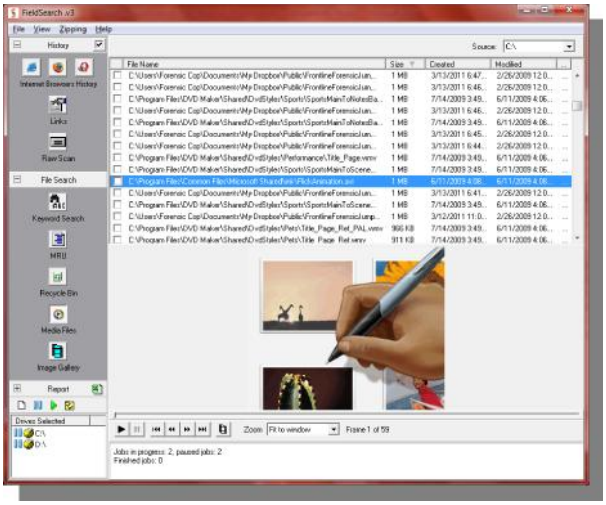


Gambar IV.8. *Screenshot* situs Justnet yang menyediakan aplikasi FieldSearch.

Setelah FSWin.exe diakses, akan muncul jendela FieldSearch. Sebelum memulai explorasi data, diperlukan adanya proses *scanning* terlebih dahulu terhadap *harddisk* atau partisi dari barang bukti komputer yang mungkin akan memakan waktu yang cukup lama. Setelah proses *scanning* ini selesai, *forensic analyst* dan *investigator* dapat melakukan pencarian dengan cepat data-data digital seperti yang disebutkan di atas yang ada kaitannya dengan kasus.



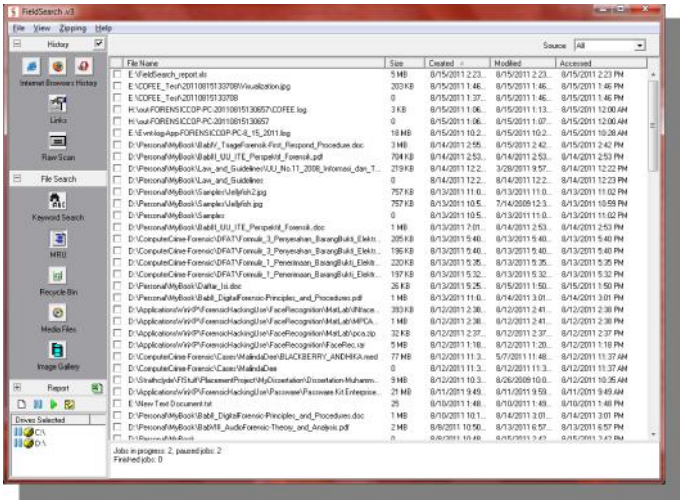
Gambar IV.9. Hasil pencarian *file-file* gambar dengan FieldSearch



Gambar IV.10. Hasil pencarian terhadap *file-file* video dengan menggunakan FieldSearch di mana *file-file* ini bisa langsung dilihat isinya di jendela yang di bawah.

Dari kedua gambar di atas, bisa dilihat FieldSearch menyediakan kemudahan bagi *forensic analyst* dan *investigator* untuk mencari *file-file* gambar dan video yang berkaitan dengan kasus, misalnya kasus pornografi. *File-file* tersebut juga dilengkapi dengan keterangan yang penting, misalnya *time stamps* (yaitu *created*, *modified* dan *accessed date*), sehingga bisa diketahui kapan *file-file* tersebut berada di barang bukti komputer untuk pertama kali dan kapan terakhir kali *file-file* tersebut dimodifikasi.

Seperti dijelaskan di atas, FieldSearch juga memberikan informasi mengenai MRU, yaitu *file-file* yang digunakan untuk waktu-waktu terakhir. Artinya *forensic analyst* dan *investigator* dapat dengan cepat mengetahui *file-file* apa saja yang diakses, dibuat ataupun dimodifikasi terakhir kali atau pada tanggal-tanggal tertentu yang diinginkan. Ini sangat bagus sekali untuk digunakan dalam proses *triage* untuk membuktikan keterlibatan seseorang melalui analisa komputernya yang berkaitan dengan *file-file* yang dicari.



Gambar IV.11. Hasil FieldSearch untuk *file-file* MRU dilengkapi dengan *time stamps*.

Di samping hal-hal yang dijelaskan di atas, sama seperti Helix, FieldSearch juga memberikan *feature* untuk melihat historis penggunaan *internet browser* seperti *Internet Explorer*, Firefox dan Opera yang sering digunakan oleh *netter* si seluruh dunia.

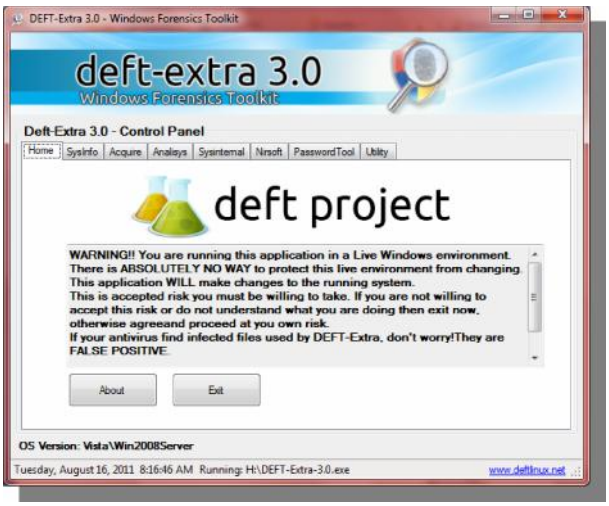
4. **DEFT (Digital Evidence Forensic Tool) Extra** dari DEFT Linux, yang bisa diakses di http://www.deftlinux.net/.

   Sama seperti Helix *Forensic*, DEFT juga memiliki 2 (dua) wajah, yaitu wajah Windows dan Linux. Wajah Windows digunakan ketika menjalankan proses *triage* terhadap barang bukti komputer yang sistem operasinya berbasis Windows, sedangkan wajah Linux yang *bootable* digunakan untuk melakukan *booting* (proses menghidupkan komputer) untuk masuk ke sistem operasi Linux dalam rangka kegiatan digital forensik seperti akuisisi, pemeriksaan dan analisa.



Gambar IV.12. *Screenshot* situs DEFT Linux yang menyediakan DEFT *Extra*.

Setelah CD DEFT dimasukkan ke dalam CD/DVD *drive* dari barang bukti komputer (jika komputer tersebut tidak memliki CD/DVD *drive*, maka *forensic analyst* dan *investigator* semestinya membawa CD/DVD eksternal atau menyiapkan DEFT dalam bentuk *flashdisk*), jalankan *file* DEFT-Extra-3.0.exe untuk memulai aplikasi DEFT.

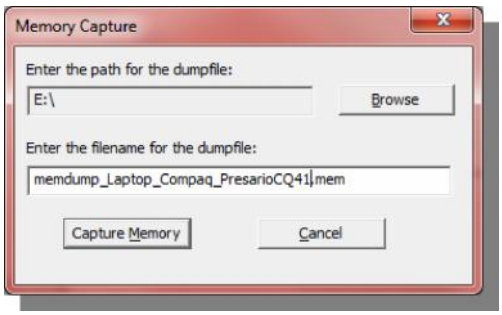


Gambar IV.13. Jendela muka DEFT dengan pengelompokkan *tab developer* aplikasi-aplikasi digital forensik, seperti Nirsoft dan Sysinternal, di samping pengelompokkan fungsi forensiknya masing-masing.

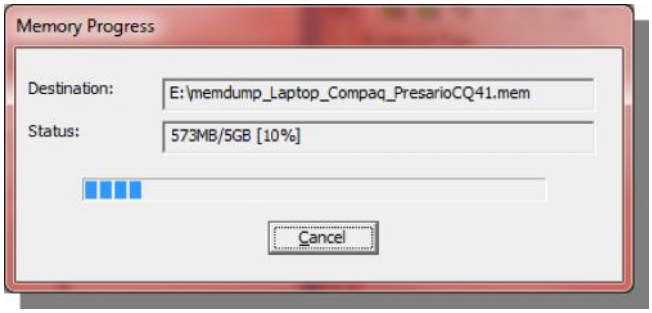
Berikut adalah fungsi-fungsi forensik yang bisa dijalankan dari aplikasi DEFT :

a. *System Information*, untuk mendapatkan informasi lengkap dari sistem yang sedang *running* pada barang bukti komputer, antara lain :
    1) *System overview*, yang menampilkan data-data tentang sistem operasi, manufaktur, model, *serial number* dari komputer tersebut, termasuk *processor*, memori, *harddisk* dan waktu lokal.
    2) *Software-software* Windows dan aplikasi-aplikasi dari *vendor* lain yang ter-*install*.
    3) Sekuriti, yang antara lain memuat data-data *port* yang terbuka, *internet software* (seperti *browser* dan *mail client*), dan *windows firewall*.
    4) *Groups* atau *users* yang ada di komputer tersebut, termasuk data *logon* terkahir kali, jumlah *logon* dan lain-lain.
    5) *Network* TCP/IP, yang memuat data-data *network* DNS (*Domain Name Server*) *host name*, DHCP (Dynamic *Host Configuration Protocol*) IP *address*, MAC (*Media Access Control*) *address* dan lain-lain untuk masing-masing *adapter*.
    6) *Hardware devices*, yang memuat informasi mengenai *hardware* yang terpasang di komputer tersebut, misalnya *disk drives*, *network adapters*, *portable devices*, *processors*, dan lain-lain.
    7) *Services*, yang menampilkan data-data tentang *driver* dan proses-proses yang ter-*install* serta program-program yang sedang *running* (berjalan).
b. *Acquisition*, untuk melakukan proses *forensic imaging*, baik terhadap RAM ataupun *harddisk* dari komputer tersebut. Dengan salah satu aplikasi yang ada di DEFT, *forensic analyst* dan *investigator* dapat menyelamatkan isi RAM yang sangat *volatile*

ketika barang bukti komputer tersebut dalam keadaan *on* (hidup). Artinya jika barang bukti komputer dimatikan, maka informasi yang tersimpan di RAM juga akan hilang. Sangat memungkinkan RAM tersebut memiliki informasi penting terkait dengan kasus yang sedang di-investigasi, oleh karena itu salah satu fungsi *triage* yang sangat penting adalah menyelamatkan isi RAM melalui *forensic imaging*. Pada proses RAM *imaging*, dibutuhkan media penyimpanan yaitu *flashdisk* atau *harddisk* eksternal untuk menyimpan *file* hasil dari proses tersebut. Jika RAM dari barang bukti komputer tersebut, misalnya 4GB, maka dibutuhkan media penyimpanan lebih dari 4 GB.



Gambar IV.14. *Screenshot* jendela untuk memulai proses RAM *imaging*.

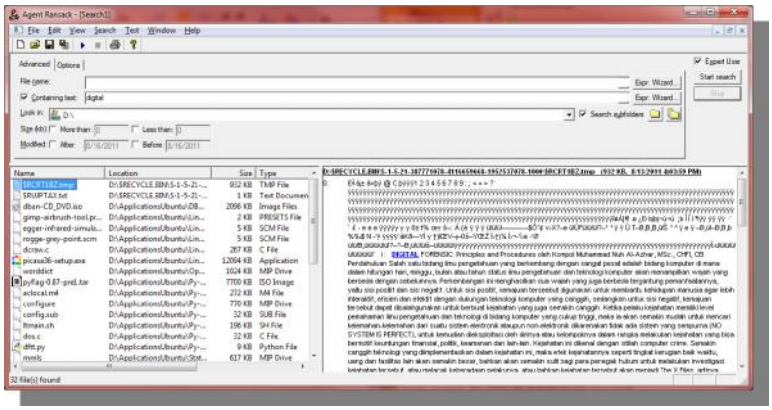


Gambar IV.15. *Screenshot* jendela proses RAM *imaging* yang sedang *running*.

Untuk proses *imaging* terhadap *harddisk* dari barang bukti komputer, bisa dilaksanakan secara *live* (langsung) atau dalam keadaan *dead-state* (dalam keadaan komputer sudah mati, kemudian *harddisk*-nya diambil dan melalui kabel data

dihubungkan dengan *analysis workstation* untuk proses *forensic imaging*). Seperti dijelaskan pada bab sebelumnya bahwa *forensic imaging* harus dilakukan secara *physical* atau sektor per sektor (*bit stream copy*) dan harus diverifikasi nilai *hash* dari *image file* hasil dari *forensic imaging* tersebut dengan *harddisk* barang bukti komputer. Nilai *hash* dari *image file* dan *harddisk* haruslah sama, artinya proses *imaging* sukses membuat *image file* yang identik dengan isi *harddisk* tersebut.

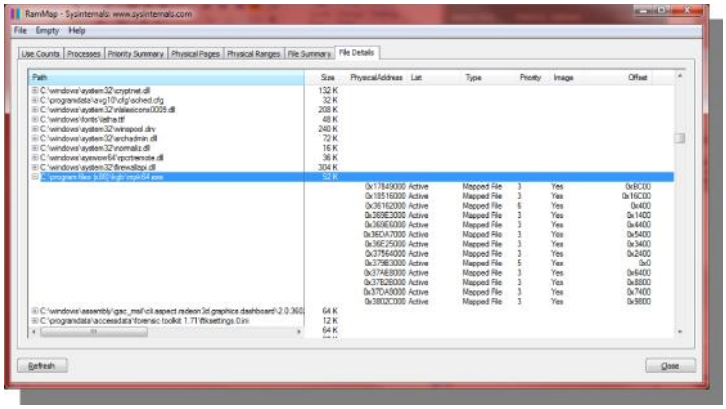
c. *Analysis*, salah satu teknik analisis yang disediakan di DEFT ini adalah pencarian *file* yang berbasis isinya (*contents-based searching*). Teknik ini sangat membantu *forensic analyst* dan *investigator* untuk mempersempit dan mempercepat pencarian terhadap *file-file yang* memiliki isi berupa data-data yang diinginkan dari sekian banyak *file* yang ada.



Gambar IV.16. Hasil pencarian berbasis isi terhadap seluruh *file-file* yang tersimpan di suatu partisi.

Teknik ini memudahkan *forensic analyst* dan *investigator* untuk melihat isi dari *file-file* yang hasil *keyword searching*-nya sama tanpa perlu membukanya sama sekali. Hal ini mempersingkat waktu untuk mendapatkan file yang isinya seperti yang diinginkan dalam investigasi.

d. Sysinternal, merupakan produk dari Microsoft yang menyediakan aplikasi-aplikasi yang antara lain dapat digunakan untuk kepentingan *triage*, misalnya analisa RAM dari barang bukti komputer.



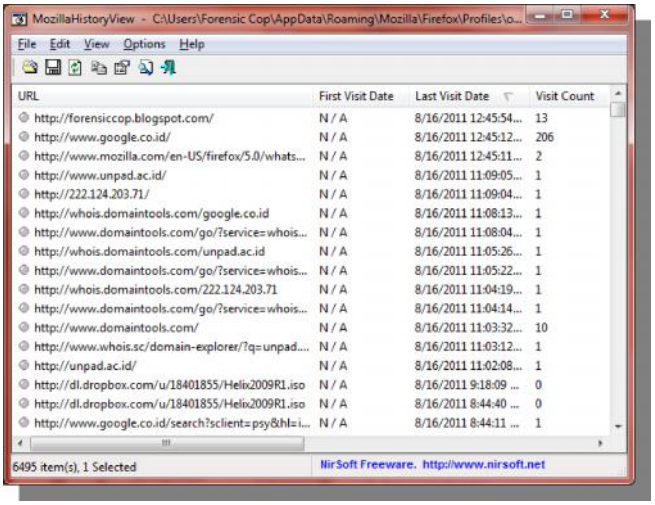
Gambar IV.17. *Screenshot* jendela aplikasi untuk analisa RAM yang dipetakan secara detil.

Pemetaan RAM yang disediakan oleh Sysinternal ini lumayan lengkap mulai dari proses-proses yang sedang *running*, *physical address* (aktif, *stand by*, atau *zero*/tidak digunakan), *physical range* dengan *size* (ukuran) besar memorinya, ringkasan *file* dengan *size* alokasi memorinya, hingga data detil dari masing-masing *file*, misalnya *physical address* yang digunakan berikut nomor *offset*-nya.

Selain aplikasi untuk analisa RAM, terdapat juga aplikas-aplikasi lain seperti untuk memonitor aktivitas-aktivitas *file system* secara *real time*, untuk memonitor aplikasi-aplikasi yang mengakses *sistem registry* dari komputer tersebut, dan lain-lain.

e. Nirsoft, merupakan salah satu *developer* yang terkenal untuk aplikasi-aplikasi digital forensik. Di bawah ini antara lain aplikasi-aplikasi yang bisa digunakan untuk mendapatkan data secara cepat lewat prosedur *triage* :

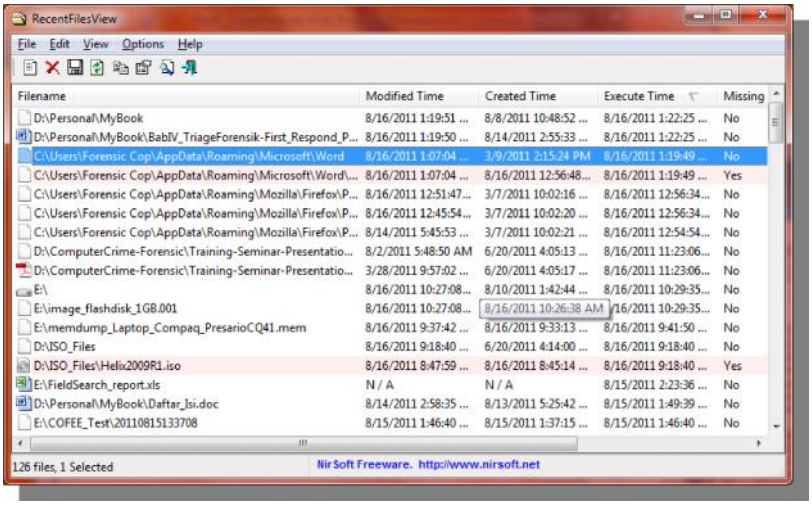
    1) Historis penggunaan *internet browser* seperti Chrome, Firefox, Opera dan *Internet Explorer*.



Gambar IV.18. Historis penggunaan Mozilla Firefox v5 berikut tanggal/waktu kapan akses ke suatu situs dilakukan.

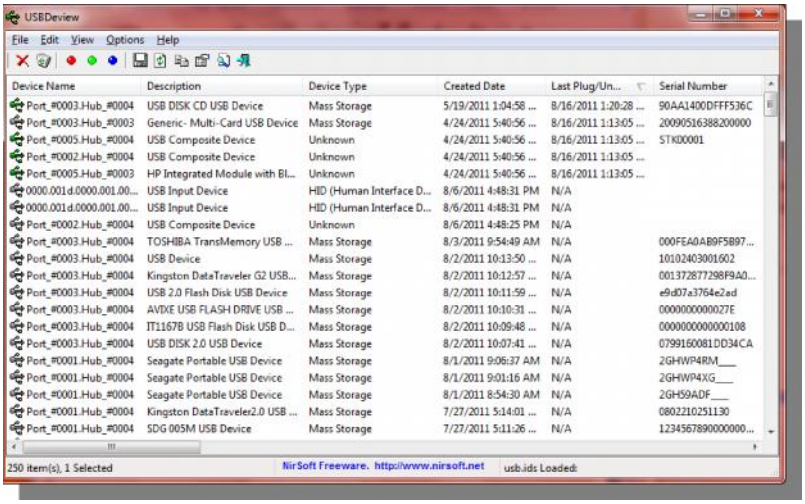
Dengan adanya aplikasi ini, hal ini memudahkan bagi *forensic analyst* dan *investigator* untuk mendapatkan data secara cepat mengenai penggunaan *internet browser* dari barang bukti komputer tersebut, untuk selanjutnya dapat digunakan sebagai bahan untuk mengklarifikasi atau bahkan meng-*counter* pernyataan dari pelaku.

2) Historis *file-file yang* pernah dibuka atau diakses, termasuk dalam rentang beberapa waktu terakhir. Ini bisa digunakan oleh *forensic analyst* dan *investigator* untuk memastikan pelaku atau pemilik barang bukti komputer apakah dia pernah membuka atau mengakses *file* yang dicari atau tidak. Data ini dilengkapi dengan *time stamps*, yaitu *modified date*, *created date* dan *execute date* kapan *file-file* tersebut diakses, di samping *path file* yang lengkap, termasuk *drive letter* dan informasinya. Misalnya *file* yang diakses itu berasal dari flashdisk, maka *drive letter*-nya akan menunjukkan hal tersebut dan keterangan keberadaan *file* adalah tidak ada (*missing*).



Gambar IV.19. *Screenshot* hasil pencarian *recent files* yang dilengkapi dengan *time stamps* dan *path*-nya.

3) Sejarah penggunaan *port* USB yang diakses oleh media penyimpanan seperti *flashdisk*, *harddisk* eksternal atau *memory card* yang mungkin berasal dari *handphone*. Dengan rekaman ini, *forensic analyst* dan *investigator* dapat mengetahui kapan *port* USB digunakan pada rentang waktu-waktu tertentu dan jenis media penyimpanan apa yang terpasang di *port* USB pada saat itu. Jika informasi ini sudah didapat, maka selanjutnya *forensic analyst* dan *investigator* dapat meminta kepada pelaku untuk menyerahkan media penyimpanan tersebut untuk diperiksa dan dianalisa lebih lanjut. Jika pelaku memberikan *flashdisk* yang berbeda, walaupun merk-nya sama, maka hal tersebut dapat dicek atau dipastikan lewat *serial number* yang berbeda untuk masing-masing peralatan.



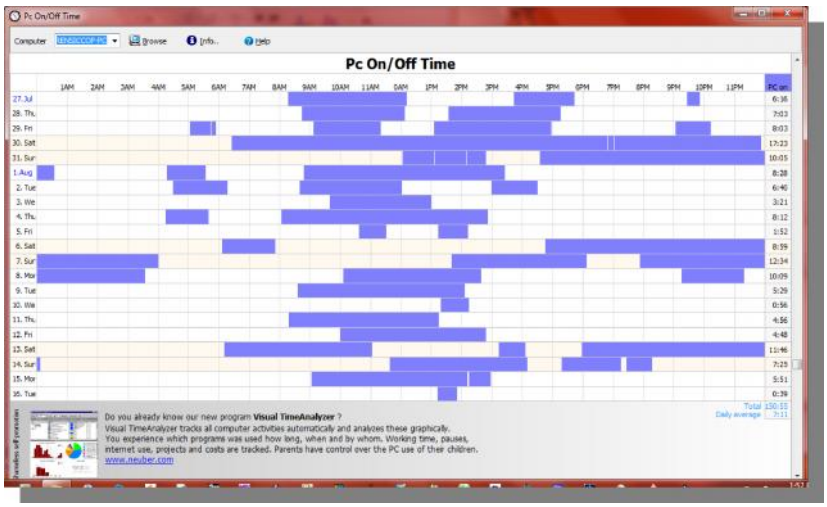
Gambar IV.20. Historis penggunaan *port* USB yang dilengkapi dengan data-data tentang jenis media yang terpasang pada *port* tersebut dan kapan digunakannya serta informasi *serial number* dari media tersebut.

4) Menampilkan *events* atau kejadian-kejadian yang pernah terjadi dan tercatat dalam bentuk *log files* di barang bukti komputer tersebut, misalnya sistem, aplikasi, sekuriti dan bahkan *errors* yang terjadi. Data-data tersebut dilengkapi dengan tanggal/waktu kejadian.

f. *Password tools*, antara lain untuk mendapatkan *password-password* yang tersimpan misalnya dari *internet browser*, seperti *Internet Explorer*, Firefox, Chrome dan Opera. Di samping itu, juga terdapat *tool* untuk mendapatkan *password* (key) dari *wireless hot spot* yang pernah digunakan.

g. *Utility*, antara lain untuk mendapatkan historis penggunaan komputer, kapan hidup/mati dalam rentang waktu 3 (tiga) minggu terakhir. Data ini dilengkapi dengan tanggal dan jam serta dikemas dalam bentuk grafis yang baik. Informasi ini kadang-kadang dibutuhkan oleh *forensic analyst* dan *investigator* untuk memastikan kapan barang bukti komputer tersebut digunakan oleh

pelaku, bahkan data ini bisa juga digunakan untuk meng-*counter* keterangan pelaku.



Gambar IV.21. Historis penggunaan komputer dalam keadaan *on/off* dalam 3 (tiga) minggu terakhir. Tanda biru menunjukkan komputer dalam keadaan hidup

Pencarian file enkripsi

2 (dua) alasan utama perlunya *triage* forensik terhadap barang bukti komputer yang ditemukan dalam keadaan *on* (hidup), di samping alasan-alasan lain yang dijelaskan di atas, yaitu :

Pertama, RAM yang bersifat *volatile* dan menyimpan informasi dari seluruh proses dan *service* dimulai ketika komputer dihidupkan, sehingga isi yang tersimpan di RAM perlu diselamatkan, dan

Kedua, untuk mengantisipasi adanya kemungkinan *encrypted file/container* yang sedang di-*mounting* atau dalam bahasa lain adalah dalam keadaan ter-dekripsi. Jika ini terjadi, maka *triage* harus dilaksanakan untuk menyelamatkan data dari *file-file* yang dalam keadaan ter-dekripsi. Karena inilah satu-satunya cara yang sangat mungkin dan praktis untuk mendapatkan isi dari *file-file* enkripsi. Jika ini tidak dilakukan, maka sangat sulit bagi *forensic analyst* dan *investigator* untuk membongkar sistem algoritma kriptografi yang memproteksi *file-file* tersebut.

Salah satu bentuk enkripsi yang sering digunakan adalah bentuk kontainer. Misalnya pelaku membuat *encrypted container* dengan ukuran 100 MB, maka untuk selanjutnya pelaku tinggal memindahkan *file-file* yang dia ingin amankan agar tidak terdeteksi atau diakses oleh *forensic analyst* dan *investigator* ke dalam kontainer tersebut hingga penuh. Jumlah *file-file* sifatnya tidak terbatas, yang dibatasi adalah jumlah total *size* dari *file-file* tersebut. Teknik ini sangat memudahkan dalam proses enkripsi, tinggal *file*-nya di-*move* ke kontainer. Ketika kontainer di-*mounting* yang menghasilkan *drive letter* tersendiri, ini artinya *file-file* yang tadinya di-enkripsi, semuanya sekarang dalam keadaan ter-dekripsi. *File-file* tersebut saat ini bisa diakses dengan normal, baik oleh pelaku, maupun oleh *forensic analyst* dan *investigator*. Untuk itu, dalam proses *triage*, *forensic analyst* dan invest*i*gator harus memastikan ada/tidaknya *encrypted container* yang ter-*mounting*/dekripsi lewat pengecekan *drive letter*. Jika ada, maka mereka harus menyelamatkan semua *file* yang ada pada *drive* tersebut.

Di samping itu, teknik lain enkripsi yang kadang-kadang juga diaplikasikan adalah enkripsi partisi, baik *system* maupun *non-system*, dan enkripsi *disk* secara keseluruhan, yang dikenal dengan istilah FDE (*Full Disk Encryption*). Pada prinsipnya, enkripsi partisi dan FDE memiliki pola kerja yang sama dengan enkripsi kontainer. Data-data yang ada di dalam enkripsi partisi dan FDE hanya bisa diakses jika partisi dan FDE tersebut di-*mounting* yang artinya dalam keadaan ter-dekripsi. Jika barang bukti komputer yang ditemukan dalam keadaan *on*, ternyata memiliki *harddisk* FDE, maka itu artinya setelah komputer tersebut dimatikan secara kasar seperti yang dijelaskan pada Bab II, maka data-data yang tersimpan di *harddisk* tersebut menjadi *inaccessible* (tidak dapat diakses karena ter-enkripsi). Tahapan-tahapan digital forensik selanjutnya menjadi tidak berarti lagi karena tidak bisa memunculkan data-data tersebut, apalagi untuk mencari bukti-bukti digital yang diinginkan.

Dan jika memang *harddisk* dari komputer tersebut merupakan FDE, teknik akuisisi yang dikenakan kepada *harddisk* tersebut adalah *live acquisition* (yaitu akuisisi langsung) yang targetnya adalah partisi-partisi dari *harddisk* tersebut. Metode akuisisi yang dijalankan tetap *physical imaging* yang berbasis sektor per sektor (*bit stream copy*) seperti yang dijelaskan pada bab sebelumnya. Teknik/metode

akuisisi ini juga berlaku untuk enkripsi kontainer dan partisi. Dengan *live acquisition* seperti ini, diharapkan data-data yang tersimpan di masing-masing partisi masih bisa diakses untuk kemudian diperiksa dan dianalisa lebih lanjut oleh *forensic analyst* dan *investigator* untuk mendapatkan bukti digital yang diinginkan.

Dari penjelasan di atas, dapat diketahui bahwa enkripsi memainkan peranan yang sangat penting kenapa triage menjadi suatu kewajiban bagi *forensic analyst* dan *investigator* untuk menerapkannya pada barang bukti komputer yang ditemukan dalam keadaan *on* (hidup).

Bibliography

1. ACPO, 7Safe (2008). *Good Practice Guide for Computer-Based Electronic Evidence*. UK ACPO and 7Safe.
2. Al-Azhar, M.N. (2010). *Standard Operating Procedure (SOP) 1 : Prosedur Pemeriksaan Digital Forensik*. DFAT Puslabfor.
3. Carrier, B. (2002). *Open Source Digital Forensic Tools: The Legal Argument.* @stake.
4. Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Elsevier Academic Press.
5. Cox, I. J. et al. (2008). *Digital Watermarking and Steganography*. Morgan Kaufmann
6. DEFT Linux. (2011). *DEFT Extra 3.0*. Dapat diakses di http://www.deftlinux.net.
7. E-fense. (2009). *Helix Forensic*. Dapat diakses di www.e-fense.com.
8. Johnson, T. A. (2005). *Forensic Computer Crime Investigation*. Taylor & Francis.
9. Justnet. (2011). *FieldSearch*. Dapat diakses di http://www.justnet.org/Pages/fieldsearch.aspx.
10. Konheim, A. G. (2007). *Computer Security and Cryptography*. Wiley

11. Microsoft. (2010). *Computer Online Forensic Evidence Extractor*. Dapat diakses di http://www.microsoft.com/industry/government/solutions/cofee/default.aspx.
12. Middleton, B. (2002). *Cyber Crime Field Handbook*. CRC Press
13. National Institute of Justice (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. US National Institute of Justice
14. National Institute of Justice (2001). *Electronic Crime Scene Investigation: A Guide for First Responder*. US National Institute of Justice.
15. Sammes, T. and Jenkinson, B. (2007). *Forensic Computing: A Practitioner's Guide*. Springer.
16. Undang-Undang No. 11 tahun 2008 tentang *Informasi dan Transaksi Elektronik*.

Bab V

WINDOWS FORENSIC: File System Analysis

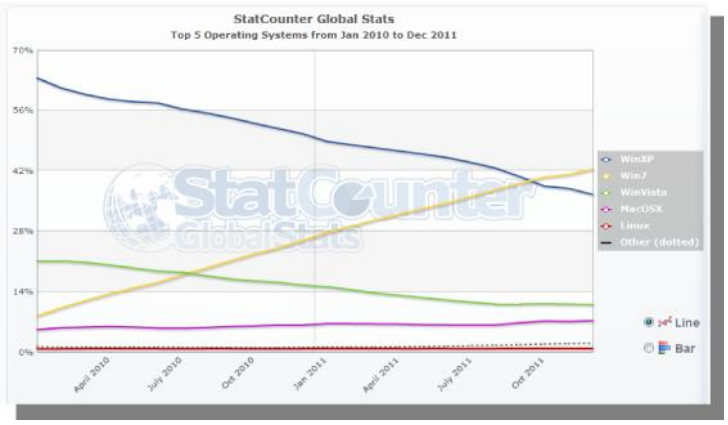
Seperti diketahui, penggunaan Microsoft Windows sebagai sistem operasi baik untuk komputer *client* maupun *server* di seluruh dunia sangat tinggi. Persentase penggunaan sistem operasi ini khususnya di komputer *client* dibandingkan dengan sistem operasi lain seperti Macintosh dan Linux sangat jauh sekali bedanya. Berdasarkan statistik yang dikeluarkan oleh W3schools, dapat diketahui bahwa penggunaan Windows 7 dan Windows XP sangat tinggi, misalnya untuk bulan November 2011 masing-masing sekitar 46% dan 33% di antara sistem-sistem operasi yang lain seperti Windows Vista (sekitar 5%), Linux (5%) dan Macintosh (9%) seperti yang ditunjukkan pada tabel di bawah ini.

2011	Win7	Vista	Win2003	WinXP	Linux	Mac	Mobile
November	45.5%	5.2%	0.7%	32.8%	5.1%	8.8%	1.0%
October	44.7%	5.5%	0.7%	33.4%	5.0%	8.9%	1.0%
September	42.2%	5.6%	0.8%	36.2%	5.1%	8.6%	0.9%
August	40.4%	5.9%	0.8%	38.0%	5.2%	8.2%	0.9%
July	39.1%	6.3%	0.9%	39.1%	5.3%	7.8%	1.0%
June	37.8%	6.7%	0.9%	39.7%	5.2%	8.1%	0.9%
May	36.5%	7.1%	0.9%	40.7%	5.1%	8.3%	0.8%
April	35.9%	7.6%	0.9%	40.9%	5.1%	8.3%	0.8%
March	34.1%	7.9%	0.9%	42.9%	5.1%	8.0%	0.7%
February	32.2%	8.3%	1.0%	44.2%	5.1%	8.1%	0.7%
January	31.1%	8.6%	1.0%	45.3%	5.0%	7.8%	0.7%
2010	**Win7**	**Vista**	**Win2003**	**WinXP**	**W2000**	**Linux**	**Mac**
December	29.1%	8.9%	1.1%	47.2%	0.2%	5.0%	7.3%
November	28.5%	9.5%	1.1%	47.0%	0.2%	5.0%	7.7%
October	26.8%	9.9%	1.1%	48.9%	0.3%	4.7%	7.6%
September	24.3%	10.0%	1.1%	51.7%	0.3%	4.6%	7.2%
August	22.3%	10.5%	1.3%	53.1%	0.4%	4.9%	6.7%
July	20.6%	10.9%	1.3%	54.6%	0.4%	4.8%	6.5%
June	19.8%	11.7%	1.3%	54.6%	0.4%	4.8%	6.8%
May	18.9%	12.4%	1.3%	55.3%	0.4%	4.5%	6.7%
April	16.7%	13.2%	1.3%	56.1%	0.5%	4.5%	7.1%
March	14.7%	13.7%	1.4%	57.8%	0.5%	4.5%	6.9%
February	13.0%	14.4%	1.4%	58.4%	0.6%	4.6%	7.1%
January	11.3%	15.4%	1.4%	59.4%	0.6%	4.6%	6.8%

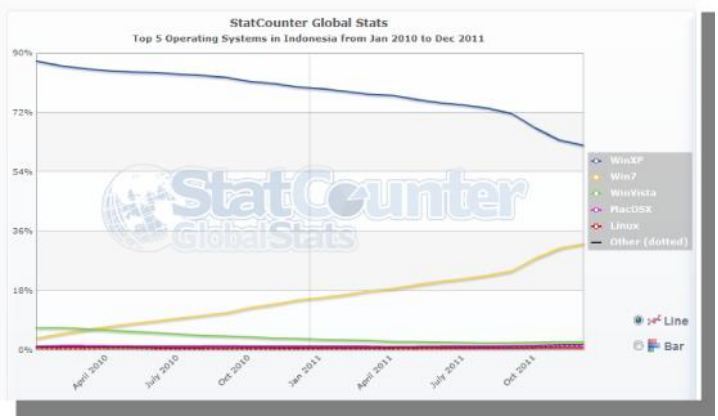
Tabel V.1. Statistik penggunaan OS (*Operating System*) selama tahun 2010/2011 berdasarkan *log files* dari W3schools, yang dapat diakses di http://www.w3schools.com/browsers/browsers_os.asp.

Dari tabulasi di atas, secara keseluruhan di tahun 2010 dan 2011, sistem operasi Windows 7 mengalami peningkatan yang sangat signifikan, dari sekitar 11% di awal tahun 2010 hingga menjadi 46% di penghujung tahun 2011, sedangkan Windows XP emngalami penurunan secara bertahap mulai dari sekitar 59% di Januari 2010 menjadi 33% di November 2011. Untuk platform non-Windows seperti Linux dan Macintosh mengalami peningkatan yang tipis untuk awal tahun 2010 hingga akhir 2011, masing-masing dari 4,6% ke 5,1% dan 6.8% menjadi 8,8%.

Hal yang relatif sama juga dirilis oleh StatCounter bahwa penggunaan Windows XP dan Windows 7 di seluruh dunia misalnya di bulan Desember 2011 sangat tinggi, masing-masing sekitar 37% dan 42%, sedangkan sistem operasi lain seperti Macintosh dan Linux sangat minim, yaitu sekitar 7% dan 1%. Ini dapat dilihat pada gambar di bawah ini.



(i)



(ii)

Gambar V.1. Statistik penggunaan sistem operasi untuk seluruh dunia (i) dan untuk di Indonesia (ii) mulai dari Januari 2010 hingga November 2011 berdasarkan data yang dikeluarkan oleh StatCounter, yang dapat diakses di http://gs.statcounter.com.

Berdasarkan data-data dari tabulasi dan gambar di atas, dapat diketahui bahwa Windows XP dan Windows 7 merupakan 2 (dua) sistem operasi yang paling banyak digunakan di seluruh dunia, namun menariknya sistem operasi Windows XP sudah tidak lagi menjadi yang paling dominan, posisinya sudah digeser oleh Windows 7. Temuan yang berbeda untuk penggunaan sistem operasi di Indonesia. Windows XP masih menempati posisi puncak sebagai *platform* yang paling banyak digunakan di Indonesia dengan persentase 62%, disusul kemudian oleh Windows 7 sebesar 32%, sedangkan sistem operasi Macintosh dan Linux masih sangat minim digunakan di Indonesia, masing-masing sebesar 1,6% dan 0,6%. Hal ini bisa dilihat pada Gambar V.1.

Untuk itu sistem operasi yang mungkin didapat oleh *forensic analyst* dan *investigator* ketika menemukan barang bukti komputer adalah Windows XP dan/atau Windows 7. Untuk itu, sangatlah penting bagi *forensic analyst* dan *investigator* mempelajari dan memahami tata cara kerja dari sistem operasi Windows.

Struktur harddisk : track, sektor, head dan cylinder

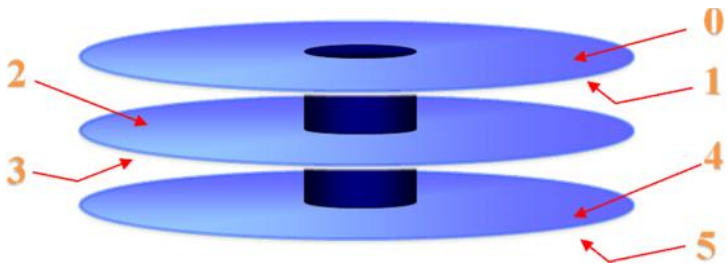
Harddisk pada sebuah komputer yang digunakan sebagai media penyimpanan utama yang menyimpan sistem operasi, *file-file* aplikasi, *file-file* data dan lain sebagainya yang mungkin terbagi lebih dari satu partisi, sebenarnya secara fisik terdiri dari beberapa piringan *platter* yang dilengkapi dengan beberapa *head* seperti terlihat pada gambar di bawah ini.

Piringan-piringan *platter* yang terbuat dari logam dan permukaannya seperti *mirror* (kaca) ini berputar dengan daya dari *spindle* (alat putar piringan) yang diikuti dengan gerakan dari *heads* untuk proses *read-write* (baca-tulis) dengan menggunakan prinsip bahasa *binary* (biner) yang terdiri dari kombinasi *bit* 0 dan 1 sebanyak 8 *bit* untuk setiap *byte* (karakter).



Gambar V.2. Struktur fisik *harddisk* yang antara lain terdiri dari piringan *platter* dan *head* (sumber : http://dedenthea.files.wordpress.com/2007/08/hd6.jpg).

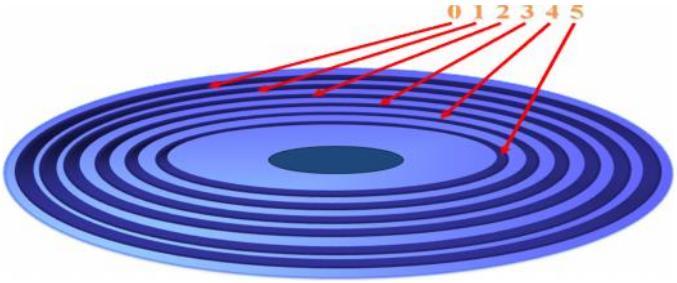
Piringan *platter* tersebut dapat dibaca sisi atas dan bawahnya, oleh karena itu pada masing-masing sisi terdapat *head* untuk mengaksesnya. Ini artinya untuk 1 (satu) *platter* terdapat 2 (dua) *head*. *Head* ini memiliki penghitungan yang dimulai dari *head* 0 yaitu sisi atas dari *platter* paling atas, untuk kemudian berturut-turut ke *platter-platter* di bawahnya.



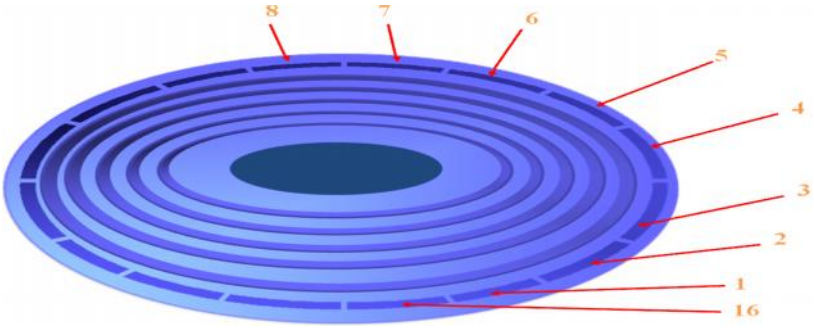
Gambar V.3. Struktur penghitungan *head* untuk masing-masing *platter*, dimulai dari sisi atas dari *platter* paling atas yang ditandai dengan *head* 0 dilanjutkan dengan *head* 1, 2, 3 dan seterusnya.

Secara fisik, piringan *platter* terdiri dari lingkaran-lingkaran spiral yang dimulai dari ujung luar ke bagian dalam yang disebut dengan istilah *track*. *Track* yang penghitungannya dimulai dari *track* 0 ini terdiri dari sektor-sektor sebagai unit penyimpanan terkecil. Untuk tempat penyimpanan data, sektor-sektor ini dapat di-setting besarnya mulai dari 512, 1024, 2048, 4096, 8192 *bytes* hingga sampai

dengan 64 *kilobytes* per sektor. Untuk *harddisk* berkapasitas besar seperti saat ini biasanya mengalokasikan 4096 *bytes* per sektor-nya.



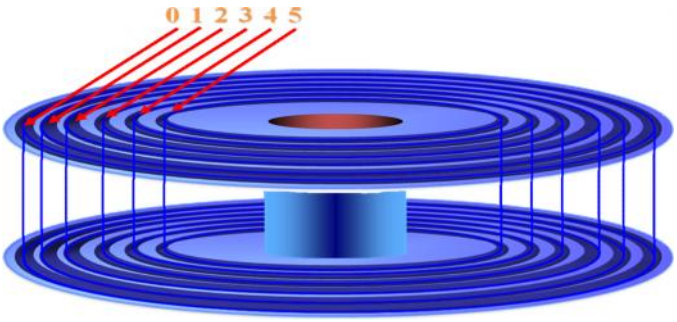
Gambar V.4. Struktur *track* yang dimulai dari ujung luar ditandai dengan *track* 0 kemudian berturut-turut menuju ke bagian dalam.



Gambar V.5. Struktur sektor untuk masing-masing *track*.

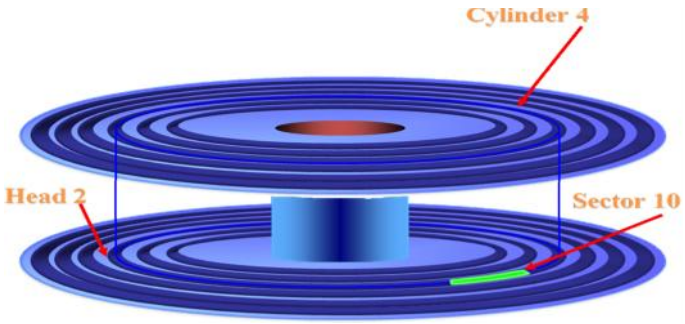
Sektor pada prinsipnya terbagi atas 3 (tiga) bagian utama, yaitu *header*, data dan ECC (*Error Correcting Code*). *Header* berisikan informasi antara lain tentang *address identification* (mekanisme pemposisian *head* untuk berada pada sektor yang benar untuk proses *read-write*) yang digunakan oleh *drive* dan *controller*, sedangkan area data digunakan untuk menyimpan data-data dalam bentuk biner, dan ECC berisikan kode-kode pengecekan *error* pada data. Berbeda dengan *head* dan *track* yang penghitungannya dimulai dari 0, penghitungan sektor dimulai dari sektor 1.

Di samping *tracks*, sektor dan *head*, pada *harddisk* juga terdapat *cylinder* untuk menandai posisi masing-masing *track*. Sama seperti *track*, *cylinder* juga dimulai dari *cylinder* 0 yang berada di ujung paling luar, untuk kemudian berturut-turut ke bagian dalam.



Gambar V.6. Struktur *cylinder* pada masing-masing *platter* yang dimulai dari *cylinder* 0 di bagian paling luar, kemudian dilanjutkan dengan *cylinder* 1, 2, 3 dan seterusnya sampai ke bagian paling dalam.

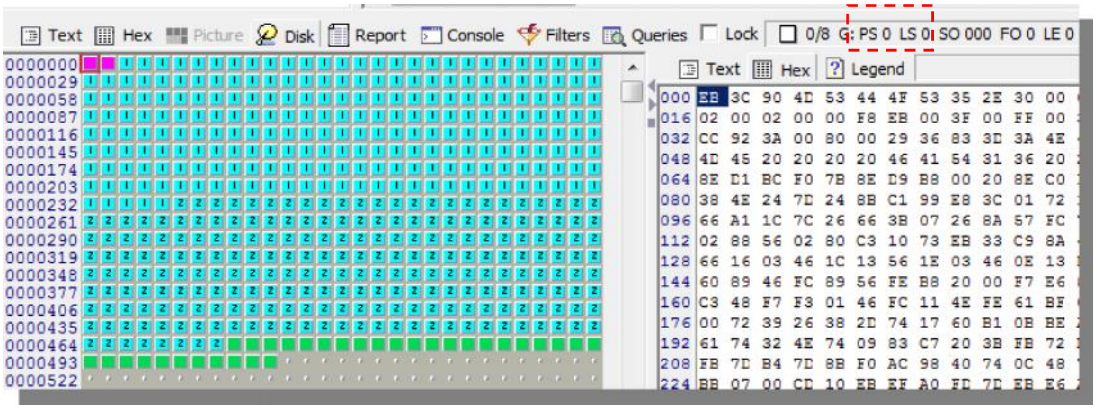
Dengan adanya sistematika *cylinder*, *head* dan sektor yang biasa disingkat CHS, maka pergerakan *head* menuju ke posisi sektor tertentu untuk proses *read-write* suatu *file/folder* dapat berjalan dengan benar. Misalnya sistematika CHS menunjukkan 4-2-10 untuk proses *read-write file* pertama.txt, maka posisi sektor yang harus diakses oleh *head* adalah seperti yang dimaksud pada gambar di bawah ini.



Gambar V.7. Sistematika CHS 4-2-10 menunjukkan posisi sektor yang sebenarnya yang harus diakses oleh *head*.

Sistematika CHS memiliki keterbatasan ketika mengakses *harddisk* berukuran besar yaitu lebih dari 8,1 GB, oleh karena itu sistematika ini tidak lagi digunakan sebagai *primary addressing method* (metode pengalamatan utama), dan digantikan dengan metode LBA (*Logical Block Address*). Metode LBA ini tidak lagi didasarkan pada lokasi fisik sektor, melainkan pada urutan alamat masing-masing

sektor, yang dimulai dari sektor 0. Keuntungan dari metode ini adalah *software* tidak perlu lagi mengetahui sistem geometri sektor pada *harddisk*, software hanya perlu tahu alamat tunggal untuk masing-masing sektor. Seperti pada gambar di bawah ini, *flashdisk* berukuran 2 GB dilakukan *re-format* pada *file system* FAT 16 dengan besarnya unit untuk pengalokasian data adalah 512 *bytes*.

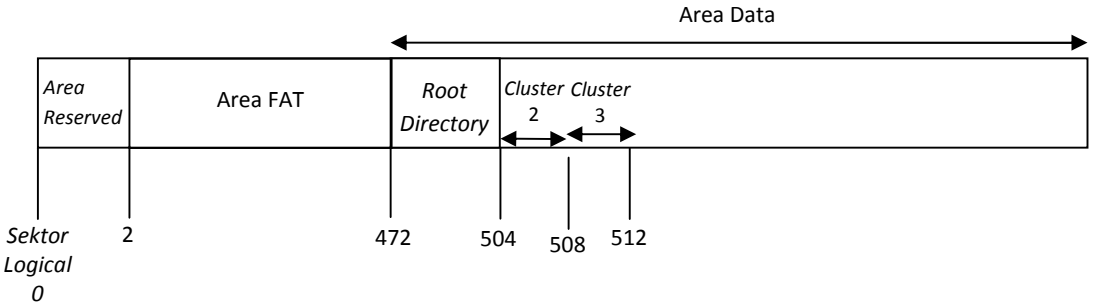


Gambar V.8. Pengalamatan sektor dimulai pada sektor 0, baik PS (*Physical Sector*) maupun LS (*Logical Sector*) pada *flashdisk* dengan format FAT 16 seperti yang ditunjukkan pada kotak bergaris merah putus-putus.

Pengalokasian data : clusters dan slacks

Untuk *file system* FAT (*File Allocation Table*) dan NTFS (New *Technology File System*) pada sistem operasi Windows, unit pengalokasian area untuk penyimpanan data dihitung per satuan tertentu dari jumlah sektor, yang dikenal dengan istilah *cluster*. Misalnya 1 *cluster* berisikan 4 sektor, maka 1 *cluster* tersebut memiliki 2048 *bytes*. Setelah jumlah *byte* ini habis, maka pengalokasian data akan masuk ke *cluster* berikutnya, dan seterusnya sampai data yang akan dialokasikan dari *file* tertentu sudah habis (masuk) ke dalam *cluster*-nya. *Cluster* berikutnya akan digunakan untuk memulai pengalokasian *file* yang lain. Besarnya ukuran *cluster* berdasarkan spesifikasi dari Microsoft bahwa cluster merupakan kelipatan 2 dari jumlah sektor, misalnya jumlah sektor untuk per *cluster* adalah 1, 2, 4, 8, 16, 32 dan 64 sektor. Artinya *size* minimum *cluster* dalah 512 *bytes* dan maksimum adalah 32 KB.

Berbeda dengan *head*, *track*, *cylinder* maupun sektor, penomoran *cluster* untuk *file system* FAT dimulai dari *cluster* 2, artinya tidak ada *cluster* 0 ataupun *cluster* 1. Penempatan posisi *cluster* pertama (yaitu cluster 2) berbeda-beda tergantung pada jenis *file system*-nya.

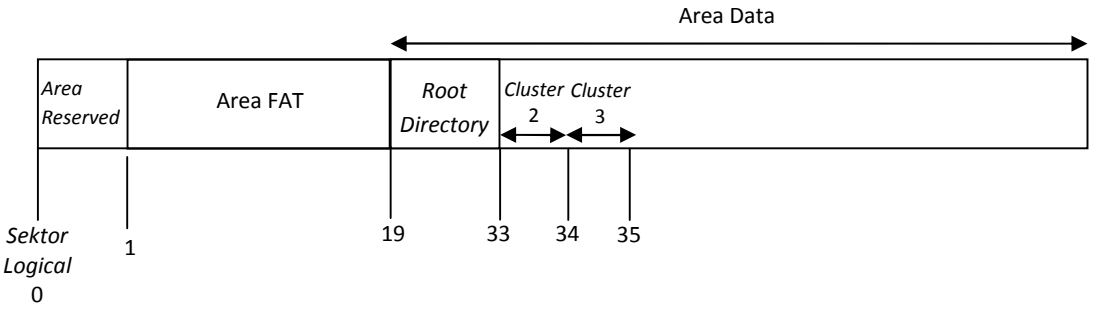


Gambar V.9. Sistematika *cluster* pada FAT 16 yang *cluster* 2 dimulai pada sektor pertama (sektor 504) setelah *root directory*, dan *cluster* selanjutnya adalah per 8 sektor, dengan asumsi 1 *cluster* berukuran 4096 bytes.

Pada gambar di atas, yaitu pada FAT 16, *cluster* 2 terletak di sektor pertama setelah *root directory*. Besarnya *root directory* ini sudah ditentukan di *boot sector*, misalnya 32 sektor pertama dari area data. Sistematika *cluster* hanya terdapat di area data *non-root directory*, tidak di area *reserved* yang dialokasikan untuk *volume boot* sebanyak 2 sektor, ataupun di area FAT yang dialokasikan untuk FAT 1 (*primary* FAT) dan FAT 2 (*secondary* FAT) masing-masing sebanyak 235 sektor. Jika *root directory* diawali dari sektor 472 dan besarnya *root directory* adalah 32 sektor, maka sektor 504 akan merupakan sektor pertama dari *cluster* 2. Jika 1 *cluster* besarnya 2048 *bytes*, yang artinya terdiri dari 4 sektor, maka *cluster* 2 akan sampai pada sektor 507, sedangkan *cluster* 3 berada pada sektor 508 sampai dengan 511. Demikian juga untuk *cluster-cluster* berikutnya yang merupakan kelipatan dari 4 sektor (2048 *bytes*).

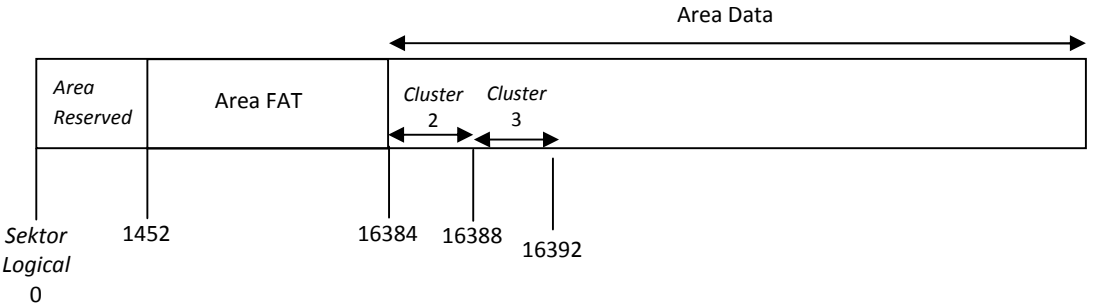
FAT 12 sama seperti pada FAT 16, yaitu penghitungan *cluster* 2 dimulai pada sektor pertama dari area data non *root-directory*, seperti pada gambar di bawah ini. Area FAT dialokasikan juga untuk FAT 1 dan FAT 2 masing-masing sebanyak 9 sektor, sedangkan area *reserved* sebanyak 1 sektor dialokasikan untuk *volume*

boot, dan *root directory* ditentukan sebesar 14 sektor. Sektor 32 yang merupakan sektor akhir dari *root direc*tory, oleh karena itu sektor 33 menjadi *cluster* 2 (*cluster* pertama). Jika 1 *cluster* di-*setting* sebesar 512 *bytes* (artinya 1 sektor), maka setiap sektor berikutnya merupakan *cluster* baru, misalnya sektor 34 adalah *cluster* 3 dan seterusnya.



Gambar V.10. Sistematika *cluster* pada FAT 12 yang dimulai pada sektor pertama dari area data non *root-directory*, dan *cluster* selanjutnya adalah setiap kelipatan 1 sektor dengan asumsi 1 *cluster* berukuran 512 *bytes*.

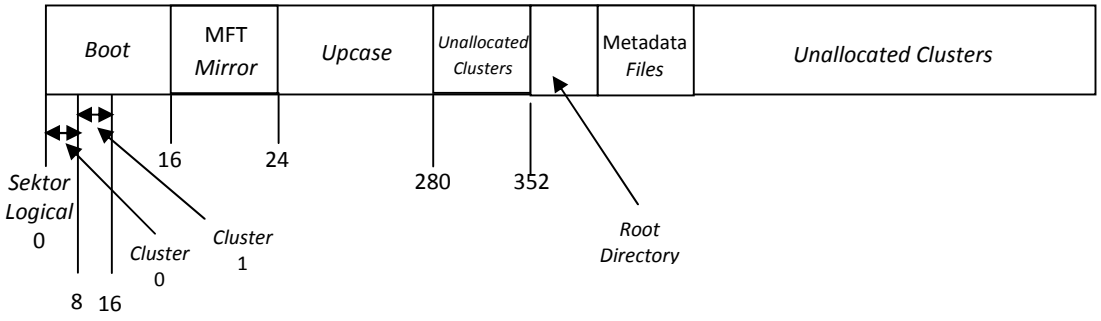
Sedangkan pada *file system* FAT 32, sektor pertama dari area data digunakan langsung untuk sektor pertama dari *cluster* 2, seperti pada gambar di bawah ini.



Gambar V.11. Sistematika *cluster* pada FAT 32 di mana *cluster* 2 tetap dimulai pada sektor pertama di area data, yaitu pada sektor 16384 s/d 16388 dengan besarnya 1 *cluster* adalah 2048 *bytes* (4 sektor).

Pada gambar di atas, are FAT yang dialokasikan untuk FAT 1 dan FAT 2 tetap masih ada, namun besarnya 7466 sektor untuk masing-masing FAT, sedangkan area *reserved* tetap dialokasikan untuk *volume boot* sebanyak 1452 sektor. Dikarenakan 1 *cluster* besarnya 2048 *bytes* (4 sektor), maka *cluster* 2 berada pada sektor 16384 s/d 16387, cluster 3 pada sektor 16388 s/d 16391, *cluster-cluster* berikutnya setiap kelipatan 4 sektor. *Cluster* pertama pada FAT 32 dialokasikan untuk *root directory*.

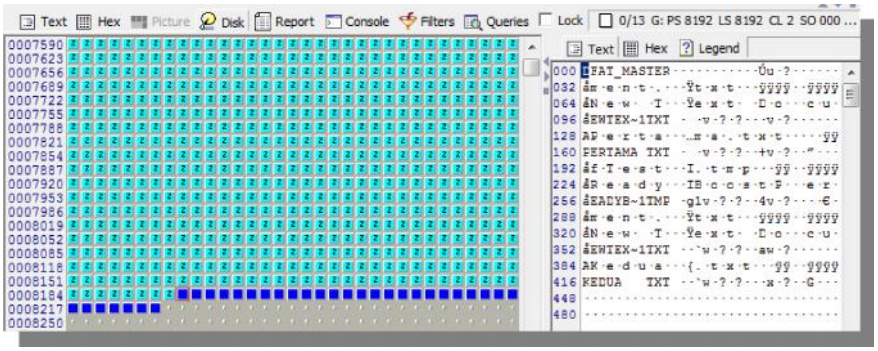
Berbeda dengan FAT 12/16 dan FAT 32, pada NTFS, sektor pertama dari *file system* tersebut langsung dialokasikan sebagai sektor pertama dari *cluster* 0. Penomoran *cluster* untuk NTFS dimulai dari *cluster* 0. Misalnya NTFS dengan 1 *cluster* besarnya 4096 *bytes* (8 sektor), maka *cluster* pertama (*cluster* 0) adalah 8 sektor (4096 *bytes*) pertama, *cluster* 1 pada sektor 8 hingga 15, *cluster* 2 pada sektor 16 hingga 23, dan seterusnya untuk *cluster-cluster* berikutnya setiap kelipatan 8 sektor (4096 *bytes*). Area *reserved* pada NTFS adalah *cluster* pertama dari area *boot*, yaitu *cluster* 0.



Gambar V.12. Sistematika *cluster* pada NTFS di mana *cluster* pertama adalah *cluster* 0 yang dimulai dari sektor 1 s/d 7 untuk ukuran besarnya 1 *cluster* adalah 4096 *bytes* (8 sektor). *Cluster-cluster* berikutnya setiap kelipatan 8 sektor.

