Muhammad Azriansyah 09011281320006 Keamanan Jaringan Komputer

Analisis Praktikum kjk “komputer forensik“

Definis komputer forensik

Secara garis besar, di rangkum dari berbagai sumber : "suatu rangkaian metodologi yang terdiri dari teknik dan prosedur untuk mengumpulkan bukti-bukti berbasis entitas maupun piranti digital agar dapat dipergunakan secara sah sebagai alat bukti di pengadilan."

Di dalam keamananan jaringan, pasti akan melakukan yang nama nya komputer forensik. Suatu rangkaian metodologi untuk mengumpulkan bukti2 digital untuk pengadilan.

Tujuan :

1. Untuk membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat butki yang sah di pengadilan.

2. Untuk mendukung proses identifikasi alat bukti dalam waktu yang relatif cepat, agar dapat diperhitungkan perkiraan potensi dampak yang ditimbulkan akibat perilaku jahat yang dilakukan oleh kriminal terhadap korbannya, sekaligus mengungkapkan alasan dan motivitasi tindakan tersebut sambil mencari pihak-pihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan tidak menyenangkan dimaksud.

Fokus :

Fokus data yang di kumpulkan di bagi menjadi 3 kategori :

1. Active data

Yaitu informasi terbuka yang dapat dilihat oleh siapa saja, terutama data, program, maupun file yang dikendalikan oleh sistem operasi.

2. Archival data

Yaitu informasi yang telah menjadi arsip sehingga telah disimpan sebagai backup dalam berbagai bentuk alat penyimpan seperti hardisk eksternal, cd rom, backup tape, dvd, dan lain-lain.

3. Latent data

Yaitu informasi yang membutuhkan alat khusus untuk mendapatkannya karena sifatnya yang khusus,

Misalnya: telah dihapus, ditimpa data lain, rusak (corrupted file), dan lain sebagainya

Manfaat :

1. Organisasi/perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti2 pendukung yg di butuhkan.

2. Seandainya terjadi peristiwa kejahatan yang membutuhkan investigasi lebih lanjut,dampak gangguan terhadap operasional organisasi atau perusahaan dapat diminimalisir.

3. Para kriminal atau pelaku kejahatan akan berpikir dua kali sebelum menjalankan aksi kejahatannya terhadap organisasi atau perusahaan tertentu yang memiliki kapabilitas forensik komputer;

4. Membantu organisasi atau perusahaan dalam melakukan mitigasi resiko teknologi informasi yang dimilikinya.

Objek :

Semboyan detektif: "Tidak ada kejahatan yang tidak meninggalkan jejak"

1. Log file atau catatan aktivitas penggunaan komputer yang tersimpan secara rapi dan detail di dalam sistem.

2. File yang sekilas telah terhapus secara sistem, namun secara teknikal masih bisa diambil dengan cara-cara tertentu.

3. Catatan digital yang dimiliki oleh piranti pengawas trafik seperti ips (intrusion prevention system) dan ids (intrusion detection system).

4. Hard disk yang berisi data/informasi backup dari sistem utama.

5. Rekaman email, mailing list, blog, chat, dan mode interaksi dan komunikasi lainnya.

6. Beraneka ragam jeis berkas file yang dibuat oleh sistem maupun aplikasi untuk membantu melakukan manajemen file (misalnya: .tmp, .dat, .txt, dan lain-lain)

7. Rekam jejak interaksi dan trafik via internet dari satu tempat ke tempat yang lain (dengan berbasis ip address misalnya).

Kasus :

Ada seorang penegdar narkoba yang tertangkap, polisi ada harddrive yang sdah korup dr tersangka. Bagaimana kita me recover nya. Kita di minta bantuan untuk mendapatkan beberapa informasi di bawah:

1.who is joe jacob's supplier of marijuana and what is the address listed for the supplier?

2.what crucial data is available within the coverpage.jpg file and why is this data crucial?

3.what (if any) other high schools besides smith hill does joe jacobs frequent?

