Digital Forensics (DFAa 22/23L)

Forensic Report: The Rhino Case

Team:

Óscar Alexander Martín Tacoronte – 252841 – Erasmus Group

Contents

1 Introduction and overview

The University of New Orleans' network administrator reported illegal rhinoceros traffic to the police after their RHINOVORE system flagged it. This report presents the findings of the forensic investigation conducted by Oscar Martin Tacoronte regarding the illegal possession of rhinoceros images by the primary user of a computer belonged to one of the University´s laboratories of the University of New Orleans. In 2004, a law was passed in New Orleans criminalizing the possession of nine or more distinct rhinoceros images

The investigation involved analyzing a computer and USB key obtained from one of the University's laboratories, as well as three network traces provided by the network administrator.

The following evidences is followed:

- The dd image of the imaged USB key was analyzed using two forensic softwares to identify and extract all relevant files and data.
  - RHINOUSB.dd

- The three network traces were analyzed to identify any suspicious network activity related to the possession of rhinoceros images. Some objects could be extracted and analyzed individually.

  - rhino.log
  - rhino2.log
  - rhino3.log

2 Tools, techniques and finding steps

2.1 Active@ Disk Editor

Firstly, it analyzes the current USB image “RHINOUSB.dd”.

1. Start Disk Editor
2. Open Disk Image
3. Select “Al files (*.*)”, and select the dd image

Evidences found in this first step:

- Two healthy files, it metadata and status of these files.
- Two kitchen recipes (Right click on these files and file preview)

Figure 1: Overview of the USB image current status

2.2 Autopsy

Secondly, it analyzes the USB image “RHINOUSB.dd” and carve out the files:

1. New case
2. Set name, number of case and your working directory for this case
3. Generate new host name base don data resource name
4. Select unallocated space image file
5. Browse and select the dd image
6. Do not break up the image
7. Select all modules and finish

Evidence found in this step:

1. Open the tree like in Figure 2, and there are 134 carved files

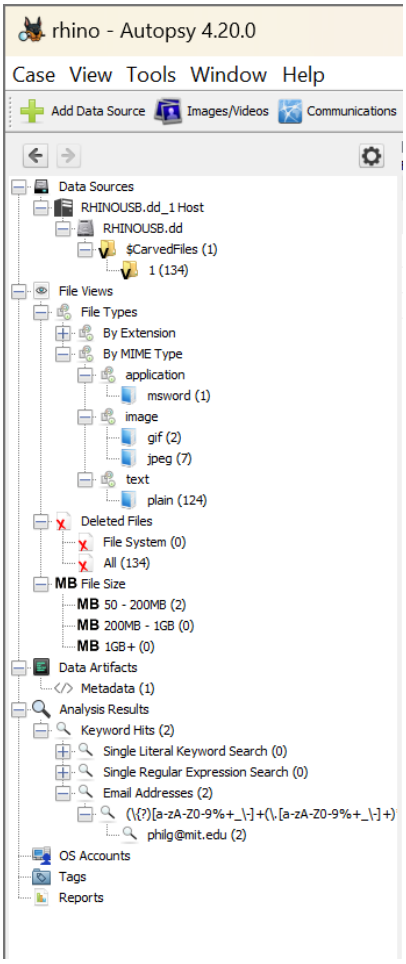

Figure 2: image dd tree analysis result

2. We can see under File Views:

   a. 134 Files deleted, which:
      i. 1 is a office document
      ii. 2 are gifs, 7 are images
      iii. The others are plain text

   b. Select both gif and jpeg Types, then Thumbnail. There is evidence of 2 rhinos image carved (jpeg) and two rhinos gif in Figure 3.

