Nama	: Riki Andika
NIM	: 09011181320015

Hang on Training, Kamis 23 Maret 2017

Computer Forensics

Keamanan komputer merupakan hal yang menarik untuk dipelajari dan ikuti perkembanganya. Perkembangan dunia Information Technology (IT) yang sangat cepat telah melahirkan dimensi lain dari teknologi, yaitu kejahatan dengan peran komputer sebagai alat utamanya, istilah yang populer untuk modus ini disebut dengan cybercrime. Adanya kecenderungan negative dari teknologi komputer tersebut telah memunculkan berbagai permasalahan baru, baik secara mikro karena hanya berefek pada tingkatan personal/perseorangan, sampai kepada persoalan makro yang memang sudah pada wilayah komunal, publik, serta memiliki efek domino kemana-mana. Suatu sudah dalam bidang Information Technology (IT) nya, Negara yang maju pemerintahan setempat atau Profesional swasta bahkan telah membentuk polisi khusus yang bertugas untuk menindak kejahatan yang spesifik menangani permasalahanpermasalahan ini.

Cyber Police adalah polisi *cyber* yang diberikan tugas untuk menindak pelakupelaku kriminalitas di dunia *cyber*, yang tentu saja agak sedikit berbeda dengan polisi konvensional, para petugas ini memiliki kemampuan dan perangkat khusus dalam bidang komputerisasi, sehingga dapat dengan mudah dalam menindak setiap tindakan jahat yang berhubungan dengan *cyber crime* (kejahatan dunia maya). *Computer Forensics* merupakan 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. Adapun tujuan dari *computer forensic* ini ialah sebagai berikut;

- Membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat butki yang sah di pengadilan.
- b. 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 pihakpihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan tersbeut.

Terdapat 3 fokus data yang dilakukan dalam *Computer Forensics* yang dikategorikan sebagai berikut;

a. Active Data

Informasi terbuka yang dapat dilihat oleh siapa saja, terutama data, program, maupun file yang dikendalikan oleh sistem operasi.

b. Archival Data

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.

c. Latent Data

Informasi yang membutuhkan alat khusus untuk mendapatkannya karena sifatnya yang khusus, misalnya: telah dihapus, ditimpa data lain, rusak (corrupted file), dan lain sebagainya

Pemahaman mengenai Computer Forensics membutuhkan pembelajaran lebih mendalam, sehingga untuk lebih mengerti, sebagai contoh dilakukan pemecahan kasus melalui simulasi yang dilakukan, dengan contoh kasus yang selesaikan ialah kasus penyebaran dan penggunaan narkoba, Kasus yang diselesaikan menggunakan tools pendukung sebagai software yang digunakan untuk membatu dalam penyelesaian kasus tersebut, dengan tools yang digunakan seperti autopsy, ghax dan foremost. Iformasi yang ada berikut ulasannya "Telah tertangkap seorang pengedar narkoba yang telaha memiliki banyak jaringan yang dapat dikatakan bos dari semua bos narkoba, polisi kesulitan untuk melakukan pengungkapan secara menyeluruh terhadap jaringan pengedar karena minimnya informasi yang tersedia, kita di minta untuk membantuan pihak kepolisi untuk melakukan forensic terhadap file yang di temukan pada harddrive pelaku guna mendapatkan informasi lebih lanjut".

Dengan beberapa point informasi yang dicari sebagai berikut;

- 1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?
- 2. What crucial data is available within the coverpage.jpg file and why is this data crucial?
- 3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?
- 4. For each file, what processes were taken by the suspect to mask them from others?
- 5. What processes did you (the investigator) use to successfully examine the entire contents of each file?

Jawab:

5. What processes did you (the investigator) use to successfully examine the entire contents of each file?

Penyelesaian kasus atau langkah-langkah investigasi dari kasus ini menjawab pertanyaan nomor 5, dengan langkah-langkah simulasi yang dilakukan dalam penyelesaian kasus narkoba tersebut sebagai berikut;



Gambar 1. Website old.honeynet.org/scans/scan24/

Download file dengan extention zib, dengan nama image.zib yang akan digunakan sebagai bhaan dalam meyelesaikan kasus narkoba tersebut, kemudian cek keaslian dari file yang telah didownload dengan menggunakan perintah md5sum image.zip. dengan hasil seperti pada gambar 2, sebagai berikut;



Gambar 2. Mengecek keaslian file

Setelah melihat keaslian file yang didownload extrak file tersebut kemudian lihat rincian dari file image yang telah di extrak dengan perintah file image, maka akan kelihatan rincian dari file image, seperti yang terlihat pada gambar 3.



