Nama : Muhammad Fachrurroji Ilham Saputra

Nim : 09011181320025

## **Computer Forensics**

Penyelesaian langkah-langkah investigasi dari kasus yang telah diberikan, dengan langkahlangkah simulasi yang dilakukan dalam penyelesaian kasus narkoba tersebut sebagai berikut:



Fungsi perintah di bawah : untuk mengecek tipe file. Jika kita menenmukan file yang tidak ada ekstensi, maka kita bisa menggunakan.



Gambar dibawah adalah hasil dari file system dalam folder yang telah dibuat dengan perintah mount image /tmpt/kasus.



File yang ada dalam folder pada gambar diatas tmp/kasus/ dengan hasil mounting dari file image tersebut, untuk melakukan pengecekan utilitas file dengan perintah file \*, yang berarti untuk mengecek semua utilitas dari file yang ada didalam folder kasus tersebut. Terlihat pada gambar dibawah perintahnya

```
root@mahasiswa:/home/mahasiswa/Downloads# cd /tmp/kasus
root@mahasiswa:/tmp/kasus# ls
cover page.jpgc SCHEDU~1.EXE
root@mahasiswa:/tmp/kasus#
root@mahasiswa:/tmp/kasus# file *
cover page.jpgc : ERROR: cannot read `cover page.jpgc
'(Input/output error)
SCHEDU~1.EXE: Zip archive data, at least v2.0 to
extract
root@mahasiswa:/tmp/kasus#
```

Langkah selanjutnya yaitu dengan menjalankan tools autopsy dan membuka local host dengan alamat localhost:9999/autopsy.



Setelah itu mengisi form yang ada pada gambar dibawah untuk menyelesaikan kasus yang diminta.

CREATE A NEW CASE					
1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols.					
2. Description: An optional,	2. <b>Description:</b> An optional, one line description of this case.				
kasus narkoba	kasus narkoba				
3. <b>Investigator Names:</b> The investigators for this case.	optional names (with no spaces) of the				
a. Ilham Saputra	b.				
c.	d				
e.	f.				
g.	h				
i	j.				
New Case	CANCEL HELP				

Maka akan muncul nama kasus yang telah kita isi tadi



Setelah itu kita membuat kasus baru yang akan diselesaikan maka akan menampilkan dialog box yang dapat kita isi dengan menggunakan tools aoutospy untuk mengimport image yang akan diinvestigasi. Pada gambar dibawah contoh langkah – langkah yang dilakukan

1. Hest Name: The name of the computer being investigated. It can contain only letters, numbers, and symbols.     The second secon
Aceteer Casea. Hes

Case: Kasus Host: host1	No images Select the Add	have been added to thi Image File button belo ADD (1965 FILE HELP	s host yet w to add one CLOSE HOST	
	FILE ACTIVITY TIME LINES	IMAGE INTEGRITY	HASH DATABASES	

Setelah melewati bagian dari dialog box diatas maka langkah selanjutnya memasukkan alamat dari file image yang akan diinvestigasi pada gambar dibawah

Case: Kasus Host: host1	ADD A NEW IMAGE
	1. Location Enter the full path (starting with /) to the image file. If the image is split (either raw or EnCase), then enter '*' for the extension.
	2. Type Please select if this image file is for a disk or a single partition. Disk Partition
	3. Import Method To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
	Symlink     Copy     Move

Terdapat langkah – langkah sebagai berikut yang akan mengarahkan keberhasilan dari file yang diupload kedalam tools autopsy untuk dilakukan forensic dari kasus narkoba untuk mencari informasi yang ada.

