Tugas Mata Kuliah

KEAMANAN JARINGAN KOMPUTER



Nama : Faris Abdul Aziz Nim : 09011181320020

Jurusan Sistem Komputer

Fakultas Ilmu Komputer Universitas Sriwijaya

2017

TUGAS 6

KOMPUTER FORENSIK

Komputer Forensik adalah salah satu cabang ilmu dalam forensic yang berkaitan dengan bukti illegal yang ditemui pada computer dan media penyimpanan digital untuk dapat disajikan sebagai barang bukti yang sah dipengadilan nanti.

Tools yang digunakan adalah:

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

Tahap pertama yang harus dilakukan ada mengekstrak file image.zip, setelah dilakukan ekstrak akan terdapat file image. Setelah itu masukkan perintah md5sum image.zip, md5sum sendiri digunakan untuk mengecek keaslian dari file tersebut. Dapat dilihat pada gambar 1.1 dibawah.



Gambar 1.1. Hasil perintah md5sum

Tahap selanjutnya adalah dengan memasukkan perintah file image, dimana file image berfungsi untuk melihat tipe filenya, dapat dilihat pada gambar 1.2 dibawah



Gambar 1.2. File Image

Tahap selanjutnya membuat directory baru dengan nama kasus.narkoba, dapat dilihat pada gambar 1.3 dibawah.

Computer				
Terminal	- + ×		Pictures	– + ×
<pre>faris@farismr - \$ sudo su [sudo] password for faris: Sorry, try again. [sudo] password for faris: farism f downloads/ farism for faris: mage.zip farism for bownloads # ls image image.zip farism Downloads # ls image image.zip farism Downloads # ls image image.zip farism Downloads # ls image image.zip farism faris faris faris faris 14096 Mar 29 12:54 . drwxr-xr-x 19 faris faris 4096 Mar 29 12:54 . drwxr-xr-x 19 faris faris 14096 Mar 29 12:54 . drwxr-xr-x 1 faris faris 14096 Mar 29 12:54 . drwxr-xr- 1 faris faris 14096 Mar 29 12:54 . drwxr-xr- 1 faris faris 18146 Mar 24 23:21 image.zip fariam Downloads # file image image.DoS floppy 1404k, x86 hard disk boot sector fariam Downloads # mkdir /tmp/kasus.narkoba/ imism Downloads # []</pre>	■ 157 GB Vol ■ 157 GB Vol ■ 105 MB Vo ▼ Network ☜ Network	bokmarks Help ↑ faris Pictures Screenshot from 2017- 03-29 12:54:49,png	Screenshot from 2017- 03-29 12:55:09.png	
			2 items, Free space: 6,2 GB	
🔟 Menu 🥅 🎽 🔚 📧 Terminal 👘 Pictures				👤 🖇 💉 🕪 🕼 97% 🚺 12:55 🖳

Gambar 1.3. Directory baru

Selanjutnya masukkan perintah mount image /tmp/kasus.narkoba/, yang dimana file image akan diekstrak pada directory kasus.narkoba, dan masuk ke dalam file kasus.narkoba dan dengan perintah ls kita dapat melihat file yang telah diekstrak. Dapat dilihat pada gambar 1.4 dibawah.



Gambar 1.4. Ekstrak file image

Selanjutnya masukkan perintah file * pada directory kasus.narkoba, yang dimana berfungsi sebagai perintah melihat tipe file secara keseluruhannya. Dapat dilihat pada gambar 1.5 dibawah.

Computer					
Terminal	- + ×		Pictures		- + ×
imaryam pownloads # LS image image.zip forlism Downloads # LS -al total 1468	File Edit View o	Bookmarks Help			ΞΞ Ξ Ξ <i>μ</i>
<pre>drwxr-xr-x 19 faris faris 4096 Mar 29 12:54 . drwxr-xr-x 19 faris faris 1474560 Sep 18 2002 image -rw-rr- 1 faris faris 1474560 Sep 18 2002 image -rw-rr- 1 faris faris 18146 Mar 24 23:21 image.zip bofo147f03923e1f420131d59D166a72 image.zip bofo147f03923e1f420131d59D166a72 image.zip image: DOS floppy 1440k, x86 hard disk boot sector foriem DownLoads # file image image image zip image zip image</pre>	' (Inp ct 57 GB Vol 105 MB Vo Vetwork	Screenshot from 2017- 03-29 1256:37,png	Screenshot from 2017- 03-29 12:55:09.png	Screenshot from 2017- 03-29 12:55:42.png	Screenshot from 2017- 03-29 12:55:16.png
			5 items, Free space: 6,2 GB		
					4 (48 B.00% (1765 B)
				I	

