

***Lab11: UNIX Drive***

CNIT42000-001

Ethan Hammond

Prof. Tahir Khan

Date Submitted: 04/21/23

Date Due: 04/21/23

## Table of Contents

<b>Table of Contents</b>	<b>2</b>
<b>Abstract</b>	<b>3</b>
<b>Task 1:</b>	<b>4</b>
<b>Task 2:</b>	<b>7</b>
<b>Conclusion</b>	<b>10</b>
<b>Appendix A: Time Chart</b>	<b>11</b>
<b>Time Chart</b>	<b>11</b>

## **Abstract**

Lab 11 consisted of searching through a UNIX drive in Autopsy to uncover information about a suspicious person 'Jim Shu'. It was instructed to find all files pertaining to this person on the drive. The files were uncovered by checking email addresses and messages, as well as utilizing keyword searches to find all instances of the name. After these files were uncovered, it was tasked to find how many images and documents were on the drive. This was also done through Autopsy's feature of categorizing files for the investigator. Taks 2 included a new E01 image file and was tasked with keyword searching and reporting all data of a few terms. The files uncovered were email addresses between Charlie and a few people talking about hidden passwords and shady business deals. This led the forensic investigation team to want to investigate this person further.

## Task 1:

The task of finding all files pertaining to ‘Jim Shu’ was investigated by looking at email addresses, as well as using a keyword search for ‘jim’ to catch all substrings of Jim Shu. All files found can be seen in Figures 1-5 below.











Listing						
Sent Messages.mbox						
Table Thumbnail Summary						
Source Name	S	C	O	E-Mail From	E-Mail To	S
 mbox				jim.shu@superiorbicycles.biz;	sebastian.mwangonde@superiorbicycles.biz;	Va
 mbox				jim.shu@superiorbicycles.biz;	sebastian.mwangonde@superiorbicycles.biz;	Pa
 mbox				jim.shu@superiorbicycles.biz;	nau.tjeriko@superiorbicycles.biz;	Mk
 mbox				jim.shu@superiorbicycles.biz;	ralph.benson@superiorbicycles.biz;	R:
 mbox				jim.shu@superiorbicycles.biz;	nau.tjeriko@superiorbicycles.biz;	R:
 mbox				jim.shu@superiorbicycles.biz;	nau.tjeriko@superiorbicycles.biz;	R:
 mbox				jim.shu@superiorbicycles.biz;	nau.tjeriko@superiorbicycles.biz;	Fv
 mbox				jim.shu@superiorbicycles.biz;	sebastian.mwangonde@superiorbicycles.biz;	D:
 mbox				jim.shu@superiorbicycles.biz;	ileen.johnson@superiorbicycles.biz;	Ex
 mbox				jim.shu@superiorbicycles.biz;	ileen.johnson@superiorbicycles.biz;	Fv

Figure 1: Sent messages from jim.shu@superiorbicycles.biz













Sent Messages.mbox						
Table Thumbnail Summary						
Source Name	S	C	O	E-Mail From	E-Mail To	
 Incoming_Mail				jim.shu@superiorbicycles.biz;	sebastian.mwangonde@superiorbicycles.biz;	
 Incoming_Mail				jim.shu@superiorbicycles.biz;	sebastian.mwangonde@superiorbicycles.biz;	
 Incoming_Mail				jim.shu@superiorbicycles.biz;	ileen.johnson@superiorbicycles.biz;	
 Incoming_Mail				jim.shu@superiorbicycles.biz;	nau.tjeriko@superiorbicycles.biz;	
 Incoming_Mail				jim.shu@superiorbicycles.biz;	nau.tjeriko@superiorbicycles.biz;	
 Incoming_Mail				jim.shu@superiorbicycles.biz;	martha.dax@superiorbicycles.biz;	
 Incoming_Mail				jim.shu@superiorbicycles.biz;	martha.dax@superiorbicycles.biz;	
 Incoming_Mail				jim.shu@superiorbicycles.biz;	jim_shu1@yahoo.com;	
 Incoming_Mail				jim.shu@superiorbicycles.biz;	ralph.benson@superiorbicycles.biz;	
 Incoming_Mail				jim.shu@superiorbicycles.biz;	robert.swartz@superiorbicycles.biz;	
 Incoming_Mail				jim.shu@superiorbicycles.biz;	martha.dax@superiorbicycles.biz;	
 Incoming_Mail				jim.shu@superiorbicycles.biz;	martha.dax@superiorbicycles.biz;	

Figure 2: Incoming mail from jim.shu@superiorbicycles.biz


Listing						
Deleted Messages.mbox						
Table Thumbnail Summary						
Source Name	S	C	O	E-Mail From	E-Mail To	Sub
 mbox				news-alert@mysql.com;	jim.shu@superiorbicycles.biz;	MyS

