# Proj 16: Sleuthkit dan Autopsy (15 pts.)

### **Kebutuhan Project**

• Komputer Linux Backtrack 5 R3. Bisa menggunakan DEFT atau Kali Linux.

### Menjalankan Komputer BackTrack Virtual

1. Masuk ke komputer Backtrack, Log in dengan user name **root** dan password **toor**. Masukkan perintah berikut diikuti dengan tombol Enter: startx

### Meletakkan Evidence pada komputer Backtrack VM

2. Pada Linux Backtrack, buka elearning dan download file **anon-dd.7z** di elearning simpan di desktop. Buka jendela Terminal dan jalankan perintah berikut.

```
cd Desktop (untuk ke direktori desktop tempat file anon1.dd)
7z x anon-dd.7z (untuk mengekstrak)
cd dd (pindah ke direktori dd)
mv anon1.dd.001 anon1.dd (merubah nama anon1.dd.001 menjadi dd)
md5sum anon1.dd (memeriksa nilai hash file)
```

Perintah di atas masuk ke direktori tempat mendownload file anon, mengekstraknya, merubah namanya untuk meremove file ekstensi .001, dan menghitung nilai MD5 hash dari evidence disk. Nilai MD5 harus sama seperti di bawah, berakhiran dengan 4419:

```
root@bt:/anon/dd# md5sum anon1.dd
0ca61246ac61c628ed98daa863354419 anon1.dd
root@bt:/anon/dd#
```

 Jalankan perintah berikut untuk mengetahui informasi tentang file file anon1.dd akan keluar informasi tentang lokasi file di hardisk.

### Menjalankan Autopsy

Di BackTrack, pada jendela Terminal, jalankan perintah berikut:
 cd /pentest/forensics/autopsy
 ./autopsy

Maka program akan berjalan, menampilkan teks sperti berikut. Biarkan jendelanya terbuaka.



5. Dari menu BackTrack menu, click Applications, Internet, "Firefox Web Browser". Ketika Firefox terbuka, arahkan ke alamat berikut: <u>http://localhost:9999/autopsy</u>

Autopsy terbuka, sperti pada gambar di bawah ini. Akan terlihat pesan peringatan "Javascript is enabled". Abaikan saja.



### Membuka Case Baru dengan Autopsy

6. Pada jendela Autopsy, click tombol "**New Case**". Isi form seperti gambar di bawah ini, ganti "Your-Name" dengan nama masing-masing.

#### Project 16 : Sleuthkit dan Autopsy

∧ ∨ × Create A New Case - Mozilla Firefox							
File Edit View History Bookmarks Tools Help							
Create A New Case	×						
← S localhost:9999/autopsy?mod=0&view=1	☆ ▼ 🥰						
BackTrack Linux MOffensive Security Deck Exploit-DB	rack-ng 📓 SomaFM						
CREATE A NEW CASE							
1. Case Name: The name of this in symbols.	vestigation. It can contain only letters, numbers, and						
P9+YOURNAME							
2. Description: An optional, one lin	e description of this case.						
ANON CASE							
3. Investigator Names: The option case.	al names (with no spaces) of the investigators for this						
a. YOUR-NAME	b						
с.	d.						
e.	f.						
q.	h.						
i.	i.						
NewCase	CANCEL HELP						

Click tombol "**New Case**". Pada window "Creating Case", click tombol "**Add Host**". Pada jendela "Add a New Host", accept default options dan click tombol "**Add Host**". Pada jendela "Adding host", click tombol "**Add Image**".

- Pada next window, click tombol "Add Image File".
   Pada jendela "Add a New Image", masukkan options berikut, seperti terlihat di bawah ini:
  - Location: /root/Desktop/dd/anon1.dd
  - Type: Disk
  - Import Method: Copy



#### Click Next.

Pada bagian "Image File Details", click tombol "**Calculate the hash value for this image**", seperti terlihat di bawah ini. Click **Add**.

