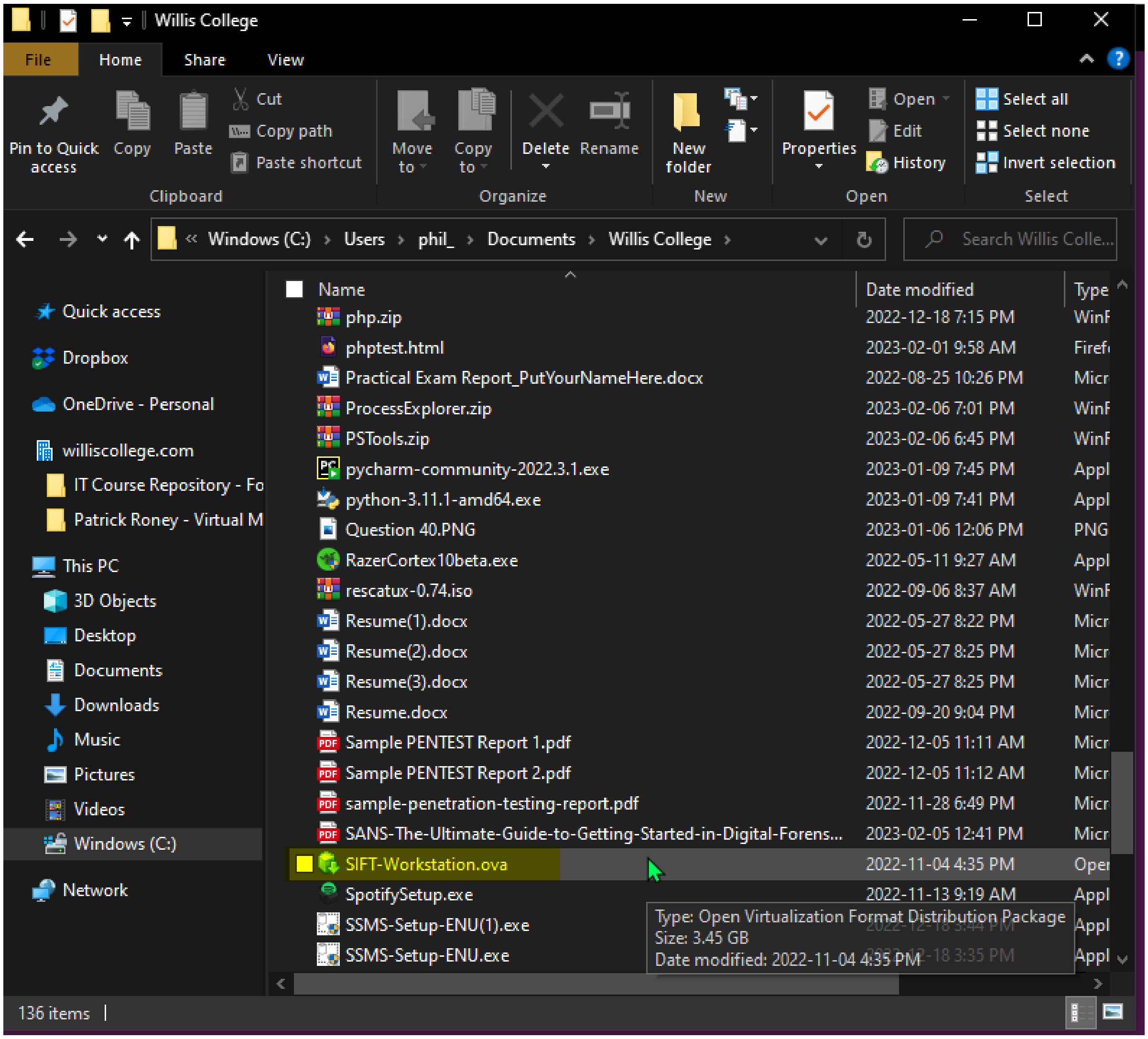
Assignment 3 - Digital Forensics: Conduct the NIST Rhino Hunt

Phil Wilson

In this assignment we were assigned to find hidden files (RHINOUSB.dd). Once running the tools and programs needed, we were able to ascertain the information needed to complete the project.

