Tugas Keamanan Jaringan Komputer “Komputer Forensik”

Nama : Somame Morianus Daely
NIM : 09011281419058

KOMPUTER FORENSIK

Forensik komputer adalah 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. Adapun tujuan dari adanya komputer forensik ini adalah :

1. Untuk membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat buti 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.

Adapun aktivitas forensik komputer biasanya dilakukan dalam dua konteks utama. Pertama adalah konteks terkait dengan pengumpulan dan penyimpanan data berisi seluruh rekaman detail mengenai aktivitas rutin yang dilaksanakan oleh organisasi atau perusahaan tertentu yang melibatkan teknologi informasi dan komunikasi. Dan kedua adalah pengumpulan data yang ditujukan khusus dalam konteks adanya suatu tindakan kejahatan berbasis teknologi.

Sementara itu fokus data yang dikumpulkan dapat dikategorikan menjadi 3 (tiga) domain utama, yaitu:

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; dan
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

A. Manfaat dan Tantangan Forensik Komputer
   a. Manfaat

      Memiliki kemampuan dalam melakukan forensik komputer akan mendatangkan sejumlah manfaat, antara lain:

- Organisasi atau perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti-bukti pendukung yang dibutuhkan.
- Seandainya terjadi peristiwa kejahatan yang membutuhkan investigasi lebih lanjut, dampak gangguan terhadap operasional organisasi atau perusahaan dapat diminimalisir;
- Para kriminal atau pelaku kejahatan akan berpikir dua kali sebelum menjalankan aksi kejahatannya terhadap organisasi atau perusahaan tertentu yang memiliki kapabilitas forensik komputer; dan
- Membantu organisasi atau perusahaan dalam melakukan mitigasi resiko teknologi informasi yang dimilikinya.

b. Tantangan

Terlepas dari manfaat tersebut, teramat banyak tantangan dalam dunia forensik komputer, terutama terkait dengan sejumlah aspek sebagai berikut:

- Forensik komputer merupakan ilmu yang relatif baru, sehingga “Body of Knowledge”-nya masih sedemikian terbatas (dalam proses pencarian dengan metode “learning by doing”);
- Walaupun berada dalam rumpun ilmu forensik, namun secara prinsip memiliki sejumlah karakteristik yang sangat berbeda dengan bidang ilmu forensik lainnya – sehingga sumber ilmu dari individu maupun pusat studi sangatlah sedikit;
- Perkembangan teknologi yang sedemikian cepat, yang ditandai dengan diperkenalkannya produk-produk baru dimana secara langsung berdampak pada berkembangnya ilmu forensik komputer tesebut secara pesat, yang membutuhkan kompetensi pengetahuan dan keterampilan sejalan dengannya;
- Semakin pintar dan trampilnya para pelaku kejahatan teknologi informasi dan komunikasi yang ditandai dengan makin beragamnya dan kompleksnya jenis-jenis serangan serta kejahatan teknologi yang berkembang;
- Cukup mahalnya harga peralatan canggih dan termutakhir untuk membantu proses forensik komputer beserta laboratorium dan SDM pendukungnya;
- Secara empiris, masih banyak bersifat studi kasus (happening arts) dibandingkan dengan metodologi pengetahuan yang telah dibakukan dimana masih sedikit pelatihan dan sertifikasi yang tersedia dan ditawarkan di masyarakat;
- Sangat terbatasnya SDM pendukung yang memiliki kompetensi dan keahlian khusus di bidang forensik komputer; dan

- Pada kenyataannya, pekerjaan forensik komputer masih lebih banyak unsur seninya dibandingkan pengetahuannya (more “Art” than “Science”).

B. Objek Forensik

Dalam dunia kriminal dikenal istilah “tidak ada kejahatan yang tidak meninggalkan jejak”. Ada banyak sekali hal yang bisa menjadi petunjuk atau jejak dalam setiap tindakan kriminal yang dilakukan dengan menggunakan teknologi seperti komputer. Contohnya adalah sebagai berikut:

- Log file atau catatan aktivitas penggunaan komputer yang tersimpan secara rapi dan detail di dalam sistem;
- File yang sekilas telah terhapus secara sistem, namun secara teknikal masih bisa diambil dengan cara-cara tertentu;
- Catatan digital yang dimiliki oleh piranti pengawas trafik seperti IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System);
- Hard disk yang berisi data/informasi backup dari sistem utama;
- Rekaman email, mailing list, blog, chat, dan mode interaksi dan komunikasi lainnya;

Beraneka ragam jeis berkas file yang dibuat oleh sistem maupun aplikasi untuk membantu melakukan manajemen file (misalnya: .tmp, .dat, .txt, dan lain-lain); Rekam jejak interaksi dan trafik via internet dari satu tempat ke tempat yang lain (dengan berbasis IP address misalnya); Absensi akses server atau komputer yang dikelola oleh sistem untuk merekam setiap adanya pengguna yang login ke piranti terkait; dan lain sebagainya. Beraneka ragam jenis obyek ini selain dapat memberikan petunjuk atau jejak, dapat pula dipergunakan sebagai alat bukti awal atau informasi awal yang dapat dipergunakan oleh penyelidik maupun penyidik dalam melakukan kegiatan penelusuran terjadinya suatu peristiwa kriminal, karena hasil forensik dapat berupa petunjuk semacam:

- Lokasi fisik seorang individu ketika kejahatan sedang berlangsung (alibi);
- Alat atau piranti kejahatan yang dipergunakan;
- Sasaran atau target perilaku jahat yang direncanakan;
- Pihak mana saja yang secara langsung maupun tidak langsung terlibat dalam tindakan kriminal;
- Waktu dan durasi aktivitas kejahatan terjadi;
- Motivasi maupun perkiraan kerugian yang ditimbulkan;
- Hal-hal apa saja yang dilanggar dalam tindakan kejahatan tersebut;
- Modus operandi pelaksanaan aktivitas kejahatan; dan lain sebagainya.

C. Tahapan Aktivitas Forensik

Secara metodologis, terdapat paling tidak 14 (empat belas) tahapan yang perlu dilakukan dalam aktivitas forensik, sebagai berikut:

1. Pernyataan Terjadinya Kejahatan Komputer – merupakan tahap dimana secara formal pihak yang berkepentingan melaporkan telah terjadinya suatu aktivitas kejahatan berbasis komputer;