Gambar 1.5. File *

Tahap selanjutnya adalah memasukkan perintah autopsy, dan akan keluar seperti pada gambar 1.6.

Computer					
Terminal	- + ×		Pictures		- + ×
<pre>Tariismr kasus.narkoba # file * cover page.jpgc ut/output error)</pre>	' (Inp	Bookmarks Help			
SCHEDU-1.EXE: Z1p archive data, at least v2.0 to extr farian kasus.narkoba # autopsy	act • My Compute		ine i		
Autopsy Forensic Browser http://www.sleuthkit.org/autopsy/	🔲 Desktop	Screenshot from 2017- 03-29 12:54:49.png	Screenshot from 2017- 03-29 12:55:09.png	Screenshot from 2017- 03-29 12:55:42.png	Screenshot from 2017- 03-29 12:56:16.png
ver 2.24	C. Music				
Evidence Locker: /var/lib/autopsy Start Time: Wed Mar 29 12:58:45 2017 Remote Host: localhost Local Port: 9999	Till Videos	03-29 12:56:37.png	03-29 12:56:55.png		
Open an HTML browser on the remote host and paste this URL in it: http://localhost:9999/autopsy	🔛 <u>File Syste</u> 🕛 Trash				
Keep this process running and use <ctrl-c> to exit □</ctrl-c>	▼ Devices ■ 321 GB V				
	157 GB Vol				
	Network				
	C Network				
			6 items, Free space: 6,2 G	3	
🔟 Menu 🥅 🐉 🖪 🖿 🛛 Terminal 👘 Pictures				1	\$ 💉 🐗 🛱 99% 🐨 12:58 🖵

Gambar 1.6. Autopsy

Selanjutnya kita buka browser dan masukkan localhost yang didapat dari autopsy tadi, dan akan muncul interface seperti pada gambar 1.7 dibawah, lalu pilih new case.



Gambar 1.7. Interface localhost autopsy

Selanjutnya masukkan data pada form create new case, dapat dilihat pada gambar 1.8 dibawah.

	Creat	te A New Case - Mo	zilla Firefox				-	+ ×
Create A New Case × +								
(I localhost:9999/autopsy?mod=0&view=1			C	Q Search	☆ 自	+ -	r 🗸	≡
	~		CLOT					
	C	REATEANEN	CASE					
1. C num	ase Name: The name bers, and symbols.	of this investiga	ition. It can contai	n only letters,				
2. D	escription: An option	al, one line des	cription of this cas	e.				
	(asus Narkoba							
3. Li inve	vestigator Names: T stigators for this case.	'he optional nar	nes (with no space	s) of the				
a	Faris	b. (
c.		d. (
e.		f. (
g.		h. (
i.		j. (
a 🖉	New Case	CANCEL		HELP				
Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla some data to Mozilla so that we can improve Firefox automatically sends some data to Mozilla so that we can improve automatically sends some data to Mozilla so that we can improve automatically sends some data to Mozilla some data to	ve your experience.				 	<u>C</u> hoose	What I Sh	nare ×
🔟 Menu 🥅 🎒 🎦 🚞 🔁 Terminal 👘 Pictures	😂 Create A Ne	w Case			1 *	× •) 🗎	¥99% 🗊	13:00 🖵

Gambar 1.8. Form Create New Case

Selanjutnya setelah membuat new case, akan muncul tampilan seperti gambar 1.9. lalu klik add host.



Gambar 1.9 Add host

Setelah itu lakukan penambahan host ada case tadi, dan isikan hostname pada kolom form host name, dapat dilihat pada gambar 1.10 dibawah.