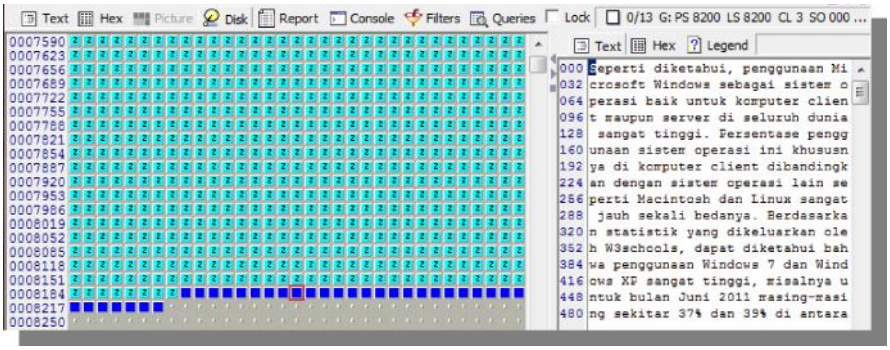
Pengalokasian area di *harddisk* untuk penyimpanan suatu *file* data didasarkan pada *cluster*. Jika ada satu *file* baru, maka *file* tersebut akan dialokasikan pada *cluster* berikutnya, tidak menimpa pada *cluster* yang sama yang sudah dialokasikan untuk *file* sebelumnya. Artinya tidak ada satu *cluster* untuk penyimpanan 2 (dua) *file* yang berbeda.

Misalnya pada *flashdisk* 2 GB dengan FAT 32 dan besaran per *clusternya* adalah 4096 *bytes* (yaitu 8 sektor). Dibuat suatu *file* yaitu Pertama.txt yang berukuran 660 *bytes*, maka file ini akan dialokasikan penyimpanannya pada *cluster* 3, karena *cluster* 2 dialokasikan untuk akses *root directory*. *File* ini akan menempati sektor pertama dan setengah sektor kedua dari *cluster* 3, sedangkan sisa sektor tidak digunakan (kosong), namun tetap dialokasikan untuk *file* tersebut. Selanjutnya dibuat *file* yang baru, yaitu Kedua.txt dengan ukuran 4679 *bytes*. Dikarenakan ukuran ini melebihi ukuran 1 *cluster*, maka file ini akan dialokasikan pada 2 *cluster* (8192 *bytes*) di mana *cluster* pertama akan penuh dengan data, sedangkan pada *cluster* kedua, hanya sektor pertama dan sedikit sektor kedua yang berisikan data, 6 sektor sisanya kosong, namun tetap dialokasikan untuk *file* tersebut.

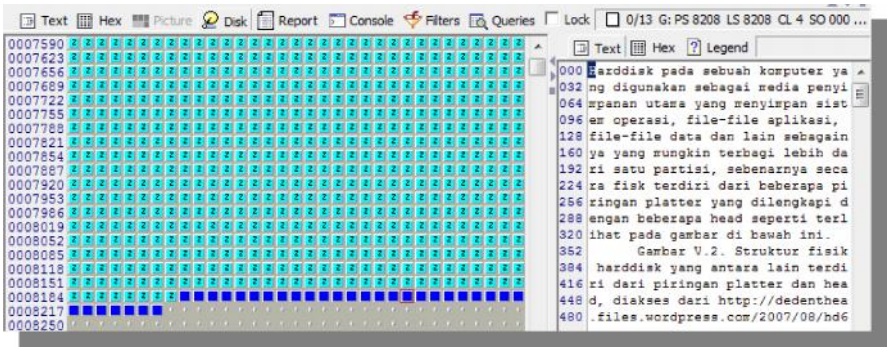


Gambar V.13. Pada FAT 32 dengan 1 *cluster* besarnya 4096 *bytes*, *cluster* 2 (sebanyak 8 sektor) dialokasikan untuk *root directory*.

Selanjutnya, jika *file* Kedua.txt dihapus, maka itu artinya *cluster* 4 dan 5 sudah tidak teralokasikan lagi (*unallocated clusters*) untuk *file* tersebut, sehingga jika dibuat *file* baru yaitu Ketiga.txt dengan ukuran 2097 *bytes*, maka *file* ini hanya akan menempati satu *cluster*, yaitu *cluster* 4 (yang sudah tidak teralokasikan lagi) sebanyak 5 sektor, sedangkan 3 sektor sisanya (yaitu sektor 6, 7 dan 8 dari *cluster* 4) merupakan *file slack*.



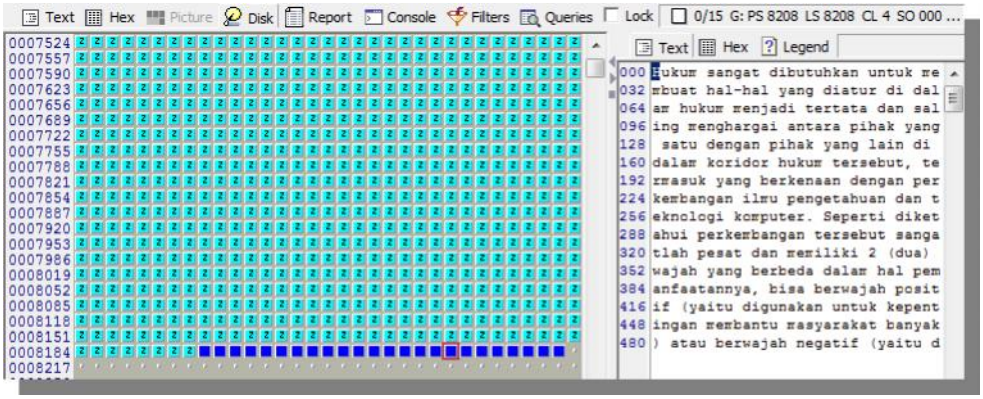
(1)



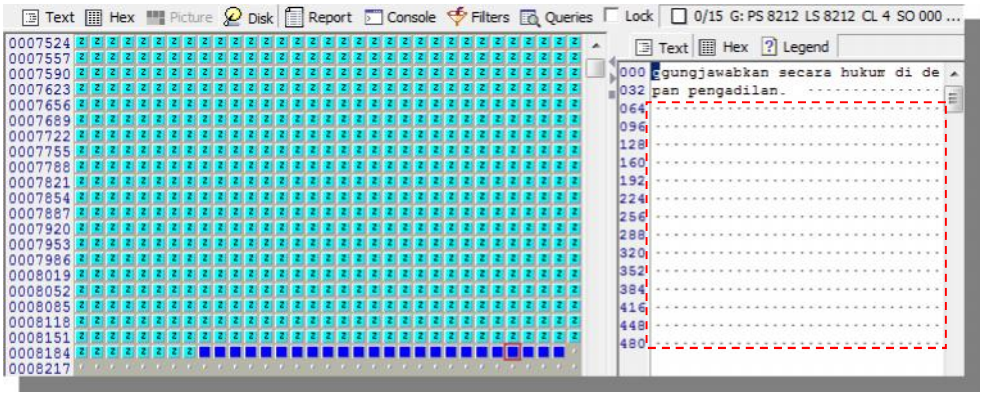
(2)

Gambar V.14. *Cluster* 3 dialokasikan untuk *file* Pertama.txt (1), sedangkan *cluster* 4 dan 5 dialokasikan untuk *file* Kedua.txt (2).

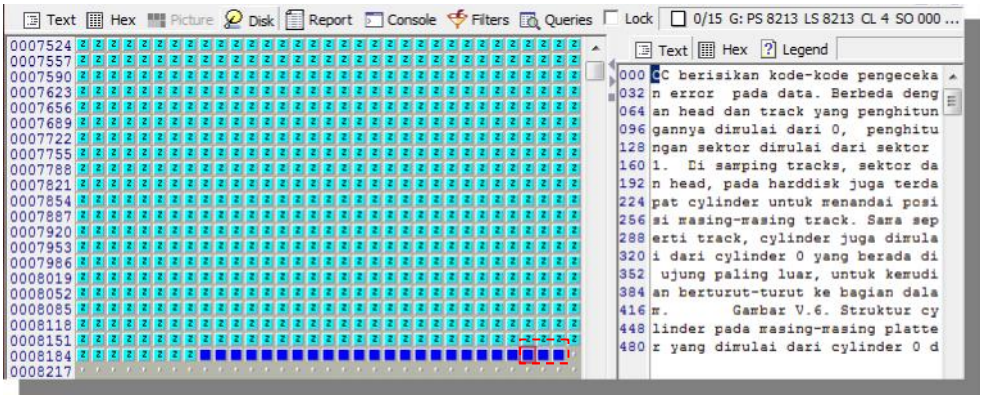
File slack adalah dimulai dari *end of sector* (eos) sampai *end of cluster* (eoc), sedangkan dari *end of file* (eof) hingga eos pada sektor 5 disebut dengan istilah *memory slack*. Pada kasus ini seperti pada gambar di atas, *memory slack* di sektor 5 dari *cluster* 4 yang ditandai dengan kotak besar bergaris merah putus-putus (Gambar V.15.(2)) tidak menyimpan data, sedangkan *file slack* yaitu sektor 6, 7 dan 8 yang ditandai dengan kotak kecil bergaris merah putus-putus (Gambar V.15.(3)) masih menyimpan data dari *file* Kedua.txt yang sudah dihapus. Data dari *file slack* ini masih bisa dilakukan *recovery*.



(1)



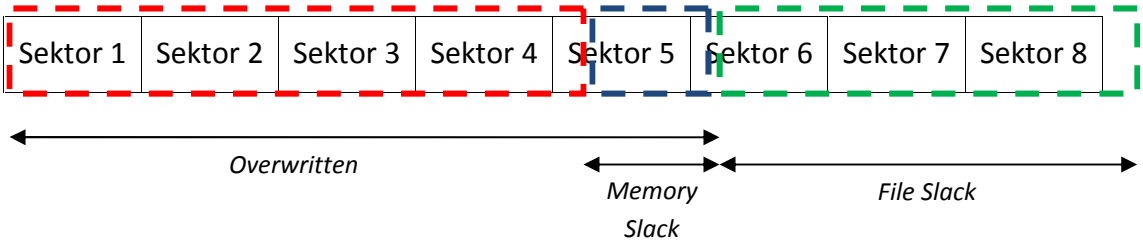
(2)



(3)

Gambar V.15. *File* Ketiga.txt menempati *cluster* 4 yang sudah tidak teraloksikan lagi untuk *file* Kedua.txt, di mana sektor 1 s/d 5 berisikan data baru (1), sektor 5 terdapat *memory slack* (2), dan sektor 6 s/d 8 terdapat *file slack*.

Sementara itu, data-data dari *file* Kedua.txt yang sudah dihapus yang tersimpan di sektor 1 s/d 5 dari *cluster* 4 sudah tertimpa (*overwritten*) dengan data baru dari *file* Ketiga.txt, sehingga data-data *file* Kedua.txt yang sudah *overwritten* tidak bisa dilakukan *recovery* lagi. Struktur penjelasan tentang *cluster* 4 ini dapat dilihat pada gambar di bawah ini.

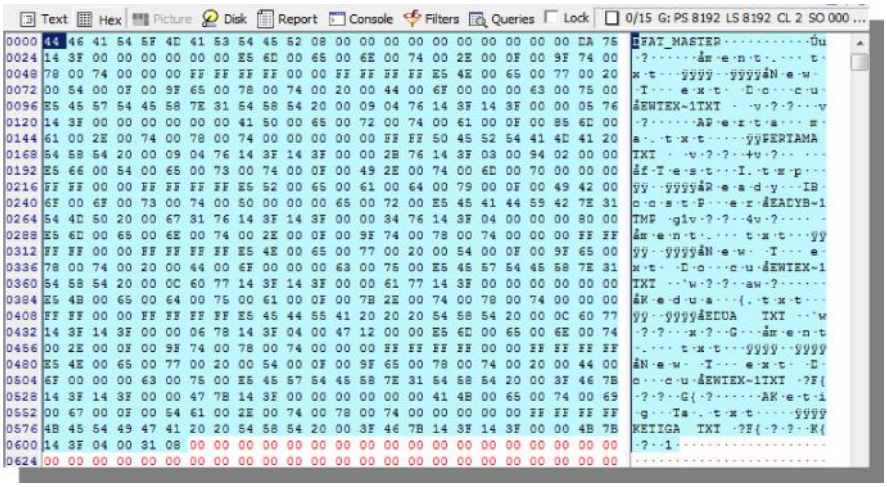


Gambar V.16. Struktur *cluster* 4 di mana sektor 1 s/d5 merupakan *overwritten* (artinya data lama yang dihapus sebelumnya sudah tertimpa dengan data baru), sedangkan pada sektor 5 terdapat *memory slack* (dari eof data baru s/d eos), dan sektor 6 s/d 8 merupakan *file slack* (dari eos data baru s/d eoc).

Dikarenakan *file slack* ini memungkinkan masih menyimpan data-data dari *file-file* yang sudah terhapus (*deleted*) sebelumnya, maka *file slack* ini menjadi salah satu target dari *forensic analyst* dan *investigator* untuk mencari dan mendapatkan informasi yang diinginkan.

Adapun *root directory* yang terletak di *cluster* 2 dapat dianalisa lebih dalam untuk melihat *time stamps* dari *file* Kedua.txt yang sudah dihapus dan sebagian sudah *overwritten*, seperti *created date* (tanggal pertama kali dibuat di *file system*), *written date* (tanggal terakhir kali dimodifikasi), dan *accessed date* (tanggal terakhir kali diakses), di samping informasi ukuran dan *cluster* tempat penyimpanannya. Informasi yang berada di *cluster* 2 ini penting untuk melihat historis dari *file* kedua.txt tersebut. Penjelasan lengkap tentang hal ini dapat dilihat pada gambar di bawah ini.

Dari Gambar V.17., dapat diketahui bahwa *file* Kedua.txt dibuat pertama kali (*created date*) pada tanggal 20 Agustus 2011 02:59:00PM, dimodifikasi terakhir pada tanggal 20 Agustus 2011 03:00:12PM dan terakhir kali diakses pada tanggal 20 Agustus 2011. *File* tersebut berukuran 4679 *bytes* dan dialokasikan pada *cluster* 4. *File* Kedua.txt ini merupakan *file* yang sudah terhapus (*deleted*) dan sebagian datanya sudah tertimpa (*overwritten*) dengan data dari *file* Ketiga.txt.



(1)

Name	Created	Written	Accessed	Size	Cluster		
DFAT_MAS.TER	Invalid	08/20/11 02:46:52PM			0	0	
_m	03/24/80 12:03:40AM		Invalid 03/20/80		4294967295	0	
_N	03/24/80 12:03:10AM		03/15/80 12:02:08AM		03/20/80	7667811	2097152
_EWTEX~1.TXT	08/20/11 02:48:08PM		08/20/11 02:48:10PM		08/20/11	0	0
AP	03/01/80 12:03:26AM		03/20/80 12:03:48AM		01/14/80	4294901760	7602176
PERTAMA.TXT	08/20/11 02:48:08PM		08/20/11 02:49:22PM		08/20/11	660	3
_f	03/20/80 12:01:28AM		Invalid 03/13/80		4294967295	7340032	
_R	03/15/80 12:02:04AM		02/16/80 12:03:40AM		03/15/80	7471205	7536640
_EADYB~1.TMP	08/20/11 02:49:34PM		08/20/11 02:49:40PM		08/20/11	8388608	4
_m	03/24/80 12:03:40AM		Invalid 03/20/80		4294967295	0	
_N	03/24/80 12:03:10AM		03/15/80 12:02:08AM		03/20/80	7667811	2097152
_EWTEX~1.TXT	08/20/11 02:59:00PM		08/20/11 02:59:02PM		08/20/11	0	0
_K	03/20/80 12:01:28AM		Invalid 03/24/80		4294967295	7602176	
_EDUA.TXT	08/20/11 02:59:00PM		08/20/11 03:00:12PM		08/20/11	4679	4
_m	03/24/80 12:03:40AM		Invalid 03/20/80		4294967295	0	
_N	03/24/80 12:03:10AM		03/15/80 12:02:08AM		03/20/80	7667811	2097152
_EWTEX~1.TXT	08/20/11 03:26:12PM		08/20/11 03:26:14PM		08/20/11	0	0
AK	01/14/80 12:03:02AM		Invalid 03/20/80		4294967295	7864320	
KETIGA.TXT	08/20/11 03:26:12PM		08/20/11 03:26:22PM		08/20/11	2097	4

(2)

Gambar V.17. *Cluster* 2 yang dialokasikan sebagai *root directory* (1), dan hasil analisa data di *cluster* 2 dengan jenis data adalah DOS *Directory Entry* yang berbentuk tabulasi yang lengkap (2).

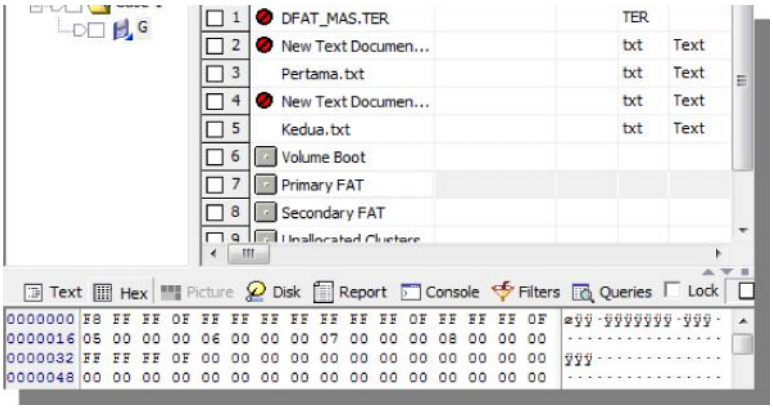
File system FAT: struktur dan boot sector

File system adalah suatu metode yang dibutuhkan oleh komputer untuk penyimpanan dan pengeluaran data dengan menyediakan suatu mekanisme untuk penyimpanan data berbasis hirarki dari *file-file* dan direktori-direktori. Untuk itu *file system* terdiri dari data struktural dan data *user* yang diorganisasi sedemikian rupa sehingga komputer akan tahu untuk mendapatkannya secara cepat dan benar. Dikarenakan pentingnya *file system* ini, maka Microsoft senantiasa mengembangkannya untuk disesuaikan dengan perkembangan

teknologi komputer termasuk *harddisk* dan pengalamatan *cluster*-nya, dimulai dari FAT 12, FAT 16, FAT 32, NTFS dan yang terkahir adalah ExFAT (*Extended* FAT).

Pada Gambar V.9, V.10 dan V.11 di atas, seperti dijelaskan sebelumnya, area FAT terdiri dari 2 (dua) bagian yaitu *primary* FAT (FAT 1) dan *secondary* FAT (FAT 2). FAT 1 merupakan *file system* yang digunakan, sedangkan FAT 2 merupakan *backup* jikalau FAT 1 tidak lagi bisa digunakan (rusak). Meskipun begitu, bisa juga FAT 2 merupakan *mirror* dari FAT1, artinya apa yang teralokasikan pada FAT 1 juga akan dapat ditemukan hal yang sama pada FAT 2. Hal ini dapat ditemukan pada FAT 32.

FAT merupakan suatu tabulasi besar yang berisikan pengalokasian sektor dan *cluster* tertentu untuk suatu *file*. Jika *cluster* dan sektor pada area data belum teralokasikan untuk suatu *file* (artinya area data masih kosong), maka FAT 1 juga akan kosong, tidak ada datanya. Sebaliknya jika ada data baru yang tersimpan pada area data, maka secara otomatis *cluster* dan sektor yang teralokasikan akan tercatat pada FAT 1.



Gambar V.18. *Byte-byte* pada FAT 1 dari *file system* FAT 32 yang berisikan data tentang pengalokasian *cluster* pada area data, di mana besarnya 1 *cluster* adalah 1024 *bytes* (2 sektor).

Pada gambar di atas yang menunjukkan FAT 1 (*primary*) dari FAT 32 dengan besarnya *cluster* adalah 1024 *bytes* (2 sektor), 4 *byte* pertama dengan nilai 0xf8, 0xff, 0xff dan 0x0f merupakan *signature* dari FAT 32. Pada byte 4 s/d 11 yang diakhiri dengan *signature* 0x0f merupakan pengaloksian untuk *root directory* yang berada pada *cluster* pertama (*cluster* 2). Pada *byte* 12 s/d 15 (sebanyak 4 *bytes*)

yang diakhiri dengan *signature* 0x0f merupakan pengaloksian *cluster* 3 untuk *file* Pertama.txt yang berukuran 940 *bytes*. Pada *byte* 16 s/d 35 yang diakhiri dengan *signature* 0x0f merupakan pengalokasian *cluster* 4 s/d 8 (sebanyak 5 *cluster*) untuk *file* Kedua.txt yang berukuran 5001 *bytes*.

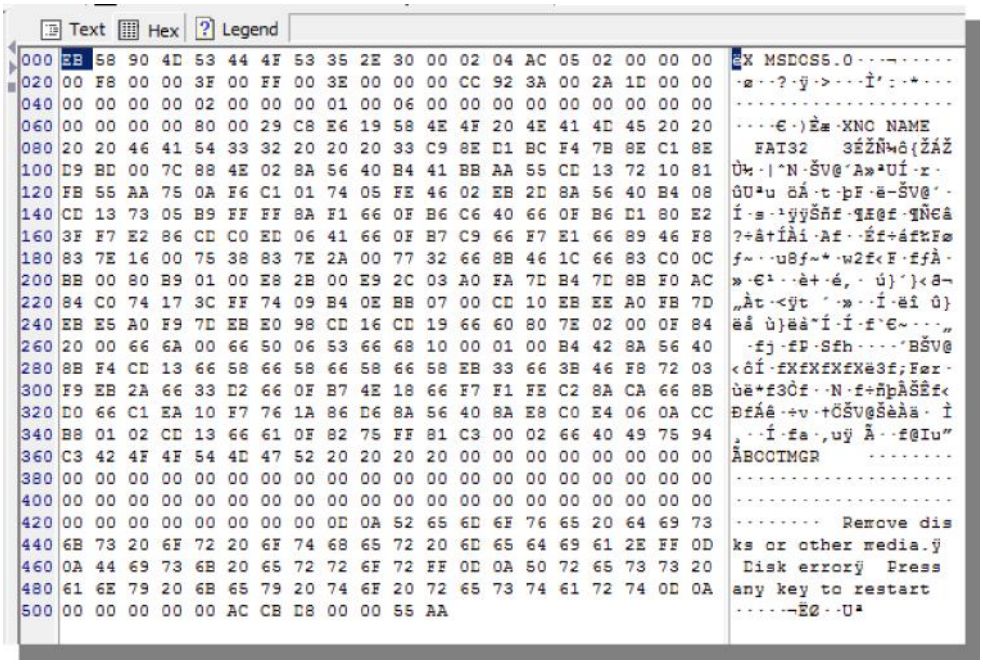
Dari penjelasan di atas, pada FAT 32, dapat diketahui bahwa setiap *cluster* pada area data yang dialokasikan untuk penyimpanan suatu *file* akan ditandai pada FAT 1 dan FAT 2 sebagai area yang sudah teralokasikan untuk file tersebut. Area tersebut adalah sebanyak 4 *byte* yang diakhiri dengan *signature* 0x0f untuk alokasi 1 *cluster*. Jika lebih dari satu *cluster* pada area data untuk dialokasikan pada satu *file* tertentu, misalnya 5 *cluster*, maka sebanyak 20 *bytes* dengan rangkaian 5x4 *bytes* yang diakhiri dengan *signature* 0x0f. Jika ada satu *file* dengan 1 *cluster* dihapus (*deleted*), maka 4 *bytes* pada FAT 1 dan FAT 2 yang dialokasikan untuk 1 *cluster* tersebut akan dikosongkan (nilainya menjadi 0x00, 0x00, 0x00 dan 0x00).

Area sebelum FAT dialokasikan untuk *volume boot*, sedangkan area sesudah FAT untuk *root directory*. Area yang dialokasikan untuk *volume boot* adalah sektor pertama, oleh karena itu disebut *boot sector* yang berisikan banyak informasi tentang pengkategorian data untuk *file system* tersebut. Untuk *boot sector*, antara FAT 12/16 dengan FAT 32, tidak ada perbedaan untuk 36 *bytes* pertama dan 2 *bytes* terakhir. Tabel berikut adalah deskripsi untuk masing-masing *bytes* tersebut. Tabel ini merujuk pada Tabel 10.1 tentang struktur data FAT (Carrier, p254).

Nomor Bytes	Deskripsi
0-2	Instruksi untuk kode *boot* yang merujuk ke *bootable file system*
3-10	Nama OEM pada bahasa ASCII
11-12	Jumlah *bytes* untuk 1 sektor. Nilai yang diijinkan adalah 512, 1024, 2048 dan 4096 *bytes*
13	Jumlah sektor per *cluster*. Jumlah yang diijinkan adalah kelipatan 2 sektor. Besarnya ukuran *cluster* mulai dari 512 *bytes* hingga 32 KB
14-15	Besarnya ukuran *area reserved* (dalam sektor)
16	Jumlah FAT. Biasanya berjumlah 2, namun bisa juga 1 untuk media penyimpanan yang kecil

17-18	Jumlah *file* maksimum yang dapat teralokasikan di *root directory* pada FAT 12/16. Nilai *range* ini 0 untuk FAT 32, dan 512 untuk FAT 16
19-20	Jumlah sektor pada *file system* yang direpresentasikan dalam nilai 16 bit (2 *bytes*), atau 4 *byte*s jika nilainya lebih dari 2 *bytes*
21	Jenis media. Jika 0xf8 artinya *fixed disk* (*harddisk* yang terpasang di dalam komputer), sedangkan 0xf0 artinya *removable media* seperti *flashdisk*
22-23	Ukuran 16 *bit* di dalam sektor-sektor FAT 12/16, sedangkan untuk FAT 32 nilainya adalah 0
24-25	Jumlah sektor per *track* dari media penyimpanan
26-27	Jumlah *heads* dari media penyimpanan
28-31	Jumlah sektor sebelum mulainya partisi
32-35	Nilai 32 *bit* dari jumlah sektor-sektor di *file system*
510	0x55 merupakan *signature* pada *footer*
511	0xaa merupakan *signature* pada *footer*

Tabel V.2. Struktur data *boot sector* pada FAT 12/16 dan FAT 32 mulai untuk 36 *bytes* pertama dan 2 *bytes* terakhir.



Gambar V.19. *Boot sector* pada FAT 32 dengan ukuran 1 *cluster* adalah 4 sektor.

Dari penjelasan Tabel V.2. di atas, dapat dilihat pada Gambar V.19 bahwa beberapa deskripsi masing-masing *byte* dari *boot sector* FAT 32 adalah sebagai berikut :

1. *Signature* pada 2 *bytes* terakhir dari *boot sector*, yaitu byte 510 dan 511 adalah 0x55 dan 0xaa. Adanya *signature* ini menunjukkan bahwa sektor tersebut adalah *boot sector*.
2. Pada *byte* 3 s/d 10, nilai teksnya merujuk pada nama OEM, yaitu 'MSDOS5.0'.
3. Pada *byte* 11 dan 12, nilainya adalah 0x00 dan 0x02, yang didasarkan pada 16-*bit integer* nilainya 0x0200 adalah 512. Ini menunjukkan bahwa besarnya ukuran sektor adalah 512 *bytes*.
4. Pada *byte* ke-13, nilainya adalah 0x04, ini artinya adalah besarnya 1 *cluster* adalah 4 sektor (2048 *bytes*).
5. Pada *byte* 14 dan 15, nilainya adalah 0xac dan 0x05 yang didasarkan pada 16-*bit interger* nilainya 0x05ac adalah 1452 sektor. Artinya jumlah sektor yang tersimpan di area *reserved* yang digunakan untuk *volume boot* adalah 1452 sektor. Ini artinya area FAT (FAT 1 dan FAT 2) akan dimulai pada sektor 1452.
6. Pada *byte* ke-16, nilainya adalah 0x02, yang artinya jumlah FAT adalah 2, yaitu FAT 1 (*primary*) dan FAT 2 (*secondary*).
7. Pada *byte* ke-21, nilainya adalah 0xf8, ini artinya media penyimpanan berupa *removable* seperti *flashdisk*.
8. Pada *byte* 24 dan 25, nilainya adalah 0x3f dan 0x00, yang didasarkan pada 16-*bit integer* nilainya 0x003f adalah 63. Ini artinya jumlah sektor untuk setiap *track* adalah 63 sektor.
9. Pada *byte* 26 dan 27, nilainya adalah 0xff dan 0x00, yang didasarkan pada 16-*bit integer* nilainya 0x00ff adalah 255. Ini menunjukkan bahwa jumlah *head* adalah 255.
10. Pada *byte* 28 s/d 31, nilainya adalah 0x3e, 0x00, 0x00 dan 0x00, yang didasarkan pada 32-*bit integer* nilainya 0x0000003e adalah 62. Ini artinya jumlah sektor sebelum dimulainya partisi tambahan (*extended partition*) adalah 62 sektor.
11. Pada *byte* 32 s/d 35, nilainya adalah 0xcc, 0x92, 0x3a dan 0x00, yang didasarkan pada 32-*bit integer* nilainya 0x003a92cc adalah 3838668. Ini

menunjukkan jumlah sektor yang tersedia pada FAT 32 tersebut adalah 3.838.668 sektor.

Selanjutnya, perbedaan pada *boot sector* antara FAT 12/16 dengan FAT 32 adalah pada *byte* 36 s/d 509, namun pada *byte* 62 s/d 509 untuk FAT 12/16 dan byte 90 s/d 509 untuk FAT 32 merupakan area yang tidak digunakan untuk kepentingan-kepentingan yang khusus, kecuali untuk menyimpan kode-kode *boot* dan pesan-pesan *error*.

Berdasarkan Tabel V.3 yang merujuk pada Tabel 10.2 dan 10.3 mengenai struktur data untuk sisa *byte* pada FAT 12/16 dan FAT 32 (Carrier, p.255, 256), dan Gambar V.19 di atas, beberapa deskripsi *byte-byte* yang ada pada *boot sector* dari FAT 32, yang dimulai dari *byte* 36 adalah sebagai berikut :

1. Pada *byte* 36 s/d 39, nilainya adalah 0x2a, 0x1d, 0x00 dan 0x00, yang didasarkan pada 32-*bit integer* nilainya 0x00001d2a adalah 7466. Ini menunjukkan jumlah sektor untuk 1 FAT adalah 7466 sektor.
2. Pada *byte* 44 s/d 47, nilainya adalah 0x02, 0x00, 0x00 dan 0x00, yang didasarkan pada 32-*bit integer* nilainya 0x00000002 adalah 2. Ini artinya *root directory* pada FAT 32 ini dapat ditemukan pada *cluster* 2.
3. Pada *byte* 48 dan 49, nilainya adalah 0x01 dan 0x00, yang didasarkan pada 16-*bit integer* nilainya 0x0001 adalah 1. Ini maksudnya adalah FSINFO terletak pada sektor 1.
4. Pada *byte* 50 dan 51, nilainya adalah 0x06 dan 0x00, yang didasarkan pada 16-*bit integer* nilainya 0x0006 adalah 6. Ini menunjukkan bahwa *copy backup* dari *boot sector* ada pada sektor 6.
5. *Signature b*oot tambahan, yaitu 0x29 pada byte 66.
6. Pada *byte* 67 s/d 70, nilainya adalah 0xc8, 0xe6, 0x19 dan 0x58, yang didasarkan pada 32-*bit integer* nilainya 0x5819e6c8 adalah 1478092488 yang merupakan *serial number* dari volume FAT 32.
7. Pada *byte* 71 s/d 81, nilai teksnya adalah '*NO NAME* diikuti 4 spasi' yang merupakan label umum. Nama label dari *volume* yang sesungguhnya dapat dilihat pada beberapa *byte* pertama dari *root directory* yang terletak di *cluster* 2 pada FAT 32 ini.

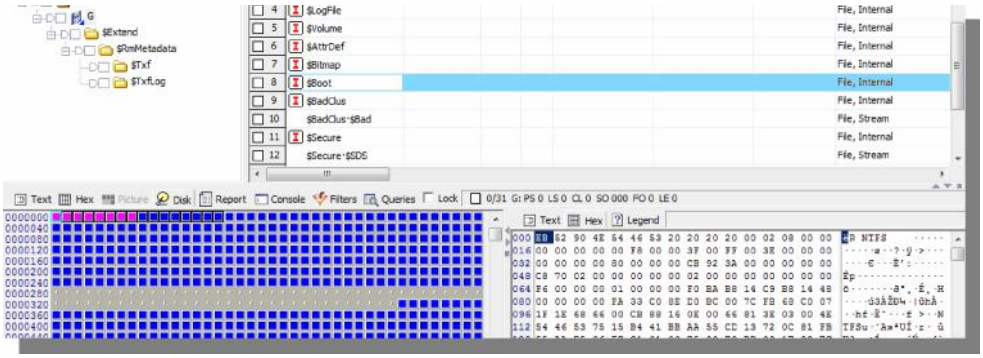
8. Pada *byte* 82 s/d 89, nilai teksnya adalah 'FAT32 diikuti 3 spasi' yang menunjukkan tipe *file system* yaitu FAT32.

FAT 12/16		FAT 32	
Nomor Byte	**Deskripsi**	**Nomor Byte**	**Deskripsi**
36	Nomor *drive* BIOS INT13h	36-39	Jumlah sektor dalam 1 FAT
37	Tidak digunakan	40-41	Mendefenisikan struktur FAT yang aktif
38	0x29 merupakan *signature boot* tambahan	42-43	Nomor versi mayor dan minor
39-42	*Serial number* dari volume yang kalkulasinya *didasarkan* pada tanggal/waktu pembuatan	44-47	*Cluster* di mana *root directory* dapat ditemukan
43-53	Label (nama) *volume* dalam bahasa ASCII	48-49	Sektor di mana struktur FSINFO dapat ditemukan
54-61	Tipe *file system* dengan nilai standar ASCII adalah FAT, FAT12 dan FAT16	50-51	Sektor di mana *copy backup* dari *boot sector* diletakkan
		52-63	*Reserved* (tersimpan untuk kepentingan yang lain)
		64	Nomor *drive* BIOS INT13h
		65	Tidak digunakan
		66	0x29 merupakan *signature boot* tambahan
		67-70	*Serial number* dari *volume* yang kalkulasinya didasarkan pada tanggal/waktu pembuatan
		71-81	Label (nama) *volume* dalam bahasa ASCII
		82-89	Tipe *file system* dengan nilai standar ASCII adalah FAT32

Tabel V.3. Struktur data *boot sector* pada FAT 12/16 dan FAT 32 mulai untuk *byte* 36 dan selanjutnya.

File system NTFS: struktur MFT dan boot sector

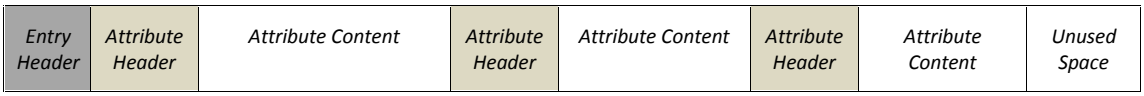
NTFS (*New Technology File System*) yang dikeluarkan juga oleh Microsoft merupakan *file system* yang berbeda dengan pendahulunya seperti FAT 12/16 dan FAT 32. *File system* NTFS ini akhirnya menjadi *default* (standar) bagi sistem operasi Windows NT, Windows 2000, Windows Server, Windows XP, Windows Vista dan Windows 7. Walaupun begitu *file system* FAT masih tetap ada untuk media penyimpanan berukuran kecil. Secara umum NTFS lebih kompleks dibandingkan dengan FAT karena NTFS memiliki banyak fitur dan mudah sekali untuk berubah (*scalable*) menurut jumlah *file* dan/atau direktori yang ada. Berbeda dengan FAT, pada NTFS, semua area pada *file system* ini merupakan area data, hanya beberapa sektor pertama (yaitu *volume boot*) yang tetap dialokasikan untuk *boot sector* dan *boot code*, seperti yang terlihat pada Gambar V.12 dan gambar di bawah ini.



Gambar V.20. Pada *file system* NTFS dengan besarnya 1 *cluster* adalah 4096 *bytes* (8 sektor), 16 sektor pertama dialokasikan untuk *boot sector* dan *boot code* dan 8 sektor kemudian untuk MFT *Mirror*.

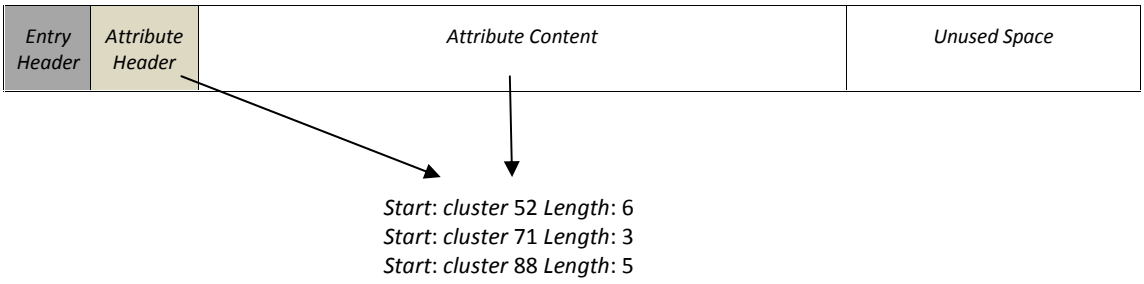
Salah satu tujuan utama dari NTFS adalah untuk men-*support* media penyimpanan berukuran besar, oleh karena itu NTF harus dapat diandalkan dengan sistem *integrity* dan sekuriti yang kuat. Untuk menunjang hal tersebut, ada satu konsep yang sangat fundamental pada NTFS yaitu '*everything is a file*', artinya segala sesuatu tentang data termasuk direktori dialokasikan dalam bentuk satu *file*. Setiap *file* tersebut diorganisasi sedemikian rupa oleh suatu mekanisme sehingga memiliki paling tidak 1 *entry* (*record*). Mekanisme ini disebut dengan MFT (*Master File Table*). Setiap *entry* memiliki ukuran 1 KB di mana hanya 42

bytes pertama yang merupakan *header* dan memiliki tujuan yang sudah didefenisikan, sedangkan *bytes* lain menyimpan atribut-atribut tentang *file* tersebut di mana setiap atribut menyimpan *header* dan atribut lain untuk menyimpan isinya, seperti yang terlihat pada gambar di bawah ini.



Gambar V.21. Struktur dari 1 MFT *entry* yang berukuran 1 KB.

Gambar di atas menunjukkan 1 MFT *entry* yang memiliki 4 *header* dengan isinya masing-masing. *Attribute header* berisikan tipe *attribute*, ukuran dan namanya, di samping *flag* (bendera) yang menunjukkan apakah isinya ter-kompresi (*compressed*) atau ter-enkripsi (*encrypted*). Sementara itu, *attribute content* menyimpan informasi format dan besarnya ukuran. Jika isi yang disimpan di *attribute content* memiliki ukuran yang kecil, maka isi tersebut akan disimpan langsung di MFT *entry* yang berukuran 1024 *bytes*. Ini disebut dengan *resident attribute* yang posisinya langsung mengikuti *header*-nya. Jika isi yang disimpan di *attribute content* memiliki ukuran sangat besar, misalnya beberapa MB hingga GB, maka penyimpanan di *attribute content* menjadi tidak praktis.



Gambar V.22. Struktur MFT *entry* dengan penyimpanan *non-resident attribute* di mana *attribute content* disimpan di *cluster* eksternal secara berurutan.

Untuk menyikapi hal tersebut, isi tersebut disimpan di *cluster-cluster* eksternal secara berurutan, kemudian nomor *cluster-cluster* tersebut ditandai di *attribute header* dengan nomor *cluster* awal (*start*) diikuti panjang *cluster*-nya (*length*).

Jenis penyimpanan seperti ini disebut dengan *non-resident attribute*, seperti yang terlihat pada Gambar V.22.

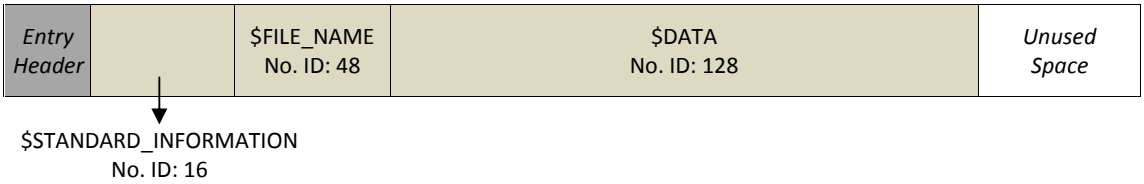
Dari gambar di atas, dapat dilihat penyimpanan *cluster* eksternal dilakukan secara berurutan yang dimulai dari *cluster* awal (*start*) dan diikuti berapa panjang (*length*) *cluster*-nya, misalnya *cluster* awal 52 dengan panjang 6 *clusters*, maka *cluster* eksternal-nya adalah 52, 53, 54, 55, 56, dan 57, begitu juga dengan yang dibawahnya dimulai dari *cluster* 71, 72 dan 73, dan yang terakhir dimulai dari *cluster* 88, 89, 90, 91 dan 92. *Cluster-cluster* tersebut merupakan LCN (*Logical Cluster Number*) yang memiliki alamat *logical* sesuai dengan pengalamatan dari *file system*. Dari contoh gambar di atas, diketahui *cluster eksternal* untuk penyimpanan *attribute content* berjumlah 14 *clusters* yang terfragmentasi menjadi 3 bagian.

Tipe atribut yang tersimpan di *attribute header* diberikan nomor identifikasi yang menunjukkan nama atribut (yang dimulai dengan $ diikuti dengan nama dengan huruf kapital) berikut deskripsinya. Hal ini tersimpan di *file* metadata $AttrDef. Tabel berikut di bawah ini berisikan beberapa tipe-tipe atribut tersebut. Tabel ini merujuk kepada Tabel 11.2 tentang tipe atribut pada MFT *entry* (Carrier, p.282).

No. ID Tipe	Nama Atribut	Deskripsi
16	$STANDARD_INFORMATION	Informasi umum seperti *flags* (tanda bendera), *time stamps* (seperti *created*, *modified*, dan *accessed date*), kepemilikan dan nomor ID sekuriti
48	$FILE_NAME	Nama *file* dalam bahasa Unicode, termasuk informasi *time stamps* dan *flags*
96	$VOLUME_NAME	Nama volume
112	$VOLUME_INFORMATION	Versi dari *file system* dan informasi *flags* yang lain
128	$DATA	Isi dari *file*
144	$INDEX_ROOT	Posisi *root* dari suatu pohon indeks
160	$INDEX_ALLOCATION	Posisi pohon indeks yang terletak di *root* $INDEX_ROOT
176	$BITMAP	Suatu pemetaan mengenai pengalokasian *file* $MFT termasuk peng-indeks-an
256	$LOGGED_UTILITY_STREAM	Berisikan *keys* (kunci-kunci) dan informasi mengenai atribut yang terenkripsi

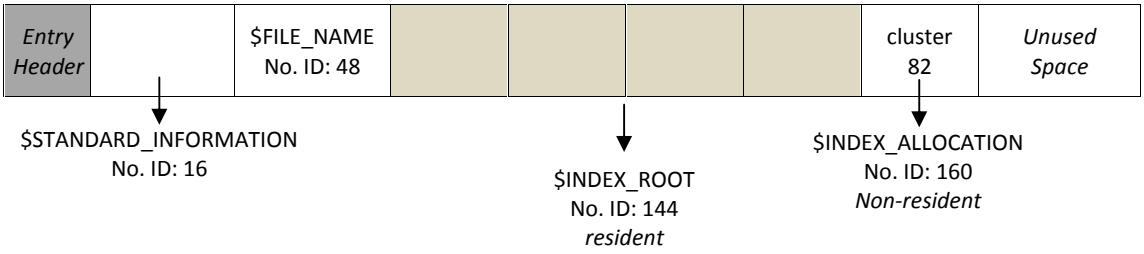
Tabel V.4. Nomor ID untuk tipe-tipe atribut pada MFT *entry* beserta deskripsinya.

Berdasarkan tabel di atas, maka hampir setiap MFT *entry* memiliki $STANDARD_INFORMATION, $FILE_NAME, dan $DATA, di mana atribut $FILE_NAME menyimpan informasi tentang nama *file*, ukuran dan *time stamps*, sedangkan atribut $STANDARD_INFORMATION berisikan informasi mengenai kepemilikan, sekuriti dan *time stamps*. Kedua atribut ini tersimpan sebagai *resident*. Jika isi *file* yang akan disimpan di atribut $DATA kurang dari 700 *bytes*, maka isi tersebut akan bersifat *resident*, sebaliknya jika isinya lebih dari 700 *bytes*, maka ia akan disimpan sebagai *non-resident* di *cluster-cluster* eksternal. Hal ini dapat dilihat pada gambar di bawah ini.



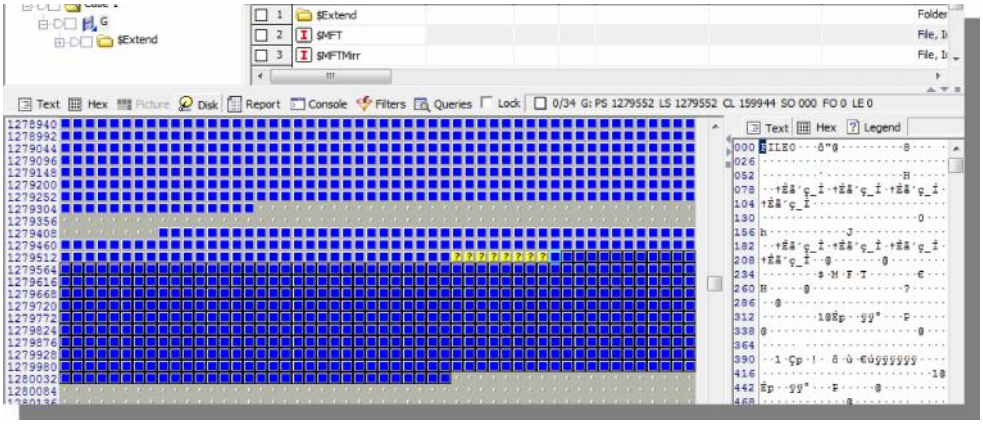
Gambar V.23. Struktur MFT *entry* dengan tipe-tipe atribut berikut nomor ID-nya.

Juga berdasarkan tabel di atas, setiap direktori yang dibuat akan memiliki atribut $INDEX_ROOT yang berisikan informasi tentang *file-file* dan sub-direktori-sub-direktori yang berada di dalam direktori tersebut. Jika direktori tersebut memiliki informasi yang besar, maka atribut $INDEX_ALLOCATION dan $BITMAP juga digunakan untuk menyimpan informasi tersebut. $INDEX_ALLOCATION akan bersifat *non-resident* dan menyimpan informasi tentang nomor *cluster*, misalnya *cluster* 82 di mana indeks-indeks *entry* tersimpan. Untuk mendapatkan informasi yang lengkap mengenai masing-masing indeks-indeks *entry* tersimpan, maka harus melihat *cluster* 82 tersebut. Hal ini dapat dilihat pada gambar di bawah ini yang menunjukkan suatu direktori dengan 4 indeks *entry* yang tersimpan sebagai *resident* dan indeks-indeks *entry* lain yang bersifat *non-resident* tersimpan di *cluster* 82.



Gambar V.24. Struktur MFT *entry* untuk direktori yang memiliki 4 indeks *entry* yang bersifat *resident* dan *cluster* 82 yang menyimpan indeks-indeks *entry* yang lain secara *non-resident*.

MFT *entry-entry* yang menyimpan informasi lengkap termasuk lokasi penyimpanan untuk setiap *file* dan/atau direktori seperti yang dijelaskan di atas tersimpan di *file* metadata $MFT. Seperti atribut yang lain, $MFT juga memiliki atribut $DATA yang berisikan *cluster-cluster* yang digunakan, dan $BITMAP yang digunakan untuk mengatur pengalokasian *entry-entry* tersebut, di samping atribut $FILE_NAME dan $STANDARD_INFORMATION. $MFT dimulai dengan ukuran sekecil mungkin dan kemudian tumbuh membesar mengikuti jumlah *file* dan direktori yang dibuat. Karena alasan inilah NTFS disebut memiliki sifat '*scalable*' (dapat berubah menurut kebutuhan). Misalnya pada *file system* NTFS dengan besarnya 1 *cluster* adalah 4096 *bytes* (8 sektor), $MFT dialokasikan sebesar 512 sektor (64 *cluster*) yang dimulai pada sektor 1279552. Sektor-sektor setelah $MFT ini merupakan *unallocated cluster*. Ini dimaksudkan agar ketika $MFT ini berkembang membesar mengikuti jumlah *file* dan direktori yang semakin banyak sehingga 512 sektor yang dialokasikan untuk $MFT sudah tidak cukup lagi, maka *unallocated cluster* ini akan digunakan untuk menampung perkembangan dari $MFT. Ini dapat dilihat pada gambar di bawah ini.



Gambar V.25. Posisi $MFT pada *file system* NTFS dengan besaran 1 *cluster* sama dengan 4096 *bytes*, di mana $MFT ini dialokasikan sebanyak 512 sektor untuk tahap awal, dan jika kemudian berkembang mengikuti jumlah *file* dan direktori yang dibuat, *unallocated clusters* yang posisinya setelah $MFT akan dialokasikan untuk itu.

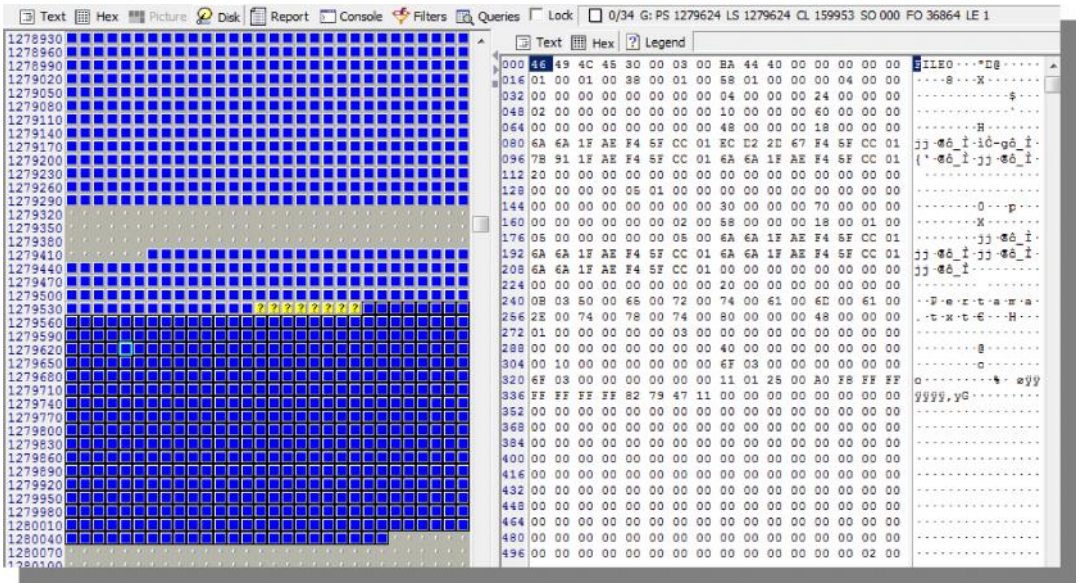
Sama seperti *file system* FAT, NTFS juga memiliki *backup* dari $MFT untuk mengantisipasi jikalau $MFT mengalami kegagalan atau *corrupt* (berkurang/berubah isinya) sehingga tidak bisa digunakan lagi. *Backup* tersebut adalah $MFTMirr. Seperti pada Gambar V.20, $MFTMirr dialokasikan sebanyak 8 sektor setelah *volume boot* yang berjumlah 16 sektor.

Pada penjelasan-penjelasan sebelumnya, ketika satu *file* dibuat, misalnya Pertama.txt, maka akan dibuat satu *entry* baru di $MFT yang berisikan lengkap tentang *file* tersebut yang tersimpan pada atribut-atribut seperti $STANDARD_INFORMATION, $FILE_NAME, dan $DATA. MFT *entry* yang memiliki ukuran 1024 *bytes* memiliki informasi untuk setiap *byte*-nya yang merujuk pada atribut-atribut tersebut. Tabel di bawah ini menjelaskan deskripsi untuk beberapa *byte* yang ada di *header* dari MFT *entry* yang memiliki informasi esensial, di mana tabel ini merujuk pada Tabel 13.1 tentang struktur data untuk MFT *entry* (Carrier, p.353).

Nomor Byte	Deskripsi
0-3	*Signature* berupa teks 'FILE'
4-5	*Offset* untuk *fixup array* (yang digunakan untuk menggantikan 2 *bytes* terakhir dari setiap sektor untuk menjaga keutuhan struktur data yang besar, jika lebih dari 1 *entry* yang digunakan).
6-7	Jumlah *entry* di *fixup array*
20-21	*Offset* untuk atribut pertama
22-23	*Flags* (tanda): 0x01 untuk *entry* yang digunakan, dan 0x02 untuk *entry* direktori
24-27	Besarnya *byte* yang digunakan untuk 1 *entry*
28-31	Besarnya ukuran 1 *entry* (dalam *byte*)

Tabel V.5. Struktur data untuk beberapa *byte* di *header* dari MFT *entry* berikut deskripsinya.

Pada contoh sebelumnya, dibuat *file* Pertama.txt dan untuk itu ada 1 *entry* baru di MFT. *Entry* ini dalokasikan pada sektor 1279624 seperti yang terlihat pada gambar di bawah ini.



Gambar V.25. MFT *entry* untuk *file* Pertama.txt yang teralokasikan di sektor 1279624.

42 *bytes* pertama dari sektor tersebut dialokasikan untuk *entry header*. 4 *bytes* pertama merupakan *signature* untuk MFT *entry*, yaitu teks '*FILE*' atau heksadesimal '0x46 0x49 0x4c 0x45'. Pada *byte* 4 dan 5, nilai *fixup array* adalah 0x30 dan 0x00 yang didasarkan pada 16-*bit integer* nilainya 0x0030 adalah 48,

artinya besarnya *fixup array* di MFT *entry* diposisikan pada *byte* 48 dengan jumlah *entry* di *fixup array* adalah 3 (nilai *integer* dari 0x0003 pada *byte* 6 dan 7. Pada *byte* 20 dan 21, nilai *integer* dari 0x0038 adalah 56, artinya atribut pertama diposisikan di *byte* 56. Pada *byte* 22 dan 23, nilai *integer* dari 0x0001 adalah 1, artinya *entry* sedang digunakan (*in use*). Jumlah *byte* yang digunakan pada *entry* ini bisa dilihat pada *byte* 24 s/d 27 yang nilai *integer* dari 0x00000158 adalah 344 *bytes*, sedangkan ukuran *entry* ini ada pada *byte* 28 s/d 31 yang nilai *integer* dari 0x00000400 adalah 1024 *bytes*.

Dari penjelasan di atas, didapat bahwa *fixup array* berada pada *byte* 48, di mana 2 *bytes* pertama, yaitu 0x0002 merupakan *signature* yang akan menggantikan 2 *bytes* terakhir pada sektor 1279624 dan 1279625. *Signature* ini berbeda dengan *entry-entry* lain.

Dari penjelasan sebelumnya, juga didapat atribut pertama dimulai pada *byte* 56, dan atribut-atribut ini akan berakhir pada *byte* 342 dengan *signature* 0xffff ffff.

Pada *byte* 56, nilai heksadesimalnya adalah 10 yang dikonversi menjadi *integer* adalah 16. Angka 16 ini merupakan nomor tipe atribut untuk $STANDARD_INFORMATION. Seperti yang telah dijelaskan sebelumnya bahwa salah satu informasi yang ada pada atribut ini adalah informasi mengenai tanggal/waktu (*date/time*) yang terbagi menjadi 4 jenis, yaitu *creation time* (*file* pertama kali dibuat), *file altered time* (*file* terakhir kali dimodifikasi), MFT *altered time* (data MFT terakhir kali berubah), dan *file accessed time* (*file* terakhir kali diakses/dibuka). Keempat jenis tanggal/waktu ini berada pada posisi :

Byte 80 s/d 87: *creation time*

Byte 88 s/d 95: *file altered time*

Byte 96 s/d 103 : MFT *altered time*

Byte 104 s/d 111: file *accessed time*

Pada Gambar V.25 di atas, nilai heksadesimal pada *byte-byte* tersebut adalah :

Byte 80 s/d 87: 0x01cc5ff4ae1f6a6a

Byte 88 s/d 95: 0x 01cc5ff4672dd2ec

Byte 96 s/d 103 : 0x01cc5ff4ae1f917b

Byte 104 s/d 111: 0x01cc5ff4ae1f6a6a

Nilai-nilai heksadesimal pada *byte-byte* di atas, kemudian dikonversi dengan menggunakan metode Windows *Date/Time* sehingga menjadi :

Byte 80 s/d 87: 08/21/11 06:22:58PM

Byte 88 s/d 95: 08/21/11 06:20:59PM

Byte 96 s/d 103 : 08/21/11 06:22:58PM

Byte 104 s/d 111: 08/21/11 06:22:58PM

Dari hasil di atas, diketahui bahwa atribut $STANDARD_INFORMATION menyimpan informasi tentang tanggal/waktu dari *file* Pertama.txt, yaitu :

Creation time: 08/21/11 06:22:58PM

File altered time: 08/21/11 06:20:59PM

MFT *altered time*: 08/21/11 06:22:58PM

File *accessed time*: 08/21/11 06:22:58PM

Setelah atribut $STANDARD_INFORMATION, terdapat atribut $FILE_NAME yang mana atribut ini dimulai pada *byte* 152 dengan nilai heksadesimalnya adalah 0x30 yang jika dikonversi menjadi *integer* adalah bernilai 48. Nomor 48 ini merupakan nomor tipe atribut ini. Untuk nama *file*, dikarenakan *file* ini bernama Pertama.txt yang jumlah karakternya kurang dari 8, maka nama *file* dimulai pada *byte* 242 s/d 262. Rentang *byte* ini diposisikan untuk nama *file* yang terdiri dari 8 karakter plus 3 karakter untuk format/ekstensinya. Jika nama *file* memiliki karakter lebih dari 8 (*long name*), maka pada karakter yang ketujuh akan diganti dengan tanda "~", kemudian diikuti nomor urutnya yang dimulai dari angka 1. Misalnya nama *file*-nya adalah Kelima_dan_Panjang.txt, maka akan tertulis pada rentang *byte-byte* tersebut "KELIMA~1.TXT". Adapun nama lengkap berikut ekstensinya akan tertampil pada *byte* 362 s/d 404.

Pada atribut ini juga, terdapat tanggal/waktu yang berkaitan dengan *file* tersebut. Tanggal/waktu tersebut terdiri dari 4 jenis yang masing-masing berada pada rentang *byte* sebagai berikut :

Byte 184 s/d 191: *file creation time* (*file* pertama kali dibuat)

Byte 192 s/d 199: *file modification time* (*file* terakhir kali dimodifikasi)

Byte 200 s/d 207 : MFT *modification time* (MFT terakhir kali dimodifikasi)

Byte 208 s/d 215 : *file accessed time* (*file* terakhir kali diakses/dibuka)

Sama seperti pada atribut sebelumnya, nilai-nilai heksadesimal pada *byte-byte* ini (seperti yang terlihat pada gambar V.25), kemudian dikonversi dengan menggunakan metode Windows *Date/Time*, sehingga didapat tanggal/waktu masing-masing sebagai berikut :

Byte 184 s/d 191: 0x01cc5ff4ae1f6a6a = 08/21/11 06:22:58PM

Byte 192 s/d 199: 0x01cc5ff4ae1f6a6a = 08/21/11 06:22:58PM

Byte 200 s/d 207 : 0x01cc5ff4ae1f6a6a = 08/21/11 06:22:58PM

Byte 208 s/d 215 : 0x01cc5ff4ae1f6a6a = 08/21/11 06:22:58PM

Dari 4 jenis kategori tanggal/waktu di atas, hanya 3 yang ditampilkan dalam *properties* dari sebuah *file*, yaitu *created date*, *modified date* dan *accessed date*, sementara MFT *modified date* tidak ditampilkan. Adapun 3 jenis tanggal/waktu yang ditampilkan pada *properties* tersebut berasal dari atribut $STANDARD_INFORMATION. Jika melihat contoh di atas, di mana *modified date* (08/21/11 06:20:59PM) usianya lebih tua dibandingkan dengan *created date* (08/21/11 06:22:58PM), maka hal ini menunjukkan bahwa *file* Pertama.txt merupakan hasil transfer (*copy-paste*) dari media penyimpanan komputer yang lain. *File* ini dibuat pertama kali di komputer yang lain tersebut pada tanggal 08/21/11 06:20:59PM, kemudian ditransfer ke media penyimpanan yang berbeda pada tanggal 08/21/11 06:22:58PM.