Gambar 3. Rincian file image

Dari rincian yang diperoleh, dapat dilihat file image yang dipeoleh tersebut merupakan file dari hardisk yang telah rusak *(boot sector)*. Setelah itu buat folder baru didalam folder tmp kemudian mount file image tersebut letakkan hasil mount dalam file system dalam folder yang telah dibuat dengan perintah mount image /tmp/kasus-narkoba/, dengan hasil screenshot yang dapat dilihat pada gambar 4 dengan hasil mounting yang telah dilakuakn dapat dilihat pada gambar 5.



Gambar 5. Mounting file image



Gambar 6. Hasil mounting

File yang ada didalam folder tmp/kasus-narkoba/ dengan hasil mounting dari file image tersebut lakukan pengecekan utilitas file dengan perintah file *, yang artinya mengecek semua utilitas dari file yang ada didalam folder kasus-narkoba, dengan hasil prenscren sebagai berikut;

Terminal	-	+	×
File Edit View Terminal Tabs Help			
riki@riki-X200MA /tmp/kasus-narkoba \$ su			
Password:			
riki-X200MA kasus-narkoba # ls			
cover page.jpgc SCHEDU~1.EXE			
riki-X200MA kasus-narkoba # file * Terminal			
cov <mark>eripagesjpgc</mark> apire-4739 kaERRORarcannot readpšcover page.jpgc		(In	р
ut/output error)			
SCHEDU~1.EXE:Zip-archive-data,=at-least-v2.0-to-extract			
riki-X200MA kasus-narkoba #			
Autopsy Forensic Browser			
had a stand of the second stand st			

Gambar 6. Cek utilitas file

Setelah file image berhasil dimounting, buka localhost dari tools The Autopsy Forensic Browser yang merupakan antarmuka grafis untuk tool analisis investigasi diginal dengan perintah baris The Sleuth Kit, yang dapat menganalisis disk dan filesistem Windows dan UNIX (NTFS, FAT, UFS1/2, Ext2/3). Langkah selanjutnya ialalh dengan menjalankan tools autopsy dan membuka local host dengan alamat localhost:9999/autopsy, dengan hasil seperti pada gambar 7.

Keamanana Jaringan Komputer_Tugas 6



Gambar 7. Tampilan localhost autopsy

Setelah membuka alamat localhost dari tools autopsy tersebut, lakukan pengisian form untuk menyelesaiakan kasus yang ditangani, dengan mengisi data-data, seperti pada gambar 8 berikut;

	Create A New Case - Mozil	la Firefox			- +	×						
http://old.hon/scans/scan24/ 🗴 🎪 Create A New Case 🔅	× +											
(♦) ♦ ③ localhost:9999/autopsy?mod=0&view=1		C	Q Search	☆ 自 ♣	* 🛡 :	≡						
o Kost Visited ▼ S Linux Mint C Community S Forums S Blog	News 🕶											
CREATE A NEW CASE												
CREATE A NEW CASE												
1. C num 2. D 3. Ir inve a. c. g. j. i.	ase Name: The name of this invest bers, and symbols. (asus escription: An optional, one line d asus Narkoba escription Names: The optional r stigators for this case. (Bid Andika) (Case) (Bid Andika) (Case) (Cancel)	igation. It can contai escription of this case hames (with no space h L L L L L L L L L L L L L L L L L L	n only letters, e. s) of the									
🔟 📰 💆 🔄 😫 Cara Recovery 😫 Create A New	7.png - Image 💼 Downloads - Fi 🚞 kasu	s-narkoba 🖪 Terminal	Terminal Save screensh	2017-03-27 17:46	🗲 et)) 🕞	*						

Gambar 8. Form create new case

Setelah kasus dibuat maka akan muncul nama kasus yang telah dibuat dengan tampilan

seperti yang terlihat pada gambar 9 berikut;

Case Details
Name: Kasus Description: Kasus Narkoba
Created: Mon Mar 27 17:45:50 2017
окъ

Gambar 9. Case Detail

Setelah membuat kasus baru yang akan diselesaikan maka akan menampilkan dialog box yang akan menuju ke import image yang akan diinvestivigasi dengan menggunakan tools autopsy, dengan menampilkan dialog box yang dapat dilihat pada gambar 10.a, 10.b, dan 10.c.

