Lab Assignment 4A – Linux and Mac Searching

Background

Students will become familiar with the basic structure of a Linux file system, a classic Mac OS 9 image, and an OS X image as they perform keyword scans and searches. Forensic investigations are not simply keyword searches, but these labs are meant to demonstrate basic search techniques for these operating systems. Additional case studies will follow the lecture material and expose students to myriad forensic techniques and artifacts.

Note: This Lab Assignment will require Autopsy, which was installed during previous exercises. Before starting these labs, create a subfolder of your work folder named LabAssignment4A.

OneDrive Link:
https://northeastern-my.sharepoint.com/:f:/g/personal/e_booker_northeastern_edu/EjLu1U7AfXlFojMXeOpGUoABTpB1cDFxetDoYNavUJxpjg?e=VN28qB

Objectives

- Review the macOS and OS 9 file system structure and perform keyword searches
- Become familiar with the Linux operating system layout and search for key terms

Exercise Preparation

1. **Using Autopsy to Process a Mac OS X Image**
   Autopsy can analyze and extract data from not only Windows and Linux file systems, but also macOS, Mac OS X, and Mac OS 9 file systems. The file system Apple developed for OS X is HFS+. In this lab, you import an OS X image into Autopsy and process it to look for potential evidence.

   NOTE: Processing the data file used in this lab can take 4 hours or more, so you might want to set up this lab to run overnight. The time it takes depends on your computer's CPU speed, the amount of RAM, and the drive access speed.

   In this lab, you import an OS X image into Autopsy to process evidence:
   a. Extract the **GCFI-OSX.zip** file to your work folder. (This process might take a few minutes.) Start Autopsy, and in the Welcome window, click the **Create New Case** button. In the New Case Information window, type **LabAssignment4a1** in the Case Name text box. Click the **Browse** button next to the Base Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**.
   b. In the Optional Information window, type **LabAssignment4a1** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
   c. Next we add data sources. In the Select Host window, choose **Generate new host name based on data source name**, and then click **Next**.

d. In the Select Data Source window, click **Disk Image or VM file** in the "Select Data Source Type" list box, if necessary, and click **Next**.
e. In the Select Data Source Window, click the **Browse** button under **Path:**, navigate to and click your work folder, click the **GCFI-OSX.001** file, and then click **Open**. Click **Next**.
f. In the Configure Ingest Modules window, click **Deselect All**, and then click the **Recent Activity**, **Hash Lookup**, **File Type Identification**, **Picture Analyzer (4.17 change)**, **Keyword Search**, **Email Parser**, and **PhotoRec Carver** check boxes.
g. Click the **Keyword Lists** down arrow. Click the **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** check boxes, and then click the **Search** button. Autopsy begins searching the image, which could take an hour or more. The application might crash or close at the end, but often the search has still completed.
h. Click **Keyword Search** at the upper right, type **Jim Shu** in the text box, and click **Search**. When the search is finished, click the **Keyword search 1 - Jim Shu** tab, if necessary. Click each item in the Result Viewer pane related to Jim Shu, and examine its contents in the Content Viewer pane (260 results with 4.19.1 on 2/20/2022).
i. Scroll to the right to display all the file attributes, such as location, timestamps, size, file types, MD5 hash sets, and keyword previews. Keep in mind some files won't have timestamps for various reasons, but certainly not files that were carved from unallocated space.

FOR THOSE USING THE PRE-PROCESSES EVIDENCE – LOAD THE EVIDENCE FILE AND START HERE

j. In the left pane, expand **Data Sources** and **GCFI-OSX.001** to view the file system folders in the image along with the number of files or folders in each folder. Next, expand **File Views**, **File Types**, and **By Extension**, and then click **Images** to see all the graphics files. Click the **Thumbnail** tab in the Result Viewer pane to see the graphics.
k. Under File Types, expand **Documents** to view the file types and the number of hits. To see the plaintext files, click **Plain Text**, and then click the **Table** tab in the Result Viewer pane. Click a file to view it in the Content Viewer pane.
l. In the left pane, expand **Analysis Results** and **Keyword Hits**, and then expand **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** to see the search results (expand the regex folders under each as well).
m. Under **Data Artifacts** in the left pane, expand **E-Mail Messages** and its subfolders to view correspondence with Jim Shu, including sent messages, deleted messages, the inbox, and so forth.
n. Leave Autopsy open as you answer the below review questions. When you're finished, click **File**, **Close Case** from the menu, and leave Autopsy running for the next lab.