Setelah atribut $STANDARD_INFORMATION dan $FILE_NAME, terdapat atribut $DATA yang dimulai pada *byte* 264 di mana berdasarkan pada Gambar V.25 memiliki nilai heksadesimal 0x80 yang jika dikonversi menjadi *integer* bernilai 128. Angka 128 ini merupakan nomor tipe atribut untuk $DATA. Pada *byte* 330 terdapat nilai heksadesimal 0x23 yang di dalam *integer* bernilai 35. Angka 35 ini menunjukkan tempat penyimpanan isi dari *file* pertama.txt, yaitu pada *cluster* 35 (*Start*). Adapun untuk panjang (*Length*) *cluster* untuk menyimpan isi *file* tersebut ditunjukkan pada *byte* 329 yang bernilai heksadesimal 0x02 atau sama dengan 02 dalam bahasa *integer*. Jadi diketahui bahwa *file* Pertama.txt disimpan isinya dimulai pada *cluster* (*Start*) 35 sebanyak (*Length*) 2 *cluster*, artinya menempati *cluster* 35 dan 36.

Untuk nama *file* yang panjang seperti contoh di atas “Kelima_dan_Panjang.txt”, maka atribut $DATA dimulai pada *byte* 408, sedangkan alamat *cluster*

penyimpanan isi *file* dimulai pada *byte* 474 s/d 476. Dari data-data ini, dapat diketahui bahwa alamat *cluster* (*Start*) penyimpanan isi *file* berada setelah 66 *bytes* dari *bytes* awal dari atribut ini yang berisikan nomor tipe atribut 128, sedangkan panjang *cluster* (*Length*) yang digunakan berada setelah 65 *bytes* dari *bytes* awal.

Setelah memahami struktur dari MFT *entry* yang memuat informasi yang lengkap mengenai sebuah *file*, yang mana MFT *entry* tersebut terdiri dari beberapa atribut seperti $STANDARD_INFORMATION, $FILE_NAME dan $DATA, penjelasan berikut di bawah ini akan berkenaan dengan *file* metadata $Boot yang berisikan informasi tentang *boot sector* yang dialokasikan pada 16 sektor pertama seperti pada Gambar V.20 di atas.

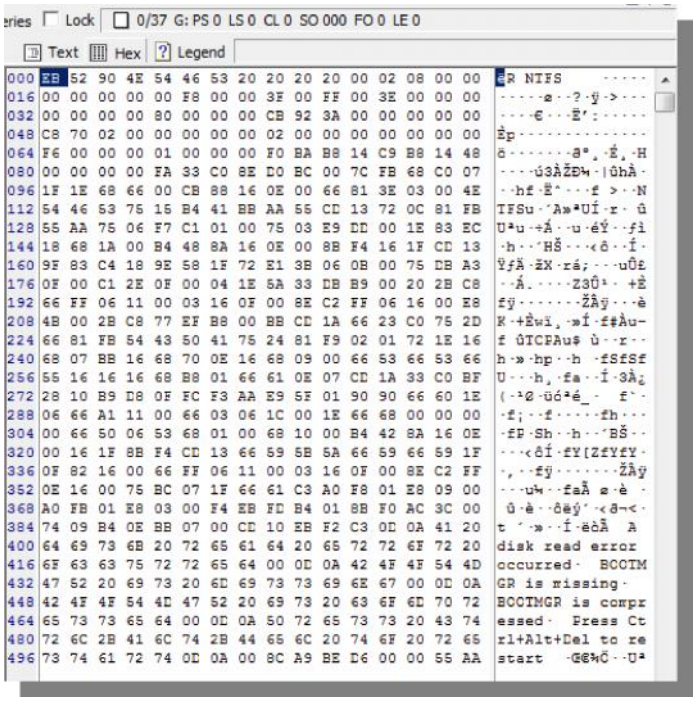
Nomor Bytes	Deskripsi
0-2	Instruksi untuk kode *boot* yang merujuk ke *bootable file system*
3-10	Nama OEM pada bahasa ASCII
11-12	Jumlah *bytes* untuk 1 sektor. Nilai yang diijinkan adalah 512, 1024, 2048 dan 4096 *bytes*
13	Jumlah sektor per *cluster*. Jumlah yang diijinkan adalah kelipatan 2 sektor. Besarnya ukuran *cluster* mulai dari 512 *bytes* hingga 32 KB
14-15	Besarnya ukuran area *reserved* (dalam sektor)
21	Jenis media. Jika 0xf8 artinya *fixed disk* (*harddisk* yang terpasang di dalam komputer), sedangkan 0xf0 artinya *removable media* seperti *flashdisk*
40-47	Jumlah total sektor di *file system*
48-55	Alamat *cluster* awal dari MFT
56-63	Alamat *cluster* awal dari MFT *Mirror*
64	Ukuran MFT *entry*
72-79	*Serial number*
84-509	*Boot code*
510	0x55 merupakan *signature* pada *footer*
511	0xaa merupakan *signature* pada *footer*

Tabel V.6. Deskripsi beberapa *bytes* di *boot sector* NTFS

Sama seperti *boot sector* pada *file system* FAT, *boot sector* (sektor 0) juga memiliki informasi-informasi penting dari byte 0 s/d 511 (512 *bytes*), namun tidak semua

byte digunakan (*unused*), misalnya pada *byte* 16 s/d 20 dan 24 s/d 39. Tabel V.8. berisikan informasi pada beberapa *byte* yang ada di *boot sector* tersebut. Tabulasi ini merujuk pada Tabel 13.18 tentang struktur data *boot sector* NTFS (Carrier, p.379-380). Deskripsi/kegunaan pada beberapa *byte* tertentu antara *boot sector* FAT dan NTFS memiliki kesamaan, misalnya pada 16 *bytes* pertama. Hal ini bisa dilihat pada Tabel V.8. dan dibandingkan dengan Tabel V.2 sebelumnya.

Seperti pada beberapa contoh sebelumnya, terhadap media penyimpanan *flashdisk* yang di-format NTFS dengan besaran 4096 *bytes* (8 sektor) per 1 *cluster* dianalisa *boot sector*-nya dengan detil *byte-byte* seperti pada tabel di atas. Gambar di bawah ini menunjukkan nilai heksadesimal masing-masing *byte* dari *boot sector* NTFS tersebut.



Gambar V.26 *Boot sector* (sektor 0) yang terdiri dari 512 *bytes* dari *file system* NTFS.

Pada gambar di atas, nama OEM yang terletak pada *byte* 3 s/d 10 adalah NTFS yang diikuti oleh beberapa spasi (0x20). Jumlah *bytes* untuk setiap 1 sektor dapat diketahui pada *byte* 11 dan 12 yang nilai *integer* dari konversi heksadesimal 0x0200 adalah 512, yang artinya terdapat 512 *bytes* per sektor. Untuk besarnya jumlah sektor per 1 *cluster*, dari byte 13 diketahui bahwa 1 *cluster* terdiri dari 8 sektor (0x08), atau 4096 *bytes*. Sementara itu, jumlah total sektor pada *file*

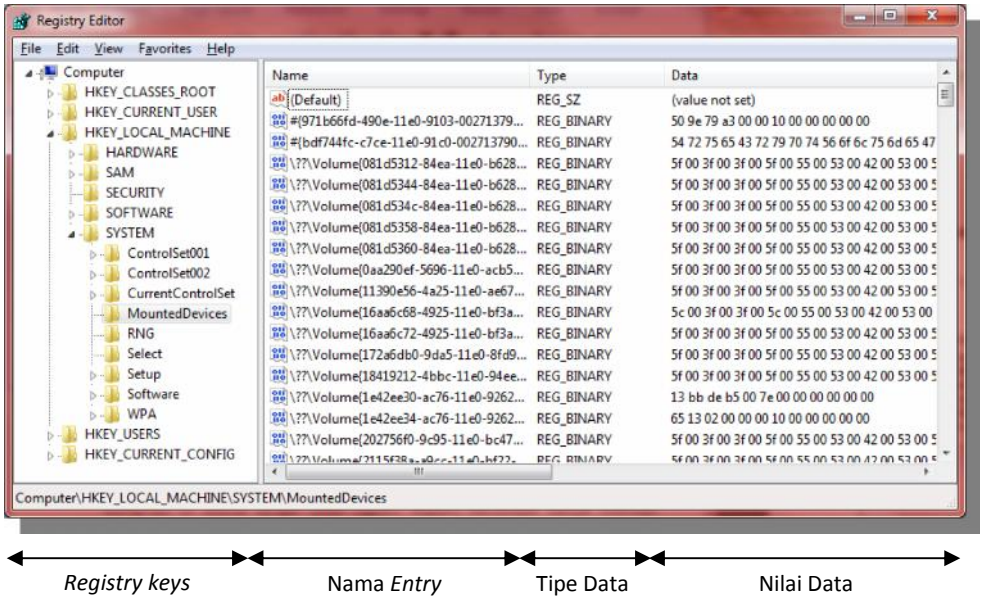
system NTFS ini dapat dilihat pada *byte* 40 s/d 47. Hasil konversi nilai heksadesimal (0x0000 0000 003a 92cb) ke nilai *integer* adalah 3838667. Ini artinya pada media penyimpanan dengan *file system* NTFS tersebut memiliki ukuran 2 GB yang terdiri dari 3.838.667 sektor. Untuk MFT dan MFT *Mirror*, alamat awal *cluster* tempat penyimpanan MFT dan MFT *Mirror* tersebut, masing-masing dapat dilihat pada *byte* 48 s/d 55 dan 56 s/d 63. Hasil konversi ke bentuk *integer* dari nilai heksadesimal pada masing-masing *byte* tersebut, yaitu 0x0000 0000 0002 70c8 dan 0x0000 0000 0000 0002 adalah 159944 dan 2. Ini artinya MFT dimulai pada *cluster* 159.944, sedangkan MFT *Mirror* pada *cluster* awal 2. Untuk *boot signature* di 2 *bytes* akhir, yaitu 510 dan 511 adalah sama dengan FAT, yaitu masing-masing 0x55 dan 0xaa.

Dari penjelasan di atas mengenai *boot sector*, dapat diketahui bahwa pada beberapa *bytes* tertentu dari *file system* FAT dan NTFS memiliki kesamaan fungsi, seperti pada beberapa *bytes* pertama (0 s/d 15) dan *signature* pada 2 *bytes* terakhir.

Analisa registry

Di dalam sistem operasi Windows, terdapat suatu perorganisasian konfigurasi sistem untuk satu atau lebih *user*, aplikasi-aplikasi dan *hardware-hardware* yang mana konfigurasi tersebut terdiri dari database yang terstruktur (*hierarchical*). Sistem pengorganisasian konfigurasi ini dikenal dengan istilah *registry*. *Registry* menyimpan banyak informasi-informasi yang penting yang digunakan oleh sistem operasi dan aplikasi-aplikasi untuk bagaimana mereka berjalan sesuai dengan setting yang dibuat oleh seorang *user*.

Registry terdiri dari 5 sampai 7 *root k*eys (kunci-kunci *setting* pada posisi *root directory*) yang juga dikenal dengan istilah *hives*, atau dengan singkatan HKEY (*Handle to a KEY*). *Registry* dengan HKEY-HKEY ini yang terdiri dari 4 elemen yang terstruktur, yaitu *registry keys*, nama *entry*, tipe data dan nilai data. Elemen-elemen ini dapat dilihat dengan aplikasi regedit (*Registry Editor*) seperti gambar di bawah ini.



Gambar V.27. Aplikasi regedit menampilkan element-element *registry* dari sistem operasi Windows 7.

Pada gambar di atas, dapat dilihat bahwa *registry keys* terdiri dari 5 *root keys* yang berbeda, yaitu

a. HKEY_CLASSES_ROOT (disingkat HKCR), berisikan informasi detil tentang *user interface* (tampilan yang sesuai dengan *setting* dari *user*), *shortcuts* (*link-link* ke aplikasi tertentu) dan aturan *drag-and-drop*. HKCR ini merupakan alias dari HKLM\SOFTWARE\Classes.

b. HKEY_CURRENT_USER (HKCU), berisikan informasi yang sifatnya '*user-specific'* yang dimulai dari *user log on* dan dikonstruksi oleh informasi yang ada di HKU. Infromasi-informasi ini terbagi dalam direktori-direktori *subkeys* yang berbeda, antara lain AppEvents, Console, Control Panel, Environment, EUDC, *Identities*, Keyboard Layout, Network, Printers, *Software*, *System* dan *Volatile Environment*. HKCU ini merupakan alias dari salah satu *user* dari HKU.

c. HKEY_LOCAL_MACHINE (HKLM), berisikan informasi yang sifatnya '*machine-specific*' yang berkaitan dengan mesin di mana sistem operasi sedang *running* (berjalan). Hal ini termasuk antara lain *drives* (media penyimpanan) yang ter-*mounting* (diakses/dibuka), *hardware-hardware* dan konfigurasi umum dari aplikasi-aplikasi yang ter-install. Informasi-

informasi tersebut terbagi dalam beberapa direktori *subkeys*, seperti HARDWARE, SAM (*Security Accounts Manager*) yang menyimpan informasi mengenai *users* dan *groups*, SECURITY, SOFTWARE dan SYSTEM.

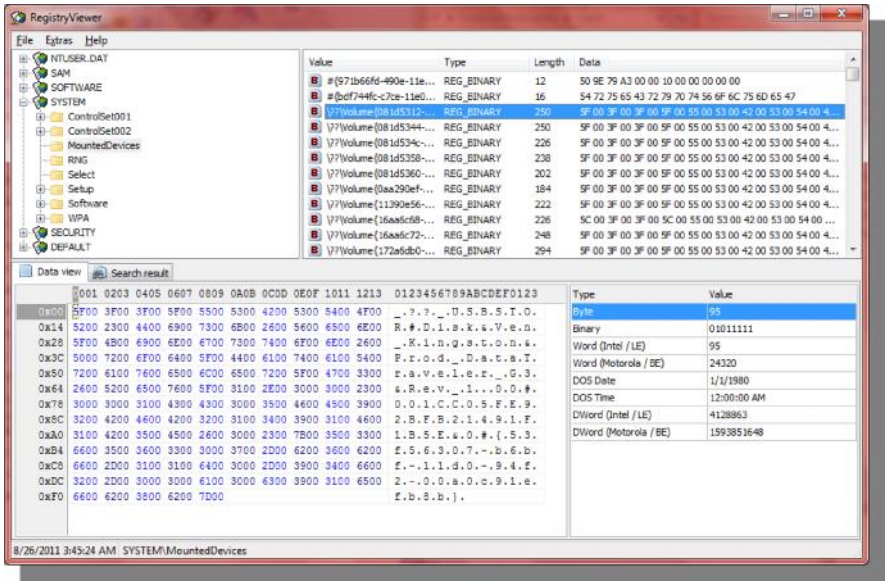
d. HKEY_USERS (HKU), berisikan informasi tentang semua *user* yang memiliki *account* pada sistem operasi. Informasi-informasi ini antara lain tentang konfigurasi aplikasi dan *visual settings*.
e. HKEY_CURRENT_CONFIG (HKCC), berisikan informasi tentang konfigurasi sistem yang sedang berjalan. Informasi-informasi tersebut tersimpan dalam direktori-direktori *subkeys* seperti *Software* dan *System*. Beberapa data *subkeys* merupakan alias dari HKLM.

Dari penjelasan di atas, dapat dilihat bahwa sistem *registry keys* pada Windows sebenarnya hanya terdiri dari 2 bagian yang penting, yaitu HKLM (*Local machine*) dan HKU/HKCU (*Users/Current Users*). Untuk *registry keys* yang lain merupakan alias (*link*) dari HKLM.

Pada Sistem operasi Windows XP, Vista dan 7, *file-file registry* tersebut tersimpan di *path* c:\Windows\System32\config, kecuali *file-file registry* yang berhubungan dengan *user* tertentu (HKCU) yang dapat dilihat pada *path* c:\Users\<*username*>\NTUSER.DAT (untuk Windows Vista dan 7) atau c:*Documents and Settings*\<*username*>\NTUSER.DAT (untuk Windows XP). *File-file* yang dibutuhkan untuk melakukan analisa *registry* dari *path* c:\Windows\System32\config tersebut adalah SYSTEM, SOFTWARE, SAM, SECURITY dan DEFAULT, di mana *file-file* tersebut tanpa memiliki ekstensi/format. Jika *forensic analyst* dan *investigator* mendapatkan barang bukti komputer dan ingin melakukan analisa registry, maka mereka harus meng-copy *file-file* tersebut, lebih baik lagi meng-*copy* satu *folder* c:\Windows\System32\config ke *analysis* workst*a*tion untuk dianalisa secara independen. Artinya analisa *registry* dilakukan secara *offline*, tanpa komputer dalam keadaan *on* (hidup).

Ada beberapa *software*, baik *commercial* maupun *freeware*, baik *Windows-based* maupun *Linux-based* untuk analisa *registry* tersebut. Salah satunya yang sering digunakan adalah aplikasi *Registry Viewer* yang dikembangkan oleh Werner Rumpeltesz (http://www.gaijin.at). Setelah memasukkan *file-file registry* yang diinginkan seperti yang dijelaskan di atas yaitu SYSTEM, SOFTWARE, SAM,

SECURITY, DEFAULT dan NTUSER.DAT, maka *forensic analyst* dan *investigator* dapat melakukan analisa lebih detil terhadap *registry* yang berasal dari barang bukti komputer seperti pada gambar di bawah ini.



Gambar V.28. Aplikasi *Registry Viewer* menampilkan data dari masing-masing *registry keys* NTUSER.DAT, SAM, SOFTWARE, SYSTEM, SECURITY dan DEFAULT.

Berikut di bawah ini adalah beberapa *registry keys* dari sistem operasi Windows 7 yang dianalisa secara detil untuk mendapatkan informasi yang lengkap darinya :

1. Informasi sistem operasi

   Untuk mendapatkan informasi tentang sistem operasi yang di-*install* pada komputer barang bukti atau milik pelaku dapat dilihat pada *registry keys* SOFTWARE\Microsoft\Windows NT\CurrentVersion. Informasi tentang sistem operasi tersebut misalnya :

   ProductName: Windows 7 Ultimate

   ProductId: xxxxx-OEM-xxxxxxx-xxxxx

   CSDVersion: Service Pack 1

   SystemRoot: C:\Windows

   RegisteredOwner:

   InstallDate: 4D7490EE

   Pada InstallDate di atas didapat nilai heksadesimal 4D7490EE yang menunjukkan waktu instalasi sistem operasi Windows dilakukan. Untuk itu

bilangan heksadesimal ini perlu dikonversi dengan menggunakan aplikasi-aplikasi *time decoder*. Salah satu aplikasi yang sering digunakan adalah *The Time Lord* yang dikembangkan oleh Paul Tew. Aplikasi ini menyediakan proses *decoding* dan *encoding* untuk mendapatkan waktu sesuai dengan tipe *file system*-nya seperti NTFS, FAT, Unix (Linux) dan HFS (Macintosh). Dengan aplikasi *The Time Lord* melalui *Big Endian*, bilangan heksadesimal di atas menunjukkan waktu 2011-03-07 15:01:50. Inilah waktu instalasi dari sistem operasi Windows 7 Ultimate pada komputer barang bukti.

2. Penyimpanan *password*

   Pengembang aplikasi seperti Microsoft menganggap *registry* merupakan tempat yang baik untuk menyimpan *username* dan *password* dari aplikasi mereka, seperti Outlook Express, Internet Explorer dan MSN Explorer. Meskipun *username* dan *password* tersebut diproteksi dengan enkripsi, namun data tersebut masih bisa didekripsi untuk dilihat isinya, misalnya dengan menggunakan aplikasi PassView dari Nirsoft. *Registry keys* yang dibutuhkan untuk melihat *password* yang tersimpan :

   HKCU\Software\Microsoft\Internet Explorer\IntelliForms\SPW

   HKCU\Software\Microsoft\Protected Storage System Provider

3. Aplikasi-aplikasi *Startup*

   Aplikasi-aplikasi ini dijalankan ketika proses *booting* dari sistem operasi Windows dimulai. Beberapa *registry keys* yang dibutuhkan untuk melihat aplikasi-aplikasi ini adalah :

   HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Runonce

   HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run

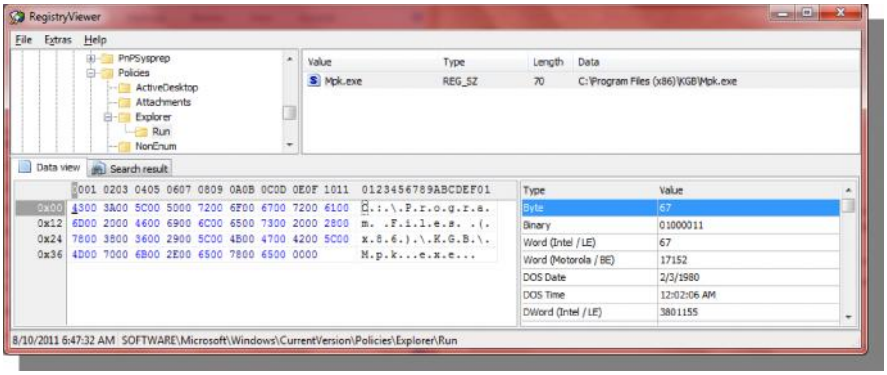
   HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

   HKCU\Software\Microsoft\Windows\CurrentVersion\Run

   HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

   Pada gambar di bawah ini, diketahui pada HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run ditemukan aplikasi Mpk.exe yang akan selalu berjalan ketika komputer dihidupkan. Aplikasi ini merupakan aplikasi *keylogger* yang biasa

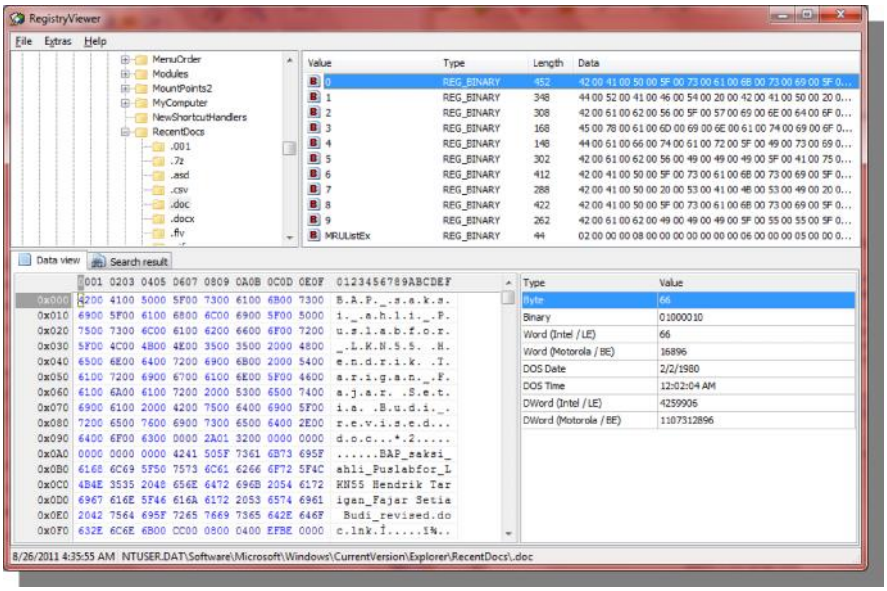
digunakan oleh *administrator* (untuk hal yang baik) atau *hacker* (untuk hal yang negatif) untuk merekam segala aktifitas pengetikan *keyboard* dari suatu komputer target.



Gambar V.29. *Registry key* HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run menunjukkan adanya aplikasi *keylogger*, yaitu Mpk.exe yang ter-*install* dan dijalankan pada *startup* dari proses *booting* sistem operasi Windows.

4. *File-file* terkini yang diakses (*recent files*)

   HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs adalah *registry keys* yang berisikan informasi mengenai *file-file* terkini yang diakses (*recent files*). Dari *registry keys* ini didapat bahwa *file-file recent* tersebut terbagi dalam beberapa sub-direktori sesuai dengan tipe ekstensi/format dari *file-file* tersebut, misalnya .doc, .docx, .ppt, .pptx, .pdf, .jpg dan lain-lain. Bagi *forensic analyst* dan *investigator*, hal tersebut memudahkan untuk mendapatkan *recent files* yang pernah diakses/dibuka oleh pelaku kejahatan di komputernya secara cepat, sekaligus untuk membuktikan keterangan yang disampaikan oleh pelaku jikalau ia mengelak bahwa pernah membuka satu *file* tertentu. Hal ini dapat dilihat pada gambar di bawah ini.



Gambar V.30. *Registry keys* HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs memuat informasi tentang *recent files* yang terbagi dalam beberapa sub-direktori sesuai dengan tipe ekstensi/format dari *file-file* tersebut.

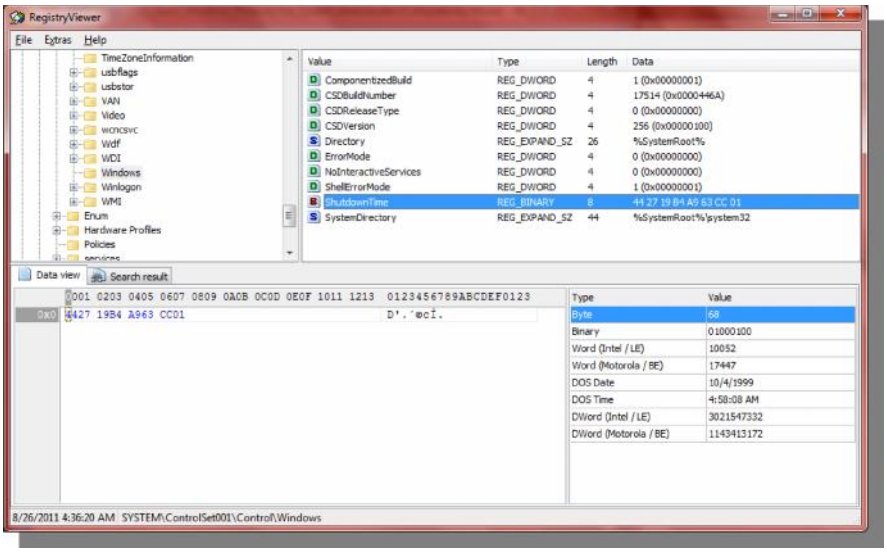
Selain *registry keys* di atas, juga terdapat *registry keys* HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32 yang menyimpan banyak informasi yang berkaitan dengan MRU (*Most recent Use*) seperti CIDSizeMRU (aplikasi-aplikasi terakhir/terkini yang digunakan), FirstFolder (*folder-folder* terakhir/terkini yang dibuka), LastVisitedPidMRU (*file-file* terakhir/terkini yang diakses oleh aplikasi tertentu), dan OpenSavePidMRU (berisikan *file-file* terkahir/terkini yang dibuka dan disimpan/*save*). OpenSavePidMRU ini terdiri dari sub-sub *folder* sesuai dengan jenis ekstensi/format dari *file-file* recent tersebut seperti 3gp, avi, doc, docx, exe, jpg, pdf, dan lain sebagainya.

5. *Last shutdown* (waktu terakhir kali komputer dimatikan) dan *time zone*

   Registry juga menyimpan informasi mengenai kapan terkahir kali suatu komputer dimatikan (*shutdown*). Informasi ini penting bagi *forensic analyst* dan *investigator* untuk mengetahui kebenaran dari keterangan pelaku mengenai penggunaan komputernya untuk terakhir kali. Informasi yang tersimpan pada *registry keys*

SYSTEM\ControlSet001\Control\Windows\ShutdownTime ini berupa bilangan heksadesimal yang perlu dibuka (*decode*) untuk mendapatkan nilai waktu yang sesungguhnya. Untuk itu dibutuhkan aplikasi-aplikasi yang dapat melakukan decoding terhadap bilangan heksadesimal tersebut. Salah satunya adalah aplikasi *The Time Lord*.

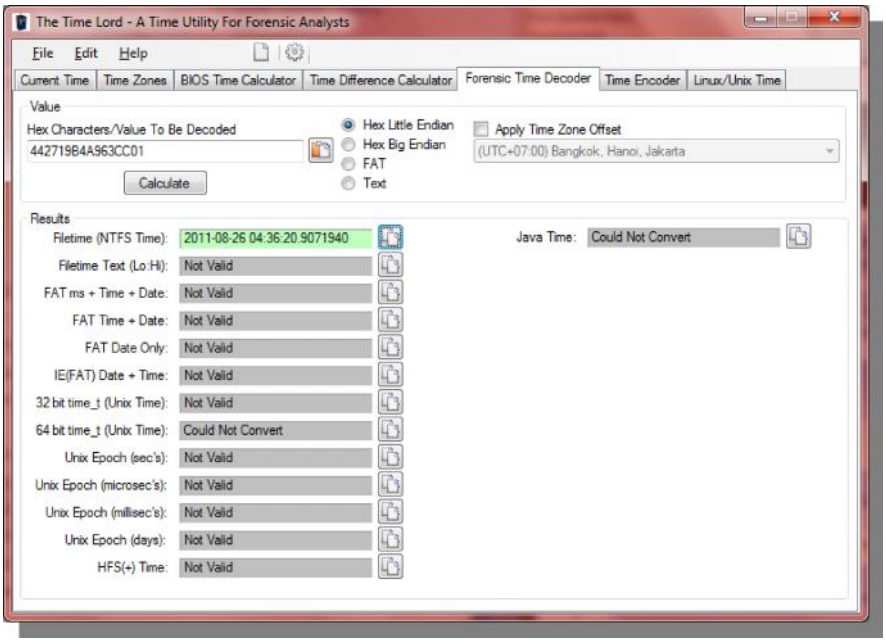
Gambar berikut adalah *registry keys* yang menunjukkan waktu *last shutdown*. Pada gambar tersebut didapat nilai heksadesimal 4427 19B4 A963 CC01.



Gambar V.31. *Registry keys* SYSTEM\ControlSet001\Control\Windows\ShutdownTime yang menyimpan informasi mengenai *last shutdown* (wkatu terkahir kali komputer dimatikan) dalam bentuk bilangan heksadesimal.

Bilangan heksadesimal 4427 19B4 A963 CC01 seperti yang didapat dari *registry keys* SYSTEM\ControlSet001\Control\Windows\ShutdownTime ini selanjutnya dilakukan proses *decoding* untuk mendapatkan informasi waktu *last shutdown* dengan menggunakan aplikasi *The Time Lord*. Dengan aplikasi tersebut diketahui bahwa bilangan heksadesimal tersebut menunjukkan waktu 2011-08-26 04:36:20.9071940 UTC seperti yang terlihat pada Gambar V.32 di bawah ini. Jika waktu tersebut disesuaikan dengan *time zone*-nya (pembagian wilayah dunia berdasarkan zona waktu) yang dalam hal ini adalah UTC+07:00 untuk Jakarta, maka didapat waktu

yang sesungguhnya yaitu 2011-08-26 11:36:20.9071940. Untuk mendapatkan kepastian mengenai *time zone* dari barang bukti komputer, *forensic analyst* dan *investigator* perlu untuk mendapatkan data tentang hal tersebut pada *registry keys* SYSTEM\ControlSet001\Control\TimeZoneInformation. Pada Gambar V.32 tersebut terlihat bahwa di samping *decoding*, aplikasi ini juga menyediakan fasilitas *encoding* (yaitu merubah waktu menjadi bilangan heksadesimal yang unik) yang disesuaikan dengan tipe *file system*-nya yaitu FAT dan NTFS (untuk Windows), Unix (Linux) dan HFS (Macintosh)



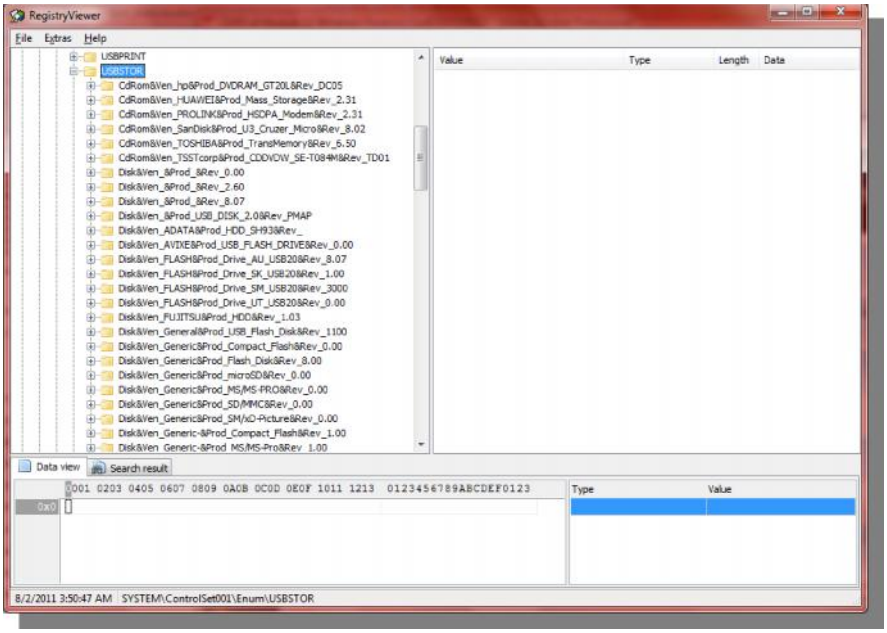
Gambar V.32. *The Time Lord* men-*decode* bilangan heksadesimal untuk mendapatkan waktu *last shutdown* yang berasal dari dari *registry keys* SYSTEM\ControlSet001\Control\Windows\ShutdownTime.

6. USB *disks*

Hal ini berkaitan dengan media penyimpanan yang bersifat *removable* (yang dapat dipindah-pindah) seperti *flashdisk*, *harddisk* eksternal, *memory card* dan lain-lain yang pernah terpasang pada barang bukti komputer. Historis USB *disks* ini penting bagi *forensic analyst* dan *investigator* untuk mendapatkan informasi media penyimpanan apa saja yang pernah terpasang dan diakses oleh komputer milik pelaku karena

sangat memungkinkan pelaku menyimpan *file-file* yang berisikan data kejahatannya di media *removable* tersebut, bukan di *harddisk* komputer. *Analyst* dan *investigator* dapat menanyakan dan meminta kepada pelaku tentang *removable disk* tersebut.

Informasi tentang USB *disks* ini tersimpan di *registry keys* SYSTEM\ControlSet001\Enum\USBSTOR seperti yang terlihat pada Gambar V.33 di bawah ini. Pada gambar tersebut, dapat dilihat berbagai jenis media penyimpanan *removable* yang pernah terpasang di *port* USB dan diakses oleh komputer barang bukti, misalnya *harddisk eksternal* merk ADATA dan FUJITSU, atau *flashdisk* merk Transcend JetFlash dan DataTraveler Kingston.



Gambar V.33. *Registry keys* SYSTEM\ControlSet001\Enum\USBSTOR menyimpan informasi mengenai *removable media* yang pernah terpasang di *port* USB dan diakses oleh komputer.

Informasi tentang *removable media* yang tersimpan di *registry keys* SYSTEM\ControlSet001\Enum\USBSTOR cukup lengkap, misalnya untuk *harddisk* eksternal ADATA yang pernah diakses oleh komputer melalui *port* USB didapat informasi sebagai berikut :

ClassGUID: {4d36e967-e325-11ce-bfc1-08002be10318}

ContainerID: {8ef4fd16-3abe-551f-b807-98d5d4aa9d6c}

FriendlyName: ADATA HDD SH93 USB Device

HardwareID: USBSTOR\DiskADATA___HDD_SH93_____

DiskId: {ba5e0b65-acf1-11e0-a4b4-9f313e56021f}

Data (*Properties*): 10 22 E1 B2 11 41 CC 01

Pada informasi Data yang berasal dari *registry keys* SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_ADATA&Prod_HDD_SH93&Rev_\SH0010226052&0\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\00000064\00000000 didapat nilai heksadesimal 10 22 E1 B2 11 41 CC 01. Bilangan heksadesimal ini kemudian di-*decode* dengan aplikasi *The Time Lord* untuk mendapatkan waktu kapan *harddisk* eksternal ADATA terpasang di *port* USB dan diakses oleh komputer barang bukti. Dengan aplikasi tersebut didapat waktu 2011-07-13 11:02:35.8250000.

Sedangkan ContainerID dan DiskId merupakan nomor identifikasi yang unik untuk membedakan antara media penyimpanan yang satu dengan yang lain, walaupun berasal dari merk dan model serta ukuran yang sama.

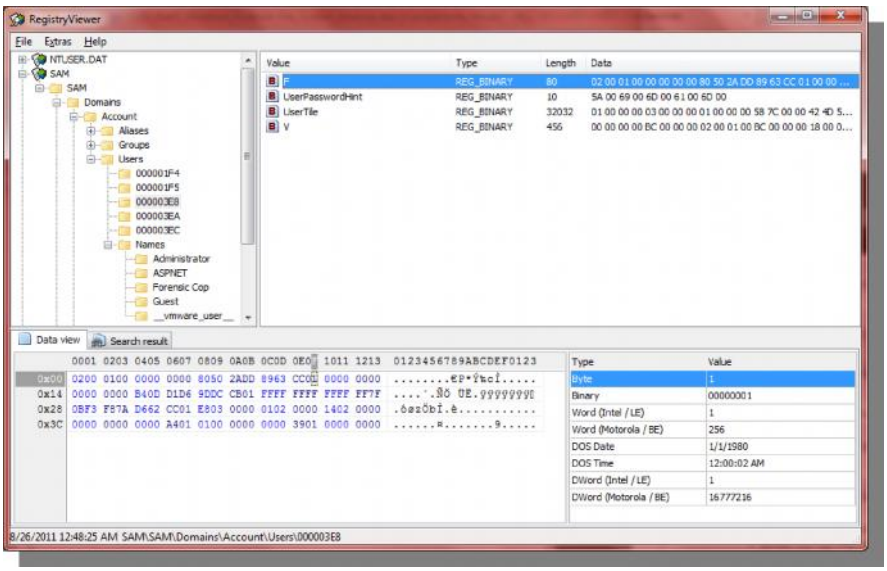
Data-data yang sama tentang USB *disks*, misalnya *harddisk* eksternal ADATA di atas juga dapat ditemukan di *registry keys* SYSTEM\ControlSet002\Enum\USBSTOR.

Di samping *registry keys* SYSTEM\ControlSet001\Enum\USBSTOR, juga terdapat *registry keys* SYSTEM\MountedDevices yang menyimpan *removable media* yang pernah di-*mounting* (dibuka dan diakses) oleh komputer.

7. *Users*

   Informasi mengenai seberapa banyak *user* yang memiliki account masing-masing di komputer barang bukti dapat diketahui pada *registry keys* SAM\SAM\Domains\Account\Users. Pada *registry keys* ini, *forensic analyst* dan *investigators* mendapatkan nama-nama *user* yang secara *default* adalah *Administrator*, ASPNET dan *Guest*. Di luar nama-nama tersebut, terdapat nama *user* yang sesungguhnya. Nama-nama *user* tersebut

berhubungan dengan data-data pada *registry keys* SAM\SAM\Domains\Account\Users\{RID} tersebut di mana pada data-data tersebut, salah satunya menyimpan informasi *password hint* yaitu petunjuk yang memiliki aosiasi dengan *password* dari *user*. Selain *password hint*, *registry keys* tersebut menyimpan informasi mengenai *last login* dari *user* yang terdapat pada *byte* 8 s/d 15, seperti pada gambar di bawah ini.



Gambar V.34. *Registry keys* SAM\SAM\Domains\Account\Users\{RID} menyimpan informasi yang berkaitan dengan *user*, misalnya *last login* yang terdapat pada *byte* 8 s/d 15 dalam bentuk bilangan heksadesimal.

Pada gambar tersebut, diketahui bilangan heksadesimal pada *byte* 8 s/d 15 adalah 80502ADD8963CC01. Dengan bantuan aplikasi *The Time Lord*, nilai heksadesimal ini dikonversi menjadi waktu 2011-08-26 07:48:25.9108992 yang menunjukkan *user* Forensic Cop terkahir kali masuk (*last login*) ke komputer tersebut.

8. *Setup log*

Pada beberapa kasus tertentu, *forensic analyst* dan *investigator* membutuhkan informasi waktu tentang kapan sistem operasi Windows di-*install* di komputer barang bukti milik pelaku. ini dibutuhkan untuk

mengetahui apakah *harddisk* pada komputer tersebut sudah di-*install* ulang sistem operasi Windows oleh pelaku dalam rangka menghilangkan jejak kejahatannya. Informasi ini dapat diketahui pada *registry keys* SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\ Setup Log Files. Pada *registry keys* didapat informasi FileList yang berisikan *file-file* yang memuat informasi tentang proses *setup* seperti setup*.log, setup*.old, setuplog.txt dan winnt32.log. Pada Windows 7, ada 2 *file* setupact.log masing-masing di C:\Windows dan C:\Windows\Panther yang berisikan historis dari proses instalasi sistem operasi Windows 7 secara lengkap. Kedua *file log* ini dapat digunakan oleh *forensic analyst* dan *investigator* untuk mendapatkan waktu instalasi Windows 7 secara tepat.

Bibliography

1. ACPO, 7Safe (2008). *Good Practice Guide for Computer-Based Electronic Evidence*. UK ACPO and 7Safe.
2. Al-Azhar, M.N. (2010). *Standard Operating Procedure (SOP) 1 : Prosedur Pemeriksaan Digital Forensik*. DFAT Puslabfor.
3. Carrier, B. (2002). *Open Source Digital Forensic Tools: The Legal Argument.* @stake.
4. Carrier, B. (2007). *File System Forensic Analysis*. Addison-Wesley.
5. Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Elsevier Academic Press.
6. Cox, I. J. et al. (2008). *Digital Watermarking and Steganography*. Morgan Kaufmann
7. Davies, P. (2009). *Forensic Analysis of the Windows Registry*. University of Glamorgan.
8. Deden, K. (2007). *Mengenal Teknologi Harddisk*. Dapat diakses di http://dedenthea.wordpress.com/2007/08/14/mengenal-teknologi-hard-disk/.
9. Dolan-Gavitt. (2008). *Forensic Analysis of the Windows registry in memory*. Elsevier-Digital Investigation.

10. EC-Council. (2010). *Module XII – Windows Forensics I*. EC-Council.
11. Johnson, T. A. (2005). *Forensic Computer Crime Investigation*. Taylor & Francis.
12. Konheim, A. G. (2007). *Computer Security and Cryptography*. Wiley
13. Middleton, B. (2002). *Cyber Crime Field Handbook*. CRC Press
14. National Institute of Justice (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. US National Institute of Justice
15. National Institute of Justice (2001). *Electronic Crime Scene Investigation: A Guide for First Responder*. US National Institute of Justice.
16. Sammes, T. and Jenkinson, B. (2007). *Forensic Computing: A Practitioner's Guide*. Springer.
17. StatCounter. (2011). *Top 5 Operating Systems*. Dapat diakses di http://gs.statcounter.com/#os-ww-monthly-201007-201107.
18. W3schools. (2011). *OS Platform Statistics*. Dapat diakses di http://www.w3schools.com/browsers/browsers_os.asp.

Bab VI

FILES RECOVERY

Ketika *forensic analyst* dan/atau *investigator* melakukan investigasi barang bukti elektronik seperti komputer dan *handphone* dari suatu kasus *computer crime* atau *computer-related crime*, seringkali mereka diminta untuk mencari dan menemukan kembali *file-file* yang berisi informasi yang penting bagi pengembangan investigasi kasus tersebut. Dengan adanya *file* tersebut yang berhasil ditemukan dan diangkat dari *harddisk* komputer barang bukti, maka *investigator* dapat mengembangkan investigasinya dengan baik serta dapat membuktikan adanya keterlibatan pelaku dalam kejahatan tersebut. *File-file* yang dicari sesuai dengan maksud investigasi dan dicoba untuk diangkat kembali dikenal dengan istilah *files recovery*.

Files recovery ini memegang peranan penting di dalam digital forensik karena hal inilah yang sering menjadi dasar dari permintaan investigasi kepada *forensic analyst* dan *investigator*. Hampir setiap kasus digital forensik yang dimintakan kepada *forensic analyst* berkaitan dengan *files recovery*, misalnya permintaan kepada *forensic analyst* untuk mengangkat kembali sms (*short message service*) yang sudah dihapus dari sebuah barang bukti *handphone* dan *simcard*. *Recovery* terhadap sms-sms tersebut penting untuk dilakukan karena sms-sms tersebut dapat membuktikan adanya komunikasi dan niat jahat di antara pelaku kejahatan yang berkomunikasi lewat *handphone*. Hal ini biasa terjadi pada kasus narkotika dan obat-obatan terlarang. Contoh lain adalah seorang pelaku yang melakukan re-*format* (membuat *file system* yang baru) terhadap *harddisk* komputernya kemudian ia melakukan proses instalasi sistem operasi Windows yang baru. Hal itu dilakukan dalam rangka untuk menghilangkan jejak kejahatannya. *Forensic analyst* dan *investigator* sering diminta untuk melakukan *files recovery* terhadap *harddisk* tersebut. Mereka diminta untuk mencari *file-file* yang sebelumnya sudah ada di *harddisk* tersebut yang kemudian hilang (*lost*) dan tidak tercatat lagi di *file system* yang baru dikarenakan adanya proses re-*formatting* dan instalasi tersebut. Namun adakalanya *files recovery* ini tidak berkaitan dengan kasus sama sekali, misalnya upaya penyelamatan data. Adakalanya seorang *user* (pengguna) melakukan kecerobohan dan secara tidak

sengaja ia melakukan proses re-*formatting* terhadap salah satu partisi *harddisk*-nya atau *removable media* seperti *flashdisk* dan *memory card*. *Forensic analyst* dan *investigator* kemudian diminta untuk melakukan langkah-langkah penyelamatan data terhadap *file-file* yang sebelumnya tersimpan di media penyimpanan tersebut. Atau bisa juga upaya penyelamatan data terhadap *file-file* yang sudah terhapus oleh aplikasi anti virus yang menganggap *file-file* tersebut sudah terinfeksi *malware* (*malicious software*, yaitu suatu program kecil yang jahat dan dikembangkan untuk mengganggu suatu sistem komputasi, misalnya virus, *worm*, *trojan* dan *rootkit*).

Dari penjelasan di atas dapat diketahui bahwa *files recovery* ini memegang peranan penting, baik di dalam upaya pengembangan investigasi suatu kasus *computer crime* dan/atau *computer-related crime*, maupun pada upaya penyelamatan data terhadap isi dari suatu media penyimpanan seperti *harddisk*, *flashdisk* dan *memory card* yang hilang secara tidak sengaja atau sengaja.

Dikarenakan pentingnya *files recovery* ini, maka penulis memutuskan untuk membahas masalah ini pada satu bab tersendiri. Pada Bab VI ini, pembahasan *files recovery* akan dibagi berdasarkan pada tipe *file* yang akan dicari dan diangkat. *File-file* tersebut terdiri dari *logical*, *deleted* dan *lost* yang pembahasannya secara detil dapat dilihat pada poin-poin berikut di bawah ini.

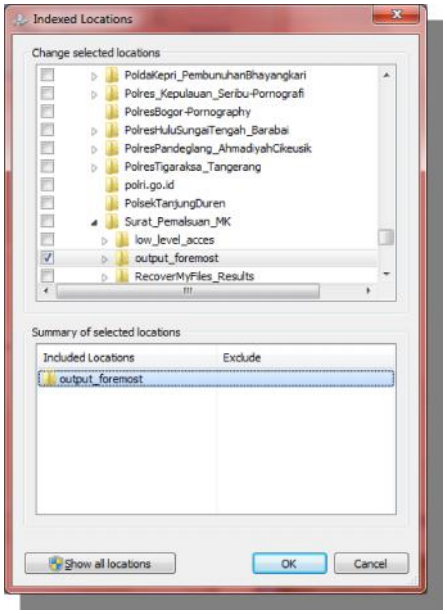
Logical files recovery

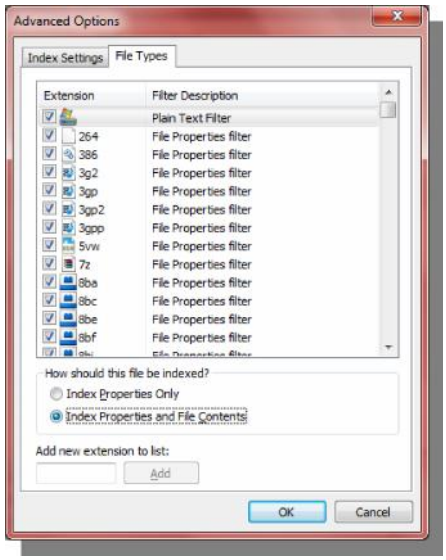
Pada Bab II tentang *Digital Forensic Principles and Procedures*, dijelaskan bahwa *logical file* adalah *file-file* yang masih ada dan tercatat di *file system* yang sedang berjalan (runn*i*ng) di suatu partisi dari media penyimpanan seperti *harddisk*, *flashdisk* dan *memory card*. Artinya *file-file* tersebut di manapun posisi *cluster* dan sektor untuk penyimpanannya masih tercatat dengan baik di *file system*-nya. Misalnya pada *file system* FAT, *root directory* akan menyimpan setiap *file* yang dibuat pada *cluster-cluster* yang sudah dialokasikan untuk itu. Begitu juga pada *file system* NTFS, $MFT (*Master File Table*) akan menyimpan seluruh *file* yang dibuat dalam satu *entry* masing-masing yang lengkap dengan pengalamatan *cluster-cluster*-nya. *File-file logical* tersebut bisa berupa *file-file* aplikasi (yang memiliki ekstensi *.exe), *library* (*.dll), *office* (dapat berupa dokumen *.doc/docx,

presentasi *.ppt/pptx, *spreadsheet* *.xls/xlsx) logs (*.log/txt), multi media (audio *.mp3/amr, video *.mp4/avi/mpeg, gambar *.jpg/bmp/png) dan lain-lain.

Berdasarkan penjelasan di atas, sebenarnya pencarian terhadap *logical files* bukanlah satu hal yang kompleks karena semua *file* berikut *cluster-cluster* penyimpanannya sudah tercatat di *file system*-nya. Untuk memudahkan pencarian terhadap *file* yang diinginkan, maka *logical files recovery* dibagi menjadi 3, yaitu berdasarkan nama *file*, ekstensi dan isi-nya.

Dalam sistem operasi Windows 7, *forensic analyst* dan *investigator* dapat memanfaatkan aplikasi Windows Explorer untuk melakukan pencarian *file-file* yang diinginkan berdasarkan nama dan ekstensi *file*. Aplikasi tersebut menggunakan metode *indexing* (pengelompokkan yang didasarkan pada *properties*, tipe ekstensi dan isi *file*) sebelumnya sehingga dapat memberikan hasil pencarian yang lebih cepat. Proses *indexing* ini dapat diubah (*customized*) oleh *user* sesuai dengan keinginannya, misalnya lokasi *indexing* bisa dipilih, misalnya pada partisi atau *folder* tertentu. Untuk itu *forensic analyst* dan *investigator* sebaiknya sudah melakukan proses *mounting* (membuka dan mengakses) secara *read-only* terlebih dahulu terhadap *image file* yang sudah didapat dari proses *forensic imaging* terhadap *harddisk* dari barang bukti komputer sebelumnya. Untuk tujuan ini, ada beberapa aplikasi forensik yang berbasis Windows yang dapat digunakan, misalnya WinHex, EnCase, FTK (*Forensic Toolkit*) *Imager* dan *Mount Image Pro*. Setelah di-*mounting* dengan menggunakan aplikasi tadi secara *read-only*, maka *forensic analyst* dan *investigator* dapat mengubah lokasi *indexing* ke *drive* atau partisi maupun *folder* dari *image file* yang di-*mounting* tersebut yang mungkin terdapat *file-file logical* yang akan dicari. Setelah itu *forensic analyst* dan *investigator* juga dapat merubah proses *indexing* berdasarkan tipe ekstensi *file* dan isinya. Ini dimaksudkan agar pencarian juga dapat menjangkau isi dari *file-file* tersebut, tidak hanya tipe ekstensi dan nama *file*. Setelah semuanya disesuaikan, barulah proses pencarian terhadap *file-file logical* dimulai dan diharapkan berjalan dengan cepat walaupun *file-file* yang akan dicari jumlah totalnya ribuan atau lebih.

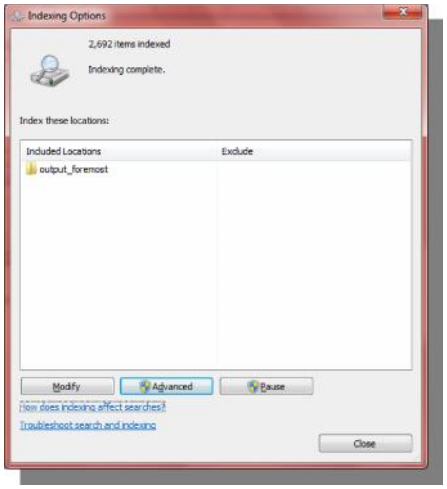




(1) (2)

Gambar VI.1. Lokasi *indexing* (bisa partisi atau *folder* tertentu) yang dapat diubah sesuai dengan keinginan *user* (1), dan perubahan *indexing* berdasarkan tipe ekstensi dan isi *file* (2).

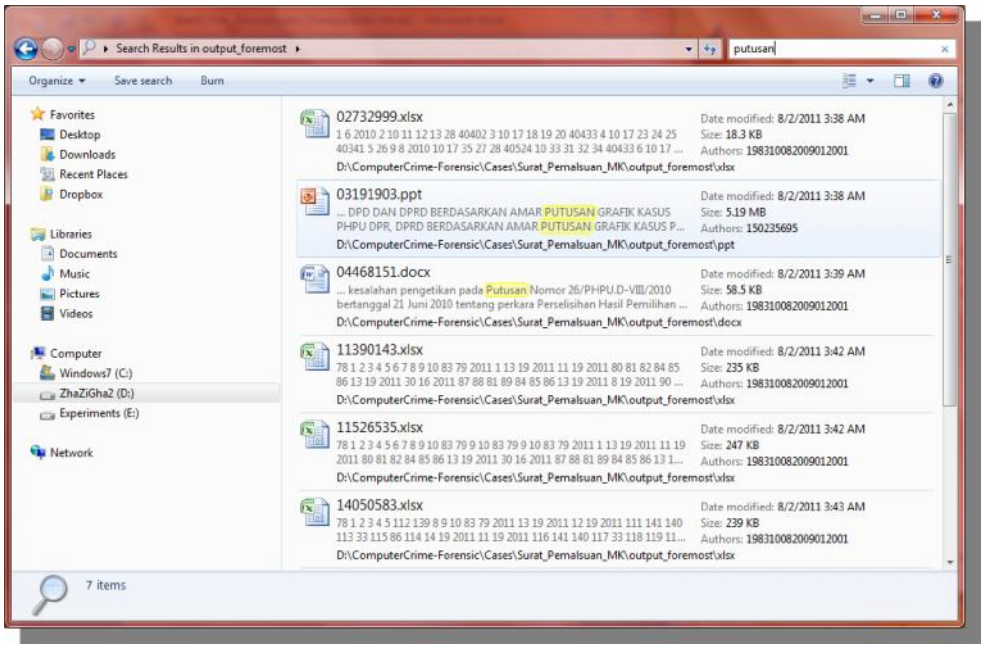
Setelah semua perubahan atau penyesuaian tersebut telah dilakukan, maka proses *indexing* dapat berjalan sesuai dengan keinginan *forensic analyst* dan *investigator* seperti pada gambar di bawah ini.



Gambar VI.2. Proses *indexing* selesai terhadap lokasi yang dinginkan.

Seperti telah dijelaskan di atas, selesainya proses *indexing* yang telah disesuaikan dengan keingingan *user* yang dalam hal ini *forensic analyst* dan *investigator*, maka

proses pencarian terhadap *file-file* yang memiliki informasi yang penting yang sesuai dengan maksud investigasi pada isinya dapat dilakukan dengan cepat terhadap kumpulan *file-file* (mungkin berjumlah ribuan lebih *file*) yang ada pada partisi atau *folder* tertentu dari *image file* yang identik dengan *harddisk* barang bukti. Dengan memasukkan *keywords*, yaitu kata kunci tertentu yang berkaitan dengan investigasi, maka aplikasi *Windows Explorer* akan memberikan hasil pencarian dengan cepat berupa *file-file* yang memiliki isi di mana kata-katanya sama dengan *keywords* yang diberikan. Artinya *forensic analyst* dan *investigator* dapat menghemat waktu yang sangat banyak (dalam jam atau hari) dan tidak perlu untuk melakukan pencarian secara manual dengan cara membuka satu per satu *file-file* tersebut untuk mengecek isinya. *Analyst* dan *investigator* tinggal membuka *file-file* hasil pencarian tersebut untuk mengecek isinya apakah sesuai dengan yang diinginkan dalam investigasi kasus. Hal ini dapat dilihat pada gambar di bawah ini.

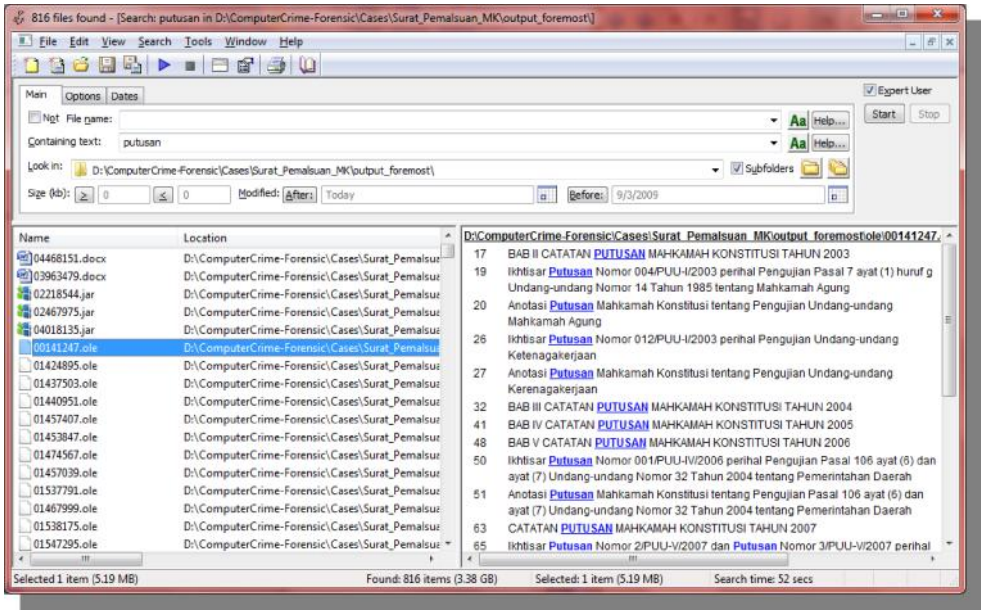


Gambar VI.3. Hasil pencarian yang tersaji dengan cepat berkat bantuan proses *indexing* sebelumnya terhadap lokasi partisi atau *folder* tertentu.

Di samping memanfaatkan proses *indexing* yang sudah tersedia di sistem operasi Windows 7, *forensic analyst* dan *investigator* juga dapat menggunakan aplikasi-aplikasi forensik pihak ketiga yang lain. Salah satunya yang sering digunakan

adalah aplikasi *Agent Ransack* dari Mythicsoft yang sempat disinggung di Bab IV tentang *Triage Forensic: First Response Procedure*. Dengan aplikasi ini, *forensic analyst* dan *investigator* dapat lebih cepat dan mudah untuk menemukan *file-file* yang memiliki informasi yang penting pada isinya dari sekian banyak (ribuan lebih) *file*. Di samping membaca isi *file* secara langsung, aplikasi ini bahkan dapat membaca *file-file* yang di-*searching* dalam bahasa *Unicode* maupun heksadesimal. Oleh karena itu aplikasi ini memberikan hasil yang lebih detil dan tajam dibandingkan dengan proses *indexing* dari Windows yang telah dijelaskan sebelumnya.

Misalnya penulis melakukan proses *searching* (pencarian) terhadap satu *folder* tertentu yang berisikan 2.675 *file* dengan ukuran total 3,89GB. Untuk keyword yang sama, dengan proses *indexing* dari Windows, penulis hanya mendapatkan 7 *files*, sedangkan dengan aplikasi *Agent Ransack* penulis bisa mendapatkan 816 *files*. Terdapat perbedaan jumlah yang sangat signifikan di antara kedua metode ini.

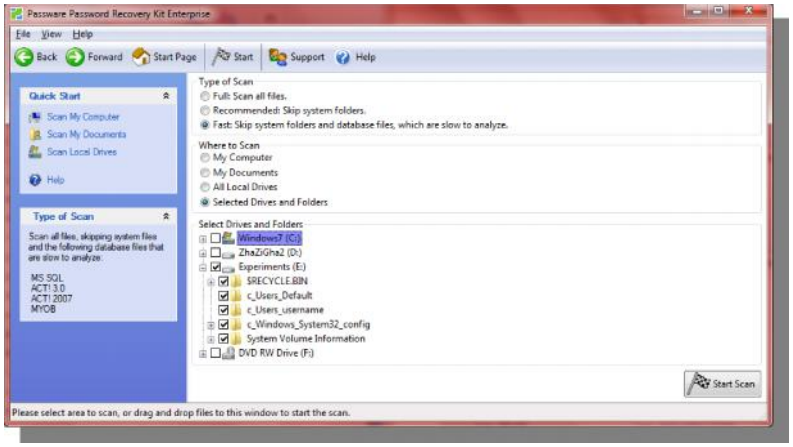


Gambar VI.4. Aplikasi *Agent Ransack* dari Mythicsoft yang dapat digunakan untuk melakukan pencarian *file-file logical* secara cepat dan mudah untuk mengeceknya satu per satu *file-file* hasil pencarian tanpa perlu membuka *file-file* tersebut.

