Requested by: University Police

Name of Investigator: Keyonna Davis

Case Name: Rhino traffic-176853

CASE

The city passed a law in making possession of nine or more unique rhinoceros’ images a serious crime. The network administrator at the University recently alerted police when his instance of RHINOVORE flagged illegal rhino traffic. Evidence in the case includes a computer and USB drive seized from one of the University’s labs. Unfortunately, the computer had no hard drive. The USB drive was imaged and a copy of the dd image was provide. In addition to the USB drive image, three network traces are also available—these were provided by the network administrator and involve the machine with the missing hard drive. The suspect is the primary user of this machine, who has been pursuing his studies at the University.

Evidence Provided

|  |  |
| --- | --- |
| ITEM | MD5 checksum |
| \*rhino.log | c0d0093eb1664cd7b73f3a5225ae3f30 |
| \*rhino2.log | cd21eaf4acfb50f71ffff857d7968341 |
| \*rhino3.log | 7e29f9d67346df25faaf18efcd95fc30 |
| RHINOUSB.dd | 80348c58eec4c328ef1f7709adc56a54 |

Forensics Analysis

On November 28, 2022 at 7:57am I acquired the evidence and started the process of analyzing the evidence provided. Using Autopsy to analyze the USB image , I was able to view 132 carved files, 9 images , and 2 txt files with gumbo recipes as shown below.

Graphical user interface, application

Description automatically generatedGraphical user interface, application, Word

Description automatically generated

I then used Wireshark to view rhino.log, rhino2.log and rhino3.log. On rhino.log I did an FTP search and found the username and password. I then proceeded to do a FTP-data search and found rhino1.jpg, rhino3.jpg and contraband.zip which contained rhino2.jpg The contraband.zip file was password protected and I used <https://www.lostmypass.com/file-types/zip/> to retrieve the password and the password is monkey.

Graphical user interface, text

Description automatically generated with medium confidenceTable

Description automatically generated

A rhinoceros and a rhinoceros in a zoo exhibit

Description automatically generated with medium confidenceA rhinoceros drinking water

Description automatically generated with low confidence Graphical user interface, text, application

Description automatically generated with medium confidence

I then opened rhino2.log in Wireshark and found rhino4.jpg and rhino5.gif shown below.

 A picture containing linedrawing

Description automatically generated Graphical user interface

Description automatically generated

While analyzing rhino3log I discovered rhino.exe file.

Conclusion

From my investigation of the provided evidence, I have found 9 hidden rhino images. File *f0334472* from the USB image disclosed that Jeremy gave the accused the account with the username gnome and the password gnome123. The USB drive and network traces connection is that the image rhino2.jpg exist in both. Text doc *f0334472* also reveals that the accused zapped the hard drive, tossed it in the Mississippi river and reformatted the USB (possibly at RadioShack). This conclude my findings.