2. Using Autopsy to Process a Mac OS 9 Image

Mac OS 9 is also known as Apple's "classic Mac" OS. This OS, introduced in 1997, lacks many of the features in current file systems, such as protected memory and preemptive multitasking; it uses the older HFS file system. In 2002, Apple officially discontinued OS 9 and later developed Mac OS X and the current macOS operating system. Because forensics investigators might still encounter OS 9 images on older Apple hardware, however, you use Autopsy in this lab to examine an OS 9 image file and search for potential evidence. Because the HFS file system is so different from other file systems, such as those in Linux and Windows, Autopsy 4.19.1 displays files as though they were carved from unallocated space on the drive. Dates and times for recovered files show only zero values.

a. Extract the **GCFI-OS9.zip** file to your work folder, which might take a few minutes. In Autopsy, click **Case**, **New Case** from the menu. In the New Case Information window, type **LabAssignment4a2** in the Case Name text box. Verify that your work folder is displayed in the Base Directory text box, and then click **Next**.
b. In the Optional Information window, type **LabAssignment4a2** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
c. Next we add data sources. In the Select Host window, choose **Generate new host name based on data source name**, and then click **Next**.
d. In the Select Data Source window, click **Disk Image or VM file** in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to and click your work folder, click the **GCFI-OS9.001** file, and then click **Open**. Click **Next**.
e. Click **Next** to accept the selected ingest modules from prior steps, and then click **Finish** to start analyzing the evidence, which could take a while.
f. Click the **Keyword Lists** down arrow. Click the **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** check boxes, and then click the **Search** button. Autopsy begins searching the image, which could take up to 4 hours or more.

FOR THOSE USING THE PRE-PROCESSES EVIDENCE – LOAD THE EVIDENCE FILE AND START HERE

g. In the left pane, expand **Keyword Hits**, if necessary, and then expand **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** to see the search results. Examine the e-mail address results for details such as timestamps and the text of messages.
h. In the left pane, expand **Views**, **File Types**, **By Extension**, and **Documents**, and click **HTML** to view carved HTML files. To view their data, click a file in the Result Viewer pane to see its data in the Content Viewer pane, or click the **Thumbnail** tab to see just the image with its filename. Repeat this process for the **Videos** and **Audio** folders.
i. Leave Autopsy open as you answer the review questions below. When you're finished, click **File**, **Close Case** from the menu, and leave Autopsy running for the next lab.

Autopsy 4.19.1 can't display filenames and metadata for HFS file systems. It can, however, carve files so that you can search for them and examine their contents. This is why Autopsy displays files starting with the letter "f" followed by a unique number and file extension. For more information on HFS and HFS+, see www.macdisk.com/macforken.php.

3. Using Autopsy to Process a Linux Image

The Ext3 file system, used in many Linux distributions, added a journaling capability, which has a built-in file recovery mechanism used after a crash. With the increasing popularity of open-source office suites, such as OpenOffice and LibreOffice, forensics investigators are likely to find systems formatted in Ext3. Ext4, the most recent file system, is included in the Linux 4.16 kernel. Autopsy can be used to search images formatted in this file system, too. In this lab, you extract a Linux image and import it into Autopsy for analysis.

NOTE: Processing the data file used in this lab can take 4 hours or more, so you might want to set up this lab to run overnight. The time it takes depends on your computer's CPU speed, the amount of RAM, and the drive access speed.

In this lab, you load a Linux image in Autopsy to process evidence:

a. Extract the **GCFI-LX.xxx.exe** file to your work folder, which might take a few minutes. In Autopsy, click **Case**, **New Case** from the menu. In the New Case Information window, type **LabAssignment4a3** in the Case Name text box, verify that your work folder is displayed in the Base Directory text box, and then click **Next**.
b. In the Additional Information window, type **LabAssignment4a3** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
c. Next we add data sources. In the Select Host window, choose **Generate new host name based on data source name**, and then click **Next**.
d. In the Select Data Source window, click **Disk Image or VM file** in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to and click your work folder, click the **GCFI-LX.001** file, and then click **Open**. Click **Next**.
e. Click **Next** to accept the selected ingest modules from prior steps, and then click **Finish** to start analyzing the evidence.