Figure 3: Deleted message from jim.shu@superiorbicycles.biz

 jimshu			2007-03-12 01:02:00 EDT	2007-03-12 01:02:00 EDT	2007-03-12 00:47:10 EDT	:
--	--	--	-------------------------	-------------------------	-------------------------	---

Figure 4: Jimshu's home directory in \users\jimshu



Name	Keyword Preview	Location	Modified Time	Change Time	Access Time
0188467655-4273976843.cache	-0800 (pst)from: "«jim shu»" <jim_shu1@yahoo.co	/img_GCFI-OSX.001/Users/jimshu/Library/Caches/Safari/1...	2007-01-05 16:49:12 EST	2007-01-05 16:49:14 EST	2007-01-05 16:49:12 EST
0874913555-3971969733.cache	n jan 21, 2007 11:11kjim shu« fwd: budget co	/img_GCFI-OSX.001/Users/jimshu/Library/Caches/Safari/0...	2007-02-04 13:42:19 EST	2007-02-04 13:42:22 EST	2007-02-04 13:42:19 EST
E-Mail Messages Artifact	rbicycles.bizfrom: «jim shu» <jim.shu@superiorbi	/img_GCFI-OSX.001/Users/jimshu/Library/Mail/POP-jim.shu...	2007-01-08 22:16:14 EST	2007-01-08 22:16:14 EST	2007-01-01 22:01:42 EST

Figure 5: Keyword search results for Jim Shu. 160 results were found under the search.

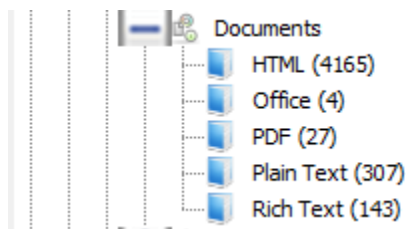
The next task was to find a count of all image files on the drive. Autopsy was able to filter the files on the drive image by Image files. The result of this categorization can be seen below in Figure 6.



File Views	File Types	By Extension
		Images (2065)
		Videos (3)

Figure 6: Image files found on the drive image.

The next task was to find all document files on the drive image. Autopsy was also able to split files into categories to present the findings. The count of document files can be seen below in Figure 7.



Documents
HTML (4165)
Office (4)
PDF (27)
Plain Text (307)
Rich Text (143)

Figure 7: Documents found on the drive image.

## Task 2:

Task 2 consisted of searching through a linux drive image to search for specific keywords and present the findings in a report. The following keyword search results can be seen below in Figures 8-12. These findings include sketchy emails, passwords, and proof of steganography encryption.

Figure 8 shows a suspicious email found on the drive. This email is from Charlie talking to someone from project2400 about a suspicious business deal. It also consists of a command to delete the email.

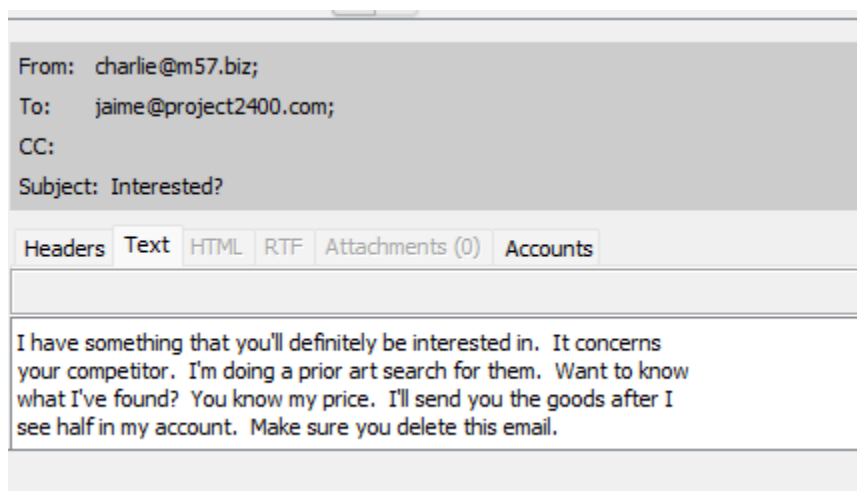


Figure 8: Project 2400 is an email domain.

Figure 9 shows an invitation to Charlie from Pat McGoo of joining the M57.biz family. This seems to be an email domain that sends suspicious business deals.

