DFRWS 2005 RODEO CHALLENGE

Wave your hand if you have a question and one of the organizers will pop over and give you a tip.

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.

MD5 hashes for evidence:

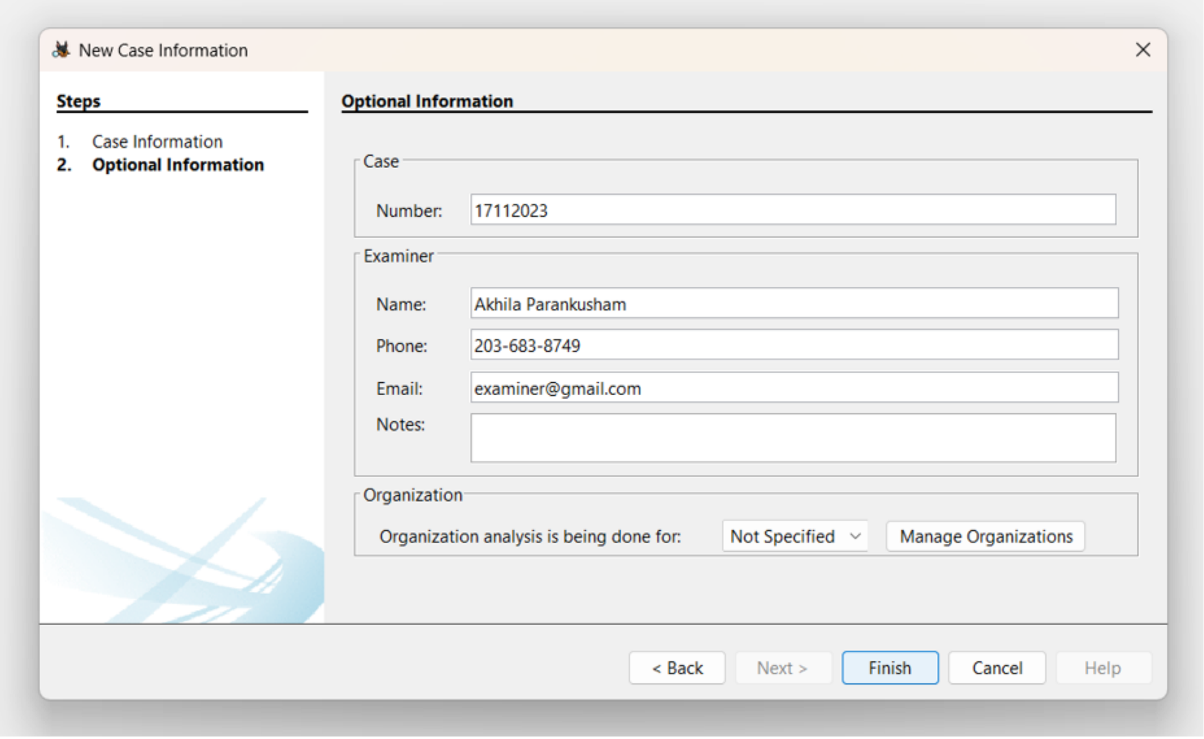
c0d0093eb1664cd7b73f3a5225ae3f30 *rhino.log
cd21eaf4acfb50f71ffff857d7968341 *rhino2.log
7e29f9d67346df25faaf18efcd95fc30 *rhino3.log
80348c58eec4c328ef1f7709adc56a54 *RHINOUSB.dd

Your task:

Recover at least nine 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?

When you're done, exclaim loudly and jump about the room.



New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: 17112023

Examiner

Name: Akhila Parankusham

Phone: 203-683-8749

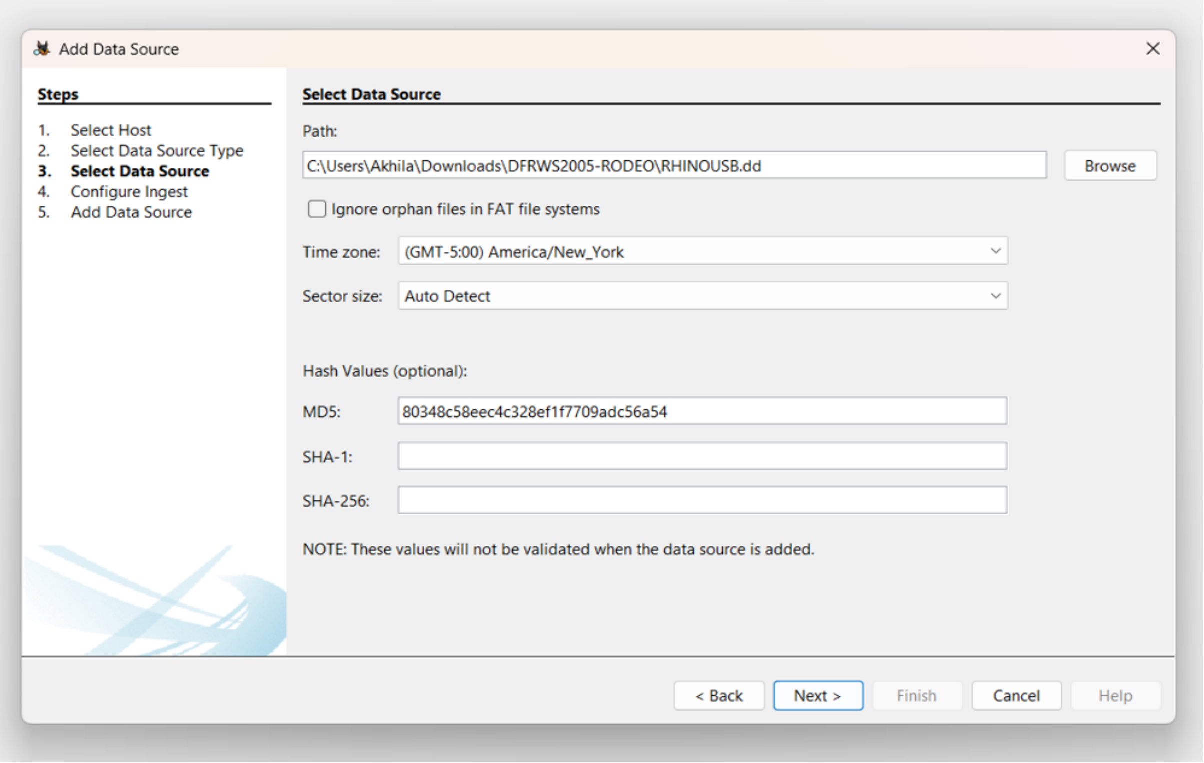
Email: examiner@gmail.com

Notes:

Organization

Organization analysis is being done for: Not Specified

Figure 1: Case Created



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: C:\Users\Akhila\Downloads\DFRWS2005-RODEO\RHINOUSB.dd

□ Ignore orphan files in FAT file systems

Time zone: (GMT-5:00) America/New_York

Sector size: Auto Detect

Hash Values (optional):

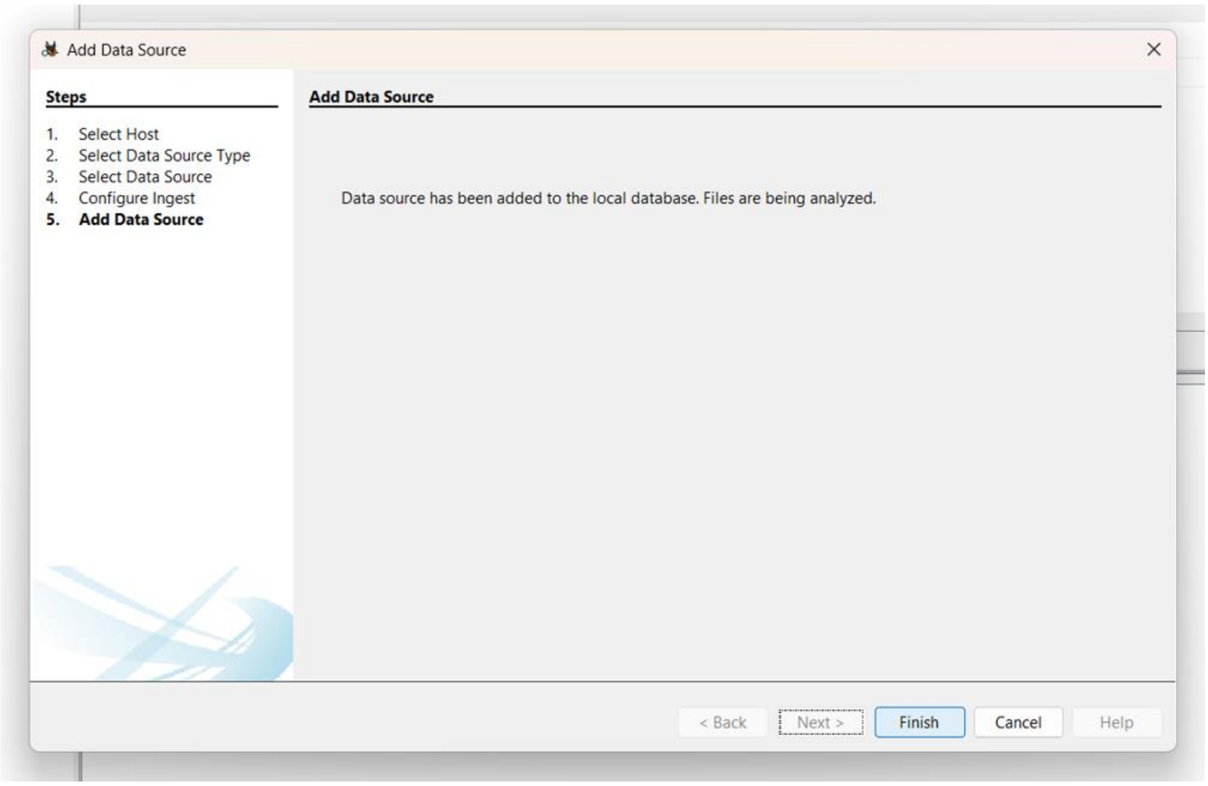
MD5: 80348c58eec4c328ef1f7709adc56a54

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Figure 2: Selecting the Data Source



Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

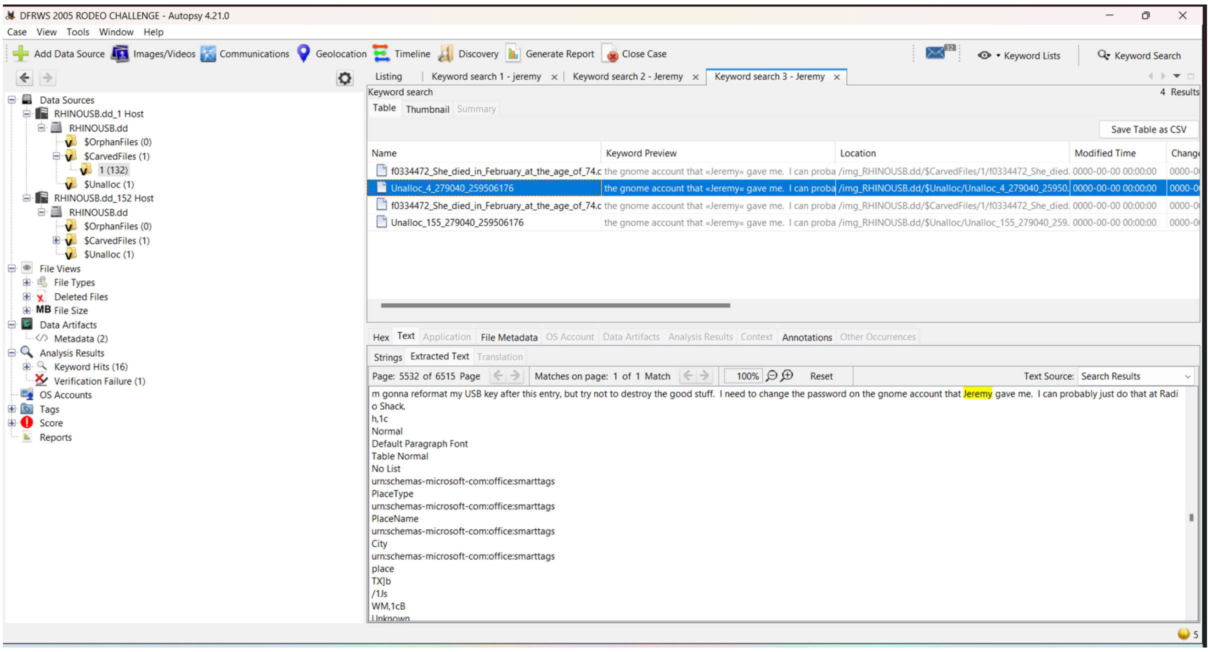
Add Data Source

Data source has been added to the local database. Files are being analyzed.

Figure 3: Data Source Added. Files are being analyzed.

Who gave the accused a telnet/ftp account?

The Telnet/FTP account details were given to the accused by **Jeremy**.



Name	Keyword Preview	Location	Modified Time	Chang
f0334472_She_died_in_February_at_the_age_of_74.c	the gnome account that «Jeremy« gave me. I can proba	/img_RHINOUSB.dd/$CarvedFiles/1/f0334472_She_died.	0000-00-00 00:00:00	0000-0
Unalloc_4_279040_259506176	the gnome account that «Jeremy« gave me. I can proba	/img_RHINOUSB.dd/$Unalloc/Unalloc_4_279040_25950.	0000-00-00 00:00:00	0000-0
f0334472_She_died_in_February_at_the_age_of_74.c	the gnome account that «Jeremy« gave me. I can proba	/img_RHINOUSB.dd/$CarvedFiles/1/f0334472_She_died.	0000-00-00 00:00:00	0000-0
Unalloc_155_279040_259506176	the gnome account that «Jeremy« gave me. I can proba	/img_RHINOUSB.dd/$Unalloc/Unalloc_155_279040_259.	0000-00-00 00:00:00	0000-0

Page: 5532 of 6515 Page Matches on page: 1 of 1 Match 100% Text Source: Search Results

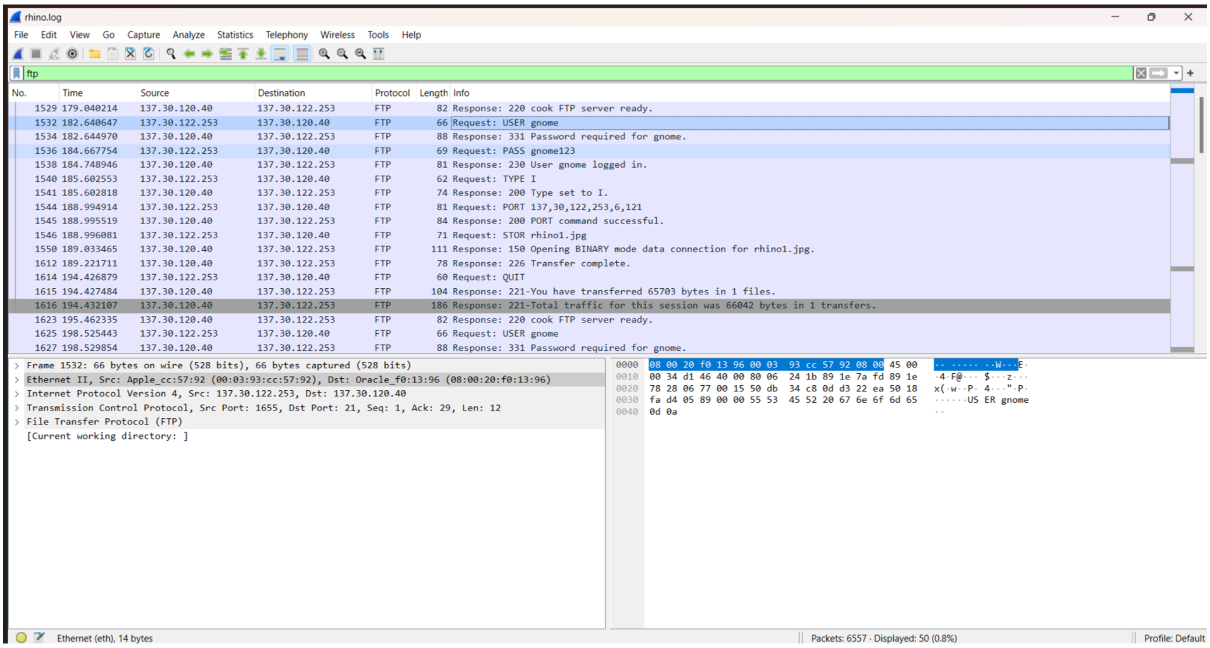
```
m gonna reformat my USB key after this entry, but try not to destroy the good stuff.  I need to change the password on the gnome account that Jeremy gave me.  I can probably just do that at Radi
o Shack.
h,1c
Normal
Default Paragraph Font
Table Normal
No List
urn:schemas-microsoft-com:office:smarttags
PlaceType
urn:schemas-microsoft-com:office:smarttags
PlaceName
urn:schemas-microsoft-com:office:smarttags
City
urn:schemas-microsoft-com:office:smarttags
place
TX]b
/1Js
WM,1cB
Unknown
```

What's the username/password for the account?

The rhino log files were analyzed in Wireshark to retrieve the username and password.

The username identified for the account is "gnome."

