TUGAS

KEAMANAN JARINGAN KOMPUTER



Nama : Dede Triseptiawan

Nim: 09011181320001

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

Forensik komputer adalah salah satu cabang ilmu forensik yang berkaitan dengan bukti legal yang ditemui pada komputer dan media penyimpanan digital. Tujuannya untuk menjabarkan keadaan kini dari suatu artefak digital. Istilah artefak digital bisa mencangkup sebuah sistem komputer, media penyimpanan, sebuah dokumen elektronik atau bahkan sederetan paket yang berpindah dalam jaringan komputer. Secara umum kebutuhan forensik komputer dapat digolongkan sebagai keperluan investigasi tindak kriminal dan perkara pelanggaran hukum, rekontruksi duduk perkara insiden keamanan komputer, dan lain-lain.

Pada tugas ini kita mencoba memecahkan kasus narkoba, dan didapatkan berupa file image, sebagai bahan investigasi kasus tersebut, tools yang dibutuhkan berupa, autopsy, foremost, strings, dan Ghex. Kegunaan autopsy untuk melakukan digital forensic, autopsy dapat melakukan analyze terhadap disk image serta partition, tujuannya agar dapat melakuan analyze terhadap file system yang dapat menjadi evidence atau bukti.

Berikut tahap-tahap dalam melakukan pemecahan kasus narkoba, pertama kita download file image.zip yang sebagai barang bukti yang ditemukan dalam kasus ini ((old.honeynet.org/scans/scan24/image.zip) md5 : b676147f63923e1f428131d59b1d6a72)



Setelah diunduh file image lalu di pindahkan di di folder documents agar lebih mudah, lalu buka terminal lalu masuk ke direktori documents, lalu ketik md5sum image.zip, perintah md5sum berfungsi untuk mengecek keaslian file, kemudian eksrak image.zip



Setelah di ekstrak lalu ketik perintah file image, fungsi perintah file untuk melihat tipe filenya.



Kemudian buat folder kasus.narkoba di direktori root /tmp/ . kemudian ekstrak file image di folder yang kita buat di direktori root /tmp/kasus.narkoba.



Kemudian kita masuk ke folder kasus.narkoba dengan perintah cd /tmp/kasus.narkoba/, kemudian kita cek isi folder, dengan perintah ls.



Kemudian kita buka tools autopsy di terminal, jangan di close terminal nya.



Kemudian buka browser masukkan alamat localhost:9999/autopsy maka akan terbuka tampilan dari tools autopsy, kemudian klik new case

Create A New Case - Mozilla Firefox	l i									e	
🏠 Create A New Case 🛛 🗙 🕂											
(I localhost:9999/autopsy?mod=0&view=1			C Q Searc	h		ជា	≜	Â	v	0	≡
Most Visited ▼ [™] Linux Mint [™] Community [™] Forums [™] Blog	News *										
	Cr	REATE A NEW C	ASE								
1.0	and Mamo, The name	of this investigati	n It con contain	only letters							
num	bers, and symbols.	or uns investigation	on. It can contain	l only letters,							
k	asus										
2. D	escription: An optiona	al. one line descri	ption of this case								
k	asus narkoba										
			6 113								
3. II inve	stigators for this case.	he optional name	s (with no spaces) of the							
a.	dede triseptiawan	b.									
c.		d									
e.		f									
g.		h.									
		J.									
	NEWCASE	CANCEL		ELD.							
	HEITCASE	CARCEL									
🕀 menu 💼 🥥 🖾 💼 🖾 Terminal 📄 [Downloads]	[Pictures]	📧 Termina	Create A No	ew 53.3°C 🖬	104)	- (NET	esx 🗲	2% 18:	10 🗳

Kemudian kita buat case baru, dengan nama case kasus, dengan deskripsi kasus narkoba, dan nama investigasi nama kita, kemudian klik new case untuk melanjutkan



Case tersimpan di direktori root /var/lib/autopsy/kasus/ kemudian kita harus membuat host untuk case ini, klik add host



