COMPUTER FORENSICS

Secara Garis Besar, di rangkum dari berbagai sumber :

"suatu rangkaian metodologi yang terdiri dari teknik dan prosedur untuk mengumpulkan buktibukti berbasis entitas maupun piranti digital agar dapat dipergunakan secara sah sebagai alat bukti di pengadilan."

Pada praktikum kali ini akan dilakukan sebuah kegiatan Computer Forensics . dapat dilihat diatas definisi dari Computer Forensics.

Tujuan dari Computer Forensics adalah sebagai berikut

- 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.

Tools yang digunakan adalah :

- 1. Autopsy
- 2. Foremost
- 3. Strings

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.

Langkah -langkah melakukan Computer Forensics.

Install tools Autopsy dan Foremost

Buka website http://old.honeynet.org/scans/scan24/ pada browser

Download file Image.Zip

(old.honeynet.org/scans/scan24/image.zip)

md5: b676147f63923e1f428131d59b1d6a72



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

Terminal	1
File Edit View Terminal Tabs. Help	
moci-Ampire-47382 suci # cd Documents suci-Ampire-47382 Documents # nd5sun image.zip b676147163923e11428131d59b1d6a72 image.zip suci-Ampire-47582 Documents # ■	
File Edit Vew Terminal Tabs Help	
nucl-Augling-ATSE nucl # cd Documents nucl-Augling-ATSE Documents # mdSsum image.zip b676147763922e17428131d59b1d6a72 image.zip carci-Augling-ATSE Documents # file (mane zip	
image.zip: Zip archive data, at least v2.0 to extract	
Archive: image.zip inflating: image Inflating: image	
<pre>image: DOS floppy 1440k, x86 hard disk boot sector sect-Aspire-47362 Documents # </pre>	

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

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



	Terminal	- + >
File Edit View Terminal	Tabs Help	
suci@suci-Aspire-4736 suci@suci-Aspire-4736 Password: suci-Aspire-4736Z kas	Z ~ \$ cd /tmp/kasus-narkoba Z /tmp/kasus-narkoba \$ su us-narkoba # ls	
cover page.jpgc	SCHEDU~1.EXE	

Perintah untuk Mengecek keaslian file

736Z kasus-narkoba # file * cover page.jpgc ut/output error) ' (Inp : ERROR: cannot read `cover page.jpgc Zip archive data, at least v2.0 to extract SCHEDU~1.EXE: kasus-narkoba #

Kemudian jalankan Autopsy dan Mengatur hostname, siapa yang melakukan forensik pada komputer target

Terminal	- + :
<pre>suci-Aspire-4736Z kasus-narkoba # autopsy</pre>	
Autopsy Forensic Browser	
http://www.sleuthkit.org/autopsy/	
ver 2.24	
Evidence Locker: /var/lib/autopsy	
Start Time: Fri Mar 24 11:13:04 2017	
Remote Host: localhost	
Local Port: 9999	
Open an HTML browser on the remote host and paste this URL in it:	
http://localhost:9999/autopsy	
Keep this process running and use <ctrl-c> to exit</ctrl-c>	

akses autopsy dengan browser http://localhost:9999/autopsy



Pembuatan New Case

Tujuan pembuatan New Case adalah agar kita dapat mudah mengakses kasus kasus sehingga tidak tercampur dengan kasus forensic lain nya .Klik New Case

Case Name: The name	of this investigation. It	can contain o	nlv letters
umbers, and symbols.	· · · · · · · · · · · · · · · · · · ·		100000000000000000000000000000000000000
kasus			
. Description: An option	nal, one line description	of this case.	
kasus narkoba			
kasus narkoba			
kasus narkoba	The optional names (with	n no spaces) (of the
kasus narkoba . Investigator Names: ivestigators for this case	The optional names (with	h no spaces) (of the
kasus narkoba Investigator Names: nvestigators for this case a. Suci Anggraeni	The optional names (with	h no spaces) (of the
kasus narkoba Investigator Names: nvestigators for this case a. Suci Anggraeni c.	The optional names (with	h no spaces) (of the
kasus narkoba . Investigator Names: westigators for this case a. Suci Anggraeni c. e.	The optional names (with . b. d. d. f.	n no spaces) (I	of the
kasus narkoba Investigator Names: hvestigators for this case a. Suci Anggraeni c. e. g.	The optional names (with b. d. f.	n no spaces) (I	of the
kasus narkoba Investigator Names: nvestigators for this case a. Suci Anggraeni c. e. g. j.	The optional names (with b. d. f. h.	n no spaces) (I	of the

isikan Case Name hingga Investigator Name nya sesuai keinginan. lalu klik lagi New Case, setelah itu langsung saja klik Add Host pada Creating Case.

