



APRIL 22, 2021

MODULE 6 LAB BOOK

CURRENT DIGITAL FORENSIC TOOLS

KATIE BARNES
BOSTON UNIVERSITY METROPOLITAN COLLEGE
Digital Forensics CS 693 Spring 2

Table of Contents

Lab 11.1 Using OSForensics to Search for E-mails and Mailboxes	2
11.1.1 Lab 11.1 Executive Summary	2
11.1.2 Lab 11.1 Activity	2-8
11.1.3 Lab 11.1 Review Questions	8
Lab 11.2 Using Autopsy to Search for E-mails and Mailboxes	9
11.2.1 Lab 11.2 Executive Summary	9
11.2.2 Lab 11.2 Activity	9-13
11.2.3 Lab 11.2 Review Questions	14
Lab 11.3 Find Google Searches and Multiple E-Mail Accounts	14
11.3.1 Lab 11.3 Executive Summary	14
11.3.2 Lab 11.3 Activity	14-17
11.3.3 Lab 11.3 Review Questions	18
Lab 12.1 Examining Cell Phone Storage Devices	18
12.1.1 Lab 12.1 Executive Summary	18
12.1.2 Lab 12.1 Activity	18-26
12.1.3 Lab 12.1 Review Questions	27
Lab 12.2 Using FTK Imager to View Text Messages, Phone Numbers, and Photos	27
12.2.1 Lab 12.2 Executive Summary	27
12.2.2 Lab 12.2 Activity	27-31
12.2.3 Lab 12.2 Review Questions	32
Lab 12.3 Using Autopsy to Search Cloud Backups of Mobile Devices	32
12.3.1 Lab 12.3 Executive Summary	32
12.3.2 Lab 12.3 Activity	32-37
12.3.3 Lab 12.3 Review Questions	38

Introduction

Windows and the MET Virtual Lab were used to perform each lab. Software for each Lab are readily available for use in the Virtual Lab. Files are in the Google Drive provided for this course. The software used for Module 6 lab Book are OSForensics, Autopsy 4.3.0, and FTK Imager Lite.

Lab 11.1 – Using OSForensics to Search for E-mails and Mailboxes

11.1.1 Lab 11.1 Executive Summary

For the first lab using Windows, I downloaded the file GCFI-NTFS.E01 with the Autopsy 4.3.0 software in the MET Virtual Lab.

11.1.2 Lab 11.1 Activity

To begin this lab, I logged onto the MET Virtual Machine and ran the OSForensics Software. The objective of this activity was to load emails into OSForensics and investigate and retrieve deleted emails and software sent between two individuals. When creating a new case in OSForensics you can create an index for viewing all email files involved in the case (see Figure 1-5).



Figure 1. Launching OSForensic Software

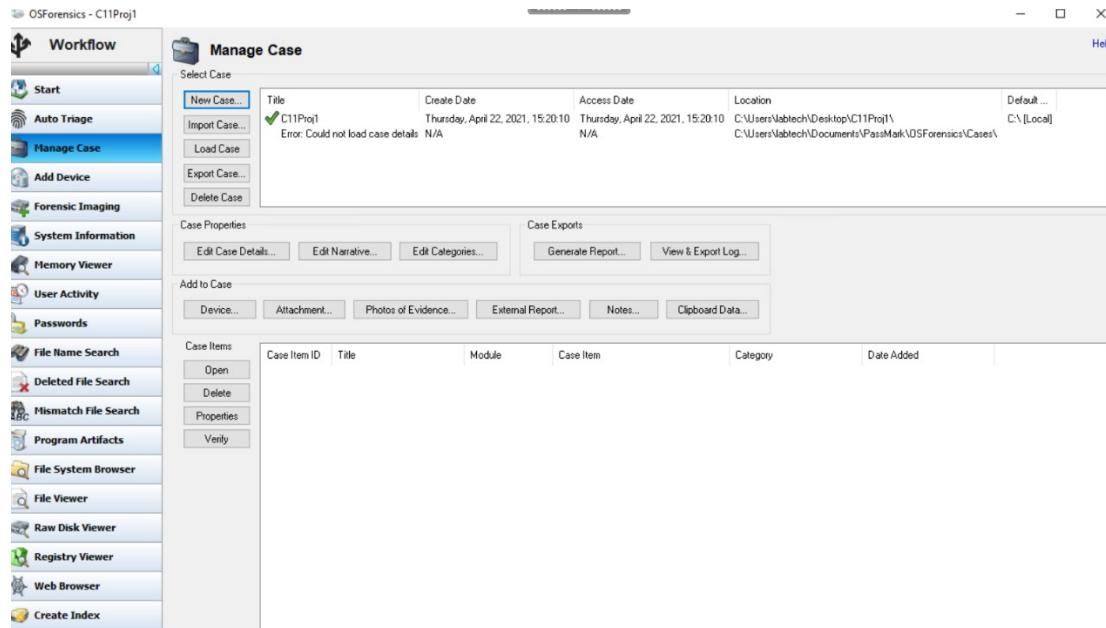


Figure 2. Managing and Creating a New Case

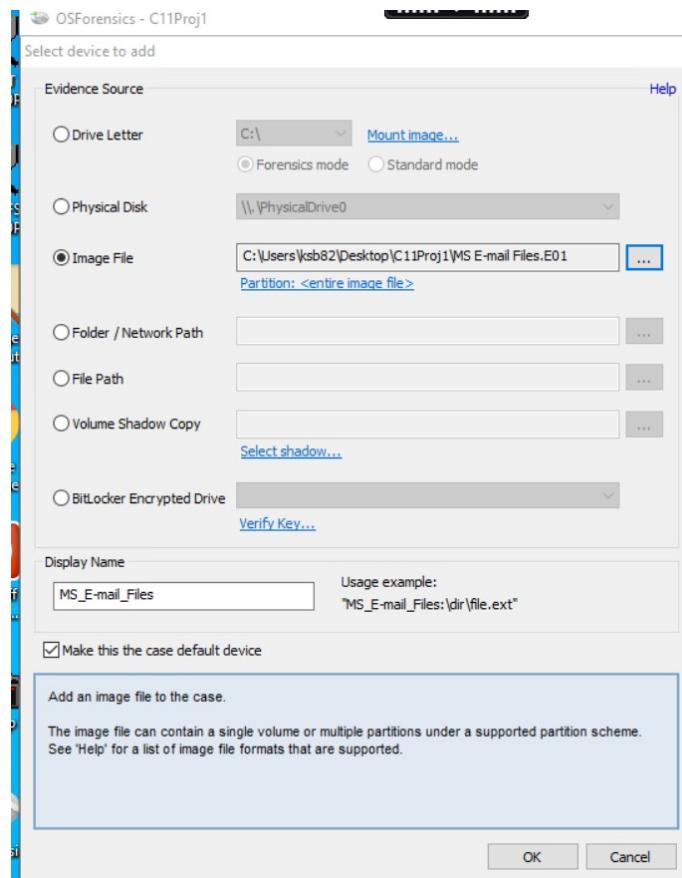


Figure 3. Adding Image File from File Source for Indexing

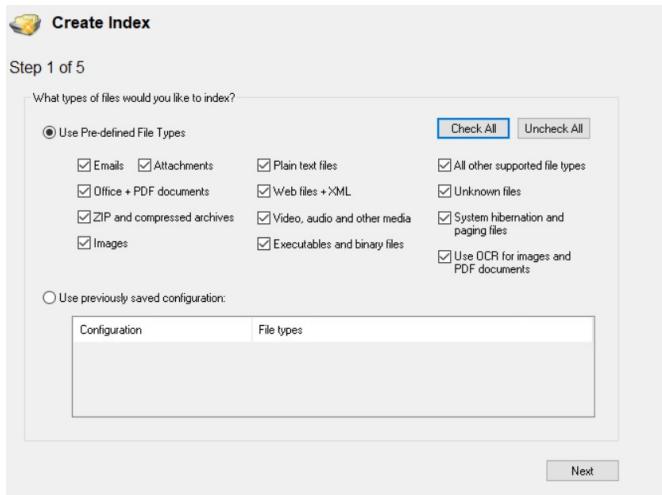


Figure 4. Creating an Index Steps 1-5

All file types are checked and the whole drive is selected for indexing.

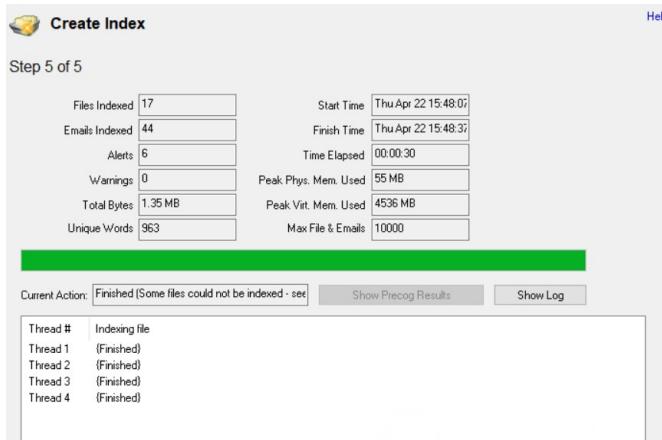


Figure 5. Finalizing Index

During the investigation process I discovered about 36 emails total between three different usernames but most importantly I discovered 3 deleted emails between Ron Torvald and Tamara Bunkley. In the emails I discovered deleted zip files, pdf's, images, and other files (see Figures 1-7).

