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\E	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	rmation	
. Case Information 2. Optional Information	Case Number:	1	1
	Examiner		
	Name:	Jackson]
	Phone:		
	Email:		
	Notes:	This is the first exam using Autopsy.	
	Organization	1	
	Organizati	on analysis is being done for: Manage Organizations	
		< Back Next > Finish Cancel Heip)

• 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 Add	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.

Select Type of Data Source To	Configure Ingest Modules		
Select Type of Data Source To Add	Run ingest modules on:		
Select Data Source Configure Ingest Modules	All Files, Directories, and Unallocated Space	~	Select keyword lists to enable during ingest:
Add Data Source	Recent Activity Hash Lookup File Type Identification Embedded File Extractor Exif Parser	^	Phone Numbers IP Addresses Gmail 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	v	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"

Add Data Source <u>III</u> Images/Video	os 🧮 Timeline 📗 Generate	Report 🛛 😠 Clos	e Case						🔺 🛙 🧕	 Keyword Lists 	Q- Keywor	d Search
>	Show Rejected Results	Listing										
2	Show Rejected Results	Data Sources										1 Result
Data Sources		Table Thumbna	al									
Views		Name		Type	⊽ Size (By	Sector Size	a (Buter)	MD5 Hash		Timezone	Device ID	
E Results												
Extracted Content		ntfs1-gen2.	E01	Image	516554752	512		27a9053e35aac	74608493e755353cb95	America/New_York	69545f3f-c3a0-	40dd-8545-46
Keyword Hits			ntfs1-gen2.	101								
🗑 🔍 Single Literal Keyword Search	h (0)		ntrs i+gen2.	201								
Single Regular Expression Se	earch (0)											
Hashset Hits												
E-Mail Messages												
- X Interesting Items												
Accounts		<										>
Tags		`										
		Hex Strings Fi	ie Metadata R	Results Mess	ige Indexed T	ext Media	Other Oc	currences				
Reports			le Metadata F of 31528	tesults Mess Page		ext Media	Other Oc	currences Jump to C	Offset 0			
							Other Oc		Offset 0			
		Page: 1	of 31528 EB 52 90 4	Page E 54 46 5	← → Go 3 20 20 2	to Page:	02 01 0	Jump to C	NTFS			^
		Page: 1 0x00000000: 0x00000010:	of 31528 EB 52 90 4 00 00 00 0	Page E 54 46 5 0 00 F9 0	Go 3 20 20 2 0 00 3F 0	to Page:	02 01 0	Jump to 0	NTFS			^
		Page: 1 0x00000000: 0x00000010: 0x00000020:	of 31528 EB 52 90 4 00 00 00 0 00 00 00 0	Page E 54 46 5 0 00 F8 0 0 80 00 0	Go 3 20 20 2 0 00 3F 0 0 00 FF 0	to Page: 0 20 00 0 FF 00 14 0F 00	02 01 0 00 00 0 00 00 0	Jump to 0	NTFS 			^
		Page: 1 0x00000000: 0x00000010: 0x00000020: 0x00000030:	of 31528 EB 52 90 4 00 00 00 0 00 00 00 0 AA 21 05 0	Page E 54 46 5 0 00 29 0 0 80 00 0 0 00 00 0	Go 3 20 20 2 0 00 3F 0 0 00 FF 0 0 00 7F 1	to Page: 0 20 00 0 FF 00 34 0F 00 12 07 00	02 01 0 00 00 0 00 00 0 00 00 0	Jump to 0	NTFS			^
		Page: 1 0x00000000: 0x00000000000000 0x00000000	of 31528 EE 52 90 4 00 00 00 0 00 00 00 0 AA 21 05 0 02 00 00 0	Page E 54 46 5 0 00 29 0 0 80 00 0 0 00 00 0 0 08 00 0	Go 3 20 20 2 0 00 3F 0 0 00 FF 0 0 00 7F 1 0 00 C7 0	to Page: 0 20 00 0 FF 00 4 0F 00 12 07 00 12 07 00 12 48 50	02 01 0 00 00 0 00 00 0 00 00 0 E8 48 5	Jump to C 00 00 .R. 00 00 00 00 00 00 50 DA	NTFS d 			^
