

TUGAS KEAMANAN SISTEM LANJUT (EI 7010)

# COMPUTER FORENSIC

**APA dan BAGAIMANA**



Dikerjakan oleh

**Rahmadi Budiman**

**232 02 004**

( [rahmadib@yahoo.com](mailto:rahmadib@yahoo.com) )

Option Teknologi Informasi  
Magister Teknik Elektro  
Institut Teknologi Bandung  
2003

# DAFTAR ISI

Abstrak .....	2
BAB I PENDAHULUAN	
1.1. Latar Belakang .....	3
1.2. Tujuan Forensik Komputer .....	4
BAB II DASAR TEORI	
2.1. Pengertian .....	5
2.2. Bukti Digital ( <i>Digital Evidence</i> ) .....	5
2.3. Empat Elemen Kunci Forensik dalam Teknologi Informasi .....	5
2.4. Manajemen Bukti .....	7
2.4.1. <i>The Chain of Custody</i> .....	7
2.4.2. <i>Rules of Evidence</i> .....	8
2.5. Metodologi Forensik Teknologi Informasi .....	8
2.5.1. <i>Search &amp; Seizure</i> .....	8
2.5.2. Pencarian Informasi .....	10
BAB III INVESTIGASI KASUS TEKNOLOGI INFORMASI	
3.1. Prosedur Forensik yang Umum Digunakan .....	11
3.1.1. Metode <i>Search &amp; Seizure</i> .....	11
3.1.2. Pencarian Informasi .....	14
3.2. <i>Data Recovery</i> .....	14
3.3. Pengelompokan Analisa Media .....	16
3.4. Pembuatan Laporan Analisa Media .....	16
3.5. <i>Log Out Evidence – Visual Inspection and Inventory</i> .....	17
3.6. <i>The Coroner’s Toolkit</i> .....	17
3.7. Pengumpulan Bukti Akhir .....	18
BAB IV KESIMPULAN .....	19
DAFTAR PUSTAKA .....	20

# FORENSIK KOMPUTER: APA DAN BAGAIMANA

## **Abstrak**

Forensik yang identik dengan tindakan kriminal, sampai saat ini hanya sebatas identifikasi, proses, dan analisa pada bagian umum. Untuk kejahatan komputer di Indonesia, forensik di bidang komputer biasanya dilakukan tanpa melihat apa isi di dalam komputer. Justru lebih banyak bukti jika forensik di dalam komputer itu diidentifikasi.

Metode yang umum digunakan untuk forensik pada komputer ada dua, yaitu *search and seizure* dan pencarian informasi (*discovery information*). Metode ini juga dikembangkan dengan manajemen bukti, antara lain *the change of custody* dan *rules of evidence*.

Penekanan metode yang digunakan serta apa saja yang perlu dilakukan, akan lebih banyak dibahas dari pada manajemen bukti. Bukti di sini bukan hanya berupa barang secara fisik, tetapi juga dapat non-fisik.

Paper ini juga mengambil beberapa acuan forensik dari perusahaan keamanan komputer dan *Hongkong Police Force*, sehingga diharapkan akan berguna bagi pihak yang berwenang untuk menyidik sesuatu yang berkaitan dengan kejahatan komputer.

**Kata kunci :** komputer, forensik, bukti

# BAB I

## PENDAHULUAN

### 1.1. Latar Belakang

Penggunaan internet yang semakin meningkat, memberikan dampak positif maupun negatif bagi pihak yang menggunakannya. Dari sisi positif, internet dapat menembus batas ruang dan waktu, di mana antara pengguna dan penyedia layanan dapat melakukan berbagai hal di internet, tanpa mengenal jarak dan perbedaan waktu. Sedangkan sisi negatif, pengaruh budaya luar yang dapat mempengaruhi budaya pengguna internet itu sendiri. Selain itu, kejahatan di dunia maya juga tidak terelakkan lagi.

Perkembangan kejahatan pun semakin luas dan beragam. Mulai dari internet *abuse*, *hacking*, *cracking*, *carding*, dan sebagainya. Mulai dari coba-coba sampai dengan ketagihan/*addicted*, kejahatan di internet menjadi momok bagi pengguna internet itu sendiri. Jika pada awalnya hanya coba-coba, kemudian berkembang menjadi kebiasaan dan meningkat sebagai kebutuhan/ketagihan.

