TUGAS

KEAMANAN JARINGAN KOMPUTER



DISUSUN OLEH :

- NAMA : INDAH SARI
- NIM : 09011181320011

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017 - 2018

HASIL TRAINING KOMPUTER FORENSICS DI LEB

DEFINISI KOMPUTER FORENSICS

Dari berbagai sumber, definisi komputer forensics secara garis besar 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.

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.

TOOLS YANG DIGUNAKAN :

- AutoPsy
- Foremost
- String
- Ghex

Berikut Langkah – Langkah Pengerjaan dari Komputer Forensics :

Lakukan penginstallan tools selain string dan buka alamat web dibawah ini:

http://old.honeynet.org/scans/scan24/



Dari alamat web tersebut muncul halaman utama dari The Honeynet Project dan download file: Image.Zip MD5 = b676147f63923e1f428131d59b1d6a72 (image.zip)

Konfig md5sum image.zip, dimana fungsi md5sum adalah sebuah file yang pasti ada md5sum yang fungsinya untuk mengecek keaslian dari file atau integritas file

md5sum image.zip

b676147f63923e1f428131d59b1d6a72 image.zip

Konfig file image, untuk mengecek tipe file. Jika kita menemukan file yang tidak ada ekstensi, maka kita bisa menggunakannya



Fungsi perintah file image di atas menampilkan image: DOS floppy 1440k, x86 hard disk boot sector, setelah mengetahui bahwa file tersebut file boot sector, maka selanjutnya bisa melakukan proses mounting.

Sebelum melakukan proses mounting buat folder kasus terlebih dahulu yaitu :

mkdir /tmp/kasus.

Konfig mount image /tmp/kasus

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

Konfig cd /tmp/kasus, untuk masuk ke folder kasus, lalu ls

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

Dari gambar diatas setelah di ls akan tampil isi dari folder kasus yang telah dibuat sebelumnya, dimana folder tersebut berisi dua file yaitu cover page.jpgc dan SCHEDU~1.EXE

Konfig file *, yang berfungsi untuk mengecek keaslian semua file pada folder kasus



Dimana file yang terbaca dalam folder kasus ini hanya SCHEDU~1.EXE Zip archive data, at least v2.0 to extract

Konfig autopsy, dimana sebelumnya telah di install terlebih dahulu



Konfigurasi dari autospy diatas menampilkan remote host dari autospy: localhost, dan memiliki local port 9999

Setelah mengetahui autospy memiliki local host yang memiliki local port 9999, lalu search alamat web localhost.9999/autospy



Dari alamat web localhost.9999/autospy maka akan tampil halaman utama dari Autopsy Forensic Browser 2.24, dimana halaman ini berfungsi untuk mengatur hostname, siapa yang melakukan forensik pada komputer target. Klik New Care

num	here and symbols	of this investigation.	It can contain o	only letters
ka	sus			
-				
2. D	escription: An option	nal, one line description	on of this case.	
ka	sus parkoba			
N.C	ISUS Harkova			
L.a	SUS Harkoba			
3. In	vestigator Names:	The optional names (v	vith no spaces) (of the
3. In	vestigator Names: T stigators for this case	The optional names (v	vith no spaces) (of the
3. In inves a.	vestigator Names: T stigators for this case indah sari	Гhe optional names (v b	vith no spaces) (of the
3. In inves a. c.	vestigator Names: 7 stigators for this case indah sari	The optional names (v b. d.	vith no spaces) (of the]]
3. In inves a. c. e.	vestigator Names: 7 stigators for this case indah sari	The optional names (v b. d. f.	vith no spaces) o	of the]]
3. In inves a. c. e. g.	vestigator Names: T stigators for this case indah sari	The optional names (v b. d. f. h.	vith no spaces) (I	of the))]

Isi Create A New Case, dengan case name: kasus, description: kasus narkoba, dan investigator names: nama user. Lalu New Case

CASE GALLERY	Host G	ALLERY	
mount) C:/	name image-0-0	fs type fat12	<u>details</u>
ANALYZE			CLOSE HOST

Setelah pengisian dari beberapa case, akhirnya akan menampilkan gambar seperti berikut:

Gambar daitas menampilkan dimana letak data image.zib yang kita simpan sebelumnya

Lalu pilih r/r jimmy jungle.doc

Directory Seek Enter the name of	Cur	rent Dire	Clory: CZ Generate M	IDS Larror Faux						
a directory that you want to view. E:/	DEL	Type dir/in	NAMELIA	Warries	Accessed	CHEATED	Set	υø	GID	Mera
		v/v	STATA	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
Vew.		v/v	MATE	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
File Name Search		v/v	2225	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
Enter a Peri		d/d	BicatureExland	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-06-00 00:00:00 (UTC)	0	0	0	45782
regular expression for the		r/r	1350F.000F.381C	2002-09-11 08:30:52 (WIE)	2002-09-11 00:00:00 (WIB)	2002-09-11 08:50:27 (WIB)	15585	0	0	8
me names you want to find.		r?r	Jime Juste des	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 Titalta.eve	2002-05-24 08:20:32 (WIB)	2002-09-11 00:00:00 (WIB)	2002-09-11 08:50:38 (WIB)	1000	0	0	ш

Setelah itu akan ada dua file yang bisa kita ambil

FAT CONTENTS (in sectors)

