Work by: Mohit Ajaykumar Dhabuwala
Course: CYFI-720

Scenario:

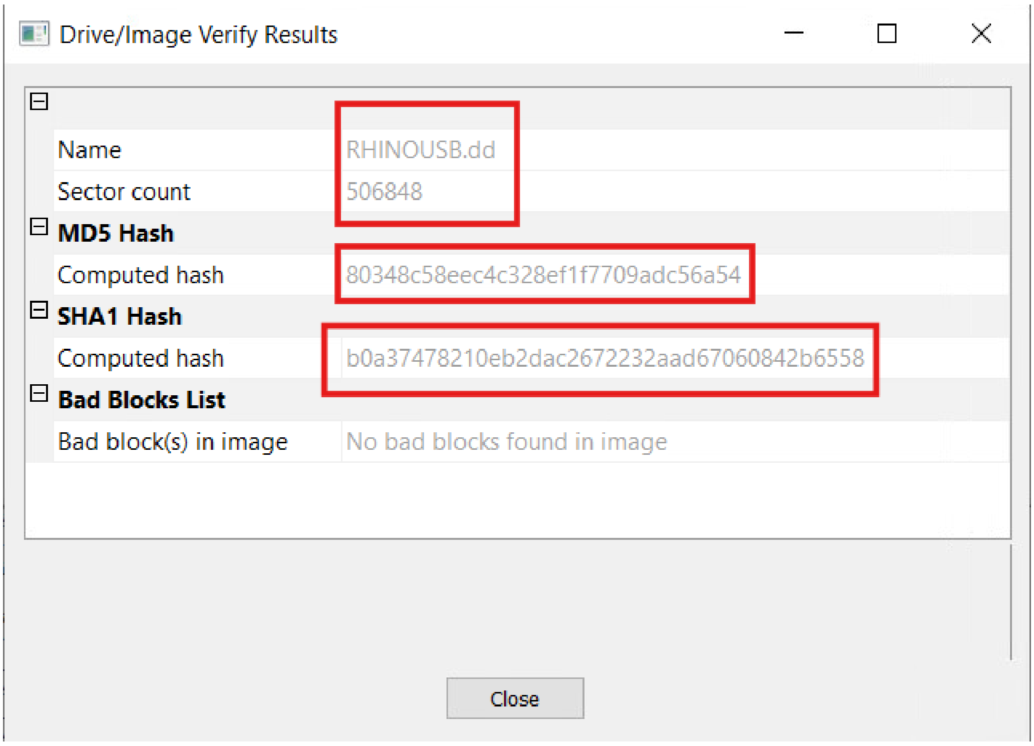
The city of New Orleans passed a law in 2004 making possession of nine or more unique rhinoceros images a serious crime. The network administrator at the University of New Orleans recently alerted police when his instance of RHINOVORE flagged illegal rhino traffic. Evidence in the case includes a computer 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

Start by verifying the hash value of the USB image(.dd file):



Name	RHINOUSB.dd
Sector count	506848
MD5 Hash	
Computed hash	80348c58eec4c328ef1f7709adc56a54
SHA1 Hash	
Computed hash	b0a37478210eb2dac2672232aad67060842b6558
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

The MD5 value is verified using FTK Imager and it has matched with the acquired hash value.

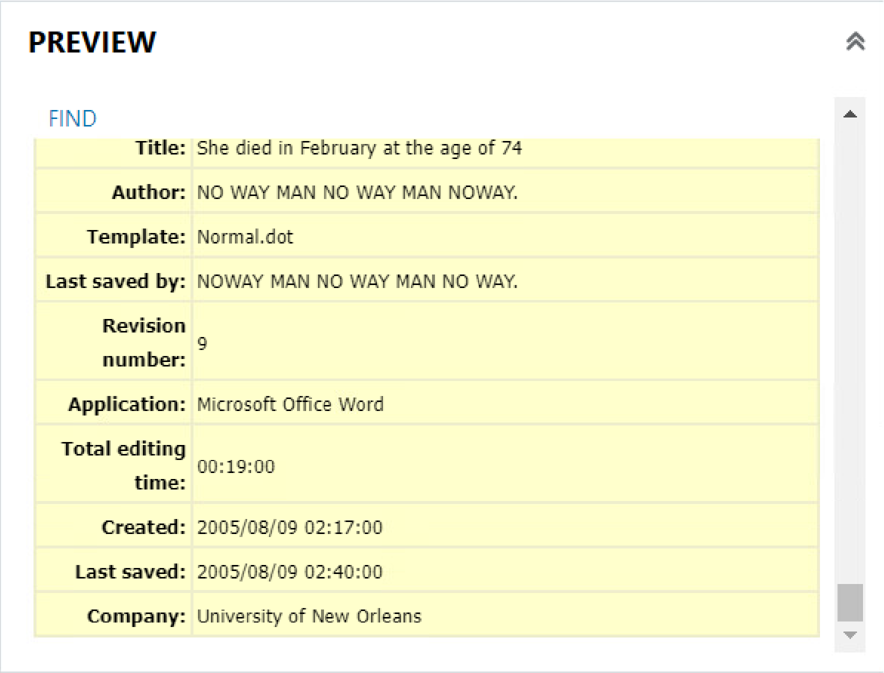
The task:

Recover at least nine rhino pictures from the available evidence and include them in a brief report. You must include at least one exhibit with your answers to the questions below. Demonstrate what worked and what did not work. In your report, provide answers to as many of the following questions as possible:

