Introduction to Digital Forensics Investigation I

The first digital forensics module gives a brief history of digital forensics and how it progressed into the modern-day version. It also explains what digital forensics is, the role it plays in our society, and an understanding of the professionals who uses it. This module uses the free tool Autopsy to analyze an evidence file to teach students about digital forensics. It teaches students how to open a new case, upload an evidence file and start analyzing it. It also gives a brief explanation of the hexadecimal system and how it correlates with computer files. This includes the explanation of how numbers can be used to represent letters and symbols by using ASCII code. Moreover, it teaches students how to learn from the information that Autopsy extracts such as email addresses and how to view detailed information about them. This detailed analysis continues with phone numbers, URL's, credit card numbers, and banking identification numbers. This session also explains how Autopsy uses an advanced series of keyword searches to find these things, and the files that it extracts them from.

Digital Forensics Module I Notes

- In this module we will learn about digital forensics through a program named Autopsy. You can find a download link for it here, https://www.sleuthkit.org/autopsy/. The version you will need will depend on the type of windows you are using at home. It comes in both a 32-bit and 64-bit version.
- So, what is digital forensics?
 - Digital forensics is a branch of forensic science that involves the recovery and investigation of materials found in digital devices. Digital forensics can be used to investigate networks, hard-drives, data bases, mobile devices, and many more things.
 - This is important because computers are everywhere and almost everyone uses them. Digital forensics is used to link criminals to crime by tracking their digital footprint (we all have one). It is used to help aid the criminal justice system by linking people to forms of cybercrime or can link them to a physical crime. It all depends on the crime being committed.
 - The police, various forms of the government (such as the FBI, DEA, NSA and others), and cyber security professionals use digital forensics in their day to day routines.
- Getting started
 - To get started with a digital forensic investigation we first need to launch Autopsy.
 There should be an icon on the desktop that looks like:



• When it opens you should see this screen:



• You are going to want to click on the button that says, "New Case", you should then see this:

😹 New Case Information			2
Steps	Case Informatio	n	
 Case Information Optional Information 	Case Name:	Our First Exam	
	Base Directory:	C:\Users\jacks\Desktop\Digital Forensics\Evidence Files\	Browse
	Case Type:	Single-user Multi-user	
	Case data will be	stored in the following directory:	
	C:\Users\jacks\[Desktop \Digital Forensics \Evidence Files \Our First Exam	
		< Back Next > Finish Cancel	Help

• You should now name your case. Then you will want to select a folder to put the Autopsy file in, I recommend making a folder on your flash drive, so that way you can open it on any computer you want. Then click next.

😹 New Case Information			\times	
Steps	Optional Info	ormation		
 Case Information Optional Information 	Case Number:	1		
	Examiner			
	Name:	Jackson		
	Phone:			
	Email:]	
	Notes:	This is the first exam using Autopsy.		
	Organizatio	n		
Organization analysis is being done for: V Manage Organization				
		<back next=""> Finish Cancel Help</back>	þ	

• On this next screen enter in information such as the case number, examiner name, a phone number, email address, and any notes you want to include that may be useful to identify the case.

😹 Add Data Source		×
Steps	Select Type of Data Source To Add	
Select Type of Data Source To Add Select Data Source Configure Ingest Modules Add Data Source	Disk Image or VM File	
	Local Disk	
	Logical Files	
	Unallocated Space Image File	
	< Back Next > Finish Cancel Help	

 Next, we need to load in our evidence file. Start off by making sure "Disk Image or VM File" is selected, then click next.

*	Add Data Source					×
Ste	eps	Select Data Source				
1.	Select Type of Data Source To	Browse for an image file:				
2.	Select Data Source	C:\Users\jacks\Desktop\Digital Fo	rensics\Evidence Files\ntfs1-gen2	2.E01		Browse
3. 4.	Configure Ingest Modules Add Data Source	Please select the input timezone:	(GMT-5:00) America/New_York	\sim		
		Ignore orphan files in FAT file	systems			
		(faster results, although some	data will not be searched)			
			< Ba	ack Next >	Finish Cancel	Help
_						

• Click where it says "Browse", then navigate to the "Evidence Files" folder on your flash drive, and select the file titled "nfts-gen2.E01". Then click next.