Gambar 1.10. Form Add New Host

Lalu klik add image untuk menbahkan image pada case tersebut. Lalu masukkan file image yang telah diekstrak sebelumnya kedalam kolom location. Lalu ganti dengan Volume Image dan tekan ok Dapat dilihat pada gambar 1.11 dibawah.



	Open Imag	e In Kasus:Joe_Jacob - Mo	zilla Firefox						- +	×
IDecalhost:9999/autopsv?mod=0&view=10&case=Kasus8	host=loe_lacob&inv=Faris		C	Q Search		☆ #	h	\$		=
Case: Kasus Host: Joe_Jacob	No images Select the Add	have been added to Image File button be ADD IMAGE FILE HELP	this host yet slow to add or CLO	ne se Host						
	FILE ACTIVITY TIME LINES		EVENT SEQUEN	DATABASES						
 Firefox automatically sends some data to Mozilla so that we ca Menu Menu Menu 	n improve your experience. Irctures Dopen Image Add Image	e In Kasus • To Kasus:Joe_Jacob - Mo:	zilla Firefox	_	-	T	<u>C</u> ho ∦ ≠ 4	ose Wh	at I Shar 6 😨 13 — +	e × :00 🖵
Add Image To Kasus: Joe J × +				O. court		~ ~			_	_
Case: Kasus Host: Joe_Jacob	bactose nobodnin fantada 1900/12	ADD & NEW IMAGE		Jearch						-
	 1. Location Enter the full path (starting If the image is split (either extension. /home/faris/Downloads/image 2. Type Please select if this image i Disk 3. Import Method To analyze the image file, i be imported from its curre or by moving it. Note that i then the image could becom Symlink 	g with /) to the imag raw or EnCase), the file is for a disk or a Partition t must be located in nt location using a s if a system failure or me corrupt. Copy	e file. n enter '*' for single partition the evidence ymbolic link, incurs during t MELP	the on. locker. It can by copying it, he move, love						
Firefox automatically sends some data to Mozilla so that we can be made and the matter and thematter and the matter and the matter and the	n improve your experience.	To Kasus: 📄 Downloads				•	<u>C</u> ho	ose Wh	at I Shar	e × :01 ⊡1



Gambar 1.11. Pengisian image

Seelah itu pilih opsi ignore the hash value for this image, lalu pilih add. Dan setelah itu klik lagi pilihan add. Dapat dilihat pada gambar 1.12 dibawah.

Collecting details on new image file - Mozilla Firefox					- +	×
& Collecting details on new × +						
O localhost:9999/autopsy?mod=0&view=14&spl_conf=1&img_path=%2Fhome%2Ffaris%2FDownloads%2Fimage&sort=1&host=joe_jacot C Q Search	☆ (ê	÷	⋒	◙	≡
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)						
Analysis of the image file shows the following partitions:						
Partition 1 (Type: fat12) Mount Point: c: File System Type: fat12 ▼						
Firefox automatically sends some data to Mozilla so that we can improve your experience.			<u>C</u> hoos	se Wha	t I Shar	e ×
🛅 Menu 🥅 🕃 💽 📷 🗈 Terminal 👘 Pictures 💕 Collecting details on 😁 Downloads	1	* 🖌	,≪ 4 3) [C +9996	13	:02 🖵

Add a new image to an Autopsy Case - Mozilla Firefox								
∫ 🏡 Add a new image to an A 🗴 🕇								
🔄 🛈 localhost:9999/autopsy?mod=0&view=15&img_path=%2Fhome%2Ffaris%2FDownloads%2Fimage#_img=1&sort=1&do_md5=1&m C 🔍 Search	☆	Ê	+	⋒		≡		
Testing partitions Linking image(s) into evidence locker Image file added with ID img1								
Volume image (0 to 0 - fat12 - C:) added with ID vol1								
Firefox automatically sends some data to Mozilla so that we can improve your experience.			Choos	e Wha	t I Shar	×		
🔟 Menu 🥅 🎢 🗈 🖿 🗈 Terminal 👘 Pictures 👘 Addia new image to 🖿 Downloads		1 * ,	× •))	1 +99%	13:	02 모		

Gambar 1.12. Ignore image

Akan muncul tampilan seperti gambar 1.13, lalu klik details untuk melihat info dari case yang telah dibuat tadi, dan dapat dilihat pada gambar 1.13 dibawah.