1. Who gave the accused a telnet/ftp account?

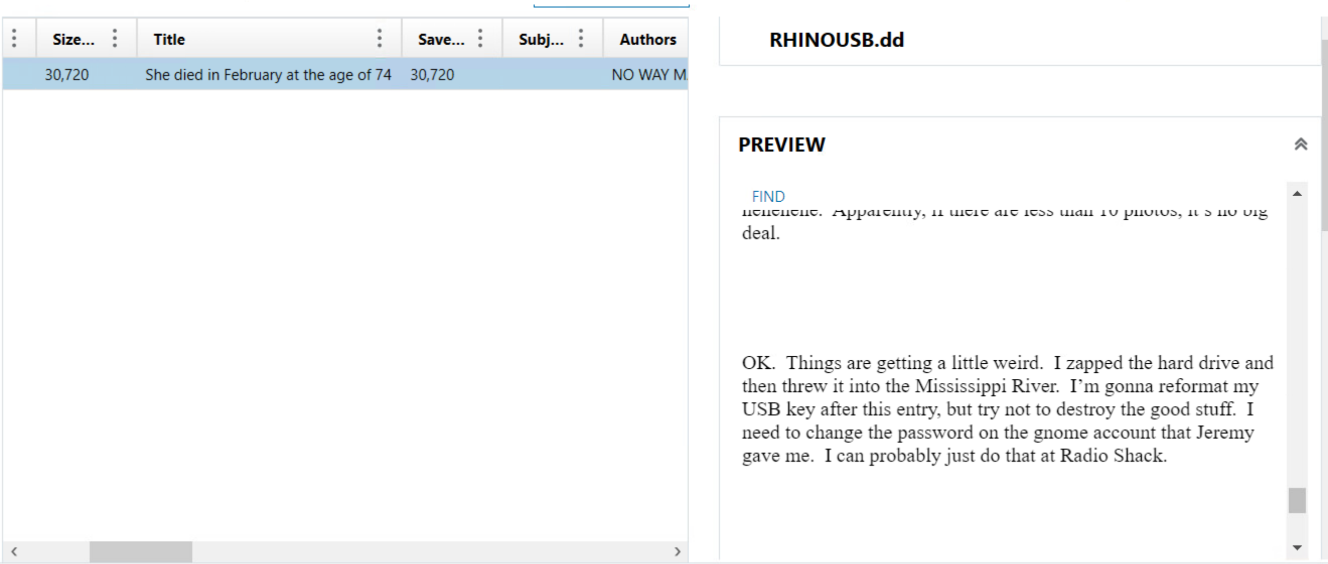
Answer: The account was given by “**Jeremy**”.

- **Location:** e3://Quiz-2_720/RHINOUSB/FAT/Partition::Free::Spaces/Partition::Free::Spaces::Detected/unallocated_blocks_0_999/unallocated_block_41813_9
- **Evidence:**



PREVIEW

Title:	She died in February at the age of 74
Author:	NO WAY MAN NO WAY MAN NOWAY.
Template:	Normal.dot
Last saved by:	NOWAY MAN NO WAY MAN NO WAY.
Revision number:	9
Application:	Microsoft Office Word
Total editing time:	00:19:00
Created:	2005/08/09 02:17:00
Last saved:	2005/08/09 02:40:00
Company:	University of New Orleans



Size...	Title	Save...	Subj...	Authors
30,720	She died in February at the age of 74	30,720		NO WAY M

RHINOUSB.dd

PREVIEW

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 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 Radio Shack.

This seems to be some sort of personal note or diary writing. I skim over this document looking for a lead. And I find it in the las two entries

Explanation: This piece of evidence shows that the suspect freaked out and got rid of the hard drive of the computer. This makes sense as the computer was found without a hard drive. Also, this leads point to the existence of more hidden pictures in the USB. The accused then formatted the USB drive, thinking that such action would erase the contents of the memory. The suspect also talks about changing the password of a "gnome account" that **Jeremy** gave him/her.

2. What's the username/password for the account?

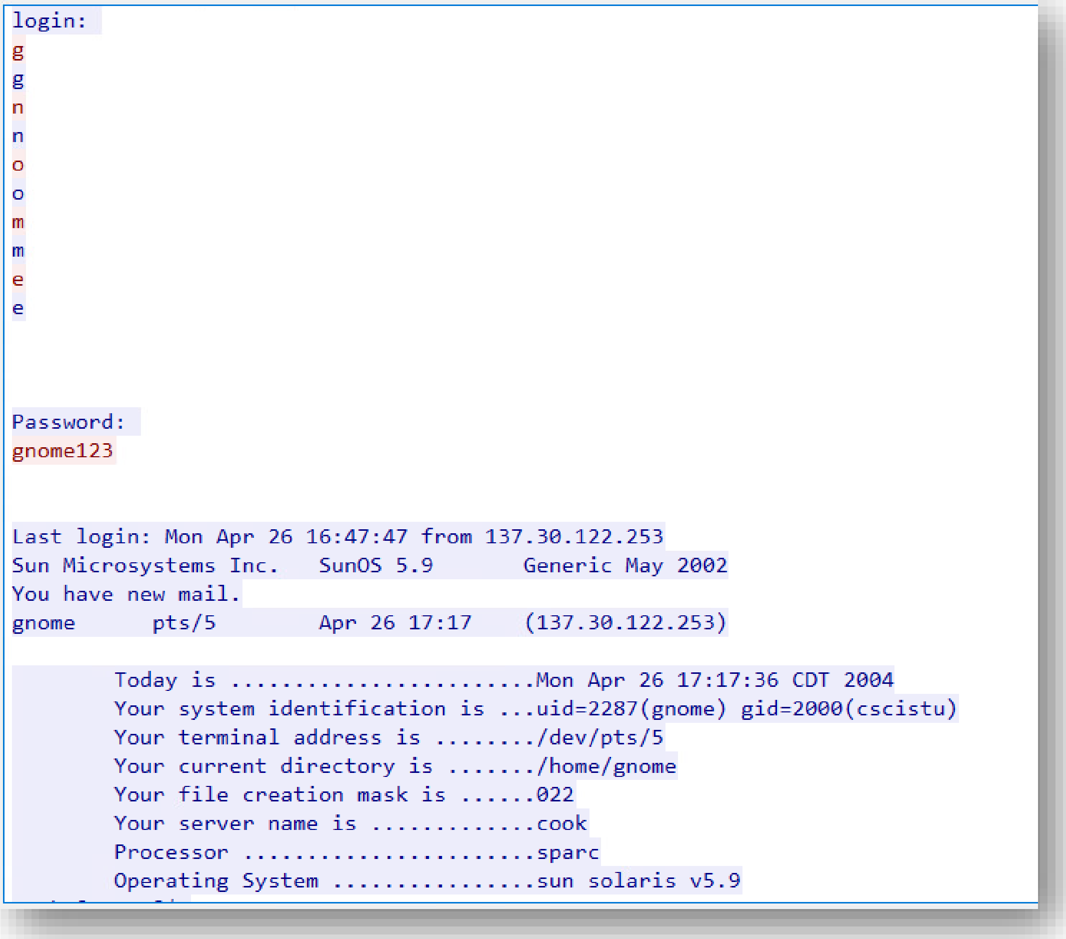
Answer: The username and password for the account:

Username	**Password**	**IP Address**	**MAC address**	**Device make**	**Last login**
Gnome	gnome123	137.30.122.253	00:03:93:cc:57:92	Apple	26th April at 16:47:47

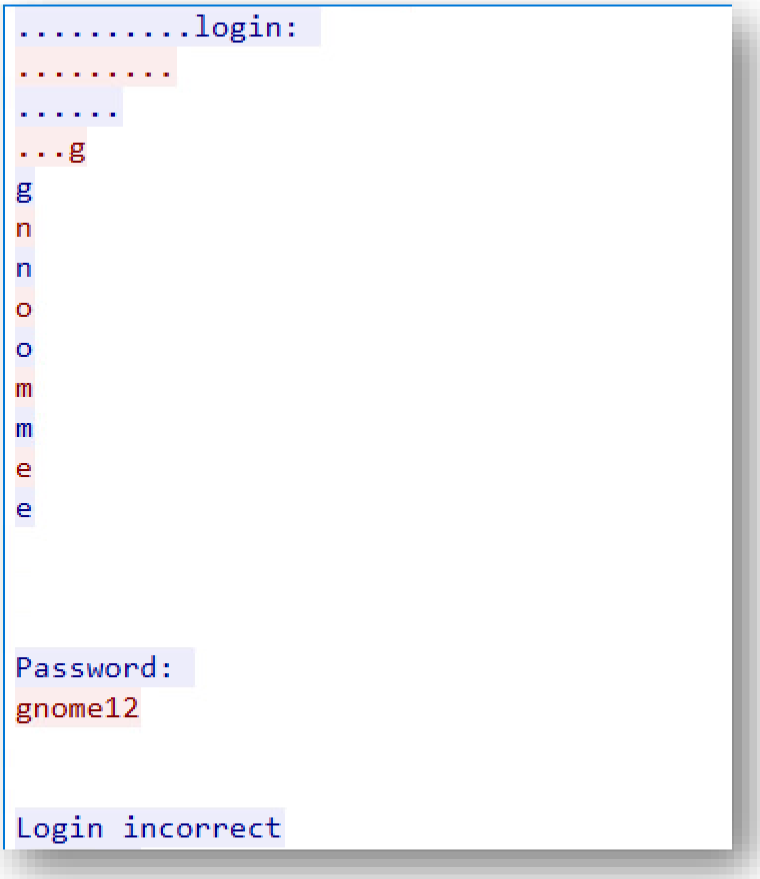
- **Location:** To locate the username and password within the network traffic, I applied a filter "telnet" in Wireshark within the **rhino.log** file to isolate only the Telnet packets. This allowed for a focused examination of the relevant data stream, revealing the login credentials within the Telnet packets ranging from number "1203 to 1247".
- **Explanation:** Telnet is an older, character-oriented protocol. This means it sends data one character at a time, rather than in larger blocks like more modern protocols. So, when I initially examined the Telnet packets, I saw each character of the username and password in separate packets.

However, by using Wireshark's "**Follow TCP Stream**" feature, you were able to reconstruct the entire Telnet conversation and extract the complete username and password from the reassembled stream.

- **Evidence**:



```
login:
g
g
n
n
o
o
m
m
e
e



Password:
gnome123


Last login: Mon Apr 26 16:47:47 from 137.30.122.253
Sun Microsystems Inc.   SunOS 5.9       Generic May 2002
You have new mail.
gnome       pts/5        Apr 26 17:17    (137.30.122.253)

        Today is .......................Mon Apr 26 17:17:36 CDT 2004
        Your system identification is ...uid=2287(gnome) gid=2000(cscistu)
        Your terminal address is ......../dev/pts/5
        Your current directory is ......./home/gnome
        Your file creation mask is ......022
        Your server name is ............cook
        Processor .......................sparc
        Operating System ................sun solaris v5.9
```



```
..........login:
.........
......
...g
g
n
n
o
o
m
m
e
e



Password:
gnome12


Login incorrect
```

This is the first attempt the user made to login into the account but failed due to incorrect password.

3. What relevant file transfers appear in the network traces?

Answer: The following relevant files were transferred over the network by the user whose traces are available in the 3 network capture logs(rhino.log, rhino2.log and rhino3.log):

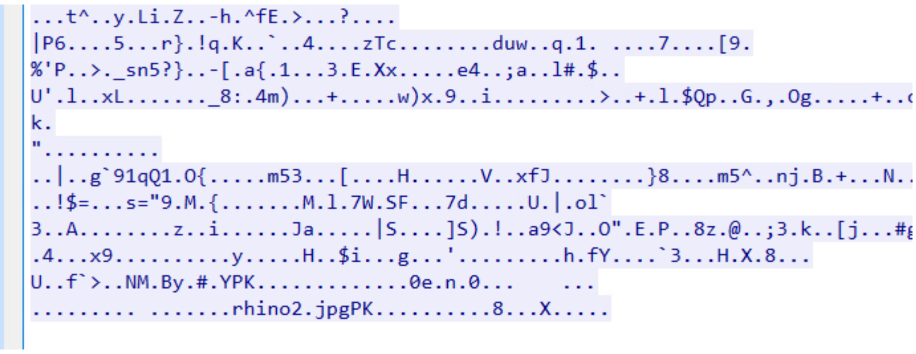
- **rhino1.jpg and rhino3.jpg (from 'rhino.log'):**These JPEG images were uploaded by the user "gnome" via FTP shortly after a Telnet session. This suggests a potential connection between the Telnet session and the transfer of these images.