Add	Run ingest modules on:				
Select Data Source	All Files, Directories, and Unallocated Space	~	Select keyword lists to enable during ingest:		
 Compute Ingest Hodules Add Data Source 	Recent Activity Hash Lookup File Type Identification Embedded File Extractor Firif Parser	^	Phone Numbers Prodeeses Email Addresses URLs Credit Card Numbers		
	Keyword Search				
	Email Parser Extension Mismatch Detector E01 Verifier Interesting Files Identifier PhotoRec Carver Correlation Engine		Scripts enabled for string extraction from unknown file types: Latin - Basic Encodings: UTF8, UTF16		
	Encryption Detection Virtual Machine Extractor	~	Performs file indexing and periodic search using keywords an		
	Select All Deselect All His	story	Global Settings		

 On this screen leave everything clicked. You need to scroll down to where it says, "Keyword Search". Make sure everything under this tab is selected, including Phone Numbers, IP Addresses, Email Addresses, URL's, and Credit Card numbers. Then click "Next" and finally "Finish"

Cur First Exam - Autopsy 4.6.0											-	٥	×
+ Add Data Source 📠 Images/Videos	🗧 🧮 Timeline 📗 Generate	Report 💊 0	Close Case						<u>A</u> 81	 Keyword Lists 	Q- Keyw	ord Search	,
$\langle \cdot \rangle$	Show Rejected Results	Listing Data Sources										()	▼ □ Results
Constant Sectors Con	(3) erch (3)	Lating Data Sources Table Thum Name	brail THE Metadata of 31528 E He Metadata of 31528 F He Metadata of 31528 F He Metadata of 31528 F He He Metadata of 31528 F He	Type Image 2.E01 Results Me Page 4X 54 46 00 00 79 00 80 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00	✓ Size (By., S16554752	Sector Size 512 512 512 512 512 512 512 512	e (Bytes) Other Oc 02 01 0 00 00 0 00 00 0 00 00 0 00 00 0 00 00 0 16 24 0 16 24 0 16 24 0 18 80 6 16 24 0 18 6 6 06 41 0 19 76 0 01 0 0 01 0 01 0 0 0 0 0 0 0 0 0 0 0 0 0 0	MD5 Hash 27 aV5 to 10 are 7 40 27 aV5 to 10 are 7 40 20 aV5 to 10	tt 0	Tinezone Ananca/New_York	Device ID 6754/513-c3a	1 R	45-46
		0x0000000 0x0000000 0x00000010 0x00000110	0: 00 66 50 0: 0F 85 0C 0: B4 42 8A 0: 66 58 66 0: 66 77 F1	06 53 66 00 E8 B3 16 24 00 58 1F EB	68 10 00 FF 80 3E 16 1F 8B 2D 66 33 Ch 66 9B	01 00 80 14 00 00 F4 CD 13 D2 66 0F	3E 14 0F 84 66 58 B7 0E	00 00 .fP.Sf 61 00 5B 07 .B\$. 18 00 fXfX	fh>a. fX[. -f3.f				
		04000012	0. 00 E/ EL	25 02 0A	08 00 08			Analuting filer	from offe1-pen2 E	68		ास्त्र	•

- When it loads, you should screen like this one above.
- In the window to the bottom right you will see a bunch of numbers and letters. Such as "00" or "AA" or combinations of the two like "D0". These are hexadecimal numbers. It is a method used to turn letters, and symbols into numbers. So instead of using digits 0-9, it uses 0-9, and A-F. For a nice video explaining the binary and hexadecimal system check out, https://www.youtube.com/watch?v=aB____6e6WkFQ
- Using hexadecimal (or hex for short) we can encode letters and symbols. For example, the number 68 has a hex code of 44. In the ASCII encoding scheme, this represents the letter D.
- This is how computers store information, so it is important to understand how this works, if wish to further understand how data is stored and manipulated in computers.
- After the computer is done analyzing the evidence file the screen should look like this:

k GenCyber Exam 1 - Autopsy 46.0 – 🗇 🗙 ase View Tools Window Help							
🕂 Add Data Source 📠 Images/Videos 🗮 Timeline 📗 Gen	🕨 Add Data Source 🤹 Images/Ndeoz 👱 Timeline 🚡 Generate Report 💊 Close Case						
Show Rejected Results Show Rejected Results	Listing Data Sources Table Thumbnail Name	Type Image	⊽ Size (By 516554752	Sector Size (Bytes)	MD5 Hash 27a9053e35aac74608493e755353cb95	Timezone America/New_York	
••••••••••••••••••••••••••••••••••••	¢						
Brogen Tegen Lin_ Reports	Hex Strings File Metade	ta Results Me	ssage Indexed T	ext Media Other C			

 Now let's use autopsy to look at email addresses. Let's first click on where it says Results, and then scroll down to where it says Email Addresses (3). Then click on the magnifying class to expand the tab.

