

Computer Forensics Lab Requirements

ERI PRASETYO WIBOWO
UNIVERSITAS GUNADARMA

Pendahuluan

- Dengan meningkatnya jumlah serangan cybercrime yang melanda baik sector publik maupun swasta , kebutuhan laboratorium forensik komputer untuk menangkap dan menganalisis bukti digital dengan akurasi tinggi juga meningkat.
- Mengakreditasi lab forensik digital adalah masalah utama yang perlu dipertimbangkan, apakah perlu berencana untuk mendirikan lab internal untuk organisasi atau berpikir untuk mengalihdayakan forensic digital ke penyedia pihak ketiga.
- Akreditasi memastikan bahwa laboratorium yang layanannya ingin digunakan memenuhi standar yang ditetapkan dari badan otoritas dalam hal menggunakan metode yang dapat diandalkan, alat yang tepat (dalam hal perangkat keras dan perangkat lunak), dan personel yang kompeten untuk melaksanakan tugasnya.

Pendahuluan (lanjutan)

- Laboratorium forensik digital bisa dalam berbagai ukuran: tentu saja, anggaran memainkan peran penting dan peran saat merencanakan lab, tetapi tugas yang diharapkan (lingkup kerja) diperlukan untuk lab ini akan menjadi landasan dalam menentukan peralatan dan perangkat lunak yang dibutuhkan.
- Misalnya, perusahaan besar berinvestasi dalam menciptakan laboratorium canggih yang menangani semua jenis perangkat komputasi dan kasus forensik seperti malware, pelanggaran eksternal, jaringan, GPS, dan seluler.
- Laboratorium ini memiliki profesional terlatih dan berisi: versi terbaru dari perangkat lunak forensik di samping alat perangkat keras khusus yang berbeda.
- Tidak peduli ukuran lab forensik , yang penting harus berisi alat minimum untuk menangkap, melestarikan, menganalisis, dan menyajikan bukti digital dengan cara yang baik secara forensic.

Persyaratan Fasilitas Fisik Lab

- 1. Harus memiliki satu pintu masuk.
- 2. Lebih disukai tidak memiliki jendela di lab.
- 3. Lab harus kedap suara, artinya tidak ada yang bisa menguping percakapan yang terjadi di dalam lab. Hal ini dapat dicapai dengan menggunakan bahan kedap suara di langit-langit dan dinding, dan menggunakan karpet di lantai.
- 4. Harus memiliki sistem alarm di pintu masuk selain sistem biometrik untuk menangani akses ke lab. Akses biometric sistem harus mencatat setiap kunjungan ke lab; log ini harus tetap ada didukung selama bertahun-tahun yang akan datang untuk tujuan audit.

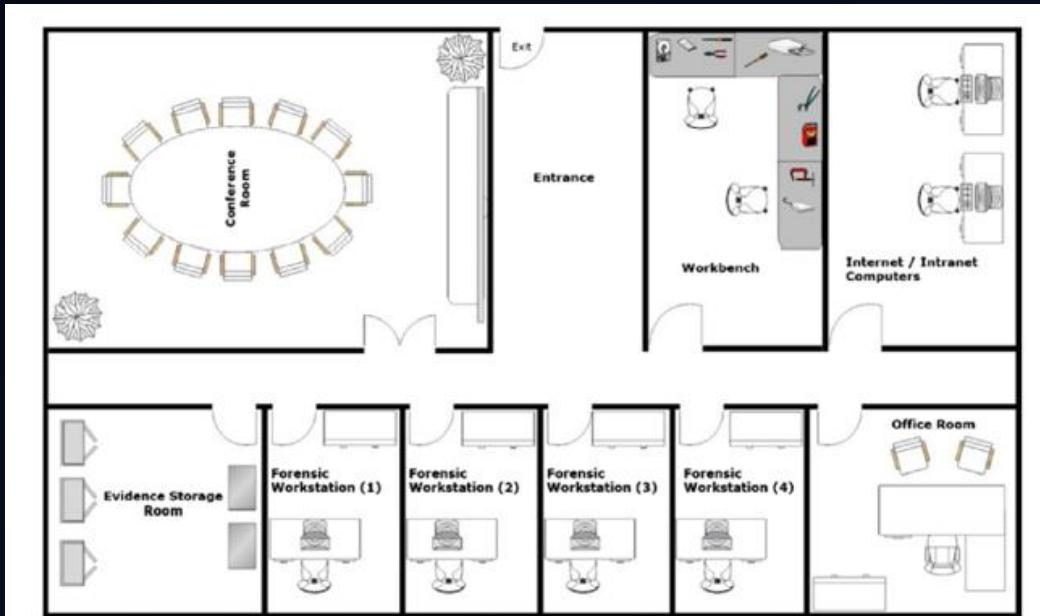
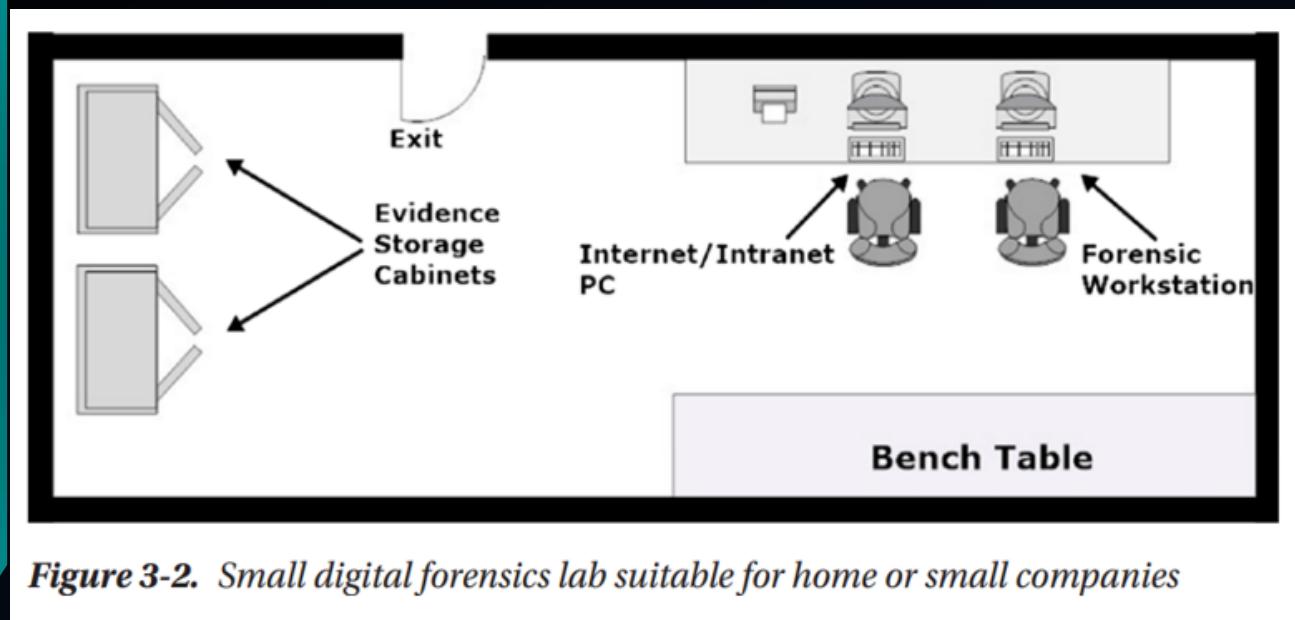


Figure 3-1. Floor plan for large digital forensic lab: license server and internal lab network equipment in addition to Internet networking devices (router, firewall, and IDS) can be placed in the Internet/intranet room

Persyaratan Fasilitas Fisik Lab



- 5. Kamera pengintai harus mencakup seluruh lab, terutama bagian pintu masuk utama dan ruang bukti digital. Perekam video dari sistem pengawasan (tempat file rekaman video disimpan) harus disimpan di ruangan yang paling aman di lab, yaitu: “ruang penyimpanan barang bukti.”
- 6. Harus memiliki sistem pencegah kebakaran.

Peralatan perangkat keras

Peralatan yang terkait dengan pekerjaan forensik digital

1. Server lisensi (ini diperlukan oleh beberapa forensik digital suite).
2. Server penyimpanan dikonfigurasi untuk hard disk standar yang dapat dilepas drive (digunakan untuk menyimpan gambar bukti digital dan data yang diproses dan diekstraksi dari gambar-gambar itu);
3. Stasiun kerja forensik (tercakup dalam bagian "Forensik" Stasiun kerja").
4. Laptop forensik portabel (digunakan di luar lab untuk menangkap bukti dan untuk melakukan beberapa analisis).
5. Komputer khusus untuk mengakses Internet/intranet.
6. Komputer administratif untuk manajemen log dan masalah lainnya.

Peralatan perangkat keras

Peralatan yang terkait dengan pekerjaan forensik digital

7. Hardware write blocker (Pemblokir writer perangkat keras). Ini adalah bagian perangkat keras yang menghubungkan media yang berisi bukti digital (seperti HDD) ke forensic stasiun kerja; tujuan perangkat ini adalah untuk mencegah modifikasi apa pun ke data pada drive bukti selama proses akuisisi.
8. Drive CD/DVD portabel.
9. Pembaca USB.
10. Penutup HDD dan SSD dengan antarmuka USB 3.0.
11. Pembaca kartu SD.
12. Hard drive eksternal dan USB thumbs (USB 2.0 dan USB 3.0) dari ukuran yang berbeda

Peralatan perangkat keras

Peralatan listrik kantor

1. Catu daya tak terputus (UPS) untuk setiap workstation/server dan perangkat jaringan.
2. Perangkat proyeksi (di ruang konferensi).
3. Pencetak.
4. Pemindai.
5. Mesin fotokopi.
6. Penghancur kertas.
7. Kamera digital, termasuk kamera video, dan aksesori.
8. Telepon (lebih disukai nirkabel).
9. Akses point Wi-Fi.
10. Headset.
11. Catu daya simetris.

Peralatan perangkat keras

Perangkat jaringan

1. Perangkat Router dan switch untuk menghubungkan workstation forensik dengan server penyimpanan di dalam lab.
2. jaringan internet; harus dipisahkan dari internal lab jaringan. Memerlukan firewall, Switch , dan router (ketiga komponen dapat digabungkan dalam satu perangkat).
3. Kabel jaringan

Backup Data

- Kumpulan media penyimpanan yang berisi bukti digital asli (seperti HDD, SSD, flash drive, kartu SD, smartphone, tablet, CD/DVD) harus disimpan di tempat terkunci yang aman ruangan dalam lemari tertutup yang aman. Lemari di ruang penyimpanan barang bukti harus bisa melindungi dari kebakaran dan banjir, dan harus bertahan jika lab runtuh akibat gempa bumi; Filling cabinet juga harus melindungi isinya dari gangguan elektromagnetik untuk menghindari kerusakan peralatan yang disita.
- Seluruh ruangan harus diamankan dari akses umum menggunakan metode keamanan yang tepat yang dapat direkam secara otomatis, seperti kunci digital dan akses kartu kunci. Ruang bukti harus berisi log yang harus ditandatangani oleh setiap orang yang mengunjungi ruangan dan merinci tujuan kunjungan dan tanggal/waktunya saat kunjungan berlangsung. Ini bisa membantu untuk menjaga rantai keaslian barang bukti yang disita.

Forensik Workstation

- Versi terbaru dari OS Windows (versi 64-bit) direkomendasikan untuk forensic stasiun kerja. Edisi Windows 10, 11 berikut direkomendasikan karena:
 - dukungan untuk perangkat keras kelas atas dan tugas komputasi intensif:
 - • Pro for Workstation—sangat direkomendasikan.
 - • Windows 10 .
- Kedua edisi mendukung hingga 6 TB RAM dan empat prosesor;
- Sekarang, mari kita bahas perangkat keras yang dibutuhkan untuk workstation forensik. Jelas, Ketika bekerja dengan bukti digital, komputer yang kuat diperlukan untuk memproses dan mencari dalam file gambar.
- Komputer forensik membutuhkan tingkat kekuatan pemrosesan yang tinggi dan jumlah memoriRAM; mereka juga membutuhkan banyak penyimpanan dan banyak slot ekspansi untuk pasang berbagai jenis perangkat.
- Membangun stasiun kerja forensik itu mahal; namun, itu masih dianggap sebagai solusi hemat biaya untuk perusahaan kecil dibandingkan dengan pembelian workstation forensik komputer siap pakai, yang harganya jauh lebih mahal.

Berikut ini adalah spesifikasi perangkat keras yang direkomendasikan saat membangun perangkat dasar workstation forensik dari bawah ke atas:

1. Memori RAM: Setidaknya 24 GB (DDR4). Lebih bagus!
2. CPU: Setidaknya dua CPU fisik (prosesor Intel i9 generasi ke-8 memiliki 10 core dan 20 thread) untuk setiap workstation.
3. Motherboard: Yang dapat menampung jumlah yang dibutuhkan prosesor dan jumlah RAM, bersama dengan pengontrol video kartu
4. Hard drive: Kombinasi SSD dan HDD—minimal 512 GB SSD dan HDD 4TB.
5. Pengontrol video: Nvidia Geforce, disarankan versi terbaru dengan setidaknya 8 GB memori GDDR5X.
6. Pembakar tiga kali lipat (Blu-ray, DVD, CD).
7. Penutup hard drive eksternal dengan antarmuka USB 3.0.

Berikut ini adalah spesifikasi perangkat keras yang direkomendasikan saat membangun perangkat dasar workstation forensik dari bawah ke atas:

8. Write protection: Anda dapat membeli bagian ini satu per satu atau Anda sendiri dapat membeli satu yang dapat diintegrasikan ke dalam workstation Anda.
perangkat keras write protector harus mendukung akuisisi data dari SATA, SAS, IDE, USB, FireWire, dan penyimpanan PCIe perangkat.
9. Sistem pendingin canggih: Lebih disukai menggunakan pendingin CPU cair sistem dengan—setidaknya—kipas ganda.
10. Panel LCD dengan resolusi tinggi (layar IPS full HD), minimal 22 inci untuk tampilan yang lebih baik.
11. Port
 - Port USB 3.0
 - Thunderbolt 3
 - Soket mikrofon dan headphone.
 - Pengontrol LAN terintegrasi untuk mengakses Lab. jaringan.

Perangkat Lunak Forensik

- Jenis perangkat lunak forensik yang dibutuhkan untuk lab akan bergantung pada ruang lingkup pekerjaan ; untuk misalnya, jenis sistem operasi (Windows, Linux, atau Mac) dan sistem file akan menentukan alat forensik yang Anda butuhkan.
- Forensik computer suite paling populer dibuat untuk OS Windows; Open source counterpart terutama diarahkan ke Linux dengan beberapa yang juga porting ke Windows OS.

Free and Open Source Forensic Tools

- Ada banyak alat forensik digital open source code dan gratis; beberapa datang dengan fitur kaya yang mirip dengan software komersial, sementara sebagian besar adalah small tools yang dibuat untuk melakukan fungsi tertentu (misalnya, mengambil riwayat browser atau mengekstrak informasi header email).
 - Daftar alat forensik digital gratis dan open source yang paling populer.
1. The Sleuth Kit (www.sleuthkit.org)
 2. Autopsy: A graphical interface to The Sleuth Kit and other digital forensics tools (www.sleuthkit.org/autopsy).
 3. dd for Windows (www.chrysocome.net/dd): A forensic imaging tool for Windows systems.
 4. Magnet RAM Capture: Capture RAM memory (www.magnetforensics.com/free-tool-magnet-ram-capture).
 5. Belkasoft Live RAM Capturer (<https://belkasoft.com/ramcapturer>).
 6. Volatility: Analyzes RAM (volatile memory) images (www.volatilityfoundation.org).
 7. Memoryze: Captures and analyzes memory images and on live systems (www.fireeye.com/services/freeware/memoryze.html)
 8. Mandiant Redline: Live memory analysis; includes Memoryze tool within it (www.fireeye.com/services/freeware/redline.html)
 9. Bulk Extractor: Scan an acquired hard drive digital image and extract useful information from it such as e-mail addresses, credit card numbers
 10. Encrypted Disk Detector: Check for encrypted volumes on a computer system during incident response (www.magnetforensics.com/free-tool-encrypted-disk-detector)

Teknologi Virtualisasi

- Teknologi virtualisasi memungkinkan pemeriksa menginstal lebih dari satu sistem operasi di stasiun kerja yang sama; ini terbukti berguna saat melakukan analisis malware (untuk menghindari menginfeksi workstation forensik) atau saat menguji alat forensik sebelum menggunakan secara resmi.
- Mesin virtual akan berjalan di Sandbox yang diisolasi sepenuhnya dari sistem operasi mesin host.
- Mesin virtual populer termasuk VirtualBox (www.virtualbox.org) dan Vmware Workstation Player (www.vmware.com/products/player/ playerpro-evaluasi.html).

Sistem Manajemen Informasi Laboratorium (LIMS)

- Sistem manajemen konten diperlukan di lab untuk mengatur penerimaan, pelacakan, penanganan, dan pengembalian barang bukti di laboratorium forensik digital. Anda dapat menggunakan open sistem manajemen konten sumber untuk tugas ini: Drupal (www.drupal.org/home) dan Moodle (<https://moodle.org>)

Validasi dan Verifikasi Perangkat Keras Forensik dan Perangkat Lunak

- Merupakan tanggung jawab laboratorium forensik digital untuk menentukan apakah suatu teknik, metode, atau perangkat keras atau perangkat lunak baru yang cocok untuk digunakan selama proses investigasi.
- Perangkat lunak/perangkat keras forensik dianggap valid untuk digunakan selama uji coba resmi dan jika telah digunakan sebelumnya oleh laboratorium ilmiah terkemuka, lembaga penegak hukum, lembaga pendidikan/ perguruan tinggi, atau sejenisnya.
- jika alat atau metodologi tertentu adalah baru dan tidak disetujui/digunakan sebelumnya oleh badan tersebut, menjadi tanggung jawab lab untuk mengujinya, memvalidasi hasilnya, dan akhirnya mendokumentasikan temuan sebelum menggunakan sebagai bukti pengujian.
- Prosedur khusus harus ada untuk melakukan validasi internal dan verifikasi alat dan metodologi baru (termasuk alat yang dikembangkan sendiri dan metode); setiap lab memiliki aturannya sendiri untuk melakukan proses ini

Manajer Lab

- Laboratorium forensik digital harus memiliki seorang manajer (juga dikenal sebagai supervisor teknis) untuk memastikan kelancaran pekerjaan di lab forensik digital dan bahwa pekerjaan yang dilakukan memenuhi standar kualitas yang telah ditetapkan. Berikut ini adalah tugas utama manajer lab:
 1. Menyarankan proses kerja untuk mengelola kasus.
 2. Mendukung kasus analisis forensik paling kompleks yang ditangani oleh laboratorium.
 3. Pastikan bahwa staf lab dilatih sesuai dengan yang diterapkan baku mutu.
 4. Melakukan pengecekan tahunan terhadap kinerja personel lab.
 5. Mendukung pengembangan teknis staf forensik digital junior.
 6. Menegakkan standar etika di antara staf lab.
 7. Membuat, memantau, dan menegakkan kebijakan dan prosedur lab untuk staf.
 8. Mengawasi pemeliharaan fasilitas.
 9. Mengawasi kesaksian pengadilan sebelum menghadirkannya secara resmi.
 10. Periksa perangkat lunak dan peralatan perangkat keras lab dan pastikan bahwa: semuanya berfungsi dengan baik.
 11. Pengadaan kebutuhan bahan habis pakai lab.
 12. Menyetujui studi validasi yang dilakukan pada alat forensik yang berbeda (baik perangkat keras dan perangkat lunak) dan memberikan persetujuan akhir untuk menggunakan di laboratorium

Pencadangan Data Lab

- Mencadangkan adalah cara untuk melindungi data sensitif saat terjadi kegagalan pada perangkat komputasi.
- Sangat penting untuk memiliki setidaknya tiga salinan data (satu di luar lokasi dan satu di lab) di lokasi yang aman, dan ini harus dilindungi dengan kata sandi yang kuat sehingga dapat mengambil data penting jika terjadi kegagalan sistem, serangan virus, atau bencana alam.
- Cadangan harus mencakup data di workstation forensik dan di server penyimpanan utama
- Windows menawarkan fitur pencadangan gratis (cocok untuk workstation forensik) yang dapat diakses dari Control Panel Backup and Restore (Windows 7).
- Utilitas ini akan memungkinkan Anda untuk membuat cadangan drive Windows ke drive eksternal. Fiturnya tersedia di Windows 7, 8, dan 10. Namun, Windows versi 8 dan 10 memiliki cadangan lain utilitas yang disebut Riwayat File, yang juga dapat dikonfigurasi untuk mencadangkan pribadi/pekerjaan file ke drive eksternal atau lokasi jaringan

Persyaratan Pelatihan

- Staf laboratorium harus memiliki pelatihan yang memadai untuk melakukan pekerjaan mereka.
 - Bidang forensik digital membutuhkan pembelajaran, penelitian, dan berkomunikasi dengan orang lain di lapangan.
 - Sebagai profesional forensik digital, harus memiliki pemahaman umum tentang teknologi terbaru.

Berikut ini adalah minimum persyaratan pelatihan untuk staf lab:

1. Perangkat keras komputer
2. Dasar-dasar jaringan
3. Pengetahuan forensik komputer umum (buku ini cukup untuk tugas ini!)
4. Pelatihan khusus perangkat lunak forensik (mis., FTK, EnCase)
5. Pelatihan hukum yang mencakup undang-undang kejahatan digital yang dilaksanakan di negara yang berbeda, surat perintah penggeledahan, bersaksi di pengadilan, dan menentukan hukum yurisdiksi yang efektif ketika menyelidiki suatu kasus.

Kebijakan dan Prosedur Lab

- Kebijakan dan prosedur lab menentukan aturan internal yang harus diikuti oleh pekerja lab selama bekerja di laboratorium.
- Kebijakan lab mencakup aturan untuk pekerjaan berikut:
 1. Kebijakan keamanan fisik lab (misalnya, tindakan keamanan yang perlu: diikuti untuk mengakses area lab).
 2. Mengakses kebijakan area terlarang teratas: Siapa yang berwenang mengakses ruang penyimpanan barang bukti?
 3. Menangani bukti digital (misalnya, pemblokir tulis harus dilampirkan ke hard drive tersangka saat memperolehnya).
 4. Barang bukti disita di TKP.
 5. Analisis bukti (misalnya, langkah-langkah dan alat untuk menangani setiap bagian dari bukti).
 6. Bukti lacak (misalnya, mendokumentasikan siapa yang telah mengakses bukti digital sejak kedatangannya ke lab, dan juga kapan dan mengapa).
 7. Disposisi bukti (misalnya, seberapa sensitif bahan seharusnya dibuang dengan aman: penghancur kertas untuk arsip kertas, pemusnahan peralatan untuk secara aman menghancurkan hard drive [secara fisik] dan lainnya media penyimpanan).
 8. Penulisan laporan forensik digital (misalnya, tata letak standar untuk melaporkan hasil analisis kasus).
 9. Evaluasi kesaksian ahli.
 10. Kebijakan pencadangan.
 11. Kebijakan pelatihan.
 12. Standar kualitas

Dokumentasi

- Mematuhi kebijakan dan prosedur yang disebutkan di bagian sebelumnya adalah penting untuk pekerjaan yang lancar dan akurat di lab forensik digital.
- Setiap bagian dari pekerjaan selama proses investigasi perlu dilengkapi dengan formulir kertas/elektronik, dan catatan pemeriksa juga sangat penting dan perlu didokumentasikan secara rinci selama proses investigasi.
- Ini memungkinkan pemeriksa lain untuk terus mengerjakan kasus yang ditentukan dan memungkinkan staf lab untuk mengulangi prosesnya lagi untuk memastikan bahwa hasil yang sama persis dihasilkan setiap saat.
- Dokumentasi merupakan bagian integral dari investigasi forensik digital; itu dimulai di lapangan sebelum mendapatkan perangkat komputasi yang disita dan berlanjut di lab sampai mencapai kesaksian.
- Proses litigasi di pengadilan dapat berlangsung selama berbulan-bulan dan bertahun-tahun, dan tanpa dokumentasi ini, seorang pemeriksa—yang mungkin diminta untuk bersaksi di pengadilan—dapat melupakan fakta-fakta kunci dari penyelidikan kasusnya, dan ini dapat mengakibatkan melemahnya kesaksian hakim dan juri.

Persyaratan Akreditasi Lab

- Akreditasi memastikan bahwa lab forensik digital mengikuti serangkaian yang diakui standar yang ditetapkan oleh badan otoritatif.
- Badan terakreditasi akan memeriksa lab untuk melihat apakah itu menggunakan metode investigasi yang andal, perangkat keras, dan perangkat lunak yang diterima pengadilan, dan personel terlatih, dan jika tata letak fisik lab Anda memenuhi standar yang ditetapkan.
- Akreditasi sangat penting untuk setiap laboratorium forensik digital, dan kami akan membahas secara singkat langkah-langkah yang diperlukan bagi setiap organisasi untuk memulai proses akreditasi.
- Ada lima langkah dalam proses akreditasi :

Step 1: Self-Assessment

Step 2: Identifying the Current Level of Conformance to the Target Accreditation Standards

Step 3: Closing the Gap

Step 4: Implementation

Step 5: Conformance to Standards Documentation

Essential Technical Concepts

ERI PRASETYO WIBOWO

UNIVERSITAS GUNADARMA

Apa yang seharusnya sudah Anda ketahui sebelum memulai penyelidikan

- ❑ Melakukan investigasi forensik digital membutuhkan pemahaman menyeluruh tentang beberapa hal dari konsep utama teknik komputasi.
- ❑ Mengetahui bagaimana data disimpan di komputer, teori bilangan, bagaimana file digital terstruktur, dan jenis unit penyimpanan dan perbedaan di antara area penting untuk mengetahui bagaimana menemukan dan menangani bukti digital.

Representasi data

- ❑ Kerja komputer menyimpan, memproses, dan mewakili data digital dengan cara tertentu.

Desimal (Base-10)

- ❑ Desimal adalah sistem penomoran yang paling banyak digunakan yang kita gunakan setiap hari ketika melakukan perhitungan matematika (misalnya, $10 + 11 = 21$); itu disebut sebagai sistem basis-10 karena menggunakan 10 digit atau simbol (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) untuk mewakili nilainya.

- ❑ Dalam desimal, posisi angka memberi arti pada nilai yang diwakilinya, di mana setiap digit dikalikan dengan pangkat 10 yang terkait dengan posisi digit tersebut.

- ❑ Misalnya, perhatikan angka desimal 5437. Angka ini ditafsirkan sebagai berikut:

$$5437 = 5000 + 400 + 30 + 7$$

Atau lebih tepatnya: $5437 = 5 \times 10^3 + 4 \times 10^2 + 3 \times 10^1 + 7 \times 10^0$

- ❑ Pemahaman tentang sistem penomoran desimal sangat penting, seperti yang lainnya system penomoran mengikuti aturan yang sama.

Representasi data

Biner (Base-2)

- Komputer menyimpan data dalam format biner, yang merupakan sistem angka basis-2 yang diwakili dengan 1 dan 0.
- Biner, bahasa komputer, mengikuti aturan yang sama dengan desimal. Namun, tidak seperti desimal, yang memiliki 10 simbol dan dikalikan dengan pangkat 10, biner memiliki dua simbol (0 dan 1) dan dikalikan dengan modulus dua.
- Di komputer, masing-masing 1 ATAU 0 disebut bit (atau biner digit); jumlah delapan bit adalah disebut byte.
- . Bit orde tertinggi terletak di bit paling kiri dan memiliki bit tertinggi nilai; bit ini disebut Most Significant Bit (MSB).
- Di sisi yang berlawanan, bit terendah nilai terletak di bit paling kanan dan disebut Least Significant Bit (LSB).

Representasi data

Hexadesimal (Base-16)

- Juga dikenal sebagai Hex, sistem penomoran ini menggunakan 16 digit atau simbol untuk mewakilinya nilai-nilai.
- berisi angka dan huruf berikut: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F (huruf besar digunakan untuk menyatakan angka dari 10 sampai 15).
- Anda akan sering menemukan nomor Hex saat bekerja dengan komputer dan lainnya sistem digital, terutama ketika menyelidiki lokasi alamat memori.
- Motif utama di balik skema penomoran ini adalah untuk mewakili nilai biner yang panjang dalam bentuk urutan yang kompak yang mudah dibaca oleh manusia. dengan mengelompokkan setiap bit (biner angka) dalam satu grup.
- Contoh: 1100 1100 1101 0101 akan lebih mudah dibaca dan dimengerti dari 1100110011010101
- Jelas, Hex lebih pendek dan lebih mudah dipahami oleh manusia. Dalam Hex, nilai tempat ditentukan dengan pangkat 16, bukan 10. Misalnya, untuk mengonversi dari Hex ke desimal:
 - $19A_{16} = (1 \times 16^3) + (9 \times 16^2) + (10 \times 16^1) + (0 \times 16^0) = 256 + 144 + 10 = 410_{10}$

Table 2-3. Hex, Binary, and Decimal Equivalents

| Decimal | Hexadecimal | Binary |
|---------|-------------|--------|
| 0 | 0 | 0000 |
| 1 | 1 | 0001 |
| 2 | 2 | 0010 |
| 3 | 3 | 0011 |
| 4 | 4 | 0100 |
| 5 | 5 | 0101 |
| 6 | 6 | 0110 |
| 7 | 7 | 0111 |
| 8 | 8 | 1000 |
| 9 | 9 | 1001 |
| 10 | A | 1010 |
| 11 | B | 1011 |
| 12 | C | 1100 |
| 13 | D | 1101 |
| 14 | E | 1110 |
| 15 | F | 1111 |

Skema Pengkodean Karakter Komputer

- Seperti yang sudah kami katakan, semua yang ada di komputer diwakili oleh 0 atau 1, tetapi mungkin Anda bertanya-tanya bagaimana 1 atau 0 akhirnya akan berakhir di layar komputer kita sebagai huruf seperti A, B, M, C, V, dan seterusnya.
- Komputer menggunakan skema pengkodean karakter untuk mengubah bilangan biner menjadi teks bermakna yang dapat dibaca manusia (misalnya, teks yang Anda lihat saat membaca buku ini di perangkat komputasi Anda). Ada dua skema pengkodean utama yang digunakan oleh komputer untuk mewakili teks:
- ASCII (*American Standard Code for Information Interchange*) telah ditemukan sejak lama dan masih didukung di hampir semua editor teks.
- ASCII hanya memiliki kemampuan terbatas untuk mewakili semua huruf dari semua bahasa di seluruh dunia, serta tanda baca dan simbol khusus lainnya dari bahasa lain, karena hanya menggunakan tujuh bit atau 128 nilai.
- The ASCII code table can be found at <https://ascii.cl>.

Skema Pengkodean Karakter Komputer

Unicode encoding

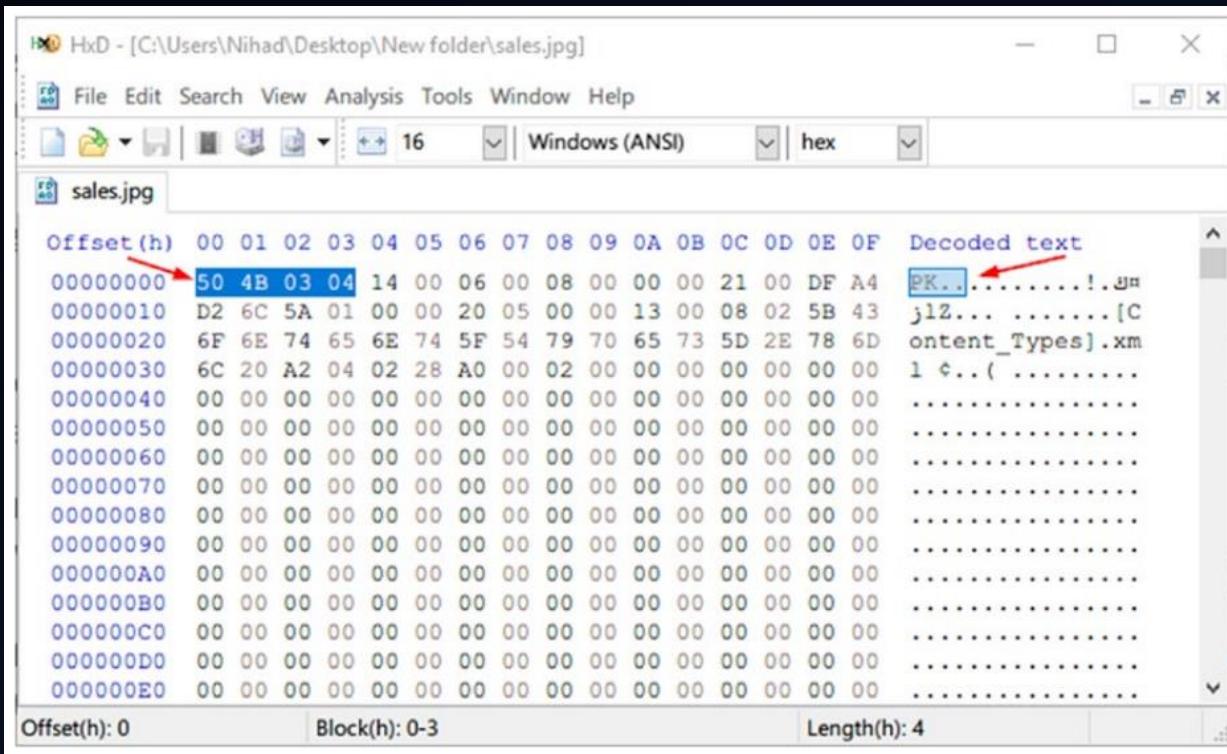
- dibuat oleh Konsorsium Unicode (<https://unicode.org>), adalah skema pengkodean karakter yang banyak digunakan yang memberikan nomor unik untuk setiap karakter dari bahasa internasional apa pun.
- Unicode didukung di sistem operasi utama, paket perangkat lunak, perangkat seluler, dan aplikasi web. Unicode sering didefinisikan sebagai UTF-8, UTF-16, UTF-32, atau UCS-2
- Memahami bagaimana komputer menyimpan dan merepresentasikan data sangat penting dalam forensik digital; misalnya, penyidik mungkin perlu mengekstrak dan membuka file dari ruang disk yang tidak terisi dari hard drive target atau dari kumpulan data mentah tanpa menggunakan program (mis., MS Word) yang awalnya membuat file ini.
- Teknik ini disebut file Carving , dan digunakan secara efektif untuk memulihkan file dan fragmen file yang terhapus dari hard drive yang dihapus atau rusak.

Struktur File

- File digital terdiri dari urutan bit: setiap jenis file memiliki skema pengkodean tertentu yang menjelaskan bagaimana informasi disimpan dalam file ini.
- Skema ini disebut "format file." Format file dapat berupa gratis (seperti Portable Network Graphics [PNG], yang merupakan format gambar raster yang distandarisasi oleh ISO/IEC) atau eksklusif (seperti format file Windows Media Audio [WMA]).
- Beberapa format file memiliki kemampuan untuk menyimpan lebih dari satu jenis konten; hal ini terjadi pada banyak format populer yang menyimpan konten multimedia. Misalnya, format Ogg dapat menyimpan video, audio, teks, dan metadata dalam satu wadah. AVI, WAV, dan 3GP juga termasuk dalam kategori ini.
- Sebagai pengguna, kami membedakan jenis file dari ekstensinya. Misalnya, file MS Word memiliki ekstensi DOCX atau DOC, dan MS Excel memiliki ekstensi XLSX atau XLS. Namun, sebagai penyelidik forensik digital, kami tidak dapat bergantung pada ekstensi file saja untuk menentukan jenis file, karena ini dapat dengan mudah diubah menjadi apa pun yang Anda inginkan (mis., File MS Word dapat diubah menjadi file DLL atau PNG untuk menyembunyikan identitas aslinya).
- Untuk mengatasi teknik penyembunyian tersebut, kita harus memeriksa file signature (header) untuk mengetahui jenisnya.

Struktur File

- Sebagian besar file digital memiliki tanda tangan yang terletak di 20 byte pertama ; Anda dapat memeriksa tanda tangan ini dengan membuka file subjek menggunakan Windows Notepad atau editor teks lainnya seperti Notepad++.
- Misalnya, kami memiliki file bernama sales.docx; kita dapat ubah ekstensinya ke JPG lalu buka file JPG menggunakan editor Hex (editor HxD, yang dapat Anda unduh dari www.mh-nexus.de) dan selidiki 20 byte pertamanya.

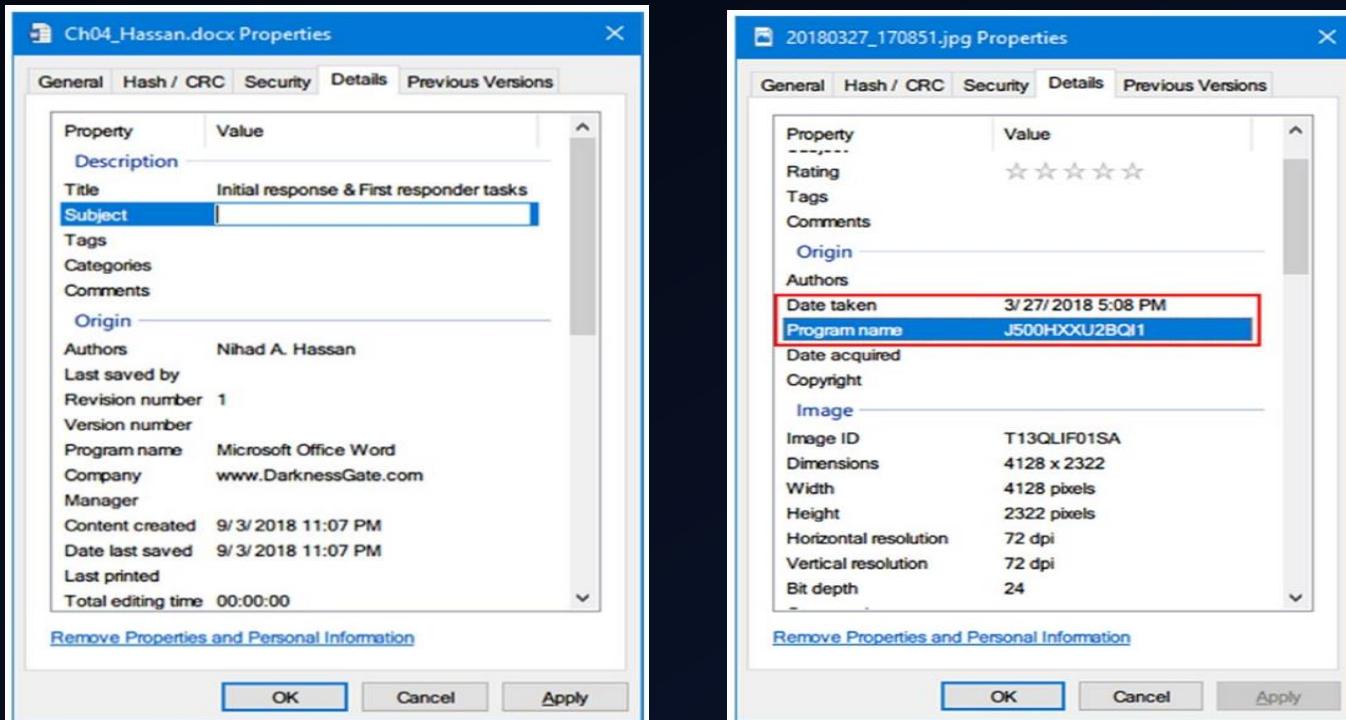


Digital File Metadata

- Metadata adalah data tentang data. Sebagian besar jenis file digital memiliki metadata yang terkait dengannya. Biasanya terintegrasi ke dalam file yang sama; namun, beberapa jenis file menyimpan metadatanya dalam file terpisah.
- Metadata menyimpan data yang menjelaskan file yang terkait dengannya.
- Misalnya, beberapa metadata yang disertakan dalam file MS Word mungkin menyertakan nama penulis, nama organisasi, nama komputer, tanggal/waktu dibuat, dan komentar.
- Dari perspektif forensik digital, metadata bisa sangat berguna dalam banyak kasus.
- Misalnya, kami dapat melacak penulis file yang berbeda (mis., File MS Office) melalui metadata terkait.
- Kami juga dapat mencari di dalam metadata file untuk menemukan informasi yang menarik (sistem operasi utama sudah mendukung pencarian dalam informasi file metadata), dan sebagian besar forensik komputer mendukung pencarian dalam metadata file gambar forensik yang diperoleh.

Digital File Metadata

- ❑ Kami dapat mengedit metadata dari banyak jenis file digital tanpa menggunakan alat pihak ketiga apa pun di bawah OS Windows.
- ❑ Misalnya, kita dapat mengedit info metadata file MS Office hanya dengan mengklik tombol kanan file Properties, yang akan membuat jendela Properties file muncul
- ❑ Metadata file gambar menyimpan informasi forensik penting seperti stempel waktu saat foto diambil dan koordinat GPS tempat pengambilannya (jika diaktifkan di perangkat penangkap).



Hash Analysis

- Hashing adalah konsep penting dalam bidang forensik digital; sebenarnya, harus menghitung nilai hash bukti digital (apakah itu gambar hard disk atau file tunggal) yang Anda peroleh selama penyelidikan untuk membuktikan bahwa data yang diperoleh (yaitu, bukti digital) belum dirusak.
- Hash bekerja dengan menerapkan fungsi hash untuk mengubah file digital (input) menjadi nilai string tetap (output); nilai hash yang dihasilkan unik dan tidak dapat dihasilkan lagi menggunakan file atau bagian data lain.
- Anda dapat menemukan nilai hashing dari file digital apa pun atau setiap bagian data dengan menggunakan alat generator hash.
- Algoritma hash kriptografi yang paling terkenal adalah MD5 dan SHA-256.
- Dalam investigasi forensik digital, hashing (juga dikenal sebagai sidik jari digital) digunakan dua kali: pertama kali untuk memverifikasi citra forensik yang diperoleh sebelum analisis dimulai (untuk membuat salinan duplikat dari citra forensik yang diperoleh) dan yang kedua di akhir pemeriksaan untuk memverifikasi integritas data dan pemrosesan forensik selama penyelidikan.

How to Calculate File Hash

- Semua forensik digital menawarkan kemampuan hashing; namun, dapat menggunakan alat third party atau cukup menggunakan alat hashing yang ada sebagai fitur bawaan di OS Windows

Method One: Using a Third-Party Tool

- Febooti Hash dan CRC (www.febooti.com).
- Instal alat ini di PC Windows Anda, klik kanan pada file yang hashnya Anda inginkan hitung, pilih Properties, dan buka tab Hash/CRC.
- HashMyFile dari www.nirsoft.net/utils/hash_my_files.html.
- Ini adalah alat portabel yang menunjukkan nilai hash dari folder/file yang dipilih menggunakan algoritma hashing yang berbeda (misalnya, md5, SHA 256).

Method Two: Using the Built-In Windows Hashing Feature

- Untuk melakukan ini, buka menu Start Windows dan pilih Windows PowerShell. Jalankan perintah di



A screenshot of a Windows PowerShell window. The command `Get-FileHash C:\Hassan_9781484227985_Online.pdf` is being run. A red arrow points to the file path in the command line. The output table shows the algorithm (SHA256) and the resulting hash value (0AAC4993E3886127252A649CC0189DAFC279F232C38B959C6D5A518480B9927F). The file path is also displayed in the output table.

| Algorithm | Hash |
|-----------|------------------------------------------------------------------|
| SHA256 | 0AAC4993E3886127252A649CC0189DAFC279F232C38B959C6D5A518480B9927F |

Memory Types

- Di komputer, memori mengacu pada bagian perangkat keras yang bertanggung jawab untuk menyimpan informasi untuk penggunaan segera atau nanti.
- Kita dapat membedakan antara dua jenis utama menurut berapa lama informasi tetap tersimpan di dalamnya

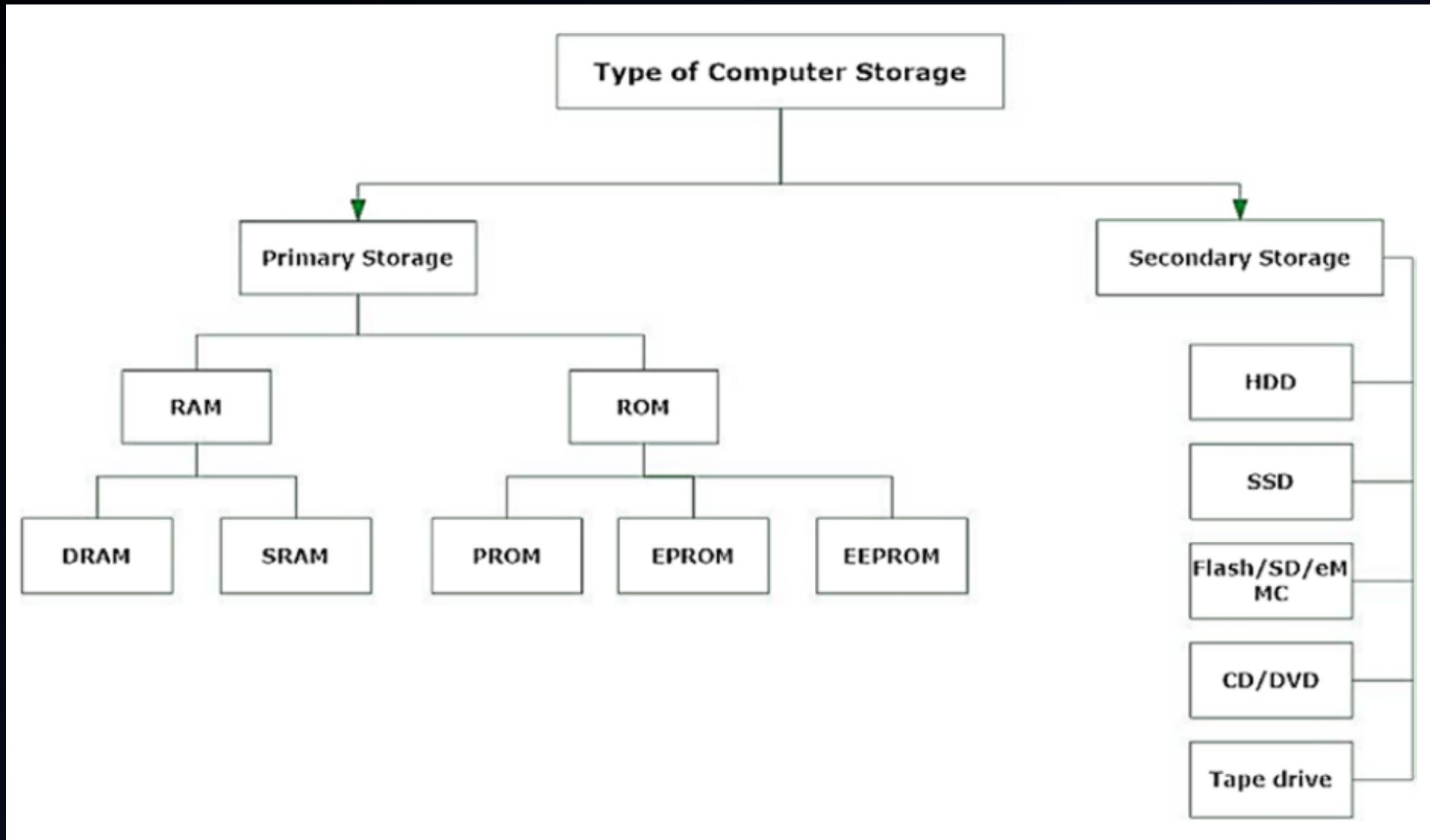
Volatile Memory

- Memori yang menyimpan informasi untuk waktu yang singkat; membutuhkan daya untuk menyimpan data, tetapi ketika daya dimatikan, ia kehilangan informasinya dengan cepat. Contoh dari memori volatil adalah RAM.

Nonvolatile Memory

- Memori nonvolatile dapat menyimpan data untuk waktu yang lama, bahkan setelah daya dimatikan. Biasanya digunakan untuk penyimpanan persisten jangka panjang. Contoh memori tersebut adalah hard drive komputer, memori flash, dan ROM (read-only memory).

Types of Computer Storage



Primary Storage

- Juga dikenal sebagai penyimpanan utama dan penyimpanan sistem, jenis ini memiliki memori yang mudah kehilangan data yang disimpan saat daya dimatikan.
- Penyimpanan primer digunakan untuk menyimpan data dan program untuk penggunaan sementara, memiliki kapasitas penyimpanan yang terbatas dan operasi baca/tulis yang lebih cepat dibandingkan dengan penyimpanan sekunder, dan dianggap lebih mahal.
- Memori penyimpanan utama utama yang ditemukan di komputer adalah RAM dan cache (memori CPU).

RAM

- Ini adalah komponen terpenting dari perangkat komputasi apa pun: ini adalah memori yang mudah hilang dengan kecepatan tinggi dibandingkan dengan media penyimpanan sekunder yang digunakan terutama untuk menyimpan semua informasi yang perlu diproses komputer.
- Misalnya, ketika meluncurkan browser web, itu akan dimuat ke dalam memori RAM.
- Dari perspektif forensik digital, banyak informasi dapat ditemukan di RAM seperti program yang dapat dieksekusi, sesi jaringan, riwayat penelusuran web, obrolan IM, kata sandi, foto, file yang didekripsi, dan sebagainya.
- Menangkap gambar RAM menjadi wajib di semua investigasi forensik digital yang mencakup komputer yang sedang berjalan.

Types of RAM:

1. DRAM (RAM dinamis). Istilah "dinamis" mengacu pada fakta bahwa memori ini harus terus-menerus disegarkan (ribuan kali per detik) untuk mempertahankan isinya.
 - ✓ DRAM adalah memori utama yang biasanya kita lihat terpasang di PC, workstation, server, dan smartphone.
 - ✓ Variasi DRAM adalah SDRAM (synchronous DRAM), nama generik yang menggambarkan berbagai jenis DRAM (DDR2, DDR3, DDR4, di mana DDR adalah singkatan dari Double Data Rate) karena mereka disinkronkan dengan kecepatan clock mikroprosesor.
2. SRAM (RAM statis).
 - ✓ Ini biasanya digunakan dalam memori CPU (CPU, cache); itu sangat cepat (lebih dari DRAM) karena tidak perlu untuk disegarkan terus-menerus seperti DRAM (maka istilah "statis").
 - ✓ SRAM sangat mahal dan menggunakan lebih banyak daya dibandingkan dengan DRAM

ROM

- Sesuai namanya, memori ini digunakan untuk melakukan operasi baca saja; itu tidak memiliki akses tulis apa pun.
- Memori ini tidak mudah hilang, karena menyimpan informasi di dalamnya, terlepas dari apakah ada daya atau tidak.
- Jenis memori ini digunakan di komputer dan di banyak perangkat digital lainnya untuk menyimpan program firmware (perangkat lunak yang disimpan di perangkat keras seperti motherboard komputer dan kartu grafis yang memberikan instruksi tentang bagaimana perangkat itu harus beroperasi).
- Memodifikasi data dalam ROM sangat sulit dan membutuhkan program khusus untuk mengaksesnya.

There are three types of ROM:

1. Programmable ROM (PROM)
2. Erasable programmable ROM (EPROM)
3. Electrically erasable programmable ROM (EEPROM)

Secondary Storage

- Penyimpanan sekunder juga dikenal sebagai memori eksternal atau memori tambahan.
- Ini adalah memori nonvolatile yang mempertahankan isinya, apakah ada daya atau tidak. Ini digunakan untuk penyimpanan data jangka panjang.
- Dibandingkan dengan penyimpanan primer seperti RAM, penyimpanan sekunder memiliki kecepatan rendah, tetapi biayanya jauh lebih murah daripada penyimpanan utama.

HDD

- Drive HDD hadir dalam dua bentuk, tetap (internal) dan eksternal.
- Yang pertama (tetap) terletak di dalam perangkat komputasi, sedangkan HDD eksternal dapat dihubungkan ke perangkat komputasi melalui kabel USB atau eSATA untuk meningkatkan penyimpanan yang tersedia.
- Perangkat HDD menyimpan data di piringan: piringan adalah piringan logam bundar yang terbuat dari aluminium, kaca, atau keramik yang dilapisi dengan bahan magnetik yang menyimpan data di kedua sisi (permukaan atas dan bawah).
- Sebuah hard disk dapat memiliki sejumlah piringan; konsumen hard drive dengan kapasitas kurang dari 500 GB hanya akan berisi satu piringan.
- Untuk hard drive konsumen berkapasitas besar, jumlah piringan dapat berkisar dari satu hingga lima tergantung pada ukuran fisik, kapasitas, pabrikan, dan model HDD.

How Is Data Stored on the HDD?

- Seperti yang telah kami katakan, setiap piringan berisi ribuan trek, dan setiap trek dibagi menjadi beberapa sektor.
- Setiap trek di piringan memiliki jumlah sektor yang sama. Sebuah hard disk dapat menampung jutaan sektor. Kapasitas penyimpanan umum setiap sektor adalah 512 byte; namun, sistem file yang lebih baru dapat menyimpan hingga 4 KB.
- Semua sistem file yang digunakan oleh Windows mengatur hard disk berdasarkan ukuran cluster (cluster terdiri dari sejumlah sektor).
- Ukuran cluster mewakili jumlah ruang disk terkecil yang dapat digunakan untuk memegang file.
- Ukuran cluster tergantung pada sistem file yang digunakan dan ukuran partisi, dan berkisar dari 4 hingga 64 sektor.
- Ini membuat satu cluster dapat menyimpan hingga 64 KB data menggunakan pengaturan default.



DISK SLACK CHECKER

There is a tool from Karen Ware called “Disk Slack Checker” (www.karenware.com/powertools/ptslack), which can calculate available slack space on a hard disk (see Figure 2-8).

| Drive C: 100.00% complete | | | | | | | |
|-----------------------------|---------|-----------|------------|-----------|---------|-----------|--|
| All Drives 100.00% complete | | | | | | | |
| Per File | Used | % of Size | % of Alloc | Per File | Slack | % of Size | |
| 467.99 KB | 1.15 TB | 532.39% | 99.51% | 465.70 KB | 5.79 GB | 2.61% | |

Size of Slack Space on target partition



Figure 2-8. Using “Disk Slack Checker” from Karen Ware to calculate available slack space on target volume

SSD

- Kita dapat menganggap SSD sebagai jenis HDD modern.
- Mirip dengan memori flash, SSD tidak memiliki bagian yang bergerak (piringan); itu menyimpan data ke dalam serangkaian sel flash NAND atau microchip (NAND terdiri dari satu set transistor yang mirip dengan yang digunakan dalam RAM; namun, transistor jenis ini tidak perlu diperbarui terus-menerus sehingga dapat menyimpan datanya, membuatnya menjadi jenis memori nonvolatile).
- SSD menggunakan semacam pengontrol (yang merupakan prosesor tertanam) untuk menentukan cara menyimpan, mengambil, dan menyimpan data.
- Tidak adanya bagian mekanis yang bergerak membuat SSD mengkonsumsi lebih sedikit daya dan menikmati kecepatan tinggi dibandingkan dengan HDD biasa (10×).
- Pada awal penggunaannya, SSD mengalami kerugian besar, yaitu terbatasnya jumlah siklus tulis yang dimilikinya; namun, seiring kemajuan teknologi, produsen SSD bekerja untuk mengatasi masalah ini dengan menciptakan algoritme yang lebih efisien yang menyebarkan data secara merata di semua sel, sehingga membuat semua sel di SSD hidup lebih lama tanpa masalah.
- SSD menjadi semakin populer di notebook dan workstation kelas menengah dan mahal, dan seiring dengan kemajuan teknologi setiap hari, kita dapat mengharapkan penurunan harga SSD.
- Kapasitas juga menjadi masalah: unit SSD masih memiliki kapasitas yang rendah dibandingkan dengan HDD.

Embedded MultiMediaCard (eMMC)

- ❑ Ini adalah pengganti yang murah untuk drive SSD; ini adalah penyimpanan non-volatile berbasis flash yang digunakan di banyak ponsel pintar Android, tablet Windows, dan laptop kelas bawah (umumnya yang datang dengan CPU Intel Atom).
- ❑ eMMC memiliki arsitektur yang mirip dengan kartu SD (keduanya menyimpan informasi dalam memori flash), dan dirancang dengan biaya seefektif mungkin.
- ❑ Ini membuatnya kecepatan dan daya tahan drive SSD kurang.
- ❑ eMMC disolder ke motherboard perangkat, dan dengan demikian Anda tidak dapat melepasnya secara terpisah dari perangkat.
- ❑ Penyimpanan semacam ini memiliki kapasitas terbatas; ukuran yang paling umum adalah 32, 64, dan 128 GB.

Optical Data Storage

- ❑ Jenis penyimpanan ini menyimpan data dalam media yang dapat dibaca secara optik. Contoh media tersebut termasuk CD-ROM, DVD, dan disk Blu-ray. Akuisisi CD/DVD mirip dengan memperoleh hard drive;
- ❑ kita perlu membuat gambar dari konten CD/DVD target dan kemudian menyelidikinya menggunakan alat forensik digital yang sesuai.

DATA MEASUREMENT CHART

Table 2-4 is a useful data measurement chart.

Table 2-4. Data Measurement Chart

| Data Measurement | Size |
|------------------|------------------------------|
| Bit | Single Binary Digit (1 or 0) |
| Byte | 8 bits |
| Kilobyte (KB) | 1,024 bytes |
| Megabyte (MB) | 1,024 KB |
| Gigabyte (GB) | 1,024 MB |
| Terabyte (TB) | 1,024 GB |
| Petabyte (PB) | 1,024 TB |
| Exabyte (EB) | 1,024 PB |
| Zettabyte (ZB) | 1 billion TB |

HPA and DCO

- Host protected area (HPA) adalah area cadangan yang dibuat oleh produsen HDD yang tidak dapat diakses oleh pengguna, OS, atau BIOS.
- Area ini biasanya berisi utilitas pendukung HDD (seperti program diagnostik dan pemulihan) dan terkadang sektor boot file dari OS yang diinstal.
- The device configuration overlay(DCO) adalah area yang dicadangkan pada HDD yang tidak didukung oleh semua produsen HDD; itu terletak di ujung disk setelah partisi HPA.
- HPA dan DCO keduanya dapat hidup berdampingan dalam hard disk yang sama, tetapi DCO harus dibuat sebelum HPA.
- Dari perspektif forensik digital, area DCO dan HPA akan bertahan bahkan setelah format disk penuh dilakukan, menjadikannya tempat yang ideal bagi kemungkinan pelanggar untuk menyembunyikan data yang memberatkan.
- Banyak forensik komputer mampu mengakses dan mencitrakan area ini pada hard drive; sebagian besar alat akuisisi perangkat keras dapat menggambarkan kedua area ini.
- Selalu berkonsultasi dengan alat forensik komputer yang ingin Anda gunakan untuk kemampuan tersebut.

Table 2-5. List of Tools for Viewing/Editing Data in HPA and DCO

| Program Name | URL |
|--------------|------------------------------------------------------------------------------------------------------------------------|
| Fiesta | http://sourceforge.net/projects/fiesta |
| TAFT | www.vidstrom.net/stools/taft/ |
| ATATool | www.datasynergy.co.uk/products/misc/atatool.aspx |
| HDAT2 | www.hdat2.com/ |
| DiskCheckup | www.passmark.com/products/diskcheckup.htm |

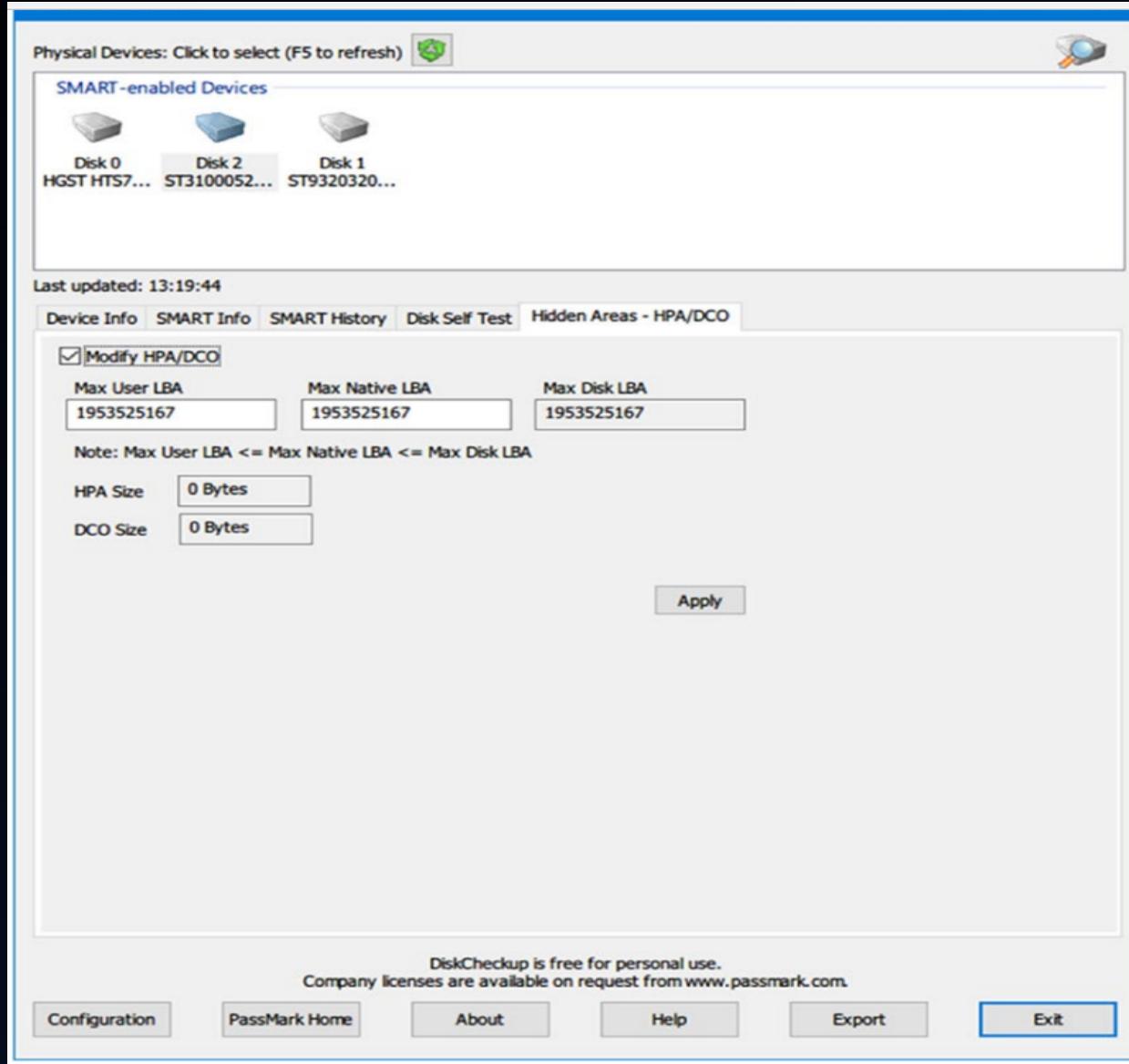


Figure 2-9. Using DiskCheckup from PassMark to edit HPA and DCO size areas

Data Recovery Considerations

- Memulihkan data dari SSD lebih sulit daripada dari HDD, dan terkadang tidak mungkin sama sekali.
- Misalnya, saat Anda menghapus file di HDD, data file subjek tidak akan langsung terhapus; sebagai gantinya, HDD hanya akan menghapus penunjuk ke file ini, menandai ruangnya pada disk sebagai kosong.
- Data file subjek akan dihapus hanya ketika sistem operasi perlu menulis data baru di lokasinya.
- SSD menggunakan mekanisme berbeda untuk menangani file yang dihapus; misalnya, ketika pengguna menghapus file, SSD akan menggunakan perintah TRIM, yang berfungsi untuk menghapus file subjek secara instan, membiarkan lokasinya bebas untuk ditempati file lain.
- Setiap tipe system operasi mengimplementasikan perintah TRIM secara berbeda: beberapa OS akan menjalankannya segera setelah pengguna menghapus file, sementara yang lain akan menjalankannya secara berkala.

File Systems

- Sistem file menyediakan mekanisme (peta konstruksi logis) untuk sistem operasi untuk melacak file dalam partisi.
- Sebelum Anda dapat menggunakan perangkat penyimpanan untuk menyimpan data dan menginstal aplikasi dan OS, Anda harus menginisialisasinya terlebih dahulu dengan menulis struktur data sistem file ke drive (juga dikenal sebagai memformat drive).
- OS Windows menggunakan sistem file FAT atau NTFS untuk menginstal sendiri pada hard drive.

NTFS

- NTFS adalah sistem file berpemilik yang dikembangkan oleh Microsoft untuk sistem operasi Windows modernnya; memformat volume dengan NTFS menghasilkan pembuatan beberapa file metadata



FAT

- FAT (File allocation Table), salah satu sistem file tertua yang masih digunakan, memiliki empat variasi: FAT12, FAT16, FAT32, dan FATX. Microsoft telah menggunakan FAT sebagai sistem file default untuk semua versi Windows lama termasuk Windows NT.
- FAT lebih portabel daripada sistem file NTFS karena Anda dapat menggunakannya di perangkat yang berbeda.
- Misalnya, FAT umumnya digunakan di kamera digital, kartu SD, smartphone, USB thumb drive, dan banyak perangkat yang disematkan.
- Perangkat penyimpanan yang diformat dengan FAT dapat dibaca di berbagai platform dengan mudah, tidak seperti NTFS, yang hanya dapat dibaca oleh OS Windows.
- NTFS melampaui FAT di banyak area; misalnya, NTFS mendukung ukuran file besar dan fitur enkripsi file.
- NTFS digunakan oleh Microsoft untuk menginstal versi OS Windows modernnya seperti Windows 8 dan 10 dan edisi Server baru.

Computing Environment

- ❑ Lingkungan komputasi akan sangat memengaruhi pilihan Anda tentang cara menangkap bukti digital.
- ❑ Seiring kemajuan teknologi dan peningkatan kecepatan Internet, kita dapat mengharapkan untuk melihat transformasi yang signifikan dari arsitektur komputer terpusat ke non-terpusat. atau arsitektur komputer terdistribusi dalam beberapa tahun ke depan.

Personal Computing Environment

- ❑ Ini mungkin yang paling umum hari ini. Di lingkungan ini, semua program diinstal secara lokal dan dijalankan dari mesin yang sama.
- ❑ Data juga disimpan ke hard drive lokal mesin. Laptop, desktop, printer, tablet, dan bahkan smartphone adalah contoh lingkungan komputasi pribadi.
- ❑ Lingkungan ini adalah yang paling mudah untuk ditangani jika perangkat pribadi menjadi bagian dari investigasi kriminal, karena lokasi barang bukti terikat pada perangkat subjek saja.

Client Server Computing Environment

- ❑ Dalam lingkungan ini, ada dua mesin: klien (misalnya, komputer pribadi, laptop, atau tablet) dan server.
- ❑ Klien meminta data dari server melalui koneksi HTTP, dan server merespons dengan data.
- ❑ Contoh lingkungan seperti itu adalah server email yang berinteraksi dengan Anda untuk mendapatkan email Anda.

Distributed Computing Environment

- ❑ Dalam lingkungan ini, aplikasi diinstal dan dijalankan di beberapa komputer; ini memungkinkan satu aplikasi untuk membagi fungsinya menjadi beberapa komponen, dengan masing-masing komponen bekerja pada komputer khusus.
- ❑ Penyimpanan data juga didistribusikan dalam tipe ini lingkungan, dan klien dan aplikasi lain perlu berkomunikasi dengan server jarak jauh melalui jaringan untuk mengakses data atau menggunakan program.
- ❑ Menangkap bukti digital dalam lingkungan seperti itu sangat menantang, karena data dan log pribadi pengguna dapat tersebar di antara server jarak jauh yang berbeda, yang pada gilirannya dapat ditempatkan di wilayah geografis yang berbeda di bawah yurisdiksi yang berbeda.
- ❑ Volume data (dan log) yang perlu diselidiki juga merupakan masalah di lingkungan seperti itu, karena volumenya bisa sangat besar dalam banyak kasus.

Cloud Computing

- Komputasi awan adalah model teknologi modern, yang dikembangkan sebagai hasil dari ledakan pertumbuhan Internet dan komunikasi online, yang memungkinkan penyedia layanan untuk memberikan berbagai layanan komputasi kepada pengguna melalui Internet.
- Jangkauan layanan komputasi yang dapat ditawarkan dengan cara ini sangat luas; misalnya, alih-alih membeli hard drive eksternal untuk menyimpan data cadangan, Anda dapat menyimpan data ini di penyedia cloud dengan sedikit biaya.
- Penyedia cloud akan bertanggung jawab untuk mengelola data pengguna di cloud (misalnya, membuat salinan cadangan dan melindungi data ini dari perangkat lunak berbahaya dan serangan siber).
- Komputasi awan tidak hanya terkait dengan penyimpanan data pengguna; perusahaan menggunakan komputasi awan untuk mengurangi biaya infrastruktur TI.
- Misalnya, perusahaan dapat menggunakan layanan komputasi awan yang menyediakan aplikasi yang diperlukan (seperti suite MS Office) untuk pekerjaannya, daripada membeli lisensi perangkat lunak untuk setiap pengguna secara individual.
- Biaya muncul lebih banyak saat menggunakan perangkat lunak mahal seperti SQL Server dan Windows Server OS; membayar untuk menggunakan perangkat lunak tersebut berdasarkan penggunaan saat di cloud lebih hemat biaya daripada menginstalnya di tempat.