	Add A New Host To Kasus - Mozilla Firefox				-	+ ×
http://old.hon/scans/scan24/ 🗙 🎪 Add A New Host To Kasus 🗙 🕂						
O localhost:9999/autopsy?mod=0&view=7&case=Kasus&x=76&y=8	67%) C] 🔍 Search	☆ (1	俞		≡
🛅 Most Visited 🔻 🖺 Linux Mint 🐌 Community 🐌 Forums 🐌 Blog 📗 News	•					
Case: Kasus						
	ADD A NEW HOST					
	1. Host Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols.					
	host					
	2. Description: An optional one-line description or note about this computer.		₽			
	 Time zone: An optional timezone value (i.e. ESTSEDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files. 					
	 Timeskew Adjustment: An optional value to describe how many seconds this computer's clock was aut of sync. For example, if the computer was 10 seconds fault, then enter'-10 to compensate. 					
	5. Path of Alert Hash Database: An optional hash database of known bad files.					
	6. Path of Ignore Hash Database: An optional hash database of known good files.					
	ADD HOST CANCEL HELP					
🔟 🥅 😫 🔲 😫 Cara Recovery 😫 Add A New Ho 🦷 9.ppg - I	mage 🔄 Downloads - Fi 📄 kasus-parkoba 🖪 Terminal 🛛 🗖 Terminal	L O 2	017-03-2	7 💉	⊲ ≫) □	

Gambar 10.a Dialog Box 1

Keamanana Jaringan Komputer_Tugas 6

Adding Host host1 to Kasus - Mozilla Firefox						
http://old.hon/scans/scan24/ × 🎪 Adding Host host1 to Kasus × +						
🔄 🛈 localhost:9999/autopsy?mod=0&view=8&case=Kasus&host=host1&desc=&tz=8ks=0&alert_db=&exclude_db=&x=81&y=17 C Q. Search] ☆	≜ √	ŀ ∧		≡	
📷 Most Visited 🔻 🕲 Linux Mint 🕲 Community 🗟 Forums 🗟 Blog 🛛 🔊 News 🕶						
Adding host: host1 to case Kasus						
Host Directory (/var/lib/autopsy/Kasus/host1/) created						
Configuration file (/var/lib/autopsy/Kasus/host1/host.aut) created						
We must now import an image file for this host						
Add Image						
Ν						
ty.						
🔟 📰 🔯 📓 🔛 🖉 Cara Recovery 💱 Adding Host h 💻 11.png- Imag 👔 Downloads - Fi 📷 kasus-narkoba 🖻 Terminal 🖉 Terminal	.0	2017-03 17:48	-27 💉	«») 🗆	8	

Gambar 10.b Dialog Box 2.

Open Image In Kasus:host1 - Mozilla Firefox http://old.hon/scans/scan24/ 🛪 👔 Open Image In Kasus:hos 🗙 🕂								×
() localhost:9999/autopsy?mod=0&view=10&case=Kasus&host=host1		C	Q Search	☆	≙ ∔	俞		=
😸 Most Visited ▼ 🖺 Linux Mint 🐌 Community 🖫 Forums 🐌 Blog 🔊 News ▼								
Case: Kasus Host: host1	· · · · · · · · · · · · · · · · · · ·							
No	images have been added to th	us host yet						
Select	the Add Image File button bel	ow to add or	ne					
	ADD MAGE FILE	CLO	SE HOST					
	INES MAGE INTEGRITY	HASH I	DATABASES					
🔟 📰 💆 📓 🔛 💐 Cara Recovery 💆 Open Image In 💻 11.png - Imag	💼 Downloads - Fi 🚞 kasus-narkoba	Terminal	Terminal	Save screensh	2017-03-27 17:48	((1) کم		*