The password discovered for the account is "gnome123."



rhino.log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ftp
```

```
No.     Time        Source          Destination     Protocol Length Info
   1529 179.040214  137.30.120.40   137.30.122.253  FTP        82 Response: 220 cook FTP server ready.
   1532 182.640647  137.30.122.253  137.30.120.40   FTP        66 Request: USER gnome
   1534 182.644970  137.30.120.40   137.30.122.253  FTP        88 Response: 331 Password required for gnome.
   1536 184.667754  137.30.122.253  137.30.120.40   FTP        69 Request: PASS gnome123
   1538 184.748946  137.30.120.40   137.30.122.253  FTP        81 Response: 230 User gnome logged in.
   1540 185.602553  137.30.122.253  137.30.120.40   FTP        62 Request: TYPE I
   1541 185.602818  137.30.120.40   137.30.122.253  FTP        74 Response: 200 Type set to I.
   1544 188.994914  137.30.122.253  137.30.120.40   FTP        81 Request: PORT 137,30,122,253,6,121
   1545 188.995519  137.30.120.40   137.30.122.253  FTP        84 Response: 200 PORT command successful.
   1546 188.996081  137.30.122.253  137.30.120.40   FTP        71 Request: STOR rhino1.jpg
   1550 189.033465  137.30.120.40   137.30.122.253  FTP       111 Response: 150 Opening BINARY mode data connection for rhino1.jpg.
   1612 189.221711  137.30.120.40   137.30.122.253  FTP        78 Response: 226 Transfer complete.
   1614 194.426879  137.30.122.253  137.30.120.40   FTP        60 Request: QUIT
   1615 194.427484  137.30.120.40   137.30.122.253  FTP       104 Response: 221-You have transferred 65703 bytes in 1 files.
   1616 194.432107  137.30.120.40   137.30.122.253  FTP       186 Response: 221-Total traffic for this session was 66042 bytes in 1 transfers.
   1623 195.462335  137.30.120.40   137.30.122.253  FTP        82 Response: 220 cook FTP server ready.
   1625 198.525443  137.30.122.253  137.30.120.40   FTP        66 Request: USER gnome
   1627 198.529854  137.30.120.40   137.30.122.253  FTP        88 Response: 331 Password required for gnome.
```

```
> Frame 1532: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: Apple_cc:57:92 (00:03:93:cc:57:92), Dst: Oracle_f0:13:96 (08:00:20:f0:13:96)
> Internet Protocol Version 4, Src: 137.30.122.253, Dst: 137.30.120.40
> Transmission Control Protocol, Src Port: 1655, Dst Port: 21, Seq: 1, Ack: 29, Len: 12
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  08 00 20 f0 13 96 00 03  93 cc 57 92 08 00 45 00   ·· ····· ··W···E·
0010  00 34 d1 46 40 00 80 06  24 1b 89 1e 7a fd 89 1e   ·4·F@··· $···z···
0020  78 28 06 77 00 15 50 db  34 c8 0d d3 22 ea 50 18   x(·w··P· 4···"·P·
0030  fa d4 05 89 00 00 55 53  45 52 20 67 6e 6f 6d 65   ······US ER gnome
0040  0d 0a                                              ··
```

What relevant file transfers appear in the network traces?

Four rhino photos (1–4) were found on the USB drive.

Photos in the free space were potentially recoverable.

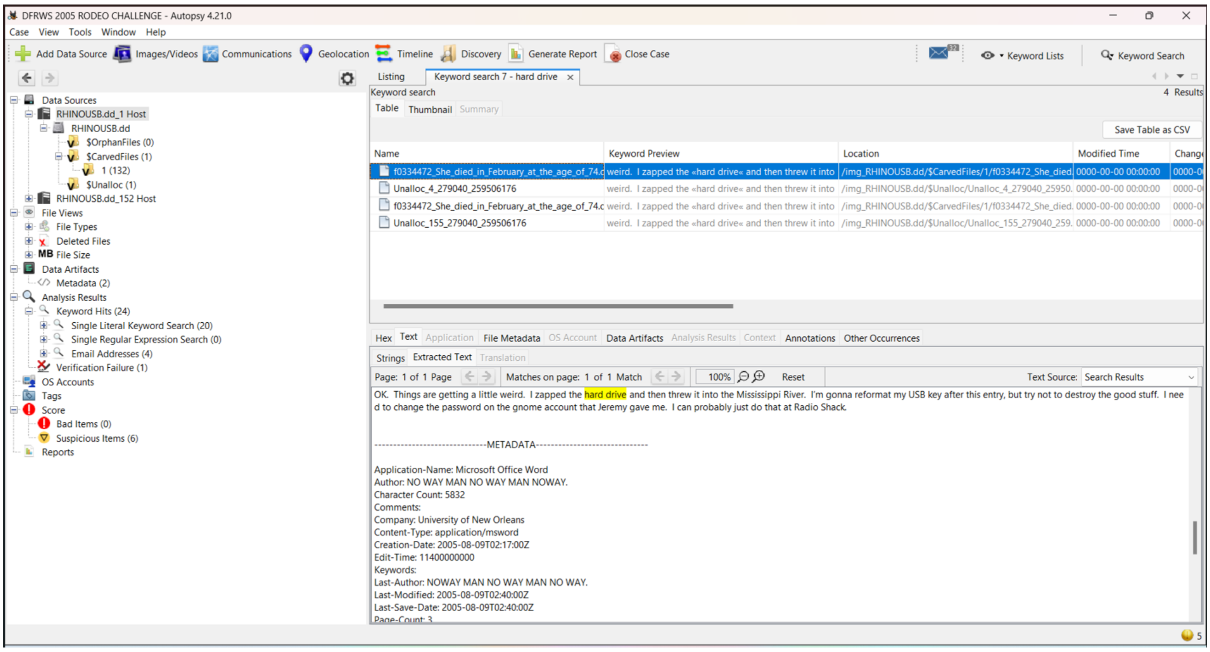
Two pictures (5 and 6) were found in the rhino.log trace.

From the rhino2.log trace, two photos (7 and 8) have been recovered.

- f0106393.jpg with MD5sum ca03f2eed3db06a82a8a31b3a3defa24
- f0106409.jpg with MD5sum ed870202082ea4fd8f5488533a561b35
- f0106865.gif with MD5sum 76610b7bdb85e5f65e96df3f7e417a74
- f0106889.gif with MD5sum d03dc23d4ec39e4d16da3c46d2932d62
- rhino1.jpg with MD5sum d5a83cde0131c3a034e5a0d3bd94b3c9
- rhino3.jpg with MD5sum b058218ea0060092d4e01ef3d7a3b815
- rhino4.jpg with MD5sum aa64102afff71b93ed61fb100af8d52a
- rhino5.gif with MD5sum 1e90b7f70b2ecb605898524a88269029

What happened to the hard drive in the computer? Where is it now?

The suspect zapped the hard drive and then threw it into the Mississippi River.



Name	Keyword Preview	Location	Modified Time	Change
f0334472_She_died_in_February_at_the_age_of_74.c	weird. I zapped the «hard drive« and then threw it into	/img_RHINOUSB.dd/$CarvedFiles/1/f0334472_She_died.	0000-00-00 00:00:00	0000-0
Unalloc_4_279040_259506176	weird. I zapped the «hard drive« and then threw it into	/img_RHINOUSB.dd/$Unalloc/Unalloc_4_279040_25950.	0000-00-00 00:00:00	0000-0
f0334472_She_died_in_February_at_the_age_of_74.c	weird. I zapped the «hard drive« and then threw it into	/img_RHINOUSB.dd/$CarvedFiles/1/f0334472_She_died.	0000-00-00 00:00:00	0000-0
Unalloc_155_279040_259506176	weird. I zapped the «hard drive« and then threw it into	/img_RHINOUSB.dd/$Unalloc/Unalloc_155_279040_259.	0000-00-00 00:00:00	0000-0

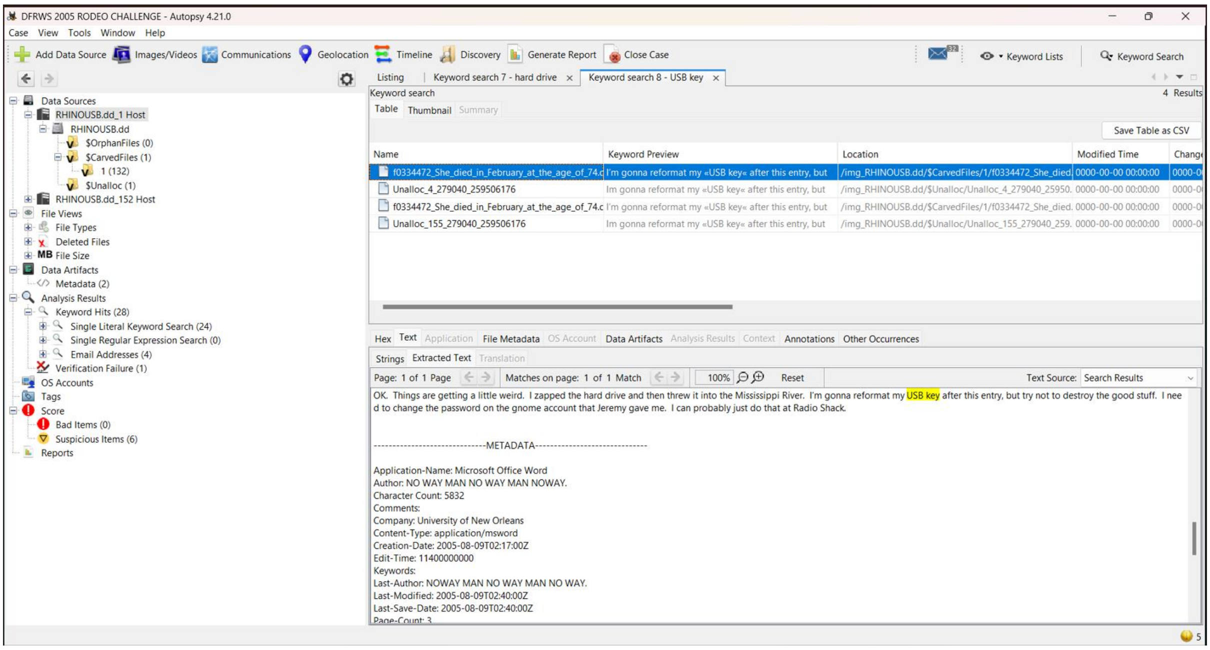
```
OK.  Things are getting a little weird.  I zapped the hard drive and then threw it into the Mississippi River.  I'm gonna reformat my USB key after this entry, but try not to destroy the good stuff.  I nee
d to change the password on the gnome account that Jeremy gave me.  I can probably just do that at Radio Shack.