Software as a Service (SaaS)

- Dalam model ini, pengguna membeli akun di penyedia komputasi awan dan memilih aplikasi mana yang ingin ia instal.
- Dengan cara ini, pengguna akan melakukan pekerjaannya di server cloud (jarak jauh) alih-alih menggunakan aplikasi ini di mesin lokal.
- Contoh layanan tersebut adalah Google Apps for Education dan Microsoft Office 365.

Platform as a Service (PaaS)

- Model ini populer di antara perusahaan pengembangan perangkat lunak/web, di mana pelanggan—perusahaan pengembangan web, misalnya—membayar akun di penyedia layanan cloud yang menyediakan lingkungan yang disesuaikan sesuai dengan kebutuhan klien (misalnya, untuk menginstal alat pengembangan web yang diperlukan, mempersiapkan pengembangan dan pengujian lingkungan, dll).
- Hal ini memungkinkan pelanggan untuk memulai pekerjaannya dengan cepat dengan biaya minimum.

Infrastructure as a Service (IaaS)

- Dalam model ini, penyedia cloud menyediakan perangkat keras (server fisik dan perangkat keras pusat data) yang dibutuhkan oleh klien melalui Internet secara sewa.
- Klien membeli dan menginstal aplikasi dan OS yang diperlukan dan mengonfigurasinya sesuai dengan kebutuhan bisnis.
- Layanan tersebut biasanya digunakan oleh penyedia hosting web dan perusahaan untuk penyimpanan, pencadangan, dan pemulihan data di luar lokasi perusahaan.
- Yang kami pedulikan dari diskusi ini adalah bahwa layanan cloud computing akan menambah kesulitan tambahan bagi aparat penegak hukum saat menyelidiki kasus kriminal.
- Misalnya, bagaimana jika seorang warga negara Inggris yang menjadi tersangka kasus pidana mengunggah datanya ke penyedia penyimpanan cloud yang berlokasi di Singapura; dapatkah polisi Inggris memaksa provider Singapura untuk menyerahkan salinan data pengguna?

IP Address

- Anda benar-benar akan menemukan informasi yang memerlukan pemahaman skema pengalamatan yang digunakan di Internet dan banyak jaringan pribadi selama penyelidikan Anda, jadi memahami protokol IP merupakan prasyarat bagi penyelidik digital mana pun.
- Pada bagian ini, kita akan berbicara secara singkat tentang konsep alamat IP dan bagaimana perangkat komputasi terhubung ke Internet

What Is an IP Address?

- Alamat IP adalah alamat unik yang membedakan perangkat komputasi ketika terhubung ke IP jaringan.
- Alamat IP mirip dengan sidik jari; karenanya, tidak ada dua perangkat yang dapat memiliki alamat IP yang sama pada jaringan IP yang sama.
- IP biasanya digabungkan dengan protokol lain bernama Transmission Control Protocol (TCP), yang memungkinkan sebuah perangkat komputasi untuk membuat koneksi virtual antara tujuan dan sumber untuk bertukar informasi.

What Is an IP Address?

- Alamat IP publik: Ini memungkinkan koneksi langsung ke Internet dan ditetapkan oleh ISP Anda, di mana setiap IP adalah unik.
 - Misalnya, server email harus memiliki alamat IP publik yang unik secara global.
 - Alamat IP publik dapat berupa statis atau dinamis.
- Alamat IP statis. Alamat ini sudah diperbaiki—sama seperti telefon Anda nomor – dan tetap sama selama ISP memesannya untukmu.
- Alamat IP dinamis. Yang ini berubah setiap kali pengguna terhubung ke Internet.
- ISP menggunakan protokol yang disebut Dynamic Host Configuration Protocol (DHCP) untuk menetapkan alamat IP secara otomatis untuk pelanggan mereka
- Alamat IP pribadi (alias alamat IP lokal): Ini adalah alamat IP yang tidak menghadap ke Internet untuk perangkat yang biasanya berada di belakang perangkat perutean.
- Semua perangkat yang ada di jaringan tertutup (mis. Jaringan rumah atau sekolah) akan menggunakan alamat IP pribadi.
- Alamat-alamat ini biasanya ditetapkan secara otomatis menggunakan DHCP router.

Wireless LAN adapter Wi-Fi:

| | |
|------------------------------------------|---------------------------------------|
| Connection-specific DNS Suffix | : domain.name |
| Description | : Broadcom 802.11n Network Adapter |
| Physical Address | : [REDACTED]-9F-D1 |
| DHCP Enabled. | : Yes |
| Autoconfiguration Enabled | : Yes |
| Link-local IPv6 Address | : [REDACTED] %3 (Preferred) |
| IPv4 Address. | : 192.168.1.102 (Preferred) |
| Subnet Mask | : 255.255.255.0 |
| Lease Obtained. | : Wednesday, April 4, 2018 7:39:06 PM |
| Lease Expires | : Monday, April 9, 2018 10:10:48 AM |
| Default Gateway | : [REDACTED] 192.168.1.1 |
| DHCP Server | : 192.168.1.1 |
| DHCPv6 IAID | : [REDACTED]435 |
| DHCPv6 Client DUID. | : 00-01-00-01-[REDACTED] |
| DNS Servers | : 8.8.8.8 8.8.4.4 |
| NetBIOS over Tcpip. | : Enabled |



Reference web sites:

1. OSINT: The author's dedicated portal for OSINT resources (www.osint.link)
2. DarknessGate: The author's IT security and digital forensic reference portal (www.darknessgate.com)
3. Cyber Forensicator (www.cyberforensicator.com)
4. DFIR Training: Check the "Resources" section (www.dfir.training)
5. Tools Watch (www.toolswatch.org)

Blogs:

1. Another Forensics Blog (az4n6) (<http://az4n6.blogspot.com>)
2. Black Bag (www.blackbagtech.com/index.php/blog)
3. Malware Byte Blog (<https://blog.malwarebytes.com>)
4. Security Score Card (<https://securityscorecard.com/blog>)
5. Forensic Focus (www.forensicfocus.com)
6. SANS Digital Forensics and Incident Response Blog (<https://digital-forensics.sans.org/blog>)
7. Digital Forensics Magazine (<http://digitalforensicsmagazine.com/blogs>)
8. Heimdalsecurity blog (<https://heimdalsecurity.com/blog>)
9. Hak5 (<https://shop.hak5.org/blogs/news>)

1. IT security news:
 1. Dark Reading (www.darkreading.com)
 2. CIO (www.cio.com/category/security)
 3. PC Mag (<http://sea.pc当地>.com)

IT security/forensics tutorials:

1. Info security institute (<https://resources.infosecinstitute.com>)
2. Forensics Wiki (www.forensicswiki.org)
3. Life in Hex (<https://lifeinhex.com>)

IT security alerts

1. US-CERT (www.us-cert.gov/ncas/alerts)
2. Norse: Global cyberattack map (www.norse-corp.com)

Forensik Digital (Pendahuluan)

ERI PRASETYO WIBOWO

UNIVERSITAS GUNADARMA

Title and Content Layout with List

- Apa Itu Digital Forensik?
- Tujuan Forensik Digital
- Cybercrime
- Kategori Digital Forensik

Apa itu Forensik Digital

- ❑ Forensik digital adalah cabang ilmu forensik yang menggunakan pengetahuan ilmiah untuk mengumpulkan, menganalisis, mendokumentasikan, dan menyajikan bukti digital yang berkaitan dengan kejahatan komputer untuk dipergunakan di pengadilan.
- ❑ Tujuan utamanya adalah mengetahui apa yang dilakukan, kapan itu dilakukan, dan siapa yang melakukannya.
- ❑ Istilah "forensik digital" secara luas digunakan sebagai sinonim untuk forensik komputer (juga dikenal sebagai cyberforensics)
- ❑ Tetapi telah diperluas mencakup penyelidikan semua perangkat yang mampu menyimpan data digital, seperti perangkat jaringan, ponsel, tablet, digital kamera, perangkat Internet of Things (IoT), peralatan rumah tangga digital, dan perangkat digital lainnya media penyimpanan seperti CD/DVD, drive USB, kartu SD, drive eksternal, dan kaset cadangan.
- ❑ Definisi yang lebih luas, forensik digital juga bertanggung jawab untuk menyelidiki hampir semua serangan siber terhadap sistem terkomputerisasi seperti ransomware, phishing, Serangan perintah SQL, serangan penolakan layanan (DDoS), pelanggaran data, spionase siber, akun yang disusupi, akses tidak sah ke infrastruktur jaringan, dan serangan siber terkait lainnya yang dapat menyebabkan kerugian komersial atau reputasi.

Tujuan Forensik Digital

- ❑ Menyelidiki kejahatan berkomitmen menggunakan perangkat komputasi seperti komputer, tablet, ponsel, atau lainnya perangkat yang dapat menyimpan/memproses data digital dan mengekstraksi bukti digital darinya dalam acara yang sehat secara forensik untuk diajukan di pengadilan.
- ❑ Tujuan utamanya adalah mengetahui apa yang dilakukan, kapan itu dilakukan, dan siapa yang melakukannya.

Forensik Digital dicapai dengan cara:

1. Menemukan bukti hukum dalam perangkat komputasi dan melestarikannya integritas dengan cara yang dianggap dapat diterima di pengadilan.
2. Melestarikan dan memulihkan bukti setelah diterima di pengadilan prosedur teknis.
3. Mengatribusikan suatu tindakan kepada inisatornya.
4. Mengidentifikasi kebocoran data dalam suatu organisasi.
5. Mengakses kemungkinan kerusakan yang terjadi selama pelanggaran data.
6. Menyajikan hasil dalam bentuk laporan formal yang layak untuk dipresentasikan di Pengadilan.
7. Memberikan pedoman keterangan ahli di pengadilan.

Kejahatan Dunia Maya

- kejahatan dunia maya mencakup aktivitas ilegal apa pun yang dilakukan menggunakan jenis komputasi perangkat atau jaringan komputer seperti Internet.
- Departemen Kehakiman AS (DOJ) mendefinisikan cybercrime sebagai “setiap tindak pidana yang dilakukan terhadap atau dengan penggunaan komputer atau jaringan komputer.”
- Motivasi utama di balik kejahatan dunia maya adalah finansial gain (contoh: menyebarkan malware untuk mencuri kode akses ke rekening bank).
- Namun, sebagian besar kejahatan dunia maya memiliki motivasi yang berbeda, seperti mengganggu layanan (untuk misalnya, serangan DDoS untuk menghentikan layanan yang ditawarkan oleh organisasi target), mencuri data rahasia (contoh: data konsumen, informasi medis), pertukaran hak cipta materi dengan cara yang melanggar hukum, dan spionase cyber (perdagangan perusahaan dan rahasia militer).

Mode Serangan Kejahatan Dunia Maya

- sumber utama: serangan orang dalam dan serangan eksternal.
- Serangan orang dalam: Ini adalah risiko siber paling berbahaya yang dihadapi organisasi hari ini, karena dapat bertahan lama tanpa mereka mengetahui tentang hal itu; serangan seperti itu datang ketika ada pelanggaran kepercayaan dari karyawan—atau orang lain seperti mantan karyawan, kontraktor pihak ketiga, atau rekan bisnis—yang bekerja dalam target organisasi yang memiliki akses sah ke sistem komputasinya dan/atau informasi tentang praktik dan pertahanan keamanan sibernya. Spionase ekonomi termasuk dalam kategori ini.
- Serangan eksternal: Jenis serangan ini berasal dari luar target organisasi, biasanya berasal dari peretas yang terampil. Serangan seperti itu merupakan serangan terbesar terhadap organisasi di seluruh dunia. Peretas topi hitam dapat mencoba menembus organisasi target jaringan komputasi dari negara lain untuk mendapatkan yang tidak sah mengakses.
- Terkadang penyerang eksternal mendapatkan intelijen dari orang dalam (karyawan yang tidak puas) di perusahaan sasaran yang informasi tentang sistem keamanannya untuk memfasilitasi akses ilegal mereka.

Kategori Kejahatan Dunia Maya

- ❑ Perangkat komputasi digunakan sebagai senjata untuk melakukan kejahatan. Contoh: Meluncurkan serangan penolakan layanan (DoS) atau mengirim ransomware.
- ❑ Perangkat komputasi adalah target kejahatan. Contoh: Mendapatkan akses tidak sah ke komputer target.
- ❑ Perangkat komputasi digunakan sebagai fasilitator kejahatan. Contoh: Menggunakan komputer untuk menyimpan data yang memberatkan atau membuat online komunikasi dengan penjahat lainnya.

Distribusi Malware

- ❑ Malware adalah kependekan dari "malicious software" dan merupakan perangkat lunak apa pun yang digunakan untuk membawa kerusakan ke perangkat komputasi (komputer, telepon pintar, dll.) atau konten yang disimpan (data atau) aplikasi).
- ❑ Malicious malware dapat bermanifestasi dalam berbagai cara, seperti memformat hard disk Anda, menghapus atau merusak file, mencuri informasi login yang disimpan, mengumpulkan informasi sensitif (file dan foto pribadi Anda), atau hanya menampilkan iklan yang tidak diinginkan di layar Anda.
- ❑ Banyak varian malware yang tersembunyi dan beroperasi secara diam-diam tanpa sepengetahuan atau kesadaran pengguna. Malware adalah istilah yang digunakan untuk merujuk pada banyak jenis perangkat lunak berbahaya seperti virus komputer, worm, Trojan horse, spyware, ransomware, rootkit, scarware, dan adware.

Distribusi Ransomware

- ❑ Ransomware adalah malware komputer yang menginstal diam-diam di mesin penggunanya tujuannya adalah untuk menolak akses ke file pengguna, terkadang mengenkripsi seluruh hard drive (HD) dan bahkan semua drive eksternal yang terpasang dan akun penyimpanan cloud yang terhubung.
- ❑ kemudian menuntut agar pengguna membayar uang tebusan agar pembuat malware menghapus pembatasan sehingga pengguna dapat memperoleh kembali akses ke sistem dan aset yang disimpan.

Pembajakan Kripto

- ❑ Ini adalah bagian dari kode, biasanya ditulis dalam JavaScript, yang menginfeksi komputer Anda secara diam-diam melalui browser web untuk menambang cryptocurrency.
- ❑ Saat gelombang cryptocurrency sedang meningkat, lebih banyak penjahat dunia maya menggunakan teknik semacam itu untuk keuntungan komersial menggunakan komputer orang tanpa sepengetahuan mereka. Serangan ini menghabiskan banyak target kecepatan CPU komputer.

Peretasan

- Peretasan adalah proses menyerang privasi Anda dengan mendapatkan akses tidak sah ke perangkat komputasi atau jaringan internal Anda. Peretas biasanya memindai mesin Anda untuk kerentanan (seperti pembaruan Windows yang tidak ditambal) dan mendapatkan akses melaluinya. Setelah mendapatkan akses, mereka dapat menginstal keylogger atau Trojan horse untuk mempertahankan akses, untuk mulai mencuri informasi, atau untuk memata-matai aktivitas pengguna.

Injeksi SQL

- Ini adalah teknik peretasan yang memungkinkan peretas menyerang kerentanan keamanan dari database yang menjalankan situs web. Penyerang memasukkan kode SQL ke situs web target formulir web dan menjalankannya untuk memaksa database back-end situs web untuk dirilis informasi rahasia kepada penyerang.

Pharming

- Ini adalah serangan siber yang dimaksudkan untuk mengarahkan pengguna dari situs web yang sah ke situs penipuan situs tanpa sepengertahanan mereka. Tujuan akhirnya biasanya menginfeksi komputer target dengan perangkat lunak jahat.

Pengelabuan Pesan (phishing)

- Phising datang dalam berbagai bentuk, seperti pesan SMS, email, dan web tautan situs (URL), yang semuanya dirancang agar terlihat asli dan menggunakan format yang sama seperti perusahaan yang sah mereka berpura-pura menjadi.
- Phishing bertujuan untuk mengumpulkan detail sensitif pengguna (seperti informasi perbankan, kredensial login, dan info kartu kredit) dengan mengelabui akhir pengguna untuk menyerahkan informasi kepada penyerang.

Pengeboman dan Spamming Email

- Pengeboman email terjadi ketika penyusup, atau sekelompok penyusup, mengirimkan volume besar email ke server target atau akun email target, membuatnya macet.
- Spam tidak diminta email yang biasanya dikirim ke sejumlah besar pengguna untuk tujuan komersial (menunjukkan iklan atau promosi); namun, banyak email spam berisi tautan tersamar yang dapat mengarah korban ke situs web phishing atau situs web jahat yang menghosting malware untuk lebih lanjut menginfeksi mesin pengguna.
- Pencurian identitas adalah mencuri informasi pribadi tentang orang-orang dan menggunakannya secara ilegal.

Cyberstalking

- ❑ Ini adalah pelanggaran privasi pengguna; itu bekerja ketika penyusup mengikuti target aktivitas online seseorang dan mencoba melecehkan/mengancamnya menggunakan intimidasi verbal melalui email, layanan chat, dan media sosial.
- ❑ Jangkauan luas situs media sosial dan sejumlah besar detail pribadi yang tersedia untuk umum membuat cyberstalking menjadi masalah besar di era digital sekarang ini.

Menggunakan Jaringan Internet Secara Ilegal

- ❑ Menyebarluaskan konten ilegal dan menjual layanan dan produk ilegal.
- ❑ Contoh termasuk menyebarluaskan kebencian dan menghasut terorisme, mendistribusikan pornografi anak secara online, dan menjual obat-obatan dan senjata (terutama di pasar darknet).

Serangan DDoS

- ❑ Serangan DDoS adalah upaya untuk membuat layanan online tidak tersedia dengan cara yang berlebihan dengan lalu lintas dari berbagai sumber.
- ❑ Penyerang membangun jaringan komputer yang terinfeksi, yang bisa berupa jutaan mesin, yang dikenal sebagai botnet, dengan menyebarluaskan perangkat lunak berbahaya melalui email, situs web, dan media sosial.
- ❑ Setelah terinfeksi, mesin ini dapat dikendalikan dari jarak jauh oleh master bot, tanpa sepengetahuan pemiliknya, dan digunakan seperti tentara untuk melancarkan serangan terhadap target apapun.

Rekayasa Sosial (Social Engineering)

- ❑ Rekayasa sosial adalah jenis serangan yang menggunakan trik psikologis (trik sosial) secara berlebihan telepon atau menggunakan perangkat komputasi untuk meyakinkan seseorang untuk menyerahkan sensitif informasi tentang dirinya sendiri atau tentang organisasi dan sistem komputernya.

Pembajakan Perangkat Lunak (Software Piracy)

- ❑ Ini adalah penggunaan, pengunduhan, dan distribusi materi bajakan secara tidak sah seperti film, game, perangkat lunak, lagu, buku, dan produk kekayaan intelektual lainnya.
- ❑ Kejahatan dunia maya dapat dilakukan oleh satu orang atau sekelompok orang yang terorganisir penjahat; yang terakhir lebih berbahaya karena memiliki sumber daya untuk melakukan dan mengembangkan serangan canggih terhadap organisasi sasaran dan individu.

Kategori Forensik Digital

Forensik Komputer

- Ini adalah jenis forensik digital tertua; ini berkaitan dengan penyelidikan digital bukti yang ditemukan di komputer desktop, di laptop, di perangkat penyimpanan digital (seperti hard drive eksternal, thumb drive, dan kartu SD), dan dalam memori akses acak (RAM), selain sistem operasi dan jejak aplikasi yang diinstal dan log terkait.
- Aktivitas utama dari jenis ini adalah memulihkan data yang dihapus dari target penyimpanan perangkat dan menganalisisnya untuk memberatkan atau membebaskan bukti.

Forensik Seluler

- Forensik seluler adalah jenis forensik digital yang berkaitan dengan perolehan bukti digital dari perangkat seluler.
- Perangkat seluler mencakup perangkat komputasi apa pun (seperti telepon, smartphone, tablet, dan perangkat yang dapat dikenakan seperti jam tangan pintar) dapat membuat ponsel panggilan menggunakan jaringan komunikasi standar seperti GSM, 3G, 4G, dan sebagainya.
- Misalnya perangkat biasanya sadar lokasi, artinya ia memiliki GPS bawaan atau satelit serupa sistem penentuan posisi.
- Proliferasi teknologi seluler di antara pengguna secara global akan segera menjadikan mobile forensik cabang yang paling banyak digunakan di antara jenis forensik digital lainnya.

Forensik Jaringan

- Jenis forensik digital ini berkaitan dengan pemantauan dan analisis arus lalu lintas di jaringan komputer untuk mengekstrak bukti yang memberatkan (misalnya, menemukan sumber serangan keamanan) atau untuk mendeteksi penyusupan.
- Aliran data melalui jaringan dapat ditangkap sebagai massa secara real time dan disimpan untuk analisis nanti atau dianalisis secara real time dengan opsi untuk simpan hanya segmen acara menarik untuk analisis offline lebih lanjut (opsi ini memerlukan lebih sedikit ruang penyimpanan).
- Forensik jaringan hanya berurusan dengan data yang mudah menguap (langsung), tidak seperti jenis yang lain forensik digital.

Forensik Basis Data

- Forensik basis data berkaitan dengan analisis data dan metadata yang ada dalam suatu database seperti Microsoft SQL Server, Oracle, MySQL, dan lain-lain.
- Forensik basis data mencari siapa yang mengakses database dan tindakan apa yang dilakukan untuk membantu mengungkap aktivitas jahat yang dilakukan di dalamnya.

Analisis Data Forensik

- Cabang ini berurusan dengan analisis data terstruktur perusahaan untuk mencegah dan menemukan kegiatan penipuan yang dihasilkan dari kejahatan keuangan.
- Ini melihat pola yang bermakna dalam perusahaan aset data dan membandingkannya dengan hasil historis untuk mendeteksi dan mencegah penyalahgunaan sumber daya perusahaan.
- Ada juga jenis forensik digital khusus lainnya seperti forensik email, cloud forensik penyimpanan, forensik untuk aplikasi tertentu (mis., Forensik browser web), sistem file forensik (NTFS, FAT, EXT), forensik perangkat keras, forensik multimedia (teks, audio, video, dan gambar), dan forensik memori (RAM [memori volatil]); Namun, semua ini adalah cabang kecil yang termasuk dalam tipe utama yang telah disebutkan.

Pengguna Forensik Digital

- Forensik digital dapat digunakan dalam konteks yang berbeda di hampir semua sektor dan bisnis. Meluasnya penggunaan teknologi komputasi dan komunikasi Internet membuat ilmu ini terintegrasi di domain yang berbeda.

Penegakan hukum (Law Enforcement)

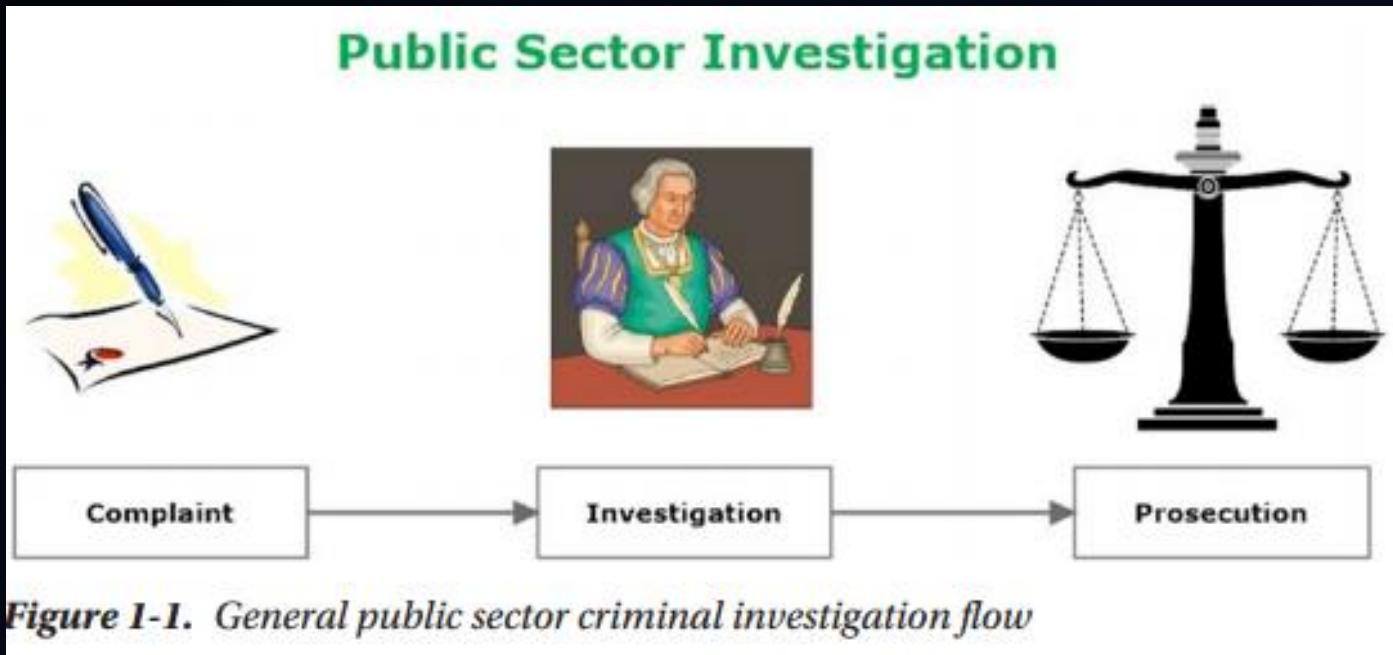
- Forensik digital pada awalnya dikembangkan untuk membantu lembaga penegak hukum dalam menerapkan hukum dan untuk melindungi masyarakat dan bisnis dari kejahatan.
- Aparat penegak hukum menggunakan forensik digital dalam konteks yang berbeda untuk mendeteksi pelanggaran dan mengaitkan tindakan ilegal dengan orang-orang yang bertanggung jawab atas mereka.
- Memang, menggunakan forensik digital tidak terbatas pada kejahatan dunia maya, karena sebagian besar kejahatan tradisional mungkin memerlukan pengumpulan bukti digital dari TKP (misalnya, ponsel yang ditemukan di TKP pasti akan membutuhkan penyelidikan, dan hal yang sama berlaku untuk laptop dan/atau thumb drive yang ditemukan dalam narkoba rumah dealer).
- Untuk spesialis forensik komputer penegak hukum, forensik digital yang telah ditentukan metodologi harus diikuti secara ketat ketika mengumpulkan, melestarikan, menganalisis, dan menyajikan bukti digital.
- Prosedur investigasi akan sangat tergantung pada yurisdiksi yang bertanggung jawab untuk menyelidiki subjek kejahatan.
- Surat perintah penggeledahan biasanya diperlukan, jika memungkinkan, sebelum petugas penegak hukum dapat menyita perangkat keras (perangkat komputasi) yang terlibat dalam kejahatan.

Intelijen dan Kontra-intelijen

- Badan intelijen menggunakan teknik dan alat forensik digital untuk memerangi kegiatan teroris, perdagangan manusia, kejahatan terorganisir, dan perdagangan narkoba, kegiatan kriminal yang berbahaya.
- Alat forensik digital dapat membantu petugas mengungkap informasi penting tentang organisasi kriminal melalui penyelidikan kejahatan perangkat digital, memantau jaringan, atau memperoleh informasi dari yang tersedia untuk sumber umum seperti situs media sosial—dikenal sebagai open source intelligence (OSINT)— tentang orang/badan yang berkepentingan.

Jenis Investigasi Forensik Digital

1. Investigasi publik



Investigasi publik melibatkan lembaga penegak hukum dan dilakukan sesuai untuk negara atau hukum negara; mereka melibatkan kasus kriminal yang berkaitan dengan investigasi komputer dan diproses sesuai dengan pedoman hukum yang diselesaikan oleh otoritas yang dihormati.

Jenis Investigasi Forensik Digital

2. Investigasi sektor swasta (perusahaan)

- Investigasi pribadi biasanya dilakukan oleh perusahaan untuk menyelidiki pelanggaran kebijakan, sengketa litigasi, penghentian yang salah, atau pembocoran rahasia perusahaan (misalnya, spionase industri).
- Tidak ada aturan (atau undang-undang) khusus untuk melakukan investigasi hal tersebut karena tergantung pada aturan masing-masing perusahaan; Namun, banyak organisasi sekarang mengikuti prosedur ketat untuk menyelidiki kejahatan digital secara internal.
- Ini prosedurnya mirip dengan investigasi publik ketika menyelidiki kejahatan, karena beberapa kasus kemudian dapat dilimpahkan ke pengadilan dan menjadi perkara pidana resmi.

Kesiapan Forensik

- Kesiapan forensik adalah tentang kemampuan organisasi tertentu untuk mengumpulkan, melestarikan, melindungi, dan menganalisis bukti digital secara forensik.
- Prosesnya harus melanjutkan tanpa mengganggu operasi saat ini untuk meminimalkan biaya investigasi.

Pentingnya Kesiapan Forensik untuk Organisasi

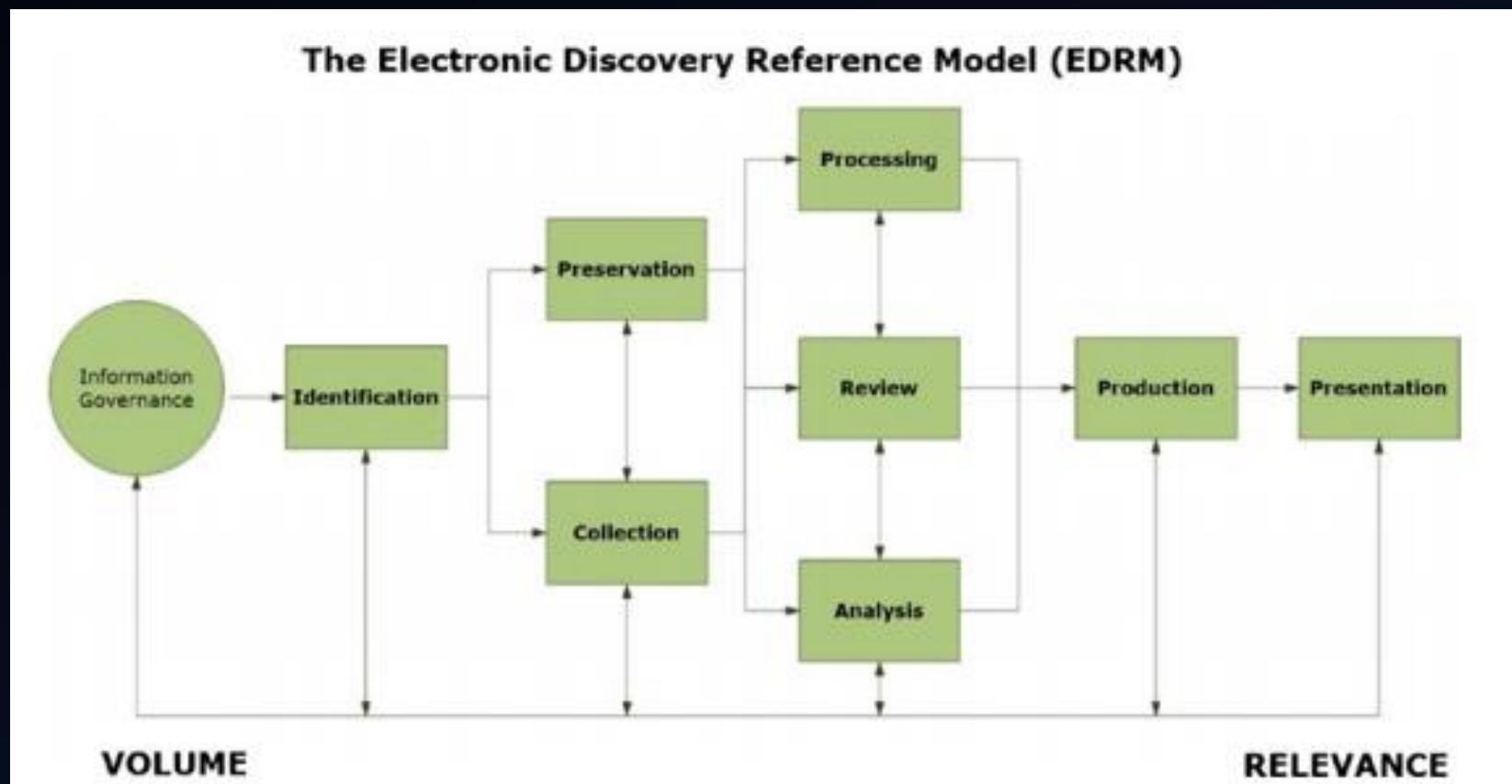
- Respon tinggi terhadap insiden dengan bukti digital. Ketika sebuah kejadian (misalnya, pelanggaran data atau kebocoran informasi) yang terjadi memerlukan pengumpulan bukti digital, adanya proses e-discovery yang jelas di tempat akan membantu organisasi bertindak segera dan memperoleh bukti digital secara forensik.
- Kepatuhan terhadap peraturan yang diterapkan pemerintah. Sejak 2015, Aturan Prosedur Perdata Federal US telah memberlakukan serangkaian persyaratan pada pihak-pihak yang terlibat dalam sengketa hukum tentang cara mengumpulkan dan melestarikan bukti digital agar dapat diterima di pengadilan. kesiapan Forensik akan mengurangi biaya untuk memperoleh bukti digital dan tentunya akan membawa penyelesaian yang lebih cepat jika kasus tersebut dibawa ke pengadilan.
- Penguatan pertahanan keamanan organisasi. Memanfaatkan kesiapan forensik akan membuat organisasi siap untuk menangani insiden keamanan internal dan eksternal dan mampu mengidentifikasi serangan dengan cepat sebelum masuk jauh ke dalam infrastruktur TI-nya (misalnya, memantau penggunaan di komputer titik akhir dapat mengungkap malware berbahaya, seperti ransomware, sebelum infeksi menyebar ke seluruh organisasi jaringan).

Pentingnya Kesiapan Forensik untuk Organisasi

- Meminimalkan serangan internal. Seperti yang sudah kami katakan, ancaman internal (misalnya, berasal dari karyawan yang tidak puas) lebih berbahaya dari serangan eksternal; adanya rencana kesiapan forensik dalam organisasi akan membuat orang dalam yang jahat takut ditangkap jika mereka melakukan kegiatan ilegal apapun.
- Meningkatkan postur keamanan organisasi. Kesiapan perencanaan forensik akan membuat organisasi menonjol sebagai entitas dengan pertahanan terhadap ancaman siber. Pelanggan akan lebih bersedia untuk berurusan dengan organisasi ini karena transaksi rahasia mereka akan menjadi terlindungi dan aman. Investor juga akan diyakinkan bahwa investasi dilindungi.

ELECTRONIC DISCOVERY REFERENCE MODEL (EDRM)

- eDrM (www.edrm.net) adalah standar populer untuk meningkatkan e-discovery dan informasi pemerintahan. ini adalah standar konseptual untuk proses e-discovery yang menguraikan standar untuk pemulihan dan penemuan data digital selama penyelidikan, litigasi, atau melanjutkan sejenisnya. Penyelidik dapat memilih untuk menggunakan beberapa langkah dalam model atau melakukan langkah dalam urutan yang berbeda



Bukti Digital

Jenis Bukti Digital

1. Kita dapat membedakan antara dua jenis utama artefak digital menurut siapa yang menciptakannya:
2. Data buatan pengguna
3. Data yang dibuat pengguna mencakup segala sesuatu yang dibuat oleh pengguna (manusia) menggunakan perangkat digital. Ini termasuk yang berikut dan lebih banyak lagi:
 4. File teks (misalnya dokumen MS Office, obrolan IM, bookmark), spreadsheet, database, dan teks apa pun yang disimpan dalam format digital,
 5. File audio dan video ,
 6. Gambar digital,
 7. Rekaman webcam (foto dan video digital),
 8. Buku alamat dan kalender,
 9. File tersembunyi dan terenkripsi (termasuk folder zip) yang dibuat oleh pengguna komputer,
 10. Pencadangan sebelumnya (termasuk pencadangan penyimpanan cloud dan offle backup seperti CD/DVD dan kaset),
 11. Detail akun (nama pengguna, gambar, kata sandi),
 12. Pesan dan lampiran email (baik online maupun email klien sebagai Outlook),
 13. Halaman web, akun media sosial, penyimpanan cloud, dan semua online akun yang dibuat oleh pengguna.

Data Buatan Mesin/Jaringan Data yang dibuat

1. Log komputer. Ini termasuk log berikut di bawah Windows OS: Aplikasi, Keamanan, Pengaturan, Sistem, Acara Teruskan, Aplikasi, dan Log Layanan,
2. Log router, termasuk penyedia layanan pihak ketiga (mis., Internet penyedia layanan (ISP) biasanya menyimpan web akun pengguna riwayat log penelusuran),
3. Konfigurasi dan jejak audit,
4. Data browser (riwayat browser, cookie, riwayat unduhan),
5. Riwayat instant messenger dan daftar teman (Skype, WhatsApp),
6. Riwayat info pelacakan GPS (dari perangkat dengan kemampuan GPS),
7. Protokol Internet perangkat (IP) dan alamat MAC selain alamat IP yang terkait dengan jaringan LAN dan siaran pengaturan,
8. Riwayat aplikasi (mis., file yang baru dibuka di MS Office) dan histori jendela,
9. Kembalikan poin di bawah mesin Windows,
10. Fies sementara,
11. Informasi header email,
12. Registry files di OS Windows,
13. Sistem files (baik tersembunyi dan biasa),
14. Spooler printer menyala,
15. Partisi tersembunyi dan ruang kendur (juga dapat berisi informasi tersembunyi pengguna),
16. Cluster buruk,
17. Paging dan hibernasi files,
18. Memori dump files,
19. Mesin virtual,
20. Rekaman video pengawasan.

Lokasi Barang Bukti Elektronik

1. Desktop
2. Laptop
3. Tablet
4. Server dan RAID
5. Perangkat jaringan seperti hub, switch, modem, router, dan titik akses nirkabel
6. Perangkat berkemampuan internet yang digunakan dalam otomatisasi rumah (mis., AC dan kulkas pintar)
7. Perangkat IoT
8. DVR dan sistem pengawasan
9. Pemutar MP3
10. Perangkat GPS
11. Smartphone
12. PDA
13. Stasiun permainan (Xbox, PlayStation, dll.)
14. Kamera digital
15. Kartu pintar
16. Pager
17. Perekam suara digital
18. Hard drive eksternal
19. Flash/thumb drive
20. Printer
21. Pemindai
22. Mesin faks (mis., nomor faks masuk dan keluar)
23. Mesin fotokopi (misalnya, file yang baru saja disalin)
24. Telepon tetap dan telepon nirkabel (misalnya, panggilan yang dilakukan, diterima, dan dijawab, pesan suara dan nomor favorit)
25. Mesin penjawab
26. Pita cadangan

Tantangan Memperoleh Bukti Digital

1. Komputer terkunci dengan kata sandi, kartu akses, atau dongle.
2. Teknik steganografi digital untuk menyembunyikan data yang memberatkan dalam gambar, video, audio fie, sistem fie, dan di depan mata (misalnya, dalam dokumen MS Word).
3. Teknik enkripsi untuk mengaburkan data, sehingga tidak dapat dibaca tanpa kata sandi.
4. Enkripsi disk penuh (FDE) termasuk partisi sistem (mis., enkripsi drive BitLocker).
5. Kata sandi yang kuat untuk melindungi sistem/volume; memecahkannya sangat memakan waktu dan mahal.
6. Mengganti nama file dan mengubah ekstensinya (mis., Mengubah DOCX ke DLL, yang merupakan jenis sistem Windows yang dikenal).
7. Upaya untuk menghancurkan bukti dengan menghapus hard drive dengan aman menggunakan berbagai alat dan teknik perangkat lunak.
8. Menghapus riwayat dari browser web saat keluar dan menonaktifkan sistem/aplikasi logging jika tersedia.

Tantangan Memperoleh Bukti Digital

9. Media digital yang rusak secara fisik; misalnya, kami tidak dapat mengambil menghapus files dari HDD yang gagal sebelum memperbaikinya.
10. Sensitivitas bukti digital; jika tidak ditangani dengan hati-hati mungkin hancur. Panas, dingin, lembab, medan magnet, dan bahkan hanya menjatuhkan perangkat media dapat menghancurnyanya.
11. Pengubahan bukti digital yang mudah; misalnya, jika komputer AKTIF, Anda harus membiarkannya AKTIF dan mendapatkan memori volatilnya (jika memungkinkan), tetapi jika komputer OFF, biarkan OFF untuk menghindari mengubah data apa pun.
12. Undang-undang yang mengatur pengumpulan bukti dan perangkat digital kejang, yang berbeda dari satu negara ke negara lain (dan antara satu negara dan lainnya). Kejahatan dunia maya dapat melintasi perbatasan dengan mudah melalui internet, membuat minimnya standarisasi cyberlaw masalah utama dalam domain ini.
13. Masalah kepemilikan data; misalnya, jika penyelidik menangkap USB thumb drive milik tersangka, tetapi data di dalamnya sepenuhnya dienkripsi dan dilindungi dengan kata sandi, tersangka dapat menyangkal kepemilikan jempol ini, membuat proses dekripsi sangat sulit untuk dicapai tanpa kata sandi/kunci yang benar.

Siapa yang Harus Mengumpulkan Bukti Digital?

- Bukti digital harus diperiksa hanya oleh profesional terlatih yang memiliki: keahlian dan pengetahuan untuk menangani data sensitif tanpa merusaknya selama penyelidikan.

Ketrampilan yang harus dimiliki

- Pemikiran analitis: Ini termasuk kemampuan untuk membuat korelasi antara peristiwa/fakta yang berbeda ketika menyelidiki suatu kejahatan.
- • Latar belakang yang kuat dalam pengetahuan TI: Ini termasuk pengetahuan yang luas tentang berbagai teknologi TI, perangkat keras, sistem operasi, dan aplikasi. Ini tidak berarti bahwa seorang penyelidik harus tahu bagaimana setiap teknologi bekerja secara detail, tetapi dia harus memiliki pemahaman umum tentang bagaimana setiap teknologi beroperasi.
- Keterampilan Hacking: Untuk memecahkan kejahatan, Anda harus berpikir seperti seorang hacker. Mengetahui teknik serangan dan konsep keamanan siber sangatlah penting untuk investigasi yang sukses.
- Keterampilan komunikasi dan organisasi: Seorang penyelidik harus memiliki keterampilan dokumentasi untuk mengatur temuannya dan mempresentasikannya mereka kepada anggota tim lainnya dan kepada pengacara dan hakim.
- Pemahaman masalah hukum tentang investigasi kejahatan digital.
- Pengetahuan yang sangat baik tentang keterampilan teknis yang terkait dengan forensik digital seperti pemulihan data dan akuisisi dan menulis laporan teknis.
- Keterampilan mencari online dan kemampuan untuk mengumpulkan informasi dari sumber yang tersedia untuk umum (yaitu, OSINT).

THE ROLE OF EXPERT WITNESS

- Seorang profesional forensik digital akan memainkan peran sebagai saksi ahli di pengadilan, namun apa yang membedakan saksi ahli dengan saksi tidak ahli atau saksi konvensional?
- saksi ahli punya kesempatan untuk memberikan pendapatnya kepada pengadilan. Juri dan juri tidak selalu akrab dengan perincian teknis yang terkait dengan kejahatan digital, jadi saksi ahli harus membantu mereka untuk mengasimilasi dan memahami detail teknis ini.
- seorang saksi ahli tidak harus memiliki gelar akademis yang lebih tinggi untuk bersaksi. dia perlu menunjukkan kemampuan teknis yang terbukti dengan jelas yang menunjukkan bahwa dia akan bersaksi mengerti sepenuhnya tentang subjek dia. untuk mengefektifkan keterangan saksi ahli di pengadilan, maka direkomendasikan bahwa ahli ini memiliki kemampuan untuk menyampaikan teknis detail yang rumit untuk sesuatu yang mudah diasimilasi oleh orang-orang nonteknis seperti hakim dan anggota juri.

Rantai Pengawasan (Chain of Custody)

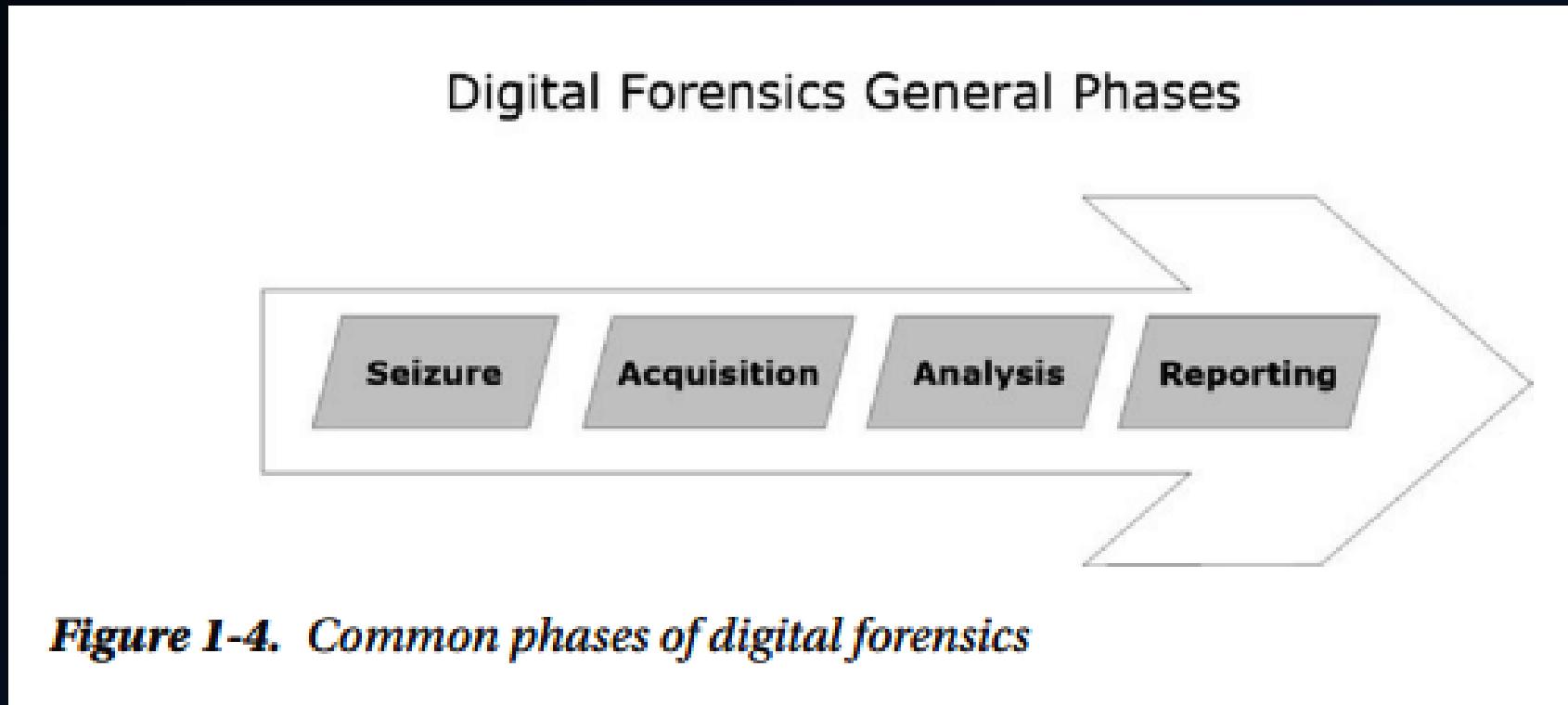
- Rantai pengawasan merupakan bagian integral dari setiap proses investigasi forensik digital.
- Lacak bukti valid harus menyatakan dengan jelas bagaimana bukti digital ditemukan, diperoleh, diangkut, diselidiki (dianalisis), diamankan , dan ditangani antara pihak yang berbeda terlibat dalam penyelidikan.
- Tujuan utamanya adalah untuk memastikan integritas digital bukti dengan mengetahui semua orang yang berhubungan dengan bukti ini dari akuisisi hingga presentasinya di pengadilan. Jika kita gagal memahami siapa yang melakukan kontak dengan bukti selama fase investigasi apa pun, rantai penahanan akan terancam dan bukti yang diperoleh akan menjadi tidak berguna di pengadilan.
- Untuk mempertahankan lacak balak yang benar yang dapat diterima di pengadilan, log audit harus dipelihara untuk semua bukti digital yang diperoleh yang melacak pergerakan dan pemilik bukti digital setiap saat.

Rantai pengawasan yang benar akan memungkinkan penyidik untuk menjawab pertanyaan-pertanyaan berikut di pengadilan:

1. Apa bukti digitalnya? (Misalnya, jelaskan digital yang diperoleh bukti.)
2. Di mana bukti digital ditemukan? (Misalnya, komputer, tablet, ponsel, dll .; juga untuk dimasukkan adalah keadaan komputasi perangkat setelah memperoleh bukti digital—ON atau OFF?)
3. Bagaimana bukti digital diperoleh? (Misalnya, alat yang digunakan; Anda juga perlu menyebutkan langkah-langkah yang diambil untuk menjaga integritas bukti selama fase akuisisi.)
4. Bagaimana bukti digital diangkut, diamankan, dan ditangani?
5. Bagaimana bukti digital diperiksa? (Misalnya, alat apa saja dan teknik yang digunakan.)
6. Kapan bukti digital diakses, oleh siapa dan untuk apa? alasan?
7. Bagaimana bukti digital digunakan selama investigasi?

Proses Pemeriksaan Forensik Digital

- Empat fase utama Proses Pemeriksaan Forensik Digital:
- 1. Penangkapan 2. Akuisisi 3. Analisis 4. Pelaporan



PENDAHULUAN FORENSIC TEKNOLOGI INFORMASI

Introduction

Introduction

About Me



ABOUT US



RULES!

- 1. You SHALL!
- 2. You WILL!
- 3. You MUST!

INTRODUCTION OF WHAT WE WILL LEARN

- Cybercrime
- Forensic Computer
- Definition
- Background
- Example of Forensic Computer Law
- Specification of Forensic Computer
- Implementation of Forensic Computer
- Digital Evidence

WHAT IS ?



PREFERENCE

- “Cybercrime is a bigger risk now than ever before due to the sheer number of connected people and devices”.

Statement of Norton in their website

PREFERENCE

- You often hear the term ‘Cybercrime’ bandied about these days, as it’s a bigger risk now than ever before due to the sheer number of connected people and devices.
- **But What is it Exactly?**



DEFINITION

- It is simply a crime that has some kind of computer or cyber aspect to it.
- **According to Interpol :**

Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual

CYBERCRIME: THE FACTS

- Cybercrime has now surpassed illegal drug trafficking as a criminal moneymaker
- Somebody's identity is stolen every 3 seconds as a result of cybercrime
- Without a sophisticated security package, your unprotected PC can become infected within four minutes of connecting to the Internet.



CYBERCRIME

- Criminal committing cybercrime use a number of methods, depending on their skill-set and their goals.
- **Here are some of different ways cybercrime can take shape:**
 - Theft of personal data
 - Copyright infringement
 - Fraud
 - Child Pornography
 - Cyberstalking
 - Bullying



TYPE OF CYBERCRIME BY NORTON

- The broad range of cybercrime can be better understood by dividing it into two overall categories, defined for the purpose of this research as :
- **Type I and**
- **Type II cybercrime**

TYPE 1 OF CYBERCRIME

- Usually a single event from perspective of the victim. An example would be where the victim unknowingly downloads a Trojan horse virus, which installs a keystroke logger on his or her machine.
- Another common form of Type 1 Cybercrime is phising. This is where the victim receives a supposedly legitimate email (quite often claiming to be a bank or credit card company) with a link that leads to a hostile website. Once the link is clicked, the PC can then be infected with a virus.



TYPE 1 CYBERCRIME

- Hackers often carry out Type 1 cybercrime by taking advantage of flaws in a web browser to place a Trojan horse virus onto the unprotected victims computer.
- Any cybercrime that relates to theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud.



TYPE 2 OF CYBERCRIME



- Type 2 cybercrime tends to be much more serious and covers things such as cyberstalking and harassment (pelecehan), child predation, extortion (pemeraan), stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities.

TYPE 2 OF CYBERCRIME



- It is generally an on-going series of events, involving repeated interactions with the target.
- For example : the target is contacted in a chat room by someone who, over time, attempts to establish a relationship. Eventually, the criminal exploits the relationship to commit a crime. Or, criminal organization may use hidden messages to communicate in a public forum to plan activities or discuss money laundering location.

TYPE 2 OF CYBERCRIME



- More often than not, it is facilitated by programs that do not fit under the classification crimeware.
- For example, conversations may take place using IM (instant messaging) clients or files may be transferred using FTP.

CYBERCRIME ACCORDING INTERPOL

- These crimes can be divided into three broad areas:
 1. Attacks against computer hardware and software, for example, botnets, malware and network intrusion
 2. Financial crimes and corruption, such as online fraud, penetration of online financial services and phishing
 3. Abuse, in the form of grooming or 'sexploitation', especially crimes against children.

KASUS

- Kasus : Erick J Adrinsjah
- Waktu : Novermber 2008
- Pekerjaan : Account Executive Equity di Bahana Securities di Jakarta (Saat Itu)
- Media : E-mail terbatas, kemudian beredar di mailing-list
- Substansi : Informasi pasar (rumor) yang berulm di konfirmasi
- Motivasi : Informasi terbatas kepada klien
- Pelapor : Bank Indonesia dan Bank Artha Graha

KASUS

- Hasil:

Erick ditahan Unit V Cyber Crime Mabes Polri karena dianggap melanggar **UU ITE, Pasal 27 ayat 3 dan Pasal 28 ayat 1** (penyebaran berita bohong melalui sistem elektronik).

KASUS

- Konten: “Market news stated that several Indo bank is having a liquidity problem and fail to complete interbank transaction. These Indo banks include : Bank Panin (PNBN), Bank Bukopin (BBKP), Bank Arta Graha (INPC): Bank CIC (BCIC) dan Bank Victoria (BVIC). We will keep you updated’ (Berita pasar mengabarkan bahwa beberapa bank di Indonesia mendapat masalah likuiditas dan kegagalan dalam menyelesaikan transaksi antarbank.
- Bank tersebut diantaranya : Bank Panin, Bank Bukopin, Bank Arta Graha, Bank CIC, dan bank Victoria)“.
- **Keterangan: diambil dari isi e-mail Erick.**

KASUS

- Konten: “Market news stated that several Indo bank is having a liquidity problem and fail to complete interbank transaction. These Indo banks include : Bank Panin (PNBN), Bank Bukopin (BBKP), Bank Arta Graha (INPC): Bank CIC (BCIC) dan Bank Victoria (BVIC). We will keep you updated’ (Berita pasar mengabarkan bahwa beberapa bank di Indonesia mendapat masalah likuiditas dan kegagalan dalam menyelesaikan transaksi antarbank.
- Bank tersebut diantaranya : Bank Panin, Bank Bukopin, Bank Arta Graha, Bank CIC, dan bank Victoria)“.
- **Keterangan: diambil dari isi e-mail Erick.**

KASUS 2

- Pada tahun 2008, pemerintah AS menangkap lebih dari 100 orang yang diduga terlibat kegiatan pornografi anak. Dari situs yang memiliki 250 pelanggan dan dijalankan di Texas, AS, pengoperasiannya dilakukan di Rusia dan Indonesia. Untuk itulah, Jaksa Agung AS John Ashcroft sampai mengeluarkan surat resmi penangkapan terhadap dua warga Indonesia yang terlibat dalam pornografi yang tidak dilindungi Amandemen Pertama. Di Indonesia, kasus pornografi yang terheboh baru-baru ini adalah kasusnya Ariel-Luna-Cut Tari.

KASUS 2

- Pada tahun 2008, pemerintah AS menangkap lebih dari 100 orang yang diduga terlibat kegiatan pornografi anak. Dari situs yang memiliki 250 pelanggan dan dijalankan di Texas, AS, pengoperasiannya dilakukan di Rusia dan Indonesia. Untuk itulah, Jaksa Agung AS John Ashcroft sampai mengeluarkan surat resmi penangkapan terhadap dua warga Indonesia yang terlibat dalam pornografi yang tidak dilindungi Amandemen Pertama. Di Indonesia, kasus pornografi yang terheboh baru-baru ini adalah kasusnya Ariel-Luna-Cut Tari.

KASUS 2

- **Undang-Undang :**
- Pasal 26: Setiap orang dilarang menyebarkan informasi elektronik yang memiliki muatan pornografi, pornoaksi, perjudian, dan atau tindak kekerasan melalui komputer atau sistem elektronik. (*Pidana 1 tahun dan denda Rp 1 miliar*)

Spesifikasi Hardware untuk Sistem Komputer Forensik

SPESIFIKASI KOMPUTER FORENSIK

- Seorang yang bekerja di bidang komputer forensik dalam mempertahankan keaslian atau melakukan analisis terhadap **e-evidence**, memerlukan sistem komputer, yaitu hardware dan software yang khusus dalam melakukan analisinya.
- Tanpa menggunakan sistem komputer yang memadai, seorang ahli forensik tidak dapat banyak melakukan analisis.

SPESIFIKASI KOMPUTER FORENSIK

- **Ilustrasi Hardware Komputer Forensik**



SPESIFIKASI KOMPUTER FORENSIK

- Fungsi-fungsi dasar yang dapat dilakukan dari sebuah sistem **komputer forensik** adalah :
 1. Membuat sebuah kopi yang akurat dari harddisk ke harddisk lainnya atau ke dalam sebuah image file.

SPESIFIKASI KOMPUTER FORENSIK

2. Membuat sebuah kopi yang akurat dari harddisk ke sebuah media penyimpanan yang sifatnya removable atau portabel.
3. Melakukan analisis terhadap suatu media atau image file.

SPESIFIKASI KOMPUTER FORENSIK

- Sistem komputer forensik ini membutuhkan rancangan hardware dalam proses analisis dan investigasi dilakukan.
- Spesifikasi hardwarenya sebagai berikut:

SPESIFIKASI KOMPUTER FORENSIK

- Sebuah processor paling rendah Pentium IV dual core dengan hyper treading (3.2 GHz) dan paling tinggi adalah processor yang banyak dipasaran yaitu Intel Core i3, i5, dan i7. Bisa juga processor AMD. Sangat direkomendasikan untuk membeli processor 64 bit.
- Untuk motherboard menggunakan jenis socket terbaru.
- Tiga hingga lima slot PCI.
- Dua port controller EIDE ATA/100 atau ATA/133.
- Port controller untuk disk drive 3.5”

SPESIFIKASI KOMPUTER FORENSIK

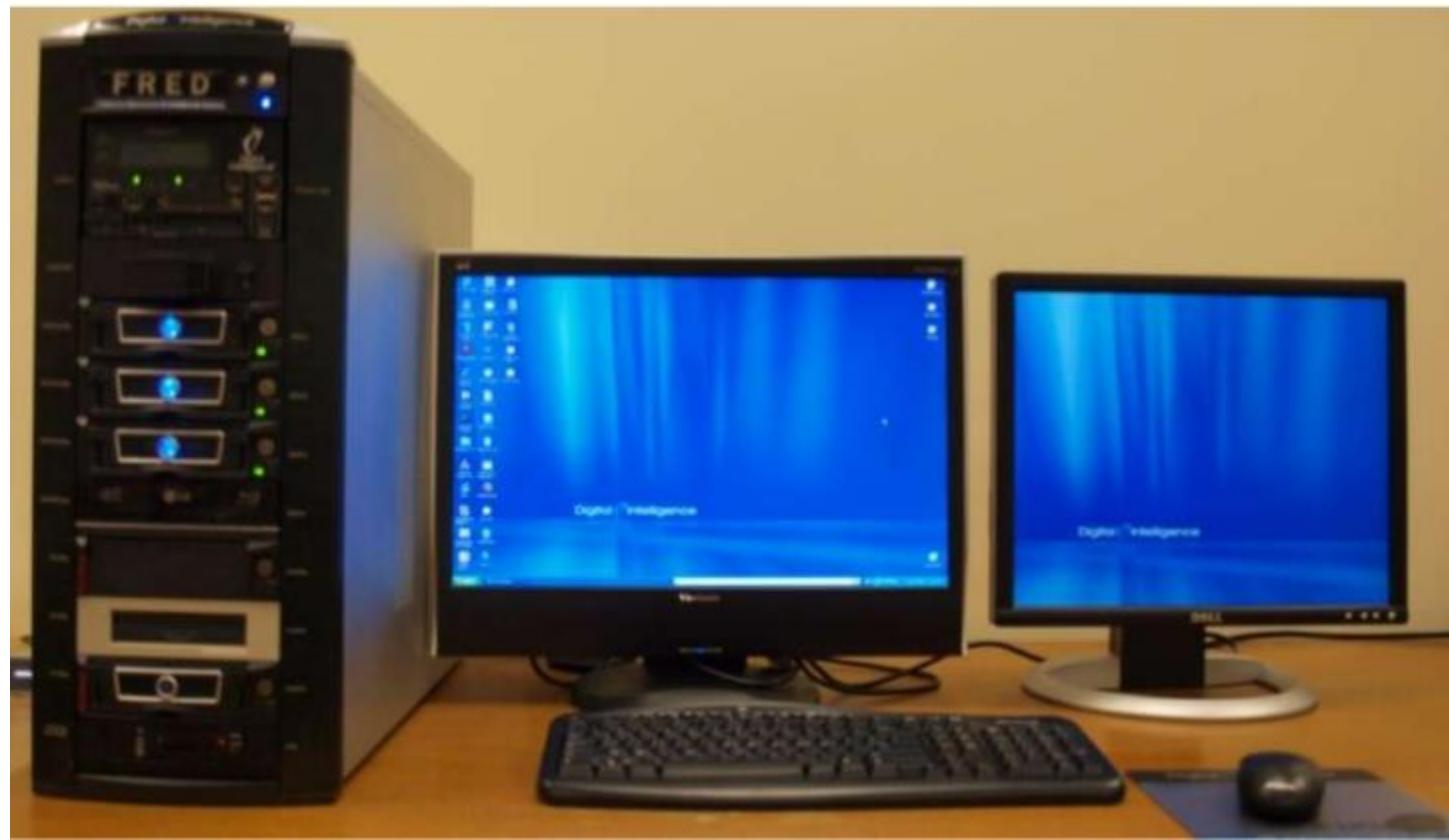
- Beberapa paket perangkat yang dapat digunakan untuk menunjang proses analisis lainnya adalah:

Forensic Recovery of Evidence Device (FRED), sebuah workstation forensik dari Digital Intelligence yang menawarkan sistem terintegrasi untuk keperluan analisis data pada komputer forensik. FRED menggabungkan hampir segala macam interface pada sebuah workstation sehingga tidak perlu membongkar pasang perangkat saat melakukan analisis. Selain itu, beberapa paket software yang ditawarkan EnCase, FTK, Paraben's P2, dan banyak lainnya.

SPESIFIKASI KOMPUTER FORENSIK

SUOLAIR

FRED (Forensic Recovery Evidence Device: Digital Intelligence)
Software: FTK suite (AccessData) - EnCase



SPESIFIKASI KOMPUTER FORENSIK

- **WiebeTech Forensic Field Kit**, yang ditawarkan oleh WiebeTech, sebenarnya merupakan beberapa kumpulan perangkat yang mudah dibawa dan berdaya guna dalam melakukan analisis.
- Sebut saja USB Writeblocker yang digunakan untuk mencegah terjadinya penulisan terhadap USB Flash disk yang hendak dianalisis, 8 TrayFree SataTMBays yang digunakan untuk memudahkan dalam memasang harddisk SATA, Forensic UltradocTM v4 yang digunakan untuk membuat image serta mencegah penulisan terhadap media yang hendak dianalisis dengan berbagai macam interface (USB 2.0, eSATA, FireWire 800) atau Drive EraserTM yang berguna untuk menghapus seluruh isi harddisk tanpa menggunakan komputer.

SPESIFIKASI KOMPUTER FORENSIK



SPESIFIKASI KOMPUTER FORENSIK



- CRU / Wiebetech
Forensic Field Kit G-0

SPESIFIKASI KOMPUTER FORENSIK

- **Logicube**, menawarkan sebuah perangkat transfer disk-to-disk dan disk-to-image yang tercepat di pasaran. Dengan semakin bertambahnya kapasitas penyimpanan, maka transfer dengan kecepatan 6 GB per menit akan dapat menghemat waktu kerja.

SPESIFIKASI KOMPUTER FORENSIK

- Beberapa produk yang menjadi andalan dari **Logicube** adalah **SuperSonix®**, **OmniSAS** yang memungkinkan untuk menggandakan harddisk ke lima target sekaligus, dan **OmniWipe** yang digunakan untuk menghapus isi tiga harddisk sekaligus dengan tipe berbeda-berbeda.

SPESIFIKASI KOMPUTER FORENSIK



SPESIFIKASI KOMPUTER FORENSIK

- Logicube OmniSAS
5 Hard Drive
Duplicator 1 TO 5
SAS/SATA



SOFTWARE UNTUK KOMPUTER FORENSIK

SOFTWARE FORENSIK

- Software-software yang digolongkan menjadi beberapa kategori, yaitu software untuk duplikasi drive, software untuk pemroses citra dan software untuk keperluan lain-lain. Produk software yang dikhususkan untuk keperluan **komputer forensik** adalah:

SOFTWARE FORENSIK

- Software-software yang digolongkan menjadi beberapa kategori, yaitu software untuk duplikasi drive, software untuk pemroses citra dan software untuk keperluan lain-lain. Produk software yang dikhususkan untuk keperluan **komputer forensik** adalah:

SOFTWARE FORENSIK

EnCase Forensic

File Edit View Tools Help

New Open Save Print Add Device Search Refresh Find

Cases Bookmarks Home Bookmarks Protected Files

Table Report Gallery Timeline Disk Code

| | Name | Comment |
|----|-------------------|------------------------------------------------------------------------------------------|
| 7 | a8-openpass.pdf | Type: Acrobat 7.0, Protection: Open Password, Permissions Password, AES Encryption |
| 8 | a9-metadata.pdf | Type: Acrobat 9.0, Protection: Open Password, Permissions Password, AES Encryption |
| 9 | a9-mixed.pdf | Type: Acrobat 9.0, Protection: Open Password, Permissions Password, AES Encryption |
| 10 | a9-openpwd.pdf | Type: Acrobat 9.0, Protection: Open Password, Permissions Password, AES Encryption |
| 11 | a9-permpwd.pdf | Type: Acrobat 9.0, Protection: Permissions Password, AES Encryption, Low Resolution |
| 12 | a9-ru-openpwd.pdf | Type: Acrobat 9.0, Protection: Open Password, Permissions Password, AES Encryption |
| 13 | a9-ru-twopwds.pdf | Type: Acrobat 9.0, Protection: Open Password, Permissions Password, AES Encryption |
| 14 | a9-twopwds.pdf | Type: Acrobat 9.0, Protection: Open Password, Permissions Password, AES Encryption |
| 15 | Document1.pdf | Type: Acrobat 3.0, Protection: Open Password, Permissions Password, RC4 Encryption |
| 16 | Document3.pdf | Type: Acrobat 3.0, Protection: Permissions Password, RC4 Encryption, Decryption required |

Text Hex Doc Transcript Picture Report Console Details Output Log EnScript Filters Con

File: Case 1\C\pk-test-cases\acbtkey\aa-(empty).pdf
Type: Acrobat 6.0
Protection: Permissions Password, RC4 Encryption, Printing Not Allowed
Decryption: Instant Unprotection, File patching required

File: Case 1\C\pk-test-cases\acbtkey\aa-daniil.pdf

EnScript Examples Forensic Include Main

SOFTWARE FORENSIK

- **EnCase** telah digunakan oleh banyak organisasi dan menjadi standar dalam investigasi komputer forensik.
- Merupakan suatu paket software produksi Guidance Software yang terdiri dari EnCase Enterprise, EnCase Forensic Edition, EnCase eDiscovery (untuk melakukan pencarian data tertentu pada suatu media), dan EnCase Lab Edition.

SOFTWARE FORENSIK

- Forensic Toolkit (FTK)

AccessData, sebuah pengembang software telah membuat software forensik yang amat mudah dalam pengoperasiannya dan relatif tidak mahal. Beberapa fitur umum dari software FTK ini adalah:

SOFTWARE FORENSIK

- Pembuatan image, melakukan analisis registry, mendeskripsi file, mengidentifikasi adanya pesan dalam suatu citra (steganografi), dan memberikan pelaporan.
- Kemampuan dalam mengembalikan password untuk lebih dari 80 aplikasi dengan memanfaatkan waktu idle CPU.
- Engine pencarian data dalam suatu media yang mendukung regular expression.