### Project 16 : Sleuthkit dan Autopsy

∧ ∨ × Collecting details on new image file - Mozilla Firefox					
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp					
🎪 Collecting details on new imag 👎					
🔶 📄 🕜 localhost:9999/autopsy?mod=0&view=14&hc 🗇 🔻 😋 🚷 🖲 Go 🔍 🏠					
Image File Details					
Local Name: images/anon1.dd					
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)					
O Ignore the hash value for this image.					
Calculate the hash value for this image.					
O 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: NTFS (0x07)) Sector Range: 63 to 20663					
Mount Point: C: File System Type: ntfs V					
ADD CANCEL HELP					
For your reference, the mmls output was the following:					
DOS Partition Table Offset Sector: 0 Units are in 512-byte sectors					
Slot         Start         End         Length         Description           02:         00:00         000000063         0000020663         0000020601         NTFS (0x07)					

Maka akan tampil MD5 hash, yang berakhiran dengan 4419, seperti terlihat di gambar bawah.

∧ ∨ × Add a new image to an Autopsy Case - Mozilla Firefox
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp
🊯 Add a new image to an Autopsy 👎
Iocalhost:9999/autopsy?mod=0&view=15&img_p; ☆ ▼  Goi     Soi     Soi
Calculating MD5 (this could take a while) Current MD5: 0CA61246AC61C628ED98DAA863354419 Testing partitions Moving image(s) into evidence locker Image file added with ID img1 Disk image (type dos) added with ID vol1 Volume image (63 to 20663 - ntfs - C:) added with ID vol2
OK ADD IMAGE
Click OK.

### Pencarian di Autopsy

FCCF – Yesi Novaria Kunang, S.T., M.Kom. Page 4 of 9

8. Jendela "Select a volume to analyze or add a new image file" terbuka, seperti pada gambar di bawah ini. Click tombol **Analyze**.

× Op	pen Image In P9-YOURNAME:host1 - Mozilla Firefox					
<u>F</u> ile <u>E</u> dit <u>V</u> iew	/ Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp					
🚯 Open Image	IN P9-YOURNAM 🗱 💮 PTK 🛛 🔺 🕂					
🔶 🗼 S (	🔞 localhost:9999/autopsy?mod=0&view=16&case=P9-YOURNAME&host=hosl 🟠 🔻 🔮 🚼 🔻 Goc 🔍 🏠					
BackTrack Lir	inux 👖 Offensive Security 📲 Exploit-DB 📡 Aircrack-ng 📓 SomaFM					
Case: P9-YOUF Host: host1	RNAME Select a volume to analyze or add a new image file.					
	Case Gallery Host Gallery Host Manager					
	mount name fs type					
	o disk anon1.dd-disk raw <u>details</u>					
	C:/ anon1.dd-63-20663 ntfs details					
	ANALYZE ADD IMAGE FILE CLOSE HOST HELP					
	FILE ACTIVITY TIME LINES IMAGE INTEGRITY HASH DATABASES					
View Notes Event Sequencer						

9. Pada next window, click tab "Keyword Search". Pada kotak pencarian, ketikkan **anon** seperti terlihat di bawah ini. Click tombol **Search**.

ļ	A V X P9-YOURNAME:host1:vol1 - Mozilla Firefox							
Ì	P9-YOURNAME:host1:vol1     X     PTK     FK							
	🖕 🖒 🗿 localhost:9999/autopsy?mod=1&submod=4&case=P9-YOURNAME&host=ht 🟠 🔻 🥑 🛂 🔻 Got 🔍 🏫							
	🚬 BackTrack Linux 👖 Offensive Security 🛄 Exploit-DB 🔪 Aircrack-ng 📓 SomaFM							
	FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE ? X							
	Keyword Search of raw data							
3	Enter the keyword string or expression to search for:							
e	anon							
1	ASCII Unicode							
I	Case Insensitive grep Regular Expression							
I	SEARCH EXTRACT STRINGS							
I	Regular Expression Cheat Sheet							
I								
I	NOTE: The keyword search runs grep on the image. A list of what will and what will not be found is available here.							
I								
ł	Predefined Searches							
	CC SSN2 IP SSN1							
	Date							