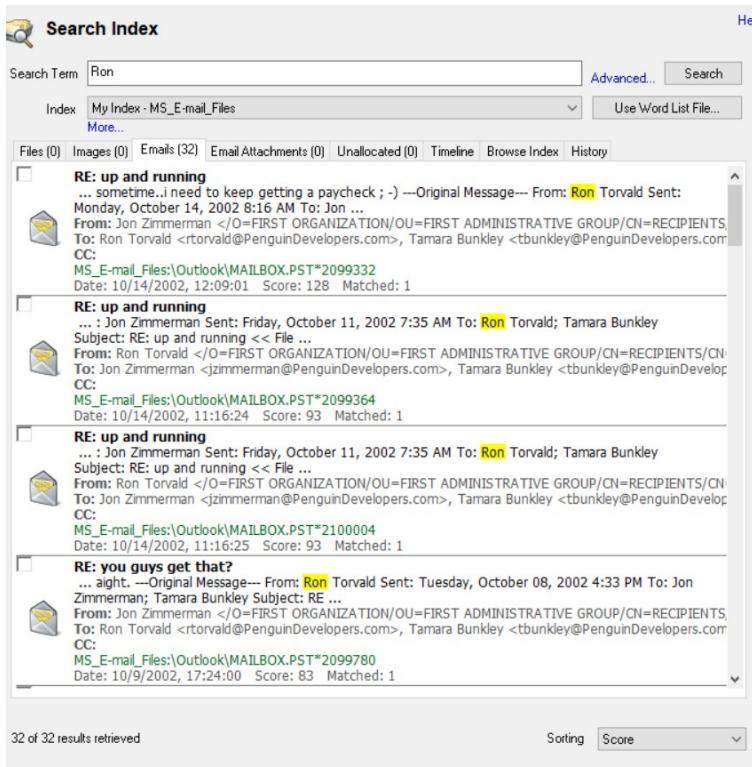


Figure 1. 32 undeleted emails

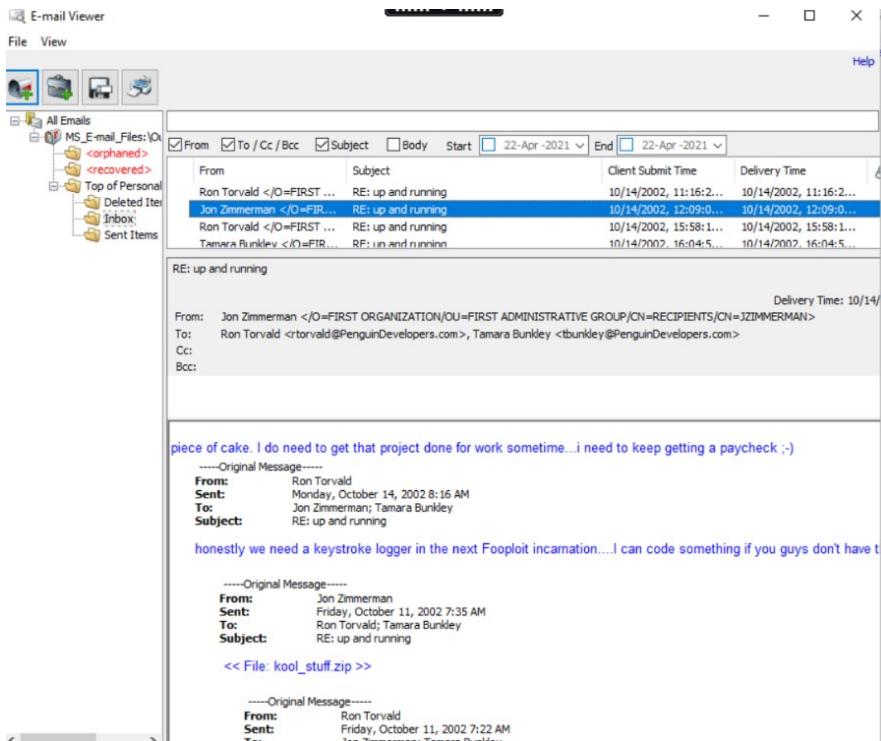


Figure 2. Email Viewer Displaying all emails and their content

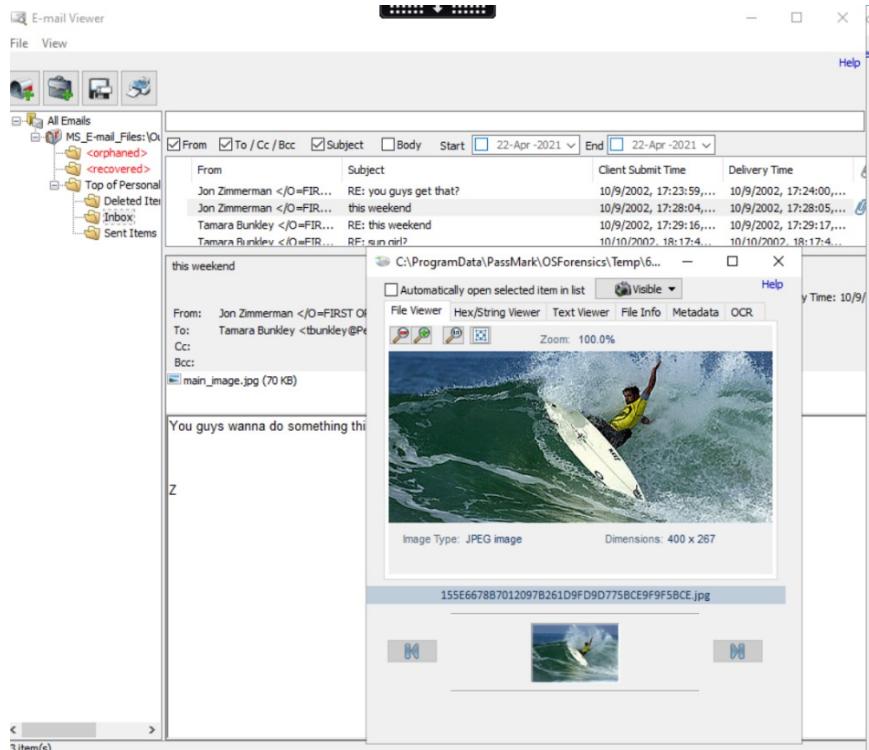


Figure 3. Inbox Emails Attached Photograph

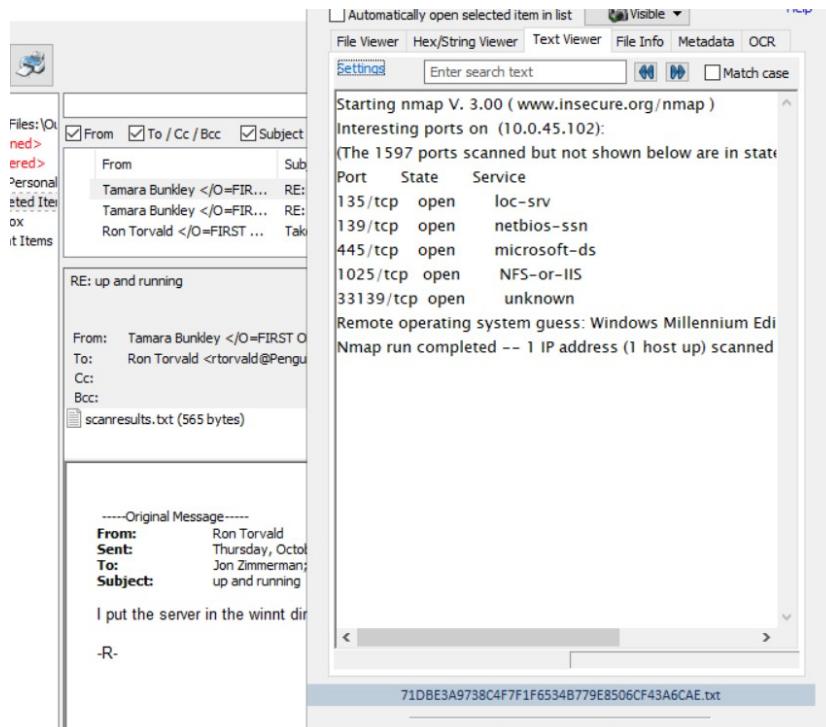


Figure 4. Deleted Items Viewing in Email Viewer of OSForensics Scan Results Txt. Evidence of Installed Software Remote Operating System.

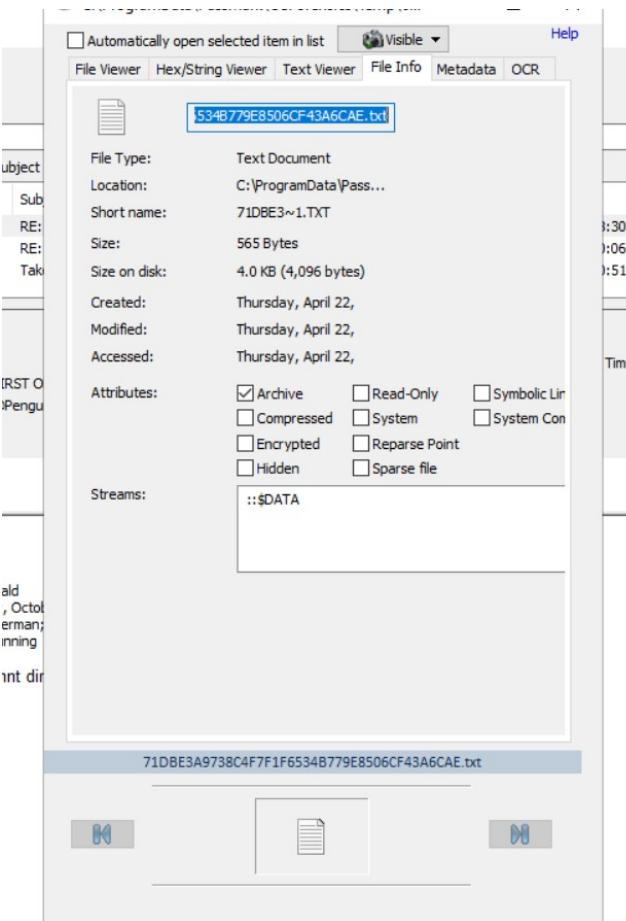


Figure 5. Operating System Size, Date Created, Modified and Accessed

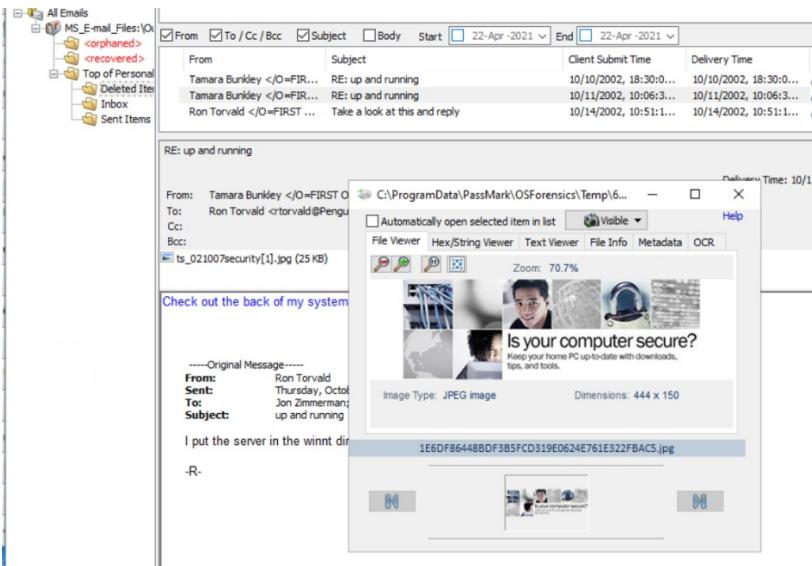


Figure 6. Deleted Program File Image

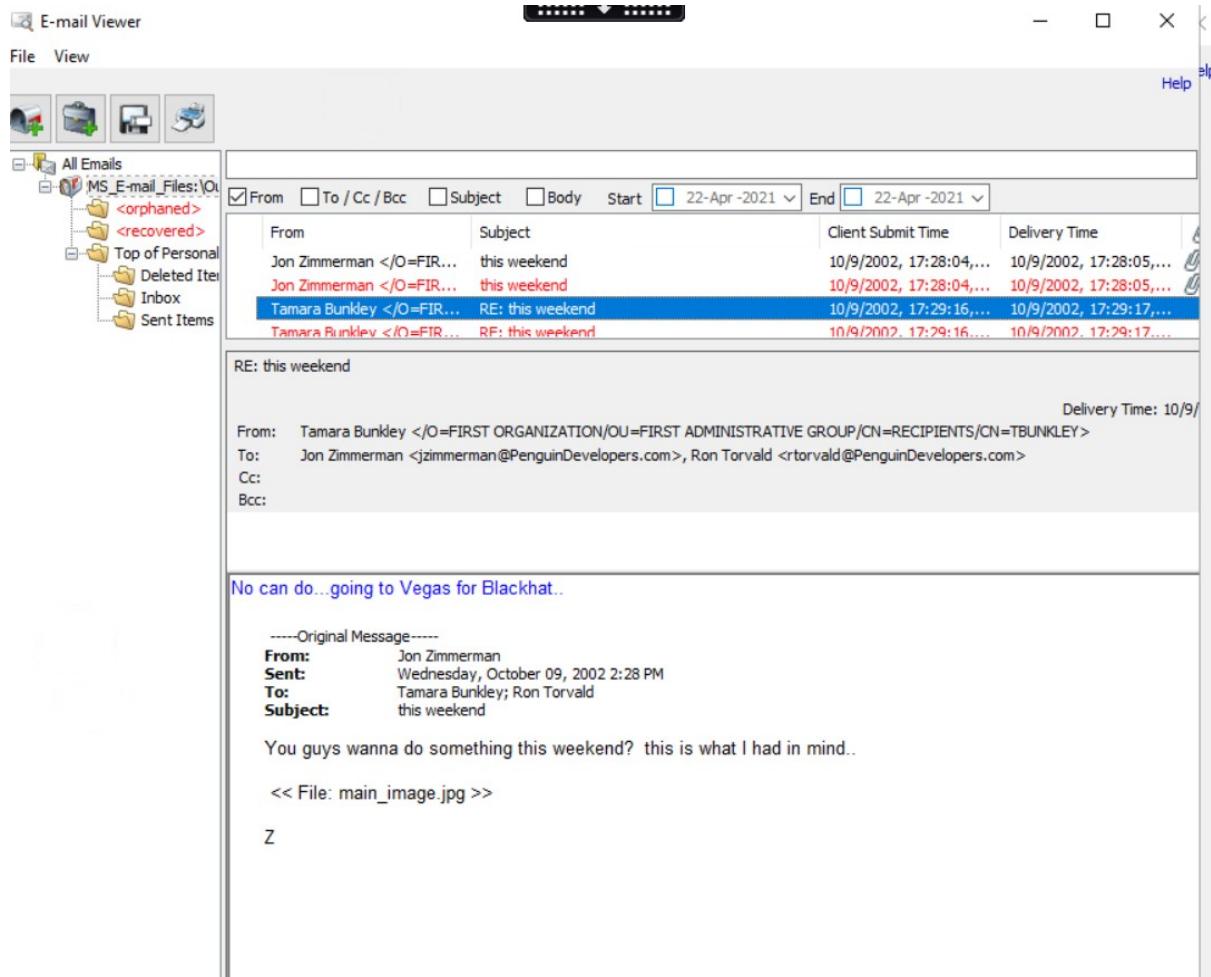


Figure 7. Deleted Email Reply from Tamara Bunkley for Jon Zimmerman and Ron Torvald

11.1.3 Lab 11.1 Review Questions

1. How many e-mails were deleted from Ron Torvald's Outlook mailbox?
3
2. How many e-mails with attached files did Ron Torvald get from Tamara Bunkley?
2
3. Deleted e-mails with attachments can't be viewed. True or False?
False
4. How many e-mails did you find by using "Ron" as a search keyword?
36
5. How many zipped files are attached to e-mails?
2

Lab 11.2 – Using OSForensics to Search for E-mails and Mailboxes

11.2.1 Lab 11.2 Executive Summary

In the second lab Autopsy 4.3.0 software was used in the MET Virtual Lab. In addition, the file MS E-mail Files.E01 were utilized during the lab session.

11.2.2 Lab 11.2 Activity

To start up the second lab I logged onto the MET Virtual Machine and launched Autopsy 4.3.0. The objective of this activity was to look for evidence in e-mails and load images containing e-mails in Autopsy. Upon Autopsy startup I created a new case in my work folder, add files using the courses Google Drive and collected my data source from the file MS E-Mail Files. E01. I discovered Graphic content and many web searches (see Figures 1-11).



Figure 1. Starting up Autopsy 4.3.0.



Figure 2. Creating a new case with Autopsy 4.3.0.

