COMPUTER FORENSICS

Computer Forensic 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.

Tujuan dan Fokus Computer Forensic

Selaras dengan definisinya, secara prinsip ada tujuan utama dari aktivitas forensik komputer, yaitu :

- 1. 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.

Adapun aktivitas forensik komputer biasanya dilakukan dalam dua konteks utama. Pertama adalah konteks terkait dengan pengumpulan dan penyimpanan data berisi seluruh rekaman detail mengenai aktivitas rutin yang dilaksanakan oleh organisasi atau perusahaan tertentu yang melibatkan teknologi informasi dan komunikasi. Dan kedua adalah pengumpulan data yang ditujukan khusus dalam konteks adanya suatu tindakan kejahatan berbasis teknologi.

Sementara itu fokus data yang dikumpulkan dapat dikategorikan menjadi 3 (tiga) domain utama, yaitu:

- Active Data yaitu informasi terbuka yang dapat dilihat oleh siapa saja, terutama data, program, maupun file yang dikendalikan oleh sistem operasi.
- 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.

 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.

Manfaat dan Tantangan Computer Forensic

Memiliki kemampuan dalam melakukan forensik komputer akan mendatangkan sejumlah manfaat, antara lain :

- Organisasi atau perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti-bukti pendukung yang dibutuhkan.
- 2. Seandainya terjadi peristiwa kejahatan yang membutuhkan investigasi lebih lanjut, dampak gangguan terhadap operasional organisasi atau perusahaan dapat diminimalisir.
- 3. Para kriminal atau pelaku kejahatan akan berpikir dua kali sebelum menjalankan aksi kejahatannya terhadap organisasi atau perusahaan tertentu yang memiliki kapabilitas forensik komputer.
- 4. Membantu organisasi atau perusahaan dalam melakukan mitigasi resiko teknologi informasi yang dimilikinya.

Terlepas dari manfaat tersebut, teramat banyak tantangan dalam dunia forensik komputer, terutama terkait dengan sejumlah aspek sebagai berikut :

- Forensik komputer merupakan ilmu yang relatif baru, sehingga "Body of Knowledge"nya masih sedemikian terbatas (dalam proses pencarian dengan metode "learning by doing").
- Walaupun berada dalam rumpun ilmu forensik, namun secara prinsip memiliki sejumlah karakteristik yang sangat berbeda dengan bidang ilmu forensik lainnya – sehingga sumber ilmu dari individu maupun pusat studi sangatlah sedikit.
- 3. Perkembangan teknologi yang sedemikian cepat, yang ditandai dengan diperkenalkannya produk-produk baru dimana secara langsung berdampak pada berkembangnya ilmu forensik komputer tesebut secara pesat, yang membutuhkan kompetensi pengetahuan dan keterampilan sejalan dengannya.
- 4. Semakin pintar dan trampilnya para pelaku kejahatan teknologi informasi dan komunikasi yang ditandai dengan makin beragamnya dan kompleksnya jenis-jenis serangan serta kejahatan teknologi yang berkembang.

- 5. Cukup mahalnya harga peralatan canggih dan termutakhir untuk membantu proses forensik komputer beserta laboratorium dan SDM pendukungnya.
- 6. Secara empiris, masih banyak bersifat studi kasus (happening arts) dibandingkan dengan metodologi pengetahuan yang telah dibakukan dimana masih sedikit pelatihan dan sertifikasi yang tersedia dan ditawarkan di masyarakat.
- 7. Sangat terbatasnya SDM pendukung yang memiliki kompetensi dan keahlian khusus di bidang forensik komputer.
- 8. Pada kenyataannya, pekerjaan forensik komputer masih lebih banyak unsur seninya dibandingkan pengetahuannya (more "Art" than "Science").

Objek Forensik

- 1. Log file atau catatan aktivitas penggunaan komputer yang tersimpan secara rapi dan detail di dalam sistem.
- 2. File yang sekilas telah terhapus secara sistem, namun secara teknikal masih bisa diambil dengan cara-cara tertentu.
- 3. Catatan digital yang dimiliki oleh piranti pengawas trafik seperti IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System).
- 4. Hard disk yang berisi data/informasi backup dari sistem utama.
- 5. Rekaman email, mailing list, blog, chat, dan mode interaksi dan komunikasi lainnya.
- 6. Beraneka ragam jeis berkas file yang dibuat oleh sistem maupun aplikasi untuk membantu melakukan manajemen file (misalnya: .tmp, .dat, .txt, dan lain-lain).
- 7. Rekam jejak interaksi dan trafik via internet dari satu tempat ke tempat yang lain (dengan berbasis IP address misalnya).

Tahapan Aktivitas Forensik

Secara metodologis, terdapat paling tidak 14 (empat belas) tahapan yang perlu dilakukan dalam aktivitas forensik, sebagai berikut :

- Pernyataan Terjadinya Kejahatan Komputer merupakan tahap dimana secara formal pihak yang berkepentingan melaporkan telah terjadinya suatu aktivitas kejahatan berbasis komputer.
- Pengumpulan Petunjuk atau Bukti Awal merupakan tahap dimana ahli forensik mengumpulkan semua petunjuk atau bukti awal yang dapat dipergunakan sebagai bahan kajian forensik, baik yang bersifat tangible maupun intangible.