Hukum *cyber* yang masih belum jelas kapan diundangkan menjadikan pelaku kejahatan internet (*cybercrime*) leluasa melawan hukum. KUHP yang notabene warisan Belanda jelas belum menyentuh secara utuh kejahatan di dunia maya ini. Pasal-pasal yang digunakan cenderung tidak membuat jera pelaku kejahatan ini. Pihak berwajib juga masih menunggu hukum *cyber* yang menurut beberapa pakar hukum merupakan hukum yang tidak begitu mengikat.

Segala bentuk kejahatan baik di dunia nyata maupun di dunia maya, sering meninggalkan jejak yang tersembunyi ataupun terlihat. Jejak tersebut yang kemudian dapat meningkat statusnya menjadi bukti, menjadi salah satu perangkat/entitas hukum penting.

## 1.2. Tujuan Forensik Komputer

Dari data yang didapat melalui survei<sup>1</sup> oleh FBI dan *The Computer Security Institute*, pada tahun 1999 mengatakan bahwa 51% responden mengakui bahwa mereka telah menderita kerugian terutama dalam bidang finansial akibat kejahatan komputer. Survei yang sama juga dilakukan pada tahun 2000, terjadi peningkatan menjadi 74% dari responden yang mengatakan bahwa mereka menderita kerugian finansial akibat kejahatan komputer. Pemaparan data di atas memberikan gambaran bahwa terjadi kecenderungan peningkatan kerugian finansial dari pihak pemilik komputer karena kejahatan komputer. Tabel di bawah ini menunjukkan *cybercrime* di Hongkong, mulai dari tahun 2000-2002

**Tabel 1. Jumlah Kriminalitas di Hongkong tahun 2000-2002**

TAHUN	Jumlah Kasus	Total Kejahatan yang Terdeteksi	Total kasus <i>computer crime</i>	Total <i>Computer Crime</i> yang Terdeteksi
2000	77,245	43.6%	368	23%
2001	73,008	44%	235	20.4%
2002	75,877	42.7%	272	21%

Dapat dilihat dari tabel di atas angka kejahatan secara umum meningkat, tetapi angka kejahatan dengan komputer variatif. Dari tabel tersebut juga terlihat adanya *computer crime* yang terdeteksi oleh pihak yang berwenang, dengan prosentase yang fluktuatif.

Kejahatan komputer dibagi menjadi dua, yaitu *computer fraud* dan *computer crime*. *Computer fraud* meliputi kejahatan/pelanggaran dari segi sistem organisasi komputer. Sedang *computer crime* merupakan kegiatan berbahaya di mana menggunakan media komputer dalam melakukan pelanggaran hukum (*computer as a tool*). Untuk menginvestigasi dan menganalisa kedua kejahatan di atas, maka digunakan forensik dalam teknologi informasi.

## BAB II

### DASAR TEORI

#### 2.1. Pengertian

Terminologi forensik komputer sendiri adalah suatu proses mengidentifikasi, memelihara, menganalisa, dan mempergunakan bukti digital menurut hukum yang berlaku<sup>1</sup>. Forensik komputer yang kemudian meluas menjadi forensik teknologi informasi masih jarang digunakan oleh pihak berwajib, terutama pihak berwajib di Indonesia.

#### 2.2. Bukti Digital (*Digital Evidence*)

Bukti digital adalah informasi yang didapat dalam bentuk/format digital (**Scientific Working Group on Digital Evidence, 1999**). Bukti digital ini bisa berupa bukti yang riil maupun abstrak (perlu diolah terlebih dahulu sebelum menjadi bukti yang riil). Beberapa contoh bukti digital antara lain :

- E-mail, alamat e-mail
- Wordprocessor/spreadsheet files
- Source code dari perangkat lunak
- Files berbentuk image ( .jpeg, .tif, dan sebagainya)
- *Web browser bookmarks, cookies*
- Kalender, *to-do list*

