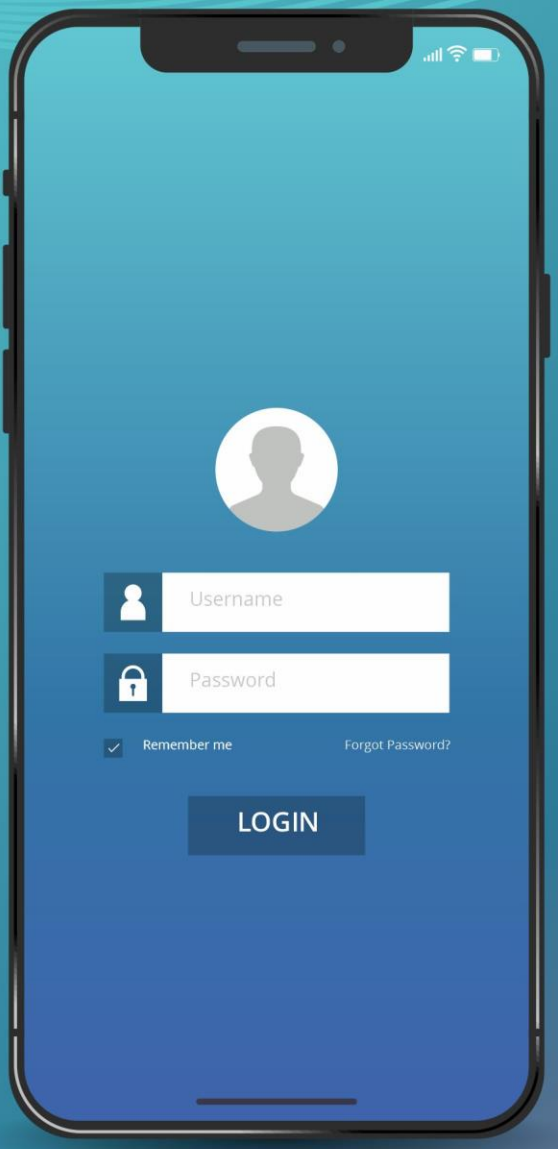
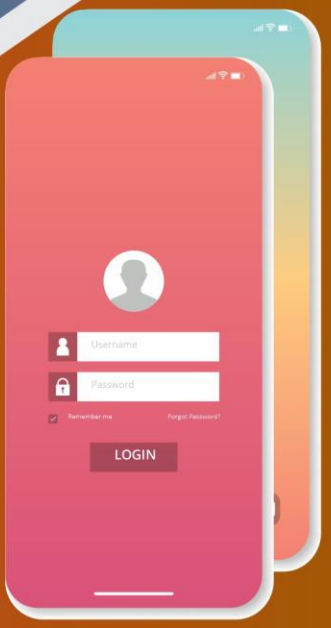
MODUL PRAKTIKUM



MOBILE forensic



UNIVERSITAS TEKNOLOGI MATARAM

Jl. Kampus Universitas Teknologi Mataram, Kekalik, Mataram

1. MOBILE FORENSIC

Mobile Forensics merupakan ilmu atau keahlian dalam proses dan mengelola barang bukti digital yang berasal dari mobile devices, handphone/cell-phone, tablets, dan berbagai istilah serta varian sejenis lainnya dengan metode yang dapat dipertanggung jawabkan. Pada prinsipnya mobile forensics memiliki kesamaan metode dengan digital forensics yang sudah ada, hanya saja kita mengubah point of view dari target bukti digital yang biasanya terdapat pada perangkat computer desktop atau laptop kemudian dialihkan pada perangkat telepon bergerak atau mobile devices, perbedaan yang sangat besar adalah pada sisi teknis pelaksanaanya.

Mobile forensics merupakan respon digital forensics terhadap perkembangan teknologi informasi yang telah mengevolusi perangkat komputer tradisional menjadi komputer tablet dan dunia telekomunikasi yang telah mengaplikasikan komputer dengan sangat baik sehingga menjadi smartphone. Sehingga ketergantungan manusia terhadap perangkat telekomunikasi saat ini sangatlah besar, karena hampir semua tugas sederhana dari prinsip kerja komputer telah dapat diaplikasikan. Kemajuan teknologi ini juga mempengaruhi perubahan gaya hidup dan cara bersosialisasi masyarakat modern saat ini, yang mau tidak mau juga banyak melibatkan teknologi ini dalam setiap aktivitas manusia baik itu positif dan negatif termasuk diantaranya aktivitas yang berhubungan dengan kejahatan. Banyak modus operandi yang terjadi dengan melibatkan perangkat telekomuniasi bergerak bahkan popularitas smartphone juga menjadi ladang baru yang sangat menarik bagi hacker dalam kejahatan dunia maya.