- 3. Penerbitan Surat Pengadilan merupakan tahap dimana sesuai dengan peraturan dan perundang-undangan yang berlaku, pihak pengadilan memberikan ijin resmi kepada penyelidik maupun penyidik untuk melakukan aktiivitas terkait dengan pengolahan tempat kejadian perkara, baik yang bersifat fisik maupun maya.
- 4. Pelaksanaan Prosedur Tanggapan Dini merupakan tahap dimana ahli forensik melakukan serangkaian prosedur pengamanan tempat kejadian perkara, baik fisik maupun maya, agar steril dan tidak tercemar/terkontaminasi, sehingga dapat dianggap sah dalam pencarian barang-barang bukti.
- 5. Pembekuan Barang Bukti pada Lokasi Kejahatan merupakan tahap dimana seluruh barang bukti yang ada diambil, disita, dan/atau dibekukan melalui teknik formal tertentu.
- Pemindahan Bukti ke Laboratorium Forensik merupakan tahap dimana dilakukan transfer barang bukti dari tempat kejadian perkara ke laboratorium tempat dilakukannya analisa forensik.
- Pembuatan Salinan "2 Bit Stream" terhadap Barang Bukti merupakan tahap dimana dilakukan proses duplikasi barang bukti ke dalam bentuk salinan yang identik.
- 8. Pengembangan "MD5 Checksum" Barang Bukti merupakan tahap untuk memastikan tidak adanya kontaminasi atau perubahan kondisi terhadap barang bukti yang ada.
- 9. Penyiapan Rantai Posesi Barang Bukti merupakan tahap menentukan pengalihan tanggung jawab dan kepemilikan barang bukti asli maupun duplikasi dari satu wilayah otoritas ke yang lainnya.
- Penyimpanan Barang Bukti Asli di Tempat Aman merupakan tahap penyimpanan barang bukti asli (original) di tempat yang aman dan sesuai dengan persyaratan teknis tertentu untuk menjaga keasliannya.
- 11. Analisa Barang Bukti Salinan merupakan tahap dimana ahli forensik melakukan analisa secara detail terhadap salinan barang-brang bukti yang dikumpulkan untuk mendapatkan kesimpulan terkait dengan seluk beluk terjadinya kejahatan.
- Pembuatan Laporan Forensik merupakan tahap dimana ahli forensik menyimpulkan secara detail hal-hal yang terjadi seputar aktivititas kejahatan yang dianalisa berdasarkan fakta forensik yang ada.
- 13. Penyerahan Hasil Laporan Analisa merupakan tahap dimana secara resmi dokumen rahasia hasil forensik komputer diserahkan kepada pihak yang berwajib.
- Penyertaan dalam Proses Pengadilan merupakan tahap dimana ahli forensik menjadi saksi di pengadilan terkait dengan kejahatan yang terjadi.

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.

Kita di minta bantuan untuk mendapatkan beberapa informasi di bawah ini :

- 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?

Tools yang digunakan untuk mendapatkan beberapa informasi yang diinginkan di atas:

- Autopsy
- Foremost
- Strings (*tidak perlu di install karena telah tersedia strings default pada linux/ubuntu)
- Ghex

Download file Image.zip pada situs <u>(old.honeynet.org/scans/scan24/image.zip)</u> dengan <u>md5 : b676147f63923e1f428131d59b1d6a72</u> untuk memastikan bahwa file yang telah di download adalah file yang asli maka gunakan opsion : md5ceksum image.zip pada terminal dan samakan dengan md5 file diatas.



Gambar.1 old.honeynet.org/scans/scan24/image.zip

Setelah file selesai di download, buka terminal pada direktori tempat file image.zip disimpan. Buat folder dengan option : mkdir /tmp/kasus.narkoba lalu image di maunting menggunakan option : #maunt image /tmp/kasus.narkoba/, masuk pada direktori folder yang telah dibuat cd /tmp/kasus.narkoba jika dijalankan option -1s akan tampak dua file yaitu cover page.jpgc dan SCEDU~1.EXE. Kita coba untuk mengekstrak file tersebut dengan option file *, maka hasilnya akan tampil seperti pada Gambar.2. Tampak bahwa file cover page.jpgc tidak bisa terbaca sedangkan SCEDU~1.EXE ternyata merupakan zip archive data.



Gambar.2 Ekstrak File Image.zip

Sampai pada langkah di atas, kita belum mendapatkan informasi apapun dari kasus yang kita tangani. Langkah selanjutnya fokus pada Latent Data karena data yang kita dapatkan sifatnya khusus (telah ditimpa data lain, dilakukan rename yang tidak sesuai dengan tipe file sesungguhnya). Jalankan tool autopsy sesuai gambar-gambar dibawah ini untuk mengidentifikasi file.