#### 2.3. Empat Elemen Kunci Forensik dalam Teknologi Informasi

Adanya empat elemen kunci forensik dalam teknologi informasi<sup>2</sup> adalah sebagai berikut :

### 1. Identifikasi dari Bukti Digital

Merupakan tahapan paling awal forensik dalam teknologi informasi. Pada tahapan ini dilakukan identifikasi di mana bukti itu berada, di mana bukti itu disimpan, dan bagaimana penyimpanannya untuk mempermudah tahapan selanjutnya. Banyak pihak yang mempercayai bahwa forensik di bidang teknologi informasi itu merupakan forensik pada komputer. Sebenarnya forensik bidang teknologi informasi sangat luas, bisa pada telepon seluler, kamera digital, *smart cards*, dan sebagainya. Memang banyak kasus kejahatan di bidang teknologi informasi itu berbasis komputer. Tetapi perlu diingat, bahwa teknologi informasi tidak hanya komputer/internet.

### 2. Penyimpanan Bukti Digital

Termasuk tahapan yang paling kritis dalam forensik. Pada tahapan ini, bukti digital dapat saja hilang karena penyimpanannya yang kurang baik. Penyimpanan ini lebih menekankan bahwa bukti digital pada saat ditemukan akan tetap tidak berubah baik bentuk, isi, makna, dan sebagainya dalam jangka waktu yang lama. Ini adalah konsep ideal dari penyimpanan bukti digital.

### 3. Analisa Bukti Digital

Pengambilan, pemrosesan, dan interpretasi dari bukti digital merupakan bagian penting dalam analisa bukti digital. Setelah diambil dari tempat asalnya, bukti tersebut harus diproses sebelum diberikan kepada pihak lain yang membutuhkan. Tentunya pemrosesan di sini memerlukan beberapa skema tergantung dari masing-masing kasus yang dihadapi.

### 4. Presentasi Bukti Digital

Adalah proses persidangan di mana bukti digital akan diuji otentifikasi dan korelasi dengan kasus yang ada. Presentasi di sini berupa penunjukan bukti digital yang berhubungan dengan kasus yang disidangkan. Karena proses penyidikan sampai dengan proses persidangan memakan waktu yang cukup lama, maka sedapat mungkin bukti digital masih asli dan sama pada saat diidentifikasi oleh investigator untuk pertama kalinya.

## 2.4. Manajemen Bukti

Jika ditelusuri lebih jauh, forensik itu sendiri merupakan suatu pekerjaan identifikasi sampai dengan muncul hipotesa yang teratur menurut urutan waktu. Sangat tidak mungkin forensik dimulai dengan munculnya hipotesa tanpa ada penelitian yang mendalam dari bukti-bukti yang ada. Investigator harus mampu menyaring informasi dari bukti yang ada tetapi tanpa merubah keaslian bukti tersebut. Adanya dua istilah dalam manajemen (barang) bukti antara lain *the chain of custody* dan *rules of evidence*, jelas akan membantu investigator dalam mengungkap suatu kasus.

### 2.4.1. *The Chain of Custody*

Satu hal terpenting yang perlu dilakukan investigator untuk melindungi bukti adalah *the chain of custody*. Maksud istilah tersebut adalah pemeliharaan dengan meminimalisir kerusakan yang diakibatkan karena investigasi. Barang bukti harus benar-benar asli atau jika sudah tersentuh investigator, pesan-pesan yang ditimbulkan dari bukti tersebut tidak hilang. Tujuan dari *the chain of custody* adalah :

1. Bukti itu benar-benar masih asli/orisinal
2. Pada saat persidangan, bukti masih bisa dikatakan seperti pada saat ditemukan.  
(biasanya jarak antara penyidikan dan persidangan relatif lama)

Beberapa pertanyaan yang dapat membantu *the chain of custody* ini adalah :

1. Siapa yang mengumpulkan bukti ?
2. Bagaimana dan di mana ?
3. Siapa yang memiliki bukti tersebut ?
4. Bagaimana penyimpanan dan pemeliharaan selama penyimpanan bukti itu ?
5. Siapa yang mengambil dari penyimpanan dan mengapa ?

