Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer

Computer Forensics : A Critical Process in Your Incident Respon Plan

Black Hat Conference USA 2001	
Speaker	Gregory S. Miles, Ph.D
Director	JAWZ Cyber Crime Unit
COO	Security Horiszon Inc
Information Technology : 14 Tahun	
Information Security : 10 Tahun	
E-mail	**gmiles@jawzinc.com**
	gmiles@securityhorizon.com
WEB	**www.jawzinc.com**
	www.securityhorizon.com

Incident Response

1. Mengatasi masalah
   - Cari tahu apa yang terjadi
   - Bagaimana hal itu terjadi
   - Siapa yang melakukannya
2. Buat catatan insiden untuk kemudian digunakan
3. Buat catatan untuk mengamati tren
4. Buat catatan untuk memperbaiki proses
5. Menghindari kebingungan

Element Incident Response

1. Preparation

   Tanpa persiapan yang memadai, sangatlah mungkin bahwa upaya menaggapi insiden tidak akan terorganisir dan akan ada kebingungan antara personil. Persiapan membatasi potensi kerusakan dengan memastikan tindakan respon yang dikenal dan terkoordinasi.

2. Identification

Proses menentukan ada atau tidaknya insiden yang telah terjadi dan sifat dari insiden. Identifikasi dapat terjadi melalui penggunaan peralatan intrusi otomatis jaringan atau melalui user atau SA. Indentifikasi adalah proses yang sangat sulit. Melihat gejala dari insiden yang seringkali sulit. Ada banyak kesalahan positif, namun melihat sebuah anomali harus mendorong pengamat untuk menyelidiki lebih lanjut.

Orang-orang yang bisa mengidentifikasi insiden :

- User seperti sitem saya lambat, surat saya yang hilang, file saya telah berubah.
- System support personnel seperti server terkunci, file yang hilang, menambahkan akun atau menghapus akun, hal-hal aneh yang terjadi, anomali dalam log.
- Intrusion Detection Systems dan Firewall seperti pelanggaran kebijakan ID otomatis.

Kemungkinan Klasifikasi insiden :

- Unauthorized Privileged (root) Access : memperoleh akses ke sistem dan penggunaan hak akses root tanpa otorisasi.
- Unauthorized Limited (user) Access : memperoleh akses ke sistem dan penggunaan hak pengguna tanpa otorisasi.
- Unauthorized Unsuccessful Attempted Access : berulang upaya untuk mendapatkan akses sebagai root atau pengguna pada host, layanan atau sistem yang sama dengan sejumlah koneksi dari sumber yang sama.
- Unauthorized Probe : usaha untuk mengumpulkan informasi tentang sistem atau pengguna online dengan memindai situs dan mengakses port melalui kerentanan sistem operasi.
- Poor Security Practices : bad password, direct privileged login dan lain-lain yang dikumpulkan dari sistem monitor jaringan.
- Denial of Service (DOS) Attack : setiap tindakan yang menurunkan kinerja dari sistem atau jaringan yang mempengaruhi misi, bisnis atau fungsi dari suatu organisasi.
- Malicious Logic : Self-replicating software yang bersifat sebagai virus, disebarluaskan dengan melampirkan atau meniru kewenangan sistem file komputer atau bertindak sebagai kuda trojan, worm, skrip yang berbahaya atau bom logika.
- Hardware/Software Failure : Non-malicious failure dari Hardware atau aset Software.

- Infrastructure Failure : Non-malicious failure yang mendukung infrastruktur untuk menyertakan kegagalan daya, bencana alam, evakuasi secara paksa dan kegagalan penyediaan layanan untuk menyampaikan layanan.
- Unauthorized Utilization of Services : ini dapat mencakup bermain game, menyampaikan surat tanpa persetujuan, menciptakan akses dial-up, menggunakan peralatan organisasi untuk keuntungan pribadi dan server pribadi didalam jaringan.

3. Containment

   Proses untuk membatasi lingkup dan besarnya insiden.

   Contoh :

   - insiden yang melibatkan penggunaan malicious-code dan karena insiden malicious-code bisa menyebar dengan cepat, kerusakan besar mungkin akan terjadi.
   - Tidak jarang ditemukan workstation yang terhubung ke LAN yang terinfeksi ketika ada wabah virus.