Sejak pertama mobile devices mulai dihadirkan dalam persidangan dan menjadi barang bukti hukum yang sah dengan teknologi yang sangat jauh tertinggal dari smartphone saat ini, tantangan yang dihadapi oleh investigator digital forensics semakin hari semakin kompleks karena teknologi yang mengikutinya juga semakin lama semakin berkembang. Perbedaan mobile device tentu berbeda juga karakteristik dari hardwarenya, berbeda juga arsitektur dari sistem operasinya dan berbeda teknologi celullarnya. Butuh keahlian yang khusus dan proses belajar yang cukup mendalam untuk dapat menjadi ahli dibidang ini. Basic knowledge yang harus dimiliki untuk menjadi seorang ahli dalam mobile forensics?



Gambar 1 : Mobile Forensik

Seorang ahli mobile forensics harus mengerti dan paham mengenai apa itu mobile phone dan berbagai jenisnya, apa saja sistem operasi yang terdapat dalam mobile phone tersebut, mengerti bagaimana mobile forensics itu dilakukan serta prosesnya, tahu apa saja tools software dan hardware yang harus digunakan pada masing - masing jenis dari mobile phone dan sistem operasinya. Untuk mencakup semua ilmu pengetahuan yang diperlukan ini, seorang ahli mobile forensics harus peka terhadap perkembangan teknologi dari mobile phone. Potensi mobile devices sebagai alat kejahatan.

Banyak hal yang dapat dilakukan dengan menggunakan mobile devices saat ini, kemajuan teknologi seakan membuat komputer dalam genggaman kita. Berbagai potensi manfaat dari mobile devices baik itu buruk maupun positif seiring mengikuti para penggunanya. Terkait dengan bahasan pada artikel ini yaitu mobile forensics, maka apa saja potensi kejahatan yang bisa dilakukan dengan menggunakan sebuah mobile devices, beberapa diantaranya adalah sebagai berikut:

- Penyebaran pornografi (gambar dan video)
- Transaksi data rahasia dari perusahaan
- Sms dan mms berbau ancaman
- Kloning SIM data untuk penipuan
- Spamming
- Penyebaran virus dan trojan yang bertujuan untuk aktivitas ilegal Informasi penting sebagai alat bukti digital terkait mobile forensics

Tujuan utama dari mobile forensics adalah mencari dan menggali berbagai informasi yang terkandung dalam mobile devices yang berpotensi sebagai alat bukti digital untuk kemudian dianalisa

dan diolah agar dapat dihadirkan ke tengah persidangan sebagai alat bukti yang sah tanpa mengurangi kaidah dari aturan dan metode digital forensics sehingga hasilnya dapat dipertanggung jawabkan. Berikut adalah beberapa hal penting yang dapat berpotensi menjadi bukti digital dalam digital forensics secara umum (belum termasuk berbagai aplikasi smartphone teknologi terbaru):

- Call history, phonebook, informasi data dari SIM card
- SMS dan MMS
- Internet Setting (GPRS & WAP)
- Network informasi (GPS location)
- Email, memo, calender events
- Aktivitas browsing
- Photo, audio files dan video, audio recording

Banyaknya informasi yang bisa didapat dan besarnya potensi yang dimiliki oleh informasi tersebut untuk membuka tabir sebuah investigasi menjadikan mobile forensics salah satu elemen yang penting didalam digital forensics saat ini. Pesatnya kemajuan teknologi mobile devices dan semakin bertambahnya pengguna dari mobile devices itu sendiri membuat mobile forensics sangat menantang dan menjadi lahan yang menjanjikan sebagai sebuah profesi dimasa yang akan datang. Sehingga pengetahuan ini sangatlah layak jadi pilihan bagi kita yang bergelut didunia digital forensics khususnya dan dunia IT pada umumnya. Semoga artikel ini dapat bermanfaat bagi orang banyak dan dapat menjadi gambaran sederhana tentang apa itu Mobile forensics.

2. Handled Forensik

Handheld forensik adalah pemeriksaan perangkat keras dan perangkat lunak yang biasanya merupakan unit terpadu dalam mengejar bukti untuk membantah atau membuktikan sebuah tuduhan.

Mengapa perangkat genggam begitu penting dalam pemrosesan forensik? Jawabannya sederhana. Handhled device adalah satu-satunya perangkat yang dapat dimiliki oleh tersangka dengan setiap saat berdasarkan ukurannya, dan mereka memiliki akses langsung ke perangkat satu sama lain karena mereka adalah perangkat boot siklus langsung. Selain itu, ini adalah perangkat yang biasanya menyimpan semua rahasia kecil kami yang kotor dengan gambar berwarna dan pesan teks deskriptif.