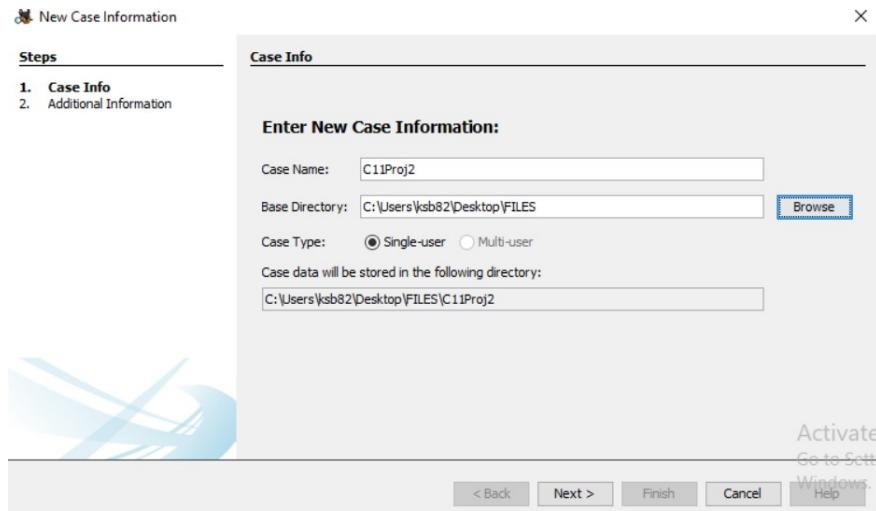


Figure 3. Step 1 Entering and Retrieving New Case Information

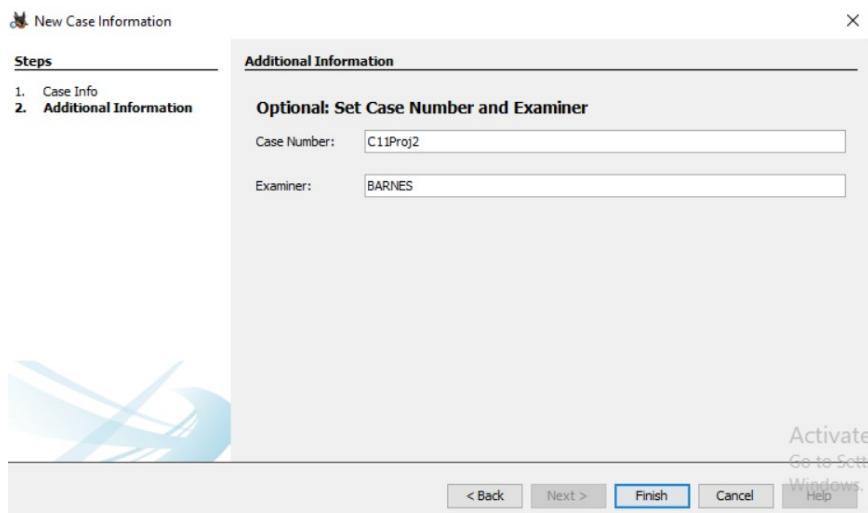


Figure 4. Step 2 Creating a Case Number and Entering Examiner Information

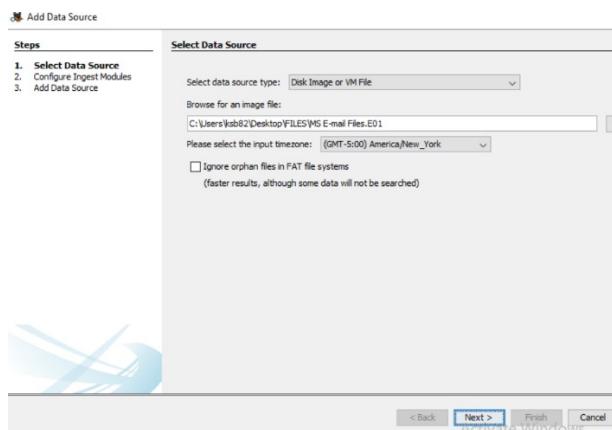


Figure 5. Creating a Data Source

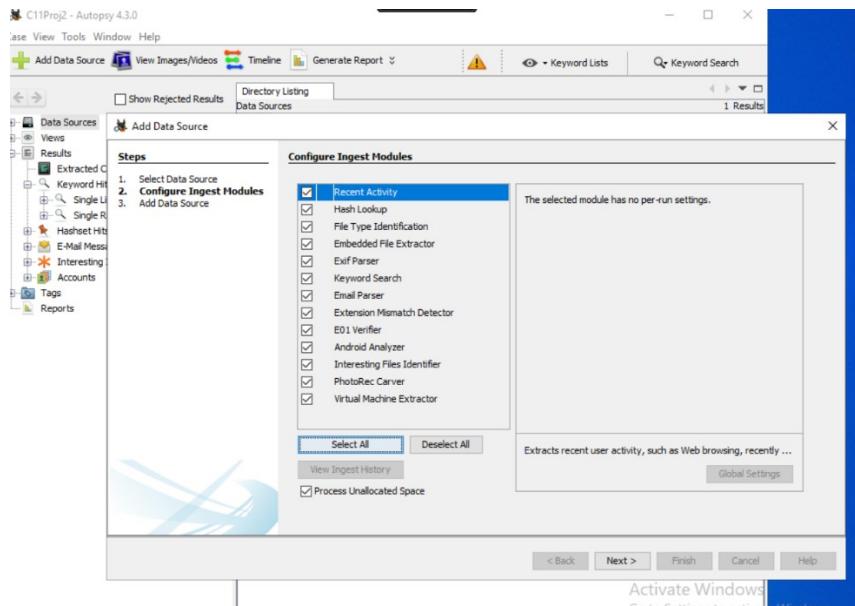


Figure 6. Configuring Ingest Modules

In the figure posted in the above image I needed to select all modules to get the best possible result to find all web searches and any information that may be available for extraction such as hash information, web searches, embedded searches, or any hidden files.

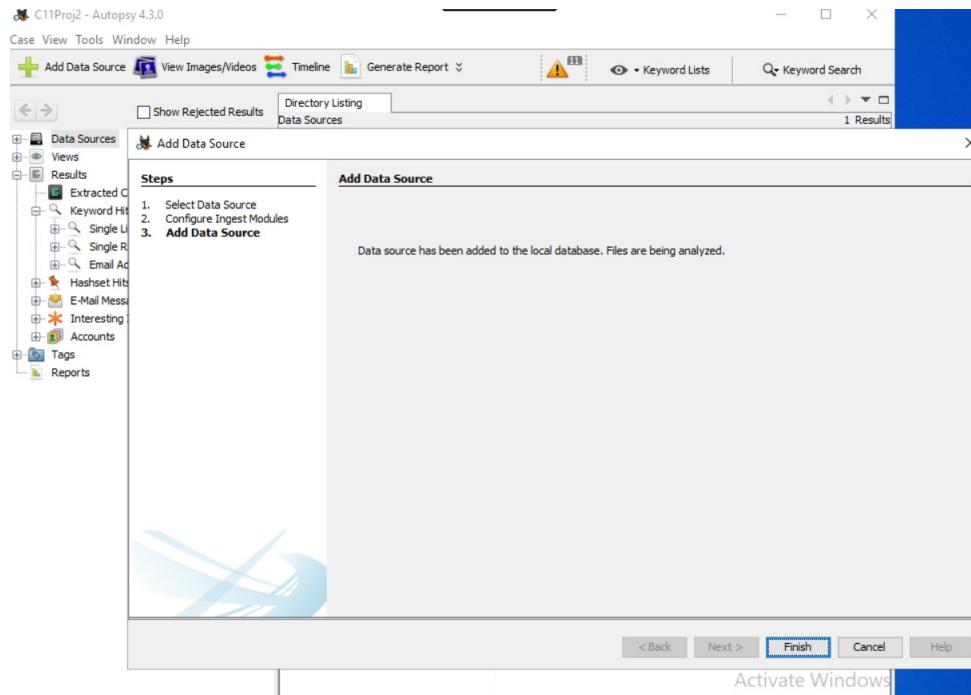


Figure 7. Adding a Data Source

The above figure demonstrates the next step needed to take to navigate through evidence. When creating my work folder, I added the file MS E-Mail Files. E01, which contained all evidence for this case.

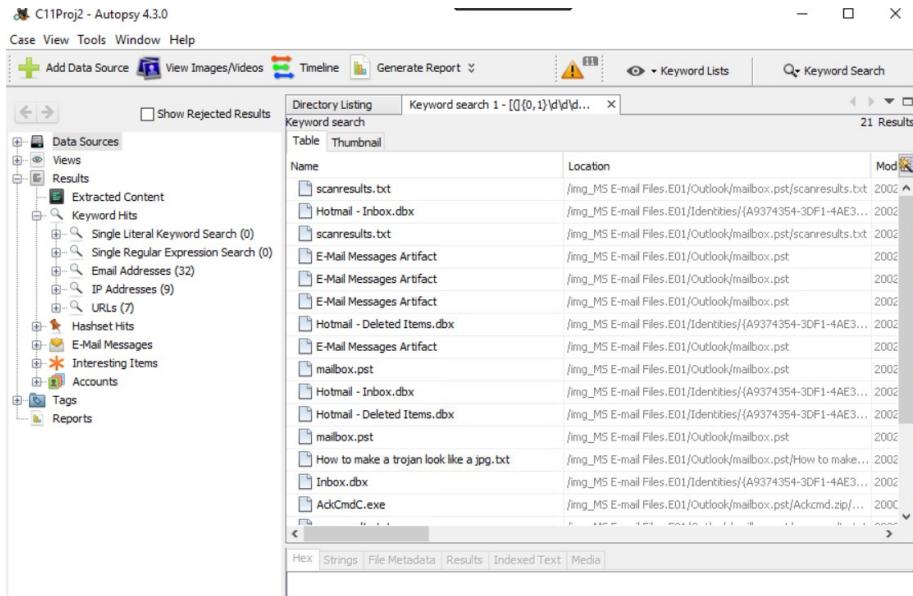


Figure 8. Keyword Search 1 For all Keyword Hits

In the above image provided shows all E-Mail artifacts discovered through a keyword search. This keyword such was done searching Phone Numbers, Email Addresses, IP addresses, and URL's.

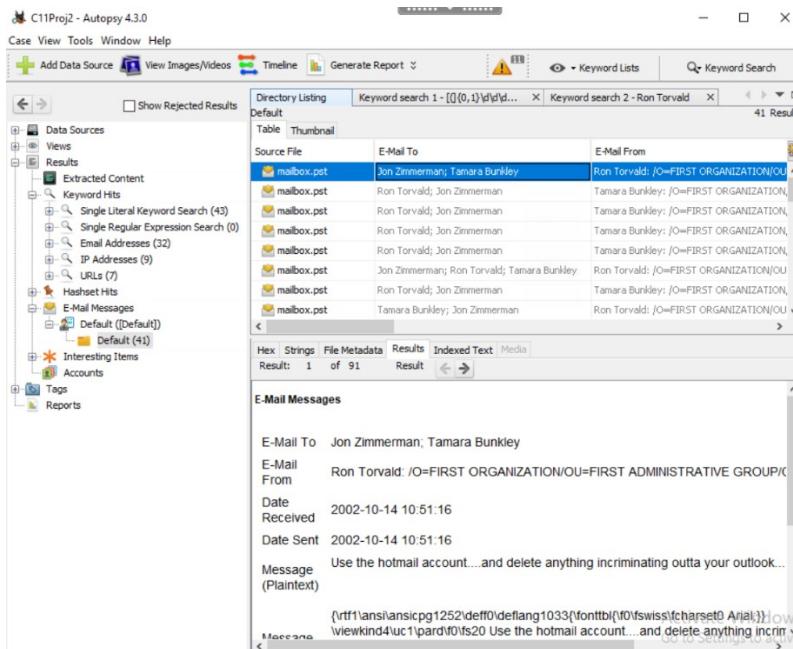


Figure 9. Checking the E-Mail Default Folder Results

I am able to see the Hex, strings, File Metadata, results that contain the user information of all parties involved, date sent and received ect. In addition the intexed content.

In Hashsets	MD5 Hash	Object ID	MIME Type	Tags
own	edaff5acf07f69c39e342282057bbe38	65	image/jpeg	
own	edaff5acf07f69c39e342282057bbe38	68	image/jpeg	
own	2c5cdf5d5bd6227c513d96177d0a0083	70	image/vnd.adobe.photoshop	
own	edaff5acf07f69c39e342282057bbe38	71	image/jpeg	
own	a07be511885c5fce56df0cd5fb495	72	image/jpeg	
own	2c5cdf5d5bd6227c513d96177d0a0083	74	image/vnd.adobe.photoshop	
own	9960f5b852089a6d20c566b58e0bce03	82	image/png	
own	b7e2a5183839c83b5beb46d529831fb9	83	image/jpeg	
own	7098107b46b53663d2edf0e91b09689e	84	image/jpeg	
own	5e20b8beadb0fe1dc57654500de9497b	85	image/png	
own	8e9056b7b61323f7b98188697eacd9f	86	image/png	
own	9960f5b852089a6d20c566b58e0bce03	88	image/png	
own	b7e2a5183839c83b5beb46d529831fb9	89	image/jpeg	
own	7098107b46b53663d2edf0e91b09689e	90	image/jpeg	
own	5e20b8beadb0fe1dc57654500de9497b	91	image/png	
own	8e9056b7b61323f7b98188697eacd9f	92	image/png	

Figure 10. Second Keyword Search Revealing Images, Documents and MD5 Hash Information

List Name	Files with Hits
FooCrewed_foocrew@hotmail.com (2)	2
RATS.Nest@usa.net (4)	4
Staffstaff@hotmail.com (2)	2
Teamoe5@microsoft.com (2)	2
Zimmermanjzimmerman@PenguinDevelopers.com (2)	2
Zed_FooCrew@hotmail.com (4)	4
anne.vidstrom@ntsecurity.nu (2)	2
bunky_FooCrew@hotmail.com (4)	4
diggy_FooCrew@hotmail.com (4)	4
diggy_foocrew@hotmail.com (4)	4
ew@hotmail.com (2)	2

Figure 11. Directory Listing Revealing 32 E-Mail Addresses

11.2.3 Lab 11.2 Review Questions

1. How many graphics files did Autopsy recover?
16
2. How many Hotmail e-mail addresses did you find?
7
3. How many video files are attached to e-mails in the MS E-mail Files.E01 image?
0
4. In the Archive folder (under the File Type, By Extension path), how many archive files did Autopsy recover?
2
5. Autopsy recovered the same number of e-mails as OSForensics did. True or False?
False

Lab 11.3 – Find Google Searches and Multiple E-Mail Accounts

11.3.1 Lab 11.2 Executive Summary

In the next lab I used Autopsy 4.3.0 the MET Virtual Lab. In addition, I downloaded the file precious.001 from the classroom Google Drive.

11.3.2 Lab 11.2 Activity

To start this lab, I launched Autopsy 4.3.0 software. The goal to this lab is find Google searches and mailboxes associated with multiple e-mail accounts (see Figures 1-9) (Cengage,2019).

The screenshot shows the Autopsy 4.3.0 interface with the title bar "C11Proj3 - Autopsy 4.3.0". The menu bar includes "Case View Tools Window Help". The toolbar has icons for "Add Data Source", "View Images/Videos", "Timeline", "Generate Report", "Close Case", "Keyword Lists", and "Keyword Search". The left sidebar is titled "Data Sources" and lists "Results", "Extracted Content" (with sub-items like "Encryption Detected", "Extension Mismatch Detected", "Operating System User Account", "Recent Documents", "Remote Drive", "Web Bookmarks", "Web Cookies", "Web History", "Web Search"), "Keyword Hits" (with sub-items like "Single Literal Keyword Search", "Single Regular Expression Search", "Email Addresses"), "Hashes", "E-Mail Messages", "Interesting Items", "Accounts", "Tags", and "Reports". The central pane displays a "Directory Listing" table with one row for "precious.001". The table columns are Name, Type, Size (Bytes), Sector Size (Bytes), MD5 Hash, Timezone, and Device ID. The row shows "precious.001" as an Image file, 128450048 bytes, 512 sectors, MD5 hash a14e2da7-bc9d-478c-b659-f13f0a0000d6b, America/New_York timezone, and Device ID a14e2da7-bc9d-478c-b659-f13f0a0000d6b. Below the table is a navigation bar with tabs: Hex, Strings, File Metadata, Results, Indexed Text, and Media.