- **contraband.zip (from 'rhino.log'):** This password-protected ZIP file was also uploaded via FTP right before a second Telnet session. It contains a single encrypted file named `rhino2.jpg`. The password for this ZIP file is "monkey." The timing of this transfer, near the Telnet sessions, raises suspicion about its contents and purpose.

- **rhino4.jpg and rhino5.gif (from 'rhino2.log'):** These image files were transferred via HTTP from a machine with the hostname `www.cs.uno.edu` to a machine with IP address `137.30.123.234`. The images were located in a directory associated with the user "gnome" (`/~gnome`). This suggests that the user "gnome" might have a connection to this remote machine and might be involved in sharing or distributing these images.

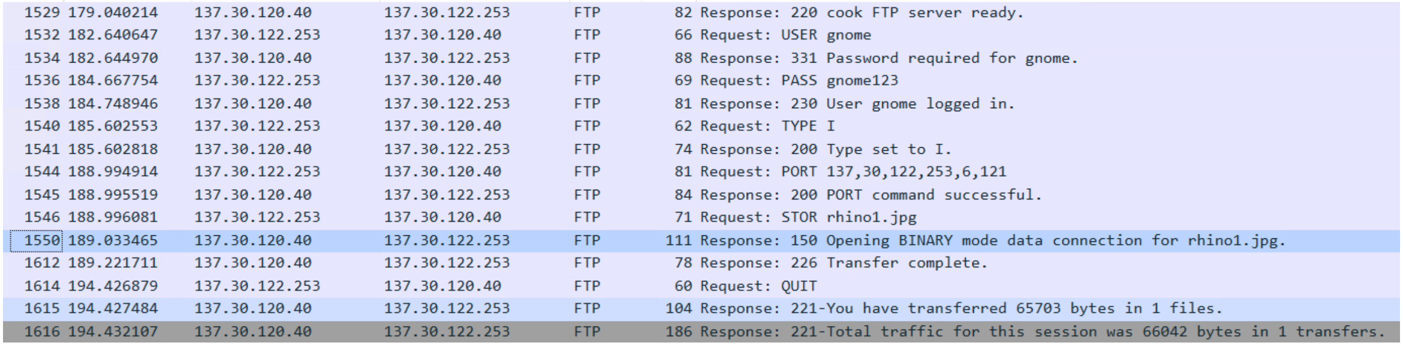
- **rhino.exe (from 'rhino3.log'):** This executable file was downloaded via HTTP from the same machine (`www.cs.uno.edu`) to the same IP address (`137.30.123.234`). It is suspected to be an early version of the MS DISKPART utility, which is used for disk partitioning and manipulation. This raises concerns about the user's potential intentions to modify or manipulate disk partitions, possibly for hiding or obscuring data.

- ➢ Rhino2.jpg found within the contraband.zip file



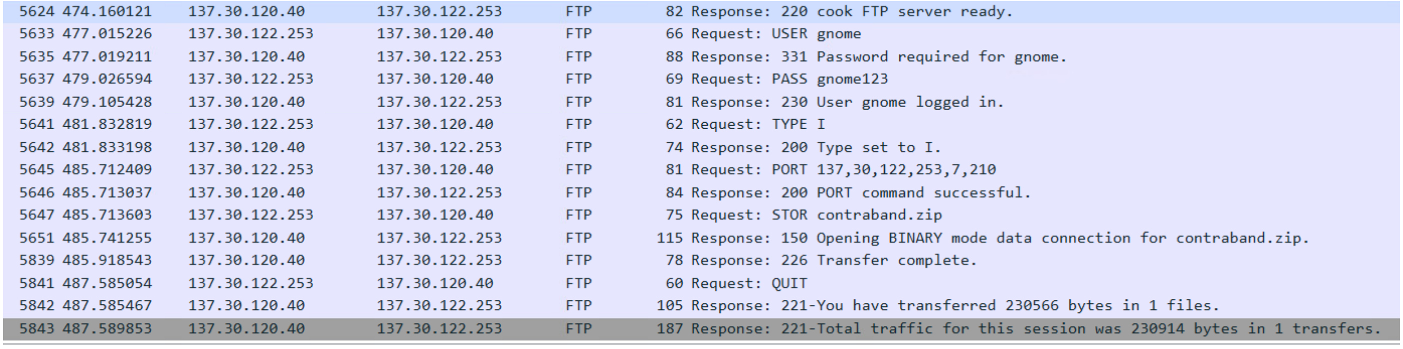
```
...t^..y.Li.Z..-h.^fE.>...?....
|P6....5...r}.!q.K..`..4....zTc........duw..q.1. ....7....[9.
%'P..>._sn5?}..-[.a{.1...3.E.Xx.....e4..;a..l#.$..
U'.l..xL......_8:.4m)...+.....w)x.9..i.........>..+.l.$Qp..G.,.Og.....+..
k.
".........
..|..g`91qQ1.O{.....m53...[....H......V..xfJ........}8....m5^..nj.B.+...N..
..!$=...s="9.M.{.......M.l.7W.SF...7d.....U.|.ol`
3..A........z..i......Ja.....|S....]S).!..a9<J..O".E.P..8z.@..;3.k..[j...#
.4...x9.........y.....H..$i...g...'.........h.fY....`3...H.X.8...
U..f`>..NM.By.#.YPK............0e.n.0...    ...
.........  .......rhino2.jpgPK..........8...X.....
```

