# Project 15: Menggunakan FTK (25 pts.)

### **Kebutuhan Project**

• Komputer Windows, real atau virtual. Bisa menggunakan Windows XP /7virtual machine.

### Mendownload Evidence File

- 1. Dowload file evidence yang ada di elearning: <u>anon-E.7z</u>
- Gunakan Hashcalc (bisa di download di sini : http://www.slavasoft.com/hashcalc/) untuk menghitung nilai hash dari file yang didownload. Hasilnya harusnya sama dengan berikut:

H HashCalc		
Data Format: File	Data: C:\Documents and Settings\Student\Desktop\anon-E.7z	
	Key Format: Key:	
MD5	d75b6639f7054e80cede72fb82e30124	
MD4	19be5fe178058c811dc50fd906b04be7	
🔽 SHA1	8a2495ee349ae9cab2cb6fa9ac80dad18dd4f5b1	

Lakukan Unzip dengan software 7-Zip (yang bisa didownload di : http://www.7-zip.org/download.html).

### **Menginstall FTK**

3. Download file yang tersedia di elearning "FTK-Forensic\_Toolkit-1.81.6.exe" install software dengan default options.

### Menjalankan FTK

- 4. Setelah proses instalasi, jalankan FTK. Cat: Jika menggunakan Windows 7 klik kanan icon dan pilih "Run as Administrator".
  - a. Ketika ada pesan Error "No security device was found...", click No.
  - b. Jika ada pesan Error box "The KFF Hash library file was not found...", click OK.
  - c. Ketika ada kotak pops up menjelaskan keterbatasan versi demo, click **OK**.

### Memulai Kasus Baru

- 5. Pada korak "AccessData FTK Startup", pilih "Start a new case" dan click OK.
  - a. Pada layar berjudul titled "Wizard for Creating a New Case", isi seperti berikut seperti terlihat di gambar, rubah "YOUR\_NAME" menjadi nama kalian. click **Next**.

/ Case	_		ĺ
Forensic	*	AccessData's Forensic Toolkit®-FTK® The Complete Analysis Tool	)
Part County of Case		Wizard for Creating a New Cas	se
Investigator Name: Yo	urname	•	
Case Information	Case Number:	18-YOURNAME	
	Case Name:	18-YOURNAME	
	Case Path:	c:\	Browse
Case Description:	Case Folder:	c:\18-YOURNAME	
			*
			-
		Next >	Cancel

- b. Pada layar berjudul "Forensic Examiner Information", biarkan fields nya kosong dan click **Next**.
- c. Pada layar yang bagian "Case Log Options", biarkan pihan default, yang akan mencatat semua log. click **Next**.
- d. Pada bagian "Processes to Perform", buang pilihan "**KFF Lookup**" dan "**Decrypt EFS Files**". click (Next Karena untuk versi demo fitur ini tidak tersedia).
- e. Pada bagian "Refine Case-Default", pilih default "Include All Items". click Next.
- f. Pada bagian "Refine Index Default", click Next.

### Menambahkan Evidence

- 6. Pada kotak "Add Evidence", click tombol "Add Evidence..."..
  - a. Pada bagian kotak "Add Evidence to Case", pilih "Acquired Image of Drive", dan click Continue.
  - b. Pada kotak "Browse for Folder", arahkan ke Desktop, buka folder "E", dan doubleclick file **anon1a.E01**.
  - c. Pada kotak "Evidence Information", click OK.
  - d. Pada kotak "Add Evidence", click Next.
  - e. Pada kotak "New Case Setup is Now Complete", click Finish.
  - f. Kotak pesan "Processing Files..." akan muncul. Tunggu beberapa detik sampai proses selesai.
  - g. Click tab Explore.

h. Pada kiri tengan, entang kotak "List all Descendants". Akan terlihat deretan files, dengan "104 Listed" pada Status Bar, seperti terlihat di bawah ini.