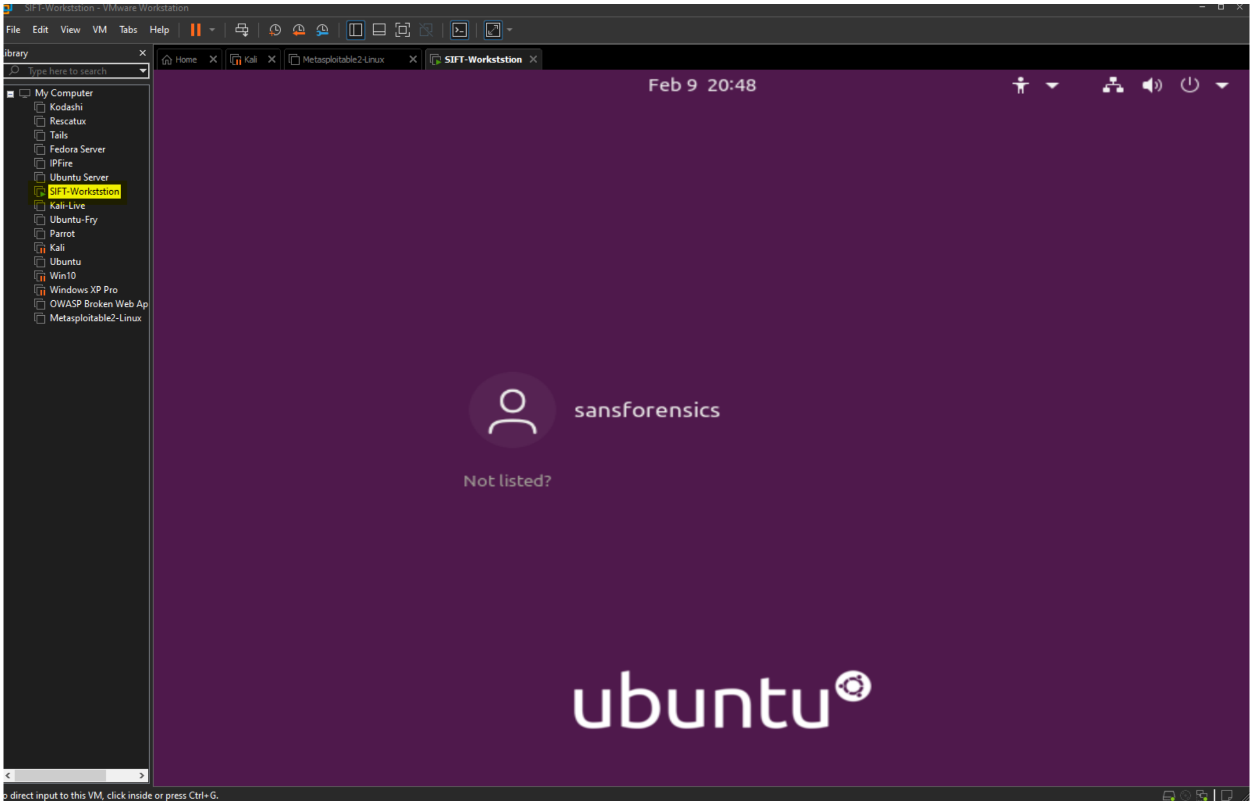
Step 1: Download SIFT Workstation



Name	Date modified	Type
php.zip	2022-12-18 7:15 PM	WinF
phptest.html	2023-02-01 9:58 AM	Firef
Practical Exam Report_PutYourNameHere.docx	2022-08-25 10:26 PM	Micr
ProcessExplorer.zip	2023-02-06 7:01 PM	WinF
PSTools.zip	2023-02-06 6:45 PM	WinF
pycharm-community-2022.3.1.exe	2023-01-09 7:45 PM	Appl
python-3.11.1-amd64.exe	2023-01-09 7:41 PM	Appl
Question 40.PNG	2023-01-06 12:06 PM	PNG
RazerCortex10beta.exe	2022-05-11 9:27 AM	Appl
rescatux-0.74.iso	2022-09-06 8:37 AM	WinF
Resume(1).docx	2022-05-27 8:22 PM	Micr
Resume(2).docx	2022-05-27 8:25 PM	Micr
Resume(3).docx	2022-05-27 8:25 PM	Micr
Resume.docx	2022-09-20 9:04 PM	Micr
Sample PENTEST Report 1.pdf	2022-12-05 11:11 AM	Micr
Sample PENTEST Report 2.pdf	2022-12-05 11:12 AM	Micr
sample-penetration-testing-report.pdf	2022-11-28 6:49 PM	Micr
SANS-The-Ultimate-Guide-to-Getting-Started-in-Digital-Forens...	2023-02-05 12:41 PM	Micr
SIFT-Workstation.ova	2022-11-04 4:35 PM	Oper
SpotifySetup.exe	2022-11-13 9:19 AM	Appl
SSMS-Setup-ENU(1).exe	2022-12-18 3:44 PM	Appl
SSMS-Setup-ENU.exe	2022-12-18 3:35 PM	Appl