-----------------------------METADATA-----------------------------

Application-Name: Microsoft Office Word
Author: NO WAY MAN NO WAY MAN NOWAY.
Character Count: 5832
Comments:
Company: University of New Orleans
Content-Type: application/msword
Creation-Date: 2005-08-09T02:17:00Z
Edit-Time: 11400000000
Keywords:
Last-Author: NOWAY MAN NO WAY MAN NO WAY.
Last-Modified: 2005-08-09T02:40:00Z
Last-Save-Date: 2005-08-09T02:40:00Z
Page-Count: 3
```

What happened to the USB key?

The USB key was supposedly reformatted by the suspect, possibly at Radio Shack, aiming to preserve the "good" information.



Name	Keyword Preview	Location	Modified Time	Change
f0334472_She_died_in_February_at_the_age_of_74.c	I'm gonna reformat my «USB key« after this entry, but	/img_RHINOUSB.dd/$CarvedFiles/1/f0334472_She_died.	0000-00-00 00:00:00	0000-0
Unalloc_4_279040_259506176	Im gonna reformat my «USB key« after this entry, but	/img_RHINOUSB.dd/$Unalloc/Unalloc_4_279040_25950.	0000-00-00 00:00:00	0000-0
f0334472_She_died_in_February_at_the_age_of_74.c	I'm gonna reformat my «USB key« after this entry, but	/img_RHINOUSB.dd/$CarvedFiles/1/f0334472_She_died.	0000-00-00 00:00:00	0000-0
Unalloc_155_279040_259506176	Im gonna reformat my «USB key« after this entry, but	/img_RHINOUSB.dd/$Unalloc/Unalloc_155_279040_259.	0000-00-00 00:00:00	0000-0

```
OK.  Things are getting a little weird.  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.  I nee
d to change the password on the gnome account that Jeremy gave me.  I can probably just do that at Radio Shack.


-----------------------------METADATA-----------------------------

Application-Name: Microsoft Office Word
Author: NO WAY MAN NO WAY MAN NOWAY.
Character Count: 5832
Comments:
Company: University of New Orleans
Content-Type: application/msword
Creation-Date: 2005-08-09T02:17:00Z
Edit-Time: 11400000000
Keywords:
Last-Author: NOWAY MAN NO WAY MAN NO WAY.
Last-Modified: 2005-08-09T02:40:00Z
Last-Save-Date: 2005-08-09T02:40:00Z
Page-Count: 3
```

What is recoverable from the dd image of the USB key?

These files can be retrieved from the dd image of the USB key. They are:

rhino6.jpg in alligator2.jpg

[stego jphide, password = gator]

rhino7.jpg in alligator3.jpg

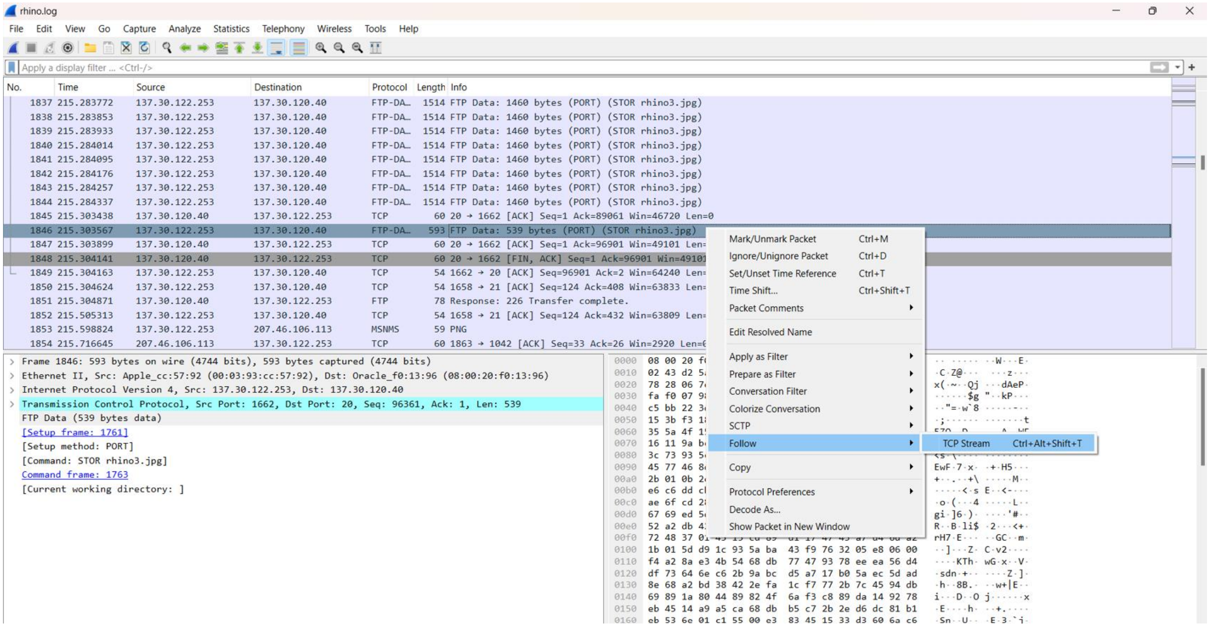
[stego jphide, password = gumbo]

rhino2, rhino8.gif, rhino9.gif, rhino10.bmp directly carve-able.

alligator1.jpg, alligator4.jpg are carve-able but irrelevant.

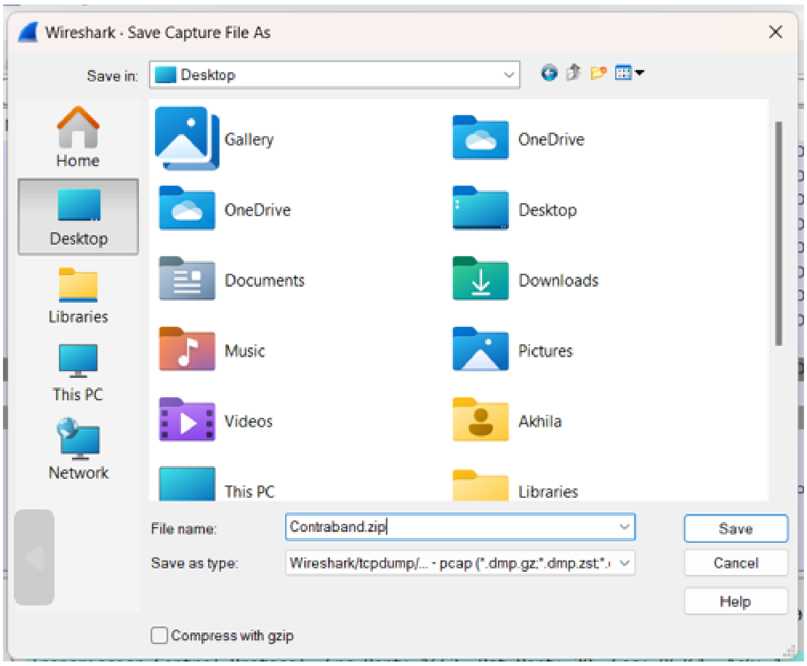
Is there any evidence that connects the USB key and the network traces? If so, what?

Similar to rhino2.jpg in the zip file from the network trace, rhino2.jpg was carved from a USBKEY.


rhino.log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
TCP Stream Ctrl+Alt+Shift+T
Copy
Protocol Preferences
Decode As...
Show Packet in New Window