Disk Image 💿	Volume Image O	
olume System Type (disk image o	my: dos 👻	
ок		
	Image File Details	
	Local Name: images/image	
	<b>Data Integrity:</b> An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)	
	Ignore the hash value for this image.	
	<ul> <li><u>Calculate</u> the hash value for this image.</li> <li>Add the following MD5 hash value for this image:</li> </ul>	
	Verify hash after importing?	
	File System Details	
	Analysis of the image file shows the following partitions:	
	Partition 1 (Tyme, fat12)	
	Mount Point: C: File System Type: fat12	
	**	
ana hann		
C <b>ase:</b> kasus <b>Iost:</b> Joe_Jacob		
C <b>ase:</b> kasus <b>Iost:</b> Joe_Jacob	No images have been added to this host yet	
C <b>ase:</b> kasus <b>lost:</b> joe_jacob	No images have been added to this host yet Select the Add Image File button below to add one	
c <b>ase:</b> kasus <b>iost:</b> joe_jacob	No images have been added to this host yet Select the Add Image File button below to add one	
C <b>ase:</b> kasus f <b>ost:</b> Joe_Jacob	No images have been added to this host yet Select the Add Image File button below to add one	
ase: kasus lost: joe_jacob	No images have been added to this host yet Select the Add Image File button below to add one  ADD IMAGE FILE CLOSE HOST HELP  FILE ACTIVITY TIME LINES MAGE INTEGRITY HASH DATABASES VIEW NOTES  EVENT SEQUENCER	
:ase: kasus lost: joe_jacob	No images have been added to this host yet Select the Add Image File button below to add one ADD IMAGE FILE HELP FILE ACTIVITY TIME LINES VIEW NOTES VIEW NOTES EVENT SEQUENCER	
:ase: kasus tost: joe_Jacob	No images have been added to this host yet Select the Add Image File button below to add one ADD IMAGE FILE HELP FILE ACTIVITY TIME LINES VIEW NOTES VIEW NOTES EVENT SEQUENCER	
:ase: kasus Iost: Joe_Jacob	No images have been added to this host yet Select the Add Image File button below to add one ADD IMAGE FILE HELP FILE ACTIVITY TIME LINES VIEW NOTES VIEW NOTES EVENT SEQUENCER	
:ase: kasus tost: Joe_Jacob	No images have been added to this host yet Select the Add Image File button below to add one ADD IMAGE FILE HELP FILE ACTIVITY TIME LINES VIEW NOTES VIEW NOTES EVENT SEQUENCER	
C <b>ase:</b> kasus <b>Iost:</b> Joe_Jacob	No images have been added to this host yet Select the Add Image File button below to add one ADD IMAGE FILE HELP FILE ACTIVITY TIME LINES VIEW NOTES EVENT SEQUENCER	
'ase: kasus lost: joe_jacob	No images have been added to this host yet Select the Add Image File button below to add one DD IMAGE FILE HELP FILE ACTIVITY TIME LINES VIEW NOTES EVENT SCOUNCER	
ase: kasus lost: joe_jacob	No images have been added to this host yet Select the Add Image File button below to add one CODE HOST FILE ACTIVITY THE LINES VIEW NOTES VIEW NOTES VIEW NOTES VIEW NOTES	

Pada gambar dibawah menunjukkan kasus yang telah dimasukkan dalam tools aoutospy dengan nama kasus yaitu kasus dan nama hostnya ialah Joe\_Jacob.

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-0-0         fat12         details
	ANALYZE ADD IMAGE FILE CLOSEHOST
	FILE ACTIVITY TIME LINES INAGE INTEGRITY HASH DATABASES
	đ

Kemudian dari kasus yang telah dimasukkan lakukan analisa dengan mengklik tombol analyse, gambar dibawah merupakan isi dari informasi yang dimiliki oleh hardrive, dengan menampilkan hasil seperti pada gambar dibawah.

	FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE									
Directory Seek Enter the name of		NOTE	ctory: <u>C:/</u> Generate	MD5 LIST OF FILES						
a directory that you want to view. c:/	DEL	Type <u>dir</u> / <u>in</u>		WRITTEN	Accessed	CREATED	Size	UID	GID	Мета
		v / v	SFAT1	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	SFAT2	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)	15585	0	0	<u>8</u>
file names you want to find.	1	r / r	Jimmy Jungle.doc	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	<u>11</u>
SEARCH										ſ
					File Browsing Mode					

Pada gambar diatas terdapat list yang berwarna merah, yang merupakan isi dari list tersebut filenya sudah dihapus.

FAT CONTENTS (in sectors)
<u>73-103 (31)</u> -> EOF <u>104-108 (5)</u> -> EOF

Dua file yang ada diatas merupakan jejak yang ditinggalkan dalam kasus narkoba, dengan nama file 73-103 (31) dengan maksud yaitu 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.