     # Internet worm dari tahun 1988 menyerang 6.000 komputer di Amerika Serikat dalam satu hari.

     # Lovebug terkena virus lebih dari 10 juta komputer dengan kerusakan yang diperkirakan berkisar antara $2.5B-$10B US.

4. Eradication

   Proses menghilangkan penyebab dari insiden. Misalnya untuk jaringan mungkin melibatkan alamat IP yang di blok atau di filter pada router/firewall.

5. Recovery

   Proses pemulihan sebuah sistem untuk status operasi yang normal.

6. Follow-up

   Membantu untuk meningkatkan prosedur penanganan insiden.

Computer Forensics

Secara sederhana Komputer Forensik dapat diartikan sebagai proses menerapkan teknik ilmiah dan analitis untuk Sistem Operasi komputer dan struktur file dalam menentukan potensi bukti hukum.

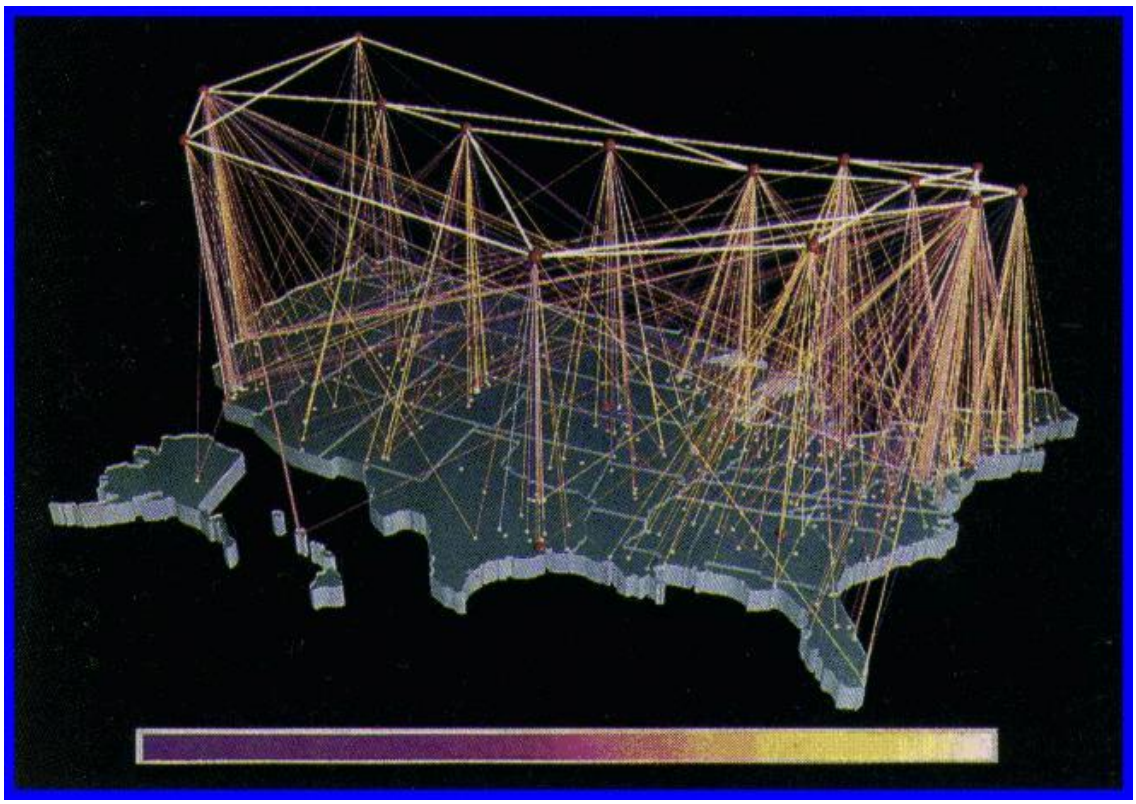
Mengapa bukti penting ? karena dalam dunia hukum, bukti adalah semuanya. Bukti digunakan untuk membangun fakta-fakta. Siapa yang membutuhkan Komputer Forensik ?

korban (seperti private business dan pemerintah), penegak hukum, asuransi, pada akhirnya sistem hukum.

