MODUL PRAKTIKUM



FORENSIK BERGERAK DAN MULTIMEDIA

UNIVERSITAS TEKNOLOGI MATARAM

2019

Jl. Kampus Universitas Teknologi Mataram, Kekalik, Mataram

KATA PENGANTAR

Dengan menyebut nama Allah SWT yang Maha Pengasih lagi Maha Panyayang, kami panjatkan syukur ke hadirat-Nya, yang telah melimpahkan rahmat dan hidayatnya, sehingga modul matakuliah forensik bergerak dan multimedia ini bisa kami selesaikan dengan baik.

Modul matakuliah forensik bergerak dan multimedia ini diambil dari berbagai sumber dan kajian para ahli dan para pakar didalam ilmu forensik. Adapun keluaran dari modul ini adalah sebagai pembelajaran kepada mahasiswa dalam pengembangan forensik bergerak dan multimedia di masa mendatang.

Modul matakuliah forensik bergerak dan multimedia ini telah kami susun dan mendapatkan bantuan dari berbagai pihak. Untuk itu kami menyampaikan banyak terima kasih kepada semua pihak yang telah berkontribusi dan memberikan masukan dalam pembuatan modul ini.

Akhir kata kami berharap semoga modul ini dapat memberikan manfaat ataupun inspirasi kepada seluruh mahasiswa yang mengambil dan mempelajari matakuliah forensik bergerak dan multimedia. Sekian dan terima kasih.

Mataram, November 2019

DAFTAR ISI

HALAMAN COVER i
KATA PENGANTAR ii
DAFTAR ISI iii
DAFTAR GAMBAR v
BAB I FORENSIK DIGITAL 1
A. PENGANTAR FORENSIK DIGITAL 1
B. TERMINOLOGI 2
C. KOMPONEN 2
D. SEJARAH 3
E. PROSES FORENSIK 6
F. PENERAPAN 11
G. PERTIMBANGAN HUKUM 13
H. ALAT FORENSIK DIGITAL 16
I. CABANG 18
BAB II FORENSIK BERGERAK DAN MULTIMEDIA 21
A. PENGANTAR FORENSIK BERGERAK DAN MULTIMEDIA 21
B. ASPEK DALAM MULTIMEDIA FORENSIK 21
C. PERBEDAAN DIGITAL FORENSIK DAN MULTIMEDIA FORENSIK 23
BAB III FORENSIK BERGERAK DAN MULTIMEDIA SAMA DENGAN FORENSIK KOMPUTER 25
A. PENGANTAR 25
B. CONTOH KASUS 26
C. KESIMPULAN 31
BAB IV ANALISIS FORENSIK BERGERAK DAN MULTIMEDIA 32
A. ANALISIS FORENSIK GAMBAR 32
B. ANALISIS FORENSIK VIDEO 39
C. HASIL SIMULASI 44

BAB V KESIMPULAN 45
A. KESIMPULAN 45
B. SARAN 45
REFERENSI 46

DAFTAR GAMBAR

Gambar 1. Foto A 27
Gambar 2. Foto B 28
Gambar 3. Analisa Foto A 29
Gambar 4. Analisa Foto B 29
Gambar 5. Metadata Foto A 30
Gambar 6. Metadata Foto B 31
Gambar 7. Contoh Gambar 32
Gambar 8. Berita Gambar 33
Gambar 9. Foto A1 34
Gambar 10. Foto A2 34
Gambar 11. Metadata Foto A1 35
Gambar 12. Metadata Foto A1 Lanjutan 36
Gambar 13. Metadata Foto A2 37
Gambar 14. Metadata Foto A2 Lanjutan 38
Gambar 15. Hasil Metadata Video Asli 40
Gambar 16. Hasil Metadata Video Edited 41
Gambar 17. Frame 75 dari Video Asli 42
Gambar 18. ELA pada Frame 75 42
Gambar 19. Frame 56 dari Video Editan 43
Gambar 20. 17 ELA pada Frame 56 43

BAB I
FORENSIK DIGITAL

A. PENGANTAR FORENSIK DIGITAL

Forensik digital (bahasa Inggris: *Digital forensics*) (juga dikenal sebagai ilmu forensik digital) adalah salah satu cabang ilmu forensik, terutama untuk penyelidikan dan penemuan konten perangkat digital, dan sering kali dikaitkan dengan kejahatan komputer. Istilah forensik digital pada awalnya identik dengan forensik komputer tetapi kini telah diperluas untuk menyelidiki semua perangkat yang dapat menyimpan data digital. Forensik digital diperlukan karena biasanya data di perangkat target dikunci, dihapus, atau disembunyikan. Berawal dari bangkitnya revolusi komputasi personal pada akhir 1970-an dan awal 1980-an, disiplin ini berkembang secara alami selama tahun 1990-an, dan baru pada awal abad ke-21 negara-negara secara bertahap membentuk kebijakannya terhadap disiplin ini.

Landasan forensik digital ialah praktik pengumpulan, analisis, dan pelaporan data digital. Investigasi forensik digital memiliki penerapan yang sangat beragam. Penggunaan paling umum adalah untuk mendukung atau menyanggah asumsi kriminal dalam pengadilan pidana atau perdata.

Forensik juga dapat dilakukan di sektor swasta; seperti penyelidikan internal perusahaan (in-house) atau penyelidikan intrusi (penyelidikan khusus mengeksplorasi sifat dan dampak intrusi jaringan yang tidak sah).

Penguasaan ilmu forensik digital tidak hanya menuntut kemampuan teknis semata tetapi juga terkait dengan bidang lain, seperti bidang hukum. Aspek teknis dari penyelidikan dapat dibagi menjadi beberapa subcabang, sesuai dengan jenis perangkat digital yang terlibat; forensik komputer, forensik jaringan, analisis data forensik dan forensik peranti bergerak. Proses forensik umumnya meliputi penyitaan, forensic imaging (akuisisi) dan analisis media digital dan penyusunan laporan berdasarkan bukti yang dikumpulkan.

Selain mengidentifikasi bukti langsung sebuah kejahatan, forensik digital dapat digunakan untuk mengkonfirmasi hubungan antara tersangka dan kasus tertentu, mengkonfirmasi alibi-alibi atau pernyataan-pernyataannya, untuk memahami niat, mengidentifikasi sumber

(misalnya, dalam kasus sengketa hak cipta), atau mengotentikasi dokumen-dokumen. Ruang lingkup investigasi forensik digital lebih luas daripada bidang pengetahuan forensik lainnya (di mana sebagian besar ilmu forensik lain dirancang untuk menjawab pertanyaan yang relatif sederhana), sering melibatkan garis waktu atau hipotesis yang kompleks.

B. TERMINOLOGI

Ilmu forensik adalah ilmu yang digunakan untuk tujuan hukum, bersifat tidak memihak yang merupakan bukti ilmiah untuk digunakan dalam kepentingan peradilan dan penyelidikan. Forensik digital merupakan salah satu cabang dari ilmu forensik, terutama untuk menyelidiki dan memulihkan konten perangkat digital, berkaitan dengan bukti legal yang terdapat pada perangkat komputer dan media penyimpanan digital lainnya sebagai bukti-bukti digital yang digunakan dalam kejahatan komputer dan dunia maya. Forensik digital diperlukan karena biasanya data di perangkat target dikunci, dihapus, atau disembunyikan. Forensik digital merupakan ilmu yang relatif baru.

Forensik digital adalah ilmu yang menganalisis barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan. Istilah forensik digital pada awalnya identik dengan forensik komputer tetapi definisinya telah diperluas hingga mencakup forensik semua teknologi digital. Sedangkan forensik komputer didefinisikan sebagai "kumpulan teknik dan alat yang digunakan untuk menemukan bukti pada komputer. Landasan forensik digital ialah praktik pengumpulan, analisis, dan pelaporan data digital.

Forensik digital dapat juga diartikan sebagai pengumpulan dan analisis data dari berbagai sumber daya komputer yang mencakup sistem komputer, jaringan komputer, jalur komunikasi, dan berbagai media penyimpanan yang layak untuk diajukan dalam sidang pengadilan.

C. KOMPONEN

Dalam suatu model forensik digital melibatkan tiga komponen terangkai yang dikelola sedemikian rupa sehingga menjadi sebuah tujuan akhir dengan segala kelayakan serta hasil yang berkualitas. Ketiga komponen tersebut adalah:

1. **Manusia** (*People*), diperlukan kualifikasi untuk mencapai manusia yang berkualitas. Memang mudah untuk belajar komputer forensik, tetapi untuk menjadi ahlinya, dibutuhkan lebih dari sekadar pengetahuan dan pengalaman.
2. **Peralatan** (*Equipment*), diperlukan sejumlah perangkat atau alat yang tepat untuk mendapatkan sejumlah bukti yang dapat dipercaya dan bukan sekadar bukti palsu.
3. **Aturan** (*Protocol*), diperlukan dalam menggali, mendapatkan, menganalisis, dan akhirnya menyajikan dalam bentuk laporan yang akurat. Dalam komponen aturan, diperlukan pemahaman yang baik dalam segi hukum dan etika, kalau perlu dalam menyelesaikan sebuah kasus perlu melibatkan peran konsultasi yang mencakup pengetahuan akan teknologi informasi dan ilmu hukum.

D. SEJARAH

Sebelum tahun 1980-an kejahatan yang melibatkan komputer ditangani dengan ketentuan hukum yang ada. Kejahatan komputer pertama kali diakui dalam Undang-Undang Pidana Komputer Florida 1978 (*the 1978 Florida Computer Crimes Act*) termasuk undang-undang yang melarang modifikasi tidak sah atau penghapusan data pada sistem komputer. Pada tahun-tahun berikutnya, ruang lingkup cybercrime mulai berkembang, dan beberapa undang-undang kemudian disahkan untuk mengatasi permasalahan hak cipta, privasi/pelecehan (misalnya intimidasi dunia maya, cyber stalking, dan predator daring) serta pornografi anak. Baru pada tahun 1980-an undang-undang federal mulai memasukkan pelanggaran komputer. Kanada adalah negara pertama yang mengeluarkan undang-undang terkait kejahatan komputer pada tahun 1983. Hal ini diikuti oleh Amerika Serikat dengan *Computer Fraud and Abuse Act* pada tahun 1986, Australia mengamendemen undang-undang kriminalnya pada tahun 1989 dan Inggris menerbitkan Undang-Undang Penyalahgunaan Komputer (*Computer Misuse Act*) pada tahun 1990.

1980-an 1990-an: Pertumbuhan

Pertumbuhan kejahatan komputer selama tahun 1980-an dan 1990-an menyebabkan lembaga-lembaga penegak hukum membentuk tim khusus, biasanya di tingkat nasional, untuk menangani aspek-aspek teknis dalam penyelidikan. Sebagai contoh, pada tahun 1984 FBI membentuk Tim Analisis dan Tanggapan Komputer (*Computer Analysis and Response Team*), dan tahun berikutnya Departemen Kejahatan Komputer didirikan di dalam kelompok anti-

penipuan Polisi Metropolitan Inggris. Selain personel penegak hukum profesional, banyak anggota awal tim-tim ini terdiri dari penggemar/penghobi komputer dan bertanggung jawab untuk penelitian dan petunjuk awal serta arah masa depan bidang forensik digital.

Salah satu contoh kasus penerapan digital forensik yang pertama (atau paling tidak kasus publik yang paling awal) adalah kasus pengejaran peretas Markus Hess oleh Clifford Stoll pada tahun 1986. Meskipun Stoll penyelidikannya menggunakan teknik forensik komputer dan jaringan, bukanlah pemeriksa khusus. Banyak kasus identifikasi awal forensik digital mengikuti profil yang serupa.

Sepanjang tahun 1990-an, permintaan terhadap sumber daya penyelidikan baru ini semakin meningkat. Beban dan ketegangan pada unit pusat mengarah pada pembentukan tim-tim di tingkat regional bahkan di tingkat lokal. Misalnya, National Hi-Tech Crime Unit di Inggris dibentuk pada tahun 2001 guna menyediakan infrastruktur nasional untuk kejahatan komputer; dengan personel yang berlokasi di pusat kota London dan pasukan polisi di daerah (unit ini masuk ke dalam Serious Organised Crime Agency (SOCA) pada tahun 2006).

Selama periode ini ilmu forensik digital berkembang dari sarana dan teknik-teknik ad-hoc yang dikembangkan oleh para praktisi penghobi di bidang ini. Berbeda dengan ilmu forensik lainnya yang dikembangkan dari karya-karya komunitas ilmiah. Pada 1992 istilah "forensik komputer" mulai digunakan dalam literatur akademik (meski sebelumnya sudah digunakan secara informal); sebuah makalah oleh Collier dan Spaul berusaha untuk memasukkan disiplin baru ini ke dunia sains forensik.[16] Perkembangan yang cepat ini mengakibatkan minimnya standardisasi dan pelatihan-pelatihan. Dalam bukunya, "High-Technology Crime: Investigating Cases Involving Computers", K. Rosenblatt tahun 1985 menuliskan:

Menyita, mengamankan, dan menganalisis bukti yang tersimpan dalam komputer adalah tantangan forensik terbesar yang dihadapi penegak hukum pada tahun 1990-an. Ketika sebagian besar pengujian forensik, seperti uji sidik jari dan DNA dikerjakan oleh para ahli yang dilatih secara khusus, pekerjaan pengumpulan dan analisis bukti komputer kebanyakan ditugaskan kepada petugas patroli dan detektif.

2000-an: Pengembangan standar

Sejak tahun 2000, sebagai tanggapan terhadap kebutuhan standardisasi, berbagai badan dan lembaga telah menerbitkan pedoman untuk forensik digital. Kelompok Kerja Ilmiah

tentang Bukti Digital (SWGDE) menerbitkan makalah "Best practices for Computer Forensics" pada tahun 2002, kemudian pada tahun 2005 diikuti oleh publikasi standar ISO (ISO 17025, General requirements for the competence of testing and calibration laboratories). Sebuah perjanjian internasional Eropa, "Konvensi tentang Kejahatan Dunia Maya" mulai berlaku pada tahun 2004 dengan tujuan merekonsiliasi undang-undang kejahatan komputer nasional, teknik investigasi dan kerjasama internasional. Perjanjian itu telah ditandatangani oleh 43 negara (termasuk AS, Kanada, Jepang, Afrika Selatan, Inggris dan negara-negara Eropa lainnya) dan diratifikasi oleh 16 negara.