Mereka adalah bukti bukti bagi pemeriksa forensik. Banyak perangkat genggam diperdagangkan di situs lelang populer secara online karena orang selalu mencari gadget terbaru mereka. dapat memamerkan.Kami mengumpulkan berbagai perangkat ini untuk tujuan pengujian dan menemukan bahwa 80 persen dari mereka menyimpan informasi pengguna pada perangkat. Informasi berkisar dari buku alamat lengkap, e-mail terkait pekerjaan, hingga gambar yang merupakan momen intim. . Anehnya saat kami menghubungi orang-orang yang termasuk dalam perangkat, kebanyakan dari mereka tidak tahu bahwa data itu tersimpan di perangkat, apalagi bisa dipulihkan. Rahasia kecil yang bagus sudah matang untuk taki. ng untuk pemeriksa forensik terlatih. Hal-hal ini membuatnya jadi perangkat genggam dapat membawa beberapa bukti paling penting dalam pemeriksaan forensik Anda. Jejak digital pada perangkat genggam jauh lebih besar daripada kebanyakan anggapan. Jadi sekarang kita tahu betapa pentingnya perangkat dalam pemrosesan forensik, penting untuk memiliki pemahaman yang baik tentang bagaimana forensik genggam mempengaruhi empat fondasi utama forensik digital.

Penggunaan ponsel dalam kejahatan secara luas diakui untuk beberapa tahun, tetapi studi forensik perangkat mobile merupakan bidang yang relatif baru, berasal dari awal 2000-an. Sebuah proliferasi ponsel (terutama smartphone) di pasar konsumen menyebabkan permintaan untuk pemeriksaan forensik dari perangkat, yang tidak dapat dipenuhi oleh ada komputer forensik teknik.

Proses investigasi biasanya difokuskan pada data yang sederhana seperti data panggilan, dan komunikasi seperti email atau sms, dan juga data yang sudah terhapus dari media penyimpanan mobile device. Mobile devices biasanya juga bisa digunakan untuk menemukan informasi mengenai lokasi, yaitu mengunakan GPS atau alat pencari lokasi atau melalui cell site logs, yang melacak perangkat yang masuk di dalam range nya.

Informasi yang diambil dari perangkat mobile dapat berguna dalam berbagai masalah hukum, administratif dan investigasi seperti:

- Pencurian Kekayaan Intelektual
- Perusahaan Penipuan
- Penyalahgunaan Properti

- Perceraian & Hukum Keluarga
- Geo-Lokasi Kontroversi
- Bukti Kejahatan

a. Protokol Komunikasi

- Tools Komunikasi utama perangkat mobile melalui tiga teknologi Seluler, WiFi, dan Bluetooth :
- Komunikasi seluler melibatkan teknologi ini membagi sebuah daerah dengan layanan geografis yang besar ke daerah yang lebih kecil yang disebut sel. Setiap sel berisi perangkat komunikasi, biasanya pada sebuah menara yang mentransmisikan sinyal radio ke dan dari perangkat mobile. Teknologi transmisi yang digunakan untuk komunikasi, diantaranya GSM, CDMA, GPRS, EV-DO, EDGE, DECT, TDMA dan iDEN.
- WiFi sama seperti seluler, yaitu mentransmisikan komunikasi dengan menggunakan gelombang radio, tetapi menggunakan frekuensi yang lebih tinggi dan umumnya jauh lebih cepat. Perjalanan komunikasi WiFi dari perangkat mobile ke titik akses nirkabel, kira-kira dengan modem/router decode komunikasi dan kemudian meneruskannya sampai ke internet. Titik akses harus dalam jarak relatif sebuah fisik (biasanya sekitar 100 kaki atau kurang) ke perangkat mobile untuk menerima sinyal WiFi-nya.
- Bluetooth adalah komunikasi nirkabel, tetapi tujuannya agak berbeda dari selular atau WiFi. Bluetooth dirancang untuk memungkinkan berbagai perangkat yang secara fisik dekat satu sama lain (umumnya kurang dari 30 kaki). Dengan kata lain, Bluetooth dapat mengaktifkan iPhone anda untuk berkomunikasi secara otomatis dengan audio headset, atau iPad anda untuk berkomunikasi secara otomatis dengan keyboard eksternal anda.

b. Storage Pada Mobile Device

Perangkat mobile pada umumnya dapat menyimpan informasi pada tiga lokasi. Salah satunya adalah memori internal. Memori internal pada perangkat mobile terdiri dari RAM (Random Access Memory) dan ROM (ReadOnlyMemory). RAM adalah ruang memori pada perangkat mobile yang dapat digunakan untuk menyimpan sementara informasi selama perangkat melakukan tugas. Saat

perangkat dimatikan, semua data dalam RAM umumnya akan hilang. ROM umumnya pre-diprogram, sering dirancang untuk melakukan tugas-tugas diskrit tertentu. Perangkat mobile juga menyimpan informasi dalam SIM (SubscriberIdentityModule) dan kartu memory. terakhir, perangkat mobile dapat menyimpan informasi tentang berbagai mesin dan perangkat lainnya yang berinteraksi dengan perangkat mobile, termasuk server email, server dari selular penyedia jasa (untuk pesan teks), dan komputer pribadi.