ORENSIK



Overview Explore Graphics E-Mail Search Bookmark

| Evidence Items | | File Status | | File Category | |
|---------------------|--------------|--------------------|---|-------------------|---|
| Evidence Items: | 1 | KFF Alert Files: | 0 | Documents: | 0 |
| | | Bookmarked Items: | 0 | Spreadsheets: | 0 |
| Total File Items: | 5 | Bad Extension: | 0 | Databases: | 0 |
| Checked Items: | 0 | Encrypted Files: | 0 | Graphics: | 0 |
| Unchecked Items: | 5 | From E-mail: | 0 | Multimedia: | 0 |
| Flagged Thumbnails: | 0 | Deleted Files: | 0 | E-mail Messages: | 0 |
| Other Thumbnails: | 0 | From Recycle Bin: | 0 | Executables: | 0 |
| Filtered In: | 5 | Duplicate Items: | 0 | Archives: | 0 |
| Filtered Out: | 0 | OLE Subitems: | 0 | Folders: | 0 |
| Unfiltered | Filtered | Flagged Ignore: | 0 | Slack/Free Space: | 5 |
| All Items | Actual Files | KFF Ignorable: | 0 | Other Known Type: | 0 |
| | | Data Carved Files: | 0 | Unknown Type: | 0 |

| File Data View | | | | | | | | | | | | | | | |
|----------------|---------|--------|--------------|------------|-------------------|-----------|----------|---------|---------|----------|-------|--------|------------|-----------|-----------|
| File Number | Cluster | Length | Start Sector | End Sector | Allocation Status | File Type | Category | Subject | Cr Date | Mod Date | Owner | Access | Protection | File Name | File Path |
| 00000000 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00-00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000010 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00-00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000020 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00-00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000030 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00-00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000040 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00-00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000050 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00-00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000060 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00-00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000070 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00-00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000080 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00-00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000090 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00-00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000a0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00-00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000b0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00-00 | 00 | 00 | 00 | 00 | 00 | 00 | |

Cursor position = 0; cluster = 0; physical sector = 0

| File Name | Full Path | Recycle Bi... | Ext | File Type | Category | Subject | Cr Date | Mod Date |
|-----------------|--------------------------------------|---------------|-----|-----------------|-----------------|---------|---------|----------|
| DriveFreeSpace1 | Disk1\NONAME-Unknown\DriveFreeSpace1 | | | Drive Free S... | Slack/Free S... | | N/A | N/A |
| DriveFreeSpace2 | Disk1\NONAME-Unknown\DriveFreeSpace2 | | | Drive Free S... | Slack/Free S... | | N/A | N/A |
| DriveFreeSpace3 | Disk1\NONAME-Unknown\DriveFreeSpace3 | | | Drive Free S... | Slack/Free S... | | N/A | N/A |
| DriveFreeSpace4 | Disk1\NONAME-Unknown\DriveFreeSpace4 | | | Drive Free S... | Slack/Free S... | | N/A | N/A |
| DriveFreeSpace5 | Disk1\NONAME-Unknown\DriveFreeSpace5 | | | Drive Free S... | Slack/Free S... | | N/A | N/A |



UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Teknik Informatika

Profesi Ahli Forensik TI

Pengantar Komputer Forensik Teknologi Informasi



lahuluan

- ▶ Meningkatnya kejahatan dibidang TI, menyebabkan profesi atau keahlian yang berkaitan dengan masalah pengungkapan adanya kejahatan ini dibutuhkan.
- ▶ Seorang analisis forensik dalam pekerjaannya membantu penegak hukum atau pimpinan keamanan perusahaan



langan Ahli

- ▶ Menurut James O. Holly [National computer forensics lab Ernst & Young]
 - ▶ Anda perlu membuka pintu untuk pemrosesan administratif, sipil atau kriminal dan merespon kejadian komputer, dan penyelidik perlu menangani insiden dari awal sampai masuk kepersidangan
- ▶ www.pcforensics.com
 - ▶ Data yang sudah dihapus masih bisa dihidupkan lagi



langan Ahli

- ▶ Menurut Thomas Welch [The information security management handbook]
- ▶ Praktisi keamanan komputer harus mempedulikan teknologi dan faktor legal yang berdampak pada sistem dan penggunanya, termasuk masalah penyelidikan dan penegakan hukum





Programmer vs Ahli Komputer Forensik

- ▶ **Programmer ;**
 - ▶ Bekerja melawan diri sendiri
 - ▶ Memcoba memperbaiki permasalahan yang kita buat sendiri
- ▶ **Ahli Komputer Forensik**
 - ▶ Bekerja menyelesaikan kejadian komputer
 - ▶ Melawan seorang “programmer”



Ilian Komputer Forensik tuhkan oleh :

- ▶ Jaksa Penuntut mempergunakan barang bukti komputer dalam kejahatan yang bermacam-macam, seperti obat bius, pornografi anak, pembunuhan, dan penggelapan keuangan
- ▶ Detektif swasta bisa mempergunakan rekaman pada sistem komputer untuk melacak kasus penggelapan, perceraian, diskriminasi dan pelecehan.
- ▶ Perusahaan asuransi bisa mengurangi biaya dengan bukti komputer yang menyatakan kemungkinan penggelapan pada insiden, kebakaran, atau kompensasi pekerja



Julian Komputer Forensik dilakukan oleh :

- ▶ Perusahaan menyewa ahli komputer forensik untuk menentukan bukti yang berkaitan dengan pelecehan seksual, penipuan, pencurian rahasia dagang, dan informasi rahasia internal lainnya
- ▶ Petugas penegak hukum sering memerlukan bantuan dalam persiapan penggeledahan dan penyitaan perangkat komputer.
- ▶ Perorangan kadang menyewa ahli komputer forensik untuk mendukung klaim pemutusan kerja, pelecehan seksual atau dikriminasi umur.



GETAHUAN YANG DIPERLUKAN AHLI ENSIK

- ▶ Dasar-dasar hardware dan pemahaman bagaimana umumnya sistem operasi bekerja
- ▶ Bagaimana partisi drive, *hidden partition*, dan di mana tabel partisi bisa ditemukan pada sistem operasi yang berbeda
- ▶ Bagaimana umumnya *master boot record* tersebut dan bagaimana *drive geometry*
- ▶ Pemahaman untuk *hide*, *delete*, *recover* file dan directory bisa mempercepat pemahaman pada bagaimana tool forensik dan sistem operasi yang berbeda bekerja.
- ▶ Familiar dengan header dan ekstension file yang bisa jadi berkaitan dengan file tertentu



TERIA AHLI FORENSIK

- ▶ Menurut Peter Sommer [Virtual City Associates Forensic Technician]
 - ▶ Metode yang berhati-hati pada pendekatan pencatatan rekaman
 - ▶ Pengetahuan komputer, hukum dan prosedur legal
 - ▶ Keahlian untuk mempergunakan utility
 - ▶ Kepedulian teknis dan memahami implikasi teknis dari setiap tindakan



TERIA AHLI FORENSIK

- ▶ Penguasaan bagaimana modifikasi bisa dilakukan pada data
- ▶ Berpikiran terbuka dan mampu berpandangan jauh
- ▶ Etika yang tinggi
- ▶ Selalu belajar
- ▶ Selalu mempergunakan data dalam mengambil kesimpulan



ivitas Penyelidik Forensik

- ▶ Perlindungan sistem komputer selama pengujian forensik dari semua kemungkinan perubahan, kerusakan, korupsi data, atau virus
- ▶ Temukan semua file pada sistem. Termasuk file normal, terhapus, *hidden*, *password-protected*, dan terenkripsi.
- ▶ *Recovering* file terhapus sebisa mungkin.
- ▶ Ambil isi file *hidden* juga file *temporary* atau *swap* yang dipergunakan baik oleh sistem operasi atau program aplikasi
- ▶ Lakukan akses (jika dimungkinkan secara legal) isi dari file terproteksi atau terenkripsi



ivitas Penyelidik Forensik

- ▶ Analisa semua data yang relevan pada area spesial di disk. Misal *unallocated* (tidak terpakai, tapi mungkin menyimpan data sebelumnya), *slack space* (area di akhir file pada *last cluster* yang mungkin menyimpan data sebelumnya juga)
- ▶ Cetak semua analisis keseluruhan dari sistem komputer, seperti halnya semua file yang relevan dan ditemukan. Berikan pendapat mengenai layout sistem, struktur file yang ditemukan, dan informasi pembuat, setiap usaha menyembunyikan, menghapus, melindungi, mengenkripsi informasi, dan lainnya yang ditemukan dan nampak relevan dengan keseluruhan pengujian sistem komputer.
- ▶ Berikan konsultasi ahli dan kesaksian yang diperlukan



AKTERISTIK SEORANG AHLI FORENSIK

- Pendidikan, pengalaman dan sertifikasi merupakan kualifikasi yang baik untuk profesi komputer forensik. Pendidikan dengan pengalaman memberikan kepercayaan yang diperlukan untuk membuat keputusan dan mengetahui keputusan yang tepat. Sertifikasi menunjukkan bahwa pendidikan dan pengalamannya merupakan standar yang tinggi dan dapat dipahami.
- Yakinkan pada setiap tindakan dan keputusan, agar mencukupi untuk kesaksian di pengadilan
- Semua proses dilakukan dengan menyeluruh
- Memiliki pengetahuan yang banyak mengenai bagaimana *recover* data dari berbagai tipe media



AKTERISTIK SEORANG AHLI ENSIK

- Mampu memecah password dari aplikasi dan sistem operasi yang berbeda dan mempergunakannya untuk penyelidikan
- Perlu pengetahuan yang memadai, tanpanya bisa terjadi kesalahan yang akan membuat barang bukti ditolak di pengadilan. Barang bukti bisa dirusak, diubah, atau informasi yang berharga terlewat.
- Obyektif dan tidak bias, harus *fair* pada penyelidikan, dengan fakta yang akurat dan lengkap
- Inovatif dan memiliki kemampuan interpersonal yang baik
- Memiliki kemampuan verbal dan oral yang baik
- Menggunakan penalaran dan logika yang tepat



CERTIFIKASI AHLI FORENSIK TI

- ▶ EnCase Certified Examiner Program (EnCE)
<http://www.iacis.com>
- ▶ Computer Forensics External Certification (CCE)
<http://www.giac.org/certifications/security/gcfa.php>
- ▶ GCFA – GIAC Certified Forensics Analyst
<http://www.giac.org/certifications/security/gcfa.php>
- ▶ Q/FE Qualified Forensics Expert
<http://www.securityuniversity.net/certification.htm>
- ▶ TruSecure ICSA Certified Security Associate
<http://www.icsalabs.com>
- ▶ CCE – Certified Computer Examiner <http://www.certified-computer-examiner.com/>
- ▶ Computer Forensic Training Online
http://www.kennesaw.edu/coned/sci/for_online.htm



mpulan

- ▶ Ahli komputer forensik merupakan suatu bidang pekerjaan yang akan banyak dibutuhkan
- ▶ Ahli komputer forensik merupakan area kerja relatif baru dan akan berkembang
- ▶ Ahli komputer forensik dibutuhkan keahlian khusus, pengalaman dan jam terbang



mpulan

3. Analis Komputer Forensik

- ▶ Komputer forensik adalah analisis informasi yang terkandung dalam dan dibuat dengan sistem komputer dan perangkat komputasi. Analis komputer forensik sering berkontribusi untuk investigasi kriminal kerah putih dan menyelidiki penyebab kebocoran komputer, sistem penyalahgunaan komputer, atau rincian kejahatan yang terkandung dalam sistem komputer.

- ▶ **Analis Komputer Forensik pemula akan menerima gaji rata-rata US\$ 47,700+**

<http://www.sahacrash.com/2013/10-profesi-dengan-gaji-tertinggi.html>



na Kasih





UNIVERSITAS GUNADARMA
Fakultas Teknik Industri
Jurusan Teknik Informatika

KOMPUTER FORENSIK DALAM HUKUM INDONESIA

Pengantar Komputer Forensik Teknologi Informasi



FORENSIK TI DALAM HUKUM INDONESIA

PENGERTIAN / UNSUR HUKUM

Ada beberapa pendapat mengenai pengertian hukum, dari beberapa pengertian tersebut hukum itu meliputi **beberapa unsur** sbb :

1. Aturan tentang tingkah laku masyarakat;
2. Dibuat oleh yang berwajib / berwenang ;
3. Berisi perintah dan larangan;
4. Bersifat memaksa;
5. Terhadap pelanggaran ada sanksi yang tegas.

TUJUAN HUKUM adalah menjamin adanya kepastian hukum dalam masyarakat yang bersendikan keadilan.



KATEGORI HUKUM

Hukum menurut isinya :

- **Hukum Privat (Hukum Sipil)**, hukum yang mengatur hubungan / kepentingan antar perseorangan. Contoh ; Hukum Perdata, Hukum Dagang.
- **Hukum Publik (Hukum Negara)**, hukum yang mengatur hubungan antara Negara dengan alat perlengkapan negara atau perseorangan (warga-negara). Contoh ; Hukum Pidana, Hukum Tata Negara.



KATEGORI HUKUM

Hukum menurut cara mempertahankannya :

- **Hukum Material**, hukum yang berisi peraturan berupa perintah dan larangan. Contoh ; Hukum Pidana (KUHPidana), Hukum Perdata (KUHPerdata).
- **Hukum Formal (Hukum Proses atau Hukum Acara)**, hukum yang memuat peraturan tentang cara melaksanakan dan mempertahankan Hukum Material, yaitu cara-cara mengajukan suatu perkara ke Pengadilan hingga Putusan Hakim. Contoh ; Hukum Acara Pidana (KUHAPidana), Hukum Acara Perdata (KUHAPerdata).
- **Forensik TI dikategorikan sebagai bagian dari Hukum Acara Pidana**, karena memuat tentang cara-cara/ prosedur pembuktian terjadinya suatu pelanggaran / kejahatan di bidang TI agar dapat diajukan ke Pengadilan untuk mendapatkan Putusan Hakim.



Kebijakan penanggulangan kejahatan (cybercrime) dengan Hukum Pidana perlu memperhatikan hal-hal sbb : (Mas Wigrantoro Roes Setiyadi, 2000)

1. Materi / substansi :

Apa saja yang dapat dinamakan sebagai tindak pidana di bidang TI.

2. Kebijakan Formulasi

Apakah peraturan hukuman pidana bagi kejahatan bidang TI akan berada di dalam atau di luar KUHP.

Kebijakan Hukum Pidana :

Kriminalisasi :

Suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana) (Barda Nawawi Arief, 2003)



Asas Legalitas (*Principle of Legality*) :

Asas yang menentukan bahwa tidak ada perbuatan yang dilarang dan diancam dengan pidana jika tidak ditentukan terlebih dahulu dalam perundang-undangan (Moeljatno, 2000)

Asas berlakunya hukum pidana menurut tempat (Pasal 2 – 9 KUHP) :

a. Asas Teritorial

UU Hukum Pidana Indonesia berlaku terhadap setiap orang yang melakukan pelanggaran / kejahatan di dalam wilayah RI.

b. Asas Nasional Aktif

UU Hukum Pidana Indonesia berlaku juga bagi warga negara Indonesia yang berada di luar negeri.

c. Asas Nasional Pasif

UU Hukum Pidana Indonesia berlaku bagi WNI maupun WNA diluar RI. Disini kepentingan hukum suatu negara yang dilanggar, misal : pemalsuan uang Indonesia, materai, cap negara dll

d. Asas Universal

UU Hukum Pidana Indonesia dapat juga diberlakukan thd perbuatan jahat yang bersifat merugikan keselamatan internasional



Kebijakan Formulasi terhadap tindak pidana mayantara :

1. Kejahatan biasa diatur dalam KUHP

Jika tindak pidana mayantara merupakan kejahatan biasa (ordinary crime) yang dilakukan dengan komputer teknologi tinggi (high-tech), penanggulangannya cukup dengan KUHP, baik melalui amandemen KUHP maupun perubahan KUHP secara menyeluruh.

2. Kejahatan baru diatur dalam UU Khusus

Jika tindak pidana mayantara dianggap sebagai kejahatan kategori baru (new category of crime) yang membutuhkan suatu kerangka hukum yang baru dan komprehensif untuk mengatasi sifat khusus teknologi yang sedang berkembang dan tantangan baru yang tidak ada pada kejahatan perlu diatur secara tersendiri di luar KUHP.



Peraturan mengenai Cybercrime / Kejahatan mayantara di Indonesia

1. KONSEP KUHP YANG BARU (RUU KUHP)

a. Buku I (Ketentuan Umum)

Pasal 174 :

“Barang adalah benda berwujud termasuk air dan uang giral, dan benda tidak berwujud termasuk listrik, gas, data dan program komputer, jasa, jasa telepon, jasa telekomunikasi, atau jasa komputer.”

Pasal 178 :

“Anak kunci adalah alat yang digunakan untuk membuka kunci, termasuk kode rahasia, kunci masuk komputer, kartu magnetik, atau signal yang telah diprogram yang dapat digunakan untuk membuka sesuatu oleh orang yang diberi hak untuk itu.”

Pasal 188 :

“Surat adalah selain surat yang tertulis di atas kertas, juga surat atau Data yang tertulis atau tersimpan dalam disket, pita magnetik, atau media penyimpanan komputer atau media penyimpanan data elektronik lain.”



Pasal 189 :

"Ruang adalah bentangan atau terminal komputer yang dapat diakses dengan cara-cara tertentu."

Pasal 190 :

"Masuk adalah termasuk mengakses komputer atau masuk ke dalam sistem komputer."

Pasal 191 :

"Jaringan Telepon adalah termasuk jaringan komputer atau sistem komunikasi komputer."

b. Buku II Konsep KUHP

Pasal 263 : menyadap pembicaraan di ruangan tertutup dengan alat bantu teknis

Pasal 264 : memasang alat bantu teknis untuk tujuan mendengar/ merekam pembicaraan

Pasal 266 : merekam gambar dengan alat bantu teknis di ruangan tidak untuk umum

Pasal 546 : Merusak/ membuat tidak dapat dipakai bangunan untuk sarana/ prasarana pelayanan umum (a.l. bangunan telekomunikasi/ komunikasi lewat satelit/ komunikasi jarak jauh)

Pasal 641-642 : Pencucian uang



2. UU KHUSUS CYBERCRIME / KEJAHATAN MAYANTARA

a. RUU TIPITI (Tindak Pidana Di Bidang Teknologi Informasi)

Hal- hal yang merupakan **Pelanggaran** dalam Undang-Undang ini (Bab V):

1. MemanfaatkanTeknologi Informasi dengan melawan hukum.
2. Melakukan intersepsi dengan melawan hukum.
3. Sengaja dan melawan hukum merusak atau mengganggu data yang tersimpan dalam alat penyimpan data elektronik yang tersusun sebagai bagian dari sistem komputer.
4. Sengaja menghilangkan bukti–bukti elektronik yang dapat dijadikan alat bukti sah di pengadilan yang terdapat pada suatu sistem informasi atau sistem komputer.
5. Sengaja merusak atau mengganggu sistem informasi, sistem komputer, jaringan komputer, dan Internet.



2. UU KHUSUS CYBERCRIME / KEJAHATAN MAYANTARA

1. Memanfaatkan Teknologi Informasi untuk menipu, menghasut, memfitnah, menjatuhkan nama baik seseorang atau organisasi.
2. Memanfaatkan Teknologi Informasi untuk menyebarkan gambar, tulisan atau kombinasi dari keduanya yang mengandung sifat – sifat pornografi.
3. Memanfaatkan Teknologi Informasi untuk membantu terjadinya percobaan, atau persekongkolan yang menjurus pada kejahatan.
4. Setiap badan hukum penyelenggara jasa akses Internet atau penyelenggara layanan Teknologi Informasi, baik untuk keperluan komersial maupun keperluan internal perusahaan, dengan sengaja tidak menyimpan atau tidak dapat menyediakan catatantransaksi elektronik sedikitnya untuk jangka waktu 2 tahun.



2. UU KHUSUS CYBERCRIME / KEJAHATAN MAYANTARA
 - a. **RUU TIPITI** (Tindak Pidana Di Bidang Teknologi Informasi)
 - **Pelanggaran Pemanfaatan Teknologi Informasi** (Bab VI)
 - Pasal 9 : Kejahatan terhadap nyawa dan keselamatan negara
 - Pasal 10 : Pencurian
 - Pasal 11 : Mengakses tanpa hak
 - Pasal 12 : Mengakses tanpa hak terhadap sistem informasi strategis
 - Pasal 13 : Pemalsuan identitas
 - Pasal 14 : Mengubah dan memalsukan data
 - Pasal 15 : Mengubah data yang merugikan orang lain
 - Pasal 16 : Perbuatan asusila
 - Pasal 17 : Pornografi anak - anak
 - Pasal 18 : Bantuan kejahatan
 - Pasal 19 : Mengakses tanpa hak terhadap komputer yang dilindungi
 - Pasal 20 : Teror



- a. RUU TIPITI (Tindak Pidana Di Bidang Teknologi Informasi)
 - **Tindak Pidana Yang Berkaitan Dengan Teknologi Informasi Sebagai Sasarannya (Bab VII) :**
 - Pasal 21 : Intersepsi
 - Pasal 22 : Merusak Situs Internet
 - Pasal 23 : Penyadapan Terhadap Jaringan Komunikasi Data
 - Pasal 24 : Pemalsuan Nomor Internet Protocol
 - Pasal 25 : Merusak Database atau Enkripsi
 - Pasal 26 : Penggunaan Nama Domain Tidak Sah
 - Pasal 27 : Penyalah-gunaan Surat Elektronik
 - Pasal 28 : Pelanggaran Hak Cipta.
 - Pasal 29 : Pelanggaran Hak Privasi



b. UU ITE (Informasi dan Transaksi Elektronik) No. 11 Th. 2008

- Bab I Ketentuan Umum
- Bab II Asas dan Tujuan
- Bab III Informasi, Dokumen dan Tanda Tangan Elektronik
- Bab IV Penyelenggaraan Sertifikasi Elektronik dan Sistem Elektronik
- Bab V Transaksi Elektronik
- Bab VI Nama Domain, Hak Kekayaan Intelektual dan Perlindungan Hak Pribadi
- Bab VII Perbuatan yang Dilarang
- Bab VIII Penyelesaian Sengketa
- Bab IX Peran Pemerintah dan Peran Masyarakat
- Bab X Penyidikan
- Bab XI Ketentuan Pidana
- Bab XII Ketentuan Peralihan
- Bab XIII Ketentuan Penutup



PERATURAN INTERNASIONAL MENGENAI CYBER LAW :

1. Konvensi tentang Kejahatan Cyber (Convention on Cyber Crime)

oleh Uni Eropa (Council of Europe) di Budapest, Hongaria pada tgl 23 November 2001 mengatur tentang delik mayantara sbb: (Mardjono Reksodiputro, 2002:3-4)

- a. Delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer termasuk didalamnya: mengakses sistem komputer tanpa hak, tanpa hak menangkap/mendengar pengiriman dan pemancaran, tanpa hak merusak data, tanpa hak mengganggu sistem, menyalahgunakan perlengkapan.
- b. Delik-delik yang berhubungan dengan komputer (pemalsuan dan penipuan dengan komputer)
- c. Delik-delik yang bermuatan pornografi anak
- d. Delik-delik yang berhubungan dengan hak cipta.



PERATURAN INTERNASIONAL MENGENAI CYBER LAW :

- 2. Komisi Franken** tahun 1987 dan Kaspersen dari Belanda merumuskan sembilan bentuk penyalahgunaan komputer :
 - a. Tanpa hak memasuki sistem komputer
 - b. Tanpa hak mengambil data komputer
 - c. tanpa hak mengetahui
 - d. tanpa hak menyelin
 - e. tanpa hak mengubah
 - f. mengambil data
 - g. tanpa hak mempergunakan peralatan
 - h. sabotase sistem komputer
 - i. mengganggu telekomunikasi.

- 3. Resolusi PBB No, 55 / 63**

Berisi tentang memerangi tindakan kriminal penyalah-gunaan TI

- 4. APEC (Asia Pasific Economy Cooperation) Cybercrime Strategy**



BEBERAPA CONTOH CYBERLAW

MALAYSIA :

- Computer Crime Act (Akta Kejahatan Komputer) 1997
- Communication and Multimedia Act (Akta Komunikasi dan Multimedia) 1998
- Digital Signature Act (Akta Tandatangan Digital) 1997



BEBERAPA CONTOH CYBERLAW

SINGAPORE :

- The Electronic Act (Akta Elektronik) 1998
- Electronic Communication Privacy Act (Akta Privasi Komunikasi Elektronik) 1996



BEBERAPA CONTOH CYBERLAW

AMERIKA :

- US Child Online Protection Act (COPA) : Adult verification required on porn sites.
- US Child Pornography Protection Act : Extend law to include computer — generated child porn.
- US Child Internet Protection Act (CIPA) : Requires Schools & Libraries to filter
- US New Laws and Rulemaking : Spam, Deceptive Marketing Tactics, Mouse trapping

Terima Kasih

20





**UNIVERSITAS
GUNADARMA**

Fakultas Teknologi Industri
Jurusan Teknik Informatika

Metode Komputer Forensik

Pengantar Komputer Forensik Teknologi Informasi



Pemodelan Forensik

- ▶ Model forensik melibatkan tiga komponen :
 - ▶ Manusia [People]
 - ▶ Peralatan [Equipment]
 - ▶ Aturan [Protocol]



Manusia

- ▶ Manusia berhubungan dengan brainware
- ▶ Kriteria :
 - ▶ Computer forensic examiner
 - ▶ Computer investigator
 - ▶ Digital evidence collection specialist



Computer Forensic Examiner

- ▶ Melakukan pengujian terhadap media original
- ▶ Mengekstrak data bagi investigator untuk di review
- ▶ Dibutuhkan 4 sampai 6 minggu pelatihan



Computer Investigator

- ▶ Harus memiliki pengalaman yang sudah teruji dan ahli
- ▶ Memahami jaringan komputer, internet, komunikasi dan teknologi komputer dan informasi
- ▶ Dibutuhkan sampai 2 minggu pelatihan



Digital evidence collection specialist

- ▶ Sebagai first responder
- ▶ Mendapatkan dan menghadirkan bukti komputer mencakup media penyimpanan
- ▶ Dibutuhkan 2 sampai 3 hari pelatihan



Peralatan

- ▶ Dibutuhkan peralatan guna mendapatkan bukti – bukti (evidence) yang berkualitas dan bersih
- ▶ Jenis peralatan :
 - ▶ Perangkat lunak
 - ▶ Perangkat keras
 - ▶ Media penyimpanan



Aturan

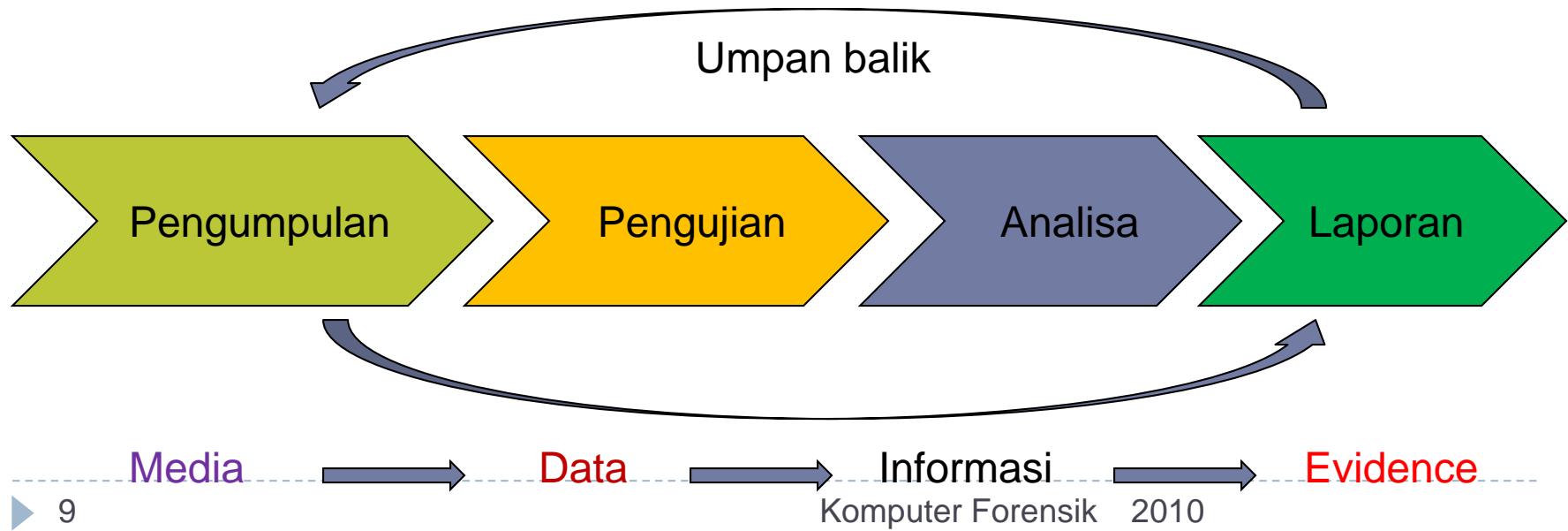
- ▶ Merupakan hal yang terpenting
- ▶ Aturan :
 - ▶ Aturan dalam mengali
 - ▶ Aturan mendapatkan
 - ▶ Aturan menganalisa
 - ▶ Aturan penyajian laporan
- ▶ Pemahaman hukum dan etika



Tahap Komputer Forensik

- ▶ Pengumpulan
- ▶ Pengujian
- ▶ Analisa
- ▶ Laporan

Jangan lupa umpan balik





Pengumpulan Data

- ▶ Mengidentifikasi sumber – sumber potensial dan bagaimana kemudian data dikumpulkan
- ▶ Data bertumpu pada
 - ▶ Personal computer
 - ▶ Mobile computer
 - ▶ Jaringan komputer
 - ▶ Media penyimpanan
 - ▶ Integrasi penyimpanan



Pengumpulan Data

- ▶ Pengumpulan data mencakup
 - ▶ Identifikasi
 - ▶ Penamaan
 - ▶ Perekaman
 - ▶ Mendapatkan data



Langkah yang dibutuhkan

- ▶ Membuat perencanaan untuk mendapatkan data
 - ▶ Kemiripan nilai
 - ▶ Volatility (Volatile)
 - ▶ Upaya dalam mendapatkan data
- ▶ Mendapatkan data
- ▶ Analisa integritas data



Pengujian

- ▶ Melakukan pengujian, menilai dan mengekstrak kepingan informasi yang relevan dari data – data yang dikumpulkan
- ▶ Tahap ini melibatkan :
 - ▶ Bypassing fitur – fitur sistem
 - ▶ Filtrasi (eliminasi data)
 - ▶ Meng-exclude file
 - ▶ Mengalokasi file
 - ▶ Mengekstrak file



Analisa

- ▶ Melakukan analisa untuk merumuskan kesimpulan dalam menggambarkan informasi
- ▶ Cakupan analisa :
 - ▶ Identifikasi user di luar pengguna
 - ▶ Identifikasi lokasi
 - ▶ Identifikasi barang
 - ▶ Identifikasi kejadian
 - ▶ Menentukan bagaimana komponen terelasi satu dengan lainnya



Dokumentasi dan Laporan

- ▶ Merepresentasikan informasi yang merupakan hasil dari proses analisis
- ▶ Faktor yang mempengaruhi reporting
 - ▶ Alternative explanation (penjelasan alternatif)
 - ▶ Audience consideration (pertimbangan peserta)
 - ▶ Actionable information



Tip Pemberlakuan Forensik

1. Konsisten menjadi suatu keharusan dalam setiap proses forensik
2. Tahapan forensik mungkin tidak seluruhnya mendapatkan effort yang sama
3. Analisa memperhatikan berbagai sumber daya potensial
4. Examiner harus memiliki kejelian dalam mengalokasi sebaran data yang mungkin
5. Examiner harus mempertimbangkan setiap alternatif yang reliable



Tip Pemberlakuan Forensik

6. Dibutuhkan tindakan proaktif dalam mengumpulkan data – data yang berharga
7. Examiner harus menghadirkan data melalui standar yang sudah didefinisikan
8. Pertimbangkan setiap tahapan
9. Keputusan harus dibut mencakup kebutuhan dalam mengunmpulkan data dan menangani bukti dengan serangkaian cara tertentu
10. Examiner harus menggunakan pendekatan yang ilmiah dalam mempelajari data



Tip Pemberlakuan Forensik

11. Buat detail, langkah mendapatkan dan dokumentasi jika bukti dibutuhkan dalam hukum dan persidangan
12. Examiner harus melaklukan review kembali proses yang sudah dilaksanakan dan dapat dipertanggungjawabkan



Tip Umum

- ▶ Tip umum dalam menangani dan menganalisa bukti untuk menjaga keutuhan dan kelayakan data
 1. Jangan terlebih dahulu menyalakan komputer untuk alasan apapun
 2. Hubungi agen yang bersangkutan untuk menganalisa
 3. Lekatkan – tandai evidence tape
 4. Miliki surat izin untuk melakukan analisa terhadap komputer dan data



Tip Umum

5. Pernyataan tertulis yang sah atau ringkasan kasus untuk melegalkan examiner untuk bekerja
6. Buat daftar kata – kata untuk melakukan pencarian
7. Lupakan kata “tepat waktu” dalam komputer forensik
8. Konsisten terhadap kasus dn identifikasi kepentingan
9. Orang – orang yang menggunakan komputer alokasi ke ruang komputer untuk dilakukan indikasi



Tip Umum

- I0. Indikasi apakah komputer terintegrasi dengan jaringan atau tidak
- I1. Indikasikan apakah terdapat encryption atau password protection
- I2. Indikasikan skill komputer user yang komputernya diambil untuk komputer forensik
- I3. Secara umum hanya komputer dan media penyimpan untuk keperluan forensik



Tip Bagi Pemula

- ▶ Investigasi sederhana
- ▶ Hubungi pihak yang berwenang
- ▶ Amankan lokasi
- ▶ Minimalkan interupsi terhadap lokasi
- ▶ Jangan jalankan program apapun
- ▶ Jangan biarkan user menggunakan komputer
- ▶ Kumpulkan dan dokumentasikan sumber data lainnya
- ▶ Amankan barang yang berhubungan dengan bukti
- ▶ Mulailah dokumentasi chain of custody



Kuis 3

1. Jelaskan tentang hukum cybercrime di Indonesia ?
2. Bagaimana konsep penerapan hukum mayantara di Indonesia ?
3. Bagaimana konsep pemodelan forensik ?
4. Jelaskan perbedaan programmer dengan ahli komputer forensik ?
5. Dalam tahap pengujian langkah apa yang yang dapat dilakukan, jelaskan ?



Terima kasih





UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Teknik Informatika

STANDAR METODOLOGI KOMPUTER FORENSIK

Pengantar Komputer Forensik teknologi Informasi



lahuluan

- ▶ Apakah diperlukan standarisasi komputer forensik ?
- ▶ Bahasa pemograman, sistem komputer, perangkat keras dan lunak sudah memiliki standarisasi !
- ▶ Organisasi sudah memiliki prosedur, metode, aturan dan berbagamacam proses !
- ▶ Masalah inkompatibilitas selalu muncul seiring perkembangan komputer dan komunikasi



lahuluan

- ▶ Kebutuhan akan standarisasi di level manapun, sudah menjadi kebutuhan.
- ▶ Di masa sekarang kebutuhan akan ahli komputer forensik menjadi penting untuk penegak hukum, pemerintah, perusahaan dan individu.
- ▶ Jadi dibutuhkan suatu standar metodologi yang pasti dalam analisis dan penyelidikan forensik komputer



urut David Morrow

- ▶ “Seperti halnya anda tidak memulai perjalanan jauh ke daerah asing tanpa peta jalan, jangan memulai penyelidikan tanpa memperhatikan rencana “
- ▶ Mengikuti metode standar merupakan hal penting demi kesuksesan dan efektifitas komputer forensik



Uapan Standar Metodologi

- ▶ Pendefinisan
- ▶ Prinsip
- ▶ Proses dan metode
- ▶ Hasil
- ▶ Bahasa



5 faktor

- ▶ Standar komputer forensik mengacu pada lima faktor, yaitu :
 - ▶ Identifikasi subjek
 - ▶ Memperbaiki komputer
 - ▶ Mengungkapkan jalur komunikasi
 - ▶ Permintaan investigasi
 - ▶ Pengumpulan digital evidence lainnya



Pengembangan Standar Komputer Forensik

- ▶ Tahun 1993 ; Diselenggarakan konferensi internasional computer evidence
- ▶ Tahun 1995 ; Usulan pembentukan IOCE (International organization of computer evidence)
- ▶ Tahun 1997 ; G8 dan IOCE menentukan pengembangan standar Computer evidence
- ▶ Tahun 1998 ; Muncul tanggapan dan memunculkan organisasi seperti SWG-DE, ACPO, FCG, ENSFI dan INTERPOL
- ▶ Tahun 1999 ; SWG-DE, ACPO, FCG, dan ENSFI membahasan mengenai standar computer evidence di Eropa



luan Keprofesian

- ▶ Pengujian komputer forensik harus dilakukan secara menyeluruh
- ▶ Media pengujian harus disterilisasi
- ▶ Image bit dari media asli harus dibuat dan untuk dianalisa
- ▶ Intregritas dari media asli harus dipelihara selama penyelidikan



Cara menangani PPAD pada komputer forensik

- ▶ **Preserve** the data to ensure the data is not changed
- ▶ **Protect** the evidence to ensure no one else has access to the evidence
- ▶ **Analyze** the data using forensically sound techniques
- ▶ **Document** everything



• Syarat pengujian Forensik

- ▶ The international association of computer investigative specialists – IACIS memberikan tiga syarat pengujian komputer forensik :
 - ▶ Penggunaan media forensik yang steril
 - ▶ Pengujian harus mempertahankan integritas media asli
 - ▶ Printout dan copy data hasil pengujian harus ditandai, dikenali dan disertakan



yang diperlukan

- ▶ Peralatan dan keahlian harus disinkronisasikan dengan penegak hukum
- ▶ Dibutuhkan dokumentasi dan rangkaian penanganan barang bukti, serta cukup banyak variabel dalam kasus forensik
- ▶ Diperlukan :
 - ▶ Definisikan metodologi (aturan dan panduan)
 - ▶ Kerjakan sesuai metodologi tersebut



ampuan penyelidik

- ▶ Aspek untuk meningkatkan kemampuan penyelidik :
 - ▶ Lakukan pemeriksaan ulang dengan tool yang berbeda
 - ▶ Tetap berusaha objektif selama penyelidikan
 - ▶ Yakinkan langkah anda disetujui pihak manajemen dan hukum
 - ▶ Kaitkan barang bukti dengan hardware tertentu



ampuan penyelidik

- ▶ Buatlah log tertulis selama penyelidikan (logis dan akurat)
- ▶ Gunakan capture full screen
- ▶ Backup barang bukti
- ▶ Kumpulkan juga barang bukti pada tempat terpisah



jakan dan Prosedur

- ▶ Personel
- ▶ Pertimbangan administratif
- ▶ Permintaan layanan
- ▶ Manajerial kasus
- ▶ Pemprosesan kasus
- ▶ Mengembangkan prosedur teknikal



Pertimbangan administratif

- ▶ Pertimbangan administratif yang diperlukan
 - ▶ Software
 - ▶ Ketersediaan Sumber daya
 - ▶ Pelatihan



Ajerial Kasus

- ▶ Buatlah prioritas tertentu dengan mempertimbangkan faktor :
 - ▶ Tidak kriminal
 - ▶ Tanggal persidangan
 - ▶ Batas waktu
 - ▶ Pertimbangan hukum
 - ▶ Ketersediaan sumber daya
 - ▶ Korban potensial
 - ▶ Volatile dan non-volatile evidence



Pengembangkan prosedur teknikal

- ▶ Langkah – langkah pengembangan dan menilai kelayakan suatu prosedur adalah :
 - ▶ Identifikasi tugas dan masalah
 - ▶ Mengajukan solusi
 - ▶ Pengetasan setiap solusi pada sample
 - ▶ Evaluasi hasil pengetesan
 - ▶ Menyempurnakan prosedur



SWG-DE

- ▶ SWG-DE : Scientific working group on digital evidence
- ▶ Dibentuk tahun 1998 oleh the federal crime laboratory directors group
- ▶ Fokus kerja pada forensik digital evidence



E

-
- ▶ IOCE :The international organization computer evidence, didirikan tahun 1995
 - ▶ Sebagai media atau sarana pertukaran informasi bagi para penegak hukum skala internasional mengenai investigasi kejahatan komputer dan masalah forensik



sip IOCE

- ▶ Konsisten terhadap sistem perundangan
- ▶ Menggunakan bahan umum
- ▶ Berdaya tahan
- ▶ Berkemampuan untuk melewati batas – batas internasional
- ▶ Mampu menanamkan keyakinan terhadap integritas evidence
- ▶ Dapat diaplikasikan pada setiap forensic evidence
- ▶ Aplikatif untuk setiap tingkatan mencakup individual, organisasi dan negara



S

- ▶ IACIS :The international association of computer investigative specialist
- ▶ Organisasi internasional yang terdiri dari para penegak hukum profesional yang ditujukan untuk kepentingan edukasi spesifikasi ilmu komputer forensik



na Kasih





UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Teknik Informatika

HUKUM PEMBUKTIAN KEJAHATAN TI

Pengantar komputer forensik teknologi informasi



HUKUM PEMBUKTIAN KEJAHATAN

TEKNOLOGI INFORMASI

- **HUKUM PEMBUKTIAN :**

- Merupakan sebagian dari hukum acara pidana yang mengatur **macam-macam alat bukti yang sah** menurut hukum, **sistem yang dianut** dalam pembuktian, **syarat-syarat** dan **tata cara mengajukan bukti** tersebut serta kewenangan hakim untuk menerima, menolak dan menilai suatu pembuktian

- **SUMBER HUKUM PEMBUKTIAN :**

1. Undang-undang (UU No. 8 Tahun 1981 ttg Hukum Acara Pidana/ KUHAP)
2. Doktrin atau ajaran
3. Jurisprudensi



- **Alat Bukti**
 - Segala sesuatu yang ada hubungannya dengan suatu perbuatan, dimana dengan alat-alat bukti tersebut, dapat dipergunakan sebagai bahan pembuktian guna menimbulkan keyakinan hakim atas kebenaran adanya suatu tindak pidana yang telah dilakukan oleh terdakwa.
- **Sistem Pembuktian**
 - Pengaturan tentang macam-macam alat bukti yang boleh dipergunakan, penguraian alat bukti dan dengan cara-cara bagaimana alat bukti tersebut dipergunakan dan dengan cara bagaimana hakim harus membentuk keyakinannya



TUJUAN DAN GUNA PEMBUKTIAN

- **Bagi Penuntut Umum,**
 - Pembuktian adalah merupakan usaha untuk meyakinkan hakim yakni berdasarkan alat bukti yang ada, agar **menyatakan seorang terdakwa bersalah** sesuai dengan surat atau catatan dakwaan.
- **Bagi Terdakwa atau Penasehat Hukum,**
 - Pembuktian merupakan usaha sebaliknya, untuk meyakinkan hakim, yakni berdasarkan alat bukti yang ada, agar **menyatakan terdakwa dibebaskan** atau dilepaskan dari tuntutan hukum atau meringankan pidananya. Untuk itu terdakwa atau penasehat hukum jika mungkin harus mengajukan alat-alat bukti yang menguntungkan atau meringankan pihaknya. Biasanya bukti tersebut di sebut bukti kebalikan.
- **Bagi Hakim**
 - Atas dasar pembuktian tersebut yakni dengan adanya alat-alat bukti yang ada dalam persidangan baik yang berasal dari Penuntut Umum atau Penasehat Hukum/ Terdakwa dibuat **dasar untuk membuat keputusan**



ALAT BUKTI

- Pada dasarnya seluruh kegiatan dalam proses hukum penyelesaian perkara pidana, sejak penyidikan sampai putusan adalah berupa kegiatan yang berhubungan dengan **pembuktian** atau kegiatan **untuk membuktikan**.
- Mencari bukti sesungguhnya adalah mencari alat bukti. Bukti yang terdapat pada alat bukti itu kemudian dinilai oleh pejabat penyelidik untuk menarik kesimpulan, apakah bukti yang ada itu menggambarkan suatu peristiwa yang diduga tindak pidana ataukah tidak
- **ALAT BUKTI** menurut **UU INFORMASI DAN TRANSAKSI ELEKTRONIK** :
- Pasal 5 (1) dan (2) UU ITE :
 - **Informasi Elektronik** dan/atau **Dokumen Elektronik** dan/atau **hasil cetaknya** merupakan **alat bukti hukum yang sah**.
- Pasal 44 UU ITE :
 - **Alat bukti penyidikan, penuntutan dan pemeriksaan** di pengadilan adalah sbb :
 - Alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dana
 - Alat bukti lain berupa **Informasi Elektronik** dan/atau **Dokumen Elektronik**.



SUMBER BUKTI DIGITAL

- ▶ Selain deskripsi undang-undang ITE tersebut, dikenal pula alat bukti digital. Atribut-atribut khas serta identitas dalam sebuah proses kejahatan dalam dunia komputer dan internet inilah yang disebut dengan bukti-bukti digital.
- ▶ Tiga kategori besar **SUMBER BUKTI DIGITAL**, yaitu :
 - ▶ **Open Computer Systems**
 - ▶ **Communication Systems**
 - ▶ **Embedded Computer Systems**



en Computer Systems

- ▶ Perangkat-perangkat yang masuk dalam kategori jenis ini adalah apa yang kebanyakan orang pikir sebagai **perangkat komputer**. Sistem yang memiliki media penyimpanan, keyboard, monitor, dan pernak-pernik yang biasanya ada di dalam komputer masuk dalam kategori ini. Seperti misalnya laptop, desktop, server, dan perangkat-perangkat sejenis lain.
- ▶ Perangkat yang memiliki sistem media penyimpanan yang kian membesar dari waktu ke waktu ini merupakan sumber yang kaya akan bukti-bukti digital. Sebuah file yang sederhana saja pada sistem ini dapat mengandung informasi yang cukup banyak dan berguna bagi proses investigasi. Contohnya detail seperti kapan file tersebut dibuat, siapa pembuatnya, seberapa sering file tersebut diakses, dan informasi lainnya semua merupakan informasi penting.



Communication Systems

- **Sistem telefon tradisional, komunikasi wireless, Internet, jaringan komunikasi data**, merupakan salah satu sumber bukti digital yang masuk dalam kategori ini. Sebagai contoh, jaringan Internet membawa pesan-pesan dari seluruh dunia melalui e-mail. Kapan waktu pengiriman e-mail ini, siapa yang mengirimnya, melalui mana si pengirim mengirim, apa isi dari e-mail tersebut merupakan bukti digital yang amat sangat penting dalam investigasi.



Embedded Computer Systems

- ▶ Perangkat telefon bergerak (**ponsel**), personal digital assistant (**PDA**), **smart card**, dan perangkat-perangkat lain yang tidak dapat disebut komputer tapi memiliki sistem komputer dalam bekerjanya dapat digolongkan dalam kategori ini. Hal ini dikarenakan bukti-bukti digital juga dapat tersimpan di sini. Sebagai contoh, sistem navigasi mobil dapat merekam ke mana saja mobil tersebut berjalan. Sensor dan modul-modul diagnosa yang dipasang dapat menyimpan informasi yang dapat digunakan untuk menyelidiki terjadinya kecelakaan, termasuk informasi kecepatan, jauhnya perjalanan, status rem, posisi persneling yang terjadi dalam lima menit terakhir. Semuanya merupakan sumber-sumber bukti digital yang amat berguna



Bersalah atau Tidak

- **Dasar pemberian seseorang dapat dikatakan bersalah atau tidak melakukan tindak pidana :**
 1. perbuatannya dapat dipersalahkan atas kekuatan UU yang telah ada sebelumnya (asas legalitas),
 2. perbuatan tersebut didukung oleh kekuatan bukti yang sah (pembuktian)
 3. kepadanya dapat dipertanggung-jawabkan (unsur kesalahan).
- Pembuktian dalam hukum acara pidana bertujuan untuk mencari kebenaran materiil (kebenaran yang sesungguhnya).
- **ALAT BUKTI** menurut KUHAP Pasal 184 :
 - a. Keterangan saksi
 - b. Keterangan ahli
 - c. Surat
 - d. Petunjuk
 - e. Keterangan terdakwa



TEORI PEMBUKTIAN

- **Pasal 183 KUHAP** secara tegas merumuskan bahwa "Hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya **dua alat bukti yang sah** ia memperoleh **keyakinan** bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya".
- **Teori Pembuktian dalam Hukum Acara Pidana :**
 - Teori pembuktian berdasarkan Undang-Undang secara positif
 - Teori ini adalah pembuktian yang didasarkan hanya kepada **alat-alat pembuktian yang disebut UU**. Dikatakan **secara positif**, karena didasarkan **hanya pada UU**.
 - Teori pembuktian berdasarkan keyakinan hakim
 - Teori ini didasarkan kepada **keyakinan hati nurani hakim**, yang menetapkan bahwa terdakwa telah melakukan perbuatan yang didakwakan.



TEORI PEMBUKTIAN

➤ Teori pembuktian berdasarkan keyakinan Hakim atas alasan yang logis;

- Menurut teori ini hakim dapat memutuskan seseorang bersalah berdasar keyakinannya, **keyakinan yang didasarkan kepada dasar-dasar pembuktian disertai dengan suatu kesimpulan (conclusi) yang berlandaskan kepada peraturan-peraturan pembuktian tertentu.** Sistem atau teori pembuktian ini disebut juga pembuktian bebas, karena hakim bebas untuk menyebut alasan-alasan keyakinannya (*vrije bewijstheorie*)

➤ Teori pembuktian berdasarkan Undang-Undang secara negatif ;

- Teori ini di samping **berdasarkan alat-alat bukti yang sah berdasarkan Undang-Undang** juga alat bukti yang sah tersebut disertai dengan **keyakinan hakim.**
- Memperhatikan teori pembuktian tersebut di atas, maka nampak dengan jelas **rumusan Pasal 183 KUHAP didasarkan pada suatu teori pembuktian berdasarkan Undang-Undang secara negatif (*Negatief Wettselijk*).**



IBUKTIAN CYBERCRIME

- Berdasarkan teori pembuktian berdasarkan Undang-Undang secara negatif (*Negatief Wettelijk*) tersebut perkara “Cyber Crime” bila dikaitkan dengan Pasal 1 ayat (1) KUHP tentang asas legalitas juncto perintah undang-undang sebagaimana dirumuskan dalam Pasal 3 KUHAP, yang selengkapnya berbunyi “ Peradilan dilakukan menurut cara yang diatur dalam undang-undang ini”, maka penerapan sistem pembuktian yang dianut dalam KUHAP secara legalitas tidak dapat mengakomodir alat bukti (terutama yang mirip dengan bukti surat) sebagai kemungkinan dipergunakan dalam Cyber Crime.



IBUKTIAN CYBERCRIME

- Pendapat demikian setidaknya didasarkan alasan sebagai berikut :
 - **Masih dipertahankannya Asas Legalitas dalam Hukum Pidana Indonesia** ; Moelyatno menulis bahwa asas legalitas itu mengandung 3 pengertian, yaitu :
 1. Tidak ada perbuatan yang dilarang dan di ancam dengan pidana kalau hal itu terlebih dahulu belum dinyatakan dalam suatu aturan undang-undang ;
 2. Untuk menentukan adanya perbuatan pidana tidak boleh digunakan analogi (kiyas) ;
 3. Aturan-aturan hukum pidana tidak berlaku surut.



IBUKTIAN CYBERCRIME

- menurut Groenhuijsen, ada **empat makna yang terkandung dalam asas legalitas** ini. Dua dari yang pertama ditujukan kepada **pembuat undang-undang** (*de wetgevende macht*), dan dua yang lainnya merupakan **pedoman bagi hakim**, yaitu :
 1. Pembuat UU tidak boleh memberlakukan suatu ketentuan pidana berlaku mundur.
 2. Semua perbuatan yang dilarang harus dimuat dalam rumusan delik sejelas-jelasnya.
 3. Hakim dilarang menyatakan bahwa terdakwa melakukan perbuatan pidana didasarkan pada hukum tidak tertulis atau hukum kebiasaan,
 4. Terhadap peraturan hukum pidana dilarang diterapkan analogi



IBUKTIAN CYBERCRIME

- Dikatakan selanjutnya bahwa asas ini dikenal dengan adagium “ *Nullum delictum noella poena praevia sine lege peonali* ”.
- *Nullum crimen sine lege* berarti tidak ada tindak pidana tanpa undang-undang dan
- *Nulla poena sine lege* berarti tidak ada pidana tanpa undang-undang.
- Jadi **undang-undang menetapkan dan membatasi perbuatan mana dan pidana (sanksi) mana yang dapat dijatuhkan kepada pelanggarnya**



Nilai Evidence

- ▶ Faktor yang menjadi pertimbangan :

- ▶ Penilaian kasus
- ▶ Onsite consideration
- ▶ Analisa lokasi pemprosesan
- ▶ Pertimbangan hukum
- ▶ Analisa evidence



Analisa Evidence

- Lokasi ditemukan evidence
- Stabilitas media yang dilakukan pemeriksaan
- Menentukan bagaimana evidence didokumentasi
- Mengevaluasi lokasi media penyimpanan
- Memastikan kondisi dari evidence
- Menganalisa kebutuhan akan cadangan listrik



Interiksaan Evidence

▶ Pengujian dilakukan dengan tahap :

- ▶ Persiapan sebagai langkah awal
- ▶ Ekstraksi
- ▶ Menganalisa data terekstrak
- ▶ Kesimpulan



indungan Barang Bukti

- ▶ Menurut Jim Mc Millan “ Banyak kasus tidak dibawa ke pengadilan karena barang bukti yang tidak memadai “
- ▶ Barang bukti komputer berupa :
 - ▶ Barang sensitif
 - ▶ Salah menangani akan rusak
 - ▶ Bersifat mekanis - elektromekanis



aman terhadap barang bukti

- ▶ Menurut Jim Mc Millan “ Importance of a standard methodology in computer forensics ” :
 - ▶ Virus
 - ▶ Prosedur cleanup
 - ▶ Ancaman eksternal - lingkungan



aman terhadap barang bukti

- ▶ Menurut Judd Robin “An explanation of computer forensics“ mensyaratkan :
 - ▶ Barang bukti tidak akan rusak oleh prosedur penyelidikan
 - ▶ Tidak terinfeksi virus komputer
 - ▶ Barang bukti dilindungi dari keruksakan mekanis dan elektromekanis
 - ▶ Penerapan pemelihraan
 - ▶ Membatasi dampak pada operasi bisnis
 - ▶ Informasi client dihargai secara etis dan tidak diumumkan



tor yang tidak berkaitan dengan barang ti secara fisik

- ▶ Rangkaian pemeliharaan
- ▶ Batasan waktu
- ▶ Informasi yang tidak diumumkan – informasi client
- ▶ Register, peripheral memori dan cache
- ▶ Memori (kernel dan fisik)
- ▶ Keadaan jaringan
- ▶ Proses yang sedang berjalan
- ▶ Disk
- ▶ Floppy disk dn media backup
- ▶ CD-Rom dan printout



sip ketidakpastian Heisenberg

- ▶ Dan Farmer “ Computer forensic analysis class hendouts ” :

“Melakukan pengujian sekumpulan atau suatu bagian dari sistem akan menimbulkan gangguan pada komponen lainnya, sehingga akan mustahil untuk melakukan *capture* keseluruhan sistem pada satu saat saja”
- ▶ Jim Mc Millan

“Banyak barang bukti dalam bentuk terenkripsi atau hidden”

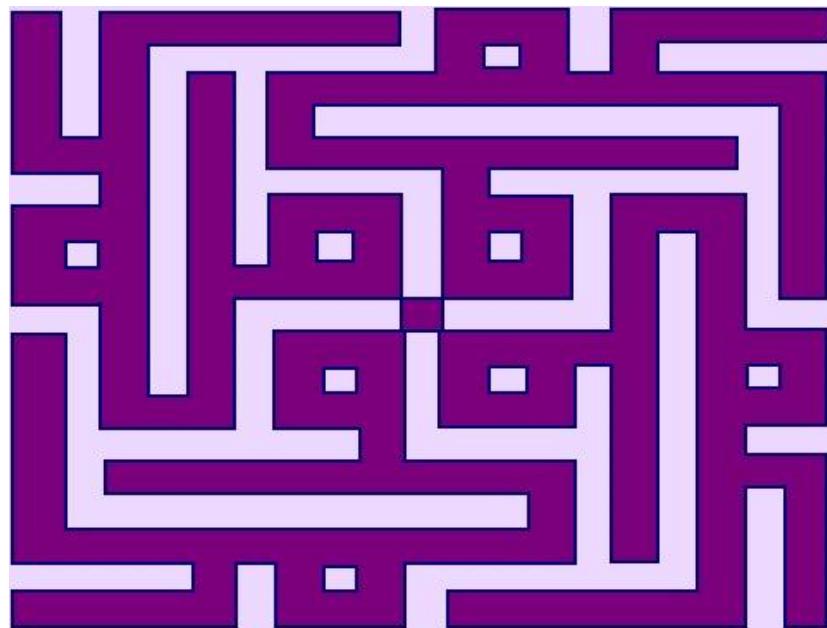


S 4

1. Jelaskan standar metodologi komputer forensik menurut SANS institute ?
2. Jelaskan perkembangan penetapan standar metodologi komputer forensik ?
3. Jelaskan syarat pengujian forensik berdasarkan standar metodologi komputer forensik ?
4. Hal apa saja yang diperlukan oleh seorang penyidik ?
5. Bagaimana pengambaran pengembangan prosedur teknikal ?



ma Kasih





UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Teknik Informatika

KEJAHATAN BIDANG TEKNOLOGI INFORMASI

Pengantar Komputer Forensik Teknologi Informasi



Pendahuluan

- ▶ Kecenderungan insiden di bidang teknologi komputer dan komunikasi digolongkan ke dalam program hacking :
 - Packet flooding
 - Packet sniffing
 - Backdoor
- ▶ Secara umum kita fokus pada sistem komputer berbasis windows
- ▶ Dalam kenyataan kejahatan komputer sudah sangat meluas, sudah tidak melihat kepada basis sistem operasi saja.



KEJAHATAN BIDANG TEKNOLOGI INFORMASI

- ▶ Beberapa istilah Kejahatan di bidang Teknologi Informasi :
 - Cybercrime
 - Kejahatan Mayantara (Barda Nawawi A.)
 - Computer Crime
 - Computer Abuse
 - Computer Fraud
 - Computer Related Crime dll
- ▶ **Computer Crime** → perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana / alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.
- ▶ **Cybercrime** → perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi (Teguh Wahyono, S. Kom, 2006)



Karakteristik unik Kejahatan bidang TI :

▶ **Ruang Lingkup kejahatan**

- Bersifat global (melintasi batas negara) menyebabkan sulit menentukan yuridiksi hukum negara mana yang berlaku terhadapnya.

▶ **Sifat Kejahatan**

- Tidak menimbulkan kekacauan yang mudah terlihat (non-violence), sehingga ketakutan terhadap kejahatan tersebut tidak mudah timbul.

▶ **Pelaku Kejahatan**

- Pelaku kejahatan ini tidak mudah didentifikasi, namun memiliki ciri khusus yaitu pelakunya menguasai penggunaan internet / komputer.

▶ **Modus Kejahatan**

- Modus kejahatan hanya dapat dimengerti oleh orang yang mengerti dan menguasai bidang teknologi informasi.

▶ **Jenis Kerugian**

- Kerugian yang ditimbulkan lebih luas, termasuk kerugian dibidang politik, ekonomi, sosial dan budaya.



Kejahatan Bidang TI

- ▶ Menurut Heru Sutadi, 2003 digolongkan menjadi dua bagian, yaitu :
 - Kejahatan yang menggunakan TI sebagai **FASILITAS**
 - Contoh : pembajakan, pornografi, pemalsuan dan pencurian kartu kredit, penipuan lewat e-mail, penipuan dan pembobolan rekening bank, perjudian online, terorisme, situs sesat, Isu SARA dll
 - Kejahatan yang menjadikan sistem dan fasilitas TI sebagai **SASARAN**.
 - Contoh : pencurian data pribadi, pembuatan dan penyebaran virus komputer, pembobolan situs, cyberwar dll



JENIS CYBERCRIME

- ▶ Menurut Teguh Wahyono, S. Kom., 2006 jenis cybercrime dikelompokan dalam :
 1. Cybercrime berdasarkan JENIS AKTIFITAS
 2. Cybercrime berdasarkan MOTIF KEGIATAN
 3. Cybercrime berdasarkan SASARAN KEJAHATAN



CYBERCRIME ; JENIS AKTIFITAS

a. Unauthorized Acces

- Kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer sedara tidak sah, tanpa izin atau tanpa sepenuhnya dari pemilik sistem jaringan komputer yang dimasukinya, contoh : Probing dan Port Scanning

b. Illegal Contents

- Kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum, contoh : penyebarluasan pornografi, isu-isu / fitnah terhadap individu (biasanya public figure).



CYBERCRIME ; JENIS AKTIFITAS

c. **Penyebaran virus secara sengaja**

- Melakukan penyebaran virus yang merugikan seseorang atau institusi dengan sengaja

d. **Data Forgery**

- Kejahatan yang dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet, biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database.

e. **Cyber Espionage, Sabotage and Extortion**

- *Cyber Espionage* merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran.
- *Sabotage and Extortion* merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.



CYBERCRIME ; JENIS AKTIFITAS

f. *Cyberstalking*

- ▶ Kejahatan yang dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya dengan melakukan teror melalui pengiriman e-mail secara berulang-ulang tanpa disertai identitas yang jelas.

g. *Carding*

- ▶ Kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

h. *Hacking dan Cracking*

- ▶ Hacker sebenarnya memiliki konotasi yang netral, namun bila kemampuan penguasaan sistem komputer yang tinggi dari seorang hacker ini disalahgunakan untuk hal negatif, misalnya dengan melakukan perusakan di internet maka hacker ini disebut sebagai cracker. Aktifitas cracking di internet meliputi pembajakan account milik orang lain, pembajakan situs web, probing, penyebaran virus, hingga pelumpuhan target sasaran (menyebabkan hang, crash).



CYBERCRIME ; JENIS AKTIFITAS

i. **Cybersquatting and Typosquatting**

- *Cybersquatting* merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo karcis.
- *Typosquatting* adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain, biasanya merupakan nama domain saingan perusahaan.

j. **Hijacking**

- *Hijacking* merupakan kejahatan pembajakan terhadap hasil karya orang lain, biasanya pembajakan perangkat lunak (Software Piracy).

k. **Cyber Terorism**

- Kejahatan yang dilakukan untuk mengancam pemerintah atau warga negara, termasuk cracking ke situs pemerintah atau militer.



CYBERCRIME ; JENIS KEGIATAN

a. ***Cybercrime sebagai tindakan murni kriminal***

- Kejahatan ini murni motifnya kriminal, ada kesengajaan melakukan kejahatan, misalnya *carding* yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam bertransaksi di internet.

b. ***Cybercrime sebagai kejahatan “abu-abu”***

- Perbuatan yang dilakukan dalam jenis ini masuk dalam “wilayah abu-abu”, karena sulit untuk menentukan apakah hal tersebut merupakan kriminal atau bukan mengingat motif kegiatannya terkadang tidak dimaksudkan untuk berbuat kejahatan, misalnya *Probing* atau *portscanning* yaitu tindakan pengintaian terhadap sistem milik orang lain dengan mengumpulkan informasi sebanyak mungkin, namun data yang diperoleh berpotensi untuk dilakukannya kejahatan.



CYBERCRIME ; JENIS KEJAHATAN

- a. ***Cybercrime yang menyerang individu (Against Person)***
 - Jenis kejahatan ini sasaran serangannya adalah perorangan / individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut, contoh : Pornografi, Cyberstalking, Cyber-Tresspass.
- b. ***Cybercrime menyerang Hak Milik (Against Property)***
 - Kejahatan yang dilakukan untuk mengganggu atau menyerang hak milik orang lain, contoh : pengaksesan komputer secara tidak sah, pencurian informasi, carding, cybersquatting, typosquatting, hijacking, data forgery.
- c. ***Cybercrime Menyerang Pemerintah (Against Government)***
 - Kejahatan ini dilakukan dengan tujuan khusus penyerangan terhadap pemerintah, contoh : cyber terorism, craking ke situs resmi pemerintah.



PENANGGULANGAN CYBERCRIME

I. Pengamanan Sistem

- Tujuan yang paling nyata dari suatu sistem keamanan adalah mencegah adanya perusakan bagian dalam sistem karena dimasuki oleh pemakai yang tidak diinginkan. Pengamanan sistem ini harus terintegrasi pada keseluruhan subsistem untuk mempersempit atau bahkan menutup adanya celah-celah unauthorised actions yang merugikan.

2. Penanggulangan Global

- OECD (The Organization for Economic Cooperation and Development) telah merekomendasikan beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan Cybercrime, sbb :



PENANGGULANGAN CYBERCRIME

4. Perlunya Cyberlaw

- Cybercrime belum sepenuhnya terakomodasi dalam peraturan / Undang-undang yang ada, penting adanya perangkat hukum khusus mengingat karakter dari cybercrime ini berbeda dari kejahatan konvensional.

4. Perlunya Dukungan Lembaga Khusus

- Lembaga ini diperlukan untuk memberikan informasi tentang cybercrime, melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan cybercrime.
- Indonesia sendiri sudah memiliki IDCERT (Indonesia Computer Emergency Response Team) yang diperlukan bagi orang-orang untuk melaporkan masalah-masalah keamanan komputer,



Penanggulangan Global

akukan modernisasi hukum pidana nasional dengan hukum acaranya, yang diselaraskan dengan konvensi internasional.

2. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.
3. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan cybercrime.
4. Meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya mencegah kejahatan tersebut terjadi.
5. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan cybercrime, antara lain melalui perjanjian ekstradisi dan mutual assistance treaties.