Figure 1. precious.001 File

In the above image I was able to extract the precious.001 image using Autopsy 4.3.0. located under results and the extracted content folder. In the next image you can see that there are many different pieces of data that are enclosed in this one file.

The screenshot shows the Autopsy 4.3.0 interface. The left sidebar shows various data sources like Data Sources, Views, Results, and Tags. Under Results, the Extracted Content folder is expanded, showing items like Encryption Detected, Extension Mismatch Detected, Operating System User Account, Recent Documents, Remote Drive, Web Bookmarks, Web Cookies, Web History, and Web Search. The Keyword Hits section is also visible. The main pane displays a 'Directory Listing' table for the 'precious.001' file. The table has columns for Name, Type, Size (Bytes), and Sec. A checkbox for 'URLs' is selected in the 'Phone Numbers' row. To the right, a 'Keyword Lists' panel shows a single result: '(((ht|f)tp(s?))://|www\.)[a-zA-Z0-9.-]+\.[a-zA-Z]{2,4}' with a 'Regular Expression' keyword type. The status bar at the bottom indicates 'Files Indexed: 5,325'.

Figure 2. precious.001 File Keyword Search for Phone Numbers, IP Addresses, E-Mail Addresses, and URLs.

This screenshot shows the same Autopsy interface as Figure 2, but with a different keyword search applied. The search term in the top bar is 'Keyword search 1 - [[0,1]\d\d\d...'. The main pane now displays a table of files found in the 'precious.001' file. The columns are Name, Location, Modified Time, and Change Time. The table lists numerous files including 'Inbox.dbx', 'f0029229.dbx', '8BF5F7Fd01', 'NTUSER.DAT', 'E-Mail Messages Artifact', 'PHONE TEST.txt', 'Frodo Baggins.wab', 'abook.mab', 'Unalloc_5389_12027392_128318976', 'E-Mail Messages Artifact', 'E-Mail Messages Artifact', 'Saved Mail', '9CC092Fc01', and 'Digital Evidence Standards (Public).ppt'. The status bar at the bottom indicates '1142 Results'.

Figure 3. Data Contained in precious.001 File

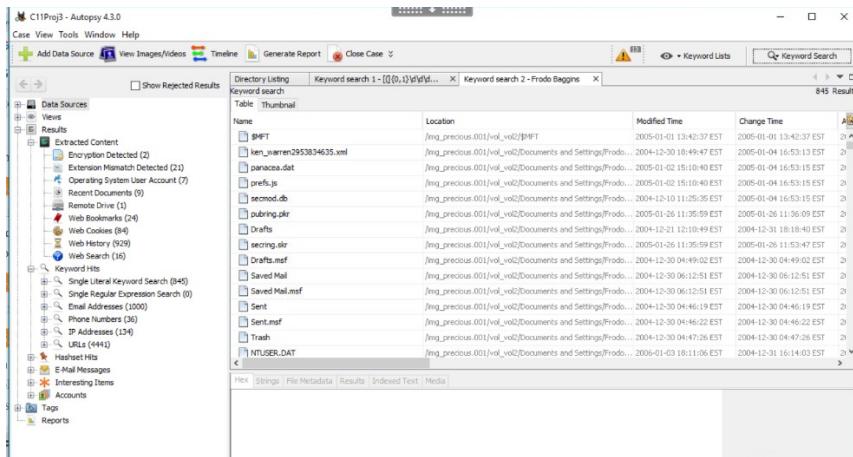


Figure 4. Keyword Search 2 for Frodo Baggins

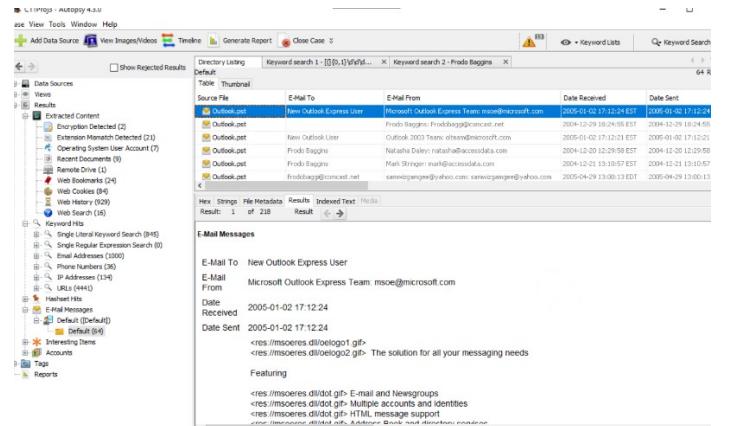


Figure 5. Keyword Search 2 Default Folder Evidence

The image in the above picture shows E-Mail messages with the username Frodo Baggins.

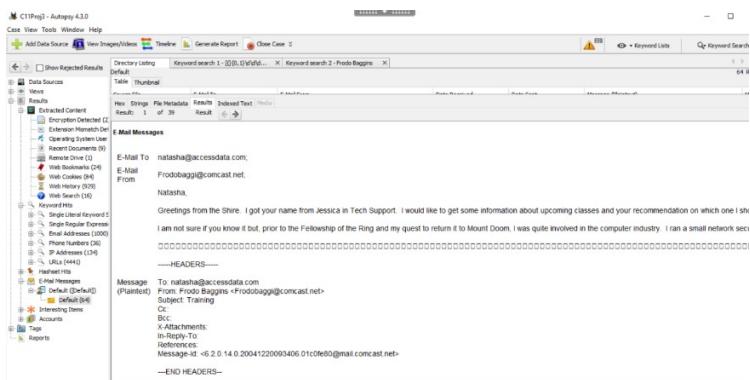


Figure 6. Further E-Mail Evidence with Keyword Search 2

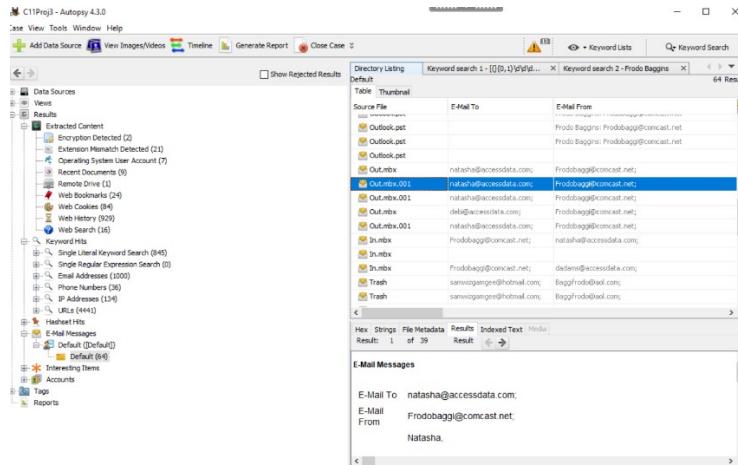


Figure 7. Default E-Mail containing 54 Messages

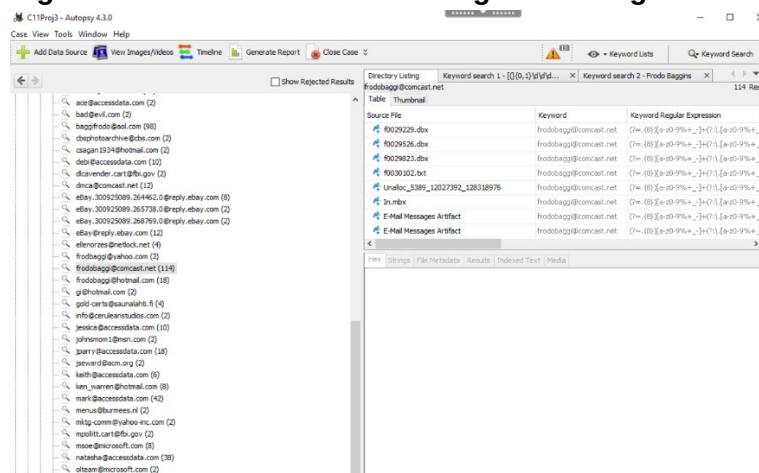


Figure 8. Frodo Baggins name in many different E-Mail addresses and E-Mail Artifacts

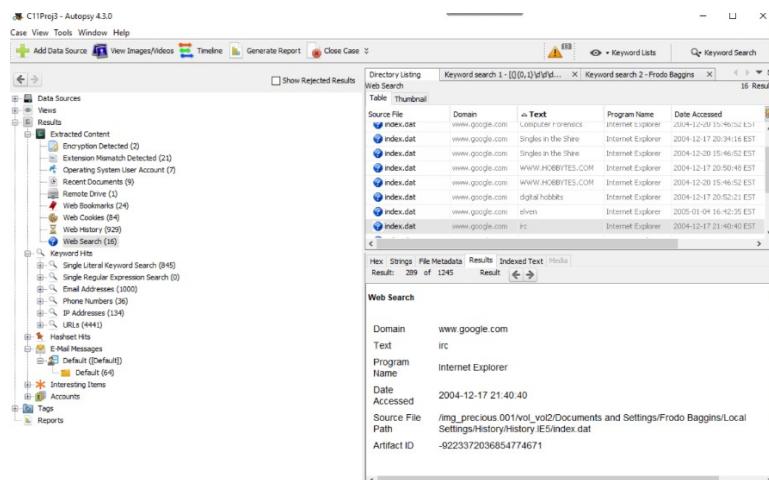


Figure 9. Web Search Containing Hex, Strings, File Metadata, Results, and Indexed Text.

In the above image displayed the domain (Google) was used in the web searches for 16 different web searches through the Internet Explorer.

11.3.3 Lab 11.3 Review Questions

1. How many e-mails, including duplicates, did you find?
64
2. How many different Frodo Baggins e-mail addresses did Autopsy recover?
8
3. Frodo Baggins didn't have an AOL e-mail account. True or False?
False
4. How many Google searches for the term "computer forensics" were made?
3
5. MD5 hash values are displayed automatically in the default mailbox view. True or False?
False

Lab 12.1– Examining Cell Phone Storage Devices

12.1.1 Lab 12.1 Executive Summary

Working with Windows, I downloaded the file Motorola.E01 (available in Google Drive provided by this class) to use with the Autopsy 4.3.0 software in the MET Virtual Lab.

12.1.2 Lab 12.1 Activity

To begin this lab, I logged onto the MET Virtual Machine and opened Autopsy 4.3.0 to gather examine forensic storage data from a cell phone and process images. (see Figure 1-5).

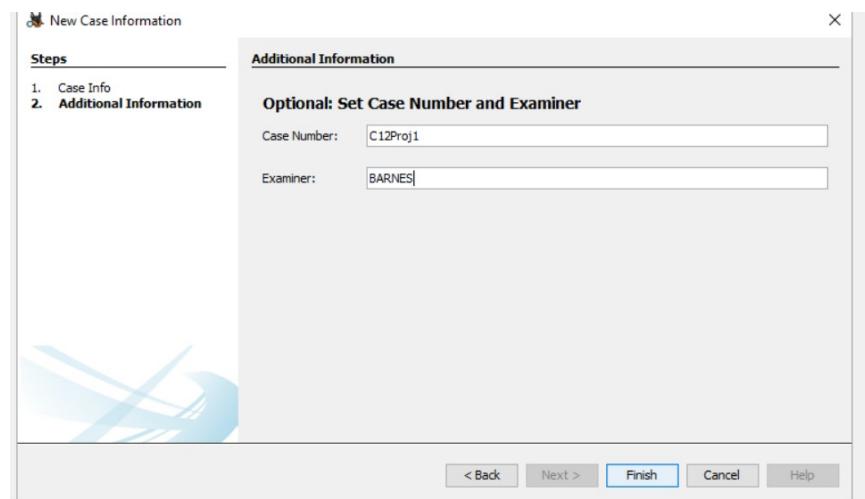


Figure 1. Creating a New Case in Autopsy 4.3.0

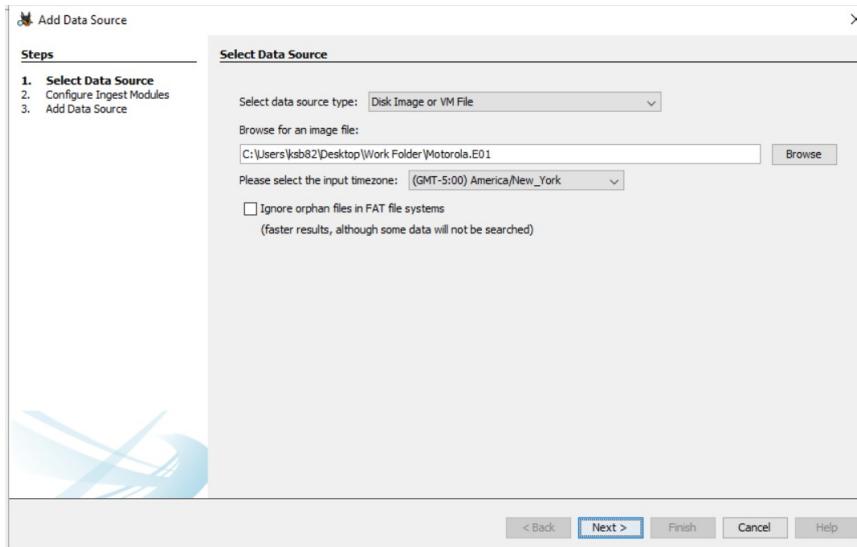


Figure 2. Selecting Data Source for Autopsy 4.3.0.