Case View Tools Window Help		
case view roos window riep		
🕂 Add Data Source 📠 Images/Videos 🗮 Timeline 📗 Genera	te Report 🛛 💊 Close Case 🗧	
← →	Listing (\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-	-ZO-9%+_\-]+)*(\}?)\@([a-zA-Z(
🖃 🖷 Data Sources	Table Thumbnail	
🖮 🧾 ntfs1-gen2.E01	△ List Name	Files with Hits
\$OrphanFiles (0)	S bullock@rti.org (2)	2
\$Extend (5)	Q vi 6@3ov KE (1)	1
SUnalloc (1)		1
Encrypted (7)		
System Volume Information (2)		
. Views		
E Results		
Extracted Content		
🛱 🔍 Keyword Hits	Hex Strings File Metadata	lesults Message Indexed Tex
⊡ Single Literal Keyword Search (0)		
Generation Search (0) Single Regular Expression Search (0)		
Email Addresses (3)	1/1	
Hachset Hits	+u	
- Mail Messages		
★ Interesting Items		
Accounts		
Tags		
Reports	1	

- If you click on the first email address <u>bullock@rti.org</u>, it shows two different files that appear.
- We see two files named "report02-3.pdf". Then if you look you can also see a phone number in the Keyword Preview area.

Listing							
bullock@rti.org	2 Results						
Table Thumbhail							
Source File	Keyword	Keyword Regular Expression	Keyword Preview	Modified Time			
👘 report02-3.pdf	bullock@rti.org	(\{?)[a-zA-Z0-9%+_\-]+([a-zA-Z0-9%+_\-]+)*(\}?)\@([(919) 485-5599 or «bullock@rti.org«. Thank you in	2008-12-31 18:08:33			
🌴 report02-3.pdf	bullock@rti.org	$(\ (\ (\)[a-zA-Z0-9\%+_\]+(\ (a-zA-Z0-9\%+_\)+)*(\))(@([\ \ldots)$	(919) 485-5599 or «bullock@rti.org«. Thank you in	2008-12-31 18:08:33			
		Tedaurd Text, M. E., Office		1			
Hex Strings File Metadata	Results Message	Indexed Text Media Other Occurrences					
Matches on page: 1 of	1 Match 🧲 ·	Page: 15 of 19 Page ← →	Text Source: Search Re	sults ~			
Question 4.1)				^			
World with Improved Testing							
Tools				_			
Requirements gathering an architectural design	d analysis/ hours	hours					
Coding/unit testing	hours	hours		Ŷ			

- By moving the scroll bar over to the right, we can see some other interesting things. Like the time it was modified, accessed, and changed. Along with the file path.
- If we look in the box underneath the area we were just looking at we can view the email by moving the vertical scroll bar up and down.
- We can also view other information such as the hexadecimal values for the strings in the file, we can view just the strings with no blank lines in between the strings, the file metadata (Which is an informational panel describing the file), the results, and the indexed text which you are looking at now.

<		>
Hex Strings File Metadata Results Message Indexed Text Media Other Occurrences		
Matches on page: 1 of 1 Match < > Page: 15 of 19 Page <	Text Source: Search Results	~
<pre>[report02-3.pdf, have any questions as you complete the survey, please contact Michelle Bullock at (919) 485-5599 or bullock@rti.org.</pre>		^
Thank you in advance for your participation.		
The Freemis Tourses of Teadsmines Tefreedownstone for Saferra Tasking		~

- We can view that data by clicking the corresponding tabs on the top left section of this window.
- Now lets click on the other email address. Labeled <u>xL6@30v.ke</u>. This address contains a file named "logfile1.txt". If you view the contents of this email, you will see this.
- This looks like this because this file is encrypted.
- If we look at the File Meta-Data for this, we can learn something useful.
- \circ $\;$ As you can see in the name, this file belongs to the encrypted folder.
- A little bit further down, you can see the MD5 hash.