Terima kasih





UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Teknik Informatika

Perangkat Teknologi Forensik

Pengantar Komputer Forensik Teknologi Informasi



lahuluan

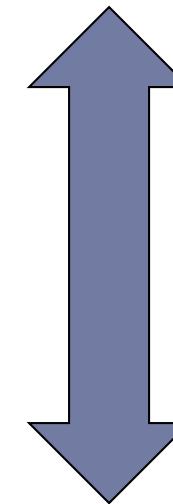
- ▶ Dalam komputer forensik dibutuhkan sumber daya informasi
- ▶ Sumber daya informasi komputer forensik sama dengan sumber daya informasi pada sistem komputer
- ▶ Perbedaannya pada implementasinya



Sumber daya informasi

▶ Komponen sumber daya informasi pada komputer forensik adalah :

- ▶ Perangkat keras
- ▶ Perangkat lunak
- ▶ Basis data – database
- ▶ Data – informasi
- ▶ Brain ware



Perilaku

Pengguna



ngkat keras

- ▶ Perangkat masukan
- ▶ Perangkat keluaran
- ▶ Media penyimpanan
- ▶ Komponen pengolahan



ngkat masukan - Input

- ▶ Keyboard
- ▶ Mouse
- ▶ Tracball
- ▶ Trackpoint
- ▶ Trackpad – Touchpad
- ▶ Touch screen
- ▶ Joystick
- ▶ Source data automation
- ▶ Scanner
- ▶ WebCam
- ▶ Kartu magnetik – Smartcard
- ▶ Biometric peripheral



Tujuan Keluaran - Output

- ▶ **Monitor**
 - ▶ Cathode ray tube
 - ▶ Liquid crystal display
- ▶ **Printer**
 - ▶ Impact printer
 - ▶ Non impact printer
- ▶ **Plotter**
- ▶ **Speaker**
- ▶ **Video output – Proyektor multimedia**
- ▶ **Micro Film**



ia Penyimpanan

- ▶ **Media penyimpanan sekunder**

- ▶ Mass storage
- ▶ Simpanan luar
- ▶ Auxiliary storage
- ▶ Permanen storage
- ▶ Backing storage
- ▶ Computer data bank



ia Penyimpanan

- ▶ Media penyimpana sekunder digolongkan :
 - ▶ SASD - Sequential access storage device
 - ▶ Magnetic tape
 - ▶ DASD - Direct access storage device
 - ▶ Magnetic disk
 - Floppy disk
 - Harddisk
 - ▶ Optical disk
 - CD ROM



Teknologi Penyimpanan Yang Populer

- ▶ Digital versatile disk – DVD
- ▶ Fluorescent multilayer disk – FMD
- ▶ Magneto optical disc – MO-Disc

- ▶ Teknologi penyimpanan
 - ▶ CD ROM Drive
 - ▶ CD R Drive
 - ▶ CD RW Drive
 - ▶ DVD Drive
 - ▶ Combo drive



Toponem pengolahan

- ▶ CPU – central processing unit
 - ▶ Control unit
 - ▶ Pengatur lalulintas data didalam CPU
 - ▶ Arithmetic logic unit
 - ▶ Pemrosesan perhitungan matematikan dan perbandingan
 - ▶ Register
 - ▶ Pencatat-penyimpan data yang akan diproses (memori kecil yang membantu CPU)



Pengaruh yang pengaruhi kinerja CPU

- ▶ Register
- ▶ Memori
- ▶ Komputer BUS
- ▶ Cache memory
- ▶ Faktor lain
 - ▶ Expansion slot
 - ▶ Port
 - ▶ CPU fan
 - ▶ Casing



ster

- ▶ Suatu ukuran penyimpanan informasi, dalam register disebut wordsize
- ▶ Ukuran
 - ▶ Secara umum 2 Bit
 - ▶ 16 Bit
 - ▶ 32 Bit
 - ▶ 64 Bit
 - ▶ 128 Bit



▶ ROM – Read only memory

- ▶ Berisikan perintah yang merada di dalam sebuah chip, dan isinya tidak dapat dirubah atau dihapus user
- ▶ Dengan perkembangan teknologi dan kejahanan komputer ROM dapat dirubah atau diisi kembali

▶ RAM – Random access memory

- ▶ Berisi informasi – informasi selama CPU dijalankan, bersifat volatile



Computer BUS

- ▶ Jenis BUS
 - ▶ Data BUS
Untuk mengalirkan data
 - ▶ Address BUS
Untuk mengalirkan alamat tujuan data
 - ▶ Control BUS
Untuk mengalirkan informasi status peralatan
 - ▶ Ukuran BUS
 - ▶ 16 Bit
 - ▶ 32 Bit
 - ▶ 64 Bit
 - ▶ Perkembangan BUS
 - ▶ ISA
 - ▶ EISA
 - ▶ MCA
 - ▶ PCI
 - ▶ AGP
 - ▶ PCIx



Cache Memory

- ▶ Komponen yang mirip dengan RAM, tetapi prosesnya lebih cepat
- ▶ Digunakan untuk menyimpan instruksi yang sering digunakan oleh CPU (Jika dibutuhkan CPU tidak perlu mencari informasi dari RAM)
- ▶ Semakin besar cache memory , maka semakin cepat proses CPU



Perangkat lunak

- ▶ Sebagai perangkat lunak yang digunakan sebagai mediator dan pemberi instruksi terhadap sumber daya hardware.
- ▶ Perangkat lunak digolongkan ke dalam :
 - ▶ Perangkat lunak sistem
 - ▶ Perangkat lunak aplikasi



bagian Perangkat lunak

- ▶ Audio dan multimedia
- ▶ Communication
- ▶ Business
- ▶ Desktop
- ▶ Education
- ▶ Games dan entertainment
- ▶ Graphics
- ▶ Home dan hobby
- ▶ Network dan internet
- ▶ Security
- ▶ Servers
- ▶ Development
- ▶ System utilities
- ▶ Web development
- ▶ Online – only apps
- ▶ Printing
- ▶ Hotkeys, scripting



nware

- ▶ Profesional TI
 - ▶ Technical support
 - ▶ Network administrator
 - ▶ Database administrator
 - ▶ Sistem analis
 - ▶ Programmer
- ▶ Insiden handlers
 - ▶ Tindak kriminal – pelanggaran
 - ▶ Keamanan komputer - sistem
- ▶ Investigator
 - ▶ Komputer forensik



l Base

- ▶ Database sudah memiliki ruang tersendiri dan difungsikan dalam manajerial data (alokasi data dan analisa data)
- ▶ Database dikelompokan :
 - ▶ Database skala desktop multi user
 - ▶ Database skala server

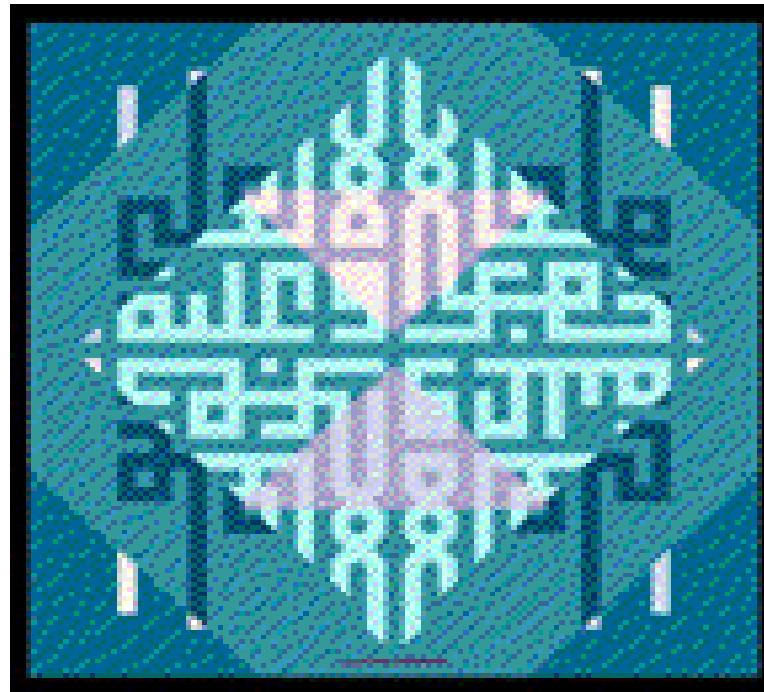


Kuis 5

- ▶ Apa yang dimaksud dengan cybercrime ?
- ▶ Jelaskan jenis dari cybercrime ?
- ▶ Jelaskan tiga fungsi dari program hacking ?
- ▶ Bagaimana cara menanggulangi tindak kejahatan komputer ?
- ▶ Kejahatan komputer sudah dikatakan berdifikat global, bagaimana cara menghadapinya ?



na Kasih





UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Teknik Informatika

Penanganan Insiden Forensik

Pengantar Komputer Forensik teknologi Informasi



Insiden

- ▶ Jenis insiden menurut the information security management :
 - ▶ Virus
 - ▶ Unauthorized access
 - ▶ Pencurian atau kehilangan kepercayaan pada informasi
 - ▶ Serangan denial of service pada sistem
 - ▶ Korupsi informasi



iapan

- ▶ Pengunaan beberapa tool untuk mencegah penyusupan dengan deteksi
- ▶ Backup sistem
- ▶ Kebijakan password
- ▶ Kebijakan keamanan sistem
- ▶ Lakukan instalasi patch security
- ▶ Pergunakan security – auditing tools
- ▶ Pelajari sistem lebih lama
- ▶ Aktifkan fasilitas logging dan accounting
- ▶ Lakukan audit dan pengujian pada sistem secara rutin



sedur penanganan insiden

- ▶ Bagaimana mengamankan dan menjaga barang bukti
- ▶ Dimana dan bagaimana mencari barang bukti
- ▶ Daftar yang dipersiapkan untuk laporan menyeluruh
- ▶ Daftar orang untuk keperluan pelaporan
- ▶ Daftar software yang digunakan
- ▶ Daftar ahli



sedur penanganan insiden

- ▶ Jika ahli forensik tidak dimiliki atau tidak berada ditempat dan terdapat insiden, yang harus dilakukan oleh seorang staff :
 - ▶ Membuat image
 - ▶ Analisis forensik dilakukan semua dari copy
 - ▶ Memelihara rincian media dalam proses



edur penanganan insiden secara rhana

- ▶ Menurut Scott Grace “ Computer incident response and computer forensics overview” :
 - ▶ Amankan lingkungan
 - ▶ Shutting down komputer
 - ▶ Label barang bukti
 - ▶ Dokumentasikan barang bukti
 - ▶ Transportasikan barang bukti
 - ▶ Dokumentasikan rangkaian penyimpanan



sedur penanganan insiden

- ▶ Dokumen penanganan insiden dari SANS institute :
 - ▶ Semua partisipan menyarankan elemen dan perubahan
 - ▶ Proses berjalan dengan banyak perulangan
 - ▶ Beberapa masalah disajikan dengan banyak pilihan
 - ▶ Setiap partisipan harus menyetujui keseluruhan dokumen



• merespon insiden

- ▶ Fase 1 : Persipan (42 tindakan)
- ▶ Fase 2 : Identifikasi (6 tindakan)
- ▶ Fase 3 : Pengisian (17 tindakan)
- ▶ Fase 4 : Pembasmian (10 tindakan)
- ▶ Fase 5 : Pemulihan (6 tindakan)
- ▶ Fase 6 : Tindak lanjut (9 tindakan)



rgency action card

1. Tetap tenang sehingga terhindari kesalahan fatal
2. Buatlah catatan yang baik dan relevan
3. Beritahu orang yang tepat dan carilah pertolongan
4. Tetapkan kebijakan orang – orang terpercaya yang boleh tahu
5. Gunakan jalur komunikasi terpisah dari sistem yang mengalami compromise



rgency action card

6. Isolasi maslah sehingga tidak bertambah buruk
7. Buat backup sistem
8. Temukan sumber masalah
9. Kembali ke pekerjaan semula setelah backup terjamin dan lakukan restore sistem
10. Belajar dari pengalaman



rosesan Barang Bukti

► Menurut Lori Willer “ Computer forensics”, panduan :

1. Shut down komputer, dan perlu dipertimbangkan keruksakan proses yang berjalan dibackground
2. Dokumentasikan konfigurasi hardware dari sistem
3. Pindahkan sistem komputer ke lokasi yang aman
4. Buat backup bit dri hard disk dan floppy



luan

5. Uji otentifikasi data dari semua penyimpanan
6. Dokumentasikan tanggal dan waktu yang berhubungan dengan file komputer
7. Buat daftar key word pencarian
8. Evaluasi swap file
9. Evaluasi file slack, dari dump memori yang terjadi selama file ditutup
10. Evaluasi unallocated space – erased file



luan

11. Pencarian keyword pada file, file slack dn unallocated space
12. Dokumentasikan nama file (atribut tanggal dan file)
13. Identifikasikan anomali file, program dan storage
14. Evaluasi fungsionalitas program untuk mengetahui kegunaannya
15. Dokumentasikan temuan dan software yang dipergunakan
16. Buat copy dari software yang dipergunakan



Apakah pemrosesan barang bukti

- ▶ Menurut Jim Mc Millan, lima tahap dalam pemrosesan barang bukti :
 - ▶ Persiapan
 - ▶ Snapshot
 - ▶ Transport
 - ▶ Pengujian
 - ▶ Analisa



iapan

- ▶ Sterilkan semua media dari virus
- ▶ Pastikan semua tool forensik bisa dipergunakan secara resmi
- ▶ Periksa kerja semua peralatan lab
- ▶ Pilih ahli forensik yang tepat dan mampu memberikan kesaksian dan penjelasan di persidangan



osshot

- ▶ Foto lingkungan
- ▶ Catat rinciannya
- ▶ Foto barang bukti
- ▶ Dokumentasikan konfigurasi hardware
- ▶ Labeli barang bukti sesuai metodologi
- ▶ Foto barang bukti lagi setelah dilabeli
- ▶ Dokumentasikan apa terjadi



Isport

- ▶ Lakukan pengemasan secara aman
- ▶ Foto dan dokumentasikan penanganan barang bukti meninggalkan tempat kejadian sampai ke lab pengujian



ujian

- ▶ Lakukan unpack sesuai metodologi
- ▶ Lakukan ujimvisual dan catatt setiap konfigurasi yang tidak semstinya
- ▶ Buatlah image hard disk
- ▶ Setelah membuat image simpan barang bukti di tempat aman dan catat
- ▶ Lakukan pembuat image kedua



isa

- ▶ Analisa barang bukti dilakukan secara dua level :
 - ▶ Level fisik
 - ▶ Level lojik
- ▶ Perhitungan rangkaian kepercayaan – chain of evidence



gkaian kepercayaan

- ▶ Shell
- ▶ Command
- ▶ Dynamic libraries
- ▶ Device driver
- ▶ Kernel
- ▶ Controller
- ▶ Hardware



na Kasih

- ▶ Berjumpa kembali mimgu depan

INVESTIGASI KASUS TI

Pengantar Komputer Forensik Teknologi Informasi



UNIVERSITAS GUNADARMA
TEKNIK INDUSTRI - TEKNIK INFORMATIKA



INVESTIGASI KASUS TEKNOLOGI

- A. Prosedur Forensik yang biasa dilakukan Investigator
- 1. Membuat *copies* dari keseluruhan *log data*, files dll yang dianggap perlu pada suatu media yang terpisah.
- 2. Membuat *fingerprint* dari data secara matematis (contoh *hashing algorithm*, MD5).
- 3. Membuat *fingerprint* dari *copies* secara matematis.
- 4. Membuat suatu *hashes masterlist*.
- 5. Dokumentasi yang baik dari segala sesuatu yang telah dikerjakan.
- Selain itu perlu dilakukan investigasi lanjutan dengan menggunakan metodologi forensik TI. Metode Search and seizure biasanya lebih banyak digunakan dibanding metode pencarian informasi.



A1. Metode Search dan Seizure

- Selain melakukan tahap *Search* dan *Seizure* mulai dari identifikasi sampai dengan evaluasi hipotesa, metode ini juga memberikan penekanan dan **batas-batas untuk investigator** agar hipotesa yang dihasilkan sangat akurat, yaitu :
 1. Jangan merubah bukti asli
 2. Jangan mengeksekusi program pada bukti (komputer) terutama *Operating Systemnya*
 3. Tidak mengijinkan tersangka untuk berinteraksi dengan bukti (komputer)
 4. Sesegera mungkin mem-backup bukti yang ada dalam komputer tersangka. Jika pada saat diidentifikasi komputer masih menyala, jangan dimatikan sampai seluruh data termasuk *temporary* selesai dianalisa dan disimpan.
 5. Rekam seluruh aktifitas investigasi
 6. Jika perlu, pindahkan bukti ke tempat penyimpanan yang lebih aman



A2. Pencarian Informasi

- Hal-hal yang harus diperhatikan dalam pencarian informasi sebagai bukti tambahan untuk memperkuat hipotesa, yaitu :
 1. Jika melakukan penggalian informasi lebih dalam ke saksi, gunakan wawancara interaktif, sehingga bukti yang ada dapat di *cross-check* agar keberadaan bukti tersebut diakui oleh tersangka
 2. Jika memungkinkan, rekonstruksi dilakukan dengan / tanpa tersangka sehingga apa yang masih belum jelas dapat tergambar dalam rekonstruksi.



B. Data Recovery

- Data recovery merupakan bagian dari analisa forensik yang merupakan komponen penting untuk mengetahui apa yang telah terjadi, rekaman data, korespondensi dan petunjuk lainnya



C. Pengelompokan Analisa Media

- ▶ Pengelompokan ini bertujuan untuk mengetahui aliran dan proses dalam media yang digunakan dalam kejahatan. Dari pengelompokan ini dapat disimpan informasi penting yang didukung oleh sistem yang ada. Pengelompokan dalam bentuk laporan ini diisi dengan keadaan fakta di lapangan



D. Pembuatan Laporan dalam Analisa Media

- ▶ Beberapa hal penting yang perlu dimasukkan dalam laporan analisa media adalah sbb :
 1. Tanggal dan waktu terjadinya pelanggaran hukum pada CPU
 2. Tanggal dan waktu pada saat investigasi
 3. Permasalahan yang signifikan terjadi
 4. Masa berlaku analisa laporan
 5. Penemuan yang berharga (bukti)
 6. Teknik khusus yang dibutuhkan atau digunakan (contoh; *password cracker*)
 7. Bantuan pihak yang lain (pihak ketiga)
- ▶ Pada saat penyidikan, pelaporan dalam bentuk worksheet ini di *cross-check* dengan saksi yang ada, baik yang terlibat langsung maupun tidak langsung



E. Log Out Evidence – Visual

- Tahapan yang dilalui dalam inspeksi komputer secara visual adalah:

1. Log out seluruh komputer untuk dianalisa lebih lanjut
2. Jika ada media penyimpanan yang lain (CD / disket), diberi label khusus agar bukti tersebut tetap utuh.
3. Inspeksi visual dilakukan dengan melakukan *physical makeup*
4. Buka casing CPU, identifikasi dan analisa sirkuit internal, buat catatan apa saja yang ada dalam CPU tersebut. Catat juga kartu tambahan (expansion cards) jika ada.
5. Beri rekomendasi apakah CPU tersebut bisa dijadikan sebagai barang bukti fisik atau tidak.
6. Catat keseluruhan letak perangkat keras (harddisk, CD ROM, RAM dsb)
7. Dokumentasikan dalam bentuk gambar sebelum dan sesudah identifikasi dan analisa.



- ▶ Memahami media penyimpanan
Data File
 - ▶ Format
 - ▶ Partisi
- ▶ Partisi
 - ▶ Menbagi media secara logika
- ▶ File system
 - ▶ Mendefinisikan bagaimana file dinamai, disimpan, diakses dan diorganisir pada logical volume



File System

- ▶ FAT12
- ▶ FAT16 MSDos dan windows
- ▶ FAT32
- ▶ NTFS windows
- ▶ HPFS
- ▶ ext2fs Linux OS
- ▶ ext3fs
- ▶ HFS MAC OS
- ▶ HFS plus
- ▶ UFS Unix
- ▶ CDFS CDRom
- ▶ ISO 9660



- ▶ **Teknik meng-copy file**
 - ▶ Mengcopy file dan direktori secara logika tersimpan di media penyimpanan
- ▶ **Bit stream imaging**
 - ▶ Copy mebcakup free space dan slack space



- ▶ **Informasi lain** yang dibutuhkan dan menjelaskan data file sewaktu user beraktivitas :
 - ▶ Waktu modifikasi
 - ▶ Waktu pengaksesan
 - ▶ Waktu pembuatan



- ▶ Pemeriksaan dilakukan terhadap data backup

Meneriksa Data

- ▶ Proses :

- ▶ Akses read only
 - ▶ Untuk menjaga konsistensi – integritas data
- ▶ Write bloker
 - ▶ Untuk mencegah memodifikasi terhadap data yang diperiksa



- ▶ Melakukan ekstraksi data, dengan melihat kerakteristik file
- ▶ Mengextrak Data
- ▶ Jika ragu gunakan aplikasi untuk mengetahui header information file
- ▶ Contoh aplikasi :
 - ▶ Program identifyimagefile
 - ▶ Atau program lain



Menggunakan Software

- ▶ Tercdapat beberapa software foerensik untuk menangani data file :
 - ▶ Forensik
 - ▶ File viewer
 - ▶ Uncompressing files
 - ▶ Menampilkan struktur direktori dalam interface grafis
 - ▶ Mengidentifikasi file yang tidak dikenal
 - ▶ Melakukan pencarian terhadap string atau pola tertentu
 - ▶ Mengakses metadata



Ma Sistem Operasi

- ▶ Data non - volatile
 - ▶ File konfigurasi
 - ▶ Logs file
 - ▶ Application file
 - ▶ Data files
 - ▶ Swap files
 - ▶ Dump files
 - ▶ Hibernation files
 - ▶ Temporary files
- ▶ Data volatile
 - ▶ Slack space
 - ▶ Free space
 - ▶ Network configuration
 - ▶ Network connection
 - ▶ Running process
 - ▶ Open files
 - ▶ Login session
 - ▶ Operating system time



Penanganan Data Berdasarkan

- ▶ Network connection
- ▶ Login sessions
- ▶ Contents of memory
- ▶ Running processes
- ▶ Open files
- ▶ Network configuration
- ▶ Operating system time

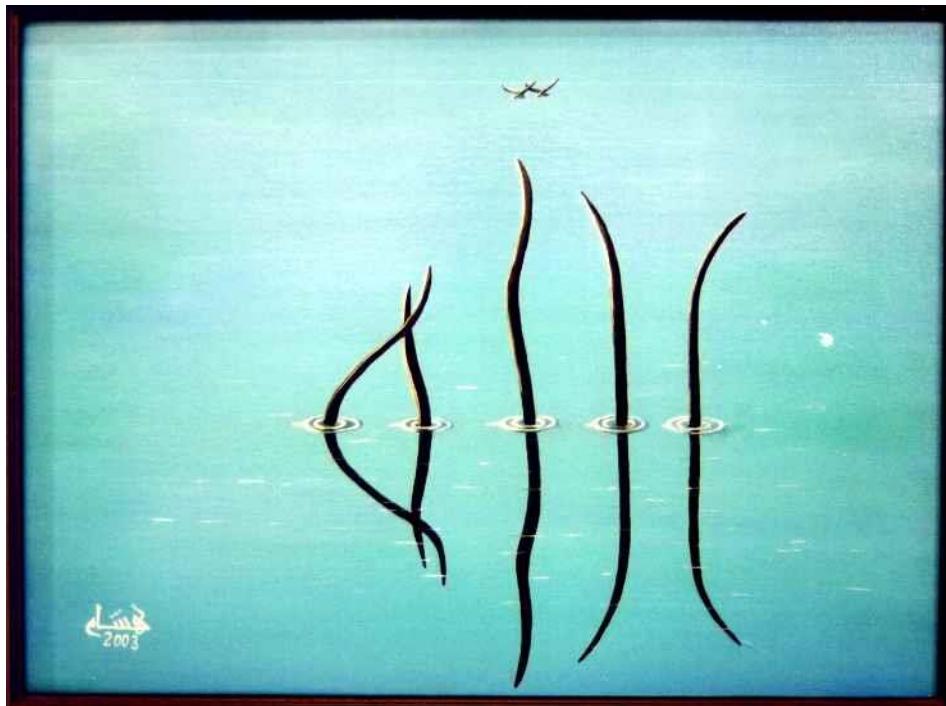


6

- ▶ Sebutkan sumber daya dalam komputer forensik ?
- ▶ Jelaskan mengapa database memiliki ruang dan fungsi tersendiri dalam konteks sumber daya ?
- ▶ Jelaskan komponen – komponen pengolahan ?
- ▶ Jelaskan pembagian dari brainware ?
- ▶ Jelaskan tentang BUS, cache memory dan RAM ?



Terima Kasih





**UNIVERSITAS
GUNADARMA**

Fakultas Teknologi Industri
Jurusan Teknik Informatika

KEAMANAN DALAM BIDANG TI

Pengantar Komputer Forensik Teknologi Informasi



KEAMANAN DALAM BIDANG TEKNOLOGI INFORMASI

- ▶ Keamanan dalam penggunaan komputer dan internet sangat tergantung minimal pada 3 pihak, yaitu :
 1. Pengguna - user
 2. Fasilitator (penyedia layanan) komputer / internet/ Penyelenggara Sistem Elektronik
 3. Penyedia produk (teknologi), yaitu perusahaan pembuat perangkat lunak (software)



KEAMANAN PADA SISI PENGGUNA

- ▶ Kesadaran pengguna komputer / internet tentang keamanan fasilitas yang digunakan merupakan hal terpenting / utama karena pada akhirnya Pengguna-lah yang biasanya paling banyak menjadi korban.
- ▶ **Penggunaan Password**
 - Password mudah ditebak, misal ; menggunakan nama anggota keluarga, tempat/ tanggal lahir, nomor telepon dll.
 - Password terlalu singkat dan umum, semakin sedikit dan umum karakter yang digunakan akan semakin mudah password ditebak. Metode *brute force attack* telah umum dipakai untuk menjebol password file-file Ms. Office, zip, rar, sistem operasi dll.



KEAMANAN PADA SISI PENGGUNA

▶ Phising (Spoofing)

- ▶ Dalam dunia hacking, teknik phising (dari kata fishing : memancing)/ spoofing bertujuan untuk mengecoh / menipu pengguna seolah-olah telah membuka situs asli, padahal situs palsu, misal situs www.klikbca.com dipalsukan menjadi wwwklikbca.com, kilkbca.com, clickbca.com, klickbca.com, dan klikbac.com.
- ▶ Metode phising juga dilakukan secara aktif, misalnya dengan mengirim email palsu berisi informasi tertentu dan penerima email dapat mengklik link yang disediakan dalam email tersebut, misalnya email tentang software terbaru, request teman, menang hadiah dsb.



Cara menghindari phising

- Usahakan selalu login menggunakan bookmark atau ketik sendiri dengan benar dan teliti pada web browser.
- Sebisa mungkin tidak melakukan login dari link, atau periksa dahulu keaslian link situs tersebut.
- Jika login pertama gagal, segera periksa halaman web sekarang dan sebelumnya, jika terbukti palsu segera ganti password.
- Pengguna Mozilla Firefox dapat menginstal add on anti phising, misal; PhishTank SiteChecker, kunjungi <https://addons.mozilla.org/en-US/firefox/addon/3840>.



KEAMANAN DI TEMPAT PUBLIK

- ▶ Jika terpaksa harus koneksi internet melalui warnet, waspadai adanya indikasi penggunaan program penyadapan dalam komputer yang kita gunakan, misal ;
 - **Keylogger**, merupakan program yang merekam setiap ketikan pada keyboard, termasuk saat login dan mengisi password.
 - **Sniffing**, merupakan kegiatan penyadapan yang dilakukan saat membuka situs yang tidak menggunakan enkripsi, sehingga semua data akan mudah terekam mentah2 karena tanpa terenkripsi. Situs yang telah menggunakan enkripsi ditandai dengan alamat yang diawali https://, bukan http://.
 - **DNS**, merupakan program yang dapat memblokkan situs yang kita ketik ke situs yang lain.
- ▶ Antisipasi untuk menghindari penyadapan adalah dengan menggunakan warnet terpercaya, hindari menyimpan password dalam web browser, hapus semua data history setelah browsing.



KEAMANAN PADA SITUS DAN SOFTWARE

- ▶ **Kesalahan pada Penyedia Layanan Web**
- ▶ Pencegahan yang dapat dilakukan atas kesalahan Penyedia Layanan Web ini, yaitu :
 - Gunakan password yang berbeda untuk situs yang berbeda, minimal memiliki 3 password untuk keperluan berbeda sesuai urgensinya.
 - Manfaatkan fitur-fitur sekuriti/ keamanan yang disediakan oleh penyedia layanan web, misal pada mail Yahoo terdapat fitur Sign Seal untuk mencegah phising.
 - Jangan gunakan fitur yang berlebihan dan membebaskan pengguna lain untuk berbuat banyak, misalnya setiap testimoni dalam Friendster harus di-approve secara manual.
 - Sering-sering membaca artikel tentang sekuriti di internet.
 - Gunakan penyedia layanan web yang kredibel, telah banyak digunakan, dan dapat diandalkan.



KEAMANAN PADA SITUS DAN SOFTWARE

- ▶ **Kesalahan Software**
- ▶ Kesalahan dapat terjadi karena program yang diinstal pada komputer memiliki kelemahan yang dapat dieksplorasi, misalnya enkripsi PDF pada Adobe Acrobat dapat langsung dijebol dengan Password Recovery buatan ElcomSoft. Ditemukan nya kelemahan pada browser dan sistem operasi juga dapat membahayakan keamanan.



KEAMANAN PADA SITUS DAN SOFTWARE

▶ Pencegahan gangguan keamanan akibat kesalahan program :

- Jangan terlalu banyak menginstal program apalagi jika tidak perlu, karena akan semakin rawan dengan masalah sekuriti, apalagi jika pembuat software kurang memperhatikan masalah keamanan.
- Pastikan bahwa firewall selalu aktif untuk memblok port-port yang tidak perlu, sehingga meminimalkan serangan trojan, worm dan pengiriman data ilegal.
- Gunakan program aplikasi versi terbaru yang sudah rilis (stabil)



KEAMANAN PADA SITUS DAN SOFTWARE

- ▶ **Penipuan Produk**
- ▶ Terdapat Penyedia jasa dan produk palsu yang menyediakan program aplikasi anti virus palsu, padahal sebetulnya dikategorikan sebagai malware atau software/ program yang berbahaya bagi komputer.
- ▶ Pengguna harus lebih berhati-hati saat mendownload atau menginstal program, termasuk menjalankan semua file yang dapat dieksekusi, seperti .exe, .com, .bat.



PROGRAM-PROGRAM YANG MENGGANGGU KEAMANAN

- **ADWARE**, program iklan yang ikut menumpang dengan software tertentu. Setelah diinstal, program ini cenderung mengganggu seperti men-download dan menyalangkan iklan-iklan secara otomatis.
- **SPYWARE**, program mata-mata yang mengirimkan informasi tanpa izin. Spyware dapat digunakan sebagai alat marketing, mencuri informasi, dan mengarahkan browser ke situs pengiklan.
- **WORM**, program yang memanfaatkan kelemahan jaringan dan mampu menduplikasikan diri tanpa campur tangan manusia. Akibatnya, bandwidth jaringan yang dimakan cukup besar dan mengakibatkan koneksi jaringan/internet lamban, komputer tidak stabil dan sering restart



PROGRAM-PROGRAM YANG MENGGANGGU KEAMANAN

- **TROJAN**, program yang seperti memberi manfaat, namun dibalik itu bisa merusak sistem operasi atau data-data. Ketika software ini dijalankan, tanpa sadar data-data dicuri atau komputer kita dikendalikan oleh pembuat trojan.
- **VIRUS**, merupakan program yang bersifat mengganggu bahkan merusak komputer dan melakukan aktifitasnya secara sembuni-sembuni tanpa sepengetahuan pemilik komputer, juga dapat menduplikasikan diri untuk menyerang komputer lain, misalnya dengan media file sharing dan flash disk,



KEAMANAN SITUS

- ▶ Pemilik Situs atau Administrator Situs perlu memperhatikan masalah keamanan suatu situs agar tidak mengganggu pengguna-nya atau bahkan ditinggalkan pengguna. Beberapa bentuk serangan yang potensial mengancam keamanan, diantaranya adalah :
 - **Hacker Log**, dalam tahap ini seorang Hacker hanya mengamati atau mungkin dalam tahap pencarian celah keamanan (security hole)
 - **Warning Message**, Hacker dalam hal ini sudah menyusup ke dalam sistem dan memberikan pesan tertentu agar Admin memperbaiki celah keamanannya.



KEAMANAN SITUS

- **Deface Site**, Hacker sudah berhasil masuk kedalam sistem sepenuhnya dan tidak segan mengubah tampilan situs terkait.
- **Destroyed Site**, Hacker pada tahap ini tidak segan untuk menghapus data-data penting, melumpuhkan situs sehingga tidak dapat diakses.



Pencegahan Gangguan Terhadap Situs

- Backup Database, segera backup database pada tempat yang aman, terutama untuk situs yang dinamis dan menggunakan banyak database.
- Update Sistem, segera update atau migrasi ke sistem yang lebih aman, terutama jika situs rawan tindak kejahanan dan banyak celah keamanan (security hole).
- Update Web Server ke versi terbaru yang sudah dipatch lubang keamanannya.
- Update Engine Web ke versi terbaru yang sudah dipatch keamanannya.
- Jangan Gunakan Nama Database yang Default.



Pencegahan Gangguan Terhadap Situs

- Jangan Gunakan Username dan Password Default, misal ; admin atau 123456.
- Memasang Firewall
- Lakukan Monitoring dan Cek Log secara berkala, meng-update patch keamanan dan mengecek berkas log karena tidak ada yang tahu kapan serangan terjadi.
- Lakukan keamanan intern dari pihak-pihak yang tidak berwenang, pisahkan ruangan server dengan ruangan lain.



Terima Kasih





**UNIVERSITAS
GUNADARMA**

Fakultas Teknologi Industri
Jurusan Teknik Informatika

TOOL FORENSIK

Pengantar Komputer Forensik teknologi Informasi



Tool Forensik

- Tool yang dipergunakan oleh ahli forensik harus **bekerja baik** dan **tidak mengubah data**. Di samping itu, **komunitas komputer forensik harus menerima tool dan hasilnya**.
- *Tool kit* untuk pengujian forensik memungkinkan untuk **mengumpulkan** dan **analisis data**, seperti tcpdump, Argus, NFR, tcpwrapper, sniffer, nstat, tripwire, diskcopy (/v pada DOS), DD pada Unix.
- Karena ahli hukum percaya bit lebih mudah dipalsukan daripada kertas, maka aturan utamanya adalah “*preserve then examine*”.



Kategori software forensik

- ▶ Forensic software tools for Windows
- ▶ Image and Document Readers
- ▶ Data Recovery/Investigation
- ▶ Password Cracking
- ▶ Network Investigation
- ▶ Phone Investigation
- ▶ PDA Investigation
- ▶ Lab Tools
- ▶ Assessments utilities
- ▶ Foundstone SASS Tools
- ▶ Intrusion Detection Tools
- ▶ Scanning Tools
- ▶ Stress Testing Tools



Tool Forensik

- ▶ Contoh dari aplikasi yang dapat digunakan dalam komputer forensik, yaitu :
 - ▶ Encase www.guidancesoftware.com
 - ▶ Forensics toolkit www.accessdata.com
 - ▶ LoPe www.evidencetalks.com
 - ▶ Forager www.inforenz.com/software/forager.html
 - ▶ X-Ways Forensics www.x-ways.net/forensic/index-m.html



Tool Forensik

- Beberapa tool untuk komputer forensik :
 - The Coroner Toolkit - Dan Farmer & Wietse Venema , www.fish.com
 - Byte Back - oleh TechAssist, <http://www.toolsthatwork.com/>
 - DriveSpy - <http://www.digitalintel.com/>
 - EnCase - oleh Guidance Software, <http://www.encase.com/>
 - Forensic ToolKit - <http://www.accessdata.com/>
 - Maresware Suite - <http://www.dmares.com/>
 - Drive Image Pro – PowerQuest
 - Linux "dd" - Red Hat
 - Norton Ghost 2000 – Symantec
 - SafeBack - New Technologies
 - SnapBack DatArrest oleh Columbia Data Products



Tool Forensik

- SC Magazine merekomendasikan DriveSpy dan EnCASE ;
- ▶ DriveSpy beroperasi pada lingkungan DOS dan memberikan semua tool yang diperlukan untuk melakukan **eksplorasi suatu media** dan **menemukan data yang relevan**.
- ▶ EnCASE memiliki GUI yang menarik dan beroperasi pada image ketimbang bukti asli. EnCase juga mengikutsertakan fungsi pembangkitan laporan dan suatu feature yang sangat berguna yang mendukung bahasa pemrograman bernama Escript. EnCase, dari Guidance Software bisa **mengelola** dan **melihat semua bukti**. Terdapat feature untuk **mencatat siapa yang bekerja** dan kapan dengan data.
- ▶ SafeBack dari New Technologies, Inc untuk **memelihara barang bukti** dipakai secara khusus oleh pihak penegak hukum AS



Tool Forensik

- Terdapat bermacam vendor perangkat lunak forensik. Paket dari The New Technologies Corporate Evidence Processing Suite menyertakan :
 - CRCND5: CRC (*checksum*) yang memvalidasi isi file.
 - DISKSIG: CRC program yang memvalidasi image backup.
 - FILELIST: Tool katalog disk untuk evaluasi komputer berdasarkan waktu
 - FILTER I: Filter berkecerdasan dengan *fuzzy logic*.
 - GETFREE: Tool pengumpulan *unallocated data*.



Tool Forensik

- GETSLACK: Tool pengumpulan untuk *file slack*.
- GETTIME: Program untuk dokumentasi waktu dan tanggal sistem sebagai barang bukti
- NTI-DOC: Program dokumentasi untuk merekam atribut, tanggal dan waktu file.
- SEIZED: Program untuk mengunci dan mengamankan komputer
- SHOWFL: Program untuk analisa keluaran daftar file
- Text Search Plus: Utility pencarian teks untuk menentukan letak kata kunci dari teks dan grafik



Tool Forensik

Key Computer Service menawarkan paket ;

- Program *password cracker*
- WIPER/WIPEDRV - Menghapus keseluruhan informasi secara lojik atau fisik dengan menulis setiap byte karakter.
- LISTDRV - utility yang menguji file FAT12, FAT16, dan FAT32 yang dibatasi koma dan tanda petik untuk disiapkan diimport ke database atau *spreadsheet*.
- CHKSUM - utility yang mengkalkulasi 64-bit *checksum* untuk drive fisik atau lojik



Tool Forensik

Key Computer Service menawarkan paket ;

- DISKIMAG - membuat copy image floppy untuk analisis
- FREESECS - Untuk mencari drive lojik spesifik tertentu untuk *free space* dan menyimpan informasi yang termuat di *unallocated space* ke file..
- DISKDUPE- utility berbahasa assembly yang membuat copy forensik dari floppy disk
- DATASNIFTER- utility yang memotong file data dari file atau *unused space* (saat recovery dengan utility seperti FREESECS).



Tool Forensik

Alternatif lain :

- Meski terdapat program khusus forensik yang tersedia, program seperti MS-DOS bisa merupakan tool forensik yang berguna. Misal perintah
 - DISKCOPY,
 - DEBUG,
 - UNDELETE, dan
 - UNFORMAT.

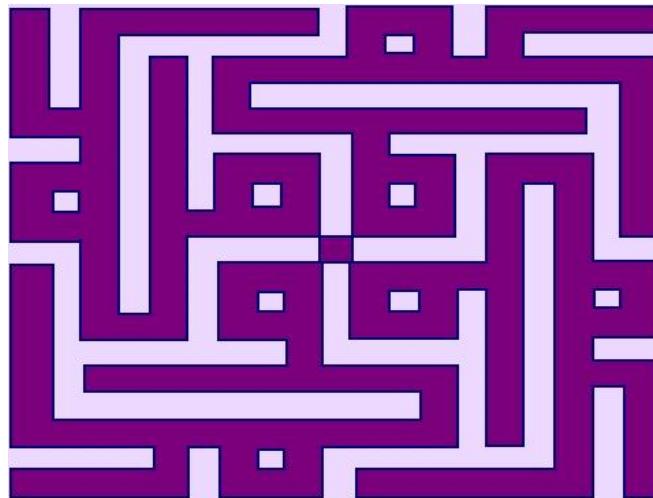


Kuis 7

1. Bagaimana cara menangani keamanan situs dan aplikasi ?
2. Bagaimana menangani keamanan di sisi pengguna ?
3. Jelaskan program apa saja yang selalu mengganggu keamanan ?
4. Bagaimana mencegah gangguan situs ?
5. Sebutkan penggolongan tool forensik ?



Terima Kasih





Pendahuluan Forensik TI

FORENSIK TEKNOLOGI INFORMASI



Pendahuluan

Perkembangan Teknologi

- Positif ; Memajuan dan kesejahteraan
- Negatif ; Kemunduran dan kerugian

Teknologi informasi dan komputer

- Dalam perkembangannya telah membuka dimensi lain dari teknologi, yaitu kejahatan komputer
- Istilah “ Cybercrime ”

Cybercrime : memunculkan masalah baru



Menentukan Kriteria Cybercrime

Terdapat 3 skenario

1. Mr X mencuri printer dari sebuah lab computer
 2. Mr X masuk ke lab computer (tanpa ijin) dan kemudian mengintai
 3. Mr X masuk ke lab komputer dimana dia punya ijin untuk masuk, dan kemudian menaruh bom untuk mematikan sistem computer di lab
- Ke 3 kejahatan tsb adalah kejahatan yang biasa terjadi
 - Apakah bisa disebut sebagai Cybercrime?



Menentukan Kriteria Cybercrime

Skenario lain:

Mr X menggunakan computer untuk menggelapkan pajak penghasilan

Mr X memnggunakan computer sebagai senjata utama melakukan kejahatan

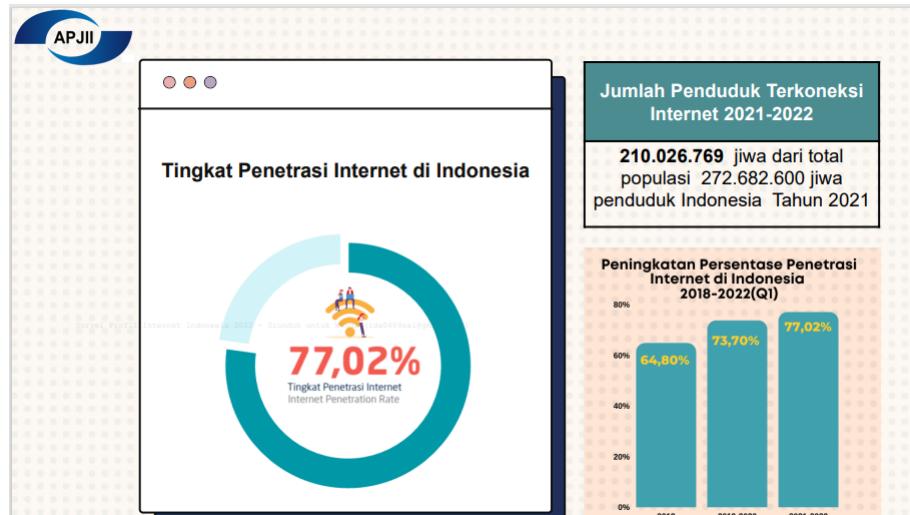
- Apakah Mr X telah melakukan kejahatan computer?
- Tetapi Mr X dapat dituntut untuk kejahatan yang biasa apabila Mr X mengubah secara manual form pendapatannya dg menggunakan pensil
- Tavani (2000) Cybercrime: kejahatan dimana Tindakan criminal hanya bisa dilakukan dengan menggunakan teknologi cyber dan terjadi di dunia cyber



Cybercrime

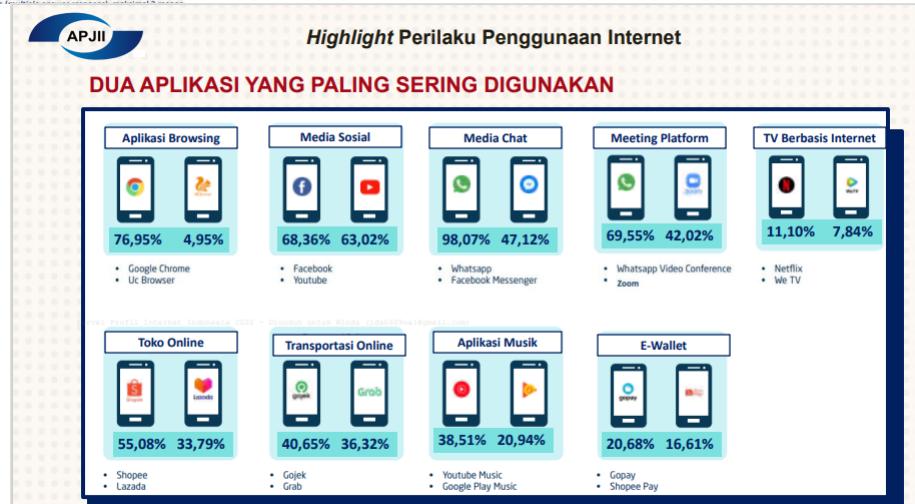
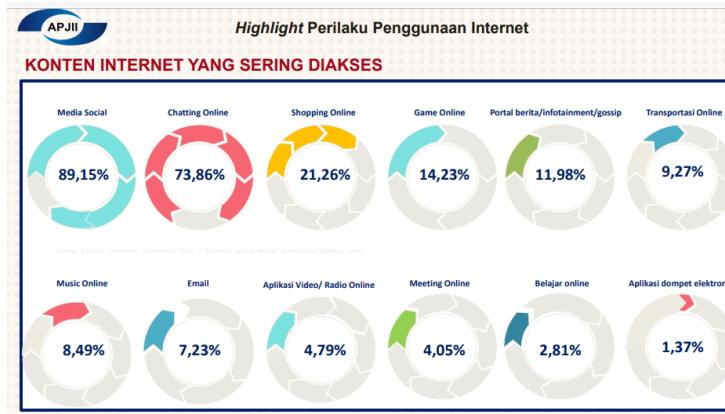
Cybercrime : Suatu Kejadian yang terjadi melalui media internet

Menurut APJII (Asosiasi Penyedia Jasa Internet Indonesia) th 2022
kurang lebih 77 persen penduduk Indonesia sudah menggunakan internet



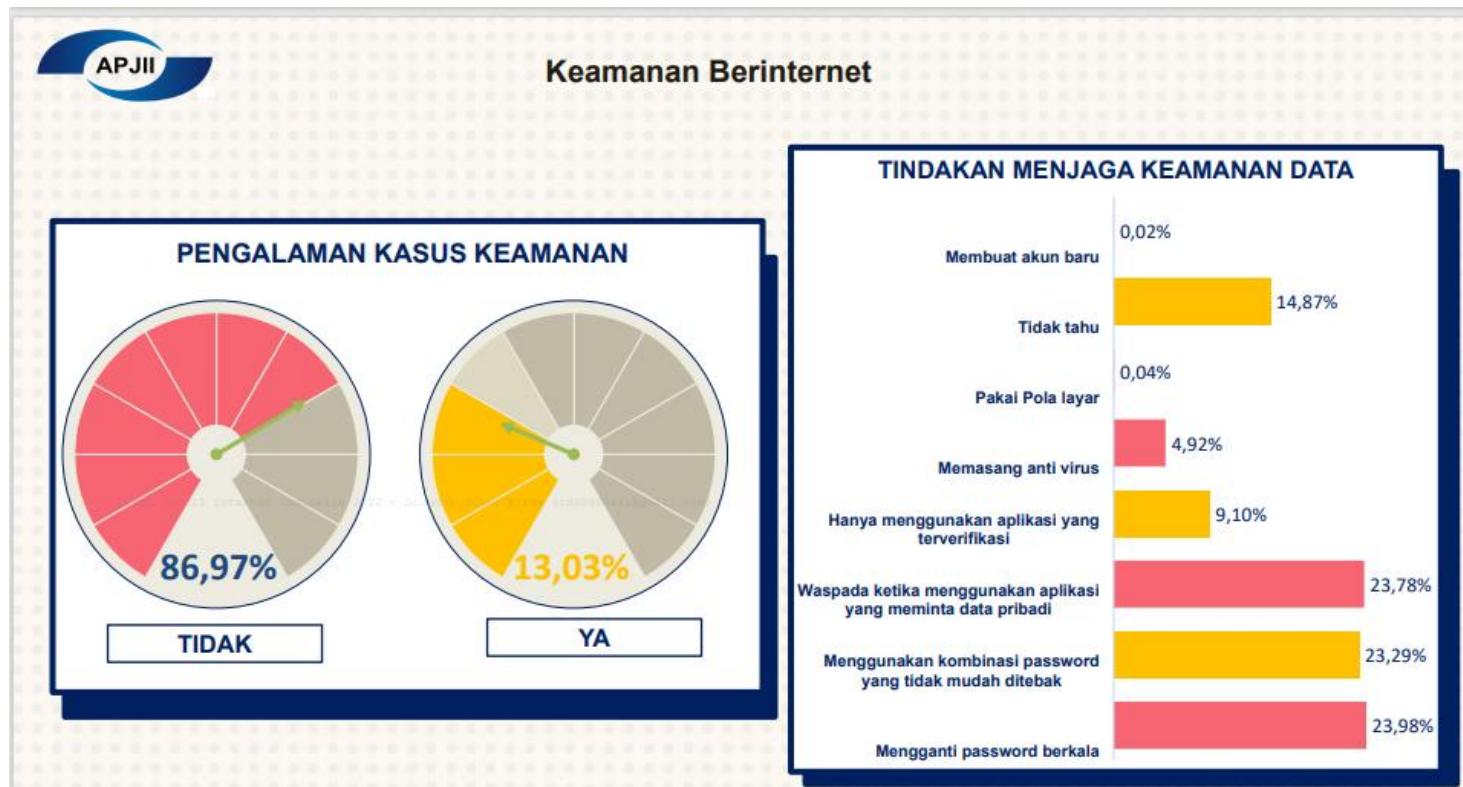


Cybercrime



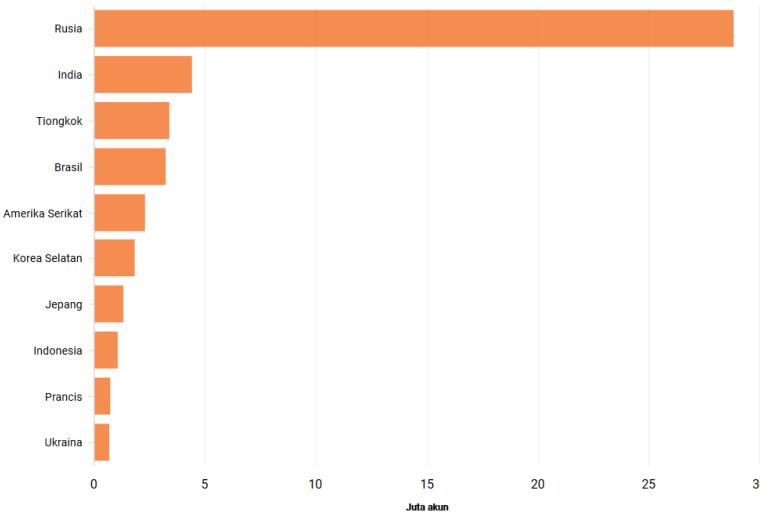


Cybercrime





Cybercrime



Indonesia masuk 10 besar negara dengan jumlah kasus kebocoran data terbanyak di internet.

Menurut data perusahaan keamanan siber *Surfshark*, ada 1,04 juta akun yang mengalami kebocoran data di Tanah Air selama kuartal II 2022.



Cybercrime

→ Menurut Badan Siber
dan Sandi Negara
([BSSN](#)),

serangan siber melanda
Indonesia

2019: 290jt

2020: 495jt

2021: 888.711.736

Jenis-jenis serangan siber yang sering terjadi

1. **Crypto Mining**
2. **Social Engineering**
3. **Kebocoran Data**
4. **Hacking**
5. **Cross-Site Scripting (XSS)**
6. **SQL Injection**
7. **Clickjacking**
8. **DoS (Denial of Service)**
9. **Credential Reuse**
10. **Man in the Middle**
11. **Insider Threat**
12. **Phishing**
13. **Ransomware**
14. **Malware**



Cybercrime

Cybercrime : Kejahatan komputer

Masalah baru

- Mikro ; Perseorangan
- Makro ; Komunal, publik dan efek domino

Cybercrime perlu ditangani sebab ;

- Sifat alami dari TI ; Memungkinkan pelaku kejahatan untuk menyembunyikan jejaknya
- Cybercrime tidak memiliki batas geografis
- Dapat dilakukan secara jarak dekan atau jauh dan hasilnya sama



Ciri Cybercrime

- Parker (1998) percaya bahwa ciri hacker computer biasanya menunjukkan sifat:
 - Terlambau lekas dewasa
 - Memiliki rasa ingin tahu yang tinggi
 - Keras hati
- Sementara banyak orang yang beranggapan bahwa hacker adalah orang yang sangat pintar dan muda
- Parker menunjukan bahwa ciri tetap dari hacker (tidak seperti kejahatan professional) adalah tidak dimotivasi oleh materi
- Hal tersebut dapat dilihat bahwa hacker menikmati apa yang mereka lakukan



Cybercrime

Target Hacker:

- Database akun kredit
- Database akun bank
- Database informasi pelanggan pembelian barang dengan CC palsu atau CC orang lain yang bukan merupakan hak kita
- Mengacaukan sistem



Kategori Cybercrime

1. Cyberpiracy

Penggunaan teknologi computer untuk:

- Mencetak ulang SW atau informasi
- Mendistribusikan informasi atau SW tsb melalui jaringan computer

2. Cybertrespass

Penggunaan teknologi computer untuk meningkatkan akses pada:

- Sistem computer sebuah organisasi atau individu
- Website yang di protect dengan password

3. Cybervandalism

Penggunaan teknologi computer untuk membuat program yang:

- Mengganggu proses transmisi informasi elektronik
- Menghancurkan data di komputer



Contoh Cybercrime Berdasarkan Kategori

1. Mendistribusikan mp4 di internet
2. Membuat Virus
3. Melakukan serangan ke sebuah web

Jadi,

1. Cyberpiracy → Kategori 1
2. Cybertrespass → Kategori 3
3. Cybervandalism → Kategori 2 dan 3



Membedakan Cybercrime dengan Cyber-Related Crime

- Banyak kejahatan yang menggunakan teknologi computer tidak bisa disebut dengan Cybercrime
- Phedophilia stalking, dan pornografi bisa disebarluaskan dengan atau tanpa cyber teknologi
- Sehingga hal diatas tidak bisa disebut Cybercrime
- Hal diatas biasanya disebut Cyber related crime



Komputer Forensik

Forensik :

- Secara Bahasa berasal dari Yunani: FORENSIS: debat atau perdebatan
- Menurut istilah: salah satu bidang ilmu pengetahuan yang digunakan untuk membantu menegakkan proses keadilan melalui proses penerapan ilmu



Komputer Forensik

Forensik :

- Suatu proses ilmiah dalam mengumpulkan, menganalisa, dan menghadirkan berbagai bukti dalam sidang pengadilan terkait adanya suatu kasus hukum.

Forensik Komputer:

- Suatu proses **mengidentifikasi, memelihara, menganalisa** dan **menggunakan bukti digital** menurut hukum yang berlaku (Moroni Parra, 2002). Istilah ini kemudian meluas menjadi **Forensik Teknologi Informasi**



Komputer Forensik ; Terminologi

Komputer forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan – penyaringan dan dokumentasi bukti komputer dalam kejadian komputer

Melakukan penyelidikan dan analisis komputer untuk menentukan potensi bukti legal



Komputer Forensik

Mengumpulkan dan analisa data dari sumber daya komputer :

- Sistem komputer
- Jaringan komputer
- Jalur komunikasi
- Media penyimpanan
- Aplikasi komputer

Forensik komputer : mengabungkan keilmuan hukum dan komputer

Forensik komputer dikenal sebagai digital forensik



Data Elektronik ; Bukti Digital

Data elektronik ;

- Dokumen, informasi keuangan, e-mail, job schedule, log, transkripsi voice-mail

Bukti digital

- Informasi yang didapat dalam bentuk / format digital (Scientific Working Group on Digital Evidence, 1999), baik berupa bukti yang riil maupun abstrak (perlu diolah terlebih dahulu sebelum menjadi bukti yang riil),



Kebutuhan Komputer Forensik

Keperluan investigasi tindak kriminal dan pelanggaran perkara pelanggaran

Rekontruksi duduk perkara insiden keamanan komputer

Upaya pemulihan akan keruksakan sistem

Troubleshooting yang melibatkan hardware dan software

Keperluan memahami sistem atau berbagai perangkat digital dengan lebih baik



Definisi Komputer Forensik

Penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk mengekstrak dan memelihara barang bukti tindakan kriminal

Menurut Judd robin ; Penerapan secara sederhana dari penyelidikan komputer dan teknik analisisnya untuk menentukan bukti – bukti hukum yang mungkin



Definisi Komputer Forensik

Menurut New Technologies ; Komputer forensik berkaitan dengan pemeliharaan, identifikasi, ekstrasi dan dokumentasi dari bukti – bukti komputer yang tersimpan dalam wujud informasi magnetik



Tujuan Komputer Forensik

- Untuk mengamankan dan menganalisis bukti digital
- Memperoleh berbagai fakta yang objektif dari suatu kejadian atau pelanggaran keamanan dari sistem informasi
- Berbagai fakta tsb akan menjadi bukti yang akan digunakan dalam proses hukum



Tahapan Komputer Forensik

1. Pengumpulan Data
2. Pengujian
3. Analisis
4. Dokumentasi dan Laporan



Latar Belakang Komputer Forensik

Bukti komputer dipersidang sudah ada sejak 40 tahun lalu

Bukti komputer tersebut dalam persidangan diperlakukan serupa dengan bukti tradisional, menjadi ambigu

Tahun 1976 US federal rules of evidence menyatakan permasalahan tersebut



Contoh Hukum Berkaitan dengan kejahatan komputer

Economic espionage act 1996

The electronic communications privacy act 1986

The computer security act 1987

Undang-Undang No. 11 tahun 2008

SK BI Nomor 27/164/KEP/DIR 31 maret 1995

Undang-undang Nomor 8 Tahun 1999



Spesifikasi Komputer Forensik

Forensik Disk

Forensik System

Forensik Jaringan Komputer

Forensik Internet





Penerapan Komputer Forensik

Prinsip

- Harus ada prinsip yang menetapkan bahwa keahlian dan pengalaman lebih penting dari pada tools

Kebijakan

- Pertimbangkan kebijakan dalam melakukan investigasi komputer forensik

Prosedur dan metode

- Buat prosedur dan metode terhadap peralatan dan mendapatkan – mengumpulkan electronic evidence



Bidang Keilmuan Forensik

Forensik pathologi

Forensik dentistry

Forensik anthropology

Forensik entomology

Psikologi forensik

Forensik kejiwaan

Fingerprint analysis

Forensik accounting

Bloodstain pattern analysis

Ballistics

Forensik toxicology

Forensik footwear evidence

Questioned document examination

Explosion analysis

Forensik teknologi informasi

Komputer forensik



Kesimpulan

Jika akan menyelesaikan suatu perkara “ misteri komputer ”, maka lakukan pengujian sistem sebagai seorang detektif bukan sebagai seorang user.

Kejahatan komputer memiliki sifat alamiah



Terima kasih





UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Informatika

Profesi Ahli Forensik TI

FORENSIK TI



Pendahuluan

Keamanan komputer berbeda dengan forensik digital, sehingga dibutuhkan pengetahuan dasar tentang keamanan komputer yang dapat menunjang untuk mempelajari teknologi forensik digital.

Meningkatnya kejahatan dibidang TI, menyebabkan profesi atau keahlian yang berkaitan dengan masalah pengungkapan adanya kejahatan ini dibutuhkan.

Seorang analisis forensik dalam pekerjaannya membantu penegak hukum atau pimpinan keamanan perusahaan



Pendahuluan

Analis Komputer Forensik sendiri adalah profesional yang terlatih khusus dan bekerja sama dengan lembaga penegak hukum serta perusahaan swasta.

Bidang pekerjaan ini menggabungkan pengetahuan ilmu komputer dengan keterampilan forensik mereka untuk memulihkan informasi dari komputer serta perangkat penyimpanan.

Seorang Analis Komputer Forensik juga bertanggung jawab mengikuti seluruh prosedur keselamatan dan privasi ketika menangani informasi keuangan maupun pribadi yang sensitif seperti dokumen, video, atau gambar.

Mereka juga harus menangani dan menerima bukti dengan cermat serta menyimpan catatan tugas dengan akurat.



Pandangan Ahli

Menurut James O. Holly [National computer forensics lab Ernst & Young

- Anda perlu membuka pintu untuk pemrosesan administratif, sipil atau kriminal dan merespon kejahatan komputer, dan penyelidik perlu menangani insiden dari awal sampai masuk kepersidangan

www.pcforensics.com

- Data yang sudah dihapus masih bisa dihidupkan lagi



Pandangan Ahli

Menurut Thomas Welch [The information security management handbook]

- Praktisi keamanan komputer harus mempedulikan teknologi dan faktor legal yang berdampak pada sistem dan penggunanya, termasuk masalah penyelidikan dan penegakan hukum





Programmer vs Ahli Komputer Forensik

Programmer ;

- Bekerja melawan diri sendiri
- Mencoba memperbaiki permasalahan yang kita buat sendiri

Ahli Komputer Forensik

- Bekerja menyelesaikan kejahatan komputer
- Melawan seorang “programmer”



Ahli computer forensik sangat dibutuhkan ?

Seorang ahli computer Forensik memiliki kriteria yang tidak dimiliki oleh orang lain sehingga sangat dibutuhkan seorang ahli computer forensic dalam penyelesaian hukum, kriteria yang dimaksudkan sebagai berikut :

- Penguasaan bagaimana modifikasi bias dilakukan pada data
- Berpikiran terbuka dan mampu berpandangan jauh
- Etika yang tinggi
- Selalu belajar
- Selalu mempergunakan data dalam mengambil kesimpulan



Tanggung Jawab dan Peran Analis Komputer Forensik

Tugas seorang Analis Komputer Forensik yaitu menggunakan berbagai metode serta teknik khusus untuk mengambil dan menganalisis data yang terkait dengan berbagai kegiatan kriminal.

Ada beberapa tanggung jawab dan peran seorang Analis Komputer Forensik yang perlu diketahui, antara lain:

- Melakukan investigasi tentang pelanggaran data dan insiden keamanan.
- Mengambil dan periksa data dari komputer serta perangkat penyimpanan elektronik.
- Membongkar serta membangun kembali sistem yang rusak untuk memulihkan data yang hilang.
- Identifikasi sistem atau jaringan tambahan yang tidak terkena serangan *cyber*.
- Kompilasi bukti untuk kasus hukum.
- Menyusun laporan teknis, menulis deklarasi, serta menyiapkan bukti untuk diadili.
- Memberi nasihat ahli kepada pengacara mengenai bukti elektronik dalam suatu kasus.
- Menyarankan penegak hukum tentang kredibilitas data yang diperoleh.
- Memberi kesaksian ahli di persidangan.



Di Mana Analis Komputer Forensik Bekerja?

- Organisasi jasa keuangan.
- Instansi dan departemen pemerintah.
- Badan intelijen pemerintah.
- Perusahaan IT dan telekomunikasi.
- Kepolisian dan lembaga penegak hukum.
- Sektor publik lainnya.



Keahlian Komputer Forensik dibutuhkan oleh :

- Jaksa Penuntut mempergunakan barang bukti komputer dalam kejahatan yang bermacam-macam, seperti obat bius, pornografi anak, pembunuhan, dan penggelapan keuangan
- Detektif swasta bisa mempergunakan rekaman pada sistem komputer untuk melacak kasus penggelapan, perceraian, diskriminasi dan pelecehan.
- Perusahaan asuransi bisa mengurangi biaya dengan bukti komputer yang menyatakan kemungkinan penggelapan pada insiden, kebakaran, atau kompensasi pekerja



Keahlian Komputer Forensik dibutuhkan oleh :

- Perusahaan menyewa ahli komputer forensik untuk menentukan bukti yang berkaitan dengan pelecehan seksual, penipuan, pencurian rahasia dagang, dan informasi rahasia internal lainnya
- Petugas penegak hukum sering memerlukan bantuan dalam persiapan penggeledahan dan penyitaan perangkat komputer.
- Perorangan kadang menyewa ahli komputer forensik untuk mendukung klaim pemutusan kerja, pelecehan seksual atau dikriminasi umur.



PENGETAHUAN YANG DIPERLUKAN AHLI FORENSIK

- Dasar-dasar hardware dan pemahaman bagaimana umumnya sistem operasi bekerja
- Bagaimana partisi drive, *hidden partition*, dan di mana tabel partisi bisa ditemukan pada sistem operasi yang berbeda
- Bagaimana umumnya *master boot record* tersebut dan bagaimana *drive geometry*
- Pemahaman untuk *hide*, *delete*, *recover* file dan directory bisa mempercepat pemahaman pada bagaimana tool forensik dan sistem operasi yang berbeda bekerja.
- Familiar dengan header dan ekstension file yang bisa jadi berkaitan dengan file tertentu



KRITERIA AHLI FORENSIK

Menurut Peter Sommer [Virtual City Associates Forensic Technician]

- Metode yang berhati-hati pada pendekatan pencatatan rekaman
- Pengetahuan komputer, hukum dan prosedur legal
- Keahlian untuk mempergunakan utility
- Kepedulian teknis dan memahami implikasi teknis dari setiap tindakan



KRITERIA AHLI FORENSIK

- Penguasaan bagaimana modifikasi bisa dilakukan pada data
- Berpikiran terbuka dan mampu berpandangan jauh
- Etika yang tinggi
- Selalu belajar
- Selalu mempergunakan data dalam mengambil kesimpulan



Aktivitas Penyelidik Forensik

- Perlindungan sistem komputer selama pengujian forensik dari semua kemungkinan perubahan, kerusakan, korupsi data, atau virus
- Temukan semua file pada sistem. Termasuk file normal, terhapus, *hidden*, *password-protected*, dan terenkripsi.
- *Recovering* file terhapus sebisa mungkin.
- Ambil isi file *hidden* juga file *temporary* atau *swap* yang dipergunakan baik oleh sistem operasi atau program aplikasi
- Lakukan akses (jika dimungkinkan secara legal) isi dari file terproteksi atau terenkripsi



Aktivitas Penyelidik Forensik

- Analisa semua data yang relevan pada area spesial di disk. Misal *unallocated* (tidak terpakai, tapi mungkin menyimpan data sebelumnya), *slack space* (area di akhir file pada *last cluster* yang mungkin menyimpan data sebelumnya juga)
- Cetak semua analisis keseluruhan dari sistem komputer, seperti halnya semua file yang relevan dan ditemukan. Berikan pendapat mengenai layout sistem, struktur file yang ditemukan, dan informasi pembuat, setiap usaha menyembunyikan, menghapus, melindungi, mengenkripsi informasi, dan lainnya yang ditemukan dan nampak relevan dengan keseluruhan pengujian sistem komputer.
- Berikan konsultasi ahli dan kesaksian yang diperlukan



KARAKTERISTIK SEORANG AHLI FORENSIK

- Pendidikan, pengalaman dan sertifikasi merupakan kualifikasi yang baik untuk profesi komputer forensik. Pendidikan dengan pengalaman memberikan kepercayaan yang diperlukan untuk membuat keputusan dan mengetahui keputusan yang tepat. Sertifikasi menunjukkan bahwa pendidikan dan pengalamannya merupakan standar yang tinggi dan dapat dipahami.
- Yakinkan pada setiap tindakan dan keputusan, agar mencukupi untuk kesaksian di pengadilan
- Semua proses dilakukan dengan menyeluruh
- Memiliki pengetahuan yang banyak mengenai bagaimana **recover** data dari berbagai tipe media



KARAKTERISTIK SEORANG AHLI FORENSIK

- Mampu memecah password dari aplikasi dan sistem operasi yang berbeda dan mempergunakannya untuk penyelidikan
- Perlu pengetahuan yang memadai, tanpanya bisa terjadi kesalahan yang akan membuat barang bukti ditolak di pengadilan. Barang bukti bisa dirusak, diubah, atau informasi yang berharga terlewat.
- Obyektif dan tidak bias, harus *fair* pada penyelidikan, dengan fakta yang akurat dan lengkap
- Inovatif dan memiliki kemampuan interpersonal yang baik
- Memiliki kemampuan verbal dan oral yang baik
- Menggunakan penalaran dan logika yang tepat



SERTIFIKASI AHLI FORENSIK TI

EnCase Certified Examiner Program (EnCE) <http://www.iacis.com>

Computer Forensics External Certification (CCE)
<http://www.giac.org/certifications/security/gcfa.php>

GCFA – GIAC Certified Forensics Analyst
<http://www.giac.org/certifications/security/gcfa.php>

Q/FE Qualified Forensics Expert
<http://www.securityuniversity.net/certification.htm>

TruSecure ICSA Certified Security Associate
<http://www.icsalabs.com>

CCE – Certified Computer Examiner <http://www.certified-computer-examiner.com/>

Computer Forensic Training Online
http://www.kennesaw.edu/coned/sci/for_online.htm



Kesimpulan

Ahli komputer forensik merupakan suatu bidang pekerjaan yang akan banyak dibutuhkan

Ahli komputer forensik merupakan area kerja relatif baru dan akan berkembang

Ahli komputer forensik dibutuhkan keahlian khusus, pengalaman dan jam terbang



Ierima Kasih





UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Informatika

UNDANG - UNDANG INFORMASI dan TRANSAKSI ELEKTRONIK



Kronologis RUU ITE

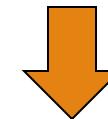
RUU PTI

(RUU Pemanfaatan Teknologi Informasi)

+

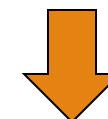
RUU IETE

(RUU Informasi Elektronik dan Transaksi Elektronik)



RUU-IKTE

(RUU Informasi, Komunikasi dan Transaksi Elektronik)



RUU-ITE

(RUU Informasi Dan Transaksi Elektronik



KETENTUAN UMUM

Informasi Elektronik :

- *Satu atau sekumpulan data elektronik, termasuk tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.*

Transaksi Elektronik :

- *Perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.*



KETENTUAN UMUM

Teknologi Informasi :

- Suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.

Dokumen Elektronik :

- Setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik



KETENTUAN UMUM

Sistem Elektronik :

- *Serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.*

Tanda Tangan Elektronik :

- *Tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikas*



KETENTUAN UMUM

Sertifikat Elektronik :

- Sertifikat yang *bersifat elektronik* yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan *status subjek hukum* para pihak dalam Transaksi Elektronik yang *dikeluarkan oleh Penyelenggara Sertifikasi Elektronik*.

Penyelenggara Sertifikasi Elektronik :

- Badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.



Asas Pemanfaatan Teknologi Informasi dan Transaksi Elektronik

- **Asas kepastian hukum** berarti landasan hukum bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik serta segala sesuatu yang mendukung penyelenggarannya yang mendapatkan pengakuan hukum di dalam dan di luar pengadilan.
- **Asas manfaat** berarti bahwa pemanfaatan teknologi informasi dan transaksi elektronik diupayakan untuk mendukung proses berinformasi sehingga dapat meningkatkan kesejahteraan masyarakat.



Asas Pemanfaatan Teknologi Informasi dan Transaksi Elektronik

-
- **Asas hati-hati** berarti para pihak yang bersangkutan harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian bagi dirinya maupun pihak lain dalam pemanfaatan teknologi informasi dan transaksi elektronik.
 - **Asas itikad baik** berarti para pihak dalam melakukan Transaksi Elektronik tidak bertujuan untuk secara sengaja dan tanpa hak atau melawan hukum mengakibatkan kerugian bagi pihak lain tanpa sepengetahuan pihak lain tersebut.



Asas Pemanfaatan Teknologi Informasi dan Transaksi Elektronik

Asas netral teknologi berarti pemanfaatan teknologi informasi dan transaksi elektronik tidak terfokus pada penggunaan teknologi tertentu sehingga dapat mengikuti perkembangan teknologi di masa mendatang



ESENSI PERTUKARAN INFORMASI

- **Informasi Elektronik**
- **Bukti Elektronik**
 - Bukti elektronik menjelaskan adanya informasi elektronik yang dipertukarkan dalam transaksi elektronik
- **Transaksi Elektronik**
 - Transaksi tidak sekedar pertukaran yang dapat dilihat secara fisik sebagaimana terjadi dalam pengertian konvensional, seperti jual dan beli, namun diperluas mencakup pertukaran informasi elektronik melalui media elektronik (Internet).