```
No.     Time         Source           Destination      Protocol  Length Info
   1837 215.283772   137.30.122.253   137.30.120.40    FTP-DA…   1514 FTP Data: 1460 bytes (PORT) (STOR rhino3.jpg)
   1838 215.283853   137.30.122.253   137.30.120.40    FTP-DA…   1514 FTP Data: 1460 bytes (PORT) (STOR rhino3.jpg)
   1839 215.283933   137.30.122.253   137.30.120.40    FTP-DA…   1514 FTP Data: 1460 bytes (PORT) (STOR rhino3.jpg)
   1840 215.284014   137.30.122.253   137.30.120.40    FTP-DA…   1514 FTP Data: 1460 bytes (PORT) (STOR rhino3.jpg)
   1841 215.284095   137.30.122.253   137.30.120.40    FTP-DA…   1514 FTP Data: 1460 bytes (PORT) (STOR rhino3.jpg)
   1842 215.284176   137.30.122.253   137.30.120.40    FTP-DA…   1514 FTP Data: 1460 bytes (PORT) (STOR rhino3.jpg)
   1843 215.284257   137.30.122.253   137.30.120.40    FTP-DA…   1514 FTP Data: 1460 bytes (PORT) (STOR rhino3.jpg)
   1844 215.284337   137.30.122.253   137.30.120.40    FTP-DA…   1514 FTP Data: 1460 bytes (PORT) (STOR rhino3.jpg)
   1845 215.303438   137.30.120.40    137.30.122.253   TCP         60 20 → 1662 [ACK] Seq=1 Ack=89061 Win=46720 Len=0
   1846 215.303567   137.30.122.253   137.30.120.40    FTP-DA…    593 FTP Data: 539 bytes (PORT) (STOR rhino3.jpg)
   1847 215.303899   137.30.120.40    137.30.122.253   TCP         60 20 → 1662 [ACK] Seq=1 Ack=96901 Win=49101 Len=
   1848 215.304141   137.30.120.40    137.30.122.253   TCP         60 20 → 1662 [FIN, ACK] Seq=1 Ack=96901 Win=49101
   1849 215.304163   137.30.122.253   137.30.120.40    TCP         54 1662 → 20 [ACK] Seq=96901 Ack=2 Win=64240 Len=
   1850 215.304624   137.30.122.253   137.30.120.40    TCP         54 1658 → 21 [ACK] Seq=124 Ack=408 Win=63833 Len=
   1851 215.304871   137.30.120.40    137.30.122.253   FTP         78 Response: 226 Transfer complete.
   1852 215.505313   137.30.122.253   137.30.120.40    TCP         54 1658 → 21 [ACK] Seq=124 Ack=432 Win=63809 Len=
   1853 215.598824   137.30.122.253   207.46.106.113   MSNMS       59 PNG
   1854 215.716645   207.46.106.113   137.30.122.253   TCP         60 1863 → 1042 [ACK] Seq=33 Ack=26 Win=2920 Len=0
```