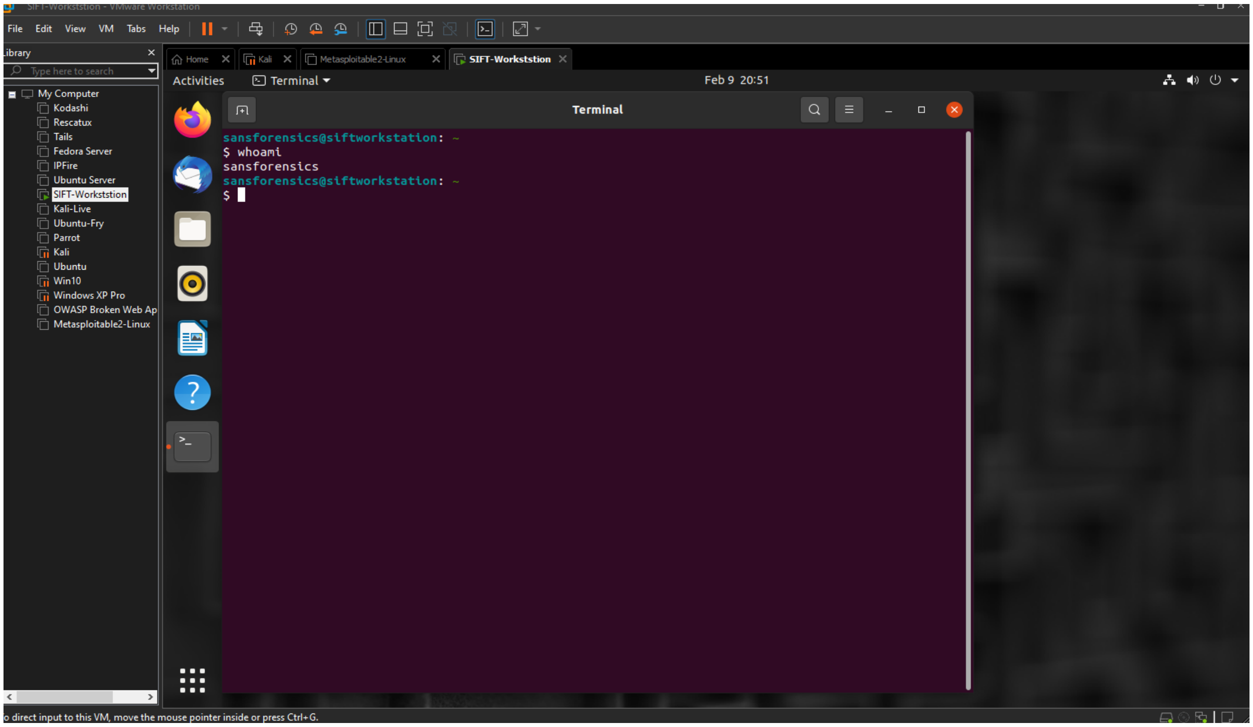
Type: Open Virtualization Format Distribution Package
Size: 3.45 GB
Date modified: 2022-11-04 4:35 PM

Step 2: Import SIFT Workstation to VMware and open it.



o direct input to this VM, click inside or press Ctrl+G.

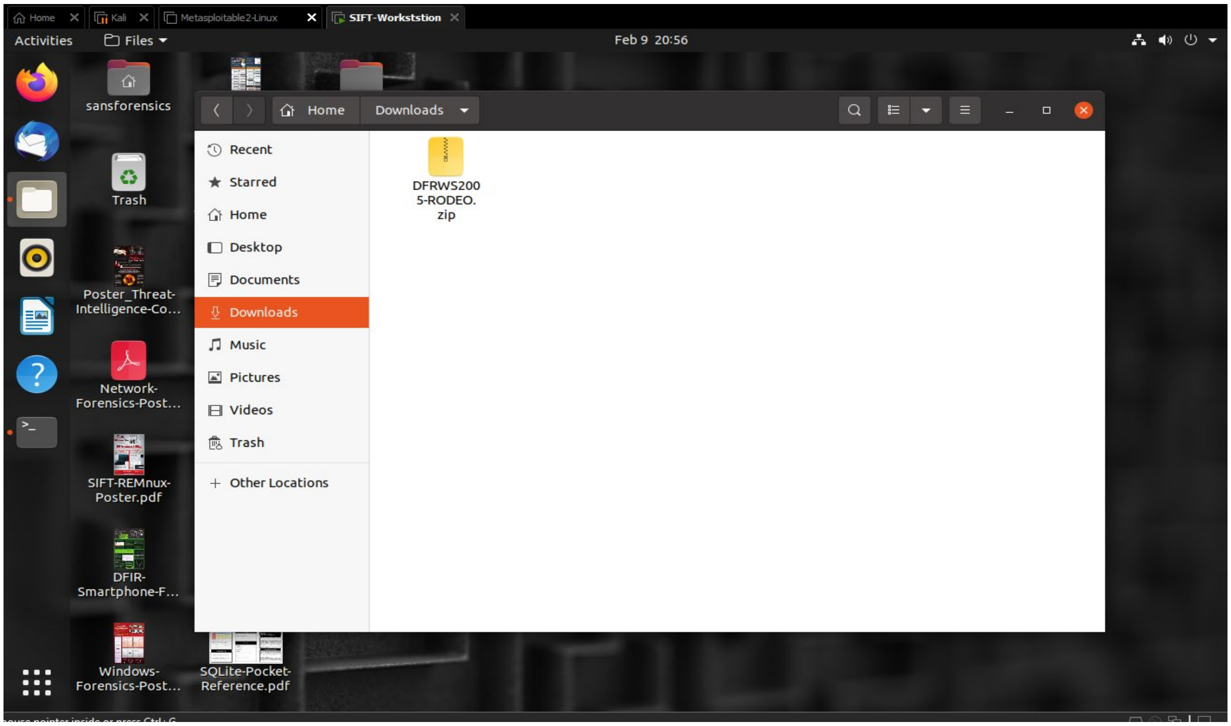
Step 3: Login to SIFT Workstation



```
sansforensics@siftworkstation: ~
$ whoami
sansforensics
sansforensics@siftworkstation: ~
$ 
```