Alasan untuk analisis forensik : ID pelaku, ID vulnerability dari jaringan yang memungkinkan pelaku untuk mendapatkan akses ke dalam sistem, bukti untuk tindakan pengadilan.

Tipe dari komputer forensik :

- Disk Forensic → proses memperoleh dan menganalisis data yang tersimpan pada beberapa bentuk media penyimpanan fisik seperti : floopydisk, hardisk, CD-ROM. Termasuk pemulihan data yang disembunyikan dan dihapus juga identifikasi file.
- Network Forensic → proses pemeriksaan lalu lintas jaringan meliputi analisis transaksi log, analisis real-time melalui monitoring jaringan, IP Spoofing, Hijacking, Password Attack, Distributed-Coordinated Attack, Identity Concealed dari Connection Laundering. Tool : Network Sniffer, System Log, NTSC Adapter



Connection Laundering

- E-mail Forensics → studi tentang sumber dan isi surat elektronik sebagai bukti. Ini mencakup proses identifikasi pengirim yang sebenarnya dan penerima pesan, tanggal dan waktu itu dikirim dan kemana itu dikirim.
- Internet (Web) Forensic → proses piecing bersama dimana dan kapan pengguna telah berada di internet. Misalnya digunakan untuk mengetahui apakah download pornografi itu disengaja atau tidak.
- Source Code Forensic → digunakan untuk menentukan kepemilikan perangkat lunak atau kewajiban masalah perangkat lunak, hal ini tidak hanya review dari source code yang sebenarnya. Ini adalah pemeriksaan keseluruhan proses pembangunan, termasuk prosedur pengembangan, review dokumentasi.

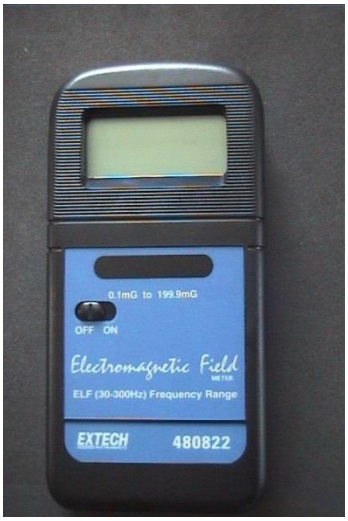
Proses Forensik

1. Preparation → konfirmasi kewenangan untuk melakukan analisis atau pencarian media, verifikasi tujuan analisis dan hasil yang diinginkan jelas, pastikan bahwa media steril tersedia dan dimanfaatkan untuk pencitraan, pastikan bahwa semua perangkat lunak digunakan untuk analisis tersebut teruji dan diterima ssecara luas untuk digunakan dalam komunitas forensik.
2. Protection → melindungi keutuhan dari bukti, memelihara kendali sampai disposisi akhir. Sebelum melakukan booting pada komputer target, putuskan HDD dan lakukan verifikasi CMOS. Ketika boot mesin untuk analisis, manfaatkan software HD Lock.
3. Imaging → memanfaatkan disk “imaging” software untuk membuat gambar yang tepat untuk media target. Ketika melakukan analisis terhadap media target, memanfaatkan gambar yang telah dipulihkan dari media target, tidak pernah memanfaatkan media target yang sebenarnya.
4. Examination → pemeriksaan sistem operasi, jasa, aplikasi, perangkat keras, logfile, sistem, keamanan, berkas sistem, hidden file, perangkat lunak, enskripsi software, SIDS, arsitektur jaringan atau hubungan terpercaya.
5. Documentation

Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer

Forensik Tool

1. Forensic Tool Kit



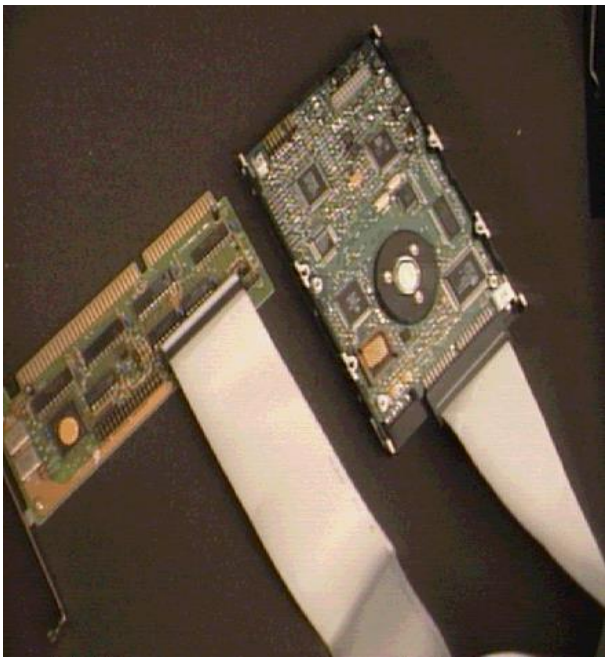
2. Forensic System Hardware

- Sistem utama
  - Pentium-based Computer
  - Multiple OS (UNIX, Windows, MAC)

- Media pilihan

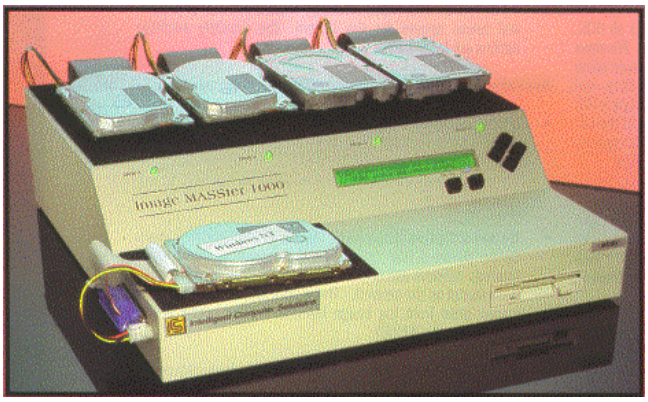
  Sistem forensik kita harus memiliki banyak ruang untuk ekspansi dan media eksternal, hal ini biasanya didukung oleh sistem SCSI.

  - Internal Hard Disk
  - Media Tape (QIC Tape Drive, Travan Tape Drive, DAT)
  - Media Optik (CD-ROM, CD-Writer, DVD)



- Removable Media (REM-KIT)
  - Hard Drive
  - ZIP Drive
  - Jazz Drive
  - PCMCIA Flash Disk

- Disk Imaging Hardware seperti Image MASSter 500 & 1000

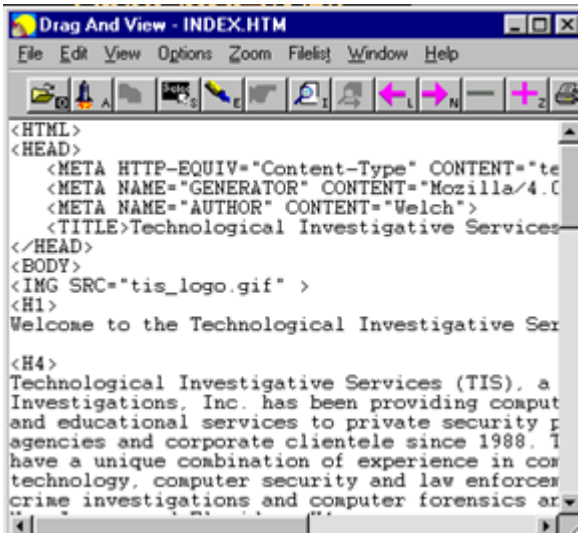


- Wrist Strap
- UPS

3. Forensic Software

- Clean Operating System(s)
- Disk Image Backup Software
- Search & Recovery Utilities
  - Forensic Software : EnCase, Coroners Tool Kit
  - File System Utilities : DOS, Windows, NT, UNIX
  - Norton Utilities
- File Viewing Utilities
  - Quick View Plus
  - Drag & View
  - Thumbs Plus

Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer



- Cracking Software
- Archive & Compression Utilities