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

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).

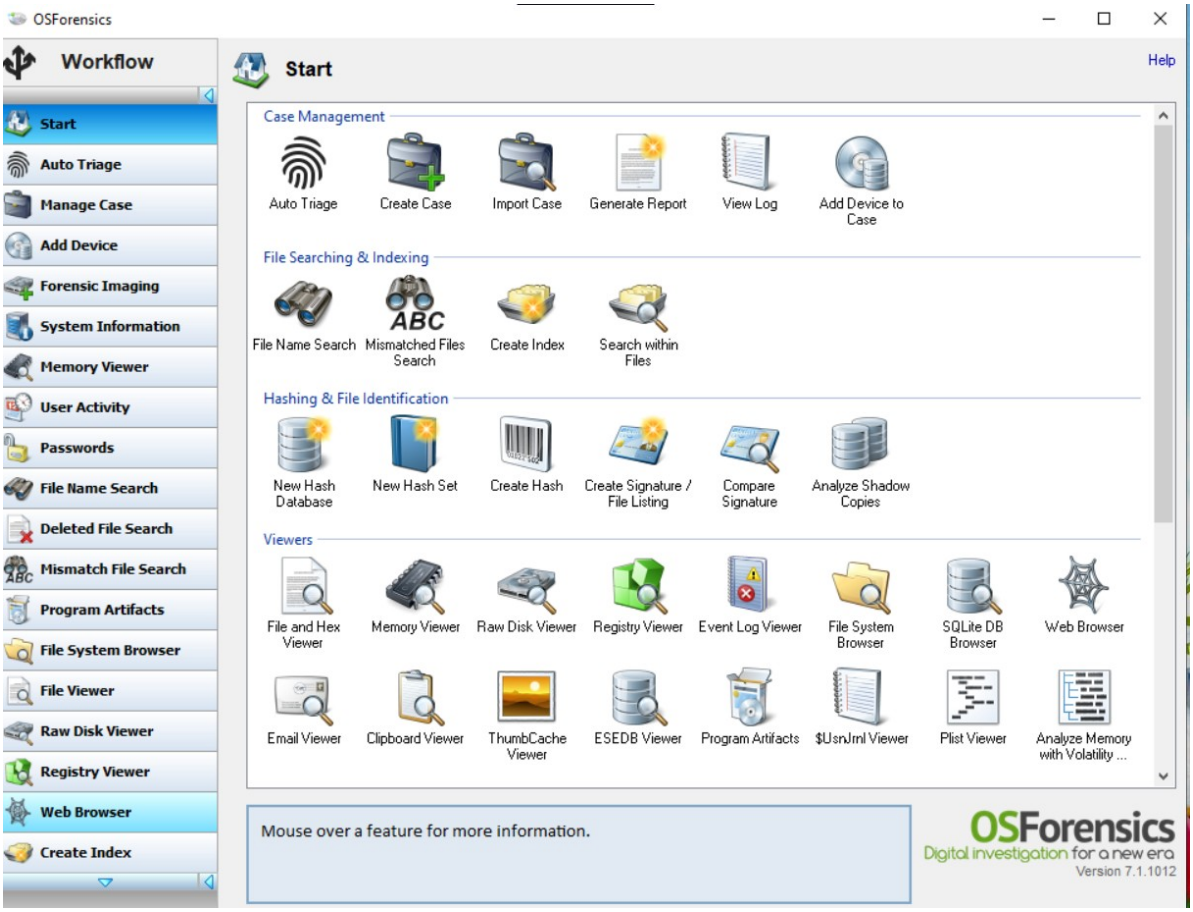

Figure 1. Launching OSForensic Software

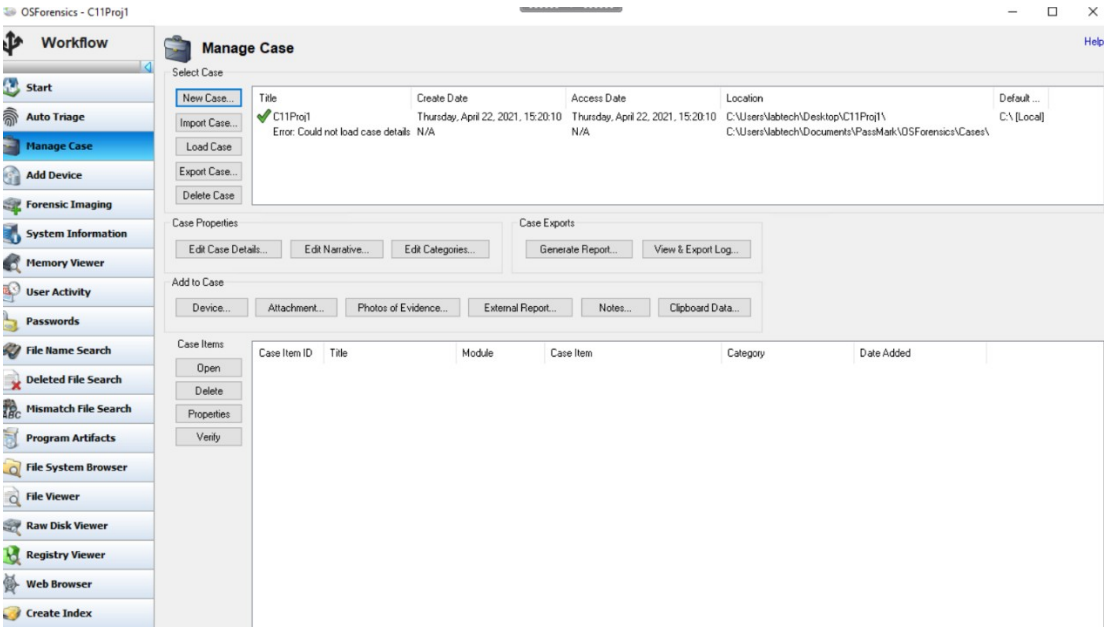

Figure 2. Managing and Creating a New Case

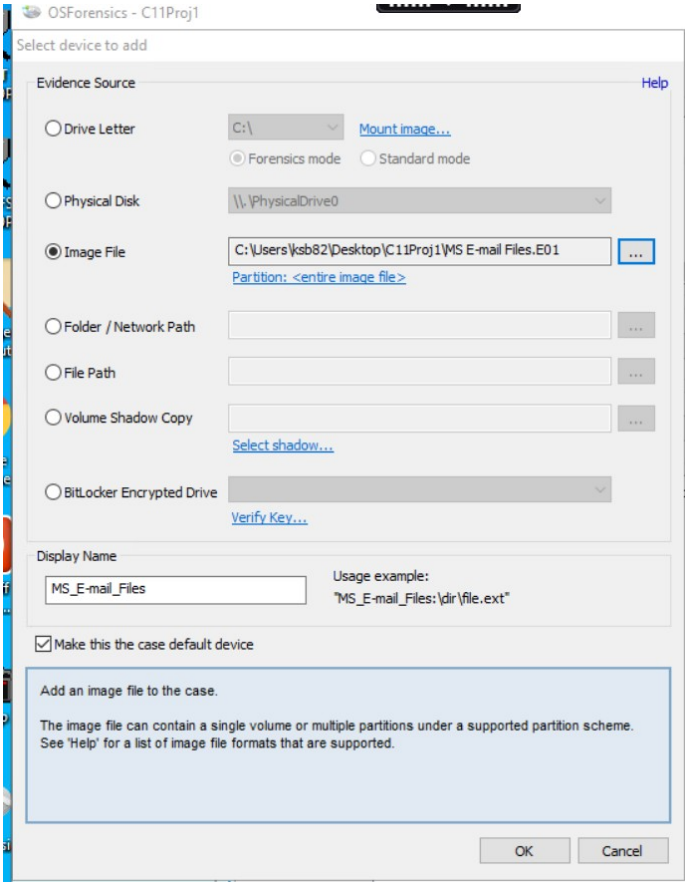

Figure 3. Adding Image File from File Source for Indexing

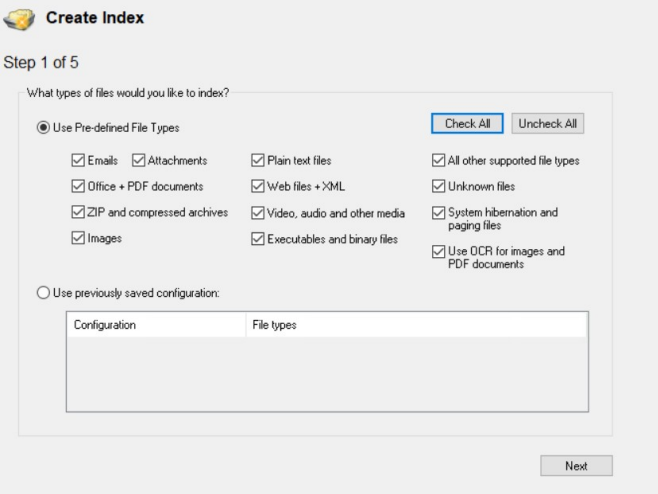

Figure 4. Creating an Index Steps 1-5

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

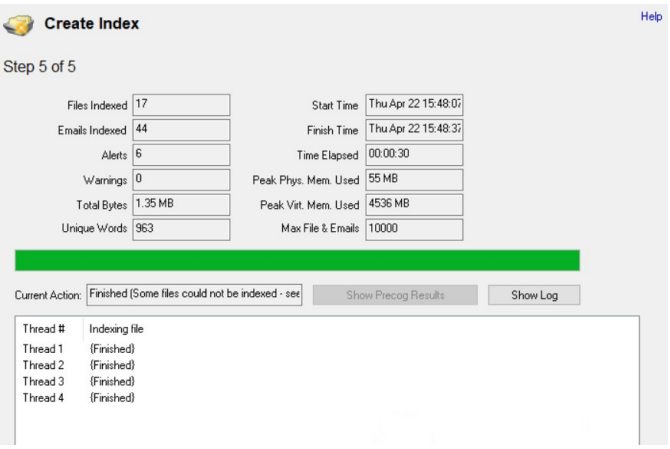

Figure 5. Finalizing Index

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).

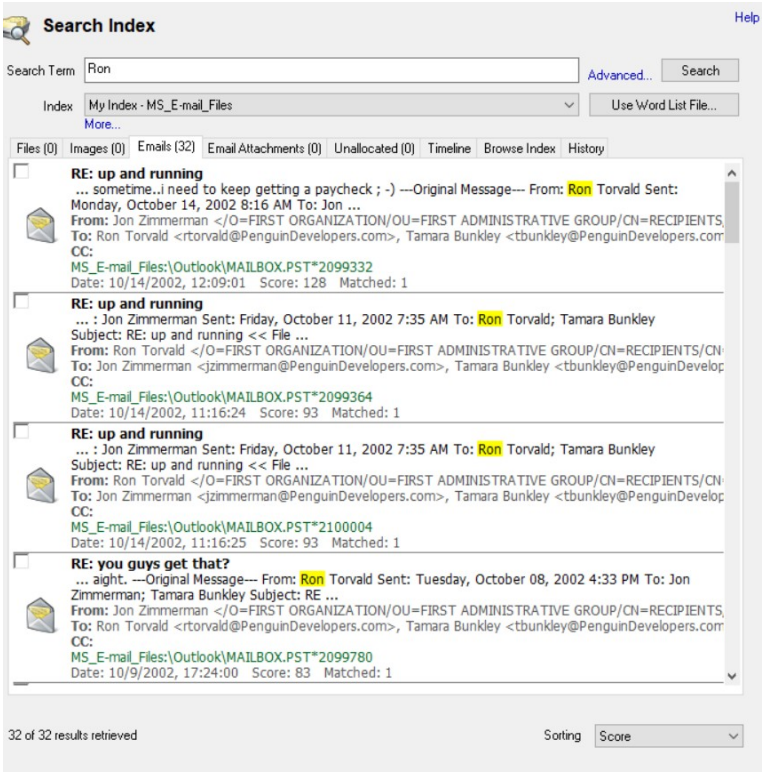

Figure 1. 32 undeleted emails

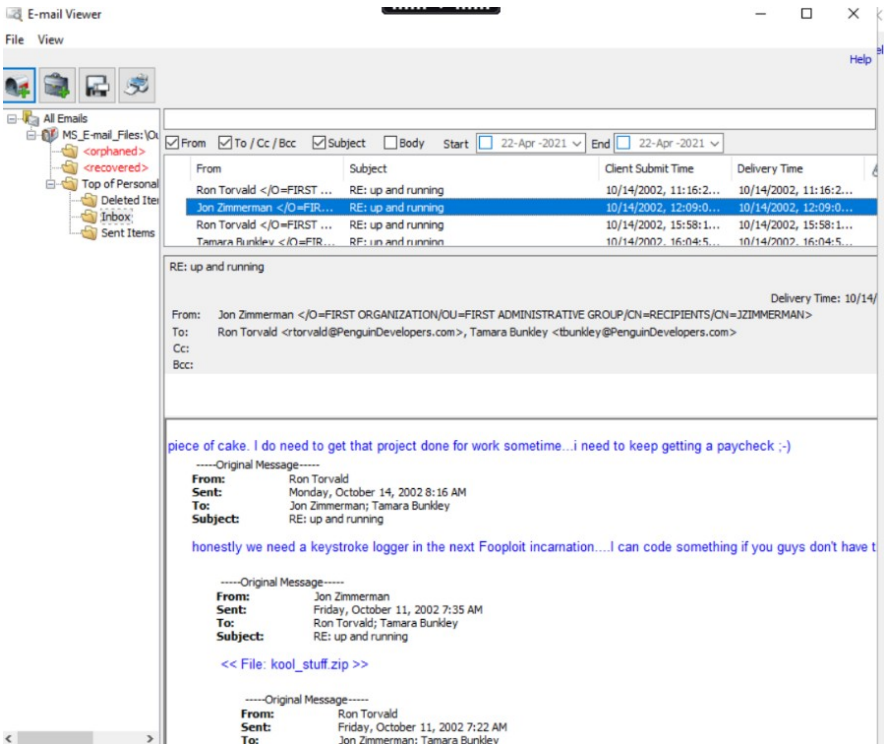

Figure 2. Email Viewer Displaying all emails and their content

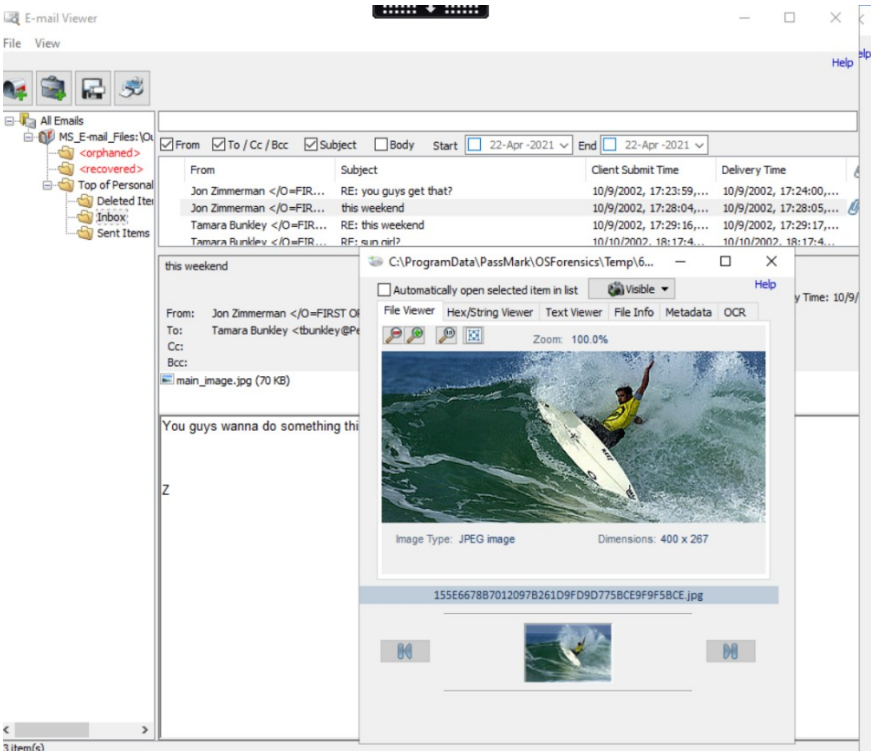

Figure 3. Inbox Emails Attached Photograph

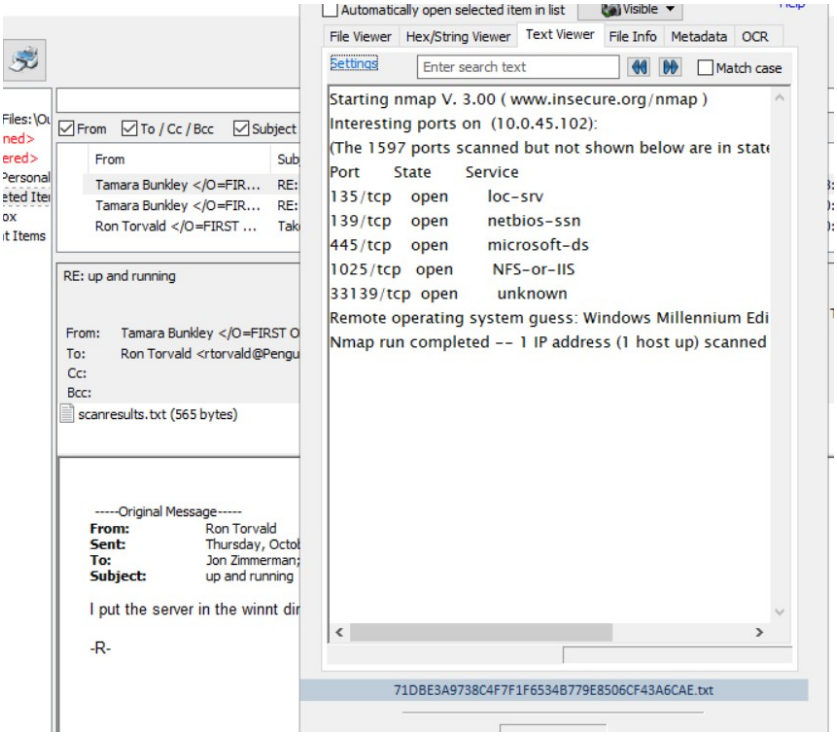

Figure 4. Deleted Items Viewing in Email Viewer of OSForensics Scan Results Txt. Evidence of Installed Software Remote Operating System.

