HOMEWORK 5 CSEC-450 rhino REPORT – TASKE 5

DATE: 2/28/2025 – ERIC SOMOGYI – ID #2180405

Rhino-report.pdf

Prompt: Your task is to find at least one rhino picture in the data using any combination of tools that you like. Write a report with text and images/screenshots that describes how you found the picture. You should include screenshots of any commands/tools that you run to find and extract the rhino picture, and you should explain any reasoning that you have for why you run those commands (including why you choose particular offsets, for example).

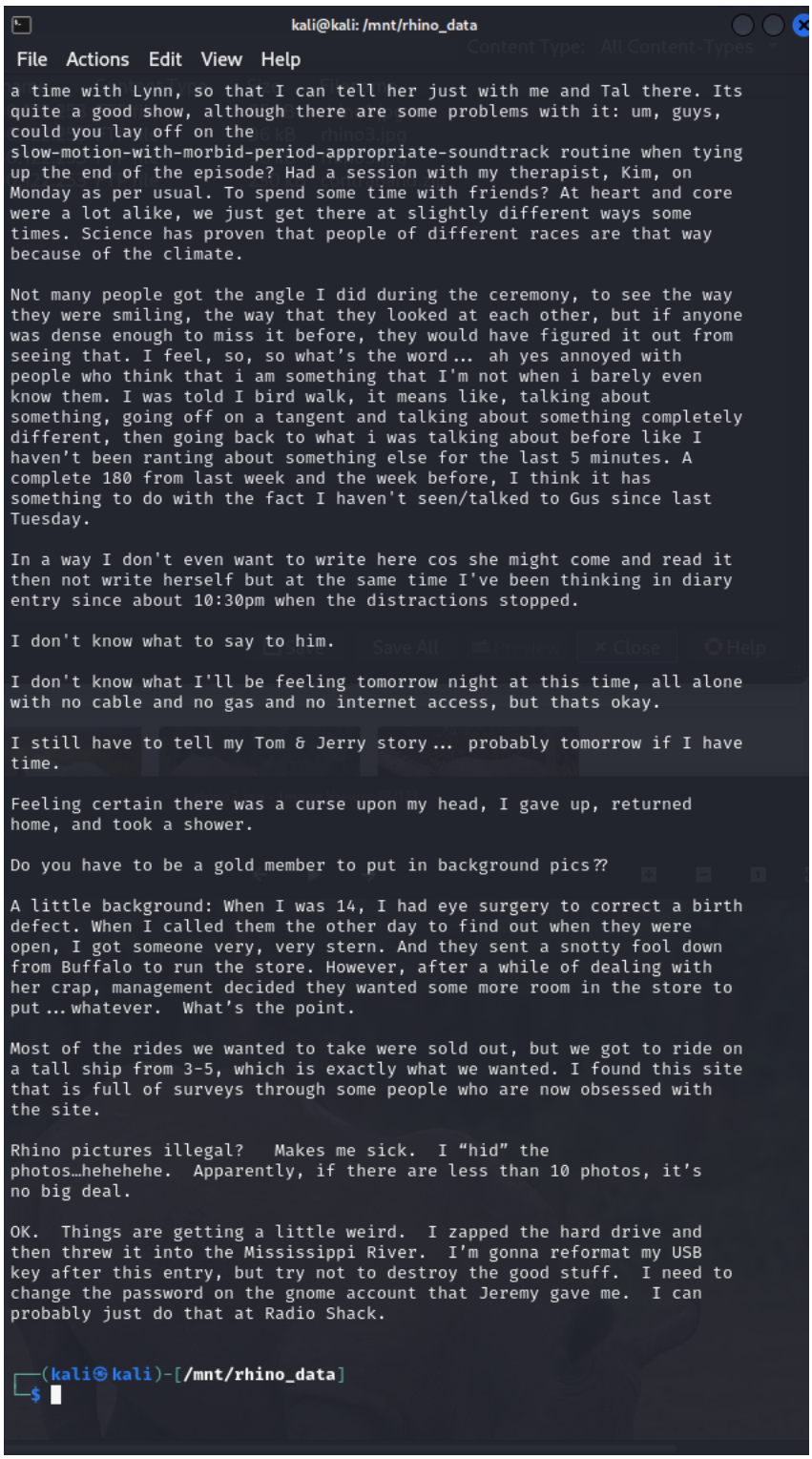
Questions/Answers:

- Who gave the accused a telnet/ftp account?

  Answer: Jeremy gave the accused the telnet/ftp account. I found this answer by finally getting into the diary which is the 00335017.ole file which is seen below. I included multiple screnenshots to show how I got to this result. (I did this last right before the assignment was due) See screenshot below:


kali@kali: /mnt/rhino_data
File Actions Edit View Help
┌──(kali㉿kali)-[~/Downloads/rhino]
└─$ cd /mnt/rhino_data
┌──(kali㉿kali)-[/mnt/rhino_data]
└─$ ls -la /mnt/rhino_data/ole
ls: cannot access '/mnt/rhino_data/ole/00335017.ole': Permission denied
ls: cannot access '/mnt/rhino_data/ole/..': Permission denied
ls: cannot access '/mnt/rhino_data/ole/.': Permission denied
total 0
d????????? ? ? ? ? ? .
d????????? ? ? ? ? ? ..
-????????? ? ? ? ? ? 00335017.ole
┌──(kali㉿kali)-[/mnt/rhino_data]
└─$ sudo ls -la /mnt/rhino_data/ole
[sudo] password for kali:
total 40
drwxr-xr-- 2 root root 4096 Feb 28 22:55 .
drwxr-xr-x 5 root root 4096 Feb 28 22:55 ..
-rw-r--r-- 1 root root 31744 Feb 28 22:55 00335017.ole
┌──(kali㉿kali)-[/mnt/rhino_data]
└─$ sudo ls -la /mnt/rhino_data/gif
total 28
drwxr-xr-- 2 root root 4096 Feb 28 22:55 .
drwxr-xr-x 5 root root 4096 Feb 28 22:55 ..
-rw-r--r-- 1 root root 11407 Feb 28 22:55 00106865.gif
-rw-r--r-- 1 root root 4105 Feb 28 22:55 00106889.gif
┌──(kali㉿kali)-[/mnt/rhino_data]
└─$ libreoffice
Command 'libreoffice' not found, but can be installed with:
sudo snap install libreoffice # version 24.8.4.2, or
sudo apt install libreoffice-common
See 'snap info libreoffice' for additional versions.
┌──(kali㉿kali)-[/mnt/rhino_data]
└─$ catdoc
Command 'catdoc' not found, but can be installed with:
sudo apt install catdoc
Do you want to install it? (N/y)y
sudo apt install catdoc
Installing:
catdoc
Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1432
Download size: 89.8 kB
Space needed: 702 kB / 49.1 GB available
Get:1 http://kali.download/kali kali-rolling/main amd64 catdoc amd64 1:0.95-5 [89.8 kB]
Fetched 89.8 kB in 0s (343 kB/s)
Selecting previously unselected package catdoc.
(Reading database ... 400883 files and directories currently installed.)
Preparing to unpack .../catdoc_1%3a0.95-5_amd64.deb ...
Unpacking catdoc (1:0.95-5) ...
Setting up catdoc (1:0.95-5) ...
Processing triggers for mailcap (3.74) ...
Processing triggers for kali-menu (2024.4.0) ...
Processing triggers for man-db (2.13.0-1) ...
┌──(kali㉿kali)-[/mnt/rhino_data]
└─$ catdoc /mnt/rhino_data/00335017.ole
catdoc: No such file or directory
7 kB 100.0%