		Page: 1 0x00000000: 0x00000010: 0x00000020: 0x00000030:	of 31528 EB 52 90 4 00 00 00 0 00 00 00 0 AA 21 05 0 02 00 00 0 00 00 00 0	Page E 54 46 5 0 00 28 0 0 80 00 0 0 00 00 0 0 08 00 0 0 28 33 0	Go 3 20 20 2 0 00 3F 0 0 00 FF 0 0 00 7F 1 0 00 C7 0 0 8E D0 5	to Page: 0 20 00 0 FF 00 4 0F 00 12 07 00 12 07 00 12 48 50	02 01 0 00 00 0 00 00 0 00 00 0	Jump to C 00 00 .R. 00 00 00 00 00 00 00 00 50 DA 50 07	NTFS			^
		Page: 1 0x000000000: 0x00000020: 0x00000020: 0x00000030: 0x00000040: 0x00000050:	of 31528 EB 52 90 4 00 00 00 0 AA 21 05 0 02 00 00 0 00 00 00 0 8E D0 E0 1	Page E 54 46 5 0 00 79 0 0 80 00 0 0 00 00 0 0 08 00 0 0 7A 33 0 6 00 89 0	Go 3 20 20 2 0 00 3F 0 0 00 7F 0 0 00 77 5 0 00 77 5 0 00 77 5 0 00 8E D0 5 0 00 8E D0 5 0 00 8E D0 5	to Page: 0 20 00 0 FF 00 4 0F 00 12 07 00 12 0 12 07 00 12 000	02 01 0 00 00 0 00 00 0 E8 48 5 FB 88 0	Jump to C 00 00 .R. 00 00 00 00 00 00 00 00 00 DA 00 07	NTFS d			^
		Page: 1 0x000000000 0x000000000 0x000000000 0x000000	of 31528 EB 52 90 4 00 00 00 0 00 00 00 0 AA 21 05 0 02 00 00 0 00 00 00 0 6E DE EE 1 10 EE 53 0	Page E 54 46 5 0 00 F8 00 0 00 00 00 0 00 00 00 0 7A 33 C 6 00 B9 0 0 68 00 0	Go 3 20 20 2 0 00 3F 0 0 00 7F 8 0 00 7F 8 0 00 77 8 0 00 70 8 0 00 8	to Page: 0 20 00 0 FF 00 4 0F 00 12 07 00 12 0 12 07 00 12 000	02 01 0 00 00 0 00 00 0 29 49 5 FB 88 0 C6 06 0	Jump to 0 00 00 .R. 00 00 00 00 00 00 50 DA 00 07 00 07 00 00 00 04 00 00	NTFS 			^
		Page: 1 0x000000000 0x00000000 0x00000000 0x000000	of 31528 EB 52 90 4 00 00 00 0 00 00 00 0 AA 21 05 0 00 00 00 0 00 00 00 0 00 00 00 0 00 ED EC 1 10 ES 53 0 00 CD 13 7 0F B6 D1 8	Page E 54 46 5 0 00 F8 0 0 00 00 0 0 00 00 0 0 FA 33 C 6 00 B9 0 0 E2 3F F	Go 3 20 20 2 0 00 3F 0 0 00 FF 6 0 00 7F 8 0 00 7F 6 0 00 7F 6 0 00 8E D0 8 0 00 8E 00 8 0 00 8E 00 8 0 00 8 0 00 8 0 00 8 0 00 8 0 00 8 0 0 0 8 0 0 0 8 0	to Page: 0 20 00 0 FF 00 14 0F 00 12 07 00 12 000	02 01 0 00 00 0 00 00 0 E8 48 5 FB 88 0 C6 06 0 16 24 0 B6 C6 4 06 41 6	Jump to C 00 00 .R. 00 00 00 00	NTFS			^
		Page: 1 0x000000010: 0x00000020: 0x00000040: 0x00000040: 0x00000050: 0x00000060: 0x00000070: 0x00000090: 0x00000090: 0x00000090:	of 31528 EB 52 50 4 00 00 00 0 00 00 00 0 AA 21 05 0 00 00 00 0 AB 21 05 0 00 00 00 0 00 00 00 0 E D0 E0 1 10 E8 53 0 00 CD 13 7 00 F B6 D1 3 B7 C9 66 F	Page E 54 46 5 0 00 F8 0 0 00 00 0 0 00 00 0 0 FA 33 0 6 00 B9 0 0 68 00 0 3 05 B9 F 7 E1 6 A	Go Go 3 20 20 20 0 00 3F 0 0 00 FF 0 0 00 C7 0 0 00 C8 6A 0 C6 6A 0 C 0 0 0 20 0 0	to Page: 0 20 00 0 FF 00 14 0F 00 12 07 00 12 07 00 12 07 00 12 08 8A 1 66 0F 1 66 0F 10 C0 ED 13 B4 41	02 01 0 00 00 0 00 00 0 E9 49 9 FB B8 0 C6 06 0 B6 C6 4 06 41 6 BB AA 5	Jump to C 00 00 .R. 00 00 00 00 00 00 00 00 00 DA 00 DA 00 DA 00 B4 00 B4 00 B4 00 B4	MTTS d HP.HP. .3l. .h.hj sfdef .f			Â