Open Image In Kasus:Joe_Jacob - Mozilla Firefox									
🖉 Open Image In Kasus:Joe 🗙 🕂									
(i) localhost:9999/autopsy?mod=0&view=16&case=Kasus&	host=Joe_Jacob&inv=Faris	C Search	☆ 自 ♣	⋒	≡				
Case: Kasus Host: Joe_Jacob	Select a volume to analyze or add a new	image file.							
	Case Gallery Host Gallery	HOST MANAGER							
	mountnamefs typeC:/image-0-0fat12	details							
	Analyze Add Image File Hep	CLOSE HOST							
	FILE ACTIVITY TIME LINES IMAGE INTEGRITY VIEW NOTES EVEN	HASH DATABASES							
🖸 Siefer automatically cande come data to Maxilla esthature ca			Chaos	a What I Ch					
Contraction automaticany sends some data to Mozilla so that we can	ictures 😂 Open Image In Kasus 📄 Downloads		<u>€noos</u> £ * ≠ ••) (e what I Sh ≩•99% (1) 1	13:03 🖵				

Gambar 1.13. Tampilan open image

Pada tampilan ini terlihat file yang di analisis oleh autopsy pada case yang telah dibuat tadi, dapat dilihat pada gambar 1.14 dibawah.

Kasus:loe lacob:vol1	×	+			Kasus:Joe_J	acob:vol1 - Mozilla	Firefox								- +	×
(i localhost:9999/auto	psy?mod	=1&submod=	-2&case=Kasus&	host=Joe_Jacob&inv=Far	is&vol=vol1		C	Q Search			☆	Ê	+	俞		≡
		-		KEYWORD SEARCH	FILE TYPE	IMAGE DETAILS	META DATA	DATA UNIT	HELP	CLOSE						
Directory Seek Enter the name of		rent Dire	ectory: <u>C:/</u> Ge	NERATE MD5 LIST OF F	ILES											
a directory that you want to view. C:/	DEL	Type dir / in		WRITTEN		Accesse	D	CREATE	D		Sizi	E	UID	GID	ME	ra
		v / v	<u>SFAT1</u>	0000-0 00:00:0	0-00)0 (UTC)	0000-0 00:00:0	0-00 00 (UTC)	0000- 00:00	00-00 :00 (UT	C)	46	08	0	0	<u>45'</u>	<u>780</u>
View		v / v	<u>SFAT2</u>	0000-0 00:00:0	0-00)0 (UTC)	0000-0 00:00:0	0-00 00 (UTC)	0000- 00:00	00-00 :00 (UT	C)	46	08	0	0	<u>45</u>	<u>781</u>
File Name Search		v / v	<u>SMBR</u>	0000-0 00:00:0	0-00)0 (UTC)	0000-0 00:00:0	0-00 00 (UTC)	0000- 00:00	00-00 :00 (UT	C)	51:	2	0	0	<u>45'</u>	7 <u>79</u>
Enter a Perl regular expression		d / d	<u>\$0rphanFile</u>	<u>es/</u> 0000-0 00:00:0	0-00 00 (UTC)	0000-0 00:00:0	0-00 00 (UTC)	0000- 00:00	00-00 :00 (UT	C)	0		0	0	<u>45'</u>	<u>782</u>
for the file names you want to find.		r / r	<u>cover page</u>	<u>jpgc</u> 2002-0 08:30:5	9-11 52 (WIB)	2002-0 00:00:0	9-11 00 (WIB)	2002- 08:50	09-11 :27 (WI	B)	15	585	0	0	<u>8</u>	
	1	r / r	<u>Jimmy Jung</u> l	Le.doc 2002-0 14:42:3	4-15 80 (WIB)	2002-0 00:00:0	9-11 00 (WIB)	2002- 08:49	09-11 :49 (WI	B)	204	480	0	0	<u>5</u>	
SEARCH		r/r	<u>Scheduled</u> <u>Visits.exe</u>	2002-0 08:20:3	5-24 32 (WIB)	2002-0 00:00:0	9-11 00 (WIB)	2002- 08:50	09-11 :38 (WI	B)	10	00	0	0	11	
ALL DELETED FILES																
EXPAND DIRECTORIES						File Brow	vsing Mode	e								
Firefox automatically sends	some da	ata to Mozilla	so that we can ir	nprove your experience.									Choos	e What	I Share	×
🔟 Menu 🥅 🍯 🔁 🖿	🔁 Ter	minal	Pict	ures 🛛 👢	Kasus:Joe_Jacob:vo	ol1 📄 Download					1	2 *	_ه (۹۹ ک ^م	_ \ 99%	👽 13:	03 🖵