Certification (Contraction of the Contraction of th	C Q Search	合自	÷	^ (∍ ≡
📷 Most Visited 👻 🐌 Linux Mint 🐌 Community 🐌 Forums 🐌 Blog	<mark>ฌ</mark> News ▼				
	WARNING: Your browser currently has Java Script enabled.				
You do not need Java	Script to use Autopsy and it is recommended that it be turned off for security reason	15.			
	Autopsy Forensic Browser 2.24				
	OPEN CASE HELP				

Gambar.3 Autopsy Forensic Browser 2.24

(Iocalhost:9999/autopsy?mod=0&view=1		G	🔋 🔍 Search	☆自	ŧ	r 9	≡
🗑 Most Visited 🔻 🖫 Linux Mint 🖫 Community 🖫 Foru	ims 🔟 Blog 🔊 News 🔻						
	1. Case Name: The nam numbers, and symbols.	CREATE A NEW CASE	contain only letters,				
ې ۲	 Description: An optic kasus narkoba Investigator Names: investigators for this cas 	nal, one line description of th	is case. spaces) of the				
	a. leny novita sari c e g i	b d f h j					
	NewCase	CANCEL	Нер				

() localhost:9999/autopsy?mod=0&view=2&case=kasusa	&desc=kasus+narkoba&inv1=leny+novita+sari&inv2=&inv3=&inv4=&inv5=8 🛛 🤇 Searc	h	☆ 自	♥ ↓	俞	9	≡
Some the second	© Blog 🔊 News ▼						
Creating Case: kasus							
Case directory (/var/lib/autopsy/kasus/) created Configuration file (/var/lib/autopsy/kasus/case.a	l ut) created						
We must now create a host for this case.							
ADD HOST							
		N					
Iocalhost:9999/autopsv?mod=0&view=7&case=kasus/	مر المر المر المر المر المر المر المر ال	h	☆ 自	•	Â	0	=
Most Visited T I Linux Mint I Community I Forums						~	_
	ADD A NEW HOST						
							Ω
	1. Host Name: The name of the computer being investigated. It of contain only letters, numbers, and symbols	can					
	Joe Jacob						
	2. Description: An optional one-line description or note about th	is					
	computer.						
	3. Time zone: An optional timezone value (i.e. EST5EDT). If not defaults to the local setting A list of time zones can be found in the	given, it be beln					
	files.	ie neip					
	4. Time allow A live to and An antional value to describe how we						
	4. Timeskew Adjustment: An optional value to describe how misseconds this computer's clock was out of sync. For example, if the	any e					
	computer was 10 seconds fast, then enter -10 to compensate.						
	5. Path of Alert Hash Database: An optional hash database of had files	known					
							U
	6. Path of Ignore Hash Database: An optional hash database of	of known					
	good mes.						
Incalhost:9999/autopsy2mod=0&view=8&case=kasus	Shost=loe_larob&desr=&tr=&ts=0&alert_db=&exclude_db=&x=62&v=9	h	☆ 白		\$	0	=
Mact Vicited T D Linux Mint TD Computity TD Forums							_
Most visited • Community Community Community							
Adding host: Joe_Jacob to case kasus							
Host Directory (/var/lib/autopsy/kasus/Joe_Jacob	/) created						
Configuration file (/var/lib/autopsy/kasus/Joe_Ja	cob/host.aut) created						
We must now import an image file for this he	ost						
ADD IMAGE							
	\$						

			 ~ ~	-		~ ~	. –
Ocalnost:9999/autopsy:mod=0&view=10&case=kasus	knost=joe_jacob	C Q search	 ਯ ∎	0	*	m s	=
🛅 Most Visited 👻 🕒 Linux Mint 🕒 Community 🐚 Forums 🚺	🗟 Blog 🔊 News 🔻						
Case: kasus Host: Joe_Jacob	No imagas barra	hear added to this heat not					
	No images have	been added to this host yet					
	Select the Add Imag	e File button below to add one					
		CLOSE HOST					
9							
		IAGE INTEGRITY HASH DATABASES					
	VIEW NOTES	EVENT SEQUENCER					
	₽						
Iocalhost:9999/autopsy?mod=0&view=13&host=Joe_Jac	ob&case=kasus&inv=unknown&x=91&y=8	C Search	☆ 自		+	î 🤅	∍ ≡
Most Visited 🔻 🔟 Linux Mint 🔟 Community 🔟 Forums 😈	Blog 🔂 News 👻						
Cases Issue	, <u> </u>						
Host: Joe Jacob							
	Add	A NEW IMAGE					
	1. Location						
	Enter the full path (starting with	/) to the image file.					
	extension.	I Encase), then enter \sim for the					
	/home/leny/Documents/image	_					
	2. Туре						
	Please select if this image file is	for a disk or a single partition.					
	O Disk	Partition					
⊳	3 Import Mothod						
	To analyze the image file, it must	t be located in the evidence locker. It can					
	be imported from its current loca	ation using a symbolic link, by copying it,					
	then the image could become co	rrupt.					
	Svmlink O	Copy O Move					
	, i i i i i i i i i i i i i i i i i i i	15					
		NEXT					
	Cultor	Line a					
	CANCEL	HELP					
(Iocalhost:9999/autopsy?mod=0&view=14&host=Joe_Jac	ob&case=kasus&inv=unknown&img_path=%2Fho	ome%2Fleny%2FDocume C 🔍 🔍 Search	☆ 自		÷	^	∍ ≡
Most Visited	Blog News -						
Warning: Autopsy could not determine the vo	lume system type for the disk ima	ge (i.e. the type of partition table).					
Theuse select the type from the list below of h	celussity the mage us a volume n	nuge instead of as a disk image.					
Disk Image 🔍		Volume Image 🔍					
Volume System Type (disk image only): dos	-	U U					
ОК							