Pada *Agent Ransack*, *file-file logical* hasil pencarian (khususnya *file-file* dokumen, misalnya *.doc/docx/txt) dapat langsung dilihat isinya tanpa perlu membuka *file-file* tersebut. Hal ini sangat menghemat waktu bagi *analyst* dan *investigator* untuk mendapatkan *file* yang diinginkan, seperti yang terlihat pada gambar di atas.

Aplikasi ini juga menyediakan *option* (pilihan) pencarian yang didasarkan pada *time stamps* dari *file-file* tersebut. Pencarian yang dilakukan dapat di-*filter* melalui tanggal/waktu yang diinginkan pada *created date*, *modified date* maupun *accessed date*. Tanggal/waktu dari *time stamps* tersebut dapat dipilih berdasarkan rentang waktu sebelum, sesudah atau kombinasi keduanya. Ini memudahkan *forensic analyst* dan *investigator* untuk lebih cepat mencari *file-file* logical yang diinginkan dengan didasarkan pada waktu *time stamps* yang sudah diketahui pada proses investigasi sebelumnya.

Di samping aplikasi di atas, juga terdapat aplikasi yang dapat digunakan untuk mencari *file-file logical office* (yaitu Microsoft Office) yang terproteksi dengan *password* dan terenkripsi (misalnya menggunakan algoritma enkripsi RSA dan AES 128 *bit*) sehingga *file-file* tersebut tidak dapat dibuka untuk dibaca isinya kecuali yang sudah mengetahui *password*-nya untuk mendekripsi file tersebut. Salah satu aplikasi yang dapat digunakan untuk tujuan ini adalah *Password recovery Kit* dari Passware. Dengan aplikasi ini, *forensic analyst* dan *investigator* dapat lebih mudah mencari *file office* yang mana yang terpoteksi dengan *password* dan terenkripsi dari sekian banyak *file-file logical office* yang ada di *harddisk* barang bukti. *File-file office* yang terproteksi tersebut biasanya menyimpan informasi yang penting dari yang membuat *file* tersebut yang mungkin berkaitan dengan kejahatan yang dilakukan oleh pelaku, oleh karena itu penting bagi *analyst* dan *investigator* untuk mendapatkan *file-file logical* terproteksi tersebut. Pencarian *file-file logical* terproteksi tersebut dapat dirubah atau difilter oleh *analyst* dan *investigator* sesuai dengan partisi atau *folder-folder* tertentu yang mungkin berisikan *file-file* tersebut, seperti terlihat pada gambar di bawah ini.



Gambar VI.5. Aplikasi *Password Recovery Kit* dari Passware menyediakan pilihan lokasi untuk melakukan pencarian terhadap *file-file logical office* yang terproteksi *password* dan terenkripsi.

Setelah *file-file* terproteksi tersebut ditemukan dari hasil *searching* sebelumnya, selanjutnya aplikasi ini juga menyediakan *tools* untuk melakukan *recovery* terhadap *password* yang memproteksi *file-file* tersebut. Metode (*attack*) yang digunakan untuk *password recovery* tersebut adalah biasa atau sama yang digunakan juga oleh aplikasi-aplikasi pihak lain yang sejenis, misalnya dicti*onary attack* (didasarkan pada kata-kata *password* yang mungkin dan sering digunakan) dan *brute-force attack* (didasarkan pada kombinasi huruf besar, huruf kecil, angka dan karakter lain berikut panjang karakternya). Untuk kepentingan *password recovery* ini, sebaiknya *forensic analyst* dan *investigator* dapat menggunakan aplikasi-aplikasi lain yang sejenis dikarenakan masing-masing aplikasi memiliki kelebihan dan kekurangan masing-masing dalam proses tersebut. Di samping itu, kecepatan *password recovery* (dalam hitungan jumlah *password* per detik) pada masing-masing aplikasi biasanya berbeda, meskipun menggunakan *analysis workstation* yang sama. *Hardware* juga ikut berpengaruh terhadap proses ini, khususnya *microprocessor*. Semakin canggih teknologi *microcporcessor* yang digunakan, misalnya i3, i5 dan i7 dari Intel maka akan semakin cepat proses tersebut. *Microprocessor* yang terdiri dari beberapa *core* memberikan kecepatan komputasi pada level yang tinggi.

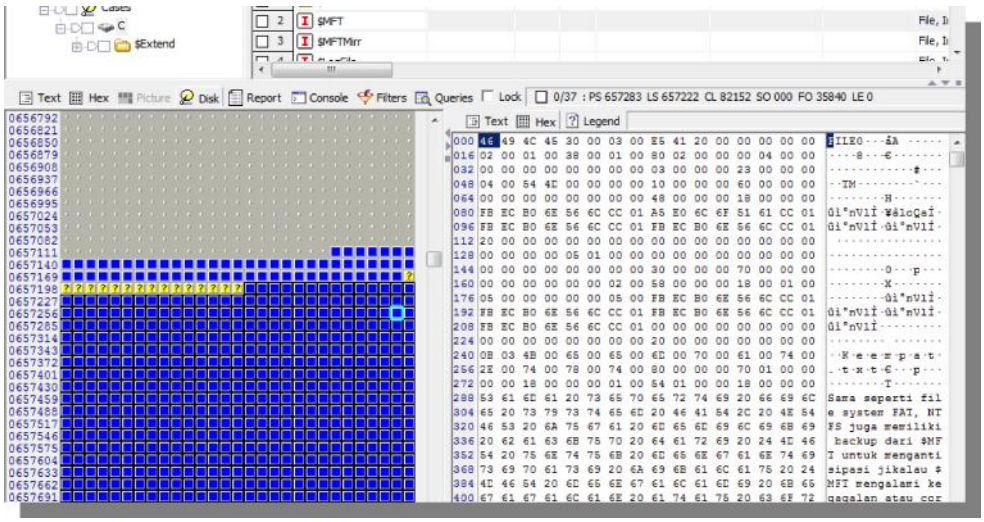
Deleted files recovery

Sempat disinggung pada Bab II tentang *Digital Forensic Principles and Procedures* dan Bab V tentang *Windows Forensic: File System Analysis* sebelumnya bahwa *deleted files* adalah *file-file* yang sudah terhapus namun masih tercatat di *file system*-nya yang dalam hal ini adalah *root directory* dari sistem FAT atau $MFT pada sistem NTFS. Dikarenakan sudah terhapus, maka *cluster-cluster* yang ditempati oleh *deleted files* tersebut ditandai sebagai *unallocated cluster* yang merujuk kepada *cluster* yang sudah tidak teralokasikan lagi untuk *file-file* tersebut dan kemudian dapat digunakan lagi untuk penyimpanan *file-file* yang baru. Artinya *file* yang sudah terhapus tersebut masih tetap berada di *cluster* atau sektor tempat penyimpanannya sampai tertimpa (*overwritten*) oleh *file-file* yang baru pada *cluster* atau sektor tersebut. Pada kondisi di mana *deleted file* tersebut belum tertimpa, maka proses *recovery* secara utuh terhadap *file* tersebut sangat memungkinkan terjadi. Adapun jika *cluster* dan sektor dari *deleted file* tersebut tertimpa sebagian oleh *file* yang baru, maka sisa sektor dari *deleted file* tersebut dikenal dengan istilah *file slack*. *File slack* ini merupakan area di antara *end of sector* (eos) hingga *end of cluster* (eoc). *File slack* ini dibahas juga pada Bab V. Silahkan ke Bab V untuk melihat dan mengetahui historis dari *file slack* ini.

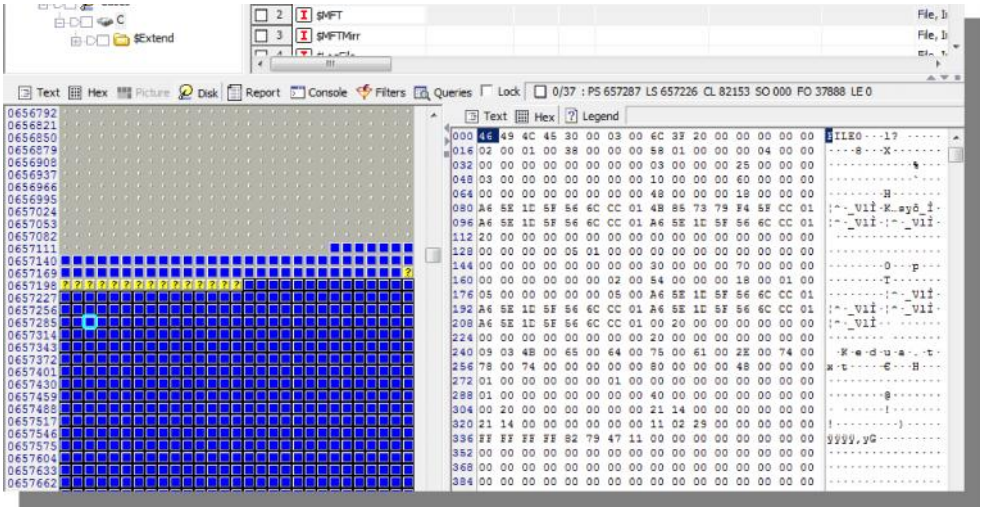
Dikarenakan *deleted files* ini masih tercatat pada *file system*-nya maka proses *recovery* terhadap *deleted files* ini tidak begitu kompleks. Artinya *forensic analyst* dan *investigator* tinggal menganalisa *root directory* dari *file system* FAT 12/16 dan FAT32, atau $MFT dari file system NTFS. Analisa terhadap *root directory* dan $MFT ini juga sudah dibahas pada Bab V sebelumnya. Sebagai contoh pada Gambar V.17 di Bab V, gambar tersebut menampilkan struktur *directory entry* yang berhasil di-*recovery* pada area *root directory* dari *file system* FAT 32. Dari gambar tersebut dapat diketahui bahwa *file* Kedua.txt yang sudah dihapus (*deleted*) yang ditandai dengan penamaan _KEDUA.TXT berada pada *cluster* 4. Pada *cluster* yang sama juga terdapat *file* KETIGA.TXT. *Forensic analyst* dan *investigator* kemudian mengecek *cluster* 4 yang dimaksud untuk melihat seberapa jauh *file* KEDUA.TXT yang sudah dihapus tertimpa (*deleted and overwritten*) oleh file KETIGA.TXT. Nantinya *analyst* dan *investigator* akan dapat menemukan sebagian isi dari *file* KEDUA.TXT yang belum tertimpa (yang dikenal dengan istilah

file slack). Jikalau *cluster* dari deleted file tersebut belum tertimpa oleh *file* baru, maka *analyst* dan *ivestigator* juga akan dapat menemukan *deleted file* tersebut secara utuh pada *cluster*-nya.

Prinsip yang hampir sama juga berlaku pada *file system* NTFS. Perbedaannya adalah pada NTFS, MFT *entry* dari *file* yang dihapus (*deleted*) akan tetap berada pada $MFT sampai MFT *entry* tersebut ditimpa oleh MFT *entry* dari fi*l*e baru. Untuk MFT *entry* dari *deleted file* yang sudah tertimpa tersebut, isi dari *deleted file* tersebut masih tetap berada di *cluster* penyimpanannya, walaupun MFT *entry*-nya sudah tidak tercatat lagi di $MFT, oleh karena itu *recovery* terhadap *deleted file* tersebut dianggap sebagai proses *recovery* untuk *lost* file yang didasarkan pada *signature* dari *file*. Sementara itu, untuk MFT *entry* dari *deleted file* yang masih tetap di $MFT akan menunjukkan bahwa *deleted file* tersebut bisa dilakukan *recovery* secara penuh.

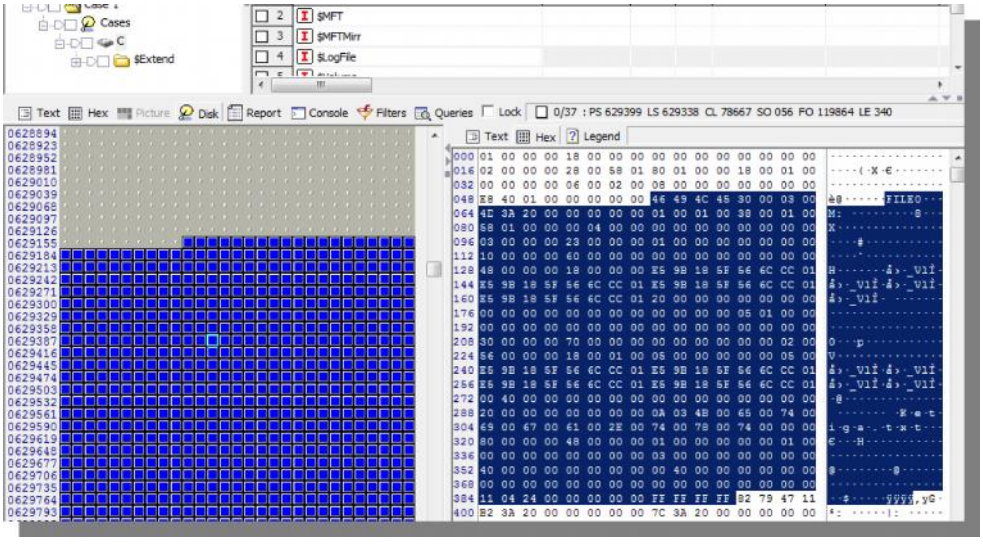


Gambar VI.6. Pada $MFT, MFT *entry* dari *file* Ketiga.txt yang sudah terhapus (*deleted*) ditimpa oleh MFT *entry* dari *file* Keempat.txt yang baru di tempat yang sama.



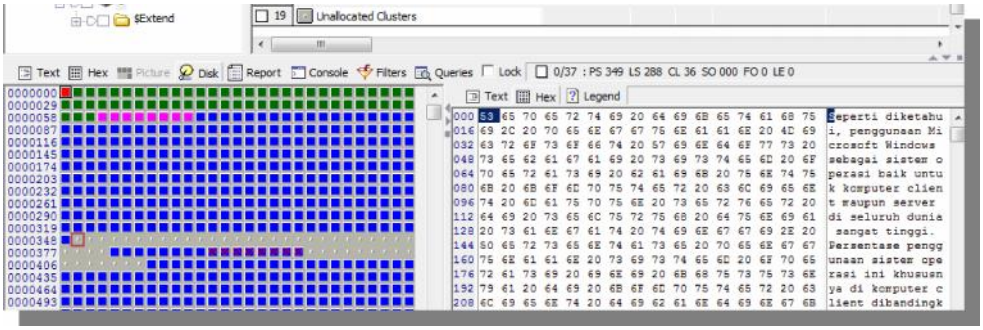
Gambar VI.7. MFT *entry* dari deleted *file* Kedua.txt masih tetap berada pada $MFT dan belum tertimpa oleh MFT *entry* dari *file* baru.

Pada kedua gambar di atas, diketahui bahwa pada *file system* NTFS, ketika satu *file* dihapus, maka MFT *entry* untuk *file* tersebut masih berada pada $MFT (Gambar VI.7), namun MFT *entry* dari *deleted file* tersebut dapat tertimpa oleh MFT *entry* dari *file* baru (Gambar VI.6) sehingga tidak tercatat lagi di $MFT. Meskipun begitu, *deleted file* yang MFT *entry*-nya sudah tertimpa masih bisa dilacak keberadaannya pada *file* metadata $LogFile yang dalam kasus ini yaitu pada *cluster* 78667, seperti terlihat pada gambar di bawah ini.



Gambar VI.8. MFT *entry* dari *deleted file* Ketiga.txt masih bisa terlacak keberadaannya di *file* metadata $LogFile yang dalam kasus ini yaitu di *cluster* 78667.

Pada gambar tersebut di atas, MFT *entry* dari *deleted file* Ketiga.txt dimulai dari *signature* '*FILE*' pada *byte* 56. Selisih 330 *bytes* dari *byte* 56, yaitu pada *byte* 386 ditemukan nilai heksadesimal 0x24 yang bernilai *integer* 36. Nilai 36 ini menunjukkan posisi *cluster* awal (*starting cluster*) di mana isi dari *deleted file* Ketiga.txt disimpan. Sementara itu 1 *byte* di depannya, yaitu *byte* 385 memiliki nilai heksadesimal 0x04 yang bernilai integer 4. Nilai 4 ini menunjukkan panjang *cluster* (*length*) yang digunakan untuk menyimpan *deleted file* ketiga.txt. artinya *deleted file* Ketiga.txt memiliki cluster penyimpanan mulai 36 s/d 39.



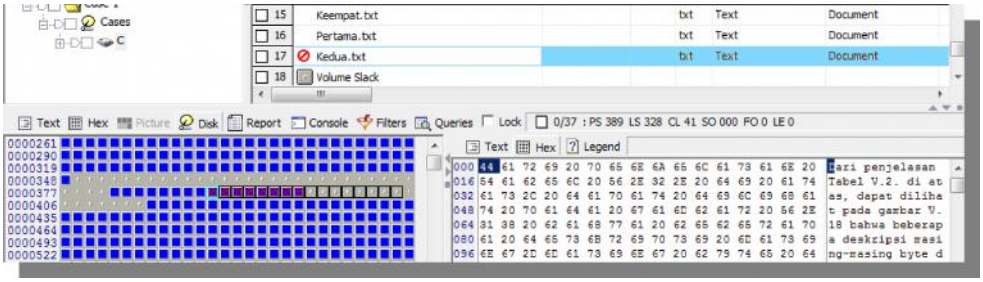
Gambar VI.9. *Cluster* 36 s/d 39 merupakan tempat penyimpanan dari *deleted file* Ketiga.txt.

Dari gambar di atas, diketahui *cluster* 36 s/d 39 menyimpan isi dari file Ketiga.txt yang sudah terhapus (*deleted*), oleh karena itu *forensic analyst* dan *investigator* dapat melakukan *recovery deleted file* Ketiga.txt pada *cluster-cluster* tersebut. Pada gambar tersebut juga diketahui bahwa *cluster-cluster* tersebut termasuk dalam *unallocated clusters*, yaitu *cluster-cluster* yang tidak teralokasi untuk penyimpanan *file-file*.

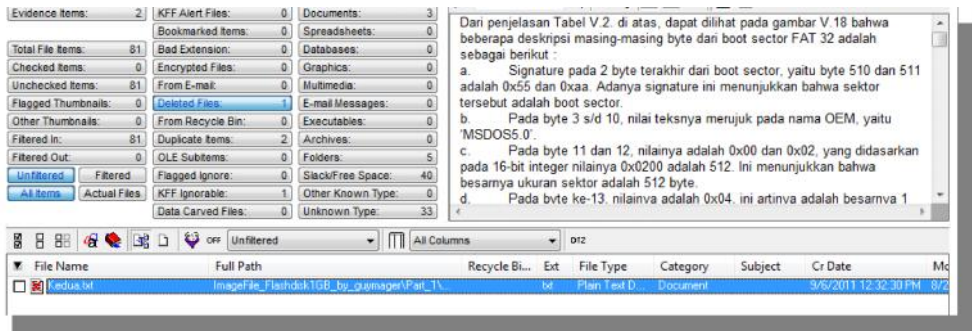
Dari penjelasan di atas, diketahui bahwa untuk *deleted file* yang MFT *entry*-nya sudah tertimpa oleh MFT *entry* dari file baru, maka isi dari *deleted file* tersebut sebenarnya masih ada di *cluster-cluster* penyimpanannya. Meskipun begitu, *deleted file* tersebut sudah tidak tercatat lagi di $MFT sehingga ia dianggap sebagai *lost file*. Untuk kasus seperti ini, *recovery* terhadap *file* tersebut bisa menggunakan metode seperti yang telah dijelaskan di atas yaitu melacak keberadaan *file* tersebut di file metadata $LogFile, selain menggunakan metode

lost file recovery yang didasarkan pada *file signature*, atau menggunakan metode *low level recovery* yang didasarkan pada *keywords*.

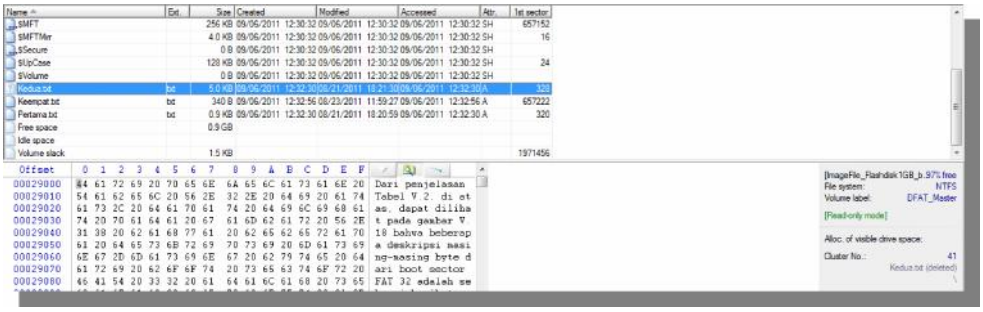
Berdasarkan prinsip dan penjelasan di atas, banyak aplikasi-aplikasi yang dikembangkan untuk tujuan *deleted files recovery*. Aplikasi-aplikasi ini tinggal membaca *root directory* (untuk *file system* FAT) dan/atau $MFT (untuk NTFS) untuk mencari *file-file* yang sudah dihapus (*deleted*), dan kemudian menuju *cluster* tempat penyimpanan *file-file* tersebut guna dilakukan proses pengangkatan kembali (*recovery*). Beberapa aplikasi forensik berbasis Windows yang dapat juga digunakan untuk tujuan *deleted files reocvery* ini adalah EnCase (Gambar V.10), FTK (Gambar VI.11), WinHex (Gambar VI.12) dan Recover My Files (Gambar VI.13). Melalui aplikasi-aplikasi ini, *forensic analyst* dan *investigator* tinggal memasukkan image file yang berasal dari proses *forensic imaging harddisk* barang bukti, kemudian jalankan proses *recovery* untuk mendapatkan hasilnya.



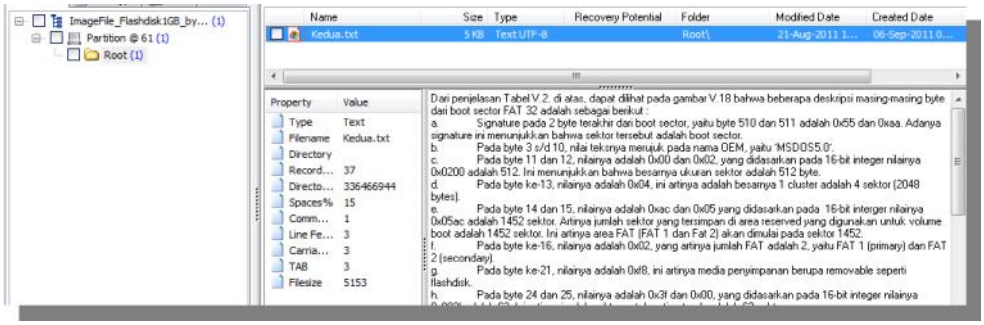
Gambar VI.10. *Recovery* terhadap *deleted file* Kedua.txt dengan menggunakan aplikasi EnCase dari Guidance Software.



Gambar VI.11. *Recovery* terhadap *deleted file* Kedua.txt dengan menggunakan aplikasi FTK dari AccessData.



Gambar VI.12. *Recovery* terhadap *deleted file* Kedua.txt dengan menggunakan aplikasi WinHex dari X-Ways.



Gambar VI.13. *Recovery* terhadap *deleted file* Kedua.txt dengan menggunakan aplikasi *Recover My Files* dari GetData.

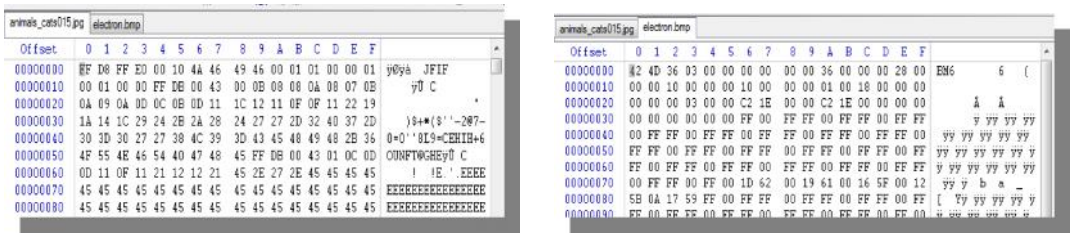
Lost files recovery

Pada Bab II tentang *Digital Forensic Principles and Procedures* dijelaskan bahwa *lost file* merupakan *file* yang sudah tidak tercatat lagi di *file system* yang sedang berjalan (*running*) dari suatu partisi media penyimpanan seperti *harddisk*, *flashdisk* dan *memory card*, namun *file* tersebut masih ada di *cluster* dan sektor sektor penyimpanannya. Ini bisa terjadi ketika misalnya suatu *flashdisk* atau *harddisk* maupun partisinya dilakukan proses re-*format* yang menghapus *file system* yang lama dan menghasilkan *file system* yang baru, sehingga *file-file* yang sudah ada pada *file system* sebelumnya menjadi tidak tercatat lagi di *file system* yang baru. *File-file* tersebut dikenal dengan istilah *lost files*.

Dikarenakan *lost files* sudah tidak tercatat pada *root directory* dari *file system* FAT atau pada *file* metadata $MFT dari *file system* NTFS, maka proses *recovery* terhadap tipe *file* ini tidak bisa disandarkan pada *file system* yang sedang berjalan tersebut. *File system* yang sedang berjalan tersebut tidak memiliki catatan apapun

tentang *lost files* tersebut. Meskipun *lost files* masih tetap berada di *cluster* dan sektor penyimpanannya, pengalamatan untuk *cluster* dan sektor yang berkaitan dengan isi dari *lost files* tersebut tidak tercatat di *file system* yang sedang berjalan. Saat ini solusi yang paling memungkinkan adalah melakukan proses *recovery*-nya dengan didasarkan pada *signature* dari *header* maupun *footer* yang tergantung pada jenis format *lost file* tersebut.

File signature adalah beberapa *byte* pertama (dari *header*) atau terakhir (*footer*) dari suatu format/ekstensi *file*. *Byte-byte* ini sifatnya unik dan selalu konsisten nilainya sama sesuai dengan tipe ekstensi *file*-nya. Jika ekstensi *file* yang satu berbeda dengan yang lain, maka nilai *byte-byte* tersebut juga akan berbeda. Misalnya *file* gambar *.jpg dan *.bmp. Meskipun keduanya merupakan *file* gambar, namun memiliki ekstensi yang berbeda, dan ini dapat juga dipastikan lewat *signature*-nya masing-masing. *Signature* ini biasa dinyatakan dalam bilangan heksadesimal.



(1) (2)

Gambar VI.14. *Signature* 0xff d8 ff untuk *file* *.jpg (1), dan signature 0x42 4d untuk *file* *.bmp (2).

File *.jpg memiliki signature pada beberapa *byte* awal, secara umum yaitu 0xff d8 ff (seperti pada Gambar VI.14.1), sedangkan *file* *.bmp memiliki *signature* 0x42 4d (Gambar VI.14.2). Untuk *file* *.jpg, secara khusus *signature*-nya akan dibahas lebih detil pada tabel di bawah ini. Oleh karena masing-masing ekstensi/format *file* memiliki *signature* yang berbeda-beda antara yang satu dengan yang lain, maka *file signature* ini juga dikenal dengan istilah *magic numbers*.

Berikut adalah tabel yang memuat nilai *signature* untuk beberapa ekstensi *file* yang sering digunakan dalam pencarian yang dilakukan oleh *forensic analyst* dan *investigator*. Tabel ini sebagian mengacu pada *File Signature Table* yang

dikembangkan oleh Gary Kessler dan dapat diakses di http://www.garykessler.net/library/file_sigs.html.

Tipe Ekstensi *File*	*Signature*
***File-file* Gambar Digital**	
*.bmp (*Bitmap Image*)	0x42 4d
*.jpg (*File* grafik JPEG/JFIF) *.jpg (JPG dari *digital camera* yang menggunakan EXIF (*Exchangeable Image File Format*) *.jpg (JPG dengan SPIFF (*Still Picture Interchange File Format*)	0xff d8 ff e0 xx xx 4a 46 49 46 00 0xff d8 ff e1 xx xx 45 78 69 66 00 0xff d8 ff e8 xx xx 53 50 49 46 46 00
*.png (*file Portable Network Graphics*)	0x89 50 4e 47 0d 0a
***File-file* Video**	
*.avi (*file* Audio Video *Interleave* dari Windows)	0x41 56 49 20 4c 49
*.wmv/wma (*file* Windows Media Audio/Video)	0x30 26 b2 75 8e 66 cf 11
*.mp4 (*file* video MPEG-4)	0x00 00 00 14 66 74
*.flv (*file* video *flash*)	0x46 4c 56 01
*.mpeg/mpg (*file* video) *.mpg/vob (*file* video dvd atau mpeg2)	0x00 00 01 bx 0x00 00 01 ba
***File-file* Audio**	
*.wav (*file* audio Windows)	0x52 49 46 46 xx xx xx xx 57 41 56 45 66 6d 74 20
*.mp3/mpeg/mpg (*file* audio mpeg) *.mp3 (*file* audio mpeg-1 audio layer 3)	0xff fx 0x49 44 33
*.amr (*file* audio Adaptive Multi-Rate, sering ditemukan sebagai format audio di *handphone* GSM)	0x23 21 41 4d 52
***File-file* Office**	
*.pdf (*file Portable Document Format*)	0x25 50 44 46
*.odt/odp (*file* OpenDocument untuk dokumen dan presentasi) *.kwd (*file* dokumen KWord) *.sxc, sxi, sxw (*file* OpenOffice untuk *spreadsheet*, presentasi dan dokumen)	0x50 4b 03 04

*.zip (*file* arsip PKZIP)	
*.zip (*file* arsip kompresi WinZip)	0x57 69 6e 5a 69 70
*.doc/ppt/xls (file Microsoft Office 2003 untuk dokumen, presentasi dan *spreadsheet*) *.db (*file* database MSWorks)	0xd0 cf 11 e0 a1 b1 1a e1
*.docx/pptx/xlsx (*file* Microsoft Office 2007 untuk dokumen, presentasi dan *spreadsheet*)	0x50 4b 03 04 14 00 06 00
*.doc (*file* dokumen Perfect Office)	0xcf 11 e0 a1 b1 1a e1 00
*.doc (*file* dokumen DeskMate)	0x0d 44 4f 43
*.rtf (file dokumen Rich Text Format)	0x7b 5c 72 74 66 31
*.ws (*file* dokumen Wordstar 5.0/6.0)	0x1d 7d
*.ws2 (*file* dokumen Wordstar 2)	0x57 53 32 30 30 30
*.dbx (*file* untuk *folder email* Outlook Express)	0xcf ad 12 fe
*.pst (*file* untuk *personal* Microsoft Outlook)	0x21 42 44 4e

Tabel VI.1. Tabel *signature* (*magic numbers*) untuk beberapa *file* yang sering digunakan misalnya *file-file* office (dokumen, presentasi dan *spreadsheet*), audio, video dan gambar digital.

Dengan didasarkan pada *file signature* seperti yang dijelaskan di atas, beberapa pengembang membuat aplikasi-aplikasi untuk *lost files recovery*. Aplikasi-aplikasi ini akan melakukan proses *scanning* setiap sektor yang ada pada media rekam target/barang bukti untuk mencari *signature* dari *file* yang diinginkan, oleh karena itu proses *lost file recovery* ini biasanya memakan waktu yang cukup lama. Semakin besar ukuran dari media rekam tersebut, maka akan semakin lama waktu yang dibutuhkan untuk proses *recovery* ini. Jumlah ekstensi *file* berbasis *signature* yang akan digunakan juga menambah beban waktu *proses recovery*. Semakin banyak tipe ekstensi (*signature*) *file* yang digunakan, maka akan semakin lama juga waktu yang dibutuhkan untuk menyelesaikan proses tersebut.

Oleh karena aplikasi ini berbasis *sector scanning*, maka semua *file* yang sama (*matched*) dengan *signature* yang diinginkan akan langsung di-*recovery*. Masalah yang timbul adalah *file-file* yang berhasil di-*recover* belum tentu semuanya *lost files*, bisa jadi sebagian merupakan *logical* atau *deleted files*. Namun ada juga aplikasi yang sudah dikembangkan untuk membaca *file system* terlebih dahulu

untuk memetakan *file* mana yang *logical* dan *deleted*, sehingga *file-file* yang berhasil di-*recovery* dan tidak termasuk dalam *file system*, akan dianggap sebagai *lost files*. Hal inilah yang dikembangkan oleh GetData untuk aplikasi *Recover My Files*, seperti yang terlihat pada gambar di bawah ini.

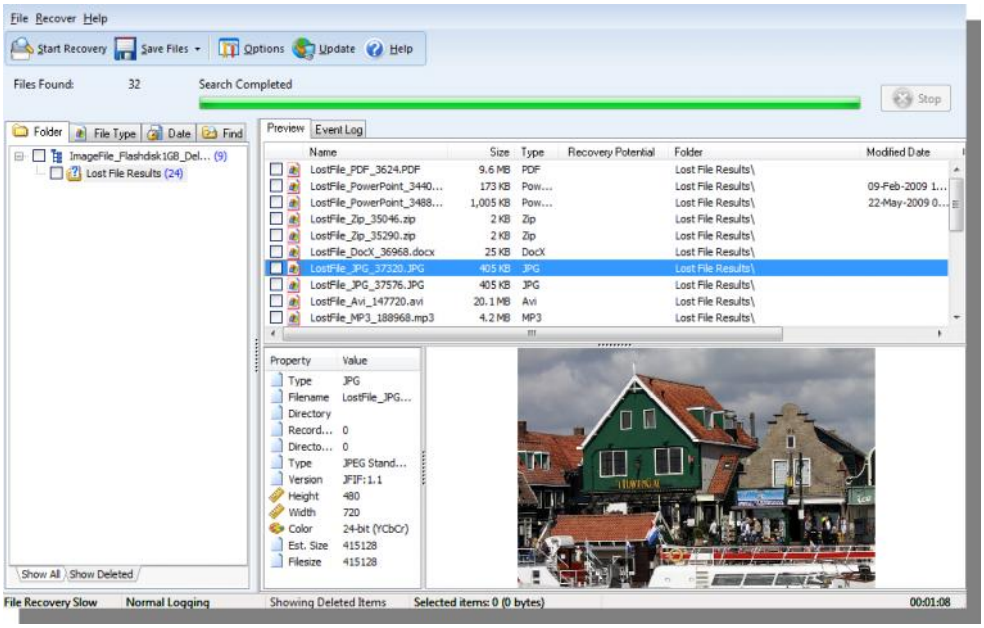


Gambar VI.15. Aplikasi *Recover My Files* dari GetData menyediakan fitur mencari *deleted files* terlebih dahulu, kemudian baru *lost files*.

Untuk melakukan proses *lost files recovery*, seperti biasa *forensic analyst* dan *investigator* tinggal memasukkan *source*-nya (sumber/asal media rekam) yang berupa *image file* (yang merupakan hasil dari proses *forensic imaging* pada proses akuisisi sebelumnya) ke tempat dari aplikasi yang digunakan, misalnya *Recover My Files* dari GetData, kemudian pilih '*lost file recovery*' untuk memulai proses tersebut. Seperti yang telah dijelaskan sebelumnya bahwa proses berbasis *sector scanning* memakan waktu yang cukup lama, maka *analyst* dan *investigator* harus bersabar untuk mendapatkan hasilnya. Agar proses tersebut tidak *stuck* (berhenti di tengah jalan), sebaiknya menggunakan *analysis workstation* yang memiliki *processor* banyak *core* (inti) berkecepatan tinggi (minimal 4 *core* seperti *processor* Intel i3, i5 dan i7 dengan kecepatan minimal 2GHz), di samping ukuran RAM (*Random Access Memory*) yang cukup besar, minimal 4GB.

Gambar di bawah ini menunjukkan proses *lost files recovery* yang sudah selesai berikut hasilnya. Tidak hanya *lost files*, aplikasi dari GetData ini juga memberikan

hasil untuk *deleted files* dan *logical files*. Di samping itu, juga terdapat filterisasi berdasarkan tanggal modifikasi-nya (*modified date*) dan tipe ekstensi *file*.



Gambar VI.16. Hasil dari proses *lost files recovery* dengan menggunakan aplikasi *Recover My Files* dari GetData.

Sama seperti *deleted files*, *lost files recovery* juga berhubungan dengan *cluster* dan sektor tempat penyimpanannya. Jika *cluster*/sektor tersebut belum tertimpa dengan *file-file* baru, maka *lost files recovery* dapat berjalan penuh. Semua isi *lost files* dapat diangkat. Sebaliknya jika *cluster*/sektor dari *lost files* tersebut sudah tertimpa (*overwritten*) oleh file-file baru maka *lost files* tersebut tidak bisa di-*recovery* lagi.

Low level recovery

Di samping teknik *deleted* dan *lost files recovery* seperti yang telah dijelaskan di atas, ada teknik *recovery* yang lain yang ditujukan untuk mencari isi dari *deleted* maupun *lost files* di mana *file-files* tersebut sebagian sudah tertimpa oleh *file-file* baru, bahkan *signature* dari *lost file* sendiri juga sudah tertimpa. Untuk kondisi seperti ini, *lost files recovery* tidak akan menghasilkan informasi/*file* yang diinginkan karena *reocvery* berbasis *signature* ini tidak dapat menemukan lagi

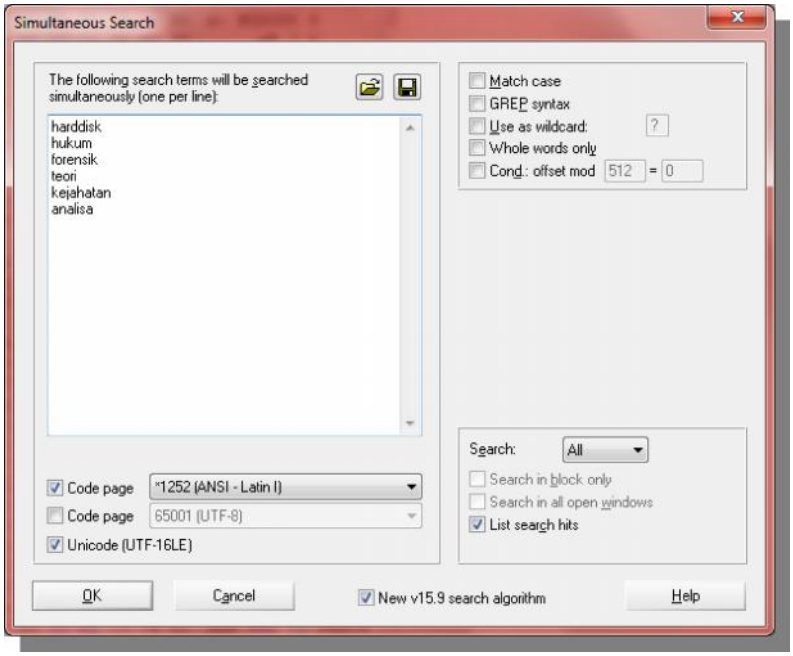
signature dari *lost files* yang sudah tertimpa pada posisi *cluster*/sektornya. Begitu juga dengan *deleted files* yang sebagian isinya sudah tertimpa. Teknik yang ditujukan untuk mencari sisa-sisa isi dari *deleted* dan *lost files* yang sudah tertimpa ini disebut dengan teknik *low-level recovery*.

Sebenarnya teknik ini memiliki kemiripan dengan teknik analisa *slack files* di mana kedua teknik ini sama-sama mencari sisa-sisa dari *deleted* dan *lost files* yang sudah tertimpa pada posisi *cluster*/sektornya. Meskipun begitu, *low level recovery* memiliki jangkauan yang lebih luas dan tepat dikarenakan teknik ini didasarkan pada *keyword searching*. Artinya *low level recovery* akan mencari semua kata yang ada di media penyimpanan yang sama (*matched*) dengan *keyword* yang digunakan. Bisa jadi *hits* (kata yang *matched*) yang didapat berupa *link* dari suatu *file* yang dicari di mana *file* tersebut ternyata disimpan di *removable media*, bukan di *harddisk* dari komputer milik pelaku. Namun adakalanya, *hits* sering juga menemukan informasi yang tidak penting, yaitu bahasa-bahasa *unicode* dari sistem, aplikasi atau *file* yang ada di komputer tersebut, di mana bahasa-bahasa *unicode* tersebut sama sekali tidak ada kaitannya dengan informasi yang dicari. *Hits* yang dihasilkan dari *low level recovery* sebenarnya merupakan teknik untuk langsung ke sasaran, yaitu informasi yang dicari, sehingga *forensic analyst* dan *investigator* tinggal memilah dan menganalisa satu per satu *hits* untuk memastikan *hits* yang mana yang sesuai dengan maksud investigasi.

Dikarenakan *low level recovery* ini berbasis *keyword searching*, maka teknik *recovery* ini sangat cocok untuk mencari informasi dari *file* yang bertipe dokumen, misalnya *file-file* office Microsoft Office, OpenOffice dan OpenDocument. *File –file* dokumen ini memuat teks sebagai isinya, sehingga jika *file-file* ini bersifat *deleted* dan *lost* yang sebagian *cluster* dan sektornya sudah tertimpa oleh *file-file* baru, maka masih memungkinkan untuk mendapatkan sisa-sisa isi dari *file* dokumen tersebut yang belum tertimpa dengan menggunakan teknik *recovery* ini. Meskipun begitu, *low level recovery* ini tidak hanya bekerja untuk *deleted* dan *lost files*, namun teknik ini juga melihat semua data/kata dari *logical files* dan *file-file* dari sistem/aplikasi serta informasi lain yang berkaitan dengan sistem.

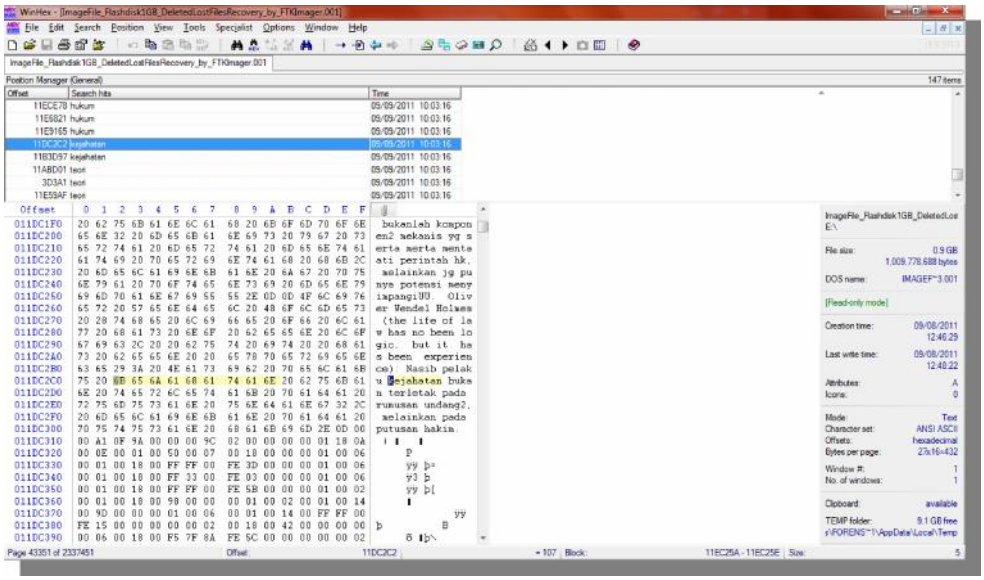
Keywords searching yang digunakan bisa jadi berjumlah lebih dari satu atau banyak *keywords*. Untuk kasusu seperti ini, *forensic analyst* dan *investigator*

dapat menjalankan semua *keywords* tersebut secara bersamaan dalam proses *sector scanning*-nya. Metode seperti ini disebut dengan istilah *simultaneous search*, seperti yang terlihat pada Gambar VI.17 di bawah ini. Hal ini dimaksudkan untuk menghemat waktu semaksimal mungkin.



Gambar VI.17. Aplikasi WinHex menyediakan fitur *simultaneous search* untuk mencari beberapa *keywords* dalam satu kesempatan yang sama.

Dengan adanya *simultaneous search* ini, *analyst* dan *investigator* tidak perlu menjalankan *keyword searching* berkali-kali karena hal tersebut akan sangat memboroskan waktu. Hanya jalankan satu proses dengan banyak *keywords*, selanjutnya *analyst* dan *investigator* tinggal mengecek satu per satu *hits* yang didapat/dihasilkan, seperti yang terlihat pada Gambar VI.18. Pada gambar tersebut dapat dilhat bahwa posisi *hits* yang ditemukan dalam proses *low level recovery* ini ditunjukkan dalam bilangan *offset*. Nilai *offset* ini adalah posisi *byte* per *byte* yang ada di media rekam di mana sistem *byte* ini dimulai dari byte 0 yang merupakan *boot sector* dari media rekam seperti sempat dijelaskan pada Bab V tentang *Windows Forensic: File System Analysis*. *Hits* dengan posisi *offset*-nya merupakan bukti yang kuat untuk menunjukkan keberadaan adanya informasi yang berkaitan dengan maksud investigasi.



Gambar VI.18. *Hits* hasil *keyword searching* yang menggunakan *simultaneous search* untuk beberapa kata, yang dilengkapi dengan posisi *offset*-nya untuk masing-masing *hits*.

Seperti yang disinggung tadi bahwa *low level recovery* ini juga didasarkan pada *sector scanning*. Artinya teknik *recovery* ini akan membaca semua sektor yang ada di media penyimpanan barang bukti (yang dalam hal ini berupa *image file*) untuk mencari kata-kata yang *matched* dengan *keyword* yang digunakan. Semakin besar ukuran dari media penyimpanan, maka akan semakin banyak sektor yang dimiliki oleh media tersebut yang akan berakibat semakin lama waktu yang dibutuhkan untuk menyelesaikan proses *low level recovery* ini.

Bibliography

1. ACPO, 7Safe (2008). *Good Practice Guide for Computer-Based Electronic Evidence*. UK ACPO and 7Safe.
2. Al-Azhar, M.N. (2010). *Standard Operating Procedure (SOP) 1 : Prosedur Pemeriksaan Digital Forensik*. DFAT Puslabfor.
3. Carrier, B. (2002). *Open Source Digital Forensic Tools: The Legal Argument.* @stake.
4. Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Elsevier Academic Press.

5. Johnson, T. A. (2005). *Forensic Computer Crime Investigation*. Taylor & Francis.
6. Kessler, G. (2011). *File Signatures Table.* http://www.garykessler.net/library/file_sigs.html.
7. Middleton, B. (2002). *Cyber Crime Field Handbook*. CRC Press
8. National Institute of Justice (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. US National Institute of Justice
9. National Institute of Justice (2001). *Electronic Crime Scene Investigation: A Guide for First Responder*. US National Institute of Justice.
10. Sammes, T. and Jenkinson, B. (2007). *Forensic Computing: A Practitioner's Guide*. Springer.
11. Solomon, M. G. et al. (2005). *Computer Forensics Jumpstart*. Sybex.

Bab VII

MOBILE FORENSIC: Theory and Analysis

Salah satu bentuk teknologi tinggi yang saat ini sering digunakan oleh manusia adalah *handphone*. Tujuan utama orang menggunakan *handphone* adalah untuk berkomunikasi antara yang satu dengan yang lain. Bentuk komunikasi lewat udara ini bisa beragam tujuannya, dari yang sekadar berbicara tentang hal-hal sepele sampai hal-hal yang serius, misalnya tentang pekerjaan dan kegiatan baik yang bersifat positif maupun negatif. Bentuk negatif ini bisa berupa pembicaraan mengenai rencana tentang tahapan-tahapan pelaksanaan suatu kejahatan, misalnya pembunuhan, perampokan, pemerasan, korupsi dan transaksi narkoba. Pembicaraan tentang hal ini bisa juga masuk ke topik tentang bagaimana cara untuk menghilangkan jejak kejahatannya.

Ketika satu atau beberapa *handphone* digunakan sebagai alat komunikasi di antara beberapa pelaku kejahatan untuk mengorganisir kejahatannya, maka *handphone* tersebut dapat disita oleh aparat penegak hukum atau *investigator* sebagai salah satu barang bukti. Barang bukti *handphone* ini kemudian diperiksa secara forensik oleh *forensic analyst* dan/atau *investigator* untuk mencari informasi-informasi yang menunjukkan hubungan antara pelaku kejahatan yang satu dengan yang lain, terutama dalam hal pengorganisasian kejahatannya. Informasi-informasi yang dicari tersebut bisa berupa *logical* (artinya masih bisa diakses seperti biasa) atau *deleted* (sudah dihapus). Jika informasi yang dicari ternyata sudah dihapus oleh pemiliknya, maka *forensic analyst* dan *investigator* harus berusaha untuk melakukan *recovery* terhadap informasi tersebut. Untuk poin ini, akan dibahas pada salah satu sub bab tentang pemeriksaan forensik pada bab ini.

Seperti yang disinggung di atas, barang bukti *handphone* yang disita untuk diperiksa oleh *investigator* dan *analyst* pada saat ini jumlahnya sangat banyak sekali dikarenakan *handphone* sudah menjadi kebutuhan dan alat utama orang untuk berkomunikasi antara yang satu dengan yang lain. Hal ini disebabkan *handphone* memotong batas jarak dan waktu antara 2 orang yang ingin berkomunikasi. Walaupun kedua orang tersebut terpisahkan oleh jarak yang cukup jauh, mereka tidak perlu menghabiskan waktu

bepergian ke tempat salah satu untuk bertemu secara fisik di antara mereka. Oleh karena *handphone* ini sangat mudah sekali digunakan untuk komunikasi tanpa ada halangan jarak dan waktu, alat ini seringkali dipilih oleh para pelaku kejahatan sebagai alat utama komunikasi mereka.

Pada tahun 2010, DFAT (*Digital Forensic Analyst Team*) Puslabfor telah memeriksa barang bukti dengan total jumlah 214 item yang berasal dari 52 kasus dari berbagai macam jenis kejahatan seperti jaringan narkoba, pornografi, perjudian, korupsi, pencemaran nama baik, penipuan, penyuapan dan lain-lain. Dari jumlah tersebut, sebanyak 118 item (sekitar 55% atau lebih dari sebagian dari jumlah total barang bukti) berupa barang bukti *handphone*. Artinya pelaku kejahatan masih menganggap *handphone* sebagai salah satu alat komunikasi utama mereka. Untuk itu *digital forensic analyst* dan *investigator* harusnya dapat mengantisipasi hal ini, sehingga ketika ada barang bukti *handphone*, baik versi lama maupun versi yang baru dikeluarkan yang disita dari pelaku kejahatan, maka barang butki elektronik dapat diperiksa dengan benar sesuai dengan prinsip-prinsip dasar digital forensik.

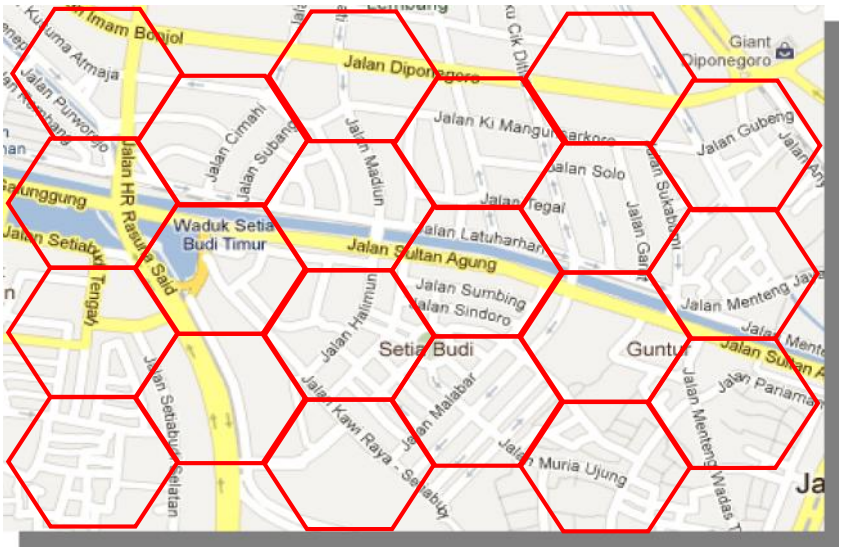
Mekanisme kerja

Salah satu hal yang mendasar yang perlu dipahami oleh *analyst* dan *investigator* adalah mekanisme kerja dari *handphone* itu sendiri. Karena *handphone* sifatnya *wireless* (tidak menggunakan kabel), maka ia membutuhkan satu pemancar yang mampu mengirimkan dan menerima sinyal pada frekwensi tertentu dari *handphone* tersebut. Pemancar tersebut dikenal dengan istilah BTS (*Base Transceiver Station*). BTS inilah yang menghubungkan antara *handphone* dengan jaringan yang disediakan oleh *provider* (penyedia jasa layanan komunikasi). Jaringan tersebut bisa berupa 2G, 2.5G, 2.75G, 3G dan 4G.

Jaringan 2G merupakan jaringan yang digunakan untuk panggilan suara dan teks SMS (*Short Message Service*). Jaringan ini biasa dikenal sebagai jaringan GSM (*Global System for Mobile Communication*). Kemudian jaringan 2.5G yang merupakan jaringan yang sudah bisa digunakan untuk transfer data di samping panggilan dan teks SMS. Pada jaringan 2.5G terdapat jaringan GPRS (*Global Packet Radio Service*) berkecepatan sekitar 160 *Kbit* per detik untuk transfer data.

Selanjutnya jaringan 2.75G sebagai jaringan EDGE (*Enhanced Data rates for GSM Evolution*) dengan kecepatan transfer data sekitar 400 *Kbit* per detik, dan jaringan 3G dengan kemampuan transfer data berkecepatan tinggi sekitar 800 *Kbit* per detik sehingga bisa digunakan untuk kebutuhan tertentu misalnya berselancar lebih cepat di internet dan *video calls*. Di atas jaringan 3G, terdapat jaringan HSDPA (*High Speed Data Packet Access*) yang kadang-kadang dikenal sebagai jaringan 3.5G di mana jaringan ini memiliki kecepatan transfer data sekitar 14 *Mbit* per detik sehingga jaringan ini sering digunakan untuk *wireless modem* yang menghubungkan komputer dengan internet. Malah pada saat ini telah dikembangkan jaringan berkecepatan data sangat tinggi yaitu 4G yang memiliki kecepatan sekitar 1 *Gbit* per detik.

Dikarenakan BTS merupakan garda terdepan dari *provider* untuk menghubungkan *handphone* dari *customer* (pelanggan) dengan jaringannya, maka BTS didesain untuk mempunyai jangkauan wilayah frekwensi radio (dikenal dengan istilah *coverage area*) dengan batasan jarak tertentu.



Gambar VII.1. *Coverage area* dari masing-masing BTS berbentuk heksagonal.

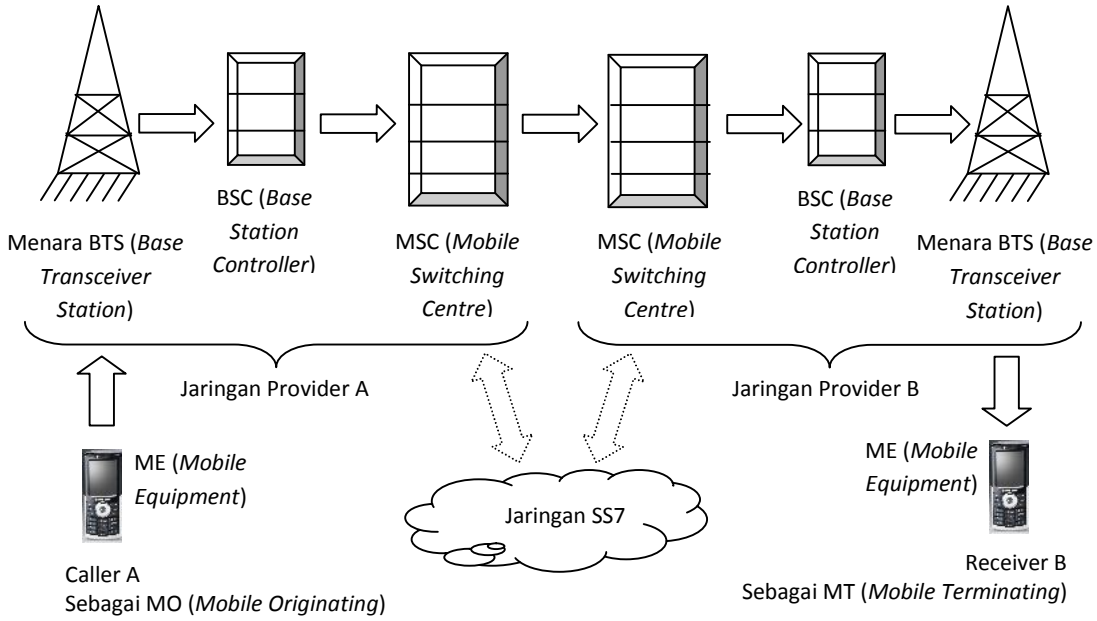
Coverage area yang sifatnya berbentuk heksagonal ini (seperti yang terlihat pada Gambar VII.1 di atas) diusahakan oleh *provider* agar terhubung antara satu BTS dengan BTS yang lain tanpa adanya *gap* (wilayah) kosong di antara BTS-BTS tersebut. Jika terdapat *gap* kosong (artinya tanpa adanya frekwensi radio), maka

handphone tidak bisa mendapatkan sinyal untuk jaringan dari *provider* tersebut. Artinya *handphone* tidak bisa digunakan untuk berkomunikasi selama *customer* berada di wilayah tersebut. *Coverage area* dari BTS inilah yang dapat memudahkan seorang *customer* bergerak dari satu tempat ke tempat lain sambil tetap menerima sinyal jaringan dari *provider* tanpa putus (dengan catatan tidak adanya *gap* kosong frekwensi radio). Misalnya ketika ia bergerak dari Jakarta menuju Bogor dengan menggunakan jalan tol Jagorawi, maka sangat memungkinkan selama perjalanan ia dapat melakukan panggilan telepon melalui *handphone*-nya dari berangkat hingga sampai di tempat tujuan. Hal ini dikenal dengan istilah *dynamic handover*, yaitu posisi *handphone* diteruskan dari satu *coverage area* ke *coverage area* berikutnya mengikuti pergerakan *handphone* tersebut.

Masing-masing BTS dengan *coverage area*-nya diberi tanda pengenal oleh *provider* untuk memudahkan *provider* melakukan organisasi dan administrasi kerja untuk tiap-tiap BTS. Tanda (ID) pengenal ini juga dilengkapi dengan posisi alamat dari BTS tersebut. ID dan lokasi masing-masing BTS inilah yang sering digunakan oleh aparat penegak hukum untuk mengetahui lokasi seseorang melalui metode *lawful interception* (penyadapan secara resmi dan prosedural menurut hukum yang berlaku). Meskipun begitu, lokasi yang dihasilkan dari posisi BTS masih merupakan wilayah yang cukup luas, oleh karena itu aparat penegak hukum masih harus menggunakan alat tambahan dengan didasarkan pada frekwensi radio dari *handphone* target untuk memetakan posisinya secara tepat di dalam wilayah BTS tersebut. Alat tambahan tersebut dikenal dengan istilah *Direction Finder*.

Dari BTS-BTS, sinyal frekwensi dari *handphone* diteruskan ke suatu peralatan yang dinamakan BSC (*Base Station Controller*). BSC ini bertugas mengontrol sejumlah BTS (bisa puluhan hingga ratusan BTS) dengan tanggungjawab berupa pengalokasian *channel* frekwensi radio untuk *handphone-handphone* yang terkoneksi di area BTS-nya untuk dapat berkomunikasi melalui panggilan, SMS dan lain-lain, di samping melakukan proses *paging* (mekanisme untuk memastikan posisi handphone di area BTS yang menjadi tanggungjawabnya).