Untuk menjaga bukti itu dalam mekanisme *the chain of custody* ini, dilakukan beberapa cara :

1. Gunakan catatan yang lengkap mengenai keluar-masuk bukti dari penyimpanan
2. Simpan di tempat yang dianggap aman.
3. Akses yang terbatas dalam tempat penyimpanan.
4. Catat siapa saja yang dapat mengakses bukti tersebut.

### **2.4.2. Rules of Evidence**

Manajemen bukti kejahatan komputer juga mengenal istilah “Peraturan Barang Bukti” atau *Rules of Evidence*. Arti istilah ini adalah barang bukti harus memiliki hubungan yang relevan dengan kasus yang ada. Dalam *rules of evidence*, terdapat empat persyaratan yang harus dipenuhi, antara lain :

1. Dapat Diterima (*Admissible*)

Harus mampu diterima dan digunakan demi hukum, mulai dari kepentingan penyidikan sampai dengan kepentingan pengadilan.

2. Asli (*Authentic*)

Bukti tersebut harus berhubungan dengan kejadian/kasus yang terjadi dan bukan rekayasa.

3. Lengkap (*Complete*)

Bukti bisa dikatakan bagus dan lengkap jika di dalamnya terdapat banyak petunjuk yang dapat membantu proses investigasi.

4. Dapat Dipercaya (*Believable & Reliable*)

Bukti dapat mengatakan hal yang terjadi di belakangnya. Jika bukti tersebut dapat dipercaya, maka proses investigasi akan lebih mudah. Walau relatif, dapat dipercaya ini merupakan suatu keharusan dalam penanganan perkara.

### **2.5. Metodologi Forensik Teknologi Informasi**

Metodologi yang digunakan dalam menginvestigasi kejahatan dalam teknologi informasi dibagi menjadi dua :

1. *Search & Seizure*

2. Pencarian informasi

#### **2.5.1. Search & Seizure**

Investigator harus terjun langsung ke dalam kasus yang dihadapi, dalam hal ini kasus teknologi informasi. Diharapkan investigator mampu mengidentifikasi, menganalisa, dan memproses bukti yang berupa fisik. Investigator juga berwenang untuk melakukan penyitaan terhadap bukti yang dapat membantu proses penyidikan, tentunya di bawah koridor hukum yang berlaku.

### 2.5.2. Pencarian Informasi

Beberapa tahapan dalam pencarian informasi khususnya dalam bidang teknologi informasi :

1. Menemukan lokasi tempat kejadian perkara
2. Investigator menggali informasi dari aktivitas yang tercatat dalam log di komputer
3. Penyitaan media penyimpanan data (*data storages*) yang dianggap dapat membantu proses penyidikan

Walaupun terlihat sangat mudah, tetapi dalam praktek di lapangan, ketiga tahapan tersebut sangat sulit dilakukan. Investigator yang lebih biasa ditempatkan pada kasus kriminal non-teknis, lebih terkesan terburu-buru mengambil barang bukti dan terkadang barang bukti yang dianggap penting ditinggalkan begitu saja.

Dalam menggali informasi yang berkaitan dengan kasus teknologi informasi, peran investigator dituntut lebih cakap dan teliti dalam menyidik kasus tersebut. Celah yang banyak tersedia di media komputer menjadikan investigator harus mengerti trik-trik kasus teknologi informasi.

Kedua metodologi di atas setidaknya menjadi acuan pihak yang berwenang dalam menyidik kasus kejahatan dalam bidang teknologi informasi.

## BAB III

### INVESTIGASI KASUS TEKNOLOGI INFORMASI

#### 3.1. Prosedur Forensik yang Umum Digunakan

Beberapa literatur menyebutkan bahwa prosedur yang perlu dilakukan oleh investigator dapat dijelaskan sebagai berikut :

1. Membuat *copies* dari keseluruhan *log data*, files, dan lain-lain 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

Bukti yang biasanya digunakan dalam forensik komputer adalah berupa :

1. *Logs*
2. *Stand alone system*
3. *Networked system*
4. *Harddisk*
5. *Floppy disk* atau media lain yang bersifat *removable*

Selain itu, perlu dilakukan investigasi lanjutan di mana digunakan dua metodologi yang telah disebut sebelumnya. Dari kedua metode tersebut, metode *search* and *seizure* lebih banyak digunakan dari pada pencarian informasi. Walaupun di sisi lain, tidak ada salahnya jika metode *search* dan *seizure* tersebut dilengkapi dengan pencarian informasi yang lebih rinci.