(Iocalhost:9999/autopsy?mod=0&view=14&spl_conf=1&ir	ng_path=%2Fhome%2Fleny%2FDocuments%2Fimage&sort=1&host=Joe_ C Q Search	☆ 自 ♥ ♣ 俞 (∍ =
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)		
	File System Details		
	Analysis of the image file shows the following partitions:		
	Partition 1 (Type: fat12) Mount Point: C: File System Type: fat12 V	4	
	ADD CANCEL HELP		
♦ ♦ localhost:9999/autopsy?mod=0&view=15&img_path	=%2Fhome%2Fleny%2FDocuments%2Fimage#_img=1&sort=1&do_ C C Search	☆ 自 ♥ ♣ 余 🤅	. ■
Most Visited 👻 🕒 Linux Mint 🕲 Community 🕲 Forums 🕲	Blog 🔊 News 🔻		
Linking image(s) into evidence locker Image file added with ID ing1 Volume image (0 to 0 - fat12 - C:) added with I	D vol1		
(◆) ④ localhost:9999/autopsy?mod=0&view=16&case=kasus&	host=Joe_Jacob&inv=unknown C Search	☆ 自 ♥ ♣ 余 🤅	9 ≡
Most Visited 👻 🖺 Linux Mint 🐌 Community 🐌 Forums 🐌	Blog 🔊 News 🕶		
Case: kasus Host: Joe_Jacob	Select a volume to analyze or add a new image file. CASE GALLERY HOST GALLERY HOST MANAGER mount name fs type c:/ image-8-8 fat12 ANALYZE ADD IMAGE FILE CLOSE HOST FILE ACTIVITY TIME LINES IMAGE INTEGRITY HASH DATABASES		

Gambar.4 Running Tool Autopsy

Setelah file image selesai diinputkan pada autopsy, maka akan didapatkan file analisis seperti pada Gambar.5. Pada menu meta data seperti Gambar.6, jika dilihat terdapat 2 FAT Content dalam sektor yaitu 73-103 dan 104-108 yang jika dibuka akan terdapat kumpulan kode ASCII baik yang redable ataupun yang tidak bisa di redable seperti pada Gambar.7 dan Gambar.12.

kasus:joe_jacob:vol1 - Mozilla Firefox — + ×													
🅼 kasus:Joe_Jacob:vol1	×	+											
(Iocalhost:9999/aut	🔶 🖲 localhost:9999/autopsy?mod=1&submod=2&case=kasus&host=joe_Jacob&inv=unknown&vol=vol1 🛛 🖓 Q, Search 🔗 🖨 🔗 🚍										≡		
📷 Most Visited 🔻 🚇 Linux M	Son Most Visited ▼ 🔞 Linux Mint 🐌 Community 🐌 Forums 🕲 Blog 🔂 News ▼												
		Œ	ILE ANALYSIS KEYWO	RD SEARCH FILE TYPE	IMAGE DETAILS	МЕТА ДАТА	DATA UNIT HELP	CLOSE					
Directory Seek Enter the name of	Cur	Trent Dire	Ctory: <u>C:/</u> Generate N	ID5 LIST OF FILES									
a directory that you want to view. C:/	DEL	Type <u>dir</u> / in		WRITTEN	Accessed		CREATED		Size	UID	GID	MET	A
		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 (UT	°C)	4608	8 0	0	<u>457</u>	<u>80</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 (UT	°C)	4608	3 0	0	<u>457</u>	<u>81</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 (UT	°C)	512	0	0	<u>457</u>	<u>79</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 (UT	°C)	0	0	0	<u>457</u>	<u>82</u>
regular expression for the		r / r	<u>cover page.jpgc</u>	2002-09-11 08:30:52 (WIB)	2002-09- 00:00:00	-11 (WIB)	2002-09-11 08:50:27 (WI	B)	1558	35 0	0	<u>8</u>	
want to find.	~	r / r	<u>Jimmy Jungle.doc</u>	2002-04-15 14:42:30 (WIB)	2002-09- 00:00:00	-11 (WIB)	2002-09-11 08:49:49 (WI	B)	2048	80 0	0	<u>5</u>	
		r / r	<u>Scheduled</u> <u>Visits.exe</u>	2002-05-24 08:20:32 (WIB)	2002-09- 00:00:00	-11 (WIB)	2002-09-11 08:50:38 (WI	B)	1000	0 (0	11	
SEARCH													Π
ALL DELETED FILES					File Brow	sing Mode							
EXPAND DIRECTORIES			\$										
🔟 📰 🐸 🖻 🗐	🎒 kasus;	joe_Jacob:vol1 -	- Mozill 🧮 25.PNG - I	mage Viewer [25/ 📄 Docu	ments - File Manager	Terminal				الأهر	#1) 🧕	10:42	æ

