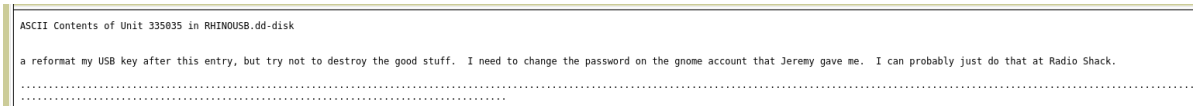
Rhino Hunt (DFRWS 2005) Examination Report

Examiner: Ronnie Helser

This report documents an examination of the DFRWS 2005 “Rhino Hunt” evidence set, a digital forensics scenario built around a USB key disk image (RHINOUSB.dd) and three network packet captures. The purpose of the examination was to determine how the suspect obtained unauthorized access, identify the files transferred over the network, and recover any data concealed on the USB device. All analysis was performed on a Kali Linux workstation using Autopsy 2.x, Wireshark, Foremost, John the Ripper, and jphide/jpseek.

Who gave the suspect a Telnet/FTP account?

Jeremy provided the suspect with a gnome account. This is documented in Autopsy 2.x under the “Data Unit” tab, within Unit 335035 of the disk image, where the admission appears in plain ASCII text.

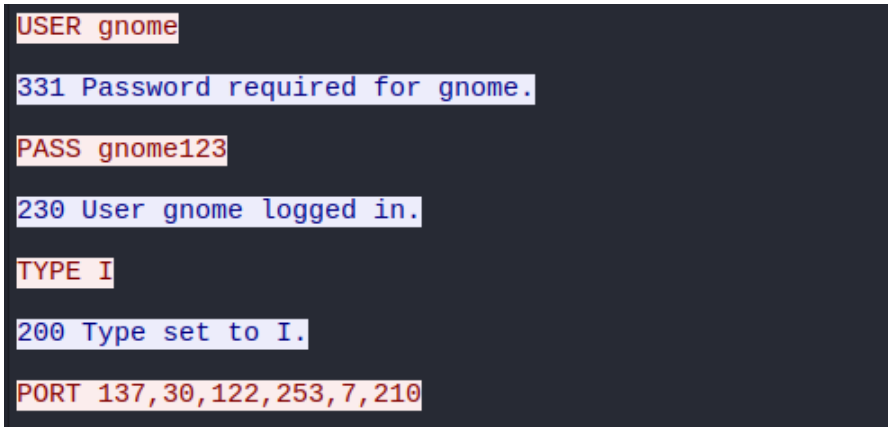


Unit 335035: Jeremy admits to providing the suspect with the gnome account.

What is the username and password for that account?

Username: `gnome`
Password: `gnome123`

These credentials were recovered from rhino.log by following the TCP stream on frame 1538. The login exchange was transmitted in cleartext and appears directly in the stream.



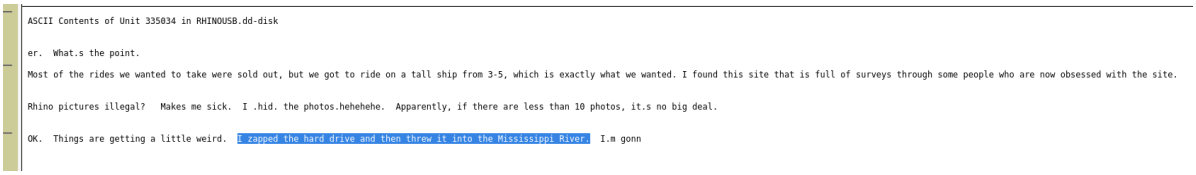
TCP stream, frame 1538: USER and PASS values transmitted in cleartext.

What file transfers appear in the network traces?

rhino1.jpg, rhino2.jpg (delivered inside contraband.zip), and rhino3.jpg were transferred over FTP-DATA and exported from rhino.log. rhino4.jpg and rhino5.gif were transferred over HTTP and exported from rhino2.log. rhino.exe followed a different path: a reference to the executable appeared in IMAP traffic within rhino3.log, and the file itself was later located and exported from an HTTP packet.

What happened to the hard drive?