	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)	ASCII Contents of Sectors 73-103 in image-0-0
View	.21.1222222222222222222222222222222222
ALLOCATION LIST	

Gambar diatas menampilkan detail dari file 73-103 (31) dengan informasi yang dapat diambil yang terdapat pada baris pertama yaitu JFIF.

setelah informasi dari gambar diatas dapat dilihat dengan jelas, dengan mencari secara manual informasi di list of file singnature (wikipedia) seperti yang terilihat pada gambar dibawah, dan juga untuk file yang ada pada sector 104-108 (5).

	exr	OpenEXR image	0	v/1.	76 2F 31 01
	bpg	Better Portable Graphics format <sup>[7]</sup>	0	BPGû	42 50 47 FB
				ັງຍັງບໍ	FF D8 FF DB
	jpg jpeg	IPEG raw or in the JEIE 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
https://en.wikipedia.org/wiki/JFIF	ilbm Ibm ibm	IFF Interleaved Bitmap Image	0 any	FORM ILBM	46 4F 52 4D nn nn nn nn 49 4C 42 4D

Jalankan perintah dibawah untuk mengecek utilitas dari file dengan sector 104-108 seperti pada gambar dibawah.

```
root@mahasiswa:/home/mahasiswa# cd Downloads/
root@mahasiswa:/home/mahasiswa/Downloads# ls
image image.zip Link to image vol1-Sector73.raw
root@mahasiswa:/home/mahasiswa/Downloads# file vol1-Sector73.ra
w
vol1-Sector73.raw: JPEG image data, JFIF standard 1.01
root@mahasiswa:/home/mahasiswa/Downloads#
```

Dengan melakukan pengecekan utilitas dari file sector 104-108 (51) dengan nama file voll-Sector73.raw, maka dapat dilakukan pencarian list of file signature (wikipedia) seperti pada gambar dibawah.

		lz	lzip 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 ods odp	zip file format and formats based on it, such as JAR, ODF,	0	РК	50 4B 03 04 50 4B 05 06
		docx xlsx pptx vsdx apk				(empty archive) 50 4B 07 08 (spanned archive)
https://en.wikipedia.org/wiki/JAR_	_(file	rar e_format)	RAR archive version 1.50 onwards <sup>[8]</sup>	0	Rar!	52 61 72 21 1A 07 00
zip	^	✓ Highlight <u>All</u> Match Case <u>W</u> hole W	lords 4 of 9 matches			

Untuk mendapatkan password dari file sector yang disimpan oleh pelaku kita menggunakan tools strings dan contoh perintahnya ada pada gambar dibwah.



	FFFy	
l		NrH'
	pu0	k
	go}b `/9'	
	Tw	1
	c\[M0	
	T[9j	
	k}Bx`VE	
	s\$6s,	
	zz7q	
	K;dMj	
	)UfRcvm	
	8-'H\$	
	FFFy	
		NrH'
	7g%	
	9.b+	
	R*JI	
۱	oqK4	
J	1+^L	
	pw=good	Lines
	rootemar	las Lswa : / nome / manas Lswa / Down Loads#

Dari hasil srtings diatas kita dapat mengetahui password yang disimpan oleh 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 dibawah.

				Scheduled Vi	sits.xls - Li	breOffice C	alc								-	+ ×
File	Edit View	v Insert Format	<u>T</u> ools <u>D</u> ata <u>W</u> indow <u>H</u> elp													×
	• 6	• 🔤 📭 🗐	🖶 💩 🗙 D 😩 - 🛓	······································	. 🖽 1			I+ I+	7	ይ 🛱	₩ -	• / =	<b>*</b>		1	
Ari	al	▼ 10 <b>▼</b>	a a <u>a</u> · 🗐 ·	= = = <b>=</b> = =	<b></b>	÷ \$	% 0.	0 🗄 🖣	00. ₽0 4000.	= =	⊞ -	:: • <u>::</u> :	•			
B50			= (Monday (1)													≡
	Α	В	С	D	E	F	G	н	I	J	К	L	М	N	(T	
1	Month	DAY	HIGH SCHOOLS													
2	2002	2														E
3	April	Monday (1)	Smith Hill High School (A)													
4		Tuesday (2)	Key High School (B)													1993
5		Wednesday (3)	Leetch High School (C)													
6		Thursday (4)	Birard High School (D)													ň
7		Friday (5)	Richter High School (E)													~
8		Monday (1)	Hull High School (F)	N												f(x)
9		Tuesday (2)	Smith Hill High School (A)	2												5(~)
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)		1	1			1							
HI 4	► H <b>+</b>	Sheet1 Sheet2	Sheet3												· ·	
She	et 1 of 3			PageStyle_Sheet1					B		Sum=	0			+	100%

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 dibawah.

```
root@mahasiswa:/home/mahasiswa/Downloads# foremost -v -i image
-o recover
```

Folder yang aka nada didalam recover nantinya merupakkan informasi yang dibutuhkan dalam menangani kasus narkoba, contohnya untuk file yang ada didalam folder doc, berisi file 0000003.doc dengan info didalamnya yaitu surat dari pengedar narkoba dikasus tersebut, terlihat pada gambar dibawah.

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