Gambar.5 File Analisis Image.zip



Gambar.6 Meta Data

Olicalhost:9999/autopsy?case=kasus&	host=joe_Jacob&inv=unknown&vol=vol1&mod=1&submod=5█=73&len=31 C 🔍 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:	FPREVIOUS NEXT EXPORT CONTENTS ADDNOTE ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) File Type: JPEG image data, JFIF standard 1.01 Status: Allocated										
Sector Size: 512 Address Type:	ASCII Contents of Sectors 73-103 in image-0-0										
Regular (dd)											
View	.21.1222222222222222222222222222222222										
ALLOCATION LIST											
₽	A. t										

Gambar.7 ASCII dari sektor 73-103

Coba ambil salah satu header konten ASCII pada sektor 73-103, kemudian cek tipe file dengan menggunakan sample header yang telah ditentukan pada *List of File Signatures*. Dari file signature didapatkan bahwa sektor 73-103 dengan header JFIF ternyata merupakan tipe file gambar (jpg/jpeg). Eksport contents seperti Gambar.9 kemudian lakukan rename pada file yang telah di eksport, dari .raw menjadi .jpg atau .jpeg maka akan tampil gambar seperti Gambar.11.

https://en.wikipedia.or	rg/wiki/List_of_file_signatures	C Q Search	I	☆ 🛙) 🛡 🖡 🏟 🖻	≡
🕅 Most Visited 👻 🔟 Linux Min	t 🔟 Community 🔟 Forums 🔟 Blog 🔂 News	▼				
	bpg	Better Portable Graphics format ^[7]	0	BPGû	42 50 47 FB	
2				ÿøÿÛ	FF D8 FF DB	0
	jpg jpeg	JPEG raw or in the 🔝 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	
	ilbm Ibm ibm iff	IFF Interleaved Bitmap Image	0 any	FORM ILBM	46 4F 52 4D nn nn nn nn 49 4C 42 4D	

Gambar.8 File Signature Header JFIF

ASCII (display - r F Sectors: 73-103 Status: Allocated		ay - report)				
ASCII Contents of Sectors 73-103 in image-0-0	You have chosen to open:	\$				
JFIFS.' ",#(7),01444.'9=82<.342 S.' ",#(7),01444.'9=82<.342 .21.122222222222222222222222222222	which is: BIN file from: http://localhost:9999 Would you like to save this file? Cancel Save File					
f[.5,rF.:", fp.0.3e0.\$j.41(.x11.v.P.j8.@.6y4K,y#Y);FWW.[T.>\$.VXs.M#@.m.XH]fw.2/.dmYhw w.&*.{[e.7.n.sN.Y.K`Y?XW]M6o29r6q1~{B.0,.y.o.n.n.dR.B.Z.VKW1YY".w"2.9ec] 'L.P.W. !Aq.h.nn.xg.Q						

Gambar.9 Eksport File pada Sektor 73



Gambar.10 File Sektor73.raw



Gambar.11 File Sektor73.jpg

Lakukan hal yang sama untuk pengolahan sektor 104-108. Coba ambil salah satu header konten ASCII, kemudian cek tipe file dengan menggunakan sample header yang telah ditentukan pada *List of File Signatures*. Dari file signature didapatkan bahwa sektor 104-108 dengan header PK ternyata merupakan tipe file zip/jar/odt/ods/odp/docx/xlsx/pptx/vsdx/apk. Eksport contents seperti Gambar.14 kemudian lakukan rename pada file yang telah di eksport, dari .raw menjadi .zip maka akan tampil gambar seperti Gambar.16, yang ternyata setelah dibuka didalamnya terdapat sebuah dokumen bertipe .xls, untuk mebuka file tersebut dibutuhkan sebuah password.

(Iocalhost:9999/autopsy?case=kasus&	host=Joe_Jacob&inv=unknown&vol=vol1&mod=1&submod=5█=104&len=5 C 🔍 🔍 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:	FPREVIOUS NEXT EXPORT CONTENTS ADD NOTE ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) File Type: empty (Zip archive data, at least v2.0 to extract) Sectors: 104-108 Status: Allocated										
Address Type: Regular (dd)	ASCII Contents of Sectors 104-108 in image-0-0 Image: Contents 104-108 in image-0-0										
VEW ALLOCATION LIST	mbgumg[A.U.U0.Mi.[.dz.e.xT3.wx.N.2.'3G.8z.q8. <z^%+b>nW3' N[!z.UfIZ,7 .rP6d.U ?%.xXJ8B.KR. w ab.g.02.X7Z.Jw{.m.LsC6g(.yGUj.T?S.nRUfH0I+.60.g.42.+bN.c.X.W.G(.>Yt.p?;u.jp. Fw#eAq.S.q.0SIncG4.K%04M'L".1d.Q_DY.ZG.h S]XK.,8.64);'.c.EG.l.^81r4.~.B>3F.:S.LY/*9.MKXZ. 3).3).</z^%+b>										
	CZ. H.AR.RU.T5, №! ZNL9.e.!eC.Db, №5R.7 C.Cm. i V.K?h.e.j										

Gambar.12 ASCII dari sektor 104-108

	(including NE and PE)			
zip jar odt ods odp docx xlsx pptx vsdx apk	zip file format and formats based on it, such as JAR, ODF, OOXML	0	X	50 4B 03 04 50 4B 05 06 (empty archive) 50 4B 07 08 (spanned archive) 50 10 10 10
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
			3	