According to Unit 335034 of the disk image, the suspect admits to wiping (“zapping”) the hard drive and disposing of it in the Mississippi River.



```
ASCII Contents of Unit 335034 in RHINOUSB.dd-disk

er.  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 gonn
```

Unit 335034: the suspect's account of wiping and disposing of the hard drive.

What happened to the USB key?

The USB key was reformatted using a downloaded DISM-based utility named rhino.exe, the same executable referenced in the IMAP traffic described above.

What could be recovered from the dd image of the USB key?

A number of rhinoceros images were recovered from the disk image, along with several alligator images. Two of the alligator images were found to contain hidden rhinoceros image data, embedded using jphide. The same admission from Jeremy referenced above also appears within Unit 335034 of this image. Several gumbo recipe files were present on the drive as well; these initially appeared unremarkable, but one of the two steganographically encoded alligator images was later found to use the passphrase “gumbo.”

Does any evidence connect the USB key to the network traces?

Yes. The file recovered from contraband.zip, itself pulled from an FTP-DATA transfer in rhino.log, was password protected. John the Ripper cracked the password as “monkey,” revealing a copy of rhino2.jpg. This image is identical to a rhinoceros photograph independently recovered from the USB key using Foremost and Autopsy, establishing a direct link between the USB key and the observed network traffic.

IMAP Account

Webmail credentials believed to belong to the suspect were also recovered during the examination:

Email: `hugerhinolover@hotmail.com`
Username: `Golden`
Password: `kinky!tang`

Supporting Evidence

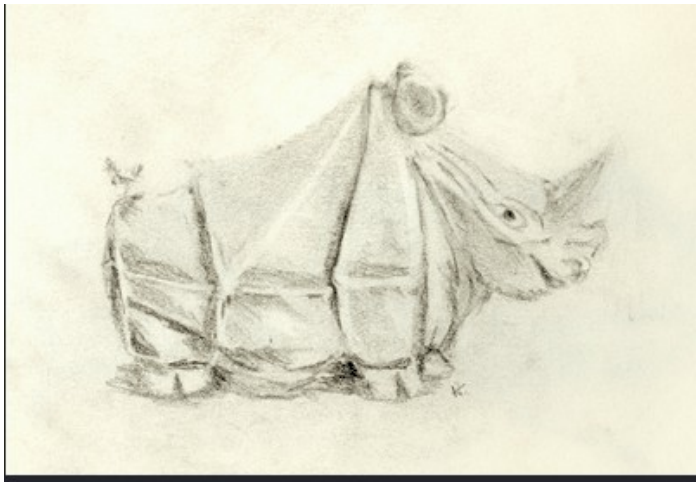
The following exhibits correspond to the findings described above, presented in the order referenced.

rhino1.jpg captured in transit over FTP (Log 1, packet 1551).

contraband.zip containing rhino2.jpg, captured over FTP and later cracked with John the Ripper, password “monkey” (Log 1, packet 5652).

rhino3.jpg captured in transit over FTP (Log 1, packets 1654 and 1768).

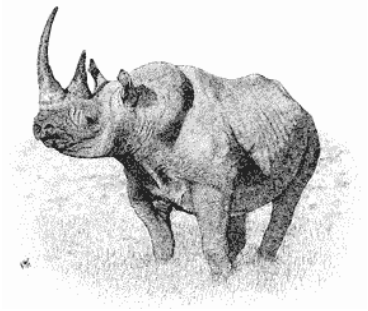
rhino4.jpg captured in transit over HTTP (Log 2, packet 215).



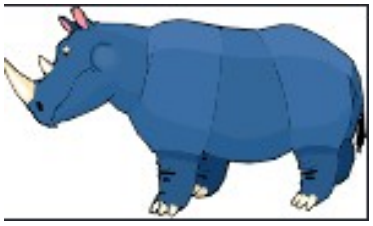
rhino5.gif captured in transit over HTTP (Log 2, packet 312).

The following three files were recovered directly from RHINOUSB.dd using Foremost:

00106393.jpg



00106865.gif



00106889.gif

rhino6.jpg, extracted using jpseek from the jphide-encoded alligator image, password “gumbo.”