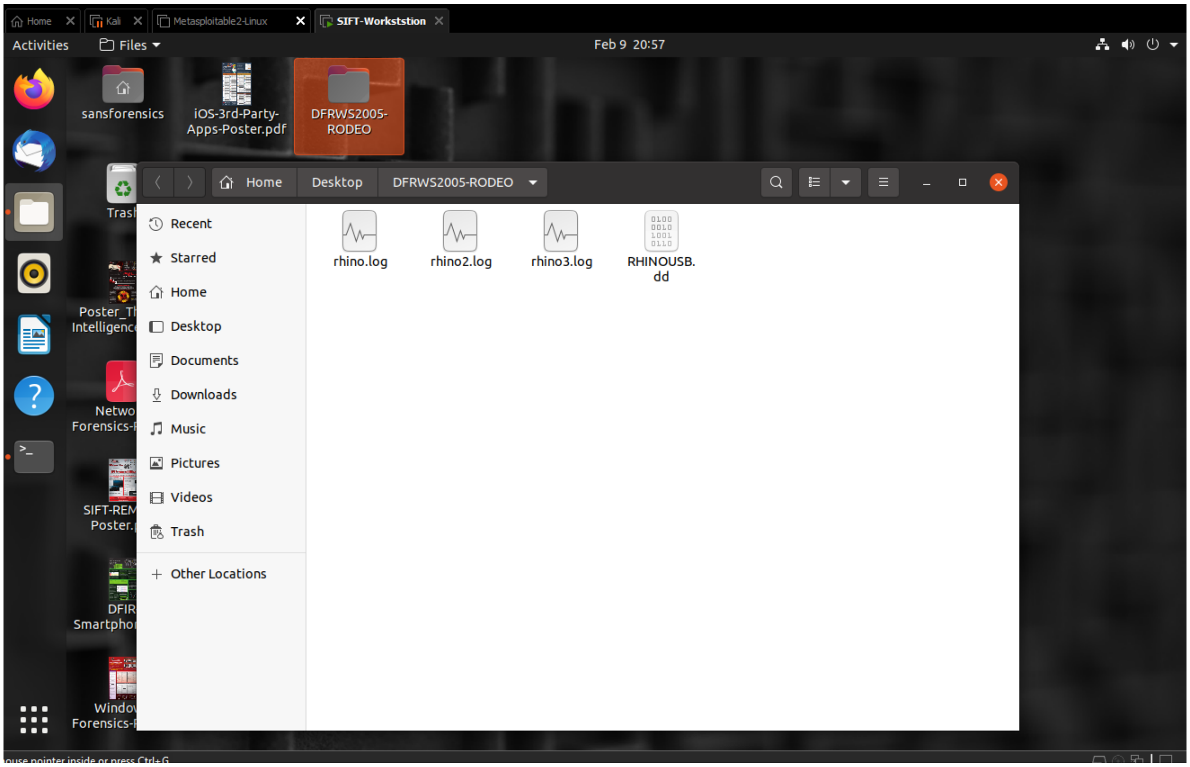
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Step 4: Download the SANS Rhino Hunt

