# **TUGAS KEAMANAN JARINGAN**

# " Komputer Forensik "



**OLEH :** 

- NAMA : MARDIAH
- NIM : 09011281320005

### SISTEM KOMPUTER

### FAKULTAS ILMU KOMPUTER

#### **UNIVERSITAS SRIWIJAYA**

### INDERALAYA

2017

Komputer Forensik adalah cabang dari ilmu forensik berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital.

Maraknya tindakan kejahatan dalam dunia komputer, membutuhkan proses pembuktian yang tidaklah mudah, oleh karena itu, kajian bidang komputer forensik ini masih tergolong baru dan masih terus dikembangkan, sehingga nantinya, semua kasus-kasus kejahatan komputer mampu dibuktikan secara sah di pengadilan.

Saat ini, kajian komputer forensik dibagi menjadi beberapa bidang seperti Internet Forensik yang khusus membahas forensik dalam ranah internet dan aplikasinya, lalu ada Network Forensik, Disk Forensik, Database Forensik, Firewall Forensik, Mobile Device Forensik dan System Forensik yang kesemuanya secara umum berada dalam kontek komputer forensik.

Tujuan dari Komputer Forensik adalah untuk mengamankan dan menganalisa bukti digital. Selain itu juga bertujuan untuk mendapatkan fakta-fakta objektif dari sebuah insiden / pelanggaran keamanan sistem informasi. Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum.

#### KASUS :

Ada seorang pengedar narkoba yang tertangkap polisi, polisi mendapatkan barang bukti berupa harddrive yang sudah korup dari tersangka. Bagaimana cara kita me- recover harddrive tersebut sehingga kita mendapatkan informasi di dalam nya.

Pada percobaan kali ini, menggunakan beberapa tools berikut :

1. Autopsy

Merupakan sebuah antarmuka grafis yang menyediakan fungsi manajemen kasus, integritas gambar, pencarian kata kunci, dan operasi lainnya.

2. Foremost

Foremost merupakan aplikasi berbasis console yang melakukan recovery file yang terhapus berdasarkan header file, footer file, data struktur data. Foremost dapat bekerja pada image file (.iiso, dll), seperti yang dihasilkan oleh dd, Safeback, Encase, dll, atau langsung pada drive.

3. Strings

Adalah sebuah aplikasi yang digunakan untuk mengetahui password dalam suatu file. Pada percobaan ini yaitu file image Langkah kerja :

- 1. Install tools, selain strings karena tools string sudah tersedia pada OS ubuntu
- 2. Buka wesite berikut <u>http://old.honeynet.org/scans/scan24/</u>. Kemudian download " file image.zip ". File tersebut merupakan bahan yang akan kita analisa menggunakan 3 tools diatas.

Image.Zip (old.honeynet.org/scans/scan24/image.zip) md5 : b676147f63923e1f428131d59b1d6a72

Interpretion of the second sec	町 C Q fb ナ	☆自	01	► <b>^</b>	⊜ ≡
The Honeynet PROJECT®	[an error occurred while processing this directive]				
Home					
About The Project					
Research Alliance	Scan of the Month				
Challenges	Scan 24				
In esenvations	This month's challenge is a little different. Sponsored by the folks from Digital Porensic Research WorkShop, they have created a fictional situation, where your job is to analyze				
wintepapers	forensic evidence. All submissions are due no later then 23:00 EST, Friday, 25 October. Results will be released Friday, 01 November.				
Tools	Skill Level: Intermediate				
UUP BOOK	The Challenge				
Funding/Donations	The folks from Digital Forensic Research WorkShop have created a unique challenge for you. Your mission is to analyze a recovered floppy and answer the questions below. What				
Mirrors	information and some evidence, but its up to you and your technical skills to dig up the answers. Below is the dd image of the recovered floppy. This is the image that will provide you the answers. Below is the dd image of the recovered floppy. This is the image that will provide you the answers.				
Search	ne answers, provoing you can extract the data.				
	image zip MD5 = b676147f63923e1f428131d69b1d6a72 ( image zip )				
	Make sure you check the MD5 checksum of your download before you unzip it.				
	Questions You can find all the criteria for judging and rules at the SotM main page.				
	<ol> <li>Who is Joe Jacob's supplier of manijuana and what is the address listed for the supplier?</li> <li>What crucial data is available within the coverpage jpg file and why is this data crucial?</li> <li>What if any other high schools besides Smith IIII does Joe Jacobs frequent?</li> <li>For each file, what processes we taken by the suspect to mask them from others?</li> <li>What any consessed show the investigatory use to successfully examine the entire contents of each file?</li> </ol>				
	Bonus Question:				
	6. What Microsoft program was used to create the Cover Page file. What is your proof (Proof is the key to getting this question right, not just making a guess).				
	Some URLs to help you out				
	Forensic Tools,     Scan of the Month 15,     Homer Forensic Challenge,				
	The Results:				