4.for each file, what processes were taken by the suspect to mask them from others?

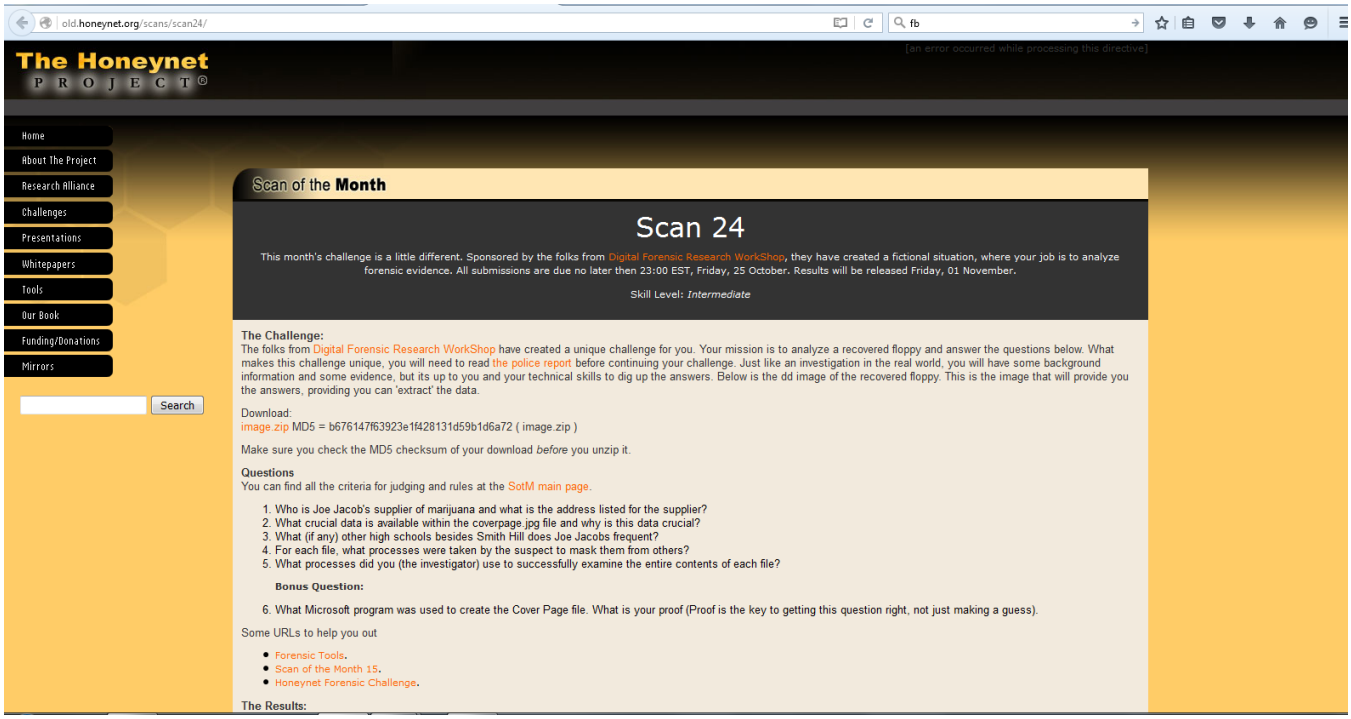
5.what processes did you (the investigator) use to successfully examine the entire contents of each file?

Tools yang di gunakan:

1. Autopsy
2. Foremost
3. Strings

Langkah kerja :

1. Install tools, selain strings
2. Buka wesite berikut. File tersebut merupakan source barang bukti dari kasus yang sedang di miliki, di mana image.zip yang akan di download merupakan barang bukti yang berhasil di dapatkan dari computer tersangka yang mana harus di selidiki dengan computer forensic.