		Page: 1 0x00000000: 0x00000000: 0x000000000: 0x00000000: 0x000000000: 0x00000000: 0x00000000: 0x00000000: 0x00000000: 0x00000000: 0x00000000: 0x000000000: 0x00000000: 0x00000000: 0x00000000: 0x00000000: 0x00000000: 0x00000000: 0x000000000: 0x000000000:	of 31528 EB 52 90 4 00 00 00 0 00 E D8 E0 1 00 ED 13 7 07 B6 D1 8 P1 62 40 0 C	Page E 54 46 5 0 00 F8 0 0 00 00 0 0 00 00 0 0 08 00 0 0 FA 33 0 0 FA 33 0 0 68 00 0 3 05 B9 F 0 E2 3F F 7 E1 66 A D 13 72 0	Go 3 20 20 2 0 00 3F 0 0 00 FF 6 0 00 C7 0 0 00 C7 0 0 00 C7 0 0 00 00 FF 6 0 00 C7 0 0 00 00 FF 6 0 00 C7 0 0 00 00 FF 6 0 00 C7 0 0 00 FF 6 0 00 0 0 00 0 0 00 FF 6 0 00 0 0 00 FF 7 0 00 0 0 0 0 0 0 0 0 0 0 0 0 0	to Page: 0 20 00 0 FF 00 14 0F 00 12 07 00 12 07 00 12 08 50 12 08 8A 1 66 0F 13 84 41 15 AA 75	02 01 0 00 00 0 00 00 0 59 48 9 58 88 0 C6 06 0 16 24 0 86 C6 4 06 41 4 88 AA 8 09 F6 0	Jump to C 00 00 .R. 00 00 00 00 00 00 00 00 00 DA 00 B4 00 B4	NTFS			^
		Page: 1 0x00000000 0x00000000 0x000000000 0x00000000 0x000000000 0x00000000 0x000000000 0x00000000 0x000000000 0x00000000 0x000000000 0x00000000 0x000000000 0x000000000 0x000000000 0x000000000 0x000000000 0x000000000 0x0000000000 0x0000000000	of 31528 EB 52 50 4 00 00 00 0 00 00 00 0 AA 21 05 0 02 00 00 0 00 00 00 0 8E D0 E0 1 10 E8 53 0 00 CD 13 8 0 CD 13 8 B7 C9 66 F 16 24 00 C	Page E 54 46 5 0 00 F8 0 0 00 00 0 0 00 00 0 0 FA 33 C 6 00 B9 0 0 68 00 0 6 00 B9 F 0 E2 3F F 7 E1 66 A D 13 72 0 1 40 0	Go 3 20 20 20 0 00 3F 0 0 00 7F 1 0 00 7F 1 0 00 7F 1 0 00 7F 1 0 00 8E 00 8E 0 00 8E 0 1 0 8E 0 1 8 66 0 1 5 6 0 1 5 7 5 1 5 8 6 0 1 5 8 6	to Page: 0 20 00 0 FF 00 4 0F 00 12 07 00 13 DB 14 41 15 8 A 75 E 0 6 60 15 8 A 15 8	02 01 0 00 00 0 00 00 0 E8 48 5 FB 88 0 C6 06 0 16 24 0 B6 C6 4 06 41 4 B8 A 5 09 F6 0 A1 10 0	Jump to 0 00 00 .R. 00 00 00 00	NTFS			^
		Page: 1 0x00000000: 0x00000000: 0x000000000: 0x00000000: 0x000000000: 0x00000000: 0x00000000: 0x00000000: 0x00000000: 0x00000000: 0x00000000: 0x000000000: 0x00000000: 0x00000000: 0x00000000: 0x00000000: 0x00000000: 0x00000000: 0x000000000: 0x000000000:	of 31528 EB 52 90 40 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 02 00 00 00 00 01 02 02 00 00 02 00 00 00 00 01 02 53 0 00 09 CD 13 7 0F Be D1 8 97 C9 E0 13 7 07 Be D1 8 16 2.4 00 C 74 04 FE 0 0 0 10 10 3 06 12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 <td< td=""><td>Page 54 46 5 0 00 F8 0 0 00 00 0 0 00 00 0 0 00 00 0 0 00 00 0 0 7A 33 C 6 00 B8 0 0 68 00 0 3 05 B9 F 7 E1 66 A D 13 72 0 0 13 72 0 0 66 3B 0 0 66 3B 0 0 66 3B 0 0 50 5B 1 1 4 00 5 0 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5</td><td>Go 3 20 20 2 0 00 3F 0 0 00 7F 0 0 00 7F 0 0 8E D0 5 0 00 8E C0 5 0 8E D0 5 0 00 8E C0 5 0 8E D0 5 0 00 8E C0 5 0 00 8E C0 5 0 00 8E C0 5 0 00 8E C0 5 0</td><td>to Page: 0 20 00 0 FF 00 4 0F 00 12 07 00 13 DB 14 41 15 8 A 75 E 0 6 60 15 8 A 15 8</td><td>02 01 0 00 00 0 00 00 0 59 48 9 58 88 0 C6 06 0 16 24 0 86 C6 4 06 41 4 88 AA 8 09 F6 0</td><td>Jump to C 00 00 .R. 00 00 .R. 00 00 00 00 .1. 00 00 .1. 00 00 00 84 00 84</td><td>NTFS</td><td></td><td></td><td>~</td></td<>	Page 54 46 5 0 00 F8 0 0 00 00 0 0 00 00 0 0 00 00 0 0 00 00 0 0 7A 33 C 6 00 B8 0 0 68 00 0 3 05 B9 F 7 E1 66 A D 13 72 0 0 13 72 0 0 66 3B 0 0 66 3B 0 0 66 3B 0 0 50 5B 1 1 4 00 5 0 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	Go 3 20 20 2 0 00 3F 0 0 00 7F 0 0 00 7F 0 0 8E D0 5 0 00 8E C0 5 0 8E D0 5 0 00 8E C0 5 0 8E D0 5 0 00 8E C0 5 0 00 8E C0 5 0 00 8E C0 5 0 00 8E C0 5 0	to Page: 0 20 00 0 FF 00 4 0F 00 12 07 00 13 DB 14 41 15 8 A 75 E 0 6 60 15 8 A 15 8	02 01 0 00 00 0 00 00 0 59 48 9 58 88 0 C6 06 0 16 24 0 86 C6 4 06 41 4 88 AA 8 09 F6 0	Jump to C 00 00 .R. 00 00 .R. 00 00 00 00 .1. 00 00 .1. 00 00 00 84 00 84	NTFS			~