- ➡ Fungsi md5sum : sebuah file pasti ada md5sum yang berfungsi untuk mengecek keaslian dari file atau integritas file
- 3. Fungsi perintah di bawah ini yaitu untuk mengecek tipe file. Jika kita menemukan file yang tidak ada ekstensi, maka kita bisa menggunakan perintah sintaks tersebut.



4. Setelah kita tahu bahwa file tersebut file boot sector, maka akan melakukan proses mounting. Lalu Mengecek keaslian file

```
root@mardiah-X455LF:/home/mardiah/Downloads# mkdir /tmp/Narkoba
root@mardiah-X455LF:/home/mardiah/Downloads# mount image /tmp/Narkoba
root@mardiah-X455LF:/home/mardiah/Downloads# cd /tmp/Narkoba
root@mardiah-X455LF:/tmp/Narkoba# ls
cover page.jpgc SCHEDU~1.EXE
root@mardiah-X455LF:/tmp/Narkoba# file *
cover page.jpgc : ERROR: cannot read `cover page.jpgc ' (Inp
ut/output error)
SCHEDU~1.EXE: Zip archive data, at least v2.0 to extract
root@mardiah-X455LF:/tmp/Narkoba#
```



- 5. Kemudian menggunakan tools autopsy. Karena tools ini bekerja menggunakan search engine, jadi tools ini memberikan informasi yaitu :
- Remote Host : localhost
- Local Port : 9999

```
oot@mardiah-X455LF:/tmp/Narkoba# autopsy
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
Evidence Locker: /var/lib/autopsy
Start Time: Wed Mar 29 03:35:50 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
```

6. Buka search engine dengan alamat dari informasi diatas "localhost : 9999 / autopsy "



7. Mengatur hostname, siapa yang melakukan forensik pada komputer target

8 🔿 🗊	Сг	reate A New Case - Mozilla Firefox								
🊯 Creat	e A I	New Case 🕂								
< >		localhost:9999/autopsy?mod=0&vie	w=1		ź	3 <b>- C</b>	<mark>8</mark> ▼ Google	Q	$\mathbb{Q}$	
< >		Iocalhost:9999/autopsy?mod=0&vie	<ul> <li>w=1</li> <li>1. Case Name: The nanumbers, and symbols Kasus_Narkoba</li> <li>2. Description: An op KJK</li> <li>3. Investigator Name investigators for this c</li> <li>a. Mardiah</li> <li>c.</li> <li>e.</li> <li>g.</li> <li>i.</li> </ul>	CREATE A NEW ame of this investig	<b>W CASE</b> nation. It can contain only scription of this case. mes (with no spaces) of the	letter:	S,			
			NEW CASE	CANCEL	HEIR					
				CANCEL						

8. Menambahkan file yang akan di autopsy. Dalam percobaan ini menggunakan file image



EVENT SEQUENCER

VIEW NOTES

🙆 🗇 🕼 Kasus_Narkoba:host2:vol1 - Mozilla Firefox											
🚯 Kasus_Narkoba:host2:vol1 👘											
localhost:9999/a	🕜 localhost:9999/autopsy?mod=1&submod=2&case=Kasus_Narkoba&host=host2&inv=Mardiah&vol=vol1 🗘 🗸 🕐 🚷 🕻 Google 🔍 🦆 🏠										
FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE											
Directory Seek		ent Dire	C <b>tory: <u>C:/</u> Generate N</b>	1D5 LIST OF FILES							
you want to view.	DEL	Type dir / in		WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	МЕТА	
		v / v	<u>SFAT1</u>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	<u>45780</u>	
		v / v	<u>SFAT2</u>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	<u>45781</u>	
File Name Search		v / v	<u>SMBR</u>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	<u>45779</u>	
Enter a Perl		d / d	<pre>\$0rphanFiles/</pre>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	<u>45782</u>	
regular expression for the		r / r	<u>cover page.jpgc</u>	2002-09-11 08:30:52 (WIB)	2002-09-11 00:00:00 (WIB)	2002-09-11 08:50:27 (WIB)	15585	0	0	<u>8</u>	
want to find.	~	r / r	<u>Jimmy Jungle.doc</u>	2002-04-15 14:42:30 (WIB)	2002-09-11 00:00:00 (WIB)	2002-09-11 08:49:49 (WIB)	20480	0	0	<u>5</u>	
		r / r	<u>Scheduled</u> <u>Visits.exe</u>	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	
SEARCH											
ALL DELETED FILES											
EXPAND DIRECTORIES					File Browsing Mo	ode					