Gambar 10.c Dialog Box 3

Setelah melalui beberapa dialog box yang akan mengarahkan ke inport image yang akan diinvestivigasi, maka langkah selanjutnya memasukkan alamat dari file image yang akan diinvestivigasi, seperti pada gambar 11 berikut;

Keamanana Jaringan Komputer_Tugas 6



Gambar 11. Add a new image

Setelah memasukkan image yang akan diinvestivigasi, makan akan menampilkan beberapa dialog box yang akan mengarahkan keberhasilan dari file yang diupload kedalam tools autopsy untuk dilakukan forensic dari kasus narkoba untuk mencari informasi-informasi terkait.

Collecting details on new image file - Mozilla Firefox							
() localhost:9999/autopsy?mod=0&view=14&host=host1&case=Kasus&inv=unknown&img_path=%2Fhome%2Frik%2FDownloads%2Fim; C Q Search	☆自	+	俞		≡		
🛅 Most Visited 🔻 🗓 Linux Mint 📱 Community 🖫 Forums 🖺 Blog 🔂 News 🔻							
Warning: Autopsy could not determine the volume system type for the disk image (i.e. the type of partition table). Please select the type from the list below or reclassify the image as a volume image instead of as a disk image.							
Disk Image O Volume Image O Volume Image O Volume Image O							
ок b							
🔟 📰 📓 📓 🖓 Cara Recovery 👹 Collecting deta — 14.png - Imag 🗊 Downloads - Fi 📷 kasus-narkoba 🛽 Terminal 🖉 Terminal	. 🔿 201	17-03-27 17:51	<u>م</u> ر 12) 🗗	*		

Gambar 12.a

Keamanana Jaringan Komputer_Tugas 6

Collecting details on new image file - Mozilla Firefox			-	+ ×
http://old.hon/scans/scan24/ 🗙 🛞 Collecting details on new 🗙 🕂				
O localhost:9999/autopsy/mod=0&view=14&spl_conf=1&img_path=%2Fhome%2Frik%2FDownloads%2Fimage&sort=1&host=host1&cas C Search	☆自	+	r 🛡	≡
👼 Most Visited 🔻 🖫 Linux Mint 🖫 Community 🖫 Forums 🖺 Blog 🛛 🔂 News 🔻				
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)				
 <u>Ignore</u> the hash value for this image. 				
 <u>Calculate</u> 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 V				
Ň				
🔟 📰 🛂 📓 📴 🖉 Cara Recovery 😰 Collecting deta — 12 png - Imag 📷 Downloads - Fi 📷 kasus-narkoba 🕿 Terminal 🛛 🖉 Terminal	0 2017	-03-27 :52	≶ ৰা)) ⊑) 💦

Gambar 12. B

Open Image In kasus-joe_Jacob - Mozilla Firefox									+ ×
👻 Bantu Evakuasi Mahasis 🗴 💪 un	niversitas sriwijaya - Pe 🗴 The Honeynet Project	🗙 📑 (1) Facebook	×	Open Image In kasus:Joe × +					
(Iocalhost:9999/autopsy?mod=0&view	w=10&case=kasus&host=Joe_Jacob		C	Q Search	☆ 自	+		7	≡
🛅 Most Visited 👻 🕒 Linux Mint 🕲 Commun	nity 🖲 Forums 🖺 Blog 🔝 News 🕶								
Case: kasus Host: Joe_Jacob	No income		h						
	No image	s have been added to this	nost yet						
	Select the Ad	d Image File button below	to add on	le					
			CLOS	E HOST					
		HELP							
	FILE ACTIVITY TIME LINES		HASH D	DATABASES					_
	View Notes	Ev	ENT SEQUENCE	ER					
			N						
			6	3					
		Litteratio file	uluba G	Terminal Streminal	2017	-03-28		_	-
🕛 📰 🛃 📓 🔛 💆 Open Image In	Ka – 10.png - Image VI – 10.png - Image VI	kjktorensic - Hie	arkoba - Fi	erminal		:00	11 100	0	1