		Page: 1 0x00000000000000000000000000000000000	of 31528 EB 52 90 4 00 00 00 0 0 00 00 00 0 0 0 02 00 00 00 0 0 0 02 00 00 00 00 0 <td>Page E 54 46 5 34 0 00 F8 0</td> <td>Go 3 20 20 20 3 20 20 3F 0 0 00 7F 1 0 0 0 0 7F 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td> <td>to Page: 0 20 00 0 20 00 0 0 7 00 12 07 00 12 12 07 00 12 07 12 07 00 7C 00 12 07 00 33 DB 12 CB 8A 1 60 07 12 CB 10 33 DB 1</td> <td>02 01 0 00 00 0 00 00 0 59 48 5 FB 88 0 C6 06 0 16 24 6 88 AA 5 09 F6 4 Al 10 0 00 12 6</td> <td>Jump to C 00 00 .R. 00 00 .R. 00 00 .R. 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 84 00 84 00 84 00 66 t 00 66 t 00 66 t 00 00 </td> <td>NTTS</td> <td></td> <td></td> <td>^</td>	Page E 54 46 5 34 0 00 F8 0	Go 3 20 20 20 3 20 20 3F 0 0 00 7F 1 0 0 0 0 7F 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	to Page: 0 20 00 0 20 00 0 0 7 00 12 07 00 12 12 07 00 12 07 12 07 00 7C 00 12 07 00 33 DB 12 CB 8A 1 60 07 12 CB 10 33 DB 1	02 01 0 00 00 0 00 00 0 59 48 5 FB 88 0 C6 06 0 16 24 6 88 AA 5 09 F6 4 Al 10 0 00 12 6	Jump to C 00 00 .R. 00 00 .R. 00 00 .R. 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 84 00 84 00 84 00 66 t 00 66 t 00 66 t 00 00	NTTS			^
		Page: 1 0x00000000000000000000000000000000000	of 31528 EB 52 90 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 02 00 00 00 00 01 02 02 01 10 02 00 00 00 00 00 01 02 02 00 00 00 02 00 00 00 00 00 03 06 12 00 00 00 06 50 00 04 FE 50 00 00 50 00 00 50 00	Page E 54 46 5 0 00 78 0 0 00 78 0 0 00 00 00 0 0 00 00 00 0 0 00 80 0 0 0 60 180 0 0 0 68 00 0 23 5 7 21 66 30 0 0 0 64 10 0 0 0 0 64 38 0 0 0 0 64 38 0	Go Go 3 20 20 2 0 00 3F 0 0 00 3F 0 0 00 3F 0 0 00 3F 0 0 00 7F 1 0 00 7F 0 0 00 7F 0 0 00 7F 0 0 00 7F 0 0 00 00 0 00 00 0 00 00 0 00 00 7 52 86 6 20 00 1 6 20 00 9 10 00 1 6 20 00	to Page: 0 20 00 0 20 00 0 0 7 00 12 07 00 12 12 07 00 12 07 12 07 00 7C 00 12 07 00 33 DB 12 CB 8A 1 60 07 12 CB 10 33 DB 1	02 01 0 00 00 0 00 00 0 28 48 5 78 88 0 16 24 0 86 66 4 06 41 8 09 F6 0 A1 10 0 00 12 4	Jump to C 00 00 .R. 00 .	NTFS			^
		Page: 1 0x00000000000000000000000000000000000	of 31528 EB 52 90 4 00 00 00 00 00 00 00 00 AA 21 05 0 00 00 00 00 00 85 00 00 75 65 D1 6 00 75 65 00 00 75 65 00 00 65 50	Page E 54 46 50 0 0 70 00 10 0 0 0 00 00 00 0 0 0 0 00 00 00 0	Go Go 3 20 20 20 0 00 3 FC 000 3 FC 0 00 0 FF 000 7 FF 0 00 0 FF 000 7 FF 0 00 0 FF 000 7 FF 0 00 0 FF 00.10 8 EC 0 00 0 FF 0.00 000 0 66 3 20 000 000 3 66 600 000 8 E 0 10 000 000 8 E 6 10 000 000 8 E 0 10 000 000 9 E 6 10 000 000 1000 000 6 10 000 000 1000 000 1000 000 6 10 000 000 1000 000 1000 000 1000 000 0 10 000 000 000 000 000 1000 0000 1000 000 100	to Page: 0 20 00 0 FF 00 14 0 F 00 12 07 00 12 00 7 12 00 7 12 00 13 B4 41 15 0 15 06 66 15 06 60 15 06 0 15 06 0 15 06 15 06 0 15 00 15 00	02 01 0 00 00 0 00 00 0 E 48 8 FB B8 0 C 6 0 0 16 24 0 B8 C 6 4 06 41 4 06 41 4 05 F6 0 A1 10 0 00 12 8 A 1 00 00 5 6 6 A1 10 0 00 5 6 8 B8 A 8 00 5 6 6 A1 10 0 B8 A 8 00 5 6 6 A1 10 0 B8 A 8 05 7 6 8 B8 A 8 05 7 6 8 05 7 6 8 05 7 7 7 7 05 7	Jump to C 00 00 .R. 00 00 00 00 00 00 00 00 00 00 00 00 00 84 00 95 00 95	NTIS			^