Masalah pelatihan juga mendapat perhatian. Perusahaan komersial (biasanya perusahaan pengembang perangkat lunak forensik) mulai menawarkan program sertifikasi dan topik analisis forensik digital dimasukkan dalam fasilitas pelatihan spesialis penyidik Inggris, Centrex.

Sejak akhir 1990-an perangkat seluler mulai tersedia secara luas, berkembang melebihi perangkat komunikasi sederhana, dan lebih kaya informasi, bahkan untuk kejahatan yang tidak secara tradisional terkait dengan forensik digital. Meskipun demikian, analisis digital pada ponsel jauh ketinggalan di banding media komputer tradisional, sebagian besar karena sifat hak kepemilikan (proprietary) perangkat tersebut.

Fokus juga telah bergeser ke kejahatan internet, khususnya risiko perang dunia maya dan cyberterrorism. Laporan pada Februari 2010 oleh Komando Pasukan Gabungan Amerika Serikat menyimpulkan:

Melalui dunia maya, musuh dapat menargetkan industri, akademisi, pemerintah, serta militer di udara, darat, maritim, dan domain ruang angkasa. Dengan cara yang sama seperti kekuatan udara yang mengubah medan perang selama Perang Dunia II, dunia maya telah mematahkan hambatan fisik yang melindungi suatu bangsa dari serangan terhadap perniagaan dan komunikasinya.

Bidang forensik digital masih menghadapi masalah yang belum terselesaikan. Sebuah makalah tahun 2009, "Digital Forensic Research: The Good, the Bad and the Unaddressed", oleh Peterson dan Shenoi mengidentifikasi bias terhadap sistem operasi Windows dalam penyelidikan forensik digital.[23] Pada tahun 2010 Simson Garfinkel mengidentifikasi masalah yang dihadapi penyelidikan digital di masa depan, termasuk meningkatnya ukuran media digital, ketersediaan enkripsi yang luas bagi konsumen, semakin beragamnya sistem operasi dan format berkas,

semakin banyaknya individu yang memiliki banyak perangkat, dan batasan-batasan hukum pada para penyidik. Makalah ini juga mengidentifikasi berlanjutnya masalah-masalah pelatihan, serta biaya yang sangat tinggi untuk memasuki bidang ini.

Pengembangan peralatan forensic

Selama tahun 1980-an sangat sedikit alat forensik digital khusus yang tersedia, sebagai akibatnya para penyidik kebanyakan melakukan live analysis pada media, memeriksa komputer dari dalam sistem operasi menggunakan peralatan sysadmin yang tersedia untuk mengekstrak barang bukti. Praktik ini berisiko memodifikasi data pada diska, baik secara tidak sengaja atau sebaliknya, yang dapat menyebabkan klaim kerusakan barang bukti. Sejumlah alat diciptakan pada awal 1990-an untuk mengatasi permasalahan tersebut.

Kebutuhan untuk perangkat lunak pertama kali diakui pada tahun 1989 di Pusat Pelatihan Penegakan Hukum Federal, sehingga tercipta IMDUMP (oleh Michael White) dan pada tahun 1990, SafeBack (dikembangkan oleh Sydex). Perangkat lunak serupa juga dikembangkan di negara lain; DIBS (solusi perangkat keras dan perangkat lunak) dirilis secara komersial di Inggris pada tahun 1991, dan Rob McKemmish merilis Fixed Disk Image gratis untuk penegak hukum Australia. Alat-alat ini memungkinkan pemeriksa untuk membuat salinan yang identik dari media digital untuk diselidiki, sehinggan media asli utuh untuk verifikasi. Pada akhir 1990-an, untuk memenuhi permintaan untuk bukti digital yang semakin banyak, peralatan komersial yang canggih seperti EnCase dan FTK dikembangkan, yang memungkinkan analis untuk memeriksa salinan media tanpa melakukan forensik secara langsung. Belakangan tren ke arah "forensik memori secara langsung" telah berkembang sehingga diciptakan alat seperti WindowsSCOPE.

Baru-baru ini, perkembangan alat yang sama juga tersedia untuk perangkat seluler; penyidik awalnya mengakses data langsung pada perangkat, tetapi kemudian alat khusus seperti XRY atau Radio Tactics Aceso muncul.

E. PROSES FORENSIK

Dalam penyelidikan forensik digital, proses forensik digital merupakan proses ilmiah dan forensik yang diakui. Peneliti forensik Eoghan Casey mendefinisikannya sebagai langkah-langkah mulai dari sinyal awal insiden hingga pelaporan temuan.

Media digital yang disita untuk penyelidikan biasanya disebut sebagai "barang bukti" dalam terminologi hukum. Penyelidik menggunakan metode ilmiah untuk menemukan bukti digital untuk mendukung atau menyangkal hipotesis, baik untuk pengadilan atau proses perdata.

1. Personel

Tahapan proses forensik digital memerlukan pelatihan dan pengetahuan spesialis yang berbeda-beda. Secara garis besar ada dua tingkatan personel yang dibutuhkan:

Teknisi forensik digital (*digital forensics technicians*)

Teknisi mengumpulkan atau memproses bukti di TKP. Teknisi ini dilatih mengenai penanganan teknologi secara benar (misalnya bagaimana memelihara/mempertahankan bukti). Teknisi mungkin juga diminta untuk melakukan "Analisis langsung". Berbagai alat untuk menyederhanakan prosedur ini telah diproduksi, misalnya dengan COFEE milik Microsoft.

Pemeriksa bukti digital (*digital evidence examiners*)

Pemeriksa mengkhususkan diri dalam satu bidang bukti digital; baik pada tingkat yang luas (yaitu forensik komputer atau jaringan dll.) atau sebagai subspesialis (yaitu analisis gambar).

2. Model proses

Metodologi yang teliti dan prosedur standar dari proses investigasi sangat penting dalam melakukan penyelidikan forensik. Ada banyak upaya untuk mengembangkan model proses tetapi sejauh ini tidak ada yang diterima secara universal. Sebagian alasannya mungkin karena fakta bahwa banyak model proses dirancang untuk lingkungan tertentu, dan karena itu tidak dapat langsung diterapkan di lingkungan lain. Area populer bagi para peneliti forensik digital adalah mencari metodologi standar agar proses forensik digital lebih akurat, kuat, dan efisien. Model proses forensik digital pertama yang diusulkan berisi empat langkah: Akuisisi, Identifikasi, Evaluasi, dan Admisi. Sejak itu, banyak model proses telah diusulkan untuk menjelaskan langkah-langkah mengidentifikasi, memperoleh, menganalisis, menyimpan, dan melaporkan bukti yang diperoleh dari berbagai perangkat digital. Dalam beberapa tahun terakhir, semakin banyak model proses yang lebih canggih telah diusulkan. Model-model ini mencoba untuk mempercepat seluruh proses investigasi atau memecahkan berbagai masalah yang biasa ditemui dalam penyelidikan forensik. Dalam dekade terakhir, komputasi awan membuat pengumpulan bukti menjadi lebih sulit. Di bidang investigasi forensik digital, beralih ke model pemrosesan bukti berbasis cloud akan sangat bermanfaat dan upaya awal telah dibuat dalam implementasinya.

Investigasi forensik digital umumnya terdiri dari 3 tahap: pengumpulan (*akuisisi*) atau imaging barang bukti, analisis, dan pelaporan. Pengetahuan yang paling penting adalah bahwa pemeriksaan forensik dilakukan dan dilaporkan dengan cara yang tidak bias dan dapat direproduksi.

3. Pengumpulan

Idealnya pengumpulan bukti atau akuisisi melibatkan pengambilan citra (*imaging*) memori volatil komputer (RAM), atau media penyimpanan lain, dan membuat duplikat sektor yang sama ("duplikasi forensik" atau "citra forensik") dari media tersebut, tindakan ini sering dibantu perangkat write blocking untuk mencegah modifikasi pada media asli. Pertumbuhan ukuran media penyimpanan dan perkembangannya, seperti komputasi awan mengharuskan akuisisi secara 'langsung' di mana salinan data logical diambil alih-alih citra lengkap dari perangkat penyimpanan fisik. Citra yang diperoleh (atau salinan logical) dan media/data asli kemudian di-hash (menggunakan algoritma seperti SHA-1 atau MD5) dan nilai-nilainya dibandingkan untuk memverifikasi bahwa salinannya akurat.

Sebuah pendekatan alternatif (dan dipatenkan, yang disebut hybrid forensics atau distributed forensics) menggabungkan tahapan forensik digital dan ediscovery. Pendekatan ini diwujudkan dengan peralatan komersial yang disebut ISEEK yang dipresentasikan bersama dengan hasil tesnya pada konferensi tahun 2017.

Forensik statik (*static forensic*)

Forensik statik menggunakan prosedur dan pendekatan konvensional di mana bukti di olah secara bit-by-bit image untuk melakukan proses forensik. Proses forensiknya sendiri berjalan pada sistem yang tidak dalam keadaan menyala. Forensik statik difokuskan pada pemeriksaan hasil imaging untuk menganalisis isi dari bukti digital, seperti berkas yang dihapus, riwayat penjelajahan web, berkas fragmen, koneksi jaringan, berkas yang diakses, riwayat user login, dll guna membuat timeline berupa ringkasan tentang kegiatan yang dilakukan pada bukti digital sewaktu digunakan.

Saat perangkat dalam keadaan mati, data yang dapat diperiksa hanya yang tersimpan di memori statis, seperti diska keras. Namun, masih ada beberapa pemrosesan yang perlu dilakukan sebelum menganalisis data aktual pada unit penyimpanan. Ketika melakukan pemeriksaan forensik, terutama dalam penegakan hukum, harus diambil tindakan untuk menghilangkan peluang memodifikasi bukti yang sebenarnya. Menyalakan perangkat dan mengoperasikannya bisa saja memodifikasi data asli dan dengan demikian mencemari bukti. Bukti

yang terkontaminasi pada gilirannya tidak akan layak di pengadilan. Sehingga perlu membuat salinan bukti yang identik (dalam hal konten) menggunakan perangkat khusus atau komputer biasa dengan bantuan perangkat keras write blocker dan perangkat lunak pencitraan diska (disk imaging). Dalam istilah forensik, salinan ini umumnya disebut disk image atau forensic disk image. Kemudian forensic disk image ini dibawa ke laboratorium forensik untuk dianalisis.

Forensik langsung (*live forensic*)

Dalam forensik langsung semua bukti digital dikumpulkan saat sistem sedang berjalan, sehingga pemeriksa mendapat kesempatan untuk mengumpulkan data volatil (mudah hilang) yang memuat informasi tentang apa yang sedang dilakukan perangkat. Tujuan utama dari penyelidikan langsung adalah untuk mengumpulkan data volatil sebanyak-banyaknya. Forensik langsung juga memberi kesempatan untuk memeriksa apakah ada diska keras yang aktif dienkripsi sehingga bisa mengumpulkan data versi yang tidak terenkripsi. Implementasi full disk encryption (FDE) memastikan bahwa semua data pada diska keras dienkripsi saat komputer mati. Namun, data akan didekripsi saat komputer aktif. Oleh karena itu perlu melakukan pencarian menyeluruh untuk perangkat lunak enkripsi yang mungkin terpasang di komputer. Jika ada tanda-tanda enkripsi, pemeriksa harus membuat logical image dari diska keras tersebut untuk menjamin bahwa data dapat dipertahankan dan tersedia untuk analisis nanti.

4. Analisis

Selama fase analisis, seorang penyelidik mendapatkan bukti menggunakan sejumlah metodologi dan instrumen yang berbeda-beda. Pada tahun 2002, sebuah artikel dalam International Journal of Digital Evidence merujuk pada langkah ini sebagai "pencarian sistematis dan mendalam atas bukti yang terkait dengan dugaan kejahatan." Pada tahun 2006, peneliti forensik Brian Carrier menjelaskan mengenai "prosedur intuitif" di mana bukti yang terang diidentifikasi terlebih dahulu lalu kemudian "pencarian menyeluruh dilakukan untuk melengkapi kekurangannya."

Analisis forensik pada dasarnya untuk menjawab pertanyaan penyelidikan dengan menganalisis data yang ditemukan pada citra forensik yang dibuat pada tahapan "pengumpulan bukti". Proses analisis yang sebenarnya dapat bervariasi antara investigasi, tetapi metodologinya secara umum termasuk melakukan pencarian kata kunci di seluruh media digital (dalam berkas serta dalam unallocated dan slack space), memulihkan berkas yang dihapus dan ekstraksi informasi registry (misalnya untuk menampilkan akun pengguna, atau perangkat USB yang terpasang). Bukti

yang telah diperoleh dianalisis untuk merekonstruksi peristiwa atau tindakan dan untuk mencapai kesimpulan, pekerjaan yang sering dapat dilakukan oleh personel yang kurang terspesialisasi.

5. Pelaporan

Tahapan terakhir jika penyelidikan telah selesai, data yang diperoleh disajikan dalam bentuk laporan tertulis dengan istilah-istilah atau bahasa non-teknis. Laporan menyajikan temuan obyektif dan kesimpulan berdasarkan temuan tersebut. Isi laporan dapat berbeda tergantung undang-undang dan kebijakan lokal. Namun, secara umum laporan memuat:

Data kasus

Data kasus memuat informasi orang yang memerintahkan pemeriksaan, beberapa identifier yang mejadi fokus penyelidikan dan informasi yang mengidentifikasi potongan bukti yang harus diperiksa. Poin utamanya adalah mempertahankan lacak balak serta agar dapat membedakan suatu pemeriksaan dari pemeriksaan lain. Informasi yang tepat yang harus dimuat dalam laporan sangat bergantung pada peraturan dan undang-undang setempat.