[logfile	l.txt, Th}!
E*tsa	
^nY+	
{cBg	
SOF	
н	w+
6+Bw	
HMn2	
UcNg	
	Gt6
u/ktb	
-1-080	

	Hex Strings File Metadata	Results Message Indexed Text Media Other Occurren					
	Name	/img_ntfs1-gen2.E01/Encrypted/logfile1.txt					
	Туре	File System					
3	MIME Type	text/plain					
	Size	21888890					
	File Name Allocation	Allocated					
	Metadata Allocation	Allocated					
	Modified	2009-01-05 17:01:26 EST					
	Accessed	2009-01-05 17:01:26 EST					
	Created	2009-01-05 17:00:20 EST					
	Changed	2009-01-05 17:01:26 EST					
	MD5	cb45c6ad5abb2ff240217aead1e85f13					
	Hash Lookup Results	UNKNOWN					
	Internal ID	45					
		· · · · · ·					

- From The Sleuth Kit istat Tool:
- The MD5 hash is a way on encoding a whole file into a 32-bit hash. This is used to ensure that files are the same, this is particularly useful when two people are downloading the same value. Instead of having to download the whole file, they could download this. If the hashes match, this means that the file the people downloaded is the same.

4	>	Show Rejected Results	Listing					$\leftrightarrow \bullet \bullet \bullet$		
-	Data	Sources	(919) 485-5599 Table Thumboail					2 Results		
	- III 1	ntfs1-gen2.E01	Course Ele	Kauward	Keyword Decider Expression	Keyword Draview		Madified Time		
	- T- 0	\$OrphanFiles (0)	Source File	Neyword	Reyword Regular Expression	Reyword Preview		Modified fille		
		\$Extend (5)	😤 report02-3.pdf	(919) 485-5599	[\.\-\?\;\\!\!\:\[\]\/\(\)\"\">\{\}](\([0-9]{3}\) [0-9]{3}	Michelle Bullock at «(919) 485-55	99«or bullock@rti.org.	2008-12-31 18:0		
	_	\$Unalloc (1)	🕂 report02-3.pdf	(919) 485-5599	$[\ . -!? , : !!: [!] /!(!)!"" > {!}](!([0-9]{3}!))[[0-9]{3}$	Michelle Bullock at «(919) 485-55/	99«or bullock@rti.org.	2008-12-31 18:0		
		Compressed (7)								
Data Sources This-gen2.E01 SorpharFiles Subalac (1) SorpharFiles Subalac (2) SorpharFiles Subalac (2) SorpharFiles SorpharFiles Results Results Results SorpharFiles SorpharFiles Results SorpharFiles Sorpha	Encrypted (7)	<					>			
		BAW (7)	The second							
		System Volume Information (2)	Hex Strings File Metadata	Results Message	Indexed Text Media Other Occurrences					
b -1	View	IS IS	Matches on pages 1 of	2 Match	Page 15 of 10 Page 4	Text	Sources Search Denuity			
i-a	E Resu	ults	Hatches on page. 1 of	2 Mator C	Page. 13 of 15 Page	TEXT	Source. Search Results	· · ·		
Τ.	- 🖬 🛙	Extracted Content	(515) 405-5559 or bullock@rti.org.							
11.	E- Keyword Hits		· · · · · · · · · · · · · · · · · · ·							
	b _0	Single Literal Keyword Search (0)								
		Single Regular Expression Search (0)								
	- C	URLs (184)	Inank you in advance for	your pareicipae	ava.					
	- C	IP Addresses (2)								
	- C	Phone Numbers (2)								
	ITa	I L I-17L I: I/U I: V(1) V(1)/"(1>V(1)] (V(0-9]{3}) (0-9]{3}								
		(919) 485-5599 (2)	he Economic Impacts of Inadequate Infrastructure for Software Testing							
	<u>ا</u> (Email Addresses (3)								
	- 1	Hashset Hits								
	👱 🛛	E-Mail Messages	1. Background Information							
	*	Interesting Items								
	b-🗊 /	Accounts	1.1 Flease type your nam	e, company name						
	<u>i</u> ا	🔋 Credit Card	Name :							
0 -1	Tags	s								
	Rep	orts	Company:							
			E-mail:							
<		>						¥		

- If you click on where it says phone numbers, then expand the directory underneath that tab you can see the files that we found in the email section.
- These phone numbers match what we previously found.
- What this tells us is that Autopsy, scans the files search by search.