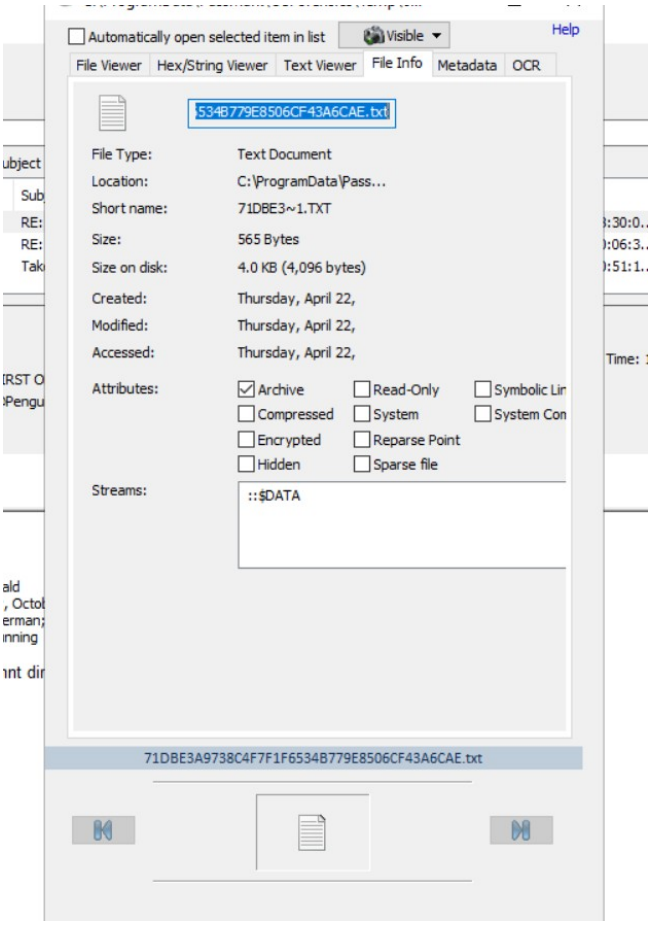

Figure 5. Operating System Size, Date Created, Modified and Accessed

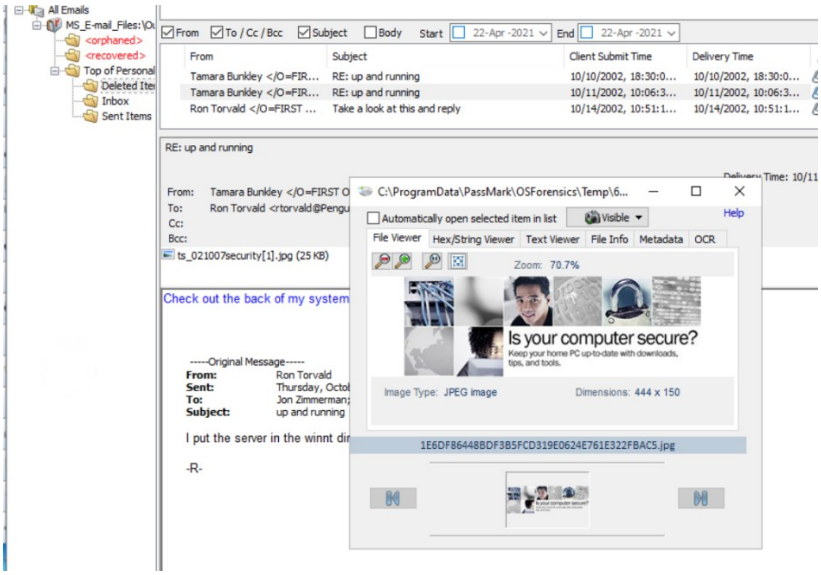

Figure 6. Deleted Program File Image

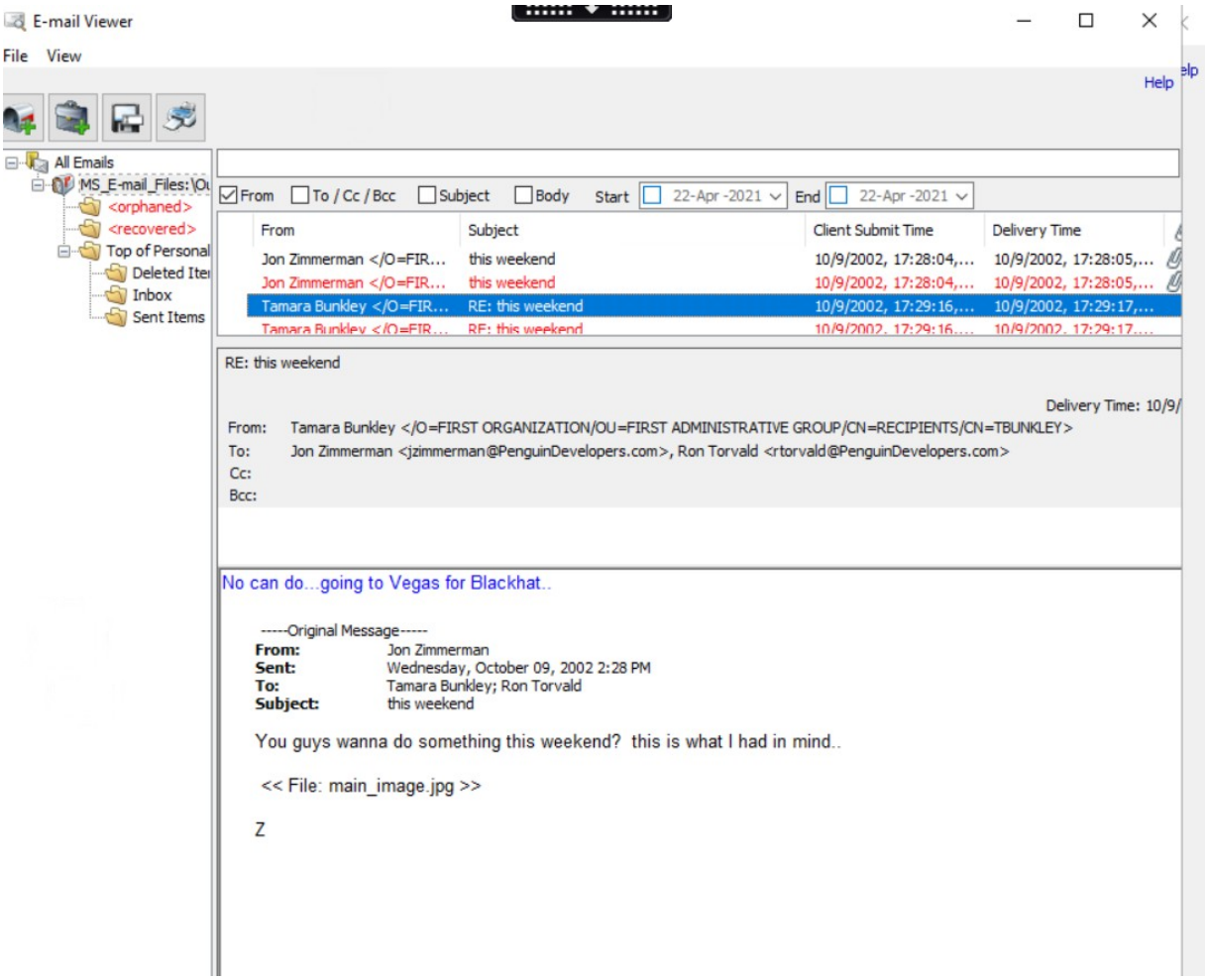

Figure 7. Deleted Email Reply from Tamara Bunkley for Jon Zimmerman and Ron Torvald

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).

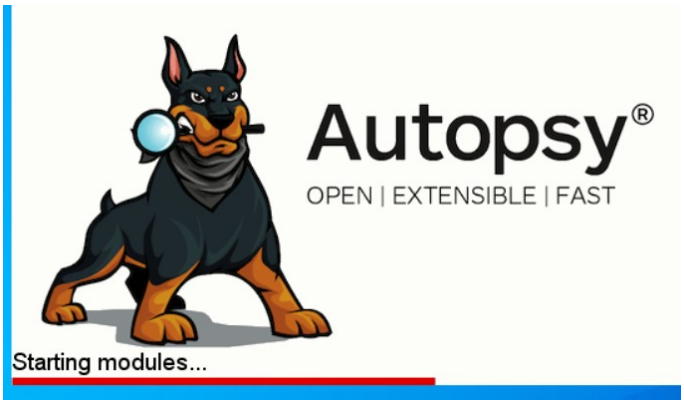

Figure 1. Starting up Autopsy 4.3.0.

Figure 2. Creating a new case with Autopsy 4.3.0.

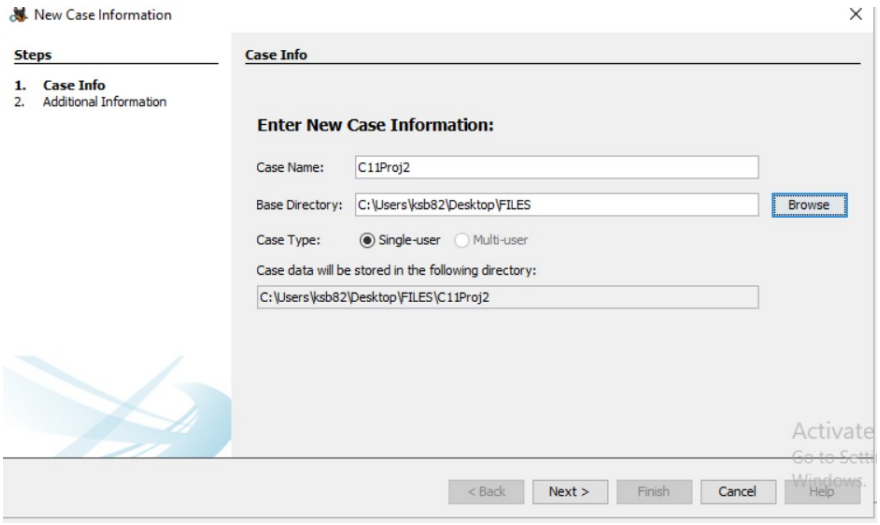

Figure 3. Step 1 Entering and Retrieving New Case Information

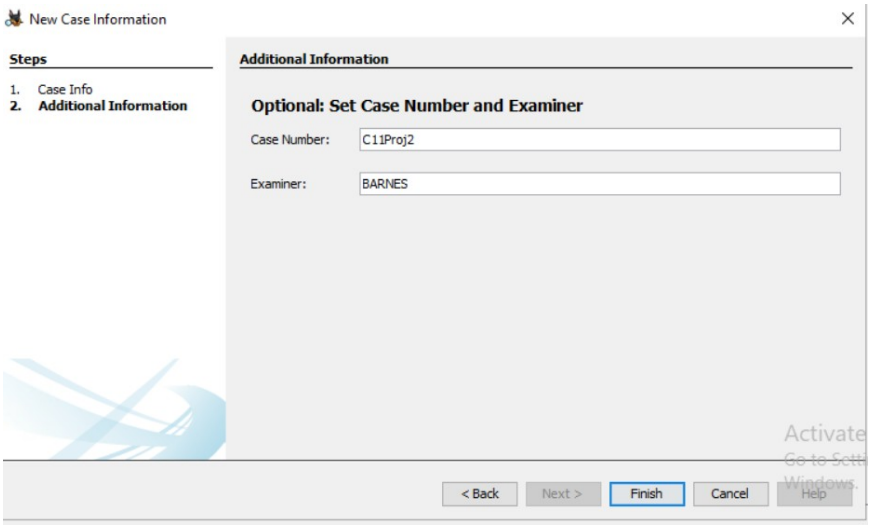

Figure 4. Step 2 Creating a Case Number and Entering Examiner Information

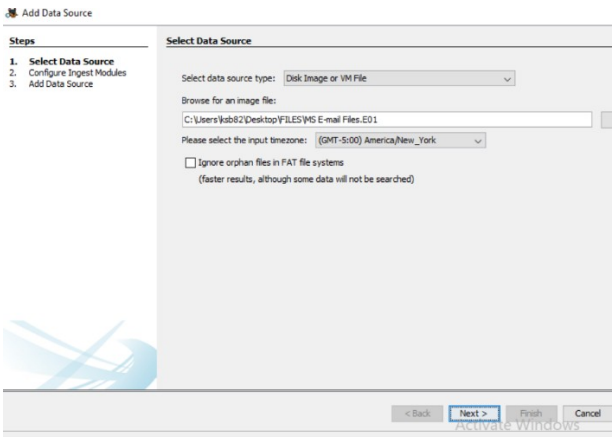

Figure 5. Creating a Data Source

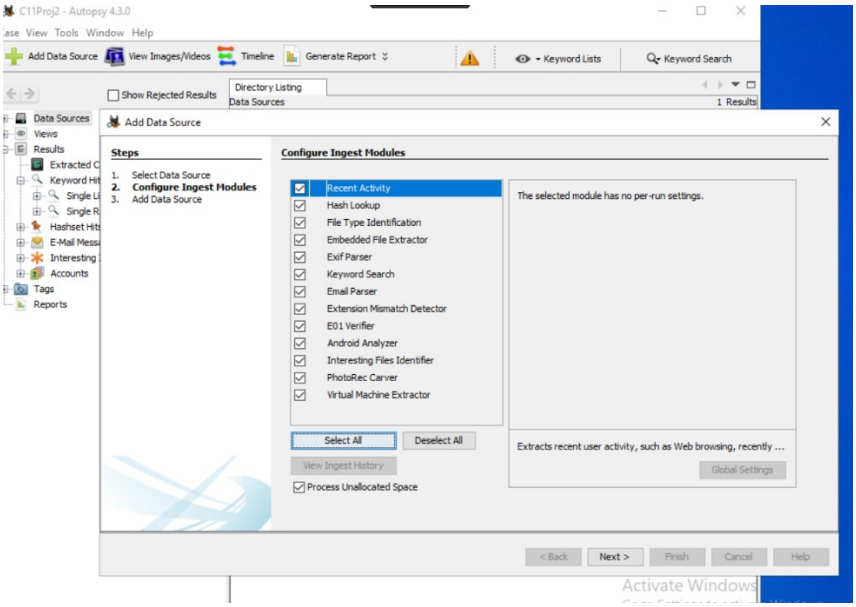

Figure 6. Configuring Ingest Modules

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.