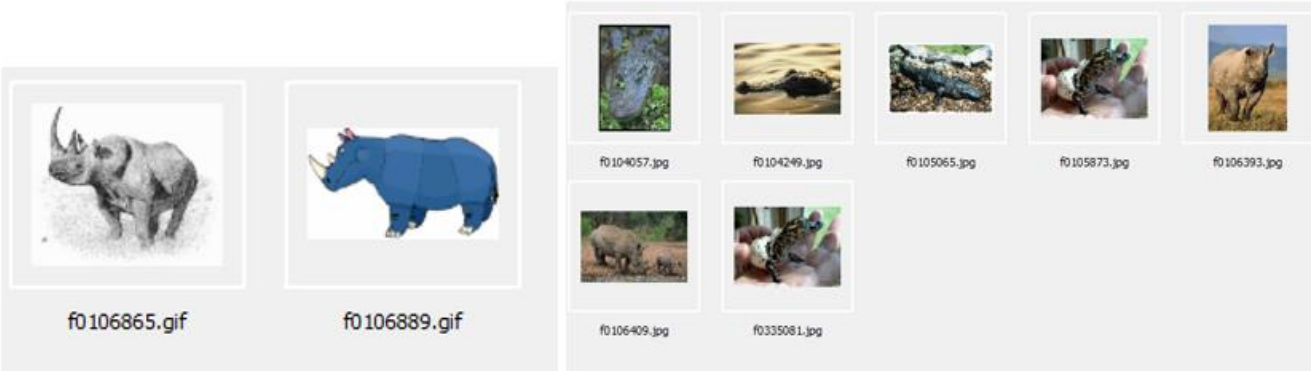

Figure 3: images carved from USB image

   c. Select “msword” and then select the one carved document found, and press the shortcut “CTRL + E”
      i. We can read a document which was deleted with important information. This will be too important to the final conclusions in the next points.

3. Under Data Artifacts:
    a. Select Metadata and then, the one document file.
        i. We can see the date created of this document in figure 4: 2005-08-09