Tujuan pemeriksaan

Tujuan pemeriksaan harus dinyatakan dalam laporan karena menyajikan apa yang dicari selama pemeriksaan. Tujuan pemeriksaan menggambarkan fokus dari pemeriksaan sehingga memberikan pembaca pemahaman tentang apa yang dia harapkan sebagai hasilnya. Menyatakan tujuan dimulai dengan pertanyaan atau tujuan yang diungkapkan oleh orang yang memerintahkan pemeriksaan. Namun, bisa juga mencakup tujuan apa pun yang dilakukan oleh pemeriksa forensik ketika menganalisis kasus.

Temuan

Menyajikan temuan termasuk menyajikan potongan-potongan bukti yang ditemukan selama pemeriksaan. Temuan disajikan secara obyektif (sebagaimana adanya), dan tidak membuat kesimpulan atau interpretasi subjektif.

Kesimpulan

Kesimpulan dibuat oleh ahli forensik berdasarkan temuan, pengetahuan dan pengalamannya. Sehingga kesimpulan dapat bersifat subyektif dan aspek yang sangat penting dalam menulis laporan forensik adalah memisahkan temuan obyektif dari kesimpulan subyektif. Saat menulis daftar kata, protokol harus dapat dimengerti oleh orang yang tidak memiliki keahlian IT.

F. PENERAPAN

Forensik digital umumnya digunakan baik dalam hukum pidana maupun penyelidikan pribadi. Biasanya forensik ini dikaitkan dengan hukum pidana, di mana bukti yang telah terkumpul digunakan untuk mendukung atau menentang hipotesis di depan pengadilan. Sama seperti bidang forensik lainnya, forensik digital biasanya merupakan bagian dari penyelidikan yang lebih luas yang mencakup berbagai disiplin ilmu. Pada beberapa kasus, bukti yang terkumpul berfungsi sebagai bentuk pengumpulan intelijen yang digunakan untuk tujuan lain selain proses pengadilan (misalnya untuk menemukan, mengidentifikasi atau menghentikan kejahatan lain). Akibatnya, pengumpulan intelijen terkadang dilakukan dengan standar forensik yang kurang ketat.

Dalam perkara perdata atau permasalahan perusahaan, forensik digital menjadi bagian dalam proses electronic discovery (atau eDiscovery). Prosedur forensiknya serupa dengan yang digunakan dalam investigasi pidana, sering kali dengan persyaratan dan batasan hukum yang berbeda. Di luar pengadilan forensik digital dapat menjadi bagian dari penyelidikan internal perusahaan.

Contoh umum misalnya setelah terjadinya intrusi jaringan tanpa otorisasi. Pemeriksaan pakar forensik mengenai sifat dan dampak serangan dilakukan sebagai upaya untuk membatasi kerusakan. Baik untuk menetapkan sejauh mana intrusi tersebut maupun sebagai upaya untuk mengidentifikasi penyerang. Pada tahun 1980-an serangan semacam ini biasanya dilakukan melalui saluran telepon, tetapi di era modern penyebarannya melalui Internet.

Fokus utama penyelidikan forensik digital adalah untuk mengungkap bukti yang objektif dari aktivitas kriminal (disebut actus reus dalam bahasa hukum). Namun, beragam data yang tersimpan dalam perangkat digital dapat membantu bidang penyelidikan lainnya.

Pertalian

Metadata dan log lainnya dapat digunakan untuk mengaitkan suatu tindakan kepada seseorang. Misalnya, dokumen pribadi pada drive komputer mungkin mengidentifikasi pemiliknya.

Alibi dan pernyataan

Informasi yang diberikan oleh mereka yang terlibat dapat diperiksa silang dengan bukti digital. Misalnya, selama penyelidikan pembunuhan Soham alibi pelaku dibantah ketika catatan ponsel dari orang yang dia temui menunjukkan bahwa dia berada di luar kota pada saat itu.

Maksud

Selain untuk menemukan bukti yang obyektif dari suatu kejahatan, penyelidikan juga dapat digunakan untuk membuktikan niat (dikenal sebagai mens rea dalam istilah hukum). Sebagai contoh, riwayat Internet dari terpidana pembunuh Neil Entwistle di antaranya merujuk ke situs yang membahas Cara membunuh orang.

Evaluasi sumber

Artefak-artefak dan metadata berkas dapat digunakan untuk mengidentifikasi asal-usul bagian data tertentu; misalnya, versi Microsoft Word yang lebih lama menyematkan Global Unique Identifer ke dalam berkas-berkas yang mengidentifikasi komputer di mana berkas tersebut dibuat. Membuktikan apakah suatu berkas dibuat pada perangkat digital yang sedang diperiksa atau diperoleh dari tempat lain (mis., Internet) bisa menjadi sangat penting.

Otentikasi dokumen

Terkait dengan "Evaluasi sumber," metadata yang terkait dengan dokumen-dokumen digital dapat dengan mudah dimodifikasi (misalnya, dengan mengubah jam komputer maka dapat mempengaruhi tanggal pembuatan sebuah berkas). Otentikasi dokumen berkaitan dengan pendeteksian dan mengidentifikasi pemalsuan pada rincian-rincian tersebut.

Batasan

Tugas umum selama pemeriksaan forensik adalah mencoba mendekripsikan data yang terenkripsi dalam berbagai bentuk mulai dari berkas atau folder terenkripsi hingga komunikasi yang terenkripsi seperti surat ekektronik dan obrolan atau bahkan menyelidiki diska keras yang telah dienkripsi dengan enkripsi diska penuh (FDE). Salah satu keterbatasan utama dalam penyelidikan forensik adalah penggunaan enkripsi ini, yang dapat menghalangi pemeriksaan awal jika bukti yang bersangkutan terdeteksi menggunakan kata kunci. Hukum yang memaksa seseorang untuk mengungkapkan kunci enkripsi masih relatif baru dan kontroversial.

Media penyimpanan Solid State Drive (SSD) yang mengaktifkan teknologi TRIM dapat menjadi hambatan dalam melakukan forensik digital khususnya pada pemulihan data. Karena fitur TRIM berfungsi untuk memusnahkan garbage data yang telah dihapus. TRIM pada dasarnya adalah sebuah fungsi di mana data yang telah dihapus dimusnahkan secara permanen dari sistem operasi, sehingga pemulihan sulit dilakukan. Namun, tidak semua SSD fitur TRIM-nya diaktifkan.

G. PERTIMBANGAN HUKUM

Pemeriksaan media digital dicakup dalam undang-undang nasional maupun internasional. Khusus penyelidikan perdata, undang-undang dapat membatasi kemampuan analis untuk melakukan pemeriksaan. Pembatasan pemantauan jaringan, atau pembacaan komunikasi pribadi sering terjadi. Dalam penyelidikan pidana, undang-undang nasional membatasi seberapa banyak informasi yang dapat disita. Misalnya, di Inggris, penyitaan barang bukti oleh penegak hukum diatur oleh Police and Criminal Evidence Act 1984. Selama keberadaan awalnya di bidang ini, "International Organization on Computer Evidence" (IOCE) adalah salah satu lembaga yang bekerja untuk menetapkan standar internasional yang kompatibel terhadap penyitaan barang bukti.

Di Inggris, hukum yang sama terkait kejahatan komputer juga dapat mempengaruhi penyelidik forensik. Computer Misuse Act 1990 mengatur larangan akses tanpa otorisasi pada materi komputer, aturan ini menjadi perhatian khusus bagi penyidik sipil yang memiliki lebih banyak batasan dibanding penegak hukum.

Hak individu atas privasi adalah salah satu bidang forensik digital yang sebagian besar belum diputuskan oleh pengadilan. Electronic Communications Privacy Act (ECPA) di AS memberikan batasan kemampuan kepada penegak hukum atau penyidik sipil untuk menyadap dan mengakses bukti. Undang-undang tersebut membedakan antara komunikasi tersimpan (misalnya arsip surat elektronik) dan komunikasi yang ditransmisikan (seperti VoIP). Yang terakhir, lebih dianggap sebagai serangan privasi, dan lebih sulit untuk mendapatkan surat perintah. ECPA juga mempengaruhi kemampuan perusahaan dalam menyelidiki komputer dan komunikasi karyawan mereka, suatu aspek yang masih diperdebatkan adalah sejauh mana perusahaan dapat melakukan pemantauan tersebut.

Pasal 5 Konvensi Eropa tentang Hak Asasi Manusia menegaskan pembatasan privasi yang serupa dengan ECPA dan membatasi pemrosesan dan pembagian data pribadi baik di dalam UE maupun dengan negara-negara luar. Kemampuan penegak hukum Inggris untuk melakukan penyelidikan forensik digital diatur oleh Regulation of Investigatory Powers Act 2000.

Bukti Digital

Bukti digital adalah data-data yang dikumpulkan dari semua jenis penyimpanan digital yang menjadi subjek pemeriksaan forensik komputer. Dengan demikian segala sesuatu yang membawa informasi digital dapat menjadi subjek penyelidikan, dan setiap pembawa informasi

yang ditargetkan untuk pemeriksaan harus diperlakukan sebagai bukti. Menurut Pasal 5 UU No. 11/2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menyebutkan bahwa "informasi elektronik dan atau dokumen elektronik dan atau hasil cetaknya merupakan alat bukti hukum yang sah". Contoh barang bukti digital: alamat E-Mail, berkas wordprocessor/spreadsheet, kode sumber perangkat lunak, berkas gambar (JPEG, PNG, dll), bookmarks penjelajah web, cookies, kalender, to do list, dan lainnya.

Seorang pakar digital forensik harus benar-benar terlatih dan berpengalaman dalam menggunakan cara untuk mengumpulkan semua data-data yang diperlukan sehingga bisa dijadikan bukti legal yang semuanya sudah diatur dalam undang-undang. Ketika digunakan dalam pengadilan, bukti digital berada di bawah pedoman hukum yang sama seperti bentuk bukti lainnya; pengadilan biasanya tidak memerlukan panduan yang lebih ketat. Di Amerika Serikat, Federal Rules of Evidence digunakan untuk mengevaluasi diterimanya bukti digital, PACE Kerajaan Inggris dan Civil Evidence acts memiliki pedoman serupa dan banyak negara lain memiliki hukumnya sendiri. Undang-undang federal AS membatasi penyitaan hanya pada barang bukti yang jelas. Hal ini diakui tidak selalu memungkinkan dilakukan pada media digital sebelum dilakukan pemeriksaan.

Hukum yang berurusan dengan bukti digital terkait dengan dua permasalahan: integritas dan keaslian. Integritas memastikan bahwa tindakan menyita dan memperoleh media digital tidak mengubah bukti (baik yang asli atau salinannya). Keaslian mengacu pada kemampuan untuk mengkonfirmasi integritas informasi; misalnya bahwa media yang dicitrakan (*imaged*) sesuai dengan bukti asli. Mudahnya media digital untuk termodifikasi berarti mendokumentasikan lacak balak [en] mulai dari TKP, analisis, hingga ke pengadilan penting dilakukan untuk menjaga keaslian barang bukti.

Lembaga penegak hukum harus memiliki lacak balak yang tepat ketika menangani bukti digital dan menjamin bahwa semua bukti digunakan untuk analisis forensik yang tepat. Agensi juga harus mengambil tindakan pencegahan yang tepat saat menangani bukti digital. Ketika para penyelidik mengumpulkan bukti dari perangkat digital, bukti yang terkait dengan kejahatan lain mungkin ditemukan. Penyelidik perlu mendapatkan surat perintah kedua agar bukti dapat diterima ke pengadilan. Penanganan bukti digital perlu dilakukan secara khusus mengingat barang bukti digital tergolong "rapuh" sehingga besar kemungkinan terjadinya pencemaran barang bukti digital baik disengaja maupun tidak disengaja. Kesalahan kecil pada penanganan barang bukti

dapat membuat barang bukti digital tidak dapat diajukan dipengadilan sebagai alat bukti yang sah dan akurat. Data digital juga dapat diciptakan dengan mudah. Salah satu hal yang ditakutkan adalah adanya penambahan data oleh penyidik (misalnya ada penambahan data untuk menyudutkan pemilik perangkat digital). Untuk itu, diperlukan adanya mekanisme yang memastikan bahwa penyidik tidak dapat (atau sulit) untuk melakukan rekayasa terhadap data. Ada beberapa mekanisme yang dapat dilakukan, seperti penggunaan message digest terhadap berkas yang akan dievaluasi dan penggunaan tools yang sudah disertifikasi.

Para pengacara berpendapat karena bukti digital secara teoritis mudah berubah (dimodifikasi dan digandakan), hal itu dapat merusak keandalan bukti. Para hakim AS mulai menolak teori ini, dalam kasus AS v. Bonallo, pengadilan memutuskan "fakta bahwa data yang ada dalam komputer dapat berubah jelas tidak cukup untuk membentuk ketidakpercayaan." Dalam pedoman Inggris seperti yang dikeluarkan oleh Association of Chief Police Officers diikuti untuk membantu mendokumentasikan keaslian dan integritas barang bukti.