- ➢ Rhino1.jpg



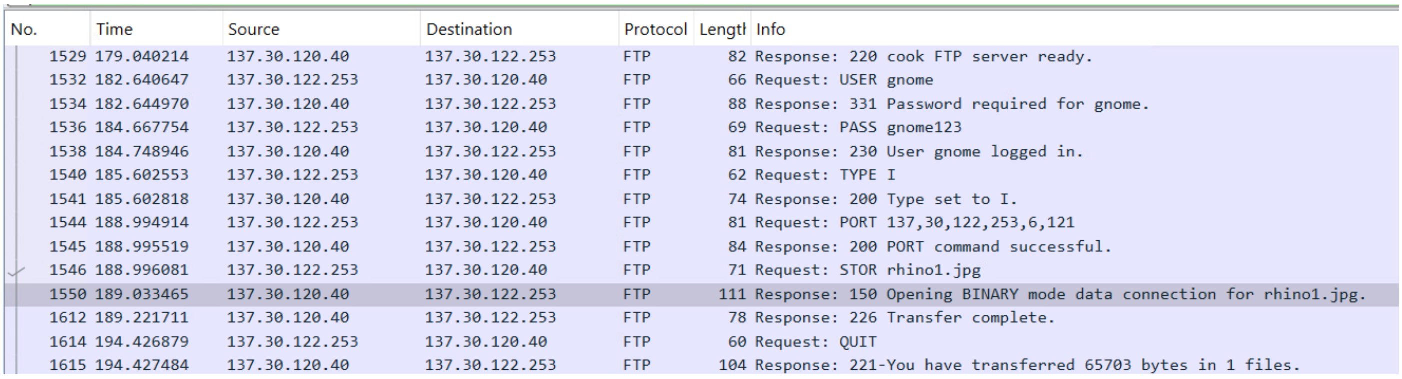
```
1529 179.040214   137.30.120.40    137.30.122.253   FTP    82 Response: 220 cook FTP server ready.
1532 182.640647   137.30.122.253   137.30.120.40    FTP    66 Request: USER gnome
1534 182.644970   137.30.120.40    137.30.122.253   FTP    88 Response: 331 Password required for gnome.
1536 184.667754   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.
```

- ➢ Contraband.zip



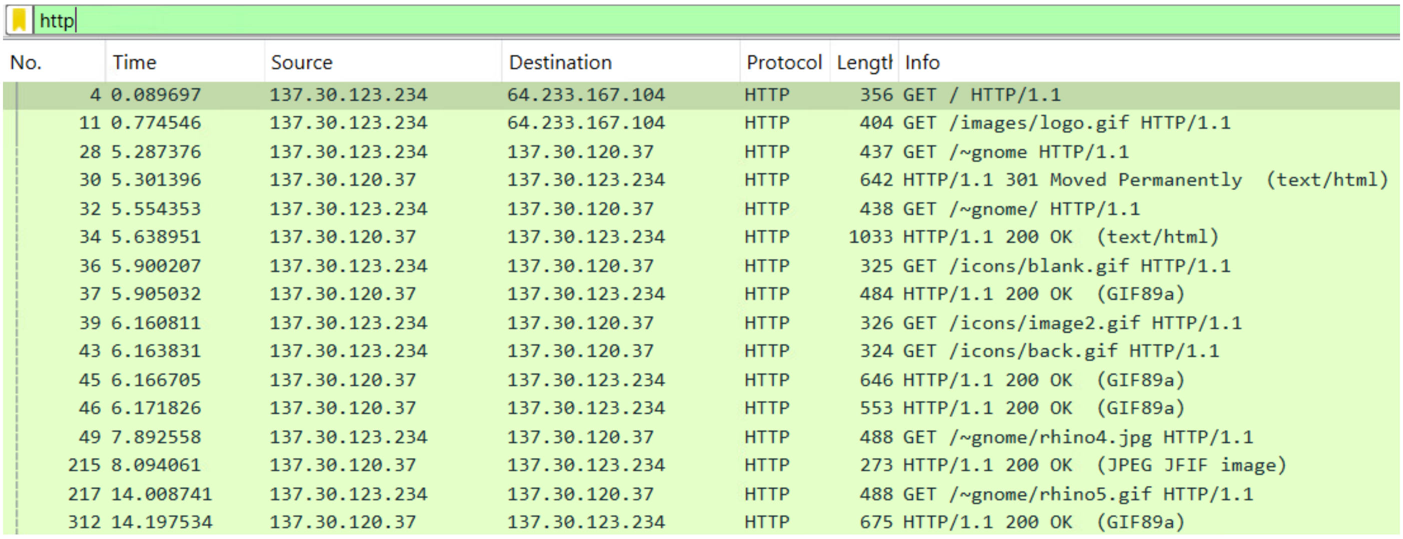
```
5624 474.160121   137.30.120.40    137.30.122.253   FTP    82 Response: 220 cook FTP server ready.
5633 477.015226   137.30.122.253   137.30.120.40    FTP    66 Request: USER gnome
5635 477.019211   137.30.120.40    137.30.122.253   FTP    88 Response: 331 Password required for gnome.
5637 479.026594   137.30.122.253   137.30.120.40    FTP    69 Request: PASS gnome123
5639 479.105428   137.30.120.40    137.30.122.253   FTP    81 Response: 230 User gnome logged in.
5641 481.832819   137.30.122.253   137.30.120.40    FTP    62 Request: TYPE I
5642 481.833198   137.30.120.40    137.30.122.253   FTP    74 Response: 200 Type set to I.
5645 485.712409   137.30.122.253   137.30.120.40    FTP    81 Request: PORT 137,30,122,253,7,210
5646 485.713037   137.30.120.40    137.30.122.253   FTP    84 Response: 200 PORT command successful.
5647 485.713603   137.30.122.253   137.30.120.40    FTP    75 Request: STOR contraband.zip
5651 485.741255   137.30.120.40    137.30.122.253   FTP   115 Response: 150 Opening BINARY mode data connection for contraband.zip.
5839 485.918543   137.30.120.40    137.30.122.253   FTP    78 Response: 226 Transfer complete.
5841 487.585054   137.30.122.253   137.30.120.40    FTP    60 Request: QUIT
5842 487.585467   137.30.120.40    137.30.122.253   FTP   105 Response: 221-You have transferred 230566 bytes in 1 files.
5843 487.589853   137.30.120.40    137.30.122.253   FTP   187 Response: 221-Total traffic for this session was 230914 bytes in 1 transfers.
```