- **Tablet**

Tablet merupakan perangkat komputer layar sentuh. Teknologi tablet digital ini memungkinkan pengguna computer untuk mempergunakan stylus atau pulpen digital selain keyboard ataupun mouse.Istilah tablet dipopulerkan oleh Microsoft pada tahun 2001, tetapi PC tablet sekarang mengacu pada setiap komputer pribadi yang berukuran tablet, jika pun ada tidak menggunakan Windows melainkan sistem operasi PC yang lain. Tablet dapat menggunakan papan ketik virtual dan pengenalan tulisan tangan untuk input teks melalui layar sentuh.Perangkat keras sebuah tablet pada umumnya hampir sama dengan seperti netbook, yang memiliki prosessor, RAM, storage, hanya saja pada tablet menjadi satu kesatuan, yang dinamakan SoC (system on a chip).

Tempat penyimpanan informasi pada sebuah tablet terdiri dari memory internal yang terbagi jadi dua yaitu internal tablet storage serta internal SD card. Biasanya sebuah tablet menyediakan slot yang dapat digunakan untuk menambah kapasitas penyimpanan informasi yang lebih besar dengan menambahkan MicroSD.

- **Handphone dan PDA (Personal Digital Assistant)**

PDA adalah sebuah komputer seukuran telapak tangan yang dapat digunakan untuk menyimpan, meng-akses dan meng-organize informasi. Beberapa PDA bekerja dengan menggunakan sistem operasi berbasis Windows atau juga sistem operasi Palm. Biasanya PDA juga dilengkapai dengan virtual keyboard pada layarnya dan juga dapat menggunakan keyboard tambahan yang dipasang ke PDA agar proses input menjadi lebih cepat. Proses memasukkan data yang paling umum pada PDA adalah lewat StylusPen yang

disertakan bersama PDA tersebut, sehinga kita dapat memasukkan huruf dengan menuliskannya pada permukaan layar PDA dengan menggunakan software Grafitti.

HP(HandPhone) dan PDA (Personal Digital Assistants) sudah tak dianggap sebagai barang mewah lagi . Dari sekian banyak teknologi yang berkembang, salah satunya HP dan PDA lah yang sudah berkembang pesat dan sudah bermasyarakat bahkan sampai kalangan menengah kebawah. HP dan PDA dapat digunakan untuk berkomunikasi jika sudah terpasang SIM(SubscriberIdentityModule) dari salah satu provider telekomunikasi. MS(mobilestation) dilengkapi dengan sebuah smartcard yang dikenal dengan SIM (SubscriberIdentityModule) yang berisi nomor identitas pelanggan. Dengan memasukkan SIM ke dalam terminal GSM (handphone), pemakai dapat menerima panggilan, melakukan panggilan, dan memperoleh layanan yang lain seperti SMS, MMS serta GPRS.

Dari SIM (Subscriber Identity Module) itu semua data pelanggan akan terinput ke Home Location Register (HLR) yang merupakan bagian system dari NetworkSwitching System (NSS). HLR adalah jaringan database tersentral yang menyimpan dan mengatur semua mobilesubscription yang dimiliki operator tertentu.HLR bekerja sebagai penyimpanan permanen untuk informasi subscription seseorang sampai subscription itu dibatalkan.Data SIM (SubscriberIdentityModule) pelanggan bisa kita lacak keberadaan lokasi asal SIM card bersangkutan dengan menggunakan aplikasi HLR Lookup. Pada PDA palm, terdapat deviceRAM-based “always on”. Hal tersebut merupakan kelebihan sekaligus kelemahan dari PDA Palm. Karena RAM volatile memerlukan arus yang konstan. Jadi ketika baterai rundown, informasi akan terhapus. Data akan hilang jika belum dilakukan sinkrinisasi ke desktop. Untuk mengatasi masalah ini, pembuat PDA menyertakan slot untuk nonvolatileflashmemory. Memori tersebut berguna untuk menyimpan data saat daya dimatikan.

c. Paraben

Paraben Device Seizure (PDS) dirancang untuk memungkinkan peneliti untuk memperoleh data yang terdapat pada ponsel, smartphones, GPS dan perangkat PDA tanpa mempengaruhi integritas data. Ponsel tersebut dirancang untuk mengambil data seperti nomor telepon, tanggal, gambar,

riwayat panggilan, dan dump data penuh (mirip dengan dump flasher). Serta dirancang dengan menyediakan pilihan beberapa analitik dengan built in mesin pencari, alat-alat manajemen kasus seperti bookmark dan data impor dan dirancang untuk memperoleh, mencari, dan melaporkan semua data yang terkait dengan sebagian besar versi dari OS perangkat ponsel tersebut atau bias juga dari RIM tersebut seperti RIM pada blackberry.