Dari BSC-BSC, sinyal frekwensi dari *handphone* dilanjutkan ke MSC (*Mobile Switching Centre*) yang bertugas melakukan proses *switching*, yaitu mekanisme pengaturan komunikasi antara jaringan-jaringan mobile (saluran telepon bergerak) dan/atau *fixed line* (saluran telepon dengan posisi tetap). Di MSC ini terdapat HLR (*Home Location Register*) yang merupakan database terpusat yang berisikan detil masing-masing *subscriber* yang memiliki otorisasi untuk menggunakan jaringan *provider* termasuk juga posisinya pada wilayah BTS tertentu, dikenal dengan istilah LAI (*Location Area Identity*). Di samping HLR, di MSC juga terdapat proses pengaturan VLR (*Visitor Location Register*) yang berupa database temporer dari *subscriber* (pelanggan mobile) tamu yang menggunakan jaringan provider, oleh karenanya untuk satu *subscriber*, hanya ada satu VLR pada waktu yang bersamaan. Untuk pergerakan masing-masing *subscriber*, VLR ini berkomunikasi dengan HLR.



Gambar VII.2. Mekanisme kerja jaringan telekomunikasi antara 2 *provider* yang berbeda untuk panggilan dari *caller* A sebagai MO (*Mobile Originating*) ke *recipient* B sebagai MT (*Mobile Terminating*).

Di samping itu di MSC, juga terdapat AuC (*Authentication Centre*) yang berfungsi untuk melakukan proses otentikasi tiap-tiap *subscriber* berdasarkan nomor IMSI (*International Mobile Subscriber Identity*) masing-masing. Jika proses otentikasi

IMSI sukses maka subscriber akan diberikan akses untuk menggunakan jaringan provider.

Dari Gambar VII.2. di atas, diketahui bahwa MSC memegang peranan yang penting untuk menyalurkan panggilan ataupun pengiriman pesan SMS dari jaringan *provider* yang satu ke *provider* yang lain. Untuk itu, MSC menyimpan banyak data-data yang berasal dari lalu lintas panggilan dan/atau pesan SMS antar *subscriber* dari masing-masing *provider*. Dikarenakan hal tersebut, seringkali *investigator* atau aparat penegak hukum harus berhubungan dengan *provider* untuk meminta data yang biasa disebut dengan CDR (*Call Data Record*) yang berkaitan dengan *subscriber* tertentu. CDR dari masing-masing *subscriber* tersimpan di database *provider* dalam jangka waktu tertentu, disesuaikan dengan besarnya kapasitas penyimpanan *server* yang ada. Semakin besar kapasitas penyimpanan, maka akan semakin lama CDR tersimpan di database *provider*. Di samping itu, penyimpanan CDR juga dipengaruhi oleh jumlah *subscriber* yang ada di provider. Semakin banyak *subscriber*, maka akan semakin sedikit waktu yang tersedia untuk menyimpan CDR tersebut di database. Ini dikarenakan kapasitas penyimpanan harus dibagi dengan sekian banyak jumlah *subscriber* yang ada.

Pada gambar di atas, terdapat jaringan SS7 yang digunakan oleh *provider* untuk menyediakan akses bagi *susbcriber* yang sedang *roaming* (yaitu berada di luar jangkauan jaringan provider). SS7 ini menggunakan jaringan berkecepatan sangat tinggi untuk transfer data *subscriber*. Misalnya *subscriber* A dari Indonesia yang menggunakan SIM *card* Telkomsel sedang berada di Singapura. SIM *card* tersebut tetap aktif di *handphone* A selama ia berada di Singapura. SIM *card* tersebut akan mencari jaringan yang melakukan kerja sama *provider* antar negara dengan Telkomsel, misalnya SingTel. Ketika A ingin mengirimkan SMS kepada temannya B yang menggunakan kartu yang sama dan berada di Jakarta, maka ia akan menggunakan jaringan SingTel untuk mengirimkan pesan SMS tersebut. Dari jaringan SingTel, pesan SMS akan diteruskan ke jaringan SS7 di internet, kemudian masuk ke jaringan Telkomsel, selanjutnya diteruskan hingga ke MT B.

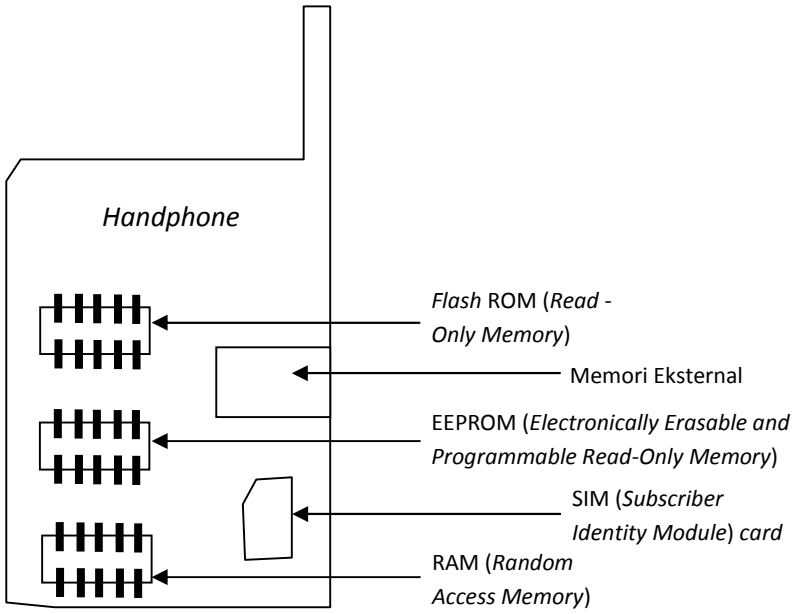
Jaringan SS7 ini sering juga disalahgunakan untuk mengirimkan pesan SMS palsu, yaitu pesan SMS yang menggunakan nomor panggilan atau yang dikenal dengan istilah teknis nomor MSISDN (*Mobile Subscriber Integrated Services Digital*

Network) milik orang lain, namun tanpa menggunakan SIM *card* yang bersangkutan, sehingga pesan SMS tersebut seolah-olah dikirimkan oleh orang tersebut padahal tidak. Permasalahan ini terjadi karena tidak adanya proses otentikasi posisi *subscriber* (dalam hal ini adalah pengirim pesan) dengan menggunakan VLR (*Visitor Location Register*) dan HLR (*Home Location Register*) di MSC (*Mobile Switching Centre*) dari *provider*. Mengenai VLR, HLR dan MSC akan dijelaskan pada sub bab berikutnya. Untuk jaringan GSM yang biasa, *provider* memang melakukan proses otentikasi posisi *subscriber* tersebut, namun untuk jaringan SS7 hal tersebut tidak ada. Pesan SMS yang dikirim dari nomor panggilan tertentu lewat jaringan SS7 akan dianggap oleh *provider* sebagai pesan SMS dari nomor panggilan *subscriber* yang sedang *roaming*, sehingga pesan tersebut akan tetap diteruskan oleh *provider* ke *recipient*.

Untuk *provider* yang sama, proses otentikasi posisi *subscriber* masih memungkinkan untuk dilakukan karena VLR dengan data MSC dari pengirim akan dilakukan *cross-check* dengan data MSC yang ada di HLR *provider*. Jika data MSC dari VLR ternyata berbeda dengan HLR maka pengiriman SMS palsu tersebut akan dihentikan. Untuk *provider* yang berbeda antara pengirim dan penerima, maka proses ini akan sulit untuk dilakukan karena HLR *provider* penerima tidak memiliki data MSC dari VLR *provider* pengirim. Untuk kasus ini, data MSC dari VLR *provider* pengirim akan dianggap benar oleh *provider* penerima, meskipun pelaku pengirim SMS palsu sama sekali tidak menggunakan jaringan *provider* pengirim.

Mekanisme penyimpanan data

Handphone yang disita dari pelaku menyimpan banyak informasi yang dapat digali oleh *forensic analyst* dan *investigator* untuk mencari kaitan/hubungan antara pelaku dengan kejahatan dan antara pelaku yang satu dengan pelaku yang lain. Informasi-informasi yang tersimpan di *handphone* tersebut sebenarnya berada pada beberapa media penyimpanan yang berbeda seperti yang terlihat pada Gambar VII.3, sehingga *analyst* dan *investigator* dapat meng-*eksplore* media penyimpanan tertentu untuk mencari dan mendapatkan informasi yang memang tersimpan di tipe media penyimpanan tersebut.



Gambar VII.3. Struktur mekanisme penyimpanan data di *handphone*.

Dari gambar di atas, media-media penyimpanan tersebut adalah sebagai berikut :

1. SIM (*Subscriber Identity Module*) *card*

   SIM *card* menyimpan hanya data-data tertentu, yaitu :

   a. *Phonebook*, yang terdiri dari *contact-contact* yang berisikan nomor telepon yang berasosiasikan dengan nama tertentu yang dibuat oleh pemilik *handphone* secara manual.

   b. *Call logs*, yang berisikan catatan panggilan yang pernah terjadi seperti *dialled calls* (panggilan keluar), *received calls* (panggilan masuk) dan *missed calls* (panggilan tak terjawab).

   c. SMS (*Short Message Service*), yaitu pesan teks pendek baik *inbox* (pesan masuk) maupun *sent* (pesan terkirim). Penyimpanan SMS di SIM *card* bersifat terbatas yang didasarkan pada slot (tempat penyimpanan) di mana 1 slot untuk 1 SMS standar. Untuk itu jumlah slot di SIM card bersifat terbatas, hanya dalam jumlah tertentu, biasanya berjumlah 40 slot untuk 40 SMS standar. Lebih dari itu, SMS tidak dapat diterima sampai ada SMS-SMS yang dihapus (*deleted*) untuk mendapatkan slot-slot kosong.

d. ICCID (*integrated Circuit Card Identifier*), terdiri dari sejumlah angka yang unik/khas dan merupakan identitas yang diberikan oleh *provider* untuk setiap SIM *card* guna keperluan yang bersifat administratif. Jumlah digit ICCID biasanya sekitar 19-20 digit. ICCID bukan merupakan nomor panggilan SIM *card*. Nomor panggilan SIM *card* GSM yang biasanya diawali dengan +628xx untuk di Indonesia adalah nomor MSISDN (*Mobile Subscriber Integrated Services Digital Network*) di mana nomor MSISDN ini hanya tersimpan di *provider*. Meskipun begitu, *analyst* dan *investigator* masih bisa mendapatkan nomor MSISDN ini dengan berbekal nomor ICCID. *Analyst* dan *investigator* tinggal membawa nomor ICCID tersebut ke *provider* untuk mendapatkan informasi tentang nomor MSISDN.

   2 digit pertama dari ICCID merupakan MII (*Major Industry Identifier*) yang biasanya bernilai 89 yaitu menginformasikan bahwa SIM *card* dibuat dan digunakan untuk kepentingan telekomunikasi.

   Digit 3-5 merupakan *country code*, yaitu kode unik untuk masing-masing negara di mana Indonesia memiliki *country code* 62.

   Sisa digit yang lain merupakan *issuer identifier* dan *individual account identification number* yang bervariasi metodenya untuk tiap-tiap *provider*.

   1 digit terakhir merupakan *check digit* (CN) yang didasarkan pada algoritma Luhn. CN sesuai algoritma Luhn akan dijelaskan pada penjelasan tentang IMEI.

e. IMSI (*International Mobile Subscriber Identity*), merupakan identitas yang unik/khas untuk setiap *subscriber* yang diberikan oleh *provider* ketika *subscriber* menggunakan jaringannya setelah melalui proses otentikasi sebelumnya. *Provider* menggunakan nomor IMSI untuk mengizinkan SIM *card* yang satu berkomunikasi dengan SIM *card* yang lain di dalam jaringannya.

3 digit pertama dari IMSI merupakan MCC (*Mobile Country Code*). Tabel berikut memuat MCC untuk sejumlah negara di dunia

MCC	Negara
204	Belanda
208	Perancis
214	Spanyol
222	Italia
232	Austria
234	Inggris
238	Denmark
240	Swedia
250	Federasi Rusia
262	Jerman
268	Portugal
286	Turki
302	Kanada
310	Amerika Serikat
404	India
410	Pakistan
412	Afghanistan
420	Saudi Arabia
425	Israel
432	Iran
440	Jepang
452	Vietnam
454	Hongkong
460	Republik Rakyat Tiongkok
466	Taiwan
502	Malaysia
505	Australia
510	Indonesia
515	Filipina
520	Thailand
525	Singapura
528	Brunei Darussalam

602	Mesir
606	Libia
621	Nigeria
655	Afrika Selatan
722	Argentina
724	Brazil
732	Kolombia

Tabel VII.1. Daftar MCC (*Mobile Country Code*) untuk sejumlah negara di dunia

2 digit selanjutnya adalah MNC (*Mobile Network Code*) yang memberikan identitas yang khas untuk masing-masing *provider* di seluruh dunia. Tabel berikut memuat MNC untuk wilayah Indonesia.

MNC	Provider	Merk
01	PT. Indonesian Satellite Corporation Tbk (Indosat)	Indosat
03	PT Indosat Tbk	StarOne
07	PT. Telkom	TelkomFlexi
08	PT. Natrindo Telepon Seluler	Axis
09	PT. Smart Telecom	Smart
10	PT. Telekomunikasi Selular	Telkomsel
11	PT. XL Axiata Tbk	XL
21	PT. Indonesian Satellite Corporation Tbk (Indosat)	IM3
28	PT. Mobile-8 Telecom	Fren
89	PT. Hutchison CP Telecommunications	3
99	PT. Bakrie Telecom	Esia

Tabel VII.2. Daftar MNC (*Mobile Network Code*) untuk sejumlah *provider* di Indonesia.

Digit-digit berikutnya merupakan MSIN (*Mobile Station Identification Number*) yaitu identitas yang unik, biasanya sekitar 10 digit yang diberikan oleh *provider* masing-masing.

2. EEPROM (*Electronically Erasable and Programmable Read-Only Memory*)

   EEPROM merupakan tempat penyimpanan data-data default (yang berasal dari pabrikan), seperti :

   a. Sistem Operasi
   b. Aplikasi-aplikasi default
   c. IMEI (*International Mobile Equipment Identity*), merupakan identitas (ID) yang unik/khas bagi masing-masing handphone GSM yang terorganisir secara internasional. Nomor IMEI ini biasanya terletak di bagian belakang *handphone* yaitu di bawah batere dan mungkin juga tercatat di kotak pembungkus *handphone*. Namun nomor IMEI ini juga bisa didapat dengan mengetikkan *#06#, yang secara otomatis akan menampilkan nomor IMEI di layar *handphone*.

      8 digit pertama merupakan TAC (*Type Allocation Code*), yang merujuk kepada merk pabrikan, model dan negara pembuat (*country of origin*)

      Digit ke 9 s/d 14 merupakan *serial number* dari *handphone* yang secara unik diberikan oleh pabrikan untuk *handphone* tersebut.

      Digit ke 15 merupakan *check digit* yang digunakan untuk mengecek validitas IMEI dengan menggunakan algoritma Luhn. Pada algoritma ini, digit genap dikalikan dengan 2. Jika hasil perkalian menghasilkan 2 digit, maka kedua digit tersebut merupakan digit yang terpisah antara digit yang satu dengan yang lain. Langkah selanjutnya kedua digit tersebut dijumlahkan bersama-sama dengan digit ganjil sampai ke digit 14. Contoh berikut menjelaskan penggunaan *check digit* yang didasarkan pada algoritma Luhn tersebut.

IMEI : 354237/03/863616/3

Algoritma Luhn :

= 3+(5x2)+4+(2x2)+3+(7x2)+0+(3x2)+8+(6x2)+3+(6x2)+1+(6x2)

= 3+(1+0)+4+(4)+3+(1+4)+0+(6)+8+(1+2)+3+(1+2)+1+(1+2)

= 47

Check digit (CN) = 50 – 47 = 3

Dari kalkulasi algoritma Luhn, diketahui bahwa nomor IMEI tersebut adalah valid dengan CN = 3.

d. ESN (*Electronic Serial Number*), terdiri dari 32 *bit* dan merupakan identitas *handphone* yang berbasis jaringan CDMA (*Code Division Multiple Access*). 14 *bit* pertama dari ESN digunakan sebagai kode pabrikan, kemudian 18 *bit* berikutnya digunakan sebagai kode untuk tiap-tiap *handphone* hingga 262.144 kode totalnya.

3. RAM (*Random Access Memory*)

Sama seperti komputer, *handphone* juga memiliki RAM untuk menyimpan data yang bersifat temporer yang berasal dari aplikasi-aplikasi, di samping *date/time* (tanggal/waktu). Artinya begitu *handphone* dimatikan, maka data-data yang tersimpan di RAM akan hilang secara otomatis. RAM akan kosong, dan berisi kembali setelah *handphone* dihidupkan lagi.

Dari penjelasan di atas, data-data yang tersimpan di RAM bersifat *volatile*, yaitu hanya ada selama *handphone* hidup (*on*) dan akan hilang ketika *handphone* dimatikan (*off*). Oleh karena itu, seringkali *user* diminta untuk melakukan *setting date/time* setelah *handphone* dihidupkan kembali dari posisi mati (*off*).

4. *Flash* ROM (*Read-Only Memory*)

Flash ROM bersama-sama dengan EEPROM seringkali dikenal dan disebut sebagai memori internal *handphone*. *Flash* ROM ini memiliki ukuran yang cukup besar untuk *handphone-handphone* keluaran saat ini, oleh karena itu *Flash* ROM dapat menampung banyak data-data sebagai berikut :

a. *Phonebook*
b. Call logs
c. SMS

d. MMS (*Multi Media Services*)
e. *File-file* audio, termasuk juga rekaman suara
f. *File-file* video
g. *File-file* gambar digital
h. Kalendar
i. Notes
j. Data-data penggunaan internet, termasuk *emails*
k. Aplikasi-aplikasi tambahan, termasuk *games*
l. *File-file* data *user* yang lain

5. *External Memory*

   Sesuai dengan namanya, memori penyimpanan data ini bersifat eksternal dengan menggunakan *memory card*, misalnya yang sering dipakai adalah MicroSD. Memori eksternal ini mempunyai ukuran yang lumayan besar hingga mencapai 32GB untuk beberapa *smartphone* (*handphone* cerdas dengan akses data berkecepatan tinggi) terkini. Untuk itu, memori eksternal juga menyimpan banyak data, misalnya :

   a. *File-file* gambar digital
   b. *File-file* audio, termasuk juga rekaman suara
   c. *File-file* video
   d. *File-file* office, seperti dokumen, presentasi dan spreadsheet
   e. *Notes*
   f. Aplikasi *games*
   g. *File-file* data *user* yang lain

Di samping data-data tersebut di atas, tersimpan di media-media penyimpanan yang berbeda-beda di *handphone* sesuai dengan peruntukannya, juga terdapat data-data yang tersimpan di jaringan *provider*, yang juga bisa disebut dengan istilah *network data*. *Network data* tersebut berupa :

1. CDR (*Call Data Record*), yang berisikan catatan panggilan (*call logs*) dan pesan SMS yang dibuat oleh masing-masing *subscriber*. Penyimpanan CDR ini di jaringan *provider* dibatasi oleh rentang waktu, biasanya sekitar 2 s/d 4 minggu, tergantung dengan besarnya kapasitas penyimpanan dan

jumlah *subscriber* di *provider*. Untuk itu semakin cepat *forensic analyst* dan *investigator* datang ke *provider* untuk meminta CDR dari nomor *subscriber* tertentu, maka hal tersebut akan semakin baik. Data di CDR akan semakin lengkap dan diharapkan data yang dicari belum terhapus.

2. *Voice mails*

   Disebut juga dengan istilah kotak suara. Ini merupakan pesan dari *caller* A (pemanggil) yang tidak terjawab oleh *recipient* B (yang dipanggil) kemudian tersambung dengan *recorder* (alat rekam suara) dari *provider* untuk merekam pesan dari *caller* A dan *provider* akan memberikan notifikasi/pemberitahuan adanya *voice mails* kepada *recipient* B. Selanjutnya ketika *recipient* B memegang dan mengakses *handphone*, dia akan mengetahui bahwa ada *voice mails*, kemudian dia akan mengakses nomor tertentu yang disediakan oleh *provider* untuk mendapatkan/mengetahui *voice mails* tersebut.

3. MSISDN (*Mobile Subscriber Integrated Services Digital Network*)

   Merupakan nomor panggilan yang unik untuk tiap-tiap *subscriber*. MSISDN ini berbeda dengan IMSI dan ICCID dari SIM *card* yang sudah dibahas di atas. MSISDN tidak tersimpan di SIM *card*. Seperti sempat disinggung, di Indonesia MSISDN ini diawali dengan digit +628xx di mana xx ini merupakan digit unik yang diberikan oleh otorisasi telekomunikasi untuk masing-masing provider untuk tiap-tiap produk-nya, misalnya kartu Halo (+62811), kartu SimPati (+62812, +62813 dan +62821) dan kartu As (+62852) untuk PT. Telekomunikasi Selular.

Pemeriksaan forensik

Sama seperti komputer, *handphone* butuh sistem operasi untuk menjalankan banyak fungsi (*service*) dan aplikasi di *handphone* dengan benar. Pada saat ini, banyak sekali jenis sistem operasi yang bisa digunakan oleh *handphone*, misalnya sistem operasi Symbian, Windows Mobile, Blackberry, Android, Linux Mobile, Palm dan iOS. Masing-masing sistem operasi tersebut memiliki sistem kerja antar fungsi dan aplikasi yang khas dan berbeda antara yang satu dengan yang lain. Hal

inilah yang harus dipahami oleh pengembang aplikasi-aplikasi forensik untuk pemeriksaan barang bukti *handphone*, agar aplikasi yang dikembangkan dapat mengakses *handphone* dari berbagai jenis sistem operasi, tidak tergantung hanya pada satu sistem operasi.

Untuk melakukan pemeriksaan forensik tersebut, ada juga pengembang yang juga menyediakan *hardware* (yang juga dilengkapi dengan kabel-kabel data yang bervariasi) di samping *software* seperti UFED dari Cellebrite dan XRY dari Micro Systemation seperti yang terlihat pada Gambar VII. 4. Hal ini dimaksudkan agar *analyst* dan *investigator* dapat lebih mudah melakukan konektivitas dan/atau sinkronisasi terhadap berbagai macam jenis merk *handphone* berikut variasi sistem operasi, jadi *analyst* dan *investigator* sebagai *user* tidak perlu melakukan *settings* komputer mereka untuk proses instalasi *software* berikut sinkronisasinya. Apapun jenis *handphone* barang buktinya dengan mudah dapat diakses melalui *toolkit* (*hardware* dan *software* yang kompak) tersebut.



(1) (2)

Gambar VII.4. *Toolkit* yang kompak dan terdiri dari *hardware*, *software* dan kabel data untuk pemeriksaan *mobile forensic*, dari UFED (*Universal Forensics Extraction Device*) dari Cellebrite (1) dan XRY dari Micro Systemation (2).

Meskipun begitu, di samping sistem operasi, permasalahan utama yang lain yang sering muncul adalah konektivitas *toolkit* dan/atau *software* terhadap *handphone* keluaran terbaru. Pengeluaran *handphone* terbaru tersebut oleh pabrikan senantiasa bermunculan dalam rentang waktu yang dekat. *Handphone-handphone* tersebut sangat variatif. Hal ini perlu diantisipasi oleh pengembang aplikasi dengan menyediakan *update* bagi *customer*-nya. Sebaiknya aplikasi dan/atau *toolkit* tersebut di-*update* secara reguler agar *handphone-handphone* terbaru tersebut masuk dalam database aplikasi dan *toolkit*. Dengan masuknya *handphone* tersebut akan memudahkan *analyst* dan *investigator* untuk sewaktu-waktu melakukan pemeriksaan barang bukti *handphone* dengan merk dan model yang sama.

Sebelum melakukan pemeriksaan barang bukti *handphone* berikut SIM *card*-nya secara forensik dengan menggunakan *toolkit* dan/atau aplikasi, *analyst* dan *investigator* sebaiknya sudah memahami prosedur yang semestinya dilakukan terhadap barang bukti *handphone* tersebut.

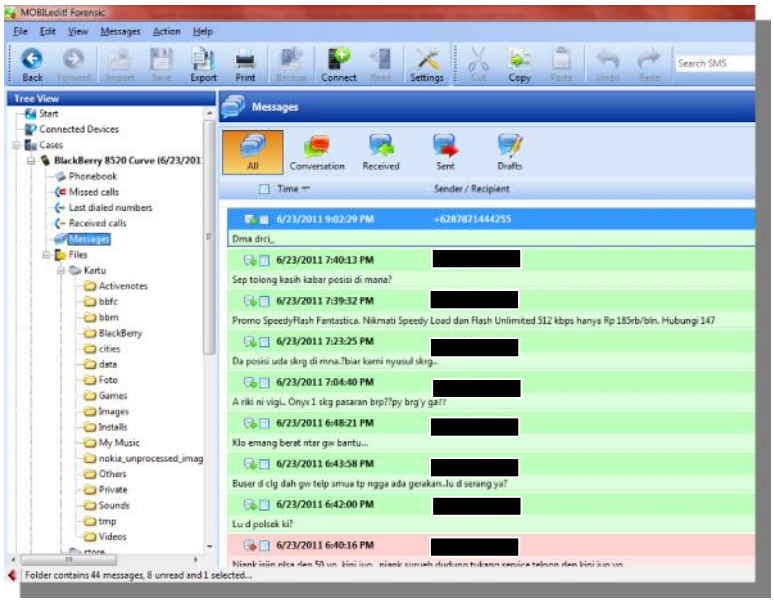
1. ***Handphone* dalam keadaan *on* (hidup)**

   Berikut adalah prosedur untuk barang bukti *handphone* yang ditemukan atau disita dari pelaku dalam keadaan hidup.

   a. Jangan dimatikan! Biarkan dalam keadaan hidup.
   b. Dokumentasikan *handphone* tersebut dengan fotografi forensik berupa foto umum (posisi TKP secara utuh berikut barang bukti *handphone* di dalamnya), foto medium (kaitan barang bukti *handphone* dengan barang-barang di sekitarnya) dan foto *close up* (hanya *handphone* dari depan dan belakang). Di samping foto-foto tersebut, juga dilakukan fotografi terhadap layar *handphone* yang sedang *running* pada saat itu, kemudian layar *home* (*desktop* depan yang biasanya memuat aplikasi-aplikasi tertentu dan tanggal/waktu). Tanggal/waktu ini sangat penting untuk memastikan seberapa jauh perbedaan antara waktu yang sebenarnya dengan waktu lokal di *handphone*.

Di samping fotografi, dokumentasi juga dilakukan dengan pencatatan merk, model dan hal-hal lain yang berkaitan dengan *handphone* tersebut, misalnya tentang pemilik dan penggunaannya.

c. Bangun suatu area tanpa sinyal, bisa dengan menggunakan kantong *Faraday* (suatu kantong yang terbuat dari bahan tertentu untuk meminimalisir sinyal frekwensi radio *handphone*) atau *jammer* (suatu peralatan untuk mengacak sinyal frekwensi radio). Selanjutnya bawa barang bukti *handphone* tersebut ke area tersebut. Ini dilakukan agar selama proses pemeriksaan forensik terhadap *handphone* tersebut, *handphone* tersebut tidak memiliki sinyal frekwensi radio sehingga tidak ada *incoming calls* (panggilan masuk) atau SMS *inbox* (masuk) ke *handphone* tersebut. Ini dimaksudkan agar isi dari *handphone* tersebut benar-benar tetap terjaga dan tidak terkontaminasi dengan hal-hal tersebut di atas.
d. Akses nomor IMEI dari *handphone* tersebut dengan mengetikkan *#06# yang secara otomatis akan menampilkan nomor IMEI dari handphone tersebut, kemudian lakukan fotografi terhadap layar yang menampilkan nomor IMEI tersebut, di samping mencatatnya.
e. Akses *handphone* dengan *analysis workstation* dengan menggunakan kabel data, *bluetooth* atau *infra red*. Disarankan pengaksesan *handphone* tersebut menggunakan kabel data melalui *port* USB yang sudah terproteksi akses penulisan (*write-protect*).
f. Setelah proses konektifitas dan sinkronisasi melalui instalasi *driver handphone* selesai, *handphone* sudah dapat dikenal oleh *analysis workstation*. Selanjutnya jalankan aplikasi forensik misalnya MOBILedit *Forensic* dari Compelson seperti yang terlihat pada Gambar VII.5 di bawah ini.



Gambar VII.5. Aplikasi MOBILedit Forensic mengakses barang bukti handphone secara physical.

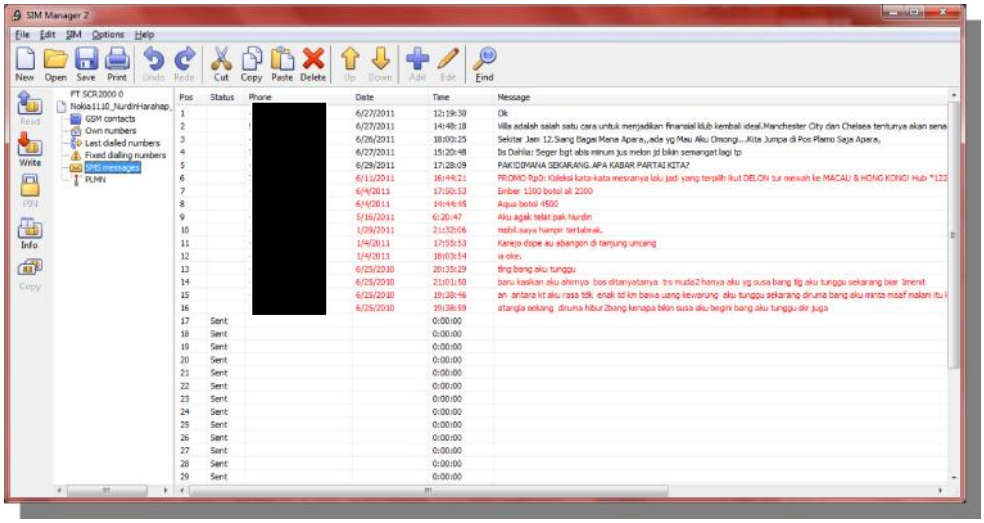
Aplikasi yang men-support banyak merk dan model *handphone* ini didesain untuk dapat melakukan proses *dumping* (mengambil keseluruhan data secara *physical*) terhadap isi dari *handphone* barang bukti, mulai dari *phonebook*, SMS, MMS, *call logs*, *file-file* audio, video, dan gambar-gambar digital, termasuk *file-file* dari sistem operasi dan aplikasi. Hal ini dilakukan secara *physical*, sehingga jika ada *file-file* yang dihapus misalnya SMS, maka masih memungkinkan untuk dilakukan proses *recovery* terhadap SMS-SMS tersebut selama lokasi sektor penyimpanannya belum tertimpa oleh *file-file* yang lain. Pencarian data-data di isi *handphone* disesuaikan dengan maksud investigasi agar pemeriksaan dapat dilakukan secara efektif dan efisien.

Dalam proses pengaksesan *handphone* dengan menggunakan aplikasi *mobile* forensik, *analyst* dan *investigator* seharusnya membuat *file backup* dari proses *dumping* yang sudah dilakukan. Hal ini dimaksudkan untuk memudahkan dalam pencarian data-data yang berkaitan dengan investigasi tanpa perlu mengakses *handphone* lagi. Dengan adanya *file backup* ini, pemeriksaan terhadap isi *handphone* dapat dipindahkan dan dilakukan di *workstation* yang lain oleh analyst

atau *investigator* yang berbeda untuk mendapatkan hasil yang lebih komprehensif.

g. Setelah proses pemeriksaan *handphone* secara forensik selesai dilakukan, matikan *handphone* dengan menekan tombol *power* atau melalui prosedur yang disediakan oleh *handphone*. Setelah itu, cabut batere kemudian lakukan fotografi terhadap label spesifikasi yang berada di sisi dalam handphone yang biasanya memuat merk, model, IMEI dan *serial number* (S/N). untuk IMEI, lakukan pengecekan nomor IMEI yang ada di label dengan yang tertampil di layar setelah pengetikkan *#06#. Jika berbeda, maka salah satu dari nomor IMEI tersebut adalah palsu dan untuk itu diperlukan pengecekan dan pemeriksaan lebih lanjut.

   Dilanjutkan dengan ambil SIM *card* dan catat merk dan nomor ICCID yang ada di SIM *card*. SIM *card* tersebut kemudian dimasukkan ke dalam SIM *card reader* untuk selanjutnya diakses dengan *analysis workstation* melalui *port* USB yang sudah *write-protect*. Jalankan aplikasi forensik misalnya SIM *Manager* dari Dekart untuk pemeriksaan SIM *card* tersebut seperti yang terlihat pada Gambar VII.6. Dapatkan semua data yang tersimpan di dalam SIM *card* melalui proses *dumping* termasuk SMS-SMS yang sudah dihapus (*deleted*) dan nomor ICCID serta IMSI. Setelah itu *analyst* dan *investigator* seharusnya juga membuat *file backup* dari isi SIM *card* tersebut. Setelah semua proses itu selesai, ambil kembali SIM *card* dari *reader*-nya kemudian masukkan kembali ke *slot handphone*-nya.



Gambar VII.6. Aplikasi SIM *Manager* dari Dekart yang digunakan untuk pemeriksaan forensik SIM *card* menghasilkan banyak informasi termasuk *deleted* SMS (yang diberi warna merah).

h. Untuk memori eksternal (jika ada), cabut memori tersebut dari slot *handphone*-nya kemudian masukkan memori tersebut ke *reader* dan lakukan pengaksesan dengan *analysis workstation* melalui *port* USB yang sudah *write-protect*. Setelah itu lakukan proses *forensic imaging* secara *physical bit* per *bit* seperti yang sempat dibahas di Bab II tentang *Digital Forensic: Principles and Procedures* untuk mendapatkan *image file yang* isinya identik sektor per sektor dengan isi dari memori eksternal *handphone* tersebut. Selanjutnya *image file* tersebut diperiksa dan dianalisa dengan menggunakan aplikasi forensik secara mendalam untuk mendapatkan data-data yang berkaitan dengan investigatif.

i. Setelah semua proses pemeriksaan tersebut selesai, SIM *card* dan memori eksternal dimasukkan kembali ke *slot*-nya masing-masing, sehingga kembali menjadi satu kesatuan yang utuh sebagai barang bukti. Jangan pernah menghidupkan kembali *handphone* berikut SIM *card* dan memori eksternal tersebut kecuali di area tanpa sinyal dan untuk kebutuhan pemeriksaan *cross-check* dari pihak ketiga.

j. Hasil dari proses pemeriksaan *handphone*, SIM *card* dan memori ekternal tersebut di atas, baik *softcopy* maupun *hardcopy* diberikan

kepada *investigator* yang berkompeten dengan kasus agar ia dapat menelaah lebih jauh, mana informasi yang berkaitan dengan investigasi dan mana yang tidak. Selanjutnya informasi yang berkaitan dengan investigasi dimasukkan/dituangkan ke dalam laporan hasil pemeriksaan forensik.

k. Untuk *handphone* yang batere-nya hampir habis (*low battery*), sebaiknya dicarikan *charger* (peralatan pengecas) untuk memberikan atau menambah daya batere. Jika *charger* untuk tipe *handphone* tersebut tidak dapat ada dan batere sangat low, maka handphone tersebut dapat dimatikan dan untuk proses pemeriksaan selanjutnya dianggap sebagai barang bukti *handphone* dalam keadaan *off*.

2. Handphone dalam keadaan *off* (mati)

Tahapan berikut merupakan prosedur pemeriksaan untuk barang bukti handphone yang ditemukan atau disita dari pelaku dalam keadaan mati.

a. Untuk pemeriksaan awal, jangan menghidupkan kembali *handphone*!
b. Lakukan fotografi forensik dengan mengambil gambar umum, medium dan *close up*. Untuk foto *close up*, lakukan fotografi dari depan dan belakang, termasuk label yang memuat merk, model, IMEI dan S/N, yang berada di sisi dalam belakang setelah batere dicabut.
c. Setelah cabut batere, ambil SIM *card*, catat nomor ICCID dan lakukan pemeriksaan secara forensik terhadap SIM *card* seperti yang telah dijelaskan pada poin g sebelumnya.
d. Jika memori eksternal ada, cabut dan pasang memori tersebut di *reader* untuk kemudian diakses dengan *analysis workstation* melalui *port* USB yang sudah *write-protect*. Selanjutnya lakukan proses *forensic imaging*, pemeriksaan dan analisa seperti yang dijelaskan pada poin h di atas.
e. Bangun area tanpa sinyal frekwensi radio, baik menggunakan kantong *Faraday* maupun *jammer* seperti yang telah dijelaskan pada poin c di atas.

f. Masukkan kembali SIM *card* dan memori eksternal termasuk batere (pastikan batere memiliki daya listrik yang cukup) ke slot *handphone*-nya masing-masing, kemudian hidupkan *handphone*. Pastikan *handphone* tersebut tidak memiliki sinyal frekwensi radio agar isi *handphone* tetap terjaga dan tidak terkontaminasi dengan *incoming calls* dan SMS *inbox* selama proses pemeriksaan berlangsung. Ketikkan *#06# untuk mendapatkan nomor IMEI dari *handphone* tersebut. Lakukan pengecekan nomor IMEI ini dengan yang tertera di label.
g. Setelah itu, lakukan pemeriksaan forensik terhadap *handphone* tersebut seperti yang dijelaskan pada poin f di atas.
h. Pemeriksaan SIM card, *handphone* dan memori eksternal sebaiknya menghasilkan *file backup* atau *image file* masing-masing. Ini dimasudkan untuk memudahkan pemeriksaan lanjutan secara mendalam terhadap isi barang bukti tersebut, baik oleh *analyst* dan *investigator* itu sendiri maupun oleh pihak ketiga untuk tujuan *cross-check*.
i. Setelah selesai semua proses pemeriksaan SIM *card*, memori eksternal dan *handphone*, *handphone* dimatikan lewat tombol *power* atau lewat prosedur yang diberikan oleh *handphone*. Hasil pencarian data-data, baik *softcopy* maupun *hardcopy* selanjutnya diberikan kepada *investigator* yang berkompeten untuk memilah dan memastikan mana data yang berkaitan dengan investigasi dan mana yang tidak. Data yang berkaitan dengan investigasi nantinya dimasukkan dalam laporan hasil pemeriksaan forensik.

Bibliography

1. ACPO, 7Safe (2008). *Good Practice Guide for Computer-Based Electronic Evidence*. UK ACPO and 7Safe.
2. Al-Azhar, M.N. (2010). *Standard Operating Procedure (SOP) 10 : Akuisisi Handphone dan SIM Card*. DFAT Puslabfor.

3. Al-Azhar, M.N. (2010). *Standard Operating Procedure (SOP) 11 : Analisa Handphone dan SIM Card*. DFAT Puslabfor.
4. Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Elsevier Academic Press.
5. EC-Council. (2010). *CHFI module 38: Cell Phone Forensic*. EC-Council.
6. ECTEG (European Cybercrime Training & Education Group). (2009). *Introduction to GSM and 3G Mobile Networks*. ECTEG.
7. ECTEG. (2009). *Introduction to Mobile Devices & their Components*. ECTEG.
8. ECTEG. (2009). *Seizure and handling*. ECTEG.
9. ECTEG. (2009). *SIM/UICC*. ECTEG.
10. Johnson, T. A. (2005). *Forensic Computer Crime Investigation*. Taylor & Francis.
11. Middleton, B. (2002). *Cyber Crime Field Handbook*. CRC Press
12. National Institute of Justice (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. US National Institute of Justice
13. National Institute of Justice (2001). *Electronic Crime Scene Investigation: A Guide for First Responder*. US National Institute of Justice.
14. Sammes, T. and Jenkinson, B. (2007). *Forensic Computing: A Practitioner's Guide*. Springer.
15. Solomon, M. G. et al. (2005). *Computer Forensics Jumpstart*. Sybex.

Bab VIII

AUDIO FORENSIC: Theory and Analysis

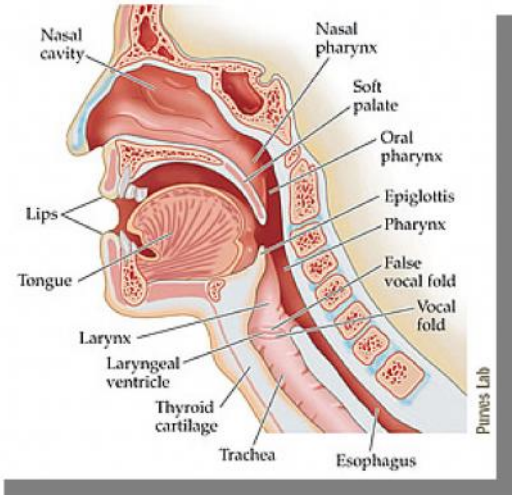
Salah satu barang bukti elektronik yang ditemukan di TKP atau yang berkaitan dengan kasus, baik pidana maupun perdata adalah barang bukti *audio recorder* (alat rekam suara) yang menghasilkan rekaman suara pembicaraan seseorang dengan orang lain. Rekaman suara pembicaraan yang merupakan barang bukti digital ini, pada kasus-kasus tertentu memiliki peranan yang sangat penting untuk pengungkapan kasus atau menunjukkan keterlibatan seseorang dengan kasus yang sedang diinvestigasi. Dari rekaman suara, terdengar percakapan seseorang dengan orang lain. Orang-orang tersebut dapat diketahui identitasnya melalui pemeriksaan audio forensik untuk *voice recognition* dengan metode komparasi, yaitu membandingkan suara di dalam rekaman barang bukti (*unknown samples*) dengan suara yang direkam sebagai pembanding (*known samples*). Jika hasil *voice recognition* menunjukkan bahwa suara *unknown samples* adalah identik dengan suara *known samples*, maka suara percakapan di dalam rekaman barang bukti dapat disimpulkan berasal dari pemilik suara pembanding.

Dengan prosedur penanganan barang bukti rekaman suara yang benar yang kemudian dilanjutkan dengan pemeriksaan dan analisanya yang prosedural, diharapkan hasil pemeriksaan audio forensik untuk *voice recognition* dapat menunjukkan secara ilmiah kepemilikan suara yang ada di dalam rekaman tersebut untuk disajikan sebagai alat bukti yang kuat di pengadilan.

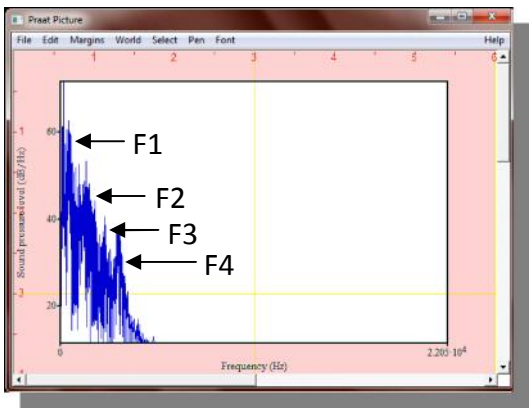
Bab ini mencoba membahas teori suara dan tahapan-tahapan analisa *voice recognition* terhadap contoh suara yang berasal dari rekaman barang bukti (*unknown samples*) dengan memperbandingkannya dengan contoh suara pembanding (*known samples*) secara komprehensif seperti analisa statistik *One Way* Anova (*Analysis of Variance*) terhadap *pitch*, *formant* dan *formant bandwidth*, serta analisa spektrogram yang didasarkan pada pola khas *formant*. Di samping itu, juga dibahas bagaimana melakukan pengambilan contoh (*sampling*) suara pembanding.

Teori Suara

Suara dihasilkan melalui proses *Generation* dan *Filtering*. Pada proses *Generation*, suara pertama kali diproduksi melalui bergetarnya pita suara (*vocal cord* atau *vocal fold*) yang berada di *larynx* untuk menghasilkan bunyi periodik. Bunyi periodik yang bersifat konstan tersebut kemudian di-filterisasi melalui *vocal tract* (juga disebut dengan istilah resonator suara atau *articulator*) yang terdiri dari lidah (*tongue*), gigi (*teeth*), bibir (*lips*), langit-langit (*palate*) dan lain-lain sehingga bunyi tersebut dapat menjadi bunyi keluaran (*output*) berupa bunyi vokal (*vowel*) dan atau bunyi konsonan (*consonant*) yang membentuk kata-kata yang memiliki arti yang nantinya dapat dianalisa untuk *voice recognition*.



Gambar VIII. 1. *Human vocal tract*. (sumber: http://www.dukemagazine.duke.edu/issues/050608/images/050608-lg-figure1purves.jpg)



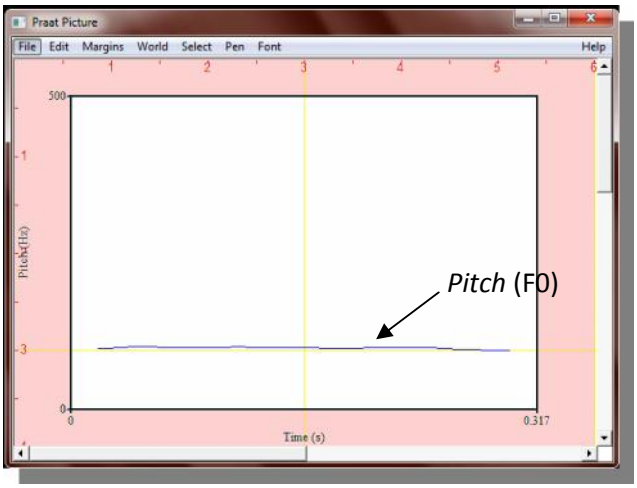
Gambar VIII. 2. Suara Keluaran (*output*) setelah melalui filterisasi *vocal tract*.

Komponen Suara

Suara terdiri dari beberapa komponen, yaitu *pitch*, *formant* dan *spectrogram* yang dapat digunakan untuk mengidentifikasi karakteristik suara seseorang untuk kepentingan *voice recognition*.

1. *Pitch*

   Frekwensi getar dari pita suara yang juga disebut dengan istilah frekwensi fundamental (dasar) dengan notasi F0. Masing-masing orang memiliki *pitch* yang khas (*habitual pitch*) yang sangat dipengaruhi oleh aspek fisiologis *larynx* manusia. Pada kondisi pembicaraan normal, level *habitual pitch* berkisar pada 50 s/d 250 Hz untuk laki-laki dan 120 s/d 500 Hz untuk perempuan. Frekwensi F0 ini berubah secara konstan dan memberikan informasi linguistik seseorang seperti perbedaan intonasi dan emosi.

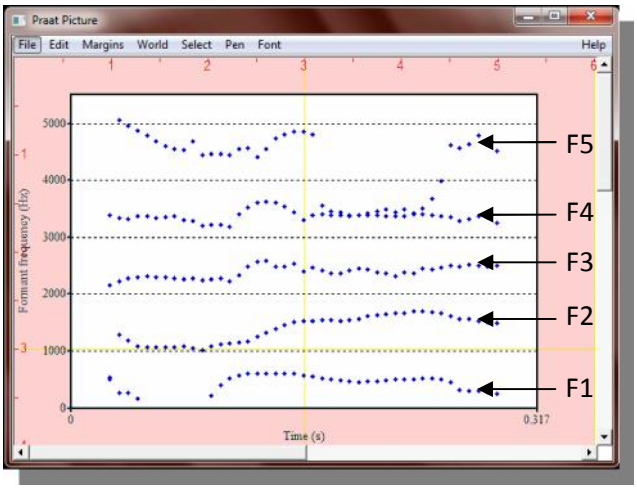


Gambar VIII.3. Diagram *pitch* terhadap waktu yang berubah secara konstan.

Analisa *pitch* dapat digunakan untuk melakukan *voice recognition* terhadap suara seseorang, yaitu melalui analisa statistik terhadap minimum *pitch*, maximum *pitch* dan mean *pitch*. Meskipun begitu, analisa statistik sederhana ini tidak berpengaruh banyak ketika kondisi suara seseorang yang berbicara di rekaman barang bukti jauh berbeda dengan kondisi pengambilan suara pembanding.

2. *Formant*

Formant adalah frekwensi-frekwensi resonansi dari filter, yaitu *vocal tract (articulator)* yang meneruskan dan memfilter bunyi periodik dari getarnya pita suara (*vocal cord*) menjadi bunyi keluaran (*output*) berupa kata-kata yang memiliki makna. Secara umum, frekwensi-frekwensi *formant* bersifat tidak terbatas, umumnya tergambar mulai dari *Formant* 1 (F1) sampai dengan *Formant* 5 (F5), namun untuk identifikasi suara seseorang, paling tidak ada 3 (tiga) *formant* yang dianalisa, yaitu *Formant* 1 (F1), *Formant* 2 (F2) dan *Formant* 3 (F3).



Gambar VIII. 4. Diagram masing-masing *formant* F1, F2, F3, F4 dan F5.

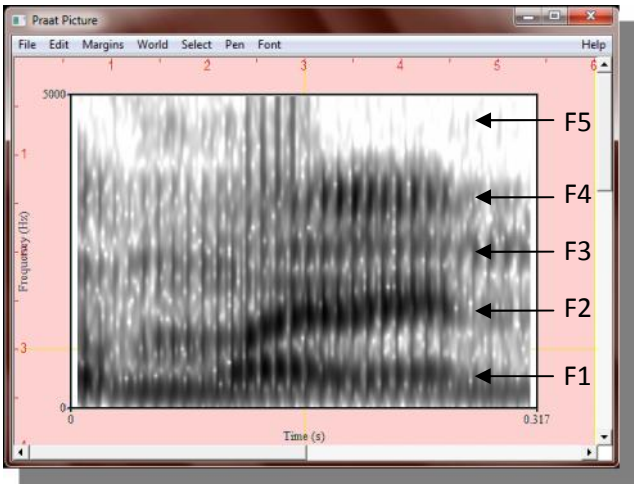
Selain gambar di atas, gambar 2 juga menunjukkan spektrum suara berbasis nilai masing-masing *formant*.

3. *Spectrogram*

Spectrogram merupakan representasi spectral yang bervariasi terhadap waktu yang menunjukkan tingkat *density* (intensitas energi) *spektral*. Dengan kata lain *spectrogram* adalah bentuk visualisasi dari masing-masing nilai *formant* yang dilengkapi dengan level energi yang bervariasi terhadap waktu. Level energy ini dikenal dengan istilah *formant bandwidth.* Nantinya pada kasus-kasus yang bersifat pemalsuan suara dengan teknik *pitch shift* atau si subyek berusaha untuk menghilangkan

karakter suara aslinya, maka *formant bandiwidth* dapat digunakan untuk memetakan atau mengidentifikasi suara aslinya. Dikarenakan *spectrogram* memuat hal-hal yang bersifat detil dalam hal pola khas *formant* dan *bandwidth*, maka *spectrogram* oleh beberapa ahli juga dikenal dengan istilah sidik jari suara (*voice fingerprint*). Walaupun begitu pengistilahan *spectrogram* sebagai sidik jari suara juga mendapat tentangan dari ahli-ahli lain. Mereka berpendapat bahwa yang namanya sidik jari itu bersifat unik dan sulit untuk berubah, sedangkan *spectrogram* itu sendiri dapat berubah atau berbeda untuk pengucapan kata yang sama walaupun berasal dari orang yang sama. Namun mereka sependapat bahwa untuk analisa identifikasi suara, *spectrogram* perlu dianalisa karena ia menampilkan visualisasi detil dari *formant* berikut *bandwidth*-nya sehingga membentuk pola-pola pengucapan kata yang khas untuk masing-masing nilai *formant*.

Spectrogram membentuk pola umum yang khas dalam pengucapan kata dan pola khusus masing-masing *formant* dalam pengucapan suku kata, sehingga *spectrogram* juga digunakan untuk melakukan analisa identifkasi suara seseorang.



Gambar VIII. 5. *Spectrogram* menunjukkan representasi spektral dengan tingkatan energinya.

Jika durasi rekaman suara *unknown* lumayan panjang, maka analisa *spectrogram* juga dapat digunakan untuk mempercepat pemilihan

pengucapan kata-kata yang akan dianalisa dalam rangka untuk mendapatkan jumlah minimal 20 kata untuk dapat menunjukkan ke-identik-an suara *unknown* dengan *known* (pembanding).

Prosedur Audio Forensic

Untuk melakukan analisa suara seseorang dalam rangka mengidentifikasi suara yang berasal dari rekaman barang bukti dan memverifikasinya dengan suara pembanding, berikut adalah tahapan-tahapan yang digunakan sesuai dengan *Standard Operating Procedure* (SOP) 12 tentang Analisa Audio Forensik dari *Digital Forensic Analyst Team* (DFAT) Puslabfor yang mengacu salah satunya kepada *Spectrographic Voice Identification: A Forensic Survey* yang dikeluarkan oleh FBI (*Federal Bureau of Investigation*), Amerika Serikat.

1. ***Acquisition***
    1) Catat spesifikasi teknis *audio recorder* seperti merk, model, ukuran dan *serial number*, dilanjutkan dengan foto bagian depan dan belakan *recorder*. Untuk pemotretan barang bukti, harus dilengkapi dengan label 'Puslabfor' dan skala ukur.
    2) Sebelum melakukan langkah-langkah audio forensik lebih lanjut, pemeriksa harus terlebih dahulu mendapatkan fakta kasus yang berkaitan dengan barang bukti rekaman suara dari penyidik dengan melakukan gelar perkara terhadap kasus tersebut.
    3) Selain fakta kasus, pemeriksa juga harus sudah mendapatkan suara pembanding (*control* atau *unknown samples*) terhadap suara yang ada di dalam *audio recorder* yang akan dianalisa dan dilengkapi dengan administrasi penyidikan yang lengkap. Pengambilan contoh suara pembanding ini dapat dilakukan oleh penyidik atau pemeriksa di dalam lingkungan yang bebas dari suara *noise*. Pengambilan contoh suara pembanding ini juga harus dilengkapi dengan Berita Acara Pengambilan Contoh Suara Pembanding yang disetujui dan ditandatangani oleh subyek yang contoh suaranya

akan dianalisa.

4) Pengambilan contoh suara pembanding juga dapat dilakukan dari rekaman video asli yang menunjukkan subyek dalam berbicara. Rekaman video ini harus berasal dari sumber yang jelas dan resmi.
5) Untuk proses akuisisi *audio recorder* yang menghasilkan *file dd image* mengikuti langkah-langkah seperti yang dijelaskan pada Bab II tentang *Digital Forensic: Principles and Procedures*.
6) Setelah mendapatkan *file dd image* yang IDENTIK dengan isi dari *audio recorder*, *file dd image* tersebut dilakukan proses *logical mounting* untuk melihat isi dari *audio recorder* tersebut.
7) Proses *mounting* bisa dilakukan di komputer analisis baik yang berbasis Ms. Windows maupun Linux Ubuntu. Sebelum *proses mounting*, harus dipastikan bahwa *file dd image* telah di-set *read-only*, dan dalam proses *mounting* itu sendiri, harus dalam lingkungan yang *forensically-sound write protect*. Untuk yang berbasis Ms. Windows dapat menggunakan aplikasi digital forensik yang telah teruji untuk lingkungan tersebut, sedangkan untuk yang berbasis Linux, dapat menggunakan perintah '*mount –o ro,loop File_Image.dd*'.
8) Setelah di-*mounting* dalam lingkungan tersebut, pemeriksa dapat melakukan proses *keyword searching*, *file content checking* atau *file recovery* untuk dapat menemukan rekaman suara yang dicari.
9) *File* yang berisikan rekaman suara barang bukti kemudian di-ekspor dan diekstraksi metadata-nya untuk dianalisa lebih lanjut untuk mendapatkan historis teknis dari *file* rekaman tersebut termasuk keaslian *file* rekaman yang juga dapat diperiksa melalui *spectrum analysis*.

2. Audio Enhancement

1) Rekaman suara barang bukti diperdengarkan (*playback*) untuk melihat kualitas rekaman. Jika kualitasnya tidak bagus dikarenakan banyak suara *noise*, maka terhadap rekaman suara tersebut harus

dilakukan proses *enhancement* untuk menaikkan kualitas rekaman sehingga pembicaraan yang ada di dalam rekaman suara tersebut dapat didengar dengan jelas.

2) Proses *enhancement* ini dapat dilakukan di komputer analisis berbasis Ms. Windows dan Linux dengan didukung aplikasi-aplikasi audio yang dapat diandalkan untuk pemrosesan yang efisien dan efektif. Sebagian aplikasi ini bahkan dapat menghilangkan suara noise yang kuat sehingga memunculkan kembali suara pembicaraan yang ada.
3) Pelaksanaan proses *enhancement* ini mengikuti petunjuk (manual) dari aplikasi-aplikasi tersebut.

3. Decoding

a. Setelah suara pembicaraan yang berasal dari rekaman barang bukti jelas, dilanjutkan dengan pembuatan transkrip rekaman.
b. Pembuatan transkrip rekaman harus dilakukan oleh minimal 2 (dua) orang pemeriksa. Ini dimaksudkan untuk mendapatkan nilai akurasi yang lebih presisi terhadap hasil transkrip.
c. Transkrip rekaman harus mencantumkan label subyek (misalnya; subyek 1, subyek 2 dan seterusnya) dan waktu (dalam jam:menit:detik) yang sesuai dengan berjalannya rekaman. Interval penandaan waktu dapat disusun setiap 30 detik atau 1 menit.
d. Jika suara pembicaraan di dalam rekaman tersebut tidak jelas, maka ditulis 'tidak jelas'. Artinya hasil transkrip hanya memperlihatkan suara pembicaraan yang jelas dan dapat dipahami pengucapan kata-katanya.

4. Voice Recognition

1) Proses ini untuk memastikan apakah suara yang ada di dalam rekaman barang bukti adalah IDENTIK dengan contoh suara pembanding. Untuk itu proses ini mengambil kata-kata yang

pengucapannya sama antara suara barang bukti dengan suara pembanding. Terhadap kata-kata tersebut dilakukan analisa audio forensik yang berbasiskan analisa terhadap *pitch*, *formant*, *formant bandwidth* dan *spectrogram*.

2) Disyaratkan minimal 20 (duapuluh) kata yang memiliki kesamaan antara suara barang bukti dan suara pembanding dari hasil analisa *pitch*, *formant*, *bandwidth* dan *spectrogram*, untuk menentukan apakah suara barang bukti IDENTIK dengan suara pembanding. Ini merujuk pada '*Spectrographic Voice Identification: A Forensic Survey*' yang disusun oleh Koenig, B.E. dari Federal Bureau of Investigation.
3) Jika jumlah kata yang diucapkan dalam rekaman barang bukti tidak mencapai minimal 20 (duapuluh) kata, maka status rekaman suara barang bukti adalah TIDAK MEMENUHI SYARAT AUDIO FORENSIK. Selanjutnya tidak dapat dilakukan analisa *voice recognition*.
4) Analisa *pitch* didasarkan pada perhitungan statistik nilai *pitch* minimum, maksimum dan rata-rata (*mean*) serta *standard deviation* yang dilengkapi dengan grafiknya antara suara barang bukti dengan suara pembanding. Meskipun begitu, analisa *pitch* yang lebih lengkap dapat menggunakan metode perhitungan statistik *One-Way* Anova sehingga perbandingan dua kelompok data pitch antara suara barang bukti (*unknown*) dengan suara pembanding (*known*) dapat diketahui secara akurat.
5) Analisa *formant* dan *formant bandwidth* didasarkan pada perhitungan statistik *One-Way* Anova yang dilengkapi dengan bentuk *graphical distribution* untuk melihat pola penyebaran nilai antara suara barang bukti dengan suara pembanding. Analisa *formant* dan *bandwidth* ini meliputi *formant* 1, *formant* 2, dan *formant* 3.
6) Analisa *spectrogram* didasarkan pada pola umum dan pola khusus yang bersifat khas antara suara barang bukti dan suara pembanding. Pola-pola yang khas ini meliputi *formant* 1, *formant* 2

dan *formant* 3 yang disertai level energi (*bandwidth*) pada masing-masing *formant*. Dikarenakan *spectrogram* dapat mem-visualisasikan secara lengkap masing-masing *formant* dan *bandwidth* dari kata yang diucapkan secara konsisten, maka analisa *spectrogram* sangat penting dalam penentuan akhir analisa *voice recognition*.

Sampling Suara Pembanding

Untuk memastikan apakah suara yang ada pada rekaman suara barang bukti adalah IDENTIK atau TIDAK IDENTIK dengan suara orang lain atau subyek, maka perlu untuk dilakukan pengambilan (*Sampling*) contoh suara pembanding yang berasal dari suara si subyek. Pengambilan contoh suara pembanding ini dapat dilakukan oleh pemeriksa ahli Audio Forensik atau investigator. Berikut adalah teknik *sampling* suara pembanding.