- ➢ Rhino1.jpg:



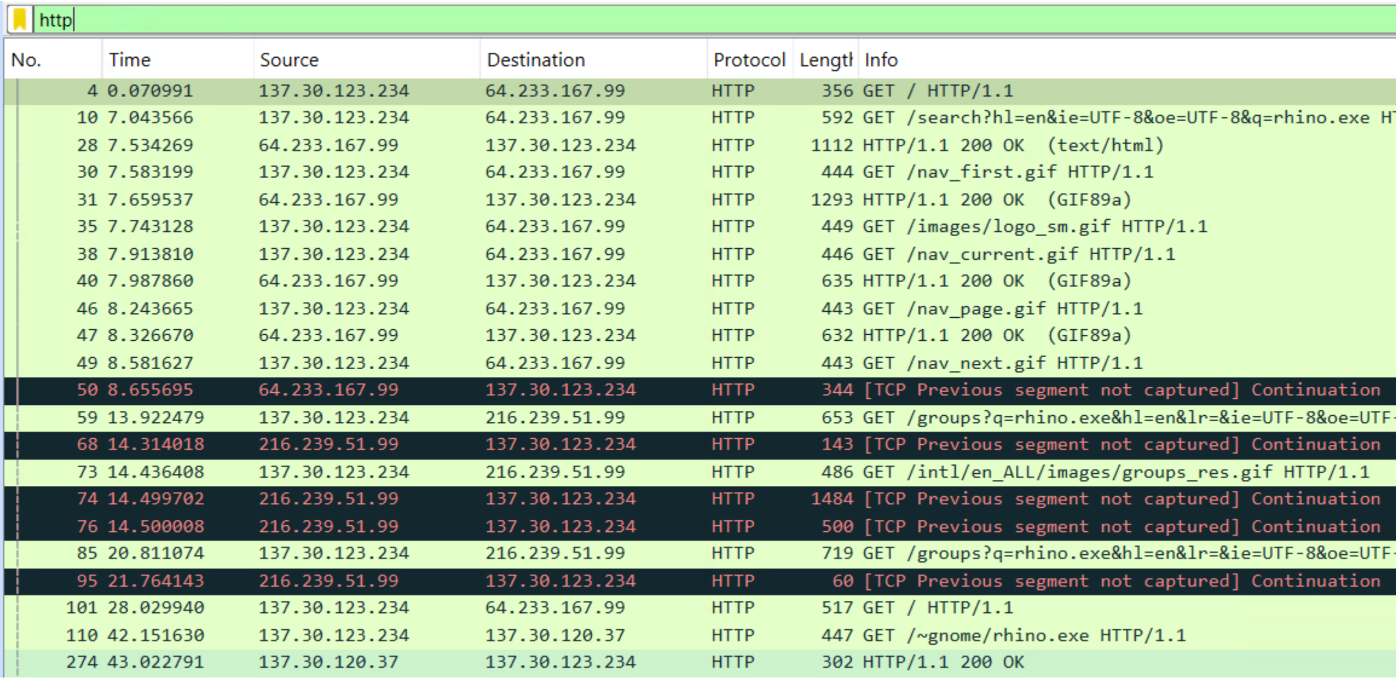
```
No.     Time         Source           Destination      Protocol Lengtl Info
   1529 179.040214   137.30.120.40    137.30.122.253   FTP       82 Response: 220 cook FTP server ready.
   1532 182.640647   137.30.122.253   137.30.120.40    FTP       66 Request: USER gnome
   1534 182.644970   137.30.120.40    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.
```

- Rhino4.jpg and Rhino5.jpg:

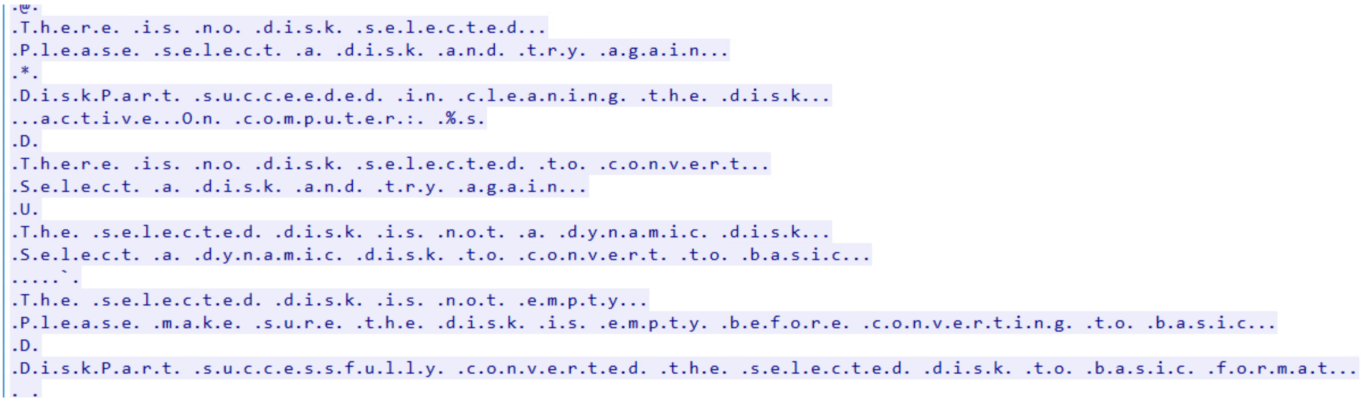


```
http
No.    Time        Source           Destination      Protocol  Lengtl  Info
     4 0.089697    137.30.123.234   64.233.167.104   HTTP        356 GET / HTTP/1.1
    11 0.774546    137.30.123.234   64.233.167.104   HTTP        404 GET /images/logo.gif HTTP/1.1
    28 5.287376    137.30.123.234   137.30.120.37    HTTP        437 GET /~gnome HTTP/1.1
    30 5.301396    137.30.120.37    137.30.123.234   HTTP        642 HTTP/1.1 301 Moved Permanently  (text/html)
    32 5.554353    137.30.123.234   137.30.120.37    HTTP        438 GET /~gnome/ HTTP/1.1
    34 5.638951    137.30.120.37    137.30.123.234   HTTP       1033 HTTP/1.1 200 OK  (text/html)
    36 5.900207    137.30.123.234   137.30.120.37    HTTP        325 GET /icons/blank.gif HTTP/1.1
    37 5.905032    137.30.120.37    137.30.123.234   HTTP        484 HTTP/1.1 200 OK  (GIF89a)
    39 6.160811    137.30.123.234   137.30.120.37    HTTP        326 GET /icons/image2.gif HTTP/1.1
    43 6.163831    137.30.123.234   137.30.120.37    HTTP        324 GET /icons/back.gif HTTP/1.1
    45 6.166705    137.30.120.37    137.30.123.234   HTTP        646 HTTP/1.1 200 OK  (GIF89a)
    46 6.171826    137.30.120.37    137.30.123.234   HTTP        553 HTTP/1.1 200 OK  (GIF89a)
    49 7.892558    137.30.123.234   137.30.120.37    HTTP        488 GET /~gnome/rhino4.jpg HTTP/1.1
   215 8.094061    137.30.120.37    137.30.123.234   HTTP        273 HTTP/1.1 200 OK  (JPEG JFIF image)
   217 14.008741   137.30.123.234   137.30.120.37    HTTP        488 GET /~gnome/rhino5.gif HTTP/1.1
   312 14.197534   137.30.120.37    137.30.123.234   HTTP        675 HTTP/1.1 200 OK  (GIF89a)
```