### **Hasil Pencarian**

10. Terdapat "120 hits", seperti terlihat di bawah ini:

<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp
🚯 P9-YOURNAME:host1:vol1 🗱 🗍 PTK 🛛 🙀
🖕 🌼 🔕 🔞 localhost:9999/autopsy?mod=1&submod=4&case=P9-YOURNAME&host=host 🔂 🛪 🍘 🚼 🛪 Goo 🔍 🏫
🕿 BackTrack Linux 👖 Offensive Security 🛄 Exploit-DB 🐚 Aircrack-ng 📓 SomaFM
FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE ? X
Searching for ASCII: Done Saving: Done 120 hits- link to results
Searching for Unicode: Done Saving: Done 0 hits
New Search
120 occurrences of anon were found Search Options: ASCII Case Sensitive
Unit 2142 ( <u>Hex</u> - <u>Ascii</u> ) 1: 458 (anon - sf@o) 2: 486 (anon - sf@m) 3: 510 ( <anon -="" sf@m)<="" td=""></anon>
Unit 2238 ( <u>Hex</u> - <u>Ascii</u> ) 4: 245 (SF" <anon -="" sf@o)<br="">5: 272 (To: <anon -="" sf@m)<="" td=""></anon></anon>

### Memeriksa Hits

11. Pada sisi kiri, click link biru Ascii pertama yang terllihat untuk melihat details hits pada panel sebelah kanan, seperti terlihat di bawah ini.

Perhatikan bagaimana merepotkan—gunakan mouse untuk mengclick tiap item; mereka tidak dikelompokkan dalam 22 files seperti FTK, dan tampilannya formatnya sangat minim sehingga kita hanya bisa meihat sebagian kecil dari horizontal line.

#### Project 16 : Sleuthkit dan Autopsy



Meskipun dengan keterbatasannya, saudara masih bisa mencari incriminating email message – untuk membuktikan kejahatan. Ketika ditemukan file incriminating email message, simpan screen image.

### Simpan Screen Image

12. Pastikan layar yang ditampilkan berisi incriminating email message. Tekan tombol Printscreen. UNTUK MENDAPATKAN POIN MAKSIMAL SUBMIT WHOLE-DESKTOP IMAGE. Simpan dengan nama filename "NamaKamu\_Proj16".

### **File Analysis**

Pada halaman pencarian, di sisi kanan atas, click Close.
 Pada halaman Case Gallery, click C:\, seperti terlihat di bawah ini:



14. Di sisi bawah kiri, click tombol Analyze.

Di sisi kiri atas next screen, click tombol "File Analysis".

Sejumlah file akan terlihat seperti pada gambar di bawah ini.

Perhatikan empat timestamps di tiap file: Written, Accessed, Changed, and Created. Inilah Keunggulan Autopsy: karena autopsy menginformasikan ke empat timestamps, sementara FTK hanya tiga.

