UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Teknik Informatika

Mengumpulkan Bukti Digital Forensik Freezing the scene

Pengantar Komputer Forensik Teknologi Informasi

Pemodelan Forensik

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

Pemodelan Forensik

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

Pemodelan Forensik

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

Pemodelan Forensik

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

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 ayng sudah teruji dan ahli
- Memahami jaringan komputer, internet, komunikasi dan teknologi komputer dan informasi
- Dibutuhkan sampai 2 minggu pelatihan

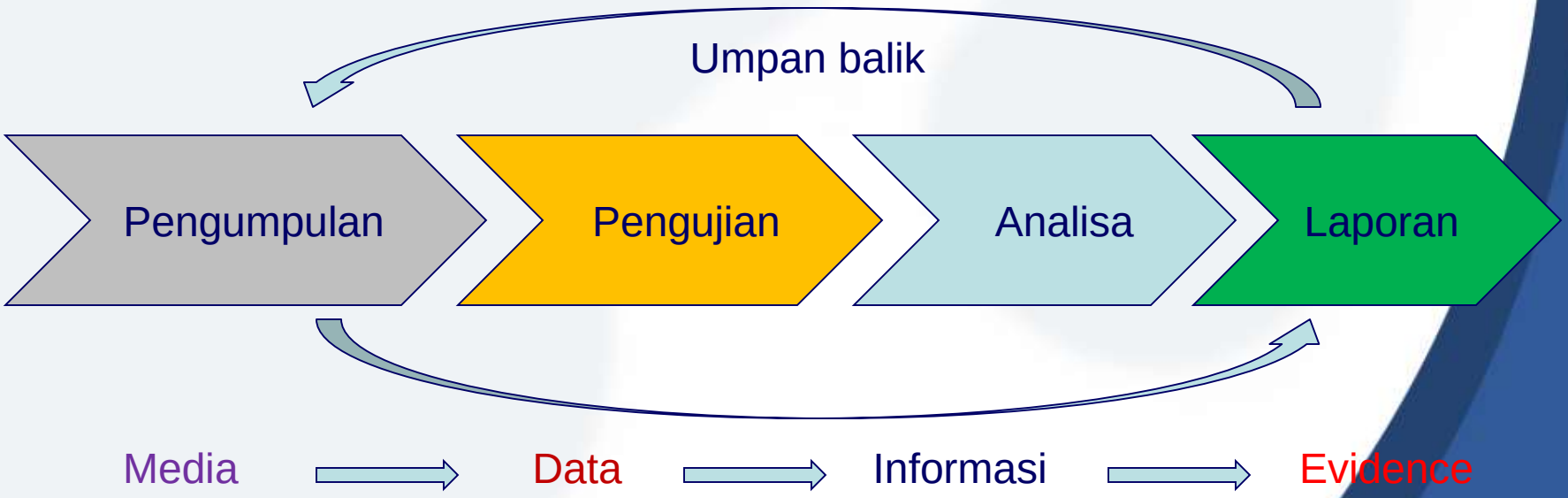
Digital evidence collection specialist

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

Tahap Komputer Forensik

- Pengumpulan
- Pengujian
- Analisa
- Laporan

Jangan lupa umpan balik



Pengumpulan Data

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

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

Bukti Digital (Digital Evidence)

- Informasi yang didapat dalam bentuk – format digital, seperti :
  - E-mail, alamat e-mail
  - Word processor – spreadsheet file
  - Source code dari perangkat lunak
  - Files berbentuk image
  - Web browser bookmark, cookies
  - Kalender, to do list

Manajemen Bukti

- The chain of custody
  - Pemeliharaan dengan meminimalisir kerusakan akibat karena investigasi
- Rules of evidence
  - Barang bukti harus memiliki hubungan yang relevan dengan kasus yang ada

The Chain Of Custody

- Tujuan :
  - Bukti itu benar – benar masih asli/orisinil
  - Pada saat persidangan ; bukti masih bisa dikatakan seperti pada saat ditemukan

- Untuk menjaga bukti dalam mekanisme the chain of custody :
  - Gunakan catatan yang lengkap keluar masuk bukti dari penyimpanan
  - Simpan di tempat yang aman
  - Akses yang terbatas dalam penyimpanan
  - Catat siapa saja yang dapat mengakses bukti tersebut

Rules Of Evidence

- Ada empat persyaratan
  - Dapat diterima (admissible)
  - Asli (authentic)
  - Lengkap (complete)
  - Dapat dipercaya (believable dan reliable)

Hal – Hal yang dapat digunakan sebagai bukti

- Audio recorder
- Mesin penjawab
- Kabel
- Peralatan caller ID
- Telpon selular
- Chips
- Mesin fotokopi
- Databank/digital organizer
- Camera digital
- Dongle
- Hardware protection devices – keys
- Drive duplicators
- External drives
- Fax machines
- Flash memory card
- Floppy
- CD Rom
- Perangkat GPS
- Pagers
- Palm pilot/Electronic organizer
- PCMCIA cards
- Printers
- Removable media
- Scanners
- Smart card/secure ID tokens
- Telpon, VCR
- Wireless access point