- Rhino.exe:



```
http
No.    Time        Source           Destination      Protocol  Lengtl  Info
     4 0.070991    137.30.123.234   64.233.167.99    HTTP        356 GET / HTTP/1.1
    10 7.043566    137.30.123.234   64.233.167.99    HTTP        592 GET /search?hl=en&ie=UTF-8&oe=UTF-8&q=rhino.exe H
    28 7.534269    64.233.167.99    137.30.123.234   HTTP       1112 HTTP/1.1 200 OK  (text/html)
    30 7.583199    137.30.123.234   64.233.167.99    HTTP        444 GET /nav_first.gif HTTP/1.1
    31 7.659537    64.233.167.99    137.30.123.234   HTTP       1293 HTTP/1.1 200 OK  (GIF89a)
    35 7.743128    137.30.123.234   64.233.167.99    HTTP        449 GET /images/logo_sm.gif HTTP/1.1
    38 7.913810    137.30.123.234   64.233.167.99    HTTP        446 GET /nav_current.gif HTTP/1.1
    40 7.987860    64.233.167.99    137.30.123.234   HTTP        635 HTTP/1.1 200 OK  (GIF89a)
    46 8.243665    137.30.123.234   64.233.167.99    HTTP        443 GET /nav_page.gif HTTP/1.1
    47 8.326670    64.233.167.99    137.30.123.234   HTTP        632 HTTP/1.1 200 OK  (GIF89a)
    49 8.581627    137.30.123.234   64.233.167.99    HTTP        443 GET /nav_next.gif HTTP/1.1
    50 8.655695    64.233.167.99    137.30.123.234   HTTP        344 [TCP Previous segment not captured] Continuation
    59 13.922479   137.30.123.234   216.239.51.99    HTTP        653 GET /groups?q=rhino.exe&hl=en&lr=&ie=UTF-8&oe=UTF
    68 14.314018   216.239.51.99    137.30.123.234   HTTP        143 [TCP Previous segment not captured] Continuation
    73 14.436408   137.30.123.234   216.239.51.99    HTTP        486 GET /intl/en_ALL/images/groups_res.gif HTTP/1.1
    74 14.499702   216.239.51.99    137.30.123.234   HTTP       1484 [TCP Previous segment not captured] Continuation
    76 14.500008   216.239.51.99    137.30.123.234   HTTP        500 [TCP Previous segment not captured] Continuation
    85 20.811074   137.30.123.234   216.239.51.99    HTTP        719 GET /groups?q=rhino.exe&hl=en&lr=&ie=UTF-8&oe=UTF
    95 21.764143   216.239.51.99    137.30.123.234   HTTP         60 [TCP Previous segment not captured] Continuation
   101 28.029940   137.30.123.234   64.233.167.99    HTTP        517 GET / HTTP/1.1
   110 42.151630   137.30.123.234   137.30.120.37    HTTP        447 GET /~gnome/rhino.exe HTTP/1.1
   274 43.022791   137.30.120.37    137.30.123.234   HTTP        302 HTTP/1.1 200 OK
```