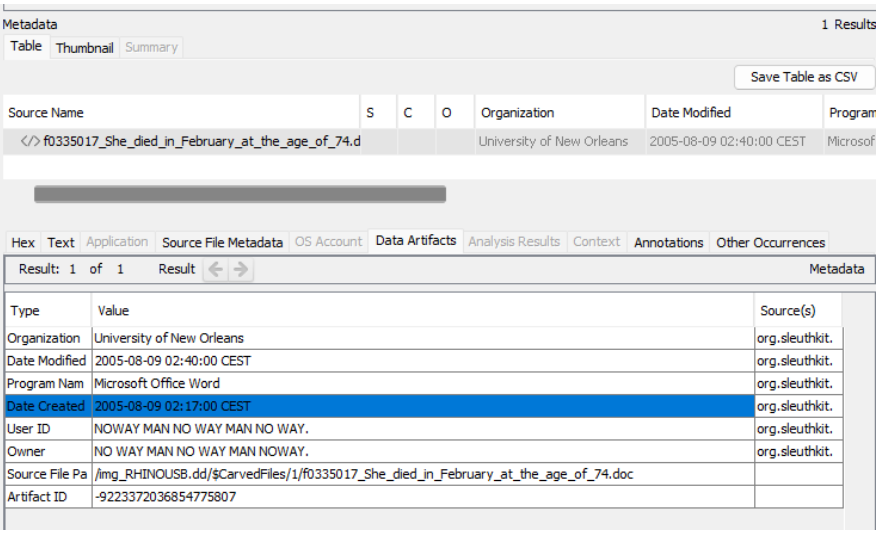

Figure 4: Metadata of the word document

4. Under Analysis Results
    a. Select the "philg@mit.edu(2)"
        i. We can see an email hidden in one file

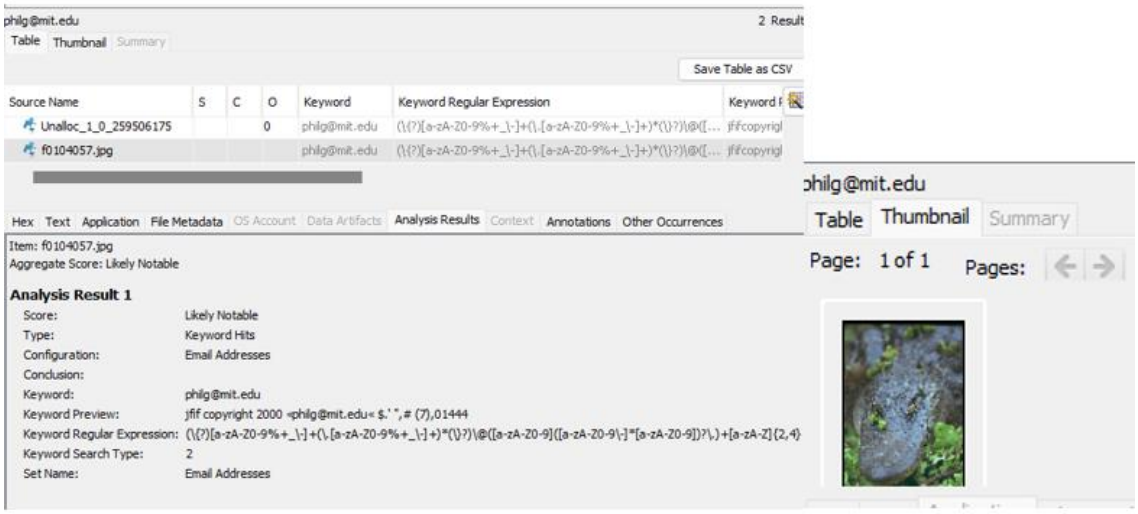

Figure 5: email hidden in a image

2.3 Wireshark

Thirdly, it analyzes the network traces:

1. File
2. Open
3. Select any of the three log network files

Evidences found in this step according each “log” file:

i rhino.log

1. In Apply “http” filter and, press shortcut “CTRL + F” and write “premail”. Then, select you are looking for a “string”, and search “packet details”, how it is shown in Figure 6

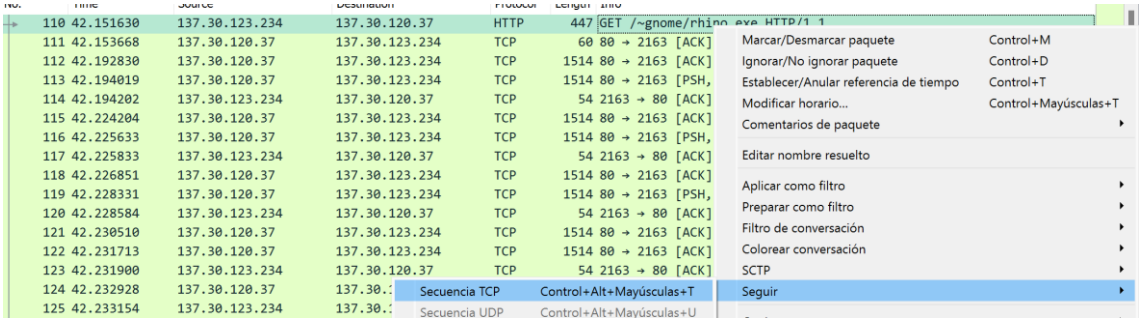

Figure 6: Filter configuration

a. Packet 2600 and Packet 5331 evidences:

   i. Someone names “John” with the login of “hugerhinolover” uploads rhino images on the gnome account on the hosting cook.cs.uno.edu.
   ii. The suspect login with "bighonkingrhino" and the evidence suggests that suspect login in the laboratory of the laboratory of the University.

2. Apply FTP filter as shown in Figure 7 and we can see the credentials found for the gnome account

Figure 7: FTP filter

3. Go to File → export object →FTP-DATA as shown in Figure 8
    a. Download all files as shown in Figure 10:
        i. we can see more rhino images, and a zip file which a another rhino image which cannot open because is protected with a password. The name “contraband.zip” is suspect:
            i. An online password recovery got the password (see reference[3]) and it is another rhino image as we can see in Figure 11

    b. We can see in the Figure 9, how the suspect stored rhino image in a server (At the packet 1546, where suspect execute a STOR FTP command, select right click, follow frames TCP)

    c. Server “cook” were used to allocate the rhinos photos as shown in Figure 18. (Apply “gnome” string filter with the shortcut “CTRL + F”). Then, if we follow the TCP secquency, we can find the Figure 19 (Right click → follow TCP sequency) how the suspect changed it password.