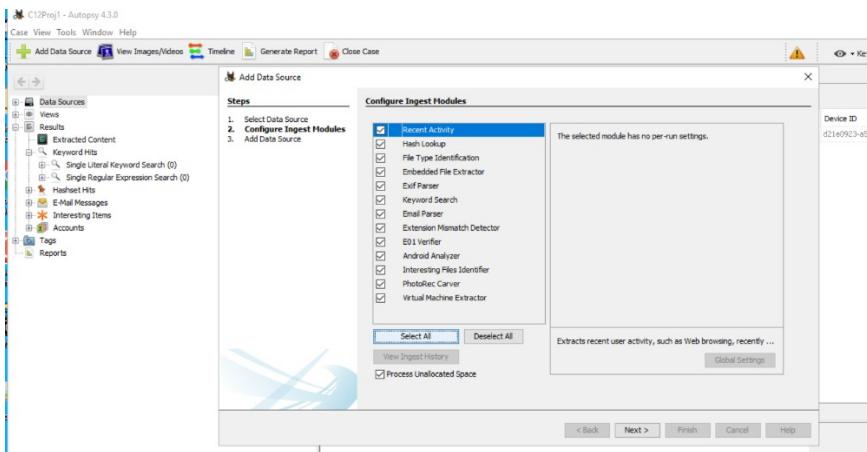


Figure 3. Configuring Ingest Modules

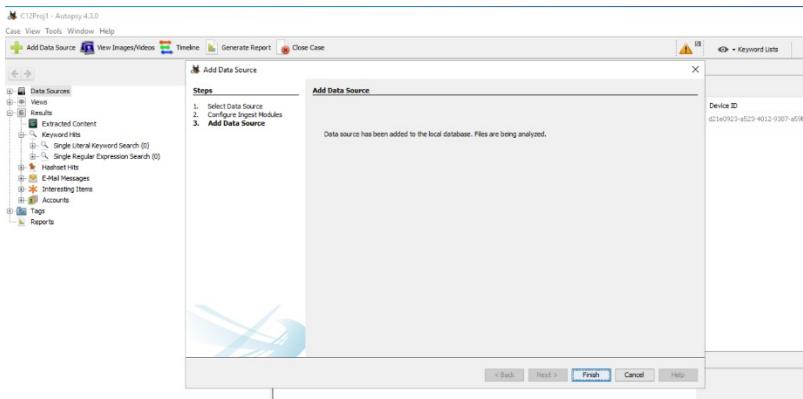


Figure 4. Adding a Data Source which is the file Motorola.E01 (see Figure 5.)

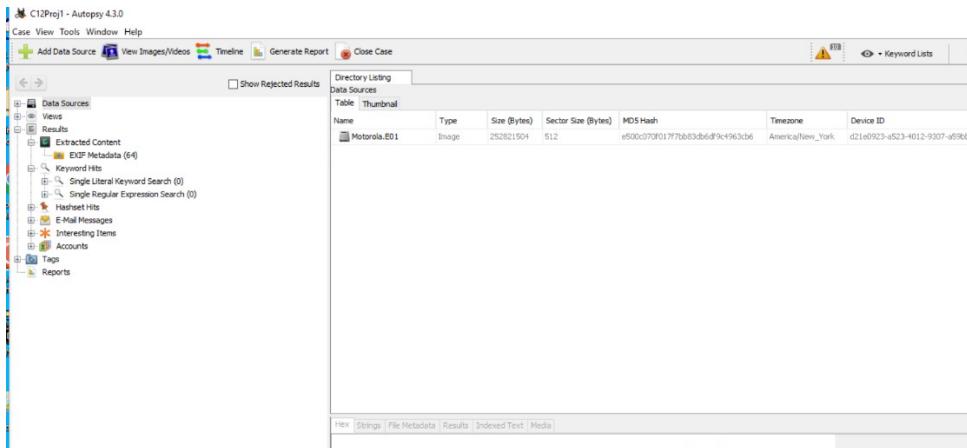


Figure 5. Motorola.E01 File Directory Listing

After gathering evidence data files, I can then review the evidence in Autopsy 4.3.0. under the Motorola.E01 Folder. In the following images I have extracted deleted (orphan) files (see Figures 1-13).

Name	Modified Time	Change Time	Access Time	Created Time
\$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
\$Unalloc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
mobile	2006-03-09 06:38:38 EST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
motorola	2006-03-09 06:38:20 EST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
02-05-07_1651.jpg	2006-07-13 00:40:00 EDT	2000-00-00 00:00:00	2010-05-31 00:00:00 EDT	0000-00-00 00:00:00
02-10-07_1450.jpg	2006-07-18 00:06:26 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
02-15-07_1419.jpg	2006-07-23 00:11:34 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
02-19-07_2101.jpg	2006-07-27 04:00:34 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
02-21-07_1108.jpg	2006-07-29 19:37:08 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
02-21-07_1109.jpg	2006-07-29 19:38:22 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
02-21-07_1622.jpg	2006-07-29 00:49:00 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
02-24-07_1211.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00	2010-06-01 00:00:00 EDT	0000-00-00 00:00:00
02-24-07_1212.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00	2010-06-01 00:00:00 EDT	0000-00-00 00:00:00
02-24-07_1213.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00	2010-06-01 00:00:00 EDT	0000-00-00 00:00:00
02-24-07_1214.ico	0000-00-00 00:00:00	0000-00-00 00:00:00	2010-06-01 00:00:00 EDT	0000-00-00 00:00:00

Figure 1. Deleted and Undeleted Files Under Motorola.E01 File Folder the Items that have a Red X Mark are Identified as Deleted Files

The screenshot shows the Autopsy 4.3.0 interface. The top menu bar includes File, View, Tools, Window, Help, Add Data Source, View Images/Videos, Timeline, Generate Report, Close Case, Keyword Lists, and a search bar. The left sidebar lists Data Sources (Motorola.E01), Views, Results, Extracted Content (EXIF Metadata (64)), Keyword Hits, Single Literal Keyword Search (0), Single Regular Expression Search (0), Hashset Hits, E-Mail Messages, Interesting Items, Accounts, Tags, and Reports. The main pane displays 'Directory Listing /Img_Motorola.E01' with a 'Table' view. A 'Results' tab is selected, showing detailed file metadata for '/Img_Motorola.E01/motorola'. The metadata includes:

Name	/Img_Motorola.E01/motorola
Type	File System
MIME Type	null
Size	4096
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2006-03-09 06:38:20 EST
Accessed	0000-00-00 00:00:00
Created	0000-00-00 00:00:00
Changed	0000-00-00 00:00:00
MD5	Not calculated
Hash Lookup Results	UNKNOWN
Internal ID	4

Below this, a section titled 'From The Sleuth Kit istat Tool:' provides similar information:

Directory Entry:	4
Allocated	
File Attributes:	Directory
Size:	4096
Name:	MOTOROLA
Directory Entry Times:	
Written:	2006-03-09 06:38:20 (EST)
Accessed:	0000-00-00 00:00:00 (UTC)
Created:	0000-00-00 00:00:00 (UTC)

Figure 2. Under Directory Listing File Metadata

This item above is the file Metadata for the image Motorola.E01 which is a cell phone image. It shows the image type, File name and allocation, date modified, date created, date accessed or changed and the size of the image. However, notice that it does not display the MD5 Hash results are unknown and not calculated.

The screenshot shows the Autopsy 4.3.0 interface. The left sidebar lists Data Sources (Motorola.E01), Views, Results, Extracted Content (EXIF Metadata (64)), Keyword Hits, Single Literal Keyword Search (0), Single Regular Expression Search (0), Hashset Hits, E-Mail Messages, Interesting Items, Accounts, Tags, and Reports. The main pane displays 'Directory Listing /Img_Motorola.E01' with a 'Table' view. A 'Results' tab is selected, showing a list of files with their names, modified times, change times, access times, and creation times. One file, '02-05-07_1651.jpg', is highlighted. Below the table, there is a preview window showing a photograph of two people in a room, one standing and one sitting, with a presentation screen in the background.

Figure 3. Deleted Image 02-05-07_1651.jpg Retrieved Under Extracted Content and EXIF Metadata which Includes 64 Items Within

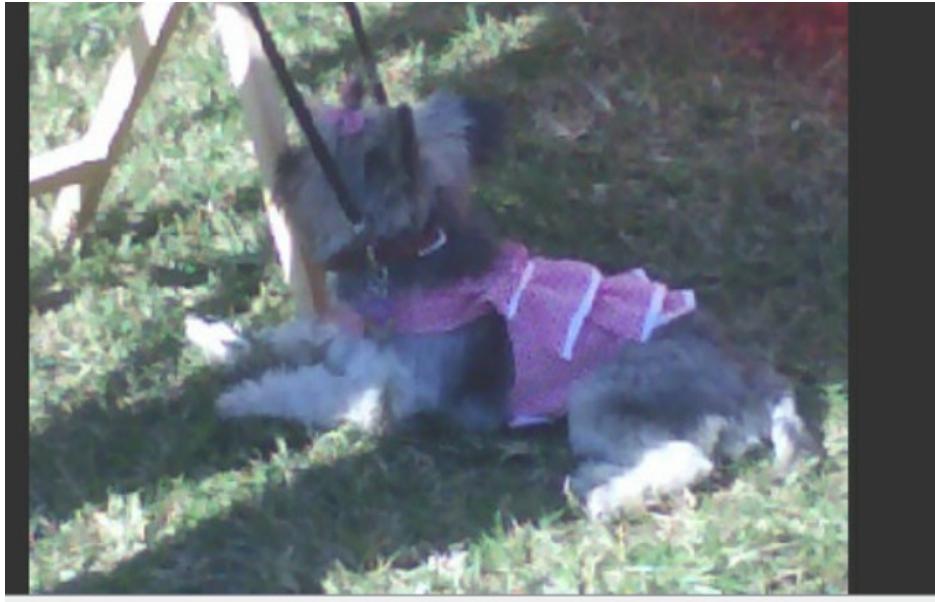


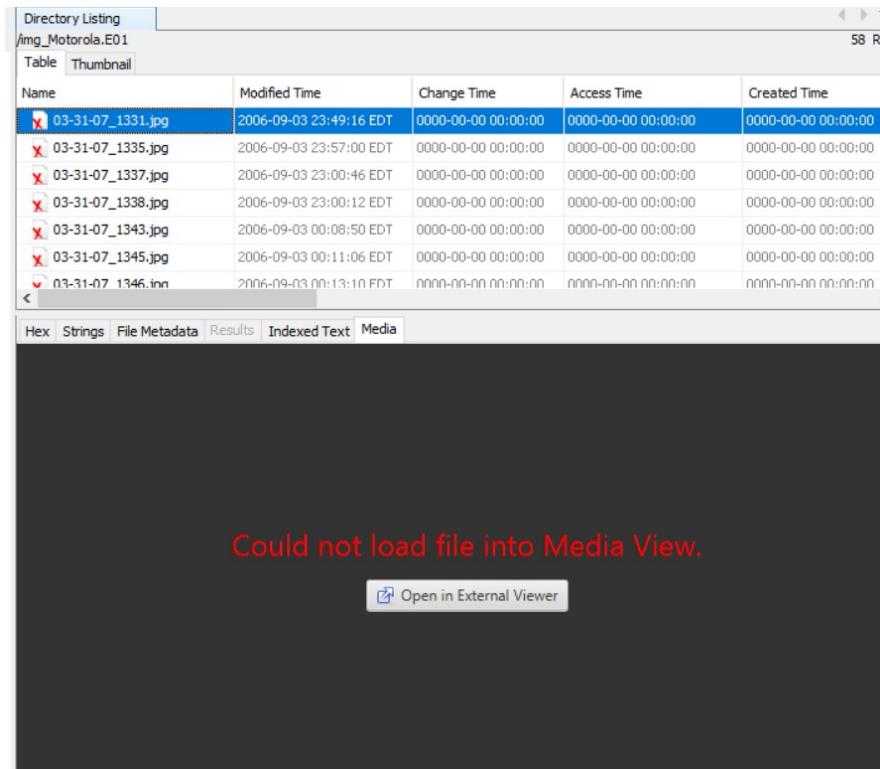
Figure 4. Deleted Image Recovered in the Same Folder

✗	02-15-07_1419.jpg	2006-07-23 00:11:34 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00
✗	02-19-07_2101.jpg	2006-07-27 04:00:34 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00
✗	02-21-07_1108.jpg	2006-07-29 19:37:08 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00
✗	02-21-07_1109.jpg	2006-07-29 19:38:22 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00
✗	02-21-07_1622.jpg	2006-07-29 00:49:00 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00
📄	02-24-07_1211.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00	2010-06-01 00:00:00 EDT
📄	02-24-07_1212.inn	nnnn-nn-nn nn:nn:nn	nnnn-nn-nn nn:nn:nn	2010-06-01 00:00:00 FDT

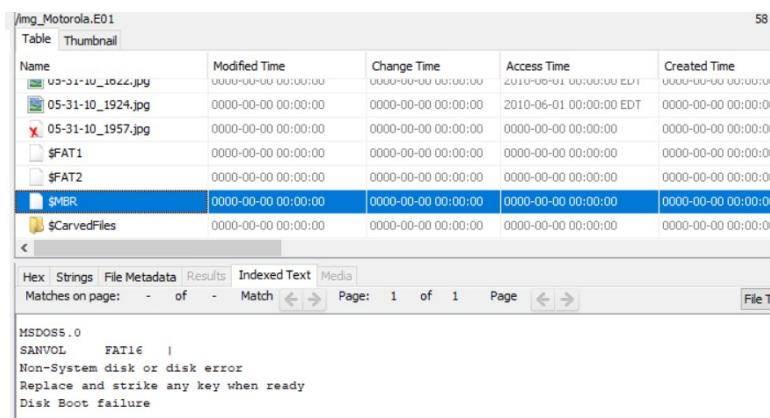
Hex Strings File Metadata Results Indexed Text Media

A screenshot of a digital forensic analysis interface. At the top, there is a table listing several files with their names, creation dates, and timestamps. Below the table, there is a large, solid black rectangular area, likely a redaction or a placeholder for a recovered image file. At the bottom of the interface, there are tabs labeled "Hex", "Strings", "File Metadata", "Results", "Indexed Text", and "Media".

Figure 5. Deleted Image that Could not be Found

**Figure 6. Image Could not be Displayed it Would not Load**

The above images that were retrieved only the File headers were recovered but not the actual images.