Beberapa isu

Kemampuan Internet dalam memfasilitasi transaksi antar pihak menurut Wigrantoro Roes Setiyadi, 2003 :

1. Masalah keberadaan para pihak (reality)
2. Kebenaran eksistensi dan atribut (accuracy)
3. Penolakan atau pengingkaran atas suatu transaksi (**non-repudiation**)
4. Keutuhan informasi (integrity of information)
5. Pengakuan saat pengiriman dan penerimaan
6. Privasi
7. Jurisdiksi



INFORMASI ELEKTRONIK

- Informasi Elektronik & / Dokumen Elektronik & / hasil cetaknya merupakan **alat bukti hukum yang sah**, dan merupakan **perluasan dari alat bukti** yang diatur dalam Hukum Acara yang berlaku di Indonesia.
- Informasi elektronik dapat berupa **catatan elektronik, dokumen elektronik, kontrak elektronik, surat elektronik, atau tanda tangan elektronik.**
- Informasi Elektronik & Dokumen Elektronik dinyatakan **sah** bila menggunakan Sistem Elektronik sesuai ketentuan dalam UU ITE



INFORMASI ELEKTRONIK

Ketentuan mengenai Informasi Elektronik & Dokumen Elektronik **tidak berlaku** untuk :

- Surat yang menurut UU harus ***dibuat dalam bentuk tertulis***, diantaranya yaitu surat berharga, surat yang berharga, dan surat yang digunakan dalam proses penegakan hukum acara perdata, pidana, dan administrasi negara.
- Surat beserta dokumennya yang menurut UU harus ***dibuat dalam bentuk akta notaril*** atau ***akta yang dibuat oleh pejabat pembuat akta***



INFORMASI ELEKTRONIK

Selain pengecualian sebelumnya yang mensyaratkan suatu informasi elektronik harus berbentuk tertulis atau asli, **Informasi Elektronik & Dokumen Elektronik dianggap sah** bila informasi yang tercantum didalamnya memenuhi ketentuan UU sbb :

1. Dapat terjamin keutuhannya dan dapat dipertanggungjawabkan

Pesan yang dimaksud dalam informasi elektronik tersebut tidak berubah isinya dalam proses penyimpanan, pengiriman, penerimaan dan tampilannya.

2. Dapat diakses

Informasi elektronik tersebut dapat ditelusuri keberadaannya.

3. Dapat ditampilkan sehingga menerangkan suatu keadaan

Informasi elektronik tersebut memiliki makna tertentu atau menjelaskan isi atau substansi yang dimaksud oleh penggunanya.



INFORMASI ELEKTRONIK

- Ketentuan tersebut dimaksudkan sebagai **dasar timbulnya hak**, yakni :
 - Menyatakan suatu hak,
 - Memperkuat hak yang telah ada, atau
 - Menolak hak orang lain



TANDA TANGAN ELEKTRONIK

- ❖ **Tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi ketentuan dalam undang-undang ini.**
- ❖ Undang-undang memberikan pengakuan secara tegas bahwa tanda tangan elektronik meskipun hanya merupakan suatu kode akan tetapi memiliki kedudukan yang sama dan sejajar dengan tanda tangan manual pada umumnya yang memiliki kekuatan hukum dan akibat hukum



TANDA TANGAN ELEKTRONIK

- ❖ **Teknik, metode, sarana, atau proses pembuatan tanda tangan elektronik memiliki kedudukan hukum yang sah selama memenuhi persyaratan yang ditetapkan dalam undang-undang ini.**
- ❖ Tanda tangan elektronik yang dimaksud dalam pasal ini termasuk penggunaan infrastruktur kunci publik, biometrik, kriptografi simetrik, dan sebagainya.



PENYELENGGARAAN SERTIFIKASI ELEKTRONIK

- Setiap Orang berhak menggunakan jasa Penyelenggara Sertifikasi Elektronik untuk **pembuatan Tanda Tangan Elektronik**.
- Penyelenggara Sertifikasi Elektronik harus **memastikan keterkaitan suatu Tanda Tangan Elektronik dengan pemiliknya**.
- **Penyelenggara Sertifikasi Elektronik** terdiri atas :
 - a. Penyelenggara Sertifikasi Elektronik **Indonesia**, berbadan hukum Indonesia, berdomisili di Indonesia
 - b. Penyelenggara Sertifikasi Elektronik **asing**. Jika beroperasi di Indonesia harus terdaftar di Indonesia.



PENYELENGGARAAN SERTIFIKASI ELEKTRONIK

- Penyelenggara Sertifikasi Elektronik harus menyediakan informasi yang akurat, jelas, dan pasti kepada setiap pengguna jasa, minimum meliputi :
 - a. metode yang digunakan untuk **mengidentifikasi** Penanda Tangan;
 - b. hal yang dapat digunakan untuk **mengetahui data diri** pembuat Tanda Tangan Elektronik; dan
 - c. hal yang dapat digunakan untuk **menunjukkan keberlakuan dan keamanan** Tanda Tangan Elektronik.



PENYELENGGARAAN SISTEM ELEKTRONIK

Informasi dan transaksi elektronik diselenggarakan oleh sistem elektronik yang **terpercaya**, yakni :

- 1. Andal** artinya sistem elektronik tersebut memiliki kemampuan yang sesuai dengan kebutuhan penggunaannya.
- 2. Aman** artinya sistem elektronik tersebut terlindungi baik secara fisik maupun non fisik.
- 3. Beroperasi sebagaimana mestinya** artinya sistem elektronik tersebut memiliki kemampuan sesuai spesifikasinya.

Penyelenggara sistem elektronik **bertanggung jawab** terhadap **penyelenggaraan sistem elektronik** yang diselenggarakannya. Yang dimaksud dengan bertanggung-jawab artinya **ada subyek hukum** yang bertanggung-jawab terhadap penyelenggaraan sistem elektronik tersebut.



PERSYARATAN MINIMUM SISTEM ELEKTRONIK

- a. Dapat **menampilkan kembali** Informasi Elektronik & / Dokumen Elektronik **secara utuh** sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;
- b. Dapat **melindungi ketersediaan, keutuhan, keotentikan, kerahasia-an, dan keteraksesan** Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;
- c. Dapat **beroperasi sesuai dengan prosedur** atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;
- d. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan **bahasa, informasi, atau simbol yang dapat dipahami** oleh pihak ybs dengan Penyelenggaraan Sistem Elektronik tersebut;
- e. Memiliki **mekanisme yang berkelanjutan** untuk menjaga kebaruan, kejelasan, dan kebertanggung-jawaban prosedur atau petunjuk



TRANSAKSI ELEKTRONIK

- Transaksi elektronik yang dituangkan dalam **kontrak elektronik mengikat para pihak**.
- Para pihak memiliki kewenangan untuk **memilih hukum yang berlaku** bagi transaksi elektronik internasional yang dibuatnya. Apabila para pihak tidak melakukan pilihan hukum, hukum yang berlaku didasarkan pada asas-asas Hukum Perdata Internasional.
- Para pihak memiliki kewenangan untuk menetapkan **forum pengadilan, arbitrase atau lembaga penyelesaian sengketa alternatif** yang berwenang menangani sengketa yang mungkin timbul dari transaksi elektronik. Apabila para pihak tidak melakukan pilihan forum, penetapan kewenangan forum tsb didasarkan pada asas-asas Hukum Perdata Internasional



Asas - Asas Hukum Perdata Internasional

- Asas tersebut dikenal dengan :

a. The basis of presence

Tempat tinggal tergugat

b. Principle of effectiveness

Efektivitas yang menekankan pada tempat dimana harta-harta tergugat berada



TERJADINYA TRANSAKSI ELEKTRONIK

- **Transaksi elektronik** terjadi pada saat penawaran transaksi yang dikirim pengirim telah **diterima dan disetujui penerima dengan pernyataan penerimaan secara elektronik.**
- **Penanggung-jawab atas segala akibat hukum dalam pelaksanaan transaksi elektronik , yaitu :**
 - Jika dilaksanakan sendiri → para pihak yang bertransaksi.
 - Jika melalui pemberian kuasa → pemberi kuasa.
 - Jika melalui agen elektronik → penyelenggara Agen Elektronik.

Ketentuan tersebut diatas tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.



PERBUATAN YANG DILARANG

a. Mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan sbb :

- Melanggar kesusailaan.
- Perjudian.
- Penghinaan dan atau pencemaran nama baik.
- Pemerasan dan atau pengancaman.

b. Menyebarluaskan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

c. Menyebarluaskan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA).



PERBUATAN YANG DILARANG

- d. Mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.
- e. mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun.
- f. melakukan intersepsi atau penyadapan
- g. dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik



PERBUATAN YANG DILARANG

- h. melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.
- i. memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki :
- perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan yg dilarang UU ITE.
 - sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan yang dilarang UU ITE.
- j. melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.



INTERNET BANKING

Internet Banking adalah salah satu pelayanan jasa Bank yang memungkinkan nasabah untuk memperoleh **informasi**, melakukan **komunikasi** dan melakukan **transaksi** perbankan melalui jaringan internet.

BI menolak kehadiran *Internet bank* atau bank visual dan bank yang hanya memiliki jasa layanan *Internet banking*. Kegiatan **Internet Bank only** tidak diperkenankan.

Bank penyelenggara *i-banking* harus memiliki **wujud fisik** dan **jelas keberadaannya dalam suatu wilayah hukum**. BI tidak memperkenankan kehadiran bank visual, dan tidak memiliki kedudukan hukum.

i-banking dipandang BI merupakan **salah satu jasa layanan perbankan**, sehingga bank bersangkutan harus memiliki jasa layanan, seperti layaknya bank konvesional



Ketentuan / peraturan untuk memperkecil resiko dalam penyelenggaraan Internet Banking :

1. Surat Keputusan Direksi Bank Indonesia Nomor 27/164/KEP/DIR tanggal 31 Maret 1995 tentang Penggunaan Teknologi Sistem Informasi oleh Bank.
2. Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsume
3. Ketentuan Bank Indonesia tentang Penerapan Prinsip Mengenal Nasabah (*Know Your Customer*)
4. Peraturan Bank Indonesia Nomor 5/8/PBI/2003 tentang Penerapan Manajemen Risiko Bagi Bank Umum.
5. Surat Edaran Bank Indonesia Nomor 6/ 18 /DPNP tanggal 20 April 2004 ttg **Pedoman Penerapan Manajemen Risiko Pada Aktivitas Pelayanan Jasa Bank Melalui Internet (*Internet Banking*)**.



JASA INTERNET BANKING

1. Informational Internet Banking :

Pelayanan jasa Bank kepada nasabah dalam bentuk **informasi** melalui jaringan internet dan tidak melakukan eksekusi transaksi (*execution of transaction*).

2. Communicative Internet Banking :

Pelayanan jasa Bank kepada nasabah dalam bentuk **komunikasi** atau melakukan interaksi dengan Bank penyedia layanan *internet banking* secara terbatas dan tidak melakukan eksekusi transaksi (*execution of transaction*).

3. Transactional Internet Banking :

Pelayanan jasa Bank kepada nasabah untuk **melakukan interaksi** dengan Bank penyedia layanan *internet banking* dan melakukan eksekusi transaksi (*execution of transaction*).



JASA INTERNET BANKING

Kewajiban penerapan manajemen risiko sebagaimana diatur dalam Surat Edaran Bank Indonesia Nomor 6/ 18 /DPNP tanggal 20 April 2004 hanya diberlakukan bagi penyelenggaraan ***transactional internet banking***, mengingat aktivitas internet banking ini yang **paling tinggi risikonya**

Internet banking meningkatkan risiko strategik, risiko operasional termasuk risiko keamanan dan risiko hukum serta risiko reputasi. Oleh karena itu Bank harus mengidentifikasi, mengukur, memantau dan mengendalikan risiko-risiko tersebut dengan prinsip kehati-hatian.



PEDOMAN MANAJEMEN RISIKO

1. Bank yang menyelenggarakan internet banking wajib menerapkan manajemen risiko pada aktivitas internet banking secara efektif, yang meliputi :
 - a. Pengawasan aktif Dewan Komisaris dan Direksi;
 - b. Sistem pengamanan (security control);
 - c. Manajemen risiko, khususnya risiko hukum dan risiko reputasi.
2. Penerapan manajemen risiko tersebut wajib dituangkan dalam suatu kebijakan, prosedur dan pedoman tertulis, dengan mengacu pada Pedoman Penerapan Manajemen Risiko pada Aktivitas Pelayanan Jasa Bank Melalui Internet (Internet Banking)



Pengawasan Aktif Komisaris dan Direksi Bank

Mengingat Komisaris dan Direksi Bank bertanggung jawab dalam mengembangkan strategi bisnis Bank serta menetapkan pengawasan manajemen yang efektif atas risiko, maka **penyelenggaraan aktivitas *internet banking* harus didasarkan atas kebijakan tertulis yang informatif dan jelas** yang ditetapkan oleh Komisaris dan Direksi Bank.

Pengawasan manajemen yang efektif meliputi antara lain **persetujuan** dan **kaji ulang** terhadap aspek utama dari proses pengendalian pengamanan Bank



Pengendalian Pengamanan

Proses pengendalian pengamanan memerlukan perhatian khusus dari manajemen karena adanya risiko pengamanan yang meningkat yang ditimbulkan oleh aktivitas *internet banking*.

Beberapa hal yang perlu dilakukan Bank :

1. Melakukan pengujian identitas nasabah.
2. Pengujian keaslian transaksi.
3. Penerapan prinsip pemisahan tugas.
4. Pengendalian terhadap penggunaan hak akses terhadap sistem.
5. Perlindungan terhadap integritas data maupun kerahasiaan informasi penting pada *internet banking*.



Manajemen Risiko Hukum dan Risiko Reputasi

- Untuk melindungi Bank dari risiko hukum dan risiko reputasi, pelayanan jasa *internet banking* harus dilaksanakan secara **konsisten** dan **tepat waktu** sesuai dengan harapan nasabah.
- Agar dapat memenuhi harapan nasabah, Bank harus memiliki **kapasitas, kontinuitas usaha dan perencanaan darurat yang efektif**.
- **Mekanisme penanganan kejadian (*incident response mechanism*) yang efektif** juga sangat penting untuk meminimalkan risiko operasional, risiko hukum dan risiko reputasi yang timbul dari kejadian yang tidak diharapkan.
- Selain itu Bank perlu **mengelola risiko yang timbul dari hubungan Bank dengan pihak ketiga** dalam menyelenggarakan *internet banking*.



E-COMMERCE

Definisi *E-Commerce*

- *E-Commerce* (*electronic commerce* / perdagangan elektronik), seringkali didefinisikan sebagai perdagangan atau jual beli barang dan jasa melalui medium elektronik, khususnya internet.
- E-Commerce juga dikenal sebagai e-bisnis, e-store, e-tailing dan e-market



Beberapa Keuntungan E-COMMERCE

- *Revenue stream* yang baru yang mungkin sulit atau tidak dapat diperoleh melalui cara konvensional
- Meningkatkan *market exposure*
- Menurunkan biaya operasi (*operating cost*)
- Memperpendek waktu *product-cycle*
- Meningkatkan *supplier management*
- Melebarkan jangkauan (*global reach*)
- Meningkatkan *customer loyalty*
- Meningkatkan *value chain* dengan mengkomplemenkan business practice, mengkonsolidasikan informasi dan membukanya kepada pihak-pihak yang terkait di dalam *value chain*.



UNIVERSITAS GUNADARMA
Fakultas Teknik Industri
Jurusan Informatika

KOMPUTER FORENSIK DALAM HUKUM INDONESIA



FORENSIK TI DALAM HUKUM INDONESIA

PENGERTIAN / UNSUR HUKUM

Ada beberapa pendapat mengenai pengertian hukum, dari beberapa pengertian tersebut hukum itu meliputi **beberapa unsur** sbb :

1. Aturan tentang tingkah laku masyarakat;
2. Dibuat oleh yang berwajib / berwenang ;
3. Berisi perintah dan larangan;
4. Bersifat memaksa;
5. Terhadap pelanggaran ada sanksi yang tegas.

TUJUAN HUKUM adalah menjamin adanya kepastian hukum dalam masyarakat yang bersendikan keadilan.



KATEGORI HUKUM

Hukum menurut isinya :

- **Hukum Privat (Hukum Sipil)**, hukum yang mengatur hubungan / kepentingan antar perseorangan. Contoh ; Hukum Perdata, Hukum Dagang.
- **Hukum Publik (Hukum Negara)**, hukum yang mengatur hubungan antara Negara dengan alat perlengkapan negara atau perseorangan (warga-negara). Contoh ; Hukum Pidana, Hukum Tata Negara.

Hukum menurut cara mempertahankannya :

- **Hukum Material**, hukum yang berisi peraturan berupa perintah dan larangan. Contoh ; Hukum Pidana (KUHPidana), Hukum Perdata (KUHPerdata).
- **Hukum Formal (Hukum Proses atau Hukum Acara)**, hukum yang memuat peraturan tentang cara melaksanakan dan mempertahankan Hukum Material, yaitu cara-cara mengajukan suatu perkara ke Pengadilan hingga Putusan Hakim. Contoh ; Hukum Acara Pidana (KUHAPidana), Hukum Acara Perdata (KUHAPerdata).
- **Forensik TI dikategorikan sebagai bagian dari Hukum Acara Pidana**, karena memuat tentang cara-cara/ prosedur pembuktian terjadinya suatu pelanggaran / kejahatan di bidang TI agar dapat diajukan ke Pengadilan untuk mendapatkan Putusan Hakim.



Kebijakan penanggulangan kejahatan (cybercrime) dengan Hukum Pidana perlu memperhatikan hal-hal sbb : (Mas Wigrantoro Roes Setiyadi, 2000)

1. Materi / substansi :

Apa saja yang dapat dinamakan sebagai tindak pidana di bidang TI.

2. Kebijakan Formulasi

Apakah peraturan hukuman pidana bagi kejahatan bidang TI akan berada di dalam atau di luar KUHP.

Kebijakan Hukum Pidana :

Kriminalisasi :

Suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana) (Barda Nawawi Arief, 2003)



Asas Legalitas (*Principle of Legality*) :

Asas yang menentukan bahwa tidak ada perbuatan yang dilarang dan diancam dengan pidana jika tidak ditentukan terlebih dahulu dalam perundang-undangan (Moeljatno, 2000)

Asas berlakunya hukum pidana menurut tempat (Pasal 2 – 9 KUHP) :

a. Asas Teritorial

UU Hukum Pidana Indonesia berlaku terhadap setiap orang yang melakukan pelanggaran / kejahatan di dalam wilayah RI.

b. Asas Nasional Aktif

UU Hukum Pidana Indonesia berlaku juga bagi warga negara Indonesia yang berada di luar negeri.

c. Asas Nasional Pasif

UU Hukum Pidana Indonesia berlaku bagi WNI maupun WNA diluar RI. Disini kepentingan hukum suatu negara yang dilanggar, misal : pemalsuan uang Indonesia, materai, cap negara dll

d. Asas Universal

UU Hukum Pidana Indonesia dapat juga diberlakukan thd perbuatan jahat yang bersifat merugikan keselamatan internasional



Kebijakan Formulasi terhadap tindak pidana mayantara :

1. Kejahatan biasa diatur dalam KUHP

Jika tindak pidana mayantara merupakan kejahatan biasa (ordinary crime) yang dilakukan dengan komputer teknologi tinggi (high-tech), penanggulangannya cukup dengan KUHP, baik melalui amandemen KUHP maupun perubahan KUHP secara menyeluruh.

2. Kejahatan baru diatur dalam UU Khusus

Jika tindak pidana mayantara dianggap sebagai kejahatan kategori baru (new category of crime) yang membutuhkan suatu kerangka hukum yang baru dan komprehensif untuk mengatasi sifat khusus teknologi yang sedang berkembang dan tantangan baru yang tidak ada pada kejahatan perlu diatur secara tersendiri di luar KUHP.



Peraturan mengenai Cybercrime / Kejahatan mayantara diIndonesia

1. KONSEP KUHP YANG BARU (RUU KUHP)

a. Buku I (Ketentuan Umum)

Pasal 174 :

“Barang adalah benda berwujud termasuk air dan uang giral, dan benda tidak berwujud termasuk listrik, gas, data dan program komputer, jasa, jasa telepon, jasa telekomunikasi, atau jasa komputer.”

Pasal 178 :

“Anak kunci adalah alat yang digunakan untuk membuka kunci,termasuk kode rahasia, kunci masuk komputer, kartu magnetik, atau signal yang telah diprogram yang dapat digunakan untuk membuka sesuatu oleh orang yang diberi hak untuk itu.”

Pasal 188 :

“Surat adalah selain surat yang tertulis di atas kertas, juga surat atau Data yang tertulis atau tersimpan dalam disket, pita magnetik, atau media penyimpanan komputer atau media penyimpanan data elektronik lain.”



Pasal 189 :

"Ruang adalah bentangan atau terminal komputer yang dapat diakses dengan cara-cara tertentu."

Pasal 190 :

"Masuk adalah termasuk mengakses komputer atau masuk ke dalam sistem komputer."

Pasal 191 :

"Jaringan Telepon adalah termasuk jaringan komputer atau sistem komunikasi komputer."

b. Buku II Konsep KUHP

Pasal 263 : menyadap pembicaraan di ruangan tertutup dengan alat bantu teknis

Pasal 264 : memasang alat bantu teknis untuk tujuan mendengar/ merekam pembicaraan

Pasal 266 : merekam gambar dengan alat bantu teknis di ruangan tidak untuk umum

Pasal 546 : Merusak/ membuat tidak dapat dipakai bangunan untuk sarana/ prasarana pelayanan umum (a.l. bangunan telekomunikasi/ komunikasi lewat satelit/ komunikasi jarak jauh)

Pasal 641-642 : Pencucian uang



2. UU KHUSUS CYBERCRIME / KEJAHATAN MAYANTARA

a. RUU TIPITI (Tindak Pidana Di Bidang Teknologi Informasi)

Hal- hal yang merupakan **Pelanggaran** dalam Undang-Undang ini (Bab V):

1. Memanfaatkan Teknologi Informasi dengan melawan hukum.
2. Melakukan intersepsi dengan melawan hukum.
3. Sengaja dan melawan hukum merusak atau mengganggu data yang tersimpan dalam alat penyimpan data elektronik yang tersusun sebagai bagian dari sistem komputer.
4. Sengaja menghilangkan bukti–bukti elektronik yang dapat dijadikan alat bukti sah di pengadilan yang terdapat pada suatu sistem informasi atau sistem komputer.
5. Sengaja merusak atau mengganggu sistem informasi, sistem komputer, jaringan komputer, dan Internet.
6. Memanfaatkan Teknologi Informasi untuk menipu, menghasut, memfitnah, menjatuhkan nama baik seseorang atau organisasi.
7. Memanfaatkan Teknologi Informasi untuk menyebarkan gambar, tulisan atau kombinasi dari keduanya yang mengandung sifat – sifat pornografi.
8. Memanfaatkan Teknologi Informasi untuk membantu terjadinya percobaan, atau persekongkolan yang menjurus pada kejahatan.
9. Setiap badan hukum penyelenggara jasa akses Internet atau penyelenggara layanan Teknologi Informasi, baik untuk keperluan komersial maupun keperluan internal perusahaan, dengan sengaja tidak menyimpan atau tidak dapat menyediakan catatantransaksi elektronik sedikitnya untuk jangka waktu 2 tahun.



2. UU KHUSUS CYBERCRIME / KEJAHATAN MAYANTARA
 - a. **RUU TIPITI** (Tindak Pidana Di Bidang Teknologi Informasi)
 - **Pelanggaran Pemanfaatan Teknologi Informasi** (Bab VI)
 - Pasal 9 : Kejahatan terhadap nyawa dan keselamatan negara
 - Pasal 10 : Pencurian
 - Pasal 11 : Mengakses tanpa hak
 - Pasal 12 : Mengakses tanpa hak terhadap sistem informasi strategis
 - Pasal 13 : Pemalsuan identitas
 - Pasal 14 : Mengubah dan memalsukan data
 - Pasal 15 : Mengubah data yang merugikan orang lain
 - Pasal 16 : Perbuatan asusila
 - Pasal 17 : Pornografi anak - anak
 - Pasal 18 : Bantuan kejahatan
 - Pasal 19 : Mengakses tanpa hak terhadap komputer yang dilindungi
 - Pasal 20 : Teror



- a. RUU TIPITI (Tindak Pidana Di Bidang Teknologi Informasi)
 - **Tindak Pidana Yang Berkaitan Dengan Teknologi Informasi Sebagai Sasarannya (Bab VII) :**
 - Pasal 21 : Intersepsi
 - Pasal 22 : Merusak Situs Internet
 - Pasal 23 : Penyadapan Terhadap Jaringan Komunikasi Data
 - Pasal 24 : Pemalsuan Nomor Internet Protocol
 - Pasal 25 : Merusak Database atau Enkripsi
 - Pasal 26 : Penggunaan Nama Domain Tidak Sah
 - Pasal 27 : Penyalah-gunaan Surat Elektronik
 - Pasal 28 : Pelanggaran Hak Cipta.
 - Pasal 29 : Pelanggaran Hak Privasi



b. UU ITE (Informasi dan Transaksi Elektronik) No. 11 Th. 2008

- Bab I Ketentuan Umum
- Bab II Asas dan Tujuan
- Bab III Informasi, Dokumen dan Tanda Tangan Elektronik
- Bab IV Penyelenggaraan Sertifikasi Elektronik dan Sistem Elektronik
- Bab V Transaksi Elektronik
- Bab VI Nama Domain, Hak Kekayaan Intelektual dan Perlindungan Hak Pribadi
- Bab VII Perbuatan yang Dilarang
- Bab VIII Penyelesaian Sengketa
- Bab IX Peran Pemerintah dan Peran Masyarakat
- Bab X Penyidikan
- Bab XI Ketentuan Pidana
- Bab XII Ketentuan Peralihan
- Bab XIII Ketentuan Penutup



PERATURAN INTERNASIONAL MENGENAI CYBER LAW :

1. Konvensi tentang Kejahatan Cyber (Convention on Cyber Crime)

oleh Uni Eropa (Council of Europe) di Budapest, Hongaria pada tgl 23 November 2001 mengatur tentang delik mayantara sbb: (Mardjono Reksodiputro, 2002:3-4)

- a. Delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer termasuk didalamnya: mengakses sistem komputer tanpa hak, tanpa hak menangkap/mendengar pengiriman dan pemancaran, tanpa hak merusak data, tanpa hak mengganggu sistem, menyalahgunakan perlengkapan.
- b. Delik-delik yang berhubungan dengan komputer (pemalsuan dan penipuan dengan komputer)
- c. Delik-delik yang bermuatan pornografi anak
- d. Delik-delik yang berhubungan dengan hak cipta.



PERATURAN INTERNASIONAL MENGENAI CYBER LAW :

- 2. Komisi Franken** tahun 1987 dan Kaspersen dari Belanda merumuskan sembilan bentuk penyalahgunaan komputer :
 - a. Tanpa hak memasuki sistem komputer
 - b. Tanpa hak mengambil data komputer
 - c. tanpa hak mengetahui
 - d. tanpa hak menyelin
 - e. tanpa hak mengubah
 - f. mengambil data
 - g. tanpa hak mempergunakan peralatan
 - h. sabotase sistem komputer
 - i. mengganggu telekomunikasi.

- 3. Resolusi PBB No, 55 / 63**

Berisi tentang memerangi tindakan kriminal penyalah-gunaan TI

- 4. APEC (Asia Pasific Economy Cooperation) Cybercrime Strategy**



BEBERAPA CONTOH CYBERLAW

MALAYSIA :

- Computer Crime Act (Akta Kejahatan Komputer) 1997
- Communication and Multimedia Act (Akta Komunikasi dan Multimedia) 1998
- Digital Signature Act (Akta Tandatangan Digital) 1997

SINGAPORE :

- The Electronic Act (Akta Elektronik) 1998
- Electronic Communication Privacy Act (Akta Privasi Komunikasi Elektronik) 1996

AMERIKA :

- US Child Online Protection Act (COPA) : Adult verification required on porn sites.
- US Child Pornography Protection Act : Extend law to include computer — generated child porn.
- US Child Internet Protection Act (CIPA) : Requires Schools & Libraries to filter
- US New Laws and Rulemaking : Spam, Deceptive Marketing Tactics, Mouse trapping

Terima Kasih





MELAKUKAN IDENTIFIKASI TEMPAT KEJADIAN PERKARA

Barang Bukti

Melakukan penanganan barang bukti digital di tempat kejadian perkara (TKP) dengan tetap menjaga tiga unsur penting dalam penanganan barang bukti, yaitu :

- Relevansi (*Relevance*), Barang bukti yang diambil harus berkaitan langsung dengan kasus yang sedang dihadapi
- Keandalan (*Reliability*), Barang bukti harus mampu diaudit oleh auditor independen, dapat diulang (*repeatable*), dan dapat di reproduksi kembali (*reproducibility*)
- Kecukupan (*Sufficiency*), Penyidik atau tenaga ahli harus telah mempertimbangkan bahwa materi cukup yang telah dikumpulkan untuk memungkinkan pelaksanaan penyelidikan yang tepat

Aspek Utama Penanganan Bukti Digital

1. Auditability (Dapat diaudit)

Proses yang dilakukan oleh penyidik ataupun tenaga ahli harus tersedia untuk penilaian independen untuk menentukan apakah sebuah metode ilmiah sudah sesuai.

2. Repeatability (Pengulangan)

Kemampuan dapat diulang dibuktikan ketika hasil tes yang sama dapat dihasilkan dalam kondisi sebagai berikut:

- Menggunakan prosedur pengukuran dan metode yang sama;
- Menggunakan peralatan yang sama dan dalam kondisi yang sama; dan
- Dapat diulang setiap saat setelah pengujian awal.

Aspek Utama Penanganan Bukti Digital

3. Reproducibility (Reproduktifitas - kemampuan untuk dapat diproduksi ulang) Kemampuan untuk menghasilkan hasil yang sama dengan lingkungan yang berbeda.

4. Justifiability (Dapat di-Justifikasi)

DEFR harus dapat memberikan justifikasi dari semua tindakan dan metode yang digunakan dalam menangani bukti digital (yang potensial).

Rantai Pengawasan (*Chain of Custody*)

- Catatan rantai pengawasan (*Chain of Custody record*) adalah dokumen atau serangkaian dokumen terkait yang merincikan rantai pengawasan dan catatan atas siapa yang bertanggung jawab untuk menangani bukti digital potensial, baik dalam bentuk data digital atau format lain (seperti catatan kertas).
- Tujuan menjaga catatan rantai pengawasan adalah untuk memungkinkan teridentifikasinya akses dan pergerakan bukti digital potensial pada titik waktu tertentu.

Rantai Pengawasan (*Chain of Custody*) (lanjutan)

- Catatan ini harus dibuat mulai dari proses koleksi atau akuisisi.

Hal ini biasanya akan diselesaikan dengan menelusuri riwayat bukti sejak berhasil diidentifikasi, dikoleksi atau diakuisisi oleh tim investigasi hingga status dan lokasi saat ini.

- Catatan rantai pengawasan itu sendiri dapat terdiri lebih dari satu dokumen

Rantai Pengawasan (*Chain of Custody*) (lanjutan)

- Catatan rantai pengawasan minimal harus berisi informasi berikut:
 - Tanda pengenal bukti yang unik;
 - Siapa yang mengakses bukti dan waktu serta lokasi terjadinya;
 - Siapa yang memeriksa bukti di dalam dan di luar dari fasilitas preservasi bukti dan kapan hal itu terjadi;
 - Mengapa bukti tersebut diperiksa (kasus dan tujuan) dan otoritas yang relevan, jika ada;
 - Setiap perubahan yang tidak dapat dihindari pada bukti digital potensial, serta nama individu yang bertanggung jawab karenanya dan justifikasi untuk pengubahan.

Tindakan Pencegahan di Lokasi Kejadian

- **Umum (General)**

- *Digital Evidence First Responder* (DEFR) harus melakukan tindakan untuk mengamankan dan melindungi lokasi bukti digital potensial segera setelah mereka tiba di lokasi.
- Tindakan harus mendukung hal berikut:
 - Mengamankan dan memegang kendali area yang berisi perangkat;
 - Menentukan siapa individu yang bertanggung jawab di lokasi;
 - Memastikan individu dijauhkan dari perangkat dan daya listrik;
 - Mendokumentasikan siapa saja yang memiliki akses ke lokasi dan siapa saja yang diduga memiliki alasan untuk terlibat dengan tempat kejadian perkara;

Tindakan Pencegahan di Lokasi Kejadian

Lanjutan...

- Tindakan harus mendukung hal berikut:
 - Jika perangkat dalam keadaan menyala jangan mematikannya dan jika perangkat dalam keadaan mati jangan menyalakannya;
 - Jika memungkinkan, dokumen (misalnya sketsa, foto atau video) tempat kejadian perkara, semua komponen dan kabel dalam posisi semula. Jika tidak ada kamera dan / atau kamera video yang tersedia, gambar sketsa denah system dan beri label pada port dan kabel sehingga sistem dapat divalidasi dan direkonstruksi di kemudian hari;

Tindakan Pencegahan di Lokasi Kejadian

Lanjutan...

- Tindakan harus mendukung hal berikut:
 - dan Jika diperbolehkan, lakukan pencarian di area untuk barang-barang seperti catatan tempel (*sticky note*), buku harian, kertas, computer notebook, atau perangkat keras dan manual perangkat lunak dengan rincian yang penting tentang perangkat seperti password dan PIN.

Tindakan Pencegahan di Lokasi Kejadian

- **Personel**

- Keselamatan personel yang terlibat dalam proses merupakan hal yang vital sehingga penting untuk melakukan penilaian risiko terhadap keamanan personel sebelum memulai proses.
- Hal yang harus dipertimbangkan dalam menilai risiko terhadap personil meliputi, namun tidak terbatas pada hal berikut:
 - Apakah individu yang diselidiki ada di lokasi? Jika ada, apakah mereka memiliki kecenderungan terhadap kekerasan?
 - Pada jam berapa kegiatan operasional akan dilakukan?
 - Dapatkah tempat kejadian perkara diisolasi dari kerumunan orang?

Tindakan Pencegahan di Lokasi Kejadian

- **Bukti Digital Potensial**

- DEFR harus berhati-hati Ketika menggunakan alat bantu khusus untuk mengoleksi atau mengakuisisi bukti digital potensial.
- Risiko harus dinilai untuk mengurangi peluang pada gugatan untuk kerusakan.
- Penilaian risiko melibatkan evaluasi risiko yang sistematis dan potensi dampak yang mungkin dimiliki pada investigasi bukti digital.

Tindakan Pencegahan di Lokasi Kejadian

- **Bukti Digital Potensial (lanjutan)...**

- Aspek yang perlu dipertimbangkan saat penilaian risiko untuk bukti digital potensial meliputi, namun tidak terbatas pada hal berikut:
 - Jenis metode koleksi/akuisisi apa yang akan diterapkan?
 - Peralatan apa yang mungkin diperlukan di lokasi?
 - Bagaimana tingkat volatile dari data dan informasi yang berkaitan dengan bukti digital potensial?
 - Apakah akses jarak jauh ke perangkat digital dimungkinkan dan apakah hal tersebut menimbulkan ancaman pada integritas bukti?
 - Apa yang terjadi jika data/peralatan rusak?

Peran dan Tanggung Jawab

Peran dan tanggung jawab DEFR:

- Mengidentifikasi, mengoleksi, mengakuisisi dan mempreservasi bukti digital potensial di TKP serta membuat laporan koleksi dan akuisisi
- Memastikan integritas dan keaslian bukti digital potensial

Dengan dukungan teknis di bidang terkait, *Digital Evidence Specialist (DES)* dengan membantu DEFR di TKP

Pengamanan yang Hati-hati

- Hindari tindakan yang bisa berujung pada kerusakan bukti digital potensial yang tersimpan dalam perangkat digital.
- DEFR tidak boleh mengakses perangkat digital, seperti melakukan *dump memory* dari perangkat digital yang menyala*

Pemeliharaan yang Hati-hati (lanjutan)

Ada beberapa situasi di mana tidak memungkinkan untuk mengoleksi atau mengakuisisi bukti digital potensial. DEFR harus mempertimbangkan situasi berikut, namun tidak hanya terbatas pada ini:

- Ketika tidak ada hak hukum atau otorisasi untuk mengoleksi perangkat digital;
- Ketika terdapat kewajiban untuk menggunakan metode lain
- Ketika DEFR ingin merekam modus operasi tersangka sepanjang terjadinya penyalahgunaan sistem;
- Ketika koleksi atau akuisisi harus dilakukan diam-diam, jika dianggap sah oleh yurisdiksi
- Ketika perangkat digital juga melayani pihak yang tidak terlibat.

Dokumentasi

- Dokumentasi menjadi sangat penting ketika menangani perangkat digital yang mengandung bukti digital potensial.
- DEFR harus mematuhi hal-hal berikut saat melakukan dokumentasi:
 - Setiap tindakan yang dilakukan harus didokumentasikan, Hal ini untuk memastikan bahwa tidak ada rincian yang tertinggal selama proses identifikasi, koleksi akuisisi dan preservasi.
 - Peka terhadap pengaturan waktu dan tanggal jika perangkat digital dalam keadaan menyala
 - Dokumentasikan semua yang terlihat pada layar perangkat digital
 - Setiap perpindahan perangkat digital harus didokumentasikan sesuai dengan kebutuhan persyaratan local
 - Mendokumentasikan semua pengenal unik dari perangkat digital dan bagian-bagian yang terkait seperti nomor seri dan tanda-tanda yang unik.

Pengarahan

- Umum

Sangat penting bahwa DEFR dan DES diberikan pengarahan yang cukup oleh otoritas yang berwenang apabila akan melakukan tugas-tugas mereka, dengan juga mematuhi segala hukum terkait kerahasiaan dan batasan-batasan.
- Spesifik pada Bukti Digital
 - Jenis perkara (jika diketahui);
 - Tanggal dan waktu perkara (jika diketahui);
 - Rencana investigasi;
 - Mempertimbangkan di mana dan bagaimana bukti digital potensial disimpan/dipindahkan setelah koleksi atau akuisisi.
 - Peralatan khusus yang diperlukan untuk mengakuisisi bukti digital potensial

Pengarahan (lanjutan)

- Spesifik pada Personil
 - Tugas, peran dan tanggung jawab anggota tim investigasi di TKP;
 - Apakah otoritas lain (tenaga medis, penyidik forensik biologis) diharapkan terlibat dalam investigasi;
 - Mewajibkan anggota tim untuk tidak menerima bantuan teknis dari individu yang tidak berwenang;
 - dan Mewajibkan anggota tim untuk mengikuti prosedur secara ketat dalam meminimalkan risiko perusakan bukti digital potensial.

Pengarahan (lanjutan)

- Insiden *Real-time*
- Informasi Pengarahan Lainnya

Terlepas dari bukti digital dan personel, informasi penting lainnya yang harus diarahkan kepada tim investigasi meliputi:

- Penetapan wilayah investigasi, termasuk nama organisasi, alamat dan peta lokasi (jika tersedia);
- Surat perintah penyidikan;
- Rincian surat perintah penggeledahan dan surat kuasa;
- Aspek hukum dan implikasinya;
- Kerangka waktu investigasi;
- Peralatan yang perlu dibawa ke tempat kejadian perkara investigasi;
- Informasi logistik; dan Potensi konflik kepentingan..

Contoh Identifikasi, Koleksi, Akuisisi dan Preservasi

- **Komputer, Perangkat Peripheral dan Media Penyimpanan Digital**
 - Identifikasi
 - Pencarian dan dokumentasi lokasi fisik kejadian perkara
 - Koleksi bukti Non-digital
 - Proses pengambilan keputusan untuk Koleksi atau Akuisisi (Pertemuan 7)
 - Koleksi (Pertemuan 7)
 - Perangkat digital dalam keadaan menyala
 - Perangkat digital dalam keadaan mati

Contoh Identifikasi, Koleksi, Akuisisi dan Preservasi

- **Komputer, Perangkat Peripheral dan Media Penyimpanan Digital (lanjutan)**
 - Akuisisi (Pertemuan 7)
 - Perangkat digital dalam keadaan menyala
 - Perangkat digital dalam keadaan mati
 - Perangkat digital mission-critical
 - Akuisisi parsial
 - Media penyimpanan digital
 - Preservasi

Contoh Identifikasi, Koleksi, Akuisisi dan Preservasi

- **Perangkat Jaringan** (Pertemuan 10)
 - Identifikasi
 - Pencarian dan dokumentasi lokasi fisik kejadian perkara
 - Koleksi bukti Non-digital
 - Koleksi, Akuisisi dan Preservasi
 - Pedoman untuk koleksi perangkat jaringan
 - Pedoman untuk akuisisi perangkat jaringan
 - Pedoman untuk preservasi perangkat jaringan
- **Koleksi, Akuisisi dan Preservasi CCTV** (Pertemuan 11)

Komputer, Perangkat Peripheral dan Media Penyimpanan Digital: Identifikasi

- **Pencarian dan Dokumentasi Lokasi Fisik Kejadian Perkara**
 - Komputer dianggap sebagai perangkat digital *independent* (yang berdiri sendiri) yang menerima, mengolah dan menyimpan data, serta mengeluarkan hasil.
 - Perangkat komputer ini tidak terhubung ke jaringan, tetapi dapat dihubungkan ke perangkat peripheral seperti printer, scanner, webcam, pemutar MP3, system GPS, perangkat RFID dan sebagainya.

Komputer, Perangkat Peripheral dan Media Penyimpanan Digital: Identifikasi

- (lanjutan)
 - Sebuah perangkat digital yang memiliki penghubung jaringan, tetapi tidak terhubung pada saat koleksi atau akuisisi, harus dianggap (untuk tujuan standar nasional ini) sebagai komputer independen.
 - Jika komputer dengan penghubung jaringan, tetapi tidak ditemukan kejelasan apakah terdapat koneksi, diperlukan yang dapat mengidentifikasi kemana saja perangkat dikoneksikan di masa lalu.

Komputer, Perangkat Peripheral dan Media Penyimpanan Digital: Identifikasi

- (lanjutan)
 - Biasanya tempat kejadian perkara akan berisi berbagai jenis media penyimpanan digital.
 - Media penyimpanan digital* digunakan untuk menyimpan data dari perangkat digital dan memiliki kapasitas memori yang berbeda.

Komputer, Perangkat Peripheral dan Media Penyimpanan Digital: Identifikasi

- (lanjutan)
 - DEFR harus mendokumentasikan jenis dan merk perangkat digital yang digunakan dan mengidentifikasikan semua komputer dan perangkat peripheral yang perlu diakuisisi atau dikoleksi pada tahap ini. Nomor seri, nomor lisensi dan tanda identitas lainnya (termasuk kerusakan fisik) harus didokumentasikan sedapat mungkin.
 - Pada tahap identifikasi, status komputer dan perangkat peripheral harus tetap dalam keadaan awal.

Komputer, Perangkat Peripheral dan Media Penyimpanan Digital: Identifikasi

- (lanjutan)
 - Jika komputer dalam keadaan menyala, DEFR harus memotret atau membuat dokumen tertulis dari apa yang ditampilkan pada layar. (Harus mencakup deskripsi dari apa yang sebenarnya).
 - Sebuah perangkat dengan baterai yang kemungkinan akan kehabisan daya, harus diisi tenaganya untuk memastikan informasi tidak hilang. DEFR harus mengidentifikasi dan mengoleksi pengisi baterai dan kabel selama fase ini.
 - DEFR juga harus mempertimbangkan penggunaan detektor sinyal wireless untuk mendeteksi dan mengidentifikasi sinyal wireless dari perangkat wireless yang mungkin disembunyikan.

Komputer, Perangkat Peripheral dan Media Penyimpanan Digital: Identifikasi

- **Koleksi Bukti Non-digital**
 - DEFR harus mempertimbangkan proses koleksi bukti non-digital.
 - Dalam pelaksanaannya, ketua tim harus mengidentifikasi individu-individu yang bertanggung jawab atas fasilitas tersebut di TKP.
 - Individu-individu tersebut kemungkinan dapat memberikan informasi dan dokumentasi tambahan seperti password untuk perangkat digital dan rincian lainnya yang relevan.
 - DEFR harus mendokumentasikan nama dan tugas individu-individu tersebut.

Komputer, Perangkat Peripheral dan Media Penyimpanan Digital: Identifikasi

- (lanjutan)
 - DEFR juga mungkin harus mengoleksi beberapa bukti dengan wawancara kepada individu yang mungkin memiliki informasi tentang bukti digital potensial atau perangkat digital yang akan dikoleksi. Setiap tanggapan harus didokumentasikan secara akurat.
 - Individu yang dimaksud dapat meliputi administrator sistem, pemilik perangkat dan pengguna komputer dan perangkat peripheral.
 - Selama pengumpulan bukti lisan, DEFR dapat meminta informasi tambahan seperti konfigurasi sistem dan password administrator/root. Informasi tersebut bermanfaat dalam tahap analisis bukti digital potensial.
 - Wawancara harus didokumentasikan untuk memastikan rinciannya akurat dan pernyataan yang didokumentasikan tidak dapat diubah.

Prosedur Standar Operasional (PSO) Tempat Kejadian Perkara

PSO I-01 Identifikasi Jaringan

- Identifikasi adalah sebuah aksi yang diambil untuk mengetahui barang bukti dan tindakan apa saja yang harus diambil di langkah berikutnya.
- Fase ini akan mendeteksi jaringan yang terhubung dengan perangkat. Keterhubungan perangkat dengan jaringan dapat dimanfaatkan oleh tersangka untuk melakukan penghilangan barang bukti digital dari lokasi tersangka berada.
- Tujuan dari prosedur ini adalah melakukan identifikasi terhadap keberadaan jaringan di TKP.

PSO I-01 Identifikasi Jaringan

- Ruang lingkup: PSO ini menjelaskan prosedur yang perlu diikuti dalam melakukan identifikasi keberadaan jaringan yang ada di TKP.
- Pra Kondisi : Telah melakukan fase pra identifikasi
- Persyaratan:
 - Surat izin melakukan olah TKP dari kejaksaan
 - Surat izin melakukan penanganan bukti digital di TKP
- Perangkat digital forensik di lapangan terdiri dari:
 - Jam Digital
 - Kamera Digital
 - Label barang bukti
 - Dokumentasi fase identifikasi

PSO I-01 Identifikasi Jaringan

- Pelaksana: Penyidik atau individu yang memiliki kompetensi dan ditunjuk oleh penyidik sebagai tenaga ahli.
- Batas Waktu: Batas waktu tergantung pada kondisi dan jumlah kemungkinan barang bukti yang bisa diidentifikasi.

PSO I-01 Identifikasi Jaringan

- Tahapan Pelaksanaan:

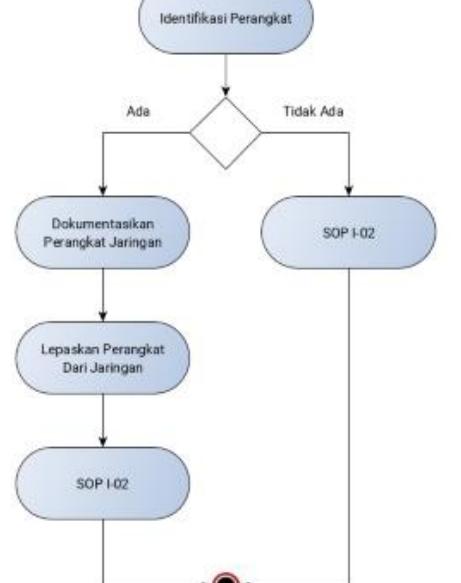
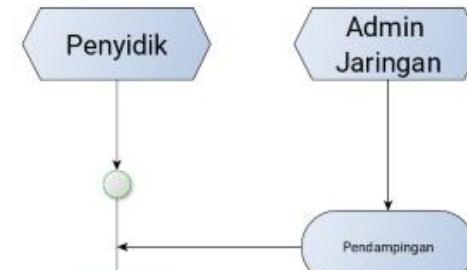
Prosedur ini dilakukan sesuai dengan situasi di TKP

- 1.Cari dan tentukan individu yang mengerti tentang jaringan di TKP dan tidak berpotensi sebagai tersangka untuk mendampingi penyidik atau tenaga ahli.
- 2.Identifikasi Apakah ada jaringan yang terhubung ke perangkat barang bukti atau tidak.

PSO I-01 Identifikasi Jaringan

- Tahapan Pelaksanaan (lanjutan):
 3. Jika terdapat jaringan :
 - a. Dokumentasikan perangkat jaringan
 - b. Lepaskan perangkat jaringan
 - c. Lanjutkan mengerjakan SOP I-02
 4. Jika tidak terdapat jaringan :
 - a. Langsung melanjutkan ke SOP I-02
 - Cek List
- Setelah melakukan tahapan akuisisi terhadap barang bukti digital, pastikan daftar berikut telah dipenuhi :
- Pastikan telah mengisi dengan lengkap dan telah ditandatangani oleh penyidik dan saksi dokumen identifikasi lapangan

Diagram PSO I-01 Identifikasi Jaringan



PSO I-02 Identifikasi Jenis Penanganan

- Terdapat dua langkah yang bisa diambil dalam penanganan barang bukti digital, yaitu: koleksi dan akuisisi.
- Koleksi adalah memindahkan barang bukti digital dari TKP ke sebuah lingkungan yang terkendali seperti laboratorium.
- Akuisisi adalah proses dimana barang bukti akan disalin sehingga menghasilkan barang bukti salinan sebagian atau penuh. Penentuan aksi yang akan diambil didasarkan pada peraturan dan perundang-undangan yang berlaku di Republik Indonesia.
- Tujuan dari prosedur ini adalah menentukan jenis penanganan barang bukti digital akan dilakukan

PSO I-02 Identifikasi Jenis Penanganan

- Ruang lingkup: PSO ini menjelaskan prosedur yang perlu diikuti ketika menentukan jenis penanganan bukti digital.
- Pra Kondisi : Telah melakukan fase pra identifikasi jaringan
- Persyaratan:
 - Surat izin melakukan olah TKP
 - Surat izin pengambilan barang bukti di TKP
- Perangkat digital forensik di lapangan terdiri dari:
 - Jam Digital
 - Kamera Digital
 - Label barang bukti
 - Dokumentasi fase identifikasi

PSO I-02 Identifikasi Jenis Penanganan

- Pelaksana: Penyidik atau individu yang memiliki kompetensi dan ditunjuk oleh penyidik sebagai tenaga ahli.
- Batas Waktu: Batas waktu tergantung pada kondisi dan jumlah kemungkinan barang bukti yang bisa diidentifikasi.

PSO I-01 Identifikasi Jaringan

- Tahapan Pelaksanaan:

Prosedur ini dilakukan sesuai dengan situasi di TKP

1. Pelaksanaan prosedur perlindungan barang bukti di TKP dibagi menjadi 2 (dua), yaitu barang bukti yang dapat dilakukan koleksi dan barang bukti yang tidak dapat dilakukan koleksi.

Berikut beberapa pertimbangan yang tidak dimungkinkannya suatu sistem di koleksi:

- a. Sistem kritis, yang diatur di Peraturan Pemerintah Republik Indonesia No. 82 tahun 2012 tentang penyelenggaraan sistem dan transaksi elektronik

PSO I-02 Identifikasi Jenis Penanganan

- Tahapan Pelaksanaan (lanjutan):
 - b. Pertimbangan Sumber daya, seperti:
 - i. ukuran penyimpanan yang diperlukan
 - ii. ketersediaan personil
 - iii. kendala waktu.
 - c. Izin yang diberikan oleh kejaksaan
- 2. Dari hasil identifikasi, tentukan langkah apa yang harus diambil oleh penyidik dalam menangani bukti digital, berikut langkah yang mungkin dipilih:
 - Koleksi perangkat dalam keadaan hidup
 - Koleksi perangkat dalam keadaan mati
 - Akuisisi perangkat dalam keadaan hidup
 - Akuisisi perangkat dalam keadaan mati

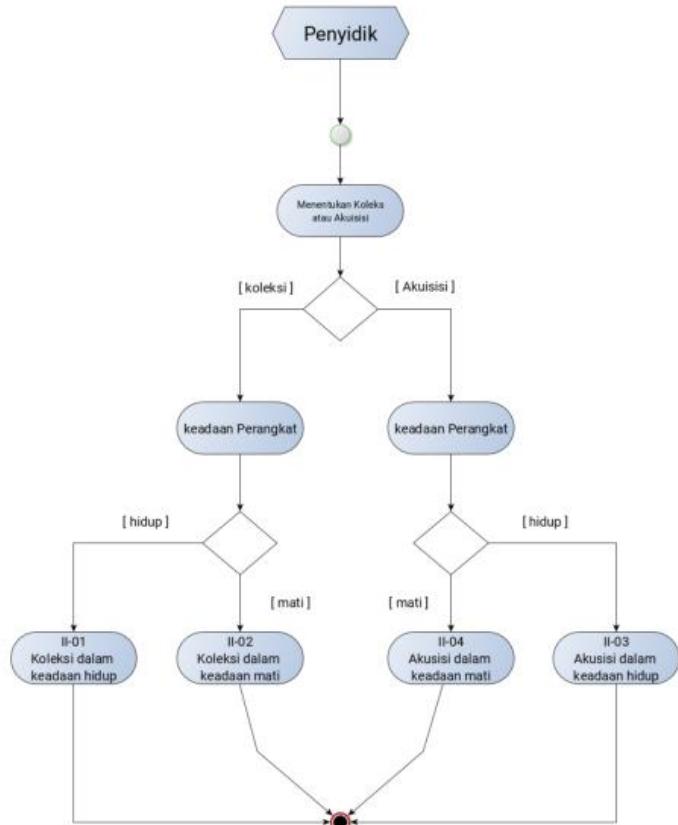
PSO I-02 Identifikasi Jenis Penanganan

- Cek List:

Setelah melakukan tahapan akuisisi terhadap barang bukti digital, pastikan daftar ikut telah dipenuhi :

- Pastikan telah mengisi dengan lengkap dan telah ditandatangani oleh penyidik dan saksi dokumen identifikasi lapangan
- Mendapatkan keputusan untuk mengambil tindakan koleksi atau akuisisi

Diagram PSO I-02 Identifikasi Jenis Penanganan



PSO I-03 Identifikasi Tanpa Izin Penanganan Bukti Digital

- Ada beberapa kasus penyidik tidak mendapatkan izin dalam melakukan penanganan barang bukti digital.
- Penyidik hanya diberikan izin untuk melakukan identifikasi TKP.
- Pada kondisi seperti ini penyidik harus mengoptimalkan kemampuan dalam mengidentifikasi perangkat yang mungkin berhubungan dengan kasus yang sedang dihadapi.
- Tujuan dari prosedur ini adalah mengidentifikasi TKP tanpa melakukan penanganan barang bukti digital dikarenakan tidak ada izin.

PSO I-03 Identifikasi Tanpa Izin Penanganan Bukti Digital

- Ruang lingkup: PSO ini menjelaskan prosedur yang perlu diikuti ketika melakukan kegiatan forensik sistem elektronik di TKP tanpa memiliki izin koleksi atau akuisisi
- Pra Kondisi : Telah melakukan fase pra identifikasi
- Persyaratan:
 - Surat izin melakukan olah TKP
- Perangkat digital forensik di lapangan terdiri dari:
 - Jam Digital
 - Kamera Digital
 - Label barang bukti
 - Dokumentasi fase identifikasi

PSO I-03 Identifikasi Tanpa Izin Penanganan Bukti Digital

- Pelaksana: Penyidik atau individu yang memiliki kompetensi dan ditunjuk oleh penyidik sebagai tenaga ahli.
- Batas Waktu: Batas waktu tergantung pada kondisi dan jumlah kemungkinan barang bukti yang bisa diidentifikasi.

PSO I-03 Identifikasi Tanpa Izin Penanganan Bukti Digital

- Tahapan Pelaksanaan:

Prosedur ini dilakukan sesuai dengan situasi di TKP

1. Jika komputer barang bukti ditemukan dalam keadaan standby atau hibernation, maka posisi komputer harus dikembalikan ke desktop sehingga ekstraksi data investigatif awal dapat dilakukan.
2. Dokumentasikan apa yang sedang berjalan di layar, termasuk tanggal/waktu lokal komputer yang dibandingkan dengan tanggal/waktu yang sebenarnya dan posisi window dari aplikasi melalui fotografi. Jika fotografi tidak dimungkinkan first responder bisa mendeskripsikan keadaan komputer secara detail.

PSO I-03 Identifikasi Tanpa Izin Penanganan Bukti Digital

- Tahapan Pelaksanaan (lanjutan):
 3. Lakukan pelabelan barang bukti. Beri label semua port dan kabel sehingga komputer dapat direkonstruksi di kemudian hari.
 4. Pastikan semua perangkat telah ditandai dan label penunjuk telah lengkap ditempel semuanya. Ketidaklengkapan dapat menimbulkan kesulitan pada proses selanjutnya dan memungkinkan perangkat ditolak oleh penguji forensik.

PSO I-03 Identifikasi Tanpa Izin Penanganan Bukti Digital

- Tahapan Pelaksanaan (lanjutan):

3. Dokumentasikan barang bukti beserta label dengan fotografi untuk menggambarkan posisi barang bukti di TKP dan foto close-up setiap barang bukti dengan menyertakan skala ukur. Dokumentasikan harus ditandatangani oleh penyidik dan saksi yang tertuang dalam berita acara serah terima barang bukti digital.
4. Lepaskan label yang melekat pada perangkat digital.

PSO I-03 Identifikasi Tanpa Izin Penanganan Bukti Digital

- Cek List:

Setelah melakukan tahapan akuisisi terhadap barang bukti digital, pastikan daftar ikut telah dipenuhi :

- Pastikan telah mengisi dengan lengkap dan telah ditandatangani oleh penyidik dan saksi dokumen identifikasi lapangan

Diagram PSO I-03 Identifikasi Tanpa Izin Penanganan Bukti Digital





MENENTUKAN OPSI UNTUK PENGUMPULAN ATAU AKUISISI

Koleksi

- Koleksi adalah proses penanganan bukti digital ketika perangkat yang berisi bukti digital potensial dipindahkan dari lokasi asli ke laboratorium atau lingkungan lain yang terkendali untuk akuisisi dan analisis selanjutnya.
- Perangkat yang berisi bukti digital potensial dimungkinkan berada di salah satu dari dua keadaan; ketika sistem dalam kondisi menyala atau ketika sistem dalam kondisi mati.

Koleksi (lanjutan)

- Proses ini meliputi pendokumentasian seluruh pendekatan, serta pembungkusan perangkat sebelum dipindahkan.
- Penting bagi DEFR dan DES untuk mengumpulkan material apapun yang mungkin berhubungan dengan informasi digital potensial (misalnya kertas dengan catatan password, stasiun dok dan konektor daya untuk perangkat sistem tertanam).
- DEFR dan DES harus mengadopsi metode koleksi terbaik yang dimungkinkan, berdasarkan situasi, biaya dan waktu, serta mendokumentasikan keputusan dalam menggunakan suatu metode tertentu.

Akuisisi

- Akuisisi adalah proses pengambilan salinan barang bukti fisik dari TKP ke media penyimpanan barang bukti.
- DEFR harus mengadopsi metode akuisisi yang sesuai berdasarkan situasi, biaya dan waktu, serta mendokumentasikan keputusan untuk menggunakan metode atau alat tertentu dengan tepat.

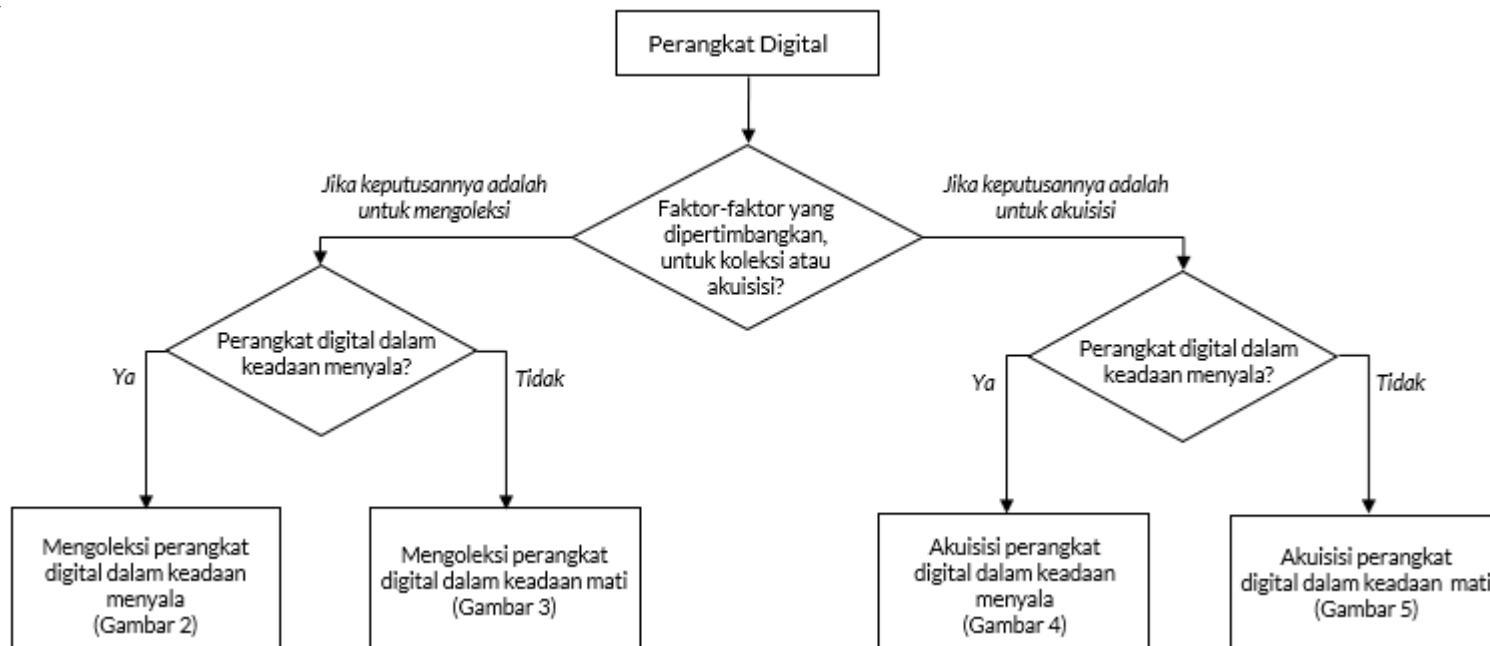
Akuisisi

- Akuisisi adalah proses pengambilan salinan barang bukti fisik dari TKP ke media penyimpanan barang bukti.
- DEFR harus mengadopsi metode akuisisi yang sesuai berdasarkan situasi, biaya dan waktu, serta mendokumentasikan keputusan untuk menggunakan metode atau alat tertentu dengan tepat.

Proses Pengambilan Keputusan untuk Koleksi atau Akuisisi

- Pengambilan keputusan untuk mengoleksi perangkat digital atau mengakuisisi bukti digital potensial, beberapa faktor harus dipertimbangkan meliputi namun tidak terbatas pada hal berikut:
 - Tingkat volatile bukti digital potensial
 - Disk yang dienkripsi seluruhnya atau Sebagian volume di mana kata sandi atau kunci mungkin berada sebagai data volatile di RAM, pada token eksternal, *smart card*, perangkat atau media lain
 - Kekritisannya dari sistem yang dibahas
 - Persyaratan hukum yurisdiksi
 - Sumber daya seperti ukuran penyimpanan yang diperlukan, ketersediaan personel, kendala waktu.

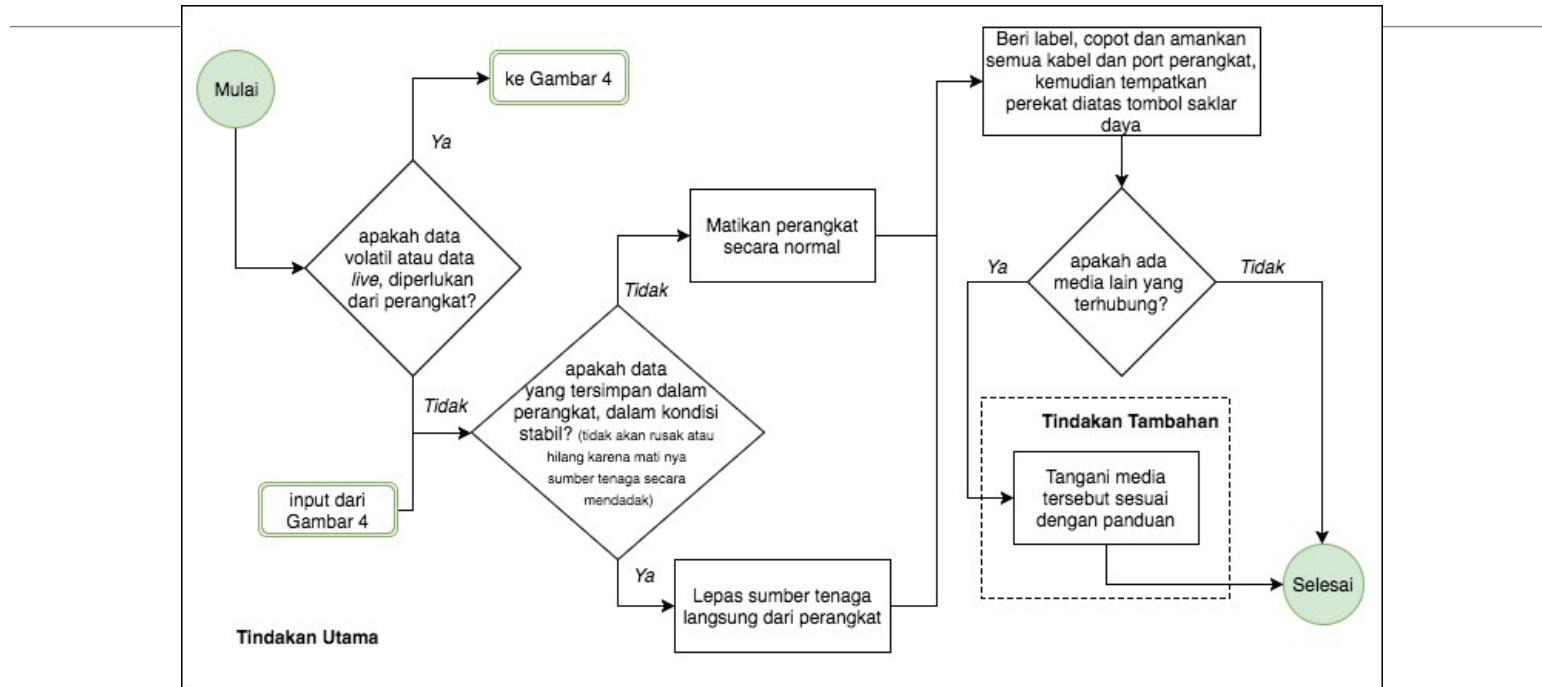
Panduan untuk Pengambilan Keputusan, Koleksi atau Akuisisi



Koleksi: Perangkat Digital dalam Keadaan Menyala

- DEFR dapat mengikuti sejumlah pedoman koleksi apabila perangkat digital dalam keadaan menyala
- Terdapat dua (2) pedoman tindakan yaitu, pedoman tindakan utama dan pedoman tindakan tambahan
- Tindakan utama harus diterapkan dalam segala sesuatu (berlaku di semua kasus)
- Tindakan tambahan harus diterapkan ketika relevan dan memungkinkan untuk diterapkan, tergantung pada perangkat atau keadaan khusus.

Panduan untuk Koleksi Perangkat Digital dalam Keadaan Menyala



Tindakan Utama: Koleksi Perangkat Digital dalam Keadaan Menyala

Tindakan utama berikut harus diikuti oleh DEFR dalam semua kasus yang melibatkan bukti digital potensial.

- Mempertimbangkan akuisisi data volatil perangkat digital dan kondisi saat sebelum mematikan sistem.
- Konfigurasi perangkat digital dapat menentukan apakah DEFR harus mematikan perangkat melalui prosedur administratif normal, atau apakah steker perangkat harus ditarik dari soket listrik.

Tindakan Utama: Koleksi Perangkat Digital dalam Keadaan Menyala

(lanjutan)

- Memberi label, melepaskan dan amankan semua kabel dari perangkat digital dan pelabelan port sehingga sistem dapat direkonstruksi pada tahap berikutnya
- Jika diperlukan, tempatkan perekat di atas saklar daya untuk mencegah perubahan kondisi saklar. Perhatikan dengan seksama apakah keadaan saklar telah didokumentasikan sebelum perekaman atau pemindahan.

Tindakan Tambahan: Koleksi Perangkat Digital dalam Keadaan Menyala

Berikut adalah kegiatan tambahan yang relevan bergantung pada konfigurasi perangkat digital tertentu.

- Jika perangkat adalah computer notebook, pastikan data volatile diakuisisi sebelum mengeluarkan baterai. DEFR harus melepaskan baterai sumber listrik utama terlebih dahulu. DEFR juga harus memperhatikan jika adaptor saya tersedia, dan jika ada, lepaskan adaptor daya setelah baterai dilepaskan.