2. Pengumpulan Petunjuk atau Bukti Awal – merupakan tahap dimana ahli forensik mengumpulkan semua petunjuk atau bukti awal yang dapat dipergunakan sebagai bahan kajian forensik, baik yang bersifat tangible maupun intangible;
3. Penerbitan Surat Pengadilan – merupakan tahap dimana sesuai dengan peraturan dan perundang-undangan yang berlaku, pihak pengadilan memberikan ijin resmi kepada penyelidik maupun penyidik untuk melakukan aktiivitas terkait dengan pengolahan tempat kejadian perkara, baik yang bersifat fisik maupun maya;
4. Pelaksanaan Prosedur Tanggapan Dini – merupakan tahap dimana ahli forensik melakukan serangkaian prosedur pengamanan tempat kejadian perkara, baik fisik maupun maya, agar steril dan tidak tercemar/terkontaminasi, sehingga dapat dianggap sah dalam pencarian barang-barang bukti;
5. Pembekuan Barang Bukti pada Lokasi Kejahatan – merupakan tahap dimana seluruh barang bukti yang ada diambil, disita, dan/atau dibekukan melalui teknik formal tertentu;
6. Pemindahan Bukti ke Laboratorium Forensik – merupakan tahap dimana dilakukan transfer barang bukti dari tempat kejadian perkara ke laboratorium tempat dilakukannya analisa forensik;
7. Pembuatan Salinan “2 Bit Stream” terhadap Barang Bukti – merupakan tahap dimana dilakukan proses duplikasi barang bukti ke dalam bentuk salinan yang identik;
8. Pengembangan “MD5 Checksum” Barang Bukti – merupakan tahap untuk memastikan tidak adanya kontaminasi atau perubahan kondisi terhadap barang bukti yang ada;
9. Penyiapan Rantai Posesi Barang Bukti – merupakan tahap menentukan pengalihan tanggung jawab dan kepemilikan barang bukti asli maupun duplikasi dari satu wilayah otoritas ke yang lainnya;
10. Penyimpanan Barang Bukti Asli di Tempat Aman – merupakan tahap penyimpanan barang bukti asli (original) di tempat yang aman dan sesuai dengan persyratan teknis tertentu untuk menjaga keasliannya;
11. Analisa Barang Bukti Salinan – merupakan tahap dimana ahli forensik melakuka analisa secara detail terhadap salinan barang-brang bukti yang dikumpulkan untuk mendapatkan kesimpulan terkait dengan seluk beluk terjadinya kejahatan;
12. Pembuatan Laporan Forensik – merupakan tahap dimana ahli forensik menyimpulkan secara detail hal-hal yang terjadi seputar aktivititas kejahatan yang dianalisa berdasarkan fakta forensik yang ada;
13. Penyerahan Hasil Laporan Analisa – merupakan tahap dimana secara resmi dokumen rahasia hasil forensik komputer diserahkan kepada pihak yang berwajib; dan
14. Penyertaan dalam Proses Pengadilan – merupakan tahap dimana ahli forensik menjadi saksi di pengadilan terkait dengan kejahatan yang terjadi

Tugas Keamanan Jaringan Komputer “Komputer Forensik”

Pada komputer forensik, informasi yang di kumpulkan di dapat dari data atau file yang ada di lokasi yang dapat membantu dan mendukung penyelidikan. Pelaku dapat menyembunyikan suatu informasi pada suatu file. Untuk mendapatkan informasi yang tersembunyi pada suatu file di linux dapat menggunakan aplikasi Autopsy, foremost, string. Ghex, dll.

Di bawah ini terdapat kasus yang harus di selesaikan oleh praktikan guna menjawab pertanyaan dari kasus ini.

KASUS

Telah tertangkap seorang pengedar narkoba kelas kakap, polisi kesulitan untuk melakukan pengungkapan secara menyeluruh terhadap jaringan pengedar karena minimnya informasi yang tersedia, kita di minta bantuan oleh polisi untuk melakukan forensic terhadap file yang di temukan pada harddrive pelaku guna mendapatkan informasi lebih lanjut.

Kita di minta untuk mendapatkan beberapa informasi di bawah ini:

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?

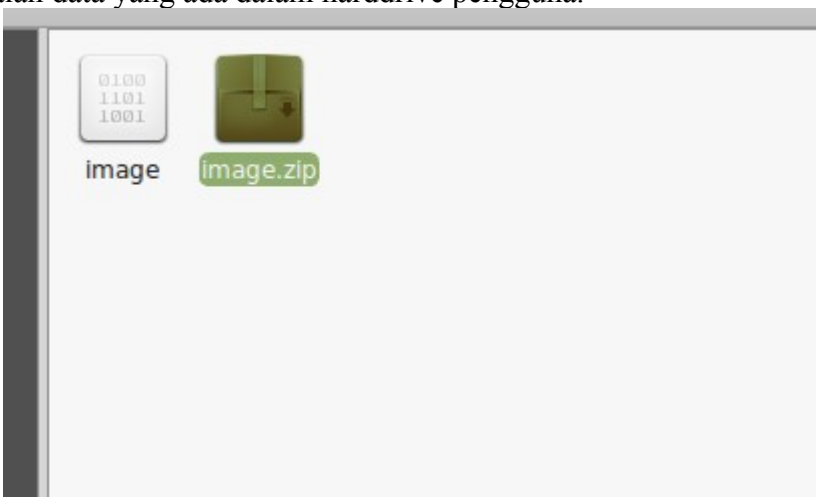
3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?

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

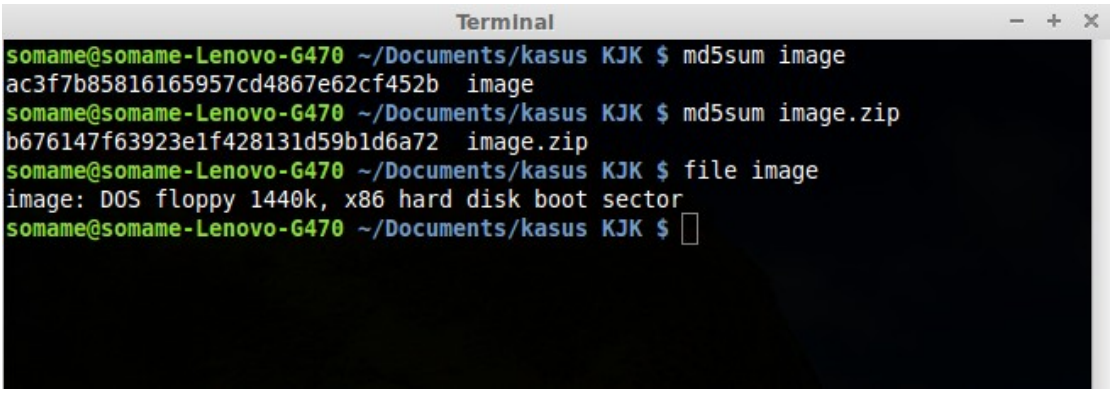
5. What processes did you (the investigator) use to successfully examine the entire contents of each file?

Tugas Keamanan Jaringan Komputer “Komputer Forensik”

Berikut adalah data yang ada dalam harddrive pengguna.

