KEAMANAN JARINGAN KOMPUTER

“COMPUTER FORENSICS”

OLEH :

AGUS JULIANSYAH

09011181320034

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

Definisi komputer forensik

Komputer Forensik merupakan salah satu cabang ilmu forensik yang berhubungan dengan bukti hukum yang ditemukan dalam komputer maupun media penyimpanan secara digital. Komputer forensik ini dikenal sebagai Digital Forensik. Banyak bidang ilmu yang dimanfaatkan dan dilibatkan pada suatu kasus kejahatan atau kriminal untuk suatu kepentingan hukum dan keadilan, dimana ilmu pengetahuan tersebut dikenal dengan ilmu forensic.

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 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

Tahapan pada Komputer Forensik

Terdapat empat fase dalam komputer forensik, antara lain yaitu:

Pengumpulan Data, Pengumpulan data yang tujuannya mengidentifikasi berbagai sumber daya yang dianggap urgent dan bagaimana seluruh data dapat terhimpun dengan baik. Pengujian, Pengujian mencakup suatu proses penilaian dan memilah berbagai informasi yang sesuai dari semua data yang telah dikumpulkan, juga bypassing proses atau meminimalisasi berbagai fitur dalam sistem operasi dan aplikasi yang bisa menghilangkan data, seperti enkripsi, kompresi, akses mekanisme kontrol, mengalokasi file, pemeriksanan pemetaanmeta data, mengekstrak file,dan lain – lain.

Analisis, Yang dapat dilakukan dengan berbagai pendekatan metode. Tugas dari analisis ini mencakup banyak kegiatan, seperti mengidentifikasi user (pengguna) yang terlibat secara tak langsung, lokasi, kejadiaan, perangkat, dan mempertimbangkan bagaimana caranya agar semua komponen itu saling terhubung sampai mendapatkan kesimpulan akhir.

KASUS :

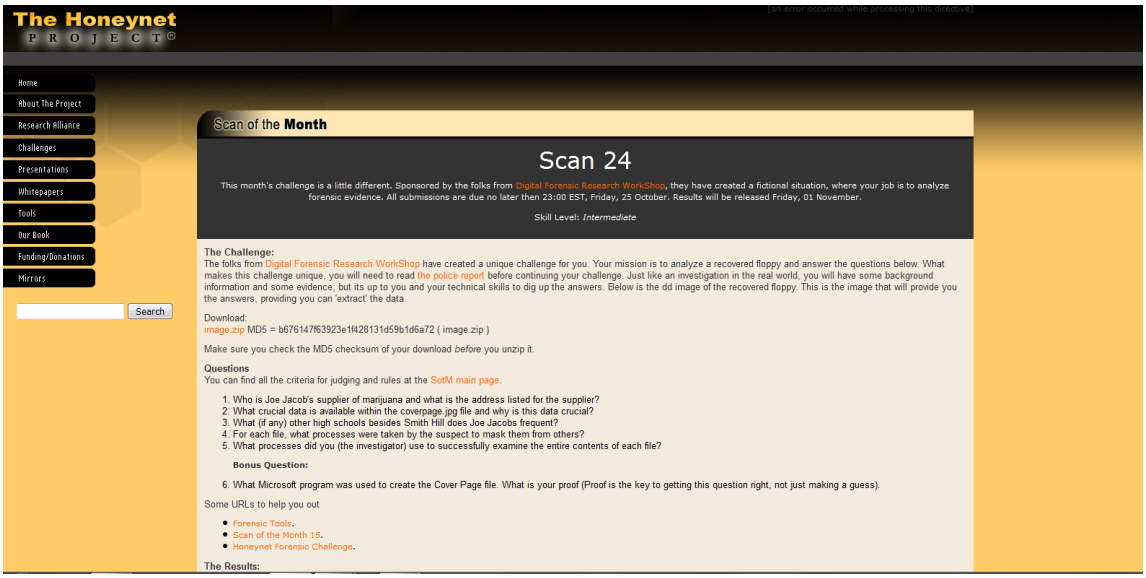
Ada seorang penegdar narkoba yang tertangkap, polisi ada harddrive yang sdah korup dr tersangka. Bagaimana kita me recover nya.