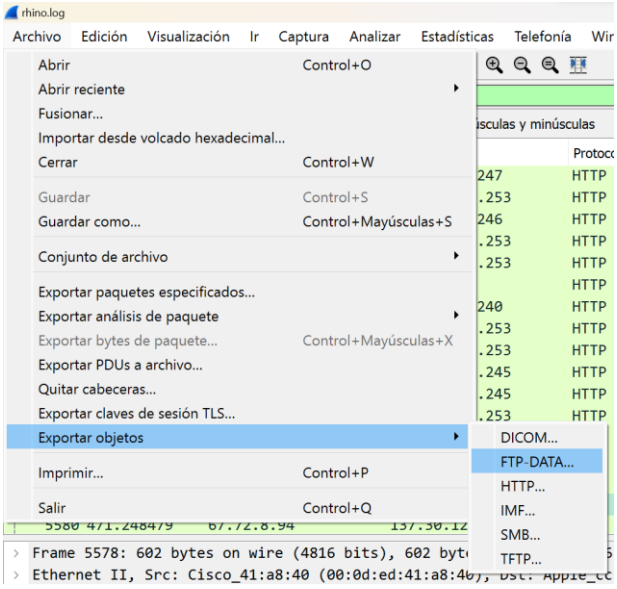

Figure 8: how to export FTP-DATA object

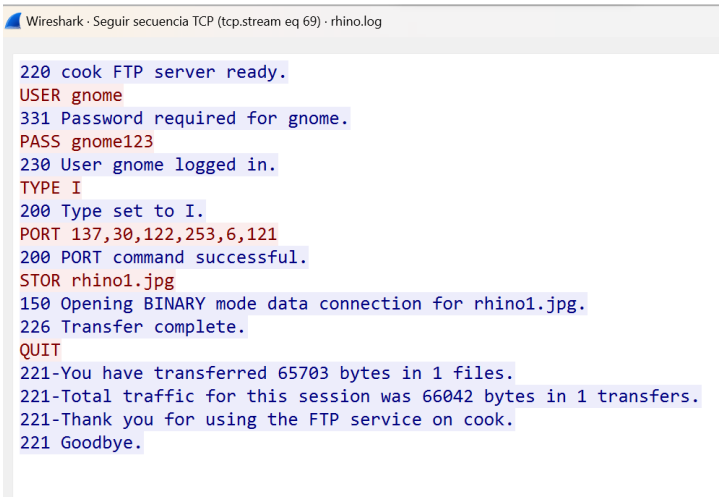

Figure 9: follow FTP packet

Figure 10: result of downloaded FTP-DATA

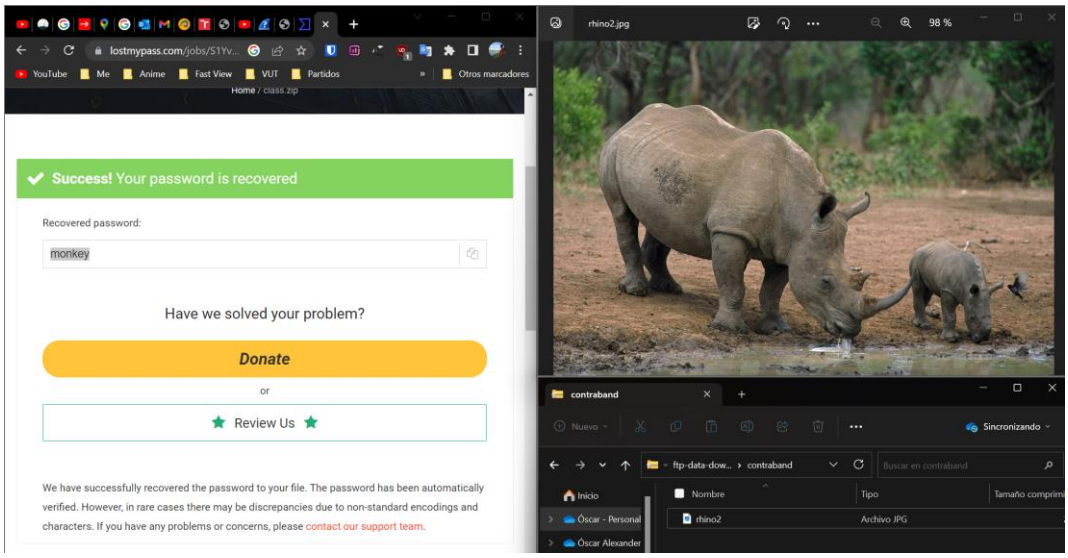

Figure 11: Descrypted zip file, Another rhino image

```
Data: \r\n
Data:         Today is .......................Mon Apr 26 17:17:36 CDT 2004\r\n
Data:         Your system identification is ...uid=2287(gnome) gid=2000(cscistu)\r\n
Data:         Your terminal address is ......../dev/pts/5\r\n
Data:         Your current directory is ........./home/gnome\r\n
Data:         Your file creation mask is ......022\r\n
Data:         Your server name is .............cook\r\n
Data:         Processor ......................sparc\r\n
Data:         Operating System ................sun solaris v5.9\r\n
Data: cook:[gnome]$
```

Figure 18: cook server

```
Wireshark · Seguir secuencia TCP (tcp.stream eq 60) · rhino.log
mailhost:/var/mail   10323610 8706021 1514353    86%    /var/mail
magellan:/export/home/stu/smandele
                     86624998 46589158 39169591    55%    /home/smandele
magellan:/export/home/stu/nsalmano
                     86624998 46589158 39169591    55%    /home/nsalmano
pigafetta:/export/home/project/java
                     15487083  278319 15053894     2%    /apps/java