P9-YOURNAME:host1:vo	12	* PT	ĸ	× +								
🖕 🗼 🗕 🔞 localho	st:9999	/autopsy?	mod=1&submod=2&case	=P9-YOURNAME&host=	host1&inv=unkno	wn&vol=vol2	Ę	े र 😋 🚼	▼ Goog	le	۹ (	
BackTrack Linux 👖 Off	BackTrack Linux 🙀 Offensive Security 🛄 Exploit-DB 🐚 Aircrack-ng 📓 SomaFM											
			YSIS KEYWORD SEARCH	FILE TYPE IMAG	E DETAILS ME		A UNIT HELP	CLOSE X				
Directory Seek		ent Directo	ory: <u>C:/</u> Generate MD	5 LIST OF FILES								Ô
want to view.	DEL	Type <u>dir</u> / <u>in</u>		WRITTEN	Accessed	CHANGED	CREATED	SIZE	UID	GID	МЕТА	
		r/r	<u>\$AttrDef</u>	2013-04-11 02:15:20 (WIT)	2013-04-11 02:15:20 (WIT)	2013-04-11 02:15:20 (WIT)	2013-04-11 02:15:20 (WIT)	2560	48	0	<u>4-128-4</u>	
View		r/r	\$BadClus	2013-04-11 02:15:20 (WIT)	2013-04-11 02:15:20 (WIT)	2013-04-11 02:15:20 (WIT)	2013-04-11 02:15:20 (WIT)	0	0	0	<u>8-128-2</u>	
File Name Search		r / r	<pre>\$BadClus:\$Bad</pre>	2013-04-11 02:15:20 (WIT)	2013-04-11 02:15:20 (WIT)	2013-04-11 02:15:20 (WIT)	2013-04-11 02:15:20 (WIT)	10547200	0	0	<u>8-128-1</u>	
Enter a Perl regular expression for the file		r/r	<u>\$Bitmap</u>	2013-04-11 02:15:20 (WIT)	2013-04-11 02:15:20 (WIT)	2013-04-11 02:15:20 (WIT)	2013-04-11 02:15:20 (WIT)	2576	0	0	<u>6-128-1</u>	
names you want to find.			ASCII (dis	<u>play</u> - <u>report</u> ) * Hex ( <u>dis</u> t	<u>play</u> - <u>report</u> ) * ASC File Type:	II Strings ( <u>display</u> - data	report) * Export * A	dd Note				

15. Coba cari file gambar. Bisa terlihat ada file anak kucing I was able to view the kittens, seperti terlihat di bawah ini, tapi tidak bisa ditemukan incriminating image, karena filenya sudah di deleted.

BackTrack Linux MOffensive Security Deckloit-DB

🔶 📄 😒 💽 localhost:9999/autopsy?

☆ 📽 🛃 🛪 Google 🔍 🏠
CLOSE
?

	0					?	X				
Directory Seek	r/r	Deleted Items.dbx	2013-04-11 01:10:04 (WIT)	2013-04-11 02:17:43 (WIT)	2013-04-11 01:10:04 (WIT)	2013-04-11 02:17:43 (WIT)	207572	0	0	<u>33-128-4</u>	-
Enter the name of a directory that you	r/r	<u>Folders.dbx</u>	2013-04-11 04:33:35 (WIT)	2013-04-11 04:33:35 (WIT)	2013-04-11 04:33:35 (WIT)	2013-04-11 02:17:43 (WIT)	75204	0	0	<u>34-128-3</u>	ļ
want to view. C:/	r/r	happy-kitten-kittens- 5890512-1600-1200.jpg	2013-04-11 02:10:36 (WIT)	2013-04-11 04:32:14 (WIT)	2013-04-11 02:10:36 (WIT)	2013-04-11 02:15:45 (WIT)	145459	0	0	<u>30-128-4</u>	-
View		ASCII ( <u>display</u> - <u>j</u>	r <u>eport</u> ) * Hex ( <u>displa</u> File Typ	<mark>y - <u>report</u>) * ASCII S</mark> e: JPEG image dat	strings ( <u>display</u> - <u>rep</u> a, JFIF standard 1.0	port) * <u>Export</u> * <u>View</u> D1	* Add Note				
File Name Search	C:/happy-kitten-kittens-5890512-1600-1200.jpg										
Enter a Perl regular expression for the file names you want to find.	T	humbnail: <u>View</u>	<u>Full Size Image</u>								
		<b>T</b>									

Sebenarnya Sleuthkit bisa melakukan file carving, untuk merekonstruksi files yang sudah didelete, tapi tentu saja sangat ribet dibandingkan FTK atau ProDiscover.

## Mengumpulkan Project

16. Kirim melalui elearning

Last modified 18-4-2013