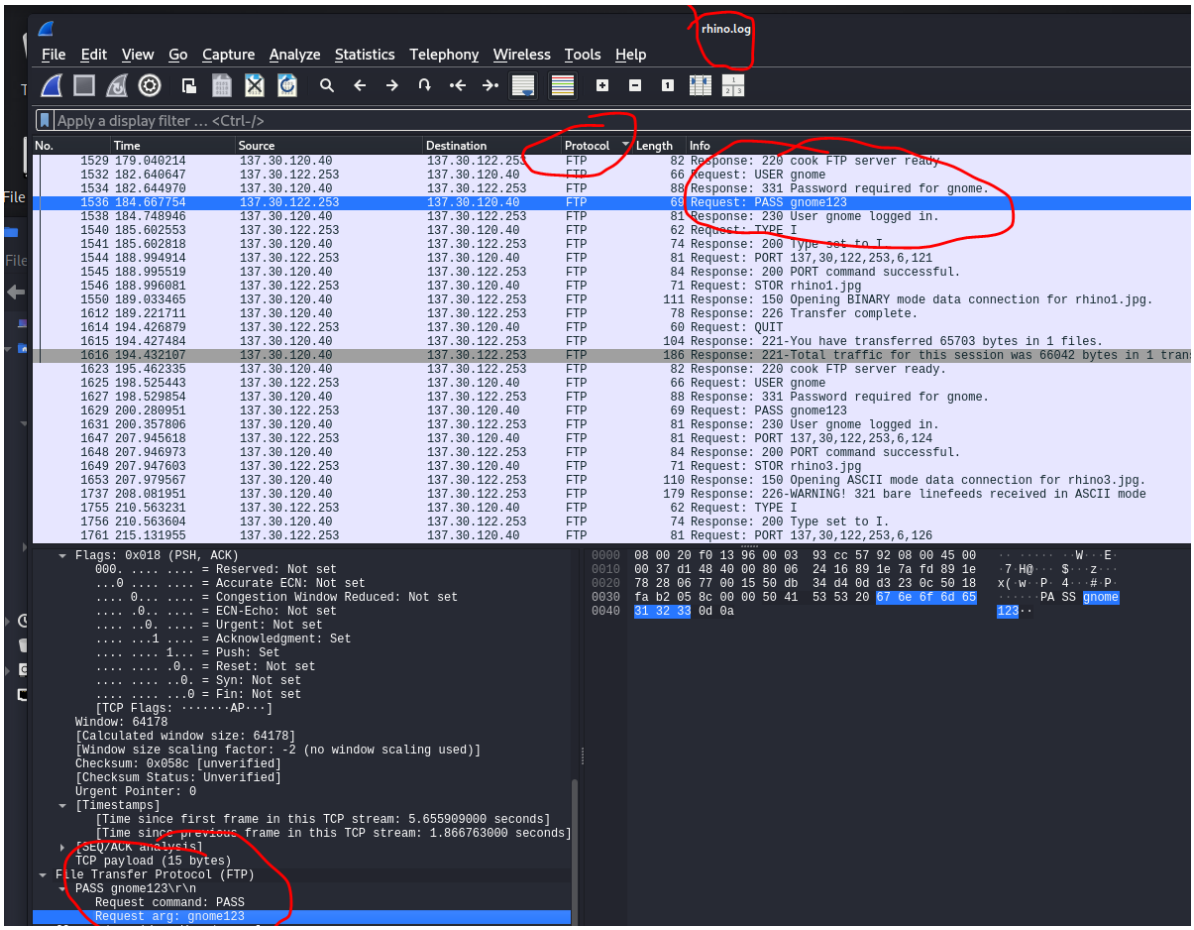

kali@kali: /mnt/rhino_data
File Actions Edit View Help
┌──(kali㉿kali)-[/mnt/rhino_data]
└─$ catdoc /mnt/rhino_data/00335017.ole
catdoc: No such file or directory
┌──(kali㉿kali)-[/mnt/rhino_data]
└─$ catdoc /mnt/rhino_data/ole/00335017.ole
catdoc: Permission denied
┌──(kali㉿kali)-[/mnt/rhino_data]
└─$ sudo catdoc /mnt/rhino_data/ole/00335017.ole
She died in February at the age of 74. In August 2001 it wasn't a
decision, since the alternative was regret. It wasn't her fault that I
didn't go to the drugstore... And then getting her to arrange a time
with Lynn, so that I can tell her just with me and Tal there.
We were walking from the restaurant to the Irish pub, and who did we run
into? Then we had dinner at this really nice restaurant with a patio
kind of in Old Town.
Back in March I did a presentation at a research conference held at UC
Irvine and presented by the Honors Transfer Council of California.
My mother and I have a unique relationship. Chasing Amy - *whimpers* By
all accounts i should have liked this film. Their relationship was a
failure! All other IB families are trying to keep their kid in IB..
trying to encourage their kid to do good.. mine is trying to make me
quit. Anyway, this one is someone she was involved with in high school
who says he's been trying to find her all these years and finally
tracked her down. So seeing how I am scared of pitch black darkness I
got up and was trying to see what made the power go out, and my parents
got up and joined me with flashlights and candles. I handed in the damn
homework, which was really quite stupid for all those who do know how to
use the damn computer. He turned back to me, completely sober,
completely serious and replied - 'No, I don't dislike you, I'm just
scared of you.' I stared at him in disbelief for a moment or two or
three - scared of me?
There truly are buckets of phenomenal things to be amazed by, and
thankful for.
Stocklos and Andrew were only there for one of the nights I was.
Then there was one 4th of July when we had just moved to a big new house
in the country & we were flat busted, so we had no funds to celebrate.
But Jon and been watching the encounter and remained at bay purposely in
order to let me say what I had to say to Andrew. I am so excited about
the trip... and so excited that Jen and Nicole are going... and so
excited that we are going to both Wolves games while we are there. And
she attempted lying to me about going Hong Kong together. And look, it's
very difficult to work both sides of the aisle.
It might last. MILLER, who actually taught my HIS 102 class last
semester, and he was the last class I had last time, and the first class
this time.
I've been so caught up in all this craziness going on and such!
This can be a very uncomfortable moment if someone walks in and busts
you.
I haven't brought it up to Amanda, but Stephen knows how uncomfortable
it is. It's all uncomfortable and awkward.
And it's so easy, we're an Irish family and all that implies.
So in honor of better times: heres something I wrote a year ago, a



- What's the username/password for the account?

  Answer: The username is gnome and the password is gnome123. I found this by looking in the rhino.log file. I first clicked the protocol column and sorted them by type. I scrolled to the top and was just scanning looking for any signs of username/passwords. In the screenshot below, it shows the username in the FTP request was for USER "gnome" and PASSWORD was "gnome123". I circled it in red

to show my findings in the screenshot below. FTP is unencrypted so it was easy to find this information right in the log just sitting there on my screen. See screenshot below:



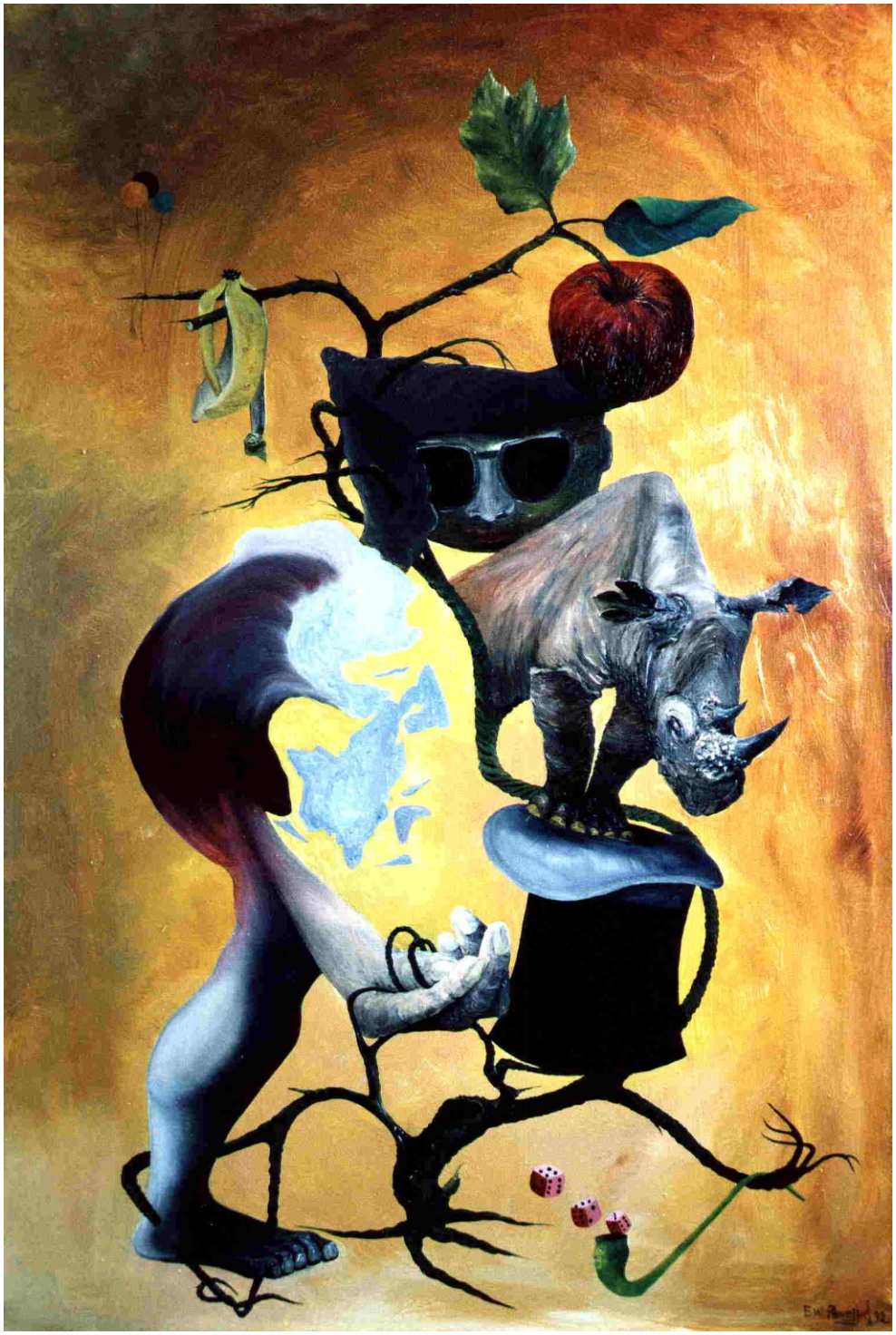
- What relevant file transfers appear in the network traces?
    - Answer: The relevant file that appears in the network traces are in rhino2.log which are: rhino5.gif and rhino4.jpg. I found these images in rhino2.log by opening the .log file in Wireshark and going to file → export objects → HTTP stream and saving the files to my folder. The relevant files that appear in rhino1.log are: rhino1.jpg, rhino3.jpg, and rhino2.jpg. I found these images in rhino.log by opening the .log in Wireshark and going to File → Export Objects → FTP-DATA → and saving the found filenames to my folder. Also in the export was contraband.zip, and I extracted it which is where I found rhino2.jpg but I had to put in a password monkey to get access. I found this password in the metadata in Wireshark. I right clicked on the contraband.zip and selected Extract and then was able to export the rhino2.jpg to my folder. The relevant files transfers that appear in rhino3.log are the rhino.exe application which I found by going to File → Export Objects → HTTP. I chose these commands because I have participated in CTF competitions and using Wireshark pcap and log files, I knew about going through the results and just going to File Export Objects to export any files that are found in the log.