Seorang ahli harus menerapkan metode dan teknik yang terbukti andal secara ilmiah untuk mencari bukti digital. Penyidik digital khususnya dalam investigasi pidana, harus memastikan bahwa kesimpulan-kesimpulannya didasarkan pada bukti faktual dan pengetahuan kepakaran mereka sendiri. Di AS, misalnya, Federal Rules of Evidence menyatakan bahwa seorang saksi yang memenuhi syarat sebagai ahli dapat bersaksi "dalam bentuk pendapat atau lainnya" jika:

> *(1) kesaksian didasarkan pada fakta atau data yang cukup, (2) kesaksian adalah produk dari kaidah-kaidah dan metode-metode yang dapat diandalkan, dan (3) ahli telah menerapkan prinsip dan metode secara andal terhadap fakta-fakta kasus.*

Subcabang forensik digital masing-masing dapat memiliki panduan khusus tersendiri untuk melakukan penyelidikan dan penanganan barang bukti. Sebagai contoh, ponsel mungkin harus diletakkan dalam sangkar Faraday selama penyitaan atau akuisisi untuk mencegah lalu lintas radio lebih lanjut ke perangkat. Di Inggris, pemeriksaan forensik komputer dalam masalah kriminal tunduk pada pedoman ACPO. Ada juga pendekatan internasional untuk memberikan panduan tentang cara menangani bukti elektronik. *"Electronic Evidence Guide"* oleh Dewan Eropa menawarkan kerangka kerja untuk penegak hukum dan otoritas peradilan di negara-negara yang

berusaha untuk mengatur atau meningkatkan pedoman mereka sendiri untuk identifikasi dan penanganan bukti elektronik.

Standar Daubert

Keberadaan bukti digital bergantung pada alat/perkakas (*tools*) yang digunakan untuk mengekstraknya. Di AS, perkakas forensik diberlakukan standar Daubert [en], di mana hakim bertanggung jawab untuk memastikan bahwa tahapan dan perangkat lunak yang digunakan dapat diterima. Dalam sebuah makalah tahun 2003, Brian Carrier berpendapat bahwa pedoman Daubert mengharuskan kode alat-alat forensik dipublikasikan dan ditelaah oleh rekan sejawat. Dia menyimpulkan bahwa "peralatan sumber terbuka mungkin lebih jelas dan komprehensif dalam memenuhi persyaratan pedoman dibanding peralatan dengan sumber tertutup." Pada tahun 2011 Josh Brunty menyatakan bahwa validasi ilmiah pada teknologi dan perangkat lunak yang terkait dengan kegiatan pemeriksaan forensik digital sangat penting untuk setiap proses laboratorium. Dia berpendapat bahwa "ilmu forensik digital didasarkan pada prinsip-prinsip proses berulang dan bukti berkualitas sehingga mengetahui bagaimana merancang dan mempertahankan proses validasi yang baik adalah syarat utama bagi setiap pemeriksa forensik digital untuk mempertahankan metode mereka di pengadilan.

H. ALAT FORENSIK DIGITAL

Para penegak hukum memanfaatkan peralatan berupa perangkat keras dan perangkat lunak khusus untuk penyelidikan forensik digital. Alat-alat ini digunakan untuk membantu pemulihan dan pelestarian bukti digital.

Perangkat keras

Peralatan yang berupa perangkat keras umumnya dirancang untuk menyelidiki perangkat penyimpanan, dan untuk menjaga agar perangkat target tidak berubah demi menjaga integritas bukti. Forensics disk controller atau pencacah perangkat keras merupakan perangkat read-only yang memungkinkan pengguna untuk membaca data di perangkat tersangka tanpa risiko memodifikasi atau menghapus konten di dalamnya. Sedangkan disk write-protector atau write-blocker berfokus pada pelestarian bukti di perangkat target dan berfungsi untuk mencegah konten dalam perangkat penyimpanan termodifikasi atau terhapus. Hard-drive duplicator adalah perangkat pencitraan (*imaging*) yang berfungsi untuk menyalin semua file pada cakram keras yang

dicurigai ke dalam cakram yang bersih, alat ini juga dapat menduplikasi data dalam cakram lepas atau kartu digital (SD) secara aman. Perangkat pemulihan kata sandi menggunakan algoritme, seperti serangan brute force atau kamus, untuk mencoba mengakses perangkat penyimpanan yang dilindungi kata sandi.

Perangkat lunak

Untuk penelitian dan investigasi yang lebih baik, para pengembang telah membuat berbagai perangkat lunak forensik. Kepolisian dan lembaga penyelidikan memilih akat-alat ini berdasarkan beberapa faktor termasuk anggaran dan ahli yang tersedia dalam tim. Sebagian besar perangkat lunak forensik bersifat multi-tujuan serta dapat melakukan berbagai tugas dalam satu aplikasi. Sebagian aplikasi bersifat sumber terbuka, sehingga kodenya dapat dimodifikasi untuk memenuhi kebutuhan yang spesifik dan penghematan biaya bagi penegak hukum. Sebagian dapat memproses beberapa perangkat sekaligus atau mengelola berbagai sistem operasi (misalnya, Windows dan Linux).

Perangkat lunak forensik komputer melengkapi perangkat keras yang tersedia untuk penegak hukum untuk memperoleh dan menganalisis bukti digital yang dikumpulkan dari perangkat tersangka. Tersangka sering menyembunyikan/ menghapus berkas atau mempartisi cakram keras komputer mereka sehingga bukti sulit ditemukan; namun, aplikasi perangkat lunak forensik dapat membantu penyelidik dalam memulihkan bukti ini. Aktivitas pengguna tertentu dapat dipulihkan dan diselidiki dengan perangkat lunak digital forensik. Alat-alat forensik ini juga dapat diklasifikasikan ke dalam berbagai kategori:

- Alat perekam cakram dan data
- Penampil berkas
- Alat analisis berkas
- Alat analisis registry
- Alat analisis internet
- Alat analisis surat elektronik
- Alat analisis peranti bergerak
- Alat analisis MacOS
- Alat forensik jaringan
- Alat forensik basis data

I. CABANG

Penyelidikan forensik digital tidak hanya terbatas pada mengambil data dari komputer, karena perangkat digital kecil (misalnya tablet, ponsel cerdas, flash drive) sekarang banyak digunakan. Beberapa perangkat ini ada yang memiliki memori volatil dan ada yang tidak. Metodologi yang memadai telah tersedia untuk mengambil data dari memori volatil, namun terdapat kekurangan metodologi atau kerangka kerja untuk pengambilan data dari sumber memori non-volatil. Ada lima cabang utama forensik digital dan mereka dikategorikan berdasarkan tempat data disimpan atau bagaimana data ditransmisikan.

Forensik Komputer

Tujuan dari forensik komputer adalah untuk menjelaskan keadaan artefak digital saat ini; seperti sistem komputer, media penyimpanan atau dokumen elektronik. Disiplin ini biasanya mencakup komputer, sistem benam (perangkat digital dengan kemampuan komputasi belum sempurna dan memori onboard) dan memori statis (seperti USB pen drive).

Forensik komputer ini bergantung pada sistem operasi yang digunakan. Sebagai contoh, kebanyakan pengguna komputer desktop menggunakan sistem operasi Microsoft Windows. Oleh karena itu, diperlukan kemampuan untuk melakukan forensik pada komputer yang menggunakan sistem operasi Microsoft Windows. Sistem operasi yang lain meletakkan data pada berkas yang berbeda dengan format yang berbeda. Sebagai contoh pada sistem UNIX catatan tersedia pada layanan syslog, sementara itu pada sistem Microsoft Windows catatan dapat dilihat dengan Event Viewer. Berbagai perkakas (tools) forensik tersedia untuk membantu penyidik dalam mengumpulkan data yang terkait dengan sistem operasi yang digunakan.

Forensik komputer dapat menangani berbagai informasi; dari log (seperti riwayat internet) hingga ke berkas yang sebenarnya dalam drive. Pada tahun 2007 jaksa menggunakan spreadsheet yang dipulihkan dari komputer Joseph E. Duncan III untuk membuktikan pembunuhan terencana dan memperkuat hukuman mati. Pembunuh Sharon Lopatka diidentifikasi pada tahun 2006 setelah pesan email dari dia yang merinci fantasi tentang penyiksaan dan kematian ditemukan di komputernya.

Forensik Peranti Bergerak

Forensik peranti bergerak adalah subcabang forensik digital yang berkaitan dengan pemulihan bukti digital atau data dari perangkat seluler. Berbeda dari forensik komputer karena perangkat seluler memiliki sistem komunikasi yang terintegrasi (mis. GSM) dan biasanya dengan mekanisme penyimpanan proprietary. Investigasi biasanya lebih berfokus pada data sederhana seperti data panggilan dan komunikasi (SMS/Email) daripada pemulihan mendalam dari data yang dihapus.[54] Data SMS dari investigasi perangkat seluler membantu membebaskan Patrick Lumumba dalam kasus pembunuhan Meredith Kercher.

Perangkat seluler juga menyediakan informasi lokasi; baik dari pelacakan gps/lokasi internal atau melalui tower seluler, yang melacak perangkat dalam jangkauan mereka. Informasi tersebut digunakan untuk melacak para penculik Thomas Onofri pada tahun 2006.

Forensik Jaringan

Forensik jaringan berkaitan dengan pengamatan dan analisis lalu lintas jaringan komputer, baik lokal maupun WAN/internet, untuk keperluan pengumpulan informasi, pengumpulan bukti, atau deteksi intrusi.[55] Lalu lintas biasanya disadap di tingkat paket, baik disimpan untuk analisis nanti atau disaring secara real-time. Tidak seperti forensik digital lainnya data jaringan sering berubah-ubah dan jarang terekam, membuat disiplin ini sering reaksioner.

Pada tahun 2000, FBI mengumpan peretas komputer Aleksey Ivanov dan Gorshkov ke Amerika Serikat untuk wawancara kerja palsu. Dengan memonitor lalu lintas jaringan dari komputer pasangan tersebut, FBI mengidentifikasi kata sandi yang memungkinkan mereka mengumpulkan bukti langsung dari komputer yang berbasis di Rusia.

Analisis Data Forensik

Analisis Data Forensik adalah cabang forensik digital. Ini menguji data terstruktur dengan tujuan untuk menemukan dan menganalisis pola kegiatan penipuan yang dihasilkan dari kejahatan keuangan.

Forensik Basis Data

Forensik basis data adalah cabang forensik digital yang berkaitan dengan studi forensik basis data dan metadatanya. Investigasi menggunakan isi basis data, berkas log, dan data dalam RAM untuk membuat garis waktu atau memulihkan informasi yang relevan.

BAB II
FORENSIK BERGERAK DAN MULTIMEDIA

A. PENGANTAR FORENSIK BERGERAK DAN MULTIMEDIA

Menurut Caldell, Amerini, et al. (2010) multimedia forensik dapat didefinisikan sebagai ilmu yang mencoba menganalisa, dengan hanya menganalisa beberapa aset digital tertentu, untuk memberikan penilaian atas konten tersebut dan mengekstrak informasi yang dapat berguna dan dapat mendukung penyelidikan terkait dengan scene/ kejadiaan yang direseprentasikan oleh dokumen digital tersebut. Ide dasar dari forensik multimedia bergantung pada pengamatan bahwa baik proses akuisisi dan setiap operasi post-processing meninggalkan jejak khas pada data, sebentuk sidik jari digital. Analisa sidik jari digital tersebut dapat mengarahkan tim analisi untuk menentukan asal ataupun sumber dari gambar/ video dan menentukan keaslian dari konten digital tersebut.

Menurut Bohme (2009) dalam multimedia forensik dapat dikategorikan menjadi 2 tindakan yang dapat dilakukan terhadap konten evidence tersebut, yaitu :

1. *Characteristic of source devices*

   Memeriksa dan mencari informasi terkait sumber devices yang digunakan dalam/ menghasilkan konten evidence / file-file multimedia.

2. *Artificacts of previous processing*

Mendeteksi setiap perubahan ataupun proses manipulasi yang terjadi terhadap file-file multimedia seperti copy,paste, insert, skala, editing, kompresi.

B. ASPEK DALAM MULTIMEDIA FORENSIK

Ada 3 aspek dalam Multimedia Forensik. Yaitu Audio Forensik, Image Forensik dan Video Forensik. Dalam pembahasan kali ini, kita akan coba bahas tentang pengenalan video forensik. Fokus dari video forensics adalah pada analisa video melalui frame by frame analysis untuk memastikan apakah dalam rekaman video tersebut ada informasi atau hal-hal tertentu yang diduga akan menguatkan atau mendukung proses penyidikan. Dalam analysis tersebut salah satu fokusnya adalah untuk memperjelas objek tertentu, baik melalui pembesaran/pengecilan objek,

perbaikan kualitas objek (enhancement dengan rekayasa image) ataupun rekontruksi object melalui aspek multiview camera. Selain melakukan eksplorasi terhadap konten video dengan zooming, enhancement dan sejenisnya, sebenarnya salah satu aktifitas lain yang masih dapat dilakukan adalah rekontruksi dan simulasi.

Dalam keilmuan digital forensik, ada perbedaan antara video analysis dan video forensik, Kalau dari aspek video analysis memang ada tampering tapi kalau dari sudut pândang video forensics maka tampering itu justru dilakukan untuk mendapatkan informasi yang ingin dicari.

Video forensic itu memang selalu dikaitkan dengan proses penyidikan, artinya investigator dan analys video forensics harus dapat menemukan informasi yang relevan yang termuat dalam video tersebut untuk mendukung data-data penyidikan. Bila informasi tersebut tidak jelas, maka harus diperjelas, bila informasi itu hilang maka harus dapat direcovery, bila informasi tersebut tidak lengkap (terputus) maka harus dapat diprediksi bagaimana yang lengkapnya.

Dan untuk melakukan analysis tersebut harus dilakukan sejumlah rekayasa baik secara algoritma ataupun melalui proses rekayasa sederhana melalui enhancement, histogram, gamma, zooming, cropping dll., Jadi analisa video memang akan bersentuhan dengan mekanisme tampering image/frame. Hanya saja semua proses tampering tersebut tidak dilakukan pada file asli kemudian semua langkahnya terdokumentasi dengan detail sehingga dapat dicoba kembali dengan cara dan hasil yang sama.

Berbicara tentang CCTV saat ini sudah bukan menjadi hal yang baru. Sebab hampir semua masyarakat Indonesia sudah mengetahui apa itu CCTV. Hal tersebut juga menjadi booming karena sering diangkat dalam pembahasan sebuah persidangan kasus pembunuhan berencana kopi yang sidangnya disiarkan secara live. Dan juga salah satu materi bahan bukti yang diperdebatkan adalah tentang CCTV ini.