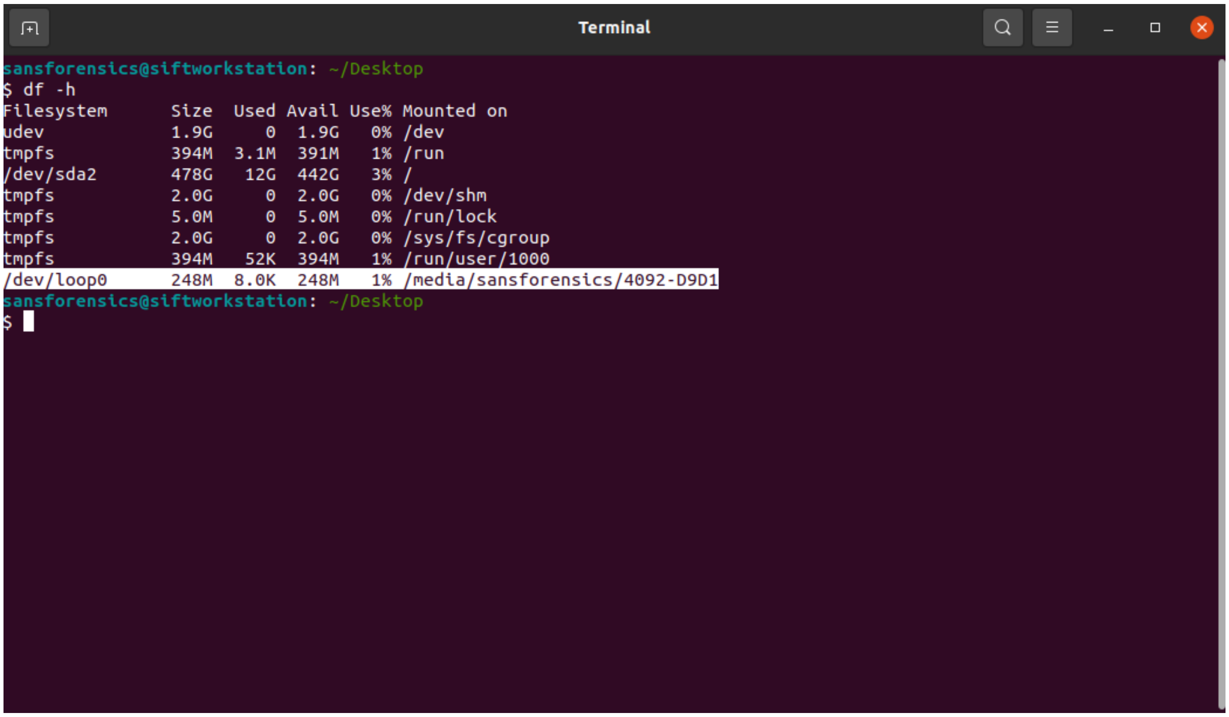


ouse pointer inside or press Ctrl+G.

Step 5: Unzip the Rhino Hunt

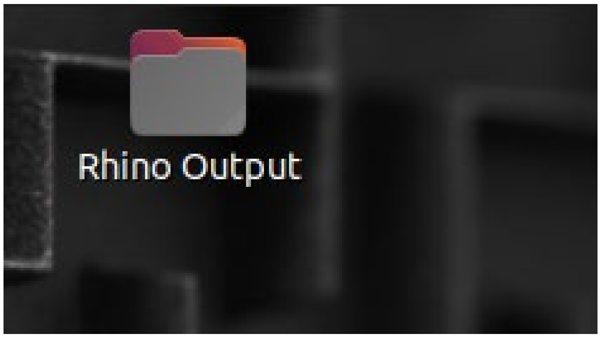


Step 6: Use SIFT to find the Rhino pictures.



```
sansforensics@siftworkstation: ~/Desktop
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           394M  3.1M  391M   1% /run
/dev/sda2       478G   12G  442G   3% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           2.0G     0  2.0G   0% /sys/fs/cgroup
tmpfs           394M   52K  394M   1% /run/user/1000
/dev/loop0      248M  8.0K  248M   1% /media/sansforensics/4092-D9D1
sansforensics@siftworkstation: ~/Desktop
$ 
```