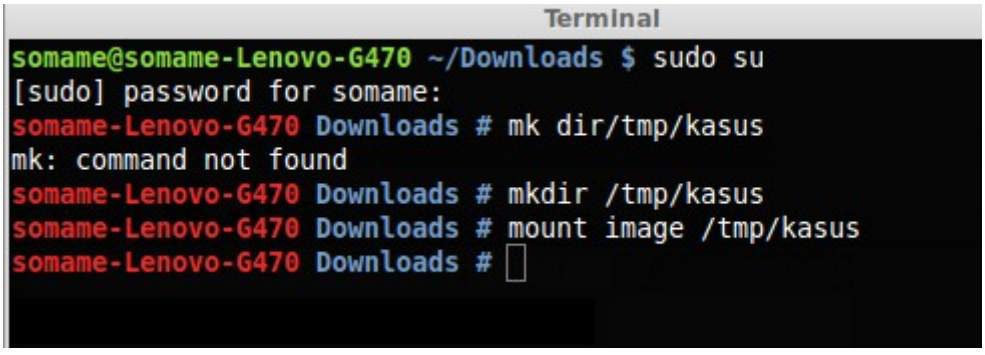


Gambar file yang terdapat pada harddrive pelaku dengan nama image

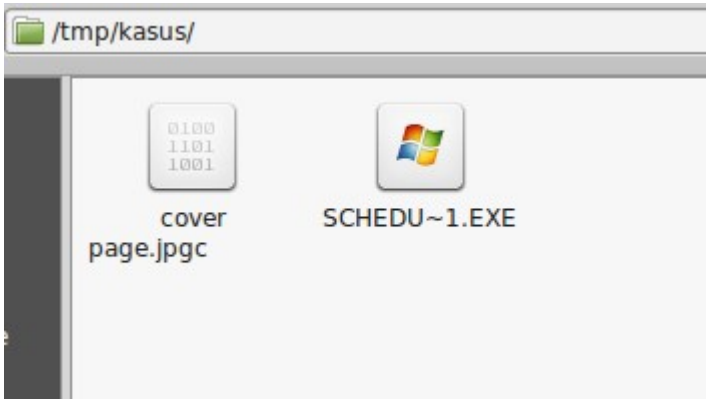


MD5 (Message-Digest algortihm 5) didesain sebagai fungsi khas kriptografi untuk keperluan keamanan data], dan bisa juga digunakan untuk mengecek integritas file. Karakter-karakter aneh di belakang merupakan MD5 yang berfungsi untuk memastikan bahwa data tidak korup pada saat memindahkan file. Jika di ubah satu bit saja isi dari suatu file maka MD5 data tersebut akan berubah sehingga akan di ketahui jika ada perubahan pada data termasuk korup.

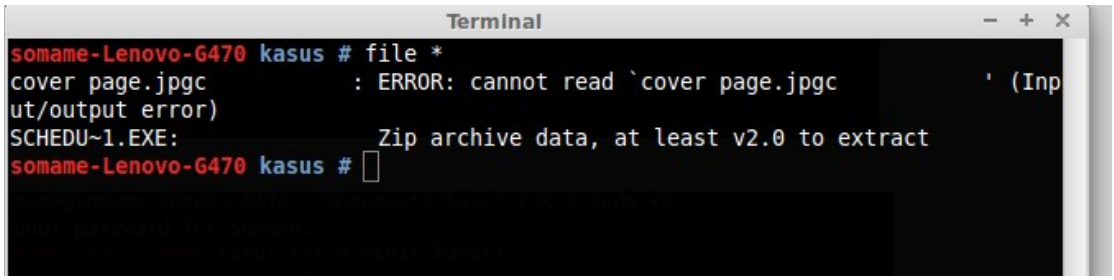
Perintah file pada $file image berfungsi untuk melihat format dari file tersebut dan informasi mengenail file tersebut. Dengan perintah file ini maka di dapat informasi bahwa file tersebut merupakan DOS floppy disk1440k. X86 harddisk boot sector.



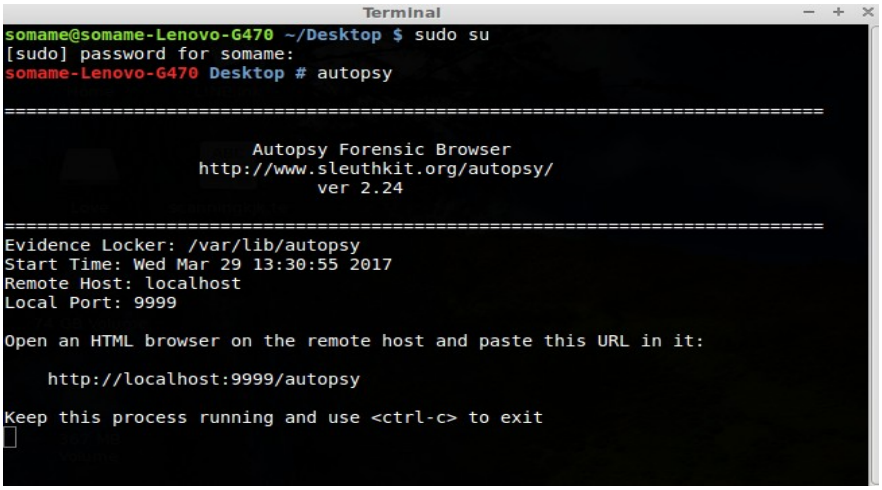
Selanjutnya kita buat folder tempat dimana informasi dari data ini akan di cari. Supaya kita tidak bingung dan data tidak hilang atau lupa menyimpan. Kemudian kita mount file image tadi kedalam folder kasus.



Setelah di mounting ternyata terdapat 2 file hasil dari mounting file image yang merupakan DOS floppy disk1440k. X86 harddisk boot sector tadi. 2 file tersebut yaitu cover page.jpgc dan SCHEDU~1.EXE. Selanjutnya kita harus mengecek file tersebut dengan perinta $file * untuk mengecek seluruh file yang ada di dalam folder td

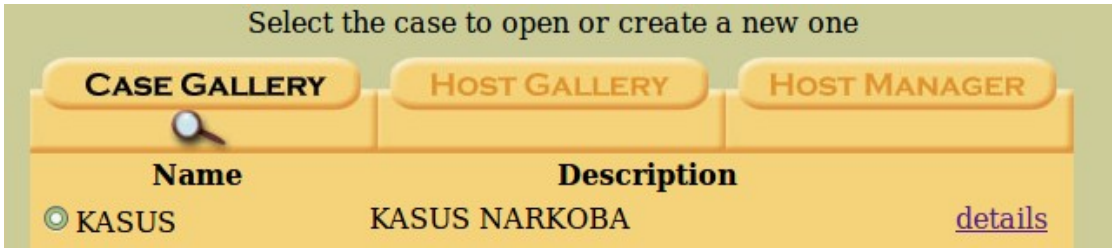


setelah di ketikkan perintah $file *, file dengan nama cover page.jpgc erro tidak bisa di baca sedangkan file dengan nama CHEDU~1.EXE merupakan file berbentuk archive. Selanjutnya kita akan mengidentifikasi file cover page.jpgc karena data tersebut error pada saat kita ingin menlihat file tersebut. Kita akan menggunakan aplikasi atau tools autopsy. Autopsy adalah tools yang di buat menggunakan bahasa perl yang dapat di gunakan untuk melakukan digital forensik, autopsy dapat melakukan analisa terhadap disk image serta partition.