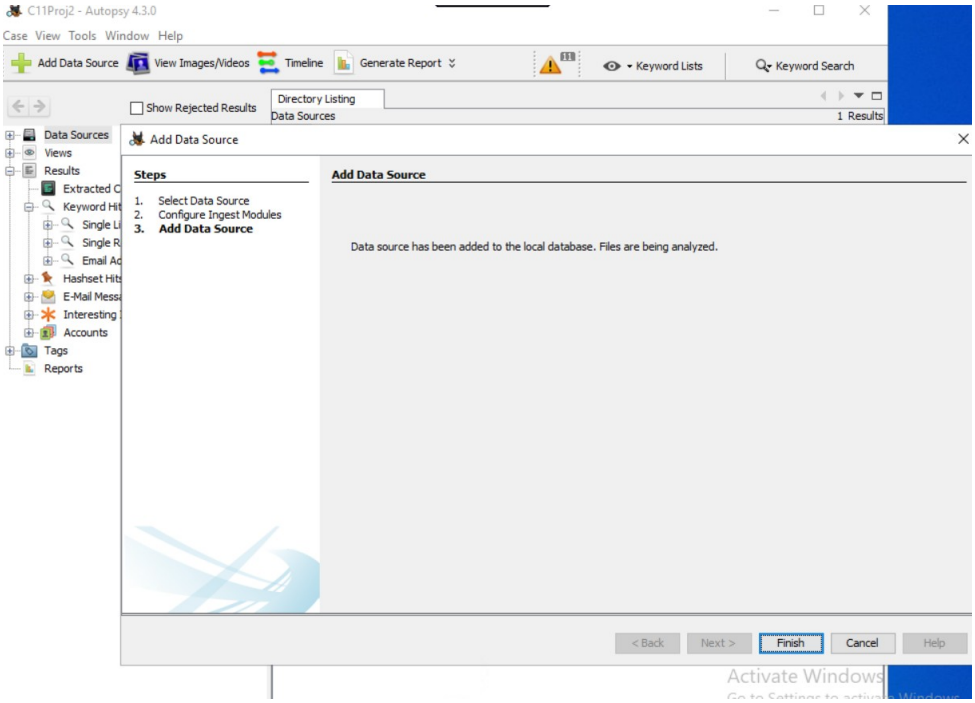

Figure 7. Adding a Data Source

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.

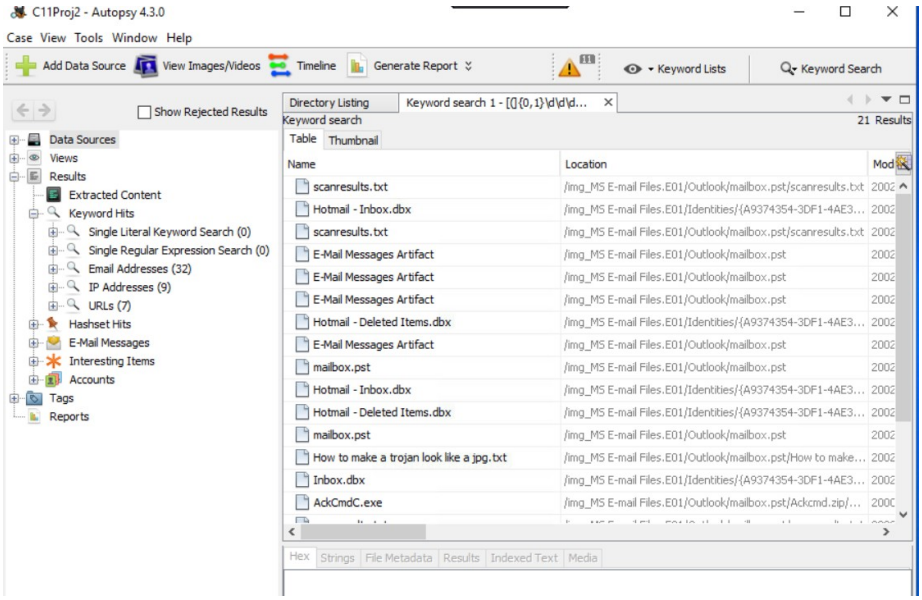

Figure 8. Keyword Search 1 For all Keyword Hits

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.

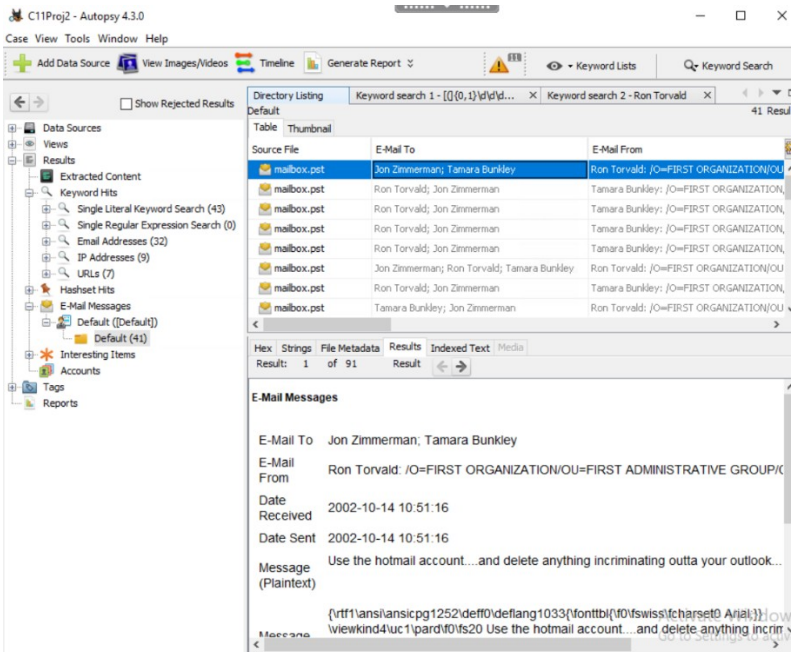

Figure 9. Checking the E-Mail Default Folder Results

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.

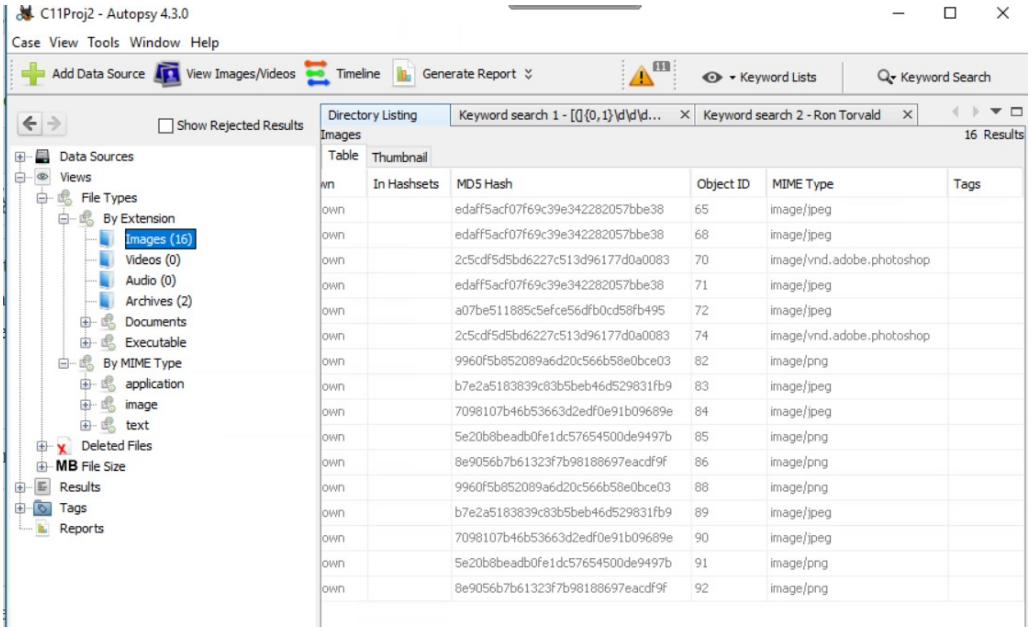

Figure 10. Second Keyword Search Revealing Images, Documents and MD5 Hash Information

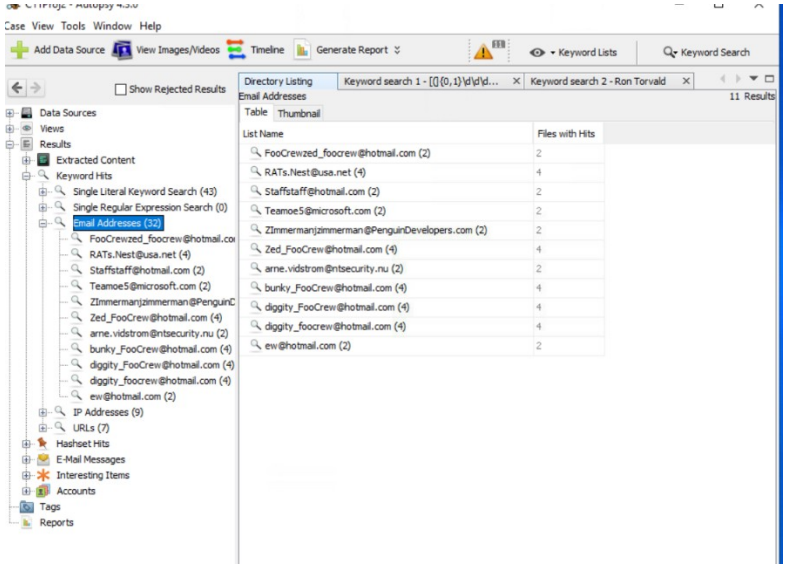

Figure 11. Directory Listing Revealing 32 E-Mail Addresses

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).

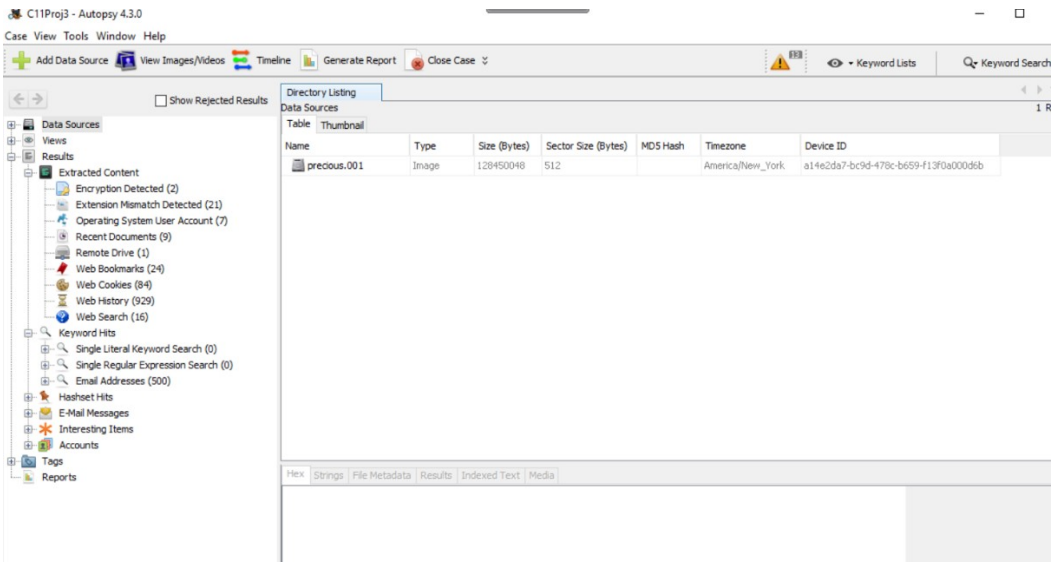

Figure 1. precious.001 File

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.

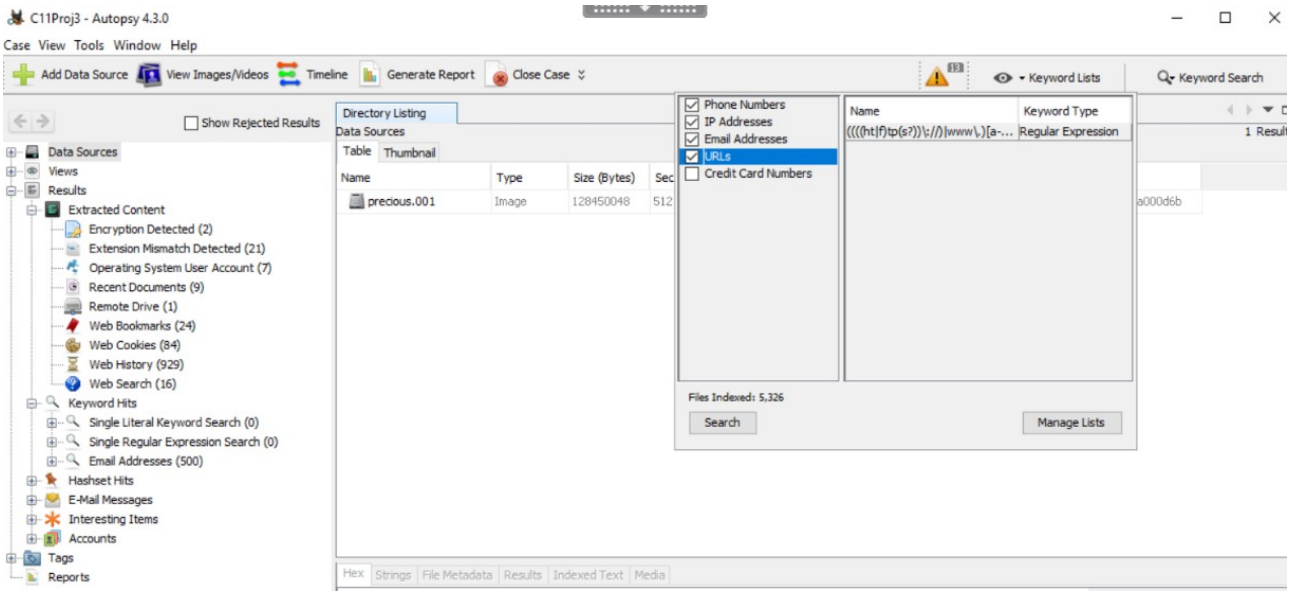

Figure 2. precious.001 File Keyword Search for Phone Numbers, IP Addresses, E-Mail Addresses, and URLs.