Gambar 12. c

Setelah dengan dialog box yang akan menuju ke kasus yang telah dibuat, maka kasus berhasil dibuat dengan menampilkan hasil seperti pada gambar 13 berikut;

Keamanana Jaringan Komputer_Tugas 6

	Open Image In kasus:Jo	oe_Jacob - Mozilla Firefox			- + ×
🟺 Bantu Evakuasi Mahasis 🗴 🌀 universitas sriwijaya - P	e 🗙 The Honeynet Project 🗙 🗙	Facebook	🗙 🏠 Open Image In kasus:Joe 🗴	+	
(I localhost:9999/autopsy?mod=0&view=16&case=kasus&h	ost=Joe_Jacob&inv=unknown		C Search	☆ 自 ♣	☆ ♡ ≡
Most Visited 🕶 🖺 Linux Mint 🖺 Community 🖫 Forums 🐚 Bl	og 🔝 News 🕶				
Case: kasus Host: Joe_Jacob	Select a volume to an	alyze or add a new ir	nage file.		
	CASE GALLERY HOS	GALLERY	HOST MANAGER		
	mount name ○ C:/ image-0-0	fs type fat12	details		
		HELP	CLOSE HOST		
	FILE ACTIVITY TIME LINES IM	AGE INTEGRITY	HASH DATABASES		
		\$			
🔟 📰 🙋 🔲 🔛 Gpen Image In — 14.png - Imag.	📁 10.png - Imag 📄 tugas6 - File M	Downloads - Fi 🚞 tug	as6 - File M 🖪 Terminal 🛛 🛛 Te	erminal 0 2017-03-2 17:09	8 al 40) 🗗 🚺

Gambar 13. Kasus yang telah dibuat pada tools autopsy

Pada gambar 13 menunjukkan kasus yang telah dimasuukan atau dibuat dalam tools autopsy dengan nama kasus ialah kasus dan hostnya adalah Joe_Jacob. Kemudian dari kasus yang telah dimasukkan lakukan analisa dengan mengklik tombol analyse, dengan menampilkan hasil seperti pada gambar 14 berikut;

			kasus:Joe_Jacob	vol1 - Mozilla Firefox	•				-	+ ×
😌 Bantu Evakuasi Mahasi	s 🗙 G uni	versitas sriwijaya - Pe 🗙	The Honeynet Project X	Facebook X	🊯 kasus:Joe_Jacob:vol1 🛛 🗙 🕂					
(Iocalhost:9999/auto	psy?mod=1⊂	nod=2&case=kasus&host=Jo	e_Jacob&inv=unknown&vol=vol1	C	Q Search	☆ 自	+	俞		≡
🛅 Most Visited 👻 🔟 Linux N	lint 👅 Communi	ty 🖫 Forums 🐚 Blog 🔂	News 🔻							
		File Analysis Keyw	ORD SEARCH FILE TYPE	IMAGE DETAILS META DATA	DATA UNIT HELP CLOSE					
Directory Seek Enter the name of		Directory: <u>C:/</u> Generate	MD5 LIST OF FILES							
a directory that you want to view. C:/	DEL Ty	De NAME Q	WRITTEN	Accessed	CREATED	Size	UID	GID	ME	та
	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>45</u>	<u>780</u>
View	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>45</u>	<u>781</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>45</u>	<u>779</u>
Enter a Perl	d /	d <u>SOrphanFiles/</u>	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>45</u>	<u>782</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>	
file names you 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				File Prouving Mod	-					
				File browsing Mod		201	7.03.28			

Gambar 14. Analis File

Gambar 14 merupakan isi dari informasi yang dimiliki oleh hardrive tersebut, yang dapat dilihat dimana terdapat banyak kegiatan yang dilakukan, yang dimulai dari waktu palaku menulis, mengakses dan membuat file. Pada gambar 14 terdapat list dengan warna merah ayng memiliki arti bahwa isi dari list tersebut filenya sudah dihapus. Fakus pada dua file yang terdapat pada contet yang memiliki dua file yang dapat didownload dan untuk mendapatkan informasi-informasi yang berhubungan dengan kasus narkoba yang akan diselesaikan, dengan hasil screenshot yang dapat dilihat pada gambar 15 berikut:



Gambar 15. FAT Content yang ada didalam sektor

Dua file yang dapat didownlaod tersebut meruakan jejak yang ditinggalkan dalam kasus narkoba ini, dengan nama file 73-103 (31) dengan maksud terdapat informasi yang disembunyikan didalam sector 73 sampai dengan sektor 103, begitu pula dengan yang kedua 104-108 (5) terdapat informasi yang disembunyikan dalam sector 104 sampai 108. Pada sector 73-103 (31) hasil screenshot dapat dilihat pada gambar 16, terdapat format yang sangat asing sehingga sulit untuk dimengerti, untuk melakukan analisa dari file tersebut dilakukan secara manual dengan melihat bit pertama atau informasi hexa yang terdapat pada awal tulisan.

Keamanana Jaringan Komputer_Tugas 6

	kasus:joe_jacob:vol1 - Mozilla Firefox + ×									
💛 Bantu Evakuasi Mahasis 🗙 G uni	versitas sriwijaya - Pe 🗴 The Honeynet Project 🗴 😭 Facebook x / 🏤 kasus joe_jacobxol1 x 🕂									
🔦 🛈 localhost 9999/utopsy/tase=kasus&host=joe jacob&inv=unknown&vol=vol1&mod=1&submod=5█=73&len=31 C Q, Search 🛠 🖨 🦊										
🐻 Most Visited 🔻 🔞 Linux Mint 🔞 Community 🖫 Forums 🖫 Blog 🛛 🔊 News 🕶										
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	EXPORT CONTENTS ADO NOTE ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) File Type: JPEG image data, JFIF standard 1.01 Sectors: 73-103 Status: Allocated Find Meta Data Address									
Address Type: Regular (dd) Lazarus Addr:	ASCII Contents of Sectors 73-103 in image-0-0									
View ALLOCATION LIST	21.12222222222222222222222222222222222									
🔟 📰 💆 📓 🔛 😫 kasus:Joe_Jaco	📧 18.png - Imag 📁 10.png - Imag)🧮 tugas6 - File M 👔 Downloads - Fi 🚞 tugas6 - File M 🛛 Terminal 🛛 😢 Terminal 🖉 Terminal 🖉 2017.03-28 📶 🔊 📼 💈									

Gambar 16. Detail dari file 73-103 (31)

Gambar 16 menampilkan detail dari file 73-103 (31) dengan informasi yang dapat diambil yang terdapat pada baris pertama yaitu JFIF, dan kemudian informasi tersebut dapat dilihat dengan jelas, dengan mencari secara manual informasi di list of file singnature (wikipedia) seperti yang terilihat pada gambar 17, Begitu juga untuk file yang ada pada sector 104-108 (5).

Y list of signature file - Linu	× W List of file signatures - Wi × +	List of file signatures - Wikipedia - Mozilla Firefox			_
🗲 🗲 🕄 🔒 https://en.wikip	edia.org/wiki/List_of_file_signatures	C] Q	☆ 自 ↓ ☆ ♥		
🖥 Most Visited 👻 👅 Linux Mint	🖲 Community 🐚 Forums 🐌 Blog 📗 News 🕶				
	exr	OpenEXR image	0	v/1.	76 2F 31 01
	bpg	Better Portable Graphics format ^[7]	0	BPGû	42 50 47 FB
				ÿØÿÛ	FF D8 FF DB
	jpg jpeg	PEG raw or in the JFIE 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
ps://en.wikipedia.org/wiki//FIF	ilbm Ibm ibm	IFF Interleaved Bitmap Image	0 any	FORM ILBM	46 4F 52 4D nn nn nn nn 49 4C 42 4D

Gambar 17. List of file signature format JFIF

File dengan sector 73-103 (31) dengan analisa format yang diperoleh ialah format JFIF tersebut merupakan file dengan format JPEG, hal ini digunakan pelaku untuk menyembunyikan gambar dengan merubah format dari gambar tersebut menjadi raw.