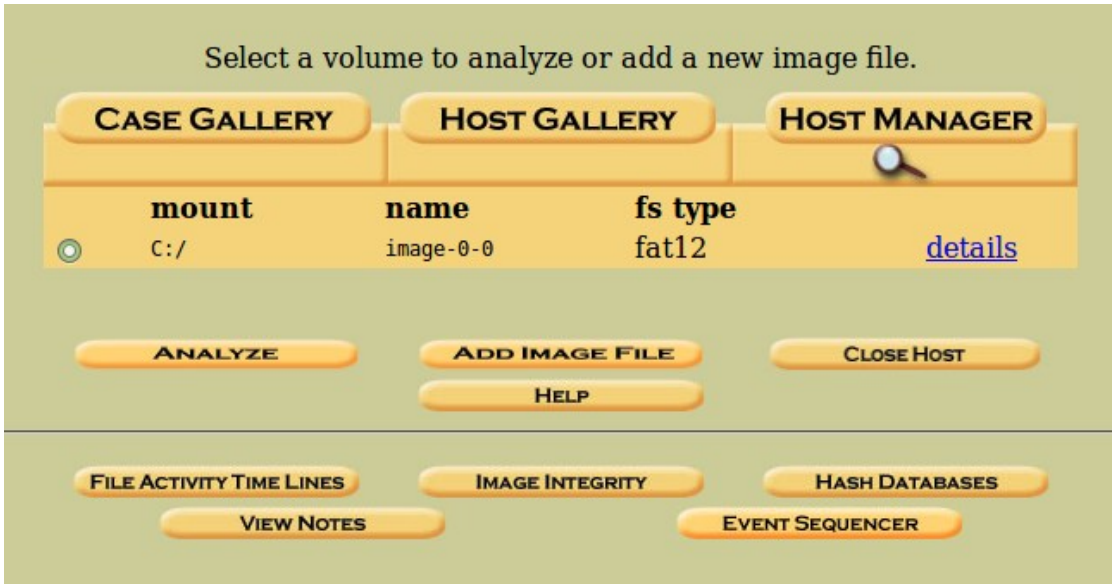


Saat kita menjalankan tools autopsy pada terminal kita akan di perintahkan untuk membuka alamat http://localhost:9999/autopsy. Berikut tampilannya pada web browser.

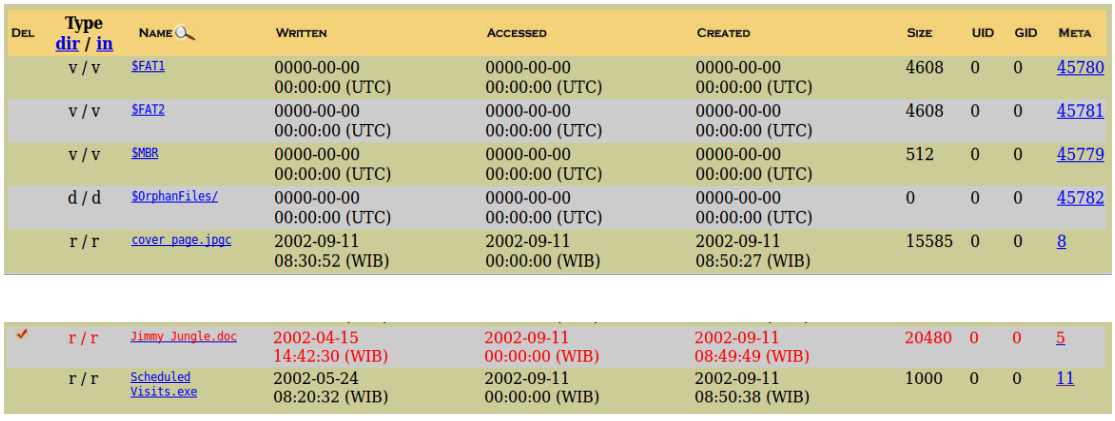
Pada aplikasi ini kita akan melakukan segistrasi atau menginput kasus yang akan kita analisa.



Gambar hasil inputan kasus dengan nama KASUS dan deskipsi KASUS NARKOBA

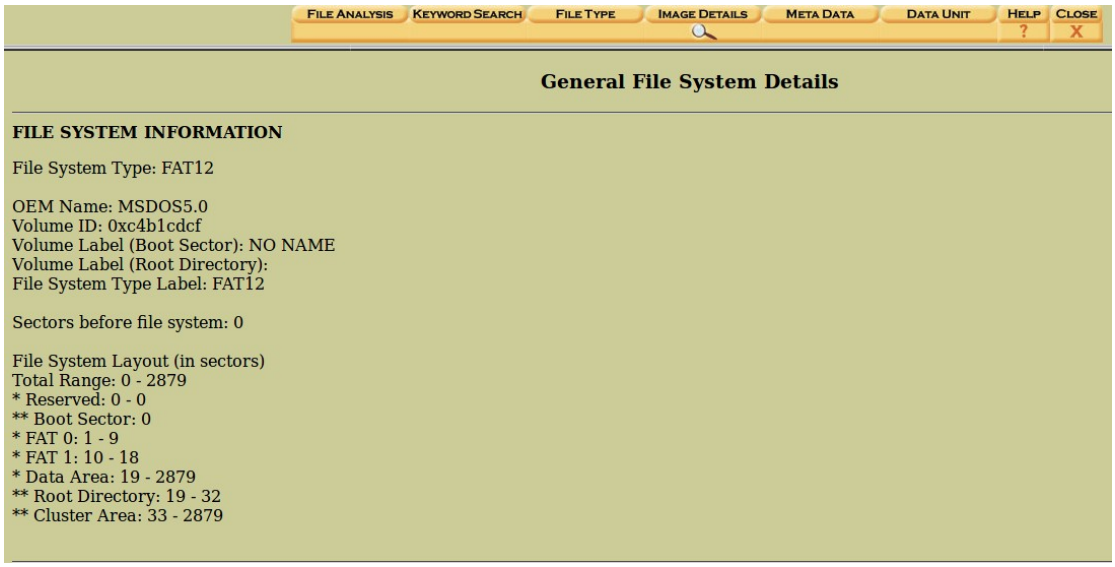


Berikut hasil inputan file yangakan kita analisa. Kita akan menganalisa file tersebut. Tekan tombol analyze.