<u>73-103 (31)</u> -> EOF <u>104-108 (5)</u> -> EOF

FAT CONTENTS (in sector) untuk 73-103 (31) \rightarrow EOF

	The Analysis Nervolis Bearow Pile Time Innoe Denke Meth Data Data Unit Help Globe
Sector Number:	Precision, Nezz Earlier Contracts, Ann Norg
Number of Sectors:	ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) File Type: jPEG image data, jPIF standard 1.01 Sectors: 73-103
Sector Size: 512	Plates Thereid
Address Type: Regular (dt)) •	Will Conterns of Sectors (3-50) in image-o-e
Lazarus Addr:	2/ (121352077777272737372727272727272727272727272
SHEW :	(11/1/1/1/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/
ALLOCATION LAST	1
	1. (1. (1. (1. (1. (1. (1. (1. (1. (1. (
	b(r) (b,q., h.m. ag., 0,, s, w,, 9, s ⁿ , p, θ,, ξ2r, cg), (, , j,, T, T, 0,, s),, pq, (b(r) (b(r), s, s), s,

Dari gambar diatas file type dari $\underline{73-103} (\underline{31}) \rightarrow \underline{EOF}$ adalah JPEG image data JFIF standard 1.01

Konfig file voli-sector73.raw

```
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#
```

Dari perintah fungsi diatas menampilkan vol1-sector73.raw: JPEG image data, JFIF standard 1.01 dimana file tipe nya sama jika dilihat dari gambar FAT CONTENTS (in sector) untuk 73-103 (31) \rightarrow EOF. Dan Rename jd jpg



FAT CONTENTS (in sector) untuk 104-108 (5) \rightarrow EOF

	The Annual Remote Bankos File Title Indee Details Meth Data Units Units Units Units
Sector Number: 104 Number of Sectors:	
Sector Size: 512	AddII Centerns of Sectors 104-388 in image-8-8
Address Type:	and the second
Regular (dd)	PR2.,0"8Steening viscos Ris. 1*. Lp1#K.u0*6.567
Lazarus Addr:	t.8m227.13m
. Yew;	8
ALLOCATION LINE	a., h., g., 0,, 2, g.,, 7,,,, 3,, 6,, 4,, 4,, 7,, 7,, 7,, 7,, 8,, 0, g, 42,, 40, c, X, M, 6(, SYL, p7,, p,, p,, F,, 6, M, 6, 4, 0,, 3,, 5,, 6,, 4,, 6,, 17,, 18,, 18,, 19,, 18,, 19,, 18,, 19,, 18,, 19,
	C. C. M. M. M. S. C. P. S. C.
	U.NN. 3. 0. %, 8

Dari gambar diatas file type dari <u>104-108 (5)</u> \rightarrow EOF adalah empty (Zip archive data, at least v2.0 to extract)

Konfig strings vol1-sector73.jpg

root@mah	asiswa:/home/mahasiswa/Downloads#	strings	vol1-Sector73
.jpg			
FFFy			
	NrH'		
pu0	k		
go}b			
/9'			
Tw	(1)		
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=good	times	222	
root@mai	hasiswa:/home/mahasiswa/Downloads#		

Menyimpan pw di dalam file gambar

				Scheduled V	uita.elsi - Li	tireOffice	Call:									• #
The	Sit yes	Steart Parnet 3	bos Data Wantow Help													
100	1 Sector			HI MANY AND		204410		the lines	0.22010/2	22						
	· D ·		4 個 60 公 m X	n D - a		10 14	î† 😶	5 0		> :						
ŧ	Lana	1. 110		= H .	5 10	10 m	m	m · a	eell -							
	- Internet				100 (HT.)		Links a			11						
H 50		T Nel E	= Monday (1)													36
	A,	in the second se	6	0	E	. F.	6	- H	1	and the second second	κ.	- E3	.16	- N	. 0	10
1	Month	DAY	HIGH SCHOOLS													21
- 2	3000	2														R
3	April 1	Monday (1)	Sweth Hill High School (A)													
- 4		Turestay (2)	Key High School (0)													
- 5		Wethenday (3)	Lectch High School (C)													
- 6		Thursday (4)	Binsid High School (D)													11
7	1	F100y (5)	Richter High School (E)													-
. 4	1	Monday (1)	Hull High School (F)													- 1
. 4		Tuesday (2)	Seem He High School (A)									_				- 11
-10	8	Westweeday (3)	Key High School (B)													-12
-11	8	Thursday (4)	Leetch High School (C)		_										_	
-12	3	Fricky (5)	Brard High School (D)													1.8
-13	1	Monday (1)	Richter High School (E)			_										
235	1	Tuesday (2)	Huli High School (F)		-				_						-	- 2
15	1	Wednesday (3)	Smith Het High School (A)		-							-				
-38		Thursday (4)	Key High School (B)													- 8
-17	1	FROM (5)	Leetch High School (C)		_											
_18		Monday (1)	Beard Heath School (D)													
11		Tuesday (2)	Fochoer High School (E)		-											
-38	a	Wednesday (3)	Hull High Sichool (P)		_											
-21	1	TRUSONY (4)	Brate Hit Hige School (A)		_											1.2
. 22	a	Peshiy (5)	Key High School (B)													- 2
:23		Manday (1)	Leetth High School (C)													- 1
.74	1. Calil	Tuesday (2)	Illing High School (D)													
- 25	May	March and and			_							-				18
.76		Wednersday (3)	Hichar High School (E)												-	
27	2	Thursday (4)	Hut High School (F)						_							
28		Preday (5)	Sente Hill High School (A)						-							
-19	3	Monday (1)	Key High School (B)													- 2
10		Tuenday (2)	Feetra with 25000 (c)				1									
814	s a Shrett	/ Weitz / Sherts / -	entre and a second second					1								1
Sh	wf 1/3		PageStyle_Sheet1				- ME - 1	201		547	0-0		-	- 0-	- + 30	10%

Konfig foremost –v –i image –o recover



Perintan fungsi diatas berfungsi untuk merecover jika signature nya hilang

Kesimpulan: dengan adanya langkah langkah komputer forensic diatas dapat membantu menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat butki yang sah di pengadilan.