Tools :

1. Autopsy
2. Foremost
3. Strings

Langkah kerja :

1. Install tools, selain strings
2. Buka wesite berikut. File tersebut merupakan



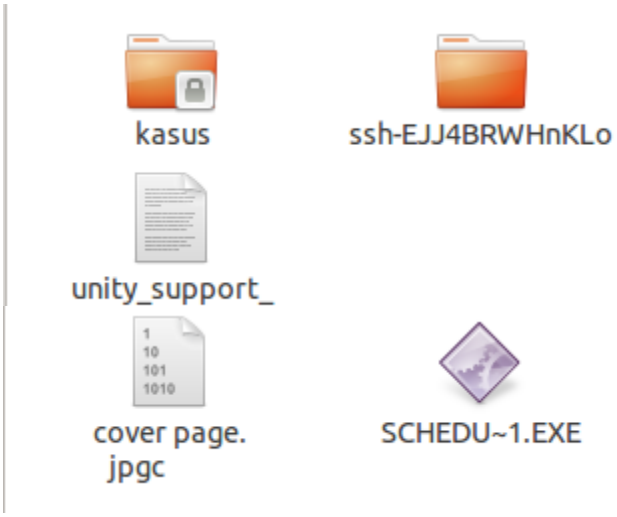
Fungsi md5sum : sebuah file pasti ada md5sum yang berfungsi untuk mengecek keaslian dari file atau integritas file

```
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#
```