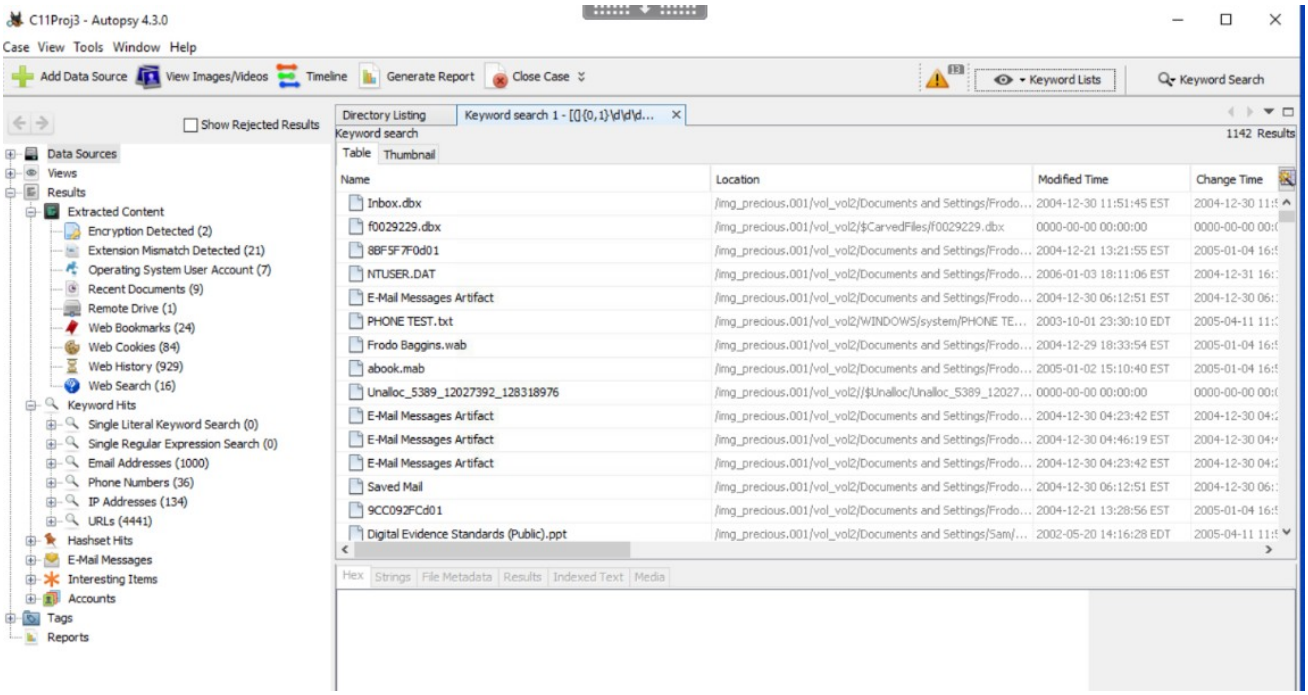

Figure 3. Data Contained in precious.001 File

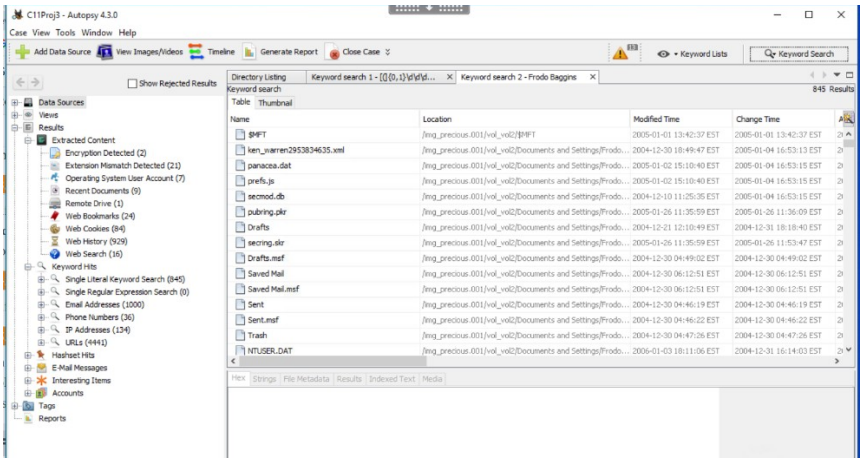

Figure 4. Keyword Search 2 for Frodo Baggins

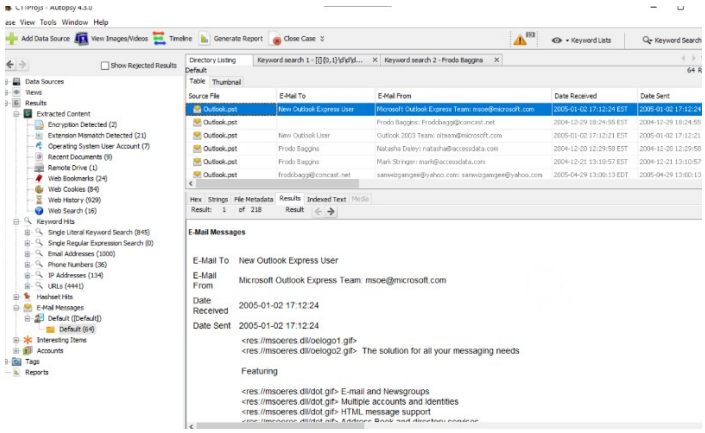

Figure 5. Keyword Search 2 Default Folder Evidence

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

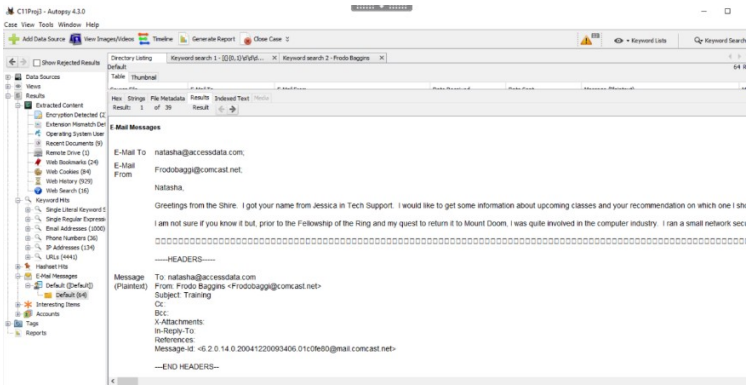

Figure 6. Further E-Mail Evidence with Keyword Search 2

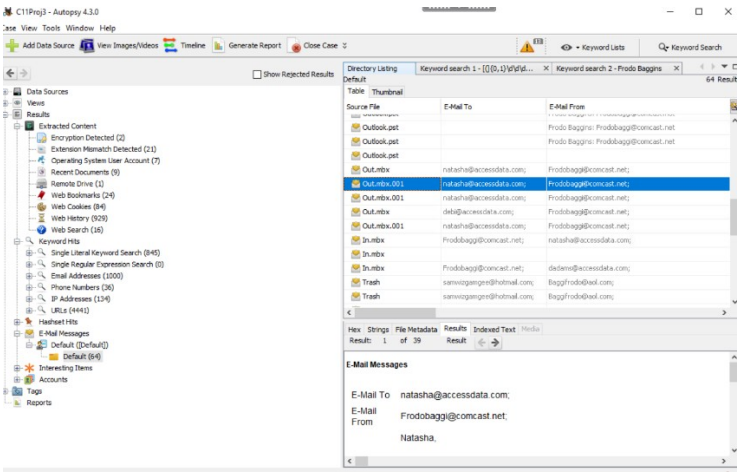

Figure 7. Default E-Mail containing 54 Messages

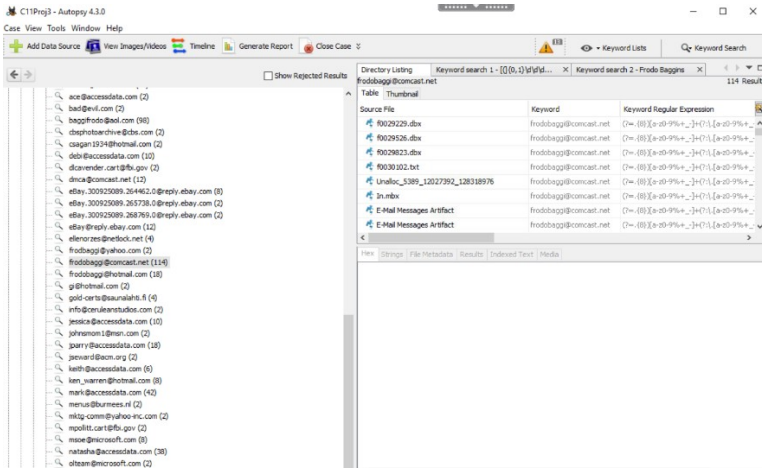

Figure 8. Frodo Baggins name in many different E-Mail addresses and E-Mail Artifacts

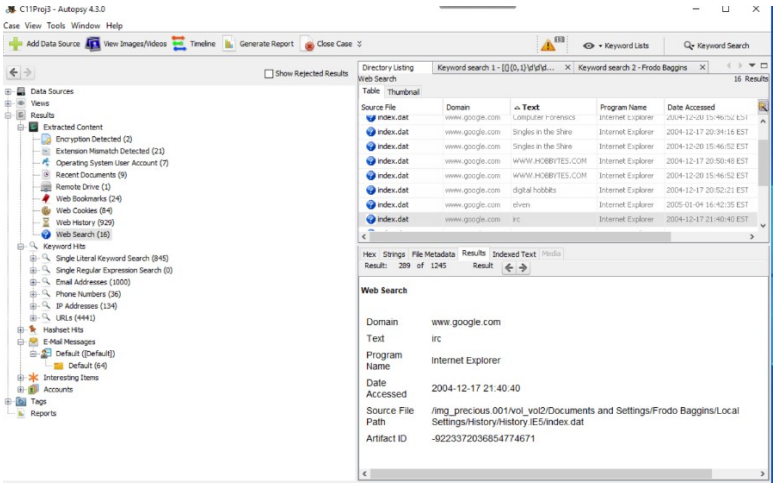

Figure 9. Web Search Containing Hex, Strings, File Metadata, Results, and Indexed Text.

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).

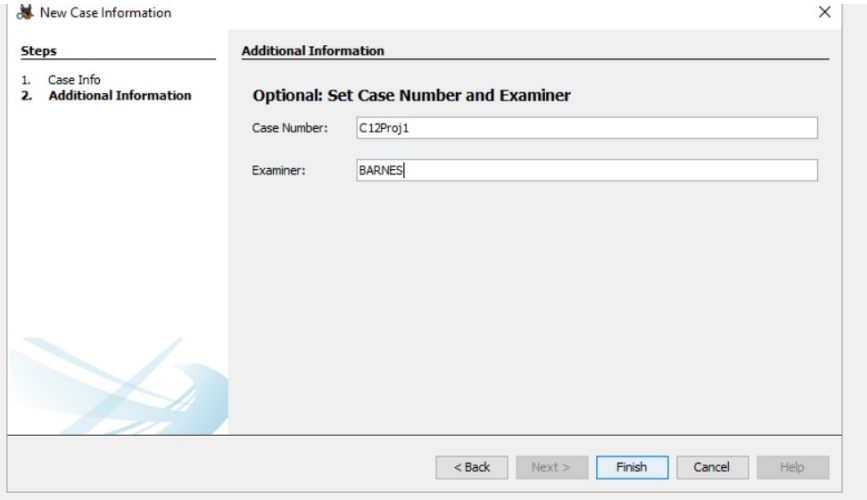

Figure 1. Creating a New Case in Autopsy 4.3.0

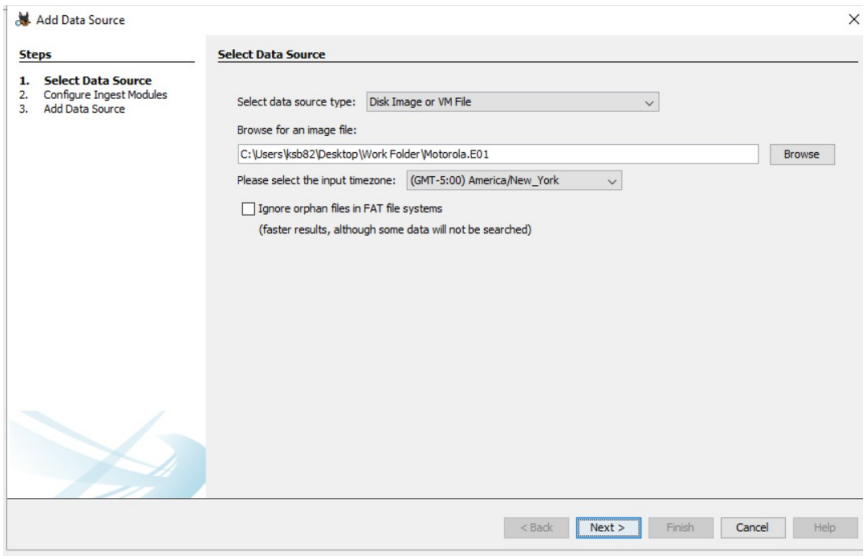

Figure 2. Selecting Data Source for Autopsy 4.3.0.

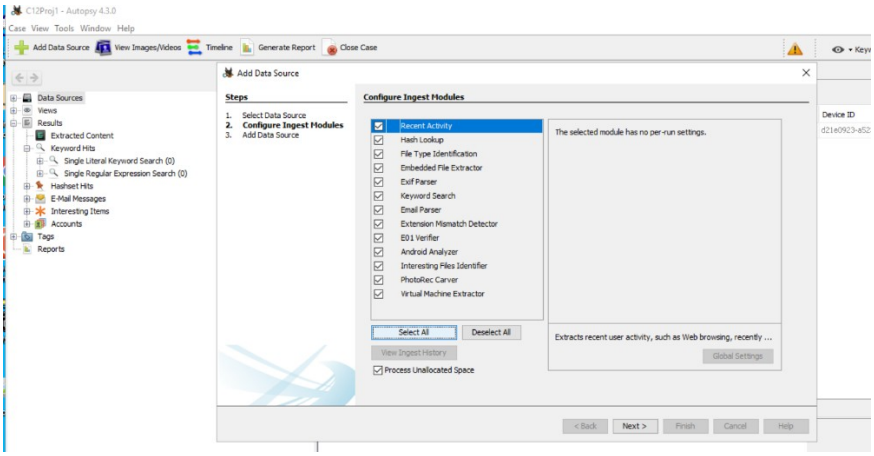

Figure 3. Configuring Ingest Modules

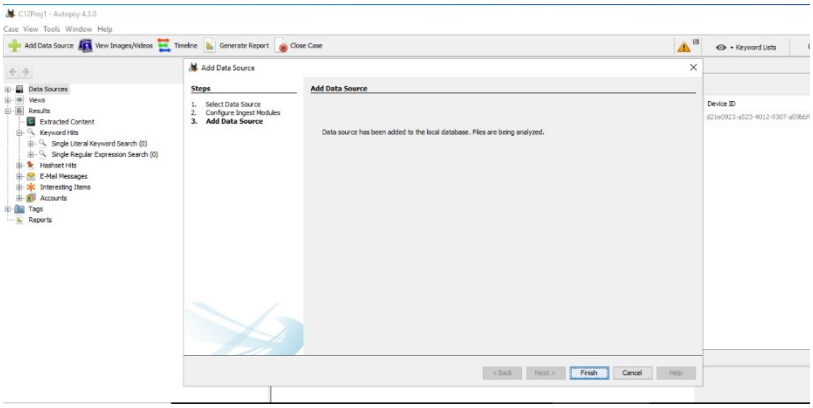

Figure 4. Adding a Data Source which is the file Motorola.E01 (see Figure 5.)