FOR THOSE USING THE PRE-PROCESSES EVIDENCE – LOAD THE EVIDENCE FILE AND START HERE

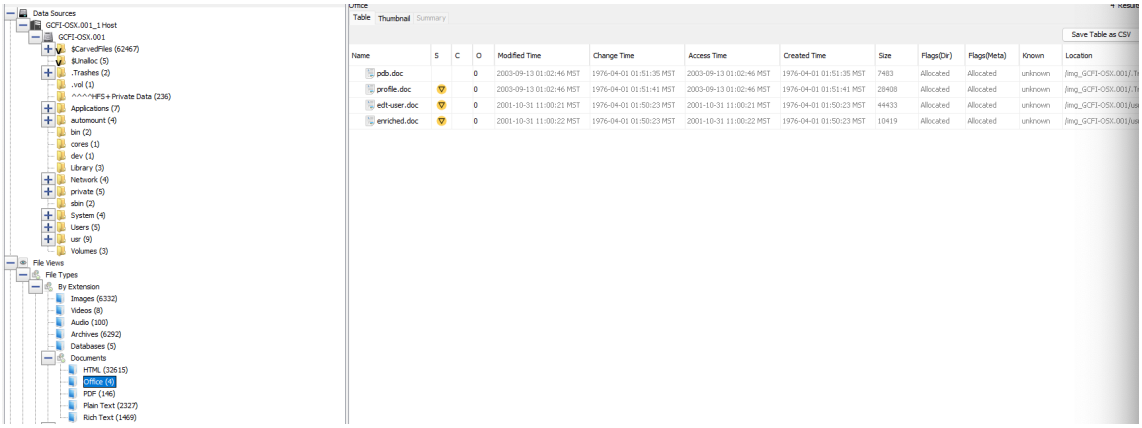
f. In the left pane, expand **Data Sources** and **GCFI-LX.001** to view the folder structure. This structure is common in many Linux distributions. Right-click **GCFI-LX.001** to see these options: Extract Unallocated Space to Single Files, Open File Search by Attributes, and Run Ingest Modules (used to process the image again with different settings).
g. Click **Keyword Search** at the upper right, type **martha** in the text box, and click **Search**. In the Result Viewer pane, click the **Keyword search 1 - martha** tab, if necessary, to view all the search results. Scroll down and click the **Inbox** entry to view the e-mail Martha Dax sent to Chris Murphy.
h. Click **Keyword Search** at the upper right, type **Chris Murphy** in the text box, and click **Search**. Click the **Keyword search 2 - Chris Murphy** tab, if necessary. In the left pane, click to expand **Results**, **E-Mail Messages**, and **Default [Default]**, and then click the **Default** folder to see all e-mail correspondence.
i. In the left pane, expand **Extracted Content**, and then click **Extension Mismatch Detected** to view file extensions that don't match their file types. This information might reveal files that have been altered to keep them hidden.
j. Leave Autopsy open as you answer the following review questions. When you're finished, exit Autopsy.

Exercise – Questions

1. Using Autopsy to Process a Mac OS X Image

a. How many Word files are in the GCFI-OSX.001 image?

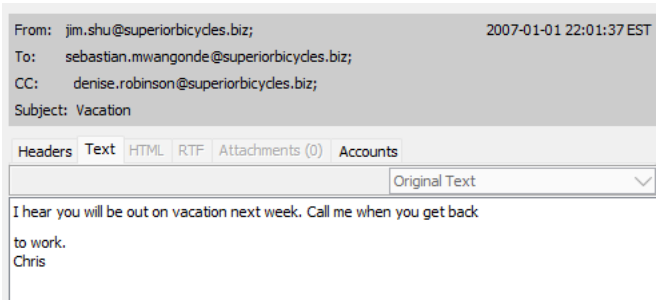
There are 4 Word files in the image found in File Views > File Types > By Extension > Documents > Office >*.doc



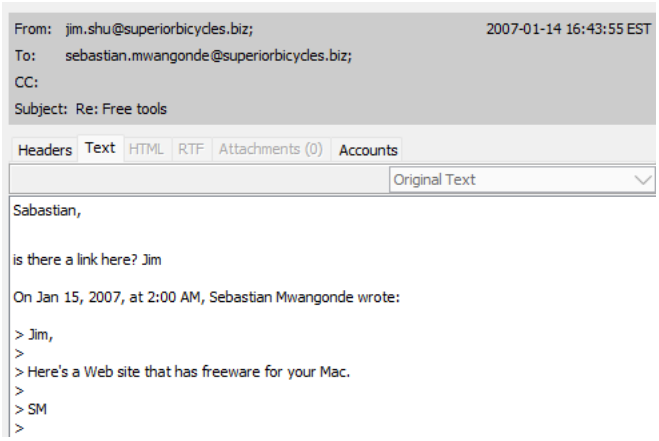
b. What **or** who is the subject of the **first** message sent by Jim Shu?