Paraben Point to point telah diinterigasikan menjadi device seizure. Point to point mempunyai fitur mengkonversi GPS poin data yang akan dibaca secara langsung ke Google Earth sehingga peneliti dapat dengan cepat dan mudah menampilkan di mana lokasi-lokasi GPS tersebut. Paraben device seizure dapat dijalankan dengan peralatan yang lama untuk ujian forensik.

Perangkat bisa mendapatkan informasi atau memperoleh data lebih lanjut tergantung pada modelnya, seperti berikut:

- SMS History (Text Messages)
- Deleted SMS (Text Messages)
- Phonebook (both stored in the memory of the phone and on the SIM card)
- Call History,Call Dates dan Durations
- Received Calls, Dialed Numbers, dan Missed calls
- Datebook, Scheduler, dan Calendar
- To-Do List
- System Files
- Multimedia Files (Images, Videos, etc.)
- Java Files
- Deleted Data
- Quicknotes
- GPS Waypoints, Tracks, Routes, etc.
- RAM/ROM
- PDA Databases
- E-mail
- Registry (Windows Mobile Devices)

d. XRY

XRY adalah sebuah perangkat lunak yang dirancang untuk berjalan pada sistem operasi windows, yang memungkinkan untuk melakukan ekstraksi data forensik yang aman dari berbagai macam perangkat mobile, seperti smartphone, gps navigasi unit, modem 3G, pemutar musik portabel dan tablet terbaru prosesor seperti iPad. XRY dikembangkan oleh Micro Systemation AB.

Mengekstrak data dari ponsel atau telepon seluler adalah keterampilan spesialis dan tidak sama dengan memulihkan informasi dari komputer. XRY dirancang dan dikembangkan untuk membuat proses yang lebih mudah, dengan dukungan untuk lebih dari 5.300 profil perangkat yang berbeda selular. XRY menyediakan solusi lengkap untuk mendapatkan apa yang dibutuhkan(user) dan perangkat lunak memandu user melalui proses langkah demi langkah untuk membuatnya semudah mungkin.

Ada beberapa jenis XRY yang berbeda tergantung pada fungsi masing-masing:

- XRY Logis

  XRY logis adalah solusi perangkat lunak berbasis PC (Windows), lengkap dengan perangkat keras yang diperlukan untuk penyelidikan forensik perangkat mobile. XRY adalah standar dalam forensik perangkat mobile dan pilihan pertama di antara lembaga penegak hukum di seluruh dunia. XRY Logis menyediakan tampilan yang ramah, dan pengguna untuk menganalisis berbagai macam ponsel melalui proses pemeriksaan yang aman untuk memulihkan data dengan cara forensik yang aman. Informasi yang dikumpulkan dari perangkat diperiksa adalah langsung tersedia untuk meninjau secara aman dan dapat dilacak, menjamin kedudukan hukum dan kredibilitas di pengadilan.

  Perangkat lunak XRY logis memungkinkan peneliti untuk melakukan ‘logis’ akuisisi data. Proses forensik digunakan untuk berkomunikasi dengan, dan membaca isi, perangkat, yang biasanya menghasilkan informasi. Dengan XRY, laporan kejadian dibuat dalam beberapa menit yang dengan mudah dapat disesuaikan dengan kebutuhan pengguna, termasuk referensi dan branding sendiri pengguna seperti yang diperlukan. Laporan yang dihasilkan dapat dicetak secara keseluruhan, atau data yang dipilih dibutuhkan oleh para

peneliti dapat disiapkan. Menggunakan fungsi ekspor XRY itu, pengguna diberikan berbagai fungsi untuk memfasilitasi distribusi lebih lanjut dan analisis data.

- XRY Fisik

XRY fisik adalah paket perangkat lunak untuk pemulihan fisik data dari perangkat mobile. Dump memori dari masing-masing perangkat individu adalah sebuah struktur data yang kompleks, sehingga Systemation Micro telah membuat XRY fisik untuk lebih mudah dalam mencari informasi. XRY fisik berbeda karena memungkinkan forensik spesialis mendorong investigasi lebih jauh dengan melakukan akuisisi data fisik. Sebuah proses yang menghasilkan hex-dump dari memori telepon, biasanya melewati sistem operasi perangkat. Hal ini mengharuskan pemulihan untuk menampilkan informasi yang telah dihapus.

XRY fisik memiliki keuntungan yaitu dapat mengungkapkan data yang dilindungi dan dihapus, yang mungkin tidak tersedia melalui analisis logis. Melalui proses dumping data serta melakukan decoding(secara otomatis) untuk merekonstruksi konten. Fisik XRY dapat mengamankan lapisan baru seluruh data berharga bagi para penyidik dan pemeriksa forensik.