Kita buat host dengan nama joe_jacob



Kemudian klik add host



Host telah di buat, kemudian kita import file image, klik add image

Open Image In kasus:joe_jacob - Mozilla Firefox						e	•••
🄏 Open Image In kasusij 🗙 🕂							
♦ (1) localhost:9999/autopsy?mod=0&view=10&case=kasus&host=joe_jacob	☆	ê,	₽ ∧		٢	0	≡
🐻 Most Visited 🔻 🖫 Linux Mint 🖫 Community 🖫 Forums 🖫 Blog 🔊 News 🕶							
Case: kasus							
No images have been added to this host yet							
Select the Add Image File button below to add one							
FILE ACTIVITY TIME LINES IMAGE INTEGRITY HASH DATABASES							
	(8	MO	I NET	DIĝK /	1000	× 40×	

Kemudian klik add image file



Masukkan lokasi file image yang telah di download tadi, lokasi file saya di direktori /home/dee/documents/image. Kemudian klik next



Kemudian centangkan pada volume image, lalu klik ok

Open Image In kasus:joe_jacob - Mozilla Firef	ox								•	08
🖉 Open Image In kasus:j 🗙 🕂										
(i) localhost:9999/autopsy?mod=0&view=16&case	=kasus&host=joe_jacob&inv=ur	nknown	0	# Q Search		☆ €	*	•	0	≡
👸 Most Visited 🔻 🐚 Linux Mint 🐚 Community 🐚 Forum	ns 🧕 Blog 🔂 News 🔻									
Case: kasus Host: joe_jacob	Select a v	volume to analyz	e or add a nev	v image file.						
	CASE GALLERY	Host G	ALLERY	HOST MANAGER						
	mount	name	fs type	~~~						
	O C:/	image-0-0	fat12	details						
	ANALYZE	ADD IM	AGE FILE	CLOSE HOST						
		H	ELP				 			
	FILE ACTIVITY TIME LINE									
	VIEWING		Ev	ENTSEQUENCER						
🜐 menu 🧰 🥏 💷 🚞 🗵 Terminal 🛛 📔 [Dow	vnloads] 🦰 [Pictures]	🗐 [lib]	Terminal	🗐 Open Image I 53.7°C 🔒	1 L L I	a)	NET DIS	1 48	2% 18:	12 🗆

File image telah di tambahkan, kemudian klik analyze untuk melihat isi analisis file image

kasus:joe_jacob:vol1	- Mozi	lla Firefox								988
🕼 kasus:joe_jacob:vol1	×	+								
(localhost:9999/au	topsy?n	nod=1&submo	d=2&case=kasus&hos	t=joe_jacob&inv=unknown&vol	=vol1 C Q Search	\$	≜ ↓ 1		۵	@ ≡
Most Visited ▼ Inux	Mint 19	Community	🖲 Forums 🐚 Blog 📗	News						
		,	ILE ANALYSIS KEYWO	RD SEARCH FILE TYPE	IMAGE DETAILS META DATA	DATA UNIT HELP CLOSE				
			9			? X				
Directory Seek Enter the name of		TTENT DITE	C tory: <u>C:/</u> Generate N	ID5 LIST OF FILES						
a directory that you want to view. C:/	DEL	Type dir / in		WRITTEN	Accessed	CREATED	Size	UID	GID	Мета
		v / v	<u>SFAT1</u>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	<u>45780</u>
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>45781</u>
File Name Search		v / v	SMBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	<u>45779</u>
Enter a Perl		d / d	<pre>\$0rphanFiles/</pre>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	<u>45782</u>
regular expression for the		r / r	<u>cover page.jpgc</u>	2002-09-11 08:30:52 (WIB)	2002-09-11 00:00:00 (WIB)	2002-09-11 08:50:27 (WIB)	1558	50	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)	2048	00	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										Π
ALL DELETED FILES					File Browsing Mode					U
💼 menu 直 🔮 🖅 🗖		erminal	[Downloads]	[Pictures] 🔄 [lib]	🖾 Terminal 🛛 🙆 kasus:joe_ja	: 55.0°C 👝 💄 🗳 🕪	CPU MEM NET	DISK	7 82%	18:13 🖵