Messages found in Data Artifacts > E-Mail Messages > Sent Messages > Incoming_Mail|mbox

The first message sent by Jim Shu in the "mbox" Source Name is on 2007-01-01 20:01:37 MST with the subject "Vacation". NOTE: Timestamp below is in EST



The first message sent by Jim Shu in the "Incoming_Mail" Source Name is on 2007-01-14 14:43:55 MST with the subject "Re: Free Tools". NOTE: Timestamp below is in EST



c. What phone number had the most search results and therefore might warrant further investigation?

Phone Numbers are found in Analysis Results > Keyword Hits > Phone Numbers. The phone number with the most search results is (800) 810-0595 with 250 hits.

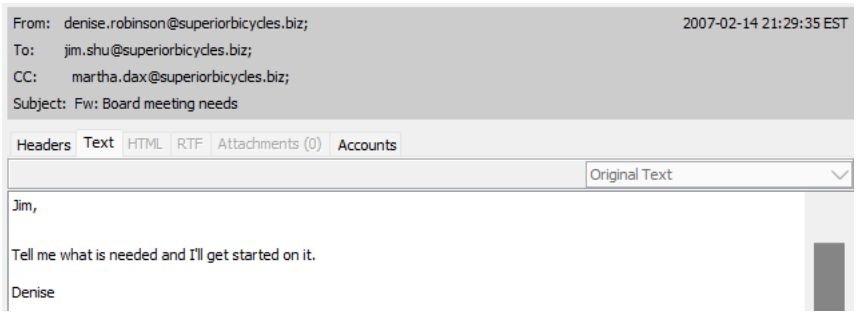
List Name	Files with Hits
800 810 0595 (250)	250
800 279 3198 (160)	160
800 902 6300 (154)	154
800 539 6275 (152)	152
800-539-6275 (134)	134
787 758 8757 (102)	102

d. What file system is used for Mac OS X?

The file system used on macOS is HFS or Hierarchical File System. I found it by going to ^^^^HFS+ Private Data

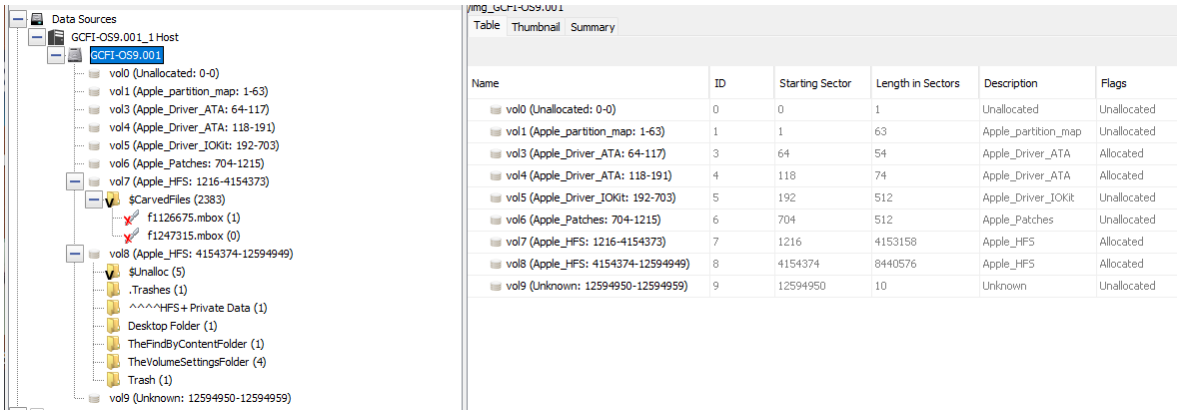
e. Who sent the **last** e-mail to Jim Shu directly?

Denise Robinson sent the last e-mail to Jim Shu at 2007-02-14 19:29:35 MST



2. Using Autopsy to Process a Mac OS 9 Image

a. What file system is used by the Mac OS 9 operating system?



b. How many videos are in the GCFI-OS9.001 image?

There are 8 videos .mov located in File Views > File Types > By Extension > Videos (8)

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
f0262419_mdat.mov			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4123214
f0308502_stbl.mov			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	283846
f0262163_moov.mov			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	73293
f0270547_moov.mov			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	67678
f0308115.mov			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8
f0308307_moov.mov			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45187
f0308499_moov.mov			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2540
f0335123_moov.mov			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	72490

c. Were there any executable files in the GCFI-OS9.001 image?

There are no executable files with extensions .exe, .dll, .bat, .cmd, .com. Located in File Views > File Types > By Extension > Executable

d. Which phone number was dialed most often, which might warrant further investigation?