- XRY Complete

XRY yang terakhir,yaitu XRY complete(lengkap) adalah sebuah sistem yang dimana semua masuk kedalam satu forensik mobile yang terbuat dari Systemation Mikro,yaitu menggabungkan kedua solusi kami logis dan fisik ke dalam satu paket. XRY ini memungkinkan peneliti dapat mengakses penuh ke semua metode yang untuk memulihkan data dari perangkat mobile tersebut.

XRY ini bertujuan agar dapat dibangun solusi perangkat lunak berbasis lengkap dengan semua perangkat keras yang diperlukan untuk memulihkan data dari perangkat mobile dengan cara forensik yang aman. Dengan XRY ini dapat mencapai lebih banyak dan lebih dalam perangkat mobile untuk mengembalikan atau memulihkan data penting yang terdapat pada perangkat mobile tersebut. Dengan kombinasi alat analisis logis dan

fisik yang tersedia untuk perangkat yang didukung XRY lengkap, dapat menghasilkan laporan gabungan yang mengandung baik data hidup dan dihapus dari perangkat yang sama. Sistem XRY adalah sebuah sistem forensik lengkap mobile disertakan dengan semua peralatan yang diperlukan yang dibutuhkan untuk melakukan pemeriksaan forensik perangkat mobile dari kotak.

e. Mobile Phone Forensik

Mobile forensik merupakan cabang dari forensik digital yang berkaitan dengan pemulihan bukti digital atau data dari perangkat mobile. Perangkat selular frase biasanya merujuk ke ponsel , namun juga dapat berhubungan dengan perangkat digital yang memiliki baik memori internal dan komunikasi kemampuan.

Penggunaan ponsel dalam kejahatan secara luas diakui untuk beberapa tahun, tetapi studi forensik perangkat mobile merupakan bidang yang relatif baru, berasal dari awal 2000-an. Sebuah proliferasi ponsel (terutama smartphone) di pasar konsumen menyebabkan permintaan untuk pemeriksaan forensik dari perangkat, yang tidak dapat dipenuhi oleh ada komputer forensik teknik. Proses investigasi biasanya difokuskan pada data yang sederhana seperti data panggilan, dan komunikasi seperti email atau sms, dan juga data yang sudah terhapus dari media penyimpanan mobile device. Mobile devices biasanya juga bisa digunakan untuk menemukan informasi mengenai lokasi, yaitu mengunakan GPS atau alat pencari lokasi atau melalui cell site logs, yang melacak perangkat yang masuk di dalam range nya.

Informasi yang diambil dari perangkat mobile dapat berguna dalam berbagai masalah hukum, administratif dan investigasi seperti:

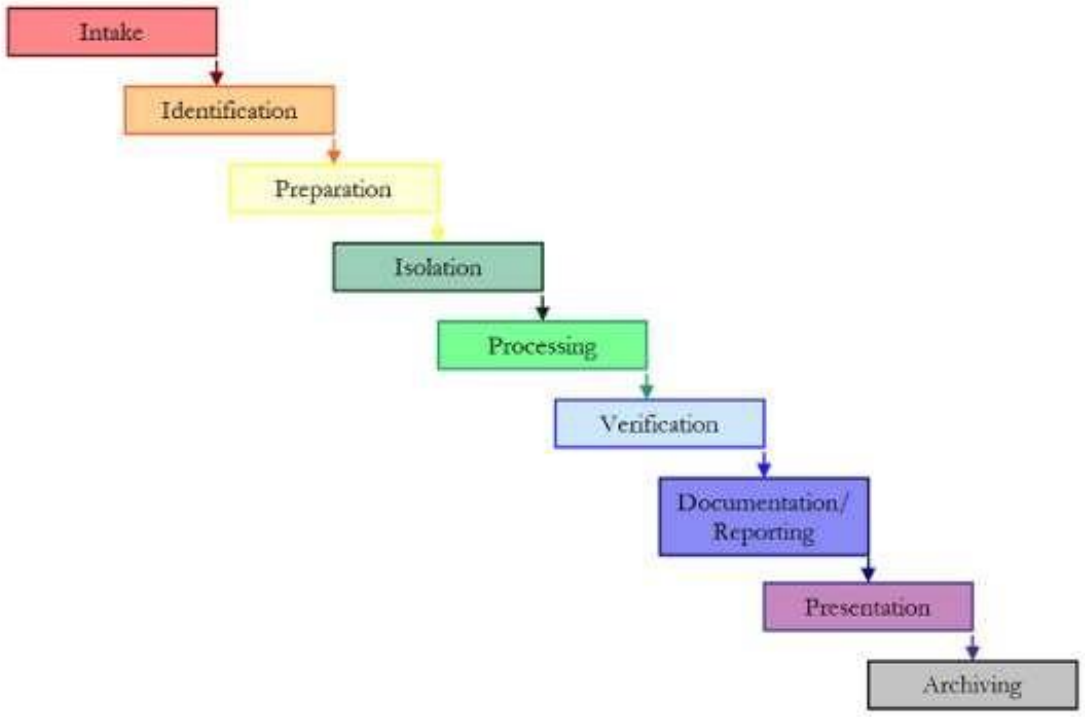
- Pencurian Kekayaan Intelektual
- Perusahaan Penipuan
- Penyalahgunaan Properti
- Perceraian & Hukum Keluarga
- Geo-Lokasi KontroversiBukti Kejahatan