See pictures below: Rhino1.jpg

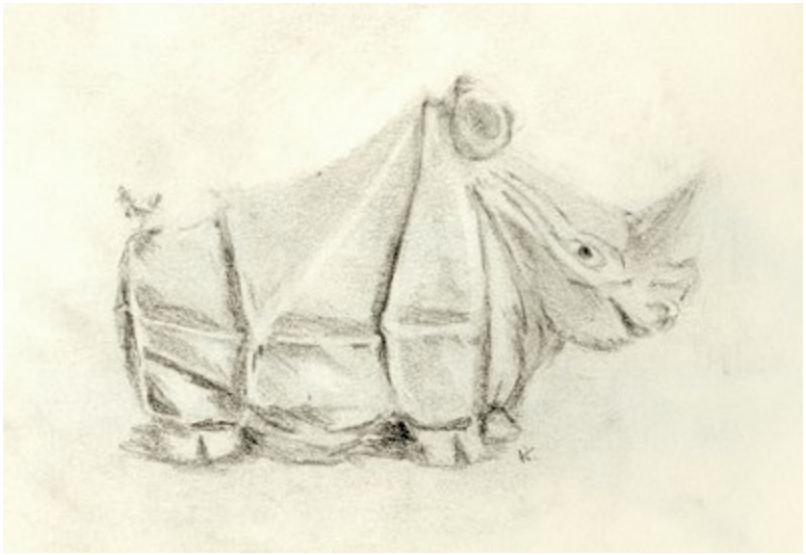
Rhino2.jpg

Rhino3.jpg

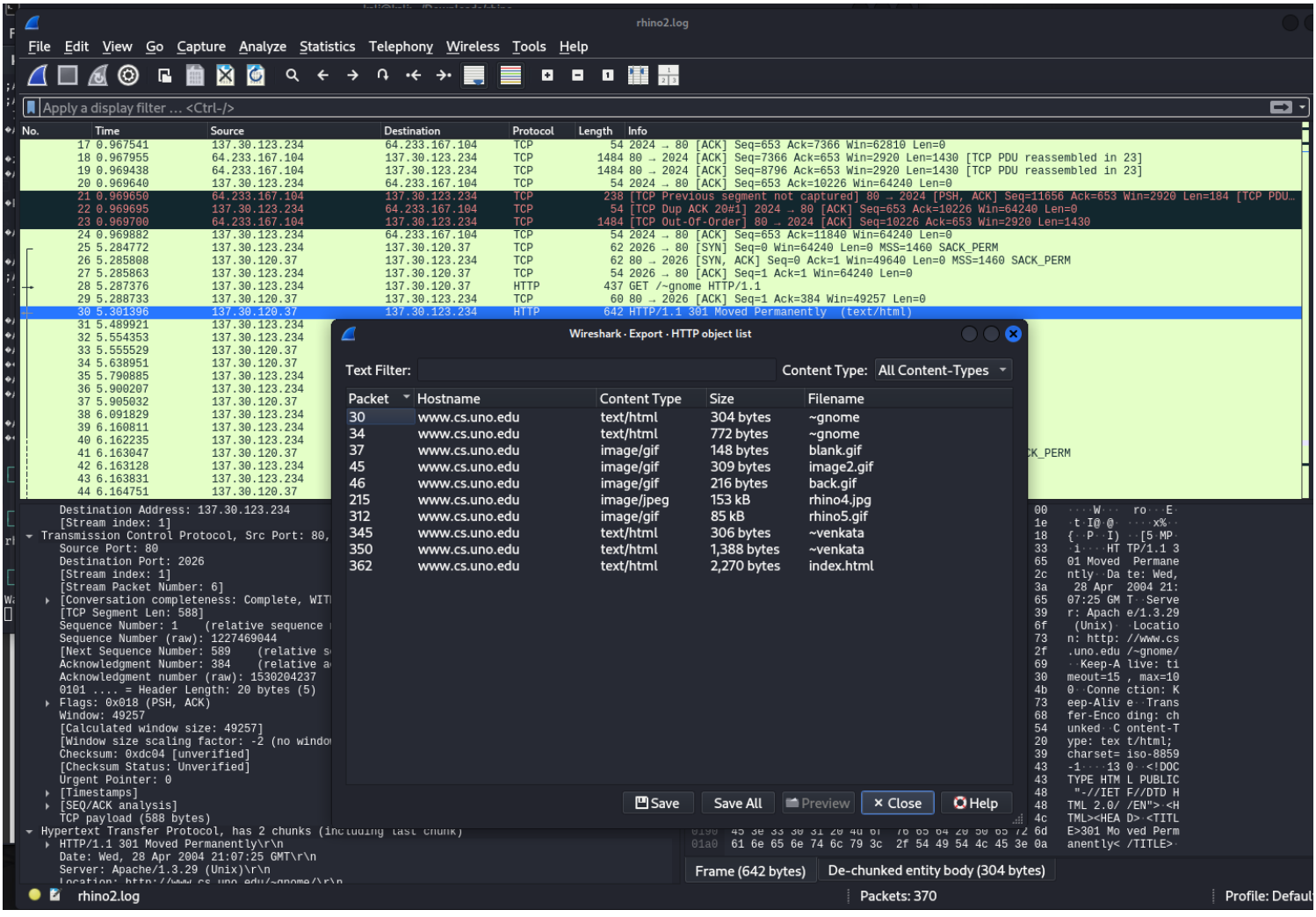
Rhino4.jpg

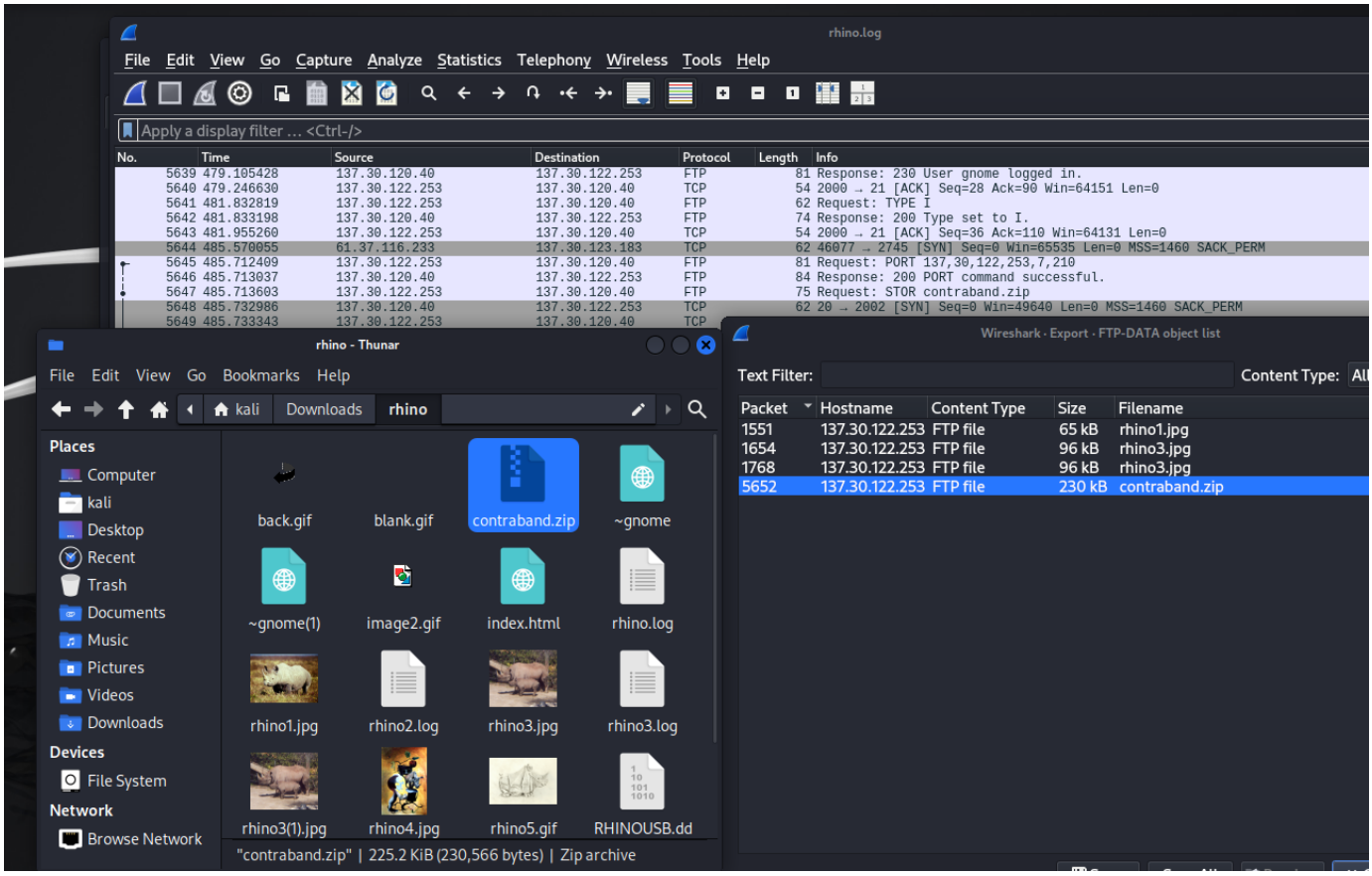


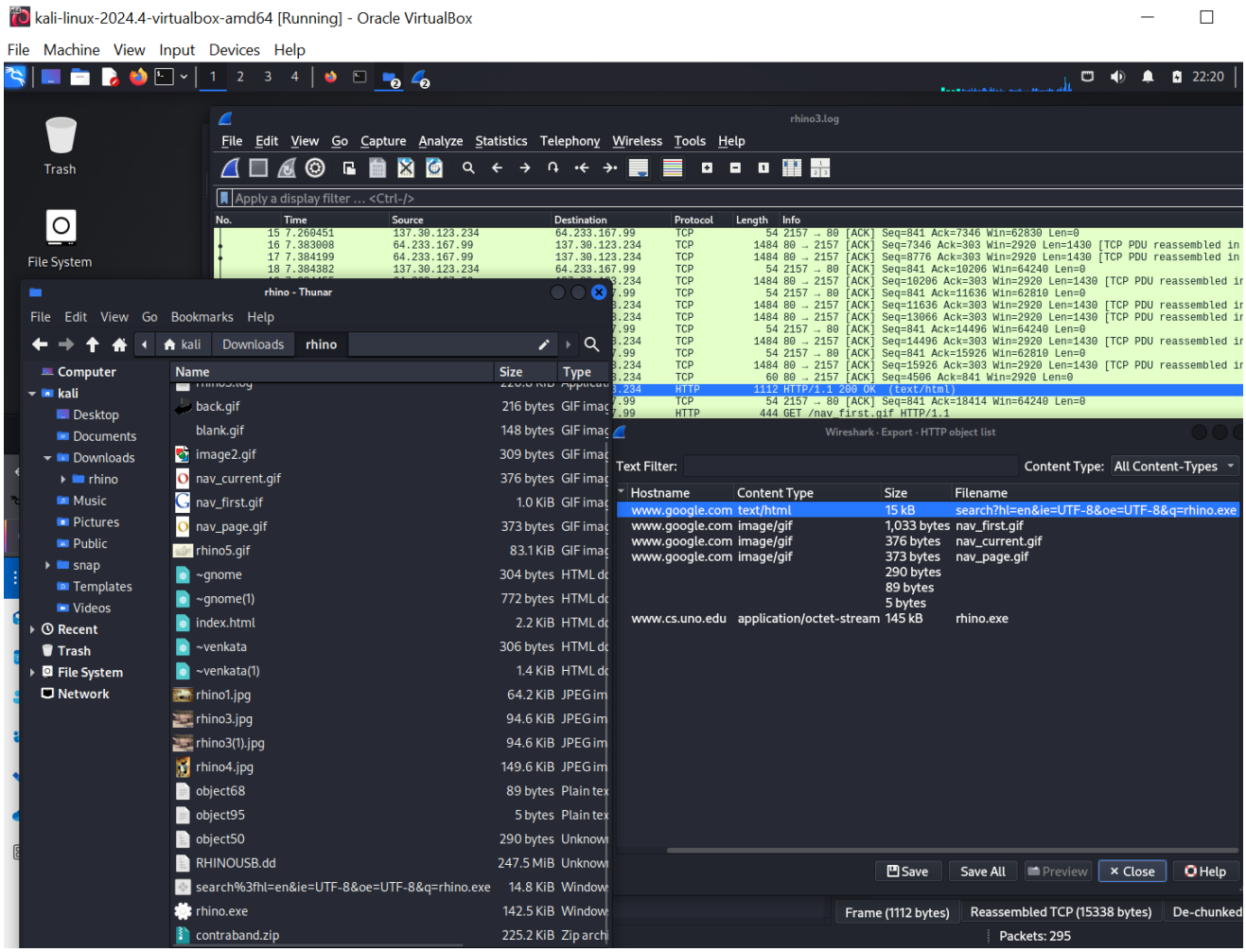
Rhino5.gif



3 Screenshots of me exporting from Wireshark of the 3 log files:

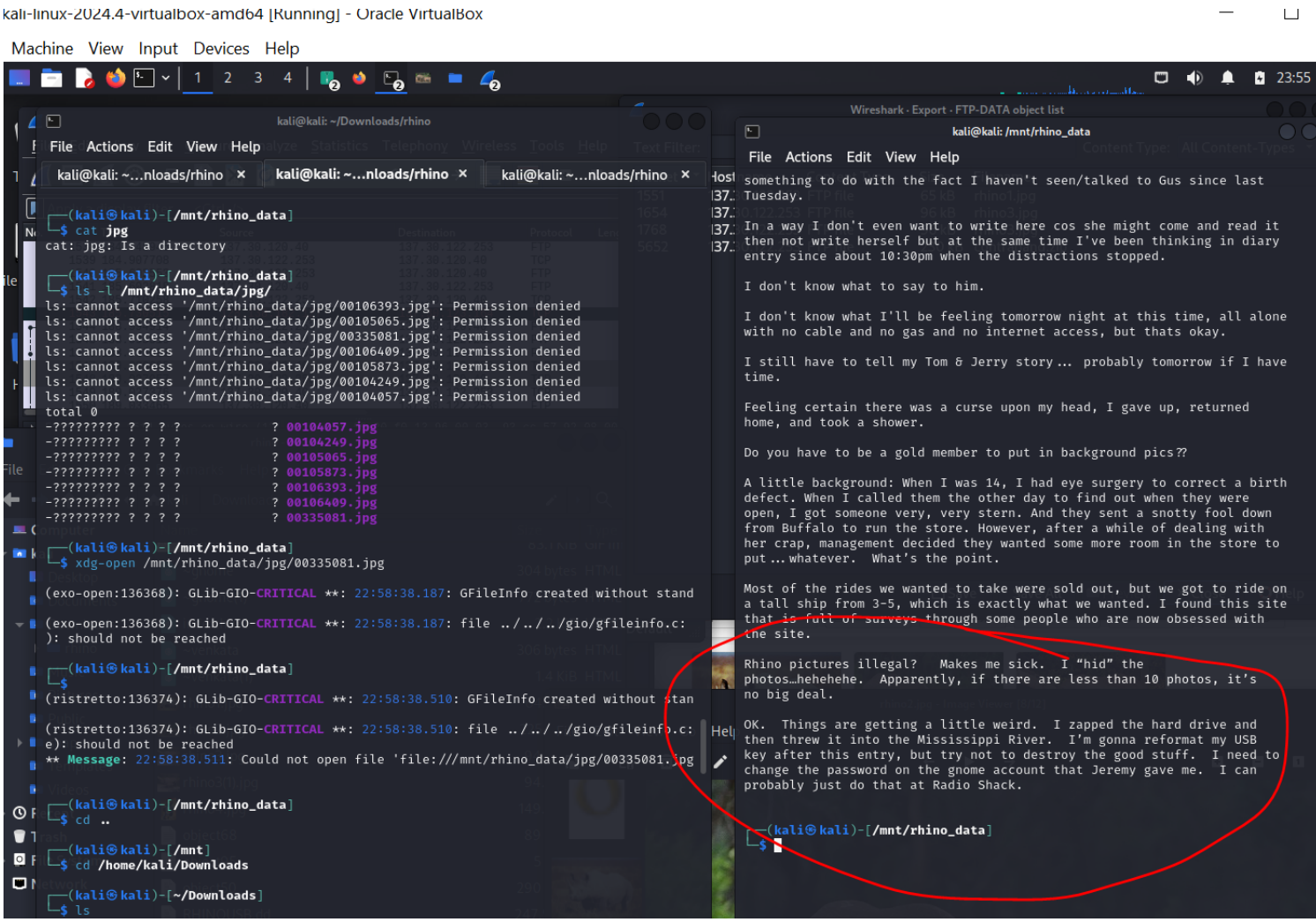



rhino.log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
5639 479.105428 137.30.120.40 137.30.122.253 FTP 81 Response: 230 User gnome logged in.
5640 479.246630 137.30.122.253 137.30.120.40 TCP 54 2000 → 21 [ACK] Seq=28 Ack=90 Win=64151 Len=0
5641 481.832819 137.30.122.253 137.30.120.40 FTP 62 Request: TYPE I
5642 481.833198 137.30.120.40 137.30.122.253 FTP 74 Response: 200 Type set to I.
5643 481.955260 137.30.122.253 137.30.120.40 TCP 54 2000 → 21 [ACK] Seq=36 Ack=110 Win=64131 Len=0
5644 485.570055 61.37.116.233 137.30.123.183 TCP 62 46077 → 2745 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
5645 485.712409 137.30.122.253 137.30.120.40 FTP 81 Request: PORT 137,30,122,253,7,210
5646 485.713037 137.30.120.40 137.30.122.253 FTP 84 Response: 200 PORT command successful.
5647 485.713603 137.30.122.253 137.30.120.40 FTP 75 Request: STOR contraband.zip
5648 485.732986 137.30.120.40 137.30.122.253 TCP 62 20 → 2002 [SYN] Seq=0 Win=49640 Len=0 MSS=1460 SACK_PERM
5649 485.733343 137.30.122.253 137.30.120.40 TCP
rhino - Thunar
File Edit View Go Bookmarks Help
kali Downloads rhino
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