##### 3.1.1. Metode *Search* dan *Seizure*

Proses *search* dan *seizure* sendiri dimulai dari perumusan suatu rencana. Cara yang paling sering digunakan adalah membuat software khusus untuk mencari bukti.

Selain merupakan cara yang tepat untuk melakukan forensik teknologi informasi, pembuatan software khusus ini juga membuktikan adanya metodologi penelitian yang ilmiah.

Tahapan dalam *search* dan *seizure*<sup>1</sup> ini dapat dijabarkan sebagai berikut :

1. Identifikasi dan penelitian permasalahan

Dalam hal ini identifikasi adalah identifikasi permasalahan yang sedang dihadapi, apakah memerlukan respon yang cepat atau tidak. Jika tidak, maka dilanjutkan dalam penelitian permasalahan secara mendalam.

2. Membuat hipotesa

Pembuatan hipotesa setelah melalui proses identifikasi dan penelitian permasalahan yang timbul, sehingga data yang didapat selama kedua proses di atas dapat dihasilkan hipotesa.

3. Uji hipotesa secara konsep dan empiris

Hipotesa diuji secara konsep dan empiris, apakah hipotesa itu sudah dapat dijadikan kesimpulan atau tidak.

4. Evaluasi hipotesa berdasarkan hasil pengujian dan pengujian ulang jika hipotesa tersebut jauh dari apa yang diharapkan

5. Evaluasi hipotesa terhadap dampak yang lain jika hipotesa tersebut dapat diterima

Tahapan-tahapan di atas bukan merupakan tahapan yang baku, disesuaikan dengan kondisi di lapangan. Kondisi keadaan yang berubah-ubah memaksa investigator lebih cermat mengamati data sehingga hipotesa yang diambil tidak jauh dari kesimpulan akhir.

*Search* dan *seizure* sendiri meliputi pemulihan dan pemrosesan dari bukti komputer secara fisik. Walaupun banyak hal yang positif, metode ini juga memberikan penekanan dan batas-batas untuk investigator agar hipotesa yang dihasilkan sangat akurat. Adapun penekanan dan batas-batas untuk investigator tersebut adalah :

1. Jangan merubah bukti asli

2. Jangan mengeksekusi program pada bukti (komputer) terutama *Operating System*-nya

3. Tidak mengizinkan tersangka untuk berinteraksi dengan bukti (komputer)

4. Segera mungkin mem-*backup* bukti yang ada di dalam komputer tersangka. Jika pada saat diidentifikasi komputer masih nyala, 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

Penekanan ini sangat berguna dalam pengumpulan, penanganan, dan penyimpanan bukti agar dalam jangka waktu yang lama (sejak proses penyidikan sampai proses persidangan) bukti tersebut tidak berubah.

Untuk *seizure* ini, terdapat *guidance* dari Manageworx Infosystem Inc sebagai berikut :

1. Perencanaan / *Planning*

- Identifikasi sistem komputer yang dihadapi
- Identifikasi komputer tersebut terhubung dengan jaringan atau tidak
- Identifikasi kebutuhan lain yang diperlukan oleh sistem administrator untuk menggunakannya
- Tunjuk satu orang yang bertanggung jawab terhadap bukti tersebut
- Buat dokumentasi apa saja yang akan dan sudah dikerjakan

2. Pemeliharaan, Pengumpulan, dan Dokumentasi

- Tunjuk bukti utama
- Buat dokumentasi berupa gambar dan video
- Berikan catatan pada dokumen gambar dan video tersebut
- Beri label pada seluruh bukti