Tindakan Tambahan: Koleksi Perangkat Digital dalam Keadaan Menyala

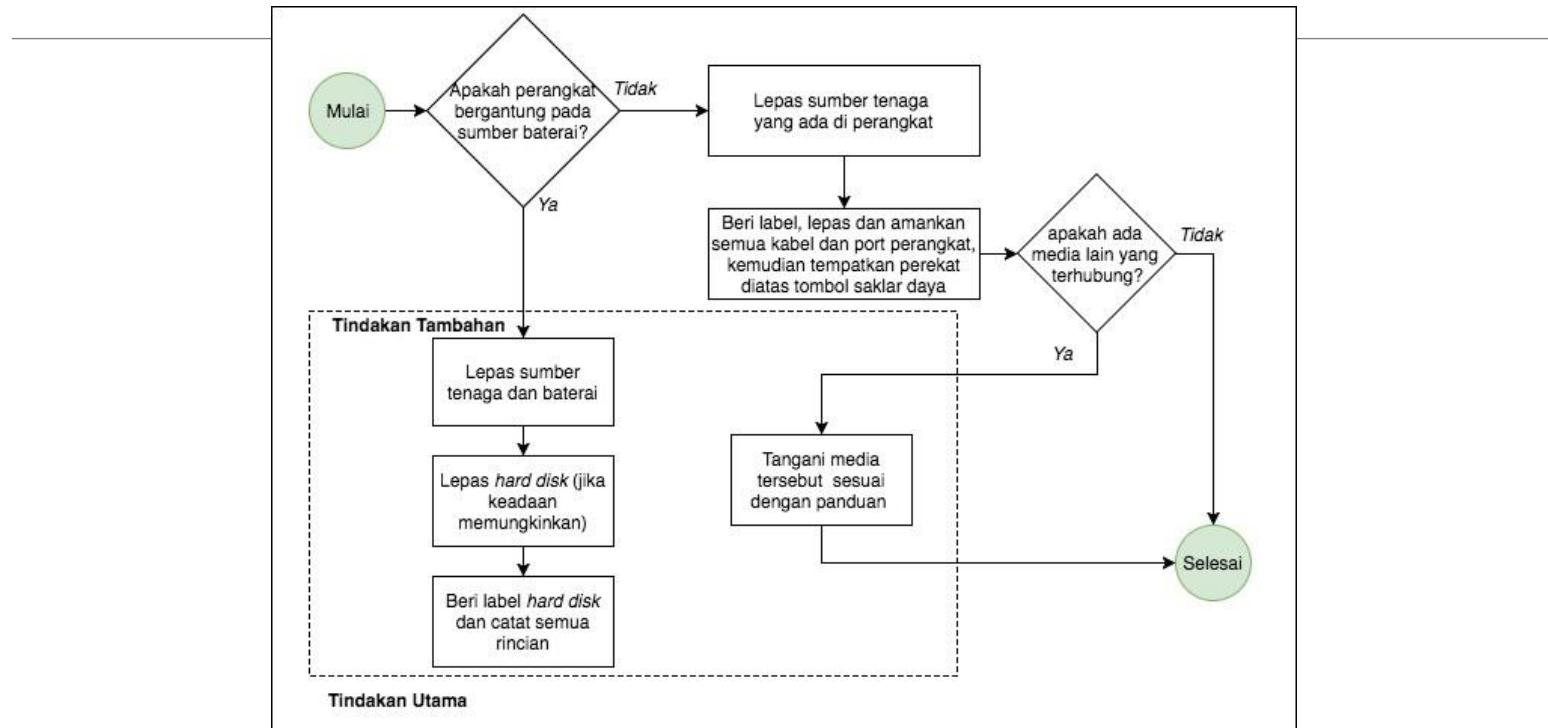
(lanjutan)

- Menempatkan perekat di atas slot floppy disk, jika tersedia
- Memastikan bahwa pemutar CD atau DVD dimasukkan kembali pada tempatnya; perhatikan apakah pemutar kosong, berisi disk, atau tidak dapat diketahui; dan tempelkan perekat pada slot drive tertutup untuk mencegahnya terbuka.

Koleksi: Perangkat Digital dalam Keadaan Mati

- DEFR dapat mengikuti sejumlah pedoman koleksi apabila perangkat digital dalam keadaan mati
- Terdapat dua (2) pedoman tindakan yaitu, pedoman tindakan utama dan pedoman tindakan tambahan
- Tindakan utama harus diterapkan dalam segala sesuatu (berlaku di semua kasus)
- Tindakan tambahan harus diterapkan ketika relevan dan memungkinkan untuk diterapkan, tergantung pada perangkat atau keadaan khusus.

Panduan untuk Koleksi Perangkat Digital dalam Keadaan Mati



Tindakan Utama: Koleksi Perangkat Digital dalam Keadaan Mati

Berikut adalah tindakan utama yang direkomendasikan untuk koleksi perangkat digital dalam keadaan mati:

- Lepaskan kabel sumber daya dengan terlebih dahulu melepaskan ujung yang terpasang ke perangkat digital dan bukan ujung yang melekat pada soket
- Putuskan hubungan dan amankan semua kabel dari perangkat digital dan beri label pada port sehingga sistem dapat direkonstruksi pada tahap berikutnya
- Tempatkan perekat di atas saklar daya jika diperlukan untuk mencegah perubahan kondisi saklar. Pertimbangkan apakah keadaan saklar telah didokumentasikan secara memadai sebelum diberi perekat atau dipindahkan.

Tindakan Tambahan: Koleksi Perangkat Digital dalam Keadaan Mati

Berikut adalah kegiatan tambahan yang relevan dengan koleksi perangkat digital dalam keadaan mati, bergantung pada konfigurasi perangkat digital yang spesifik:

- Pastikan bahwa computer notebook benar-benar dalam keadaan mati karena beberapa perangkat kemungkinan hanya dalam mode standby. Selanjutnya lepaskan baterai sumber daya utama dari computer notebook.
- Jika kondisi lapangan memaksa hard drive untuk dilepaskan, DEFR harus berhati-hati terhadap ground listrik perangkat digital untuk mencegah listrik statis merusak hard drive. Jika tidak, hard drive tidak boleh dilepaskan di lapangan. Beri label pada hard drive tersebut sebagai disk tersangka dan dokumentasikan semua rincian seperti pembuat, nama model, nomor seri dan ukuran hard drive.

Tindakan Tambahan: Koleksi Perangkat Digital dalam Keadaan Mati

(lanjutan)

- Tempatkan perekat di atas floppy disk, jika tersedia
- Pastikan bahwa penggerak CD atau DVD drive dimasukkan kembali pada tempatnya; perhatikan apakah penggerak drive kosong, berisi disk, atau tidak terperiksa; dan tempelkan perekat pada slot drive tertutup untuk mencegahnya terbuka.

Akuisisi : Perangkat Digital dalam Keadaan Menyala

Terdapat tiga (3) scenario di mana Akuisisi perlu dilakukan:

- Ketika perangkat digital dalam keadaan menyala
- Ketika perangkat digital dalam keadaan mati
- Ketika perangkat digital dalam keadaan menyala tapi tidak dapat dimatikan (seperti perangkat digital *mission-critical*)

Akuisisi : Perangkat Digital dalam Keadaan Menyala

(lanjutan)

- Jika Salinan utuh (image) tidak dapat diperoleh, Salinan akurat dari file tertentu yang diduga mengandung bukti digital potensial dapat dilakukan
- Idealnya, baik Salinan master maupun Salinan kerja lain yang terverifikasi harus dihasilkan
- Salinan master tidak boleh digunakan kembali kecuali diperlukan untuk melakukan verifikasi isi dari Salinan kerja lain atau untuk menghasilkan penganti Salinan kerja menyusul terjadinya kerusakan pada Salinan kerja pertama.

Akuisisi : Perangkat Digital dalam Keadaan Menyala

(lanjutan)

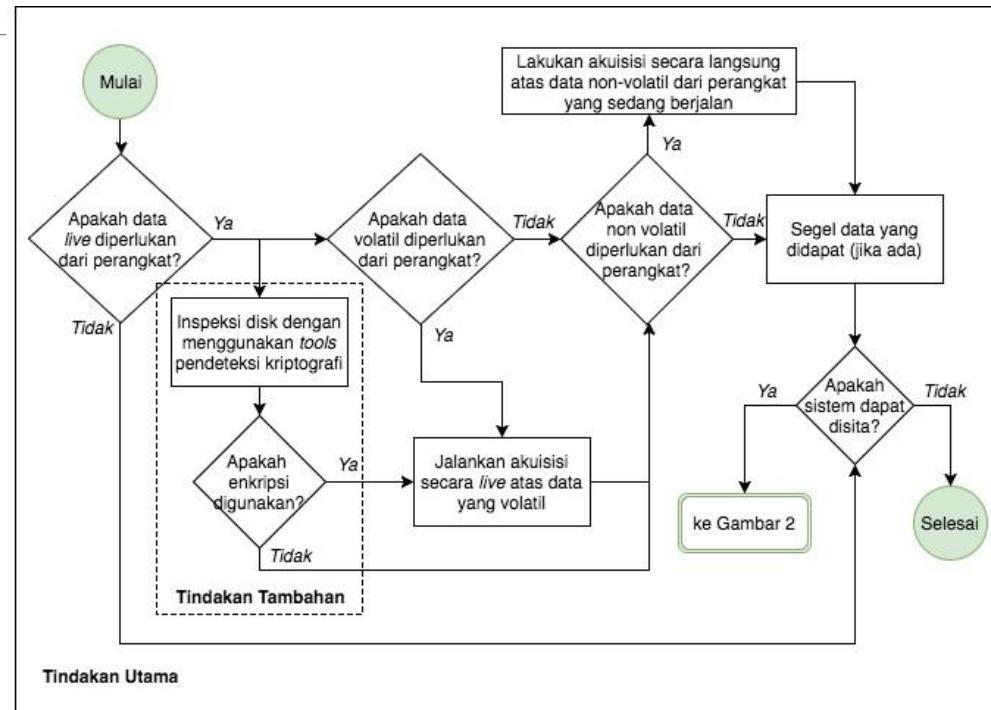
- DEFR dapat mengikuti sejumlah pedoman akuisisi apabila perangkat digital bukti ditemukan dalam keadaan menyala
- Terdapat dua (2) pedoman tindakan yaitu, pedoman tindakan utama dan pedoman tindakan tambahan
- Tindakan utama harus diterapkan dalam segala sesuatu (berlaku di semua kasus)
- Tindakan tambahan harus diterapkan ketika relevan dan memungkinkan untuk diterapkan, tergantung pada perangkat atau keadaan khusus.

Akuisisi : Perangkat Digital dalam Keadaan Menyala

(lanjutan)

- Perhatian harus diberikan terhadap kemungkinan bahwa sistem dalam keadaan menyala dapat masuk ke dalam mode screensaver atau kunci otomatis dan adanya implikasi atas usaha apapun yang dilakukan untuk mencegahnya

Panduan untuk Akuisisi Perangkat Digital dalam Keadaan Menyala



Tindakan Utama: Akuisisi Perangkat Digital dalam Keadaan Menyala

Berikut adalah tindakan utama yang direkomendasikan untuk Akuisisi perangkat digital dalam keadaan menyala:

- Pertimbangkan akuisisi bukti digital potensial yang mungkin akan hilang jika perangkat digital dimatikan.
- Melakukan akuisisi langsung (*live acquisition*) dibutuhkan untuk memperoleh data waktu nyata dari perangkat yang sedang berjalan. Akuisisi langsung dapat dilakukan pada konsol atau dari jarak jauh melalui jaringan. Prosesnya berbeda dan membutuhkan penggunaan rangkaian perangkat yang berbeda.

Tindakan Utama: Akuisisi Perangkat Digital dalam Keadaan Menyala

(lanjutan)

- DEFR tidak boleh mempercayai program sistem. Semua tindakan yang dilakukan dan perubahan yang dihasilkan pada bukti digital potensial harus didokumentasikan dan dipahami. Jika tidak memungkinkan untuk memastikan efek yang mungkin terjadi dengan dimasukkannya alat ke dalam sistem atau perubahan yang dihasilkan tidak dapat ditentukan dengan pasti, hal ini juga harus didokumentasikan.

Tindakan Utama: Akuisisi Perangkat Digital dalam Keadaan Menyala

(lanjutan)

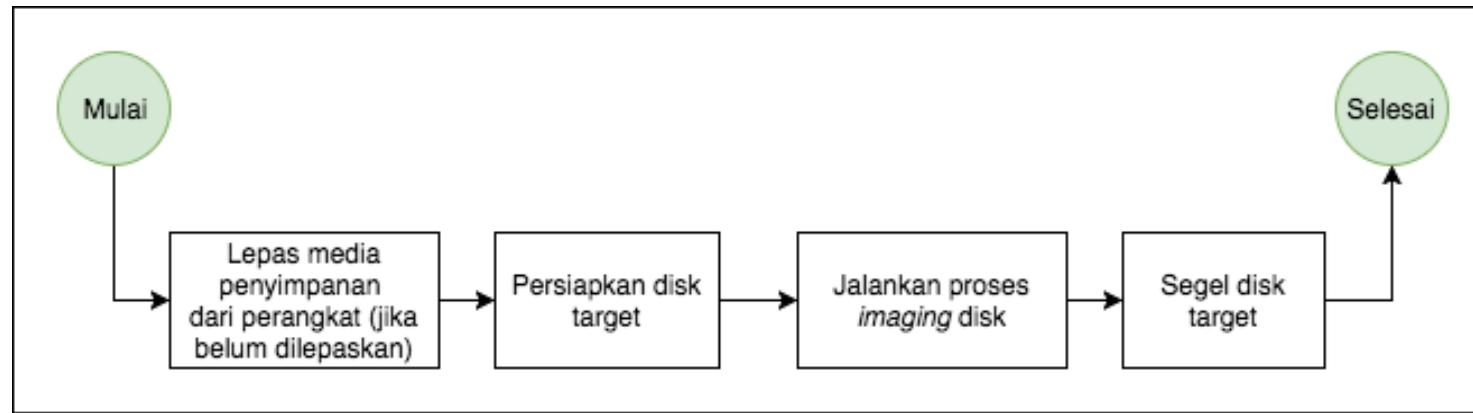
- Ketika mengakuisisi data volatil, DEFR harus menerapkan penggunaan wadah file logis jika dimungkinkan dan mendokumentasikan nilai hash-nya segera setelah wadah tersebut berisi file data volatil.
- Jalankan proses penyalinan pada media penyimpanan waktu nyata bukan volatile dengan menggunakan perangkat penyalinan yang tervalidasi.
- Salinan bukti digital yang dihasilkan harus disimpan pada media penyimpanan digital yang telah dipersiapkan untuk tujuan ini.

Tindakan Tambahan: Akuisisi Perangkat Digital dalam Keadaan Menyala

Berikut adalah kegiatan tambahan yang relevan pada akuisisi perangkat digital dalam keadaan menyala, tergantung pada konfigurasi perangkat digital yang spesifik:

- Pertimbangkan akuisisi data volatile dalam RAM ketika diduga adanya penggunaan enkripsi.
- Menggunakan acuan waktu yang terpercaya dan dokumentasikan waktu dari setiap tindakan yang dilakukan.
- Sepatutnya untuk menghubungkan DEFR dengan bukti digital potensial yang diakuisisinya, dengan menggunakan tanda tangan digital, biometrik dan fotografi.

Panduan untuk Akuisisi Perangkat Digital dalam Keadaan Mati



Akuisisi : Perangkat Digital dalam Keadaan Mati

Berikut adalah kegiatan untuk melakukan akuisisi ketika perangkat digital yang ditemukan dalam keadaan mati:

- Pastikan perangkat tersebut benar-benar dalam keadaan mati.
- Jika dinilai tepat, lepaskan media penyimpan dari perangkat digital yang dalam keadaan mati apabila belum dilepaskan. Beri label pada media penyimpanan tersebut sebagai media penyimpanan tersangka dan dokumentasikan semua rincian seperti pembuat, nama model, nomor seri dan ukuran penyimpanan.
- Menjalankan proses penyalinan dengan menggunakan alat penyalinan yang tervalidasi untuk menghasilkan salinan bukti digital dari disk tersangka.

Akuisisi : Perangkat Digital *Mission-Critical*

- Dalam beberapa kasus, perangkat digital tidak dapat dimatikan karena merupakan sistem kritis.
- Sistem ini contohnya server di pusat data yang dapat juga melayani klien yang tidak relevan, sistem pengawasan, sistem medis dan banyak lainnya yang dapat sangat terpengaruh jika mereka terganggu atau dimatikan.
- Perhatian khusus harus dilakukan ketika berhadapan dengan sistem tersebut.
- Bila perangkat digital tidak dapat dimatikan, maka dilakukan live forensic dan/atau akuisisi parsial,.

Akuisisi Parsial

Akuisisi parsial dapat dilakukan karena beberapa alasan, seperti:

- Sistem penyimpanan terlalu besar untuk diakuisisi (misalnya server database);
- Sistem terlalu kritis untuk dimatikan;
- Data yang akan diakuisisi mengandung data lain yang tidak relevan dan berada di dalam sistem yang sama; atau
- Ketika dibatasi oleh otoritas hukum seperti surat perintah penggeledahan yang membatasi ruang lingkup akuisisi.

Akuisisi Parsial (lanjutan)

Ketika keputusan telah dibuat untuk melakukan akuisisi parsial, kegiatan akuisisi harus meliputi namun tidak terbatas pada hal berikut:

- Folder, file atau kemungkinan sistem proprietary lainnya yang tersedia diidentifikasi untuk mendapatkan data yang diinginkan.
- Logical acquisition dilakukan pada data yang teridentifikasi tersebut.

Media Penyimpanan Digital

Berbagai jenis media penyimpanan digital dapat ditemukan di tempat kejadian perkara. Dalam banyak kasus, media penyimpanan digital eksternal berisi bukti yang dicari oleh analis

DEFR harus memastikan hal berikut:

- Memeriksa dan mendokumentasikan lokasi (misalnya tempat drive, kabel dan konektor, slot USB, dll), produsen, model dan nomor seri (jika ada) dari setiap media penyimpanan digital yang ditemukan.
- Menentukan pilihan untuk mengoleksi media penyimpanan digital yang teridentifikasi atau melakukan akuisisi di tempat kejadian perkara. Keputusan harus didasarkan pada sifat insiden dan ketersediaan sumber daya.

Media Penyimpanan Digital (lanjutan)

- Jika DEFR memutuskan untuk mengoleksi media penyimpanan digital dan hal tersebut diperbolehkan, media yang dikoleksi harus dibungkus atau ditempatkan dalam pembungkus yang memadai.
- Memberi label semua media penyimpanan digital dan setiap bagian yang terkait dengannya. Bila mungkin bukti harus disegel. Segel ini jelas terlihat jika diubah. DEFR atau penanggung jawab harus menandatangani label tersebut.

Media Penyimpanan Digital (lanjutan)

- Media penyimpanan digital yang dikoleksi harus disimpan dalam lingkungan yang sesuai untuk preservasi data.
- Media penyimpanan digital yang berbeda memiliki kemampuan data retensi yang berbeda. DEFR harus paham jangka waktu maksimum yang dapat diterima sesuai dengan yang telah ditentukan oleh yurisdiksi yang relevan, yang berkaitan dengan kemampuan data retensi media penyimpanan digital.

Preservasi

- Setelah proses akuisisi selesai, DEFR harus menyegel data yang diakuisisi dengan menggunakan fungsi verifikasi atau tanda tangan digital untuk menentukan bahwa salinan bukti digital sama dengan aslinya. Sebagai tambahan, aspek keamanan membutuhkan kontrol yang menerapkan prinsip-prinsip menjaga kerahasiaan, integritas dan ketersediaan bukti digital potensial. Untuk melindungi terhadap perusakan, aspek lingkungan harus ditangani dengan tindakan yang sesuai.

Preservasi (lanjutan)

DEFR harus memastikan hal berikut:

- Menggunakan fungsi verifikasi yang tepat untuk memberikan bukti bahwa file yang disalin sama dengan aslinya.
- Mengasosiasikan DEFR dengan bukti digital potensial yang diakuisisinya, menggunakan tanda tangan digital atau biometrik, dan fotografi.
- Semua perangkat digital yang dikoleksi harus dipreservasi dengan tepat. Perangkat digital dengan jenis yang berbeda memerlukan metode preservasi yang berbeda. Bukti digital

A large, colorful word cloud centered around the words "thank you" in various languages. The words are rendered in different colors and sizes, creating a dense and visually appealing composition. The languages represented include German (danke), Chinese (謝謝), French (merci), Spanish (gracias), Turkish (teşekkür ederim), Russian (спасибо), Polish (dziękuje), Portuguese (obrigado), and many others like English, Dutch, Italian, and Korean.



PENANGANAN BARANG BUKTI ELEKTRONIK
DALAM KEADAAN HIDUP

Koleksi Perangkat dalam Keadaan Hidup

Tujuan

- Mengumpulkan bukti digital dalam keadaan hidup.
- Dipindahkan ke laboratorium untuk diakuisisi dan dianalisis.

Pra-kondisi & Persyaratan

- Telah melakukan Pra Identifikasi, Identifikasi Jaringan, dan Identifikasi jenis penanganan
- Perangkat dalam keadaan hidup
- Memiliki surat perintah melakukan koleksi barang bukti digital

Peralatan

- Jam digital
- Kamera digital
- Media baru atau telah dilakukan zero format
- Toolkit (Tang, obeng, dll)
- Kantong atau kardus barang bukti digital
- Label barang bukti
- Dokumen barang bukti dan *chain of custody*

Dokumen Barang Bukti

- Dokumen barang bukti digital
- Dokumen perangkat dalam keadaan hidup
- Dokumen Barang bukti non-digital
- Dokumen barang bukti harddisk
- Dokumen barang bukti media removable (jika ada)
- Dokumen pengiriman barang bukti digital

Tahapan Pelaksanaan (Tahap 1)

- Jika komputer barang bukti dalam keadaan *standby* atau *hibernation*, kembalikan ke posisi *desktop*
- Jika komputer tersebut diproteksi *password user*, dapat memintanya ke pemilik barang bukti.

Tahapan Pelaksanaan (Tahap 2)

- Dokumentasikan yang sedang berjalan di layar, seperti:
 - Tanggal/waktu lokal komputer,
 - Posisi *window* pada aplikasi melalui fotografi,
 - Dsb.
- Dokumen Identifikasi lapangan

Tahapan Pelaksanaan (Tahap 3)

- Cari di TKP
 - catatan harian,
 - buku agenda,
 - atau potongan kertas yang berisi *password*
- Dokumen barang bukti non digital

Tahapan Pelaksanaan (Tahap 4)

- Catat waktu sistem
- Catat waktu di jam penyidik
- dokumen perangkat dalam keadaan hidup

Tahapan Pelaksanaan (Tahap 5)

- Menyalin data *live memory*
 - Sistem Operasi Windows 32bit, dapat dilihat pada Juknis J-03
 - Sistem Operasi Windows 64bit, dapat dilihat pada Juknis J-04
 - Sistem Operasi GNU/Linux (32/64 bit), dapat dilihat pada Juknis J-05

Tahapan Pelaksanaan (Tahap 6)

- Dokumentasikan kondisi barang bukti digital
 - Sistem operasi windows, dapat dilihat pada Juknis J-11
 - Sistem operasi Linux, dapat dilihat pada Juknis J-12

Tahapan Pelaksanaan (Tahap 7)

- Catat waktu di sistem dan waktu di jam penyidik.
- Sebagai waktu mematikan perangkat.

Tahapan Pelaksanaan (Tahap 8)

- Matikan perangkat, sesuai dengan Juknis J-09

Tahapan Pelaksanaan (Tahap 9)

- Cari media penyimpanan lain
- Mungkin berhubungan dengan kasus yang dihadapi

Tahapan Pelaksanaan (Tahap 10)

- Beri label barang bukti
- Label semua port dan kabel

Tahapan Pelaksanaan (Tahap 11)

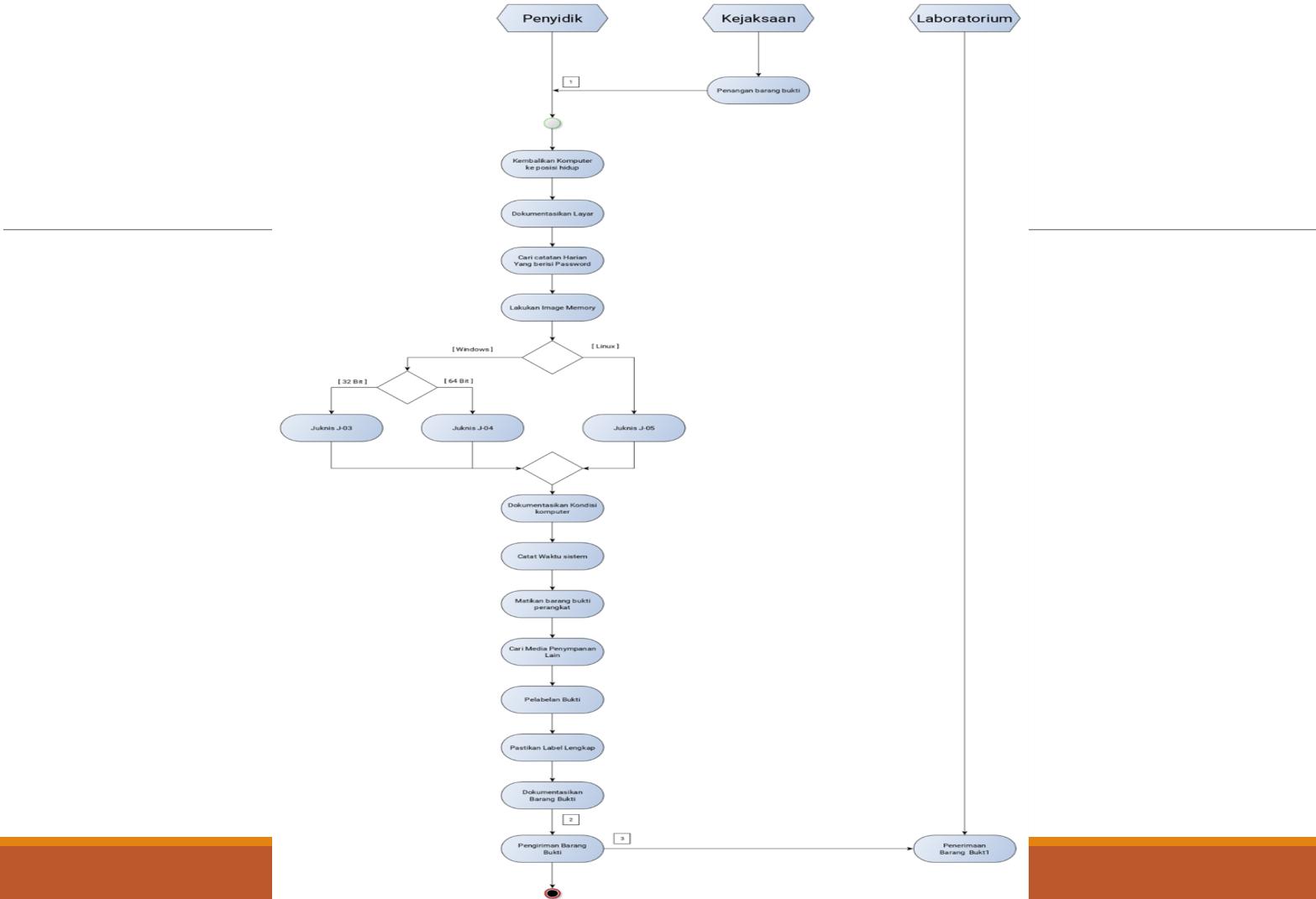
- Dokumentasikan barang bukti beserta label dengan fotografi
- Foto close-up setiap barang bukti
- Dokumentasi ditandatangani oleh kedua belah pihak

Tahapan Pelaksanaan (Tahap 12)

- Barang bukti dibawa ke laboratorium
- Pengiriman barang bukti tersebut harus disertai berita acara pengiriman barang bukti digital

Cek List

- Pastikan telah mengisi dokumen dengan lengkap dan telah ditandatangani oleh penyidik dan saksi.
- Barang bukti dikemas dengan rapi dan di segel.



Akuisisi Perangkat dalam Keadaan Hidup

Tujuan

- Memproduksi salinan barang bukti di TKP
- Secara menyeluruh atau sebagian

Pra-kondisi & Persyaratan

- Telah melakukan Pra Identifikasi, Identifikasi Jaringan, dan Identifikasi jenis penanganan
- Perangkat dalam keadaan hidup
- Memiliki surat perintah melakukan akuisisi barang bukti digital

Peralatan

- Jam digital
- *Notebook forensik*
- Media baru atau telah dilakukan *zero format*
- Toolkit (Tang, obeng, dll)
- Dokumen barang bukti dan *chain of custody*

Dokumen Barang Bukti

- Dokumen barang bukti digital
- Dokumen perangkat dalam keadaan hidup
- Dokumen Barang bukti non-digital
- Dokumen Barang bukti RAM
- Dokumen barang bukti harddisk
- Dokumen barang bukti media removable (jika ada)
- Dokumen pengiriman barang bukti digital

Tahapan Pelaksanaan (Tahap 1)

- Jika komputer barang bukti dalam keadaan *standby* atau *hibernation*, kembalikan ke posisi *desktop*
- Jika komputer tersebut diproteksi *password user*, dapat memintanya ke pemilik barang bukti.

Tahapan Pelaksanaan (Tahap 2)

- Dokumentasikan yang sedang berjalan di layar, seperti:
 - Tanggal/waktu lokal komputer,
 - Posisi *window* pada aplikasi melalui fotografi,
 - Dsb.
- Dokumen Identifikasi lapangan

Tahapan Pelaksanaan (Tahap 3)

- Cari di TKP
 - catatan harian,
 - buku agenda,
 - atau potongan kertas yang berisi *password*
- Dokumen barang bukti non digital

Tahapan Pelaksanaan (Tahap 4)

- Catat waktu sistem
- Catat waktu di jam penyidik
- Dokumen perangkat dalam keadaan hidup

Tahapan Pelaksanaan (Tahap 5)

- Menyalin data *live memory*
 - Sistem Operasi Windows 32bit, dapat dilihat pada Juknis J-03
 - Sistem Operasi Windows 64bit, dapat dilihat pada Juknis J-04
 - Sistem Operasi GNU/Linux (32/64 bit), dapat dilihat pada Juknis J-05

Tahapan Pelaksanaan (Tahap 6)

- Dokumentasikan kondisi barang bukti digital
 - Sistem operasi windows, dapat dilihat pada Juknis J-11
 - Sistem operasi Linux, dapat dilihat pada Juknis J-12

Tahapan Pelaksanaan (Tahap 7)

- Catat waktu di sistem dan waktu di jam penyidik.
- Sebagai waktu mematikan perangkat.

Tahapan Pelaksanaan (Tahap 8)

- Matikan perangkat, sesuai dengan Juknis J-09

Tahapan Pelaksanaan (Tahap 9)

- Cari media penyimpanan lain
- Mungkin berhubungan dengan kasus yang dihadapi

Tahapan Pelaksanaan (Tahap 10)

- Lakukan proses menyalin media penyimpanan perangkat beserta media penyimpanan lain yang ditemukan.
- Dokumentasikan waktu mulai dan waktu selesai.

Tahapan Pelaksanaan (Tahap 11)

- Beri label barang bukti
- Label semua port dan kabel

Tahapan Pelaksanaan (Tahap 12)

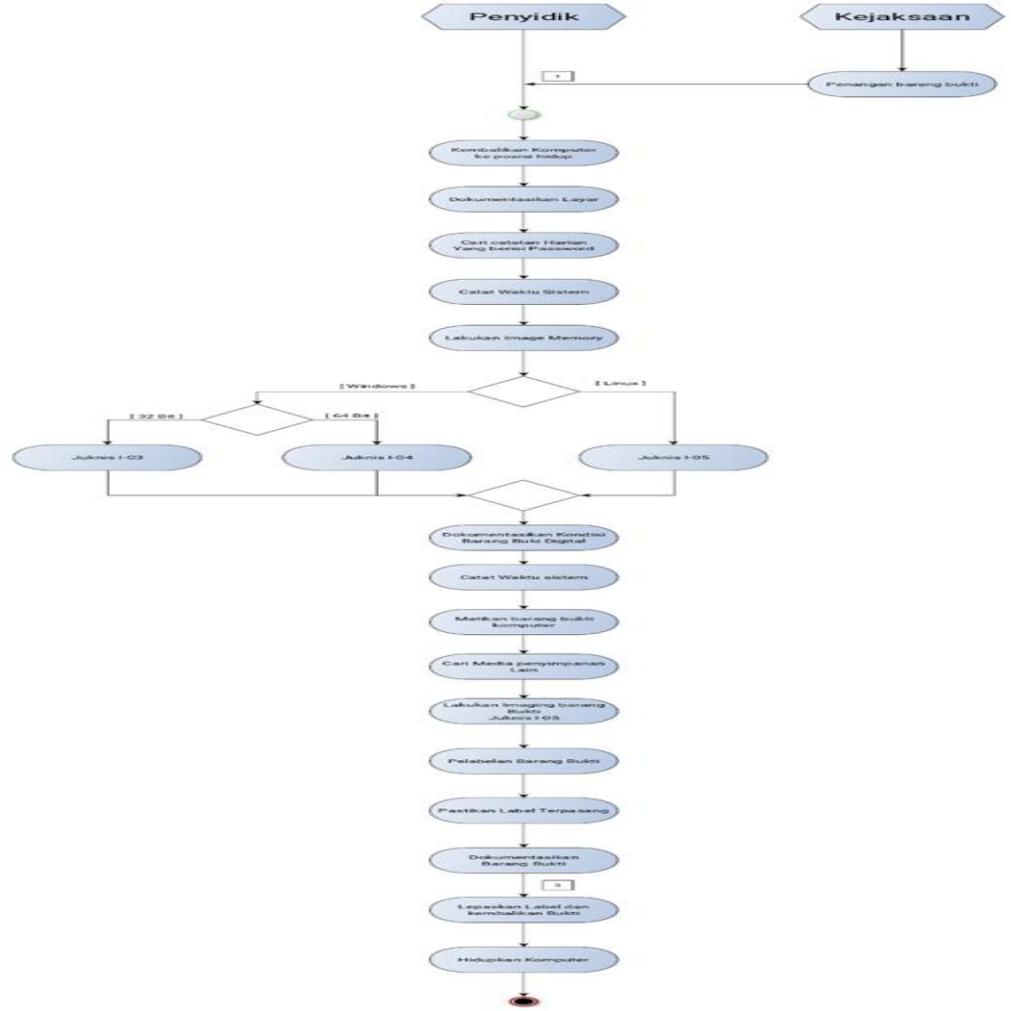
- Dokumentasikan barang bukti beserta label dengan fotografi
- Foto close-up setiap barang bukti
- Dokumentasi ditandatangani oleh kedua belah pihak

Tahapan Pelaksanaan (Tahap 13)

- Lepaskan semua label
- Kaitkan kembali media penyimpanan ke perangkat
- Kembalikan media penyimpanan lain ke tempatnya
- Hidupkan Komputer

Cek List

- Pastikan telah mengisi dokumen dengan lengkap dan telah ditandatangani oleh penyidik dan saksi.
- Pastikan komputer telah hidup dan tanpa masalah.





M8 _ Mementukan Opsi untuk Koleksi atau

Akuisisi



PENANGANAN BARANG BUKTI ELEKTRONIK
DALAM KEADAAN MATI

Koleksi Perangkat dalam Keadaan Mati

Tujuan

- Mengumpulkan bukti digital dalam keadaan mati
- Barang bukti digital dipindahkan ke laboratorium untuk diakuisisi dan dianalisis

Pra-kondisi & Persyaratan

- Telah melakukan Pra Identifikasi, Identifikasi Jaringan, dan Identifikasi jenis penanganan
- Perangkat dalam keadaan mati
- Memiliki surat perintah melakukan koleksi barang bukti digital

Peralatan

- Jam digital
- Kamera digital
- Toolkit (Tang, obeng, dll)
- Kantong atau kardus barang bukti digital
- Label barang bukti
- Dokumen barang bukti dan *chain of custody*

Dokumen Barang Bukti

- Dokumen barang bukti digital
- Dokumen perangkat dalam keadaan mati
- Dokumen Barang bukti non-digital
- Dokumen barang bukti harddisk
- Dokumen barang bukti media removable (jika ada)
- Dokumen pengiriman barang bukti digital

Tahapan Pelaksanaan (Tahap 1)

- Jangan pernah menyalakan komputer
- Pastikan komputer barang bukti dalam keadaan mati
- Lepaskan kabel sumber listrik

Tahapan Pelaksanaan (Tahap 2)

- Cari di TKP
 - catatan harian,
 - buku agenda,
 - atau potongan kertas yang berisi *password*
- Dokumen barang bukti non digital

Tahapan Pelaksanaan (Tahap 3)

- Cari media penyimpanan lain
- Mungkin berhubungan dengan kasus yang dihadapi

Tahapan Pelaksanaan (Tahap 4)

- Beri label barang bukti
- Label semua *port* dan kabel

Tahapan Pelaksanaan (Tahap 5)

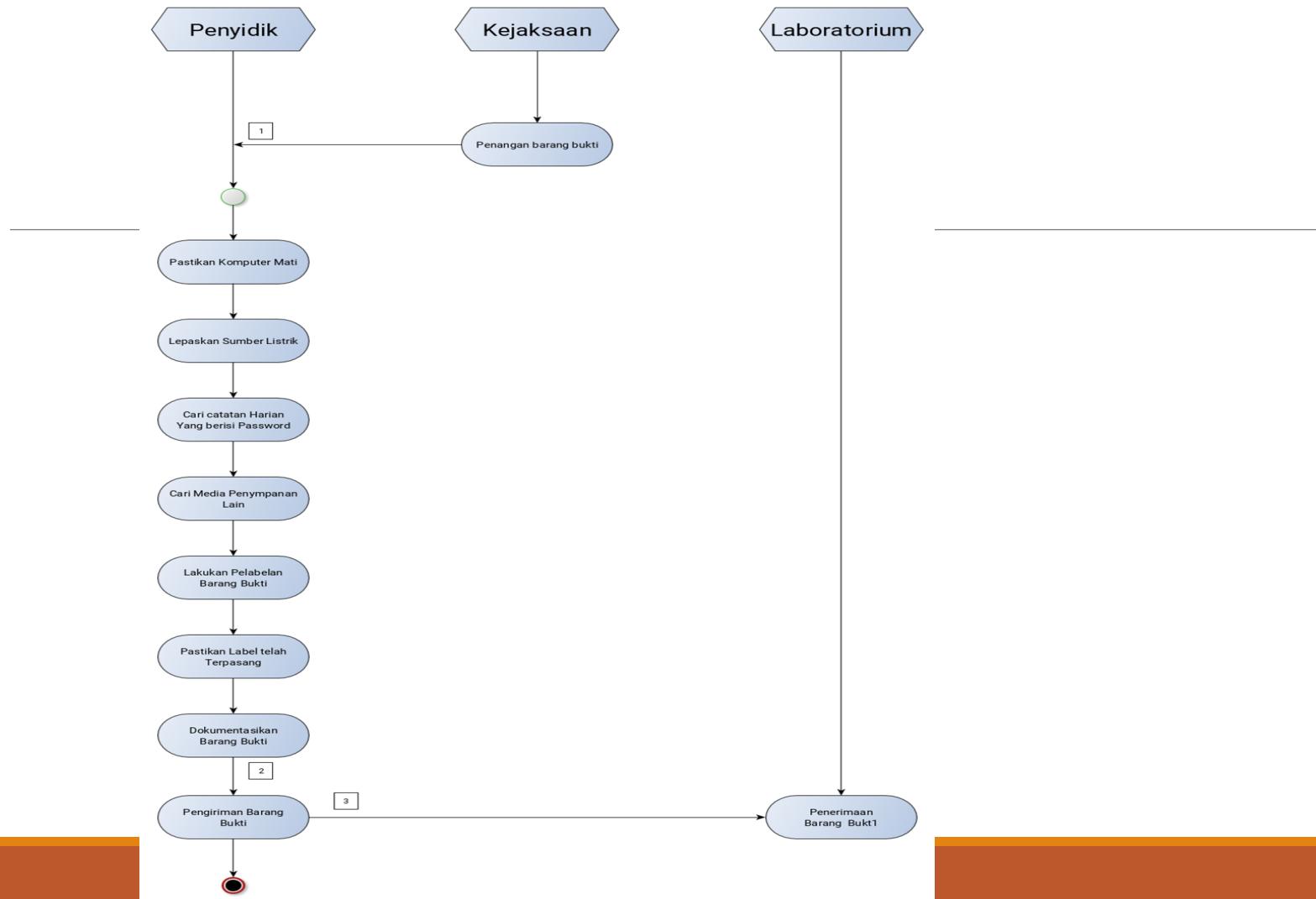
- Dokumentasikan barang bukti beserta label dengan fotografi
- Foto close-up setiap barang bukti
- Dokumentasi ditandatangani oleh kedua belah pihak

Tahapan Pelaksanaan (Tahap 6)

- Barang bukti dibawa ke laboratorium
- Pengiriman barang bukti tersebut harus disertai berita acara pengiriman barang bukti digital

Cek List

- Pastikan telah mengisi dokumen dengan lengkap dan telah ditandatangani oleh penyidik dan saksi.
- Barang bukti dikemas dengan rapi dan di segel.



Akuisisi Perangkat dalam Keadaan Mati

Tujuan

- Memproduksi salinan barang bukti di TKP
- Secara menyeluruh atau sebagian

Pra-kondisi & Persyaratan

- Telah melakukan Pra Identifikasi, Identifikasi Jaringan, dan Identifikasi jenis penanganan
- Perangkat dalam keadaan mati
- Memiliki surat perintah melakukan akuisisi barang bukti digital

Peralatan

- Jam digital
- *Notebook forensik*
- Toolkit (Tang, obeng, dll)
- Media baru atau telah dilakukan *zero format*
- Dokumen barang bukti dan *chain of custody*

Dokumen Barang Bukti

- Dokumen barang bukti digital
- Dokumen perangkat dalam keadaan mati
- Dokumen Barang bukti non-digital
- Dokumen barang bukti harddisk
- Dokumen barang bukti media removable (jika ada)
- Dokumen pengiriman barang bukti digital

Tahapan Pelaksanaan (Tahap 1)

- Jangan pernah menyalakan komputer
- Pastikan komputer barang bukti dalam keadaan mati
- Lepaskan kabel sumber listrik

Tahapan Pelaksanaan (Tahap 2)

- Cari di TKP
 - catatan harian,
 - buku agenda,
 - atau potongan kertas yang berisi *password*
- Dokumen barang bukti non digital

Tahapan Pelaksanaan (Tahap 3)

- Cari media penyimpanan lain
- Mungkin berhubungan dengan kasus yang dihadapi

Tahapan Pelaksanaan (Tahap 4)

- Lakukan proses menyalin media penyimpanan perangkat beserta media penyimpanan lain yang ditemukan.
- Dokumentasikan waktu mulai dan waktu selesai.

Tahapan Pelaksanaan (Tahap 5)

- Beri label barang bukti
- Label semua *port* dan kabel

Tahapan Pelaksanaan (Tahap 6)

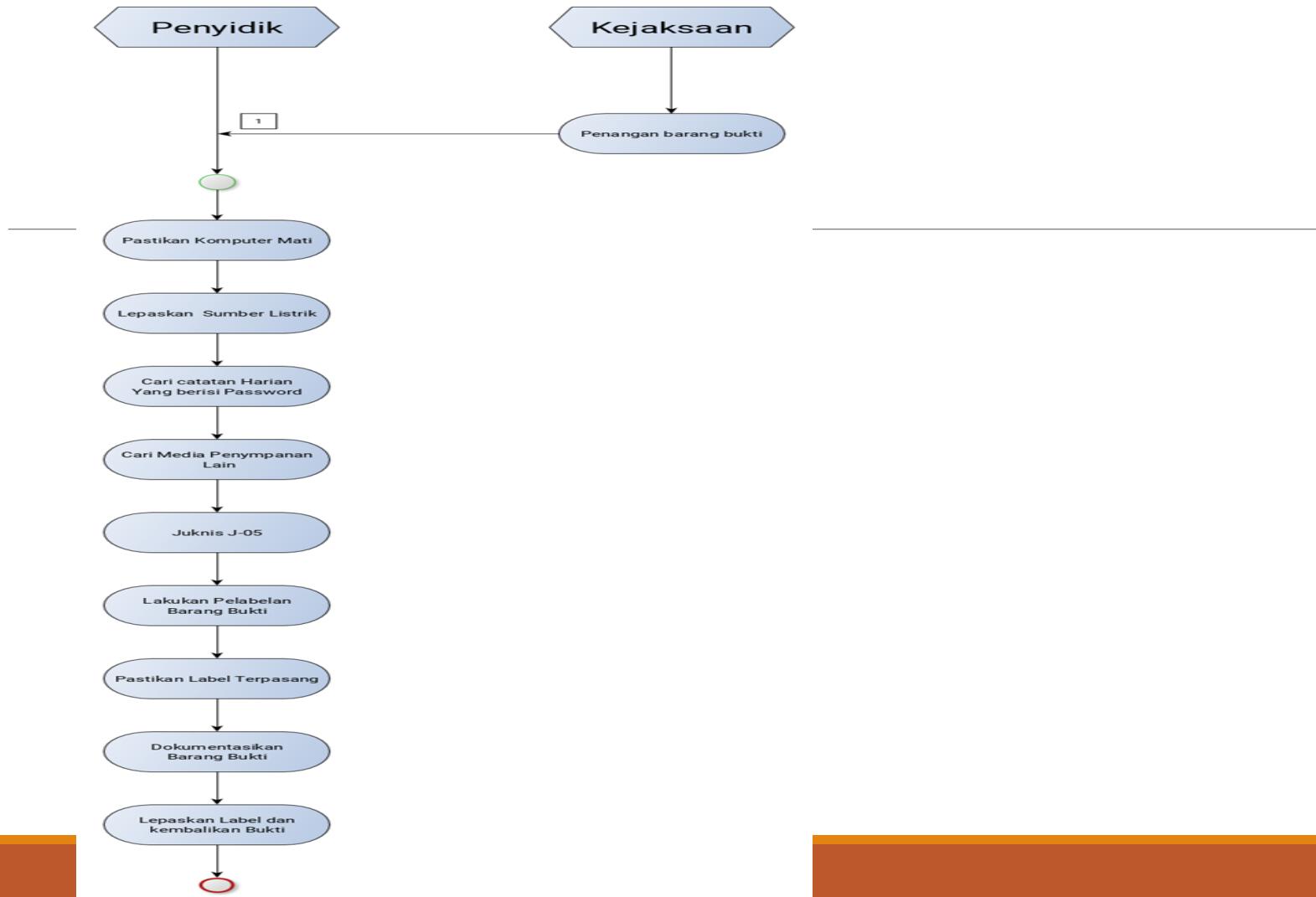
- Dokumentasikan barang bukti beserta label dengan fotografi
- Foto close-up setiap barang bukti
- Dokumentasi ditandatangani oleh kedua belah pihak

Tahapan Pelaksanaan (Tahap 7)

- Lepaskan semua label
- Kaitkan kembali media penyimpanan ke perangkat
- Kembalikan media penyimpanan lain ke tempatnya

Cek List

- Pastikan telah mengisi dokumen dengan lengkap dan telah ditandatangani oleh penyidik dan saksi.



A large, colorful word cloud centered around the words "thank you" in various languages. The words are rendered in different colors and sizes, creating a dense and visually appealing composition. The languages represented include German (danke), Chinese (謝謝), French (merci), Spanish (gracias), Turkish (teşekkür ederim), Russian (спасибо), Polish (dziękuje), Portuguese (obrigado), and many others like English, Dutch, Italian, and Korean.



PENGAMBILAN BARANG BUKTI DIGITAL
MENGGUNAKAN FTK MANAGER

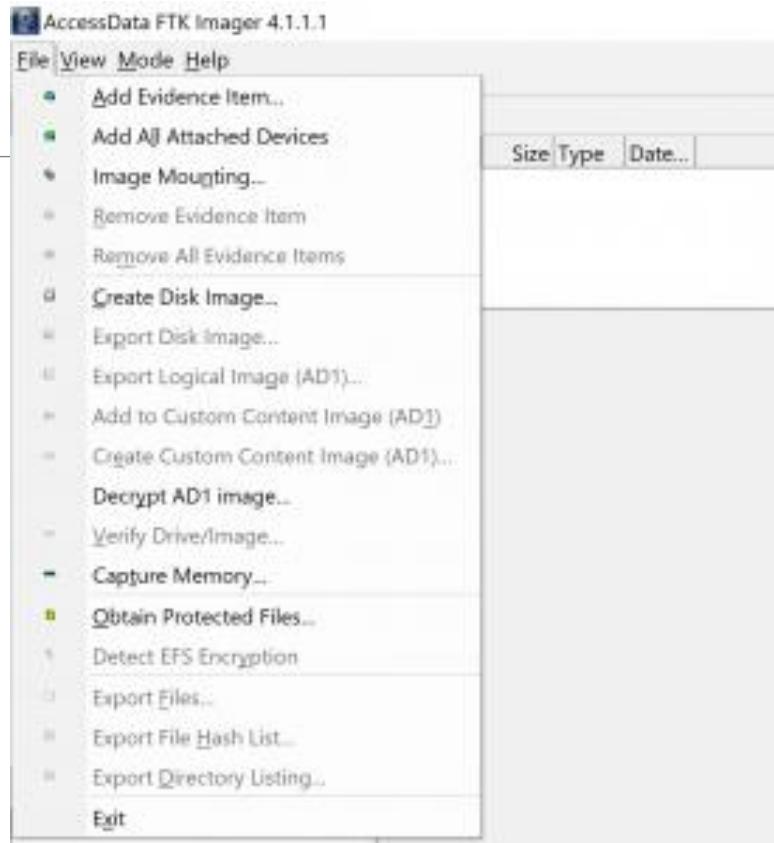
FTK Imager

FTK Imager

- FTK Imager adalah tools untuk melakukan preview dan pembuatan image
- FTK imager juga dapat melakukan perfect copy (image forensik) tanpa merubah data atau metadata dari bukti aslinya.

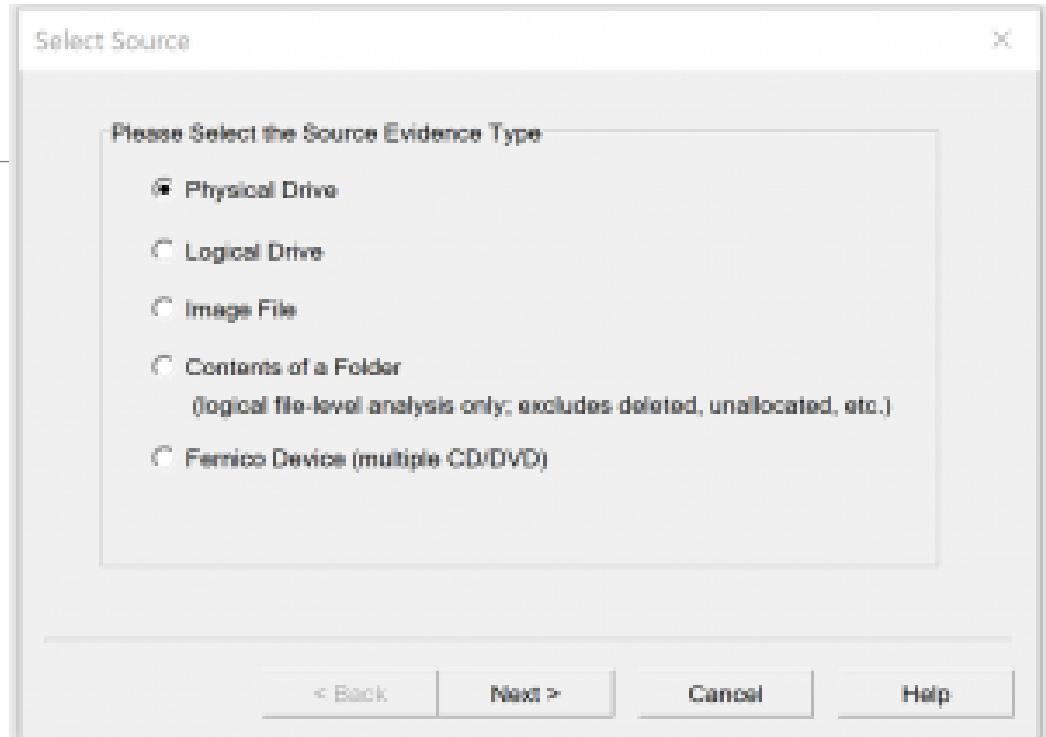
Cara Membuat Image dengan FTK Imager

1. klik File > Create Disk Image



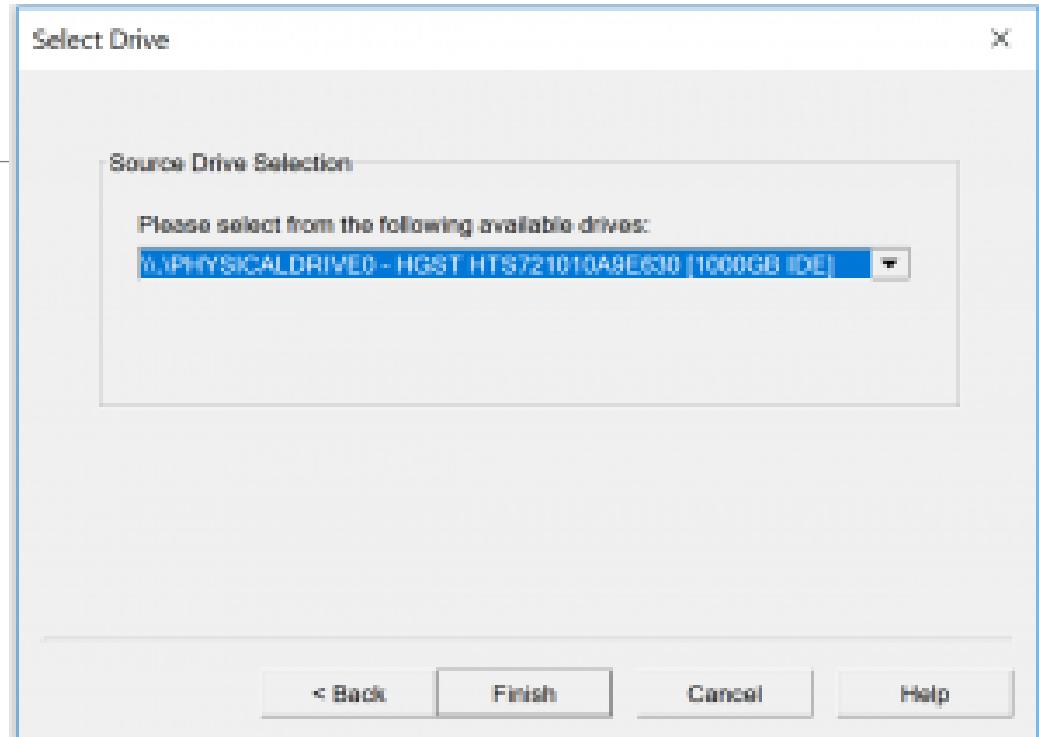
Cara Membuat Image dengan FTK Imager

2. Pilih Source yang akan dicopy



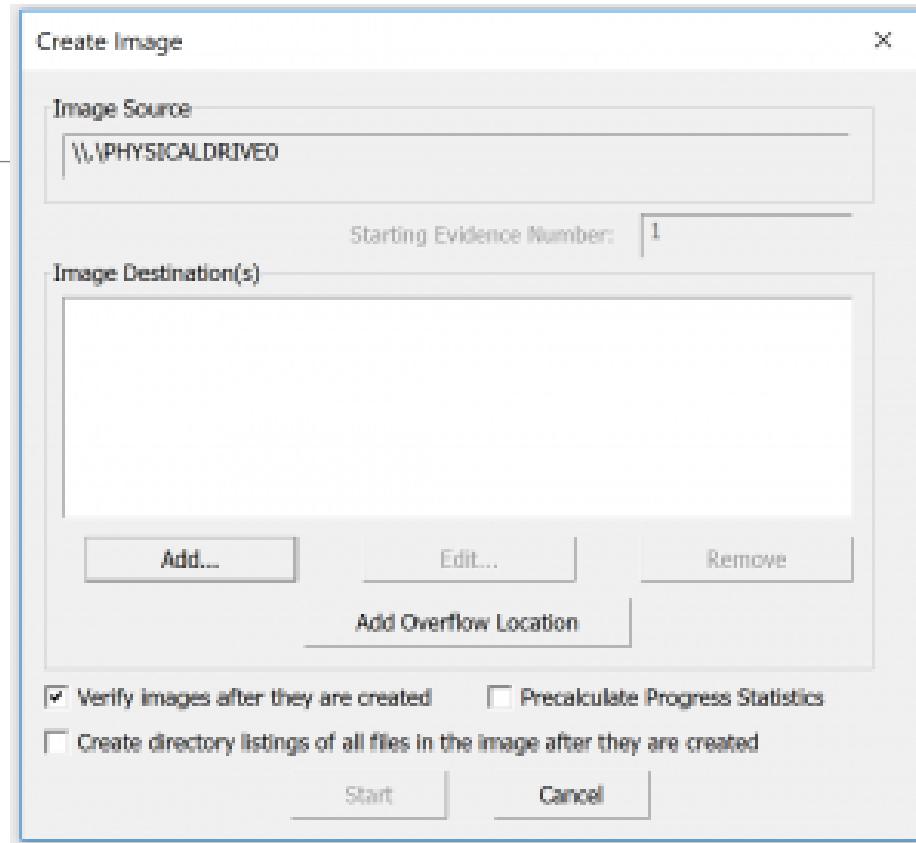
Cara Membuat Image dengan FTK Imager

3. Pilih detail Drive yang dipilih



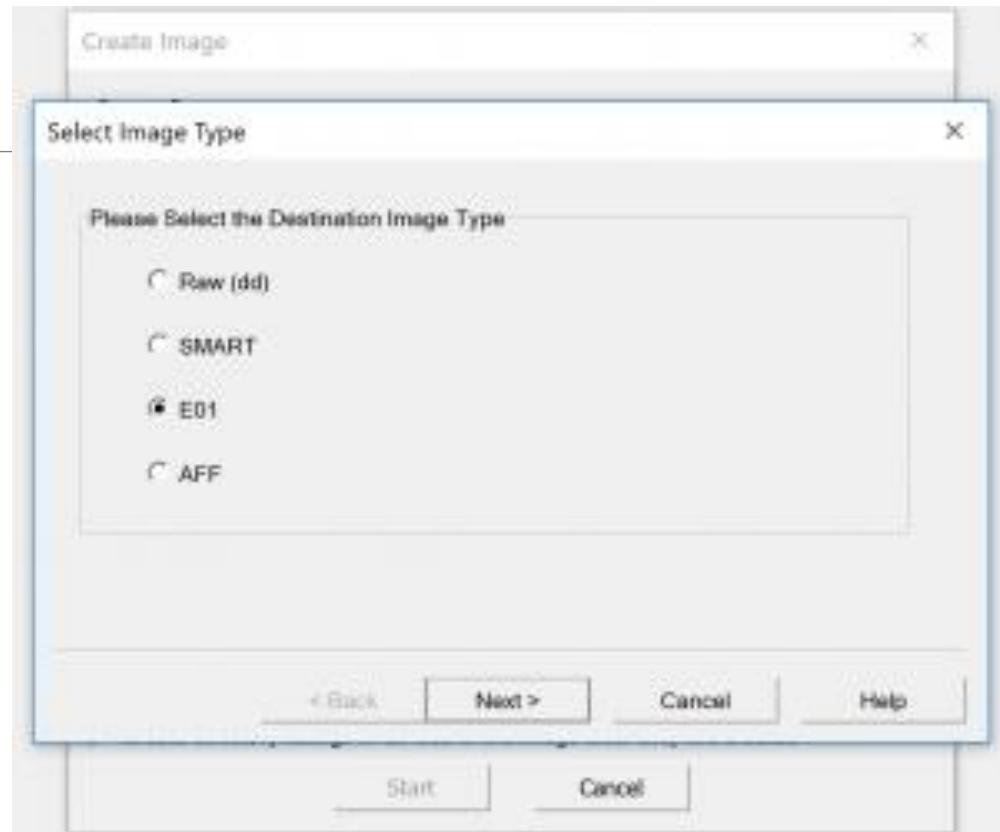
Cara Membuat Image dengan FTK Imager

4. klik add di bagian image destination untuk menentukan hasil dari copy image yang kita lakukan



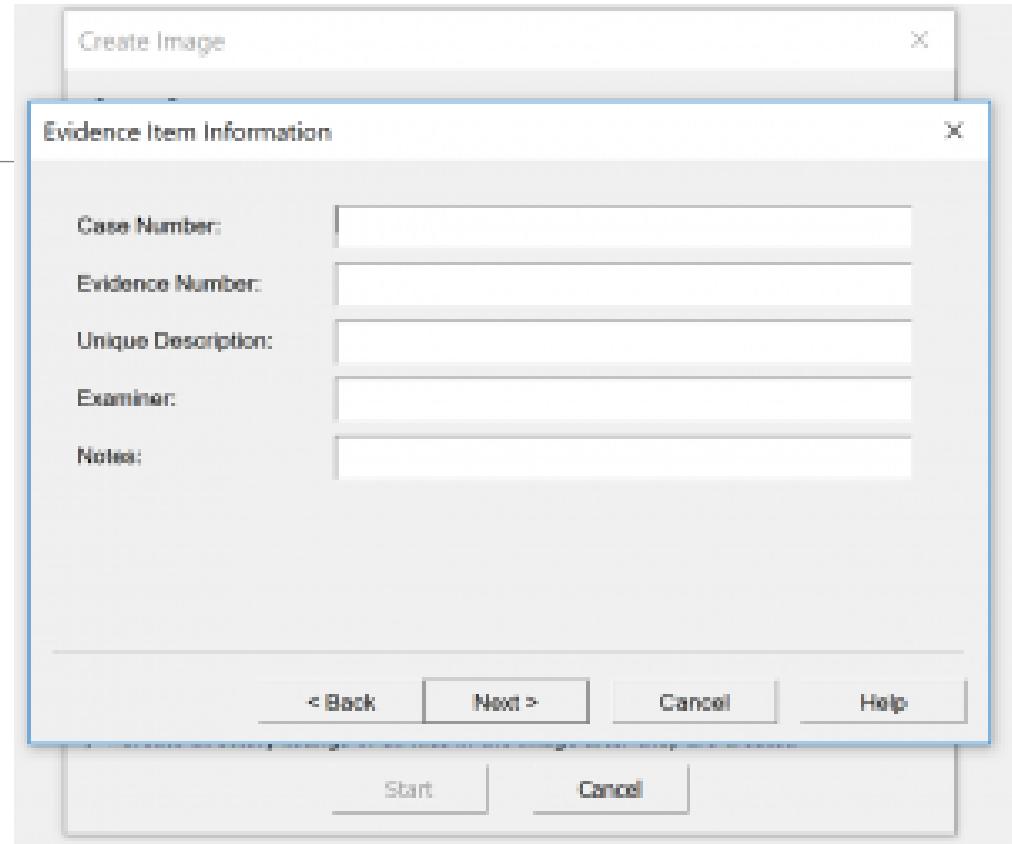
Cara Membuat Image dengan FTK Imager

5. Pilih tipe dari image yang akan dibuat



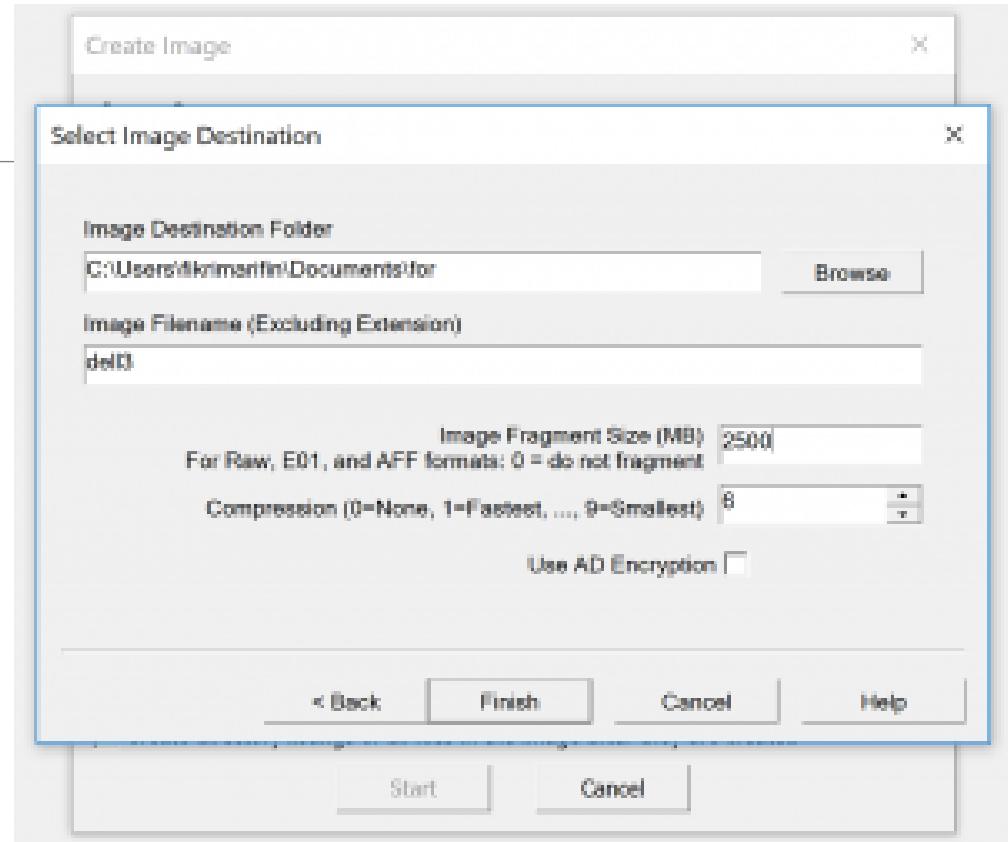
Cara Membuat Image dengan FTK Imager

6. Masukkan detail dari Drive yang akan dibuat imagennya



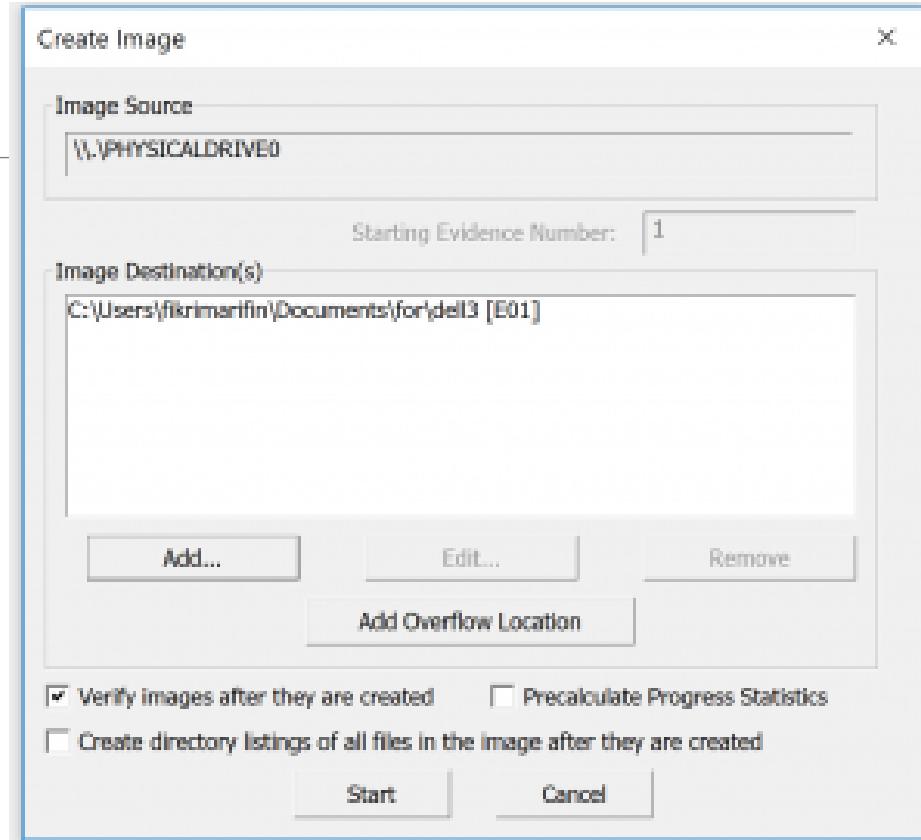
Cara Membuat Image dengan FTK Imager

7. Pilih nama image dan lokasi image yang akan dibuat



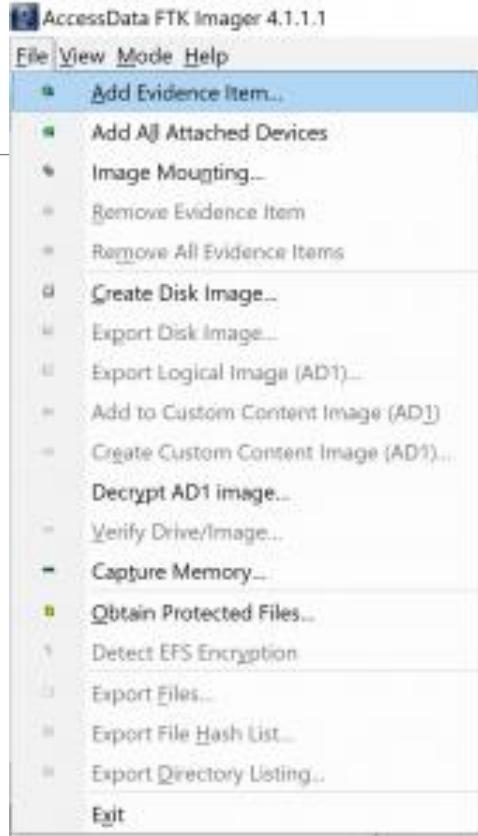
Cara Membuat Image dengan FTK Imager

8. klik start untuk memulai proses imaging, untuk 1TB hardisk biasanya memakan waktu 11-12 jam