```
> Frame 1846: 593 bytes on wire (4744 bits), 593 bytes captured (4744 bits)
> Ethernet II, Src: Apple_cc:57:92 (00:03:93:cc:57:92), Dst: Oracle_f0:13:96 (08:00:20:f0:13:96)
> Internet Protocol Version 4, Src: 137.30.122.253, Dst: 137.30.120.40
> Transmission Control Protocol, Src Port: 1662, Dst Port: 20, Seq: 96361, Ack: 1, Len: 539
  FTP Data (539 bytes data)
  [Setup frame: 1761]
  [Setup method: PORT]
  [Command: STOR rhino3.jpg]
  Command frame: 1763
  [Current working directory: ]
```

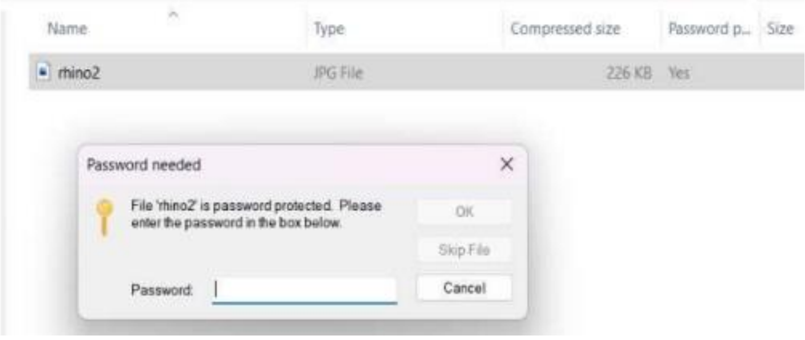


File name: Contraband.zip

Save as type: Wireshark/tcpdump/... - pcap (*.dmp.gz;*.dmp.zst;*.

□ Compress with gzip

To break the password, I used the tool fcrack.zip and was able to obtain the password, which is 'monkey,' and when I entered the password, I was able to retrieve Rhino2.jpg.



Name	Type	Compressed size	Password p...	Size
rhino2	JPG File	226 KB	Yes	

Password needed

File 'rhino2' is password protected. Please enter the password in the box below.

Password:

Conclusion

Recovered four Rhino images (2 jpeg, 2 gif) and five alligator images from deleted files.

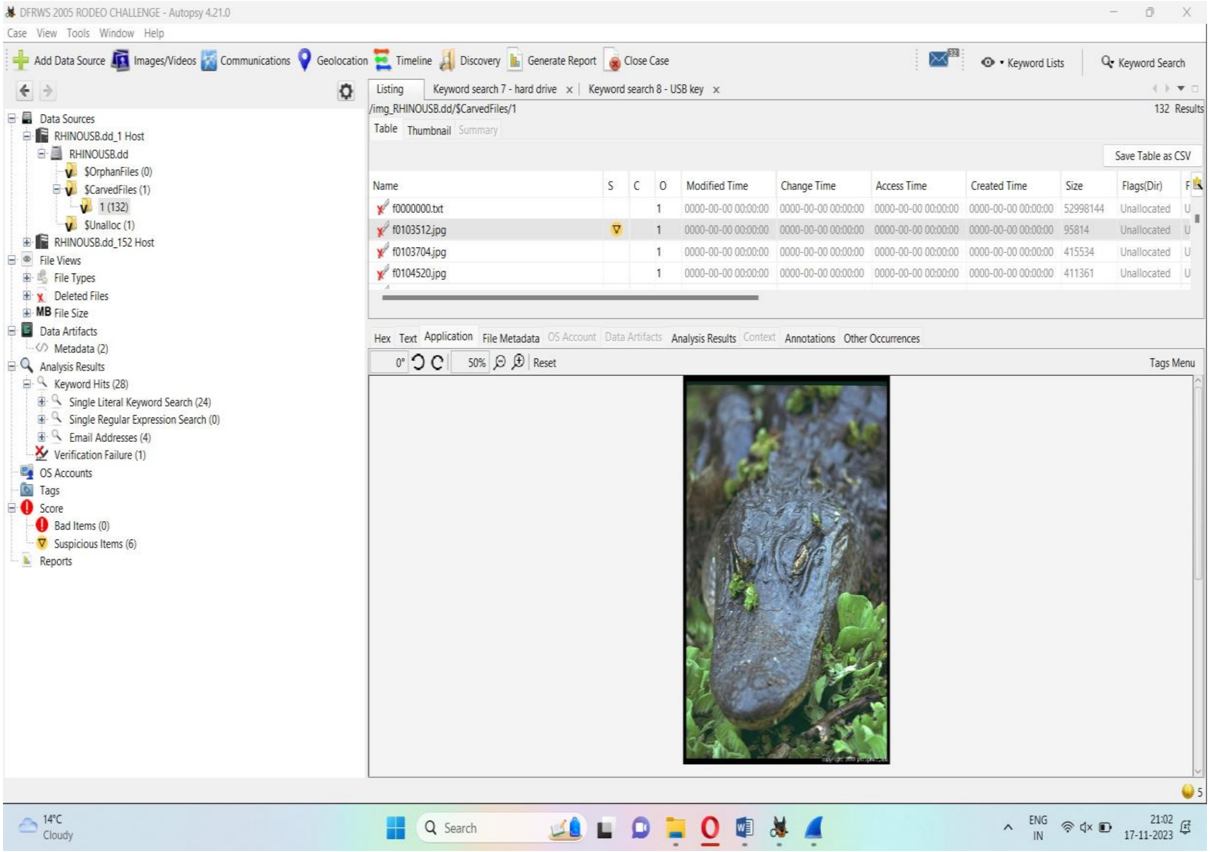
Discovered Rhino4.jpg and Rhino5.gif while analyzing Rhino log files in Wireshark.

Detected a Contraband zip file in Rhino.log and decrypted it using fcrack.zip (password - monkey).

Retrieved Rhino2.jpg from the decrypted Contraband zip file.

Images

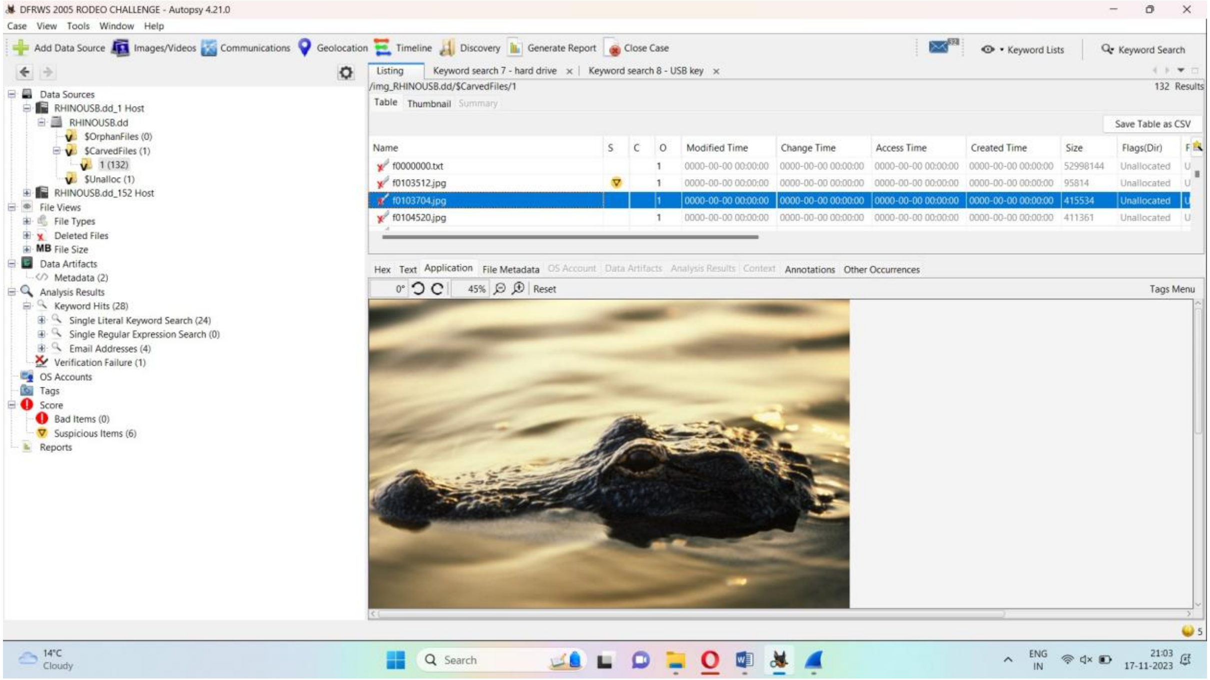
f0103512.jpg



/img_RHINOUSB.dd/$CarvedFiles/1 132 Results

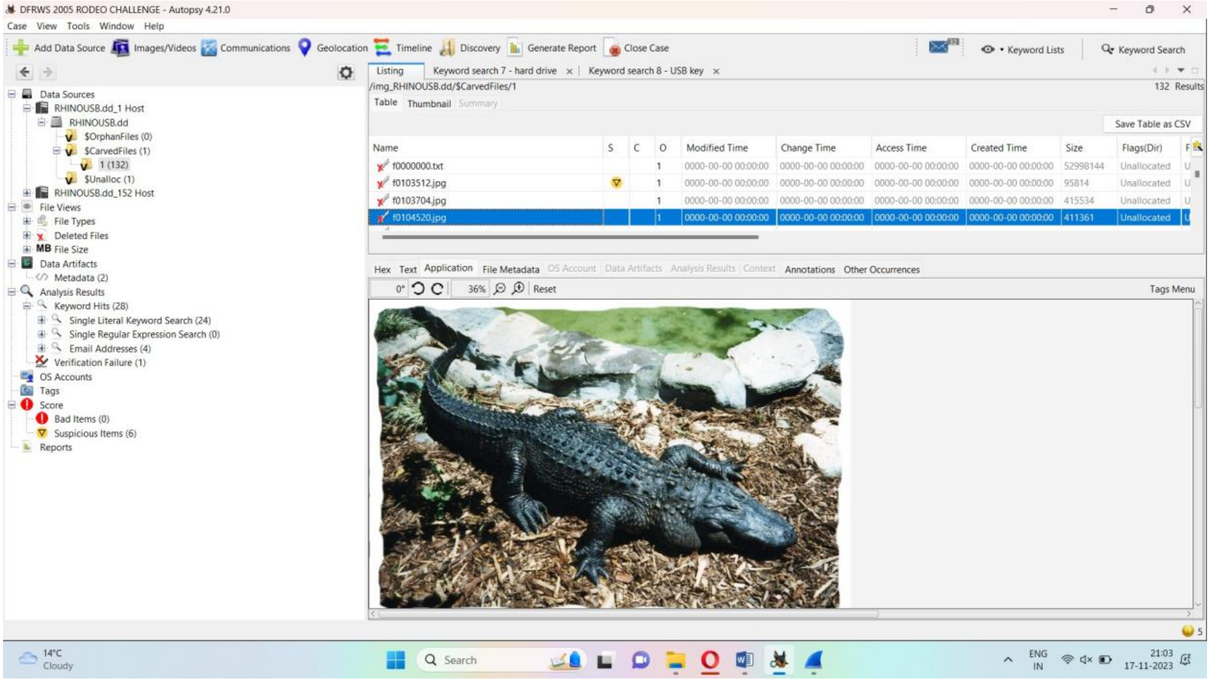
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	F
f0000000.txt			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	52998144	Unallocated	U
f0103512.jpg	▽		1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	95814	Unallocated	U
f0103704.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	415534	Unallocated	U
f0104520.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	411361	Unallocated	U

f0103704.jpg



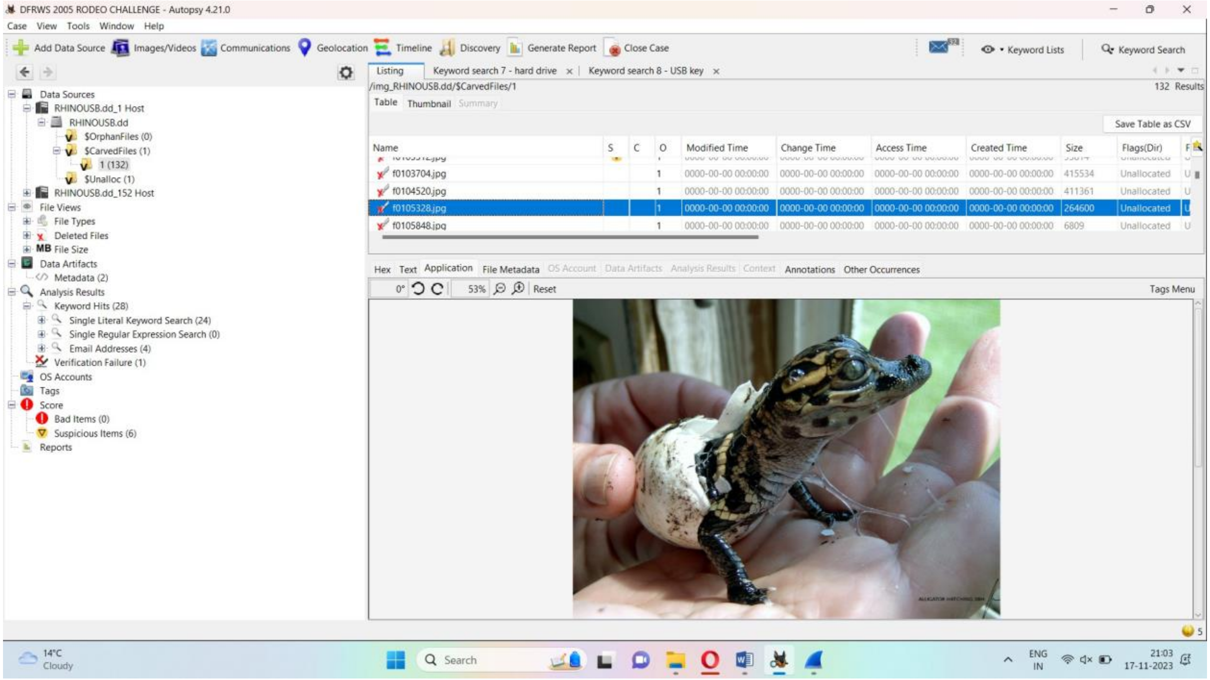
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	F
f0000000.txt			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	52998144	Unallocated	U
f0103512.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	95814	Unallocated	U
f0103704.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	415534	Unallocated	U
f0104520.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	411361	Unallocated	U

f0104520.jpg



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	F