Membuat Host Baru

Pada step ADD NEW HOST isi Host Name terserah contoh nya Forensic1,



Menambahkan Image File

Klik Add Image file



Pada form Location masukan lokasi dari image file yang ingin dilakukan forensi.

Case: kasus Host: joe_jacob		
	1. Location Enter the full path (starting with /) to the image file. If the image is split (either raw or EnCase), then enter **' for t	he
	extension. //tome//suci/Downloads/image	
	2. Type /tome/suc/Opintoscimage Please select if this image file is for a disk or a single partitior	L.
	O Disk O Partition	
	3. Import Method To analyze the image file, it must be located in the evidence lo be imported from its current location using a symbolic link, by or by moving it. Note that if a system failure occurs during the then the image could become corrupt.	cker. It can / copying it, a move,
	O Symlink Copy Mo	7e
	NEXT	

- /home/suci/Downloads/image : merupakan lokasi file image
- Pada Type masukan sesuai dengan type daei image file nya, apabila disk pilih disk apabila partisi pilih partition, pada kasus ini memilih disk.
- Pada bagian import method silahkan pilih sesuai keinginan . pada gambar diatas terlihat bahwa yang dipilih adalah symlink karena sudah punya salinan lain nya, jadi apabila file system tersebut rusak tidak menjadi masalah.

Setelah semuanya selesai langsung sakja klik next.

Maka akan muncul seperti gambar dibawah ini.

Image File Details	
Local Name: images/image Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file) Ignore the hash value for this image. Calculate the hash value for this image. Add the following MD5 hash value for this image: Verify hash after importing?	
File System Details	
Analysis of the image file shows the following partitions:	
Partition 1 (Type: fat12) Mount Point: c: File System Type: fat12	
ADD CANCEL HELP	
Warning: Autopsy could not determine the volume system type for the disk image (i.e. the type of p Please select the type from the list below or reclassify the image as a volume image instead of as a	artition table). disk image.
Disk Image Volume Image Volume Image Volume System Type (disk image only): dos	>
ок	

Lanjutkan saja dengan klik ADD->> OK.

C	ASE GALLERY	Host G	ALLERY	HOST MANAGER
				0
5	mount C:/	name image-0-0	fs type fat12	<u>details</u>
-	Analyze			CLOSE HOST

Sampai tahap ini setup pada kasus autopsy sudah selesai, tinggal melakukan analis terhadap file system dari kasus yang dibuat.

File yang dipakai



suci-Aspire-4736Z Documents # file voll-Sector73.raw
voll-Sector73.raw: JPEG image data, JFIF standard 1.01

Rename file tersebut



Tampilan image vol1-sector73.jpg



Selanjutnya gunakan string untuk menyimpan password di dalam file gambar



	Archive Manager	×
	Password required for "vol1-Sector104 Password:	.zip"
	Cancel OK	
	Terminal	- + ×
File Ealt View K;dMj)UfRcvm 8-'H\$ FFFy 9 kB, 1 abj	ect selected (16,9 kB)	
NrH' 7g% 9'p+ R*]I oqk4 I+^L		I

Dapat dilihat pada terminal password yang didapatkan adalah "goodtimes"

To be the services where Dependent Fr 10 10 10 0 <th></th> <th>unil-Sacharith.jpg - Gites</th> <th>× ± 1</th>		unil-Sacharith.jpg - Gites	× ± 1
000000000000000000000000000000000000	He for your Modern Hep		
Styreet It 84 0 Development It 84 Maxadaptivestic 00 Unsugned It 84 0 0.0443028 0.0443028 0.0443028 0.0443028 0.0116 0.03 Unsugned It 84 0 0.0443028 0.0443028 0.0116 0.03 0.0116 0.03 Styres It 84 236 From 10 100 0.0116 0.03 0.0116 0.03 0.0116	000000001F7 DE F EO 00 10 4A 4B 4B 4B 00000001F6 00 77 07 07 00 00 04 0A 0C 14 0 00000001F6 00 02 22 22 14 10 00 10 00	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	17 66 05
Unique 18 54 2 Unique 15 54 (1843)00 Disk (1843)00 Disk (1854) Dis	35pred 0.001 0	50prat 52 88 14543018	Hanadacenal: 00
Signed in Str. Free Str. Free Str. Stream Langer Stream Langer Stream Langer Interesting Stream Stream Langer Stream Stream Langer Stream Langer Interesting Interesting	Unigned 8 b4: 1	Unigent 20 bit. 14543308	0ctae 003
Array peet 16 St. 216. From 66 St. 2.7644(10+154 Stream Langest # + +	Report 10 201 214	Front BE BR. J. Hernald Son MA	Brary Generate
D three Rife ender second	Houghout 16 Dd: 258	Four 64 84 2.7644110+154	Stream Langts: 9 - + +
Offant: Sold, Ead bytes from DxS to Sold automatical	Dirace Rith and an account	t Shee u	rsigtadi anti Radi se tenediscorsi