- 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:

🕂 Add Data Source 📠 Images/Videos 🗮 Timeline 📗 Ger	erate Report 🛛 🔞 Close C	ase			<u>A</u> EB	Keyword List	ts Q- Keyword Search
← → Show Rejected Results	Listing Data Sources						() ▼ 1 1 Resi
Data Sources	Table Thumbnail						1 Kesu
• Views	Name	Type	⊽ Size (By	Sector Size (Bytes)	MD5 Hash	Timezone	Device ID
E Results	ntfs1-gen2.E01	Image	516554752		27a9053e35aac74608493e755353cb95	America/New York	80ec2016-747e-4dd0-9aa5-eac40
⊕-Q. Photesses(2) ⊕-Q. Photesharbst (2) ⊕-Q. Photesharbst (2) ⊕-Q. Photesharbst (2) ⊕-Q. Photesharbst (3) ⊕-Q. Photesharbs	C Bings File Metad	ata Results Me	ssage Indexed 1	Fext 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.

ase View Tools Window Help			
🐈 Add Data Source 📠 Images/Videos 🗮 Timeline 📗 Genera	ate Report 🛛 🍙 Close Case 💲	;	
← ⇒ Show Rejected Results	Listing (\{?)[a-zA-Z0-9%+_\-]+(\.	[a-zA-Z0-9%+_\-]+)*(\}?)	\@([a-z/
💷 🚍 Data Sources	Table Thumbnail		
🖻 🔤 ntfs1-gen2.E01	△ List Name	Files with Hits	
\$OrphanFiles (0)	Q bullock@rti.org (2)	2	
····· J \$Extend (5)	xL6@3ov.KE (1)	1	
		-	
Encrypted (7)			
D D D D D D D D D D			
RAW (7)			
RAW (7) System Volume Information (2) Views			
RAW (7) System Volume Information (2) Views Results	Hex Strings File Metada	ata Results Message II	ndexed ⁻
RAW (7) System Volume Information (2) Views Results Extracted Content Keyword Hits Single Literal Keyword Search (0)	Hex Strings File Metada	ata Results Message I	ndexed 1
RAW (7) System Volume Information (2) Views Results Extracted Content Keyword Hits Single Literal Keyword Search (0) Single Regular Expression Search (0)	Hex Strings File Metada	ata Results Message I	ndexed ⁻
RAW (7) System Volume Information (2) Views Results Extracted Content Keyword Hits Single Literal Keyword Search (0) Gamma Single Regular Expression Search (0) Gamma Addresses (3)		ata Results Message I	ndexed ⁻
RAW (7) System Volume Information (2) System Volume Information (2) Extracted Content Extracted Content Keyword Hits Single Literal Keyword Search (0) Gamma Single Regular Expression Search (0) Gamma Maddresses (3) Gamma Addresses (3) Gamma Addresses (3)		ata Results Message I	ndexed `
RAW (7) System Volume Information (2) System Volume Information (2) Extracted Content Extracted Content Extracted Content Single Literal Keyword Search (0) Extracted Content Single Regular Expression Search (0) Extracted Content C		ata Results Message I	ndexed 1
RAW (7) System Volume Information (2) System Volume Information (2) Extracted Content Extracted Content Single Extracted Content Single Literal Keyword Search (0) Single Regular Expression Search (0) Email Addresses (3) C(\{?)[a-zA-Z0-9%+_\-]+([a-zA-Z0-9%+_\-]+)*(\\??)\(3) Hashset Hits SINGLE F-Mail Messages		ata Results Message I	ndexed '
RAW (7) System Volume Information (2) System Volume Information (2) Extracted Content Extracted Content Extracted Content Single Literal Keyword Search (0) Email Addresses (3) Extracted Addresses (3) Extracted Content (\{\?\})(a-zA-Z0-9%+_\-]+)*(\\?\)(a-zA-Z0-9%+_\-]+)*(\\?\)(b-zA-Z0-9%+_\-]+)*(\\?\)(b-zA-Z0-9%+_\-]+)*(\\?\)(b-zA-Z0-9%+_\-]+)*(\\?\)(b-zA-Z0-9%+_\-]+)*(\\?\)(b-zA-Z0-9%+_\-]+)*(\\?)(c-zA-Z0-9%+_\-]+)*(\\?)(c-zA-Z0-9%+_\-]+)*(\\?)(c-zA-Z0-9%+_\-]+)*(\\?)(c-zA-Z0-9%+_\-]+)*(\\?)(c-zA-Z0-9%+_\-]+)*(\\?)(c-zA-Z0-9%+_\-]+)*(\\?)(c-zA-Z0-9%+_\-]+)*(\\?)(c-zA-Z0-9%+_\-]+)*(\\?)(c-zA-Z0-9%+_\-]+)*(\\?)(c-zA-Z0-9%+_\-]+)*(\\?)(c-zA-Z0-9%+_\-]+)*(\\?)(c-zA-Z0-9%+_\-]+)*((\\?)(c-zA-Z0-9%+_\-]+)*(\\?)(c-zA-Z0-9%+_\-]+)*((\\?)(c-zA-Z0		ata Results Message I	ndexed 1
RAW (7) System Volume Information (2) Keyword Hits Sigle Literal Keyword Search (0) Single Regular Expression Search (0) S		ata Results Message I	ndexed 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.

