**Rhinoceros Images Investigation**

**Background**

The city of New Orleans passed a law in 2004 making possession of nine or more unique rhinoceros images a serious crime. The network administrator at the University of New Orleans recently alerted police when his instance of RHINOVORE flagged illegal rhino traffic. Evidence in the case includes a computer and USB key seized from one of the University’s labs. Unfortunately, the computer had no hard drive. The USB key was imaged and a copy of the dd image is on the CD-ROM you’ve been given.

In addition to the USB key drive image, three network traces are also available - these were provided by the network administrator and involved the machine with the missing hard drive. The suspect is the primary user of this machine, who has been pursuing his Ph.D. at the University since 1972.

The case study was contributed by Dr. Golden G. Richard III and was originally used in the DFRWS 2005 RODEO CHALLENGE. The original case description is posted on [Rhino Hunt (nist.gov)](https://cfreds-archive.nist.gov/dfrws/Rhino_Hunt.html).

The investigation report is generated by Dr. Frank Xu at the University of Baltimore.

**Investigation Report**

Description:

The criminal case is focused on investigating an individual who is in possession of rhinoceros images. The investigation is led by Dr. Frank Xu, a senior investigator at the University of Baltimore. The case involves three network traffic logs named "rhino.log", "rhino2.log", and "rhino3.log" with corresponding MD5 hash codes of "c0d0093eb1664cd7b73f3a5225ae3f30", "cd21eaf4acfb50f71ffff857d7968341", and "7e29f9d67346df25faaf18efcd95fc30". In addition, there is one USB image named "RHINOUSB.dd" with an MD5 hash code of "80348c58eec4c328ef1f7709adc56a54". These files were provided by the network administrator at the University of New Orleans, and more details about them can be found in the file "Rhino Hunt.pdf". The suspect's identity is currently unknown.

Timeline

Upon completion of the investigation, the investigator reconstructed a timeline of the criminal activities performed by the suspect. The timeline encompasses five key actions, which include (1) downloading rhinoceros images, (2) uploading rhinoceros images, (3) deleting rhinoceros images from a USB drive, (4) hiding rhinoceros images, and (5) deleting a Word file containing clues on how the suspect hid the rhinoceros images.

Activities Investigation

Downloading rhinoceros images: The investigator uses a network traffic analysis tool, “Wireshark”, to find the evidence that is associated with the activity. Specifically, two rhinoceros images were found to have been downloaded from IP address 137.30.123.234 to IP address 137.30.120.37, as evidenced by the analysis of the traffic log “rhino2.log”. The investigator was able to extract the two images and save them as “rhino4.jpg” and “rhino5.gif”. These findings were used to confirm the suspicion that the suspect had indeed downloaded two rhinoceros images, and the investigator documented this activity in a corresponding “Downloading activity indicator”.

Uploading rhinoceros images: By analyzing the traffic log “rhino.log” with the network traffic analysis tool “Wireshark”, the investigator has found evidence associated with an activity. The investigation has revealed that two rhinoceros images were uploaded from IP address 137.30.120.40 to IP address 137.30.122.253. The two rhinoceros images have been extracted from the traffic log and saved as “rhino1.jpg” and “rhino3.gif”. Furthermore, the investigator has decrypted an encrypted and compressed file “contraband.zip” using the tool “fcrackzip” with the password “monkey”. The investigator has extracted another rhinoceros image, “rhino2.jpg”, from this decrypted file. The observed data suggests that a suspect has uploaded two rhinoceros images and has hidden another image in the encrypted file. The investigator has justified this conclusion and specified it in a corresponding “Uploading activity indicator”.

Deleting rhinoceros images from a USB: Using the tool "PhotoRec", the investigator has successfully retrieved four jpg files containing rhinoceros images. These images are saved as "f0106393.jpg", "f0106409.jpg", "f0106865.gif", and "f0106889.gif". The data observed in this activity suggests that the suspect has downloaded two rhinoceros images. The investigator has substantiated this conclusion and provided a corresponding “ Deleting activity indicator”.

Hiding rhinoceros images: Two additional images, “F0105065.jpg” and “F0104249.jpg”, were recovered from the USB drive using the tool “PhotoRec”. After analyzing the images with a steganography detection tool called “stegdetect”, the investigator found that a rhinoceros photo was embedded in each image. The steganography detection tool revealed that the original steganography tool used for hiding the rhinoceros photos was “jphide” and the passwords used for hiding them were “gator” and “gumbo”. The investigator used an anti-steganography tool called “jpseek” and successfully recovered two photos containing rhinoceros, which were saved as “r065.jpg” and “r246.jpg”. The investigator has justified this conclusion and specified it in a corresponding “Hiding activity indicator”.

Deleting a Word file that contains hints about how the suspect hid rhinoceros photos. A Word document has been recovered from the USB using the "PhotoRec" tool. The document is saved as "F0335017.doc". The document created by the owner of USB reveals that a suspect has hidden some rhinoceros photos. Specifically, the document creator confessed that “I ‘hid’ the photos” in the Word document. The investigator has confirmed the conclusion and specified it in a corresponding “Deleting Word activity indicator”.

Conclusion

Further investigation is needed to determine:

* If all traffic is initialed by the same suspect
* The USB belonged to the same suspect.