Gambar 18. Mengecek utilitas file vol1-Sector73.raw

Sehingga untuk mengetahui kebenaran dan hasil dari forensics yang telah dilakukan dengan mengganti format dari file 73-103 (31) dengan nama vol1-Sector73.raw menjadi format JPEG, untuk mendapatkan informasi-informasi yang berhubungan kasus narkoba yang ditangani, dengan hasil screenshot yang dapat dilihat pada gambar 20.



Gambar 19. Mengganti format file menjadi JPEG



Gambar 20. File vol1-Sector73.raw setelah dirubah format JPEG

Begitu juga dengan file yang ada pada sector 104-108 (5) dilakukan hal yang sama dengan sector yang ada sebelumnya, dengan mengecek utilitas dari file dengan sector 104-108 (51) seperti pada gambar 21, dan mencari list of file signature (wikipedia) secara manual seperti pada gambar 22.



Gambar 21. Utilitas file sector 104-108 (5)

Dengan melakukan pengecekan utilitas dari file sector 104-108 (51) dengan nama file vol1-Sector104.raw, maka dapat dilakukan pencarian list of file signature (wikipedia) seperti pada gambar 22 berikut;

📔 list of signature file - Linu	× W List of file signatures - Wi × +			-	+ ×		
() Inttps://en.wik	ipedia.org/wiki/List_of_file_signatures	(C, Se	r.	1 🔒 🖡 🖝 🛡	≡		
🔯 Most Visited 🔻 👅 Linux Mir	nt 👅 Community 🖫 Forums 🖫 Blog 🔂 News 🔻						
	Iz	Izip compressed file	0	LZIP	4C 5A 49 50		
	exe	DOS MZ executable file format and its descendants (including NE and PE)	0	MZ	4D 5A		
	zip jar odt				50 4B 03 04	0	
	ods odp docx	zip file format and formats based on it, such as JAR, ODF, OOXML	0	РК	50 4B 05 06		
	ppbx vsdx apk				50 4B 07 08		
					(spanned archive)		
https://ap.wikipadia.org/wiki/JAP	rar (file format)	RAR archive version 1.50 onwards ^[8]	0	Rar!	52 61 72 21 1A 07 00		
zip	∧ ✓ Highlight <u>A</u> ll Mat <u>ch</u> Case <u>W</u> hole W	/ords 4 of 9 matches				×	
	TUGAS-KEAMANAN-J	22.png - Image Viewe 💽 vol1-Sector73.jpg - Im 😰 Downloads -	File Man 🖪 T	ferminal 🧕	2017-03-29II #3) 🕞	*	

Gambar 22. File of signature dari sector 104-108 (51)

Setelah mendapat informasi yang berhubungan dengan file sector yang dacari, dengan menyembunyikan format file, dimana pada sector 104-108 (51) dengan nama file voll-Sector104.raw pelaku menyembunyikan format zip dengan mengganti format menjadi raw, untuk membuktikan pembenaran dari analisa yang diperoleh dengan mengganti

format file tersebut menjadi zip, seperti yang terlihat pada gambar 23 dan dengan hasil yang diperoleh seperti pada gambar 24.

vol1-Sector104.	vol1-Sector73.jpg	0100 1101 1001 image					
Rena	ame "vol1-Sector104.raw" Enter the new name:	+ ×					
	vol1-Sector104.zip						
6	Cancel	Rename K-					
installer.run installe							

Gambar 23. Mengganti format file menjadi zip

Menghasilkan file dengan format zip, dimana didalam file dengan format zip tersebut terdapat file dengan format xls, tetapi file zip tersbut memiliki password untuk membuka isi dari file tersbut, untuk mendapatkan password tersebut pelaku menyimpan passwor didalam file sector 73-103 (31), jadi untuk membuka man cari tahu password dari file tersebut menggunakan tools strings dengan mengetikkan perintah string nama file yang akan string (string vol1-Sector73.raw), yang dapat dilihat pada gambar 24.



Gambar 24. Strings vol1-Sector73.raw

Dari hasil string yang telah dilakukan dengan hasil screen yang terdapat pada gambar 25, merupakan password disimpan pelaku kedalam file sector pertama dengan password yang diperoleh ialah goodtimes yang dapat digunakan untuk membuaka file zip yang merupakan file sector kedua, dengan hasil terlihat pada gambar 25.