**Figure 7. \$MBR File Provides Indexed Text Revealing the name of the storage device SANVOL found in FAT16 as a Master Boot Record.**

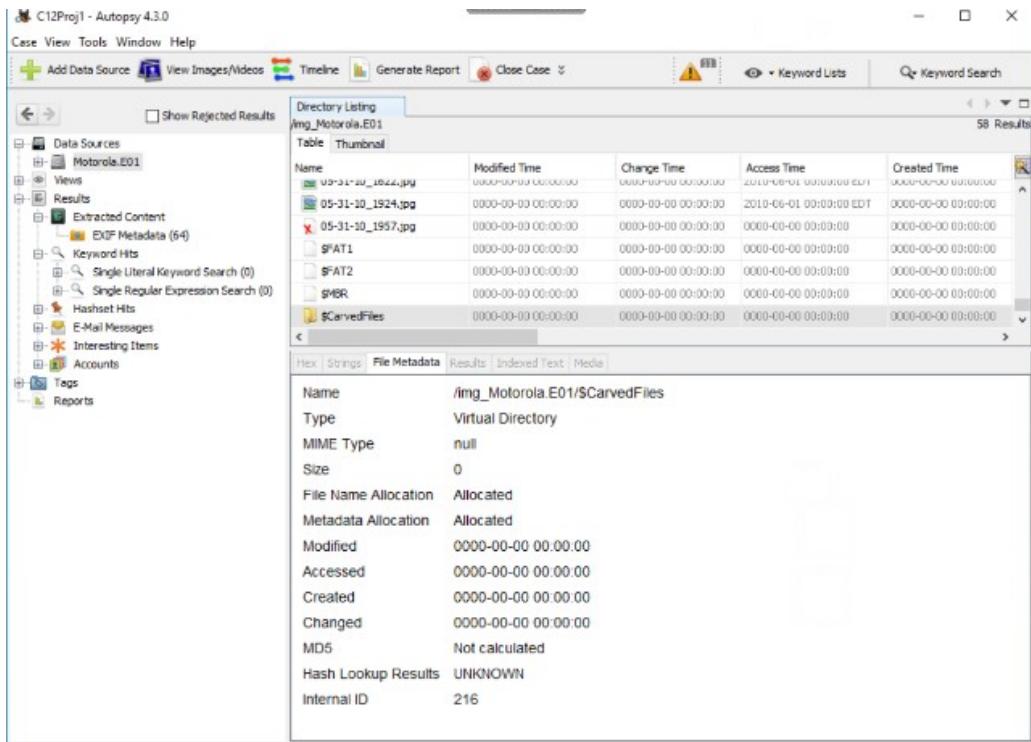


Figure 8. \$CarvedFiles Virtual Directory item

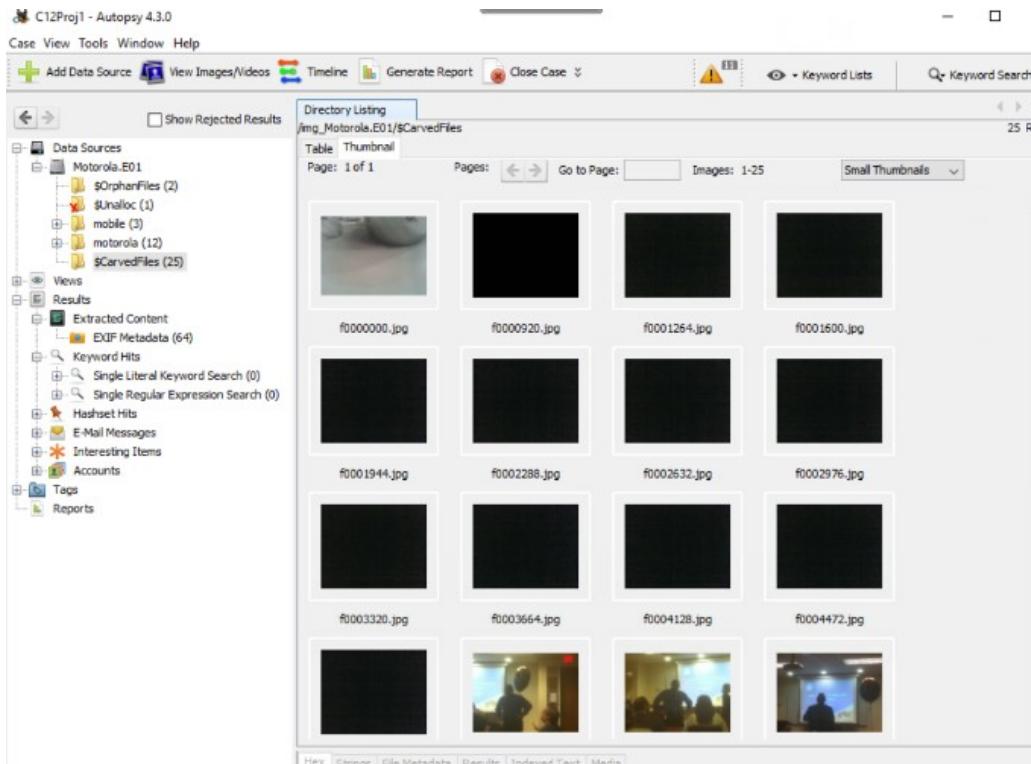


Figure 9. Deleted Images Found in \$CarvedFile Folder

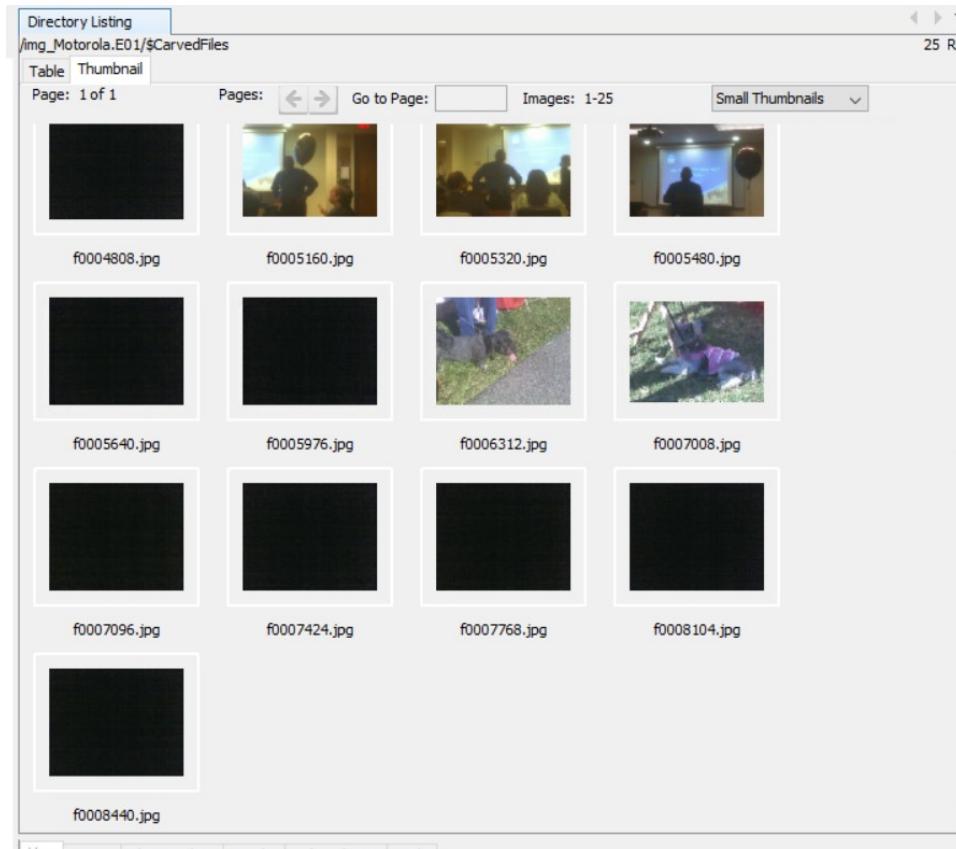


Figure 10. Deleted Items \$CarvedFiles Folder Continued

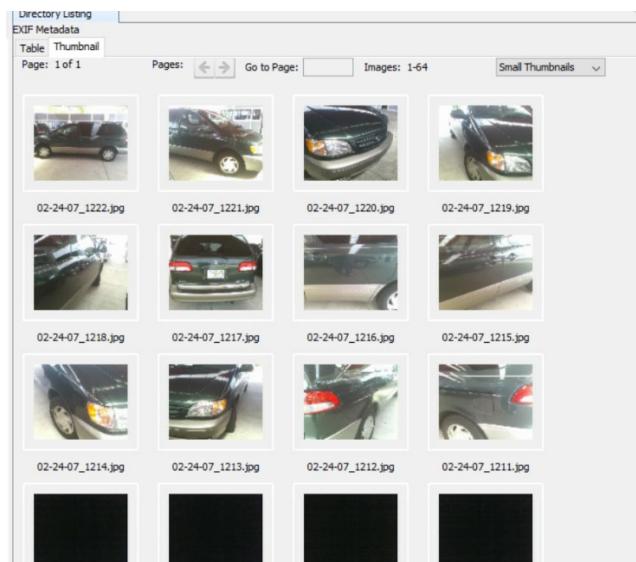


Figure 11. Images of a Car Found in Deleted Files



Figure 12. This is a deleted photograph of a car recovered from the \$CarvedFiles Folder.

Hex Strings File Metadata Results Indexed Text Media

Page: 1 of 11 Page ← → Go to Page: []

Exif
Motorola
1.3 Megapixel
0220
0100
2007:02:24 17:19:13
2007:02:24 17:19:13
0100
\$3br
%& () *456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
#3R
& ' () *56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
k+&29
q~ &0,
uc^~
.....

Figure 13. Strings Exif Motorola 1.3 Megapixel Camera

This is the camera used to take the photographs that were deleted. This is a great piece of evidence.

12.1.3 Lab 12.1 Review Questions

1. Under the EXIF Metadata folder in the left pane of Autopsy, how many pictures have been recovered from the cell phone image?
64
2. How many subfolders are under the Motorola folder (the MicroSD storage device)?
10
3. Which file system is in use on the MicroSD storage device?
FAT16
4. What's the resolution of the cell phone's camera?
1.3 MP
5. Which column do you check to determine whether a file is in unallocated space?

Under Data Sources you will find the Motorola.E01 file folder, once you expand those two folders you will find Orphan files and then unallocated files within the Orphan files.

Lab 12.2– Using FTK Imager to View Text Messages, Phone Numbers, and Photos

12.2.1 Lab 12.2 Executive Summary

In this lab FTK Imager Lite was used to look for cell phone evidence and process cell phone images. I downloaded the file LG_6000_4d76e052.ad1 from the classrooms Google Drive to use with FTK Imager Lite.

12.2.2 Lab 12.2 Activity

To start this lab, I logged onto the MET Virtual Machine and launched FTK Imager Lite to gather examine and process cell phone images. (see Figure 1-6).