9. Dua konten dalam file image yang bisa kita gunakan untuk autopsy. Yaitu :

😣 🖻 🗉 Kasus_Narkoba:host2:vo	l1 - Mozilla Firel	ox								
🚯 Kasus_Narkoba:host2:vol1	+									
localhost:9999/autopsy?m	od=1&submod=7	&case=Kasus_Narko	ba&host=host	2&inv=Mardiah&vol	=vol1	☆ ▼ 🥙	8 🔻 Google	Q	₽ (	
	FILE ANALYSIS	Keyword Search	FILE TYPE	IMAGE DETAILS	META DATA	DATA UNIT	HELP CLOSE			
File System Layout (in sector: Total Range: 0 - 2879 * Reserved: 0 - 0 ** Boot Sector: 0 * FAT 0: 1 - 9 * FAT 1: 10 - 18 * Data Area: 19 - 2879 ** Root Directory: 19 - 32 ** Cluster Area: 33 - 2879	5)									
METADATA INFORMATION Range: 2 - 45782 Root Directory: 2	J									
CONTENT INFORMATION Sector Size: 512 Cluster Size: 512 Total Cluster Range: 2 - 2848										
FAT CONTENTS (in sector 73-103 (31) -> EOF 104-108 (5) -> EOF	s)									

## FAT CONTENTS (in sectors)

<u>73-103 (31)</u> -> EOF <u>104-108 (5)</u> -> EOF  Tampilan isi konten pertama yaitu : 73 – 103 (31) .> EOF. Kemudian export contens lalu kita akan mendownload suatu file dari export contens tersebut

😣 🗐 🗊 Kasus_Narkob	a:host2:vol1 - Mozilla Firefox
🕼 Kasus_Narkoba:host2	cvol1 🔶
🔇 🛞 localhost:9999/	/autopsy?case=Kasus_Narkoba&host=host2&inv=Mardiah&vol=vol1&mod=1&submod=5█=73&len=፤ 🏠 🕈 😴 🔞 🗸 Google 🛛 🔍 🐥 🏫
	FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE
Sector Number:	
73	Export Contents Add Note
<b>XX X C</b>	ASCH (uspidy - report) - nex (uspidy - report) - ASCH Su mgs (uspidy - report) File Two: IPEG image data. IFIF standard 1.01
Number of Sectors:	Sectors: 73-103
1	Status: Allocated
Sector Size: 512	ASCII Contents of Sectors 73-103 in image-0-0
Sector Size, 512	JFIF
Address Type:	······································
Regular (dd)	.21, 12222222222222222222222222222222222
Legence Addre D	
Lazarus Addr:	
VIEW	
ALLOCATION LIST	
	B · X · · · · · · · · · · · · · · · · ·
	.w.&
	YdvT;,(p.S+>w.MQ8'.&%.8.S6.0j'K.[uTHDYaNn.w.Mf.;.a.ob.c.9~'+kk.`DB7 .MF\.7rM.J.9.w.6*.1znoB6.M4.7/.QT.2H.
	5]?.gb4; .6U.F.i%r( e/4kImp.L.+D.Cm 80KI4Vk.@.{(.>e].v.G.x{LkH\$G(c@"R%f"\$.~T >U
(( · · · · · )))	

11. Tampilan isi konten kedua yaitu : 104 – 108 ( 5 ) .> EOF. Sama seperti contents pertama, pada contents kedua juga melakukan export contents dan mendownload suatu file