magellan:/export/home/stu/vchinta
                     86624998 46589158 39169591    55%    /home/vchinta
magellan:/export/home/stu/gnome
                     86624998 46589158 39169591    55%    /home/gnome
cook:[gnome]$ llss  --ll

total 264
-rwxr-xr-x   1 gnome    cscistu     2307 Feb 26 18:26 Xinitrc.XFce
-rw-r--r--   1 gnome    cscistu      269 Feb 26 17:17 cshrc.user
-rw-r--r--   1 gnome    cscistu   117773 Apr 21 16:41 golden.jpg
cook:[gnome]$ ppaassswwdd

passwd: Changing password for gnome
Enter existing login password: gnome123

New Password: gnome1234

passwd: Old and new passwords must differ by at least 3 positions.

Please try again
New Password: gnome12345

Re-enter new Password: gnome12345

Permission denied
cook:[gnome]$ llooggoouutt
```

Figure 19:Attempt of changing password found

ii rhino2.log

1. Go to File → export object →HTTP

   d. Download rhino4, rhino5 and index.html. The result is in figure 12, and we can see two unrealistic rhino image, and one html page (see Figure 13) where we can see this email: venkata@cs.uno.edu in the html file (see Figure 14)

      i. In packet 28 we can see a grnome get request, from the host www.cs.uno.edu as well. Evidence suggest a relation between this email and this suspect gnome account which later in pakcet 49 we see a to get request one rhino gif (see figure 13) shown in figure 12.