f0000000.txt			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	52998144	Unallocated	U
f0103512.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	95814	Unallocated	U
f0103704.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	415534	Unallocated	U
f0104520.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	411361	Unallocated	U

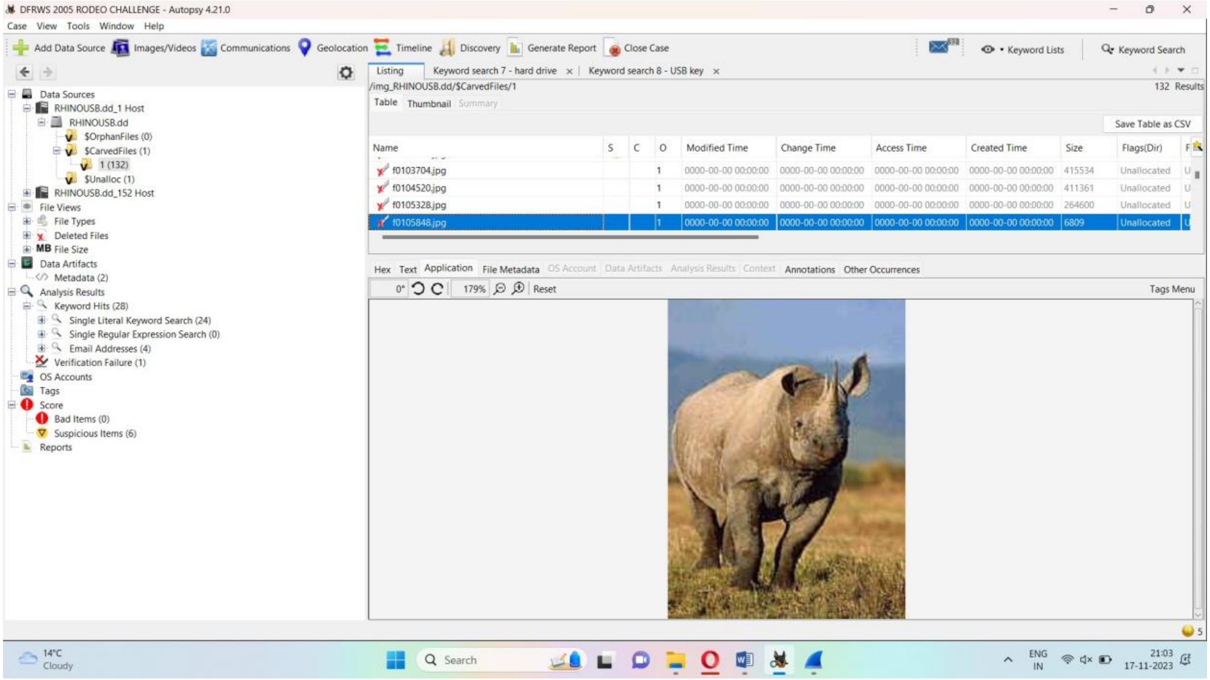
f0105328.jpg


DFRWS 2005 RODEO CHALLENGE - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing Keyword search 7 - hard drive Keyword search 8 - USB key
Data Sources
RHINOUSB.dd_1 Host
RHINOUSB.dd
$OrphanFiles (0)
$CarvedFiles (1)
1 (132)
$Unalloc (1)
RHINOUSB.dd_152 Host
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Metadata (2)
Analysis Results
Keyword Hits (28)
Single Literal Keyword Search (24)
Single Regular Expression Search (0)
Email Addresses (4)
Verification Failure (1)
OS Accounts
Tags
Score
Bad Items (0)
Suspicious Items (6)
Reports
Table Thumbnail Summary
Save Table as CSV
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
0° 53% Reset
Tags Menu
14°C Cloudy
Search
ENG IN
21:03 17-11-2023

/img_RHINOUSB.dd/$CarvedFiles/1 132 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
f0103704.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	415534	Unallocated
f0104520.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	411361	Unallocated
f0105328.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	264600	Unallocated
f0105848.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6809	Unallocated

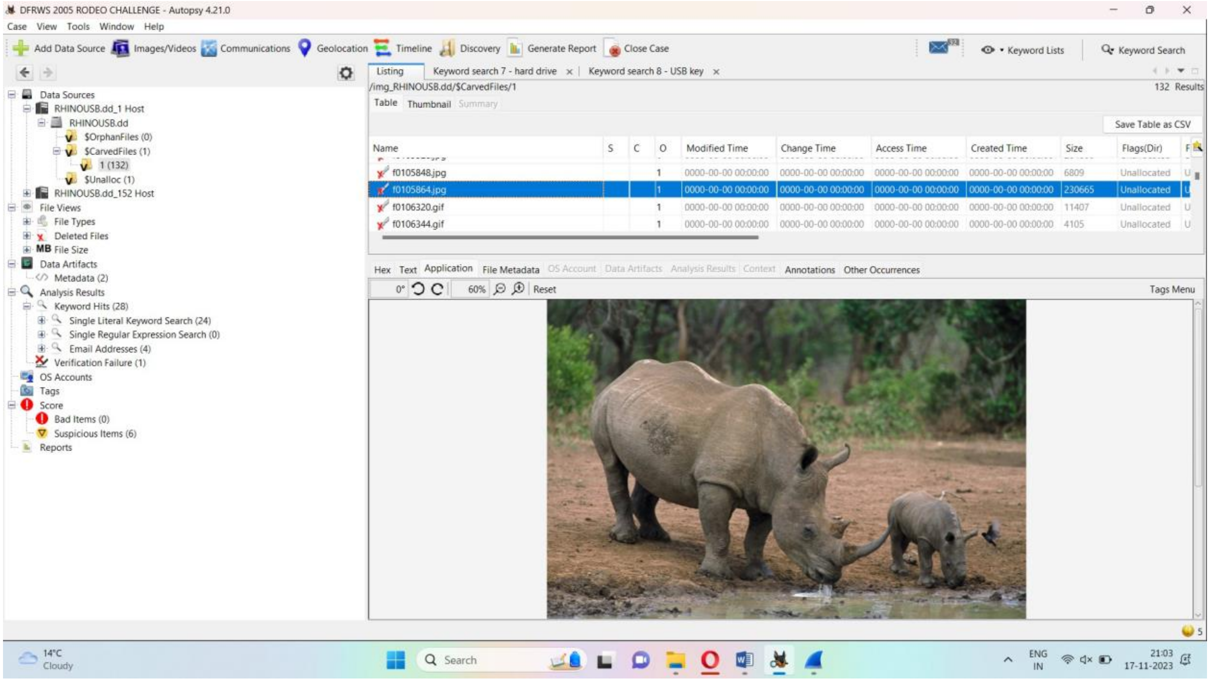
f0105848.jpg


DFRWS 2005 RODEO CHALLENGE - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing Keyword search 7 - hard drive Keyword search 8 - USB key
Data Sources
RHINOUSB.dd_1 Host
RHINOUSB.dd
$OrphanFiles (0)
$CarvedFiles (1)
1 (132)
$Unalloc (1)
RHINOUSB.dd_152 Host
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Metadata (2)
Analysis Results
Keyword Hits (28)
Single Literal Keyword Search (24)
Single Regular Expression Search (0)
Email Addresses (4)
Verification Failure (1)
OS Accounts
Tags
Score
Bad Items (0)
Suspicious Items (6)
Reports
Table Thumbnail Summary
Save Table as CSV
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
0° 179% Reset
Tags Menu
14°C Cloudy
Search
ENG IN
21:03 17-11-2023

/img_RHINOUSB.dd/$CarvedFiles/1 132 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
f0103704.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	415534	Unallocated
f0104520.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	411361	Unallocated