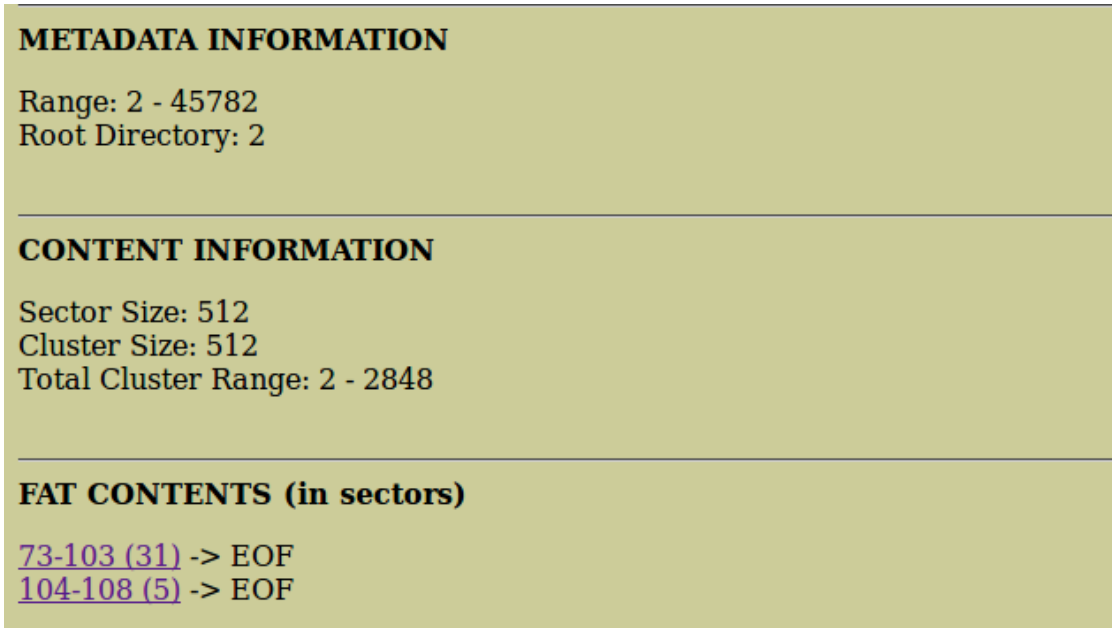


DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	v / v	$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45780
	v / v	$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45781
	v / v	$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	45779
	d / d	$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	45782
	r / r	cover page.jpgc	2002-09-11 08:30:52 (WIB)	2002-09-11 00:00:00 (WIB)	2002-09-11 08:50:27 (WIB)	15585	0	0	8
✓	r / r	Jimmy Jungle.doc	2002-04-15 14:42:30 (WIB)	2002-09-11 00:00:00 (WIB)	2002-09-11 08:49:49 (WIB)	20480	0	0	5
	r / r	Scheduled Visits.exe	2002-05-24 08:20:32 (WIB)	2002-09-11 00:00:00 (WIB)	2002-09-11 08:50:38 (WIB)	1000	0	0	11

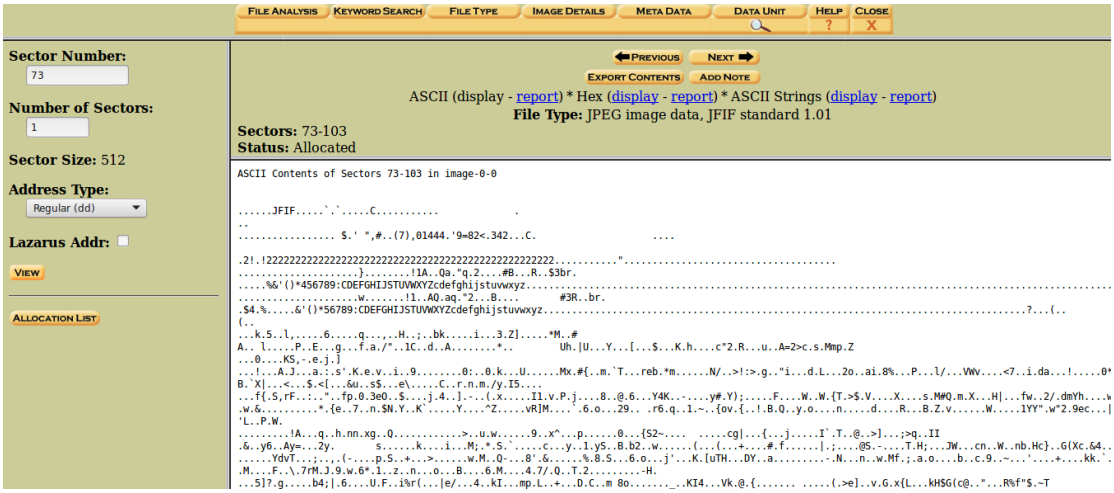
Setelah kita menekan tombol analyze, saat kita tekan menu file analysis, terdapat tabel dengan 7 daftar nama-nama keterangan dari file yang kita analisa. Dari ke 7 daftar tersebut terdapat 3 file dengan 2 berwarna biru yaitu cover page.jpgc dan SCHEDU~1.EXE. Dan satu berwarna merah dengan nama file Jimmy Jungle.doc. Kedua nama file yang berwarna biru tadi telah kita dapatkan saat melakukan mount pada file yang kita analisa. Namun file yang berwarna merah menandakan bahwa file telah di hapus. Selanjutnya kita akan mengembalikan file yang telah di hapus tadi karena kemungkinan mengandung informasi yang dapat membantu menyelesaikan kasus ini. Selanjutnya kita ke menu image detail.



Pada menu ini kita dapat mengetahui secara detail data yang sedang kita analisa seperti pada gambar di atas.



Kita fokus pada bagian FAT CONTENTS (in sector) karena bagian ini akan kita analisa. Terdapat 2 bagian yaitu 73-103 (31) dan 104-108 (5). untuk pertama kita akan menganalisa sector 73-103 (31) kita akan mulai dengan mengkliknya.

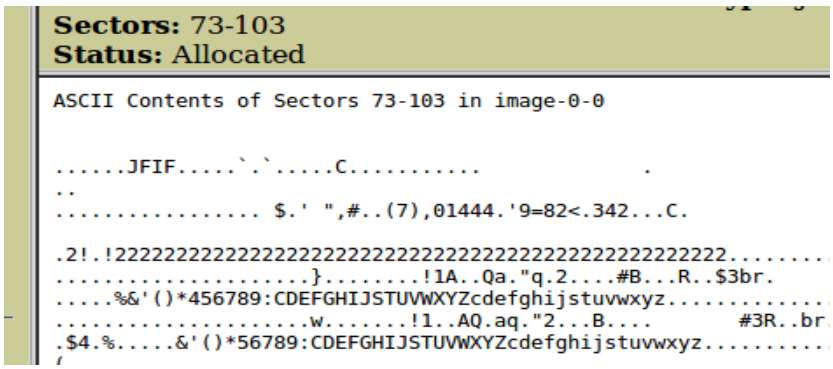


Gambar tampilan image detail pada sector 73-103. dapat kita lihat kode ascii dari sector tersebu.

Kode ASCII di atas adalah signature dari file sector 73-103. signature file adalah data yang di gunakan untuk mengidentifikasi atau memverifikasi isi file. Secara umum signature file merujuk pada dua pengertian yaitu File Magic Number yaitu byte didalam file yang digunakan untuk mengidentifikasi format dari sebuah file, biasanya dapat diidentifikasi pada bagian dari awal dari sebuah file. Ukurannya berkisar antara 2-4 byte dan File Cheksum umumnya digunakan sebagai hasil dari sebuah fungsi Hash dari file content. File Checkcum terutama digunakan untuk melakukan verifikasi integritas file dari error transmisi atau dari serangan. Signature jenis file checksum ini akan ditempatkan pada awal / akhir file atau dapat pula pada file yang terpisah.

Dari gambar di atas analisa yang kita lakukan lebih ke File Magic Number dari data yang kita analisa karena kode ASCII yang seperti pada gambar di atas. Kita dapat melihat list dari signature file dengan meggunakan google untuk membantu menganalisa file yang kita analisa.