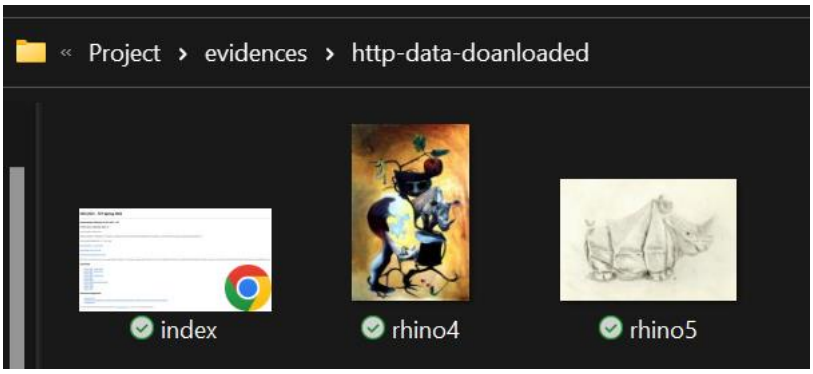

Figure 12: unrealistic rhinos images

48	6.292513	137.30.123.234	137.30.120.37	TCP	54	2028 → 80 [ACK] Seq=271 Ack=500 Win=63741 Len=0
49	7.892558	137.30.123.234	137.30.120.37	HTTP	488	GET /~gnome/rhino4.jpg HTTP/1.1
50	7.919004	137.30.120.37	137.30.123.234	TCP	1514	80 → 2026 [ACK] Seq=2590 Ack=1745 Win=49640 Len=1460

Figure 13: get request for rhino image with gnome

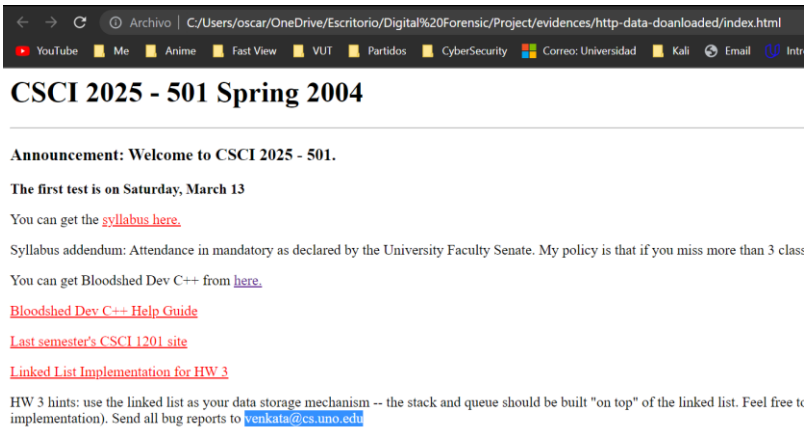

Figure 14: GUI of index.html

iii rhino3.log

1. We can see in figure 15 a get request for executing a rhino.exe from the host seen in rhino2.log

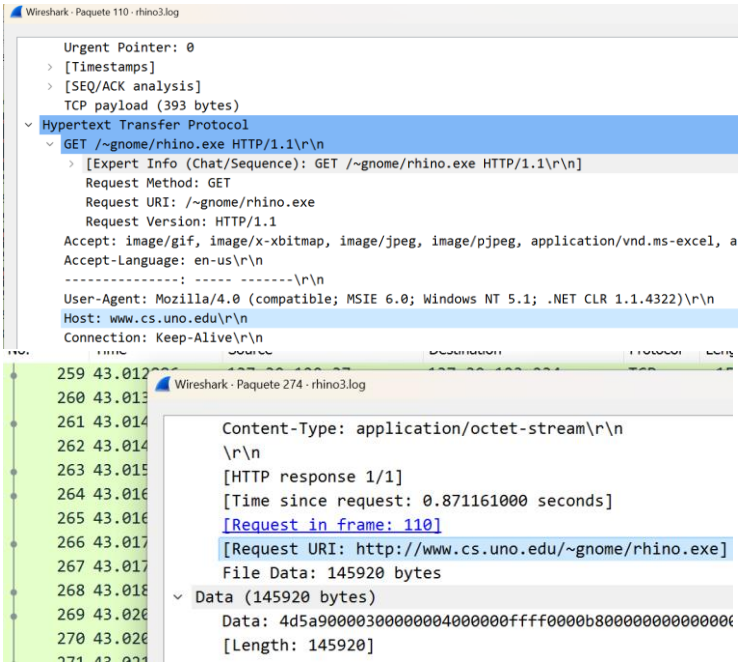

Figure 15: get request for rhino.exe execution

a. Go to File → export object →HTTP

   ii. Download rhino.exe

      i. This files is not a dangerous according to virustotal analysis (see reference of this tool in [4]), but it is a diskpart binary which evidences that suspect made some manipulations with disk.