back.gif
blank.gif
contraband.zip
~gnome
~gnome(1)
image2.gif
index.html
rhino.log
rhino1.jpg
rhino2.log
rhino3.jpg
rhino3.log
rhino3(1).jpg
rhino4.jpg
rhino5.gif
RHINOUSB.dd
"contraband.zip" | 225.2 KiB (230,566 bytes) | Zip archive
Wireshark · Export · FTP-DATA object list
Text Filter:
Content Type:
Packet Hostname Content Type Size Filename
1551 137.30.122.253 FTP file 65 kB rhino1.jpg
1654 137.30.122.253 FTP file 96 kB rhino3.jpg
1768 137.30.122.253 FTP file 96 kB rhino3.jpg
5652 137.30.122.253 FTP file 230 kB contraband.zip


kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
22:20
Trash
File System
rhino3.log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
15 7.260451 137.30.123.234 64.233.167.99 TCP 54 2157 → 80 [ACK] Seq=841 Ack=7346 Win=62830 Len=0
16 7.383008 64.233.167.99 137.30.123.234 TCP 1484 80 → 2157 [ACK] Seq=7346 Ack=303 Win=2920 Len=1430 [TCP PDU reassembled in
17 7.384199 64.233.167.99 137.30.123.234 TCP 1484 80 → 2157 [ACK] Seq=8776 Ack=303 Win=2920 Len=1430 [TCP PDU reassembled in
18 7.384382 137.30.123.234 64.233.167.99 TCP 54 2157 → 80 [ACK] Seq=841 Ack=10206 Win=64240 Len=0
rhino - Thunar
File Edit View Go Bookmarks Help
kali Downloads rhino
Computer
kali
Desktop
Documents
Downloads
rhino
Music
Pictures
Public
snap
Templates
Videos
Recent
Trash
File System
Network
Name Size Type
back.gif 216 bytes GIF imag
blank.gif 148 bytes GIF imag
image2.gif 309 bytes GIF imag
nav_current.gif 376 bytes GIF imag