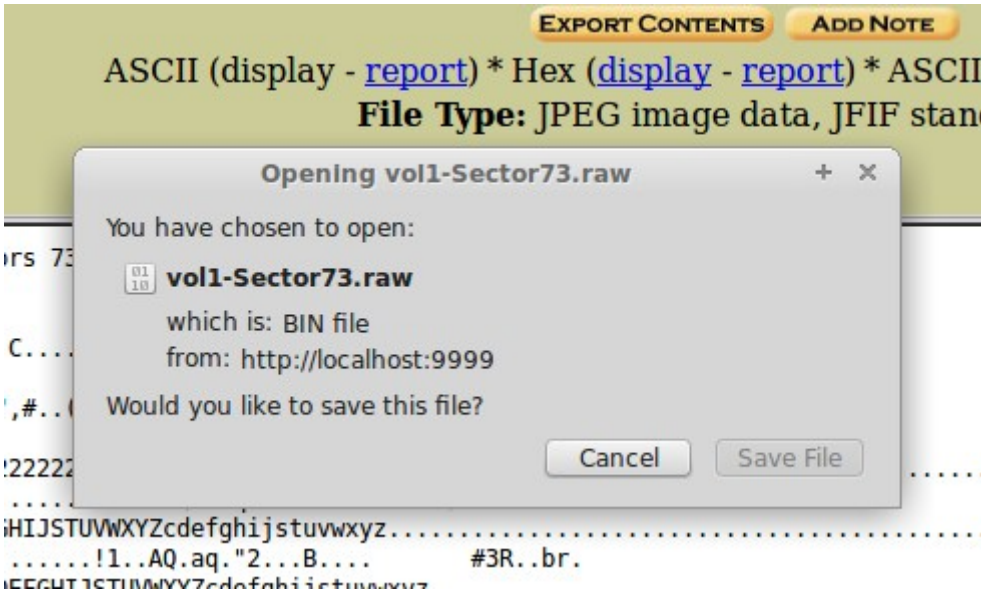
Pertama kita fokus ke bit awal pada gambar ASCII sector 73-103 tadi.



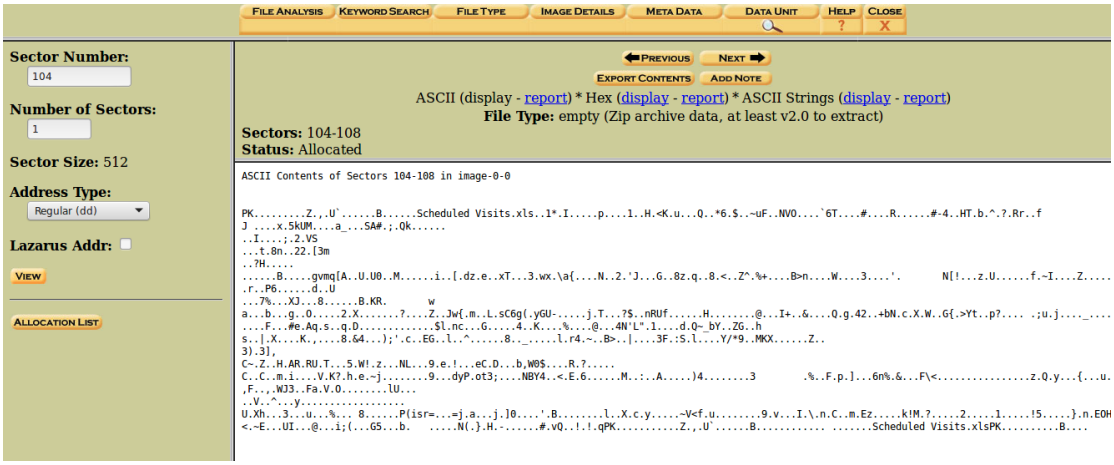
Dari kode ASCII sector 73-103 pada bit awal terdapat 6 simbol titik kemudian magic number-nya yaitu JFIF. Keenam titik-titik tersebut adalah karakter namun karakter yang tidak bisa di baca. Kita fokus pada JFIF.

jpg jpeg	JPEG raw or in the JFIF or Exif file format

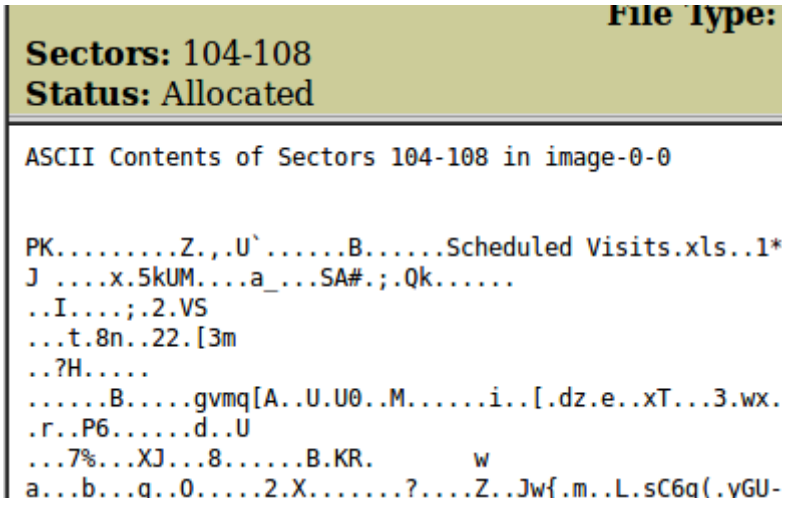
Gambar diatas adalah list signatures file yang terdapat pada situs https://en.wikipedia.org/wiki/List_of_file_signatures. Dari list tersebut di nyatakan bahwa file yang memiliki description FIF adalah file dengan ekstensi JPG atau JPEG. Lalu klik export contents dan download filenya. Kita mendapatkan file dengan nama vol1-sector73.raw.



Untuk selanjutnya kita ke sektor yang ke dua yaitu sector 104-108. Dapat kita lihat detail contens ASCII dari sector 104-108.



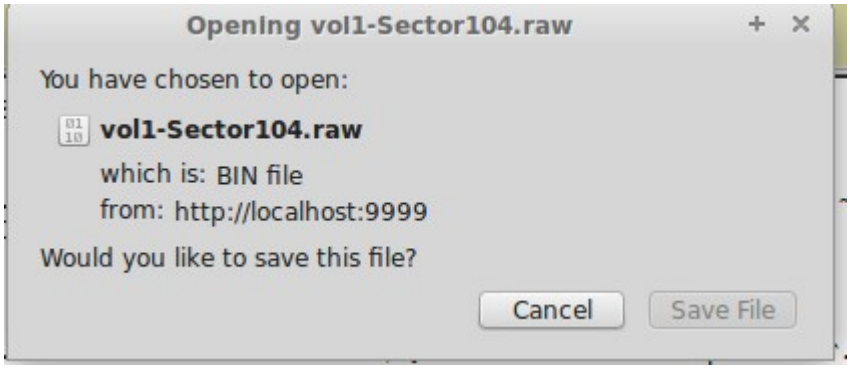
Sama seperti pada sector 73-103 tadi. Kita fokus pada magic number dari sector ini dengan melihat bit awal pada kode ASCII-nya.