      ii. Analysis of this file can be found:

https://www.virustotal.com/gui/file/93e70049b60bf5691b43d9e256ca8f459f6bfac832097985bcc6a9040b5ca555/details

b. At the packet 110, select right click, follow frames TCP as we can see in Figure 16, we can see in Figure 17 that suspect deleted the disk

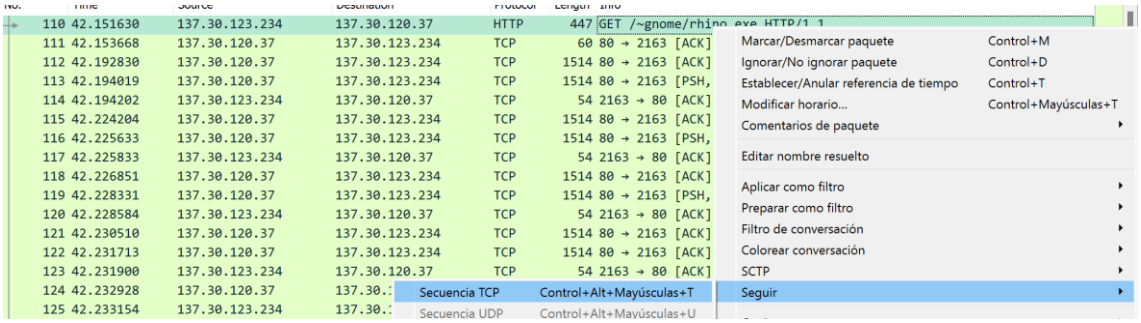

Figure 16: how to follow the flow of TCP sequency

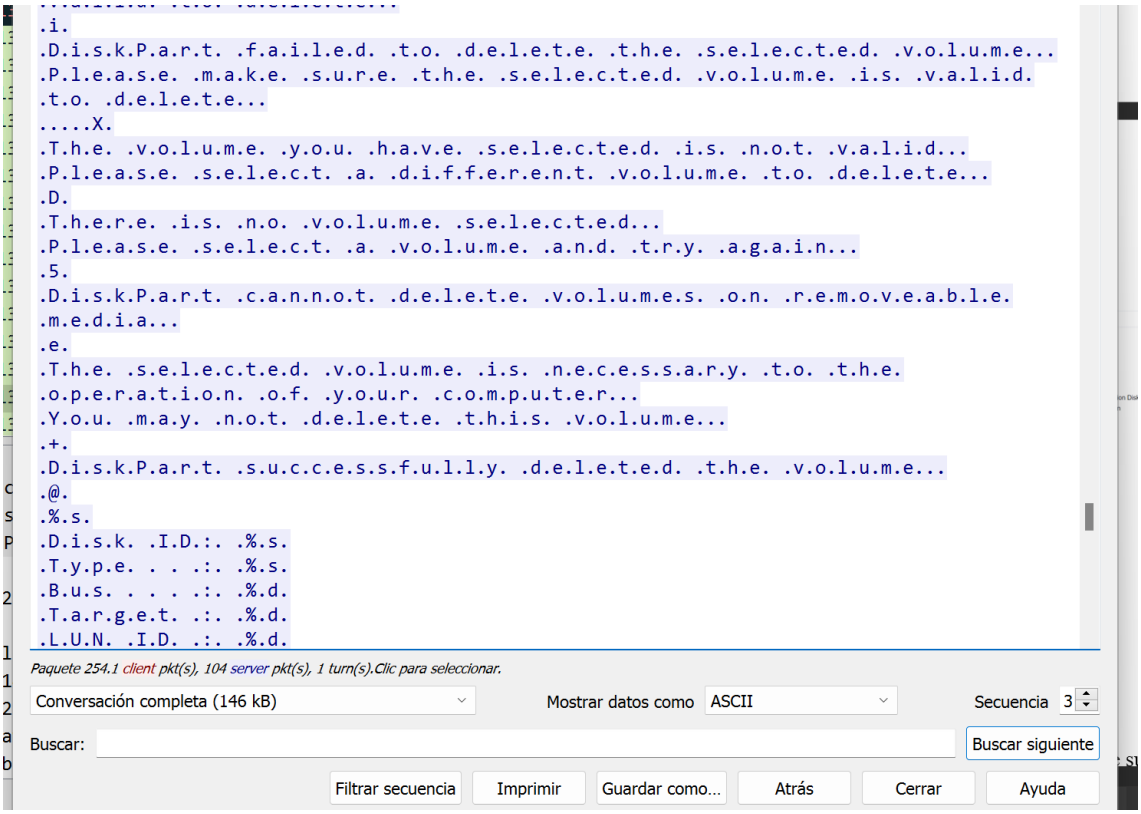

Figure 17: diskpart deleted, flow of TCP sequency of the packet 110

3 Executive summary of findings

- Jeremy provided a FTP account to the suspect, and the suspect set the credentials for this account:

  - User: gnome
  - Password: gnome123

- The hard drive of computer mainly used by the suspect was deleted, and later destroyed. It can be found on the Mississippi River.

- The USB Key was completely reformatted after allocating 2 carved rhinoceros, 124 unknown plain text documents, 1 office documents, and others images which includes variaty of themes amd unrealistic rhinos images or GIFs. However, the USB image still remains two healthy txt files, which they contain recipes kitchen intructions.

- It can retrieves from image of the USB (more specifically from a carved office document) that suspect had the following information:
  - Suspect knew that allocating 9 or more images of rhinos is illegal, and also admitted this situation "makes me sick"
  - Suspect tried to hid the photos following these steps:
    - Suspect reformartted the USB
    - Suspect destroyed the hard drive from it computer.

- There is evidences that support a connections between the USB and the network traces. These are:

  - The text found on the carved office document on the USB which says "I need to change the password on the gnome account that Jeremy gave me." And the traces which we can see a login request of the gnome account over FTP protocol

  - One rhino image carved in the USB Key is equal to one image found in one FTP trace. A object "contraband.zip" could be unzip, then the image could be shown and compared

4 Findings and evidence

Jeremy provide FTP account to the suspect, and the suspect changed the credentials (credentials can be found in point 3). This evidence were found on the USB image from the carved document