3. *Seizing Electronic Evidence*

- Jika memiliki jaringan, ambil bukti tersebut supaya tidak *dirremote*
- Gunakan *disk* yang *bootable* dan cek apakah ada virus
- Kunci media penyimpanan (*harddisk*) agar tidak ditulis/dihapus ulang

4. Catat waktu investigasi

5. Membuat gambaran arus bit dari bukti ke dalam media baru

6. Kalkulasi dan catat kriptografi *checksum* dari media penyimpanan yang asli dan *image*-nya

md5sum menyediakan 32 bit *signature* yang sensitif terhadap perubahan

```
#md5sum filename
a2c9e26fb92276cf57a59293401514b9 filename
```

7. Tidak mungkin 2 file berbeda membuat *hash* yang sama

Managework membuat *checklist* ini selain untuk mempermudah, Manageworx juga sudah memiliki software forensik yang dapat diimplementasikan dalam sistem UNIX atau non-UNIX.

### 3.1.2. Pencarian Informasi

Metode pencarian informasi yang dilakukan oleh investigator merupakan pencarian bukti tambahan dengan mengandalkan saksi baik secara langsung maupun tidak langsung terlibat dengan kasus ini. Pencarian informasi didukung bukti yang sudah ada menjadikan hipotesa yang diambil semakin akurat.

Pada intinya, pencarian ini merupakan bukti tambahan, dengan memperhatikan hal-hal sebagai berikut :

1. Jika melakukan penggalian informasi lebih dalam ke saksi, maka gunakan metode wawancara interaktif, sehingga bukti yang sudah ada dapat di-*cross check* agar keberadaan bukti tersebut diakui oleh saksi
2. Jika memungkinkan, rekonstruksi dilakukan dengan/tanpa tersangka sehingga apa yang masih belum jelas dapat tergambar dalam rekonstruksi

### 3.2. Data Recovery

*Data recovery* merupakan bagian dari analisa forensik di mana hal ini merupakan komponen penting di dalam mengetahui apa yang telah terjadi, rekaman data, korespondensi, dan petunjuk lainnya. Banyak orang tidak menggunakan informasi yang berasal dari *data recovery* karena dianggap tidak murni/asli/orisinal.

Setiap sistem operasi bekerja dalam arah yang unik, berbeda satu sama lain (walaupun berplatform sistem operasi yang sama). Seperti pada sistem UNIX, Internet FAQ (<http://rtfm.mit.edu>) telah membuat pernyataan pada tahun 1993 sebagai berikut :

*For all intents and purposes, when you delete a file with "rm" it is gone...However, never say never. It is theoretically possible \*if\* you shut down the system immediately after the "rm" to recover portions of the data. However, you had better have a very wizardly type person at hand with hours or days to spare to get it all back.*

Untuk melihat seberapa jauh data sudah dihapus atau belum, perlu memperhatikan segala sesuatu yang ada dalam *raw disk*. Jika data yang digunakan untuk kejahatan ternyata masih ada, maka cara yang termudah adalah menguji data dengan pemanfaatan tool yang ada pada standar UNIX, seperti *strings*, *grep*, *text pagers*, dan sebagainya. Sayangnya, tools yang ada tidak menunjukkan data tersebut dialokasikan di mana.

Contohnya, *intruder* menghapus seluruh system log files (dimulai dari bulan, hari, dan waktu) dari minggu pertama Januari, seharusnya ditulis untuk melihat syslog tersebut:

```
strings /dev/raw/disk/device | egrep '^Jan 0[1-7]
[0-9][0-9]:[0-9][0-9]:[0-9][0-9]' | sort | uniq -c >
date-file
```

Melalui investigasi dari sistem yang dirusak oleh *intruder*, sistem files UNIX yang modern tidak menyebar *contents* dari suatu file secara acak dalam disk. Sebagai gantinya, sistem files dapat mencegah fragmentasi file, meskipun setelah digunakan beberapa tahun.

*File content* dengan sedikit fragmentasi akan lebih mudah untuk proses *recover* dari pada *file content* yang menyebar dalam disk (media penyimpanan). Tetapi sistem file yang baik memiliki beberapa keuntungan lain, salah satunya mampu untuk menghapus informasi untuk bertahan lebih lama dari yang diharapkan.