CCTV terdiri atas beberapa arsitektur yang saling terkoneksi. CCTV biasanya terhubung ke DVR yang didalamnya terdapat hardisk untuk media penyimpanannya. DVR (Digital Video Record) merupakan alat yang berfungsi untuk merekam gambar kedalam media format digital ke dalam media penyimpanan seperti hardisk. Untuk lama penyimpanannya itu tergantung dari kapasistas hardisk yg ada. Biasanya untuk 16 camera dengan hardisk 500gb bisa menyimpan kurang lebih 2 mnggu. Dan nantinya setelah terisi penuh data yang paling lama akan otomatis terhapus.

Dalam sisi forensik, terdapat prosedur yang harus ditaati untuk dapat menjadikan CCTV menjadi sebuah barang bukti di persidangan. Berbicara tentang prosedur, ada beberapa standar atau aturan yang sudah mengaturnya. Salah satunya yang telah diatur dalam SNI 27037:2014. SNI ini sendiri adalah Standar Nasional Indonesia yang mengatur tentang pedoman standarisasi pelaksanaan investigasi forensika digital. Dalam SNI itu sudah dijelaskan prosedur lengkap seperti apa prosedur pengambilan data video nya. Salah satu nya yaitu, sebelum mengambil video, pastikan dulu waktu dan tanggal di sistem cctv atau DVR nya apakah sama dengan waktu dan tanggal kita yang sekarang atau tidak, kemudian kita harus tahu berapa kapasitas penyimpanan cctv tersebut, dan kapan waktu cctv tersebut menimpah file video yang ada.

Berikutnya dilakukan akuisisi atau pengambilan data CCTV tersebut. Bisa mengcopy video nya ke external storage, atau bisa juga via jaringan jika CCTV tersebut support. Menggunakan fitur export video yang disediakan oleh CCTV itu diperbolehkan dalam SNI. Setelah pengambilan data selesai, pastikan bahwa video yang telah dicopy sudah benar, caranya bisa dengan membandingkan memutar video hasil copy dan dibandingkan dengan video yang berada di DVR. File hasil akuisisi CCTV merupakan file masternya. Sehingga kalau mau menganalisisnya, harus di akuisisi ulang.

C. PERBEDAAN DIGITAL FORENSIK DAN MULTIMEDIA FORENSIK

Namun sebenarnya ada perbedaan fokus yang dicapai antara digital forensik dan multimedia forensik ini. istilahnya mereka ini sama tapi beda. Laksana anak kembar yang mempunyai kesamaan fisik, belum tentu memiliki kesamaan sifat. Tabel berikut akan menjelaskan tentang perbedaan tersebut.

Tabel 1. Perbedaan Digital Forensik dan Multimedia Forensik

Aspek	Komputer Forensik	Multimedia Forensik
Sumber bukti	- *Hard disk.* - RAM. - *External storage*	- Komputer - Kamera - CCTV - Internet
Proses	Tahapan *examination* berupa analisa tanpa mengalami proses perubahan	Adanya proses modifikasi terhadap barang bukti
Tujuan	Menemukan barang bukti, menganalisa metadata dan melakukan verifikasi terhadap hal-hal yang berhubungan dengan kasus	- Mencari keaslian dari sebuah barang bukti, hal tersebut dapat dilakukan dengan cara memodifikasi barang/ bukti dengan proses *enhancement*, membandingkan konten dari *evidence* dengan lingkungan luar - Multimedia forensik terdapat hubungan antara konten *evidence* dengan dunia nyata

BAB III
FORENSIK BERGERAK DAN MULTIMEDIA SAMA DENGAN FORENSIK KOMPUTER

A. PENGANTAR

Secara umum forensik perangkat-perangkat multimedia sering dijumpai di Indonesia belakangan ini. Masih ingat dengan kasus video porno ariel atau foto mantan pimpinan KPK abraham samad dengan seorang wanita atau kasus-kasus lain yang menggemparkan. Nah dalam ilmu forensik, bagaimanakah cara melakukan investigasi? Apakah cukup menggunakan metode investigasi layaknya forensik komputer atau seperti apa?

Beberapa pertanyaan tersebut jelas sering terdengar di telinga kita, mau tidak mau atau suka tidak suka setiap dokumentasi digital selalu meninggalkan jejak. Bedanya adalah jika kita bersinggungan dengan berkas multimedia maka kita bisa melihat dan atau mendengar secara langsung. Tentunya ini berbeda dengan kasus kejahatan yang meninggalkan bukti seperti log dimana cenderung sebagai saksi bisu dimana tanpa adanya campur tangan ahli untuk mengolahnya maka tidak akan berperan banyak dalam persidangan.

Menariknya adalah ketika kita berbicara tentang forensik multimedia maka akan banyak asumsi publik yang bisa di mainkan disini. Layaknya infotaiment, dengan adanya foto atau video kontroversi maka bisa dijamin akan jadi viral di dunia sosial media. Sehingga akan membuat persepsi publik yang terbangun dan biasanya terdapat split pendapat dari berbagai kalangan sesuai dengan interpretasi masing-masing. Jika hal ini tidak diklarifikasi maka bisa jadi interpretasi masing-masing individu menjadi provokasi yang bisa menumbuhkan keinginan untuk main hakim sendiri.

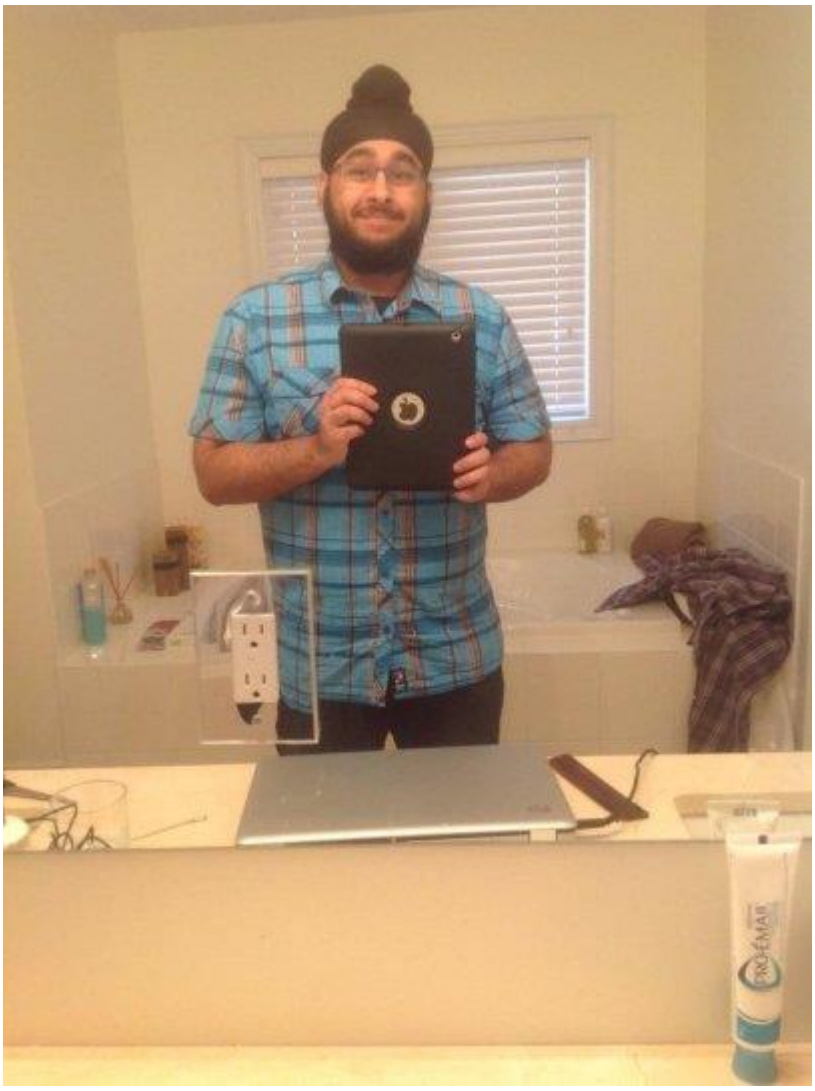
Dalam ilmu forensik apakah forensik multimedia termasuk dalam forensik komputer??? menarik untuk di bahas dan ternyata sudah di bahas oleh salah satu paper yang berjudul *"Multimedia Forensic is not Computer Forensics".* Dalam tulisan tersebut dijelaskan bahwa setiap kejadian yang melibatkan bukti multimedia tidak selalu bisa dilakukan analisa secara forensik komputer. Misalnya, pencarian polisi bisa menghasilkan image hard disk, yang foto-foto

digital yang dapat ditemukan dengan metode forensik komputer. Kemudian, forensik multimedia diterapkan untuk menetapkan foto-foto ini dengan kamera digital tertentu, yang telah disita di tempat lain. Sidik jari pada kamera ini akhirnya mengarah pada identitas pelaku melalui database kepolisian. Dalam contoh ini, semua jenis disiplin ilmu forensik berinteraksi, yang mencakup baik bukti digital dan fisik, dan bersama-sama membentuk rantai lengkap bukti. Sementara pendekatan holistik ini diharapkan membantu untuk menghukum orang yang tepat, kombinasi tersebut dalam prakteknya bisa menyembunyikan perbedaan halus antara berbagai metode yang terlibat, dan dengan demikian mempersulit latihan untuk mempelajari masing-masing secara terpisah. Dari hal tersebut sudah terlihat jelas bahwa kegiatan forensik multimedia lebih kompleks daripada forensik komputer. Sehingga mau tidak mau dalam forensik multimedia dibutuhkan kombinasi seluruh ilmu forensik.

B. CONTOH KASUS

Salah satu contoh kasus yang sempat gempar adalah kasus foto palsu pasca teror perancis. Hal ini terjadi setelah salah satu channel pro ISIS di telegram mengunggah foto yang menggambarkan seseorang membawa Al Quran dengan memakai rompi penuh BOM. Foto ini sendiri sempat menjadi viral di dunia maya. Banyak media masa dan elektronik yang mengangkat perihal hal ini. Walaupun pada akhirnya akun @Veeren_Jubbal yang merupakan orang yang ada dalam foto tersebut melakukan klarifikasi bahwa foto tersebut merupakan foto edit yang berasal dari hasil fotonya saat dikamar mandi. Akan tetapi untuk lebih jelas, pada kesempatan ini kita akan mencoba melakukan analisa terkait keaslian foto tersebut.

Foto Asli (selanjutnya disebut dengan foto A) yang diperoleh dari akun @Veeren_Jubbal



Gambar 1. Foto A

Foto Edit (selanjutnya disebut dengan foto B) yang menjadi viral yang didapatkan dari google

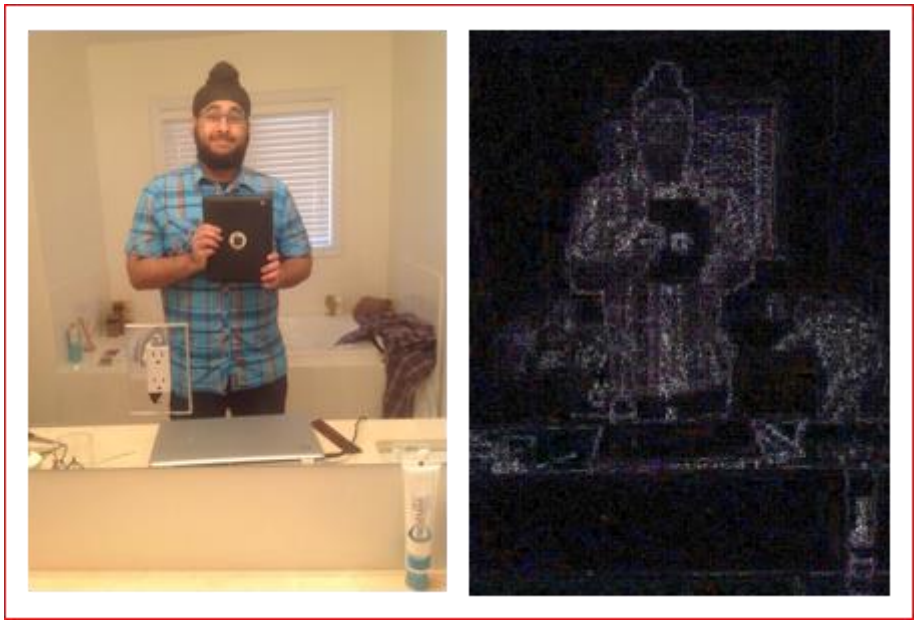


Gambar 2. Foto B

Beberapa peralatan yang akan dicoba digunakan untuk menganalisa adalah Forensik Foto yang digunakan untuk melakukan uji Error Level Analysis (ELA) pada kesalahan tingkat analisis gambar. Melalui http://fotoforensics.com/.

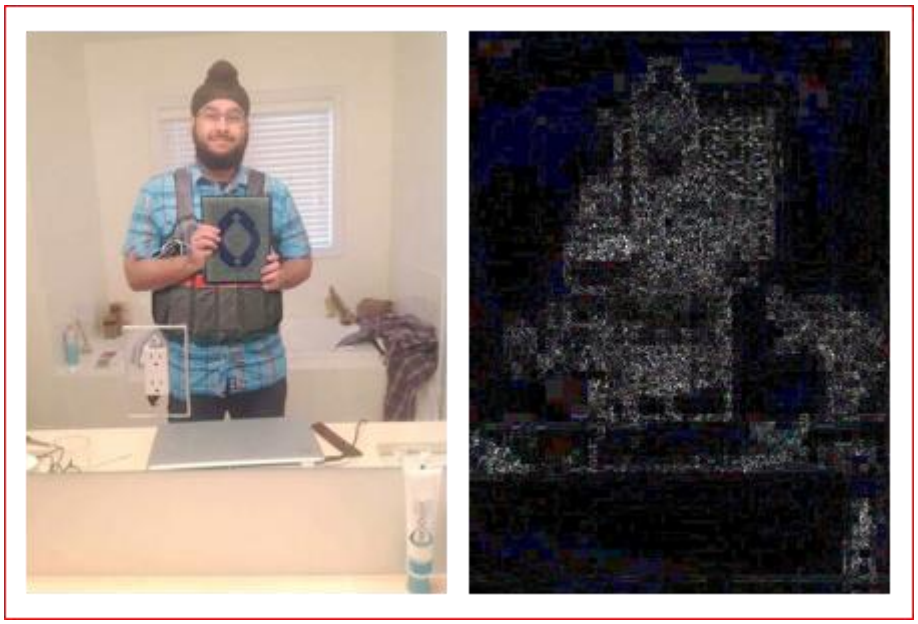
Analisa menggunakan Forensik Foto

Berikut ini kita akan coba melakukan analisa ELA pada kedua foto diatas.