Setelah terbuka, klik file analysis, terdapat beberapa file di dalam file image

kasus:joe_jacob:vol1 - Mozilla Fire	fox											e	•
🅼 kasus:joe_jacob:vol1 🛛 🗙 🕂													
(+) () localhost:9999/autopsy?mod=1&su	ubmod=7&case=k	asus&host=joe_jacob&	kinv=unknown&vo	ol=vol1	C Q Searc	h		☆自	+	☆ ♡	٢	0	≡
Most Visited ▼ □ Linux Mint □ Commun	nity 👅 Forums 👅	Blog News 🕶											
	FILE ANALYSIS	KEYWORD SEARCH	FILE TYPE	IMAGE DETAILS	META DATA	DATA UNIT	HELP CL	OSE					
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 ** Cluster Area: 33 - 2879 METADATA INFORMATION Range: 2 - 45782 Root Directory: 2								<u> </u>					
CONTENT INFORMATION Sector Size: 512 Cluster Size: 512 Total Cluster Range: 2 - 2848 FAT CONTENTS (in sectors) 73-103 (31) -> EOF 104-108 (5) -> EOF													_
🕀 menu 💼 🍪 🔟 📩 🗵 Terminal	[Downloa	ds] [Pictures]	🗐 (lib)	🖾 Terminal	😔 kasus:joe_j	ac 53.3°C L	1.1.0	(i) ^{CPU}	P		/ 83	% 18:1	3 🗅

Kemudian klik image details, pada tab ini menjelaskan detail dari file image, kemudian paling bawah terdapat 2 file contents di dalam file image, kemudian klik 73-103 (31) -> EOF

kasus:joe_jacob:vol1 - Mozilla Fire	fox 🔷 😂 🕲
🏠 kasus:joe_jacob:vol1 🗙 🕂	
(localhost:9999/autopsy?case=kasi	us&host=joe_jacob&inv=unknown&vol=vol1&mod=1&submod=5█=73&/r C Q Search 🟠 🖨 🗸 🎓 🦁 🥥 🚍
🐻 Most Visited 🔻 👅 Linux Mint 👅 Commu	nity 🖫 Forums 🖫 Blog 🔝 News 🔻
	FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE
Sector Number:	
73	EXPORT CONTENTS ADD NOTE
	ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)
Number of Sectors:	File Type: JPEG image data, JFIF standard 1.01
1	Sectors: 73-103
Sector Size: 512	Status: Allocated
	ASCII Contents of Sectors 73-103 in image-0-0
Address Type:	
Regular (dd) 🔻	JFIF`.`
Lazarus Addr.	
Lazarus Auur:	1 1000000000000000000000000000000000000
View	
· · · · · · · · · · · · · · · · · · ·	
ALLOCATION LIST	\$4.%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz?(
	(k.5l,6q,.H;.bki3.2]*M#
	A. [J]P.E
	o
	B.XJ<\$.<[6u556vCu.r.n.m./y.T5 f{SrF - "fn 3an S id]. (y TivPi R @ 6 VdK , w≇Y)- F W W (TsSV X ≤ M#∩ m X H] fw 2/dmYh wr
	.w.δ
	'LP.W. !Aah.nn.xa.0
	.6y6Ay=2y. 5kiM; * 5cy. 1.y5.B.b2.w((++#.f];@5T.H;JWcn.Wnb.Hc}G(Xc.64
	то∨, (р.s.+>м.м.u8*.«8*.s.s.s.o.o]к.цинuv.aм.мт.; а.оbC.9+кк.
	5]?.gb4;].6U.Fi%r(e/4kLmp.L.+D.Cm 80KI4Vk.@.{(.>e]v.G.x{LkH5G(c@"R\f"\$.~T
	Converting to the second secon
🕕 mend 🔝 🥑 🔤 🔛 🔛 Terminal	

Setelah di klik akan muncul ASCII contents of sectors 73-103 dalam file image, pada awal kode tersebut ada kata JFIF. Kemudian kita export contents