Dalam kasus Linux, sistem file *ext2* tidak akan menghapus lokasi dari urutan pertama 12 blok data yang tersimpan dalam *inode* jika file sudah dipindah/dihapus. Hal ini berarti menghapus data dapat dikembalikan langsung dengan menggunakan *icat* dalam *inode* yang terwakilkan. Seperti metode *data recovery* lainnya, tidak akan menjamin jika data tetap ada di tempat semula. Jika file dihapus dalam sistem operasi Linux, *inode's dtime* akan *terupdate*. Dengan menggunakan informasi tersebut, data dapat dikembalikan dari 20 *inode* pada sistem file yang dihapus. Contoh aplikasi dalam Linux adalah sebagai berikut :

```
for inode_num in `ls /dev/device |
sort -n +7 -t |
tail -20 |
awk -F | {print $1}`
do
icat /dev/device $inode_num > $inode_num.result
done
```

### 3.3. 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.

### 3.4. Pembuatan Laporan dalam Analisa Media

Beberapa hal penting yang perlu dimasukkan dalam laporan analisa media adalah sebagai berikut :

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)

Pada laporan akhir, penemuan ini sangat ditekankan sebagai bukti penting sebagai pendukung proses penyidikan.

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 dicross check dengan saksi yang ada, baik saksi terlibat langsung maupun tidak langsung.

### **3.5. Log Out Evidence – Visual Inspection and Inventory<sup>3</sup>**

Tahapan yang dilalui dalam inspeksi komputer secara visual adalah :

1. Log out seluruh komputer untuk dianalisa lebih lanjut
2. Jika ada media penyimpanan 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 di 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, dan sebagainya)
7. Dokumentasikan dalam bentuk gambar sebelum dan sesudah identifikasi dan analisa

### **3.6. The Coroner's Toolkit<sup>2</sup>**

Ada beberapa *tools* yang dapat digunakan untuk *recovery* data yang terhapus, terutama untuk UNIX. Salah satu di antaranya adalah *The Coroner's Toolkit* (TCT), *tool* yang digunakan untuk *tracking* data digital.

TCT adalah *tool* standar, di mana dapat digunakan sebagai pengujian forensik pada komputer. Walaupun didesain untuk komputer berbasis sistem operasi UNIX, tetapi pada kenyataannya dapat digunakan pada sistem operasi non-UNIX. Untuk *recovery* data non-UNIX, TCT akan menghabiskan waktu lebih lama dibandingkan jika digunakan dalam platform UNIX. Salah satu aspek dari TCT adalah sesuatu yang disebut dengan *grave-robber*, sebuah program yang mengontrol jumlah *tools* sejenis yang digunakan dalam *recovery*.

Di dalam TCT, terdapat program yang disebut dengan “Lazarus” di mana program itu akan menghasilkan hasil yang tidak biasa, yaitu *unstructured data*. Lazarus

juga dapat memanipulasi data menggunakan beberapa *heuristic* yang sederhana. Hasil akhir Lazarus adalah :

- UNIX FFS tidak akan memulai menulis suatu data dalam file kecuali dalam *well-defined boundaries*.
- Sistem file UNIX menulis file dalam blok yang kontinyu jika memungkinkan performanya memenuhi beberapa kriteria.

Program unrm juga terdapat dalam TCT. Program ini dapat menggunakan semua blok yang tidak teralokasi dalamsuatu sistem. Unrm merupakan *tool* yang *powerful* jika menginginkan *tracking* pada file yang terhapus. Contoh *bit editing* pada unrm adalah sebagai berikut :

```
unrm /dev/raw/disk/device | egrep '^.*:.*:[0-9]*:[0-9]*:.*:.*:' | sort -u > unrm-password-file
```

Data yang dicoba untuk di-*undelete* terkadang tidak sama dengan keadaan aslinya. Tetapi setidaknya elemen penting dalam data tersebut masih dapat dikatakan berhasil *direcovery*.

### 3.7. Pengumpulan Bukti Akhir

Dari keseluruhan proses investigasi, dibuat dalam *worksheet* yang digunakan untuk tahapan analisa dan proses lebih lanjut ke tingkat selanjutnya. Dalam proses ini, bukti yang digunakan tidak boleh berubah sejak digunakan sebagai alat bukti pertama kali.