AccessData FTK 1.81.6 DEM	0 VERSION C:\Program	Files \AccessData\A	ccessData Fo	rensic Toolkit 1.8	1.6\DefaultC	ase\	
File Edit View Tools Help							
Overview Explore	Graphics E-M	ail Search	Bookma	ark			
anonia	<u> </u>	🔨 🐨 🖓 🔨	🖗 TEXT HEX 😂	0 🐔			
	-5 =						~
? \$BadClus							
—————————————————————————————————							
- 🝸 \$Secure							
[unnamed]							
🕀 😨 Deleted Iter	is.dbx 🖌						
<							~
List all descendants	<						>
🖉 🛛 👷 🔏 🌭 🕀 🗅 🔅		V III All Colum	18				
File Name	Full Path		Recycle BI	Ext   File Type	Category	Subject	Cr Date
	anon1a\Fart_1\New Volu anon1a\Part_1\New Volu	me-NTFS\\$AUDEr me-NTFS\\$PadClus\\$		Unknown Fil	Unknown		4/10/2013
	anon1a\Part_1\NewVolu	me-NTFS\\$BadClus(		Unknown Fil	Unknown		4/10/2013
	anon1a\Part_1\New Volu	me-NTFS\\$Bitmap		Unknown Fil	Unknown		4/10/2013
Boot	anon1a\Part_1\New Volu	me-NTFS\\$Boot		Unknown Fil	Unknown		4/10/2013
🔲 🧰 \$Extend	anon1a\Part_1\New Volu	me-NTFS\\$Extend		Folder	Folder		4/10/2013
🗖 🎦 \$130	anon1a\Part_1\New Volu	me-NTFS\\$I30		Unknown Fil	Unknown		4/10/2013
🗖 🖸 🕄 \$130	anon1a\Part_1\New Volu	me-NTFS\MyDocume		Unknown Fil	Unknown		4/10/2013:
	anon1a\Part_1\New Volu	me-NTFS\My Docume		Unknown Fil	Unknown		4/10/2013:
SLogFile	anon1a\Part_1\New Volu	me-NTFS\\$LogFile		Unknown Fil	Unknown		4/10/2013
SMFI	anon1a\Part_1\New Volu	me-NTES\\$MET		Unknown Fil	Unknown		4/10/2013
<							>
104 Listed 0 Checked Total	0 Highlighted						
o checked rotai	v nigniighteu						

### **Background Kasus**

7. Barang bukti diambil dari komputer yang ditemukan di ruangan yang digunakan oleh tersangka hacker komuter dari Anonymous gang.

### **Prosedur Pencarian 1: File-demi-file**

8. Pada panel bagian bawah FTK, click item yang pertama. Cari pada panel kanan atas apa yang ada pada file. Tekan panah ke bawah pada keyboard untuk pindah ke file berikutnya. 20 file yang pertama berisi sangat sedikit informasi yang berguna –bisa kita lihat, cara seperti ini tidak efisien untuk mencari barang bukti yang relevan.

### **Prosedur Pencarian 2: Pencarian Keyword**

9. Prosedur yang lebih baik dengan menggunakan pencarian keyword. FTK didesain untuk bekerja dengan cara ini – dengan cara membuat index dari daftar pada file evidence. Buka Notepad dan ketikkan keywords yang terlihat pada gambar di bawah ini. Misalnya seperti kita ketahui pada kasu melibatkan gang Anonymous, keywords juga berasal dari slogan gang Anonymous "Expect Us" dan "We never forgive, we never forget".

🖪 k	eywo	rds.txt	- Not	epad	
File	Edit	Format	View	Help	
Ano ano exp for for	nymo n ect  give get	us			
<					>

- a. Simpan file di desktop sebagai "keywords.txt".
- b. Pada FTK, click tab Search.
- c. Click tombol Import.
- d. Pada kotak "Import Search Terms", arahkan ke desktop dan double-click file **keywords.txt**.
- e. Kotak pop up "Import Search Terms" muncul, yang mengatakan 'Do you wish to show items that have 0 hits?". Click **No**.

### **Hasil Pencarian**

10. Lima keywords ditemukan, seperti berikut pada panel atas FTK:

- AccessData FTK 1.81.6 DEMO VERSION C:\Program Files\AccessData\AccessData Forensic Toolkit 1.81.6\DefaultCase\	
Overview Explore Graphics E-Mail Search Bookmark	
Indexed Search Live Search Search Term: Indexed Words Co Search Items Add Import Options Indexed Words Co Search Items Anonymous 2 1 anon 70 19 expect 2 2 2 forgive Edit Item Remove Item Results » Cumulative operator: AND OR View Cumulative Results »	
· · · · · · · · · · · · · · · · · · ·	
8	~ ~
🗑 📙 🔠 🦃 🔯 🗅 💱 off: Unfiltered 🔍 🥅 All Columns 🔍 prz	
File Name Full Path Recycle Bi Ext File Type Category Subject Cr Date	te
	>
Listed 0 Checked Total 0 Highlighted	-

