Cover sheet Form 185s q.48

U.S DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

Bureau File Number #0001

CLASSIFICATION NO. 56487

FINAL PROJECT CASE

Forensic Investigator: **RICHARD MUNOZ**

X - FILE

Series

Volume Number 7 5436

032687

See also

260 458

985472

14698 0

FORENSIC REPORT

DATE: 48395
TIME OF THE INCIDENT: 5783945

SECTION I CASE DETAILS

Executive Summary:

Throughout the forensic investigation, there was success in regards to discovering several artifacts. Examiner utilized software technologies to uncover traces and files that related to the prohibited ownership of animal imagery. Steps were taken that involved using a forensic tool, Autopsy, to scan and analyze a disc image that contained traces of an operating system that was involved with flagged activity. These findings revealed numerous artifacts such as, explicit images, text-evidence, and user accounts. Also, other technologies were involved to discover other forms of technology footprint. By utilizing Kali Linux operating system and Wireshark Packet Sniffer, network traces were analyzed that contained additional explicit images of rhinoceros. All information regarding location, time, protocols were collected to demonstrate in court proceedings.

Case Background:

Purpose of the examination of the following disc image and logical files provided by authorities was to investigate and gather any evidence that pertained to the prohibited ownership of at least nine or more images that contained rhinoceros. Network administrators from the local university successfully flagged a computer system that had detected activity related to rhinoceros. When discovered, the system has been vandalized with the local disc being removed by whomever conducted illegal activity. Authorities were successful in retrieving the computer system and a USB drive which contained an image of the drive that was removed.

SECTION II EVIDENCE

The items listed in the "Physical Evidence" section of this report remained in the secure chain of custody of Richard Munoz throughout the analysis process.

- ☐ **Computer System**
- ☐ **RHINOUSB.dd (USB drive)**
- ☐ **rhino.log**
- ☐ **rhino2.log**
- ☐ **rhino3.log**

SECTION III: METHODS

Tools and **methods** used for digital evidence collection:

- ☐ **Autopsy: Digital Forensic (software)**
- ☐ **Utilized "Keyword Lists" to identify text-related evidence**
- ☐ **Kali Linux: fcrackzip (password crack)**
- ☐ **Uploaded disc image and logical files using "Data Source"**
- ☐ **Kali Linux operating system with combination of Wireshark Packet Sniffer**
- ☐ **Penetration Testing: rockyou.txt (password crack)**

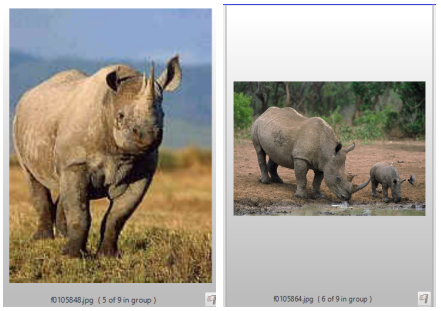
SECTION IV: FINDINGS REPORT

Results of network traffic within logical files and disc image:

Multiple images of rhinoceros appeared within location:

RHINOUSB.dd > $CarvedFiles > File: 1

Text-based evidence explains location of the hard drive taken from computer system.



Rhino running/walking in field
Two rhinos drinking water
F0105848.jpg F0105864.jpg

Location of hard drive revealed to be in the Mississippi river after being wiped.

f0334472_She_died_in_February_at_the_age_of_74.doc

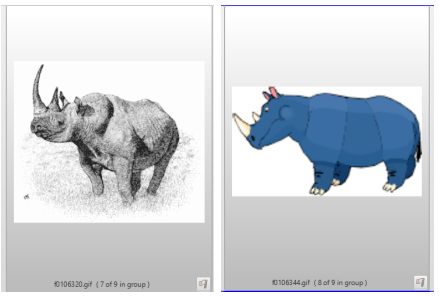
"I zapped the hard drive and then threw it into the Mississippi River. I'm gonna reformat my USB key after this entry, but try not to destroy the good stuff. "

Suspect identifies individual that gave the telnet/ftp account:

f0334472_She_died_in_February_at_the_age_of_74.doc

New suspect: Jeremy

" I need to change the password on the gnome account that Jeremy gave me. I can probably just do that at Radio Shack."



Drawing of rhino
Cartoon image of rhino
F0106320.jpg F01063344.jpg

A) Findings within RHINOUSB.dd

No. 1532

Time: 182.640647

Source: 137.30.122.253

Dest. 137.30.120.40

Protocol: FTP

Length: 66

Info: USER

gnome

B) Findings within RHINOUSB.dd

No. 1536

Time: 184.667754

Source: 137.30.122.253

Dest. 137.30.120.40

Protocol: FTP

Length: 69

Info: PASS

gnome123

C) Findings within RHINOUSB.dd

No. 1546

Time: 188.996081

Source: 137.30.122.253

Dest. 137.30.120.40

Protocol: FTP

Length: 71

Info: STOR rhino1.jpg

Rhino in the middle of a field

D) Findings within RHINOUSB.dd

No. 1763

Time: 215.133258

Source: 137.30.122.253

Dest. 137.30.120.40

Protocol: FTP

Length: 71

Info: STOR rhino3.jpg

Two rhinos standing next to eachother

E) Findings within RHINOUSB.dd

No. 5832

Time: 485.916123

Source: 137.30.122.253

Dest. 137.30.120.40

Protocol: FTP-DATA

Length: 1400

Info: contraband.zip

Two rhinos drinking water

F) Findings within RHINOUSB.dd

No. 49

Time: 7.892558

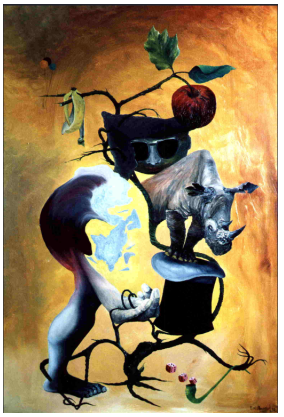
Source: 137.30.123.234

Dest. 137.30.120.37

Protocol: HTTP

Length: 488

Info: gnome/rhino4.jpg



Dynamic rhino art

G) Findings within RHINOUSB.dd

No. 217

Time: 14.008741

Source: 137.30.123.234

Dest. 137.30.120.37

Protocol: HTTP

Length: 488

Info: gnome/rhino5.gif

Side view of a drawn rhino

Additional Information Discovered:

Relevant files that appeared within network traces were:	☐ Rhino1 ☐ Rhino2 ☐ Rhino3 ☐ Rhino5
Connection between USB drive and network traces: contraband.zip file contained similar images to content within disc image.	
Supporting evidence regard to previous statement: Image of two rhinos drinking water from a puddle.	**Details of outcome of USB drive:** Suspect formatted USB
	Recoverable information from USB drive: Rhino images were discovered using Autopsy software.