😣 🖨 🗊 Kasus_Narkoba	host2:vol1 - Mozilla Firefox
🊯 Kasus_Narkoba:host2:v	ol1 🚽
🔇 🕘 localhost:9999/a	utopsy?case=Kasus_Narkoba&host=host2&inv=Mardiah&vol=vol1&mod=1&submod=5█=104&len= 🗘 🗸 🕲 Koogle 🔍 😓 🏠
	FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA DATA UNIT HELP CLOSE
Sector Number:	
104	ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)
Number of Sectors:	File Type: empty (Zip archive data, at least v2.0 to extract) Sectors: 104-108 Status: Allocated
Sector Size: 512	ASCII Contents of Sectors 104-108 in image-0-0
Address Type:	PKZ., U <sup>1</sup> BScheduled Visits.xlsl*.IplH.≪K.uQ*6.\$~uFNV0`6T#R#-4HT.b.^.?.Rrf Jx.SkUMaSA#.;.0k Z.VS
Lazarus Addr:	
View	7%XJ8B.KR. w abg.02.X?Z.Jw{.m.L.SC6g(.yGU,j.T?\$nRUfH@I+6Q.g.42+bN.c.X.WG{.>Yt.p?;u.jp.\05" F#e.Aq.s.q.0Si.ncG4.K%@4N'L".1d.Q~_bY.26h slXK.,8.64);'.cE6.l.^^8l.r4.~.B> 3F.:S.lY/9.MKXZ.
ALLOCATION LIST	3).3], (Z.H.AR.RU.T5.W!.ZNL9.e.!eC.Db,W05R.? (Z.H.AR.RU.T5.W!.ZNL.9.e.!9dyP.ot3;NBY4<.E.6M.:.A)43 .%.F.p.]6n%.&F\<

- ⇒ File yang didownload sebelumnya yaitu :
- Vol1-Sector73.raw
- Vol1-Sector104.raw

12. Lalu Mengecek ekstensi dari file tersebut. Disini merupakan file dari contents yang pertama. Setelah kita mengetahui bahwa ekstensi dari file tersebut yaitu JPEG maka kita rename file tersebut menjadi format JPG

```
root@mardiah-X455LF:/home/mardiah/Downloads# ls
image image.zip vol1-Sector104.raw vol1-Sector73.raw
root@mardiah-X455LF:/home/mardiah/Downloads# file vol1-Sector73.raw
vol1-Sector73.raw: JPEG image data, JFIF standard 1.01
root@mardiah-X455LF:/home/mardiah/Downloads#
```

13. Tampilan gambar yang kita dapat pada contents pertama.



14. Lalu melakukan pengecekan ekstensi pada contens yang kedua



- ⇒ Dan kita mengetahui ekstensi dari file tersebut, sama seperti langkah sebelumnya, kita rename file tersebut menjadi format zip. Dalam melakukan pengekstraksian, ternyata file tersebut mempunyai password untuk membuka nya, sehingga kita harus mencari tau apa passoword tersebut.
- ➡ Ternyata pada contents pertama, diselipkan password pada gambar di atas sehingga kita akan mengetahui password tersebut dengan melakukan proses string pada file contens pertama



80	root@mardiah-X455LF: /home/mardiah/Downloads
f n8e FFFv	
	NrH'
pu0 go}b	k
·/9'	,
	L
k}Bx`VF	
s\$6s.	
zz7q	
K;dMj	
)UfRcvm	
8-'H\$	
FFFy	
	NrH'
7g%	
9°0+	
K^ JI	
04K4 T+^I	
pw=goodt	imes
root@mar	diah-X455LF:/home/mardiah/Downloads#

15. Lalu akan tampil bahwa password untuk melakukan ekstraksi yaitu : goodtimes

16. Dan isi dari file zip berupa file exel dengan isi sebagai berikut :

	Α	в	С
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)
18		Monday (1)	Birard High School (D)
19		Tuesday (2)	Richter High School (E)
20		Wednesday (3)	Hull High School (F)
21		Thursday (4)	Smith Hill High School (A)
22		Friday (5)	Key High School (B)
23		Monday (1)	Leetch High School (C)
24		Tuesday (2)	Birard High School (D)