Gambar 1.14. File Analisis

Pada tampilan ini terdapat isi image detail, yang dimana pada halaman ini terlihat seluruh detail dari image pada case yang telah dibuat tadi. Dan pada halaman ini terdapat 2 sektor, yaitu sektor 73 dan 104. Dapat dilihat pada gambar 1.15 dibawah.



Kasus:Joe_Jacob:vol1 - Mozilla Firefox										- ×		
🅼 Kasus:Joe_Jacob:vol1 🗙 🕂												
(Iocalhost:9999/autopsy?mod=1&subm	od=7&case=Kasus&	host=Joe_Jacob&inv=Fa	ris&vol=vol1		C	Q Search		☆	é l	ŀ ∧		≡
	File Analysis	Keyword Search	FILETYPE		META DATA	DATA UNIT	HELP CLOSE					
Sectors before file system: 0												
File System Layout (in sectors) 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												
METADATA INFORMATION												_
Range: 2 - 45782 Root Directory: 2												
CONTENT INFORMATION												
Sector Size: 512 Cluster Size: 512 Total Cluster Range: 2 - 2848												
FAT CONTENTS (in sectors)												
<u>73-103 (31)</u> -> EOF <u>104-108 (5)</u> -> EOF												
🔟 Menu 🥅 🐉 🔄 🚞 🗈 Terminal	🚞 Pict	ures 🕴	Kasus:Joe_Jacob:vol	1 📄 Download	s			1	* 🗸	4) (+99	% 🚺 13	3:03 🖵

Gambar 1.15. Image Details

Lalu buka masing-masing sektor yang telah kita dapatkan tadi, makan tampilannya akan seperti pada gambar 1.16 dan dikategorikan sebagai data unit. Dapat dilihat pada gambar 1.16 dibawah.

Kasus:Joe_Jacob:vol1 - Mozilla Firefox —										
🅼 Kasus:Joe_Jacob:vol1 🛛 🗙 🕂										
(localhost:9999/autopsy?case=Kasus8	shost=Joe_Jacob&inv=Faris&vol=vol1&mod=1&submod=5█=73&len=31 C 🔍 🔍 Search 🏠 🖨 🗣 🏠	3	≡							
	FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA DATA UNIT HELP CLOSE									
Sector Number: 73 Number of Sectors: 1 Sector Size: 512										
Address Type: Regular (dd) Izaarus Addr: Lazarus Addr: ALLOCATION LIST	ASCII Contents of Sectors 73-183 in image-0-0 JFIF'.'	۱ ۱۹۲۰. ۹۹۲۰. ۱۰۰۰. ۱۰۰۰.	 							
🔟 Menu 🥅 🗳 🗈 🖿 🛛 Terminal	📄 Pictures 🔹 🎉 Kasusijoe Jacobvoli 📄 Downloads 👤 💲 🖉 🐠 🚇 99% 📢	13:	04 🖳							



Gambar 1.16. Data Unit

Pada sektor pada gambar 1.16 terdapat kode di awal data unit tersebut, yaitu JFIF dan PK yang artinya JFIF itu adalah gambar, dan PK ada file berupa zip. Dapat dilihat pada gambar 1.17 dibawah.