List of file signatures -	Wikipedia - Mozilla Firefox				008		
🏠 kasus:joe_jacob:vol1	× W List of file signatures × +						
(https://en.wikiped	lia.org/wiki/List_of_file_signatures	C Q Search		☆ 自 ♣	↑ ♥ ♥ ♥ ■		
🗑 Most Visited 🔻 👅 Linux Mir	nt 🖫 Community 🐚 Forums 🐌 Blog 🔂 New	5▼					
	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		
	ilbm Ibm ibm iff	IFF Interleaved Bitmap Image	0 FORM any ILBM		46 4F 52 4D nn nn nn 49 4C 42 4D		
	8svx 8sv svx snd	IFF 8-Bit Sampled Voice	0 any	FORM 1y BSVX 38 53 56 58			
于 menu 🔟 😕 💷 🚞	🔚 Terminal 🛛 🧮 [Downloads] 🛛 📄 Pictu	res 📄 [lib] 🛛 🖾 Terminal 🛛 😔 List of file sig	53.7°C ц	🕹 🦁 🕪 🛄 🍧	3 84% 18:18 🖵		

File JFIF adalah adalah format file tipe gambar



setelah kita export contents, maka akan otomatis terdownload file vol1-sector73.raw . kemudian kita ubah nama file tersebut menjadi vol1-sector73.jpg . maka akan terbuka file raw tersebut menjadi gambar diatas.





Kemudian kita buka folder tempat tersimpannya file vol1-sector73.jpg, kemudian buka terminal klik perintah strings vol1-sectors73.jpg maka terbuka seperti gambar diatas, pada paling bawah ada password "goodtimes" untuk membuka file vol1-sectors104.zip nantinya. Fungsi perintah strings untuk melihat karakter yang readable pada sebuah file.



Kemudian kita back ke file image details, kemudian kita klik 104-108(5)-> EOF



Maka akan muncul data unit ASCII contents of sector 104-108 di dalam file image, pada kode tersebut kata awal terdapat PK. Kemudian kita export contents.

kasus:joe_jacob:vol1 - Mozilla Firefox					988				
🎄 kasus:joe_jacob:vol1 🛛 🗙 🐨 List of file signatures 🗙 🕂									
(X Q. Search		☆自	- 🕆 🛡 🙂	໑ =				
Blog SNew	5▼								
	(including NE and TE)								
zip				50 4B 03 04					
jar odt ods									
odp docx	zip file format and formats based on it, such as JAR, ODF, OOXML	0	РК	. 50 4B 05 06					
xisx pptx vsdx				(empty archive)	0				
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]	Rar!	52 61 72 21 1A 07 01 00						
Transferring data from localhost	Executable and Linkable Format	0	.ELF	7F 45 4C 46					
📳 menu 🤠 🥪 💷 🚞 🗵 [Terminal] 📄 Documents 📄 [Pictures]	📄 [lib] 🛛 🔄 [Terminal] 🛛 🥥 kasus:joe 🖾 Terminal	54.3°С ц	1 🕆 🕪 🛄 🤻	M NET DISK # 86%	18:25 💷				

Kode PK adalah jenis format file zip

Documents									•••
File Edit View Go	Bookmar	ks Help							
G O O O	0	1	nome/dee/Documents					🛨 🕞	Q
 My Computer Home Desktop Documents Music Pictures Videos Downloads Recent File system Trash Devrices Don'T BU 426 GB V 157 GB V Network Network 		bsdt.c	dt DvL_1.5_Infectious_ Disease (1).iso	image	image.zip	image1	vol1-Sector73.jpg	Vol1-Sector104.zip	
					7 items, Free space: 36,3 GB				
🕀 menu 💼 🤌 🛛		🖾 (Tern	ninal] Documents [Pictures]	🗐 (lib)	📧 [Terminal] 🛛 😔 kasus:joe	. 📧 Terminal	53.0°C 📊 👤 🤠 📢	CPU MEM NET DISK	87% 18:29