## BAB IV

### KESIMPULAN

Metode yang banyak digunakan dalam forensik komputer adalah *search* dan *seizure* dan pencarian informasi. *Search* dan *seizure* merupakan metode yang paling banyak digunakan, sedangkan pencarian informasi (*information search*) sebagai pelengkap data bukti tersebut.

Tinjauan dari sisi *software* maupun *hardware* dalam forensik ini lebih mencerminkan bahwa kedua komponen komputer itu memang tidak dapat dipisahkan, karena adanya saling ketergantungan satu sama lain. Dalam menginvestigasi suatu kasus, digunakan *tools* untuk menganalisa komputer baik secara *software* maupun *hardware*.

Forensik komputer adalah bidang baru di Indonesia, di mana keberadaan forensik ini sangat dibutuhkan untuk memecahkan kasus tertentu. Jika lebih dikembangkan, maka forensik akan menjadi cabang keamanan dari komputer/jaringan dan bagian yang tidak terpisahkan dalam Labkrim Mabes Polri.

## DAFTAR PUSTAKA

- [1] Moroni Parra, "Computer Forensic", November 2002, [http://www.giac.org/practical/Moroni\\_Parra\\_GSEC.doc](http://www.giac.org/practical/Moroni_Parra_GSEC.doc)
- [2] Rodney McKemmish, "What is Forensic Computing", Australian Institut of Criminology, Canberra, June 1999, <http://www.aic.gov.au/publications/tandi/ti118.pdf>
- [3] Dave Pettinari, "Computer Forensics Processing Checklist", Pueblo County Sheriff's Office, June 2000, <http://www.crime-research.org/eng/library/Computer%20Forensics%20Checklist.pdf>
- [4] Erik K.M. Cheung, "Computer Forensic and the Law of Evidence", Hongkong Police Force, 2003, <http://law.hku.hk/teaching/cybercrime/EricCheungForensics.PPT>
- [5] Marc Rogers, PhD, "Computer Forensics: Evidence Handling & Management", Manageworx Infosystem Inc, 2002, <http://www.manageworx.com/news/CompForensic.pdf>
- [6] Andrew Sheldon, "The Future of Forensic Computing", 4Warn Forensics, 2000, [http://www.forensics.co.nz/client\\_area/ASIS\\_P13\\_23\\_Feb\\_2002.pdf](http://www.forensics.co.nz/client_area/ASIS_P13_23_Feb_2002.pdf)
- [7] Rongsheng Xu, "Security Forensic on E-Commerce, IHEP Computing Center, Chinese Academy of Science, 2000, <http://unpan1.un.org/intradoc/groups/public/documents/un/unpan001217.pdf>
- [8] John Patzakis, "Computer Forensic as Integral Component of the Information Security Enterprise, Guidance Software, 2003, [http://www.isaca-la.org/2002\\_Spring\\_Conference/Handouts/T5%20Computer\\_Forensics.pdf](http://www.isaca-la.org/2002_Spring_Conference/Handouts/T5%20Computer_Forensics.pdf)
- [9] Steve Romig, "Forensic Computer Investigations", ACM, 2003, [http://www.net.ohio-state.edu/security/talks/2000/2000-12-05\\_forensic-computer-investigations\\_lisa/forensics-notes.pdf](http://www.net.ohio-state.edu/security/talks/2000/2000-12-05_forensic-computer-investigations_lisa/forensics-notes.pdf)

- [10] Budi Rahardjo, “Hukum dan Dunia Cyber”, PT INDOCISC Jakarta, 2003
- [11] Budi Rahardjo, “Keamanan Sistem Berbasis Internet”, PT Insan Infonesia Bandung & PT INDOCISC Jakarta, 2002, <http://budi.insan.co.id/>
- [12] Budi Rahardjo, “Panduan Menulis dan Mempresentasikan Karya Ilmiah: Thesis, Tugas Akhir, dan Makalah”, 2003, <http://budi.insan.co.id/>