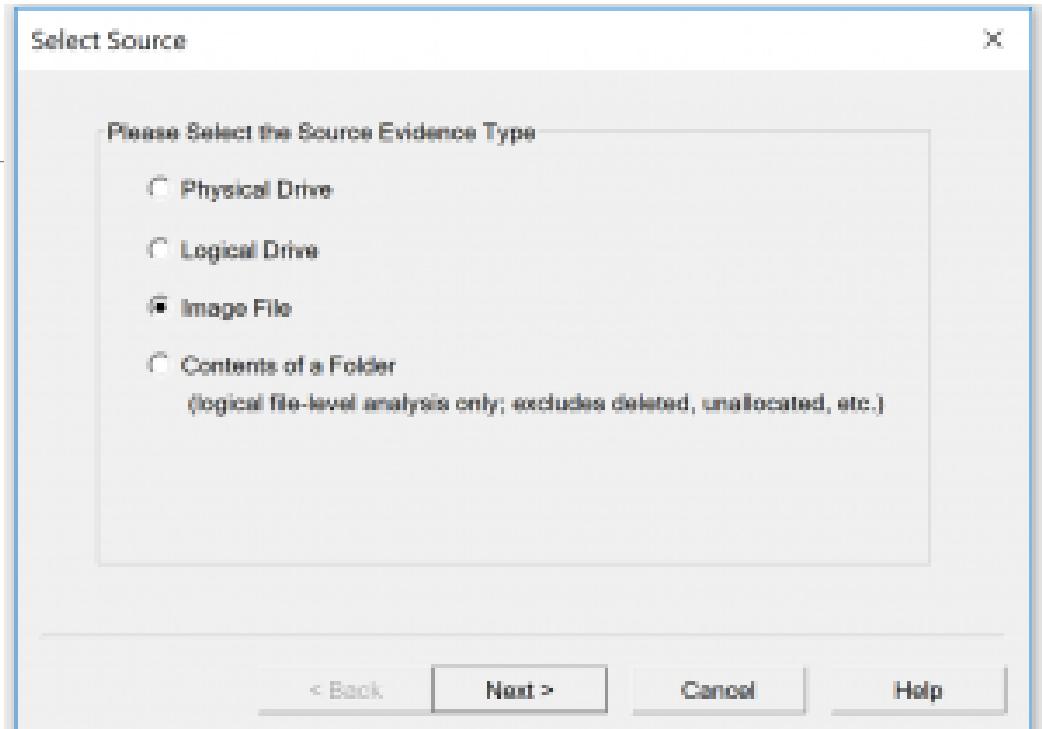
Cara Mounting Image Barang Bukti Digital

1. Klik file > Add Evidence Item



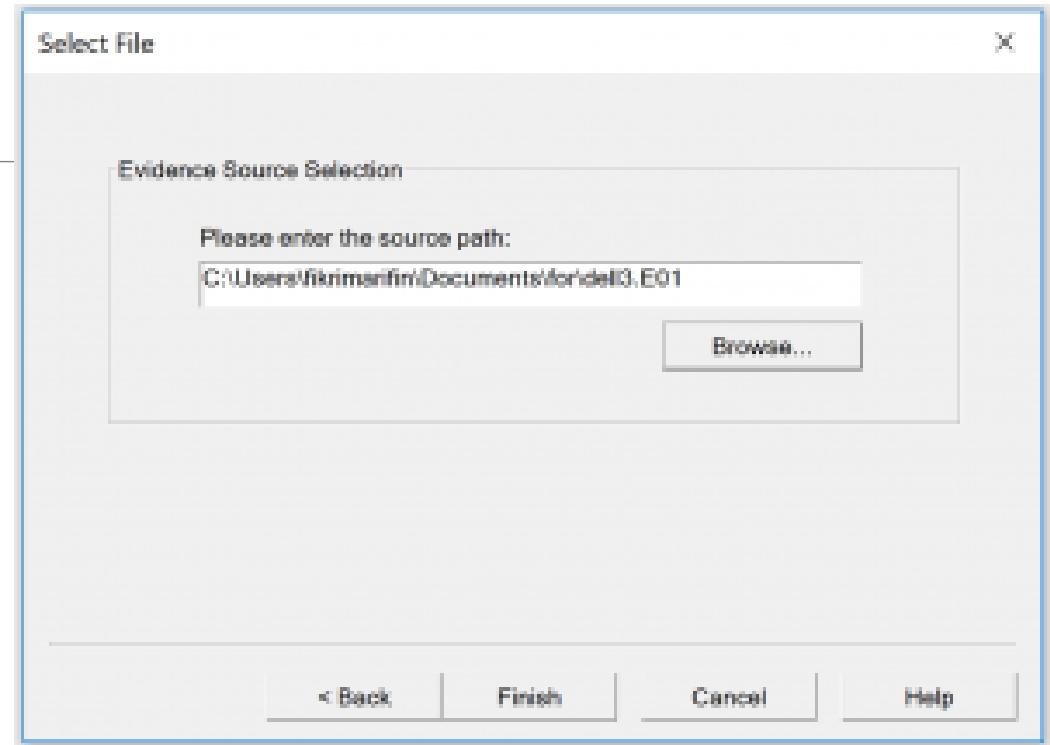
Cara Mounting Image Barang Bukti Digital

2. Pilih image yang akan di-mount dalam bentuk apa



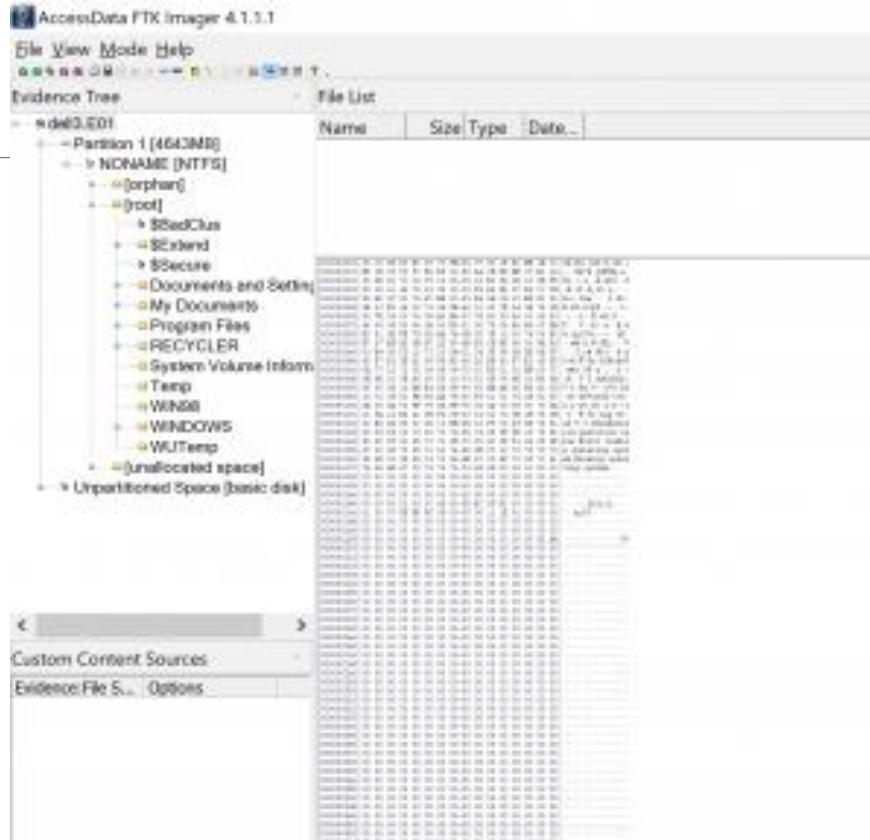
Cara Mounting Image Barang Bukti Digital

3. Cari lokasi file tersebut



Cara Mounting Image Barang Bukti Digital

4. Setelah di-mount akan terlihat ada berapa jumlah partisi dan semua file didalamnya bisa dianalisa



Cara Mounting Image Barang Bukti Digital

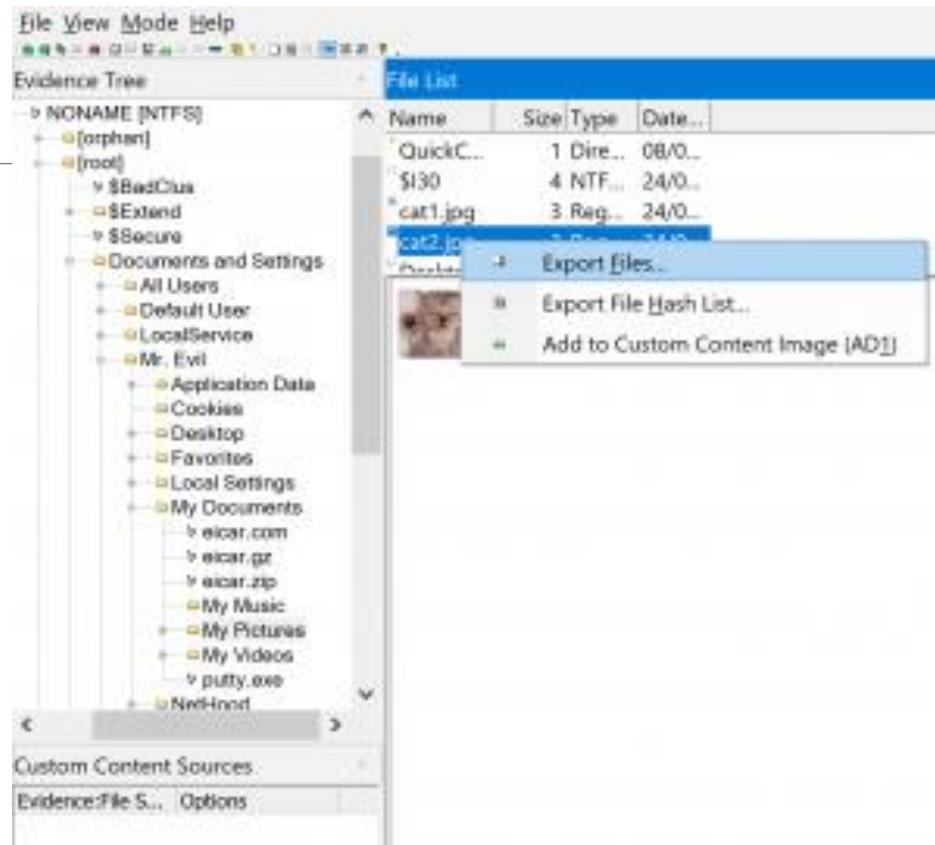
5. Dari hasil mounting image pun dapat dilihat profil user yang ada di dalam drive tersebut, dan isi filenya dapat kita ambil

The screenshot shows a digital forensic interface with two main panes. The left pane, titled 'Evidence Tree', displays a hierarchical file system structure of a mounted image. The root directory contains several subfolders and files, including 'orphan', 'root', '\$BadClus', '\$Extend', '\$Secure', 'Documents and Settings' (which further contains 'All Users', 'Default User', 'LocalService', and 'Mr. Evil' profiles), 'My Documents' (containing files like 'eicar.com', 'eicar.gz', 'eicar.zip', 'My Music', 'My Pictures', 'My Videos', and 'putty.exe'), and 'NtfsHnd'. The right pane, titled 'File List', shows a table of files with columns for Name, Size, Type, and Date. The table includes files like 'QuickC...', 'S130', 'cat1.jpg', 'cat2.jpg', and 'Desktop'. Below the table is a preview pane showing the contents of a selected file, which appears to be a compressed archive.

| Name | Size | Type | Date... |
|-----------|-----------|---------|---------|
| QuickC... | 1 Dire... | 08/0... | |
| S130 | 4 NTF... | 24/0... | |
| *cat1.jpg | 3 Reg... | 24/0... | |
| *cat2.jpg | 3 Reg... | 24/0... | |
| Desktop | < 1 M | 07/0... | |

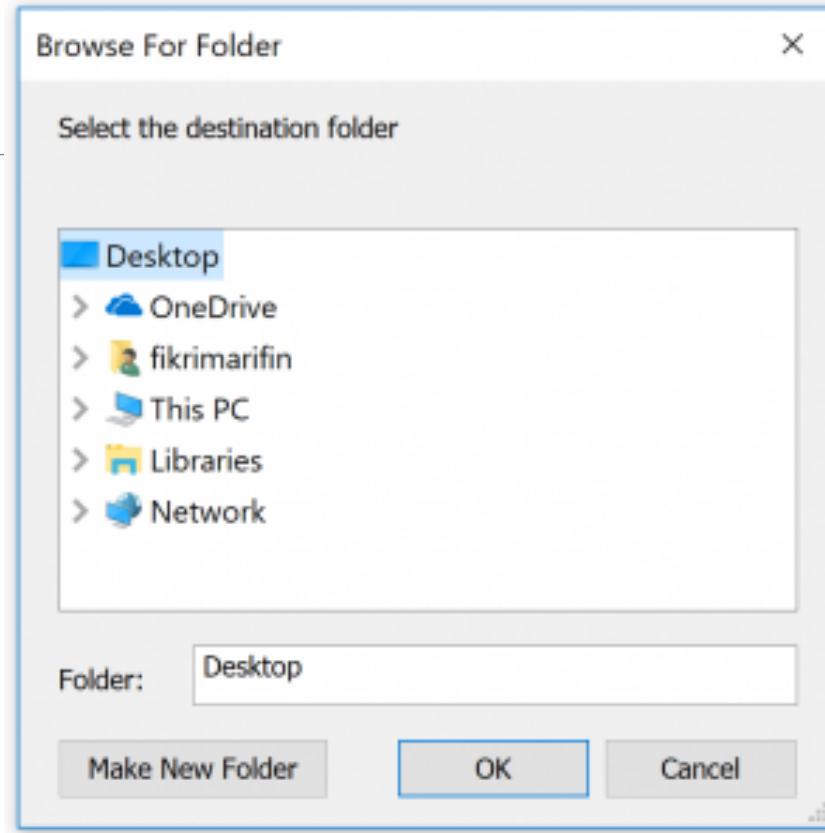
Cara Mounting Image Barang Bukti Digital

6. Pilih file yang akan dianalisa kemudian pilih export files



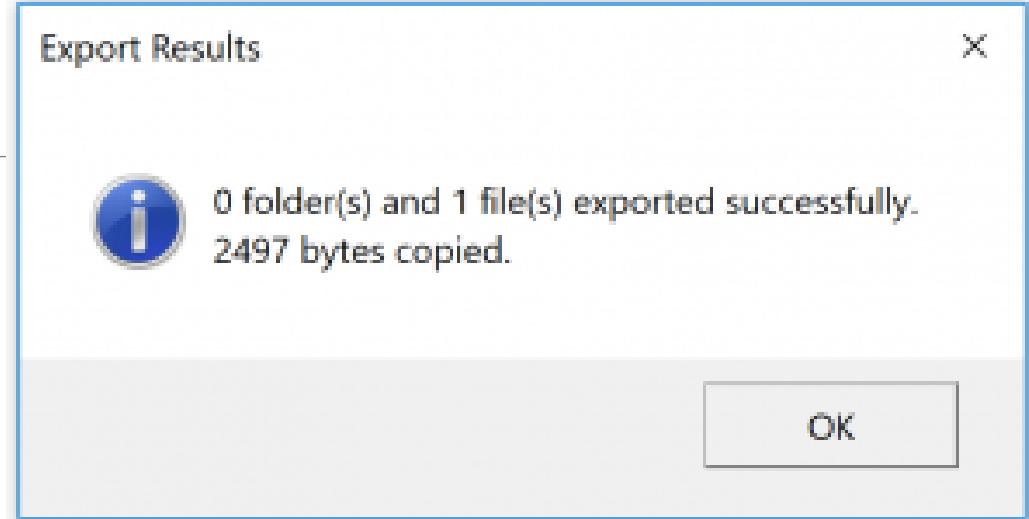
Cara Mounting Image Barang Bukti Digital

7. Pilih lokasi file tersebut akan di-export



Cara Mounting Image Barang Bukti Digital

8. Export berhasil dilakukan



Imaging Harddisk

Catatan Imaging Storage

- Lakukan akuisisi memory terlebih dahulu ketika mendapatkan komputer yang dalam kondisi hidup.
- Lakukan pencatatan waktu komputer tersebut, bandingkan dengan waktu yang sedang berjalan
- Matikan komputer dengan cara mencabut catu daya-nya langsung
- Lepaskan perangkat storage lalu attach ke forensic workstation(jika ada gunakan write blocker)
- Jika menggunakan sistem operasi yang tidak khusus digunakan untuk forensic, pastikan sudah mendukung *write blocker*

Guymager

• GUYMAGER 0.8.11 (as superuser)

Devices Misc Help

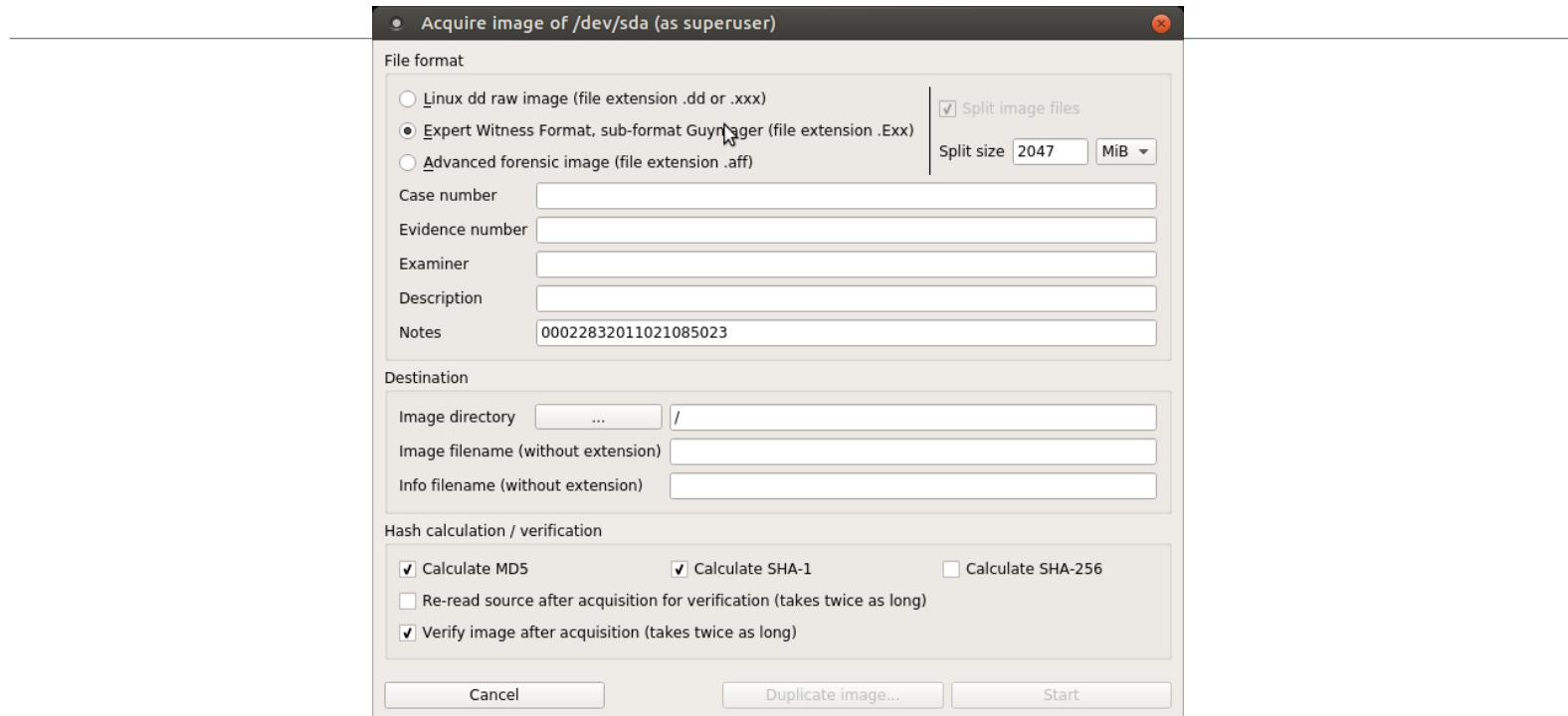
Rescan

| Serial nr. | Linux device | Model | State | Size | Hidden areas | Bad sectors | Progress | Av. s [M] |
|----------------------|--------------|---------------------|---------------------------------------|---------|--------------|-------------|----------|-----------|
| 00022832011021085023 | /dev/sda | USB SanDisk_3.2Gen1 | <input checked="" type="radio"/> Idle | 15,4GB | unknown | | | |
| S465NB0K476546M | /dev/nvme0n1 | | <input type="radio"/> Idle | 250,1GB | unknown | | | |

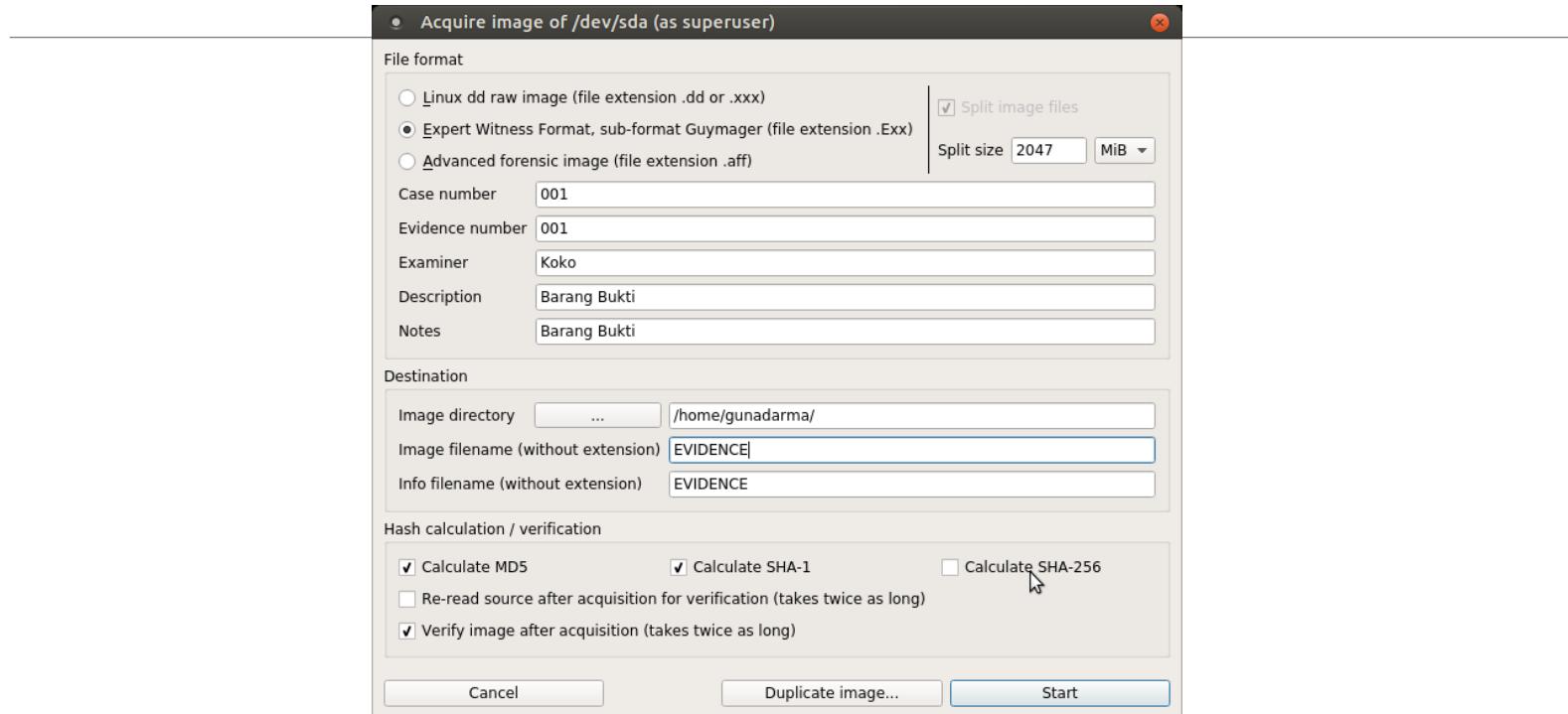
◀ ▶

| | |
|----------------------------------|-----------------------------------------|
| Size | 15.376.318.464 bytes (14,3GiB / 15,4GB) |
| Sector size | 512 |
| Image file | |
| Info file | |
| Current speed | |
| Started | |
| Hash calculation | |
| Source verification | |
| Image verification | |
| Overall speed (all acquisitions) | |

Guymager : Aquire



Guymager: Information



Guymager: Process

• GUYMAGER 0.8.11 (as superuser)

Devices Misc Help

Rescan

| Serial nr. | Linux device | Model | State | Size | Hidden areas | Bad sectors | Progress | Av. si [M] |
|----------------------|--------------|---------------------|------------------------------------------|---------|--------------|-------------|----------|------------|
| 00022832011021085023 | /dev/sda | USB SanDisk_3.2Gen1 | <input checked="" type="radio"/> Running | 15,4GB | unknown | 0 | 5% | |
| S465NB0K476546M | /dev/nvme0n1 | | <input type="radio"/> Idle | 250,1GB | unknown | | | |

Size 15.376.318.464 bytes (14,3GiB / 15,4GB)
Sector size 512
Image file /home/gunadarma/EVIDENCE.Exx
Info file /home/gunadarma/EVIDENCE.info
Current speed 136,47 MB/s
Started 18. November 13:50:04 (00:00:11)
Hash calculation MD5 and SHA-1
Source verification off
Image verification on
Overall speed (all acquisitions) 136,47 MB/s

Guymager: Finish

• GUYMAGER 0.8.11 (as superuser)

Devices Misc Help

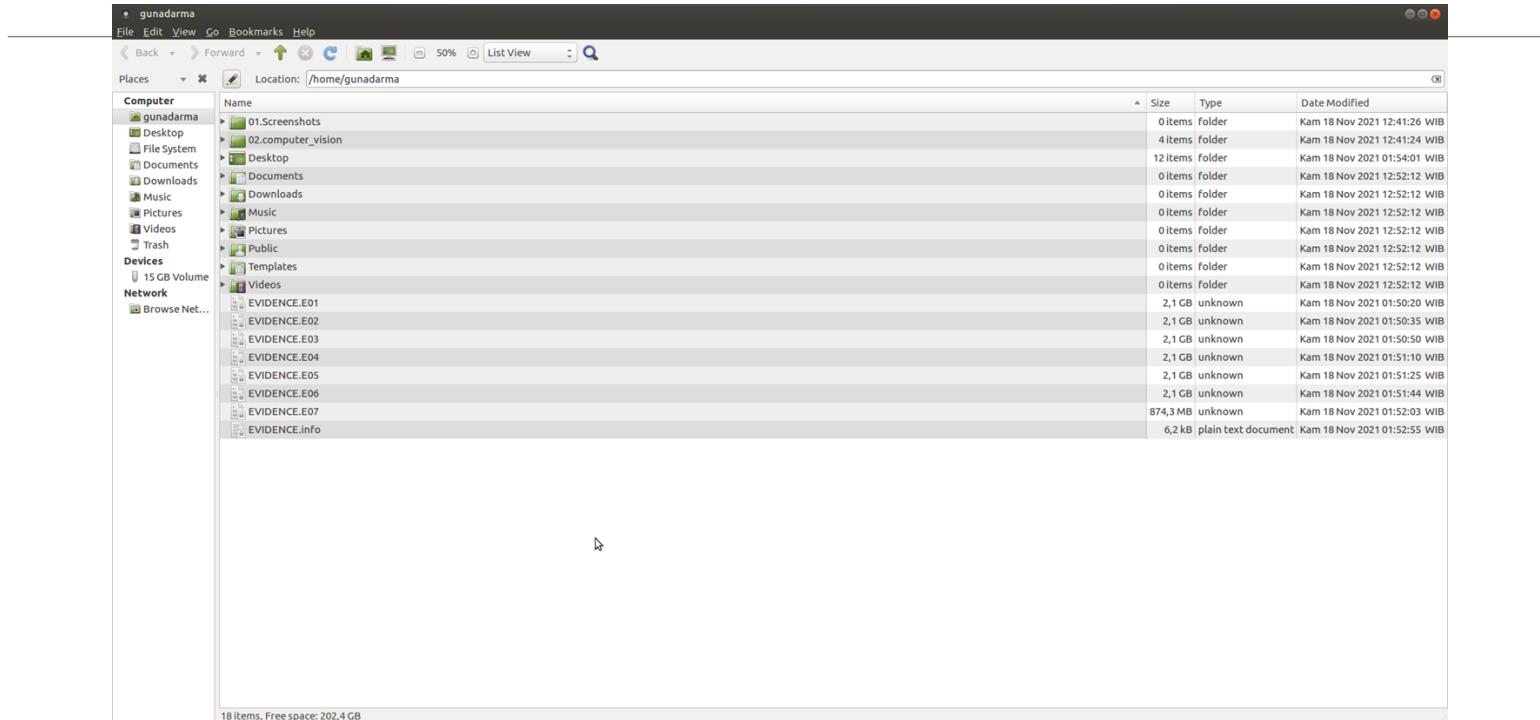
Rescan

| Serial nr. | Linux device | Model | State | Size | Hidden areas | Bad sectors | Progress | Av. size [M] |
|----------------------|--------------|---------------------|--------------------------|---------|--------------|-------------|----------|--------------|
| 00022832011021085023 | /dev/sda | USB SanDisk_3.2Gen1 | Finished - Verified & ok | 15,4GB | unknown | 0 | 100% | |
| S465NB0K476546M | /dev/nvme0n1 | | Idle | 250,1GB | unknown | | | |

◀ ▶

| | |
|----------------------------------|-----------------------------------------|
| Size | 15.376.318.464 bytes (14,3GiB / 15,4GB) |
| Sector size | 512 |
| Image file | /home/gunadarma/EVIDENCE.Exx |
| Info file | /home/gunadarma/EVIDENCE.info |
| Current speed | |
| Started | 18. November 13:50:04 (00:02:51) |
| Hash calculation | MD5 and SHA-1 |
| Source verification | off |
| Image verification | on |
| Overall speed (all acquisitions) | |

Guymager: result



Evidence Info

```
File Edit View Search Tools Documents Help
Open Save Undo Redo Cut Copy Paste Find Replace
EVIDENCE.info x
73
74 Acquisition
75 =====
76
77 Linux device      : /dev/sda
78 Device size       : 15376318464 (15,4GB)
79 Format            : Expert Witness Format, sub-format Guymager - file extension is .Exx
80 Image meta data
81   Case number      : 001
82   Evidence number  : 001
83   Examiner         : Koko
84   Description      : Barang Bukti
85   Notes             :
86 Image path and file name: /home/gunadarma/EVIDENCE.Exx
87 Image path and file name: /home/gunadarma/EVIDENCE.info
88 Hash calculation    : MD5 and SHA-1
89 Source verification : off
90 Image verification  : on
91
92 No bad sectors encountered during acquisition.
93 State: Finished successfully
94
95 MD5 hash          : 312cb4994f736d60f97848e7c1144e1b
96 MD5 hash verified source : ...
97 MD5 hash verified image : 312cb4994f736d60f97848e7c1144e1b
98 SHA1 hash          : b5b59e405df5508f74dc3a5d97087e0d1633aec
99 SHA1 hash verified source : ...
100 SHA1 hash verified image : b5b59e405df5508f74dc3a5d97087e0d1633aec
101 SHA256 hash        :
102 SHA256 hash verified source: ...
103 SHA256 hash verified image: ...
104 Image verification OK. The image contains exactly the data that was written.
105
106 Acquisition started : 2021-11-10 13:50:04 (ISO format YYYY-MM-DD HH:MM:SS)
107 Verification started: 2021-11-10 13:52:03
108 Ended              : 2021-11-10 13:52:55 (0 hours, 2 minutes and 51 seconds)
109 Acquisition speed  : 124.27 MBbyte/s (0 hours, 1 minutes and 58 seconds)
110 Verification speed : 282.00 MBbyte/s (0 hours, 0 minutes and 52 seconds)
111
112
113 Generated image files and their MD5 hashes
114 =====
115
116 No MD5 hashes available (configuration parameter CalcImageFileMD5 is off)
117 MD5                Image file
118 n/a               EVIDENCE.E01
119 n/a               EVIDENCE.E02
120 n/a               EVIDENCE.E03
121 n/a               EVIDENCE.E04
122 n/a               EVIDENCE.E05
123 n/a               EVIDENCE.E06
124 n/a               EVIDENCE.E07
```

Plain Text Tab Width: 4 Ln 99, Col 70 INS

Imaging RAM

Catatan Akuisisi RAM

- Akuisisi ram dilakukan ketika perangkat dalam kedaan hidup
- Karena sifat ram yang sebagai penyimpanan sementara, mungkin data tidak akan lengkap
- Tools *dump ram*, cukup disimpan di penyimpanan eksternal
- Hasil *dump* biasanya akan sebesar ukuran RAM

Tools yang digunakan

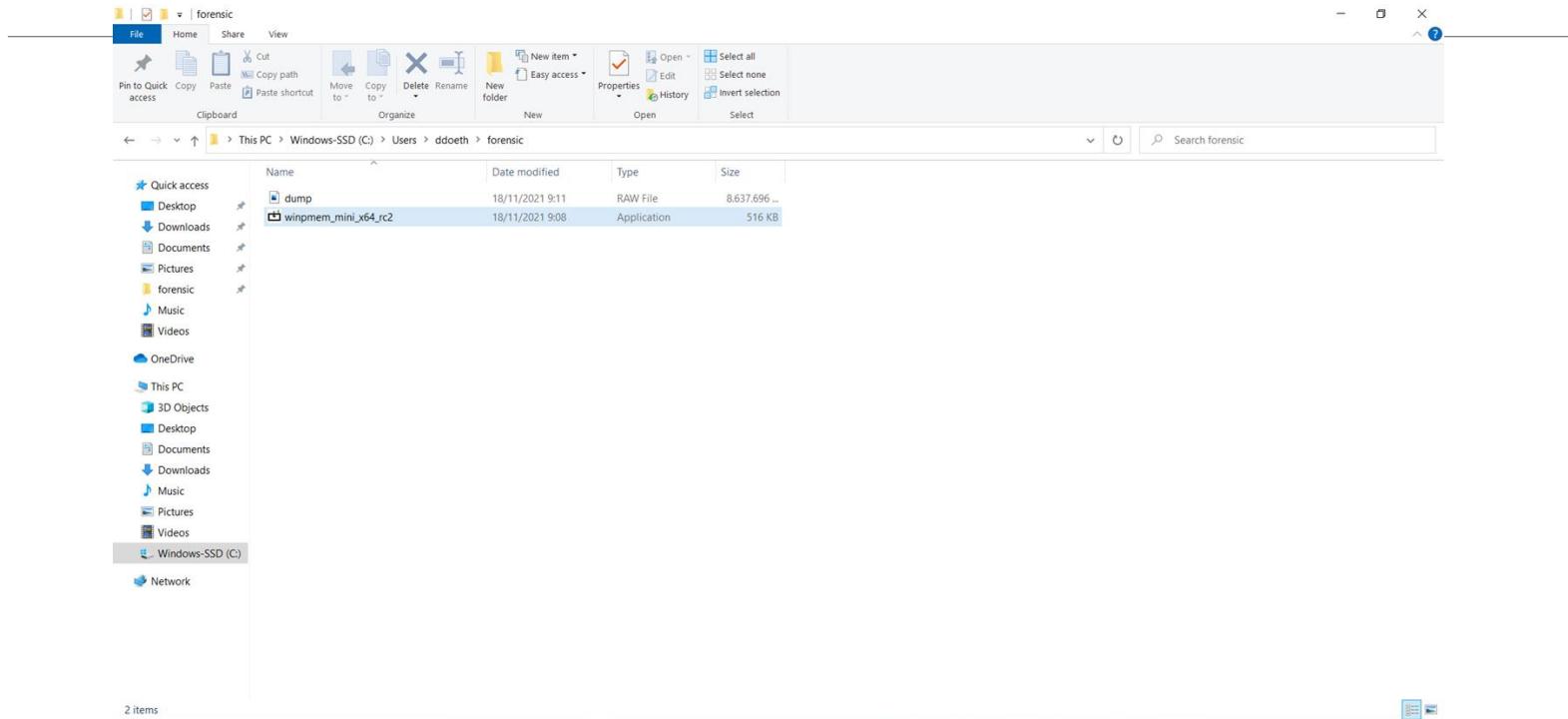
- Winpmem
- <https://github.com/Velocidex/WinPmem>

Winpmem: Ekseskusi

```
c:\Users\ddoeth\forensic>winpmem_mini_x64_rc2.exe dump.raw
WinPmem64
Extracting driver to C:\Users\ddoeth\AppData\Local\Temp\pmeEC10.tmp
Driver Unloaded.
Loaded Driver C:\Users\ddoeth\AppData\Local\Temp\pmeEC10.tmp.
Deleting C:\Users\ddoeth\AppData\Local\Temp\pmeEC10.tmp
The system time is: 02:11:46
Will generate a RAW image
- buffer_size_: 0x1000
CR3: 0x00001AD000
7 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0x09900000
Start 0x09E00000 - Length 0x00100000
Start 0x09F0F000 - Length 0xAF5A000
Start 0xBAB69000 - Length 0xE216000
Start 0xCDFFF000 - Length 0x00001000
Start 0x100000000 - Length 0x10F340000
max_physical_memory_ 0x20f340000
Acquisition mode PTE Remapping
Padding from 0x00000000 to 0x00001000
pad
- length: 0x1000

00% 0x00000000 .
copy_memory
- start: 0x1000
- end: 0x9f000
1 winpmem_mini_x64_rc2.exe
```

Winpmem: Hasil



A large, colorful word cloud centered around the words "thank you" in various languages. The words are rendered in different colors and sizes, creating a dense and visually appealing composition. The languages represented include German (danke), Chinese (謝謝), French (merci), Spanish (gracias), Turkish (teşekkür ederim), Russian (спасибо), Polish (dziękuje), Portuguese (obrigado), and many others like English, Dutch, Italian, and Korean.



PENGANTAR ANALISIS BARANG BUKTI DIGITAL

Analisis Digital Forensic

a detailed process of detecting, investigating, and documenting the reason, course, and consequences of a security incident or violation against state and organization laws

Teknik Analisis Forensik Digital

- Analisis Fisik
- Analisis Logis

Analisis Fisik

- Mengakses Barang bukti secara fisik harddisk
- Hanya beberapa file system yang didukung dengan teknik ini
- Memungkinkan mengembalikan file yang terhapus
- Tidak memungkinkan mengetahui jenis file sebenarnya Secara Langsung

Analisis Fisik (Lanjutan)

- file.jpg → diubah → file.txt
 - Pada analisis fisik, mimetype/ extention file asli tidak bisa langsung terlihat, yang terlihat hanya nama filenya saja, namun
 - Dengan bantuan satu langkah atau perangkat khusus dapat diketahui jenis file tersebut

Analisis Logis

- Mengakses barang bukti dengan menggunakan mount point di operating system
- Barang bukti harus dimounting dengan read only dan noexec (misal: dengan writeblocker)
- Tidak memungkinkan untuk mengembalikan file yang hilang
- Memungkinkan untuk mengetahui jenis file

Mengapa DEFR Perlu Mengetahui Fase Analisis

- Pada dasarnya DEFR dan DES hanya memiliki tanggung jawab sebagai individu yang mengambil barang bukti digital
- Dengan mengetahui bagaimana barang bukti digital akan diperlakukan, diharapkan DEFR dan DES dapat lebih berhati-hati dalam memperlakukan barang bukti
- Pengetahuan analisis ini hanya sebagai pondasi untuk DEFR dan DES, Fase analisis tetap harus dilakukan oleh individu yang memiliki kompetensi

Analisis Fisik

Mengetahui Struktur Media Penyimpanan

- Hardisk mungkin berisi banyak partisi, di Linux setiap partisi dapat memiliki fungsi tersendiri
- Untuk mengetahui susunan hardisk dari barang bukti:
 - cd case001/BB02
 - mmls 20130909.E01

Mengetahui Struktur Harddisk (Lanjutan)

```
linux-a5gi:/mnt/case001/BB02 # mmfs 20130909.E01
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

   Slot   Start       End       Length      Description
00: Meta 0000000000 0000000000 0000000001 Primary Table (#0)
01: ---- 0000000000 0000002047 0000002048 Unallocated
02: 00:00 0000002048 0000499711 0000497664 Linux (0x83)
03: 00:01 0000499712 0059092991 0058593280 Linux (0x83)
04: 00:02 0059092992 0098154495 0039061504 Linux (0x83)
05: ---- 0098154496 0098156543 0000002048 Unallocated
06: Meta 0098156542 0123543551 0025387010 DOS Extended (0x05)
07: Meta 0098156542 0098156542 0000000001 Extended Table (#1)
08: 01:00 0098156544 0113778687 0015622144 Linux Swap / Solaris x86 (0x82)
09: Meta 0113778688 0123543551 0009764864 DOS Extended (0x05)
10: Meta 0113778688 0113778688 0000000001 Extended Table (#2)
11: ---- 0113778688 0113780735 0000002048 Unallocated
12: 02:00 0113780736 0123543551 0009762816 Linux (0x83)
13: ---- 0123543552 0156301487 0032757936 Unallocated
```

linux-a5gi:/mnt/case001/BB02 # █

Mengetahui Struktur Harddisk (Lanjutan)

```
linux-a5gi:/mnt/case001/BB02 # mmfs 20130909.E01
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot   Start           End           Length        Description
00: Meta  0000000000  0000000000  0000000001  Primary Table (#0)
01: ----- 0000000000  0000002047  0000002048  Unallocated
02: 00:00  0000002048  0000499711  0000497664  Linux (0x83)
03: 00:01  0000499712  0059092991  0058593280  Linux (0x83)
04: 00:02  0059092992  0098154495  0039061504  Linux (0x83)
05: ----- 0098154496  0098156543  0000002048  Unallocated
06: Meta  0098156542  0123543551  0025387010  DOS Extended (0x05)
07: Meta  0098156542  0098156542  0000000001  Extended Table (#1)
08: 01:00  0098156544  0113778687  0015622144  Linux Swap / Solaris x86 (0x82)
09: Meta  0113778688  0123543551  0009764864  DOS Extended (0x05)
10: Meta  0113778688  0113778688  0000000001  Extended Table (#2)
11: ----- 0113778688  0113780735  0000002048  Unallocated
12: 02:00  0113780736  0123543551  0009762816  Linux (0x83)
13: ----- 0123543552  0156301487  0032757936  Unallocated
```

Mengetahui Struktur Harddisk (Lanjutan)

```
linux-a5gi:/mnt/case001/BB02 # mmfs 20130909.E01
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

   Slot   Start       End       Length      Description
00: Meta 0000000000 0000000000 0000000001 Primary Table (#0)
01: ---- 0000000000 0000002047 0000002048 Unallocated
02: 00:00 0000002048 0000499711 0000497664 Linux (0x83)
03: 00:01 0000499712 0059092991 0058593280 Linux (0x83)
04: 00:02 0059092992 0098154495 0039061504 Linux (0x83)
05: ---- 0098154496 0098156543 0000002048 Unallocated
06: Meta 0098156542 0123543551 0025387010 DOS Extended (0x05)
07: Meta 0098156542 0098156542 0000000001 Extended Table (#1)
08: 01:00 0098156544 0113778687 0015622144 Linux Swap / Solaris x86 (0x82)
09: Meta 0113778688 0123543551 0009764864 DOS Extended (0x05)
10: Meta 0113778688 0113778688 0000000001 Extended Table (#2)
11: ---- 0113778688 0113780735 0000002048 Unallocated
12: 02:00 0113780736 0123543551 0009762816 Linux (0x83)
13: ---- 0123543552 0156301487 0032757936 Unallocated
```

linux-a5gi:/mnt/case001/BB02 # █

Mengetahui Konten Dari Partisi

- Untuk mengetahui fungsi partisi adalah dengan melihat konten di dalam partisi
 - fls -r -o [offset] [nama_file]

```
linux-a5gi:/mnt/case001/BB02 # fls -o 2048 20130909.E01
d/d 11: lost+found
r/r 15: config-2.6.32-5-686
r/r 18: vmlinuz-2.6.32-5-686
d/d 44177: grub
r/r 17: System.map-2.6.32-5-686
r/r 12: initrd.img-2.6.32-5-686
r/- * 0: config-2.6.32-5-686.dpkg-tmp
r/- * 0: System.map-2.6.32-5-686.dpkg-new
r/- * 0: System.map-2.6.32-5-686.dpkg-tmp
r/- * 0: vmlinuz-2.6.32-5-686.dpkg-new
r/- * 0: vmlinuz-2.6.32-5-686.dpkg-tmp
d/d 124497: $OrphanFiles
```

Hasil Pemeriksaan

- Dari konten yang ada, partisi ini adalah partisi /boot dengan sistem operasi GNU/Linux

Mengetahui Struktur Hardisk (Lanjutan)

```
linux-a5gi:/mnt/case001/BB02 # mmfs 20130909.E01
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

   Slot   Start       End       Length      Description
00: Meta 0000000000 0000000000 0000000001 Primary Table (#0)
01: ---- 0000000000 0000002047 0000002048 Unallocated
02: 00:00 0000002048 0000499711 0000497664 Linux (0x83)
03: 00:01 0000499712 0059092991 0058593280 Linux (0x83)
04: 00:02 0059092992 0098154495 0039061504 Linux (0x83)
05: ---- 0098154496 0098156543 0000002048 Unallocated
06: Meta 0098156542 0123543551 0025387010 DOS Extended (0x05)
07: Meta 0098156542 0098156542 0000000001 Extended Table (#1)
08: 01:00 0098156544 0113778687 0015622144 Linux Swap / Solaris x86 (0x82)
09: Meta 0113778688 0123543551 0009764864 DOS Extended (0x05)
10: Meta 0113778688 0113778688 0000000001 Extended Table (#2)
11: ---- 0113778688 0113780735 0000002048 Unallocated
12: 02:00 0113780736 0123543551 0009762816 Linux (0x83)
13: ---- 0123543552 0156301487 0032757936 Unallocated
```

linux-a5gi:/mnt/case001/BB02 # █

Mengetahui Konten Dari Partisi 2

```
linux-a5gi:/mnt/case001/BB02 # fls -o 0499712 20130909.E01
d/d 11: lost+found
d/d 1790545:    var
d/d 883009:    boot
d/d 1798721:    home
d/d 703137:    opt
d/d 506913:    etc
d/d 1111937:    media
l/l 12: initrd.img
d/d 433329:    sbin
d/d 425153:    usr
d/d 32705:    lib
d/d 891185:    bin
d/d 1463505:    root
d/d 269809:    mnt
d/d 1651553:    tmp
d/d 441505:    dev
d/d 727665:    proc
d/d 989297:    selinux
d/d 825777:    sys
d/d 130817:    srv
l/l 13: vmlinuz
d/d 1831425: $OrphanFiles
```

Hasil Cek Konten Partisi 2

- Melihat konten yang ada bisa dilihat bahwa ini merupakan partisi / (root) di sistem operasi GNU/Linux
- Jadi sudah ada dua partisi yang terdeteksi:
 - /boot
 - /

Partisi (fstab)

- Setelah mendapatkan partisi / dapat ditelusuri keseluruhan partisi yang ada di system GNU/Linux menggunakan file bernama fstab (/etc/fstab)

```
linux-a5gi:/mnt/case001/BB02 # fls -r -o 499712 20130909.E01 | grep -i "fstab"
+ r/r 506915:    fstab
+ r/r 433703:    fstab-decode
+++++ r/r 433609:        fstab
+++++ r/r * 433609(realloc):    fstab.dpkg-new
+++++ r/r * 433770(realloc):    fstab.dpkg-tmp
+++++ r/r 441529:        fstab.example2
+++++ r/r * 441529(realloc):    fstab.example2.dpkg-new
+++++ r/r * 441598(realloc):    fstab.example2.dpkg-tmp
+++++ r/r 458022:        fstab.m4
++++ r/r * 427653(realloc):    fstab-decode.8.gz
++++ r/r 425186:        fstab-decode.8.gz
++++ r/r 427074:        fstab.5.gz
+++++ r/r 430994:        fstab.5.gz
+++ r/r 33013:  79-fstab_import.rules
++ r/r 33031:    fstab import
```

Partisi (fstab)

- Setelah mendapatkan partisi / dapat ditelusuri keseluruhan partisi yang ada di system GNU/Linux menggunakan file bernama fstab (/etc/fstab)

```
linux-a5gi:/mnt/case001/BB02 # fls -r -o 499712 20130909.E01 | grep -i "fstab"
+ r/ 506915:    fstab
+ r/r 433730:    fstab-decode
+++++ r/r 433609:        fstab
+++++ r/r * 433609(realloc):    fstab.dpkg-new
+++++ r/r * 433770(realloc):    fstab.dpkg-tmp
+++++ r/r 441529:        fstab.example2
+++++ r/r * 441529(realloc):    fstab.example2.dpkg-new
+++++ r/r * 441598(realloc):    fstab.example2.dpkg-tmp
+++++ r/r 458022:        fstab.m4
++++ r/r * 427653(realloc):    fstab-decode.8.gz
++++ r/r 425186:        fstab-decode.8.gz
++++ r/r 427074:        fstab.5.gz
+++++ r/r 430994:        fstab.5.gz
+++ r/r 33013:  79-fstab_import.rules
++ r/r 33031:    fstab import
```

Melihat isi file fstab

```
linux-a5gi:/mnt/case001/BB02 # icat -o 499712 20130909.E01 506915
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>   <options>           <dump>   <pass>
proc          /proc        proc    defaults      0         0
# / was on /dev/sda2 during installation
UUID=6464d8d8-9556-4e14-8fa7-ebea980f2a58 /           ext3    errors=remount-ro 0         1
# /boot was on /dev/sda1 during installation
UUID=65a1016a-1f7f-4162-b70e-d563b5c7ac62 /boot       ext2    defaults      0         2
# /home was on /dev/sda3 during installation
UUID=158d8900-56f9-47c6-964b-0066954aa50d /home     ext3    defaults      0         2
# /opt was on /dev/sda6 during installation
UUID=4151c311-cf8a-4ae7-b3e6-158db2f62d77 /opt      xfs    defaults      0         2
# swap was on /dev/sda5 during installation
UUID=2c20d026-4745-481b-8ccf-3bdcd7bd840 none      swap    sw            0         0
/dev/scd0      /media/cdrom0  udf,iso9660 user,noauto  0         0
```

Hasil Cek Konten Partisi

- /boot → ext2
- / → ext3
- /home → ext3
- /swap → swap
- /opt → xfs → tidak bisa dianalisis secara fisik

Cek file system xfs

- fls -o 0113780736 20130909.E01
-

```
linux-a5gi:/mnt/case001/BB02 # fls -o 0113780736 20130909.E01
Cannot determine file system type
```

A large, colorful word cloud centered around the words "thank you" in various languages. The word "thank" is in red and "you" is in green. Other words in the cloud include "danke" (German), "спасибо" (Russian), "dziekuje" (Polish), "obrigado" (Portuguese), "merci" (French), "ngiyabonga" (Swahili), "teşekkür ederim" (Turkish), "gracias" (Spanish), "mochchakkeram" (Burmese), "go raibh maith agat" (Irish), "arigatō" (Japanese), "dakujem" (Croatian), "mercs" (Hungarian), "감사합니다" (Korean), "xie xie" (Chinese), "merci" (French), "ευχαριστώ" (Greek), "dank je" (Dutch), "marsi" (Arabic), "barka" (Arabic), "welain" (Arabic), "tack" (Swedish), "misaotra" (Filipino), "matondo" (Swahili), "paldies" (Lithuanian), "grazzi" (Italian), "malao" (Swahili), "tapathit" (Thai), "хвала" (Russian), "asante manana" (Swahili), "otbrigada" (Bulgarian), and "cõeckoua pukaze" (Portuguese).



MENGUMPULKAN BUKTI ELEKTRONIK YANG
TERKONEKSI KE JARINGAN (*NETWORKED DEVICES*)

Perangkat Jaringan

- Perangkat jaringan dianggap sebagai komputer atau perangkat digital lain yang terhubung ke sebuah jaringan baik melalui kabel atau nirkabel.
- Perangkat jaringan ini dapat meliputi mainframe, server, komputer desktop, access point, switch, hub, router, perangkat mobile, PDA, PED, perangkat Bluetooth, sistem CCTV dan masih banyak lagi.
- Perhatikan jika perangkat digital merupakan perangkat jaringan, sulit untuk memastikan lokasi bukti digital potensial tersebut disimpan; Data bisa berada di manapun dalam jaringan

Identifikasi Perangkat Jaringan

Identifikasi perangkat digital termasuk komponen-komponen seperti logo manufaktur, nomor seri, docking station dan catu daya. DEFR dapat mempertimbangkan aspek-aspek berikut sebagai cara untuk mengidentifikasi:

- Karakteristik perangkat: Produsen perangkat digital terkadang dapat diidentifikasi melalui karakteristik yang dapat diamati, terutama jika terdapat elemen desain yang unik.
- Antarmuka Perangkat: Konektor daya seringkali merujuk pada produsen tertentu dan merupakan petunjuk yang dapat diandalkan untuk identifikasi.

Identifikasi Perangkat Jaringan (lanjutan)

- Label perangkat: Untuk perangkat mobile dalam keadaan mati, informasi yang diperoleh dari dalam tempat baterai dapat terlihat, terutama ketika digabungkan dengan database yang sesuai.
- Reverse lookup: Dalam kasus ponsel, jika nomor telepon dari ponsel tersebut diketahui, reverse lookup dapat digunakan untuk mengidentifikasi operator jaringan.

Pencarian dan Dokumentasi Tempat Kejadian Perkara

Sebelum akuisisi atau koleksi dapat dilakukan, tempat kejadian perkara harus didokumentasikan secara visual baik dengan foto, video atau sketsa.

- Perangkat jaringan, DEFR harus mengidentifikasi layanan yang diberikan oleh perangkat untuk memahami ketergantungan dan untuk memastikan tingkat pentingnya perangkat dalam jaringan sebelum memutuskan melepas perangkat dari jaringan
- DEFR juga harus mempertimbangkan penggunaan detektor sinyal nirkabel untuk mendeteksi dan mengidentifikasi sinyal nirkabel dari perangkat nirkabel yang mungkin disembunyikan.

Koleksi, Akuisisi dan Preservasi

- Koleksi dan akuisisi bukti digital potensial dari perangkat mobile jaringan merupakan proses yang rumit karena perangkat tersebut dapat berada pada beberapa kondisi dan moda interaksi contohnya Bluetooth, frekuensi radio, layar sentuh, dan infra merah.
- DEFR tidak boleh memasukkan perangkat Wi-Fi atau Bluetooth ke tempat kejadian perkara yang dapat mengubah informasi perangkat terkoneksi pada potensi perangkat bukti. Hal ini sangat penting khususnya jika penyidik harus mengetahui perangkat apa saja yang telah terhubung.

Koleksi, Akuisisi dan Preservasi

- Jika DEFR memutuskan untuk melakukan proses akuisisi, perangkat jaringan harus dibiarkan terus bekerja untuk analisis lebih lanjut agar dapat memastikan adanya perangkat lain yang terhubung ke perangkat jaringan.

Pedoman untuk Koleksi Perangkat Jaringan

Dalam kondisi tertentu, perangkat jaringan dibiarkan tetap terhubung sehingga kegiatan pada perangkat jaringan dapat dipantau dan didokumentasikan oleh DEFR dan/atau DES sesuai dengan kewenangannya. Apabila hal ini tidak diperlukan, perangkat harus dikoleksi seperti yang dijelaskan di bawah ini:

- DEFR harus mengisolasi perangkat dari jaringan
- Sebelum mencabut kabel, DEFR harus melacak koneksi ke perangkat digital dan memberi label pada port untuk melakukan rekonstruksi jaringan secara keseluruhan di kemudian hari. Perangkat dapat memiliki lebih dari satu metode komunikasi.

Pedoman untuk Koleksi Perangkat Jaringan (lanjutan)

- Pada tahap ini, harus diperhatikan bahwa mencabut daya dari perangkat jaringan dapat merusak data volatil seperti proses yang sedang bekerja, koneksi jaringan dan data yang tersimpan dalam memori.
- Jika koleksi dilakukan sebelum akuisisi dan diketahui bahwa perangkat berisi memori volatil, perangkat harus terus menerus terhubung ke sumber listrik.
- Jika perangkat mobile dimatikan, perangkat tersebut dibungkus secara hati-hati, disegel dan diberi label.

Pedoman untuk Koleksi Perangkat Jaringan (lanjutan)

- Dalam kondisi tertentu, perangkat mobile harus dimatikan pada saat koleksi untuk mencegah data tersebut diubah. Hal tersebut dapat terjadi melalui koneksi keluar dan masuk atau perintah yang dapat menyebabkan kerusakan bukti digital potensial.
- Selanjutnya, masing-masing perangkat digital diperlakukan sebagai perangkat independen sampai saat diperiksa. Selama pemeriksaan, perangkat tersebut harus dianggap sebagai perangkat jaringan.

Pedoman untuk Akuisisi Perangkat Jaringan

- Pada kondisi perangkat terhubung dalam sebuah jaringan, terdapat kemungkinan bahwa perangkat terhubung ke lebih dari satu (1) jaringan fisik dan / atau virtual.
- Sebagai contoh, sebuah perangkat yang terlihat memiliki satu (1) koneksi jaringan fisik dapat saja sebenarnya menjalankan Virtual Private Network (VPN) dan mesin virtual dengan lebih dari satu (1) alamat IP.
- Dengan demikian, sebelum memutuskan hubungan perangkat dari jaringan, DEFR harus melakukan logical acquisition dari data yang berkaitan dengan koneksi jaringan virtual, (misalnya jaringan internet). Data yang diambil meliputi namun tidak terbatas pada konfigurasi IP dan tabel routing.

Pedoman untuk Akuisisi Perangkat Jaringan (lanjutan)

- Jika perangkat jaringan diperlukan dalam keadaan menyala terus menerus, maka perangkat harus dicegah dari interaksi dengan jaringan radio nirkabel termasuk perangkat dengan GPS yang aktif.
- DEFR harus menggunakan metode yang diizinkan oleh peraturan perundangan untuk mengisolasi sinyal radio. Harus dipastikan bahwa perangkat memiliki sumber daya yang cukup, karena metode isolasi dapat membuat perangkat mengkonsumsi daya yang lebih dalam upaya terhubung ke jaringan. Metode isolasi dapat meliputi, namun tidak terbatas pada:

Pedoman untuk Akuisisi Perangkat Jaringan (lanjutan)

- Menggunakan perangkat jamming yang mampu memblokir transmisi dengan membuat gangguan yang kuat ketika perangkat memancarkan sinyal dalam rentang frekuensi yang sama dengan yang digunakan perangkat mobile.
- Menggunakan area kerja terlindung untuk melakukan pemeriksaan dengan aman di lokasi tertentu. Perlindungan dapat dilakukan untuk seluruh area kerja atau dengan mendirikan tenda Faraday yang dapat mudah berpindah-pindah.

Pedoman untuk Akuisisi Perangkat Jaringan (lanjutan)

- Menggunakan area kerja terlindung untuk melakukan pemeriksaan dengan aman di lokasi tertentu. Area kerja yang terlindung dari frekuensi radio atau wadah (sangkar Faraday) dapat digunakan untuk mencegah koneksi ke jaringan.
- Menggunakan sebuah (U)SIM pengganti yang meniru identitas perangkat asli dan mencegah akses jaringan oleh perangkat.
- Menonaktifkan layanan jaringan dengan mengatur operator layanan mobile dan mengidentifikasi rincian layanan yang akan dinonaktifkan (misalnya pengenal peralatan, pengenal pelanggan, atau nomor telepon).

Pedoman untuk Preservasi Perangkat Jaringan

- Karena sifat perangkat digital dan bukti digital, pedoman preservasi perangkat jaringan serupa dengan preservasi komputer, perangkat periferal dan media penyimpanan digital.

A large, colorful word cloud centered around the words "thank you" in various languages. The word "thank" is in red and "you" is in green. Other words in the cloud include "danke" (German), "спасибо" (Russian), "dziekuje" (Polish), "obrigado" (Portuguese), "merci" (French), "ngiyabonga" (Swahili), "teşekkür ederim" (Turkish), "gracias" (Spanish), "mochchakkeram" (Burmese), "go raibh maith agat" (Irish), "arigatō" (Japanese), "dakujem" (Croatian), "mercs" (Hungarian), "감사합니다" (Korean), "xie xie" (Chinese), "merci" (French), "ευχαριστώ" (Greek), "dank je" (Dutch), "marsi" (Arabic), "barka" (Arabic), "welain" (Arabic), "tack" (Swedish), "misaotra" (Filipino), "matondo" (Swahili), "paldies" (Lithuanian), "grazzi" (Italian), "malao" (Swahili), "tapathit" (Thai), "хвала" (Russian), "asante manana" (Swahili), "otbrigada" (Bulgarian), and "cõeckoua pukaze" (Portuguese).



ANALISIS BARANG BUKTI

Analisis Barang Bukti

- Dalam menganalisa ada beberapa hal yang dapat dilakukan seperti :
 - Mengetahui Jenis File
 - Mengetahui Timestamp Konten Partisi
 - Mengetahui History Browser
 - Mengetahui Windows Version
 - Mengetahui Computer Name
 - Mengetahui Keterangan OS
 - Mengetahui Daftar Koneksi
 - Mengetahui User Account

Mengetahui Jenis File

- Mengetahui jenis file yang terdapat pada barang bukti
 - sorter -l -m "c:" -e -o 63 dell3.E0* > jenis_file
 - “sorter” => perintah untuk mengurutkan file yang terdapat pada image berdasarkan jenis file
 - “-l” => argument untuk menampilkan dalam bentuk list
 - “-m” => argument mount point
 - “-e” => argument untuk pengecekan ekstensi

```
$ sorter -l -m "c:" -e -o 63 dell3.E0* > jenis_file
```

Mengetahui Jenis File (Lanjutan)

- Melihat isi file
 - vi jenis_file

```
Category: Unknown
c:/DETL0G.TXT
ASCII text, with CRLF line terminators
Image: dell3.E01 Inode: 128-128-3

Category: Unknown
c:/Documents and Settings/All Users/Application Data/Adobe/Acrobat/9.0/Replicate
/Security/directories.acrodata
FDF document, version 1.2
Image: dell3.E01 Inode: 1677-128-1

Category: Unknown
c:/Documents and Settings/All Users/Application Data/Adobe/Reader/9.3/ARM/13943/
AcrobatUpdater.exe
PE32 executable (GUI) Intel 80386, for MS Windows
Image: dell3.E01 Inode: 4755-128-4

Category: Unknown
c:/Documents and Settings/All Users/Application Data/Adobe/Reader/9.3/ARM/13943/
AdobeARM.exe
PE32 executable (GUI) Intel 80386, for MS Windows
Image: dell3.E01 Inode: 4761-128-3
```

Mengetahui Timestamp Konten Partisi

- Mengetahui timestamp :
 - Membuat daftar dari semua file yang berada pada drive “c:”
 - fls -r -o 63 -m "c:" dell3.E0* > FullFileList

```
$ fls -o 63 -r -m "c:" dell3.E0* > FullFileList
```

| 001.jpg | deleted | dell3.E04 | mdadm_sda.E01 | stuxnet.vmem |
|-------------------------|------------|--------------|------------------|--------------|
| 20130909.E01 | deletedBSD | FullFileList | MP.tmp | system |
| barangbukti001_mmls | dell3.dd | historyBSD | myfirstdump.vmem | zeus.vmem |
| barangbukti001_mmls.txt | dell3.E01 | hw_raid1.E01 | photorec.ses | |

Mengetahui Timestamp Konten Partisi (lanj.)

- Mengelompokan timestamp menjadi grouped dan merubahnya menjadi format tanggal agar mudah dibaca.
 - mactime -b FullFileList > FullFileList.grouped

```
$ mactime -b FullFileList > FullFileList.grouped
```

| | | | |
|-------------------------|--------------|----------------------|------------------|
| 001.jpg | deletedBSD | FullFileList.grouped | myfirstdump.vmem |
| 20130909.E01 | dell3.dd | historyBSD | photorec.ses |
| barangbukti001_mmls | dell3.E01 | hw_raid1.E01 | Picture |
| barangbukti001_mmls.txt | dell3.E02 | jakarta.vmem | Picture_001.jpg |
| boot | dell3.E03 | jenis_filebsd.txt | stuxnet.vmem |
| bsd.E01 | dell3.E04 | mdadm_sda.E01 | system |
| deleted | FullFileList | MP.tmp | zeus.vmem |

Mengetahui Timestamp Konten Partisi (lanj.)