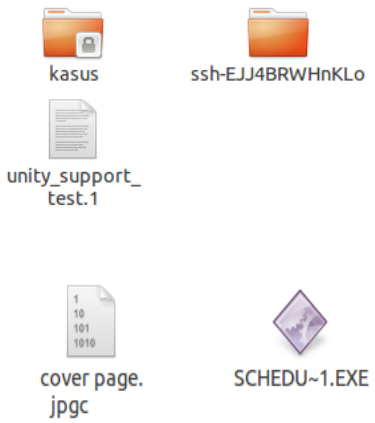
Fungsi md5sum : sebuah file pasti ada md5sum yang berfungsi untuk mengecek keaslian dari file atau integritas file

```
root@mahasiswa:/home/mahasiswa/Downloads# ls
image  image.zip
root@mahasiswa:/home/mahasiswa/Downloads# file image
image: DOS floppy 1440k, x86 hard disk boot sector
root@mahasiswa:/home/mahasiswa/Downloads#
```

Fungsi perintah di atas : untuk mengecek tipe file. Jika kita menenmukan file yang tidak ada ekstensi, maka kita bisa menggunakan

Setelah kita tahu bahwa file tersebut file boot sector, maka akan melakukan proses mounting

```
root@mahasiswa:/home/mahasiswa/Downloads# mount image /tmp/kasu
s
```




```
root@mahasiswa:/home/mahasiswa/Downloads# cd /tmp/kasus
root@mahasiswa:/tmp/kasus# ls
cover page.jpgc              SCHEDU~1.EXE
root@mahasiswa:/tmp/kasus#
```

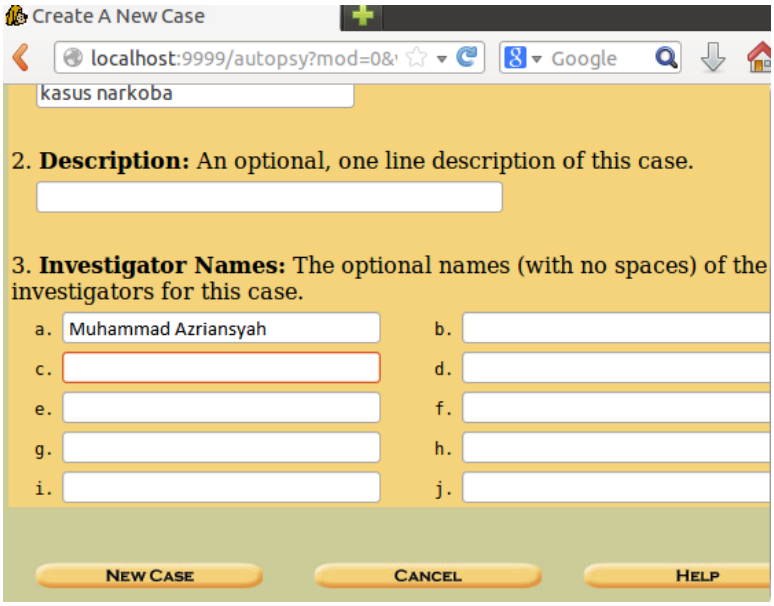
Dalam computer forensic keaslian file barang bukti menjadi tolok ukur keberhasilan dalam menguak informasi yang mampu di kumpulkan dalam mengetahui tindak-tanduk pelaku yang mungkin terekam di dalam file-file yang ada pada perangkat computer pelaku. Mengecek keaslian file bisa di lakukan seperti di bawah ini :