f0105328.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	264600	Unallocated
f0105848.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6809	Unallocated

f0105864.jpg

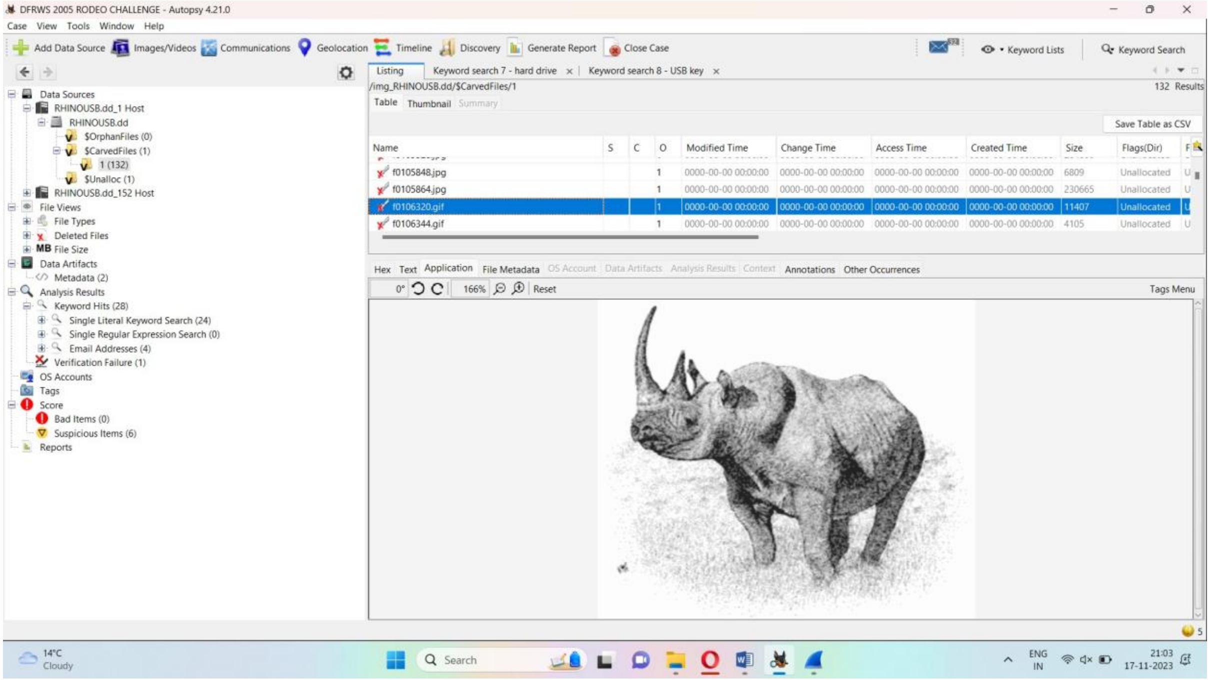


DFRWS 2005 RODEO CHALLENGE - Autopsy 4.21.0

/img_RHINOUSB.dd/$CarvedFiles/1 132 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	F
f0105848.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6809	Unallocated	U
f0105864.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	230665	Unallocated	U
f0106320.gif			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11407	Unallocated	U
f0106344.gif			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4105	Unallocated	U

f0106320.gif

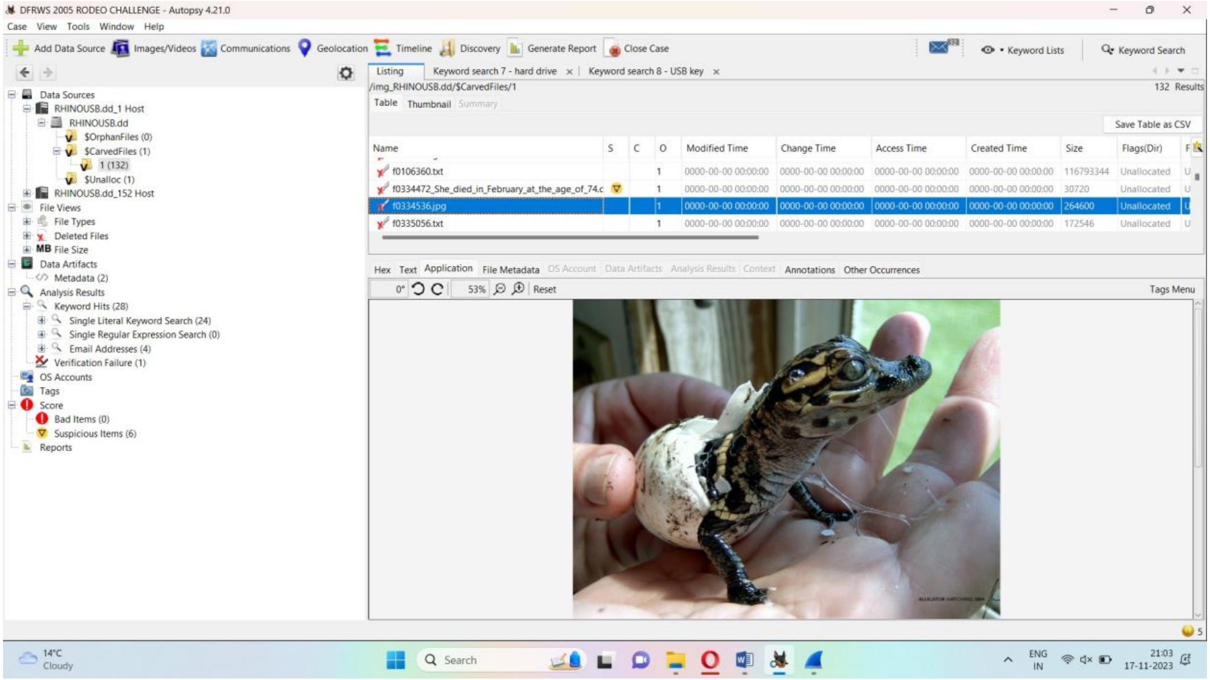


DFRWS 2005 RODEO CHALLENGE - Autopsy 4.21.0

/img_RHINOUSB.dd/$CarvedFiles/1 132 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	F
f0105848.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6809	Unallocated	U
f0105864.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	230665	Unallocated	U
f0106320.gif			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11407	Unallocated	U
f0106344.gif			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4105	Unallocated	U

f0334536.gif



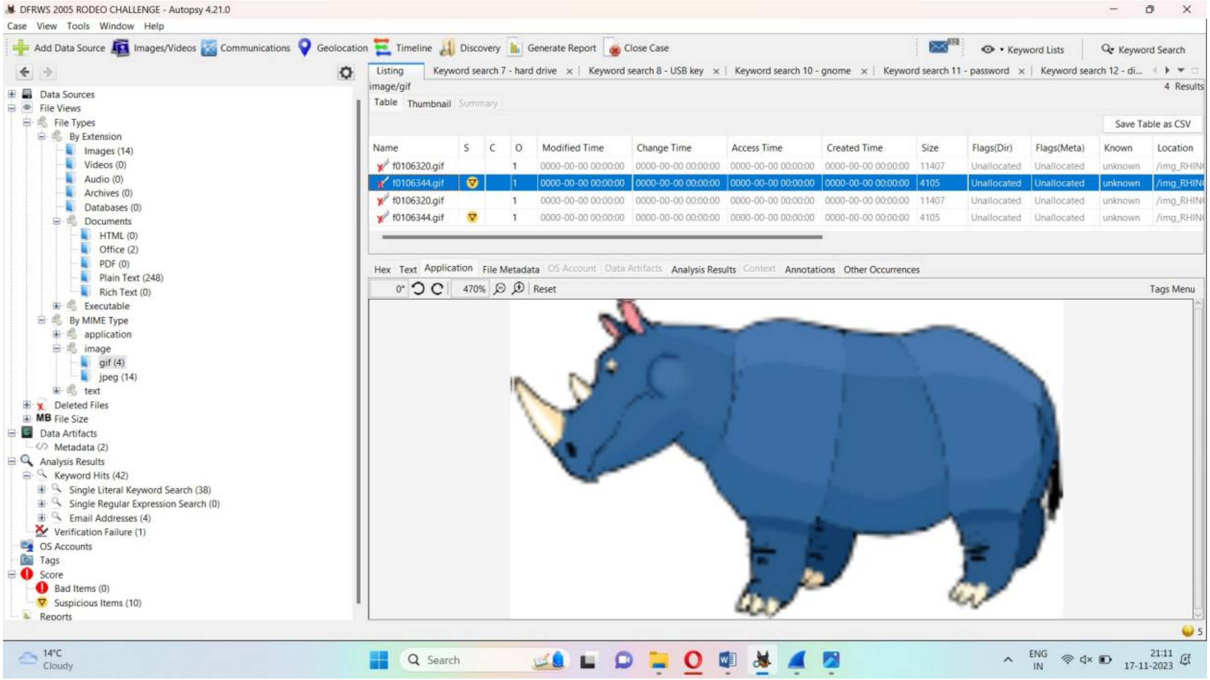
DFRWS 2005 RODEO CHALLENGE - Autopsy 4.21.0

/img_RHINOUSB.dd/$CarvedFiles/1

132 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	F
f0106360.txt			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	116793344	Unallocated	U
f0334472_She_died_in_February_at_the_age_of_74.c	▽		1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	30720	Unallocated	U
f0334536.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	264600	Unallocated	U
f0335056.txt			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	172546	Unallocated	U

f0106344.gif



DFRWS 2005 RODEO CHALLENGE - Autopsy 4.21.0

image/gif

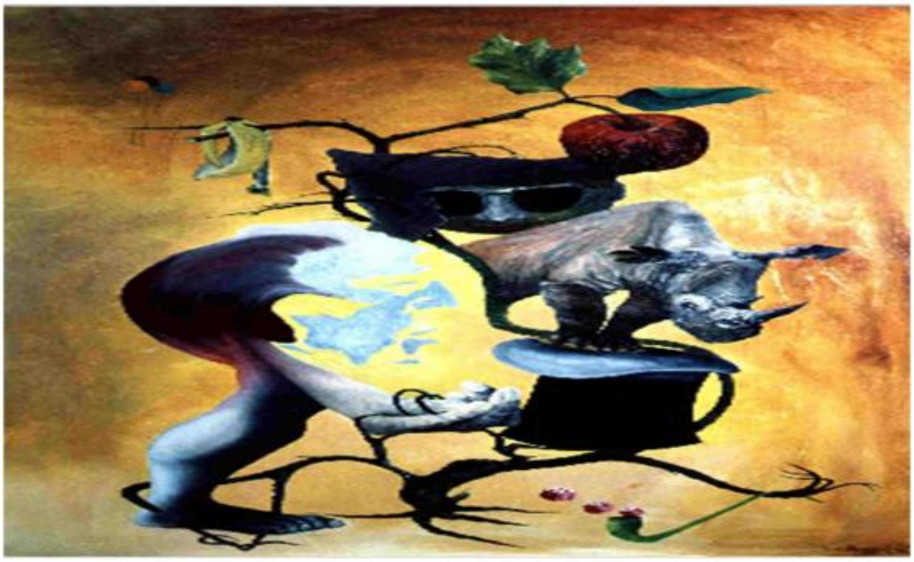
4 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
f0106320.gif			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11407	Unallocated	Unallocated	unknown	/img_RHIN
f0106344.gif	▽		1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4105	Unallocated	Unallocated	unknown	/img_RHIN
f0106320.gif			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11407	Unallocated	Unallocated	unknown	/img_RHIN
f0106344.gif	▽		1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4105	Unallocated	Unallocated	unknown	/img_RHIN

Rhino1.jpg

Rhino3.jpg

Rhino4.jpg



Rhino5.gif