Kausta lashualt	w (w list of file signatures 106 - w l	List of file signatures - Wikipedia - Mozilla Firefox			- + ×			
Rasus joe jacob voi i	a.org/wiki/List_of_file_signatures	। c Q	Search		☆ 自 ♣ 佘 ♥ ☰			
	exr	OpenEXR image 0 v/1.						
	bpg	Better Portable Graphics format ^[7]	0	BPGû	42 50 47 FB			
				ÿøÿÛ	FF D8 FF DB			
	jpg jpeg	JPEG raw or in the JFIF or Exif file format	0	ÿØÿàJ F IF	FF D8 FF E0 nn nn 4A 46 49 46 00 01			
				ÿØÿáE x if	FF D8 FF E1 nn nn 45 78 69 66 00 00			
🔟 Menu 🚃 🎒 🛛 🖿	ilbm Ibm Ibm	IFF Interleaved Bitmap Image	0 shot from 201	FORM	46 4F 52 4D nn nn nn nn ♥ ≵ 중 ♥ №99% Ф 13:11 日			

(🗲) (i) 🔒 https://en.wikipedi	a.org/wiki/List_of_file_signatures	C Q S		☆ 自 🕹 ⋒ 💟 ☰	
	exe	(including NE and PE)	0	MZ	4D 5A
	zip jar odt				50 48 03 04
	ods odp docx	zip file format and formats based on it, such as JAR, ODF, OOXML	0	РК	50 4B 05 06
	xlsx pptx vsdx				(empty archive)
	apk				(spanned archive)
	rar	RAR archive version 1.50 onwards ^[8]	0	Rar!	52 61 72 21 1A 07 00
	rar	RAR archive version 5.0 onwards ^[9]	0	Rar!	52 61 72 21 1A 07 01 00

Gambar 1.17. Kode pada sektor

Lalu periksa file sektor yang telah didapatkan tadi dengan cara file vol1-sector73.raw, dan akan tampil seperti gambar 1.18 dibawah.

	Kasus:Joe_Jacob	vol1 - Mozilla Firefox					- ×
	Terminal – + >						
faris@farismr ~ \$ Cd Downloads/		=5 C	Q Search	☆ 自	• 俞		≡
<pre>image image.zip voll-Sector10 faris@farismr ~/Downloads \$ fil voll-Sector73.raw: JPEG image d for information for the sector for the sec</pre>	4.raw voll-Sector73.raw e voll-Sector73.raw ata, JFIF standard 1.01	DETAILS META DATA	DATA UNIT HELP CLOSE ? X				
Sector Number		EXPORT CONTENTS ADD N					
Number of Sectors:		* Hex (<u>display</u> - <u>report</u>) * npty (Zip archive data, at	ASCII Strings (<u>display</u> - <u>report</u>) t least v2.0 to extract))			
Sector Size: 512							
Ac dress Type:		p1H. <k.uq*6.\$< th=""><th>~uFNV0`6T#R#-4</th><th>HT.b.^.?.Rr</th><th>rf</th><th></th><th></th></k.uq*6.\$<>	~uFNV0`6T#R#-4	HT.b.^.?.Rr	rf		
Lazarus Addr:							
		N2.'JG8z.q8.<	Z^.%+B>nW3'. N	[!z.U	.f.~I	z	.7
ALLOCATION LIST	<pre></pre>	j.T?\$RUfH %@4N'L".1d.Q~_bY.Z L.r4.~B> 3F.:S.LY/* R? <.E.6M:.A)4 lX.c.yV <f.u O.I.I.qPKZ.,U</f.u 	QI+6Q.g.42+bN.c.X.W6 G.h 9.MXXZ. 3 .%.F.p.]6n%.&F\< 9.vI.\.n.C.m.Ezk!M.? BScheduled Vis	{.>Ytp? 21 its.xlsPK	.;u.j z.Q.y !5B.	u 	p.' q HT.
🔟 Menu 🥅 🏹 🔚 🕅 Terminal	C Bictures 🛛 🖉 Kasus:joe_Jacob:vol1	🗂 Downloads 🛛 🖻 Scre	eenshot from 201 📧 Terminal	1 * 🗢	 (0) (0) 	% 🚺 13	3:13 🖵

Gambar 1.18. File vol1-secotr73.raw

Format .raw pada sector73 diubah menjadi .jpg, dan akan berubah menjadi gambar. Dan kabar tersebut dapat dilihan pada gambar 1.19 dibawah.