- vi FullFileList.grouped
-

| | | | | | | | |
|------------------------------------------------------|-------|------|--------------|---|---|-------------|----------------------------------------------|
| Sat Dec 16 1989 12:21:08 | 5212 | m... | r/rrwxrwxrwx | 0 | 0 | 10837-128-4 | c:/My Documents/FOOTPRINTING/NT/Nmapnt/nmapN |
| T-src/libpcap-possiblymodified/SUNOS4/nit_if.o.sparc | | | | | | | |
| Sat Dec 16 1989 12:21:14 | 4267 | m... | r/rrwxrwxrwx | 0 | 0 | 10838-128-4 | c:/My Documents/FOOTPRINTING/NT/Nmapnt/nmapN |
| T-src/libpcap-possiblymodified/SUNOS4/nit_if.o.sun3 | | | | | | | |
| Tue Jul 17 1990 00:30:28 | 11909 | m... | r/rrwxrwxrwx | 0 | 0 | 10894-128-3 | c:/My Documents/NOVELL/BINDIN.EXE |
| Tue Jul 23 1991 05:07:14 | 7228 | m... | r/rrwxrwxrwx | 0 | 0 | 10938-128-3 | c:/My Documents/NOVELL/Nut18/NGETTIME.EXE |
| Sun Jul 28 1991 20:31:06 | 6668 | m... | r/rrwxrwxrwx | 0 | 0 | 10931-128-3 | c:/My Documents/NOVELL/Nut18/NDISK.EXE |
| Sun Jul 28 1991 20:34:02 | 6092 | m... | r/rrwxrwxrwx | 0 | 0 | 10936-128-3 | c:/My Documents/NOVELL/Nut18/NEXTMEM.EXE |
| Sun Jul 28 1991 20:35:50 | 7060 | m... | r/rrwxrwxrwx | 0 | 0 | 10946-128-3 | c:/My Documents/NOVELL/Nut18/NMEM.EXE |
| Sun Jul 28 1991 20:38:12 | 6188 | m... | r/rrwxrwxrwx | 0 | 0 | 10970-128-3 | c:/My Documents/NOVELL/Nut18/NXMSMEM.EXE |
| Mon Oct 14 1991 03:43:26 | 7564 | m... | r/rrwxrwxrwx | 0 | 0 | 10964-128-3 | c:/My Documents/NOVELL/Nut18/NSETTIME.EXE |
| Tue Nov 26 1991 03:49:30 | 10108 | m... | r/rrwxrwxrwx | 0 | 0 | 10941-128-3 | c:/My Documents/NOVELL/Nut18/NLOGADDR.EXE |
| Sat Feb 08 1992 23:16:18 | 890 | m... | r/rrwxrwxrwx | 0 | 0 | 10891-128-3 | c:/My Documents/NOVELL/BINDERY.DOC |
| Sat Feb 08 1992 23:17:04 | 1495 | m... | r/rrwxrwxrwx | 0 | 0 | 10903-128-3 | c:/My Documents/NOVELL/USERINFO.DOC |

Melihat History Browser

- Setiap browser memiliki pencatatan history yang berbeda
- Sebagai contoh akan kita lakukan pengecekan history browser untuk 3 jenis browser
 - IE
 - Firefox
 - Chrome

Melihat History Browser IE

- History browser IE dapat dilihat pada file index.dat
- Cari tahu terlebih dahulu keberadaan lokasi file
 - fls -r -o 63 dell3.E0* | grep "index.dat"

```
+++ / / 0007-128-4: index.dat
+++++ r/r 6609-128-4: index.dat
+++++ r/r 6597-128-4: index.dat
+++ r/r 395-128-3: index.dat
+++++ r/r 396-128-3: index.dat
+++++ r/r 434-128-3: index.dat
+++ r/r 9794-128-4: index.dat
+++++ r/r 9789-128-4: index.dat
++++++ r/r 12466-128-3: index.dat
++++++ r/r 12927-128-3: index.dat
++++++ r/r 7931-128-3: index.dat
+++++ r/r 9787-128-4: index.dat
+++ r/r 12479-128-3: index.dat
+++ r/r 6405-128-4: index.dat
+++++ r/r 9737-128-5: index.dat
```

Melihat History Browser IE

- Jika sudah tau alamatnya, lakukan rekonstruksi
 - icat -o 63 dell3.E0* 12927-128-3 > index.dat
 - Ls

```
ik/IMAGE $ icat -o 63 dell3.E0* 12927-128-3 > index.dat
```

| | | |
|-------------------------|----------------------|-------------------|
| 001.jpg | dell3.E02 | jenis_filebsd.txt |
| 20130909.E01 | dell3.E03 | mdadm_sda.E01 |
| barangbukti001_mmls | dell3.E04 | MP.tmp |
| barangbukti001_mmls.txt | FullFileList | myfirstdump.vmem |
| boot | FullFileList.grouped | photorec.ses |
| bsd.E01 | historyBSD | Picture |
| deleted | hw_raid1.E01 | Picture_001.jpg |
| deletedBSD | index.dat | stuxnet.vmem |

Melihat History Browser IE

- Melihat isi file
 - vi index.dat

Mengetahui Windows Version

- Mencari tahu lokasi keberadaan file “software” yang menyimpan informasi windows
 - fls -o 63 -r dell3.E0* | grep “software”

```
ik/IMAGE $ fls -o 63 -r dell3.E0* | grep "software"
++++ r/r 9895-128-4: software-A.bmp
++++ r/r 9896-128-4: software-D.bmp
++++ r/r 9897-128-4: software-M.bmp
+++ r/r 336-128-4: software
+++ r/r 466-128-5: software.LOG
+++ r/r 471-128-3: software.sav
++ r/r 9742-128-4: software
```

Mengetahui Windows Version (lanjutan)

- rip.pl -r software -p winver
 - rip => software regripper yang digunakan untuk melakukan analisis registry
 - “-r” => argument untuk file registry
 - “-p” => argument plugins

```
$ icat -o 63 dell3.E0* 336-128-4 > software
```

```
tan@tan-K46CM /media/tan/01D08E3/82BA3050/Data_Kerjaan/Materi_Ngajar/umum/torensik/IMAGE $ rip -r software -p winver
Launching winver v.20081210
winver v.20081210
(Software) Get Windows version

ProductName = Microsoft Windows XP
CSDVersion = Service Pack 3
InstallDate = Thu Aug 19 22:48:27 2004
```

Mengetahui Nama Komputer

- rip.pl -r software -p compname
 - “compname => plugins untuk mengetahui nama komputer

```
ik/IMAGE $ rip -r system -p compname
Launching compname v.20090727
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName      = XPSP3
TCP/IP Hostname  = XPSP3
```

Mengetahui Software Build

- rip.pl -r software -p winnt_cv
 - “winnt_cv” => plugins untuk mengetahui software build

```
winnt_cv v.20080609
(Software) Get & display the contents of the Windows NT\CurrentVersion key

WinNT_CV
Microsoft\Windows NT\CurrentVersion
LastWrite Time Mon May 24 13:52:14 2010 (UTC)

RegDone :
SubVersionNumber :
RegisteredOrganization : N/A
CurrentVersion : 5.1
SourcePath : D:\|
CurrentBuildNumber : 2600
SoftwareType : SYSTEM
SystemRoot : C:\WINDOWS
PathName : C:\WINDOWS
RegisteredOwner : Greg Schardt
CSDVersion : Service Pack 3
CurrentType : Uniprocessor Free
ProductName : Microsoft Windows XP
BuildLab : 2600.xpsp.080413-2111
ProductId : 55274-640-0147306-23684
InstallDate : Thu Aug 19 22:48:27 2004 (UTC)
```

Mengetahui Daftar Koneksi

- Mencari tahu lokasi keberadaan file “system” yang menyimpan daftar koneksi
 - fls -o 63 -r dell3.E0* | grep “system”

```
++++++ -/r * 13527-128-3:    mmsystem.dll_
++++++ -/r * 14679-128-3:    system.ad_
++++++ -/r * 14680-128-3:    system.ch_
++++++ -/d * 15274-144-1:    system
++++++ -/d * 15281-144-1:    system
++++++ -/r * 20248-128-4:    system.configuration.install.dll
++++++ -/r * 20249-128-4:    system.data.dll
++++++ -/r * 20250-128-4:    system.design.dll
++++++ -/r * 20251-128-4:    system.design.ldo
++++++ -/r * 20252-128-4:    system.directoryservices.dll
++++++ -/r * 20253-128-4:    system.drawing.design.dll
++++++ -/r * 20254-128-4:    system.drawing.dll
++++++ -/r * 20255-128-4:    system.drawing.ldo
```

Mengetahui Daftar Koneksi (lanjutan)

- Terdapat beberapa file “system” yang memiliki nilai inode yang berbeda, lakukan rekonstruksi kepada semua file tersebut.
- Merekonstruksi file “system” dengan inode 2254-144-6 :
 - icat -o 63 dell3.E0* 2254-144-6 > system
 - Ls

```
001.jpg          dell3.E02          mdaum_sua.E01
20130909.E01    dell3.E03          MP.tmp
barangbukti001_mmls dell3.E04          myfirstdump.vmem
barangbukti001_mmls.txt FullFileList      photorec.ses
boot             FullFileList.grouped Picture
bsd.E01          historyBSD        Picture_001.jpg
default          hw_raid1.E01       software
deleted          index.dat         stuxnet.vmem
deletedBSD       jakarta.vmem     system
```

Mengetahui Daftar Koneksi (lanjutan)

- rip.pl -r system -p nic_mst2
 - nic_mst2 => argumen untuk mengetahui konfigurasi network

```
Launching nic_mst2 v.20080324
nic_mst2 v.20080324
(System) Gets NICs from System hive; looks for MediaType = 2

Error in /usr/local/bin/plugins/nic_mst2.pl: Can't call method "get_root_key" on
an undefined value at /usr/local/bin/plugins/nic_mst2.pl line 51.
```

Mengetahui Daftar Koneksi (lanjutan)

- Lakukan juga pada file “system” dengan inode yg lain:
 - icat -o 63 dell3.E0* 334-128-4 > system
 - ls

```
001.jpg          dell3.E02          mdadm_sda.E01
20130909.E01    dell3.E03          MP.tmp
barangbukti001_mmls  dell3.E04          myfirstdump.vmem
barangbukti001_mmls.txt FullFileList      photorec.ses
boot            FullFileList.grouped  Picture
bsd.E01          historyBSD        Picture_001.jpg
default          hw_raid1.E01       software
deleted          index.dat         stuxnet.vmem
deletedBSD       jakarta.vmem     system
```

Mengetahui Daftar Koneksi (lanjutan)

- rip.pl -r system -p nic_mst2

```
Interface {D4306202-EE6C-426D-90C1-D7CECE4C6ACF}
Name: Local Area Connection 3
Control\Network key LastWrite time Fri May  7 11:59:43 2010 (UTC)
Services\Tcpip key LastWrite time Mon May 24 13:57:31 2010 (UTC)
    DhcpDomain      = hpm.local
    DhcpIPAddress  = 192.168.0.162
    DhcpSubnetMask = 255.255.255.0
    DhcpNameServer = 192.168.0.1
    DhcpServer      = 192.168.0.2
```

Mengetahui Daftar Koneksi (lanjutan)

- Lakukan juga pada file “system” dengan inode yg lain:
 - icat -o 63 dell3.E0* 9741-128-4 > system
 - ls

```
001.jpg          dell3.E02        mdadm_sda.E01
20130909.E01    dell3.E03        MP.tmp
barangbukti001_mmls  dell3.E04    myfirstdump.vmem
barangbukti001_mmls.txt FullFileList  photorec.ses
boot            FullFileList.grouped Picture
bsd.E01          historyBSD      Picture_001.jpg
default          hw_raid1.E01     software
deleted          index.dat       stuxnet.vmem
deletedBSD       jakarta.vmem    system
```

Mengetahui Daftar Koneksi (lanjutan)

- rip.pl -r system -p nic_mst2

```
Launching nic_mst2 v.20080324
nic_mst2 v.20080324
(System) Gets NICs from System hive; looks for MediaType = 2

Network key
ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}

ControlSet001\Services\Tcpip\Parameters\Interfaces
LastWrite time Thu Aug 19 22:21:42 2004 (UTC)

Interface {6E4090C2-FAEF-489A-8575-505D21FC1049}
Name: Local Area Connection
Control\Network key LastWrite time Thu Aug 19 22:22:07 2004 (UTC)
Services\Tcpip key LastWrite time Thu Aug 19 22:21:49 2004 (UTC)
    DhcpDomain      =
    DhcpIPAddress  = 169.254.242.213
    DhcpSubnetMask = 255.255.0.0
    DhcpNameServer =
    DhcpServer      = 255.255.255.255
```

Mengetahui User Account

- Mencari lokasi file “SAM”
 - `fls -o 63 -r dell3.E0* | grep "SAM"`

```
++ r/r 10273-128-3: SAMDUMP.EXE
+++ r/r 3667-128-4: SAM
+++ r/r 3668-128-4: SAM.LOG
```

Mengetahui User Account (lanjutan)

- Merekonstruksi file “SAM”
 - icat -o 63 dell3.E0* 3667-128-4
 - ls

```
001.jpg          dell3.E02          mdadm_sda.E01
20130909.E01    dell3.E03          MP.tmp
barangbukti001_mmls dell3.E04          myfirstdump.vmem
barangbukti001_mmls.txt FullFileList      photorec.ses
boot             FullFileList.grouped Picture
bsd.E01          historyBSD        Picture_001.jpg
default          hw_raid1.E01       SAM
```

Mengetahui User Account (Lanjutan)

- rip.pl -r SAM -p samparse

```
Launching samparse v.20120722
samparse v.20120722
(SAM) Parse SAM file for user & group mbrshp info

User Information
-----
Username      : Administrator [500]
Full Name     :
User Comment   : Built-in account for administering the computer/domain
Account Type   : Default Admin User
Account Created : Thu Aug 19 16:59:24 2004 Z
Last Login Date : Never
Pwd Reset Date : Thu Aug 19 17:17:29 2004 Z
Pwd Fail Date  : Never
Login Count    : 0
    --> Password does not expire
    --> Normal user account

Username      : Guest [501]
```

A large, colorful word cloud centered around the words "thank you" in various languages. The words are arranged in a circular pattern, with "thank" at the top and "you" at the bottom. The languages include German (danke), Chinese (謝謝), Turkish (teşekkür ederim), Russian (спасибо), Polish (dziękuje), Spanish (gracias), French (merci), English (thank you), Portuguese (obrigado), Italian (grazie), Dutch (dank u), Korean (감사합니다), Japanese (ありがとうございます), Indonesian (terima kasih), Thai (ขอบคุณ), Vietnamese (cảm ơn bạn), and many others like Russian (спасибо), German (danke), and Chinese (謝謝). The words are in different colors and sizes, creating a dense and visually appealing composition.



UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Informatika

KEBIJAKAN FORENSIK DIGITAL

Landasan Hukum

Landasan hukum dalam melakukan penanganan barang bukti digital berdasarkan pada:

- Undang-undang Republik Indonesia No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik
- Peraturan Pemerintah Republik Indonesia No. 82 tahun 2012 tentang penyelenggaraan sistem dan transaksi elektronik
- Undang-undang Republik Indonesia No. 14 tahun 2008 tentang Keterbukaan Informasi Publik
- Undang-undang Republik Indonesia No. 43 tahun 2009 tentang Kearsipan

Kedudukan Bukti Elektronik

- Dalam hukum acara pidana, bukti elektronik seharusnya dikategorikan sebagai “barang bukti”, bukan sebagai “alat bukti”. Dengan demikian, harus terdapat ketentuan mengenai tata cara perolehannya
- Kedudukan alat bukti elektronik dalam Undang-Undang ITE dan kaitannya dengan alat bukti dalam KUHAP yakni:
 1. Alat bukti elektronik memperluas cakupan atau ruang lingkup alat bukti
 2. Alat bukti elektronik sebagai alat bukti lain
 3. Alat bukti elektronik sebagai sumber petunjuk

Bukti Elektronik Dalam Peraturan Perundangan Indonesia

1. Undang-Undang Republik Indonesia Nomor 8 Tahun 1997 Tentang Dokumen Perusahaan

- Bab III tentang Pengalihan Bentuk Dokumen Perusahaan dan Legalisasi, yakni pada pasal 15 ayat (1) yang menyatakan : “Dokumen Perusahaan yang telah dimuat dalam mikrofilm atau media yang lainnya dan/atau hasil cetaknya merupakan alat bukti yang sah”
- Dalam penjelasan pasal 12 ayat (1) Undang-Undang Dokumen Perusahaan, disampaikan bahwa microfilm adalah film yang memuat rekaman bahan tertulis, tercetak dan tergambar dalam ukuran yang sangat kecil.
- Surat Mahkamah Agung kepada Menteri Kehakiman tanggal 14 Januari 1988 No. 39/TU/88/102/Pid yang mengemukakan pendapatnya, bahwa microfilm atau microfiche dapat dipergunakan sebagai alat bukti yang sah dalam perkara pidana di pengadilan menggantikan alat bukti surat, dengan catatan microfilm itu sebelumnya dijamin otentikasinya yang dapat ditelusuri kembali dari registrasi maupun berita acara

Bukti Elektronik Dalam Peraturan Perundangan Indonesia

2. Undang-Undang Republik Indonesia Nomor 20 Tahun 2001 jo . Undang-Undang Nomor 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi
 - Alat bukti yang sah dalam bentuk petunjuk sebagaimana dimaksud dalam pasal 188 ayat (2) Undang-Undang Republik Indonesia No. 8 Tahun 1981 Tentang Hukum Acara Pidana (KUHAP), khusus untuk tindak pidana korupsi juga dapat diperoleh dari:
 - Alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu
 - Dokumen, yakni setiap rekaman data atau informasi yang dapat dilihat, dibaca, dan/atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana

Bukti Elektronik Dalam Peraturan Perundangan Indonesia

3. UU RI No. 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti UU No. 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang.

Alat bukti pemeriksaan tindak pidana terorisme meliputi:

- Alat bukti sebagaimana dimaksud dalam Hukum Acara Pidana
- Alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu
- Data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, termasuk tetapi tidak terbatas pada:
 - Tulisan, suara, atau gambar
 - Peta, rancangan, foto, atau sejenisnya
 - Huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.

Bukti Elektronik Dalam Peraturan Perundangan Indonesia

4. Undang-Undang Republik Indonesia Nomor 8 Tahun 2010 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang
 - Alat bukti yang sah menurut pasal 73 terdiri dari:
 - Alat bukti sebagaimana dimaksud dalam Hukum Acara Pidana
 - Alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu;
 - Alat bukti yang sah didalam ketentuan umum no 16:
 - Disebutkan juga bahwa Dokumen adalah data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas atau benda fisik apa pun selain kertas maupun yang terekam secara elektronik

Bukti Elektronik Dalam Peraturan Perundangan Indonesia

5. UU RI No 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Pasal 5 ayat (1) Undang-Undang ITE menyatakan bahwa:

1. Informasi Elektronik/Dokumen Elektronik/hasil cetaknya merupakan alat bukti hukum yang sah
2. Informasi Elektronik/Dokumen Elektronik/hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku
3. Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.
4. Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk surat yang menurut UU harus dibuat dalam bentuk tertulis dan surat beserta dokumennya yang menurut UU harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta

KUHP tentang barang bukti digital

Berdasarkan KUHAP Persyaratan yang harus hakim penuhi dalam upaya pemeriksaan di persidangan terdiri atas:

| Aspek Penilaian | Persyaratan |
|---------------------------------------|-----------------------------------------|
| Syarat wajib dalam memutuskan perkara | Dua alat bukti yang sah |
| | Keyakinan hakim |
| Syarat wajib alat bukti | Membuktikan tindak pidana benar terjadi |
| | Membuktikan terdakwa yang melakukannya |



Surat Edaran Kominfo tentang penanganan barang bukti digital

Penanganan terhadap Bukti Elektronik dilakukan dengan memperhatikan integritas atau keutuhan data, perlindungan terhadap privasi, kerahasiaan, dan kelancaran layanan publik, sesuai dengan ketentuan peraturan perundang-undangan.

Ruang lingkup Peraturan Menteri ini meliputi:

- a. prinsip dasar Bukti Elektronik;
- b. Tahapan penanganan pertama Bukti Elektronik;
- c. penjelasan personel yang terlibat dalam penanganan Bukti Elektronik;
- d. Rantai Pengawasan (Chain of Custody) Bukti Elektronik;
- e. penjaminan kerahasiaan data;
- f. ketentuan minimum alat dan perangkat yang disiapkan.



Surat Edaran Kominfo tentang penangan barang bukti digital

Bukti Elektronik adalah Sistem Elektronik, Perangkat Elektronik, dan/atau Media Penyimpan Elektronik yang didalamnya terdapat Informasi Elektronik dan/atau Dokumen Elektronik yang dapat diandalkan sebagai alat bukti.

Alat Bukti Elektronik adalah Informasi Elektronik dan/atau Dokumen Elektronik yang digunakan sebagai alat bukti dalam peradilan sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2019 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

4 langkah utama dalam penanganan barang bukti digital

- Proses penanganan awal bukti digital adalah sebagai berikut:

- 1. Identifikasi**

Proses identifikasi melibatkan pencarian, pengenalan dan dokumentasi bukti digital potensial

- 2. Koleksi**

Setelah perangkat digital yang mengandung bukti digital potensial diidentifikasi, DEFR dan DES harus memutuskan untuk mengkoleksi atau mengakuisisi pada proses berikutnya. Koleksi adalah proses penanganan bukti digital ketika perangkat yang berisi bukti digital potensial dipindahkan dari lokasi asli ke laboratorium untuk akuisisi dan analisis selanjutnya

- 3. Akuisisi**

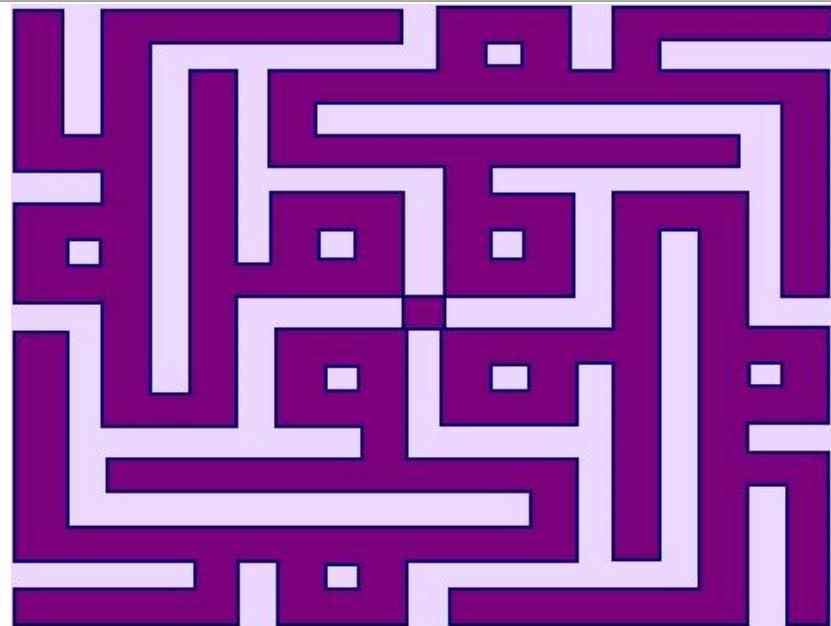
Proses akuisisi melibatkan penghasilan salinan bukti digital (misalnya hardisk utuh, partisi file terpilih) dan mendokumentasikan metode yang digunakan dan tindakan yang dilakukan

- 4. Preservasi**

Proses preservasi melibatkan pengamanan bukti digital potensial dan perangkat digital yang mengandung bukti digital dari perusakan atau pengubahan



Terima Kasih





UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Informatika

SNI/ISO 27037

Digital Evidence First Responder (DEFR)

Individu yang berwenang, terlatih dan berkualifikasi untuk bertindak terlebih dahulu di tempat kejadian perkara melakukan koleksi dan akuisisi bukti digital dengan tanggung jawab menangani bukti tersebut.

Digital Evidence Specialist (DES)

Individu yang dapat melaksanakan tugas-tugas seorang DEFR dan memiliki pengetahuan, keterampilan dan kemampuan khusus untuk menangani berbagai permasalahan teknis

DEFR dan DES

Semua proses yang akan digunakan oleh DEFR dan DES harus telah divalidasi sebelum penggunaan. Jika validasi dilakukan secara eksternal, DEFR atau DES harus memverifikasi bahwa validasi telah sesuai untuk penggunaan khusus mereka terhadap proses dan lingkungan dan keadaan di mana proses tersebut akan digunakan. DEFR atau DES juga harus:

- a) Mendokumentasikan semua tindakan;
- b) Menentukan dan menerapkan sebuah metode untuk memperlihatkan keakuratan dan keandalan dari salinan bukti digital potensial dibandingkan dengan sumber aslinya;
- c) Memahami bahwa tindakan preservasi bukti digital potensial tidak selalu dalam kondisi yang kondusif

DEFR dan DES

DEFR dan DES harus mengikuti prosedur yang terdokumentasi untuk memastikan integritas dan keandalan bukti digital potensial dapat dipertahankan. Prosedur harus meliputi pedoman penanganan sumber bukti digital potensial dan harus mencakup prinsip-prinsip dasar berikut:

- Meminimalkan penanganan perangkat digital asli atau bukti digital potensial;
- Memperhitungkan perubahan apapun dan mendokumentasikan tindakan yang diambil (hingga tahap ketika seorang ahli mampu memberikan penilaian terkait keandalan);
- Mematuhi aturan pedoman bukti lokal;
- DEFR dan DES tidak boleh melakukan tindakan melebihi kompetensi mereka

Prinsip bukti digital

Penanganan pertama terhadap Bukti Elektronik harus memenuhi 3 (tiga) prinsip dasar:

- a. relevansi;
- b. keandalan;
- c. kecukupan.

Relevansi

Relevansi: Harus dapat ditunjukkan bahwa material yang diakuisisi relevan dengan investigasi yaitu yang mengandung informasi berguna dalam membantu investigasi atas insiden tertentu dan ada alasan yang kuat sehingga material tersebut diakuisisi. Melalui audit dan justifikasi, DEFR harus dapat mendeskripsikan prosedur yang diikuti dan menjelaskan proses pengambilan keputusan untuk mengakuisisi setiap material.

Keandalan

Kecukupan: DEFR harus mempertimbangkan bahwa material yang dikoleksi telah cukup untuk melaksanakan proses investigasi yang tepat. Melalui audit dan justifikasi, DEFR harus dapat memberikan petunjuk jumlah material secara total yang perlu dipertimbangkan dan prosedur yang digunakan untuk menentukan jumlah dan jenis material yang diakuisisi.

Kecukupan

Kecukupan: DEFR harus mempertimbangkan bahwa material yang dikoleksi telah cukup untuk melaksanakan proses investigasi yang tepat. Melalui audit dan justifikasi, DEFR harus dapat memberikan petunjuk jumlah material secara total yang perlu dipertimbangkan dan prosedur yang digunakan untuk menentukan jumlah dan jenis material yang diakuisisi.

Persyaratan Untuk Penanganan Bukti Digital

- **Auditability (dapat diaudit)**
- **Dapat diulang**
- **Dapat diproduksi ulang**
- **Dapat dijustifikasi**

Auditability (dapat diaudit)

- Penilai independen atau pihak berwenang yang berkepentingan lainnya harus dimungkinkan untuk dapat mengevaluasi tindakan yang dilakukan oleh DEFR dan DES

Dapat diulang

Kemampuan dapat diulang dan dibuktikan ketika menggunakan prosedur dan peralatan yang sama serta dapat diulang setiap saat setelah pengujian awal

Dapat diproduksi ulang

Kemampuan dapat diproduksi ulang dibuktikan ketika hasil tes yang sama dapat dihasilkan dalam kondisi sebagai berikut:

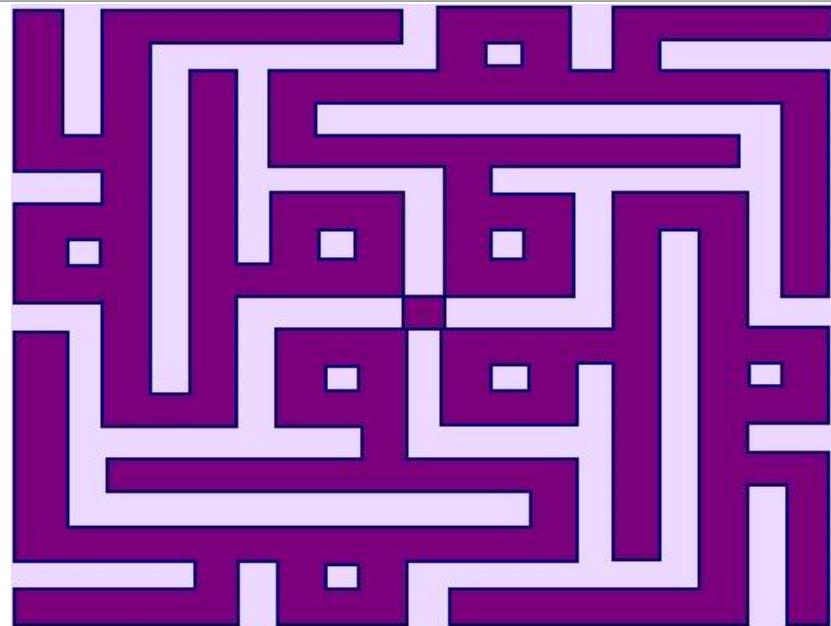
- Menggunakan metode pengukuran yang sama;
- Menggunakan peralatan yang berbeda dan dalam kondisi yang berbeda;
- Dapat diproduksi ulang setiap saat setelah pengujian awal.

Dapat dijustifikasi

DEFR harus dapat menjustifikasi semua tindakan dan metode yang digunakan dalam menangani bukti digital potensial.



Terima Kasih





UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Informatika

Proses Penanganan BB DIGITAL menurut SNI/ISO 27037

Definisi Bukti Elektronik

- Definisi menurut ISO/IEC 27073:2012 bukti elektronik adalah informasi atau data, disimpan atau dikirim dalam bentuk biner (binary form) yang diandalkan sebagai bukti
- Definisi secara umum bukti elektronik adalah data atau informasi yang tersimpan secara elektronik dalam suatu medium tertentu yang berkaitan dengan atau dapat membuktikan suatu tindak pidana.

Hal ini menunjukkan bahwa bukti elektronik bukanlah sebuah medium atau perangkat, melainkan data atau informasi yang tersimpan di dalamnya.

Karakteristik Bukti Elektronik

1. Bersifat laten (tersembunyi, tidak terlihat, tidak berwujud)

“Laten atau tidak terlihat, seperti sidik jari atau bukti DNA, dapat berpindah dengan cepat dan mudah, mudah diubah, rusak, atau hancur, dan sensitif terhadap waktu”- Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition

2. Membutuhkan mekanisme atau sarana khusus untuk dapat dilihat/dibaca

“Membutuhkan alat khusus untuk melihat/ membacanya, yang terdiri dari perangkat keras (hardware) dan perangkat lunak (software)”- Good Practice Guide for Computer-based Electronic Evidence, Association of Chief Police (ACPO)

3. Bersifat rapuh (volatile), mudah berubah, mudah rusak, dan mudah hancur tanpa penanganan yang layak dan tepat.

“...dapat menjadi rapuh secara alami. Bukti elektronik dapat diubah, dirusak, atau dimusnahkan karena penanganan atau pemeriksaan yang tidak benar” - ISO/IEC 27073:2012

Proses Penanganan Bukti Elektronik

Tahapan penanganan pertama Bukti Elektronik yakni:

- a. Identifikasi;
- b. Koleksi;
- c. Akuisisi;
- d. Preservasi

Identifikasi

Proses Identifikasi sebagaimana dimaksud pada ayat (1) huruf a dilakukan dengan tujuan:

- a. mengenali Sistem Elektronik, Perangkat Elektronik, dan Media Penyimpanan Elektronik yang berisi Informasi Elektronik dan/atau Dokumen Elektronik potensial yang relevan dengan perkara;
- b. membuat daftar prioritas Bukti Elektronik potensial yang relevan dengan perkara untuk dikoleksi terlebih dahulu; dan
- c. mengidentifikasi kemungkinan adanya Bukti Elektronik potensial yang tersembunyi

Koleksi

Proses Koleksi sebagaimana dimaksud pada ayat (1) huruf b dilakukan dengan ketentuan sebagai berikut:

- a. bukti yang dikoleksi merupakan bukti yang berdasarkan hasil penilaian Identifikasi sebagaimana dimaksud pada ayat (2) diduga berhubungan langsung dengan perkara;
- b. pelaksanaan Koleksi Bukti Elektronik tidak mengganggu kepentingan publik; dan
- c. melakukan penilaian terhadap faktor yang relevan dengan perkara yang sedang ditangani berdasarkan panduan sebagaimana tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

Akuisisi

Proses Akuisisi terhadap Bukti Elektronik harus dilakukan dengan ketentuan sebagai berikut:

- a. menggunakan metode yang dapat menghasilkan Salinan Bukti Elektronik (Penyalinan per-bit (Imaging)) yang dapat diverifikasi keakuratannya (verifikasi Nilai Hash); dan
- b. menggunakan cara yang paling aman untuk menghindari perubahan Informasi Elektronik dan/atau Dokumen Elektronik sepanjang memungkinkan.

Preservasi

Proses Preservasi terhadap Bukti Elektronik harus dilakukan dengan ketentuan sebagai berikut:

- a. memberikan pengamanan yang memadai untuk melindungi integritas dan keaslian Bukti Elektronik potensial serta Rantai Pengawasan (Chain of Custody); dan
- b. dilakukan sejak proses Identifikasi.

Komponen kunci identifikasi, koleksi, akuisisi dan preservasi bukti digital

Rantai pengawasan (Chain of custody)

Catatan rantai pengawasan (Chain of custody record) adalah dokumen yang mengidentifikasi kronologi pergerakan dan penanganan bukti digital potensial.

Catatan ini harus dibuat mulai dari proses koleksi atau akuisisi. Hal ini biasanya akan diselesaikan dengan menelusuri riwayat bukti sejak berhasil diidentifikasi, dikoleksi atau diakuisisi oleh tim investigasi hingga status dan lokasi saat ini

Rantai pengawasan (Chain of custody)

Catatan rantai pengawasan adalah dokumen atau serangkaian dokumen terkait yang merincikan rantai pengawasan dan catatan atas siapa yang bertanggung jawab untuk menangani bukti digital potensial, baik dalam bentuk data digital atau format lain (seperti catatan kertas).

Tujuan menjaga catatan rantai pengawasan adalah untuk memungkinkan teridentifikasinya akses dan pergerakan bukti digital potensial pada titik waktu tertentu.

Rantai pengawasan (Chain of custody)

Catatan rantai pengawasan minimal harus berisi informasi berikut:

- Tanda pengenal bukti yang unik;
- Siapa yang mengakses bukti dan waktu serta lokasi terjadinya;
- Siapa yang memeriksa bukti di dalam dan di luar dari fasilitas preservasi bukti dan kapan hal itu terjadi;
- Mengapa bukti tersebut diperiksa (kasus dan tujuan) dan otoritas yang relevan, jika ada;
- Setiap perubahan yang tidak dapat dihindari pada bukti digital potensial, serta nama individu yang bertanggung jawab karenanya dan justifikasi untuk pengubahan

Rantai pengawasan (Chain of custody)

Rantai pengawasan harus dipertahankan sepanjang masa alat bukti dan dipreservasi dalam jangka waktu tertentu setelah berakhirnya masa alat bukti - jangka waktu ini dapat diatur sesuai dengan yurisdiksi lokal dari pengoleksian dan pengajuan alat bukti.

Rantai pengawasan harus diterapkan sejak saat perangkat digital dan/atau bukti digital potensial diakuisisi dan tidak boleh dikompromikan

Tindakan pencegahan di lokasi kejadian

Tindakan harus mendukung hal berikut, patuh pada hukum lokal:

- Mengamankan dan memegang kendali area yang berisi perangkat;
- Menentukan siapa individu yang bertanggung jawab di lokasi;
- Memastikan individu dijauhkan dari perangkat dan daya listrik
- Mendokumentasikan siapa saja yang memiliki akses ke lokasi dan siapa saja yang diduga memiliki alasan untuk terlibat dengan tempat kejadian perkara;
- Jika perangkat dalam keadaan menyala jangan mematikannya dan jika perangkat dalam keadaan mati jangan menyalakannya;
- Jika memungkinkan, dokumen (misalnya sketsa, foto atau video) tempat kejadian perkara, semua komponen dan kabel dalam posisi semula. Jika tidak ada kamera dan / atau kamera video yang tersedia, gambar sketsa denah sistem dan beri label pada port dan kabel sehingga sistem dapat divalidasi dan direkonstruksi di kemudian hari; dan
- Jika diperbolehkan, lakukan pencarian di area untuk barang-barang seperti catatan tempel (sticky note), buku harian, kertas, komputer notebook, atau perangkat keras dan manual perangkat lunak dengan rincian yang penting tentang perangkat seperti password dan PIN.

Personel

Hal yang harus dipertimbangkan dalam menilai risiko terhadap personel meliputi, namun tidak terbatas pada hal berikut:

- Apakah individu yang diselidiki ada di lokasi? Jika ada, apakah mereka memiliki kecenderungan terhadap kekerasan?
- Pada jam berapa kegiatan operasional akan dilakukan?
- Dapatkah tempat kejadian perkara diisolasi dari kerumunan orang?
- Apakah terdapat senjata di daerah tersebut?
- Apakah terdapat bahaya fisik pada individu saat ini?
- Apakah terdapat sesuatu disekitar, termasuk perangkat, yang telah dikonfigurasi yang dapat menimbulkan kerusakan fisik jika ditangani dengan cara yang tidak tepat, misalnya perangkap tersembunyi?
- Apakah bahan yang akan dikoleksi memiliki kemungkinan dapat menyebabkan kerusakan atau gangguan psikologis?
- Apakah tempat kejadian perkara dianggap tidak aman?
- Apakah daerah sekitarnya berdampak potensi risiko?

Bukti digital potensial

Penilaian risiko melibatkan evaluasi risiko yang sistematis dan potensi dampak yang mungkin dimiliki pada investigasi bukti digital.

Aspek yang perlu dipertimbangkan saat penilaian risiko untuk bukti digital potensial meliputi, namun tidak terbatas pada hal berikut:

- Jenis metode koleksi / akuisisi apa yang akan diterapkan?
- Peralatan apa yang mungkin diperlukan di lokasi?
- Bagaimana tingkat volatil dari data dan informasi yang berkaitan dengan bukti digital potensial?
- Apakah akses jarak jauh ke perangkat digital dimungkinkan dan apakah hal tersebut menimbulkan ancaman pada integritas bukti?
- Apa yang terjadi jika data / peralatan rusak?
- Apakah data telah diubah?
- Mungkinkah perangkat digital telah dikonfigurasi untuk menghancurkan (misalnya menggunakan sebuah bom-logis), merusak atau mengaburkan data jika dimatikan atau diakses dengan cara yang tidak terkendali?

Peran dan tanggung jawab

Peran DEFR meliputi identifikasi, koleksi, akuisisi dan preservasi bukti digital potensial di tempat kejadian perkara.

Di dalamnya termasuk pembuatan laporan koleksi dan akuisisi, namun tidak perlu berbentuk laporan analisis.

Peran DEFR juga memastikan integritas dan keaslian bukti digital potensial.

Dalam memenuhi perannya, DEFR harus memiliki pengalaman, keterampilan dan pengetahuan yang memadai dalam menangani bukti digital potensial.

Hal ini sangat penting karena bukti digital potensial dapat dengan mudah dirusak.

DEFR juga mungkin memerlukan bantuan dari personel dukungan teknis di bidang terkait.

Peran dari DES termasuk memberikan dukungan teknis kepada DEFR dalam mengidentifikasi, mengoleksi, mengakuisisi dan mempreservasi bukti digital potensial di tempat kejadian perkara.

DES memberikan bantuan keahlian khusus untuk DEFR.

Matriks kompetensi untuk DEFR (lihat Lampiran A) berfungsi sebagai panduan untuk mengidentifikasi tingkat kompetensi DEFR yang relevan.

Lampiran A (informatif)

Deskripsi kemampuan dan kompetensi inti DEFR

Table A.1 – Contoh deskripsi kompetensi

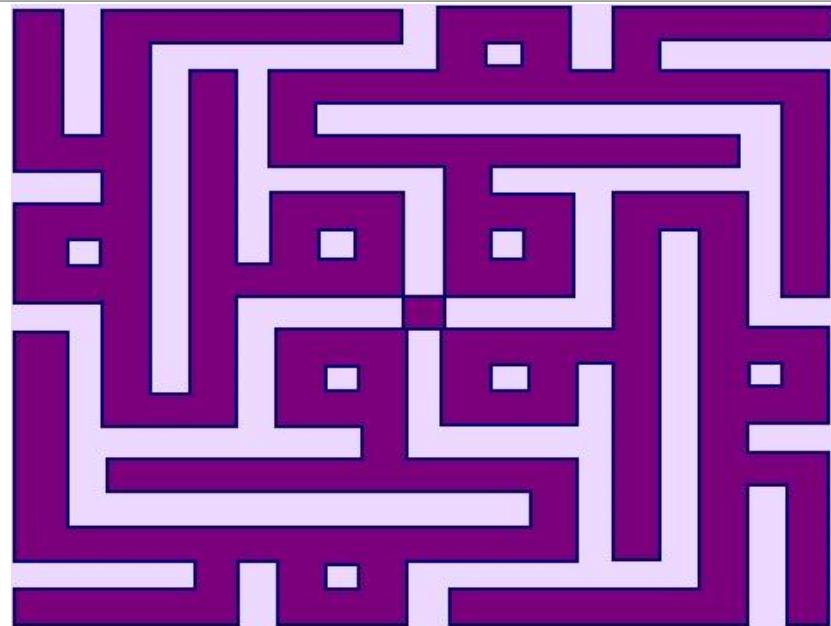
| No | Kemampuan Inti | Deskripsi kemampuan inti | Deskripsi Kompetensi | | |
|----|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | Mengetahui (1) | Memahami (2) | Menerapkan (3) |
| 1 | Identifikasi bukti digital | Merincikan perangkat digital, komponen-komponen, informasi yang dapat membantu investigasi dan hukum terkait untuk penanganan bukti digital potensial dan kejahatan yang berhubungan dengan komputer. Mengidentifikasi persyaratan alat untuk koleksi, akuisisi data dan perangkat serta penilaian risiko | Penggunaan TI secara umum dan pengadministrasian dalam beragam jenis perangkat TI dan perangkat jaringan; prosedur investigasi di tempat kejadian perkara; penentuan kondisi perangkat; nilai dari informasi yang memiliki kekuatan pembuktian; perangkat dan informasi berkaitan dengan forensik jaringan | Konfigurasi log dan konfigurasi sistem/aplikasi; identifikasi log sistem dan aplikasi meliputi log email, log web, log akses, file kata kunci, file konfigurasi sistem, informasi IP komputer host; fungsionalitas dan keterkaitan perangkat; dampak dari bukti volatil dan non-volatile | Analisis khusus; penginterpretasian log untuk deteksi intrusi dalam mengidentifikasi sistem lainnya yang terkena dampak; pengidentifikasi kata kunci yang dibutuhkan untuk masing-masing perangkat sebelum koleksi; pengidentifikasi diagram jaringan dan mekanisme kontrol akses untuk memahami keterkaitan; pengidentifikasi keterkaitan antara alamat IP dan alamat MAC untuk konfirmasi perangkat |
| 2 | Koleksi perangkat digital | Mengetahui peralatan yang dibutuhkan dalam pembungkusan bukti digital dan implementasinya, mampu melindungi bukti digital dari ancaman lingkungan, serta menjamin keutuhan informasi | Pengkoleksian data secara umum dengan mempertimbangkan aspek keselamatan; prinsip dan perancangan peralatan dasar; penentuan metode terbaik dalam pengumpulan untuk mempreservasi informasi semaksimal mungkin yang berkaitan dengan keladian perkara | Perumusan dan pelaksanaan proses koleksi; pengumpulan bukti; penulisan dokumen bukti; rantai pengawasan bukti; pengendalian kualitas dari proses koleksi bukti; cara wawancara tersangka | Optimasi proses koleksi; pendokumentasian bukti yang tidak dapat diakuisisi karena berbagai kendala; pengumpulan kata kunci, kunci, dongle, dan informasi lain yang dibutuhkan untuk melakukan analisis di laboratorium |

| | | | | | |
|---|------------------------|---------------------------------------------------------|--------------------------------------------------|--------------------------------------------|------------------------------------------------------------|
| 3 | Akuisisi bukti digital | Menerapkan persyaratan akuisisi bukti digital potensial | Informasi yang tersedia dalam perangkat digital, | Persyaratan media penyimpanan; pelaksanaan | Akuisisi pada media penyimpanan digital meliputi dan tidak |
|---|------------------------|---------------------------------------------------------|--------------------------------------------------|--------------------------------------------|------------------------------------------------------------|

| | | | | | |
|---|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | secara logis, memastikan proses dapat diulang, dapat diaudit, dapat diproduksi kembali, dan dapat dipertahankan. Lingkup area meliputi akuisisi pada sistem dalam keadaan menyala, akuisisi sistem dalam keadaan mati, dan jaringan | database, dokumen yang dihasilkan sistem, data yang dihasilkan pengguna, dan data volatil; struktur file sistem UNIX dan Windows serta perangkatnya; dampak dari data volatil | prosedur akuisisi penyalinan <i>per bit (imaging)</i> (seperti akuisisi media penyimpanan utuh dan parsial); prosedur akuisisi pada sistem dalam keadaan menyala; prosedur akuisisi pada sistem dalam keadaan mati; pembuatan nilai <i>hash</i> | terbatas pada RAID, database, perangkat, dan perangkat miniatur; pemahaman keterkaitan dan dampak dari metode akuisisi yang berbeda-beda |
| 4 | Preservasi bukti digital | Menerapkan dan menilai persyaratan untuk preservasi bukti digital potensial, memahami faktor-faktor dan parameter yang mempengaruhi akurasinya. Lingkup area meliputi metodologi, pengelolaan ratal pengawasan, penanganan perangkat komputer dan penanganan media penyimpanan digital | Persyaratan dan prosedur pengelolaan ratal pengawasan sebagai persyaratan hukum; dampak lingkungan seperti kelembapan, temperatur dan guncangan atas perangkat digital; pilihan pembungkusan, transportasi, dan persyaratan penyimpanan | Cara pembuatan dokumen audit bukti; penentuan parameter dokumen audit bukti; jaminan keamanan informasi, ancaman, kerapuhan dan pengendalian untuk bukti digital | Tindakan pengamanan bukti digital, dalam pengubahan perangkat besar menjadi perangkat miniatur genggam; prosedur untuk mendokumentasikan rincian bukti |



Terima Kasih



Respons Awal dan Tugas Responden Pertama

ERI PRASETYO WIBOWO
UNIVERSITAS GUNADARMA

Apa yang harus Anda lakukan setelah tiba di TKP?

- Entitas (badan publik atau) laboratorium swasta yang bertanggung jawab untuk melakukan penyelidikan akan mengirim satu atau lebih individu untuk menyelidiki kasus tersebut; orang ini disebut "penanggap pertama," dan dia bertanggung jawab untuk melakukan investigasi awal insiden untuk menentukan akar masalah.
- Responden pertama dapat berasal dari latar belakang yang berbeda: dia mungkin seorang administrator jaringan, administrator sistem, petugas penegak hukum.
- Peran utama responden pertama adalah mengidentifikasi, mengumpulkan, melestarikan, dan mengangkut bukti digital ke laboratorium forensik selain mengidentifikasi akar penyebab suatu kejadian. Untuk melakukan ini dengan benar dan sah, responden pertama harus sepenuhnya menyadari: undang-undang yang relevan dalam yurisdiksi di mana dia akan menyelidiki insiden tersebut.
- Dari perspektif teknis, responden pertama harus memiliki pemahaman yang menyeluruh pemahaman tentang prosedur forensik digital; dia harus tahu bagaimana memperolehnya bukti digital dengan cara yang sehat secara forensik, sehingga bukti yang diperoleh dapat digunakan dalam pengadilan. Responden pertama harus memiliki pengetahuan TI yang sesuai yang mencakup berbagai domain komputasi, dan dia juga harus memahami cara menangani TI yang berbeda peralatan, sehingga dia bisa tahu di mana mencari bukti digital.

Apa yang harus Anda lakukan setelah tiba di TKP?

- Sebelum responden pertama tiba di TKP, dia perlu mengidentifikasi identitas mereka , ruang lingkup kerja dengan jelas untuk menghindari kehilangan detail apa pun yang terkait dengan kasus subjek.
- Pertama toolkit responden harus siap untuk dibawa bersamanya atas permintaan: toolkit ini seperti yang akan kita lihat nanti—harus berisi perangkat lunak dan perangkat keras yang sesuai untuk mengelola berbagai skenario yang akan dihadapi responden pertama. Misalnya, digital TKP bisa sangat rumit karena dapat berisi berbagai jenis komputasi perangkat dengan OS, server, dan perangkat jaringan yang berbeda, dan juga dapat menjangkau berbagai wilayah geografis, bahkan ke server penyimpanan cloud yang terletak di yurisdiksi lain.
- Hal pertama yang perlu dipertimbangkan oleh responden pertama adalah bagaimana memahami dengan tepat apa diperlukan darinya sehubungan dengan insiden yang dilaporkan. Responden pertama mengajukan beberapa pertanyaan kepada pelapor/perusahaan untuk menentukan ruang lingkup pekerjaan.
- Pertanyaan-pertanyaan utama mencakup hal-hal berikut: Apakah badan pelapor perlu menyelidiki kasus ini secara resmi sehingga mereka dapat memindahkannya ke pengadilan nanti? Atau apakah mereka hanya ingin mengkonfirmasi bahwa serangan dilakukan terhadap sistem komputerisasi mereka dan memastikan tidak ada lagi kerusakan dapat terjadi? Dalam banyak kasus, tugas yang diperlukan dari responden pertama adalah untuk selidiki akar penyebab dan jenis serangan dan kemudian bekerja untuk mengembalikan sistem agar berfungsi secepat mungkin untuk menghindari gangguan bisnis.

Pencarian dan Penyitaan

- Aparat penegak hukum membutuhkan surat perintah penggeledahan untuk menggeledah dan menyita perangkat digital.
- Prinsip ini juga berlaku untuk kejahatan digital; karenanya, perangkat komputasi apa pun yang mampu menyimpan data pengguna dianggap milik pribadi yang membutuhkan surat perintah penggeledahan untuk digeledah dan disita oleh aparat penegak hukum.
- Kami tidak akan menyelidiki secara mendalam bidang hukum; Namun, perlu diingat bahwa sebelumnya mengumpulkan bukti digital apa pun, Anda memerlukan bentuk persetujuan hukum untuk mencari atau menyita bukti yang bersangkutan.
- Di bagian ini, kami akan membuat daftar pilihan yang tersedia untuk forensik digital pemeriksa untuk mencari dan menyita barang bukti digital.

Persetujuan untuk Pencarian

- Dalam tipe ini, pemilik perangkat komputasi bekerja sama dengan penyelidik dan mengizinkan mereka untuk mencari dan memperoleh bukti digital tanpa surat perintah penggeledahan resmi.
- Ini biasanya terjadi ketika pemilik perangkat bukan tersangka.
- Sebelumnya telah menandatangani formulir penggeledahan dan penyitaan sebagai syarat untuk bekerja.
- Di dalam kasus, Anda dapat memperoleh bukti digital tanpa meminta persetujuan apa pun darinya.

CONSENT TO SEARCH MOBILE DEVICE/ COMPUTER EQUIPMENT / ELECTRONIC DATA

I, _____, hereby authorize _____, who has identified him/herself as a law enforcement official, and any other person(s), including but not limited to a computer forensic examiner he/she may designate to assist him/her, to remove, take possession of and copy (image) and/or conduct a complete search of the following computer systems, electronic data storage devices, computer data storage diskettes or CD-ROMs, or any other electronic equipment capable of storing, retrieving and/or accessing data or necessary to assist in the accessing of said electronic data pertinent to their investigation, belonging to me. I understand that a complete search may include the recovery of deleted files, and the bypassing or cracking of passwords or encryption. This specific consent applies to the following items:

I further authorize the law enforcement officer(s) / official(s) to copy and keep any documents, images, or data found on the computer equipment described above that are determined by the officer to be pertinent to the criminal investigation.

I give specific consent for the aforementioned official to have possession of said equipment for:

a period of _____ business days
 an unlimited number of days
to make forensic copy (image).

I further give specific consent for a forensic analysis of the copy (image) of the aforementioned equipment for:

a period of _____ business days.
 an unlimited number of days

I give my specific consent freely and voluntarily without fear, threat, coercion or promises of any kind. I understand and acknowledge that I have an absolute right to refuse to give my consent and I hereby voluntarily waive this right.

I am also aware that if I wish to withdraw my consent at any time during the seizure and / or search of the equipment / data, it will be respected.

This specific consent is given by me this _____ day of _____, 20_____, at _____ am/pm.

Printed name: _____

Signature: _____

Address: _____

Witness name: _____
(LEO) Signature: _____

Agency/Address: _____

Phone: _____

Panggilan

- Ketika Anda tidak memiliki izin dari pemilik perangkat untuk mencari dan mengambil peralatan digital yang terkait dengan kasus yang dihadapi, Anda dapat meminta untuk memiliki perintah pengadilan atau izin.
- Perhatian khusus harus diberikan ketika meminta izin tersebut, seperti yang akan dilakukan tersangka cukup waktu untuk menghancurkan bukti digital karena dia akan mengetahui terlebih dahulu permintaan Anda untuk mendapatkan izin pengadilan untuk mencari/merampas perangkat digital yang dincar.
- Panggilan pengadilan biasanya digunakan ketika tidak mungkin memberi tahu pemilik perangkat mengakibatkan pemusnahan barang bukti digital. Misalnya, banyak organisasi (misalnya, bank) memerlukan izin dari pengadilan sebelum memberikan informasi kepada penyidik.
- Ini tidak berarti bahwa organisasi tersebut menolak untuk bekerja sama dengan penyidik; sebaliknya, kebijakan yang diterapkan dan peraturan internal mereka mencegah mereka dari serah terima informasi tersebut tanpa perintah pengadilan yang tepat.

Surat izin menggeledah

- Ini adalah prosedur pencarian dan penyitaan yang paling ampuh; penyelidik menggunakan ini Ketika ada kemungkinan besar bahwa menginformasikan subjek (misalnya, ketika dia adalah pemiliknya) perangkat digital atau terlibat dengan tersangka) akan mengakibatkan penghancuran perangkat digital bukti.
- Surat perintah penggeledahan akan dieksekusi tanpa pemberitahuan sebelumnya kepada tersangka, jadi dia tidak dapat melakukan apa pun untuk menghancurkan atau menyembunyikan bukti digital.
- Ingatlah bahwa surat perintah penggeledahan hanya tersedia untuk petugas penegak hukum; jika Anda adalah penyelidik forensik digital independen, Anda tidak dapat meminta izin ini dari pengadilan.
- Pengadilan biasanya tidak memberikan surat perintah penggeledahan dengan mudah; penyidik harus memiliki petunjuk yang masuk akal bahwa orang tertentu dan perangkat komputasi tertentu yang terkait dengannya adalah bagian dari kegiatan kriminal untuk dikeluarkan surat perintah tersebut.

Perangkat Penanggap Pertama

- Setelah mendapatkan persetujuan/surat perintah penggeledahan, responden pertama akan menuju ke tempat kejadian perkara; disarankan bagi responden pertama untuk mengetahui sebanyak mungkin tentang insiden tersebut dan TKP sedapat mungkin sebelumnya; ini akan memungkinkan dia untuk mempersiapkan peralatan yang dibutuhkan dan perangkat lunak sebelum tiba di TKP.
- Secara umum, barang-barang berikut harus ada di tas responden pertama sebelum menyelidiki setiap TKP yang melibatkan bukti elektronik:
 1. Rekaman TKP. , 2. Label tempel dan dasi.
 3. Spidol warna. 4. Buku Catatan.
 5. Sarung Tangan. 6. Kaca pembesar. 7. Senter.
 8. Kantong yang dapat ditutup dengan ukuran campuran; harus tas antistatik untuk melestarikan integritas bukti.
 9. Kamera (dapat menangkap video dan gambar dan harus dikonfigurasi untuk menunjukkan tanggal/waktu ketika penangkapan terjadi).
 10. Bahan pelindung frekuensi radio untuk mencegah beberapa jenis perangkat yang disita (mis., ponsel cerdas dan tablet dengan kartu SIM) dari menerima panggilan atau pesan (juga dikenal sebagai Faraday tas pelindung). Tas ini juga akan melindungi barang bukti dari sambaran petir dan pelepasan muatan listrik statis.
 11. Formulir lacak balak.
 12. Amankan hard drive eksternal yang bersih untuk menyimpan gambar digital apa pun pameran.
 13. USB thumb drive (minimal dua). 14. Hub USB.

Perangkat Penanggap Pertama

- Secara umum, barang-barang berikut harus ada di tas responden pertama sebelum menyelidiki setiap TKP yang melibatkan bukti elektronik:
15. CD yang dapat di-boot.
 16. Kabel jaringan.
 17. Kabel/konektor yang berbeda untuk komputer.
 18. Pemblokir tulis perangkat keras.
 19. Alat penangkap RAM. Dll.
 20. Alat penangkap hard drive.
 21. Perangkat lunak forensik untuk melakukan analisis dasar pada mengambil data jika diperlukan.
 22. Adaptor daya dengan ukuran berbeda.
 23. Strip daya multi-proteksi.
 24. Obeng khusus.
 25. Tang standar.
 26. Pemotong kawat.
 27. Satu laptop, selain workstation forensik portabel.
 28. Solusi VPN untuk melindungi komunikasi yang pertama responden.
 29. Akses ke repositori online yang aman di mana lebih banyak alat forensik berada disimpan jika diperlukan di TKP.
 30. Bahan kemasan.

Tugas Responden Pertama

Langkah-langkah berikut harus dilaksanakan dalam urutan yang benar, mempertimbangkan keadaan di TKP:

1. Saat tiba, jika ada kamera pengintai, pastikan untuk putuskan sambungan sebelum melakukan apa pun; Anda juga dapat menutupinya jika Anda tidak bisa menghentikannya secara instan.
2. Terkadang, komputer mungkin menghancurkan bukti (mis., menjalankan perangkat lunak khusus untuk menghapus hard drive bersih dan akibatnya menghancurkan bukti digital). Jika Anda mencurigai sesuatu seperti yang terjadi (misalnya, jika lampu LED hard drive menyala terus-menerus dan kipas bergerak cepat, maka ada kemungkinan bahwa operasi baca/tulis sedang dilakukan pada drive), segera matikan komputer. Lakukan ini dengan menarik kabel daya (jika komputer yang dicurigai adalah laptop dengan baterai yang tidak dapat dilepaskan dan tahan tombol daya sampai laptop dimatikan. Jika laptop memiliki baterai yang dapat dilepas, cabut batere dulu, baru cabut kabel powernya).
3. Jika komputer OFF, jangan ON kan. Masukkan di antistatic tas dan mengangkutnya dengan aman ke laboratorium forensik.

Tugas Responden Pertama

Langkah-langkah berikut harus dilaksanakan dalam urutan yang benar, mempertimbangkan keadaan di TKP:

4. Jika komputer ON dan tidak ada petunjuk kerusakan program bekerja, lakukan hal berikut:
 - A. Jika layar komputer menunjukkan jendela masuk (kata sandi prompt), matikan perangkat dengan melepas kabel daya dari dinding (lakukan hard shutdown); Anda juga dapat mencoba memecahkan kata sandi perangkat jika perlu untuk mendapatkan volatile memori (lebih lanjut tentang ini di bab berikutnya).
 - B. Jika layar komputer gelap atau menampilkan screen saver, pindahkan mouse perlahan, tanpa menekan tombol apa pun atau memutar roda mouse, untuk menampilkan layar.
 - C. Memotret layar komputer untuk menampilkan program yang sedang berjalan dan membuka file/folder, dan untuk merekam tanggal/waktu sistem.
 - D. Memperoleh memori volatil (RAM) menggunakan alat khusus, seperti yang akan kita lihat di bab berikutnya (memperoleh RAM memori juga dikenal sebagai dump memori langsung). Menangkap RAM memori adalah langkah kunci sebelum mematikan mesin karena dapat berisi banyak informasi seperti kunci kriptografi, Log obrolan IM, konten tidak terenkripsi, konten papan klip, dan memproses informasi, antara lain.
 - E. Jika komputer terhubung ke perangkat jaringan (router atau beralih), coba dapatkan informasi jaringannya terlebih dahulu (Alamat IP, sesi terbuka, port terbuka, tabel perutean, IP LAN, alamat broadcast, dan kartu antarmuka nomor jaringan).

Tugas Responden Pertama

Langkah-langkah berikut harus dilaksanakan dalam urutan yang benar, mempertimbangkan keadaan di TKP:

4. Jika komputer ON dan tidak ada petunjuk kerusakan program bekerja, lakukan hal berikut:
 - F. Lakukan pemutusan paksa (cabut kabel daya dari stopkontak). Jika perangkat adalah laptop, lepaskan baterai terlebih dahulu dan kemudian cabut kabel daya. Jika Anda tidak dapat menghapus baterai laptop, tekan dan tahan tombol daya selama 20 detik untuk mematikannya.
 - G. Terakhir, dokumentasikan semua langkah yang diambil untuk menangkap tersangka perangkat komputer sehingga tersedia jika seseorang memintanya nanti.
5. Saat mengambil perangkat portabel dengan komunikasi nirkabel kemampuan, pastikan untuk memasukkannya ke dalam kantong kedap air yang dapat memblokir komunikasi nirkabel ke perangkat.

REMEMBER!

- Seperti yang telah kami sebutkan, surat perintah penggeledahan resmi atau persetujuan dari pemiliknya perangkat digital harus tersedia sebelum penggeledahan/penyitaan tersangka perangkat komputasi.
- Disarankan untuk memiliki pemeriksa forensik komputer yang terlatih untuk memperoleh bukti data digital dari perangkat yang dicurigai untuk menghindari meninggalkan—atau bahkan menghancurkan apa pun jejak tanpa penyelidikan.
- Foto seluruh TKP sebelum mencari dan menyita digital apapun perangkat.
- Keamanan adalah pertimbangan utama saat menyelidiki TKP: keamanan tim responden pertama dan petugas penegak hukum dan semua orang di kejadian adegan harus menjadi prioritas utama.

CARA MENONAKTIFKAN PERANGKAT KOMPUTER SUSPECT SAAT ON

Saat perangkat komputasi yang dicurigai AKTIF, Anda harus mematikannya sebelum memindahkannya ke laboratorium forensik.

Dari perspektif forensik digital, ada dua metode untuk mematikan perangkat dengan berbagai konsekuensi dan efek pada perangkat komputasi target.

Pilih salah satu yang paling sesuai dengan kebutuhan Anda, dengan mempertimbangkan pertimbangan berikut.

1. Hard shutdown (lepaskan baterai/kabel listrik): Ini akan menjaga system file, mencegah menghapus program agar tidak aktif saat dimatikan, dan mencegah perubahan pada stempel waktu file dan atribut lainnya. Namun, metode ini akan hapus file terbuka yang belum disimpan dan dapat merusak file sistem dan file terbuka pengguna dokumen.
2. Shutdown yang anggun (mematikan komputer menggunakan pilihan biasa cara): Keuntungan dari metode ini termasuk menemukan file yang terbuka dan program setelah dimatikan dan mencegah kerusakan pada file sistem di selain memungkinkan aplikasi yang berjalan untuk menulis artefak apa pun ke hard drive, jadi kita bisa memulihkannya nanti.

Kerugiannya meliputi: meluncurkan destruktif program yang dikonfigurasi untuk dijalankan saat shutdown, menimpa data pada hard drive, mengaktifkan skrip buatan pengguna yang dapat melakukan berbagai tugas seperti menghapus log sistem, membersihkan file halaman sistem (jika komputer dikonfigurasi untuk melakukannya saat shutdown normal), dan mengubah beberapa atribut file

Catatan penting lainnya untuk dipertimbangkan ketika menyelidiki TKP:

- Identifikasi petunjuk apa pun yang dapat mencerminkan pengetahuan komputasi yang mencurigakan, teknologi misalnya, jika tersangka memiliki buku tentang "digital" steganografi" di rak bukunya, Anda harus curiga bahwa ini tersangka dapat menggunakan teknik tersebut untuk menyembunyikan data yang memberatkan.
- Memotret area di sekitar komputer tersangka untuk menunjukkan semua perangkat yang terhubung (mis., USB thumb drive, printer, pemindai, kamera USB, dan mikrofon). Harus cari catatan tulisan tangan di sekitar komputer atau tempel di layarnya; beberapa orang menyimpan kata sandi mereka di catatan semacam itu, dan menemukan kata sandi dengan cara ini dapat menghemat banyak waktu jika tersangka menggunakan enkripsi untuk melindungi datanya. Ingatlah bahwa catatan tulisan tangan relatif terhadap investigasi harus didokumentasikan dengan cara yang mirip dengan bukti digital lainnya.
- Bukti fisik tidak boleh dikompromikan selama di tempat kejadian (misalnya, gunakan sarung tangan saat menyentuh perangkat komputasi untuk menghindari penghancuran sidik jari yang ada). Responden pertama harus mencitrakan perangkat penyimpanan (memperoleh gambar forensik digital) sebelum mengirimkannya ke laboratorium forensik untuk DNA dan pemeriksaan sidik jari.
- Jika TKP berisi peralatan IT canggih yang melebihi keahlian responden pertama, dia harus meminta saran/bantuan dari penyidik dengan keahlian yang lebih handal.
- Jangan memindahkan perangkat elektronik dalam keadaan ON; ini dapat merusak/ bukti digital yang korup di dalamnya

Urutan Volatilitas

- Urutan berikut disarankan oleh banyak proses forensik digital, dimulai dengan yang paling fluktuatif:
 1. CPU, register, dan cache sistem.
 2. Tabel perutean, cache ARP, tabel proses, statistik kernel.
 3. Memori RAM.
 4. Sistem file sementara.
 5. Memori virtual (bernama "pagefile" di OS Windows). Ini adalah file di hard drive yang menambah jumlah RAM tersedia untuk komputer.
 6. Hard drive dan/atau penyimpanan media yang dapat dipindahkan lainnya.
 7. Data logging dan pemantauan jarak jauh.
 8. Konfigurasi fisik, topologi jaringan.
 9. Backup data dan hasil cetakan.

Mendokumentasikan TKP Digital

Poin-poin penting berikut harus didokumentasikan dengan jelas:

1. Ketika Anda memasuki TKP, berapa lama Anda tinggal di sana, dan dengan siapa.
2. Sebutkan semua orang yang mengakses TKP dan daftar masing-masing peran seseorang. Misalnya, siapa yang mengambil foto TKP? Siapa yang menyita perangkat komputasi? Buktinya jam berapa? diperoleh? Apakah Anda menangkap memori yang mudah menguap (jika komputasi perangkat AKTIF), dan jika ya, dengan metode/alat apa?
3. Responden pertama juga harus mendokumentasikan semua item yang terkait dengan kasus di tangan yang telah ditemukan di dan diperoleh dari tempat kejadian perkara; setiap item yang diperoleh harus didokumentasikan secara lengkap dalam bentuk lacak balak
4. Buat sketsa TKP yang menunjukkan di mana digital perangkat di tempatkan di samping periferal yang terpasang; NS sketsa juga dapat menyertakan detail lain seperti jenis perangkat komputasi dan nomor model.
5. Memotret semua area TKP; Anda juga dapat menggunakan video untuk tujuan ini. Pemotretan harus dilakukan dua kali, satu kali memasuki tempat kejadian dan yang kedua sebelum pergi (setelah merebut perangkat digital[s]).
6. Tulis catatan yang menjelaskan segala sesuatu yang berhubungan dengan kasus yang dihadapi rinci; catatan ini akan membantu Anda mengingat apa yang telah Anda lihat di TKP saat bersaksi di pengadilan nanti.
7. Jika undang-undang melarang responden pertama mencari dan menyita beberapa perangkat digital, dia harus menyebutkan ini di dokumentasi TKP.

Pengemasan dan Pengangkutan Perangkat Elektronik

- Setelah Anda selesai mendokumentasikan TKP dan Anda mematikan perangkat digital (jika ON), Anda siap mengemas dan mengangkutnya ke lab.
- Mulailah dengan mencabut kabel, tetapi sebelum melakukan ini, pastikan untuk memasang tag yang berisi nomor pada setiap kabel dan pada port yang sesuai pada komputer. Terakhir, fotolah kabel-kabel tersebut sebelum mencabutnya agar nanti tahu di mana masing-masing kabel telah terpasang. Ini akan membantu penyelidik untuk merekonstruksi sistem lagi di lab jika diperlukan.
- Mulailah proses pengemasan dengan menempelkan selotip di atas saklar daya, sehingga perangkat tidak akan menyala secara tidak sengaja saat dalam perjalanan, dan kemudian masukkan perangkat digital kedalam tas antistatis. Terakhir, masukkan perangkat yang diperoleh ke dalam kantong bukti yang sesuai, segel menggunakan pita, dan catat nama dan tanggal/waktu saat di sana.
- Tas bukti harus berisi panel yang berisi rincian berikut tentang isinya:
 1. Isi tas.
 2. Nama-nama penyidik yang:
 - A. Disita barang buktinya.
 - B. Bukti foto dan TKP.
 - C. Membuat diagram sketsa TKP.
 - D. Mengemas barang bukti di dalam tas.
 3. Lokasi dimana barang bukti ditemukan dan disita.
 4. Informasi tersangka dan catatan kriminal jika ada.
 5. Tanggal dan waktu penyitaan.
 6. Kata sandi perangkat yang disita (jika tersedia).
 7. Catatan tambahan.

Melakukan Wawancara

- Setelah menerima telepon dari pelapor/perusahaan tentang subjek insiden, responden pertama harus mengajukan pertanyaan untuk mengklarifikasi kasus yang akan diselidikinya.
- Di bagian ini, kami akan mengajukan pertanyaan paling umum yang harus ditanyakan oleh responden pertama sebelum tiba di TKP dan setelah tiba dan berbicara dengan saksi (misalnya, penjaga dan administrator situs) dan kemungkinan tersangka. Pertanyaan Responden Pertama Saat Dihubungi oleh Klien Ketika klien menghubungi responden pertama untuk menyelidiki insiden,

klien harus mengajukan pertanyaan awal berikut oleh responden pertama:

1. Apa masalahnya?
2. Jika klien adalah perusahaan, siapa yang bertanggung jawab menangani insiden kejahatan digital di perusahaan target?
3. Di mana lokasi kejadian?
4. Di bawah yurisdiksi (otoritas) mana bukti akan digeledah dan disita?
5. Jenis perangkat komputasi apa yang akan disita di tempat kejadian perkara?
6. Tugas apa yang diharapkan dilakukan di tempat kejadian? Untuk misalnya, apakah kita perlu melakukan penangkapan/analisis memori langsung? Apakah ada perangkat jaringan yang terlibat dalam insiden tersebut? yang perlu digeledah dan/atau disita?
7. Jenis akses Internet apa yang dimiliki organisasi target?
8. Apa nama ISPnya?
9. Apakah ada penyimpanan di luar kantor?

Pertanyaan Wawancara Saksi

- Setelah tiba di TKP, responden pertama harus mengambil sebanyak informasi yang dia dapat dari orang-orang yang tersedia pada saat kejadian ditempat. Orang-orang yang berada di TKP harus ditanyai tentang :
 1. Apa yang mereka lihat, dan juga di mana dan bagaimana.
 2. Nama-nama semua orang yang berada di TKP, selain itu ke nomor telepon, alamat email, dan peran/pekerjaan mereka di organisasi sasaran.
 3. Nama pengguna dan kata sandi akun kerja mereka (aturan yurisdiksi terapkan di sini).
 4. Profil sosial dan nama layar obrolan IM untuk semua karyawan minat.
 5. Identitas administrator/manajer situs yang dapat mengidentifikasi perangkat dan penjaga di TKP.
 6. Jumlah, jenis, dan model perangkat yang terlibat dalam insiden.
 7. Jenis data digital (misalnya, email, database, gambar, dokumen, dll.) yang diduga terlibat dalam insiden tersebut.
 8. Jenis sistem operasi yang terlibat dalam insiden tersebut.
 9. Apakah ada data digital yang dimiliki oleh organisasi target? disimpan di luar tempat (misalnya, penyimpanan cloud, lokasi terpencil, dll.).
 10. Identitas kontraktor yang memiliki kemampuan akses jarak jauh untuk menargetkan jaringan organisasi.
 11. Apakah ada pembatasan akses data.
 12. Setiap kecurigaan tentang siapa yang mungkin melakukan serangan (misalnya, mantan karyawan yang tidak puas).

Tanda tangan saksi

- Terkadang tanda tangan saksi diperlukan untuk memverifikasi informasi yang dikumpulkan dari tempat kejadian perkara; prosedur ini tidak diterapkan di semua yurisdiksi, terutama jika orang tersebut mengumpulkan bukti digital adalah petugas penegak hukum.
- Namun, pertimbangkan poin ini pertimbangan jika berlaku.