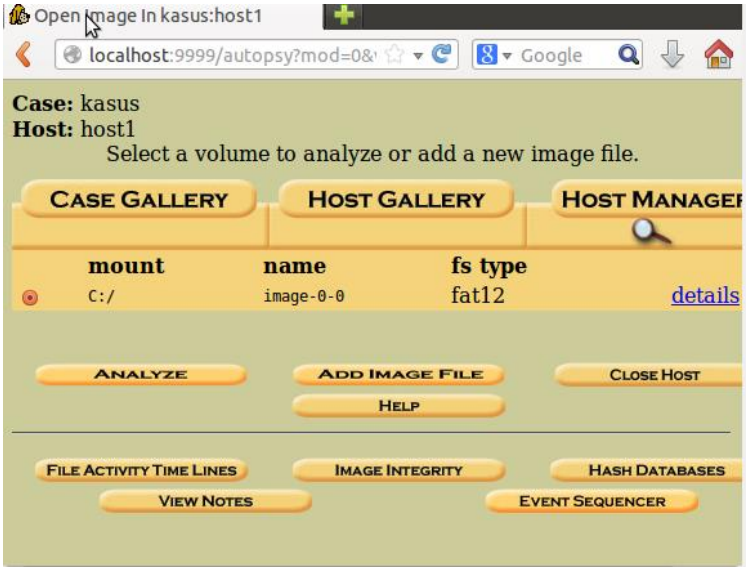
```
root@mahasiswa:/tmp/kasus# file *
cover page.jpgc           : ERROR: cannot read `cover page.jpgc
          ' (Input/output error)
SCHEDU~1.EXE:               Zip archive data, at least v2.0 to
extract
root@mahasiswa:/tmp/kasus#
```

Untuk tindakan forensic lanjutan maka bisa gunakan tool, kita bisa gunakan Tools psy. Karena psy menggunakan

```
root@mahasiswa:/tmp/kasus# autopsy
  I
================================================================
=============

                    Autopsy Forensic Browser
                http://www.sleuthkit.org/autopsy/
                           ver 2.24

================================================================
=============
Evidence Locker: /var/lib/autopsy
Start Time: Thu Mar 23 10:01:14 2017
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in i
t:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

Mengatur hostname, siapa yang melakukan forensik pada komputer target.





2 file yang bisa kita ambil

FAT CONTENTS (in sectors)

73-103 (31) -> EOF
104-108 (5) -> EOF

Yang 1. Jfif liat di wikipedia

Yang2. Pk

```
root@mahasiswa:/home/mahasiswa# cd Downloads/
root@mahasiswa:/home/mahasiswa/Downloads# ls
image  image.zip  Link to image  vol1-Sector73.raw
root@mahasiswa:/home/mahasiswa/Downloads# file vol1-Sector73.ra
w
vol1-Sector73.raw: JPEG image data, JFIF standard 1.01
root@mahasiswa:/home/mahasiswa/Downloads#
```

Rename menjadi file dengan ekstensi .jpg, lalu dapat di lihat bahwa penjual narkobanya bernama “Jimmy Jungle”.


```
root@mahasiswa:/home/mahasiswa/Downloads# strings vol1-Sector73
.jpg
```

```
FFFy
        NrH'
puO     k
go}b
`/9'
Tw      l
c\[M0
T[9j
k}Bx`VE
s$6s,
zz7q
K;dMj
)UfRcvm
8-'H$
FFFy
        NrH'
|7g%
9'p+
R*]I
oqk4
I+^L
pw=goodtimes
root@mahasiswa:/home/mahasiswa/Downloads#
```

Menyimpan password di dalam file gambar dan password yang di dapatkan adalah “goodtimes”.

1	Month	DAY	HIGH SCHOOLS
2	2002		
3	April	Monday (1)	Smith Hill High School (A)
4		Tuesday (2)	Key High School (B)
5		Wednesday (3)	Leetch High School (C)
6		Thursday (4)	Birard High School (D)
7		Friday (5)	Richter High School (E)
8		Monday (1)	Hull High School (F)
9		Tuesday (2)	Smith Hill High School (A)
10		Wednesday (3)	Key High School (B)
11		Thursday (4)	Leetch High School (C)
12		Friday (5)	Birard High School (D)
13		Monday (1)	Richter High School (E)
14		Tuesday (2)	Hull High School (F)
15		Wednesday (3)	Smith Hill High School (A)
16		Thursday (4)	Key High School (B)
17		Friday (5)	Leetch High School (C)

```
root@mahasiswa:/home/mahasiswa/Downloads# foremost -v -i image
-o recover
```

Merecover jika signature nya hilang

Menggunakan ghex