ullock@rti.org					2 Re
Table Thumbnail	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 18:0
💠 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 18:0
u Shines Ele Materi	late Davida Morray	Indexed Taxt Media Other Occurrences			
x Strings File Metad	lata Results Message	e Indexed Text Media Other Occurrences			
		e Indexed Text Media Other Occurrences → Page: 15 of 19 Page ←→	Text So	urce: Search Re	esults ·
atches on page: 1			Text So	urce: Search Re	esults ·
atches on page: 1			Text So	urce: Search Re	esults ·
atches on page: 1			Text So	urce: Search Re	esults ·
atches on page: 1			Text So	urce: Search Re	esults 🔹
atches on page: 1			Text So	urce: Search Re	esults
atches on page: 1 Mar response to stion 4.1) cld with proved Testing			Text So	urce: Search Re	esults ·
atches on page: 1 mir response to stion 4.1) cld with proved Testing			Text So	urce: Search Re	esults •
atches on page: 1 Auf response to estion 4.1) and with proved Testing pls	of 1 Match		Text So	urce: Search Re	esults
atches on page: 1 nur response to stion 4.1) ild with roved Testing ols uurements gatherin	of 1 Match E	→ Page: 15 of 19 Page	Text So	urce: Search Re	esults ·
	of 1 Match	→ Page: 15 of 19 Page	Text So	urce: Search Re	esults v