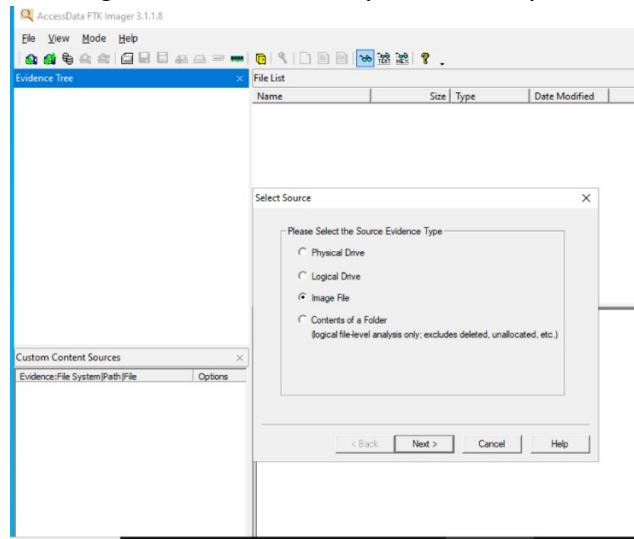


Figure 1. Launching FTK Imager Lite Selecting an Image File

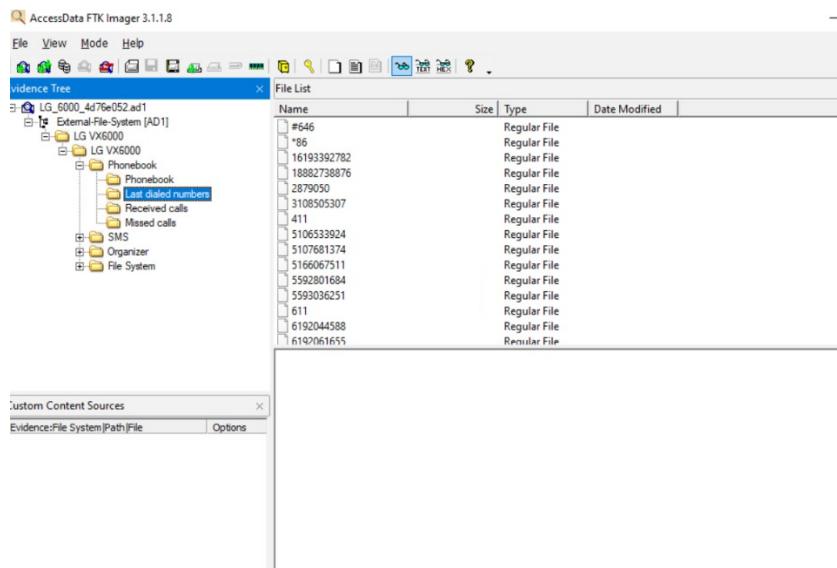


Figure 2. Phonebook Folder-Last Dialed Numbers

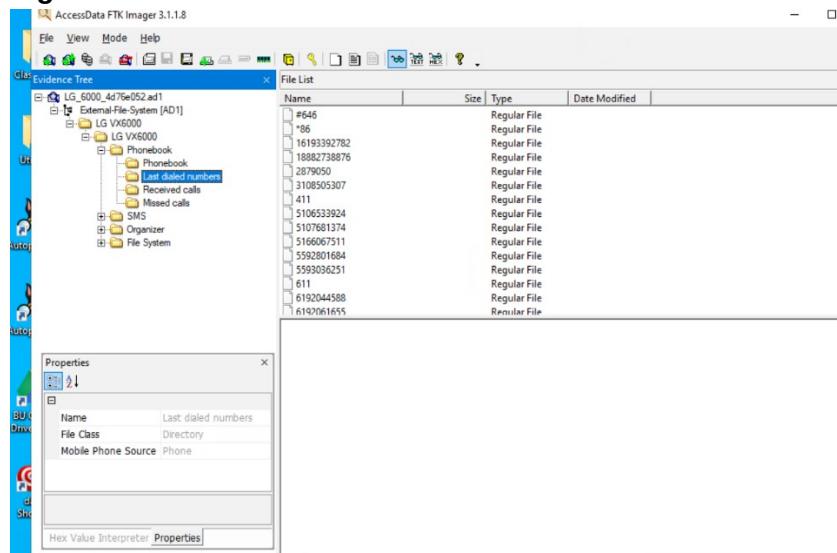


Figure 3. Last Dialed Numbers Continued

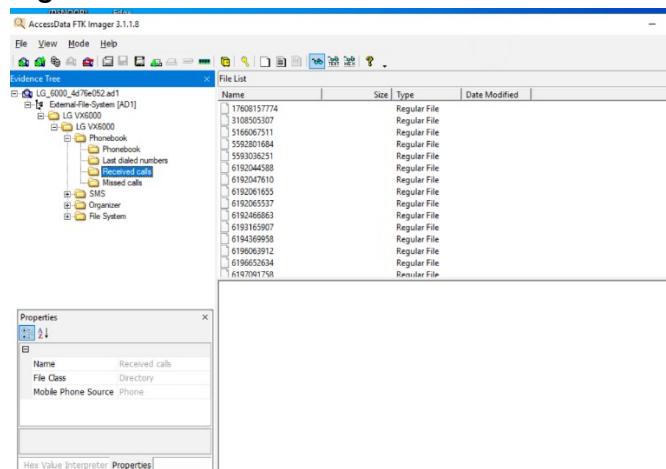
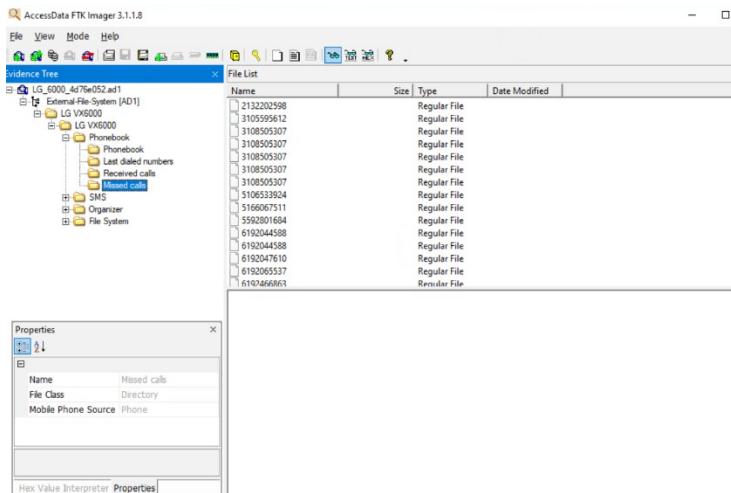
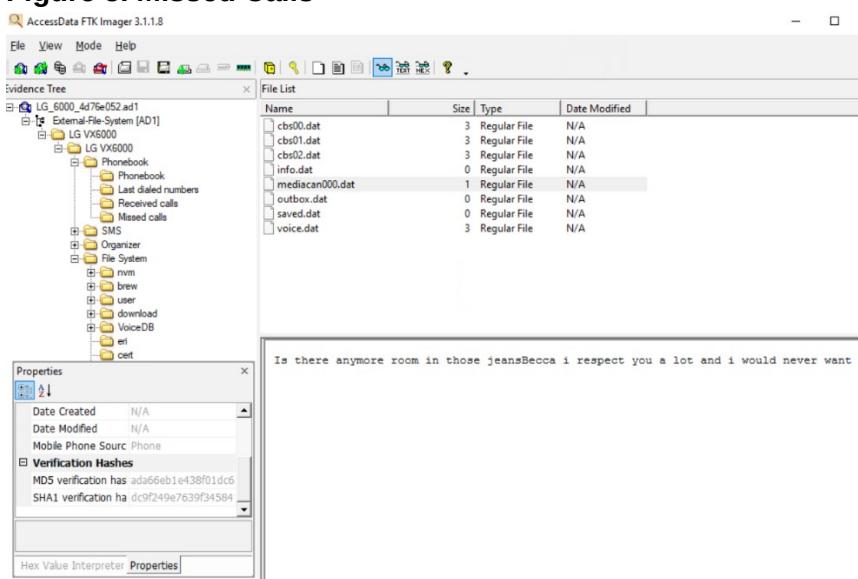


Figure 4. Received Calls

**Figure 5. Missed Calls****Figure 6. mediacan000.dat File Recovered MD5 and SHA1 Verification Hashes**

Remember that hash Verification could not be revealed in Autopsy? Well, FTK Imager Lite provides Hash Verification for the images so using Autopsy 4.3.0 combined with FTK Imager Lite to reveal all evidence would be best to utilize in a case. Next, I have recovered more images in FTK Imager Lite under the folder file mediacan000.dat. Below are some of the images retrieved.

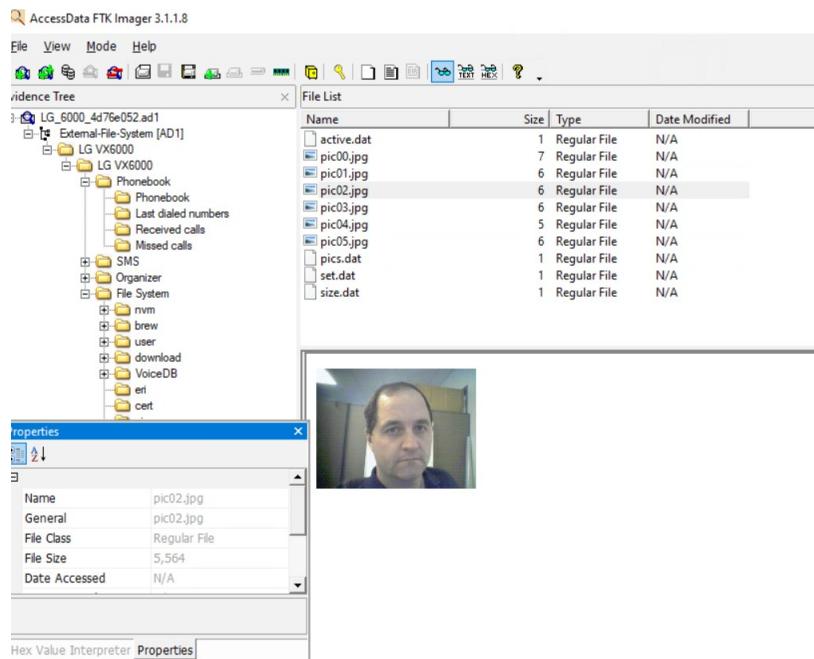


Figure 1. Pic02.jpg Image retrieved

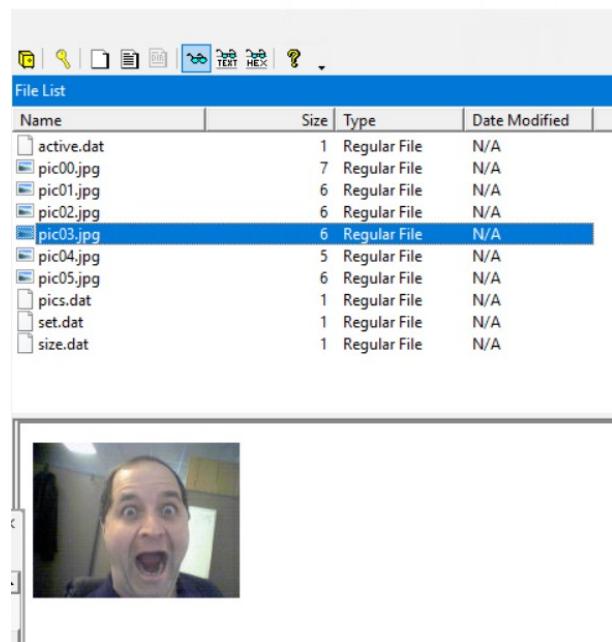


Figure 2. Pic03.jpg Image Recovered

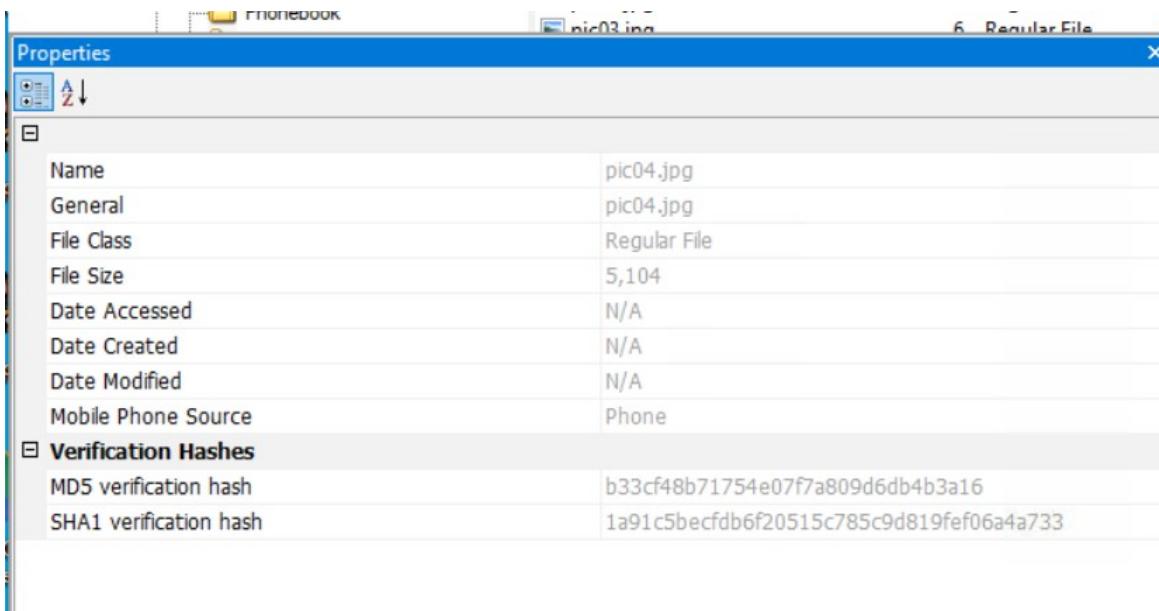


Figure 3. MD5 and SHA1 Hash Verifications for Pic04.jpg Image

The screenshot shows the AccessData FTK Imager interface. The top menu includes 'File', 'View', 'Mode', and 'Help'. The toolbar contains various forensic tools like file recovery, file list, and hex editor. The left pane shows the 'Evidence Tree' with a folder structure: 'LG_6000_4d76e052.ad1' containing 'External-File-System [AD1]' which further contains 'LG VX6000' and 'LG VX6000' (repeated). The right pane shows the 'File List' table:

Name	Size	Type	Date
active.dat	1	Regular File	N/A
pic00.jpg	7	Regular File	N/A
pic01.jpg	6	Regular File	N/A
pic02.jpg	6	Regular File	N/A
pic03.jpg	6	Regular File	N/A
pic04.jpg	5	Regular File	N/A
pic05.jpg	6	Regular File	N/A
pics.dat	1	Regular File	N/A
set.dat	1	Regular File	N/A
size.dat	1	Regular File	N/A

The bottom pane displays the recovered image 'pic05.jpg', which is a portrait of a man with short hair and a dark shirt.

Figure 4. Pic05.jpg Recovered with MD5 and SHA1 Hash Verifications

12.2.3 Lab 12.2 Review Questions

1. How many phone numbers with a valid number of digits were dialed on this phone?

28

2. How many received calls couldn't be identified?

6

3. FTK Imager Lite can be used to determine outgoing call dates and times on cell phones.
True or False?

False

4. How many photos were taken by this phone's camera?

6

5. How many dialed calls were local numbers, not long distance?

24

Lab 12.3 Using Autopsy to Search Cloud Backups of Mobile Devices

12.3.1 Lab 12.3 Executive Summary

For the first lab using Windows, I downloaded the files InCh12Randall.exe and InCh12Sarah.exe from the classroom Google Drive to use with Autopsy 4.3.0 software in the MET Virtual Lab.

12.3.2 Lab 12.3 Activity

For this lab I logged onto the MET Virtual Lab and ran the Autopsy 4.3.0. Software. The objective of this activity was to search cloud backups and evidence linked between multiple images in Autopsy (Cengage,2019). The same process at the previous lab is used to create a new case and extract files as the data source from the Google Drive provided through this course so I won't repeat the process and provide the same images. Moreover, the following images displayed are images produced with Autopsy 4.3.0. revealing the names of both users, email artifacts, email addresses and details of the messages (see Figures 1-8).