- a. Pada baris "Cumulative Operator", click tombol **OR**.
- b. Pada baris "Cumulative Operator", click tombol "View Cumulative Results".
- c. Pada kotak "Filter Search Hits", terima pilihan default "All files" dan click tombol **OK**.
- d. Pada panel kanan atas terlihat "81 Hits in 22 Files", seperti berikut.

j.	Overview Explore Graphics E-Mail Search Bookmark
J.	Indexced Search     Import     Options       Search Term     Add     Import       Indexced Words     Co     Search Terms       Hits Files     Edit term     Remove term       Currulative operator:     AMD     OR

11. Pastikan di layar terlihat "81 Hits in 22 Files". Tekan PrintScrn key untuk mengkopi seluruh desktop.

## UNTUK MENDAPAT POIN MAKSIMAL KUMPULKAN DESKTOP IMAGE KESELURUHAN.

Simpan dengan nama file "NamaKamu\_ Project15a".

### **Memeriksa Hits**

- 12. Click item pertama pada panel kanan atas. Item ini berisi, label "81 Hits in 22 Files". Expand dengan menekan panan kanan key di keyboard. Kemudian tekan panah ke bawah untuk ke item berikutnya, yang berlabel "[7 Hits -- Message004]".
- 13. Di layar akan terlihat seperti pada gambar berikut. File ini merupakan email message, dan bisa di baca pada panel bawah-tengah. File ini jelas berupa unimportant spam.

💰 AccessData FTK 1.81.6 DEMO VERSION C:\Program Files\AccessData\AccessData Forensic Toolkit 1.81.6\DefaultCase\	
File Edit View Tools Help	
Overview Explore Graphics E-Mail Search Bookmark	
Indexed Search Live Search	~
Search Term	
6 Hits - [Message002] anon1a/Part_1/New Volume-NTFS/Sent Items.dbx>Message     6 Alta - [Message002] anon1a/Part_1/New Volume-NTFS/Sent Items.dbx>Message	002
Indexed Words Co Search Items Hits Files at 5 mics (messageouoli) at ioitat/art_1(new volume-NTFS)ortic terms. AuX>>>messageouoli at ioitat/art_1(new volume-NTFS)ortic terms. AuX>>>messageouoli at ioitat/art_1(new volume-NTFS)ortic terms.	2
6 Hits - [Message0009] anon1a\Part_1\New Volume-NTF5\Inbox.dbx>>Message0009	-
G Hits - [Message0007] anon1a\Part_1\New Volume-NTF5\Inbox.dbx>>Message0007	
5 Filts - [Attachment]] anon1a/Part_1]/Wew Volume-NTF5]/nbox.dbx >> Message0009?	>Atta
Since Triessageouogi a nontagrand typew rounewith Syllox.dxx > Messageouogi Since Triessageouogi and type and type with the syllox.dxx > Messageou007	>Atta
Edit Item Remove Item Remove All View Item Results > a 4 Hits - [Message0006] anon1a\Part_1\New Volume-NTF5\Inbox.dbx>>Message0006	
Cumulative operator: AND OR View Cumulative Results > 4 Hits - [Message0005] anon1a\Part_1\New Volume-NTF5\Inbox.dbx>>Message0005	
4 Hits - [Attachment]] anon1a[Par_1]/Wew Volume-NTF5[Inbox.dbx>>Message0004]     4 Hits - [Attachment]] anon1a[Par_1]/Wew Volume-NTF5[Inbox.dbx>>Message0004]     4 Hits - [Attachment]] anon1a[Par_1]/Wew Volume-NTF5[Inbox.dbx>>Message0004]	>Atta
Sincs - Intessageout Failor rate at the would read a the state of	>
g of the 25 double of a double of the 100 source	-
id B7/CC-29928-4E5D5615; Wed, 10 Apr 2013 17:13:08 -0400	
Date: Wed, 10 Apr 2013 17:13:08 -0400	
Content-Type: multipar/alternative; boundary="1234567890"	
MIME-Version 10	
From: "Publishers Clearing House" < PublishersClearingHouse@pchcustomerservice.pch.com>	
Reply-To: "Publishers Clearing House" <publishersclearinghouse.sb207b.134597@pchcustomerservice.pch.com></publishersclearinghouse.sb207b.134597@pchcustomerservice.pch.com>	
lo: Janon-st@outlook.com	×
📓 🗄 🔠 🍕 🗣 🛱 🗅 💱 org: Unifitered 🛛 🖌 All Columns 🖌 ptz	
T File Name Full Path Recycle Bi Ext File Type Category Subject Cr Date Mod Dat	э 🔨
□ □ 個 Message0002 anon1a\Part_1\New Volume-NTFS\Inbox.dbw> E-mail "Setup yo N/A N/A N/A	
Lice messagebulus anonia Vari Livew volume Ni Fis Vindox dbx>	
Concessage0005 anona and a transmission of the structure and the s	~
	>
22 Listed 0 Checked Total anon1a/Part 11kew Volume-IITFS/Inbox.dbx>Messade0004	
	_