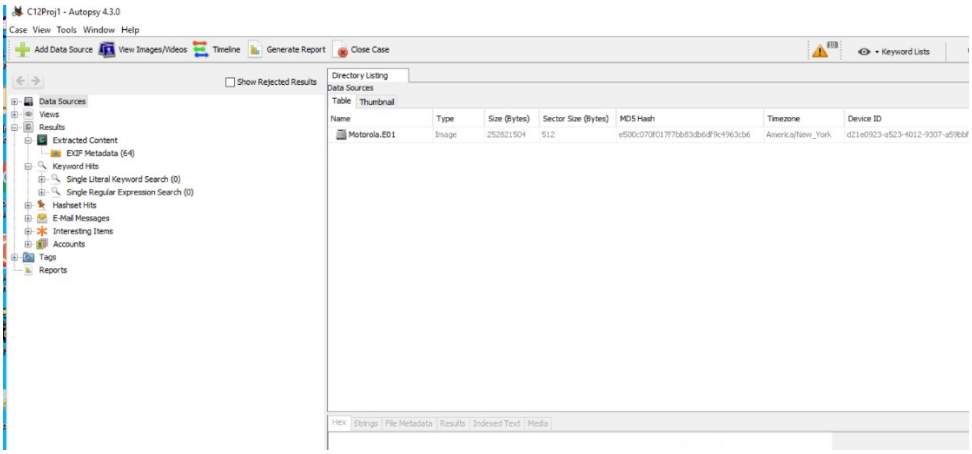

Figure 5. Motorola.E01 File Directory Listing

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

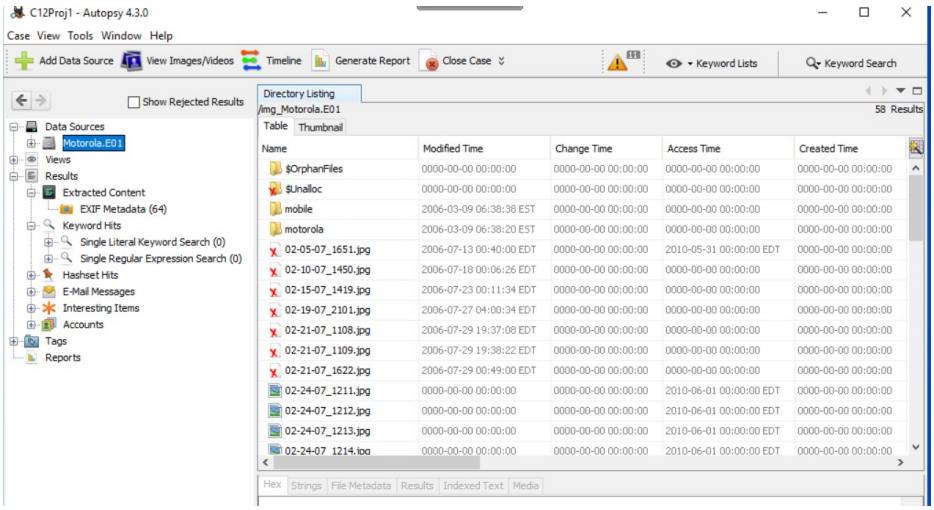

Figure 1. Deleted and Undeleted Files Under Motorola.E01 File Folder the Items that have a Red X Mark are Identified as Deleted Files

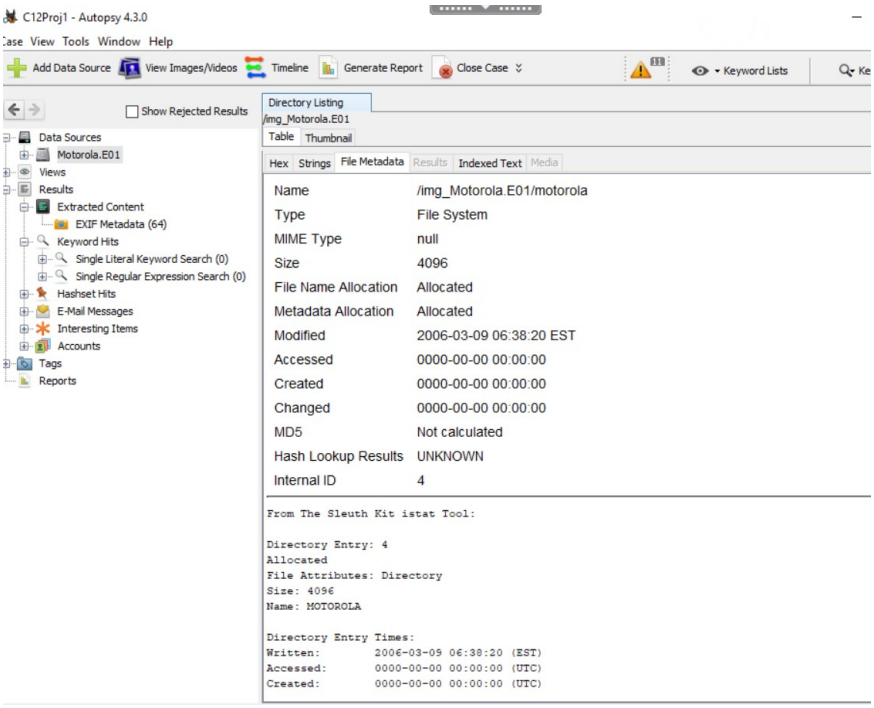

Figure 2. Under Directory Listing File Metadata

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.

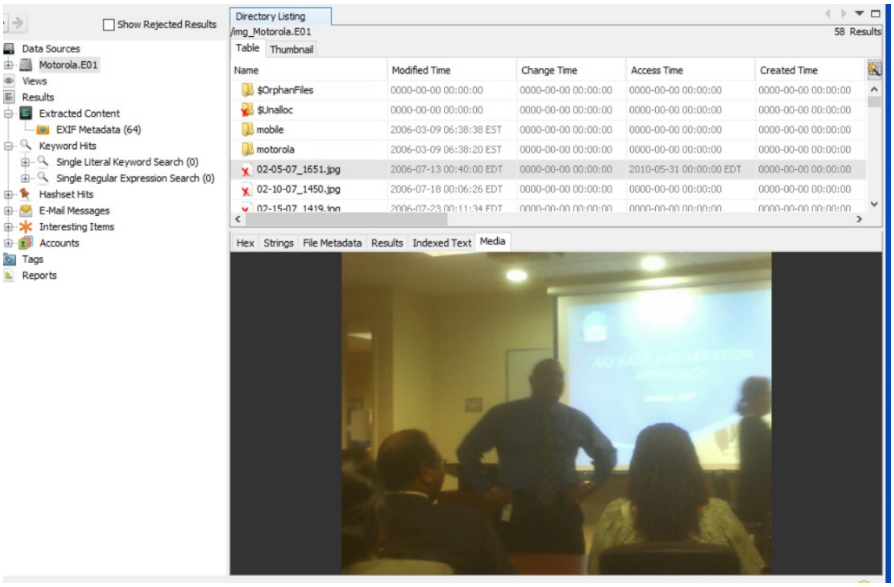

Figure 3. Deleted Image 02-05-07_1651.jpg Retrieved Under Extracted Content and EXIF Metadata which Includes 64 Items Within

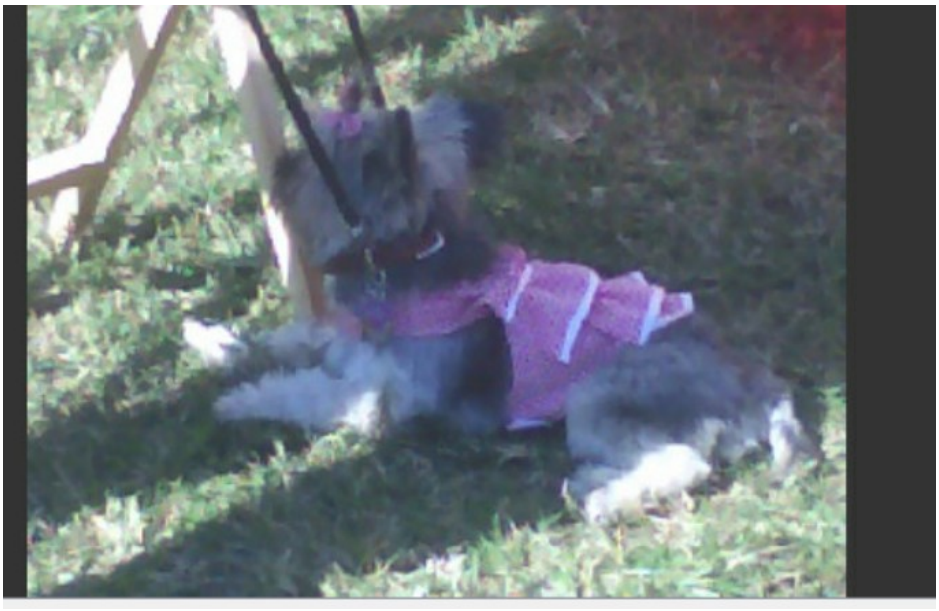

Figure 4. Deleted Image Recovered in the Same Folder

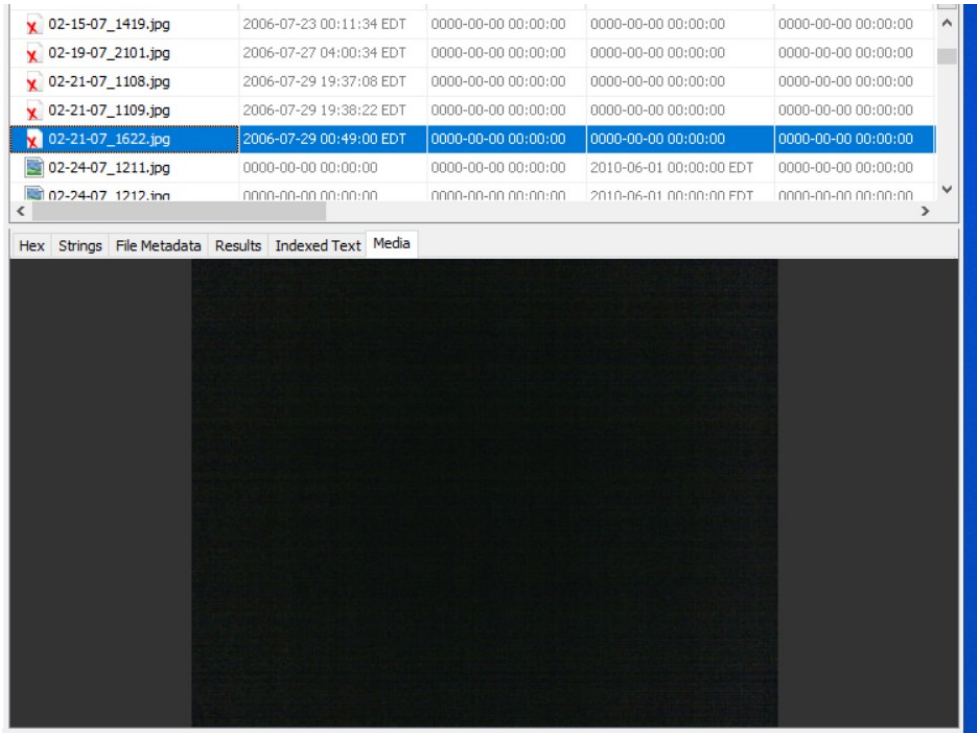

Figure 5. Deleted Image that Could not be Found

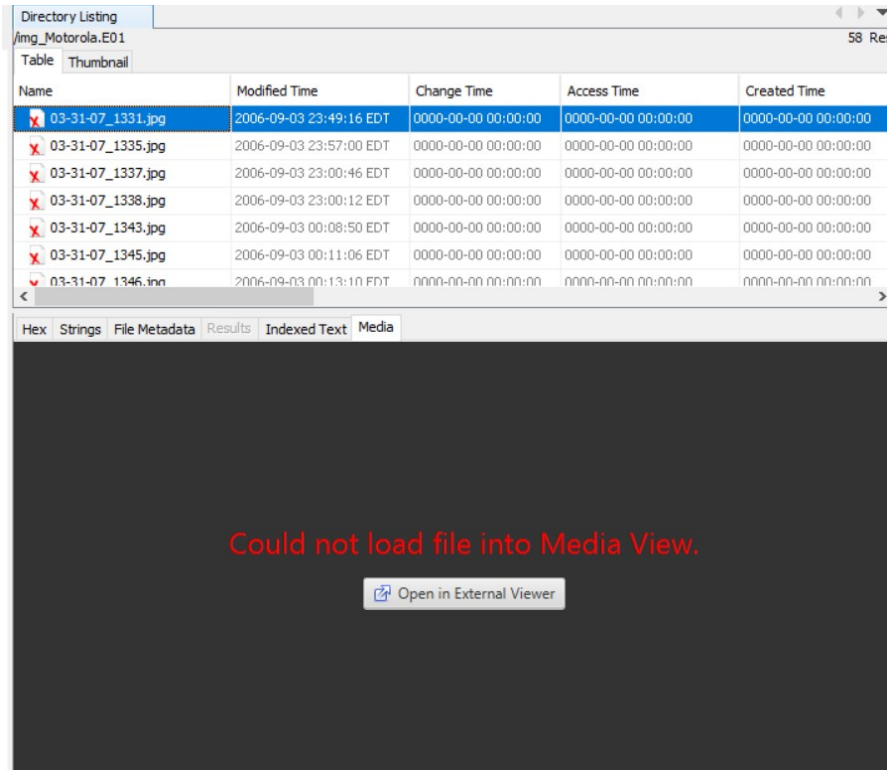

Figure 6. Image Could not be Displayed it Would not Load

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

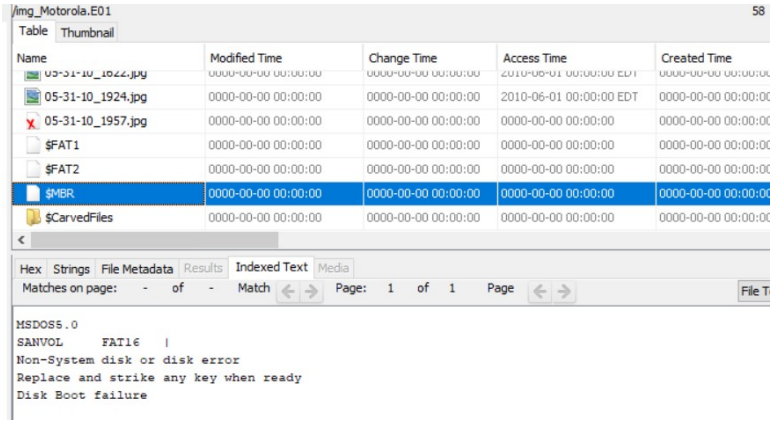

Figure 7. $MBR File Provides Indexed Text Revealing the name of the storage device SANVOL found in FAT16 as a Master Boot Record.