Gambar.13 File Signature Header PK

ASCII (display - I File Ty Sectors: 104-108	←PREVIOUS NEXT → EXPORT CONTENTS ADD NOTE eport) * Hex (display - report) * ASCII Strings (dis pe: empty (Zip archive data, at least v2.0 to extra	<u>play</u> - <u>report</u>) ict)
Status: Allocated	Opening vol1-Sector104.raw + >	
ASCII Contents of Sectors 104-108 in image-0-0	You have chosen to open:	
<pre></pre>	which is: BIN file from: http://localhost:9999 Would you like to save this file?	#-4HT.b.^.?.Rrf
Bgvmq[A.U.U0Mi.[.dz.exT .rP6d.U 7%XJ8B.KR. w abg.02.X?Z.Jwf.m.L.sC6q(Cancel Save File	'. N[!z.Uf.~IZ7 2+bN.c.X.WGf.>Ytp?;u.jp.'
	ې4N'L".1d.Q~_bYZGh l.r4.~B> 3F.:S.lY/*9MKXZ M85R.?	
CC.m.iV.K?.h.e.~j9dyP.ot3;N ,FWJ3Fa.V.OlU .V.^^.y U.Xh3U.%8P(isr==j.aj.]0 < ~F UT @ i'(65 h) H -	۱۲٬۹٬۰٬۹٬۱٬۱۲٬۹٬۱۲٬۱۲٬۱۲٬۱۲٬۱۲٬۱۲٬۱۲٬۱۲٬۱۲٬۱۲٬۱۲٬۱۲٬۱۲٬	6n%.&F\<

Gambar.14 Eksport File pada Sektor 104

				Downloads -	File Manager			
File Edit View Go Help								
DEVICES		w			w ===		no material antico managemente de la constante la constante de	
🖾 File System		Let un an un an Un an un an					The second secon	Service.
Leora	deb	Deskripsi-BO-	kaa-deb-0.9.0.tar.gz	wnsn.rar	PROJECT_PENGOLA	nano networks.rar	vol1-Sector73.jpg	vol1-Sector104.raw
🖾 AnNie Cheesers		NAC.doc			HAN_CITRA[1].docx			
🖾 50 GB Volume								
PLACES								
合 leny								
🚍 Desktop								
🔋 Trash								
Documents								
🗊 Music								
🛅 Pictures								
🚺 Videos								
🗊 Downloads								
NETWORK								
Browse Network								





Gambar.16 File Sektor104.zip

Untuk mendapatkan password hingga bisa membuka dokumen bertipe .xls diatas, kita menjalankan tool strings dengan option strings voll-sector73.jpg hingga didapatkan

password : goodtimes seperti Gambar.17. Inputkan password pada vol1-Sector104.zip untuk membuka file xls yang terdapat didalamnya, setelah file xls terbuka ternyata didalamnya berisikan bulan, hari dan nama-nama sekolah yang dikunjungi pelaku seperti pada Gambar.18.

leny@leny-Satellite-	Pro-C640	~/Downloads	<pre>\$ strings</pre>	vol1-Sect	tor73.jpg
04p(i\$TR					
eBy					
οΗ νŬ9α					
s4J\+					
@fPv					
"D?q-					
piZĺ					
d180					
- J=^k{k					
RwF5!					
wrJn%6					
v:15}61k					
pi0Fm					
e0#K3					
66SC					
89Pr0x					
f n8e					
FFFy					
Ň	IrH'				
pu0 k					
go}b					
×/9'					
Tw l					
c\[M0					
Т[9ј					
k}Bx`VE					
s\$6s,					
zz7q					
K;dMj					
)UfRcvm					
8-'H\$					
FFFy					
N	IrH'				
7g%					
9'p+					
R*]I					
oqk4					
I+^L					
pw=goodti	.mes				
Leny@Leny	-Satelli	ite-Pro-C640	~/Downlo	ads 💲 👘	

Gambar.17 Running tool Strings untuk Mendapatkan Password

				Scheduled Vis		
File	Edit View	Insert Format	Tools Data Window Help			
	<u>-</u>		<u> </u>			
	<u>•</u> •		🖶 💩 🕺 🛛 🛱 • 🛔	Ab		
Ar	ial	▼ 10 ▼	a a <u>a</u> - 📰 - 🗄	≣ च = २ ≡		
B50		▼ f(x) Σ =	Monday (1)			
	Α	в	С	D		
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	28 Friday (5) Smith Hill High School (A)					
29	I	Monday (1)	Key High School (B)			

Gambar.18 File xls pada Sektor104.zip

Kita tidak tahu apa yang dilakukan pelaku pada file image.zip yang ada, maka kita gunakan tool foremost untuk merecover file berdasarkan header dengan option foremost -v -i image -o recover. Cek folder recover pada direktori penyimpanan file image.zip seperti Gambar.20. Pada folder recover terdapat folder lagi, yaitu : folder doc/ole, jpg dan zip. Buka folder doc, di dalamnya terdapat dokumen .doc yang ternyata isinya adalah sebuah surat untuk Jimmy Jungle.