Auction Fraud - online

- Account data – online auction sites
- Accounting – bookkeeping software
- Buku alamat
- Kalender
- Chat log
- Customer information
- Basis data
- Digital camera software
- E-mail – surat - catatan
- Financial – asset record
- Image – files grafis
- Log aktivitas ber internet
- Internet bowser history
- Online financial institution access software
- Records – document of testimonials
- Catatan penggunaan telpon

Kejahatan komputer

- Buku alamat
- Configuration files
- Email – surat – catatan
- Program executable
- Log aktivitas ber – internet
- Internet protocol address an user name
- Internet relay chat (IRC) logs
- Source code
- File – file teks (user names an passwords)

Penipuan Keuangan (online – pemalsuan)

- Buku alamat
- Kalender
- Cek, mata uang dan money order images
- E-mail – surat – catatan
- Form transaksi keuangan palsu
- Identifikasi palsu
- Log aktivitas ber – internet
- Online financial institution access software
- Credit card skimmers
- Informasi konsumen
- Data kartu kredit
- Basis data

E-mail
(Ancaman - Mempermalukan – Mengganggu)

- Buku alamat
- Buku harian
- E-mail – surat – catatan
- Catatan keuangan dan perbendaharaan
- Image
- Log aktivitas ber – internet
- Dokumen – berks hukum
- Catatan penggunaan telpon
- Catatan latar belakang korban

Volatile Data Dalam RAM

Informasi yang diperoleh

- Menjalankan proses
- Eksekusi perintah konsol
- Password
- Data tidak terenkripsi
- Pesan cepat
- Alamat IP
- Trojan horse
- Siapa yang login ke sistem
- Open port dan listening application
- Daftar proses yang sedang berjalan
- Informasi registry
- Informasi sistem
- Attached devices

Mengumpulkan Data Volatile

- Mengumpulkan waktu, tanggal dan command history
- Ketika menjalankan perintah dan alat forensik akan menghasilkan waktu dan tanggal untuk jejak audit
- Dalam menjalankan perintah akan mendokumentasikan kegiatan dalam tools forensik
- Mengumpulkan semua tipe data volatile pada sistem dan jaringan
- Akhiri pengumpulan forensik dengan waktu , tanggal dan command history

Langkah Pengumpulan Data Volatile

- Mempertahankan log pada sistem yang sedang berjalan
- Foto layar pada sistem yang sedang berjalan
- Identifikasi sistem operasi yang sedang berjalan
- Catat waktu dan tanggal dan waktu secara aktual
- Dump RAM pada sistem terhadap media removable
- Periksa seluruh disk atau file terenkripsi pada sistem
- Kumpulkan data volatile lain dalam sistem operasi dan simpan yang berada pada media removable
- Tentukan determinant dari metode pembuktian
- Dokumentasikan semua tindakan ke dalam laporan secara lengkap

Tools Imaging Memory

- **Memory Imaging Techniques**
  - Crash Dumps
  - LiveKd Dumps
  - Hibernation Files
  - Firewire
  - Virtual Machine Imaging
- **Memory Imaging Tools**
  - Tribble PCI Card (research project)
  - CoPilot by Komoku
  - Forensic RAM Extraction Device (FRED) by BBN

Tools Imaging Memory - windows

- winen.exe (Guidance Software - included with Encase 6.11 and higher)
- Mdd (Memory DD) (ManTech)
- MANDIANT Memoryze
- Kntdd
- HBGary
- FTK Imager

Tools Data Recovery

- **Active Partition Recovery**
- **Advanced Email Extractor**
- **Afind**
- **AutoStart Viewer**
- **CacheView**
- **Digital Image Recovery**
- **Decode – Forensic Date/Time Decoder**
- **DriveLook**
- **FavURLView – Favourite Viewer**

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

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

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

10. Indikasi apakah komputer terintegrasi dengan jaringan atau tidak
11. Indikasikan apakah terdapat encryption atau password protection
12. Indikasikan skill komputer user yang komputernya diambil untuk komputer forensik
13. Secara umum hanya komputer dan media penyimpan untuk keperluan forensik

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

10. Indikasi apakah komputer terintegrasi dengan jaringan atau tidak
11. Indikasikan apakah terdapat encryption atau password protection
12. Indikasikan skill komputer user yang komputernya diambil untuk komputer forensik
13. Secara umum hanya komputer dan media penyimpan untuk keperluan forensik

Tip Bagi Pemula

- Investigasi sederhana
- Hubungi pihak yang berwenang
- Amankan lokasi
- Minimalisasi 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

Terima kasih