Rhino Hunt (a forensics CTF)

## Summary

This lab uses a forensics CTF supported by NIST: <https://cfreds-archive.nist.gov/dfrws/Rhino_Hunt.html>

**Scenario:**

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 involve 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.

Note: Four images are in the packet captures, four on the disk image, with one in common for a total of seven. Two images are hidden using steganography and are out of scope for this lab.

**The task:**

 Recover at least seven unique rhino pictures from the available evidence and include them in a brief report.  In your report, provide answers to as many of the following questions as possible:

* Who gave the accused a telnet/ftp account?
* What’s the username/password for the account?
* What relevant file transfers appear in the network traces?
* What happened to the hard drive in the computer?  Where is it now?
* What happened to the USB key?
* What is recoverable from the *dd* image of the USB key?
* Is there any evidence that connects the USB key and the network traces?  If so, what?

## Tools/Resources

Parrot: Wireshark and Foremost

Website: [NISTLinks to an external site.](https://cfreds-archive.nist.gov/dfrws/Rhino_Hunt.html)

## Tasks

* Download and unzip disk image for analysis: [Zip fileLinks to an external site.](https://cfreds-archive.nist.gov/dfrws/DFRWS2005-RODEO.zip)
* Validate MD5 hashes
* Answer the questions and find the Rhinos
  + Carve all data out of the disk image using Foremost.
  + The system file viewer can be used to see images and the diary.
* Reading the dairy will answer some of the questions.
  + Open the rhino.log with wireshark.
    - Set the filter to: ftp or ftp-data
    - Find user names, passwords, and download
  + Open rhino2.log in Wireshark
    - Export the relevant HTTP objects in the packet capture.

## Submission

Upload to Canvas a docx or pdf containing:

* The answers to the questions
* A screenshot of the file viewer showing the thumbnails of the rhino images you collected.

## Walkthrough

1. Download disk image for analysis: <https://cfreds-archive.nist.gov/dfrws/Rhino_Hunt.html>
   1. Zip: <https://cfreds-archive.nist.gov/dfrws/DFRWS2005-RODEO.zip>
2. Carve all data out of the disk image:

A screenshot of a computer

Description automatically generated

1. The system file viewer can be used to see images and the diary.
   1. Reading the dairy will answer some of the questions.
2. Open the rhino.log with wireshark.
   1. Set the filter to: ftp or ftp-data
   2. FTP user names and passwords are in the clear
   3. There are three downloads. Follow the TCP stream by right clicking on one of the packets. Set “show data as” to RAW then save.

A screenshot of a computer

Description automatically generated

* 1. Unzip contraband.zip

A screenshot of a computer program

Description automatically generated

1. Open rhino2.log in Wireshark
   1. Export the relevant HTTP objects in the packet capture.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## Additional Thoughts

How does knowing the MD5 values help the investigation?

What does having two similar looking images with different MD5 suggest?