Kemudian kita ubah nama file yang didownload tadi vol1-sector104.raw menjadi vol1sector104.zip agar file tersebut dapat dibuka

				000
File Edit View Go Bookmarks Help				
vol1-Sector104.zip 😑 🖼 😒			📮 🗔 🚘 🍳	
Archive Edit View Help				
🔶 🧰 Open 👻 📘 Add Files 🔛 Extract		The and a second s		
G Back 🕣 🕜 😡 Location: 📔 /	image.zip image1	vol1-Sector73.jpg vol	1-Sector104.zip	
Name 🕶 Size Type Modified				
E Scheduled Visits.xls				
Archive Manager Password required for "vol1-Sector104.zip" Password: Cancel OK				
1 object (16,9 kB), 1 object selected (16,9 kB)				
le le "vol1-Sector10	4.zip" selected (2,6 kB), Free space: 36,3 GB			
🜐 menu 🧰 🥹 🔟 📒 📧 [Terminal] 🦳 Docume 🚞 [Pictures] 📑 [lib] 👘 💷 [Ter	rminal] 🔵 kasus:jo 🔟 Terminal 🛛 🛃 vol1-Sec	54.3°C 👝 💄 🤠 📢 🖓	NET DISK	∳ 87% 18:29 ⊡

Kemudian kita buka file vol1-sector104.zip, lalu klik scheduled visits.xls, masukkan password yang didapatkan pada perintah strings vol1-sector73.jpg sebelumnya. Password "goodtimes"

Scheduled Visits.xls - LibreOffice Calc 🕒 😔 😔																
<u>F</u> ile	Edit View	Insert Format Jo	ols <u>D</u> ata <u>W</u> indow <u>H</u> elp													×
: 6	• • •				I c			< m		0						
: •			1 8 82 y 60				τιΟ	2 1 2								
1	. Arial	▼ 10	🔹 a a a 🚍 🚍	≒ ≣ ⊨ X %	00. [0	린토	🕀 🔹	🗉 - 🧧	L -							
050		- f(y) \S	- Mandau (1)							, 						50
BSU		▼ J(A) Z	- (Monday (1)													JŪ
-	A	DAY		D	E	F	G	н			K	L	м	N	0	<u>-n</u>
1	<u>Month</u> 2003		HIGH SCHOOLS													
2	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 (5)	Smith Hill High School (A)													
16	-	Thursday (4)	Key High School (B)													
1/	-	Monday (1)	Birard High School (D)													
10	-	Tuosday (1)	Diald High School (D)													
20	-	Wednesday (3)	Hull High School (E)													
20	-	Thursday (4)	Smith Hill High School (A)													
21	-	Friday (5)	Key High School (B)													
23	-	Monday (1)	Leetch High School (C)													
24		Tuesday (2)	Birard High School (D)													
25	May	,, (,	20003													
26	1 Í	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)													
R	> H Sheet1	(Sheet2 / Sheet3 / 4	Pined Ulab Dabaal (D)			-					5					
She	et 1 / 3		 PageStyle_Sheet:	1			=[[Su	m=0			-0	-+ 10	00%
-	menu 💿	🥑 💷 🚞 🔟 🛙	Termi 🦰 Docum 📄 [Pictur	📄 [lib] 🛛 📧 [Termi 🕯	🕑 kasus:j 📧] Termi	avol1-Se	📄 Sche	d 54.3	ംപു	() ()	°" (M NET	DISK	7% 18:29	0

Maka akan terbuka file xls seperti gambar diatas



Kemudian kita buka browser kembali, klik tab meta data, dan masukkan dir entry number 11. Akan menampikan tipe file, md5 dari contents, SHA-1 dari contents, dan detail dari gambar tersebut.



Kemudian buka terminal dengan perintah foremost –v –i image –o recover. Fungsi foremost untuk mengembalikan data yang tertimpa dan recover sebagai ekstrak file image.