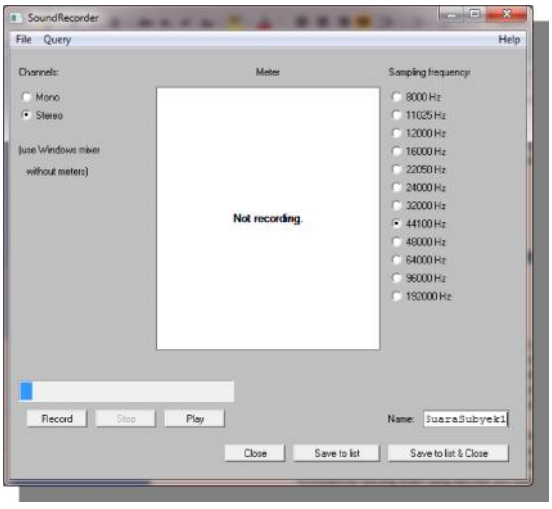
a. Siapkan administrasi pengambilan contoh suara pembanding yaitu berupa 'Berita Acara Pengambilan Contoh Suara Pembanding' yang bersifat Pro Justisia. Pada Berita Acara tersebut, harus dituliskan bahwa 'subyek dalam keadaan sehat jasmani dan rohani dan pada pengambilan contoh suara pembanding dari subyek, tidak ada paksaan dari pihak manapun'. Ini dimaksudkan untuk mengantisipasi dan memperjelas kondisi pada saat pengambilan contoh suara pembanding ketika di persidangan. Tunjukkan Berita Acara tersebut kepada subyek dan biarkan subyek membacanya sampai selesai agar subyek paham bahwa pengambilan contoh suaranya untuk kepentingan investigasi.
b. Siapkan ruangan tempat pengambilan contoh suara yang minim suara luar, kalau bisa ruangan kedap suara seperti Audio Forensic Lab di DFAT Puslabfor. Ini dimaksudkan agar kualitas contoh suara pembanding yang didapat baik dan minim suara luar (*noise*) sehingga dapat langsung digunakan untuk analisa lebih lanjut tanpa perlu dilakukan pengayaan (*enhancement*) terlebih dahulu

c. Siapkan naskah transkrip yang berasal dari proses *Decoding* sebelumnya. Minta kepada subyek untuk membaca naskah transkripnya dengan JELAS dan INTONASI NORMAL minimal sebanyak 2 (dua) kali sambil direkam. Perekaman dapat dilakukan dengan *audio digital recorder,* atau menggunakan aplikasi komputer, atau menggunakan keduanya.
d. Setelah selesai pengambilan contoh suara, subyek diminta untuk menandatangani Berita Acara tersebut.

Sampling dan Analysis dengan Praat

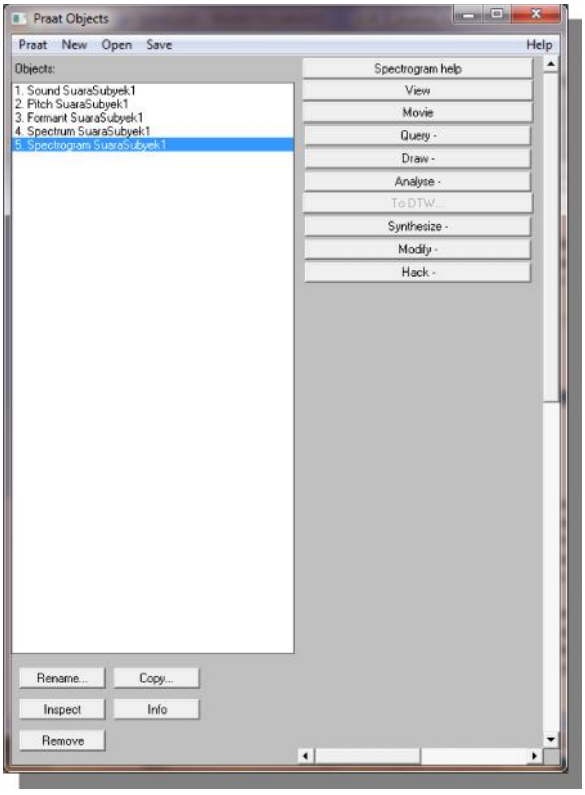
Berikut ini adalah teknik sampling dengan menggunakan aplikasi Praat yang berasal dari *University of Amsterdam*, Belanda.

1. Klik Praat.exe sampai masuk ke jendela *Praat Object*. Klik *New – Record Stereo Sound*. Klik *Record* untuk memulai perekaman. Pada contoh ini, subyek mengucapkan kalimat 'saya pasti bisa'. Setelah selesai, klik *Stop* dan *Play* untuk mendengarkan hasil perekaman. Setelah dipastikan kualitas rekamannya bagus, maka beri nama pada tab *Name*, misalnya SuaraSubyek1, kemudian klik *Save to list & Close*.



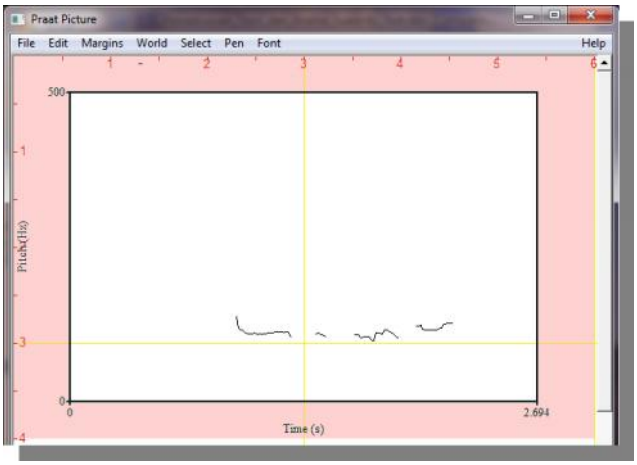
Gambar VIII. 6. *Screenshot* untuk pengambilan contoh suara pembanding.

2. Pada jendela *Praat Objects*, terlihat *Sound* SuaraSubyek1. Klik *Save* – *Save as WAV* (*Windows Audio Video*) *file*, pilih tempat penyimpanan *file* WAV tersebut di computer.
3. Klik *Periodicity* – *To Pitch* – OK, di *Praat Objects* akan terlihat *Pitch* SuaraSubyek1 yang merupakan matrikulasi nilai *pitch* dari contoh suara tersebut. Masih pada *Sound* SuaraSubyek 1, klik *Formants & LPC* – *To Formant* (*burg*) – OK, di *Praat Objects* akan terlihat *Formant* SuaraSubyek1 yang merupakan matrikulasi nilai *formant* 1, 2, 3, 4 dan 5 dari contoh suara tersebut. Masih pada *Sound* SuaraSubyek1, klik *Spectrum* – *To Spectrum* – OK. Pada *Praat Objects*, akan terlihat *Spectrum* SuaraSubyek1 yang merupakan bentuk *spectrum* dari contoh suara setelah proses filterisasi di *vocal tract.* Masih pada *Sound* SuaraSubyek1, klik *Spectrum* – *To Spectrogram* – OK. Pada *Praat Objects*, akan terlihat *Spectrogram* SuaraSubyek1 yang menunjukkan pola *spectrogram* dari contoh suara tersebut.



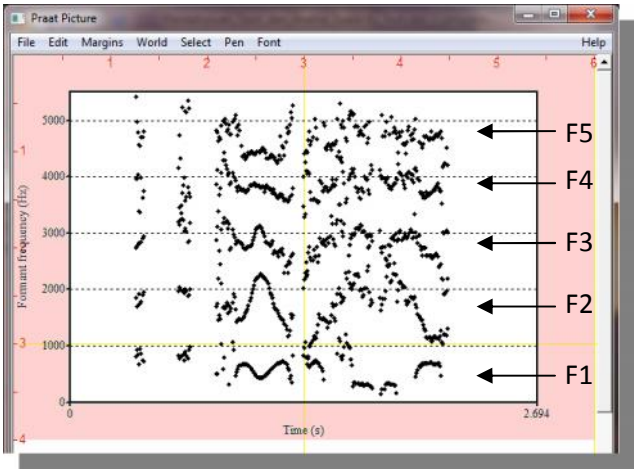
Gambar VIII. 7. *Screenshot Praat Objects*.

4. Pada masing-masing *Pitch*, *Formant*, *Spectrum* dan *Spectrogram* dari SuaraSubyek1 disimpan dengan klik *Save* – *Save as binary file*, yang nantinya akan dapat langsung dianalisa tanpa perlu *Sound* SuaraSubyek1.
5. Pada *Pitch* SuaraSubyek1, klik *Draw* – *Draw* – OK. Pada *Praat Picture*, akan terlihat grafik *pitch* dari contoh suara tersebut ketika mengucapkan kalimat 'saya pasti bisa'.



Gambar VIII. 8. *Screenshot Praat Picture* dari *pitch*

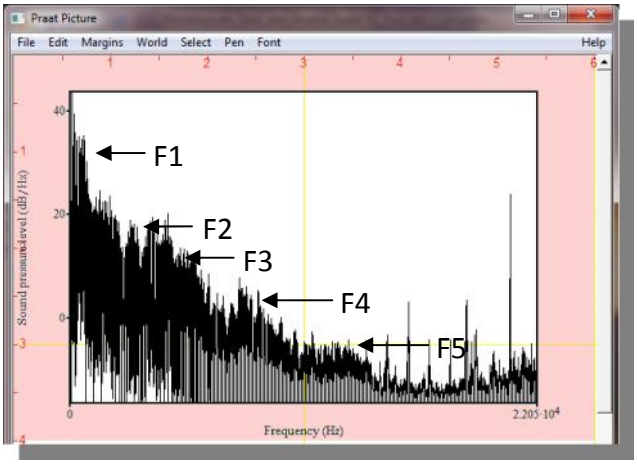
Begitu juga dengan *Formant* SuaraSubyek1, klik *Draw- Speckle* – OK. Akan terlihat *formant* 1, 2, 3, 4 dan 5 pada pengucapan kalimat 'saya pasti bisa'.



Gambar VIII. 9. *Screenshot Praat Picture* dari *formant*.

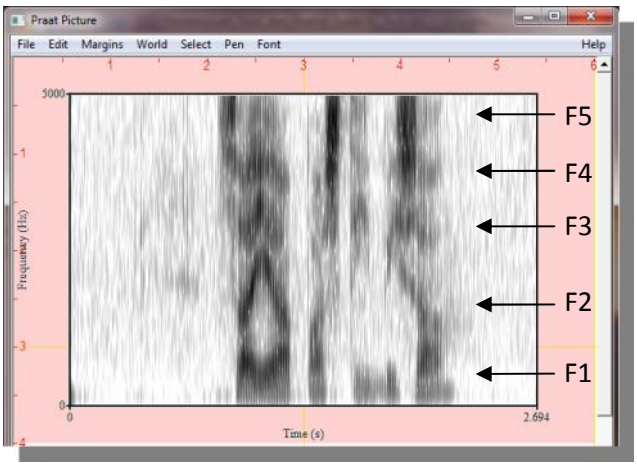
Begitu juga dengan *Spectrum* SuaraSubyek1, klik *Draw* – *Draw* – OK. Akan terlihat grafik *spectrum* hasil filterisasi bunyi periodik yang dihasilkan oleh

getarnya pita suara oleh *vocal tract* atau *articulator* pada pengucapan kalimat ‘saya pasti bisa’.



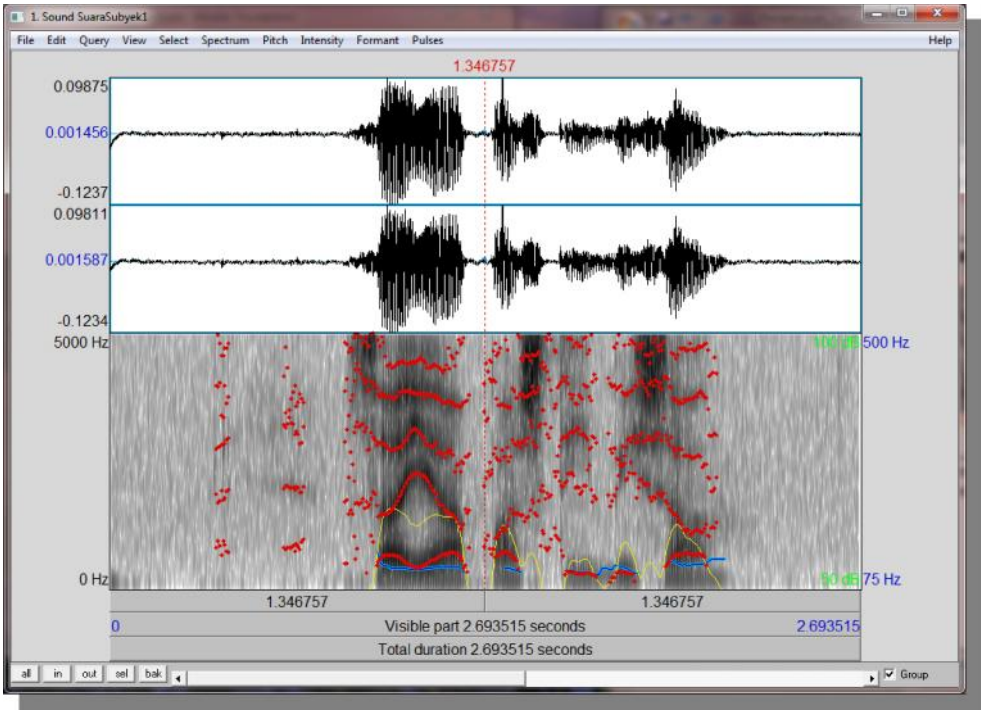
Gambar VIII.10. *Screenshot Praat Picture* dari *spectrum*

Begitu juga dengan *Spectrogram* SuaraSubyek1, klik *Draw* – *Paint* – OK. Akan terlihat bentuk visualisasi grafis nilai masing-masing *formant* berikut level energinya (*bandwidth*) yang pada masing-masing kata atau suku kata membentuk pola-pola yang khas pada masing-masing *formant* dan *bandwidth*. Pada contoh ini adalah pengucapan kalimat ‘saya pasti bisa’.



Gambar VIII.11. *Screenshot Praat Picture* dari spektrogram.

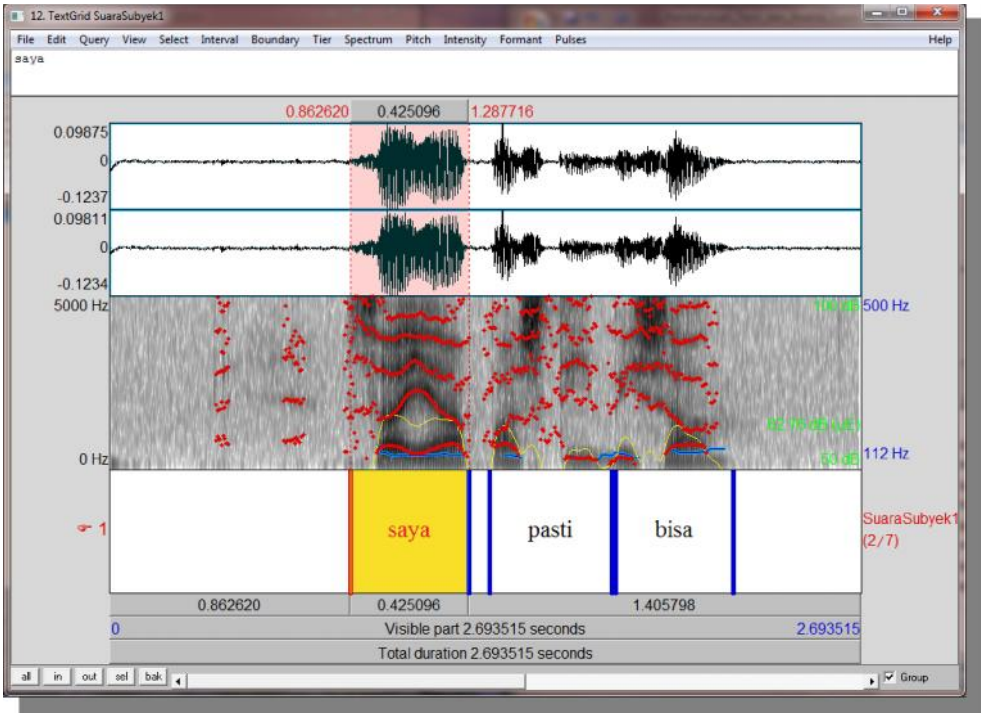
6. Untuk melihat secara komprehensif *Sound* SuaraSubyek1 berikut dengan komponen-komponen suaranya seperti *pitch*, *formant*, *spectrogram* dan lain-lain, klik *View* & *Edit*.



Gambar VIII.12. *Screenshot Praat Window* yang menampilkan spektrogram, *formant*, *pitch* dan *intensity* secara bersamaan.

Grafik yang berwarna merah menunjukkan *formant*, grafik yang berwarna biru menunjukkan *pitch*, dan grafik yang berwarna kuning menunjukkan *intensity*, sedangkan jendela bagian atas menunjukkan frekwensi pengucapan kalimat dalam bentuk *stereo* (2 *channels*).

7. Untuk memberikan anotasi (penandaan) pengucapan pada kata dan suku kata tertentu, klik *Annotate – To TextGrid*, pada *All tier names* diisi SuaraSubyek1 dan pada *which of these are point tiers* ? dikosongkan, kemudian klik OK, nantinya pada *Praat Objects* akan terlihat TextGrid SuaraSubyek1. Selanjutnya *Sound* SuaraSubyek1 dan TextGrid SuaraSubyek1 diblok dengan diklik bersama dengan tanda *Control*, kemudian klik *View* & *Edit* untuk melihat dan memberi anotasinya. Blok *spectrum* yang menunjukkan pengucapan kata atau suku kata tertentu yang pada contoh suara pembanding ini adalah ‘saya’, ‘pasti’ dan ‘bisa’. Setelah diblok kemudian tekan *Enter*, kemudian pada masing-masing blok, klik dan ketik ‘saya’, ‘pasti’ dan ‘bisa’.



Gambar VIII.13. *Screenshot Praat Window* yang menampilkan teks untuk kata yang diucapkan

8. Untuk membantu pemahaman dalam *voice recognition* yang akan dibahas selanjutnya, maka diambil *sampling* (contoh suara) yang dalam hal ini dianggap sebagai suara yang berasal dari rekaman suara barang bukti. Pengambilan contoh suara tersebut mengikuti langkah-langkah seperti yang telah dijelaskan sebelumnya, yang dalam contoh kasus ini adalah dengan menggunakan aplikasi Praat. Setelah perekaman suara selesai, maka *file* rekaman tersebut disimpan dengan nama *file* SuaraBarangBukti.wav. Selanjutnya dilakukan analisa Praat untuk mendapatkan nilai *pitch*, *formant* dan *spectrogram* untuk SuaraBarangBukti. Masing-masing nilai ini akan digunakan untuk memeriksa dan membandingkan SuaraSubyek1 dan SuaraBarangBukti dengan analisa statistic *pitch*, *formant*, *bandwidth*, *graphical distribution* dan *spectrogram* untuk menentukan apakah kedua suara tersebut IDENTIK atau TIDAK IDENTIK.

Analisa Statistik Pitch

Analisa ini didasarkan pada kalkulasi statistik nilai *pitch* dari masing-masing suara *unknown* dan *known*. Karakteristik *pitch* dari masing-masing suara tersebut dibandingkan pada *minimum pitch*, *maximum pitch* dan *mean pitch*.

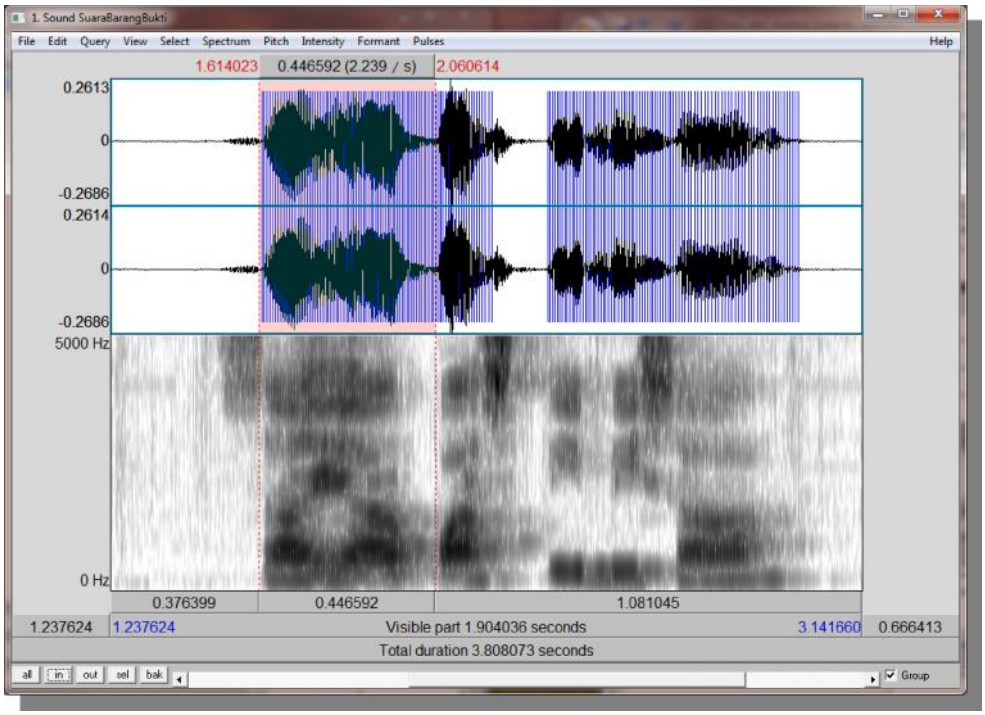
Jika karakteristik *pitch* dari masing-masing suara tersebut menunjukkan tingkat perbedaan yang besar, maka dapat disimpulkan bahwa *pitch* dari suara *unknown* dan *known* adalah berbeda. Biasanya analisa ini juga didukung bentuk grafis *pitch* dari masing-masing suara yang dianalisa seperti yang ditunjukkan pada Gambar 3 di atas.

Pada contoh suara pembanding SuaraSubyek1 seperti yang telah dijelaskan sebelumnya, didapat nilai statistic *Pitch* dengan menggunakan Praat. Pada jendela *Praat Objects*, pilih *Pitch* SuaraSubyek1 yang telah dibuat sebelumnya, atau klik *Open* untuk memilih *file Pitch* SuaraSubyek1. Klik *Query – Get minimum* untuk mendapatkan nilai terkecil *Pitch*, *Get maximum* untuk mendapatkan nilai terbesar *Pitch*, *Get quantile* untuk mendapatkan nilai tengah (*median*) *Pitch*, *Get mean* untuk mendapatkan nilai rata-rata *Pitch*, dan *Get standard deviation* untuk mendapatkan nilai standar deviasi (penyimpangan) *Pitch*, kemudian klik OK, selanjutnya akan muncul jendela *Praat Info* yang menginformasikan nilai yang diminta. Dengan cara yang sama juga dilakukan analisa statistik *pitch* untuk SuaraBarangBukti. Nilai-nilai statistic *pitch* SuaraSubyek1 dan SuaraBarangBukti seperti terlihat pada table di bawah ini.

Analisa Statistik	SuaraBarangBukti (Hz)	SuaraSubyek1 (Hz)
Pitch minimum	115.4152530251853 Hz	98.85551869539509
Pitch maximum	170.91868955661073 Hz	547.401023985919
Pitch quantile	151.7581539283354 Hz	111.12621906912594
Pitch mean	145.81597355408582 Hz	122.21609003576971
Pitch standard deviation	15.691835710766556 Hz	65.92459687770406

Tabel VIII. 1. Analisa Statistik *pitch* pada pengucapan kalimat ‘saya pasti bisa’ antara SuaraBarangBukti dengan SuaraSubyek1.

Untuk analisa *pitch*, *formant* dan *spectrogram* yang lebih detil pada kata-kata yang diucapkan, maka pada *Sound* SuarabarangBukti dan *Sound* SuaraSubyek1 dilakukan pemotongan pada kata ‘saya’, ‘pasti’ dan ‘bisa’. Pada *Praat Objects* pilih *Sound* SuaraBarangBukti, kemudian klik *View* & *Edit*. Blok *spectrum* pada pengucapan kata ‘saya’, kemudian klik *File – save selected sound as WAV file*, dan beri nama, misalnya SuaraBarangBukti-saya.wav dilanjutkan dengan klik *Save*.



Gambar VIII.14. *Screenshot Praat Window* yang menampilkan contoh suara barang bukti dan pembanding, untuk kemudian dipilih per kata-nya untuk dianalisa lebih lanjut.

Lakukan hal yang sama untuk pengucapan kata-kata ‘pasti’ dan ‘bisa’, dan masing-masing di-*save* dengan nama *file* yang menunjukkan pengucapan katanya, misalnya SuaraBarangBukti-pasti.wav dan SuaraBarangBukti-bisa.wav. Masih dengan Praat, ulangi langkah-langkah tersebut untuk *file* SuaraSubyek1.wav. setelah selesai, juga akan didapat *file-file* baru untuk masing-masing kata, yaitu SuaraSubyek1-saya.wav, SuaraSubyek1-pasti.wav dan SuaraSubyek1-bisa.wav.

Pada jendela *Praat Objects*, klik *Open* dan pilih *file* SuaraBarangBukti-saya.wav dan SuaraSubyek1-saya.wav. Pada pengucapan kata ‘saya’ yang sama, akan dilakukan analisa statistik *pitch* lagi yang lebih tajam dengan langkah-langkah

seperti yang telah dijelaskan sebelumnya. Tabel berikut menunjukkan nilai *pitch* yang lengkap untuk masing-masing kata 'saya', 'pasti' dan 'bisa'.

Analisa Statistik	SuaraBarangBukti (Hz)	SuaraSubyek1 (Hz)
Kata 'saya'		
Pitch minimum	136.5873823120346	95.78865108583372
Pitch maximum	165.51113279815547	137.6824372904897
Pitch quantile	158.91914577170476	111.09415331896598
Pitch mean	153.8641747551906	111.50764487029004
Pitch standard deviation	10.744462292408294	5.951579932901554

Analisa Statistik	SuaraBarangBukti (Hz)	SuaraSubyek1 (Hz)
Kata 'pasti		
Pitch minimum	127.63682990009453	98.9470672169626
Pitch maximum	174.74457653431784	116.837781092803
Pitch quantile	153.05680425734028	107.12902837117356
Pitch mean	153.00153894121118	106.88704716793961
Pitch standard deviation	11.520932349246682	4.274186795922285

Analisa Statistik	SuaraBarangBukti (Hz)	SuaraSubyek1 (Hz)
Kata 'bisa		
Pitch minimum	115.41765973638212	103.3894430472216
Pitch maximum	158.10445309910838	126.13424934264924
Pitch quantile	132.44728604899276	116.89182624914551
Pitch mean	134.85316984679028	117.39808712941148
Pitch standard deviation	15.479616391208856	6.204095467870283

Tabel VIII.2. Analisa Statistik *pitch* pada pengucapan masing-masing kata 'saya', 'pasti', dan 'bisa' antara SuaraBarangBukti dengan SuaraSubyek1.

Dari table di atas, dapat dilihat bahwa ada perbedaan nilai statistik *pitch minimum*, *maksimum*, *quantile*, *mean* dan *standard deviation* yang ***lebar*** antara SuaraBarangBukti dan SuaraSubyek1, baik pada kata 'saya', maupun pada kata-

kata ‘pasti’ dan ‘bisa’. Untuk menarik kesimpulan tersebut, hal yang mudah dan kuat argumentasinya untuk dianalisa terlebih dahulu adalah nilai *mean* (rata-rata) *pitch*, kemudian dilanjutkan dengan melihat nilai statistik yang lain. Pastikan nilai *standard deviation* tidak terlalu tinggi dan perbedaannya dengan nilai *mean* tidak terlalu dekat. Dari analisa ini, dapat ditarik kesimpulan bahwa berdasarkan nilai statistik *pitch* SuarabarangBukti TIDAK IDENTIK dengan SuaraSubyek1.

Analisa yang lebih komprehensif dan presisi terhadap nilai *pitch* antara suara barang bukti dan pembanding adalah dengan menggunakan metode *One-Way* Anova. Metode ini didasarkan pada perbandingan dua kelompok data *pitch* yang berasal dari suara barang bukti dan pembanding. Penjelasan lebih lengkap mengenai metode ini dapat dilihat pada analisa statistik *formant* dan *bandwidth*.

Analisa *pitch* ini dapat menghasilkan kesimpulan bahwa suara barang bukti dan pembanding adalah berbeda walaupun berasal dari subyek yang sama, jika subyek tersebut di dalam memberikan suara pembanding melakukan perubahan level intonasi yang berbeda dengan suara barang bukti.

Nilai *pitch* sangat bergantung dengan level intonasi dari suara yang diucapkan. Semakin rendah intonasi subyek mengucapkan suatu kata, maka semakin rendah pula nilai *pitch* dari kata yang diucapkan tersebut, sebaliknya semakin tinggi intonasinya, maka juga akan semakin tinggi nilai *pitch*-nya. Oleh karena itu, untuk pengucapan kata dan subyek yang sama, jika suara subyek di rekaman barang bukti lebih tinggi dibandingkan dengan suara pembanding, maka analisa statistik *pitch* tersebut akan menghasilkan bahwa suara barang bukti dan pembanding berasal dari subyek yang berbeda, meskipun diucapkan oleh subyek yang sama. Seringkali kondisi percakapan yang ada di rekaman barang bukti berbeda dengan kondisi pengambilan suara pembanding. Misalnya pada rekaman barang bukti, subyek berbicara penuh semangat di atas panggung di hadapan banyak orang, namun ketika diambil sample suara pembanding, subyek berbicara sangat datar dengan kondisi psikologi yang berbeda. Hal ini berpengaruh secara langsung terhadap nilai *pitch*. Untuk itu, secara umum dalam *voice recognition*, level analisa statistik *pitch* diposisikan berada di bawah analisa *formant* dan *spectrogram*.

Analisa Statistik Formant dan Bandwidth

Analisa Anova

Analisa ini didasarkan pada analisa *One-way* Anova (*Analysis of Variances*) yang mengkalkulasi secara statistik nilai-nilai *Formant* 1, *Formant* 2, *Formant* 3 dan *Formant* 4 dari suara *unknown* (SuaraBarangBukti) dan *known* (SuaraSubyek1). Anova akan menunjukkan tingkat perbedaaan antara 2 (dua) kelompok data pada masing-masing *formant* dari suara *unknown* dan *known*, yang ditandai dengan perbandingan ratio F dan F *critical*, dan nilai *probability* P.

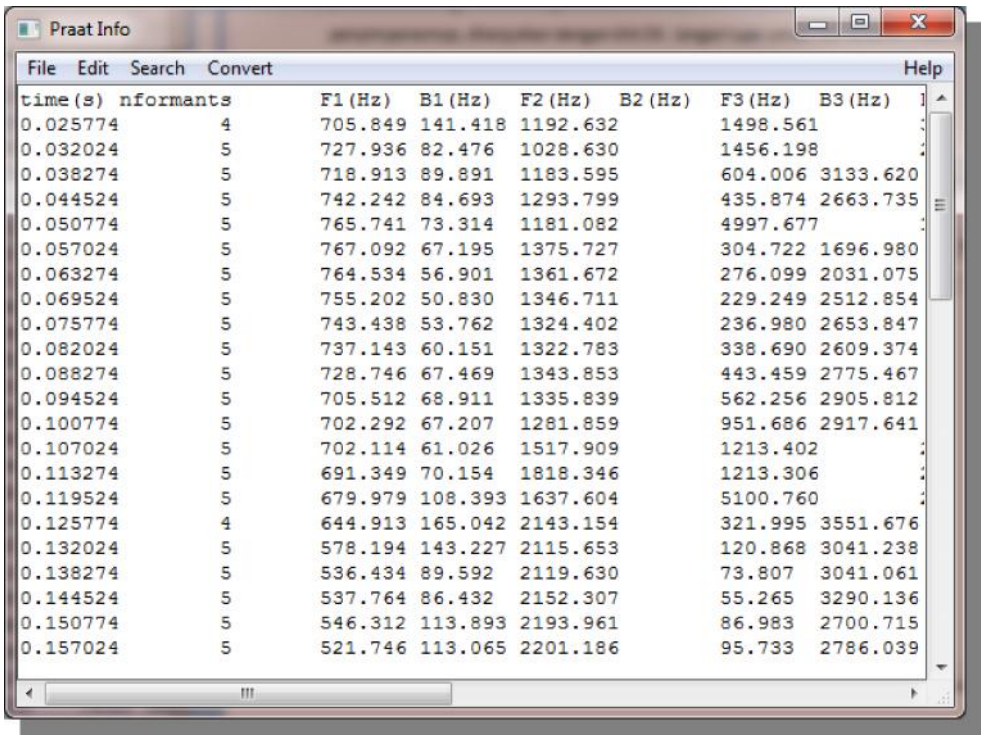
Jika nilai ratio F lebih kecil dari F *critical*, dan nilai *probability* P lebih besar dari 0.5 maka dapat disimpulkan bahwa kedua kelompok data dari nilai *formant* yang dianalisa dari suara *unknown* dan *known* tidak memiliki perbedaan (*accepted*) yang signifikan pada level 0.05. Kesimpulan ini memiliki tingkat konfidensi sebesar 95%. Berikut adalah contoh kesimpulan penggunaan Anova untuk analisa keseluruhan (*overall*).

Jenis *Formant*	*Ratio* F	P-*value*	F *critical*	*Conclusion*
***Formant* 1**	0.98	0.55	3.98	*Accepted*
***Formant* 2**	8.95	0	3.98	*Rejected*
***Formant* 3**	1.39	0.24	3.98	*Rejected*
***Formant* 4**	2.74	0.1	3.98	*Rejected*

Tabel VIII.3. Analisa *Overall Formant by One-Way Anova*.

Pada contoh suara pembanding SuaraSubyek1 seperti yang telah dijelaskan sebelumnya, didapat nilai statistik *Formant* dengan menggunakan Praat. Pada jendela *Praat Objects*, klik Open untuk memilih *file* suara untuk masing-masing kata 'saya', 'pasti' dan 'bisa' yang telah dibuat sebelumnya, yaitu SuaraBarangBukti-saya.wav, SuaraBarangBukti-pasti.wav dan SuaraBarangBukti-bisa.wav. Lakukan langkah-langkah yang sama seperti yang telah dijelaskan sebelumnya untuk mendapatkan nilai *formant* untuk masing-masing kata tersebut, setelah itu di-*save as binary file*. Masih pada jendela *Praat Objects*, pilih *Formant* SuaraBarangBukti-saya, klik List – OK untuk mendapatkan tabulasi nilai-

nilai *Formant* 1, 2, 3, 4 dan 5 berikut nilai *bandwidth* pada masing-masing *formant*.

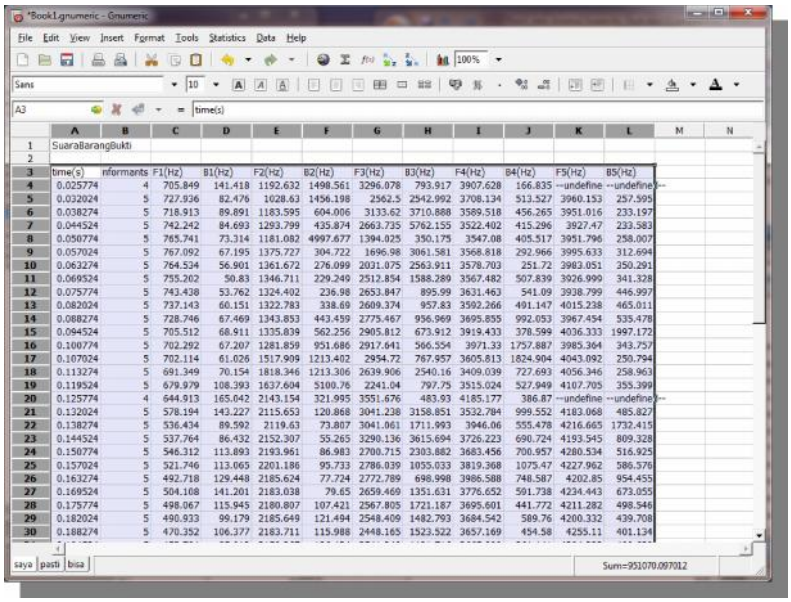

Praat Info

File Edit Search Convert Help

time(s)	nformants	F1(Hz)	B1(Hz)	F2(Hz)	B2(Hz)	F3(Hz)	B3(Hz)
0.025774	4	705.849	141.418	1192.632		1498.561	
0.032024	5	727.936	82.476	1028.630		1456.198	
0.038274	5	718.913	89.891	1183.595		604.006	3133.620
0.044524	5	742.242	84.693	1293.799		435.874	2663.735
0.050774	5	765.741	73.314	1181.082		4997.677	
0.057024	5	767.092	67.195	1375.727		304.722	1696.980
0.063274	5	764.534	56.901	1361.672		276.099	2031.075
0.069524	5	755.202	50.830	1346.711		229.249	2512.854
0.075774	5	743.438	53.762	1324.402		236.980	2653.847
0.082024	5	737.143	60.151	1322.783		338.690	2609.374
0.088274	5	728.746	67.469	1343.853		443.459	2775.467
0.094524	5	705.512	68.911	1335.839		562.256	2905.812
0.100774	5	702.292	67.207	1281.859		951.686	2917.641
0.107024	5	702.114	61.026	1517.909		1213.402	
0.113274	5	691.349	70.154	1818.346		1213.306	
0.119524	5	679.979	108.393	1637.604		5100.760	
0.125774	4	644.913	165.042	2143.154		321.995	3551.676
0.132024	5	578.194	143.227	2115.653		120.868	3041.238
0.138274	5	536.434	89.592	2119.630		73.807	3041.061
0.144524	5	537.764	86.432	2152.307		55.265	3290.136
0.150774	5	546.312	113.893	2193.961		86.983	2700.715
0.157024	5	521.746	113.065	2201.186		95.733	2786.039

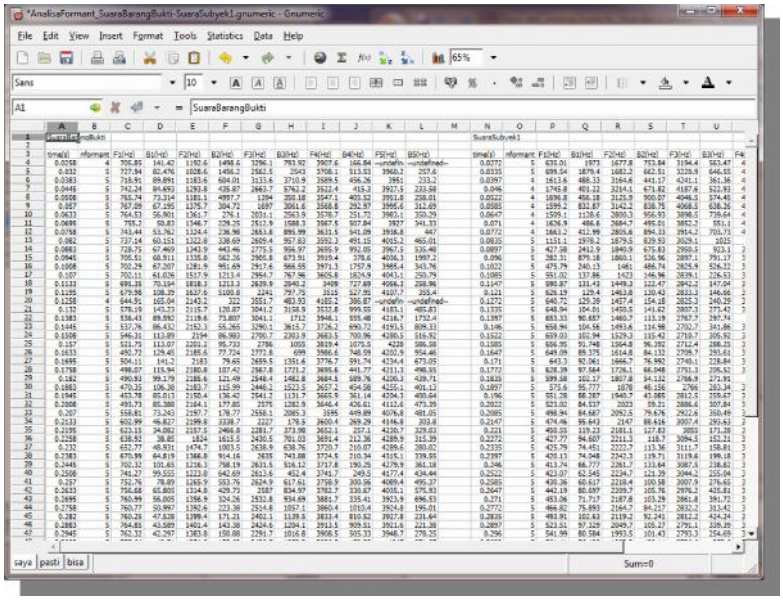
Gambar VIII.15. Tabulasi nilai masing-masing *formant* berikut *bandwidth*-nya.

Nilai-nilai *formant* ini kemudian diblok dan *copy-paste* ke aplikasi Gnumeric untuk analisa statistik lebih lanjut dengan menggunakan teknik Anova. Setelah nilai-nilai tersebut ada di Gnumeric, klik *File* – *Save*, ketik nama untuk *file* tersebut misalnya pada contoh ini adalah AnalisaFormant_SuaraBarangBukti-SuaraSubyek1 dan pilih tempat atau lokasi *folder* penyimpanannya, dilanjutkan dengan klik OK. Jangan lupa untuk me-*rename sheet* pada *file* tersebut dengan kata-kata ‘saya’, ‘pasti’ dan ‘bisa’.



Gambar VIII.16. Tabulasi nilai *formant* dan *bandwidth* yang sudah di-ekspor untuk kemudian dianalisa dengan metode *One-Way* Anova.

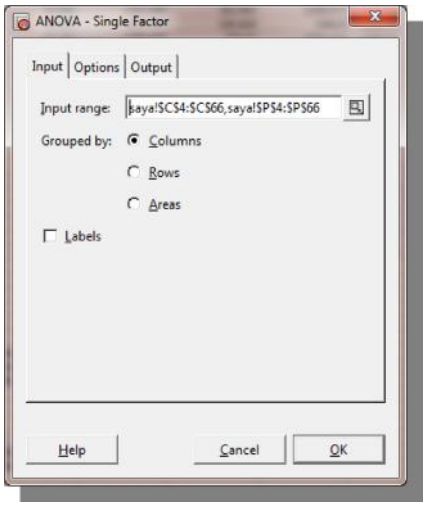
Lakukan hal yang sama untuk SuaraSubyek1, sehingga pada *file* Gnumeric akan didapatkan 2 (dua) tabel yang memuat nilai *formant* 1, 2, 3, 4, dan 5 beserta nilai *bandwidth*-nya masing-masing yang berasal dari SuaraBarangBukti dan SuaraSubyek1 untuk masing-masing kata ‘saya’, ‘pasti’ dan ‘bisa’.



Gambar VIII.17. Tabulasi nilai *formant* dan *bandwidth* yang sudah di-ekspor untuk kemudian dianalisa dengan metode *One-Way* Anova yang membandingkan secara statistik antara suara barang bukti dengan pembanding.

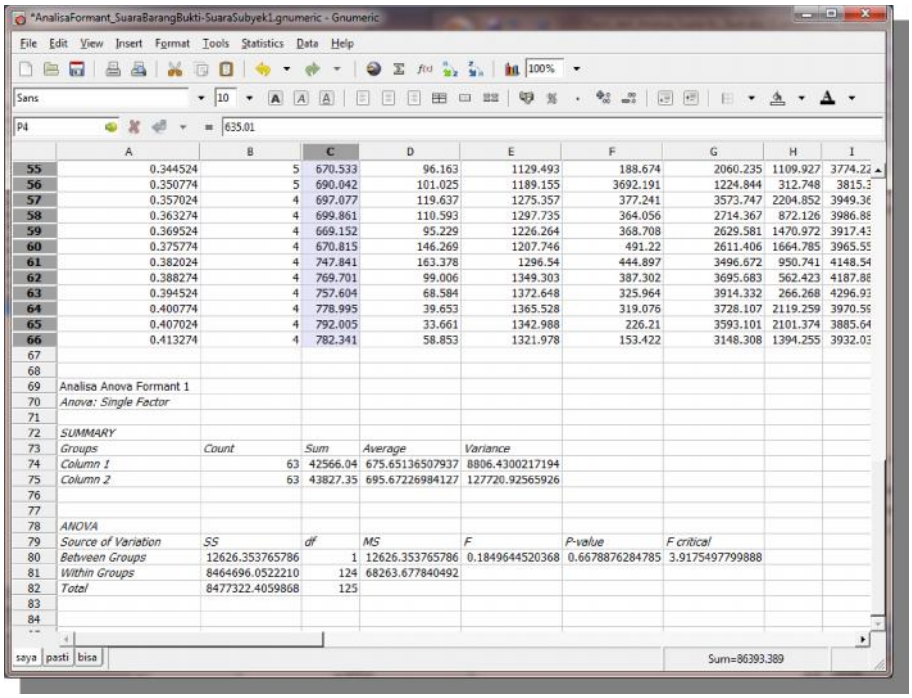
Setelah didapatkan nilai *formant* yang lengkap untuk masing-masing kata yang diucapkan dari SuaraBarangBukti dan SuaraSubyek1, maka dilakukan analisa statistic Anova untuk masing-masing nilai *formant* dan *bandwidth*.

Pada *file* Gnumeric *sheet* 'saya', lakukan blok nilai *Formant* 1 (F1) SuaraBarangBukti dan SuaraSubyek1 bersamaan dengan menggunakan <*control*>, kemudian klik *Statistics* – *Multiple Sample Test* – ANOVA – *One Factor*, akan muncul jendela ANOVA – *Single Factor*.



Gambar VIII.18. *Screenshot* jendela input data untuk analisa *One-Way* Anova.

Pada *tab Input*, pastika *Input range*-nya telah mencakup kedua blok data yang sudah dipilih sebelumnya, sedangkan pada *tab Output*, pilih lokasi untuk *Output range*-nya. Setelah itu, klik OK, akan didapat hasil kalkulasi statistik Anova untuk nilai *Formant* 1 antara SuaraBarangBukti dan SuaraSubyek1.



Gambar VIII.19. Hasil analisa *One-Way* Anova dengan nilai F, F *critical* dan *Probability* P.

Lakukan langkah-langkah yang sama untuk mendapat hasil kalkukasi Anova untuk *Formant* 2 dan 3 berikut nilai *Bandwidth*-nya. Tabel berikut memuat nilai hasil kalkulasi statistik Anova untuk *formant* dan *bandwidth* antara SuaraBarangBukti dan SuaraSubyek 1 pada pengucapan kata 'saya'.

Formant / Bandwidth	*Ratio* F	P-*value*	F *critical*	*Conclusion*
Kata 'saya'				
***Formant* 1**	0.184964	0.667888	3.917550	*Accepted*
***Formant* 2**	17.624239	0.000051	3.917550	*Rejected*
***Formant* 3**	11.063653	0.001159	3.917550	*Rejected*
***Formant* 4**	3.384234	0.068215	3.917550	*Rejected*
Formant 5	133.328322	0.000000	3.931556	*Rejected*
***Bandwidth* 1**	12.815478	0.000492	3.917550	*Rejected*
***Bandwidth* 2**	9.251233	0.002873	3.917550	*Rejected*
***Bandwidth* 3**	49.577626	0.000000	3.917550	*Rejected*
***Bandwidth* 4**	4.284423	0.040539	3.917550	*Rejected*
Bandwidth 5	11.856697	0.000826	3.931556	*Rejected*

Formant / Bandwidth	*Ratio F*	*P-value*	*F critical*	*Conclusion*
Kata 'pasti				
Formant 1	0.051100	0.821572	3.925834	*Accepted*
Formant 2	12.248086	0.000667	3.925076	*Rejected*
Formant 3	0.155900	0.693704	3.925076	*Accepted*
Formant 4	0.027920	0.867595	3.925076	*Accepted*
Formant 5	14.630304	0.000247	3.951882	*Rejected*
Bandwidth 1	27.561590	0.000001	3.925076	*Rejected*
Bandwidth 2	1.550849	0.215586	3.925076	*Rejected*
Bandwidth 3	7.316284	0.007891	3.925076	*Rejected*
Bandwidth 4	0.005027	0.943600	3.925076	*Accepted*
Bandwidth 5	11.570620	0.001019	3.951882	*Rejected*

Formant / Bandwidth	*Ratio F*	*P-value*	*F critical*	*Conclusion*
Kata 'bisa				
Formant 1	28.355878	0.000000	3.908741	*Rejected*
Formant 2	7.454755	0.007141	3.908741	*Rejected*
Formant 3	2.250941	0.135785	3.908741	*Rejected*
Formant 4	5.648096	0.018828	3.908741	*Rejected*
Formant 5	3.330265	0.072474	3.984049	*Rejected*
Bandwidth 1	3.236350	0.074175	3.908741	*Rejected*
Bandwidth 2	4.918382	0.028184	3.908741	*Rejected*
Bandwidth 3	2.551050	0.112476	3.908741	*Rejected*
Bandwidth 4	13.691972	0.000309	3.908741	*Rejected*
Bandwidth 5	1.334219	0.252159	3.984049	*Rejected*

Tabel VIII.4. Analisa Statsistik Anova antara SuaraBarangBukti dan SuaraSubyek1 untuk masing-masing nilai *formant* 1, 2, 3, 4 dan 5 berikut nilai *bandwidth*-nya.

Pada Tabel di atas, dapat ditarik kesimpulan bahwa, hasil analisa Anova untuk nilai *formant* 1, 2, 3, 4, 5 berikut nilai *bandwidth*-nya menunjukkan pengucapan kata 'pasti' SuaraBarangBukti adalah IDENTIK dengan SuaraSubyek1, karena *formant* 1, 3 dan 4 *accepted*, sedangkan pengucapan kata 'saya' dan 'bisa' SuaraBarangBukti adalah TIDAK IDENTIK dengan SuaraSubyek1.

Penilaian apakah kesimpulan dari Anova *accepted* atau *rejected*, juga bisa hanya ditentukan oleh nilai *Ratio* F dan F *critical* tanpa melibatkan nilai *probability* P. Jika *Ratio* F lebih kecil dibandingkan dengan F *critical*, hal itu sudah menunjukkan bahwa kedua kelompok data antara *unknown samples* (suara barang bukti) dengan *known samples* (suara pembanding) memiliki kesamaan. Jadi tidak perlu melihat seberapa besar nilai *probability* P. Konfidensi terhadap metode ini tetap bernilai 95% karena perbedaan signifikan natara kedua kelompok data tetap pada level 0.05. Meskipun begitu, metode ini tetap berada di bawah metode yang pertama (yang melihat nilai *probability* P harus sama atau lebih besar dari 0.5).

Dalam menarik kesimpulan Analisa Anova *Formant*, dibutuhkan paling tidak *formant* 1, 2, dan 3 yang dianalisa. Jika 2 (dua) di antara *formant* 1, 2, dan 3 menunjukkan *accepted* maka hal tersebut sudah cukup untuk menarik kesimpulan IDENTIK berdasarkan Anova. Walaupun begitu, kesimpulan ini juga biasanya didukung dengan *formant* 4 atau 5.

Bandwidth hanya digunakan pada hal-hal yang bersifat kasuistis, yaitu di mana subyek berusaha memberikan suara pembanding yang benar-benar berbeda secara *aural* dengan suara aslinya, yang dalam kasus ini, biasanya menggunakan aplikasi *pitch shift* atau subyek berbicara dengan intonasi dan aksen yang jauh berbeda ketika diambil suara pembandingnya dengan suara sesungguhnya yang ada di dalam rekaman barang bukti.

Analisa Likelihood Ratio (LR)

Penelaahan lebih detil terhadap analisa statistik terhadap *formant* dan *bandwidth* adalah dengan menggunakan *Likelihood Ratio* (LR) yang dalam contoh ini merupakan lanjutan dari Analisa Anova yang telah dijelaskan di atas. Formula LR adalah sebagai berikut :

$$LR = \frac{p\,(E \mid H_p)}{p\,(E \mid H_d)}$$

di mana :

$p\,(E \mid H_p)$ adalah hipotesis tuntutan (*prosecution*), yaitu *known* dan *unknown samples* berasal dari orang yang sama.

p (E | H_d) adalah hipotesis perlawanan (*defense*), yaitu *known* dan *unknown samples* berasal dari orang yang berbeda.

p (E | H_p) berasal dari p-value Anova, sedangkan *p* (E | H_d) = 1 - *p* (E | H_p)

Jika LR > 1, maka hal ini mendukung *p* (E | H_p), sebaliknya jika LR < 1, maka *p* (E | H_d) yang didukung. Untuk itu, haruslah nilai *p* (E | H_p) > 0.5 untuk dapat menyimpulkan bahwa suara barang bukti (*unknown*) dan suara pembanding (*known*) berasal dari orang yang sama (IDENTIK).

Besarnya ratio LR diikuti dengan *verbal statement* untuk menjelaskan nilai LR tersebut, seperti pada table berikut :

LR	LR (log)	*Verbal Statement*	Keterangan
> 10,000	> 4	*Very strong evidence to support*	Mendukung hipotesis tuntutan *p* (E | H_p)
1,000 – 10,000	3 – 4	*Strong evidence to support*	
100 – 1,000	2 – 3	*Moderately strong evidence to support*	
10 – 100	1 – 2	*Moderate evidence to support*	
1 – 10	0 – 1	*Limited evidence to support*	

Tabel VIII.5. *Verbal statement* untuk masing-masing nilai LR yang mendukung hipotesis tuntutan *p* (E | H_p).

LR	LR (log)	*Verbal Statement*	Keterangan
1 – 0.1	0 – -1	*Limited evidence against*	Mendukung hipotesis perlawanan *p* (E | H_d)
0.1 – 0.01	-1 – -2	*Moderate evidence against*	
0.01 – 0.001	-2 – -3	*Moderately strong evidence against*	
0.001 – 0.0001	-3 – -4	*Strong evidence against*	
< 0.0001	> -4	*Very strong evidence against*	

Tabel VIII.5. *Verbal statement* untuk masing-masing nilai LR yang mendukung hipotesis perlawanan *p* (E | H_d).

Dari kedua table di atas, diketahui bahwa untuk mendapatkan dukungan terhadap hipotesis penuntutan (suara *known* dan *unknown* berasal dari orang

yang sama) haruslah LR > 1, di mana semakin besar nilai LR akan semakin baik dan kuat untuk *verbal statement*-nya.

Berdasarkan hasil kalkulasi Anova yang didapat sebelumnya untuk pengucapan kata 'saya', maka perhitungan LR untuk *formant* adalah sebagai berikut :

Formant Kata 'saya'	P-*value* = p (E | H_p)	p (E | H_d)	LR	*Verbal Statement*
***Formant* 1**	0.667888	0.332112	2.011029	*Limited evidence to support*
***Formant* 2**	0.000051	0.999949	0.000051	*Very strong evidence against*
***Formant* 3**	0.001159	0.998841	0.001160	*Strong evidence against*
***Formant* 4**	0.068215	0.931785	0.073208	*Moderately strong evidence against*
Formant 5	0.000000	1.000000	0.000000	*Very strong evidence against*

Tabel VIII.6. *Verbal statement* untuk hasil analisa LR pada masing-masing *formant*.

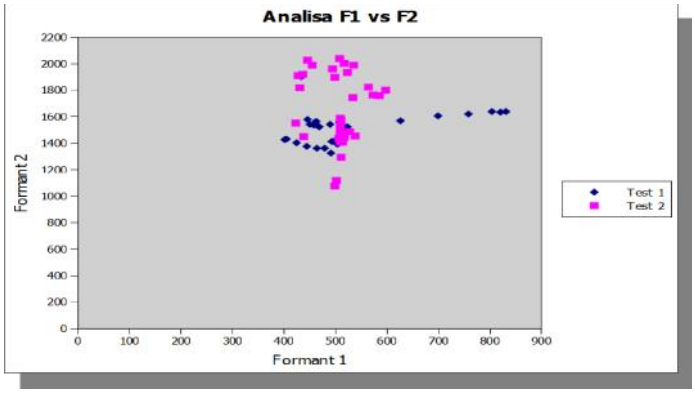
Dari table di atas, hanya *formant* 1 yang LR > 1 untuk mendukung hipotesis penuntutan, sedangkan nilai *formant* yang lain mendukung hipotesis perlawanan.

Analisa LR ini dapat digunakan untuk memperkuat hasil analisa Anova yang didapat sebelumnya, karena LR ini dapat menjelaskan seberapa level LR yang mendukung hipotesis penuntutan maupun hipotesis perlawanan.

Analisa Graphical Distribution

Analisa ditujukan untuk menggambarkan dalam bentuk grafis pola penyebaran (distribusi) masing-masing nilai *formant* untuk melihat level perbedaan distribusi nilai *formant* dari suara *unknown* dan *known*. Biasanya analisa ini dibuat dalam bentuk perbandingan F1 vs F2 dan F2 vs F3.

Jika terdapat nilai yang menyimpang pada *formant* yang dianalisa yang mana nilai menyimpang ini tidak terakomodasi dalam analisa statistik Anova, malah membuat kesimpulan yang keliru, maka analisa *graphical distribution* ini dapat mengkoreksi kesimpulan yang keliru tersebut.



Gambar VIII.20. Analisa *graphical distribution* F1 vs F2 dari masing-masing suara *Test* 1 (*unknown*) dan *Test* 2 (*known*). Hasil dari analisa ini menunjukkan bahwa *formant* 1 dan *formant* 2 antara suara *Test* 1 dan *Test* 2 memiliki perbedaan pada tingkat penyebarannya.

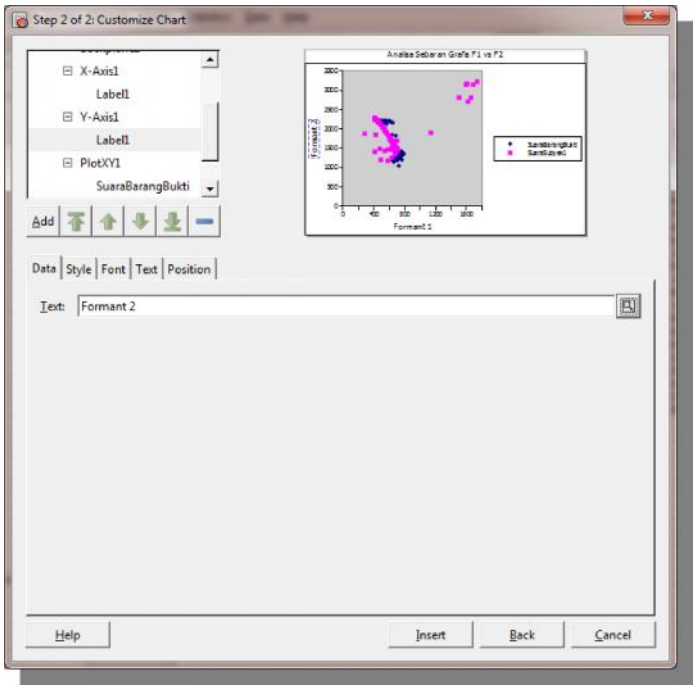
Pada contoh SuaraBarangBukti dan SuaraSubyek1 yang telah didapat dan dijelaskan sebelumnya untuk Analisa Statistik *Formant*, tabulasi data untuk kedua jenis suara tersebut dapat digunakan untuk melanjutkan analisa ke analisa sebaran grafis (*Graphical Distribution*). Analisa ini masih menggunakan aplikasi Gnumeric untuk memetakan bentuk sebaran grafisnya. Pada *Gnumeric sheet* saya, klik *Insert – Chart*, pilih *Plot type*: XY.



Gambar VIII.21. Pemilihan *Plot type*: XY.

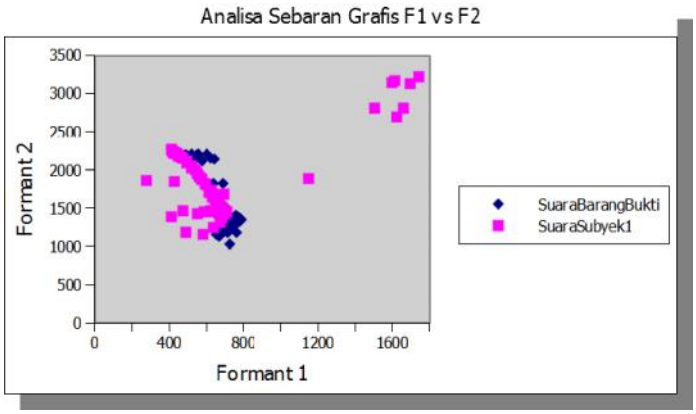
kemudian klik *Forward*, pada *Graph*, klik *Add – Title* to *Graph*, pada *tab* Data ketikkan nama judul grafik, yang dalam hal ini adalah 'Analisa Sebaran Grafis F1 vs F2'. Pada PlotXY1, klik *Add – Series* to PlotXY1, untuk menambahkan Series2 di

bawah Series1 yang sudah ada sebagai *default*-nya. Series1 difungsikan untuk SuaraBarangBukti, sedangkan Series2 untuk SuaraSubyek1. Pada Series1, pada *tab* Data, ketikkan pada baris *Name*, pilih *cell* A1 pada tabulasi yang berisikan 'SuaraBarangBukti' sebagai nama grafik pertama. Pada baris X, masukkan *input range formant* 1 sesuai pada tabulasi SuaraBarangBukti sebelumnya, sedangkan pada baris Y, masukkan *input range formant* 2. Lakukan hal yang sama pada Series2 untuk SuaraSubyek1. Pada PlotXY1, klik *Add* – *Legend* to *Chart* 1, untuk menampilkan *legend* (keterangan) untuk masing-masing *chart*. Pada X-Axis1, klik *Add* – *Label* to X-Axis1, pada *tab* Data baris *Text*, ketikkan *formant* 1 untuk nama data pada sumbu X. Begitu Juga pada Y-Axis1 untuk *formant* 2.



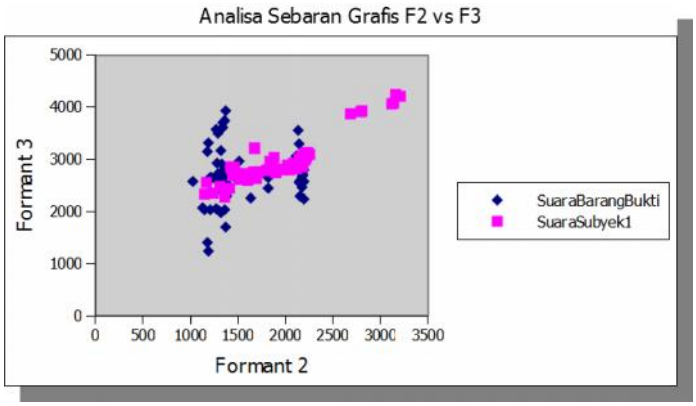
Gambar VIII.22. *Input* akhir dengan memasukkan data label sumbu X dan Y.