f. Mobile Forensik Proses

Pendekatan Digital Forensics tidak hanya bisa diterapkan pada ranah Computer Forensics saja, pada perangkat mobile seperti telepon seluler juga bisa dilakukan dengan pendekatan ilmu Digital Forensics. Terdapat beberapa perbedaan terkait computer forensics dan mobile phone forensics namun perlu dicatat bahwa keduanya memiliki tujuan akhir yang sama yaitu bukti digital yang diperoleh, dianalisis dan diajukan dapat diterima oleh pengadilan.

Setiap organisasi atau seorang yang akan melakukan pemeriksaan terhadap barang bukti untuk kepentingan digital forensics harus mempunyai panduan kerja standard agar menjamin setiap "Pemeriksa" mengikuti alur kerja yang sama sehingga setiap prosesnya dapat terdokumentasi dan hasilnya dapat diulang dan dapat dipertahankan.

Pada dasarnya tahapan kerja alur kerja pada computer forensics tidak jauh berbeda dengan mobile phone forensics, hanya ada satu perbedaan saja yaitu pada mobile forensics terhadapa satu langkah tambahan yaitu tahap Isolasi. Berikut adalah proses pada mobile phone forensics :



Gambar 2 : Mobile Forensik Proses.

- **Intake**

Tahap awal dimana barang bukti diperoleh oleh “Pemeriksa”, terdapat formulir atauoun dokumentasi pendukung lainnya terkait dengan kepemilikan barang bukti dan data informasi-informasi pendukung tentang kasus terkait. Perlu dicatat bahwa pada tahap ini “Pemeriksa” dilarang untuk mengubah data dalam barang bukti.

- **Identification**

Kemudian tahapan Identifikasi, pada taham identikasi maka pemeriksa harus dapat mengidentifikasi beberapa hal, yaitu:

- Kewenangan Hukum untuk memeriksa perangkat (berupa surat tugas resmi dari aparat hukum)
- Tujuan Pemeriksaan
- Identifikasi mengenai perangkat, mulai dari “Pabrikan mana”, model, spesifikasi atau informasi lain terkait barang bukti yang didapat.

Pada mobile phone forensics terdapat salah satu tantangan yaitu banyaknya variant dari perangkat mobile phone tersebut, dimana setiap mobile phone mempunyai ciri dan karakteristik masing-masing. maka sudah menjadi keharusan bahwa setiap pemeriksa harus tahu tentang karakteristik barang bukti yang didapat, maka hal yang harus dilakukan adalah harus mempelajari dari buku panduan manualnya atau bisa berdiskusi dengan ahli teknisi perangkat mobile, atau bisa mencari informasi di internet. salah satu yang bisa dijadikan rujukan dapat mengunjungi situs Mobile Forensic Central

- **Preparation**

Setelah data pendukung sudah didapatkan maka dilakukanlah persiapan mulai dari metode apa yang akan dilakukan dan *tools* apa saja yang akan digunakan dalam proses *ekstraksi* dan analisis.

- **Isolation**

Proses inilah yang membedakan antara computer forensics dan mobile phone forensics, proses isolasi ini adalah proses yang penting agar perangkat mobile tidak terhubung dengan jaringan komunikasi seperti jaringan telepon seluler, bluetooth, infra merah ataupun WiFi.

Isolasi telepon mencegah penambahan data baru ke telepon melalui panggilan masuk dan pesan teks atau data-data lain yang masuk karena adanya signal internet, pengisolasian perangkat juga dimaksudkan untuk menjaga akses yang terlarang dari jarak jauh yang mungkin saja terjadi untuk kepentingan pengubahan data.

- **Processing**

Setelah proses isolasi dari jaringan komunikasi, maka tahapan selanjutnya adalah memproses barang bukti tersebut. yaitu dengan melakukan ekstraksi dari barang bukti di mana metode ekstraksi sudah ditentukan dalam tahap "Preparation". Setelah itu maka dilakukan analisa terkait temuan-temuan yang didapat dari ekstraksi tersebut.

- **Verification**

Setelah memproses barang bukti maka dilakukanlah proses verivikasi, dimana pemeriksa melakukan verivikasi keakuratan data ekstraksi yang didapatkan.