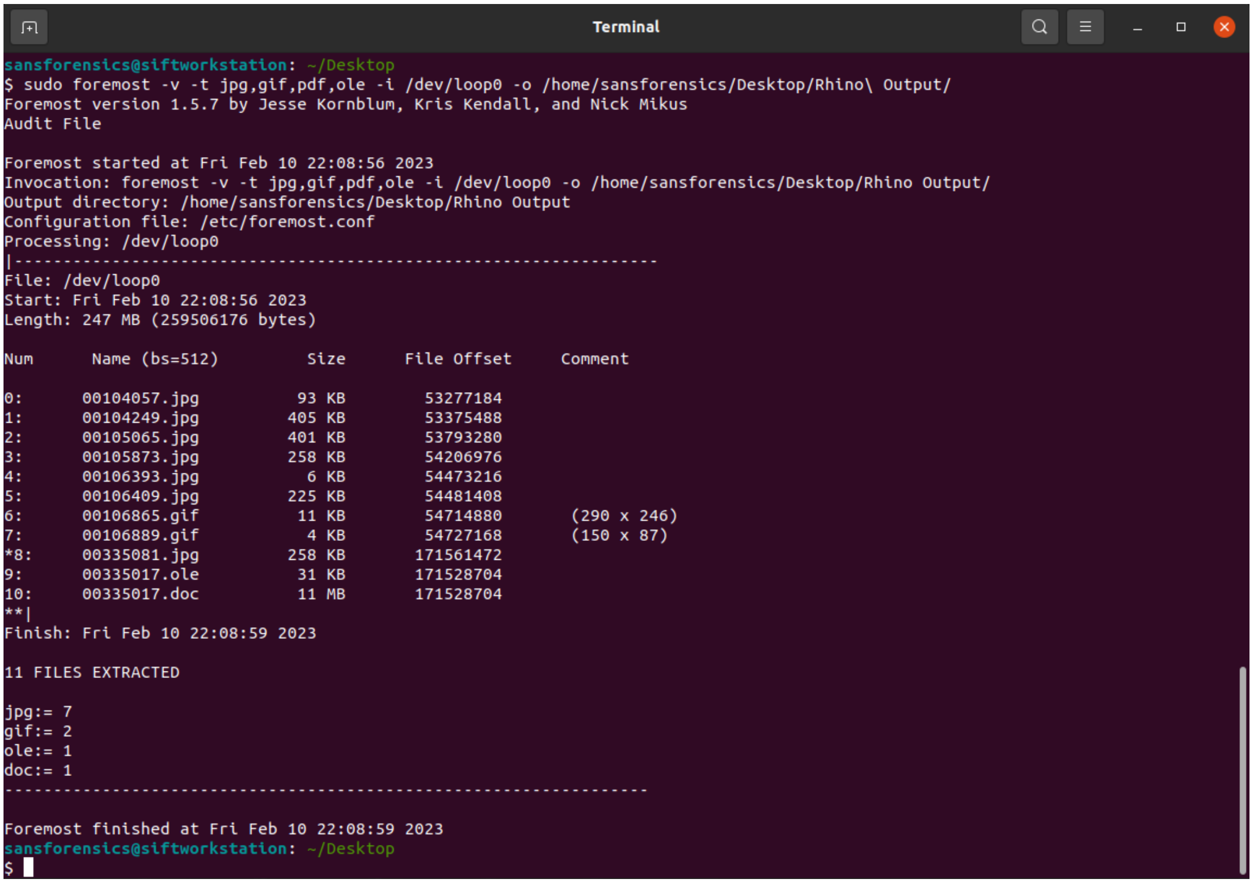
Step 7: Create a Directory for the Output



Step 8: Run Foremost against the RHINOUSB.dd image.

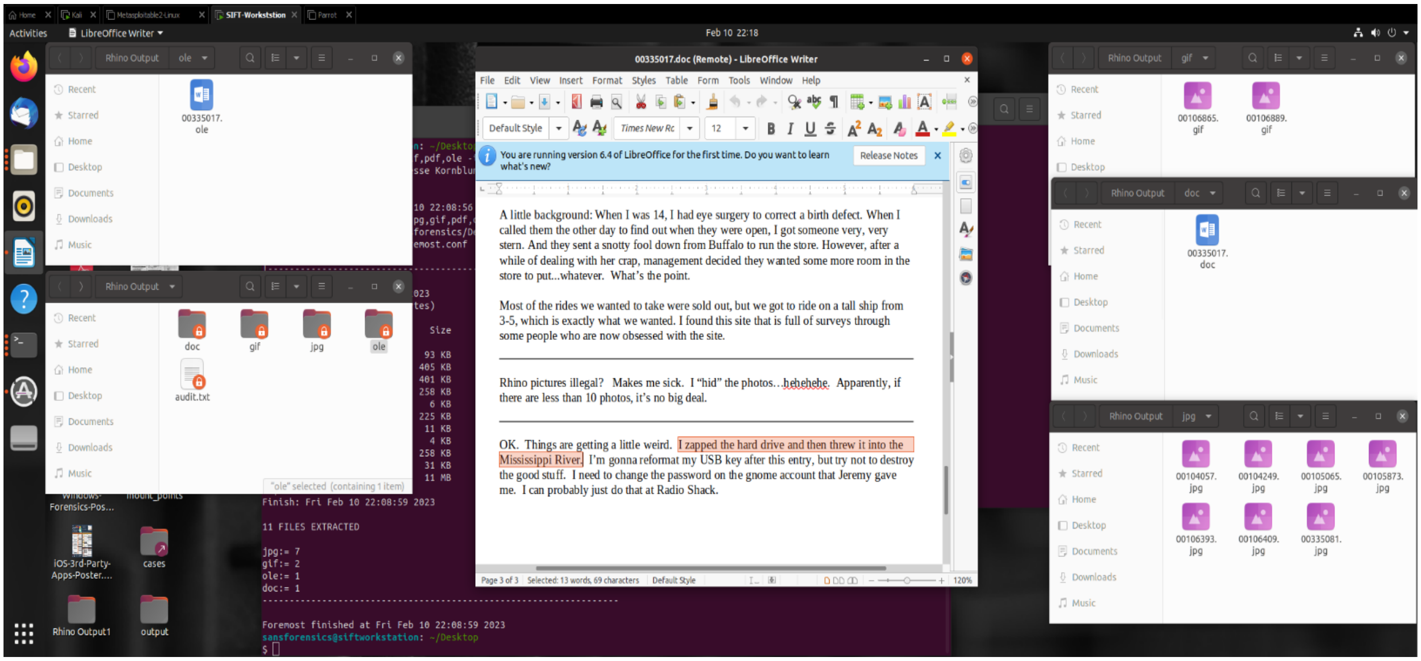
I used the command:

sudo foremost -v -t jpg,gif,pdt,ole -i /dev/loop0 -o /home/sansforensics/Desktop/Rhino Output



```
sansforensics@siftworkstation: ~/Desktop
$ sudo foremost -v -t jpg,gif,pdf,ole -i /dev/loop0 -o /home/sansforensics/Desktop/Rhino\ Output/
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Fri Feb 10 22:08:56 2023
Invocation: foremost -v -t jpg,gif,pdf,ole -i /dev/loop0 -o /home/sansforensics/Desktop/Rhino Output/
Output directory: /home/sansforensics/Desktop/Rhino Output
Configuration file: /etc/foremost.conf
Processing: /dev/loop0
|------------------------------------------------------------------
File: /dev/loop0
Start: Fri Feb 10 22:08:56 2023
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
10:     00335017.doc          11 MB       171528704
**|
Finish: Fri Feb 10 22:08:59 2023

11 FILES EXTRACTED

jpg:= 7
gif:= 2
ole:= 1
doc:= 1
------------------------------------------------------------------

Foremost finished at Fri Feb 10 22:08:59 2023
sansforensics@siftworkstation: ~/Desktop
$ 
```

Step 9: Review the Output



You are running version 6.4 of LibreOffice for the first time. Do you want to learn what's new?

A little background: When I was 14, I had eye surgery to correct a birth defect. When I called them the other day to find out when they were open, I got someone very, very stern. And they sent a snotty fool down from Buffalo to run the store. However, after a while of dealing with her crap, management decided they wanted some more room in the store to put...whatever. What's the point.

Most of the rides we wanted to take were sold out, but we got to ride on a tall ship from 3-5, which is exactly what we wanted. I found this site that is full of surveys through some people who are now obsessed with the site.

Rhino pictures illegal? Makes me sick. I "hid" the photos…hehehehe. Apparently, if there are less than 10 photos, it's no big deal.

OK. Things are getting a little weird. I zapped the hard drive and then threw it into the Mississippi River. I'm gonna reformat my USB key after this entry, but try not to destroy the good stuff. I need to change the password on the gnome account that Jeremy gave me. I can probably just do that at Radio Shack.