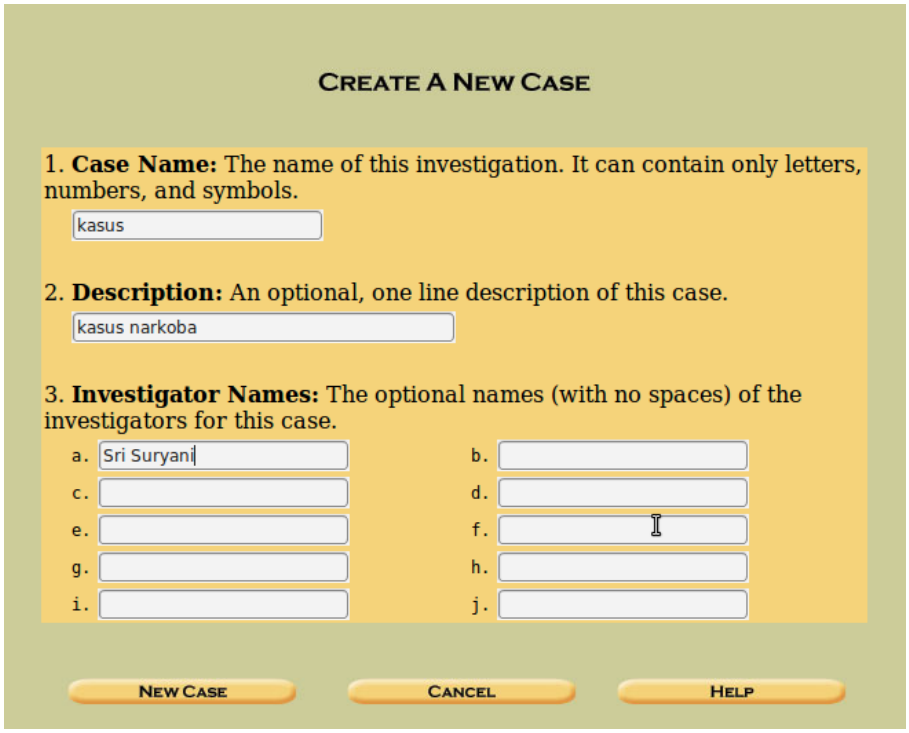
Mengecek keaslian file

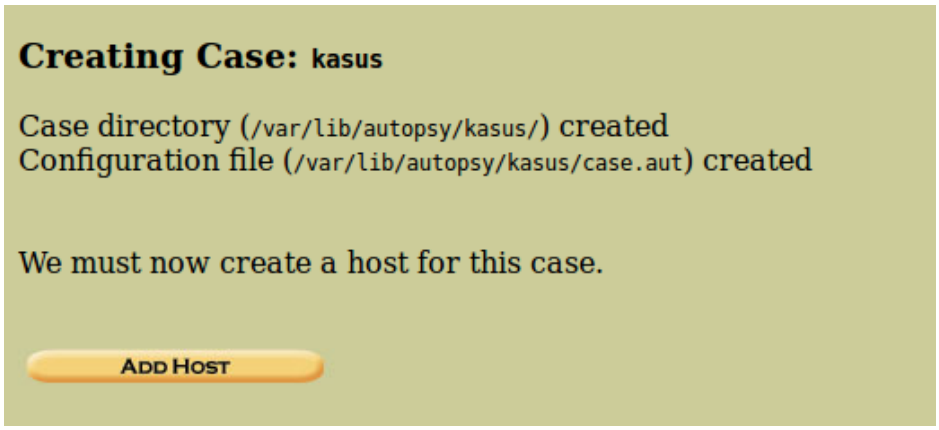
```
root@mahasiswa:/tmp/kasus# file *
cover page.jpgc           : ERROR: cannot read `cover page.jpgc
          ' (Input/output error)
SCHEDU~1.EXE:              Zip archive data, at least v2.0 to
extract
root@mahasiswa:/tmp/kasus#
```