Suspect connects with gnome account on the 26th of April to server “cook”, then tryied to change the gnome password “gnome123” to “gnome12345” but permission denied. Then, suspect stores the rhinos images (rhino1, rhino2 both jpg files, and the contraband.zip) into the cook server. This happned on the 26th of April. We also confirm the relation between the USB and network traces. This evidence were found on the rhino.log

Later, on the 28th of April, we can see more files transferred to the server at the www.cs.uno.edu. This evidence were found on the rhino2.log

Lastly, on the 28th of April, suspect deleted the diskpart. This evidence were found on the rhino3.log

5 Conclusions and opinions formed

There is no digital evidence to inculpatory the suspect as there are not 9 or more distinct rhinos images found.

During this investigation, 2 rhinos images carved were found on the USB image, 2 rhinos images were found on network traces, 2 rhinos gif were found on the USB image and 2 rhinos gif were found on the network traces, which results that the total images of rhinos is 8.

However, as seen in the document carved and in the rhino3.log evidence, the hard drive of the computer were destroyed and non-analyzed.

The documents, files and data artifacts found that reasonably the suspect tried to hid the evidence related to the allocation of the images and even destroyed the hard drive of the laboratory of the University of New Orleans.

No exact evidences were found between the cook recipes in the USB documents carved, which the investigation suggest a relationship between these recipes and the cook.cs.uno.edu. In fact server, “cook” were used for the suspecct to allocate the rhino images but no useful information provided the two recipes files. Email hidden found in one image carved out of the USB in the point 2.2 (“philg@mit.edu”), were not useful for this investigation.

6 References

[1] Active Disk Editor, from:

https://www.disk-editor.org/index.html

[2] Autopsy®, from:

http://www.sleuthkit.org/autopsy

[3] Zip Password recovery, from:

https://www.lostmypass.com/file-types/zip/

[4] VirusTotal, from:

https://www.virustotal.com/gui/home/upload

[5] Wireshark, from:

https://www.wireshark.org/