nav_first.gif 1.0 KiB GIF imag
nav_page.gif 373 bytes GIF imag
rhino5.gif 83.1 KiB GIF imag
~gnome 304 bytes HTML do
~gnome(1) 772 bytes HTML do
index.html 2.2 KiB HTML do
~venkata 306 bytes HTML do
~venkata(1) 1.4 KiB HTML do
rhino1.jpg 64.2 KiB JPEG im
rhino3.jpg 94.6 KiB JPEG im
rhino3(1).jpg 94.6 KiB JPEG im
rhino4.jpg 149.6 KiB JPEG im
object68 89 bytes Plain tex
object95 5 bytes Plain tex
object50 290 bytes Unknow
RHINOUSB.dd 247.5 MiB Unknow
search%3fhl=en&ie=UTF-8&oe=UTF-8&q=rhino.exe 14.8 KiB Windo
rhino.exe 142.5 KiB Windo
contraband.zip 225.2 KiB Zip arch
Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Hostname Content Type Size Filename
www.google.com text/html 15 kB search?hl=en&ie=UTF-8&oe=UTF-8&q=rhino.exe
www.google.com image/gif 1,033 bytes nav_first.gif
www.google.com image/gif 376 bytes nav_current.gif
www.google.com image/gif 373 bytes nav_page.gif
290 bytes
89 bytes
5 bytes
www.cs.uno.edu application/octet-stream 145 kB rhino.exe
Save Save All Preview Close Help
Frame (1112 bytes) Reassembled TCP (15338 bytes) De-chunked
Packets: 295

- What happened to the hard drive in the computer? Where is it now?

  Answer: A suspect tossed it in the Mississippi River. I found this answer in the ole diary. I circled it in red. Same screenshot from the first question, just zoomed in. See screenshot below.



- What happened to the USB key?

  Answer:

- What is recoverable from the dd image of the USB key?

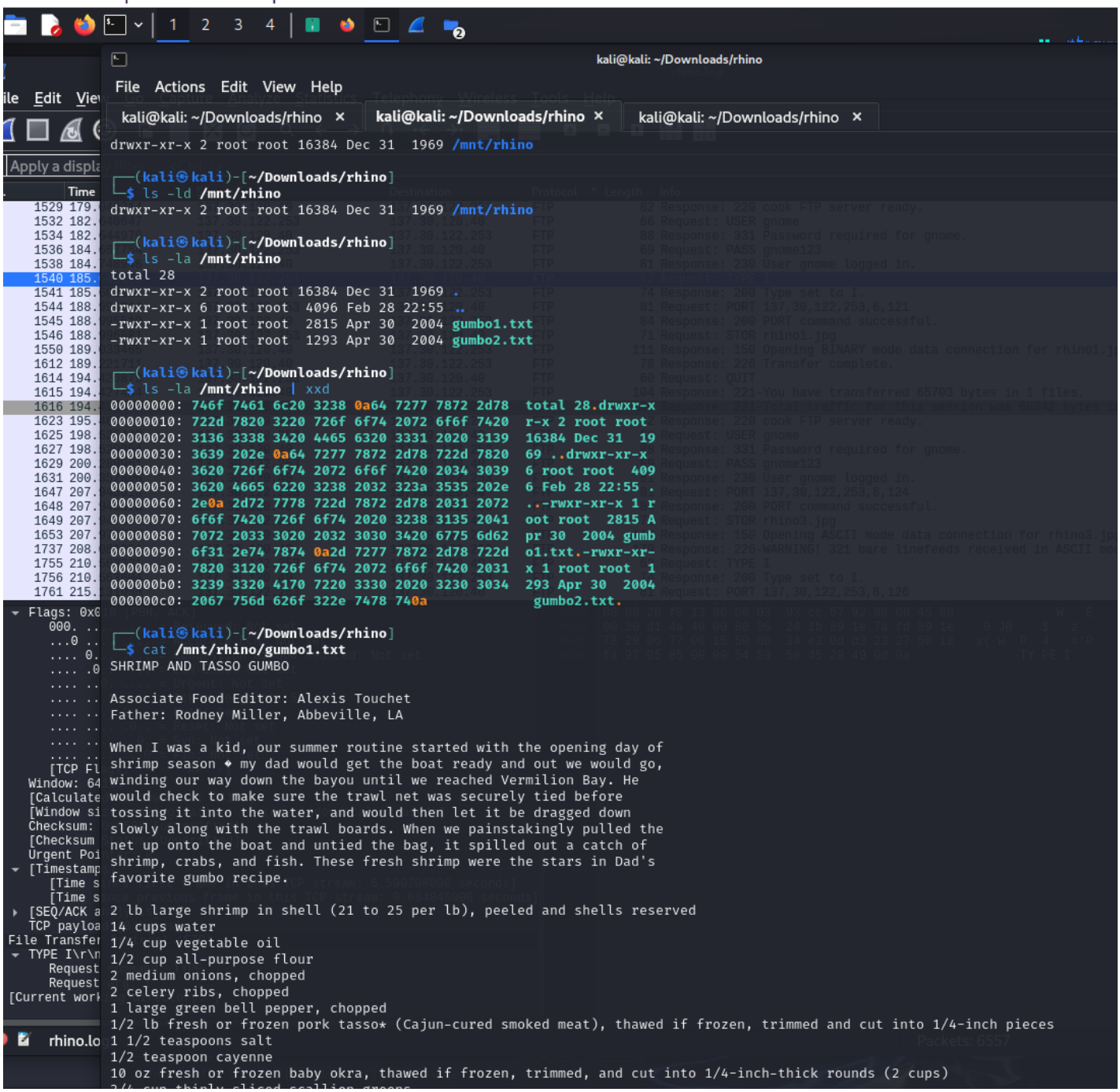
  Answer:

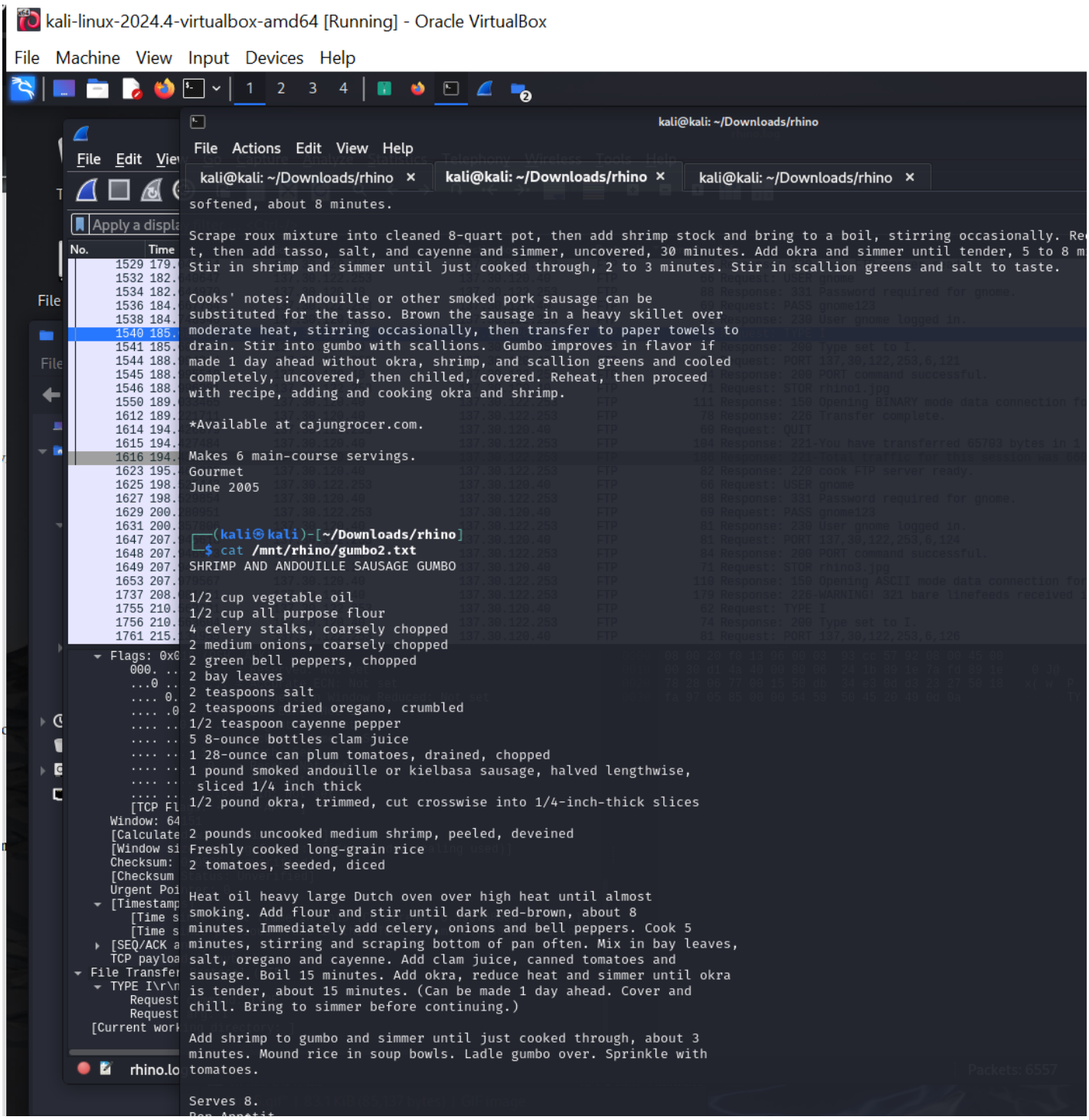
  After mounting it and going through the contents, I found 2 gumbo text files. Please see screenshot below. They had food recipes in them. I ran the cat command on my directory I made where I mounted the RHINOUSB.dd. Also, I used foremost tool to extract data from the .dd imag. I got the other following screenshots below for that. In the second screenshot shows what I did which is:

  1. I made a new directory using mdkir which I called /mnt/rhino_data because I already had mounted the RHINOUSB.dd to my other directory called /mnt/rhino.
  2. I used the command foremost -o /mnt/rhino_data RHINOUSB.dd
  3. Ls -l /mnt/rhino_data which is where I see audit.txt, and the directories: gif, jpg, and ole
  4. I ran cat audit.txt to see what was in that which shows information about the files possibly associated with the other directories.
  5. Then I ran ls -l /mnt/rhino_data/jpg/ to see what contents I could view and I saw 7 differently named jpg files
  6. To sum it up, I did some research and know I have to do the most complicated I need to use some carving tools with foremost and steghide for steganography with my screenshots but I did not have time, but I do know what to do.

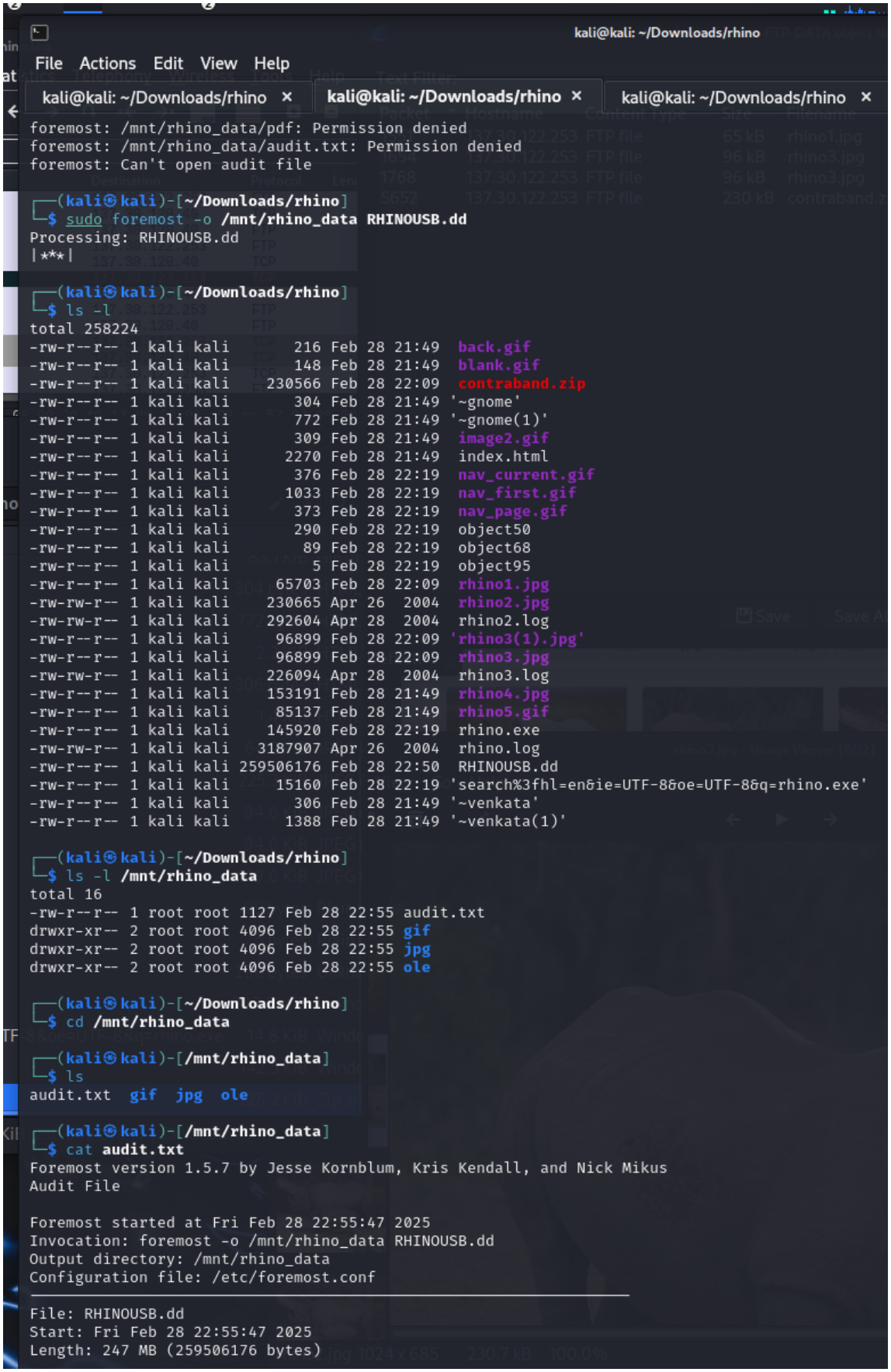
nux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox

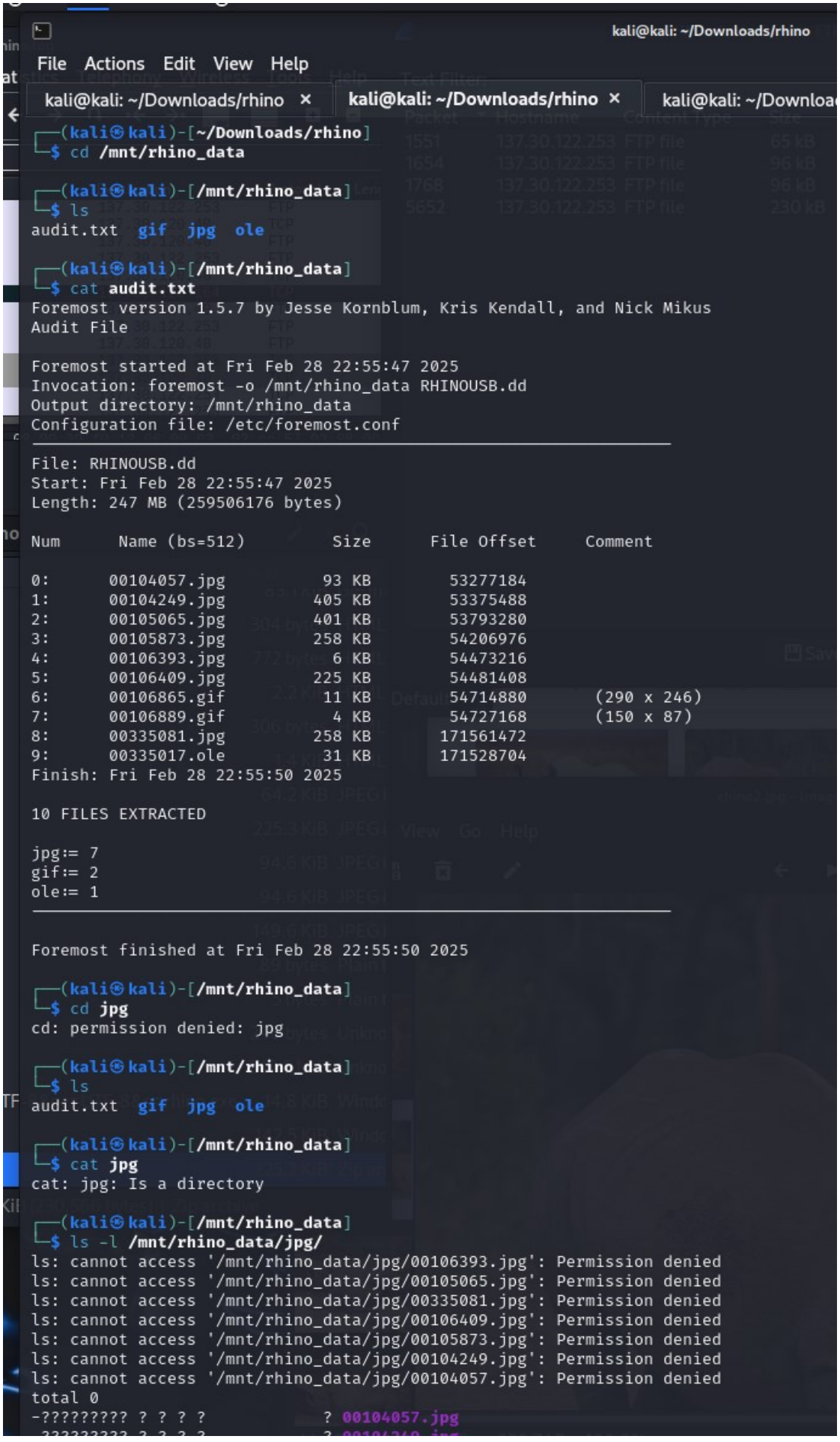
:hine View Input Devices Help

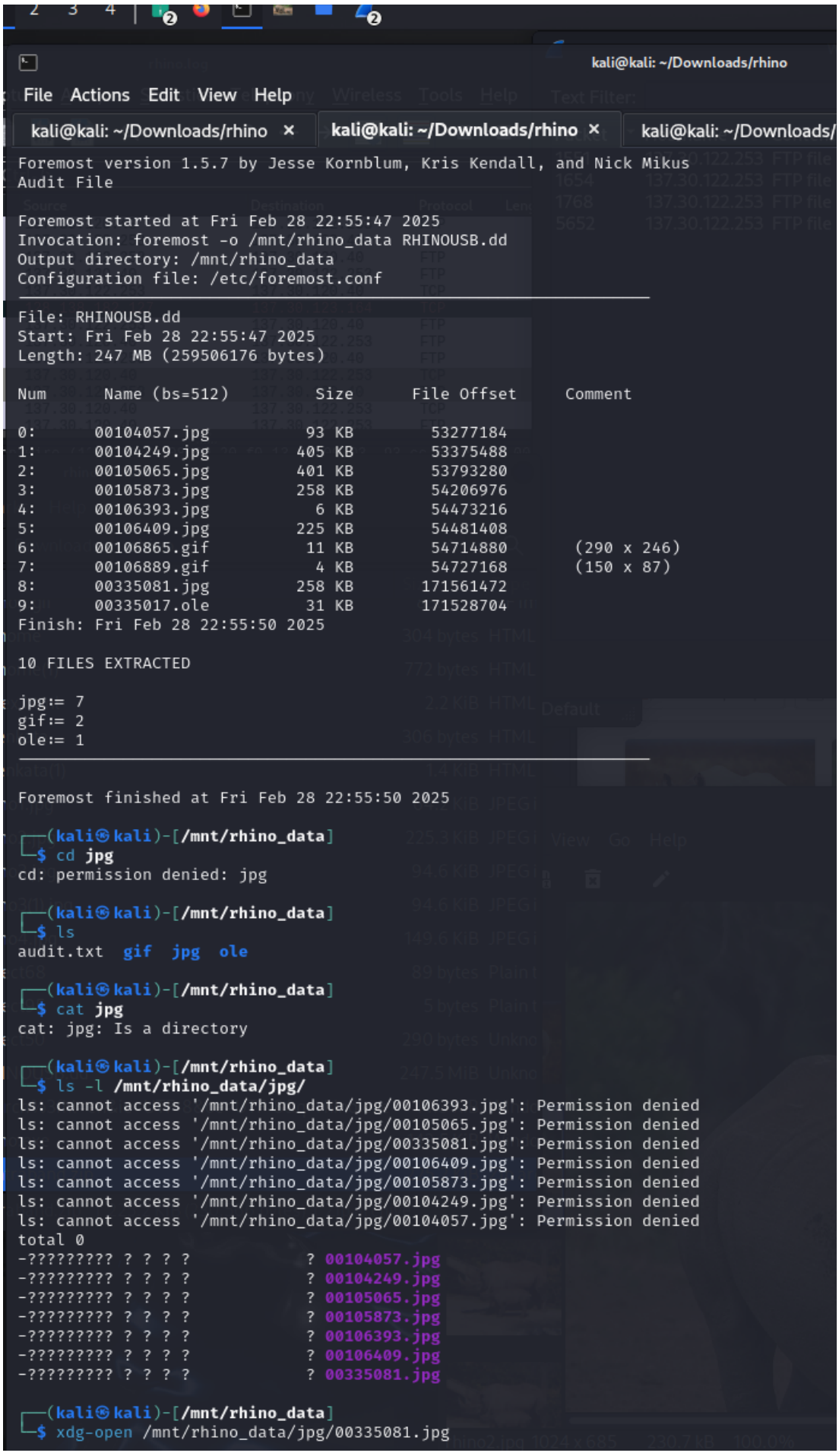



kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads/rhino
File Actions Edit View Help
kali@kali: ~/Downloads/rhino
kali@kali: ~/Downloads/rhino
kali@kali: ~/Downloads/rhino
softened, about 8 minutes.
Scrape roux mixture into cleaned 8-quart pot, then add shrimp stock and bring to a boil, stirring occasionally. Re
t, then add tasso, salt, and cayenne and simmer, uncovered, 30 minutes. Add okra and simmer until tender, 5 to 8 m
Stir in shrimp and simmer until just cooked through, 2 to 3 minutes. Stir in scallion greens and salt to taste.
Cooks' notes: Andouille or other smoked pork sausage can be
substituted for the tasso. Brown the sausage in a heavy skillet over
moderate heat, stirring occasionally, then transfer to paper towels to
drain. Stir into gumbo with scallions. Gumbo improves in flavor if
made 1 day ahead without okra, shrimp, and scallion greens and cooled
completely, uncovered, then chilled, covered. Reheat, then proceed
with recipe, adding and cooking okra and shrimp.
*Available at cajungrocer.com.
Makes 6 main-course servings.
Gourmet
June 2005
(kali㉿kali)-[~/Downloads/rhino]
$ cat /mnt/rhino/gumbo2.txt
SHRIMP AND ANDOUILLE SAUSAGE GUMBO
1/2 cup vegetable oil
1/2 cup all purpose flour
4 celery stalks, coarsely chopped
2 medium onions, coarsely chopped
2 green bell peppers, chopped
2 bay leaves
2 teaspoons salt
2 teaspoons dried oregano, crumbled
1/2 teaspoon cayenne pepper
5 8-ounce bottles clam juice
1 28-ounce can plum tomatoes, drained, chopped
1 pound smoked andouille or kielbasa sausage, halved lengthwise,
sliced 1/4 inch thick
1/2 pound okra, trimmed, cut crosswise into 1/4-inch-thick slices
2 pounds uncooked medium shrimp, peeled, deveined
Freshly cooked long-grain rice
2 tomatoes, seeded, diced
Heat oil heavy large Dutch oven over high heat until almost
smoking. Add flour and stir until dark red-brown, about 8
minutes. Immediately add celery, onions and bell peppers. Cook 5
minutes, stirring and scraping bottom of pan often. Mix in bay leaves,
salt, oregano and cayenne. Add clam juice, canned tomatoes and
sausage. Boil 15 minutes. Add okra, reduce heat and simmer until okra
is tender, about 15 minutes. (Can be made 1 day ahead. Cover and
chill. Bring to simmer before continuing.)
Add shrimp to gumbo and simmer until just cooked through, about 3
minutes. Mound rice in soup bowls. Ladle gumbo over. Sprinkle with
tomatoes.
Serves 8.

Those 2 screenshots above are of the gumbo.txt files. The screenshots below are from my bullet point numbered list explanation.




kali@kali: ~/Downloads/rhino
File Actions Edit View Help
kali@kali: ~/Downloads/rhino
kali@kali: ~/Downloads/rhino
kali@kali: ~/Downloa
(kali㉿kali)-[~/Downloads/rhino]
$ cd /mnt/rhino_data
(kali㉿kali)-[/mnt/rhino_data]
$ ls
audit.txt gif jpg ole
(kali㉿kali)-[/mnt/rhino_data]
$ cat audit.txt
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
Foremost started at Fri Feb 28 22:55:47 2025
Invocation: foremost -o /mnt/rhino_data RHINOUSB.dd
Output directory: /mnt/rhino_data
Configuration file: /etc/foremost.conf
File: RHINOUSB.dd
Start: Fri Feb 28 22:55:47 2025
Length: 247 MB (259506176 bytes)
Num Name (bs=512) Size File Offset Comment
0: 00104057.jpg 93 KB 53277184
1: 00104249.jpg 405 KB 53375488
2: 00105065.jpg 401 KB 53793280
3: 00105873.jpg 258 KB 54206976