🐈 Add Data Source 📠 Images/Videos 🗮 Timeline 脑 Gene	erate Report 🥃 Close Case 🗧				
Show Rejected Results	Listing (((((h H)(t T))(f F))(t T)(p P)(s S?)\;\\) (w W){3,3}](a-zA-Z0-9\-] Table Thumbnail	+\.([a-zA-2			
💼 Extracted Content	∧ List Name				
Keyword Hits Single Literal Keyword Search (0)	9 http://mrr.ucsd.edu/burghes/subposet.htm (2)				
⊕ Single Regular Expression Search (0)	http://cmrr.ucsd.edu/hughes/subpgset.htm. (2)				
□ URLs (184)	A http://csrc.nist.gov/fasp (2)				
$\Box \stackrel{\scriptstyle \frown}{\longrightarrow} \underbrace{(((((h H)(t T))(t F))(t T)(p P)(s S?)), V(V)(w W)}_{(w W)}$	A http://csrc.nist.gov/fasp/. (2)				
http://cmrr.ucsd.edu/hughes/subpgset.htm (A http://hissa.nist.gov/~Black (2)				
http://cmrr.ucsd.edu/nugnes/suppgset.ntm.	A http://standards.gov (2)				
http://csrc.nist.gov/fasp(2)	http:// http://standards.gov (2))	2			
http://hissa.nist.gov/~Black (2)	http://webopedia.internet.com (2)				
http://standards.gov (2)	http://wtopline.com/vol13_po18 (2)				
http://ugsolutions.com/products (2)		-			
http://webopedia.internet.com (2)	Ttp://www.PDMLC.com (2)				
http://wtonline.com/vol13_no18 (2)	http://www.americanbanker.com (2)	2			
http://www.PDMIC.com (2)	http://www.americanbanker.com/PSUser/ABO_Display.htm?type				
http://www.americanbanker.com (2)	http://www.anu.edu.au/pepple (2)	2			
http://www.americanbanker.com/PSUser/ABC	A http://www.bentley.com/bentley (2)	2			
http://www.anu.edu.au/pepple (2)	http://www.bentley.com/bentley/backgrod.htm (2)	2			
http://www.bentley.com/bentley (2)	G http://www.blc.gov/oco/home.htm (2)	2			
http://www.bentley.com/bentley/backgrnd.h		2			
http://www.bis.gov/oco/nome.ntm (2)	Hey Chiese Cie Materiate Dearlie Message Tedaurd Text Me	dia Other			
http://www.caukey.com/products (2)	Tick Strings File Metadata Results Message Indexed Text Me				
http://www.census.gov/prod/ec97/97m3361					
http://www.census.gov/prod/ec97/97m3361					
http://www.census.gov/prod/ec97/97m3361					
Q http://www.census.gov/prod/ec97/97m3362; ✓					
< >>	L				

- Next lets take a look at URL's.
- \circ $\;$ Click on where it says URL's and expand the directories.
- There is 184 results that pop up. Take a few minutes and look through them and see what you can find.
- You may notice that many of the file names that the URL's are found in match.
- This is because many of the files are reports, and have references listed somewhere in the file.
- This goes to show that though Autopsy does a thorough search through the files, but it makes it appear as if there is more data than their actually is.
- o Although there is 184 URL's listed, there is not that many files in our system.