Pada gambar di atas dapat kita lihat bahwa pada sector 104-108 bit awalnya PK. Selanjutnya kita ke list signatures file pada situs yang kita buka tadi.

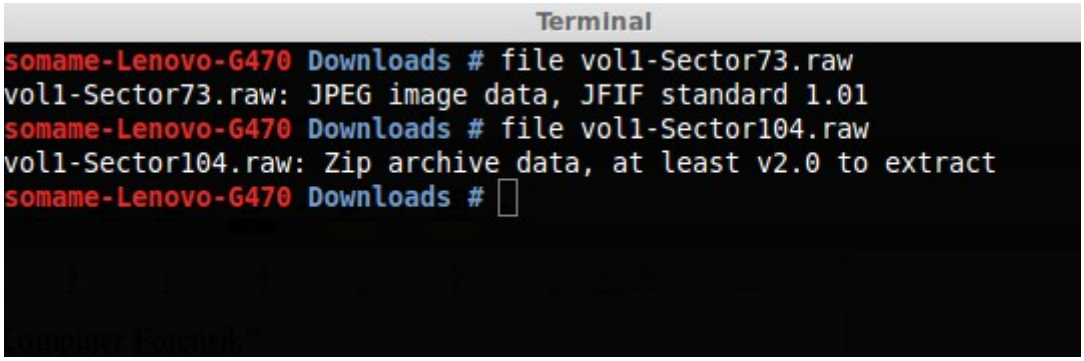
zip jar odt ods odp docx xlsx pptx vsdx apk	zip file format and formats based on it, such as JAR, ODF, OOXML	0	PK..

Dari list tersebut dapat kita lihat bahwa file pada sector ini memiliki ekstensi ZIP, JAR, ODR, dll. Selanjutnya kita eksport contents dan kita akan mendapatkan file dengan nama vol1-sector104.raw.



Berikut hasil dari contents ASCII yang kita eksport tadi. Pada analisa sebelumnya kita megetahui ekstensi dari kedua file ini. Untuk file dengan nama vol-sector73.raw berkemungkinan memiliki ekstensi jpg atau jpeg sedangkan file dengan nama vol1-sector104.raw memiliki banyak kemungkinan ekstensi yaitu ZIP, APK,

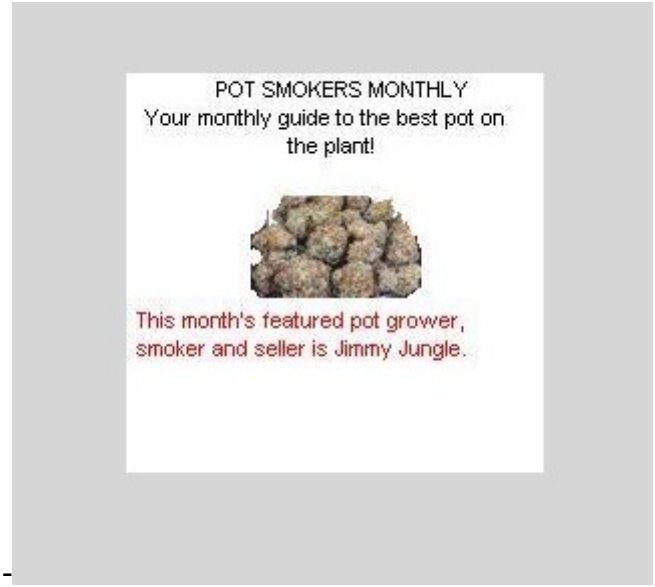
ODR, dll. Untuk mengetahui detail mengenai file ini kita mengidetifikasi kedua file seperti pada gambar di bawah ini.



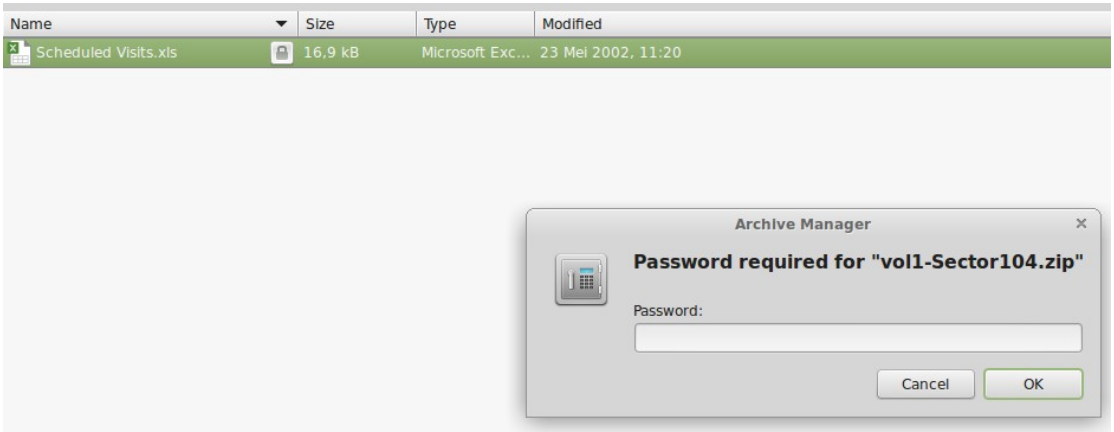
Melalui perintah $file * dapat kita lihat bahwa file dengan nama vol1-sector73.raw memiliki format file JPEG dan file dengan nama vol1-sector104.raw memiliki format file zip. Selanjutnya kedua file kita rename formatnya sesuai dengan format file sebenarnya yang kita dapatkan tadi.

Dapat kita lihat dari kedua file yang telah kita ubah formatnya menunjukkan pada file dengan nama vol-sector73 adalah gambar dan file dengan nama vol1-sector104 adalah file zip.

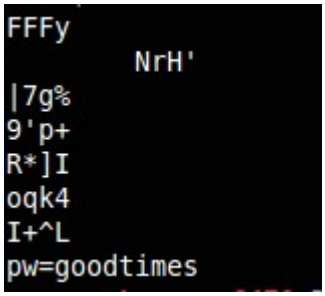
Tugas Keamanan Jaringan Komputer “Komputer Forensik”



File vol1-sector73 merupakan gambar iklan dari pot yang kemungkinan di gunakan untuk menanam tanaman narkoba. Dari gambar tersebut kita mendapatkan nama penjual sekaligus pemakainya adalah Jimmy Jungle. Nama ini terdapat pada file analysis pada autopsy yang merupakan nama file yang hilang.



Pada file vol1-sector104 yang merupakan file archive saat di buka terdapat file di dalamnya dengan nama Scheduled Visits dengan format exel. Saat ingin membuka file ternyata file tersebut meminta password. Password dari file ini adalah karakter yang kemungkinan dapat di sembunyikan. Selanjutnya kita akan menggunakan tools string. Tools ini berfungsi untuk menunjukkan karakter-karakter simbol dari file dalam bentuk gambar yang kemungkinan di dalamnya terdapat informasi. Kita string file vol1-sector73.jpeg dengan perintah $strings vol1-sector73.jpeg.