Hasil ekstrak recover foremost dapat dilihat pada gambar diatas dengan folder recover. Kemudian kita buka folder tersebut



Terdapat folder jpg, ole, zip. Kemudian kita buka folder ole



Terdapat file 00000033.ole. lalu buka file tersebut



Setelah terbuka, terdapat file dokumen berupa surat



Lalu buka folder documents kita klik kanan file vol1-sector73.jpg. lalu buka dengan Ghex. Klik ok

File Edit View Go Bookmarks Help			
C O O C I fome/dee/Documents			
vol1-Sector73.jpg - GHex	B h	1	AT DOBLOCK
Pile Edit View Windows Rep 00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60 0000010 00 60 00 00 FF D8 00 43 00 08 06 06 07 06 05 08 00000020 7 07 07 09 09 08 0A 0C 14 0D 0C 08 08 0C 19 12 000000040 00 13 0F 14 1D 1A 1F 1E 1D 1A 1C 1C 20 24 2E 27 20 00000050 39 3D 38 32 3C 2E 33 34 32 FF DB 00 43 01 09 09 9=82 00000050 90 0C 08 0C 18 0D 00 18 32 21 1C 21 32 32 22 22 00000050 32 32 32 32 32 32 32 32 32 32 32 32 32	27P image.zip	iinage1 📲	vol1-Sector73.jpg
00000008032 32 32 32 32 32 32 32 32 32 32 32 32 3			
Unsigned 3 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 little endian decoding Show unsigned and float as hexadecimal Offset: 0x9; 0x4 bytes from 0x6 to 0x9 selected			
vol1-Sector73.jpg" selected (15,9 kB), Free	space: 36,2 GB		<u> </u>
💼 menu 🧰 🧶 💷 🚞 📧 [Ter 📄 Doc 📄 [Pict 🗐 [lib] 🛛 [Ter 🧶 kas 🖾 Ter 🎡 vol 1 📷 Sch	📧 Ter 🝃 vol1 54.	7ºC 👝 💄 🐨 📢 👓	🐣 NET DISK 🛃 88% 18:37 🖵

Tools ghex berfungsi untuk konversi gambar tersebut menjadi bilangan hex. Dapat ditebali kode JFIF, dapat dilihat bilangan hex dari JFIF yaitu 4A 46 49 46.

Pertanyaan yang diminta sebuah pemecahan kasus narkoba tersebut :

1. Siapa pemasok narkoba joe jacob dan alamatnya?

Jimmy jungle, dengan alamat 626 Jungle Ave Apt 2, Jungle, NY 11111

2. Data penting apa yang terdapat di file coverage.jpg dan mengapa data tersebut penting ?

Data penting berupa password, dikarenakan coverage.jpg atau vol1-sector73.jpg memberikan sebuah password untuk membuka file zip (vol1-sector104.zip) yang berupa dokumen jadwal kunjungan pengedar narkoba / scheduled visits.xls

3. Nama sekolah selain smith hill yang sering menjadi tempat transaksi joe jacob?

Smith Hill High School (A), Key High School (B), Leetch High School (C), Birard High School (D), Richter High School (E), Hull High School (F)

4. Untuk setiap file, proses apa yang diambil oleh tersangka untuk mengelabuhi orang lain ?

Tersangka merubah file-file vol1-sector73.jpg dan vol1-sector104.zip menjadi format .raw dan tersangka menyembunyikan sebuah password untuk membuka vol1-sector104.zip pada gambar vol1-sector73.jpg

5. Proses apa yang digunakan penyidik untuk berhasil memeriksa seluruh isi dari setiap file ?

Penyidik melakukan pencarian data-data yang dianggap penting dalam mengungkapkan kasus ini, dan melakukan analisa data-data yang didapatkan, pada data yang didapat berupa file image, penyidik menggunakan tools berupa autopsy, foremost, strings, dan ghex yang berfungsi untuk menganalisa sebuah file yang nanti nya menjadi sebuah bukti dalam kasus ini. Dan terungkap ada file yang penting berupa jadwal pengedaran narkoba pada sekolah-sekolah yang menjadi target penjualan, dan surat dari pengedar narkoba(joe_jacob) untuk pemasok narkoba(jimmy jungle).