Gambar.19 Running Tool Foremost

Perumente - Elle Manner									
File Edit View Go Help	File Edit View Go Help								
+ + + 🛔 🖬	home/leny/Documents/	1							
DEVICES					(11 m) (11 m) (1	(TEANS, ME	(ELANA, MAL)	(STANG, ALL)
🧾 File System							\mathbf{O}	0	
🔤 Leora	Installation guide -	Linux install	Functions &	recover	server2.c	client2.c	Installation guide -	Linux install	Functions &
AnNie Cheesers	documentation_files	OpenRemote	OpenRemote_files				documentation.html	OpenRemote	OpenRemote.html
50 GB Volume		Forums_files						Forums.html	
PLACES	C	C	222	222	22	28	222	28	22
合 leny	ter ri								
Tesktop	simpleUDPClient.c	simpleUDPServer.c	client1	server1	server	client	server3	client3	server4
🔋 Trash		#00		\$\$C\$		# U 2			A
Tocuments									
🗊 Music	client4	server5	client5	server6	client6	server7	client7	Tabel alert.qti~	Tabel alert.qti
🛅 Pictures						0109			
💽 Videos		01010	01010 01101 01110	01101		1101 1001			
🗊 Downloads	1.pcapng	2.pcapng	3.pcapng	FIN.pcapng	image.zip	image			
NETWORK						5			
Browse Network									

Gambar.20 Folder Recover



Gambar.21 Folder Doc

<pre>index Window Help index Help</pre>		00000	033.doc - LibreOffice Writer		
Image: Interview of the set of the	<u>T</u> ools <u>W</u> indow	<u>H</u> elp			
Image: Interview of the set of the		🖻 • 🛔 🏫 • 🖓 • 💁	, AÞ ¶ ⊞ • ⊠ (T ⊨ ⊞ •	88 🖙 🗒 🗊 📲
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 enterpreneur. Am I only one you sell to? Maybe I can become distributor of the year! Iemailed 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	• • 12 •	a <u>a</u> <u>a</u> a ^b a _b	a a 🛴 🤷 🗸	• = • = •	≣ੋੜੋੜੋ≣∣≕
aracters Default Style English (USA) 💷 🖂		Jimmy Jungle 626 Jungle Ave Apt 2 Jungle, NY 11111 Jimmy: Dude, your pot must be the bes sending me the Cover Page. WI seeds? At least I know your gro These kids, they tell me marijus Man, I'm sure glad you told me some experience. It's like a gua lunch and they spend it on my s Maybe I can become distributo I emailed you the schedule that predictive. Tell me what you th before with that file. Talk to yo Thanks, Joe	t – it made the cover of High hat do you put in your soil wl wing it and not some guy in ana isn't addictive, but they d about targeting the high sch ranteed paycheck. Their pare stuff. I'm an entrepreneur. An r of the year! I am using. I think it helps m ink. To open it, use the same u later.	Times Magazine! That hen you plant the marij Columbia. lon't stop buying from ool students. You must nts give them money fo n I only one you sell to he cover myself and noi password that you sen	nks for uana me. have or ? t be t me
	aracters	Default Style	English (USA)	=[G