Gambar 3. Analisa Foto A

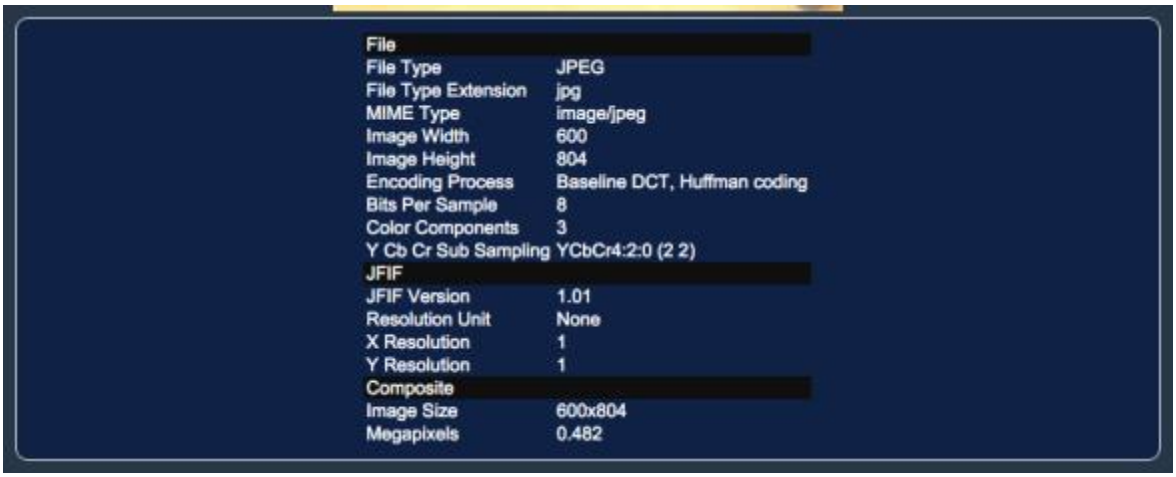
Dari gambar diatas telihat bahwa image foto A masih belum mengalami pembaruan atau editing. Hal ini bisa dilihat dari hasil ELA dimana masih mengikuti foto nyatanya.



Gambar 4. Analisa Foto B

Sudah jelas terlihat bahwa gambar foto B sudah mengalami banyak perubahan yang bisa terlihat dari hasil analisa ELA sesuai gambar di atas.

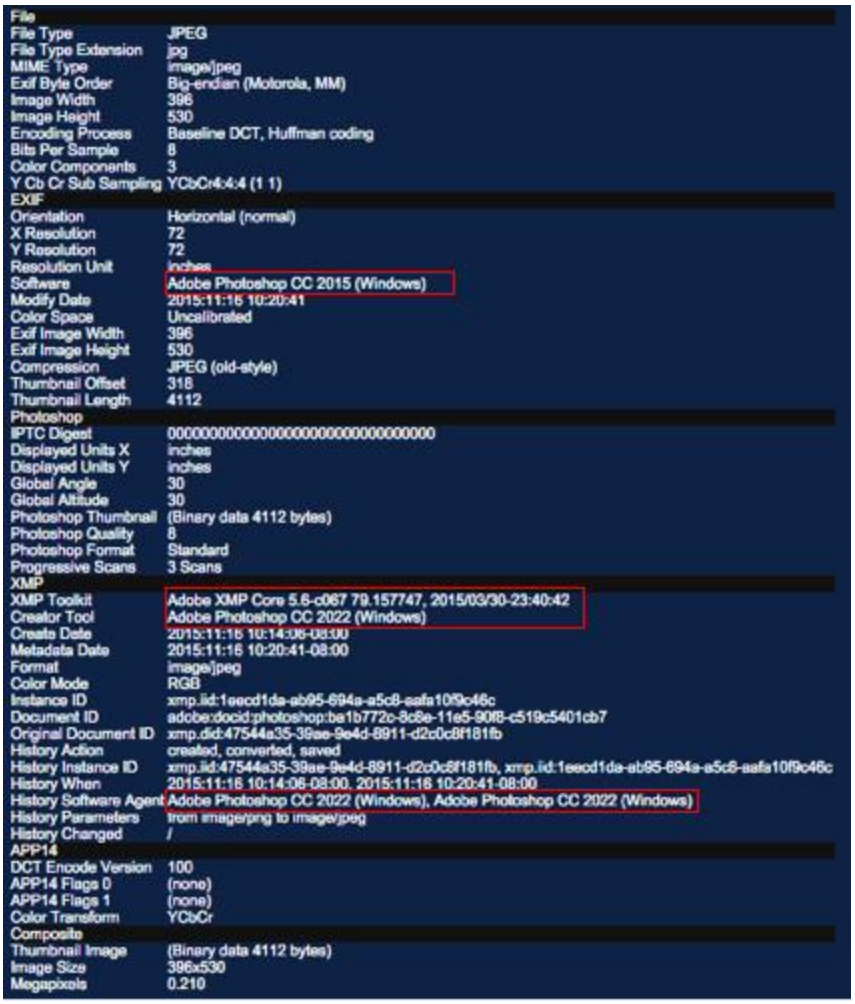
Kemudian kita coba beralih pada informasi yang ada di dalam metadata kedua file gambar tersebut.



File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Image Width	600
Image Height	804
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)
JFIF	
JFIF Version	1.01
Resolution Unit	None
X Resolution	1
Y Resolution	1
Composite	
Image Size	600x804
Megapixels	0.482

Gambar 5. Metadata Foto A

Dari gambar diatas terlihat bahwa foto A mempunyai metadata yang masih asli, dimana belum ada penambahan metadata. bisa dikatakan bahwa metadata masih digenerate oleh pengambil foto.



Gambar 6. Metadata Foto B

Gambar diatas memperlihatkan informasi metadata pada foto B yang secara teknis sudah mengalami penambahan metadata dimana foto B sudah mengalami editing menggunakan Adobe Photoshop CC 2002.

C. KESIMPULAN

Bahwa sebuah forensik multimedia memang berbeda dengan forensik komputer. Hal ini disebabkan kompleksitas kasus yang terjadi sehingga membutuhkan kombinasi ilmu forensik untuk melakukan investigasi. Sehingga forensik multimedia tidaklah sama dengan forensik komputer karena lebih kompleks baik dari sisi digital maupun non digital dalam proses investigasinya.

BAB IV
ANALISIS FORENSIK BERGERAK DAN MULTIMEDIA

Pada pembahasan sebelumnya, kita telah membahas tentang multimedia forensik. Yang mana dikatakan bahwa pada multimedia forensik, yang dicari yaitu untuk menguji keaslian dan sumber data digital tersebut. Pada kesempatan kali ini kita akan mencoba menguji sebuah gambar dan video, apakah gambar dan video tersebut asli atau rekayasa. Uji forensik pada gambar dan video ini merupakan uji forensik yang sangat sederhana. Namun walaupun sederhana, pengujian dengan cara yang akan kita bahas nantinya merupakan salah satu pengujian awal terhadap sebuah gambar dan video.

A. ANALISIS FORENSIK GAMBAR

Sebelum kita melakukan uji coba sederhana, mari kita bahas sedikit tentang foto rekayasa yang sempat heboh diawal tahun 2015 ini, yaitu foto mesra Abraham Samad yang merupakan ketua KPK dengan seorang gadis di sebuah hotel. Adapun foto yang sempat ramai dibahas tersebut seperti gambar dibawah ini.



Gambar 7. Contoh Gambar

Sekilas terlihat foto tersebut seperti asli. Foto ini dulu sangat ramai dibahas di media. Hingga akhirnya tim forensik KPK melakukan forensik multimedia terhadap foto ini dan ternyata foto ini adalah hasil rekayasa. Hasil analisis tim forensik KPK yang disampaikan oleh ketua KPK

Abraham Samad yang menyatakan foto ini adalah foto rekayasa dapat dilihat pada video dibawah ini.

Dari hasil analisis tersebut, dapat dilihat ada banyak hal yang diforensik dari foto tersebut. Mulai dari EXIFF datanya, hingga bagian-bagian terkecil fotonya. Ya memang seperti itulah hal yang dilakukan dalam multimedia forensik. Tapi seperti pembahasan kita sebelumnya, sumber yang akan diforensik multimedia haruslah sumber yang aslinya dan sumber tersebut terpercaya.

Seperti yang sempat dikatakan oleh Roy Suryo seorang pakar telematika yang dulu sempat terkenal ketika foto Abraham Samad tadi ramai tersebar, menyampaikan hal seperti yang tertulis di gambar dibawah ini.



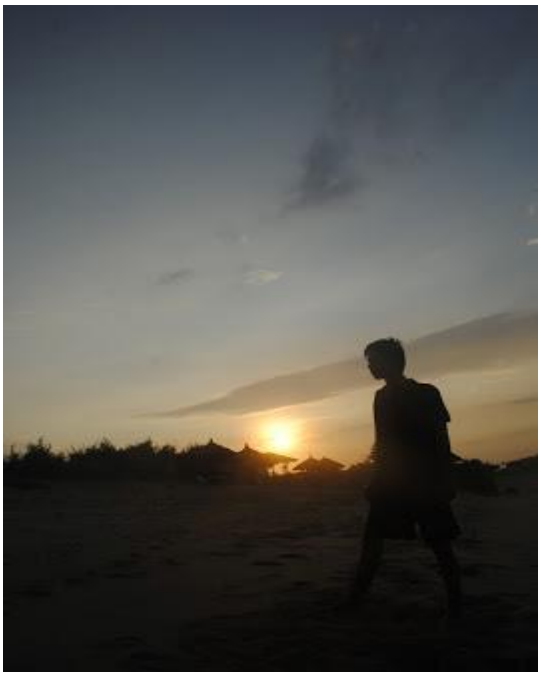
Gambar 8. Berita Gambar

Hal yang akan dilakukan Roy Suryo merupakan analisis sederhana terhadap sebuah foto. Oleh karena itu, kita juga akan mencoba melakukan eksperimen kecil untuk menganalisis meta data atau exiff file sebuah foto untuk dapat dicari mana foto yang aslinya. Ya walaupun sekali lagi perlu kita ketahui bersama bahwa melakukan pengecekkan terhadap foto asli atau tidak, tidak cukup hanya berdasarkan meta datanya saja. Tapi bisa dengan mengamati proporsi gambar, sambungan antar gambar yang tidak sempurna, perbedaan pixel warna, dan lain sebagainya.

Adapun software sederhana nan canggih yang akan kita gunakan yaitu JPEGsnoop. Software ini digunakan untuk mencek metadata sebuah foto. Oke kita coba sekarang ya. Dibawah ini ada 2 buah foto.