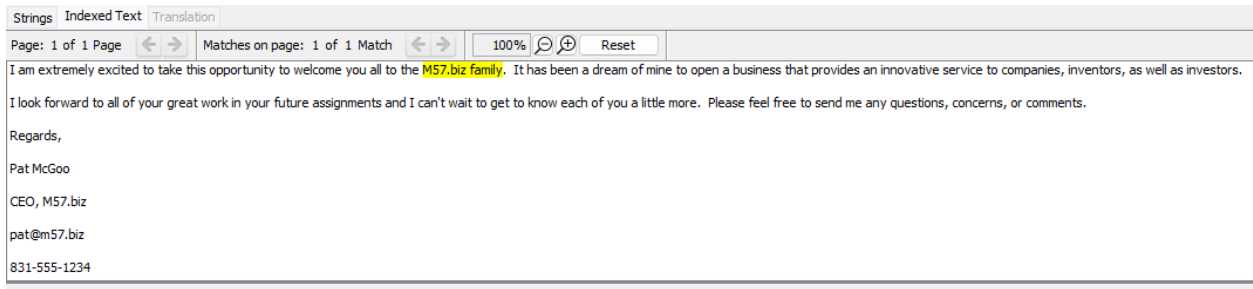


Figure 9: M57.biz is another email domain. This is a suspicious email that has to do with welcoming Charlie to the m57.biz investing organization.

Figure 10 consists of a password hidden with steganography in a microscope.jpg file. This was found through Autopsy.

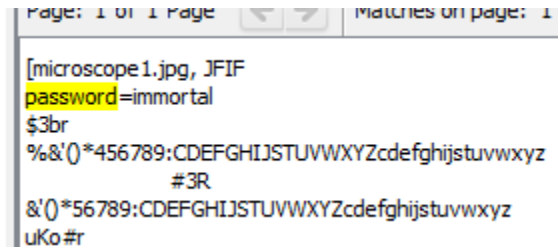


Figure 10: Password listed hidden with steg in the microscope1.jpg file.

Figure 11 consists of a suspicious email from Charlie giving someone instructions about how to get a password as it is hidden in another file with steganography.

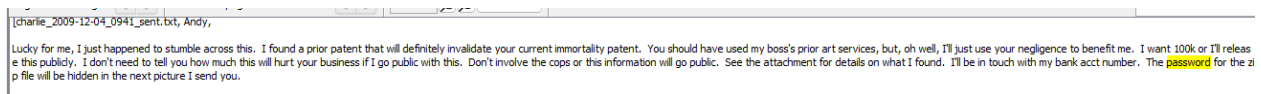


Figure 11: Suspicious email from charlie about the password file.



Figure 12 shows a suspicious email from Charlie telling someone what the password is to uncover the password hidden in the stego file. There is also the ending direction to delete the emails that he is sending him, which is suspicious.

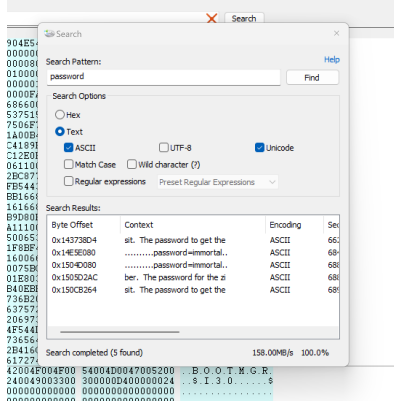
[charlie\_2009-12-04\_1306\_sent.txt, ],

Got the deposit. The password to get the info is nitro. Use the steg program we talked about. And don't forget to delete these emails.

C

Figure 12: Another suspicious email with a second password for the steg file.

It is important for forensic specialists to know how to use multiple different forensic softwares. Figure 13 below is a table comparing Autopsy's results of task 2 vs OSForensics's results to task 2.

Aspect	Autopsy	OSForensics
UI	One pane with everything on the left side	Separate panes on the left side for each ability
Keyword searching	Keyword search that is less specific but more user friendly.	 <p>The screenshot shows the OSForensics Search dialog box. The search pattern is 'password'. The search options are set to Text, ASCII, and UTF-8. The search results are displayed in a table with columns for Byte Offset, Context, Encoding, and Size. The results show four matches for the keyword 'password' at various byte offsets.</p>
Password searching	Able to find the password file automatically	Unable to detect the password file automatically.

## **Conclusion**

It is very important for digital forensic professionals to be able to find all kinds of data and files on a variety of operating systems. On a UNIX drive, it was tasked to investigate a certain person. Forensic investigators should be able to quickly and efficiently keyword search files and know what places to look for files pertaining to a certain person. This ability makes the criminal investigation process much quicker, accurate, and more efficient for both parties. It is also important for forensic investigators to be able to make sense of the files that they come across. Task 2 provided email files that had suspicious conversations on them. As a forensic specialist, it is important to be able to follow the email conversation and extract whatever data is relevant to the criminal investigation. Mentioning of steganography was included in the emails, and it is vital that an investigator knows what this process is and how it works in order to obtain the maximum amount of data possible.

**Appendix A: Time Chart**

**Time Chart**

Task Number	Time Taken
Task 1	20 minutes
Task 2	40 minutes
Report Writing	1 Hour
Total	2 hours