### Prosedur

14. Berikut ini cara memeriksa hits dengan cepat. Ikuti petunjuk berikut.

- a. Pada bagian HITS di kanan atas, tekan panah ke bawah untuk memilih item berikutnya.
- b. Perhatikan PREVIEW pada layar tengah.
- c. Jika filenya penting, check kotak pada baris yang berbayang pada bagian FILES di bawah layar.

🖇 AccessData FTK 1.81.6 DEMO VERSION C:\Program Files\AccessData\AccessData Forensic Toolkit 1.81.6\DefaultCase\ 📃 🗖 🗙
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Boolmark
Indexed Search Live Search 🔄 81 Hits in 22 Files - QUERY: (Anonymous) OR (anon) OR (expect) OR (forgive) OR (forget)
Secret Target 0 - 7 Hts - [Message0004] anon1alPart_1\\ww Volume-NTFS\Inbox.dbx>>Message0004
Account retring     A
Indexed Words Co Search Items Hits Files (Hessage0001 anon1a/Part_1/Vew Volume-I/TFS/Sent Items.dbx>>Message0001
el + 6 His - (Messageuluc) and Albart Deek violine-ut-s(Utdox.dox > Messageuluc) 0.6 His - (Messageuluc) and Albart Deek violine-ut-s(Divudox.dox > Messageuluc) 0.6 Albart - (Messageuluc) and Albart Deek violine-ut-s(Divudox - Messageuluc) 0.6 Albart - Messageuluc) and Albart Deek violine-ut-s(Divudox - Messageuluc) 0.6 Albart - Messageuluc) and Albart Deek violine-ut-s(Divudox - Messageuluc) 0.6 Albart - Messageuluc) - Alba
⊕ 5 Hts - [Attachment III S i](Inbox.dbx>>Message0009>>Atta
⊕-5 Hts - [Message001
S Hits - [Attachment1] anon1a[Part_1]Wew Volume-NTFS[Inbox.dbx>>Message0007>>Atta
Edit tem Remove tem Remove All View tem Results > (a) 4 Hits - [Message0006] anon1a/Part_1View Volume-NTFS(hox.dbx>>Message0006
Cumulative operator: AND OR View Cumulative Results > U+ 14 - (Massageuus) anon1a/Par_1/vew Volume+VH=Vhow dx>>Pressageuus)
ii) 3 Hz - [Messageout] anni 49 ar 10 w volume-NTSOutbox.dbx > Messageout]
by bm1-29 bo3 e-dialog.com (envelope-from <2N/THL1-TUS90-M1MV6-DE3R1E-HBGJH7-M-M2-20130410-e75e468eec2e18570@pchcustomerservice.pch.com>) (ecelerity 2.2.2.45 r(34222M)) with ESMTP id B7/CC-29928-4E5D5615; Wed, 10 Apr 2013 17:13:08 -0400 Date: Wed, 10 Apr 2013 17:13:08 -0400 Content-Type: multipart/alternative; boundary=*1234567890* Content-Transfer-Encoding: binary MIME-Version: 1.0 From: "Publishers Clearing House" <publishersclearinghouse@pchcustomerservice.pch.com> Reply-To: "Publishers Clearing House" <publishersclearinghouse.sb207b.134597@pchcustomerservice.pch.com> To: janon-st@outlook.com</publishersclearinghouse.sb207b.134597@pchcustomerservice.pch.com></publishersclearinghouse@pchcustomerservice.pch.com>
The rue name rue ran Recycle B Ext Prie Type Category Subject Cr Date Mod Date A
Entrain research and the second and
A Message0004 anon1a/Part_1/New Volume-NTFS/Inbox.dbx>>
TILES vai "Welcome N/A N/A 🗹
22 Listed 0 Checked Total anon1a/Part_11lew Volume-HTFS/Inbox.dbx>>Message0004

- d. Proses sampai semua 22 files dengan cara ini.
- e. Cari email yang berisi kejahatan kriminal, dan beberapa file yang dicurigai.