Gambar.22 Surat Dari Joe untuk Jimmy Jungle

	vol1-Sector73.j	pg - GHex	- + ×				
File Edit View Windows Help							
00000000 FF D8 FF E0 00 10 4A	4A 46 49 46 00 01 01 01 00 60 00 60 00	00 FF DB 00 43 00 08 06 06 07 06 05	JFIF`.`C				
0000001F08 07 07 07 09 09 08	08 0A 0C 14 0D 0C 0B 0B 0C 19 12 13 0F	14 1D 1A 1F 1E 1D 1A 1C 1C 20 24 2E	s				
0000003E27 20 22 2C 23 1C 1C	1C 28 37 29 2C 30 31 34 34 34 1F 27 39	3D 38 32 3C 2E 33 34 32 FF DB 00 43	",#(7),01444.'9=82<.342C				
0000005D01 09 09 09 0C 0B 0C	OC 18 OD OD 18 32 21 1C 21 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32 32					
0000007032 32 32 32 32 32 32 32	32 32 32 32 32 32 32 32 32 32 32 32 32 3	32 32 32 32 32 32 32 32 32 32 32 32 32 22	222222222222222222222222222222222222222				
0000009B32 32 32 FF C0 00 11	11 08 00 C7 00 D0 03 01 22 00 02 11 01	03 11 01 FF C4 00 1F 00 00 01 05 01 22	2				
000000BA01 01 01 01 01 00 00	$00 \ 00 \ 00 \ 00 \ 00 \ 00 \ 00 \ 01 \ 02 \ 03 \ 04 \ 05 \ 06$	07 08 09 0A 0B FF C4 00 B5 10 00 02					
000000D901 03 03 02 04 03 05	05 05 04 04 00 00 01 7D 01 02 03 00 04	11 05 12 21 31 41 06 13 51 61 07 22					
000000F871 14 32 81 91 A1 08	08 23 42 B1 C1 15 52 D1 F0 24 33 62 72	82 09 0A 16 17 18 19 1A 25 26 27 28 q.	2#BR\$3br%&'(
0000011729 2A 34 35 36 37 38	38 39 3A 43 44 45 46 47 48 49 4A 53 54	55 56 57 58 59 5A 63 64 65 66 67 68)*	456789:CDEFGHIJSTUVWXYZcdefgh				
0000013669 6A 73 74 75 76 77	77 78 79 7A 83 84 85 86 87 88 89 8A 92	93 94 95 96 97 98 99 9A A2 A3 A4 A5 ij	stuvwxyz				
00000155A6 A7 A8 A9 AA B2 B3	B3 B4 B5 B6 B7 B8 B9 BA C2 C3 C4 C5 C6	C7 C8 C9 CA D2 D3 D4 D5 D6 D7 D8 D9					
00000174DA E1 E2 E3 E4 E5 E6	E6 E7 E8 E9 EA F1 F2 F3 F4 F5 F6 F7 F8	F9 FA FF C4 00 1F 01 00 03 01 01 01					
0000019301 01 01 01 01 01 00	00 00 00 00 00 00 01 02 03 04 05 06 07	08 09 0A 0B FF C4 00 B5 11 00 02 01					
000001B202 04 04 03 04 07 05	05 04 04 00 01 02 77 00 01 02 03 11 04	05 21 31 06 12 41 51 07 61 71 13 22					
000001D132 81 08 14 42 91 A1	A1 B1 C1 09 23 33 52 F0 15 62 72 D1 0A	16 24 34 E1 25 F1 17 18 19 1A 26 27 2.	B#3Rbr\$4.%&'				
000001F028 29 2A 35 36 37 38	38 39 3A 43 44 45 46 47 48 49 4A 53 54	55 56 57 58 59 5A 63 64 65 66 67 68 ()	*56789:CDEFGHIJSTUVWXYZcdefgh				
0000020F69 6A 73 74 75 76 77	77 78 79 7A 82 83 84 85 86 87 88 89 8A	92 93 94 95 96 97 98 99 9A A2 A3 A4 ij	stuvwxyz				
0000022EA5 A6 A7 A8 A9 AA B2	B2 B3 B4 B5 B6 B7 B8 B9 BA C2 C3 C4 C5	C6 C7 C8 C9 CA D2 D3 D4 D5 D6 D7 D8					
0000024DD9 DA E2 E3 E4 E5 E6	E6 E7 E8 E9 EA F2 F3 F4 F5 F6 F7 F8 F9	FA FF DA 00 0C 03 01 00 02 11 03 11					
0000026C00 3F 00 F7 FA 28 A2	A2 80 0A 28 A2 80 0A C4 D7 B5 6B CD 35	B4 C8 6C 2C E1 BB B9 BF BB 36 C8 B3 .?	((k.5l,6				
Signed 8 bit: 70	Signed 32 bit:	16842822	Hexadecimal: 46				
Unsigned 8 bit: 70	Unsigned 32 bit:	16842822	Octal: 106				
Signed 16 bit: 70	Float 32 bit:	2,369375e-38	Binary: 01000110				
Unsigned 16 bit: 70	Float 64 bit:	7,120243e-307	stream Length: 8 – +				
Show	now little endian decoding	Show unsigned and float a	s hexadecimal				
Offset: 0x9; 0x4 bytes from 0x6 to 0x9 selected	1						
N							

Terakhir, running tool ghex untuk editor hexa dari Vol1-Sector73.JPG.

Gambar.23 Running Tool Ghex

Dari apa yang kita lakukan diatas, kita bisa menjawab beberapa informasi yang dibutuhkan pihak berwenang untuk penyelidikan lebih lanjut.

- Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?
 → Jimmy Jungle, alamat : 626 Jungle Ave Apt 2 Jugle NY 11111
- What crucial data is available within the coverpage.jpg file and why is this data crucial?
 → password dari file zip yang diembedd ke cover page menggunakan steganografi.
- What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?
 → Key High School, Leetch High School, Birard High School, Richter High School, Hull High School.
- 4. For each file, what processes were taken by the suspect to mask them from others?
 → Melakukan rename file zip menjadi file EXE dan menyembunyikan password dengan menggunakan file.jpg.
- 5. What processes did you (the investigator) use to successfully examine the entire contents of each file? (proses apa yang kamu lakukan sebagai investigator untuk memeriksa secara keseluruhan konten dari setiap file)

 \rightarrow pertama-tama melakukan "MD5 Checksum" pada barang bukti untuk memastikan tidak adanya kontaminasi atau perubahan kondisi terhadap barang bukti yang ada, kemudian mengekstrak file dari file yang ada, kemudian barulah diolah dengan menggunakan bantuan tool sehingga didapatkanlah beberapa file. Untuk file JPG, image.zip di identifikasi menggunakan autopsy sehingga didapatkan vol1-sector73.raw kemudian direname menjadi vol1-sector73.jpg sehingga menjadi sebuah gambar. Untuk file ZIP, sama seperti identifikasi file JPG hanya saja vol1-sector104.raw direname menjadi vol1-sector104.zip sehingga didapatkan file berbentuk XLS yang didalamnya terdapat informasi penting tentang sekolah-sekolah yang sering dikunjungi pengedar narkoba untuk melakukan aksinya. Sedangkan untuk file DOC didapatkan dari hasil recovery image.zip berdasarkan header dengan menggunakan foremost.