- 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 Freezewic Tempeter of Tendemocke Tedenophyskume for Seference Teaking		~

- 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 String	File Metadata	Results Message Indexed Text Media Other Occurr
Name		/img_ntfs1-gen2.E01/Encrypted/logfile1.txt
Туре		File System
MIME Ty	/pe	text/plain
Size		21888890
File Nan	ne Allocation	Allocated
Metadat	a Allocation	Allocated
Modified	1	2009-01-05 17:01:26 EST
Accesse	d	2009-01-05 17:01:26 EST
Created		2009-01-05 17:00:20 EST
Change	d	2009-01-05 17:01:26 EST
MD5		cb45c6ad5abb2ff240217aead1e85f13
Hash Lo	okup 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					$\leftrightarrow =$			
-		ta Sources	(919) 485-5599 2 Results Table Thumbnail								
		ntfs1-gen2.E01	Source File	Keyword	Keyword Regular Expression	Keyword Preview		Modified Time			
	- T	\$OrphanFiles (0)									
		SExtend (5)	👘 report02-3.pdf	(919) 485-5599	[\.\-\?\;\\!\!\:\[\]\/\(\)\"\">\{\}](\([0-9]{3}\) [0-9]{3}	Michelle Bullock at «(919) 485-5599	9«or bullock@rti.org.	2008-12-31 18:0			
		SUnalloc (1)	🕂 report02-3.pdf	(919) 485-5599	$[\ . -!? , : !!: [!] /!(!)!"" > {!}](!([0-9]{3}!))[[0-9]{3}$	Michelle Bullock at «(919) 485-5599	9«or bullock@rti.org.	2008-12-31 18:0			
		Compressed (7)									
		Encrypted (7)	<					>			
		B RAW (7)	Hay Shines Ele Matadata	Deadle Massage	Indexed Text Madia Other Occurrences						
	L	System Volume Information (2)	Hex Strings File Metadata Results Message Indexed Text Media Other Occurrences								
b -F	Vie Vie	ws	Matches on page: 1 of	2 Match 6	Page: 15 of 19 Page ← →	Tevt	Source: Search Results	· · ·			
b-i	E Res	sults	Hatches on pages 1 of	2 Poton	Flager 15 of 15 Hage	icae 3	Jource: Jourch resource				
11.1		Extracted Content	(\$19) 485-5559 or bullock@rti.org.								
	<u>_</u>	Keyword Hits									
	÷	Single Literal Keyword Search (0)									
		Single Regular Expression Search (0)	Thank you in advance for your participation.								
		Q URLs (184)									
		IP Addresses (2)									
	_	Phone Numbers (2)									
		(919) 485-5599 (2)	The Economic Impacts of I	nadequate Infra	structure for Software Testing						
		Email Addresses (3)	C-4								
		Hashset Hits									
	👱	E-Mail Messages	1. Background Information								
	*	Interesting Items	1.1 Flease type your name, company name, and e-mail address on the lines below.								
	ė-🗊	Accounts	1.1 Flease type your nam	e, company name	, and e-mail address on the lines below.						
	÷	📑 Credit Card	Name :								
0-1	💿 Tag	js									
			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.