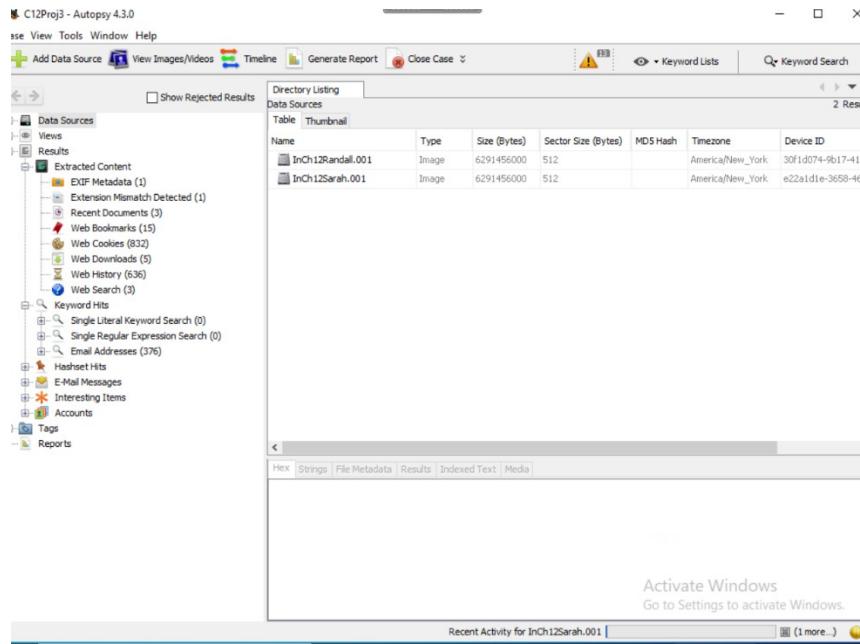


Figure 1. Extracted Content for Data Source Files InCh12Randall.001 Image and InCh12Sarah.001 Image files.

Name	Location	Modified Time	Change
Last Session	/img_InCh12Randall.001/Users/Randall/AppData/Local/Go...	2014-08-09 14:21:33 EDT	2014-08-11 20:10:34 EDT
E-Mail Messages Artifact	/img_InCh12Randall.001/Users/Randall/AppData/Roaming/...	2014-08-11 20:20:10 EDT	2014-08-11 20:20:10 EDT
Sent-1	/img_InCh12Randall.001/Users/Randall/AppData/Roaming/...	2014-08-11 20:10:34 EDT	2014-08-11 20:10:34 EDT
E-Mail Messages Artifact	/img_InCh12Sarah.001/Users/Sarah/AppData/Roaming/Th...	2014-08-09 23:38:00 EDT	2014-08-11 20:20:10 EDT
E-Mail Messages Artifact	/img_InCh12Randall.001/Users/Randall/AppData/Roaming/...	2014-08-11 20:20:10 EDT	2014-08-11 20:20:10 EDT
E-Mail Messages Artifact	/img_InCh12Sarah.001/Users/Sarah/AppData/Roaming/Th...	2014-08-10 18:36:10 EDT	2014-08-11 20:20:10 EDT
Sent Mail	/img_InCh12Sarah.001/Users/Sarah/AppData/Roaming/Th...	2014-08-09 23:38:00 EDT	2014-08-11 20:20:10 EDT
E-Mail Messages Artifact	/img_InCh12Randall.001/Users/Randall/AppData/Roaming/...	2014-08-11 20:10:34 EDT	2014-08-11 20:10:34 EDT
Trash	/img_InCh12Randall.001/Users/Randall/AppData/Roaming/...	2014-08-11 20:20:10 EDT	2014-08-11 20:20:10 EDT
E-Mail Messages Artifact	/img_InCh12Randall.001/Users/Randall/AppData/Roaming/...	2014-08-11 20:18:31 EDT	2014-08-11 20:18:31 EDT
E-Mail Messages Artifact	/img_InCh12Randall.001/Users/Randall/AppData/Roaming/...	2014-08-11 20:10:34 EDT	2014-08-11 20:10:34 EDT
INBOX	/img_InCh12Sarah.001/Users/Sarah/AppData/Roaming/Th...	2014-08-10 18:36:10 EDT	2014-08-11 20:20:10 EDT
E-Mail Messages Artifact	/img_InCh12Sarah.001/Users/Sarah/AppData/Roaming/Th...	2014-08-10 18:36:10 EDT	2014-08-11 20:20:10 EDT
E-Mail Messages Artifact	/img_InCh12Sarah.001/Users/Sarah/AppData/Roaming/Th...	2014-08-09 23:38:00 EDT	2014-08-11 20:20:10 EDT
E-Mail Messages Artifact	/img_InCh12Randall.001/Users/Randall/AppData/Roaming/...	2014-08-11 20:10:34 EDT	2014-08-11 20:10:34 EDT

Figure 2. E-Mail Artifacts

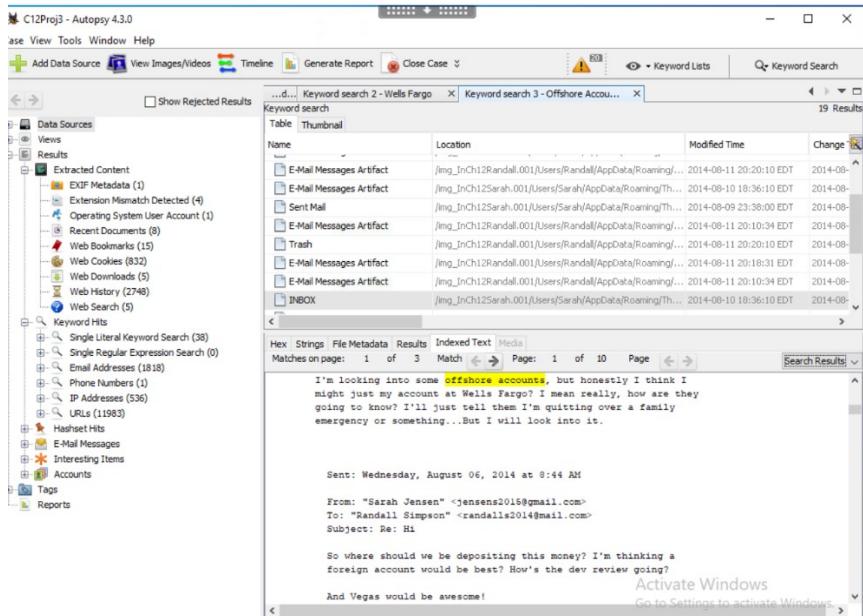


Figure 2. Indexed Text through an Offshore Account Keyword Search Through Data

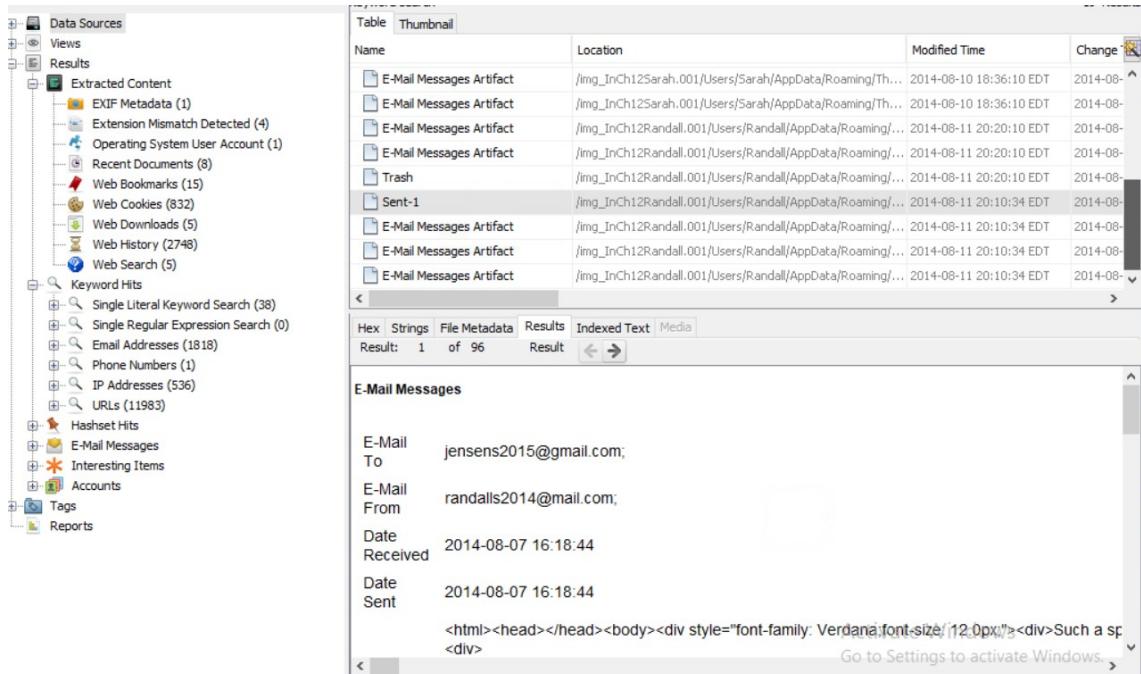


Figure 3. Sent E-Mail Artifact in Results

This E-Mail Message reveals the E-Mail addresses of both parties involved in the investigation. [Jensen2015@gmail.com](mailto:jensens2015@gmail.com) and randalls2014@gmail.com with the dates sent and received.

Name	/img_InCh12Randall.001/Users/Randall/AppData/Roaming/Thunderbird/Profiles/wqf8u2r0.default
Type	File System
MIME Type	application/xhtml+xml
Size	593029
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2014-08-11 20:20:10 EDT
Accessed	2014-08-17 19:24:13 EDT

Activate Windows
Go to Settings to activate Windows.

Figure 4. File Metadata

The screenshot shows the Autopsy 4.3.0 interface with the following details:

- Case View:** C12Proj3 - Autopsy 4.3.0
- Tools:** Add Data Source, View Images/Videos, Timeline, Generate Report, Close Case
- Search:** Keyword search 2 - Wells Fargo, Keyword search 3 - Offshore Account
- Results:** 19 Results
- Table Headers:** Name, Location, Modified Time, Change
- Table Data:**
 - E-Mail Messages Artifact (multiple entries)
 - Trash (multiple entries)
 - Sent-1 (multiple entries)
 - E-Mail Messages Artifact (multiple entries)
 - E-Mail Messages Artifact (multiple entries)
 - E-Mail Messages Artifact (multiple entries)
- Panels:** Hex, Strings, File Metadata, Results, Indexed Text, Media
- Bottom Content:** Raw email message content from Sun, 18 May 2014 14:12:12 -0700 to Sun, 18 May 2014 17:12:24 2014. The message is from Microsoft account team <account-security-noreply@account.microsoft.com> to <randalls2014@mail.com>. It contains X-Mozilla-Status and X-Mozilla-Status2 headers, and various return-path and received lines.

Figure 5. E-Mail Found in Trash providing Hex, Strings, File Metadata, Results, and Indexed Text

The screenshot shows the Autopsy 4.5.0 interface. The top menu bar includes File, View, Tools, Window, Help, Add Data Source, View Images/Videos, Timeline, Generate Report, Close Case, Keyword Lists, and Keyword Search. The main window displays a search interface with two tabs: 'Keyword search' and 'Table'. The 'Table' tab shows a list of results with columns: Name, Location, Modified Time, and Change. The results include various artifacts such as 'Last Session', 'E-Mail Messages Artifact', 'Sent Mail', and multiple entries for 'E-Mail Messages Artifact'. The 'Indexed Text' tab is selected, showing the raw text content of an e-mail message. The text discusses marketing strategy and mentions a phone number: '360-864-2230'. Below the text, there is a watermark: 'Activate Windows Go to Settings to activate Windows.'

Figure 6. Indexed Text E-Mail

This screenshot shows the same Autopsy 4.5.0 interface as Figure 6, but with a different search result. The 'Indexed Text' tab is selected, displaying the raw text content of an e-mail message. The text includes a phone number: '360-864-2230'. Below the text, there is a watermark: 'Activate Windows Go to Settings to activate Windows.'

Figure 7. Indexed Text Revealing Phone number

The screenshot shows a digital forensic tool's interface. On the left, a tree view of 'Data Sources' shows various partitions and their contents, including 'InCh12Randall.001' and 'InCh12Sarah.001'. The main area displays a 'Directory Listing' table with columns: Name, Location, Modified Time, and Change. The table lists several items, including 'Last Session', 'E-Mail Messages Artifact', and 'Sent-1'. Below the table, a preview pane shows an email message from 'Sarah Jensen' to 'Randall Simpson' dated August 6, 2014. The email body contains text about Wells Fargo and a transfer of money.

Name	Location	Modified Time	Change
Last Session	/img_InCh12Randall.001/Users/Randall/AppData/Local/Go...	2014-08-09 14:21:33 EDT	2014-08
E-Mail Messages Artifact	/img_InCh12Randall.001/Users/Randall/AppData/Roaming/...	2014-08-11 20:20:10 EDT	2014-08
Sent-1	/img_InCh12Randall.001/Users/Randall/AppData/Roaming/...	2014-08-11 20:10:34 EDT	2014-08
E-Mail Messages Artifact	/img_InCh12Randall.001/Users/Sarah/AppData/Roaming/Th...	2014-08-09 23:38:00 EDT	2014-08
E-Mail Messages Artifact	/img_InCh12Randall.001/Users/Sarah/AppData/Roaming/Th...	2014-08-11 20:20:10 EDT	2014-08
E-Mail Messages Artifact	/img_InCh12Sarah.001/Users/Sarah/AppData/Roaming/Th...	2014-08-10 18:36:10 EDT	2014-08
Sent Mail	/img_InCh12Sarah.001/Users/Sarah/AppData/Roaming/Th...	2014-08-09 23:36:00 EDT	2014-08
E-Mail Messages Artifact	/img_InCh12Randall.001/Users/Randall/AppData/Roaming/Th...	2014-08-11 20:10:34 EDT	2014-08
Trash	/img_InCh12Randall.001/Users/Randall/AppData/Roaming/Th...	2014-08-11 20:20:10 EDT	2014-08

Figure 8. Wells Fargo Bank Revealed with detailed E-mail that also provides the names of the users for each E-Mail which are Sarah Jensen and Randall Simpson

All the evidence acquired reveals the identities of both parties involved in a transfer of \$300,000 dollars from Randall Simpson to Sarah Jensen. The recovered phone number is revealed along with 225 E-Mails involved in the case. Sarah carried another conversation with a third party describing her intent to get 300k from her boss for a work-related project in which her E-Mails show intent to walk away with the money and project idea. All the evidence are provided in the figures 1-8 listed above.

12.3.3 Lab 12.3 Review Questions

- How much money did Randall Simpson tell Sarah to ask her boss to fund?
\$300K
- What phone number was recovered in the evidence?
360-864-2230
- How many recovered e-mails were in the Default folder?
225

- No photos were recovered on either mobile device. True or False?

True

- Evidence shows that both Randall and Sarah were involved in transferring money. True or False?

True