25	May		
26		Wednesday (3)	Richter High School (E)
27		Thursday (4)	Hull High School (F)
28		Friday (5)	Smith Hill High School (A)
29		Monday (1)	Key High School (B)
30		Tuesday (2)	Leetch High School (C)
31		Wednesday (3)	Birard High School (D)
32		Thursday (4)	Richter High School (E)
33		Friday (5)	Hull High School (F)
34		Monday (1)	Smith Hill High School (A)
35		Tuesday (2)	Key High School (B)
36		Wednesday (3)	Leetch High School (C)
37		Thursday (4)	Birard High School (D)
38		Friday (5)	Richter High School (E)
39		Monday (1)	Hull High School (F)
40		Tuesday (2)	Smith Hill High School (A)
41		Wednesday (3)	Key High School (B)
42		Thursday (4)	Leetch High School (C)
43		Friday (5)	Birard High School (D)
44		Monday (1)	Richter High School (E)
45		Tuesday (2)	Hull High School (F)
46		Wednesday (3)	Smith Hill High School (A)
47		Thursday (4)	Key High School (B)
48		Friday (5)	Leetch High School (C)

49	June		
50		Monday (1)	Birard High School (D)
51		Tuesday (2)	Richter High School (E)
52		Wednesday (3)	Hull High School (F)
53		Thursday (4)	Smith Hill High School (A)
54		Friday (5)	Key High School (B)
55		Monday (1)	Leetch High School (C)
56		Tuesday (2)	Birard High School (D)
57		Wednesday (3)	Richter High School (E)
58		Thursday (4)	Hull High School (F)
59		Friday (5)	Smith Hill High School (A)
60		Monday (1)	Key High School (B)
61		Tuesday (2)	Leetch High School (C)
62		Wednesday (3)	Birard High School (D)
63		Thursday (4)	Richter High School (E)
64		Friday (5)	Hull High School (F)
65		Monday (1)	Smith Hill High School (A)
66		Tuesday (2)	Key High School (B)
67		Wednesday (3)	Leetch High School (C)
68		Thursday (4)	Birard High School (D)
69		Friday (5)	Richter High School (E)

17. Kemudian melakukan recover jika signature nya hilang

root@ma	rdiah-X455LF:/home,	/mardiah/Downl	loads# foremost -	v -i image -o rec	over
Foremos Audit F	t version 1.5.7 by ile	Jesse Kornblu	ım, Kris Kendall,	and Nick Mikus	
Foremos	t started at Wed Ma	ar 29 03:59:03	3 2017		
Invocat	ion: foremost -v -i	i image -o rec	over		
Output	directory: /home/ma	ardiah/Downloa	ads/recover		
Process	ration file: /etc/1	roremost.cont			
File: i	mage				
Start:	Wed Mar 29 03:59:03	3 2017			
Length:	1 MB (1474560 byte	es)			
Num	Name (bs=512)	Size	File Offset	Comment	
0:	00000073.jpg	8 KB	37376		
1:	00000033.ole	21 KB	16896		
foundat	=Scheduled Visits.	xls@@1*@I			- 60 0
08.09 <b>%</b> ~#	- 4 <sup>0</sup> 900TabaAa2aDcaaf	ĭ₿₽�€	¢¥\$\$\$\$\$\$\$\$\$\$\$	₩\$& <u>ĭ</u> ăuF&&NVO&&& 6	T <u>ĭ¥</u> .#��[ĭ
	e5kUMeeeea eeSA#e:	o0k멏 ㅎㅎ			
Lenath:	1 MB (1474560 byte	es)			
	2 (2.1				
Num	Name (bs=512)	Size	File Offset	Comment	
0:	00000073.jpg	8 KB	37376		
1:	00000033.ole	21 KB	16896		
foundat	=Scheduled Visits.	xlsool*oI			
980.980#	- 4 BHTaba^a?aBraaf	<u>18</u> P**	<u>اظا</u> مہ< <u>د</u> ہndہñهه <sub>×</sub> c	\$\$\$ <u>14</u> UF\$\$NVU\$\$\$ 0	119.#**1
	•5kUM•••••a_••SA#•;•	ଡ଼ୡୢୢ୰ଡ଼୶ୖ୲୲			
00 19 <b>I</b> �19 �	;020VS				
2:	00000104.zip	2 KB	53248		
Finish:	Wed Mar 29 03:59:0	03 2017			
3 FILES	EXTRACTED				
ipa:= 1					
ole:= 1					
zip:= 1					1
Foremos	t finished at Wed W	Mar 20 03.50.6	13 2017		
root@ma	rdiah-X455LF:/home	/mardiah/Down]	loads#		
100 20110		rial acony bowing			

18. Berikut merupakan semua file yang kita dapatkan dari autopsy pada kasus narkoba diatas :