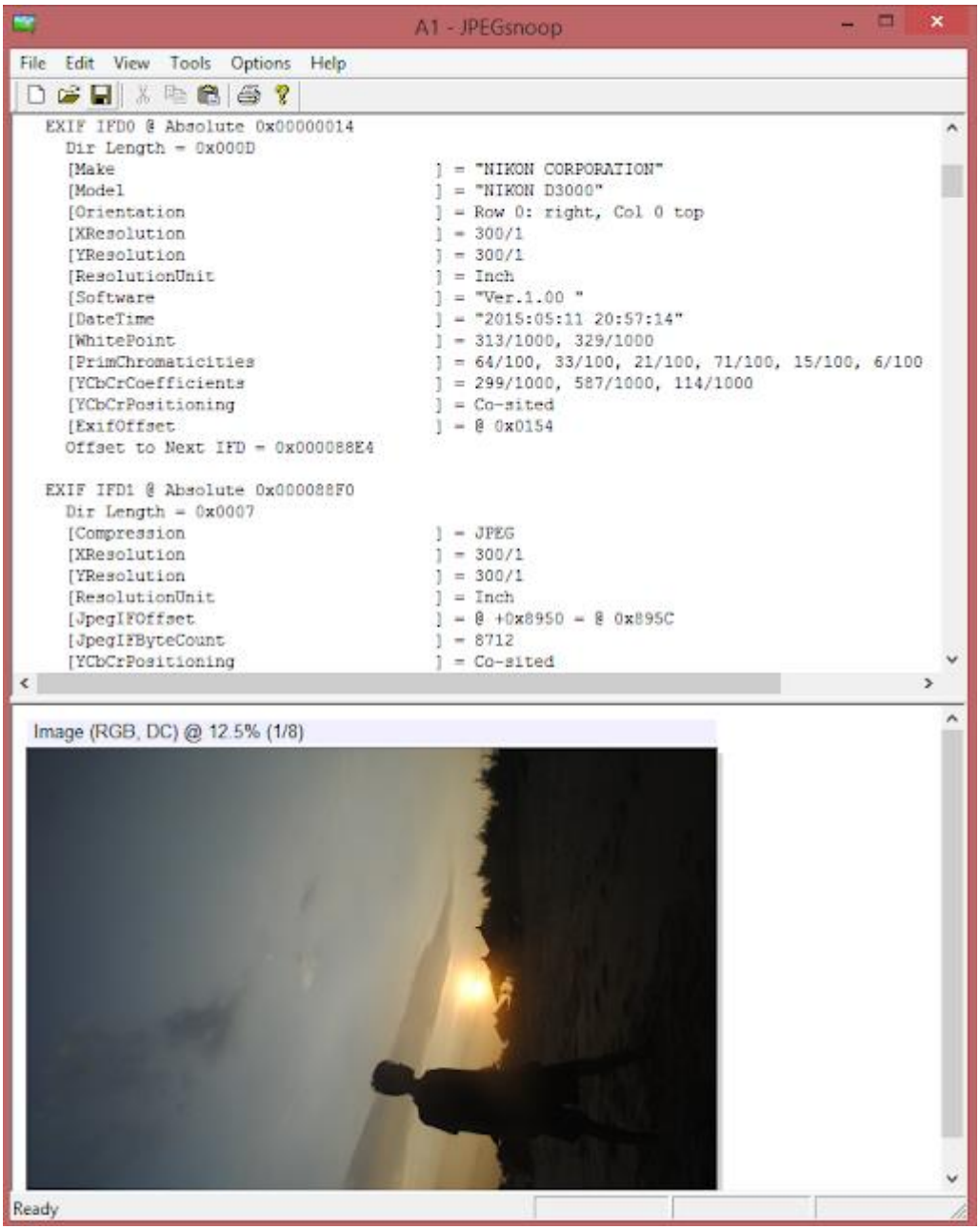


Gambar 9. Foto A1

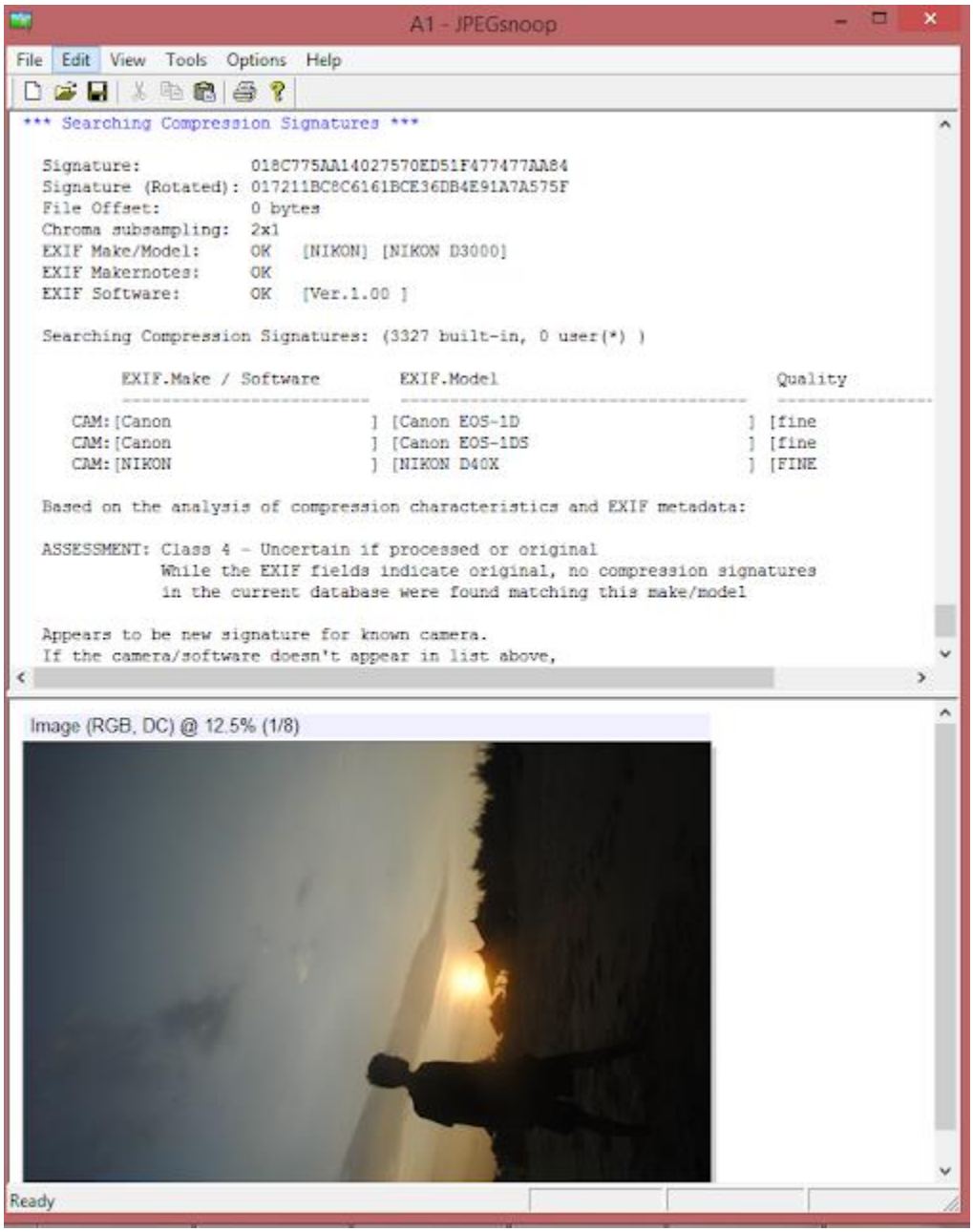


Gambar 10. Foto A2

Coba amati kedua foto diatas. Foto dengan kode A1 dan kode A2. Kira-kira manakah foto yang asli? Jika dilihat sekilas kedua foto tersebut tampak sama. Nah mari kita coba liat metadata kedua foto tersebut.



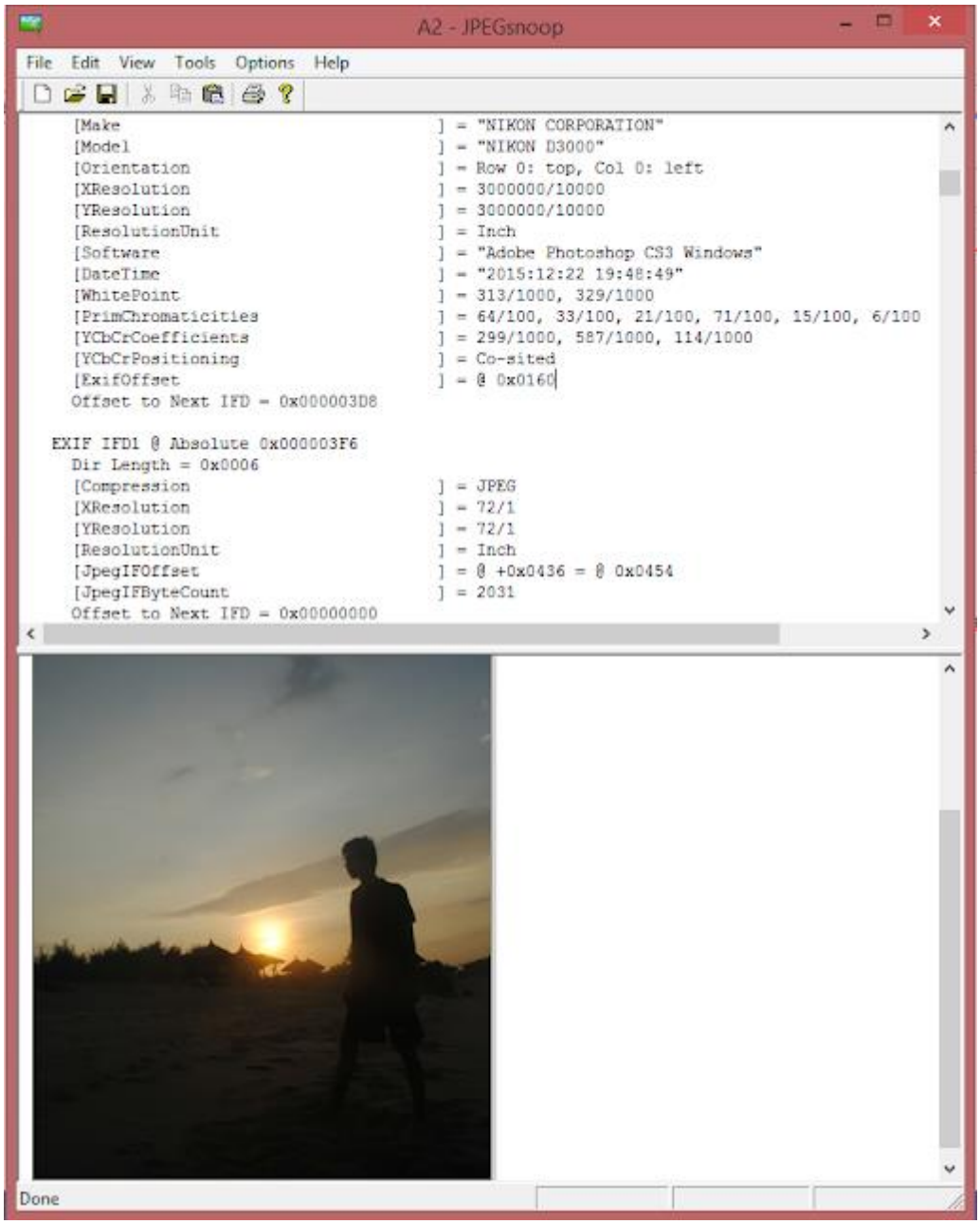
Gambar 11. Metadata Foto A1



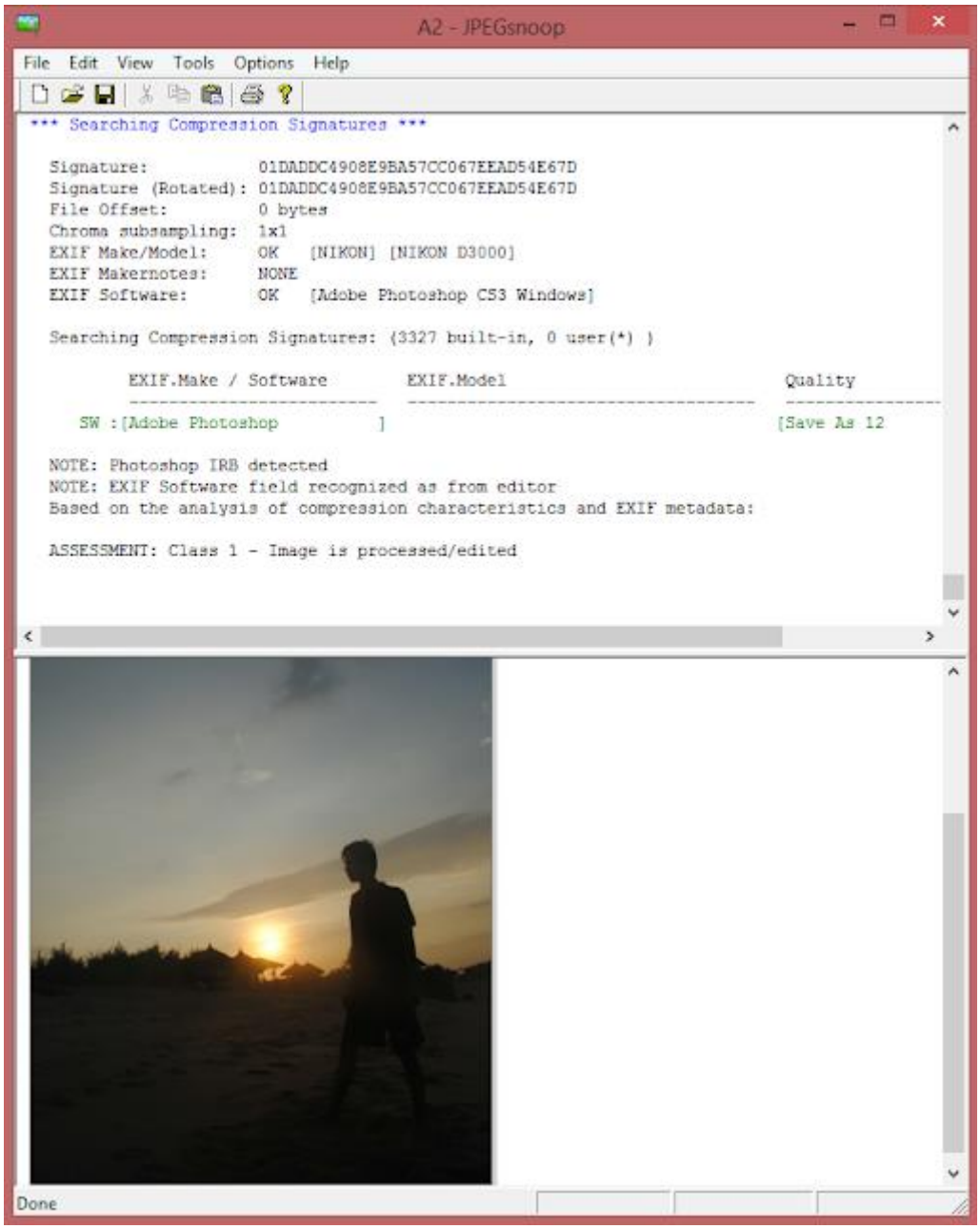
Gambar 12. Metadata Foto A1 Lanjutan

Dari metadata foto tersebut dapat kita ambil data bahwa foto ini diambil dengan menggunakan kamera Canon EOS. Dan diambil pada tanggal 11 Mei 2015. Selain itu, lihat Assessment yang diberikan oleh JPEGsnoop. Disitu tertulis kalau foto ini adalah Class 4. Yang berarti foto ini adalah foto original tanpa ada editan.

Sekarang coba kita lihat metadata foto dengan kode foto A2.