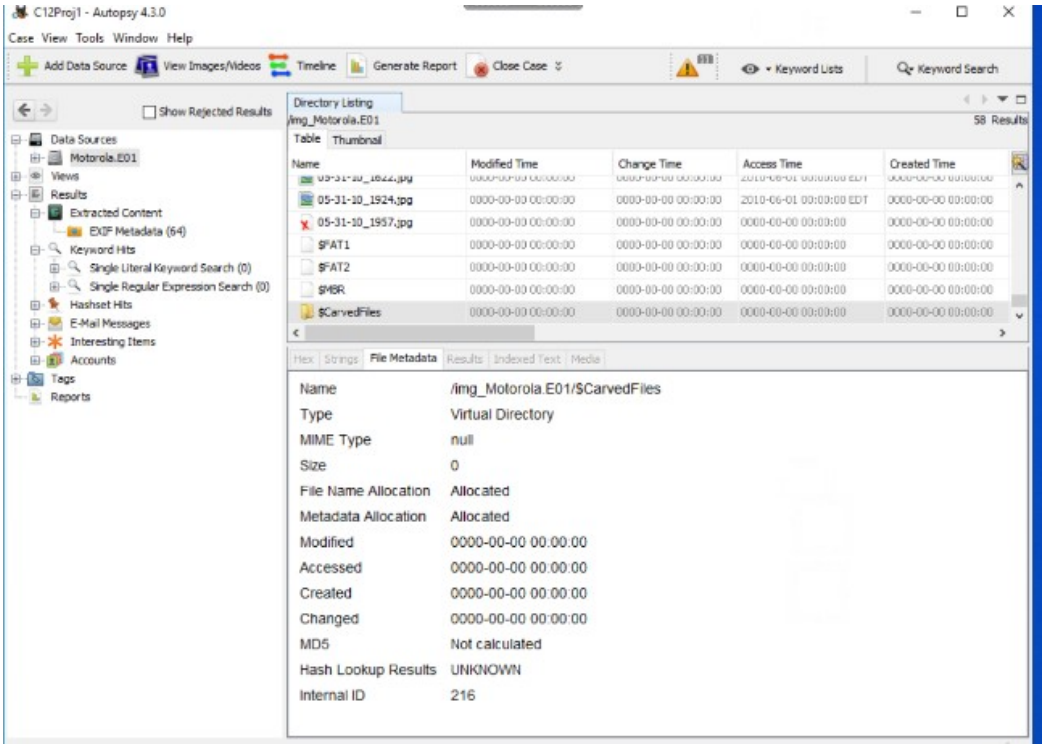

Figure 8. $CarvedFiles Virtual Directory item

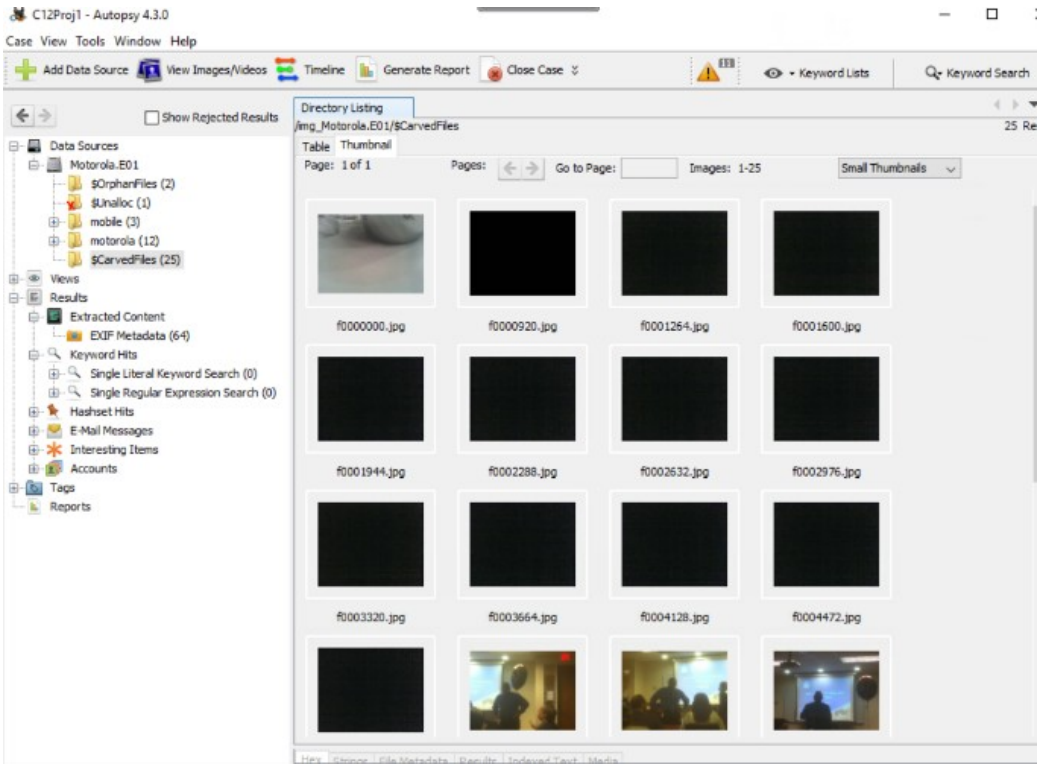

Figure 9. Deleted Images Found in $CarvedFile Folder

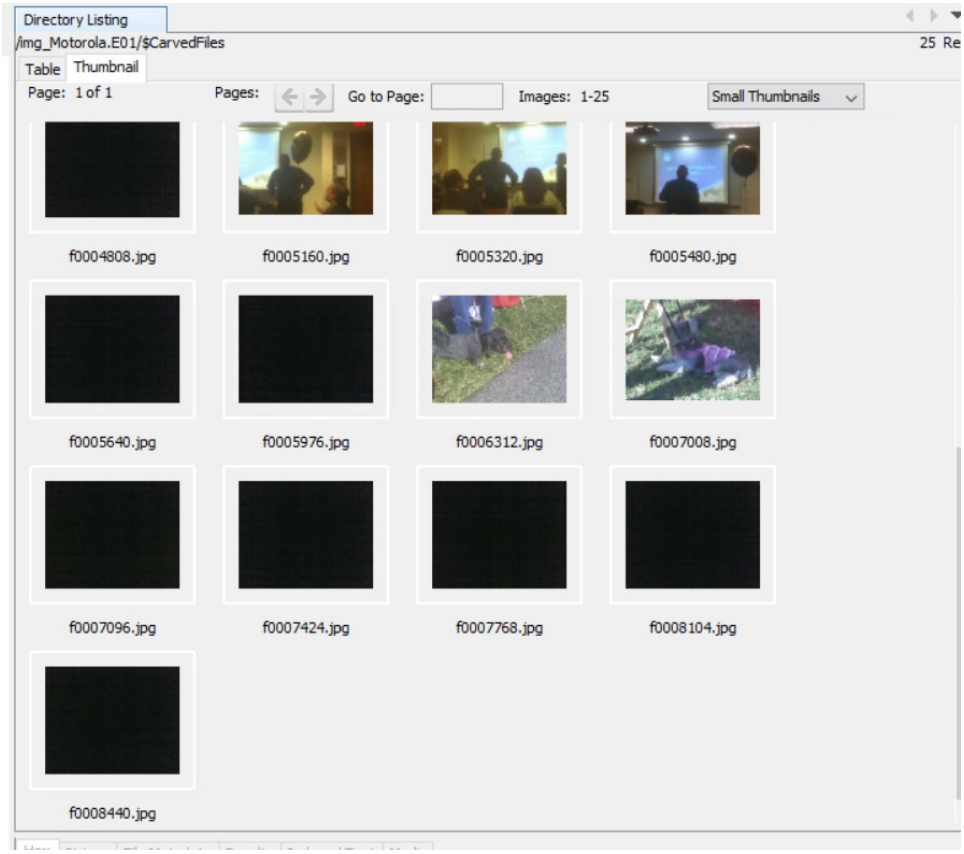

Figure 10. Deleted Items $CarvedFiles Folder Continued

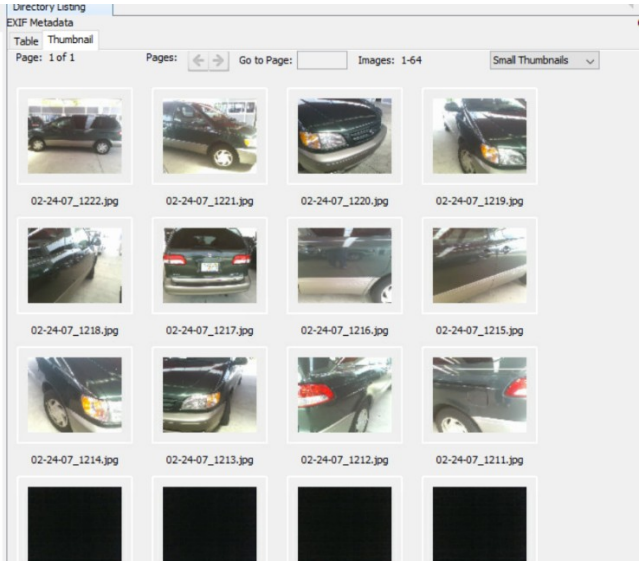

Figure 11. Images of a Car Found in Deleted Files

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

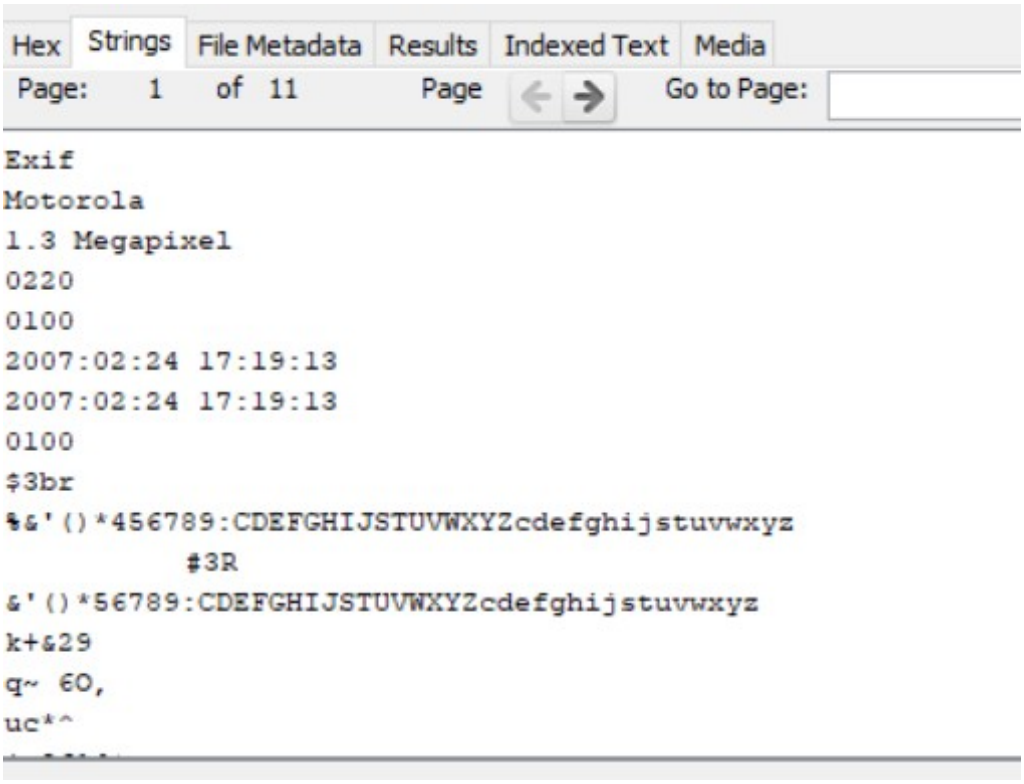

Figure 13. Strings Exif Motorola 1.3 Megapixel Camera

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).

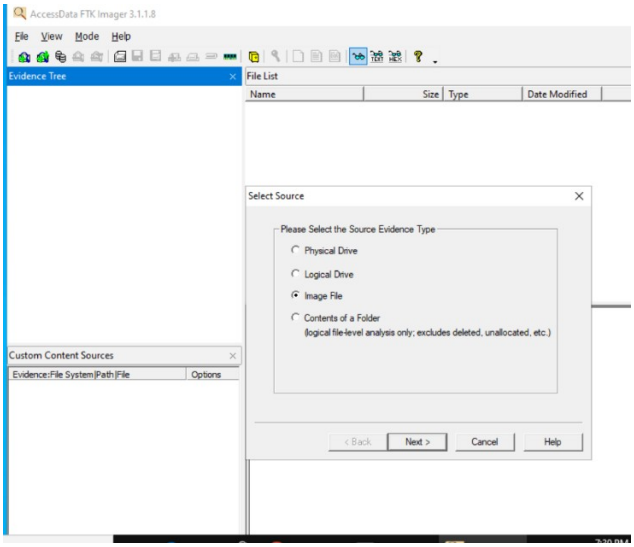

Figure 1. Launching FTK Imager Lite Selecting an Image File

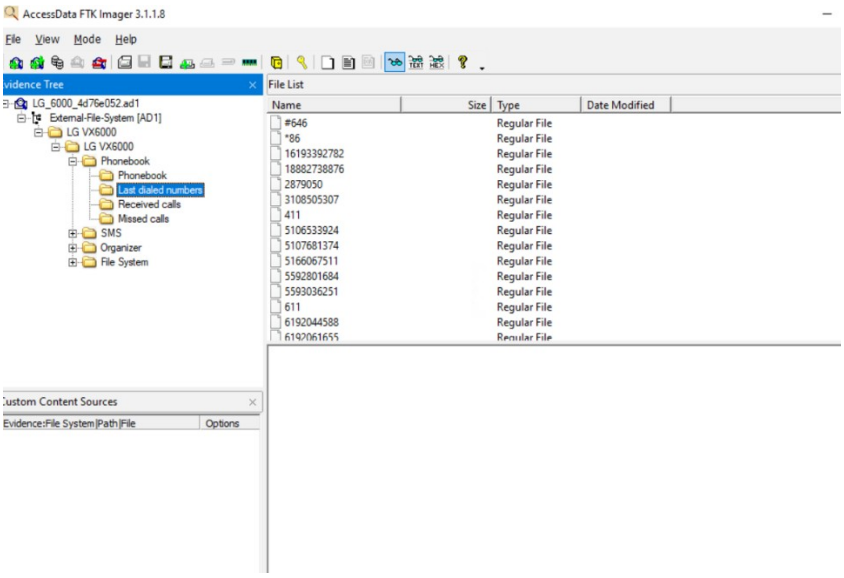

Figure 2. Phonebook Folder-Last Dialed Numbers

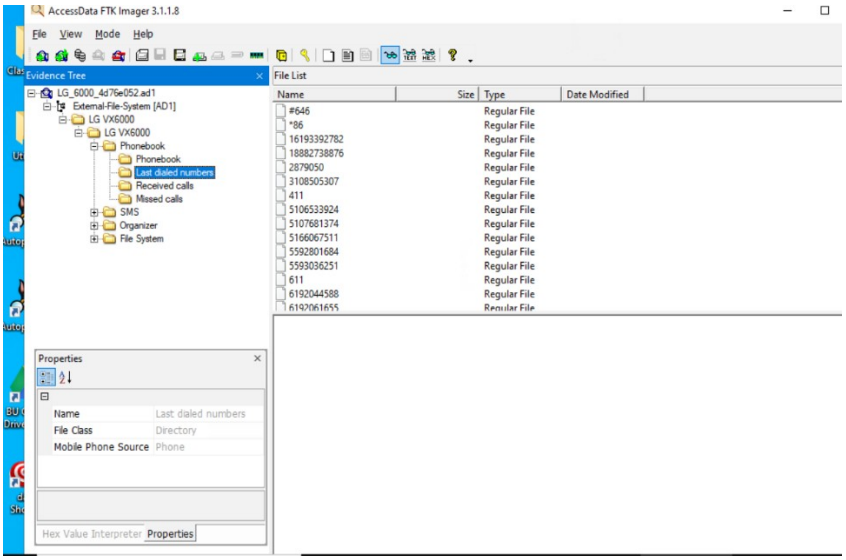

Figure 3. Last Dialed Numbers Continued

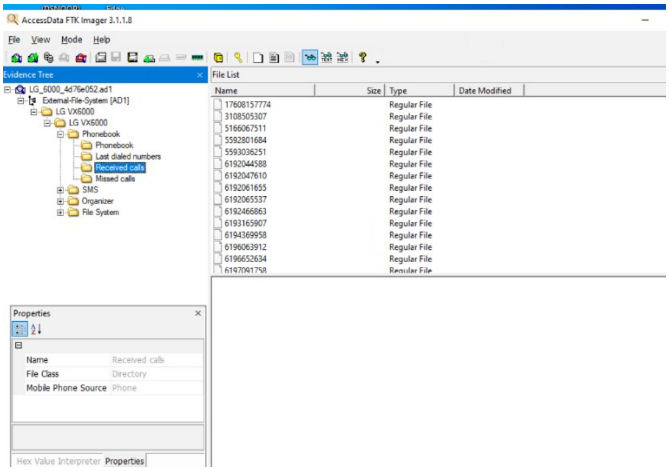

Figure 4. Received Calls

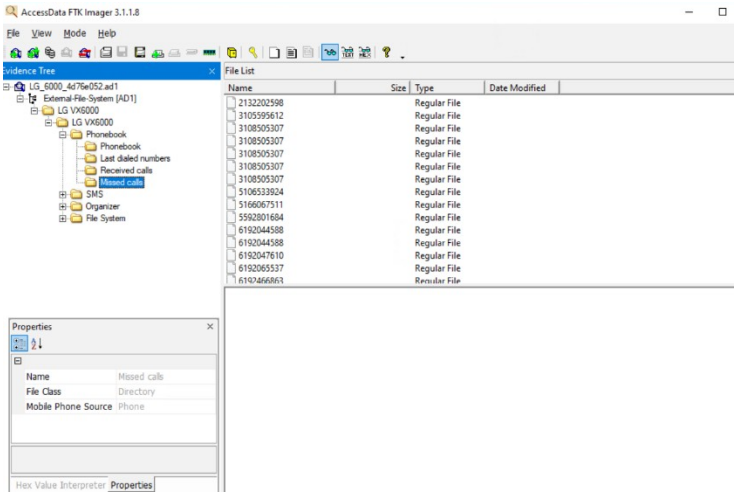

Figure 5. Missed Calls

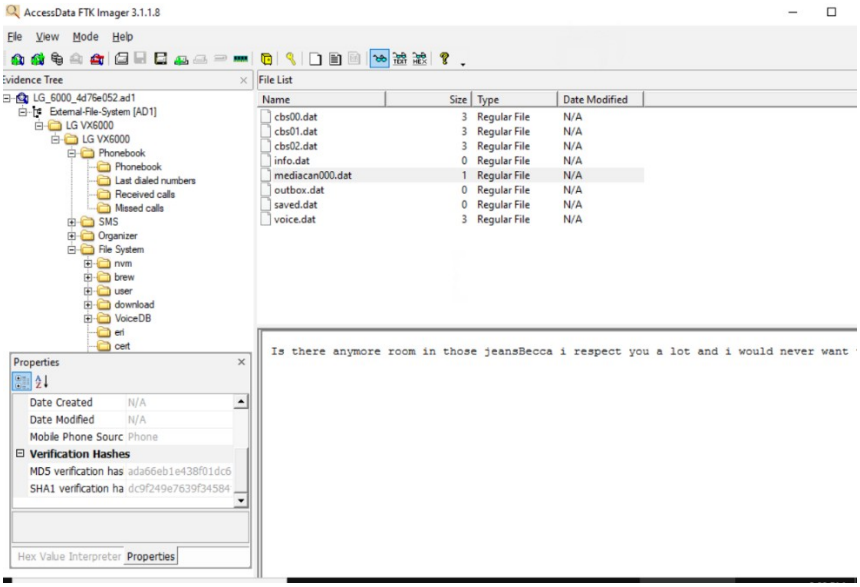

Figure 6. mediacan000.dat File Recovered MD5 and SHA1 Verification Hashes

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.