List Name	Files with Hits
(847) 718-0400 (15)	15
252.227-7013 (4)	4
770-488-4902 (4)	4
(831) 761-6200 (2)	2
(831) 761-6206 (2)	2

The phone number that was dialed most often was (847) 718-0400 with 15 hits. Found under Analysis Results > Keyword Hits > Phone Numbers

e. What URL was visited the most often by the user of this system and how many times? What can you learn about the TLD under the site's home page?

The URL that was visited the most often was http://www.w3.org/1999/02/22-rdf-syntax-ns# visited 69 times.

The TLD (Top-Level Domain) www.w3.org focuses on security and privacy to address usability challenges. This site may have been visited multiple times to learn how to exploit or reverse engineer sites visited.

3. Using Autopsy to Process a Linux Image

a. How many recovered e-mails are listed under the Default folder under Data Artifacts?

There are 79 recovered e-mails listed under the Default folder located in Data Artifacts > E-Mail Messages > Default > Default

b. How many Word (.doc) and Excel (.xls or .xlsx) files were recovered in this image? Were there are other text document files recovered?

Since it is a linux system the Office files with extension .odt were 8 recovered. There were 4 .txt files, 3 .rtf files. There were 2 PDF files and 11 HTML files recovered within File Views > File Types > By Extension > Documents

c. Did Martha communicate with anyone other than Chris Murphy, if so, who? (List up to five contacts)

Martha communicated with Nau Tjeriko and Sebastian Mwangonde independently. Martha communicated with Chris Murphy in a chained email with Robert Swartz, Ralph Benson, Ileen Johnson, Bart Jones, Sam Clemens and Jim Shu, in addition to the two he individually contacted.

d. What was the content of the two videos stored on the desktop of "nau's" Desktop under their home folder that was eventually deleted? Describe the video briefly and add the filenames of the video here.

Located in File Views > File Types > By Extension > Videos (5). The two videos stored on Nau's Desktop were "EOC_Nisqually.wmv" and "EOCfromCmmtyBldg.wmv" They were both moved into the Trash with the assumption that the user was trying to remove these files from the Desktop.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Location	Flags(Dir)
EOC_Nisqually(2).wmv				2007-01-05 13:45:34 MST	2007-01-05 13:57:04 MST	2007-01-05 13:50:18 MST	0000-00-00 00:00:00	1276930	/img_GCFI-LX.001/home/nau/.Trash/EOC_Nisqually(2).wmv	Allocated
EOCfromCmmtyBldg(2).wmv				2007-01-14 20:46:49 MST	2007-01-14 20:48:22 MST	2007-01-14 20:48:20 MST	0000-00-00 00:00:00	3613476	/img_GCFI-LX.001/home/nau/.Trash/EOCfromCmmtyBldg(2...	Allocated
EOC_Nisqually(2).wmv				2007-01-05 13:45:34 MST	2007-01-05 13:57:04 MST	2007-01-05 13:50:18 MST	0000-00-00 00:00:00	1276930	/img_GCFI-LX.001/home/nau/Desktop/EOC_Nisqually(2).wmv	Unallocated
EOC_Nisqually.wmv				2007-01-05 13:41:04 MST	2007-01-05 13:41:04 MST	2007-01-14 20:48:01 MST	0000-00-00 00:00:00	1276930	/img_GCFI-LX.001/home/nau/Desktop/EOC_Nisqually.wmv	Allocated
EOCfromCmmtyBldg.wmv				2007-01-05 13:41:49 MST	2007-01-05 13:41:49 MST	2007-01-05 13:57:53 MST	0000-00-00 00:00:00	3613476	/img_GCFI-LX.001/home/nau/Desktop/EOCfromCmmtyBldg...	Allocated

e. Review nau's address book database under the extracted databases view (File Views > File Types > By Extension > Databases) or under the path "/img_GCFI-LX.001/home/nau/.evolution/addressbook/local/system/addressbook.db" and list the e-mail address of those contacts added to the address book.

sam.clemens@superiorbicycles.biz

ileen.johnson@superiorbicycles.biz

ralph.benson@superiorbicycles.biz

sebastian.mwangonde@superiorbicycles.biz

bart.jones@superiorbicycles.biz

martha.dax@superiorbicycles.biz

robert.swartz@superiorbicycles.biz

jim_shu1@yahoo.com

denise.robinson@superiorbicycles.biz

Exercise—Key Takeaways

- Linux and macOS operating system layouts are similar and evidence artifacts overlap
- Although investigations are much more than simple keyword searches, this method can be a great start to identify potential evidence that relates to a case and easily identify valuable evidence locations

***Please submit the final assignment as a single .PDF and any applicable reports as a .ZIP file.**
**Screenshots may also be added to this document when appropriate.