Setelah kita menjalankan perintah tersebut kita mendapatkan informasi pasword yaitu goodtimes dan kemungkinan dapat di gunakan untuk membuka file zip tadi.

A	B	C
Month	**DAY**	**HIGH SCHOOLS**
2002		
April	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leetch High School (C)
	Thursday (4)	Birard High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hull High School (F)
	Tuesday (2)	Smith Hill High School (A)
	Wednesday (3)	Key High School (B)
	Thursday (4)	Leetch High School (C)
	Friday (5)	Birard High School (D)
	Monday (1)	Richter High School (E)
	Tuesday (2)	Hull High School (F)
	Wednesday (3)	Smith Hill High School (A)
	Thursday (4)	Key High School (B)
	Friday (5)	Leetch High School (C)
	Monday (1)	Birard High School (D)
	Tuesday (2)	Richter High School (E)
	Wednesday (3)	Hull High School (F)
	Thursday (4)	Smith Hill High School (A)
	Friday (5)	Key High School (B)
	Monday (1)	Leetch High School (C)
	Tuesday (2)	Birard High School (D)
May		
	Wednesday (3)	Richter High School (E)
	Thursday (4)	Hull High School (F)
	Friday (5)	Smith Hill High School (A)
	Monday (1)	Key High School (B)
	Tuesday (2)	Leetch High School (C)

Setelah di maasukkan password yang kita dapatkan tadi dan ternyata benar di file schedul visits terbuka. Isi dari file tersebut adalah jadwal nama-nama tempat yang di kunjungi untuk pengedaran pot tadi.

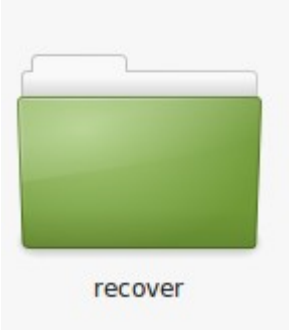
r / r	Scheduled Visits.exe	2002-05-24 08:20:32 (WIB)	2002-09-11 00:00:00 (WIB)	2002-09-11 08:50:38 (WIB)	1000	0	0	11

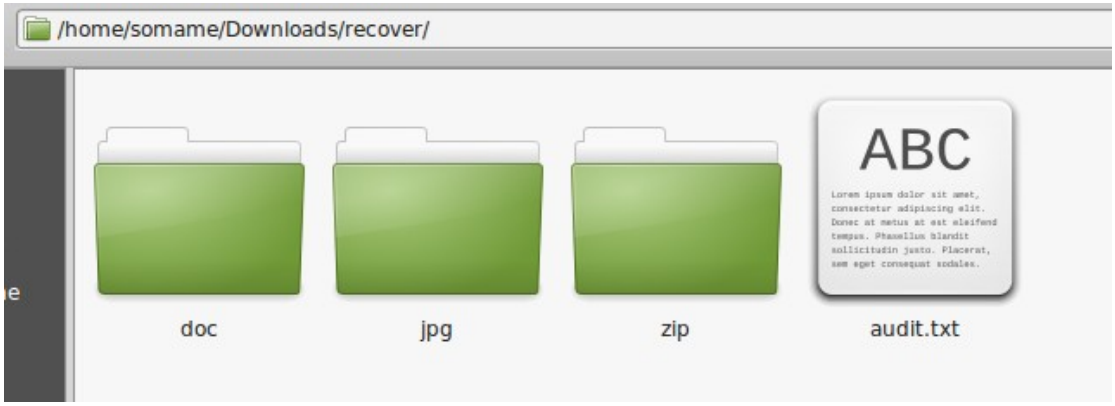
Selanjutnya kita kembali file analysis pada autopsy dan fokus pada file scheduled visits kemudian klik angka 11 pada kolom terakhir. Maka dapat kita lihat informasi detail dari file tesebut.

Pada file analysis tadi dapat kita ketahui bahwa terdapat 1 file yang sudah di hapus. Kita akan mengembalikan file ini dengan menggunakan tools foremost.

```
somame-Lenovo-G470 Downloads # foremost -v -i image -o recover
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Wed Mar 29 14:43:46 2017
Invocation: foremost -v -i image -o recover
Output directory: /home/somame/Downloads/recover
Configuration file: /etc/foremost.conf
Processing: image
|------------------------------------------------------------------
File: image
Start: Wed Mar 29 14:43:46 2017
Length: 1 MB (1474560 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

0:      00000073.jpg           8 KB           37376
1:      00000033.doc          21 KB           16896
foundat=Scheduled Visits.xls??1*?I
                                  ?p??1??<K?uq?Q??*6?$?uF??NVO???`6T??.#??
?R??3?#-4??T?b?^?2?Rr??f
J ???x?5kUM????a_??SA#?;?Qk? ??
??I?1??;?2?VS
2:      00000104.zip           2 KB           53248
*|
Finish: Wed Mar 29 14:43:46 2017

3 FILES EXTRACTED

jpg:= 1
ole:= 1
zip:= 1
------------------------------------------------------------------

Foremost finished at Wed Mar 29 14:43:46 2017
```

Pada gambar di atas dapat kita lihat setelah kita menggunakan tools foremost dan mengembalikan file yang hilang tadi terdapat 3 file yaitu jpeg, ole, dan zip. Dan akan ada folder baru dengan nama recover yang berisi data pada file image yang kita analisa tadi.





Di dalam foder recover tersebut terdapat 3 folder yaitu folder doc, jpg, dan zip. Pada folder jpg berisi file gambar yang sama persis seperti file vol1-sector73 dan folder zip berisi file zip yang sama persis dengan file vol1-sector104 dimana isi dari file zip tersebut adalah jadwal kunjungan dan tempat pengedaran alat pot memelihara narkoba. Kemudian folder dengan nama doc berisi file dengan format dokumen.

Tugas Keamanan Jaringan Komputer “Komputer Forensik”

Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

Jimmy:

Dude, your pot must be the best – it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your soil when you plant the marijuana seeds? At least I know your growing it and not some guy in Columbia.

These kids, they tell me marijuana isn’t addictive, but they don’t stop buying from me. Man, I’m sure glad you told me about targeting the high school students. You must have some experience. It’s like a guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I’m an entrepreneur. Am I only one you sell to? Maybe I can become distributor of the year!

I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you think. To open it, use the same password that you sent me before with that file. Talk to you later.

Thanks,

Joe

Isi dari file deokumen tersebut adalah surat perintah dari jimmy jungle kepada joe jacob.

Dari semua data yang telah kita dapat maka kita dapat menjawab semua pertanyaan dari kasus di atas. Mulai dari siapa supliarnya yaitu jimmy jungle dan alamatnya serta tempat-tempat dan jadwal yang di kunjungi untuk pengedaran alat tersebut.

Teknik yang di gunakan oleh pelaku adalah teknik steganografi yaitu menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Pengirim mengubah format file sehingga tidak dapat di ubah kemudian terdapat data yang di hapus lalu file pada arcive di beri password dimana sandi dari password tersebut terdapat pada karakter file image.

Tugas Keamanan Jaringan Komputer “Komputer Forensik”