Show Re	ected Results	0-9\-\.]+\.([a-zA
Extracted Content	Table Thumbnail List Name	Files w
Keyword Hits Green Content of the search (0) Green Content of the search (0) Green Content of the search (0)	A http://cmrr.ucsd.edu/hughes/subpgset.htm (2)	2
	http://cmrr.ucsd.edu/hughes/subpaset.htm. (2)	2
- Q URLs (184)	http://csrc.nist.gov/fasp (2)	2
<pre>bits (10+) ((1))((1))((1)(0)(2)(32)(*V)((w)(w))</pre>		2
	poset htm (
	pgset.htmhttp://hissa.nist.gov/~Black (2)	2
	http://standards.gov (2)	2
	http:// http://standards.gov (2)	2
	http://webopedia.internet.com (2)	2
	http://wtonline.com/vol13 no18 (2)	2
	(2)	2
http://webopedia.internet.com (
http://wtonline.com/vol13_no18		2
http://www.PDMIC.com (2)	http://www.americanbanker.com/PSUser/ABO_Display.htm	m?type= 2
http://www.americanbanker.com	<pre>circlp.//www.anu.euu.au/peppie (z)</pre>	2
http://www.americanbanker.com/PSUser/ABC	http://www.bentley.com/bentley (2)	2
http://www.anu.edu.au/pepple	C Lite II was been been been been been been been (5)	2
http://www.bentley.com/bentley (2) http://www.bentley.com/bentley/backgrnd.h	(2)	2
		2
http://www.bls.gov/oco/home.h		aut Mada Of
http://www.cata.ibm.com/catv5		ext Meula Ot
http://www.census.gov/prod/ec97/97m3361		
http://www.census.gov/prod/ec		
http://www.census.gov/prod/ec		
http://www.census.gov/prod/ec		

- 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.

se View Tools Window	/ Help						
🗕 Add Data Source 📠	Images/Videos 🧮 Timeline 📗 Ger	nerate Report 👩 Close Case 🗧				🛕 💿 🕶 Keyword Lists	Q- Keyword Search
. >	Show Rejected Results	Listing					$\leftrightarrow \mathbf{v}$
		By File					7 Res
Data Sources		Table Thumbnail					
 mtfs1-gen2.E01 \$OrphanFiles 	(2)	File	Accounts	Status			
\$Extend (5)	(0)	💾 \$UpCase	3	Undecided			
\$Unalloc (1)		SMFT \$	1	Undecided			
D Compressed (7)	20076517123273.pdf	1	Undecided			
📜 Encrypted (7)		20076517123273.pdf	1	Undecided			
📜 RAW (7)		20076517123273.pdf-slack	1	Undecided			
 System Volum Views 	e Information (2)	20076517123273.pdf	1	Undecided			
 Views Results 		20076517123273.pdf-slack	1	Undecided			
Extracted Conten	*		-	0110001000			
E- Keyword Hits		Hex Strings File Metadata Result			her Occurrences		
🖌 Hashset Hits		Stange The Presenter Present					
🗈 🔛 E-Mail Messages							
- * Interesting Items							
Accounts							
Credit Card							
By BIN (4							
- 20076							
20212							
- 28384							
	3233 (1)						
Tags							

- 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.
0	This allows as to view create cara numbers and bills.

View Tools Window Help			· · ·	,		-		
🛚 Add Data Source 📠 Images/Videos 🧮 Timeline 📗 Ge	nerate Report 🛛 🛞 Close Case 🗧		<u> </u>	 Keyword Lists 	Q- Keyword Search			
⇒ Show Rejected Results	Listing /mg_ntfs1-gen2.E01				 23 R 			
Data Sources	Table Thumbnal							
- intfs1-gen2.E01	△ Name	Location	Modified Time	Change Time	Access Time			
\$OrphanFiles (0) \$Extend (5)	\$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			
Views	\$Extend		2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST			
Results	\$LogFile		2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST	2008-12-31 17:44:02 EST			
Kenderset His Construction Kenderset His Konserstrug Items Accounts Frie For Construct Frie Sorreit Card ByrRe (7) ByrRe (7)								

- 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.