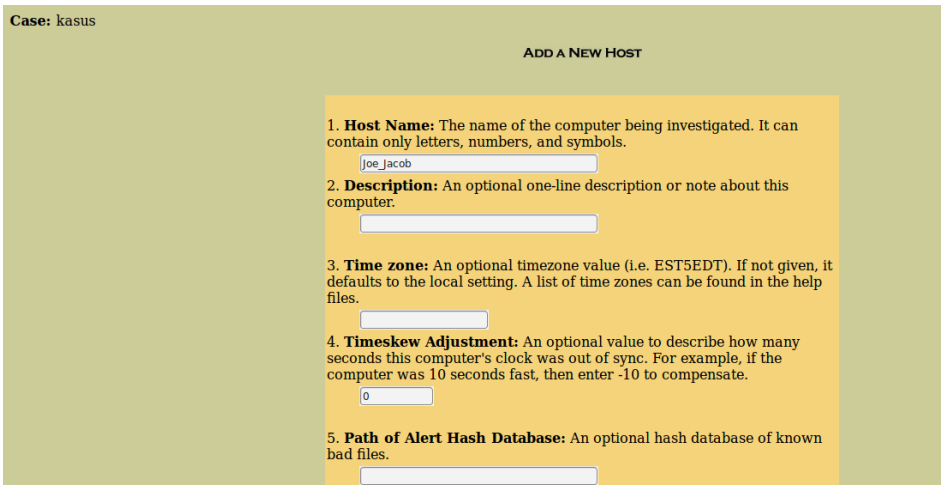
Tools psy. Karena psy menggunakan

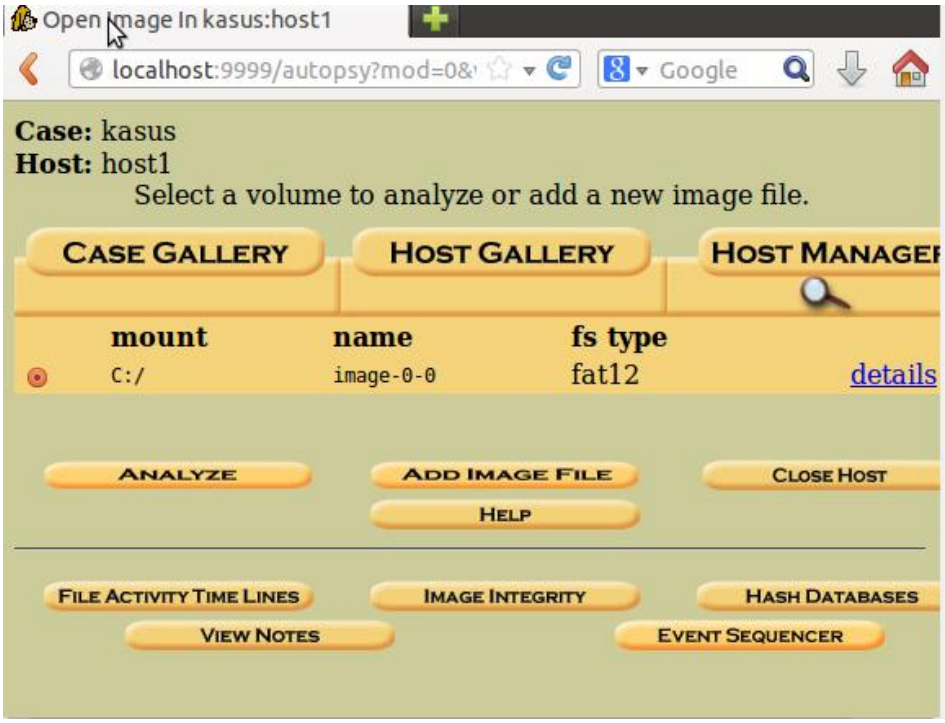
```
root@mahasiswa:/tmp/kasus# autopsy
  I
================================================================
=============

                    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

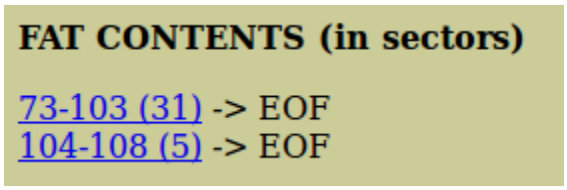

CREATE A NEW CASE
1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols.
kasus
2. Description: An optional, one line description of this case.
kasus narkoba
3. Investigator Names: The optional names (with no spaces) of the investigators for this case.
a. Sri Suryani
b.
c.
d.
e.
f.
g.
h.
i.
j.
NEW CASE
CANCEL
HELP


Creating Case: kasus
Case directory (/var/lib/autopsy/kasus/) created
Configuration file (/var/lib/autopsy/kasus/case.aut) created
We must now create a host for this case.
ADD HOST


Case: kasus
ADD A NEW HOST
1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols.
Joe_Jacob
2. Description: An optional one-line description or note about this computer.
3. Time zone: An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.
4. Timeskew Adjustment: An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.
0
5. Path of Alert Hash Database: An optional hash database of known bad files.



2 file yang bisa kita ambil



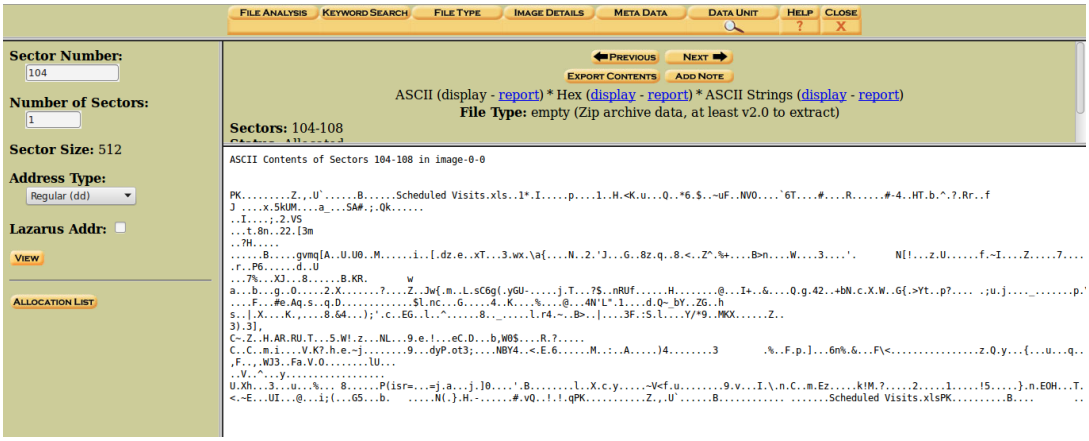
Yang 1. JfIF liat di Wikipedia

jpg jpeg	JPEG raw or in the JFIF or Exif file format	0	ÿØÿÛ	FF D8 FF DB
			ÿØÿà ..J F IF..	FF D8 FF E0 nn nn 4A 46 49 46 00 01
			ÿØÿá ..E x if..	FF D8 FF E1 nn nn 45 78 69 66 00 00

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 jd 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 pw di dalam file gambar

	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