Gambar 1.19. Gambar sector73

Lalu masukkan perintah String vol1-sector73.jpg, yang dimana string berguna untuk melihat readable pada sebuah file. Dan kita akan mendapatkan sebuah password untuk masuk pada .zip sector104.zip. Dapat dilihat pada gambar 1.20 dibawah,





Gambar 1.20. String sector73

Masukkan password yang didapatkan dari perintah string pada gambar 1.20 kedalam file sector104.zip, setelah itu buka file yang ada didalam zip tersebut. Dapat dilihat pada gambar 1.21 dibawah.

Downloads		- + ×				- + ×
File vol1-Sector104.zip	- + ×					
Archive Edit View Help		.) <				
🚔 📮 🛅 Open 👻 🖳 Add Files 👌 Extract						
🗢 Back 🗭 🛧 🃥 Location: 🚞 /						
Name 🔻 Size Type	Modified	image.zip				
Scheduled Visits.xls 🖪 16,9 kB Microsoft Exce	23 May 2002, 11:20					
Archive Manager	×					
Password required for "vol1-Sector	04.zip"					
Descurate						
Password.						
Cancel	ОК					
· · · · · · · · · · · · · · · · · · ·						
						z7
						··
1 object (16,9 kB), 1 object selected (16,9 kB)						
						(
The selected (2,6 kB), Free The selected (2,6 kB), Free	space: 6,2 GB	— 0 —				
FFFy U.Xh8						}.n.EOH
NrH' <eui@1;(65 17a%</eui@1;(65 						
9'p+						
oqk4						
I+^L nw=goodtimes						
faris@farismr ~/Downloads \$						
🔟 Menu 🥅 🛃 🔚 🗈 Terminal 🛛 🔤 Pictures 🛛 💆 Kası	us:Joe_Jac 📄 Downloads	Screenshot fr	Terminal	🖻 vol1-Sector73 🔡 vol1-Secto	r10 👤 🖇 🖘 📣 🖾 99	% 💿 13:16 🖵

	Scheduled Visits.xls - LibreOffice Calc - + ×																
File Edit View Insert Format Tools Data Window Help ×																	
1																	
-	□ Ariol																
B50	B50 \checkmark $f(x) \sum = Monday(1)$																
	Α	в	C		D	E	F	G	н	I	J	к	L	М	N	0	Τō
1	Month	DAY	HIGH SCHOOL	<u>S</u>													
2	2002	2															
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)														
HI	H Sheet1	Sheet2 /Sheet3 / 🖶 /															
She	et 1 / 3		PageStyl	e_Sheet1				=I	C		Su	um=0				+ 1	00%
	Menu 🥅	🎒 🖻 📄 🖻	Terminal 🛑 Pictures	😂 Kasus:Joe_J	Downloads	Screensho	t 🖻	Terminal	🖻 vol1	1-Sector	Vol1-Se	ctor	Scheduled	. 👤 🕴	🗢 🕪 🚉	9% 🛈 13:	16 모

Gambar 1.21. File sector104.zip

Kembali lagi pada localhost, lalu masukkan dir entry number dengan angka 11, dan akan muncul tampilan seperti gambar 1.22 dibawah.



Gambar 1.22. Meta Data

Lalu masukkan perintah foremost –v –i image –o recover, yang berfungsi untuk mengembalikan data yang tertimpa dan recover sebagi extrak file ini. Dapat dilihat pada gambar 1.23 dibawah.









Gambar 1.23. Foremost dan isi file recovery

Lalu open with pada sector73 dan ubah ke GHex. Dan akan muncul tampilan file tersebut setelah diubah menjadi format GHex, dapat dilihat pada gambar 1.24 dibawah.