 15. Pastikan di layar menampilkan email berisi kejahatan criminal yang ditemukan. Tekan tombol PrintScrn key.
 HARUS MENGUMPULKAN COMPLETE DESKTOP IMAGE UNTUK MENDAPATKAN POIN MAKSIMAL. Simpan gambar dengan nama file "NamaKamu\_Proj15b".

### **Melihat Gambar**

- 16. Salah satu kelemahan pencarian menggunakan pencarian keyword adalah tidak akan menemukan kata dalam gambar. Untuk melihat gambar, click tab **Graphics** pada bagian atas jendela FTK.
  - a. Pada kiri tengah, terdapat tiga struktur yang memperlihatkan file dan folder. Click item teratas, **Case**, dan gunakan panah ke bawah untuk pindah ke item berikutnya.
  - b. Ketika ingin membuka folder, gunakan panah kanan untuk membukanya.
  - c. Ketika memilih folder yang berisi gambar di dalamnya, akan terlihat thumbnails pada panel atas seperti berikut:

🖧 AccessData FTK 1.81.6 DEMO V	ERSION C:\Program File	s \AccessData \Acces	sData Forensic	: Toolkit 1.81.6\Default(	Case\		
File Edit View Tools Help							
Overview Explore	Graphics E-Mail	Search	Bookmark				
Cute-Kitten-kit  happy-kitten-l uni	titled.bmp						
🖃 🗶 Case	<u>_</u>	<b>₩</b> ,	<b>29</b> 음 떪	🖗 🗿 🖉			
Anon1a     Part1     Part1	bx 11 13 Total Flagged Items: 0						×
🖁 🗄 🔠 🍕 🃚 📑 🗅 🐳	OFF Unfiltered	All Columns	<b>~</b> C	ITZ			
File Name     Gute-Kitten-kittens-16122946-1     Mappy-kitten-kittens-5890512-1     Menopy-kitten-kittens-5890512-1	Full Path anon1 a\Part_1\New Volume-N anon1 a\Part_1\New Volume-N anon1 a\Part_1\New Volume-N	Rec IFS\Cute-Kitten IFS\happy-kitten IFS\untitled.bmp	tycle Bi Ext ipg ipg bmp	File Type Category JPEG/JFIF File Graphic JPEG/JFIF File Graphic Bitmap File Graphic	Subject	Cr Date 4/10/2013 12:15:42 4/10/2013 12:15:45 4/10/2013 12:15:48	Mod Date 4/10/2013 12:10:4- 4/10/2013 12:10:3 4/10/2013 12:11:3
							>
3 Listed 5 Checked Total	0 Highlighted						

- d. Kucing tersebut memang bukan bentuk kejahatan, tapi coba lihat lebih dekat untuk meyakinkan.
- e. Pada panel atas, click salah satu dari thumbnails. Maka gambar akan terlihat dalam ukuran penuh pada panel kanan atas, seperti berikut:



- f. Lanjutkan dengan memeriksa semua folder sampai ditemukan gambar yang mencurigakan. Tandai semua gambar yang mencurigakan dengan mencentang kotak pada panel bawah, seperti yang dilakukan pada email messages.
- g. Salah satu gambar memperlihatkan halaman Web yang diserang. Pastikan mendapatknya untuk membuktikan penyerangan.

17. Pastikan di layar menampilkan gambar yang berisi kejahatan criminal yang ditemukan. Tekan tombol PrintScrn key.

HARUS MENGUMPULKAN COMPLETE DESKTOP IMAGE UNTUK MENDAPATKAN POIN MAKSIMAL. Simpan gambar dangan nama fila "NamaKamu Proi15a"

#### Simpan gambar dengan nama file "NamaKamu\_Proj15c".

### Membuat Report/Laporan

18. Pada FTK, dari baris menu bagian atas, click File, "Report Wizard".

a. Pada bagian "Case Information", click Next, seperti terlihat di bawah ini.

FTK Report Wizard	Case Information	×
Case Inform	ation	
The following information	n will appear on the Case Information page of the report:	
🔽 Include Investigator	Information in report	
Agency/Company:		]
Investigator's Name:	Your name 🗸	
Address:		
		1
Phone:	Fax:	
E-Mail:		]
Comments:		]
		1
		_
	Next > Cancel	)

b. Pada halaman "Bookmarks - A", click tombol "**Yes, export all bookmarked files**", seperti terlihat di bawah ini. Kemudian click **Next**.