Kemudian untuk Merecover jika signature nya hilang gunakan foremost

SUCI-ASPIRe-47382 Documents # 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) Name (bs=512) File Offset Comment Num Size 00000073.jpg 8 KB 8: 37376 1: 16896 1: 00000033.00. foundat=Scheduled Visits.xls**601*61** foundat=Scheduled Visits.xls**601*61** (6) 36#-4 367666°8768766f
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082 6658
 (6) 6082
 (6) 6082 6658
 (6) 6082 665
 (6) 6082
 (6) 6082
 (6) 6082
 (6) 6082
 (6) 6082
 (6) 6082
 (6) 6082
 (6) 6082
 (6) 6082
 (6) 6082
 (6) 6082
 (6) 6082
 (6) 6082
 (6) 608
 (6) 608
 (6) 608
 (6) 608
 (6) 608
 (6) 608
 (6) 608
 (6) 608
 (6) 608
 (6) 608
 (6) 608
 (6) 608
 (6) 608
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6) 60
 (6)
 (6) 60
 (6)
 (6) 60
 (6)
 (6) 60
 (6)
 (6) 60
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 (6)
 2 KB 00000104.zip 53248 Finish: Fri Mar 24 12:01:57 2017 3 FILES EXTRACTED jpg:= 1 ole:= 1 zip:= 1

Foremost finished at Fri Mar 24 12:01:57 2017

			Scheduled Vetts.s	h - LibreOffue Cale		
Ele Ent yow	josert Remail 3	Rols Data Wendow Holp				
- · D ·		4 國國 ··································	08.4	it is G	5000	
	Civil Leave				m . a	
El Ana	. 11		* = _ M * =			
450	- 1(v) X	= Munday (1)				.ie
. A	And the second second	c	D	E F O	H I I I	K L M N O
1 Month	DAY	HIGH SCHOOLS				
7 200	2					De la companya de la company
3 April	Monday (1)	Smith Hill High School (A)				
4	Tuestby (2)	Key High School (9)				
5	Wednessbay (3)	Leetch High School (C)				
£	Thursday (4)	Birard High School (D)				
3	Fittay (5)	Richter High School (E)				
4	Monday (1)	Hut High School (F)				
9	Tuesday (2)	Smith Hill High Scholt (A)				
10	Wednesday (1)	Key High School (8)				
11	Thursday (4)	Ceetch Hegh School (C)				
14	Pricely (c)	Harman Hage School (U)				
1.0	Transform (1)	Here have been active in a				
18	Weinteenday (2)	South Hill Han School (A)				
16	Thurnitay (8)	Key High School (S)				
11	Friday (5)	Leaderh Made School (C)				
18	Monday (1)	Bred Hot School Eh				
18	Tuesday (2)	Bichter Hatt School (E)				
20	Wednesday (3)	Hull High School (F)				
21	Thirtutay (d)	Smith Hill High School (A)				
22	Friday (5)	Key High School (5)				
23	Monday (1)	Leetch High School (C)				
24	Tuesday (2)	Sirard High School (D)				
25 May						
24	Velidnesskey (3)	Hichter High School (E)				
27	Thursday (4)	Hull High School (F)				
28	Friday (5)	Smith Hill High School (A)				
29	Monday (I)	Key High School (9)				
29.	Tuesday (2)	Leetch High School (C)				
· · · · Sheet3	/Sheet2 / Sheet3 /	2/			1	
5heat 1 / 5		PageStyle_Sheet:		-	12 SH	m=0 + 100%

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