4: 00106393.jpg 6 KB 54473216
5: 00106409.jpg 225 KB 54481408
6: 00106865.gif 11 KB 54714880 (290 x 246)
7: 00106889.gif 4 KB 54727168 (150 x 87)
8: 00335081.jpg 258 KB 171561472
9: 00335017.ole 31 KB 171528704
Finish: Fri Feb 28 22:55:50 2025
10 FILES EXTRACTED
jpg:= 7
gif:= 2
ole:= 1
Foremost finished at Fri Feb 28 22:55:50 2025
(kali㉿kali)-[/mnt/rhino_data]
$ cd jpg
cd: permission denied: jpg
(kali㉿kali)-[/mnt/rhino_data]
$ ls
audit.txt gif jpg ole
(kali㉿kali)-[/mnt/rhino_data]
$ cat jpg
cat: jpg: Is a directory
(kali㉿kali)-[/mnt/rhino_data]
$ ls -l /mnt/rhino_data/jpg/
ls: cannot access '/mnt/rhino_data/jpg/00106393.jpg': Permission denied
ls: cannot access '/mnt/rhino_data/jpg/00105065.jpg': Permission denied
ls: cannot access '/mnt/rhino_data/jpg/00335081.jpg': Permission denied
ls: cannot access '/mnt/rhino_data/jpg/00106409.jpg': Permission denied
ls: cannot access '/mnt/rhino_data/jpg/00105873.jpg': Permission denied
ls: cannot access '/mnt/rhino_data/jpg/00104249.jpg': Permission denied
ls: cannot access '/mnt/rhino_data/jpg/00104057.jpg': Permission denied
total 0
-????????? ? ? ? ? ? 00104057.jpg


kali@kali: ~/Downloads/rhino
File Actions Edit View Help
kali@kali: ~/Downloads/rhino
kali@kali: ~/Downloads/rhino
kali@kali: ~/Downloads/
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
Foremost started at Fri Feb 28 22:55:47 2025
Invocation: foremost -o /mnt/rhino_data RHINOUSB.dd
Output directory: /mnt/rhino_data
Configuration file: /etc/foremost.conf
File: RHINOUSB.dd
Start: Fri Feb 28 22:55:47 2025
Length: 247 MB (259506176 bytes)
Num Name (bs=512) Size File Offset Comment
0: 00104057.jpg 93 KB 53277184
1: 00104249.jpg 405 KB 53375488
2: 00105065.jpg 401 KB 53793280
3: 00105873.jpg 258 KB 54206976
4: 00106393.jpg 6 KB 54473216
5: 00106409.jpg 225 KB 54481408
6: 00106865.gif 11 KB 54714880 (290 x 246)
7: 00106889.gif 4 KB 54727168 (150 x 87)
8: 00335081.jpg 258 KB 171561472
9: 00335017.ole 31 KB 171528704
Finish: Fri Feb 28 22:55:50 2025
10 FILES EXTRACTED
jpg:= 7
gif:= 2
ole:= 1
Foremost finished at Fri Feb 28 22:55:50 2025
┌──(kali㉿kali)-[/mnt/rhino_data]
└─$ cd jpg
cd: permission denied: jpg
┌──(kali㉿kali)-[/mnt/rhino_data]
└─$ ls
audit.txt gif jpg ole
┌──(kali㉿kali)-[/mnt/rhino_data]
└─$ cat jpg
cat: jpg: Is a directory
┌──(kali㉿kali)-[/mnt/rhino_data]
└─$ ls -l /mnt/rhino_data/jpg/
ls: cannot access '/mnt/rhino_data/jpg/00106393.jpg': Permission denied
ls: cannot access '/mnt/rhino_data/jpg/00105065.jpg': Permission denied
ls: cannot access '/mnt/rhino_data/jpg/00335081.jpg': Permission denied
ls: cannot access '/mnt/rhino_data/jpg/00106409.jpg': Permission denied
ls: cannot access '/mnt/rhino_data/jpg/00105873.jpg': Permission denied
ls: cannot access '/mnt/rhino_data/jpg/00104249.jpg': Permission denied
ls: cannot access '/mnt/rhino_data/jpg/00104057.jpg': Permission denied
total 0
-????????? ? ? ? ? ? 00104057.jpg
-????????? ? ? ? ? ? 00104249.jpg
-????????? ? ? ? ? ? 00105065.jpg
-????????? ? ? ? ? ? 00105873.jpg
-????????? ? ? ? ? ? 00106393.jpg
-????????? ? ? ? ? ? 00106409.jpg
-????????? ? ? ? ? ? 00335081.jpg
┌──(kali㉿kali)-[/mnt/rhino_data]
└─$ xdg-open /mnt/rhino_data/jpg/00335081.jpg

- Is there any evidence that connects the USB key and the network traces? If so, what?

  Answer: Yes. There were 2 rhino2.jpgs, one of them was in the rhino1.log in the HTTP stream contraband.zip file and also in the RHINOUSB.dd image.