FTK Report Wizard - Bookmarks	]
Bookmarks - A	
The bookmark section is optional. It contains a listing of the bookmarks that have been created during the investigation.	
Would you like to include a bookmark section in the report? <ul> <li>Yes, include all bookmarks</li> <li>Yes, include only bookmarks marked "Include in report"</li> <li>No, do not include a bookmark section</li> </ul>	
Would you like to include a thumbnail image for each bookmarked graphic file?  Include thumbnails of bookmarked graphics  Export full-size graphics and link them to the thumbnails  Include thumbnail summary of bookmarked graphics	
Would you like to export the bookmarked files to the report? Yes, export all bookmarked files Yes, export only files from bookmarks marked "Export to report" No, do not export bookmarked files	
< Back Next > Cancel	

- c. Pada halaman "Bookmarks B", click Next.
- d. Pada halaman "Graphic Thumbnails", click "Export full-size graphics and link them to the thumbnails", seperti berikut. Kemudian click Next.

FTK Report Wizard - Graphic Thu	imbnails 🛛 🔁
Graphic Thumbnails The graphic thumbnail section is option files found in the evidence. It may optic Export full-size graphics and link t Would you like to include a separate se O Yes, include all graphics in the ca	al. This section displays a thumbnail list of graphic mally contain links to the full-size images. hem to the thumbnails sction for graphic thumbnails? Ise
Yes, include only graphics riagged     No, do not include a graphic thum     Graphic thumbnail arrangement: <ul> <li>1 per row</li> <li>c:\myfolder\myfile1.jpg</li> <li>c:\myfolder\myfile2.jpg</li> <li>etc</li> </ul>	Group all filenames at end of report
	< Back Next > Cancel

FCCF – Yesi Novaria Kunang , S.T., M.Kom.

- e. Pada halaman "List by File Path", click Next.
- f. Pada halaman "List File Properties A", click Next.
- g. Pada halaman "Supplementary Files", click Next.
- h. Pada halaman "Report Location", click Finish.
- i. Kotak pop up "Report Wizard" akan muncul, menanyakan "Do you wish to view the report?".
- j. Click Yes.
- k. Report muncul, seperti berikut.



 Pastikan di layar menampilkan report dengan nama kalian Investigator seperti terlihat di atas. Tekan tombol PrintScrn key.

HARUS MENGUMPULKAN COMPLETE DESKTOP IMAGE UNTUK MENDAPATKAN POIN MAKSIMAL.

Simpan gambar dengan nama file "NamaKamu\_Proj15d".

### Mengekspor File yang dipilih

20. Pada Report tidak menyertakan file yang dipilih –kita perlu melakukannya secara terpisah.

- a. Pada FTK, dari baris menu atas, click File, "Export Files".
- b. Pada kotak "Export Files", click "**All checked files**", seperti berikut. Kemudian click **OK**.

Export Files		
File(s) to Export         All highlighted files         All highlighted files         Include email attachments with email messages		
File Name	Original Path	~
\$LogFile[9] Deleted Items[41].dbxMessage0001[ Deleted Items[41].dbxMessage0001 issues[82].htm Outbox[66].dbxMessage0002[70] Sent Items[72].dbxMessage0002[76] Sent Items[72].dbxMessage0002-my The Log2.dbxMessage0002-my	anon1a\Part_1\New Volume-NTFS anon1a\Part_1\New Volume-NTFS anon1a\Part_1\New Volume-NTFS anon1a\Part_1\New Volume-NTFS anon1a\Part_1\New Volume-NTFS anon1a\Part_1\New Volume-NTFS	
Destination Path: ogram Files\AccessData\AccessData Forensic Toolkit 1.81.6\DefaultCase\Export\ Prepend archive name to file name Append item number to file name to guarantee uniqueness Append appropriate extension to file name if bad/absent		
Export Options Don't export RAW file when exporting HTML and/or filtered text Export HTML view if available Export filtered text view		
	0)	Cancel

- c. Untuk melihat file yang diekspor, click Start, Computer, dan arahkan ke folder C:\Program Files\AccessData\AccessData Forensic Toolkit 1.81.6\DefaultCase\Export".
- d. File-file tersebut akan terlihat seperti berikut.



### Mengumpulkan Project

21. Kirim melalui elearning.

Last Modified: 22-5-13