Gambar 13. Metadata Foto A2



Gambar 14. Metadata Foto A2 Lanjutan

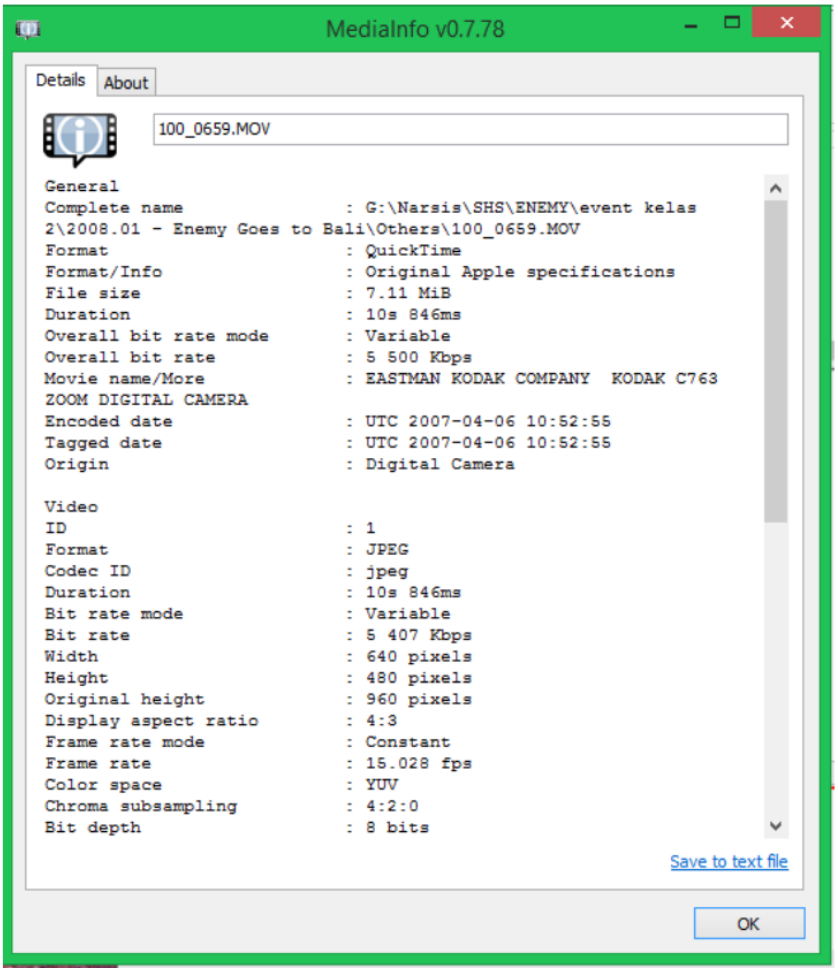
Dari metadata foto dengan kode foto A2, dapat kita lihat bahwa foto tersebut merupakan foto editan karena tertulis dengan jelas di edit menggunakan Adobe Photoshop CS3. Dan juga kode Assessment menerangkan bahwa foto ini termasuk kelas 1 yang berarti ada proses yang di edit. Walaupun identitas foto diambil dengan menggunakan Nikon masih ada, tapi di software tertulis Adobe Photoshop.

Berdasarkan metadata ini sebenarnya kita bisa ambil kesimpulan awal bahwa foto A2 merupakan foto rekayasa. Selain itu, coba perhatikan dengan saksama arah pandangan dan matahari terbenam. Di foto A1, dapat kita lihat matahari terbenam di sebelah kiri. Berarti benar matahari terbenam dari arah barat. Tapi coba perhatikan foto A2, arah pandangan dan matahari berada di sebelah kanan. Tidak mungkinkan matahari terbenam dari arah timur.

Dari analisis metadata dan analisis gambar secara sederhana, kita dapat ambil kesimpulan bahwa foto A1 merupakan foto aslinya sedangkan A2 merupakan foto editan.

B. ANALISIS FORENSIK VIDEO

Untuk melakukan simulasi sederhana ini juga diperlukan dua video, dimana yang satu merupakan video rekaman asli dan video satunya lagi merupakan video yang sudah mengalami proses diedit. Video asli yang digunakan direkam dengan menggunakan kamera digital sedangkan video edited menggunakan video film yang sudah mengalami proses edit dan kompresi kualitas. Program yang digunakan untuk melihat metada video adalah MediaInfo v0.7.78.



Gambar 15. Hasil Metadata Video Asli

Hasil metadata dari video asli menunjukkan jenis perangkat yang digunakan yaitu Eastman Kodak Company – Kodak C763 Zoom Digital Camera. Video diambil pada tanggal 2007-04-06 jam 10:52:55 dan selesai pada 2007-04-05 jam 10:53.



Gambar 16. Hasil Metadata Video Edited

Pada video ini tidak menunjukkan tanggal pengambilan video ataupun kapan video selesai diambil. Sebaliknya, video ini menunjukkan indikasi telah mengalami kompresi, yang ditandai dengan penggunaan mode kompresi lossy pada hasil analisa metadata. Selain itu terdapat informasi encoding setting. Writing library yang digunakan libmkv dan writing application yang digunakan adalah Handbrake. Handbrake adalah software open source yang digunakan untuk video transcoder.

Selain pengecekan metadata video, teknik lain yang digunakan untuk membedakan video asli atau editan adalah dengan menganalisa frame satu per satu. Video dipecah menjadi frame-frame kemudian tiap frame dianalisa apakah ada frame yang janggal atau dengan menggunakan ELA.

Berikut akan dianalisa salah satu frame dari video asli, yaitu frame 75.



Gambar 17. Frame 75 dari Video Asli



Gambar 18. ELA pada Frame 75

Pada video editan akan digunakan frame 56 yang dicurigai telah diedit. Frame 56 secara jelas memperlihatkan adanya frame transition. Dimana frame pertama adalah seorang wanita di bagian kiri frame yang terlihat transparan sedangkan frame kedua adalah terdapat dua orang yang saling bertemu di bagian kiri frame. Setelah menentukan frame yang dicurigai, kemudian dilanjutkan dengan analisa menggunakan ELA.

Hasil ELA menunjukkan terdapat beberapa bagian dari gambar yang memiliki penumpukan pixel yang ditandai dengan penumpukan titik-titik putih.



Gambar 19. Frame 56 dari Video Editan



Gambar 20. 17 ELA pada Frame 56

C. HASIL SIMULASI

Hasil simulasi sederhana menunjukkan, analisis metadata dapat digunakan untuk mengumpulkan informasi dasar seperti device yang digunakan untuk mengambil gambar atau video, waktu dan tanggal, ukuran gambar atau video, jenis kompresi yang digunakan oleh device. Deteksi device yang digunakan untuk mengambil gambar menggunakan compression signature. Hal inilah yang menyebabkan pada gambar editan tidak diketahui device yang digunakan karena gambar disimpan dengan menggunakan kompresi software bukan kompresi/proses digitalisasi dari device secara langsung.

Untuk kasus video, pada video asli, compression signature yang ada pada file adalah miliki device yang digunakan untuk merekam sedangkan pada video editan, compression signature yang digunakan berasal software yang digunakan untuk mengedit video. Namun, software editor yang canggih dapat memanipulasi metadata sehingga perlu analisa tambahan, yaitu dengan mengamati frame.

Pengamatan frame dilakukan dengan dekompresi video menjadi frame-frame. Frame yang dicurigai kemudian dianalisa dengan ELA. Berdasarkan ELA, frame yang diedit akan memiliki pesebaran pixel yang tidak rata atau penumpukan warna tertentu pada sebuah bagian gambar sehingga error levelnya dianggap tinggi, sama seperti file gambar. Pada dasarnya video adalah kumpulan dari gambar-gambar berurutan sehingga saat menganalisa frame bisa saja dianggap sedang menganalisa sebuah gambar.

BAB V
KESIMPULAN

Berkembangnya teknologi dunia digital membuat pelaku criminal juga menggunakan teknologi sebagai sarana untuk melakukan kejahatan. Salah satunya dengan menggunakan rekayasa gambar dan video baik untuk penipuan, pengancaman, ataupun merusak nama baik seseorang. Untuk itulah diperlukan pengecekan mengenai keaslian pada gambar dan video yang ada. Metode yang digunakan untuk mengetahui keaslian suatu gambar dan video bermacam-macam. Metadata analisis, frame analisis, dan pixel analisis merupakan beberapa metode forensik yang dapat dilakukan dengan program-program sederhana, sehingga dapat pula dilakukan oleh orang-orang pada umumnya. Analisis menggunakan program sederhana ini dapat membantu masyarakat umum untuk mengecek keaslian gambar dan video yang diperoleh. Hal ini diharapkan dapat menurunkan jumlah orang yang menjadi target penipuan.

A. KESIMPULAN

Analisis metadata dapat dilakukan pada file gambar dan video tetapi diperlukan analisis tambahan karena beberapa program canggih dapat memanipulasi data pada metadata. Metode sederhana untuk melakukan analisis pixel, antara lain *clone detection* dan ELA (*Error Level Analisys*).

Gambar yang dimanipulasi akan menggunakan clone untuk menyamarkan gap antara gambar asli dengan bagian yang ditambahkan pada gambar.

Secara professional, deteksi frame dilakukan dengan deteksi encoding di tiap frame sedangkan secara sederhana dapat dilakukan dengan memantau frame by frame.

B. SARAN

Perlu adanya tools online gratis yang dapat mendeteksi keaslian video karena analisis pada video membutuhkan waktu yang lebih lama, apalagi bila dilakukan oleh masyarakat pada umumnya.

REFERENSI

1) Caldell, R., Amerini, I., & Picchioni, F. (2010). Multimedia Forensic Techniques for Acquisition Device Identification and Digital Image Authentication, 130–132.https://doi.org/10.4018/978-1-60566-836-9.ch006
2) Bohme, R., Freiling, F., Gloe, T., & Kirchner, M. (2009). Multimedia Forensics is not Computer Forensics. International Workshop on Computational Forensics. Retrieved from http://www1.inf.tu-dresden.de/~rb21/publications/BFGK2009_Multimedia_Forensics_Is_Not_Computer_Forensics_IWCF.pdf
3) Lizarti, Nora. (2016). Konsep Integrated Multimedia Forensic Investigation Framework (IMFIF) Dengan Menggunakan Metode Composite Logic. Tesis. Yogyakarta.
4) Prayudi, Y. (2016). Video Forensics : Catatan dari Ruang Sidang (II). Retrieved September 30, 2016, from https://catatanforensikadigital.wordpress.com/2016/09/20/video-forensics-catatan-dari-ruang-sidang-ii/
5) Prayudi, Y. (2016). Video Forensics : Bahan Kajian. Retrieved September 30, 2016, from https://catatanforensikadigital.wordpress.com/2016/08/31/video-forensik/
6) Prayudi, Y. (2016). Video Forensics : Pelajaran dari Ruang Sidang Pengadilan. Retrieved September 30, 2016, from https://catatanforensikadigital.wordpress.com/2016/08/11/video-forensics-pelajaran-dari-ruang-sidang/
7) R. Böhme, F. C. Freiling, T. Gloe, and M. Kirchner, "Multimedia forensics is not computer forensics," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5718 LNCS, pp. 90–103, 2009.
8) Ini Pendapat Pakar Telematika Soal Foto Mesra Mirip Ketua KPK. (2015, January 14).jpnn.com. Jakarta. Retrieved from http://www.jpnn.com/index.php?mib=berita.detail&id=281301
9) Triono, S. (2015, February 2). Penjelasan Abraham Samad Soal Foto Syur Bersama Feriyani Lim.liputan6.com. Jakarta. Retrieved from http://news.liputan6.com/read/2169955/penjelasan-abraham-samad-soal-foto-syur-bersama-feriyani-lim
10) Aaron, Phillip; David, Cowen & Chris, Davis (2009). Hacking Exposed Computer Forensics, Second Edition: Computer Forensics Secrets & Solutions (dalam bahasa Inggris) (edisi ke-2). McGraw-Hill Education. ASIN B002R0JXF4. ISBN 9780071626774.
11) Adams, Richard Brian (2012). 'The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice (PDF) (dalam bahasa Inggris). Murdoch University. Diarsipkan (PDF) dari versi asli tanggal 2014-11-14.
12) Adams, Richard (2013). "The emergence of cloud storage and the need for a new digital forensic process model". Dalam Ruan, Keyun. Cybercrime and cloud forensics: applications for investigation processes (PDF) (dalam bahasa Inggris). USA: Information Science

Reference (IGI Global). hlm. 79–104. doi:10.4018/978-1-4666-2662-1.ch004 alt=Dapat diakses gratis. ISBN 9781466626935.

13) Krawetz Ph.D., N. (2007). Digital Image Analysis and Forensic - A Picture's Worth. USA: Hacker Factor Solutions.
14) Xie, Z., Jiang, Q., Wu, H., & Fu, B. (2010). Quality Control and Uncertainly Analysis Image Metadata. IEEE, 1-4.
15) Vazquez-Padin, D., Fontani, M., Bianchi, T., P. Comesana, Piva, A., & Barni, M. (2012). Detection of Video Double Encoding with GOP Size Estimation. International Workshop on Information Forensics and Security (pp. 151-156). Tenerife: IEEE.
16) Milani, S., Fontani, M., Bestagini, P., Barni, M., Piva, A., Tagliasacchi, M., Tubaro, S. (2012). An Overview on Video Forensics. APSIPA Transactions on Signal and Information Processing, 1, e2 doi:10.1017/ATSIP.2012.2.
17) National Forensic Science Technology. (2013). National Forensic Science Technology Centre. Retrieved from National Forensic Science Technology Centre: www.forensicsciencesimplified.org
18) Putusan Mahkamah Agung Republik Indonesia, 20/Pid.B/2013/PN.Rni (Pengadilan Negeri Ranai Juli 27, 2013).
19) Gironi, A., Fontani, M., Bianchi, T., Piva, A., & Barni, M. (2014). A Video Forensic Technique For Detecting Frame Deletion and Insertion. International Conference on Acoustic, Speech and Signal Processing (pp. 6226-6230). Florence: IEEE.
20) Putusan Mahkamah Agung Republik Indonesia, 87/PID/2014/PT.DKI (Pengadilan Tinggi Jakarta Maret 26, 2014).
21) Sutardja, A., Omar, R., & Zaho, Y. (2015). Forensic Methods for Detecting Image Manipulation - Copy Move. California: EECS Barkeley.
22) Sahera, C. (2015). Forensik Gambar dan Video - Kasus Pornografi. Ujian Akhir Semester. Indonesia.