Setelah selesai semuanya, klik *Insert*. Akan terlihat sebaran grafis F1 vs F2 (*Formant* 1 vs *Formant* 2) antara SuaraBarangBukti dengan SuaraSubyek1 untuk pengucapan kata 'saya'.



Gambar VIII.23. Hasil akhir analisa *graphical distribution* F1 vs F2 untuk kata 'saya'.

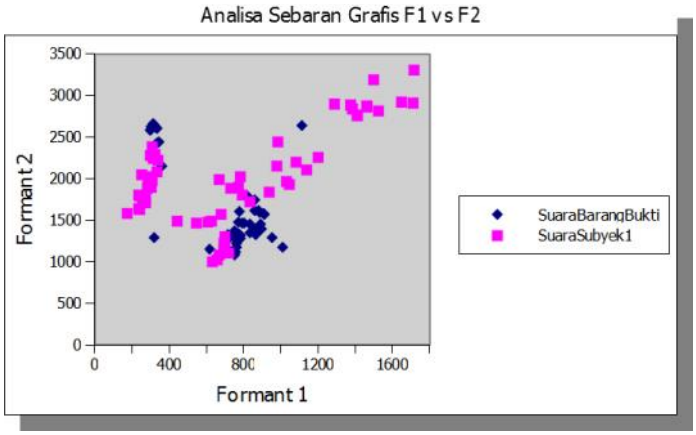
Lakukan langkah-langkah yang sama untuk mendapatkan analisa sebaran grafis F2 vs F3 (*Formant* 2 vs *Formant* 3) antara SuaraBarangBukti dengan SuaraSubyek1 untuk pengucapan kata 'saya'.



Gambar VIII.24. Hasil akhir analisa *graphical distribution* F2 vs F3 untuk kata 'saya'.

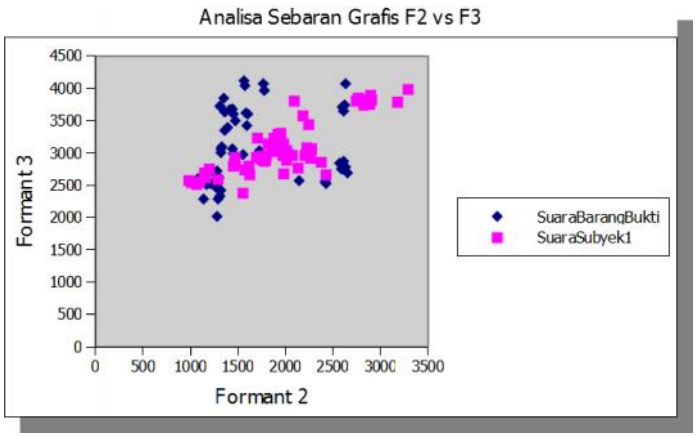
Pada kedua grafik di atas, dapat dilihat bahwa sebaran grafis *formant* 1, 2 dan 3 menunjukkan beberapa nilai dari SuaraSubyek1 yang keluar dari kelompoknya (terdistorsi). Jika beberapa nilai tersebut di-eliminir maka akan didapat bahwa nilai sebaran grafis *formant* 1, 2 dan 3 antara SuaraBarangBukti dan SuaraSubyek1 adalah masih dalam rentang kelompok yang sama (*probability* kesamaan Anova). Hal ini dapat ditarik kesimpulan bahwa *formant* 1, 2 dan 3 antara SuaraBarangBukti dengan SuaraSubyek1 adalah IDENTIK.

Tahapan-tahapan ini diulangi untuk pengucapan kata 'pasti', akan didapat Analisa Sebaran Grafis F1 vs F2 antara SuarabarangBukti dengan SuaraSubyek1.



Gambar VIII.25. Hasil akhir analisa *graphical distribution* F1 vs F2 untuk kata 'pasti'.

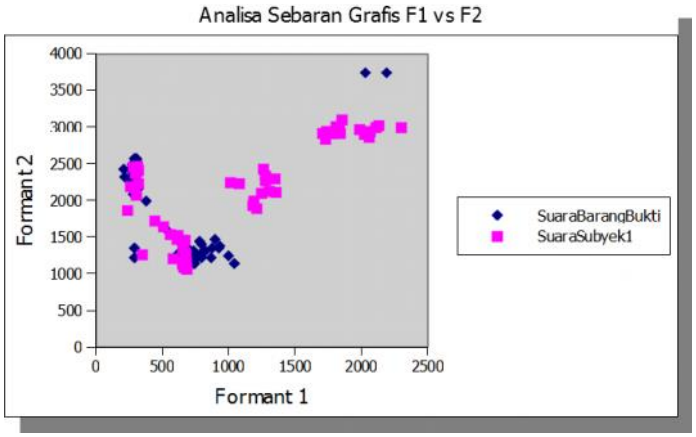
Dan Analisa Sebaran Grafis F2 vs F3 antara SuaraBarangBukti dengan SuaraSubyek1 untuk pengucapan kata 'pasti'.



Gambar VIII.26. Hasil akhir analisa *graphical distribution* F2 vs F3 untuk kata 'pasti'.

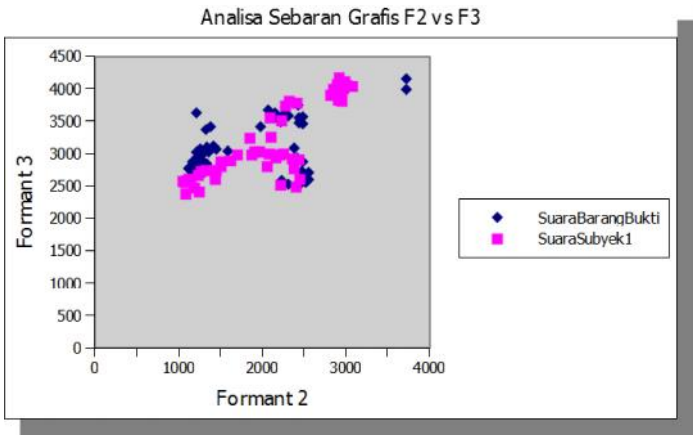
Pada kedua grafik di atas, ada beberapa nilai dari SuaraSubyek1 yang keluar dari kelompoknya (terdistorsi). Jika nilai-nilai ini dieliminir, maka dapat dilihat bahwa nilai sebaran grafis *formant* 1, 2 dan 3 antara SuaraBarangBukti dan SuaraSubyek1 adalah masih dalam rentang kelompok yang sama (*probability* kesamaan Anova). Hal ini dapat ditarik kesimpulan bahwa *formant* 1, 2 dan 3 antara SuaraBarangBukti dengan SuaraSubyek1 adalah IDENTIK.

Tahapan-tahapan ini diulangi untuk pengucapan kata 'bisa, akan didapat Analisa Sebaran Grafis F1 vs F2 antara SuarabarangBukti dengan SuaraSubyek1.



Gambar VIII.27. Hasil akhir analisa *graphical distribution* F1 vs F2 untuk kata 'bisa'.

Dan Analisa Sebaran Grafis F2 vs F3 antara SuaraBarangBukti dengan SuaraSubyek1 untuk pengucapan kata 'bisa.



Gambar VIII.28. Hasil akhir analisa *graphical distribution* F2 vs F3 untuk kata 'bisa'.

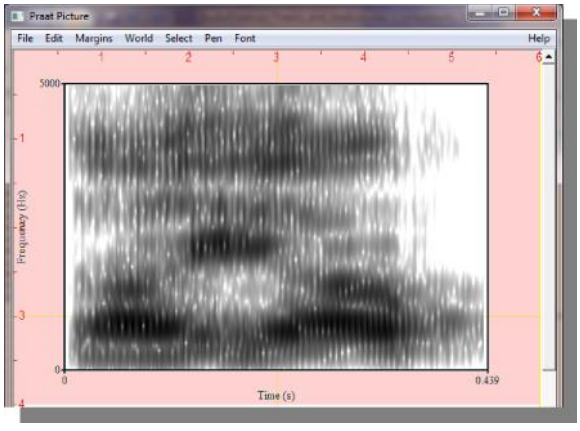
Dari kedua grafik di atas, diketahui bahwa beberapa nilai *formant* dari SuaraBarangBukti dan SuaraSubyek1 keluar dari klompoknya (terdistorsi). Jika nilai-nilai ini dieliminir, maka dapat dilihat bahwa nilai sebaran grafis *formant* 2 dan 3 antara SuaraBarangBukti dan SuaraSubyek1 adalah masih dalam rentang kelompok yang sama (*probability* kesamaan Anova). Hal ini dapat ditarik kesimpulan bahwa *formant* 2 dan 3 antara SuaraBarangBukti dengan SuaraSubyek1 adalah IDENTIK.

Analisa Spectrogram

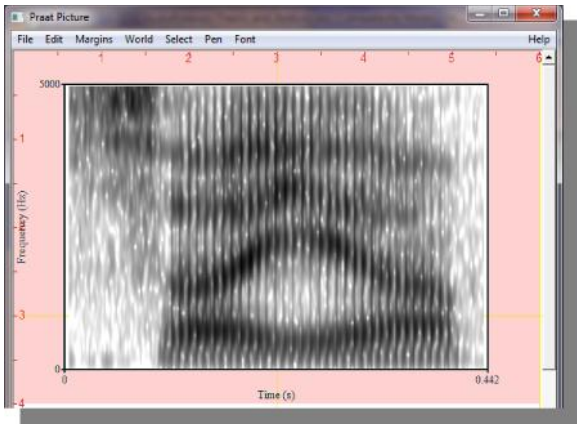
Analisa ini menunjukkan pola umum yang khas pada kata yang diucapkan dan pola khusus yang khas pada masing-masing *formant* suku kata yang dianalisa. Pola-pola khas tersebut juga termasuk dalam analisa tingkatan energi dari masing-masing *formant* seperti yang ditunjukkan pada Gambar 5 di atas.

Jika pola-pola khas tersebut untuk pengucapan kata-kata tertentu dari suara *unknown* (suara barang bukti) dan *known* (suara pembanding) tidak menunjukkan perbedaan yang signifikan, maka dapat disimpulkan bahwa kedua suara tersebut untuk pengucapan pada kata-kata tersebut adalah IDENTIK (memiliki kesamaan *spectrogram*).

Pada contoh SuaraBarangBukti dan SuaraSubyek1 yang telah dibuat dan dijelaskan sebelumnya, pada *Praat Objects*, klik *Open* – *Read from file*, pilih *file* SuaraBarangBukti-saya.wav dan SuaraSubyek1-saya.wav untuk pengucapan kata saya pada masing-masing SuaraBarangBukti dan SuaraSubyek1. Pada masing-masing *sound* tersebut, lakukan langkah-langkah seperti yang dijelaskan di atas (melalui klik *Spectrum* – *To Spectrogram* – OK) untukmendapatkan *spectrogram* untuk masingmasing *sound*. Setelah didapat *spectrogram* untuk kedua *sound* tersebut, masing-masing file di-*save as binary file*. *Spectrogram* untuk pengucapan kata ‘saya’ dari SuaraBarangBukti.



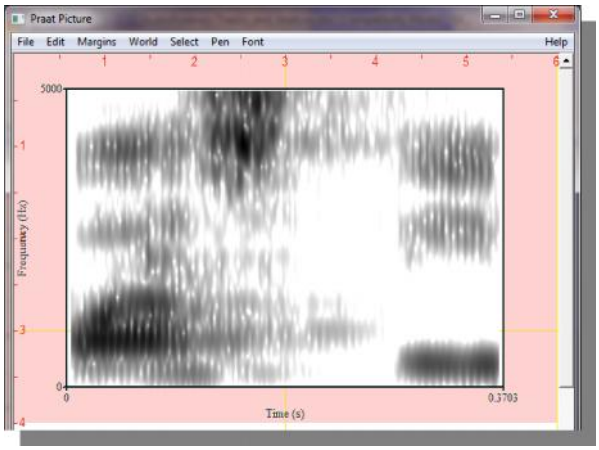
Gambar VIII.29. *Screenshot spectrogram* untuk pengucapan kata ‘saya’ dari SuaraBarangBukti.



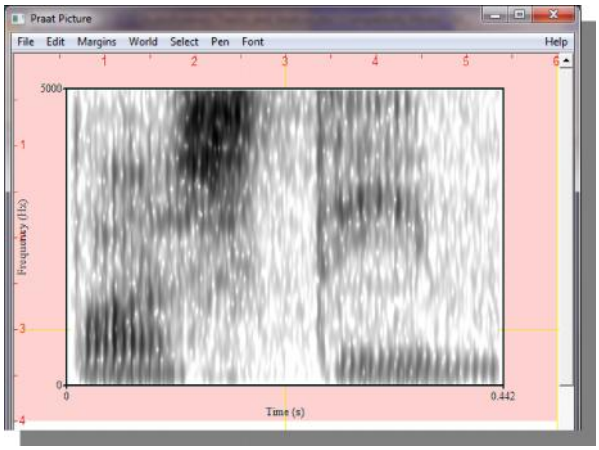
Gambar VIII.30. *Screenshot spectrogram* untuk pengucapan kata ‘saya’ dari SuaraSubyek1.

Pada kedua grafik di atas, dapat dilihat bahwa pengucapan kata ‘saya’ membentuk pola-pola yang khas pada nilai formant 1, 2 ,3 dan 4. Pola-pola khas ini memiliki kesamaan antara SuaraBarangBukti dengan SuaraSubyek1, sehingga hal ini dapat menyimpulkan bahwa spectrogram SuaraBarangBukti dan SuaraSubyek1 untuk pengucapan kata ‘saya’ adalah IDENTIK.

Langkah-langkah yang sama diulangi untuk mendapatkan *spectrogram* untuk pengucapan kata ‘pasti’ dari SuaraBarangBukti.



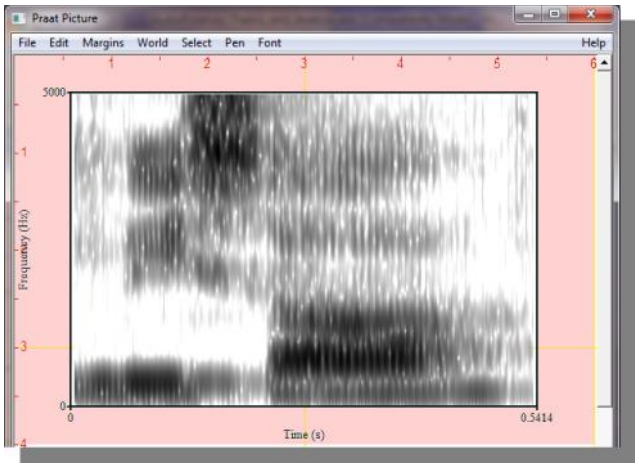
Gambar VIII.31. *Screenshot spectrogram* untuk pengucapan kata ‘pasti’ dari SuaraBarangBukti.



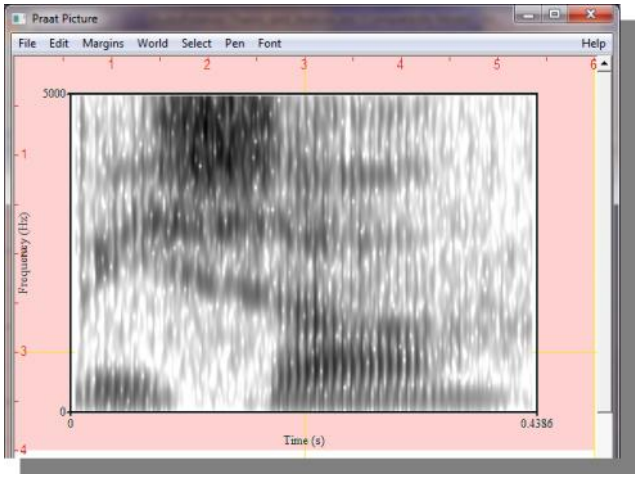
Gambar VIII.32. *Screenshot spectrogram* untuk pengucapan kata 'pasti' dari SuaraSubyek1.

Meskipun pola *spectrogram* pada kedua grafik di atas untuk pengucapan kata 'pasti' tidak begitu jelas, namun dengan pengamatan yang lebih teliti, Hasil yang sama akan didapat pada kedua grafik tersebut untuk pengucapan kata 'pasti'. Dapat dilihat bahwa pengucapan kata 'pasti' membentuk pola-pola yang khas pada nilai formant 1, 2 ,3 4, dan 5. Pola-pola khas ini memiliki kesamaan antara SuaraBarangBukti dengan SuaraSubyek1, sehingga hal ini dapat menyimpulkan bahwa *spectrogram* SuaraBarangBukti dan SuaraSubyek1 untuk pengucapan kata 'pasti' adalah IDENTIK.

Langkah-langkah yang sama diulangi untuk mendapatkan *spectrogram* untuk pengucapan kata 'bisa' dari SuaraBarangBukti.



Gambar VIII.33. *Screenshot spectrogram* untuk pengucapan kata 'bisa' dari SuaraBarangBukti



Gambar VIII.34. *Screenshot spectrogram* untuk pengucapan kata 'bisa' dari SuaraSubyek1.

Hasil yang sama juga akan didapat pada kedua grafik di atas untuk pengucapan kata 'bisa'. Dapat dilihat bahwa pengucapan kata 'bisa' membentuk pola-pola yang khas pada nilai *formant* 1, 2 ,3 4, dan 5. Pola-pola khas ini memiliki kesamaan antara SuaraBarangBukti dengan SuaraSubyek1, sehingga hal ini dapat menyimpulkan bahwa spectrogram SuaraBarangBukti dan SuaraSubyek1 untuk pengucapan kata 'bisa' adalah IDENTIK.

Oleh karena *spectrogram* mampu menampilkan pola-pola yang khas *formant* dan *bandwidth* pada pengucapan kata-kata yang mana pola-pola ini tidak terpengaruh dengan tinggi rendahnya frekwensi resonansi tiap-tiap *formant* ketika pengucapan kata-kata dibuat, maka ada sebagian ahli menyatakan bahwa spectrogram merupakan sidik jari suara (*voice fingerprint*). Walaupun begitu ada juga sebagian ahli yang tidak sependapat dengan pernyataan tersebut. Mereka berargumentasi bahwa *spectrogram* untuk pengucapan kata yang sama namun berasal dari 2 (dua) orang yang berbeda akan memungkinkan menghasilkan pola khas *spectrogram* yang sama. Hal ini bisa menyesatkan atau menghasilkan *false positive*. Artinya untuk *voice recognition*, *spectrogram* bukanlah satu-satunya komponen suara yang dianalisa. Harus ada juga analisa terhadap komponen suara yang lain seperti analisa *statistic* terhadap *pitch* dan *formant* yang berbasis Anova dan *Likelihood Ratio* (LR).

Penarikan Kesimpulan

1. Pemeriksaan dan analisa *Audio Forensic* haruslah dilakukan secara komprehensif, khususnya dalam penanganan barang bukti rekaman suara harus sesuai dengan prinsip-prinsip dasar digital forensik dengan mengikuti *Standard Operating Procedure* (SOP), misalnya SOP 12 dari DFAT Puslabfor tentang Analisa *Audio Forensic*. Seperti yang telah dijelaskan sebelumnya, SOP ini memuat langkah-langkah untuk pelaksanaan *Audio Forensic*, yaitu :
   a. *Acquisition*
   b. *Audio Enhancement*
   c. *Decoding*
   d. *Voice Recognition*

2. Sebelum melaksanakan Analisa *Audio Forensic*, sebaiknya pemeriksa ahli sudah memahami teori-teori dasar mengenai proses produksi (*generation*) suara dan filterisasinya melalui *vocal tract* atau *articulator* yang nantinya menghasilkan komponen-komponen suara seperti *pitch*, *formant* dan *spectrogram* yang dapat dianalisa lebih detil untuk kepentingan *voice recognition*.

3. Analisa *voice recognition* ini adalah bersifat komprehensif yang menganalisa dan membandingkan suara yang berasal dari rekaman barang bukti (*unknown samples*) dengan suara pembanding (*known samples*). *Voice recognition* ini mencakup :
   a. Analisa statistik *pitch*, yaitu minimum, maksimum, *quantile* (*median*), *mean* dan *standard deviation*, serta analisa komprehensif dengan menggunakan *One-Way* Anova.
   b. Analisa statistik *formant* berbasis Anova (*Analysis of Variance*) terhadap nilai-nilai *formant* 1, 2, 3, 4 dan 5, sedangkan untuk nilai-nilai *bandwidth* hanya digunakan pada hal-hal yang bersifat kasuistis seperti penggunaan *pitch shift* untuk memalsukan suara

asli atau perbedaan kondisi suara barang bukti dengan pengambilan suara pembanding. Analisa statistik berbasis Anova ini juga didukung dengan analisa *Likelihood Ratio* (LR) dengan *verbal statement*-nya yang menunjukkan seberapa tinggi level LR yang mendukung hipotesis penuntutan (suara *unknown* dan *known* berasal dari orang yang sama) atau hipotesis perlawanan (suara *unknown* dan *known* berasal dari orang yang berbeda)

c. Analisa *graphical distribution* untuk melihat pola sebaran grafis secara komprehensif sehingga dapat mengeliminir nilai-nilai *formant* yang keluar dari kelompok datanya (terdistorsi).

d. Analisa *spectrogram* untuk mendapatkan pola-pola yang khas yang membentuk *formant* 1, 2, 3, 4 dan 5 berikut level energy (*bandwidth*)-nya.

e. Urutan konfidensi analisa untuk masing-masing komponen suara dalam rangka *voice recognition* adalah sebagai berikut :

1) Analisa statistik *formant* berbasis *One-Way* Anova dan *Likelihood Ratio*

2) Analisa *graphical distribution*

3) Analisa pola-pola *formant* yang khas pada *spectrogram*

4) Analisa statistik *pitch*

4. *Voice recognition* ini harus mendapatkan minimal 20 (duapuluh) kata yang berbeda makna dan dapat diterima (*accepted*) dikarenakan memiliki kesamaan (*very similar*) pola dan analisa untuk menyimpulkan bahwa suara barang bukti adalah IDENTIK dengan suara pembanding. Jika tidak ditemukan sejumlah kata tersebut, maka kesimpulannya adalah TIDAK IDENTIK. Jika jumlah kata-kata yang ada pada rekaman barang bukti tidak mencapai 20 (duapuluh) kata yang berbeda makna yang dapat dianalisa, maka kesimpulannya adalah *INCONCLUSIVE* dan tidak layak untuk dilaksanakan pemeriksaan *audio forensic*. Jumlah 20 (duapluh) kata ini merujuk pada '*Spectrographic Voice Identification: A Forensic Survey*' yang disusun oleh Koenig, B.E. dari *Federal Bureau of Investigation*.

Bibliography

1. ACPO, 7Safe (2008). *Good Practice Guide for Computer-Based Electronic Evidence*. UK ACPO and 7Safe.
2. Al-Azhar, M.N. (2010). *Standard Operating Procedure (SOP) 10 : Analisa Audio Forensik*. DFAT Puslabfor.
3. Broeders, A.P.A. (2001). Forensic Speech and Audio Analysis Forensic Linguistics. 13th Interpol Forensic Science Symposium.
4. Koenig, B. E. (1986). *Spectrographic Voice Identification: A Forensic Survey*. Federal Bureau of Investigation.
5. Mandasari, M. I. (2010). *Pengembangan Sistem Identifikasi Pengucap untuk Aplikasi Forensik di Indonesia*. Institut Teknologi Bandung
6. National Institute of Justice (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. US National Institute of Justice.
7. Rose, P. (2002). *Forensic Speaker Identification*. Taylor & Francis Forensic Science Series.
8. Sarwono, J. (2010). *Forensic Speaker Identification*. Institut Teknologi Bandung.
9. Scientific Working Group on Digital Evidence (2008). *SWGDE Best Practices for Forensic Audio*. Scientific Working Group on Digital Evidence.

Bab IX

VIDEO FORENSIC: Theory and Analysis

Salah satu jenis barang bukti yang sering diterima untuk dianalisa lebih lanjut secara digital forensik adalah barang bukti berupa rekaman video. Rekaman video tersebut berasal bisa berasal dari kamera cctv (*Closed Circuit Television*), *handycam*, *digital camera* yang memiliki fitur video, dan *handphone*. Seiring dengan banyaknya peralatan teknologi tinggi tersebut yang dimiliki oleh masyarakat, maka sangat memungkinkan jenis barang bukti tersebut akan banyak diterima oleh para *digital forensic analyst* untuk diperiksa dan dianalisa lebih lanjut secara digital forensik. Masyarakat biasanya menggunakan peralatan *video recorder* tersebut misalnya *handycam*, *handphone* atau *digital camera* untuk mengabadikan momen-momen yang dianggap berharga bagi mereka, atau bisa juga menggunakan kamera cctv untuk kepentingan perlindungan sekuriti bisnis mereka.

Biasanya yang diminta dari barang bukti rekaman video tersebut adalah mengenai keaslian rekaman. Apakah rekaman video tersebut asli atau sudah direkayasa untuk satu kepentingan tertentu ?. Pertanyaan tersebut sering diajukan oleh *investigator* ketika menyerahkan barang bukti rekaman video kepada *digital forensic analyst*. Dipastikan asli atau tidaknya rekaman video tersebut sangat membantu *investigator* dalam mengembangkan investigasi mereka terhadap pelaku yang merekam video tersebut. Di samping itu, sering juga dari rekaman video, investigator meminta untuk dilakukan pembesaran (*zooming in*) terhadap satu atau beberapa objek tertentu yang ada di rekaman video tersebut. Hal itu dilakukan untuk memastikan kejelasan beberapa hal yang berkaitan dengan investigasi atau pengembangannya.

Meskipun pertanyaan-pertanyaan dari *investigator* mengiringi rekaman video tersebut dapat dijawab dengan baik oleh *digital forensic analyst*, namun satu hal yang pasti adalah rekaman video bersifat *volatile*, artinya rekaman tersebut dapat dengan mudah dirubah atau direkayasa, mulai dari yang mudah untuk dikenali hingga sulit untuk diketahui. Hal ini disampaikan dengan maksud agar *digital forensic analyst* dapat memahami bahwa

mereka harus lebih berhati-hati dalam melakukan analisa dan memberikan pernyataan yang berkaitan dengan rekaman video tersebut.

Pertanyaan-pertanyaan yang mengiringi barang bukti rekaman video seperti yang dijelaskan di atas akan dibahas pada bab ini, mulai dari analisa metadata dan *frame* untuk memastikan keaslian rekaman video hingga hal-hal yang berkaitan dengan teknik pembesaran objek pada rekaman video tersebut.

Analisa *Hash*

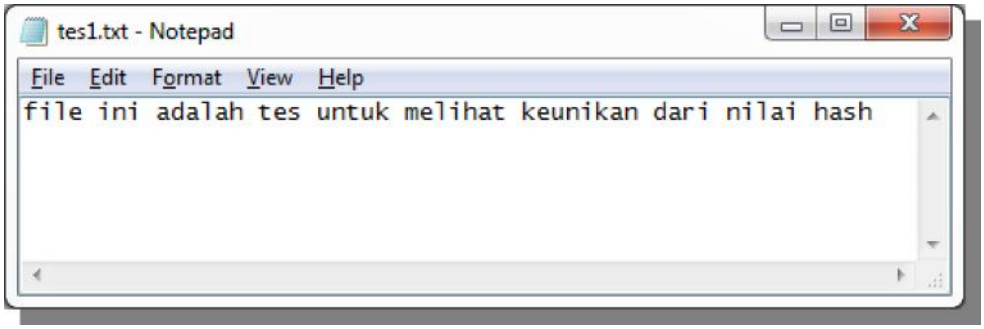
Dalam dunia digital forensik, terminologi "asli" merujuk kepada suatu *file* yang dibandingkan dengan *file* yang dianggap sumbernya, yang kemudian dilakukan proses *hashing* terhadap kedua *file* tersebut untuk melihat nilai *hash* dari masing-masing *file* di mana jika kedua *file* tersebut memiliki nilai *hash* yang sama maka *file* yang dibandingkan terhadap *file* sumber adalah identik dan dapat dinyatakan "asli". Sebaliknya jika *file* yang dibandingkan tersebut menunjukkan nilai *hash* yang berbeda dengan *file* sumber maka kedua *file* tersebut adalah tidak identik dan *file* yang dibandingkan tersebut dapat dinyatakan "tidak asli".

Dikarenakan *hash* memainkan peranan yang sangat vital untuk melihat keaslian dari suatu *file* maka banyak ahli yang menyatakan bahwa *hash* sebagai *digital fingerprint* (sidik jari digital). Istilah ini digunakan untuk merujuk penggunaan istilah sidik jari dalam dunia olah TKP (Tempat Kejadian Perkara) yang sebenarnya. Jika ditemukan sidik jari di TKP yang kemudian disebut dengan istilah sidik jari laten yang oleh *investigator* dianggap sebagai sidik jari pelaku kejahatan di TKP, maka sidik jari tersebut selanjutnya akan dibandingkan dengan database sidik jari yang ada, ataupun langsung dibandingkan dengan sidik jari yang diambil dari calon tersangka. Jika sidik jari laten tersebut identik dengan sidik jari yang diambil dari calon tersangka, maka sidik jari laten tersebut dinyatakan asli milik calon tersangka, dan oleh karena itu orang tersebut bisa dinaikkan statusnya sebagai tersangka.

Hash merupakan satu deret digit bilangan heksadesimal yang bersifat unik dan khas hasil dari pembacaan *header* dan isi dari suatu *file* dengan menggunakan algoritma tertentu seperti MD5, MD4, SHA1, SHA256, SHA384, SHA512,

RIPEMD160, CRC32 dan lain-lain. Dari sekian banyak algoritma tersebut, yang paling sering digunakan pada saat ini adalah MD5, SHA1 dan SHA256. Masing-masing algortima tersebut memiliki panjang digit yang berbeda antara satu algoritma dengan algoritma yang lain, misalnya algortima MD5 yang memiliki 32 digit bilangan heksadesimal, sedangkan algoritma SHA1 dan SHA256 masing-masing memiliki 40 dan 64 digit bilangan heksadesimal. Hal ini kontras dengan algoritma CRC32 yang dulu sering dipakai di mana CRC32 memiliki hanya 8 digit bilangan heksadesimal. Jumlah digit bilangan heksadesimal yang panjang akan menunjukkan keunikan dan kekhasan dari suatu *file* yang semakin teliti.

Berikut adalah contoh penggunaan *hashing* untuk melihat ke-identik-an suatu *file*. Misalnya dibuat suatu *file* teks dengan nama tes1.txt. Isi dari *file* tersebut adalah "*file* ini adalah tes untuk melihat keunikan dari nilai *hash*" tanpa tanda kutip, seperti yang terlihat pada gambar di bawah ini.



Gambar IX.1. File tes1.txt yang berisikan kalimat "*file* ini adalah tes untuk melihat keunikan dari nilai *hash*" tanpa tanda kutip, yang kemudian dilakukan proses *hashing*.

Terhadap *file* tes1.txt tersebut dilakukan proses *hashing* dengan menggunakan aplikasi HashCalc yang dikembangkan oleh SlavaSoft. Hasil dari proses *hashing* adalah sebagai berikut :

Algoritma MD5 : 4ae39f9ff9323c703b1b4a9a68c603ed

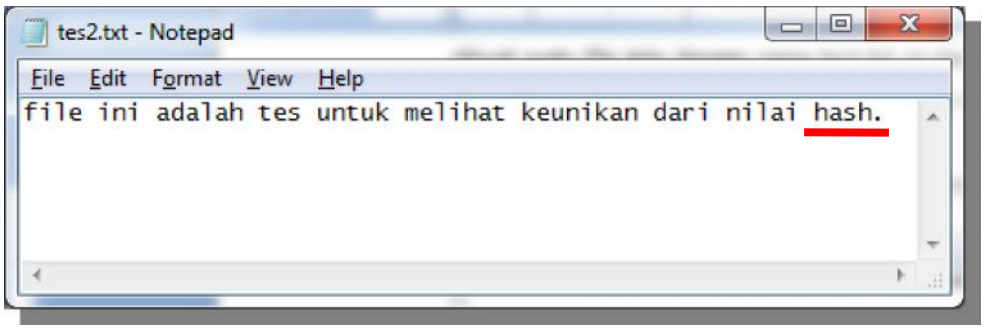
Algoritma SHA1 : bd90c9d2d57c22cefd027799462fb6c71fddff1c

Algortima SHA256 :

947258fcd4f6ccdadae1f68875f21cebe918c77ea028f33358baf6ca794e1c64

Kemudian *file* tes1.txt dibuka dan sedikit dilakukan modifikasi dengan menambahkan **titik** di akhir kalimat, selanjutnya *file* tersebut di '*save as*'

(disimpan sebagai fi*l*e baru) dengan nama tes2.txt seperti yang terlihat pada gambar di bawah ini.



Gambar IX.2. *File* tes2.txt berisikan kalimat seperti tes1.txt namun ditambahkan dengan **titik** di akhir kalimat, selanjutnya terhadap *file* ini dilakukan proses *hashing*.

Terhadap *file* tes2.txt tersebut juga dilakukan proses *hashing* yang hasilnya sebagai berikut :

Algoritma MD5 : 2922173acaeff12cd3c9949a2e511d85

Algoritma SHA1 : d9bb79eedb7d8b705ed062482c2ed33f63ad7d29

Algoritma SHA256 :

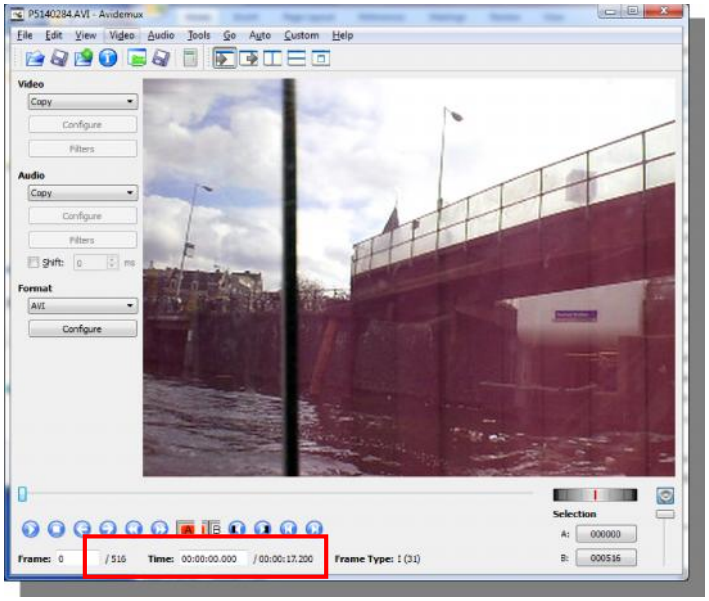
378171db41f6f859938227584ed45229a667f2df9c20a48a2bfa5b43827bc907

Hasil proses *hashing* terhadap kedua *file* tersebut selanjutnya dibandingkan. Diketahui bahwa nilai masing-masing algoritma MD5, SHA1 dan SHA256 untuk kedua fi*l*e tersebut sangat jauh berbeda, walaupun dari isi kedua *file* hanya berbeda "**titik**" di akhir kalimat. Dari fakta ini dapat diketahui bahwa algoritma *hash* memainkan peranan yang sangat penting untuk melihat ke-identik-an dari suatu *file* yang dibandingkan *file* lain yang dianggap sebagai sumbernya. Oleh karena itu, adalah wajar jika banyak ahli menyatakan bahwa *hash* merupakan *digital fingerprint*. Untuk membandingkan 2 buah *file* yang memiliki isi yang besar dan kalimat yang sangat panjang, maka untuk mengecek ke-identik-an kedua fi*l*e tersebut, *digital forensic analyst/investigator* bisa langsung melakukan proses *hashing* terhadap kedua *file* tersebut, tanpa perlu melihat dan membaca isinya. Jika nilai algoritma *hash* MD5, SHA1 dan SHA256 antara kedua *file* tersebut adalah sama, maka kedua *file* tersebut adalah identik, sebaliknya jika nilainya berbeda

maka kedua *file* tersebut adalah tidak identik. Jika identik, maka *file* yang dibandingkan terhadap *file* sumber dapat dinyatakan sebagai asli.

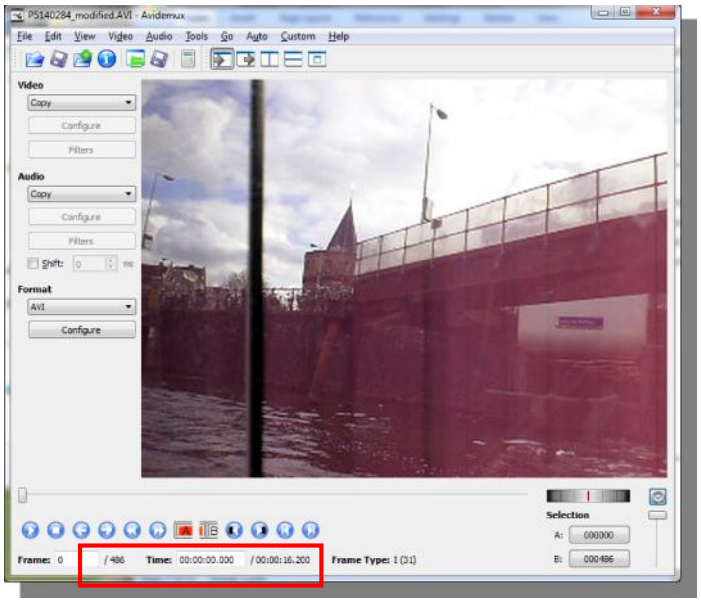
Hal yang sama juga dilakukan terhadap *file* rekaman video. Untuk melihat keaslian rekaman video tersebut, maka sebaiknya *investigator* berusaha untuk mendapatkan *file* yang diduga sumbernya. Selanjutnya terhadap rekaman video yang dipertanyakan tersebut dilakukan proses *hashing* untuk mendapatkan nilai algoritma MD5, SHA1 dan SHA256. Hal yang sama dilakukan terhadap *file* yang merupakan sumbernya. Selanjutnya nilai agoritma *hash* dari kedua *file* rekaman video tersebut dibandingkan. Jika nilainya sama, maka rekaman video yang dipertanyakan adalah asli, sebaliknya jika nilainya berbeda maka rekaman video tersebut adalah tidak asli. Kesimpulan ini mengacu pada nilai algoritma *hash* dari rekaman video sumber. Proses *hashing* ini perlu dilakukan terhadap rekaman video yang dipertanyakan, karena seperti yang sempat disinggung di awal bab ini bahwa rekaman video sifatnya *volatile*, artinya mudah sekali untuk dirubah dan direkayasa sesuai yang diinginkan oleh pelaku.

Berikut adalah contoh *file* rekaman video berformat avi. *File* video pertama yang dianggap sebagai sumber berdurasi 17,2 detik dengan *frame rate* 30 *frame* per detik (fps), sehingga *file* video tersebut memiliki 516 *frame* secara keseluruhan seperti yang terlihat pada gambar di bawah ini.



Gambar IX.3. *File* rekaman video pertama sebagai sumber memiliki 516 *frame* dengan durasi 17,2 detik.

Kemudian terhadap *file* video sumber tersebut dilakukan proses modifikasi yaitu menghilangkan 1 detik pertama dari rekaman sebanyak 30 *frame*, selanjutnya *file* di '*save as*' (disimpan sebaga *file* baru) dengan nama yang berbeda. *File* kedua hasil modifikasi ini berdurasi 16,2 detik dengan jumlah 486 *frame* secara keseluruhan, seperti yang terlihat pada gambar di bawah ini.



Gambar IX.4. *File* rekaman video kedua hasil modifikasi berdurasi 16,2 detik dengan jumlah total 486 *frame*.

Modifikasi rekaman video tersebut menggunakan aplikasi Avidemux yang merupakan aplikasi *free open-source* untuk *video editor*.

Terhadap *file* video pertama sebagai sumber ini dilakukan proses *hashing* dengan hasil sebagai berikut :

Algoritma MD5 : 2d652e0f65619a12d17b66870bbd8a94

Algoritma SHA1 : 2813cb2ff38da51d4a168dafe266fa677275685d

Algoritma SHA256 :

e3c51baafb0fdf5e818a42d44d872ba6207e3b0f75d5a450f805b7b19a34ceda

Hal yang sama dilakukan terhadap *file* video kedua hasil modifikasi dengan nilai *hash* sebagai berikut :

Algoritma MD5 : 17c492c4866195320ee44ba4bcab0b45

Algoritma SHA1 : 513f46a045d0a87837c8d76b2c9f8d35fea5f5ef

Algoritma SHA256 :

d517239df59a9cd9f8682b4ad913a4f35a36230d64e07a0f4281afd696668194

Dengan melihat nilai algoritma *hash* MD5, SHA1 dan SHA256 dari kedua file tersebut, dapat diketahui bahwa nilai hash dari kedua *file* tersebut adalah berbeda, artinya *file* rekaman video kedua yang merupakan hasil modifikasi tidak identik dengan *file* pertama sebagai sumbernya, sehingga *file* kedua dapat dinyatakan tidak asli. Meskipun momen rekaman video tersebut adalah benar adanya dan hanya dipotong 1 detik di awal rekaman pertama, namun tetap rekaman video kedua yang merupakan hasil pemotongan dinyatakan tidak asli.

Kekurangan dari analisa *hash* ini untuk kepentingan meilhat keaslian suatu *file* rekaman video adalah analisa ini mensyaratkan untuk adanya *file* rekaman video yang menjadi sumbernya. Jika *file* sumber ini belum didapatkan maka pengecekan keaslian suatu *file* rekaman video dengan menggunakan analisa *hash* tidak dapat dilakukan. Namun jika *file* sumbernya ditemukan, maka hasil analisa *hash* ini memiliki posisi yang sangat kuat sekali untuk memastikan keaslian suatu *file* rekaman video.

Analisa metadata

Selain melihat nilai agoritma *hash* MD5, SHA1 dan SHA256 dari suatu *file* rekaman video, juga dilakukan analisa terhadap metadata yang ada pada rekaman video tersebut. Sempat disinggung sebelumnya bahwa setiap *file* termasuk *file* rekaman video sebenarnya terdiri dari *header*, isi dan *footer*. *Header* terletak pada beberapa atau banyak *byte* pertama sebelum isi, sedangkan *footer* terletak pada beberapa byte terakhir setelah isi. *Header* berisikan *file signature* seperti yang dijelaskan pada Tabel VI.1 di Bab VI sebelumnya, dan juga berisikan data-data khas yang disebut dengan istilah metadata.

Metadata juga didefenisikan sebagai ‘data mengenai data’, artinya data-data kecil yang di-*encoded* sedemikian rupa yang berisikan data besar yang lengkap tentang sesuatu. Untuk *file* rekaman video, metadata dapat berupa data-data tentang :

1. Informasi umum, berisikan data-data tentang tanggal/waktu kapan dibuatnya rekaman video tersebut, ukuran *file*, format *file*, durasi dan lain-lain.
2. *Codec* video, berisikan format *codec*, panjang x lebar resolusi, *frame rate*, ukuran *stream* dan lain-lain.
3. *Codec* audio, berisikan format *codec*, *channel* (yang menentukan mono atau stereo suatu rekaman audio di mana jika *channel*-nya satu menunjukkan mono, sedangkan jika *channel*-nya dua menunjukkan stereo), ukuran *stream* dan lain-lain.

Untuk lebih jelasnya, contoh di atas yang menggunakan 2 *file* rekaman video di mana *file* pertama yang merupakan sumber dan masih asli, sedangkan *file* yang kedua merupakan rekaman video yang sudah dilakukan *editing* dengan menghilangkan 30 frame pertama dari *file* pertama. Terhadap *file* pertama dilakukan analisa metadata dengan menggunakan aplikasi MediaInfo yang dikembangkan oleh MediaArea. Hasil ekstraksi metadata dengan aplikasi tersebut adalah sebagai berikut :

Informasi umum

Format	: AVI
Format/Info	: *Audio Video Interleave*
File size	: 11.2 MiB
Duration	: 17s 496ms
Overall bit rate	: 5 384 Kbps
Mastered date	: Sat *May* 14 23:15:25 2011
Writing application	: FE20,X15,C25
Writing library	: OLYMDigital CameraOLYMPUS DIGITAL CAMERA

Codec Video

Format	: JPEG
Codec ID	: MJPG
Duration	: 17s 233ms
Bit rate	: 5 392 Kbps
Width	: 320 pixels
Height	: 240 pixels
Display aspect ratio	: 4:3
Frame rate	: 30.000 fps
Color space	: YUV

Chroma subsampling : 4:2:2
Bit depth : 8 bits
Scan type : Progressive
Compression mode : Lossy
Bits/(*Pixel***Frame*) : 2.340
Stream size : 11.1 MiB (99%)

Codec Audio

Format : PCM
Format settings, *Sign* : *Unsigned*
Codec ID : 1
Duration : 17s 496ms
Bit rate mode : *Constant*
Bit rate : 64.0 Kbps
Channel(s) : 1 *channel*
Sampling rate : 8 000 Hz
Bit depth : 8 bits
Stream size : 137 KiB (1%)

Dari ekstraksi metadata di atas, dapat dianalisa dan diketahui bahwa *file* rekaman video pertama dibuat pada tanggal 14 Mei 2011 pukul 23:15:25 UTC dengan menggunakan peralatan rekam *Digital Camera* merk OLYMPUS. Ukuran *file* berformat avi tersebut adalah 11,2 MB dengan durasi sekitar 17 detik di mana *codec* video-nya adalah jpeg dengan resolusi 320 x 240 *pixels* dan *frame rate* 30 *frame* per detik, dan *codec* audio-nya adalah pcm dengan 1 *channel*, sedangkan ukuran *stream* masing-masing *codec* video dan audio adalah 99% dan 1%. Dari ukuran *stream* ini menunjukkan bahwa *codec* video bersifat sangat dominan terhadap isi keseluruhan dari *file* tersebut.

Selanjutnya terhadap *file* rekaman video kedua yang telah dimodifikasi dengan menggunakan Avidemux sebelumnya juga dilakukan proses yang sama, dan didapat hasil ekstraksi metadata-nya sebagai berikut :

Informasi Umum

Format : AVI
Format/Info : *Audio Video Interleave*
File size : 10.6 MiB
Duration : 16s 233ms
Overall bit rate : 5 471 Kbps

Codec Video

Format	: JPEG
Codec ID	: MJPG
Duration	: 16s 233ms
Bit rate	: 5 393 Kbps
Width	: 320 *pixels*
Height	: 240 *pixels*
Display aspect ratio	: 4:3
Frame rate	: 30.000 fps
Color space	: YUV
Chroma subsampling	: 4:2:2
Bit depth	: 8 bits
Scan type	: *Progressive*
Compression mode	: *Lossy*
Bits/(*Pixel***Frame*)	: 2.341
Stream size	: 10.4 MiB (99%)

Codec Audio

Format	: PCM
Format settings, Sign	: *Unsigned*
Codec ID	: 1
Duration	: 15s 880ms
Bit rate mode	: Constant
Bit rate	: 64.0 Kbps
Channel(s)	: 1 *channel*
Sampling rate	: 8 000 Hz
Bit depth	: 8 bits
Stream size	: 124 KiB (1%)

Dari ekstrasi metadata tersebut di atas, dapat dianalisa dan diketahui bahwa *file* kedua hasil modifikasi sebelumnya tidak lagi mencantumkan data tentang peralatan rekam yang digunakan yaitu *digital camera* merk Olympus seperti yang terdapat pada *file* pertama, di samping *mastered date* yang menunjukkan tanggal/waktu pembuatan rekaman video. Dari fakta ini dapat ditarik suatu kesimpulan bahwa jikalau pada rekaman video tersebut tidak ditemukan *writing library*/*application* yang menunjukkan peralatan rekam dan *mastered date* yang menunjukkan tanggal/waktu pembuatan, maka sangat memungkinkan *file* rekaman video tersebut adalah hasil dari proses *editing*. Pada saat ini hampir semua peralatan rekam yang bersifat digital, baik *digital camera* maupun *handycam* memasukkan metadata *writing library/application* dan *mastered date* terhadap semua *file* rekaman video-nya, terkecuali *handphone* yang baru

sebagian *vendor* yang mengakomodasi kedua metadata tersebut. Namun adakalanya bagi vendor yang belum mengakomodasi *writing library/application*, mereka sebenarnya telah memasukkan metadata *mastered date* yang menunjukkan tanggal/waktu pembuatan rekaman video. Untuk itu jika suatu *file* rekaman video memiliki metadata mastered date namun tidak memiliki *writing library/application*, maka *file* rekaman video tersebut bisa dianggap asli dengan kondisi seperti yang telah dijelaskan di atas.

Untuk informasi umum lain, *codec* video dan audio, hampir semua metadata memiliki nilai yang sama seperti format *codec* video, panjang dan lebar resolusi, *frame rate*, format *codec* audio, *channel* dan lain-lain. Adapun metadata yang berbeda antara lain ukuran *file* dan durasi. Hal ini disebabkan *file* rekaman video kedua ini merupakan editing terhadap *file* rekaman pertama dengan memotong 30 *frame* pertamanya sehingga menyebabkan ukuran *file* menjadi berkurang dan durasinya menjadi lebih pendek.

Dari penjelasan terhadap contoh kedua *file* rekaman video di atas, dapat disimpulkan bahwa analisa metadata dapat menjadi salah satu cara untuk mengetahui keaslian suatu *file* rekaman video dengan mencari *metadata writing library/application* yang menunjukkan peralatam rekam digital yang digunakan dan/atau *mastered date* yang menunjukkan tanggal / waktu pembuatan rekaman video.

Untuk *file* video yang berasal dari internet melalui proses *uploading-downloading*, adakalanya sumber *server* atau *website* dari rekaman video tersebut dapat diketahui karena data mengenai hal tersebut tercatat dalam metadata-nya. Contoh berikut di bawah ini adalah *file* video yang di-*download* dari Facebook. Hasil ekstraksi metadata-nya didapat hasil sebagai berikut :

Informasi Umum

Format	: MPEG-4
Format *profile*	: Facebook
Codec ID	: FACE
File size	: 473 KiB
Duration	: 15s 0ms
Overall bit rate	: 258 Kbps
Encoded date	: UTC 2010-07-25 21:22:20

Dari data tersebut, dapat diketahui dan dianalisa bahwa dengan adanya *codec* ID FACE dan format *profile* Facebook dapat disimpulkan bahwa *file* rekaman video ini berasal dari proses *downloading* dari *website* www.facebook.com. *File* video itu sendiri di-*upload* ke *website* Facebook pada tanggal 25 Juli 2010 pada pukul 21:22:20 UTC (*Universal Time Code*, yang mengacu kepada waktu Greenwhich) seperti yang ditunjukkan pada metadata *encoded date*, yaitu tanggal/waktu yang menunjukkan kapan *file* video tersebut dilakukan proses *encoding* ke bentuk format MPEG-4 dengan *codec* ID FACE.

Untuk *file* rekaman video yang berasal dari website lain seperti youtube.com. hal yang hampir sama juga berlaku pada file video hasil proses *downloading* dari *website* tersebut, seperti pada contoh di bawah ini.

Informasi Umum

Format	: MPEG-4
Format *profile*	: *Base Media* / *Version* 2
Codec ID	: mp42
File size	: 14.5 MiB
Duration	: 3mn 23s
Overall bit rate	: 600 Kbps
Encoded date	: UTC 2007-09-25 02:50:54
gssd	: BADC23163HH1307805256244145
gshh	: v3.nonxt8.c.youtube.com

Dari data-data di atas, dapat diketahui bahwa *file* rekaman video berasal dari proses *downloading* dari *website* youtube.com dengan *link server* v3.nonxt8.c.youtube.com. *File* tersebut di-*upload* ke *website* Youtube pada tanggal 25 September 2007 pada pukul 02:50:54 UTC.

Dari kedua contoh di atas, dapat disimpulkan bahwa untuk *file-file* rekaman video yang berasal dari internet, masih memungkinkan untuk mendapatkan identitas webs*i*te sumber-nya di mana *file* tersebut di-*download* dan juga termasuk tanggal *upload*-nya ke *website* tersebut.

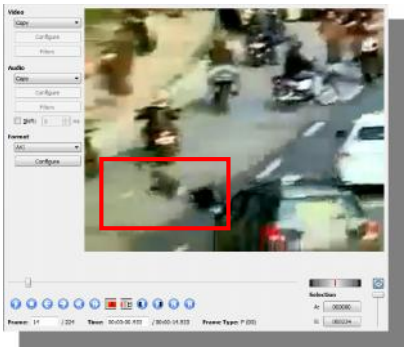
Analisa frame

Di samping analisa *hash* dan metadata yang sudah dijelaskan di atas, juga ada analisa *frame* yang biasa dilakukan untuk memastikan ada tidaknya proses *editing* yang menyebabkan *frame-frame* tersebut terlihat tidak normal (tidak alamiah). Seperti yang telah dijelaskan sebelumnya tentang *frame* per detik (fps), artinya suatu rekaman video pada hakikatnya merupakan susunan *frame-frame* dalam jumlah yang banyak yang menyusun rekaman tersebut mulai dari *frame* pertama hingga akhir sehingga jadilah rekaman video yang berisikan objek-objek yang bergerak (*moving objek*). Semakin tinggi nilai fps dan tingkat resolusi-nya maka rekaman video tersebut akan memiliki kualitas yang semakin baik dan memuaskan untuk ditonton. Hal ini dikarenakan gambar *moving objek*-nya tidak patah-patah dan bersifat normal (alamiah).

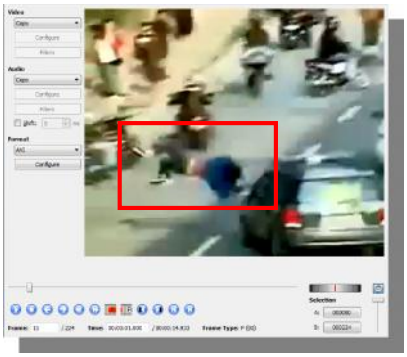
Dikarenakan video tersusun dari *frame-frame* dalam jumlah banyak, maka *frame-frame* ini selanjutnya dapat dianalisa untuk melihat tingkatan alamiah/wajar dari *moving objeks* yang ada di rekaman video tersebut. Jika terdapat *frame-frame* yang menunjukkan ketidakwajaran gerakan dari *moving objeks* maka dapat disimpulkan bahwa *file* rekaman video tersebut telah melalui proses *editing* sebelumnya. Berikut adalah contoh *file* rekaman video yang berasal dari proses *downloading* dari *website* facebook.com.



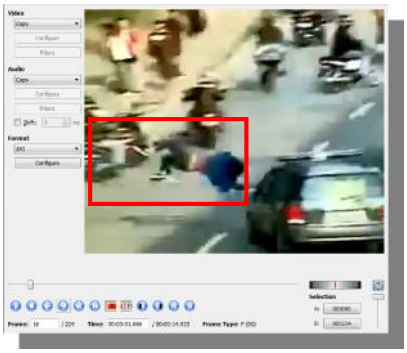
(i) *Frame* 13



(ii) *Frame* 14



(iii) *Frame* 15



(iv) *Frame* 16

Gambar IX.5. Empat buah yang berurutan mulai dari *frame* 13 s/d 16 yang menunjukkan ketidakwajaran gerakan dan bentuk dari *moving objek*.

Dari gambar di atas, dapat dilihat bahwa *moving objek* berupa orang yang terpental ketika ditabrak mobil menunjukkan hal yang wajar pada *frame* 13, 14 dan frame-frame sebelumnya, namun ketika berpindah dari *frame* 14 ke 15, ternyata ada perubahan gerakan dan bentuk yang bersifat ekstrim dari *moving objek* tersebut. Selanjutnya dari frame 15, 16 dan *frame-frame* seterusnya gerakan *moving objek* tersebut bersifat wajar.

Ketidakwajaran dari *moving objek* hanya pada perpindahan dari frame 14 ke 15. Ketidakwajaran tersebut adalah *moving objek* tersebut secara tiba-tiba gerakan dan bentuknya berubah menjadi lebih besar, perubahan bentuk dan gerakan tidak terjadi secara bertahap. Hal ini mengindikasikan adanya pemotongan beberapa *frame* yang terletak di antara *frame* 14 dan 15. Jika ada beberapa *frame* yang sebenarnya terletak di antara *frame* 14 dan 15, maka gerakan dan bentuk *moving objek* tersebut akan lebih halus dan wajar.



(i) *Frame* 26 (ii) *Frame* 27 (iii) *Frame* 28



(iv) *Frame* 29 (v) *Frame* 30 (vi) *Frame* 31

Gambar IX.6. *Frame* 26 dan 27 masih menunjukkan gerakan dan bentuk *moving objek* yang wajar, namun pada *frame* 28 s/d 31 gerakan dan bentuk *moving objek* tiba-tiba berhenti sebanyak 4 *frame*.

Dari gambar di atas, masih pada *file* rekaman video yang sama, diketahui bahwa pada *frame* 26, 27 dan *frame-frame* sebelumnya masih menunjukkan bentuk dan gerakan *moving objek* yang wajar, namun pada frame 28 s/d 31, tiba-tiba bentuk dan gerakan *moving objek* berhenti sebanyak 4 *frame*, selanjutnya pada frame 32 dan seterusnya *moving objek* melanjutkan gerkan dan bentuknya lagi. Untuk objek yang bergerak di atas udara, hal ini bersifat mustahil bahwa objek tersebut berhenti bergerak sebanyak 4 *frame* secara berurutan. Secara logika, jika ada ojek berhenti bergerak di udara, maka ia akan jatuh ke bumi akibat gravitasi bumi, sedangkan pada kasus ini, setelah berhenti sebanyak 4 *frame*, objek tersebut melanjutkan gerakannya kembali. Hal ini mengindikasikan adanya peng-*copy*-an dan *paste frame* 28 sebanyak 3 kali dan diletakkan setelah *frame* 28 tersebut, sehingga sebanyak 4 *frame* mulai dari *frame* 28 *moving objek* dan benda-benda sekitarnya terlihat tidak bergerak sama sekali.

Dari kedua contoh analisa *frame* tersebut terhadap *file* rekaman video dapat disimpulkan bahwa rekaman video tersebut telah melalui proses *editing* di mana

terjadinya indikasi pemotongan beberapa *frame* antara *frame* 14 dan 15, dan indikasi adanya *copy-paste frame* 28 sebanyak 3 kali dan diletakkan setelah *frame* 28 tersebut. Adanya 2 indikasi tersebut menunjukkan bahwa *file* video tersebut sudah dimodifikasi dan sudah sewajarnya dinyatakan bahwa *file* rekaman video tersebut sudah tidak asli.

Analisa berbasis frame ini dapat melihat perubahan gerakan dan bentuk *moving objek* secara teliti secara frame per frame, oleh karena itu analisa *frame* ini sering digunakan untuk memastikan ada tidaknya proses *editing* terhadap *file* rekaman video yang dipertanyakan. Analisa ini juga sangat bagus untuk mendukung 2 analisa sebelumnya, yaitu analisa *hash* dan metadata untuk memastikan keaslian dari suatu *file* rekaman video.

Teknik pembesaran

Teknik ini sering diimplementasikan ketika *digital forensic analyst* berhubungan dengan rekaman video yang berasal dari kamera cctv. Kamera cctv ini dikarenakan fungsinya untuk keamanan suatu tempat tertentu, maka kamera ini hidup dan beroperasi selama 24 jam penuh dalam 1 hari. Ketika ada seseorang yang dicurigai melakukan suatu tindakan kejahatan dan berada di dekat kamera tersebut maka ia dan kegiatannya juga semestinya terekam oleh kamera tersebut. Dengan adanya rekaman yang berharga tersebut, maka orang tersebut dapat ter-identifikasi setelah melalui serangkaian proses pembesaran. Untuk selanjutnya orang tersebut berikut kegiatannya dan/atau identitasnya yang lain dapat diketahui dan dilakukan pencarian oleh investigator untuk kemudian ditangkap untuk mempertanggungjawabkan kejahatannya.

Proses pembesaran yang dilakukan terhadap objek yang ada di dalam rekaman cctv sebenarnya dipengaruhi oleh 4 faktor utama, yaitu :

1. Dimensi objek

   Artinya besarnya ukuran objek. Jika objek yang akan diperbesar memiliki ukuran sebenarnya yang kecil, maka pembesaran yang dilakukan terhadap objek pada rekaman cctv tersebut tidak akan maksimal.

2. Jarak objek dengan kamera cctv

   Walaupun dimensi objek yang sebenarnya besar, namun jika ia terekam oleh kamera cctv dari jarak yang jauh, sehingga terlihat kecil di dalam rekaman, maka pembesaran terhadap objek tersebut juga tidak akan maksimal.