Add Data Source Images/Medes <	Case View Tools Window Hel	p							
Image: Street (S) Stree (S) Street (S) Street	🕂 Add Data Source 📠 Imag	jes/Videos 🧮 Timeline 📗 Ger	nerate Report 💊 Close Case 🗧				<u> </u>	 Keyword Lists 	Q- Keyword Search
Image: Source set Control (2) Price metal Price metal <td< th=""><th>4 ></th><th>Chow Pajarted Parults</th><th>Listing</th><th></th><th></th><th></th><th></th><th></th><th></th></td<>	4 >	Chow Pajarted Parults	Listing						
Image: Second			By File						7 Result
Pie Accounts State Pie State 0 Pie State	Data Sources		Table Thumbnail						
Image: Solution factory of the fact	CrobaoElec (0)		File	Accounts	Status				
Particle (1) Compressed (7) Compressed (7	Sevend (5)		💾 \$UpCase	3	Undecided				
 Compressed (7) Broughed (7) System Volume Information (2) Very System Volume Information (2) Very System Volume Information (2) System Volume Information (2) Very System Volume I	SUnalloc (1)		SMFT	1	Undecided				
Complete (7) C	Compressed (7)		20076517123273.pdf	1	Undecided				
Reports Report Reports Reports Reports Reports Reports Re	Encrypted (7)		20076517123273.pdf	1	Undecided				
Image: System Volume Information (2) Image: System Volume Information (2) Image: Verse Image: System Volume Information (2) Ima	📜 RAW (7)		20076517123273.pdf-slack	1	Undecided				
Weres 0000051722273.pdf*dack 1 Undexided Image: Strated Content 0000051722273.pdf*dack 1 Undexided Image: Strateging Items 0000051722273.pdf*dack 1 Undexided Image: Strateging Items 0000051722273.pdf*dack 1 1 Image: Strateging Items 0000051722273.pdf*dack 1 1 Image: Strateging Items 0000051722273.pdf*dack 1 1 Image: Strateging Items 000005172273.pdf*dack 1 1 Image: Strateging Items 0000005172273.pdf*dack 1 1 Image: Strateging Items 000000000000000000000000000000000000	System Volume Info	rmation (2)	20076517123273 odf	1	Underided				
Contract of Content C	Views			1	Undecided				
Keyword Hits Keyword K	Results		20076517123273.pdt-slack	1	Undecided				
Image: Second	Extracted Content		Max and last and the last	Inc. In 1	1				
	Hashset Hits		nex Strings Hie Metadata Result			Other Occurrences			
→ threesing Items → → →	E-Mail Messages								
Image: Accounts	- 🔆 Interesting Items								
	- 🗊 Accounts								
Image: Strate Of Point (S) Im	E- 🔂 Credit Card								
	By File (7)								
	□ By BIN (4)								
Bit Tags Bit Tags Reports Reports		b) 1)							
		1)							
Caps A Reports	- 30313233 (1)							
Reports	- S Tags								
	Reports								

- o In the file directory to the left-hand side of the screen there is a tab labeled "Accounts".
- Expand the directory underneath it to reveal something titled "Credit Card", then expand it. You can then view the information by card, or BIN (Banking Identification Number)

0	This allows us to	view credit	card numbers	and bins.
<u> </u>				

😹 GenCyber Exam 1 - Autopsy 4.6.0					- 0	×			
Case View Tools Window Help									
🕂 Add Data Source 📠 Images/Videos 🗮 Timeline 📗 Gen	erate Report 🛛 💰 Close Case 🗧		1	Keyword Lists	Q- Keyword Search				
Show Rejected Results	Listing				<				
E-B Data Sources	/mg_ntfs1-gen2.E01 23 Results Table Thumbnal								
intfs1-gen2.E01	△ Name	Location	Modified Time	Change Time	Access Time	8			
Surphan-lies (U)	\$AttrDef		2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST	^			
SUnaloc (1)	\$BadClus		2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST				
📜 Compressed (7)	\$BadClus:\$Bad		2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST				
Encrypted (7)	\$Bitmap		2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST				
	\$Boot		2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST				
System volume information (2)	\$Extend		2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST				
E Results	\$LogFile		2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST	~			
Everated Content Everated Content	Hex Strings File Metadata Read	Its Message Indexed Text Media Other (Occurrences						

- If you want to view every file available in the system click on "nfts-gen2.E01" in the top left of the directory. This shows every file available for examination
- Take some time and see what else you can find.
- Conclusion
 - We learned how to open Autopsy, create a new case, and load in an evidence file. We also examined some introductory data that Autopsy was able to find.
 - Autopsy has many different tools for data analyzation. If you would like to learn more there are several tutorials on the internet. There are also free evidence files for analyzation that can be found online.

• We will continue our analysis in the next module.