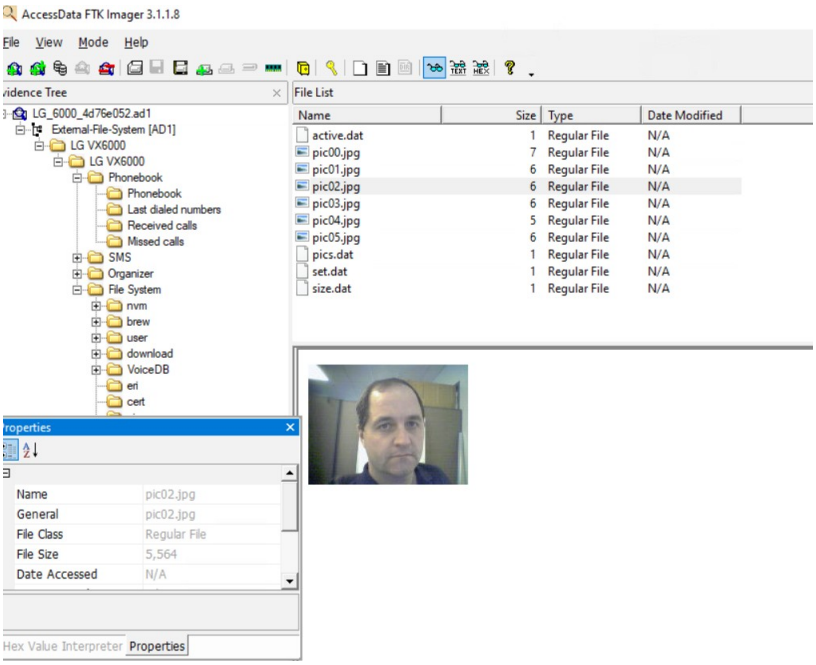

Figure 1. Pic02.jpg Image retrieved

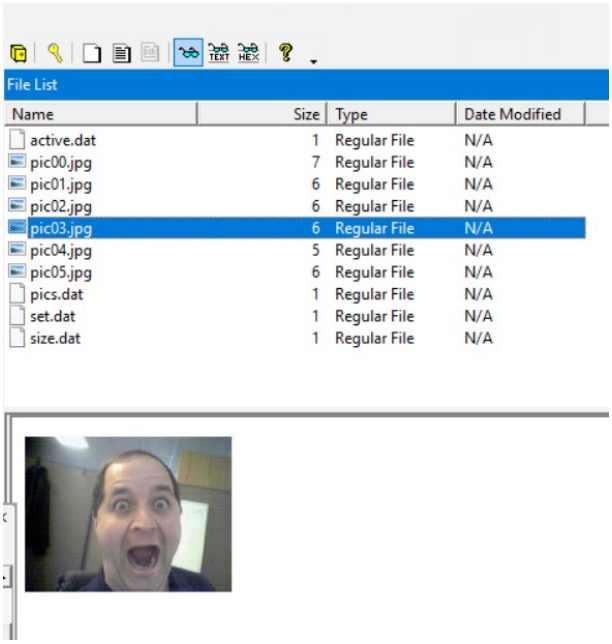

Figure 2. Pic03.jpg Image Recovered

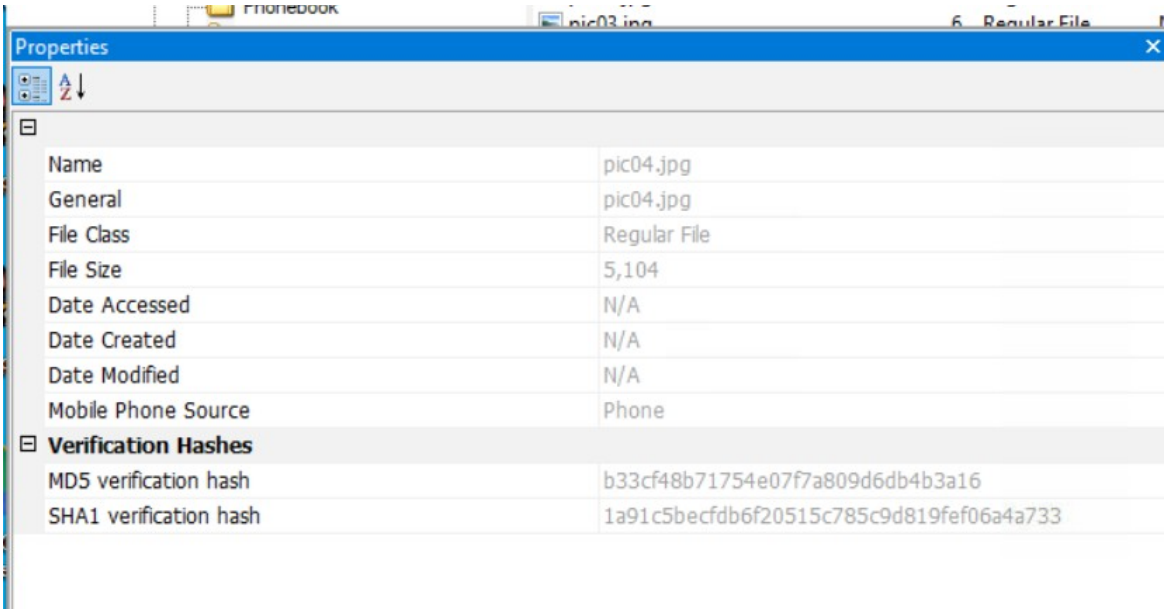

Figure 3. MD5 and SHA1 Hash Verifications for Pic04.jpg Image

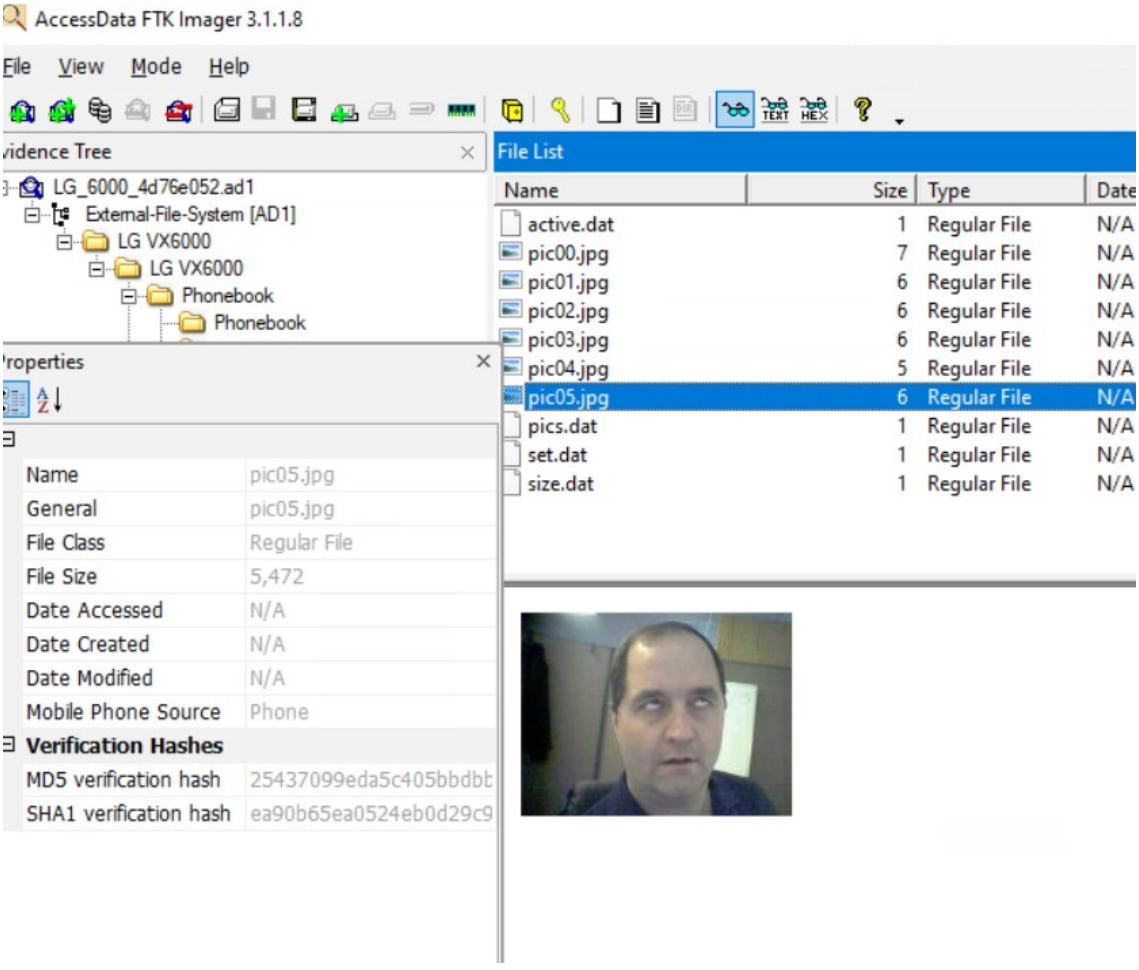

Figure 4. Pic05.jpg Recovered with MD5 and SHA1 Hash Verifications

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 filles 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).

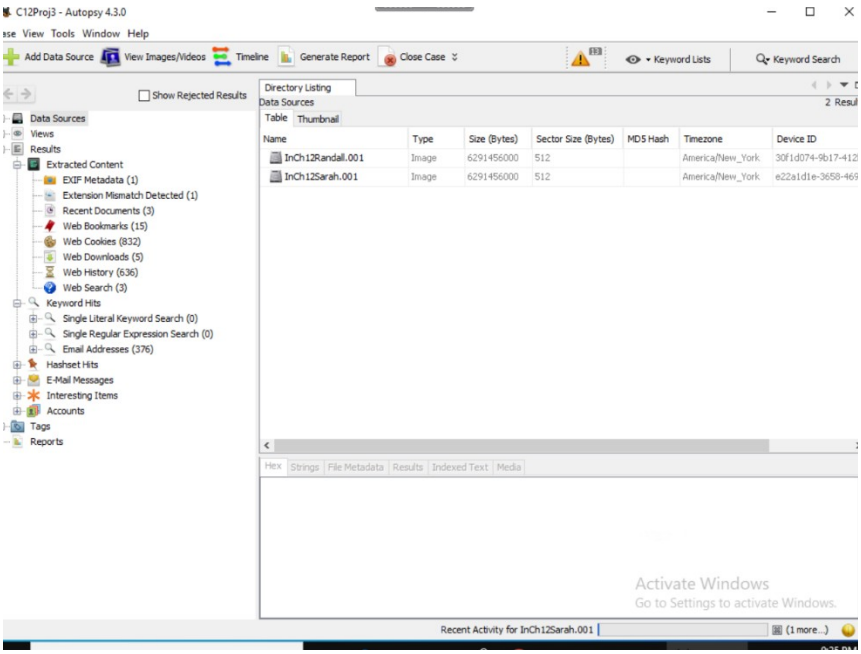

Figure 1. Extracted Content for Data Source Files InCh12Randal.001 Image and InCh12Sarah.001 Image files.