Verifikasi data yang diekstrak dapat dicapai dalam beberapa cara:

- membandingan data yang telah diekstrak dengan data dalam barang bukti yang didapat
- memeriksa *hex* dari data yang diekstraksi
- menggunakan bebrapa *tools* untuk membandingkan hasilnya
- menggunakan *hash value* untuk membandingkan hasil ekstraksi yang berupa file *image*

- **Documentation & reporting**

Proses Dokumentasi harus dilakukan dari tahap perolehan sampai pada tahapan-tahapan selanjutnya, setelah itu pelaporan harus dilakukan dengan baik, secara ringkas dan jelas agar mudah dipahami oleh pihak-pihak yang punya otoritas

- **Presentation**

Penyajian harus diberikan seluruh pemeriksaan bagaimana informasi diekstrak dan didokumentasikan dari perangkat mobile dapat dengan jelas disampaikan kepada penyidik, jaksa dan pengadilan.

- **Archiving**

Proses pengarsipan ini juga sangat penting agar seluruh data dari proses pemeriksaan baik data digital atau data dokumentasi dapat disimpan dengan baik guna menjaga data yang diperoleh pada proses-proses sebelumnya. Hal ini diperlukan untuk mempertahankan data untuk proses pengadilan yang sedang berlangsung, referensi di masa mendatang.

g. Mobile Forensik Software Tools

1. ProDiscover Forensic

ProDiscover Forensic digunakan sebagai keamanan komputer yang memungkinkan untuk menemukan semua data di disk komputer dan pada saat yang sama melindungi bukti untuk membuat laporan pembuktian kualitas untuk digunakan dalam proses hukum.

Software ini dapat memulihkan file yang telah dihapus, memeriksa ruang kendur, mengakses Windows Alternate Data Streams, dan secara dinamis memungkinkan pratinjau, pencarian, dan pengambilan gambar dari Area Lindung Perangkat Keras (HPA) dari disk yang memanfaatkan teknologi perintisnya sendiri. Tidak mungkin menyembunyikan data dari ProDiscover Forensic karena membaca disk di tingkat sektor.

2. Oxygen Forensic Suite 2013 Standard

Oxygen Forensics Suite (Edisi Standar) digunakan untuk mengumpulkan bukti dari telepon genggam. Software ini memiliki kemampuan untuk mengumpulkan Informasi Perangkat (Pabrikan, Platform OS, IMEI, Nomor Seri, dll.), Kontak, Pesan (Email, SMS, MMS, dll.) Dan pemulihan pesan yang dihapus, Log Panggilan, dan informasi Kalender

dan Tugas . Ini juga dilengkapi dengan file browser yang memungkinkan untuk mengakses dan menganalisis foto pengguna, video, dokumen dan database perangkat.

3. Volatility

Volatilitas adalah kerangka forensik memori untuk respons insiden dan analisis perangkat lunak perusak yang memungkinkan untuk mengekstrak artefak digital dari pembuangan memori yang tidak stabil (RAM). Menggunakan Volatilitas dapat mengekstrak informasi tentang menjalankan proses, soket jaringan terbuka dan koneksi jaringan, DLL dimuat untuk setiap proses, sarang registri yang di-cache, ID proses, dan banyak lagi.

h. Mobile Forensik Hardware Tools

Perangkat keras dalam komputer forensik dibagi menjadi 4 yaitu :

1. Laptop Forensik Worktations
2. Perangkat Masukan
   - Keyboard
   - Mouse
   - Trackball
   - Trackpoint
   - Trackpad – Touchpad
   - Touch screen
   - Joystick
   - Source data automation
   - Scanner
   - WebCam
   - Kartu magnetik – Smartcard
   - Biometric peripheral
3. Perangkat Keluaran
   - Monitor

        - Cathode ray tube
        - Liqid crytal display
    - Printer
        - Impact printer
        - Non impact printer
    - Plotter
    - Speaker
    - Video output – Proyektor multimedia
    - Micro Film
4. Media Peyimpanan
    - Hardisk
    - Flashdisk
5. Keperluan LAN
    - Hub
    - Switch

DAFTAR PUSTAKA

1. http://for-i.blogspot.co.id/2016/03/mobile-forensics.html
2. http://slashliciouse.blogspot.co.id/2012/10/pengertian-mobile-forensik.html
3. http://lampukamar.blogspot.co.id/2013/10/storage-pada-mobile-device.html
4. https://danarcp.wordpress.com/2017/01/28/tahapan-kerja-penanganan-barang-bukti-mobile-phone-forensik/
5. http://agustiantoraharjo.blogspot.co.id/2014/11/mobile-forensik.html
6. http://resources.infosecinstitute.com/7-best-computer-forensics-tools/#gref
7. https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/