```
srisuryani@srisuryani-Aspire-4739 ~/Unduhan $ foremost -v -i image -o recover
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Fri Mar 24 12:01:57 2017
Invocation: foremost -v -i image -o recover
Output directory: /home/srisuryani/Unduhan/recover
Configuration file: /etc/foremost.conf
Processing: image
|------------------------------------------------------------------
File: image
Start: Fri Mar 24 12:01:57 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.#
R3#-4HT0b^??Rrf
J x5kUM????a_SA#;Qk멎
I;2VS
2:      00000104.zip           2 KB           53248
*|
Finish: Fri Mar 24 12:01:57 2017

3 FILES EXTRACTED

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

Menggunakan GHex

Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

Jimmy:

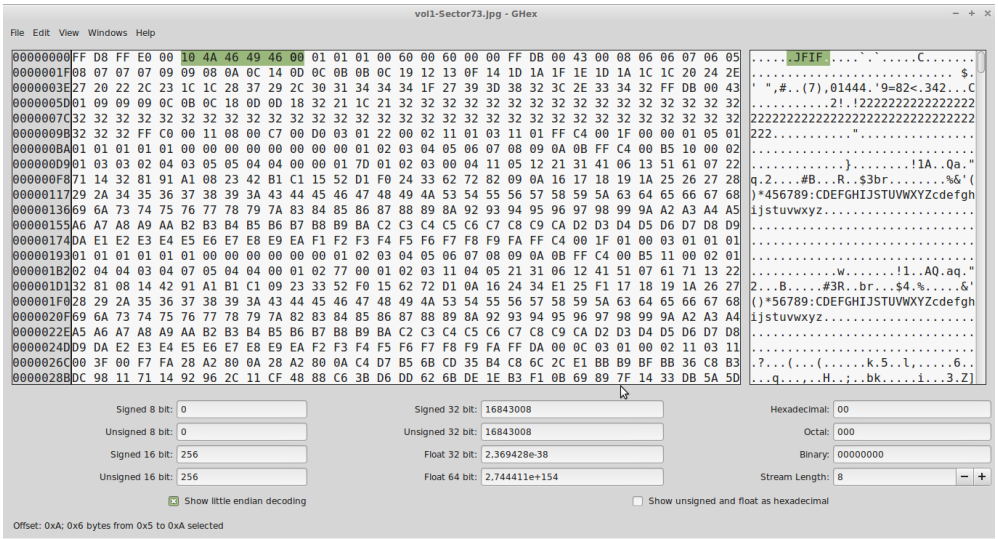
Dude, your pot must be the best – it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your soil when you plant the marijuana seeds? At least I know your growing it and not some guy in Columbia.

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




```
srisuryani-Aspire-4739 Unduhan # md5sum image.zip
b676147f63923e1f428131d59b1d6a72  image.zip
srisuryani-Aspire-4739 Unduhan #
```

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 bantuan untuk mendapatkan beberapa informasi di bawah

1.siapa adalah pemasok Joe Yakub ganja dan apa alamat yang tercantum untuk pemasok?

Jawab: Dua orang tersangka yaitu, Joe Jacob sebagai pembeli, Jimmy Jungle sebagai supplier, dan John Smith sebagai bandar narkoba

2.Apakah data penting tersedia dalam file coverpage.jpg dan mengapa data ini penting?

Jawab: Sebuah disket yang berisikan informasi tentang transaksi narkoba

3. apa (jika ada) sekolah tinggi lainnya selain Smith Bukit melakukan Joe Jacobs sering?

Jawab: 1. Smith Hill High School , 2. Key High School, 3. Leetch High School, 4. Birard High School, 5. Richter High School, 6. Hull High School, 7. 1212 Main Street Jones, 8. FL 00001, 9. Danny's Pier 12 Boat Lunch, 10. 22 Jones Ave

4.Untuk setiap file, proses apa yang di ambil oleh tersangka untuk menutupi mereka dari orang lain?

jawab: Di rektori root dan FAT akan dihapus(wipe) tetapi area data tidak terhapus karena disk telah di "Quick" diformat.

5. Proses apa kau (penyidik) menggunakan untuk berhasil memeriksa seluruh isi setiap file?

Jawab: Di rektori root dan FAT akan dihapus(wipe) tetapi area data tidak terhapus karena disk telah di "Quick" diformat.