3. Intensitas cahaya

   Level cahaya juga ikut mempengaruhi objek yang akan diperbesar. Jika objek dalam rekaman yang diperbesar memiliki level intensitas cahaya yang kurang sehingga remang-remang atau bahkan gelap sebagian, maka pembesaran terhadap objek tersebut juga tidak akan maksimal

4. Resolusi kamera

   Jika dimensi yang sebenarnya dari objek tersebut adalah besar dan terletak di dekat kamera dengan level intensitas cahaya yang cukup, namun kamera cctv yang digunakan untuk merekam ini memliki kualitas resolusi yang rendah sehingga rekaman yang dihasilkan tidak jelas dan gambarnya patah-patah, maka pembesaran terhadap objek yang ada di rekaman cctv tersebut juga tidak akan maksimal.

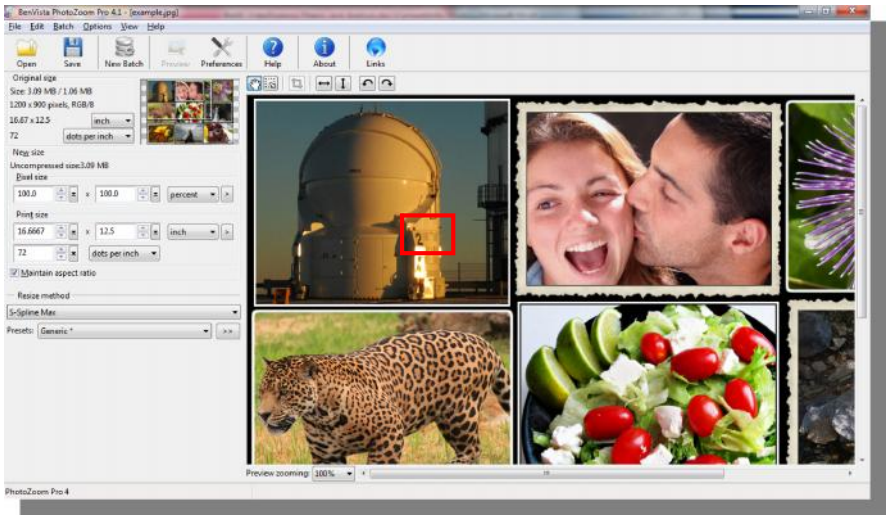
Dari penjelasan di atas, jika keempat syarat utama tersebut dapat terpenuhi, artinya dimensi objek cukup besar dan terletak di dekat kamera beresolusi tinggi dengan intensitas pencahayaan yang cukup, maka pembesaran terhadap objek yang ada di dalam rekaman kamera cctv tersebut dapat dilakukan secara maksimal.

Untuk proses pembesaran objek, rekaman video harus memiliki kualitas yang bagus. Jika rekaman tersebut masih kurang cahaya, sedikit *blurred* (kurang jelas) dan sedikit tidak stabil, maka rekaman tersebut harus dipertinggi kualitasnya (*enhancement*). Ada banyak cara untuk meningkatkan kualitas rekaman, salah satunya menggunakan aplikasi vReveal yang dikembangkan MotionDSP. Dengan aplikasi ini, suatu rekaman video dapat diproses dengan mudah untuk meningkatkan kualitasnya mulai dari *deinterlace* (proses menghilangkan garis-garis gambar yang bersifat tidak linear), *sharpen* (memperjelas titik-titik gambar yang blurred, *auto white balance* (merapikan warna-warna yang bersifat tidak natural), *fill light* (menambah intensitas cahaya lingkungan), *stabilize* (membuat

video yang bergoyang menjadi stabil), *clean* (menghilangkan noise artifacts seperti *grain*/butiran, *pixellation*, *jagged edges* dan lain-lain), *auto contrast* (meningkatkan level kontras rekaman, *vivid colors* (meningkatkan level pewarnaan) dan lain-lain.

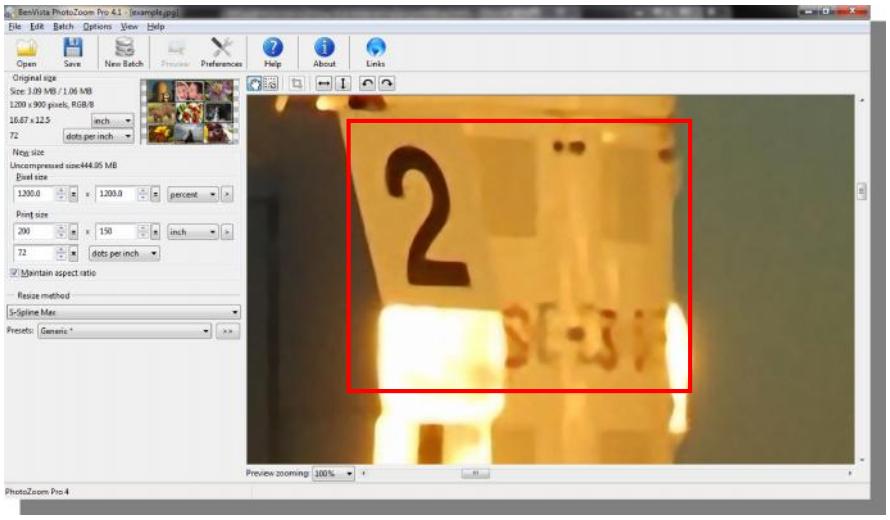
Setelah didapatkan kualitas rekaman video yang baik, maka selanjutnya rekaman tersebut diekstraksi *frame-frame* yang menyusun rekaman tersebut menjadi gambar-gambar berformat jpeg. Gambar-gambar tersebut kemudian difilter untuk mencari gambar yang mana yang menunjukkan kualitas objek yang lebih baik dibandingkan gambar yang lain. Jika kualitas objek pada gambar hasil ekstraksi *frame* masih belum memuaskan, maka kualitas gambar objek sebaiknya ditingkatkan dulu. Ada banyak cara untuk meningkat kualitas gambar, antara lain menggunakan aplikasi *Photo*! *Editor* yang dikembangkan oleh VicMan Software. Aplikasi ini menawarkan fitur *enhance color* (melakukan koreksi pewarnaan), denoise (menghilangkan *noise artifacts*), *deblur* (menghilangkan *blurred*/gambar yang tidak jelas), *lighting* (menambah efek cahaya gambar) dan lain-lain.

Setelah didapatkan kualitas gambar yang memuaskan, selanjutnya baru dilakukan proses pembesaran terhadap objek yang diinginkan. Kualitas pembesaran objek gambar tergantung pada jenis algoritma yang digunakan misalnya *fractal*, s-*spline*, *lanczos*, *bicubic* dan lain-lain. Dari banyak algoritma yang tersedia, ada 2 yang sering digunakan yaitu *fractal* dan s-*spline*. Kedua algoritma ini dapat memberikan pembesaran hingga puluhan ribu kali dengan tetap menghasilkan kualitas pixel yang masih baik, tidak patah-patah antara *pixel*. Salah satu aplikasi yang memberikan fitur algortima s-*spline* adalah Photozoom *Pro* yang dikembangkan oleh BenVista. Pada contoh gambar default dari aplikasi ini dapat dilihat proses pembesaran yang dihasilkan pada gambar di bawah ini.



Gambar IX.7. Gambar *default* aplikasi yang sebelum dilakukan pembesaran. Kotak merah menunjukkan tulisan yang ingin dilakukan pembesaran.

Setelah dilakukan pembesaran hingga 1200 persen ukuran *pixel*-nya dari ukuran 100 persen yang sebenarnya maka tulisan yang ditandai dengan warna merah seperti pada gambar di atas dapat terlihat dengan jelas seperti pada gambar di bawah ini.



Gambar IX.8. Gambar hasil pembesaran sebesar 1200 persen yang menunjukkan tulisan yang ingin diperbesar.

Dari Gambar IX.8. diatas dapat dilihat bahwa tulisan yang ditandai dengan kotak merah pada Gambar IX.7. setelah melalui proses pembesaran dengan algoritma s-*spline* max sebesar 1200 persen adalah 2 SC – C3. Dapat dilihat pada gambar di

atas, pembesaran yang dilakukan tidak membuat *pixel* menjadi patah-patah, gambar yang dihasilkan tetap masih mulus.

Dari penjelasan di atas dapat disimpulkan bahwa proses pembesaran terhadap objek yang ada pada rekaman video haruslah terlebih dahulu meningkatkan kualitas rekaman menjadi lebih baik. Dengan kualitas yang tinggi, rekaman tersebut dapat diekstraksi gambar-gambar yang berasal dari *frame-frame* penyusun rekaman video dengan kualitas yang juga baik dan memuaskan. Jikalau hasil dari proses ini belum maksimal, maka kualitas gambar hasil ekstraksi juga masih bisa dilakukan proses *enhancement* (peningkatan kualitas) agar didapat kualitas objek pada gambar yang baik. Proses pembesaran terhadap objek yang telah ditingkatkan kualitasnya akan menghasilkan pembesaran yang maksimal dan memuaskan. Meskipun begitu, proses pembesaran terhadap objek yang ada pada rekaman cctv tetap tergantung pada 4 faktor utama yang sempat dibahas di atas, yaitu dimensi objek, jarak objek dengan kamera cctv, intensitas cahaya dan resolusi kamera.

Bibliography

1. ACPO, 7Safe (2008). *Good Practice Guide for Computer-Based Electronic Evidence*. UK ACPO and 7Safe.
2. Al-Azhar, M.N. (2010). *Standard Operating Procedure (SOP) 8 : Prosedur Pemeriksaan Digital Forensik*. DFAT Puslabfor.
3. Carrier, B. (2002). *Open Source Digital Forensic Tools: The Legal Argument.* @stake.
4. Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Elsevier Academic Press.
5. Johnson, T. A. (2005). *Forensic Computer Crime Investigation*. Taylor & Francis.
6. Kessler, G. (2011). *File Signatures Table.* http://www.garykessler.net/library/file_sigs.html.
7. Middleton, B. (2002). *Cyber Crime Field Handbook*. CRC Press

8. National Institute of Justice (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. US National Institute of Justice
9. National Institute of Justice (2001). *Electronic Crime Scene Investigation: A Guide for First Responder*. US National Institute of Justice.
10. Sammes, T. and Jenkinson, B. (2007). *Forensic Computing: A Practitioner's Guide*. Springer.
11. Solomon, M. G. et al. (2005). *Computer Forensics Jumpstart*. Sybex.

Bab X

IMAGE FORENSIC: Theory and Analysis

Dalam *image forensic*, objek yang diperiksa dan dianalisis adalah *image file*. *Image file* itu sendiri memiliki 2 pengertian yang berbeda, pertama merujuk kepada hasil *forensic imaging* (duplikasi secara *physical sector per sector*) yang menggunakan metode terkini *disk to file*, dan yang kedua merujuk ke *file* gambar hasil photography menggunakan kamera, bisa kamera digital, *handycam* atau *handphone* yang menggunakan sistem penyimpanan *file* digital. Yang dibahas di dalam bab ini adalah yang kedua, yaitu *file* gambar digital.

File gambar digital berasal dari hasil proses *capturing* (menangkap) objek dengan menggunakan peralatan kamera yang bersifat digital. Ini dilakukan oleh seseorang dalam rangka mengabadikan momen-momen yang penting di sekitarnya sehingga di kemudian hari ia bisa membuka dan melihat kembali momen tersebut melalui *file* gambar digital yang telah dihasilkan. Ketika ia merasa momen yang penting dan baik tersebut perlu untuk di-*sharing* (berbagi) dengan teman-temannya, maka ia akan berbagi *file* gambar tersebut dengan mereka. Ada yang menggunakan kabel data USB dengan bantuan komputer, dan ada juga yang langsung berbagi dengan menggunakan *bluetooth* dari *device to device*, misalnya *handphone* ke *handphone*. Namun pada saat ini ada juga yang langsung *upload* gambar tersebut ke internet, biasanya ke *social website* seperti Facebook atau ia bisa *upload* gambar tersebut ke *social group* seperti BBM (*BlackBerry Messenger*) sehingga gambar tersebut akan langsung diketahui teman-temannya secara *online*. Adakalanya gambar tersebut oleh yang ahli *editing* grafis diolah terlebih dahulu dengan bantuan aplikasi komputer sebelum di-*upload*.

Gambar-gambar digital tersebut bisa menyenangkan hati bagi orang atau teman-temannya yang melihat, namun bisa juga menimbulkan masalah ketika gambar tersebut menunjukkan momen yang menjelek-jelekkan orang lain, misalnya memfitnah orang lain dengan merekayasa gambar tersebut dengan bantuan aplikasi komputer seolah-olah orang tersebut melakukan hal yang tak senonoh atau tak sepantasnya, sehingga orang tersebut merasa malu dan tercemar nama baiknya. Bagi sebagian masyarakat awam yang

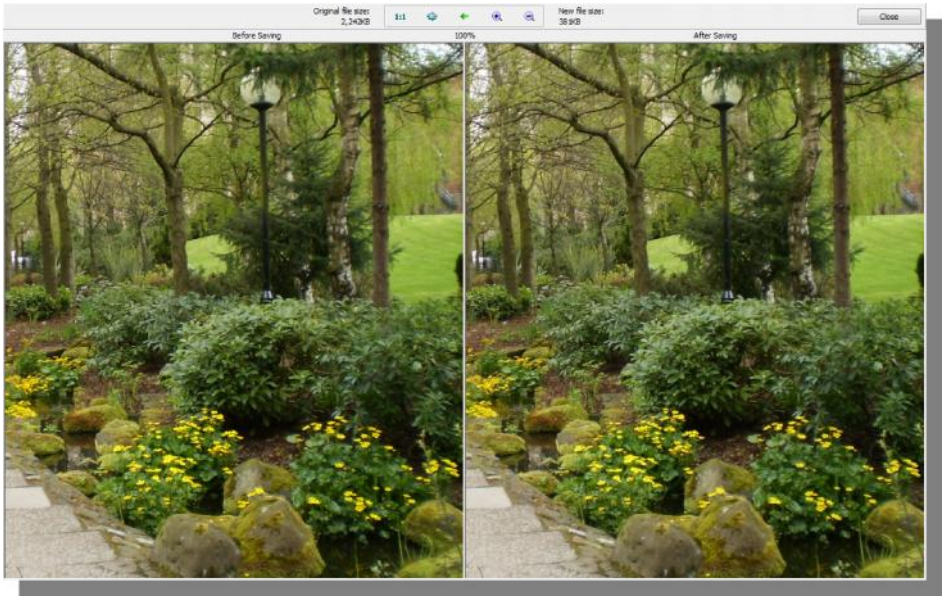
tidak memahami rekayasa gambar digital, maka mereka akan menganggap bahwa momen palsu yang ada di gambar digital tersebut seakan asli. Hal ini dapat berakibat harga diri dan posisi orang yang dijelek-jelekkan menjadi jatuh, baik di mata keluarga maupun rekan pekerjaan/bisnis.

Untuk hal-hal seperti ini, terhadap gambar digital tersebut perlu dilakukan pemeriksaan dan analisis yang mendalam untuk memastikan apakah gambar tersebut palsu hasil rekayasa grafis komputer, atau malah sebaliknya gambar tersebut asli hasil *capturing* dengan menggunakan peralatan photography. Bab ini akan membahas bagaimana analisa secara digital forensik terhadap *file* gambar digital, antara lain untuk memastikan keaslian gambar ataupun mencari historis proses *capturing* gambar tersebut, di samping jga membahas tentang teori gambar digital itu sendiri.

Format gambar digital

Ada banyak format *file* untuk gambar digital, misalnya bmp (*bitmap*) yang merupakan bentuk sebenarnya dari *file* gambar, png (*portable network graphics*) dan jpeg (*joint photographic experts group*) yang merupakan bentuk kompresi-nya. Format png didesain pada awalnya untuk menggantikan format gif (*graphics interchange format*) yang lama dan pada beberapa hal juga dianggap sebagai format tiff (*tagged image file format*) yang lebih kompleks. Ada banyak keuntungan penggunaan format png di internet dibandingkan format gif, misalnya *alpha channels* (yaitu tranparansi yang variabel), *gamma correction* (yaitu kontrol level cahaya gambar/*image brightness*), dan *two-dimensional interlacing* (yaitu metode jalinan tampilan yang maju/*progressive display*), di samping kemampuan kompresi yang lebih baik 5% s/d 25% dibandingkan format gif.

Dari sekian banyak format *file* untuk gambar digital, format yang sering digunakan untuk memproses *capturing* momen oleh peralatan fotografi digital adalah format jpeg. Format jpeg merupakan metode kompresi *file* gambar digital yang bersifat *lossy*, artinya metode ini mengabaikan beberapa data dari gambar digital tersebut yang akhirnya juga akan berdampak pada kualitas gambar. Semakin tinggi nilai kompresi yang diberikan kepada suatu gambar digital, maka akan semakin rendah kualitas gambar yang dihasilkan.



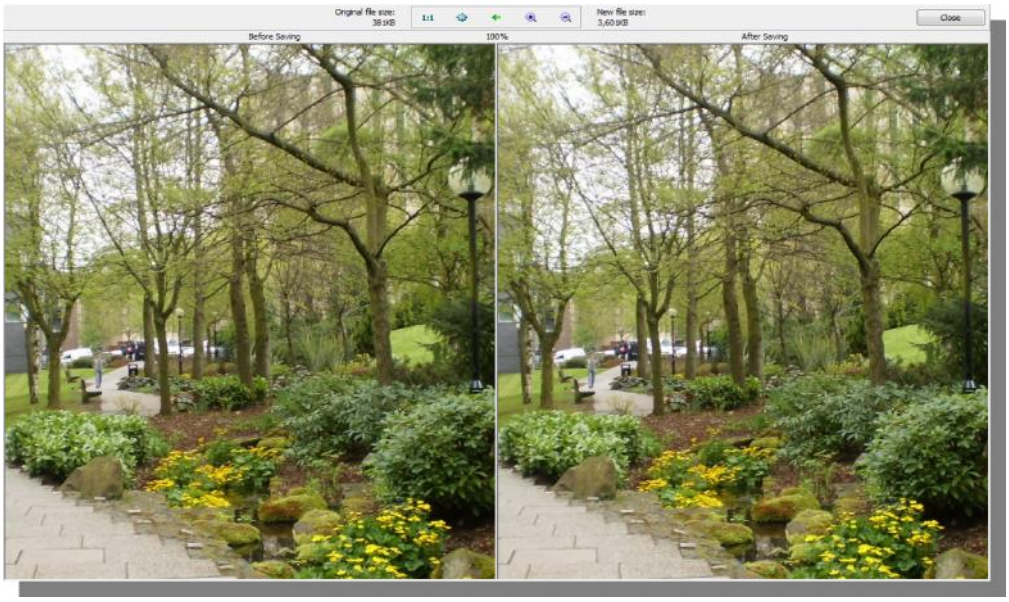
(i) (ii)

Gambar X.1. Perbandingan kualitas gambar setelah kompresi antara format png (i) dengan ukuran 2,2MB dan format jpeg (ii) dengan ukuran 381KB dengan metode kompresi jpeg 90%.

Di samping itu, kompresi ini juga berkaitan erat dengan ukuran *file* gambar, artinya semakin tinggi kompresi yang diberikan kepada gambar digital, maka semakin kecil ukuran *file* gambar tersebut. Oleh karena itu, level kompresi terhadap suatu gambar digital harus disesuaikan dengan kualitas dan ukuran (*size*) gambar yang akan dihasilkan. Dikarenakan ukuran gambar yang dihasilkan kecil namun tetap kualitas gambar digital masih terjaga melalui penyesuaian level kompresinya, jpeg sering digunakan sebagai format *file* gambar digital yang dihasilkan oleh peralatan fotografi saat ini.

Seperti pada Gambar X.1. di atas, kualitas gambar jpg yang dihasilkan setelah gambar dengan format png dikompresi sampai 90% tidak jauh berbeda dengan kualitas gambar aslinya. Dengan ukuran gambar format jpg yang hanya 381KB, artinya sekitar 17% dari ukuran yang sebenarnya 2,2 MB, dan dengan kualitas gambar yang masih baik, format jpeg menjadi pilihan utama para *developer* kamera digital untuk digunakan dalam setiap *capture* gambar digital yang dihasilkan dalam bentuk *file*. Dengan ukuran yang kecil (hanya 17% dari ukuran gambar png yang sebenarnya), *file-file* jpeg dapat disimpan dalam jumlah yang

banyak di *memory card* dari kamera digital. Secara ekonomi, hal ini sangat efisien. Apalagi kalau gambar format jpeg dibandingkan dengan format bmp seperti gambar di bawah ini. Pada Gambar tersebut, ukuran *file* jpeg yang 381KB sangat jauh sekali dengan gambar bmp yang 3,6MB, artinya ukuran 1 *file* jpeg sekitar 10% dari ukuran *file* bmp tanpa kompresi.



(i) (ii)

Gambar X.2. Perbandingan ukuran antara gambar format jpeg 381KB (i) dengan format bmp 3,6MB (ii) dengan kualitas gambar jpeg yang masih baik.

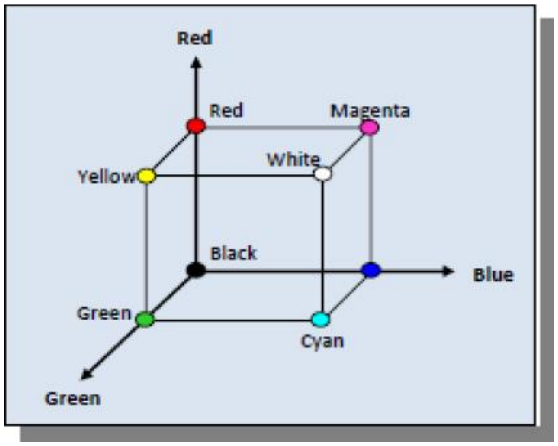
Dari penjelasan di atas, jika suatu kamera digital menggunakan *memory card* dengan ukuran 4GB, maka *memory card* tersebut akan dapat menampung sekitar 10.500 *file* jpeg dengan ukuran masing-masing *file* sekitar 380KB, namun jika format *file* dirubah menjadi bmp dan png, maka *memory card* tersebut akan dapat memuat masing-masing hanya sekitar 1.100 dan 1800 *file*. Dengan alasan efisiensi dan kualitas yang tidak jauh berbeda dengan level kompresi sekitar 90%, maka format jpeg banyak ditemukan pada *memory card* dari suatu kamera digital. Dengan alasan efisiensi yang sama, format jpeg ini pun banyak digunakan di internet. Dengan format jpeg, para pengguna internet dengan cepat untuk melakukan proses *upload* gambar digital ke *website* atau *account* mereka masing-masing, untuk kemudian di-*download* oleh pengguna internet yang lain juga dengan cepat.

Dikarenakan *format* jpeg banyak digunakan oleh peralatan fotografi digital saat ini, maka bab ini lebih banyak membahas tentang *image forensic* terhadap *file* gambar berformat jpeg tersebut. Asumsinya adalah jika barang bukti elektronik yang ditemukan di TKP adalah berupa kamera digital, maka *file-file* gambar yang ada atau tersimpan di *memory card* dari kamera tersebut sangat mungkin adalah berformat jpeg.

Istilah jpeg mengambil nama dari komite *Joint Photographic Experts Group* yang mengeluarkan standar dari format tersebut pada tahun 1992, yang kemudian diakui sebagai ISO/IEC 10918-1 di tahun 1994. Format jpeg ini mengatur bagaimana sebuah gambar digital dibuat dengan semestinya melalui metode kompresi serangkaian *byte* sehingga ukuran *file* jpeg menjadi lebih kecil, yaitu sekitar 10% dari *file* format bmp tanpa kompresi.

Pixel

Dalam proses gambar digital, unit gambar terkecil yang biasanya direpresentasikan dalam bentuk titik atau kotak kecil adalah *pixel*, di mana tiap-tiap *pixel* memiliki alamat masing-masing yang berbeda antara *pixel* yang satu dengan yang lain. Alamat *pixel* tersebut berkaitan erat dengan titik koordinasinya yang biasanya disusun berdasar pada *grid* (tabulasi) 2 dimensi. Masing-masing *pixel* memiliki intensitas warna sesuai dengan gambar yang diwakilinya. Intensitas warna *pixel* ini biasanya diwakili dalam sistem 3 komponen warna, yaitu merah, hijau dan biru (RGB – *Red Green Blue*).



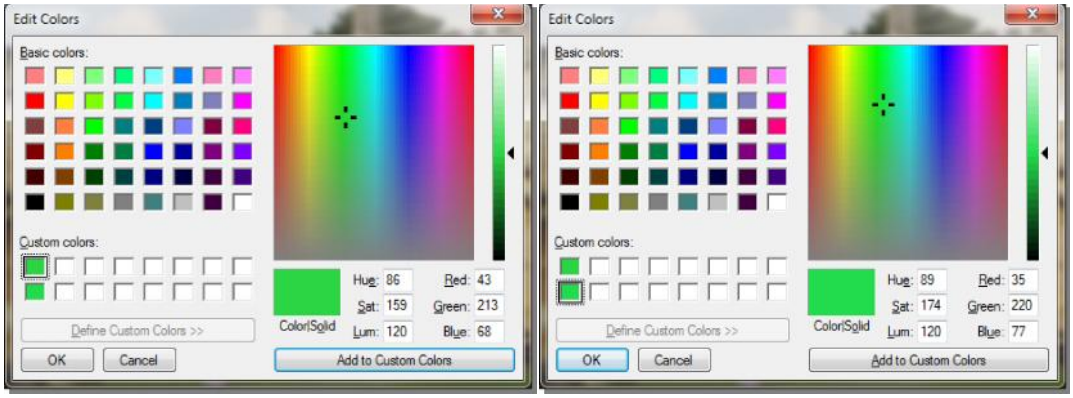
Gambar X.3. Sistem RGB (*Red* – *Green* – *Blue*) yang digunakan untuk intensitas warna *pixel* dalam menyusun suatu gambar digital.

Pada gambar di atas, diketahui bahwa tiap-tiap intensitas warna *pixel* disusun berdasarkan pada masing-masing sumbu warna merah (*Red*), hijau (*Green*) dan biru (*Blue*). Misalnya warna kuning yang disusun ketika warna hijau dan merah ada, sedangkan warna biru nol (tidak ada), begitu juga warna magenta yang disusun atas warna merah dan biru, sedangkan warna hijau tidak ada.

Tiap-tiap komponen RGB ini ditandai dengan satu *byte* sehingga jumlah total warna yang tersedia untuk setiap komponen adalah 256 jenis warna. Ini didapat karena 1 *byte* terdiri dari 8 *bit*, artinya jumlah total warna adalah 2^8 yaitu 256. Suatu gambar digital yang tersusun atas 3 komponen RGB memiliki jumlah total warna sebanyak 2^24 atau 256 x 3 yaitu 16.777.216 (lebih dari 16 juta) jenis warna. Artinya satu titik warna *pixel* disusun atas 24 *bit* yang terdiri dari 8 *bit* untuk masing-masing komponen warna RGB. Pada saat ini, banyak aplikasi digital membuat suatu gambar digital berdasarkan metode *pixel* 24 *bit* ini.

Pada gambar di bawah ini, dapat diketahui bahwa masing-masing *pixel* memiliki intensitas warna RGB yang berbeda sesuai dengan warna yang diwakilinya. Misalnya 2 warna hijau yang sulit dibedakan (i dan ii), ternyata *pixel* warna hijau (i) memiliki intensitas warna RGB 43-213-68, sedangkan yang (ii) adalah 35-220-77. Pada warna hijau yang pertama (i), intensitasnya diketahui adalah 43-213-68 untuk masing-masing komponen merah (*Red*), hijau (*Green*) dan biru (*Blue*). Dalam sistem bilangan heksadesimal, masing-masing angka tersebut bernilai 2b-d5-44, atau dalam sistem bilangan *binary*, bernilai 00101011-11010101-

01000100. Dengan menggunakan sistem *encoding* 24 *bit*, maka warna hijau pertama (i) ini ditandai dengan sistem bilangan heksadesimal 0x2bd544 yang setara dengan ukuran 3 *byte*.



(i) (ii)

Gambar X.4. *Pixel* dengan intensitas warna hijau yang didasarkan pada sistem 3 komponen warna RGB, di mana *pixel* dengan warna hijau (i) memiliki intensitas warna RGB 43-213-68, sedangkan *pixel* warna hijau yang lain (ii) memiliki intensitas warna RGB 35-220-77.

Ketika suatu gambar digital dibuat oleh suatu kamera digital, sebenarnya gambar digital tersebut terdiri dari sekian banyak *pixel* yang menyusunnya mulai dari *pixel* pertama di baris (sisi horisontal) dan kolom (sisi vertikal) pertama hingga *pixel* terakhir di baris dan kolom terakhir. *Pixel-pixel* yang menyusun gambar tersebut dalam sisi horisontal (lebar) dan vertikal (tinggi) bervariasi, misalnya 800 x 600 yang jumlah total *pixel*-nya adalah 480.000 *pixels* atau sama dengan 0.48 Mega *Pixels* (MP). Berikut adalah beberapa ukuran *pixel* dari suatau gambar digital yang sering digunakan :

- 640 x 480 = 0.31 MP
- 800 x 600 = 0.48 MP
- 1200 x 900 = 1.08 MP
- 1600 x 1200 = 1.92 MP
- 2048 x 1536 = 3.15 MP

Dikarenakan 1 titik *pixel* warna memiliki ukuran 3 *byte* yang berasal dari 1 *byte* (atau 8 *bit*) pada masing-masing komponen RGB, maka ukuran *pixel* tersebut di atas dapat diketahui ukuran *byte*-nya per 1 *file*, yaitu :

- 640 x 480 = 0.31 MP = 0.31 x 3 *byte/pixel* = 0.93 *megabyte* (MB)
- 800 x 600 = 0.48 MP = 0.48 x 3 *byte/pixel* = 1.44 MB
- 1200 x 900 = 1.08 MP = 1.08 x 3 *byte/pixel* = 3.24 MB
- 1600 x 1200 = 1.92 MP = 1.92 x 3 *byte/pixel* = 5.76 MB
- 2048 x 1536 = 3.15 MP = 3.15 x 3 *byte/pixel* = 9.45 MB

Ukuran *file* dalam *byte* tersebut di atas berlaku untuk suatu gambar digital yang belum mengalami kompresi, misalny format bmp seperti yang dijelaskan sebelumnya. Untuk *file* jpeg, ukuran tergantung pada seberapa level kompresi yang dibebankan kepadanya. Misalnya dengan level kompresi 90%, maka *file* jpeg akan berukuran sekitar 10% dari ukuran *file* bmp.

Semakin tinggi kualitas *pixel* yang digunakan, maka akan semakin banyak *space* dari media penyimpanan dari suatu kamera digital yang digunakan. Hal ini akan berdampak pada semakin sedikit jumlah gambar digital yang dapat disimpan di media tersebut. Untuk itu, pemilihan kualitas *pixel* haruslah disesuaikan dengan kebutuhan dan kapasitas dari media penyimpanan itu sendiri.

Di samping itu, juga diketahui bahwa semakin banyak jumlah total *pixel* yang menyusun suatu gambar digital akan semakin tinggi kualitasnya, sebaliknya semakin rendah jumlah total *pixel*, maka semakin rendah kualitas dari gambar digital tersebut. Efek dari jumlah total *pixel* yang tinggi adalah ketika dilakukan proses pembesaran (*zooming in*) terhadap suatu gambar digital, maka hasil pembesaran tersebut pada beberapa tahapan masih nampak jelas dan tidak kabur (*blurred*). Hal ini tidak dapat dilakukan terhadap gambar digital dengan jumlah total *pixel* yang rendah.

Banyaknya *pixel* yang menyusun suatu gambar digital dapat juga diketahui melalui satuan dpi, yaitu *dots per inch*, artinya dalam satu inchi ada berapa banyak *pixel* yang ada. Jika diketahui suatu gambar digital tersusun atas 300 dpi, maka itu artinya dalam setiap *inchi* terdapat 300 titik *pixel* yang menyusun gambar tersebut. Semakin tinggi nilai dpi, maka kualitas gambar digital tersebut akan semakin baik dan jelas.

Metadata EXIF

Exif atau *Exchangeable image file format* merupakan standar yang mengkhususkan antara lain pada *tag* (label pengenal) pada format gambar digital yang biasa digunakan oleh peralatan kamera digital. *Exif* ini digunakan pada format jpeg dct (untuk *file* gambar terkompresi) dan tiff rev. 6.0 (untuk *file* gambar tidak terkompresi), namun *exif* ini tidak mendukung format jpeg 2000, png atau gif. *Exif* dibuat oleh Japan Electronic Industries Development Association (JEIDA), di mana versi 2.1 dari *exif* dikeluarkan di tahun 1998 dan berlanjut hingga ke versi 2.3 yang dikeluarkan pada tahun 2010. Meskipun tidak ada standar *exif* yang baku secara internasional, *exif* tetap banyak dipakai oleh pembuat peralatan kamera digital untuk menyimpan metadata yang berkaitan dengan proses *capturing* dengan *tag-tag* yang kadang-kadang tidak seragam antara merk kamera yang satu dengan merk yang lain.

Oleh karena *exif* memuat beberapa *tag* yang menyimpan informasi tertentu maka *exif* juga sering disebut sebagai metadata, yaitu suatu data tertentu yang memuat tentang data lain. *Tag-tag* metadata dari *exif* ini antara lain memuat :

- Informasi mengenai *date/time* (tanggal/waktu) kapan suatu gambar digital di-*capture* oleh kamera digital.
- *Settings* dari kamera, seperti model dan *make* (pembuat), *aperture* (nilai diafragma bukaan lensa kamera), *shutter speed* (kecepatan buka-tutup lensa kamera), orientasi (arah *capturing* gambar), ukuran *pixel* (juga sering disebut sebagai tingkat resolusi gambar), dan lain-lain
- *Thumbnail*, yaitu *preview* kecil dari gambar yang ditampilkan di layar LCD kamera. Besarnya ukuran thumbnail biasanya 160 x 120 *pixels* atau tergantung besarnya layar LCD.

Ketika suatu momen di-*capture* oleh kamera digital dan menghasilkan *file* jpeg yang tersimpan di *memory card* dari kamera tersebut seperti contoh pada Gambar X.5. di bawah ini, *file* jpeg yang berisikan gambar digital dari proses *capturing* tersebut akan juga memuat *tag-tag* metadata *exif* seperti yang dijelaskan di atas. *Tag-tag* metadata *exif* ini sangat berguna bagi *analyst* atau

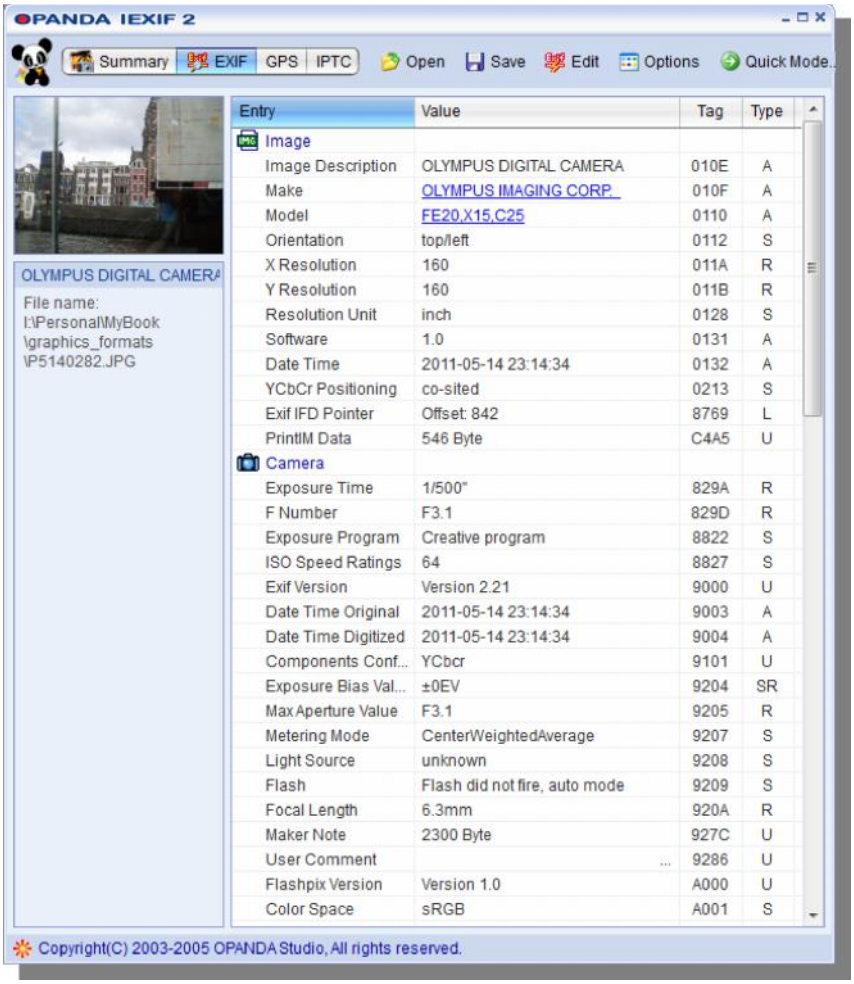
investigator untuk mengembangkan atau memperkuat investigasinya. Misalnya untuk menjawab pertanyaan tentang kapan *file* gambar digital ini dibuat ?, maka *tag* metadata exif tentang *date/time* dapat digunakan untuk memastikan tanggal/waktu pembuatannya. Begitu juga tentang peralatan kamera digital yang digunakan dapat diketahui.

Meskipun begitu, *tag* metadata *date/time* belum tentu menunjukkan tanggal/waktu yang sebenarnya karena *date/time* yang ada pada tag tersebut merupakan *date/time* hasil *settings* yang ada di kamera digital. Ketika membeli kamera digital, karyawan toko biasanya membantu untuk mencocokkan *settings date/time* dengan waktu sebenarnya dengan pilihan untuk menampilkannya pada gambar digital di pojok kanan bawah atau tidak. Adanya metadata *exif* tersebut, di samping berguna untuk merekam proses *capturing* gambar, juga membantu proses investigasi untuk menelusurinya kembali.



Gambar X.5. Gambar digital hasil proses capturing yang berformat jpeg.

Terhadap gambar di atas, kemudian dilakukan pemeriksaan untuk mendapatkan metadata *exif* secara detil. Ada beberapa aplikasi baik yang berjalan di sistem operasi Microsoft Windows maupun Linux yang dapat digunakan untuk kepentingan tersebut. Untuk di Linux, beberapa aplikasi yang dapat digunakan adalah *command* exiftool, exiftags dan metacam, serta phatch yang bersifat grafis. Pada contoh di bawah ini, digunakan aplikasi Opanda IEXIF 2 yang berjalan di *platform* Windows dan dikembangkan oleh Opanda untuk meng-ekstrak *tag-tag* metadata *exif* dari gambar digital tersebut.



Gambar X.6. Metadata *exif* yang berhasil di-ekstraksi secara lengkap termasuk detik tanggal/waktu *capturing* dan jenis kameranya.

Dari kedua gambar di atas, dapat diketahui bahwa gambar digital pada Gambar X.5. dibuat dengan menggunakan peralatan kamera digital merk Olympus model FE20.X15.C25 pada tanggal 14 Mei 2011 pukul 23:14:34. Untuk mengetahui apakah tanggal/waktu tersebut menunjukkan waktu yang sebenarnya atau tidak, *analyst* atau *investigator* dapat mengecek keakuratan waktu dengan kondisi gambar digital itu sendiri. Seperti pada contoh gambar di atas, diketahui dibuat pada pukul 23:14:34. Secara visual, waktu ini tidak cocok dengan gambar digital yang menunjukkan kondisi langit dan awan yang masih cerah. Hasil penelusuran terhadap tulisan-tulisan yang ada di gambar tersebut, diduga gambar tersebut dibuat di Belanda. Hasil pengecekan waktu matahari terbenam di Belanda pada tanggal 14 Mei 2011 di situs http://www.sunrise-and-sunset.com/en menunjukkan bahwa pada tanggal tersebut matahari terbenam pada pukul 21:21.

Artinya pada pukul 23:14, seharusnya langit sudah gelap karena pada jam tersebut hari sudah malam dan sudah lewat dari waktu matahari terbenam.

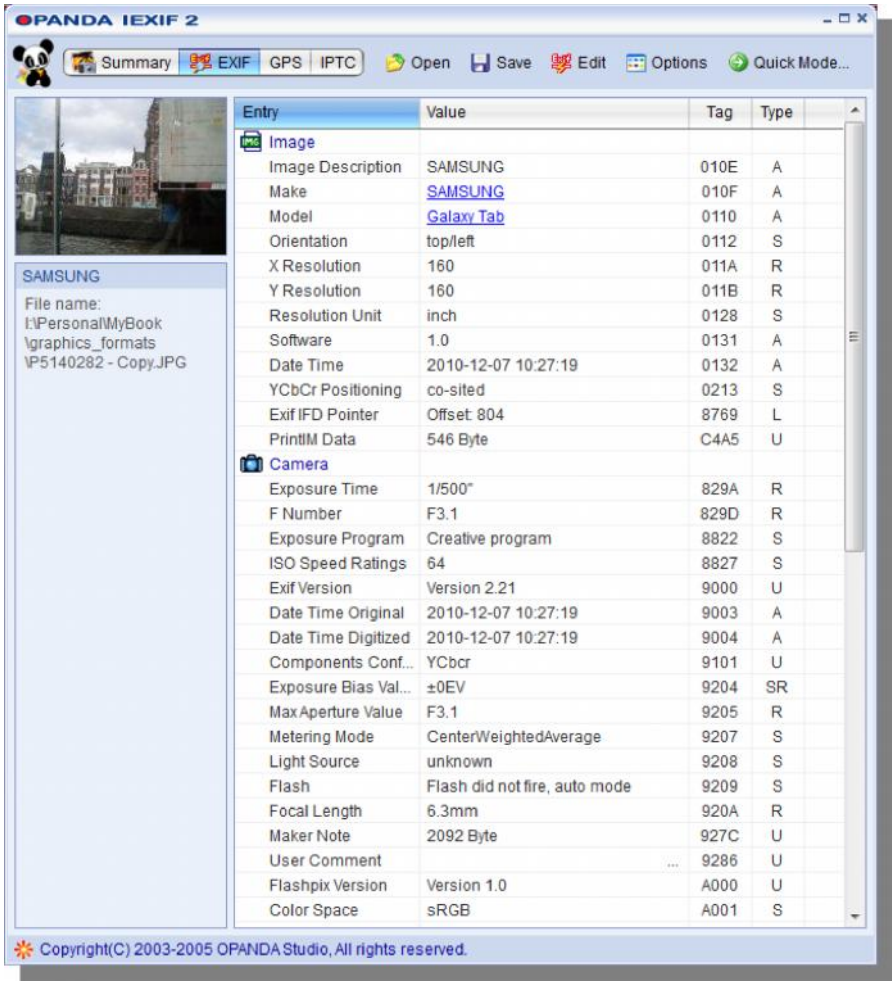
Dari data-data tersebut, dapat dipastikan untuk waktu pembuatan gambar digital tersebut tidak cocok dengan kondisi yang sebenarnya dan oleh karenanya pukul 23:14 tidak menunjukkan waktu (pukul) yang sebenarnya.

Di samping itu, juga diketahui data-data lain seperti versi *exif* yang menunjukkan versi 2.21 dan hal-hal yang menyangkut proses *capturing* gambar digital itu sendiri seperti *aperture* (besarnya bukaan lensa kamera) yang bernilai F3.1, *exposure time* (kecepatan buka-tutup lensa / *shutter speed*) yang menunjukkan 1/500", lampu *blitz* (*flash*) yang tidak menyala dan resolusi *pixel* dengan ukuran 1280 x 960.

Adakalanya gambar-gambar digital berformat jpeg tidak memiliki *tag-tag* metadata *exif* yang lengkap seperti contoh di atas. Gambar-gambar tanpa *exif* yang lengkap tersebut biasanya didapat dari hasil proses *download* dari internet. Dari gambar-gambar tersebut, biasanya *tag-tag* metadata *exif* hanya berupa ukuran (*size*) gambar dan resolusi *pixel*-nya. Bahkan sebagian besar gambar-gambar digital yang berasal dari internet tidak memiliki metadata *exif* sama sekali.

Keaslian gambar digital

Metadata *exif* yang dibahas sebelumnya sangat penting bagi *analyst* dan *investigator* untuk mengembangkan dan memperkuat investigasinya dengan cara menganalisa dan menelusuri kembali *tag-tag* metadata *exif* tersebut. Namun *analyst* dan *investigator* tidak boleh menyandarkan sepenuhnya investigasi terhadap metadata exif dari gambar digital tersebut, karena metadata exif itu sendiri dapat dimanipulasi dengan aplikasi-aplikasi tertentu. Aplikasi-aplikasi tersebut ada yang berjalan di *platform* Microsoft Windows, maupun di Linux. Informasi-informasi yang tersimpan di *tag-tag* metadata *exif* dapat dirubah sesuai dengan keinginan dari pengubahnya, sehingga seakan-akan metadata *exif* tersebut asli, padahal palsu. Misalnya pada *tag date/time* yang menyimpan informasi kapan gambar digital di-*capture* dapat dirubah dari tanggal yang sesungguhnya.



Gambar X.7. Metadata *exif* dari gambar sebelumnya yang telah mengalami manipulasi pada *tag date/time* dan *make* serta model.

Pada Gambar X.5 dan X.6 sebelumnya, diketahui gambar digital tersebut menyimpan informasi tangal/waktu pembuatannya yaitu 14 Mei 2011 pukul 23:14:34. Tanggal/waktu yang tersimpan di *tag* exif *date/time* tersebut dapat dimanipulasi menjadi tanggal/waktu yang lain, misalnya menjadi 7 Desember 2010 pukul 10:29:19 seperti yang terlihat pada Gambar X.7. Bahkan peralatan kamera digital yang digunakan pun dapat dirubah. Misalnya pada Gambar X.5 dan X.6 di atas, diketahui bahwa gambar digital tersebut di-*capture* dengan menggunakan kamera digital merk Olympus model FE20.X15.C25. Informasi mengenai *make* dan model tersebut dapat dirubah menjadi Samung Galaxy Tab yang sama sekali jauh berbeda dengan informasi sesungguhnya, seperti yang terlihat pada Gambar X.7.

Dari temuan-temuan di atas, dapat disimpulkan bahwa informasi yang tersimpan di *tag-tag* metadata *exif* harus dicek kebenarannya, *analyst* dan *investigator* tidak boleh percaya seratus persen terhadap kebenaran metadata *exif* tersebut. Jika hal tersebut masih dilakukan, maka investigasi akan berbelok ke arah yang salah dan bahkan mungkin investigasi tidak akan dapat membuka tabir kasus yang berkaitan dengan gambar digital tersebut.

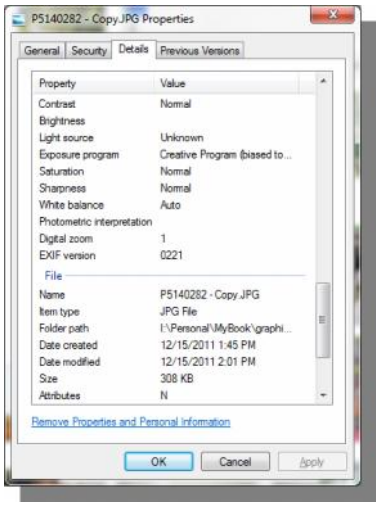
Pada contoh Gambar X.7. yang memiliki informasi metadata *exif* yang berbeda dengan yang sesungguhnya seperti pada Gambar X.6 akibat hasil proses manipulasi, keaslian dan kebenaran gambar tersebut masih dapat ditelusuri dengan melihat *properties* dari *file* jpeg yang menyimpan metadata tentang *time stamps* dari gambar digital tersebut. *Time stamps* yang diperiksa lebih lanjut adalah *created date* dan *modified date*. *Created date* merupakan tanggal pertama kali suatu *file* dibuat atau ter-*log* di *file system* yang sedang berjalan, sedangkan *modified date* menunjukkan tanggal terkahir kali suatu file dimodifikasi, di mana *modified date* ini tidak berkaitan dengan *file system* yang sedang berjalan.

Seperti yang terlihat pada Gambar X.8 di bawah ini, metadata time stamps dari Gambar X.7 menunjukkan bahwa gambar digital hasil manipulasi tersebut memiliki informasi sebagai berikut :

Created date : 15 Desember 2011 1:45 PM

Modified date : 15 Desember 2011 2:01 PM

Dari kedua data tentang *created date* dan *modified date* di atas, dapat diketahui bahwa *modified date* lebih muda dibandingkan dengan *created date*. Artinya *created date* terlebih dulu tercatat di *file system* yang sedang berjalan, kemudian *modified date* yang menunjukkan tanggal/waktu modifikasi baru tercatat di *file system* menyusul setelahnya, yaitu sekitar 16 menit kemudian dari *created date*.



Gambar X.8. *Properties* dari *file* jpeg hasil manipulasi seperti pada Gambar X.7 yang menunjukkan metadata *time stamps* berupa *created* dan *modified* date.

Dengan diketahuinya bahwa *modified date* lebih muda dibandingkan dengan *created date* maka dapat dijelaskan bahwa gambar digital seperti yang ditunjukkan metadata exif-nya di Gambar X.7 merupakan hasil modifikasi, bukan *file* jpeg dengan gambar digital yang sesungguhnya. Proses modifikasi yang mengubah metadata *exif* pada *tag date/time* dan *make*/model sebenarnya tidak memakan waktu yang lama, bahkan bisa dimungkinkan sangat singkat dengan menggunakan aplikasi-aplikasi tertentu.

Dengan adanya kepastian bahwa *file* jpeg yang berisikan gambar digital adalah hasil dari proses modifikasi dengan didasarkan pada analisa metadata *time stamps* seperti yang dijelaskan di atas, maka metadata exif yang menjelaskan proses *capturing* gambar digital tersebut tidak dapat lagi menjadi rujukan oleh *analyst* dan *investigator*. Sangat dimungkinkan metadata *exif* tersebut menyimpan informasi-informasi palsu, bukan yang sesungguhnya.

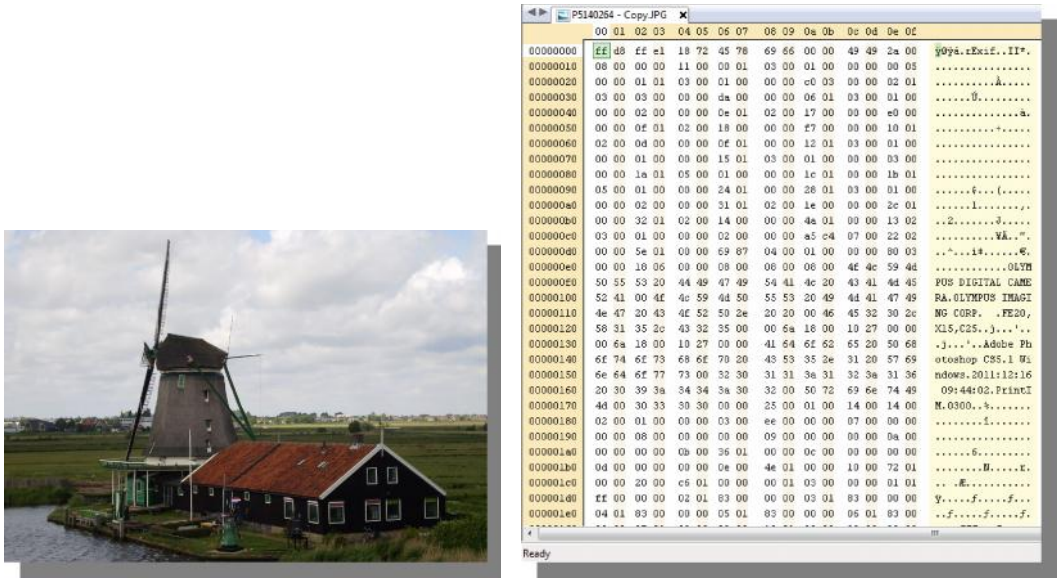
Analisa metadata *time stamps* dapat juga digunakan untuk memastikan keberadaan suatu *file* di suatu komputer X, apakah *file* tersebut merupakan hasil transfer, misalnya *copy-paste* atau *file* tersebut dibuat di komputer X dengan *file system* yang sedang berjalan. Terhadap *file* tersebut dilakukan analisa metadata *time stamps*. Jika hasilnya menunjukkan bahwa *created date* lebih muda dibandingkan dengan *modified date*, maka dapat dipastikan bahwa *file* tersebut hasil transfer, misalnya *copy-paste*, sebaliknya jika *created date* lebih tua

dibandingkan dengan *modified date*, maka *file* tersebut dibuat di komputer X dengan *file system* yang sedang berjalan di komputer tersebut, seperti pada contoh Gambar X.7 dan X.8. di atas.

Di samping analisa metadata *time stamps* yang didasarkan pada *created date* dan *modified date*, *analyst* dan *investigator* juga dapat menggunakan analisa *header* untuk melihat kemungkinan adanya proses *editing* terhadap suatu gambar digital. *Header* merupakan bagian yang paling awal dari suatu *file*, posisinya berada sebelum isi dari *file*. *Header* banyak menyimpan informasi/data yang berkaitan dengan *file* tersebut yang disebut dengan metadata, termasuk informasi tentang exif dan aplikasi *editing* fotografi. Beberapa *byte* awal dari *header* menyimpan *signature* (kadang-kadang disebut *magic numbers*) yang menunjukkan *format file* yang digunakan seperti yang dibahas dan ditunjukkan di Tabel VI.1. Bab VI tentang *Files Recovery*.

Sebagian besar aplikasi yang digunakan untuk *editing* atau modifikasi suatu gambar digital seperti Adobe Photoshop akan meninggalkan nama aplikasi atau pengembangnya yang diletakkan di bagian *header* dari *file* gambar digital tersebut. Untuk melihat dan menganalisa lebih dalam *header* tersebut, dapat digunakan aplikasi-aplikasi berbasis heksadesimal seperti WinHex dari X-Ways atau Hex Editor Neo dari HHD Software yang berjalan di sistem operasi Windows atau aplikasi HexEdit yang berjalan di *platform* Linux.

Dengan aplikasi-aplikasi ini, seluruh isi *file* termasuk bagian *header* dapat dilihat dengan jelas, baik dalam bentuk heksadesimal maupun dalam bentuk teks berbasis ANSI atau Unicode seperti yang terlihat pada gambar di bawah ini.

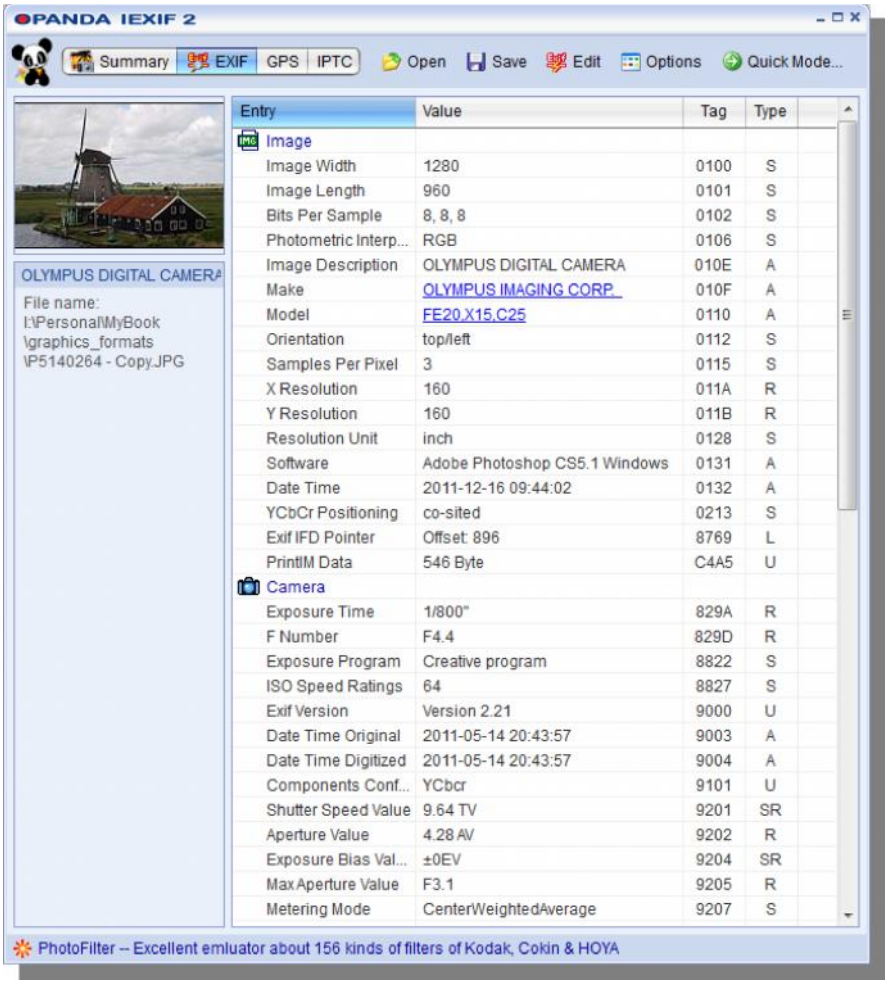


(i) (ii)

Gambar X.9. Gambar digital (i) yang telah mengalami modifikasi berupa *cropping* (pemotongan) dari gambar sebelumnya, kemudian dilihat isinya secara keseluruhan termasuk *header* dengan aplikasi *hex viewer* (ii).

Pada gambar di atas, gambar (i) merupakan gambar yang telah di-*edit* melalui proses *cropping* (pemotongan gambar dengan membuang bagian yang tidak diperlukan) dengan menggunakan aplikasi Adobe Photoshop CS5. Untuk mengetahui apakah gambar digital tersebut apakah hasil modifikasi sebelumnya atau diduga memang benar gambar asli, *header* dari *file* gambar digital tersebut dapat diperiksa dan dianalisa apakh tersimpan metadata yang berkaitan dengan aplikasi fotografi yang digunakan.

Pada contoh di atas, *header* dari *file* gambar digital tersebut diakses dengan menggunakan aplikasi *hex viewer* yang berjalan di *platform* Microsoft Windows dan diketahui bahwa di dalam *header* terekam aplikasi *editing* fotografi yang digunakan, yaitu Adobe Photoshop CS5. Bahkan di dalam *header*, juga tercatat tanggal/waktu kapan terjadinya proses *editing* terhadap gambar digital tersebut, yaitu tanggal 16 Desember 2011 pukul 09:44:02.



Gambar X.10. Metadata *exif* menyimpan informasi tentang aplikasi yang digunakan untuk manipulasi gambar digital yang berada di *header* dari *file* gambar digital.

Dengan adanya *header* dari *file* gambar digital yang menyimpan informasi penting tentang kemungkinan adanya aplikasi yang digunakan untuk manipulasi gambar digital, maka sebaiknya *analyst* dan *investigator* memeriksa secara cermat kemungkinan tersebut.

Kadang-kadang informasi metadata tentang aplikasi yang tersimpan di *header* juga dapat diekstrak dengan menggunakan aplikasi *exif viewer* seperti dari Opanda, seperti contoh di Gambar X.10.

Dari gambar di atas, dapat dilihat bahwa aplikasi tersebut juga dapat mengekstrak informasi yang tersimpan di *header* berupa aplikasi yang digunakan untuk *editing* gambar digital yaitu Adobe Photoshop CS5, di mana manipulasi gambar tersebut dilakukan pada tanggal 16 Desember 2011 pukul 09:44:02. Diketahui juga bahwa

tag date/time yang menyimpan tanggal/waktu pengambilan (*capturing*) gambar yang sesungguhnya, yaitu tanggal 14 Mei 2011 pukul 20:43:57 masih ada.

Jadi dari analisa *header* maupun exif yang dilakukan, maka gambar digital tersebut dapat diketahui bahwa gambar tersebut diambil (di-*capture*) pada tanggal 14 Mei 2011, kemudian dilakukan modifikasi pada tanggal 16 Desember 2011. Artinya gambar tersebut sudah tidak asli lagi, karena sudah berubah dari gambar digital yang sesungguhnya.

Bibliography

1. ACPO, 7Safe (2008). *Good Practice Guide for Computer-Based Electronic Evidence*. UK ACPO and 7Safe.
2. Al-Azhar, M.N. (2010). *Standard Operating Procedure (SOP) 8 : Prosedur Pemeriksaan Digital Forensik*. DFAT Puslabfor.
3. Carrier, B. (2002). *Open Source Digital Forensic Tools: The Legal Argument.* @stake.
4. Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Elsevier Academic Press.
5. Johnson, T. A. (2005). *Forensic Computer Crime Investigation*. Taylor & Francis.
6. Kessler, G. (2011). *File Signatures Table.* http://www.garykessler.net/library/*file*_sigs.html.
7. Middleton, B. (2002). *Cyber Crime Field Handbook*. CRC Press
8. National Institute of Justice (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. US National Institute of Justice
9. National Institute of Justice (2001). *Electronic Crime Scene Investigation: A Guide for First Responder*. US National Institute of Justice.
10. Sammes, T. and Jenkinson, B. (2007). *Forensic Computing: A Practitioner's Guide*. Springer.
11. Solomon, M. G. et al. (2005). *Computer Forensics Jumpstart*. Sybex.