<u>File E</u> dit <u>V</u> ie	w Insert Format	<u>T</u> ools <u>D</u> ata <u>W</u> indow <u>H</u> elp	Scheduled Visi	ts.xls - LibreO	Office Calc								-	+ × ×
🕒 • 🗗	• 🕞 📭 🖂	₿@\%0°* ₺		⊞⊞		11 1+ 1+	₩ ¤	ይ 🛱	₩ ⊶	• / =	* # #		Ø	
Arial	▼ 10 ▼	a a a 🔤 · 🗐 ·	문 표 표 교 =	₽ ₫ ₫	\$ %	0.0 🕤	00. 70 40 00.	등 원	⊞ •		•			
B50		Monday (1)												≡
A	B	C	D	E	F	G H	I	J	К	L	М	N	c T	
1 Month	DAY	HIGH SCHOOLS												
2 20	02													5
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)	N 1										0	6/11
9	Tuesday (2)	Smith Hill High School (A)	\$											J(X)
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)												1
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)												
	Sheet1 Sheet2	Sheet3												
Sheet 1 of 3			PageStyle_Sheet1				I B		Sum=0)		-0	- +	100%
🔟 📰 🐸	🗾 🔝 👪 vol1-S	ector10 🚺 (TUGAS-KEAM 🔯 (Li	st of file sign	si 🔲 25.pr	ig - Imag	[vol1-Sector7	'3 🕅 Dov	wnloads - Fil	🖪 Term	inal	2017. 13	03-29 al	«») 🗖	• 👔

Gambar 25. File dengan format xls yang ada dalam sector kedua

Tidak hanya dengan menggunakan tools string dan autopsy kasus ini juga dapat dipecahkan dengan menggunakan tools foremost, tools yang berfungsi berfungsi sebagai pengubah file tersebut menjadi folder, yang didalamnya terdapat informasiinformasi yang dibutuhkan, dengan perintah foremost –v –i nama_file –o recover, pada terminal, seperti yang terlihat pada gambar 26, setelah melakukan perintah diatas maka akan menampilkan folder yang berisi tentang informasi yang berhubungan dengan kasus narkoba yang ditangani dengan hasil yang diperoleh seperti ada gambar 27.

Keamanana Jaringan Komputer_Tugas 6



Gambar 26. Menjalankan tools Foremost

Dengan hasilyang diperoleh dari menjalankan tools foremost ini ialah mendapat kan 3 folder dari image yang dianalisa, seperti yang terlihat pada gambar 27 berikut.



Gambar 27. Hasil dari foremost file image

Folder-folder yang ada didalam folder recover, ini merupakkan informasi-informasi yang dibutuhkan dalam menangani kasus narkoba, sebagai contoh untuk file yang ada didalam folder doc, berisi file 0000003.doc dengan informasi yang ada didalammnya ialah surat pengedar narkoba dari kasus ini, seperti yang terlihat pada gambar 28.

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

Gambar 28. Isi folder doc setelah direcover

1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?

Joe Jacob adalah jimmy jungle, informasi tersebut terdapat pada sebuah email yang dikirimkan pada jimmy. (dapat dilihat pada gambar 28)

2. What crucial data is available within the coverpage.jpg file and why is this data crucial?

File gambar (jpg) yang diperoleh dari file sector 73-103 (31) adalah informasi password yang kita butuhkan untuk membuka isi dari file zip yang diperoleh dari file sector 104-108 (51). (dapat dilihat pada gambar 24)

3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent? Dari analisis yang telah dilakukan terdapat beberapa tempat yang dikunjungi oleh Joe Jacobs, untuk melakukan transaksi maupun pengedaran narkoba, seperti key high school ,leetch high school , birrard high school , richter high school dan hull high school. (dapat dilihat pada gambar 25) 4. For each file, what processes were taken by the suspect to mask them from others? Strategi yang dialkukan oleh pelaku dengan menyembunyikan format file pada file sector pertama sector 73-103 (31) dan file sector kedua sector 104-108 (51) (dapat dilihat pada gambar 19 dan 23) serta password dari file zip yang ada pada file sector 104-108 (51) yang disembunyikan didalam file sector 73-103 (31) (dapat dilihat pada gambar 24)