		Downloads	- + ×		- + × + ×
File Ed	it View Go Bookmarks Help				
+		vol1-Sector73.jpg - GHex	- + ×	s 🛎 🖪 ¶ 👂	
	File Edit View Windows Help				
▼ My	00000000EE D8 EE E0 0	00 10 44 46 49 46 00 01 01			
\odot	0000001000 60 00 00 F	FF DB 00 43 00 08 06 06 07	06 05 08.`C	······································	\cap
	0000002007 07 07 09 0	09 08 0A 0C 14 0D 0C 0B 0B	0C 19 12		
	0000003013 OF 14 1D 1	1A 1F 1E 1D 1A 1C 1C 20 24	2E 27 20 \$.'		
	0000004022 2C 23 1C 1	1C 28 37 29 2C 30 31 34 34	34 1F 27",#(7),01444.'		
		3C 2E 33 34 32 FF DB 00 43	32 32 32 32 21 12222		
1	0000007032 32 32 32 32	32 32 32 32 32 32 32 32 32 32	32 32 32222222222222222222		
	0000008032 32 32 32 3	32 32 32 32 32 32 32 32 32 32	32 32 32 2222222222222222		
s,	0000009032 32 32 32 3	32 32 32 32 32 32 32 32 32 32	32 FF C02222222222222		
1	Signed 8 bit: 70	Signed 32 bit: 16842822	Hexadecimal: 46		
🔻 Dev	Unsigned 8 bit: 70	Unsigned 32 bit: 16842822	Octal: 106	nes Magazine! Thanks for	
	Signed 16 bit: 70	Float 32 bit: 2,369375e-38	Binary: 01000110	umbia.	
	Unsigned 16 bit: 70	Float 64 bit: 7,120243e-307	Stream Length: 8 – +	't stop buying from me.	
- Net	Show little endian de	ecodina Showi	insigned and float as beyaderimal	students. You must have	
-				only one you sell to?	
•	Offset: 0x9; 0x4 bytes from 0x6 to 0x9	3 selected			
	vol1-9	Sector73.jpg" selected (15,9 kB), Free space: 6,2	2 GB	cover myself and not be	
5 TILL.	-	predictive. Tell me v	what you think. To open it, use the same pa	assword that you sent me	
jpg:=	-	before with that file.	Talk to you later.		
zip:=	-	Thanks,			
Foremo	=	Joe			č.
faris@	Page 1 / 1 175 words, 91	0 characters Default Style	English (USA)	C 0001	
🔟 Mei	nu 📺 🔮 💽 🛅 🗈 Terminal	🚞 Pictures 🛛 🛃 Kasus:J 📁 Downlo	🖻 Screen 🗈 Terminal 🔊 vol1-Se	🔡 vol1-Se 🗈 Schedul 🗈 Untitled 怪 v	ol1-Se 👤 🖇 🗢 🐗 🕞 99% 😗 13:21 🖵

Gambar 1.24. GHex

Setelah mendapatkan data yang dicari pada gambar-gambar diatas, maka kita dapat memberikan beberapa informasi yang diperlukan untuk bahan penyelidikan, Berikut beberapa pertanyaan yang diminta:

- Siapa pemasok narkoba Joe Jacob dan apa alamatnya?
 Jawab: Jimmy Jungle adalah pemasok narkoba pada Joe Jacob, dan beralamat pada 626 Jungle Ave Apt 2.
- 2. Data penting apa yang terdapat di file coverage.jpg dan mengapa data tersebut penting? Jawab: File Scheduled Visit.xls, tetapi file ini harus diakses menggunakan password yang telah diberikan sebelumnya. Informasi penting yang didapatkan pada file tersebut adalah dimana tempat-tempat yang mereka lakukan sebagai tempat transaksi kepada Joe Jacob.
- 3. Nama sekolah selain Smith Hill yang sering menjadi tempat transaksi Joe Jacob? Jawab: Key High School, Leetch High School, Birard High School, Richter High School dan Hull High School.
- 4. Untuk setiap file proses apa yang diambil oleh tersangka untuk mengelabuhi orang lain? Jawab: Dengan cara mengubah format .zip menjadi format .raw pada file vol1sector73 dan sector104.

5. Proses apa yang digunakan penyidik untuk berhasil memeriksa seluruh isi dari setiap file? Jawab: Pada penyidikan ini digunakan beberapa tools, yaitu autopsy, foremost dan GHex. Yang dimana tools tersebut dapat melacak dan mendapatkan informasi dalam kasus ini. Seperti tempat transaksi yang dilakukan kepada Joe Jacob, serta surat yang diberikan oleh Jimmy Jungle kepada Joe Jacob.