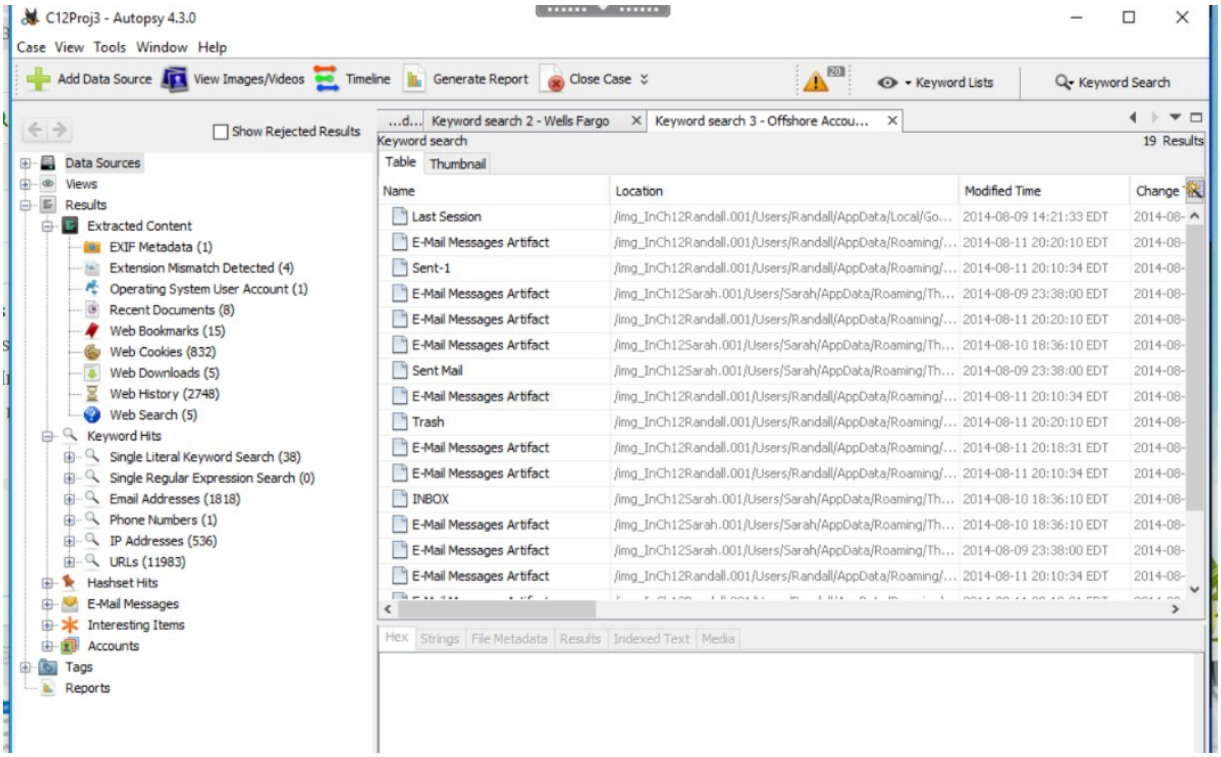

Figure 2. E-Mail Artifacts

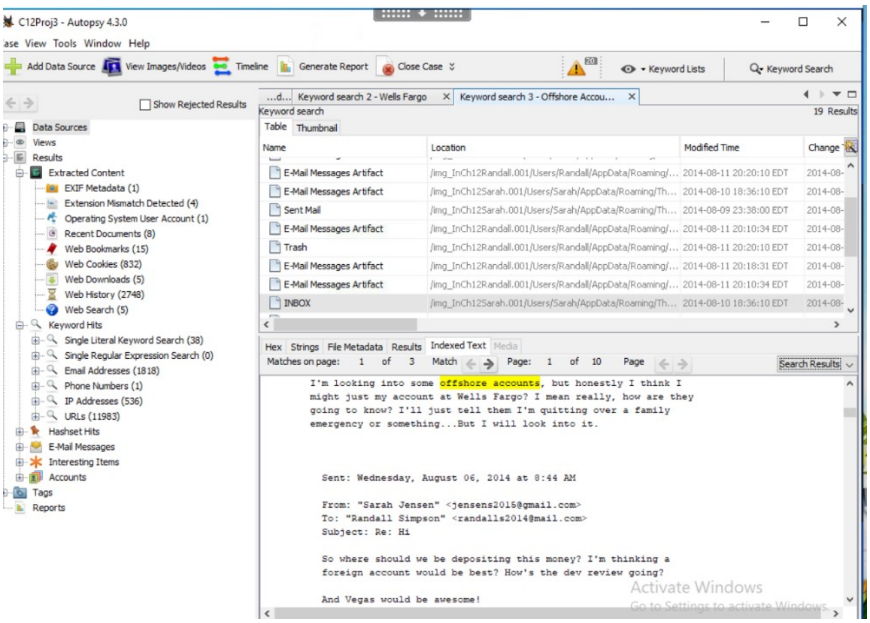

Figure 2. Indexed Text through an Offshore Account Keyword Search Through Data

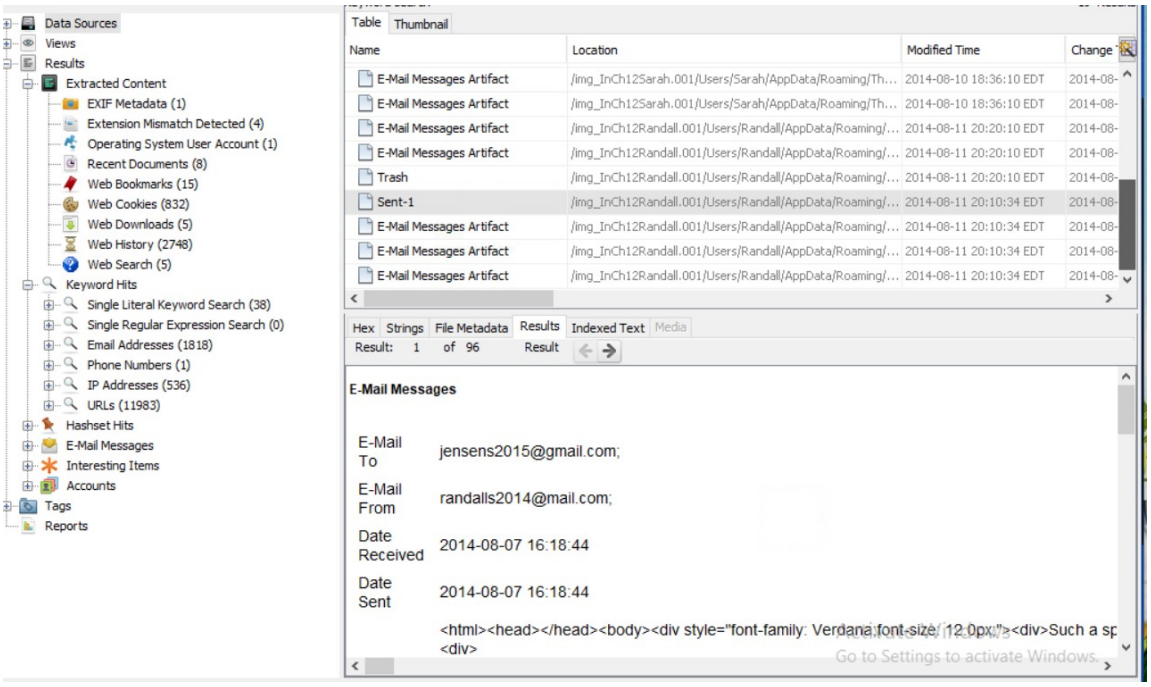

Figure 3. Sent E-Mail Artifact in Results

This E-Mail Message reveals the E-Mail addresses of both parties involved in the investigation. Jensen2015@gmail.com and randalls2014@gmail.com with the dates sent and received.

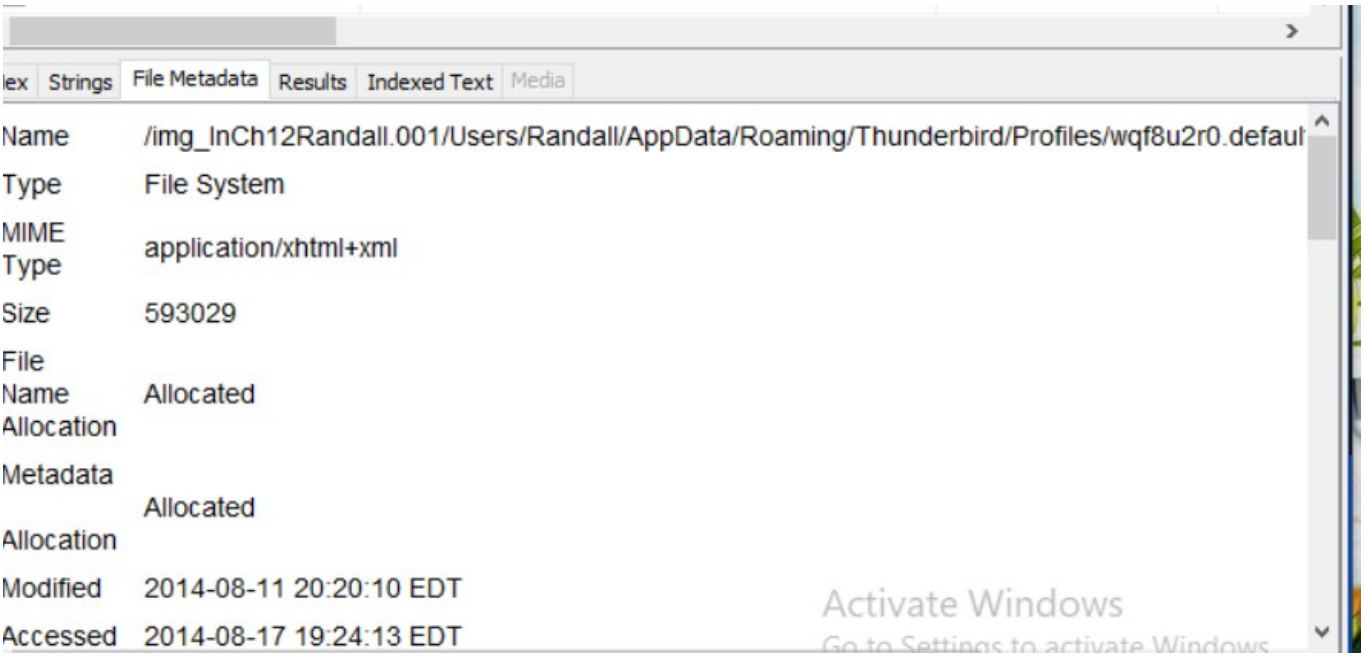

Figure 4. File Metadata

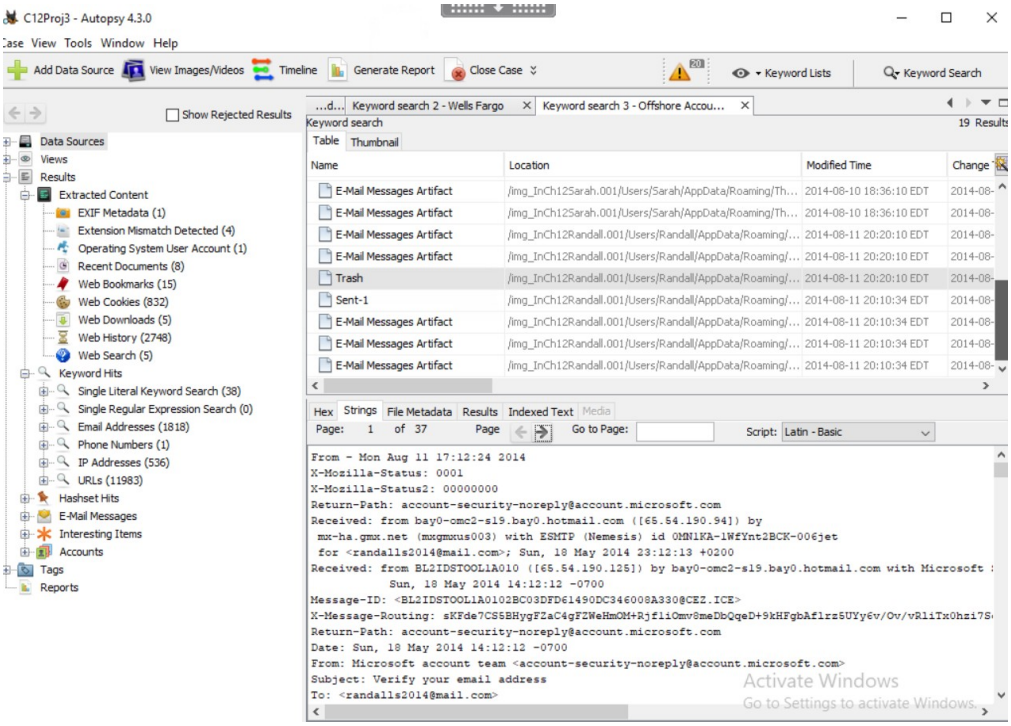

Figure 5. E-Mail Found in Trash providing Hex, Strings, File Metadata, Results, and Indexed Text

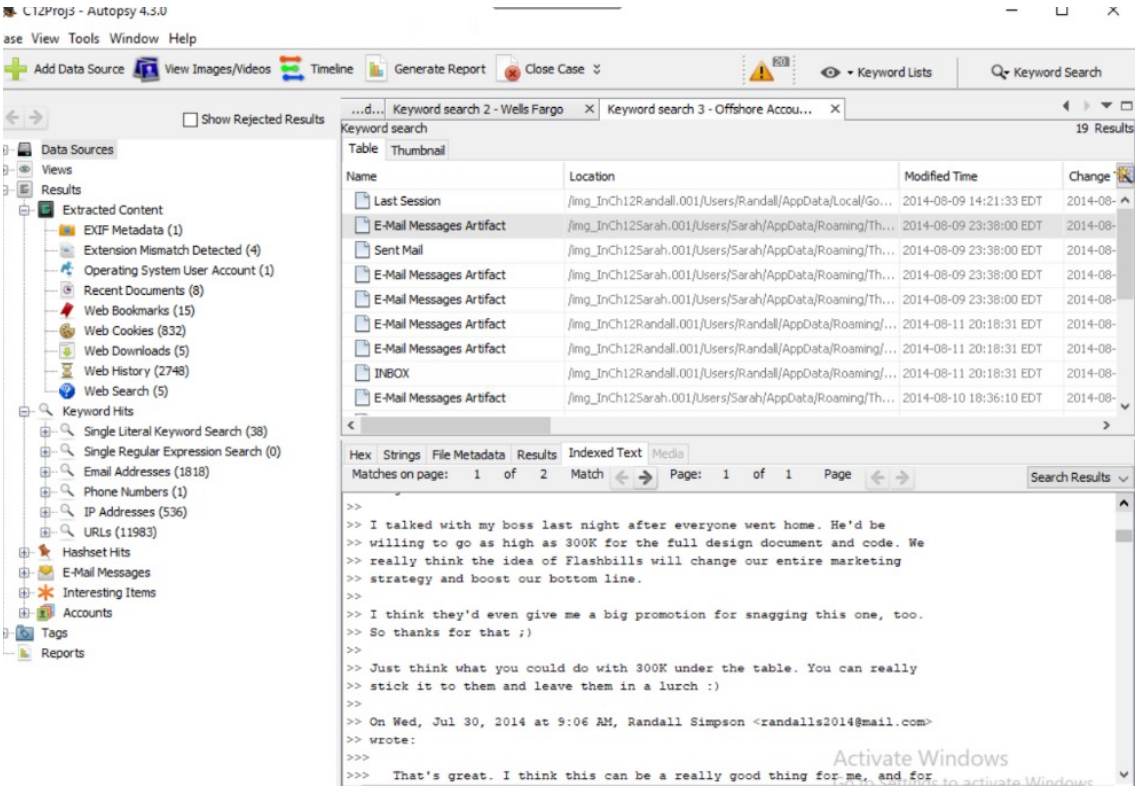

Figure 6. Indexed Text E-Mail

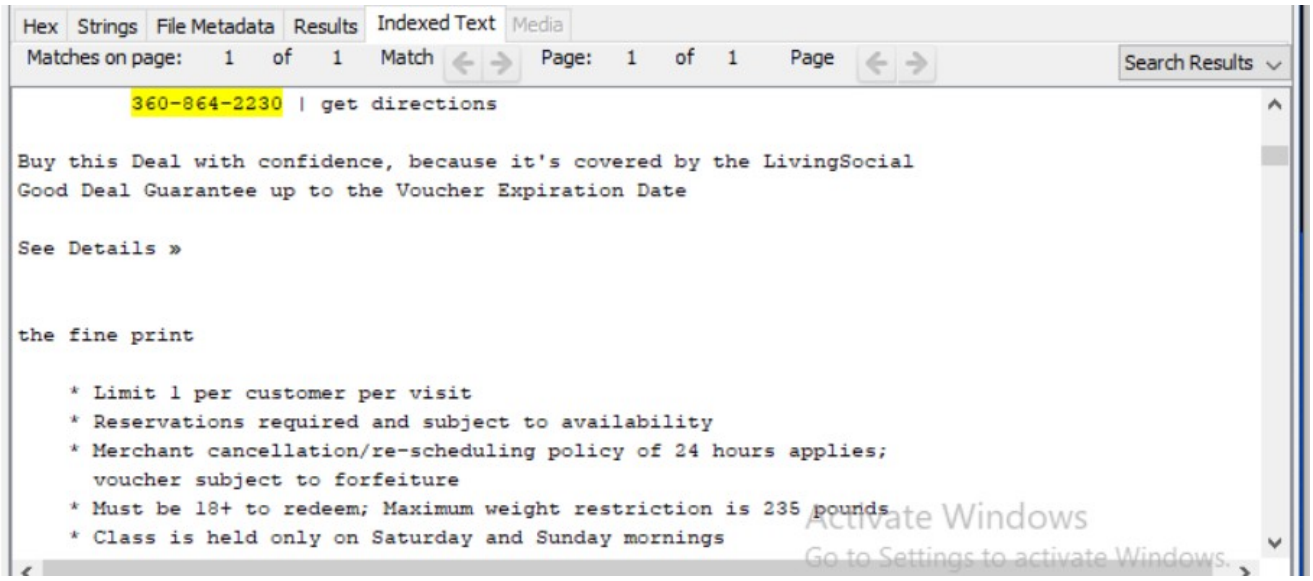

Figure 7. Indexed Text Revealing Phone number

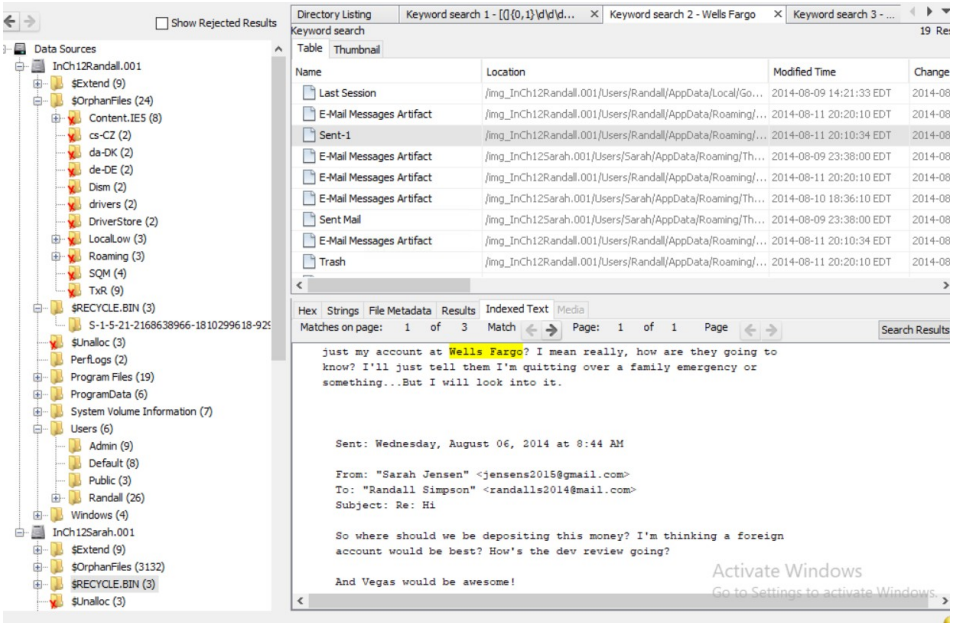

Figure 8. Wells Fargo Bank Revealed with detailed E-mail that also provides the names of the users for each E-Mail which are Sarah Jensen and Randall Simpson

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

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

   225

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

   True

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