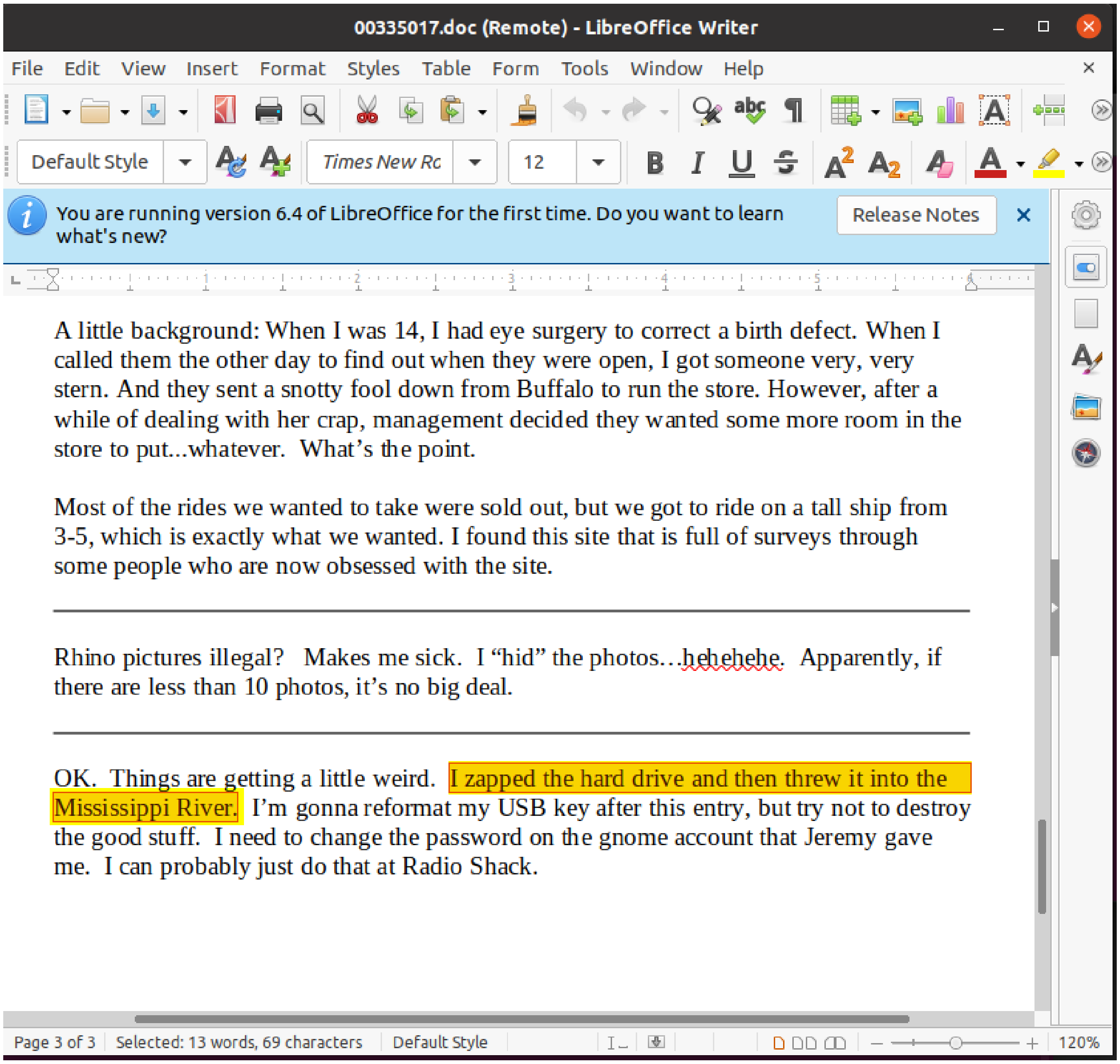
Page 3 of 3 | Selected: 13 words, 69 characters | Default Style | 120%

```
Finish: Fri Feb 10 22:08:59 2023

11 FILES EXTRACTED

jpg:= 7
gif:= 2
ole:= 1
doc:= 1
------------------------------------------------------------

Foremost finished at Fri Feb 10 22:08:59 2023
sansforensics@siftworkstation: ~/Desktop
$ 
```

Upon review of the files, you can see that there are 2 .gif files, 7 .jpg files, 1 .doc file, and 1 .ole file. When we open the .doc file and read through it you the answer to the question.

Answer on next page!

Question – What happened to the hard drive?



00335017.doc (Remote) - LibreOffice Writer
File Edit View Insert Format Styles Table Form Tools Window Help
Default Style
Times New Rc
12
You are running version 6.4 of LibreOffice for the first time. Do you want to learn what's new?
Release Notes
Page 3 of 3
Selected: 13 words, 69 characters
Default Style
120%

A little background: When I was 14, I had eye surgery to correct a birth defect. When I called them the other day to find out when they were open, I got someone very, very stern. And they sent a snotty fool down from Buffalo to run the store. However, after a while of dealing with her crap, management decided they wanted some more room in the store to put...whatever. What's the point.

Most of the rides we wanted to take were sold out, but we got to ride on a tall ship from 3-5, which is exactly what we wanted. I found this site that is full of surveys through some people who are now obsessed with the site.

Rhino pictures illegal? Makes me sick. I "hid" the photos…hehehehe. Apparently, if there are less than 10 photos, it's no big deal.

OK. Things are getting a little weird. I zapped the hard drive and then threw it into the Mississippi River. I'm gonna reformat my USB key after this entry, but try not to destroy the good stuff. I need to change the password on the gnome account that Jeremy gave me. I can probably just do that at Radio Shack.

Answer – The hard drive was zapped and thrown into the Mississippi River