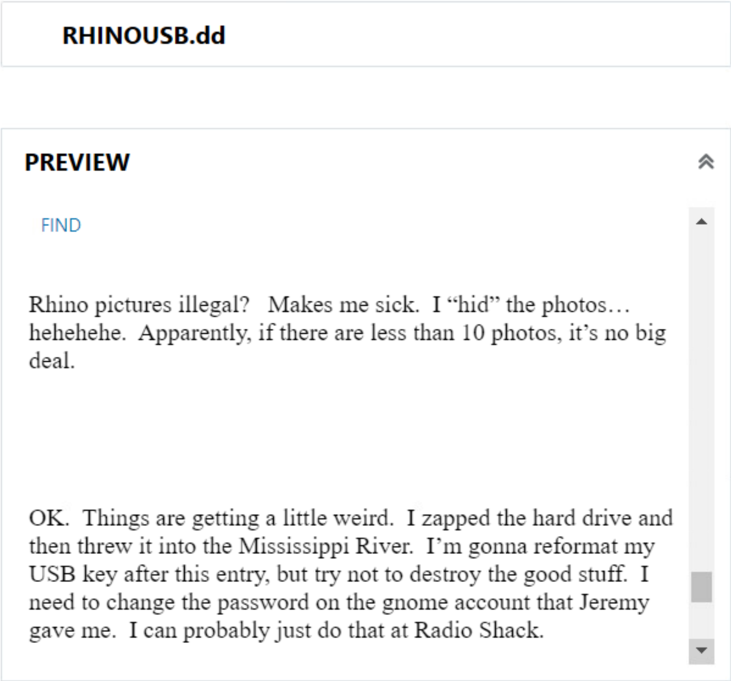


```
.@.
.T.h.e.r.e. .i.s. .n.o. .d.i.s.k. .s.e.l.e.c.t.e.d...
.P.l.e.a.s.e. .s.e.l.e.c.t. .a. .d.i.s.k. .a.n.d. .t.r.y. .a.g.a.i.n...
.*.
.D.i.s.k.P.a.r.t. .s.u.c.c.e.e.d.e.d. .i.n. .c.l.e.a.n.i.n.g. .t.h.e. .d.i.s.k...
...a.c.t.i.v.e...O.n. .c.o.m.p.u.t.e.r.:. .%.s.
.D.
.T.h.e.r.e. .i.s. .n.o. .d.i.s.k. .s.e.l.e.c.t.e.d. .t.o. .c.o.n.v.e.r.t...
.S.e.l.e.c.t. .a. .d.i.s.k. .a.n.d. .t.r.y. .a.g.a.i.n...
.U.
.T.h.e. .s.e.l.e.c.t.e.d. .d.i.s.k. .i.s. .n.o.t. .a. .d.y.n.a.m.i.c. .d.i.s.k...
.S.e.l.e.c.t. .a. .d.y.n.a.m.i.c. .d.i.s.k. .t.o. .c.o.n.v.e.r.t. .t.o. .b.a.s.i.c...
.....`.
.T.h.e. .s.e.l.e.c.t.e.d. .d.i.s.k. .i.s. .n.o.t. .e.m.p.t.y...
.P.l.e.a.s.e. .m.a.k.e. .s.u.r.e. .t.h.e. .d.i.s.k. .i.s. .e.m.p.t.y. .b.e.f.o.r.e. .c.o.n.v.e.r.t.i.n.g. .t.o. .b.a.s.i.c...
.D.
.D.i.s.k.P.a.r.t. .s.u.c.c.e.s.s.f.u.l.l.y. .c.o.n.v.e.r.t.e.d. .t.h.e. .s.e.l.e.c.t.e.d. .d.i.s.k. .t.o. .b.a.s.i.c. .f.o.r.m.a.t...
. .
```

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

Answer: The hard drive is zapped and thrown into the Mississippi River.

- **Location:** e3://Quiz-2_720/RHINOUSB/FAT/Partition::Free::Spaces/Partition::Free::Spaces::Detected/unallocated_blocks_0_999/unallocated_block_41813_9
- **Evidence**:



RHINOUSB.dd

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 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 Radio Shack.

- **Explanation:** This evidence can be inferred from the last two lines of .doc file carved from the acquired USB drive. The lines written in the doc file:" OK. *Things are getting a little weird. I zapped the hard drive and then threw it into the Mississippi River.*"

5. What happened to the USB key?

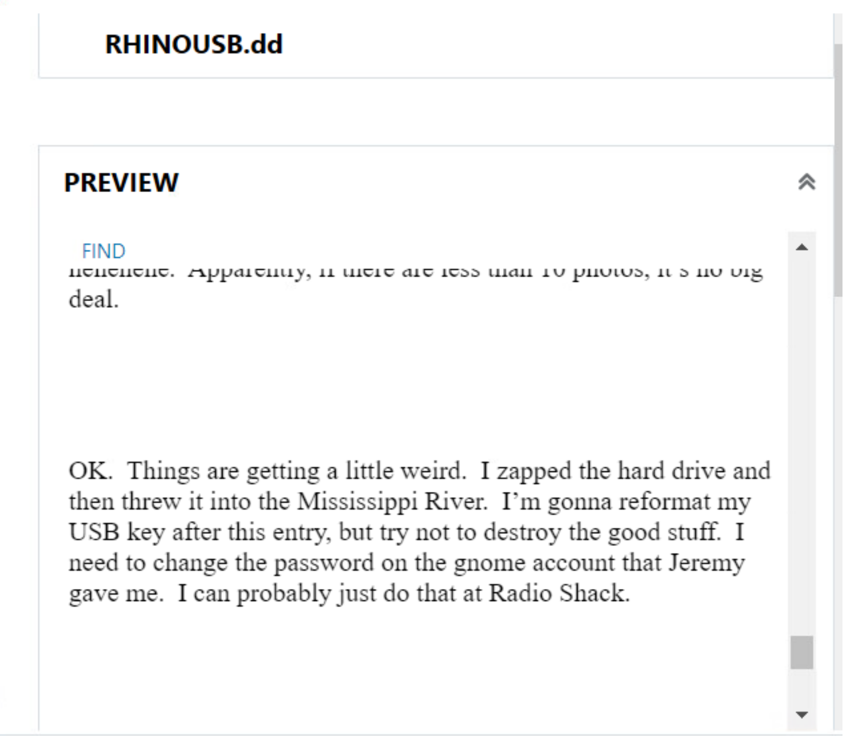
Answer: The suspect Suspect reformatted the USB key hoping not to overwrite the "good" stuff. The suspect also mentioned the location where he/she intended to overwrite the drive --- possibly at Radio Shack.

- **Location**: e3://Quiz-2_720/RHINOUSB/FAT/Partition::Free::Spaces/Partition::Free::Spaces::Detected/unallocated_blocks_0_999/unallocated_block_41813_9
- **Explanation:** This evidence can be inferred from the last two lines of .doc file carved from the acquired USB drive. The lines written in the doc file "*I'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 Radio Shack."

- ○ During the analysis, I found out that the USB key had only two allocated files. gumbo1.txt and gumbo2.txt and a huge portion of the file is filled with the same bytes over and over. Thus, there is a possibility that part of the disk has been manually overwritten with the message "SORRY and CHARLIE".

➢ **Evidence:**



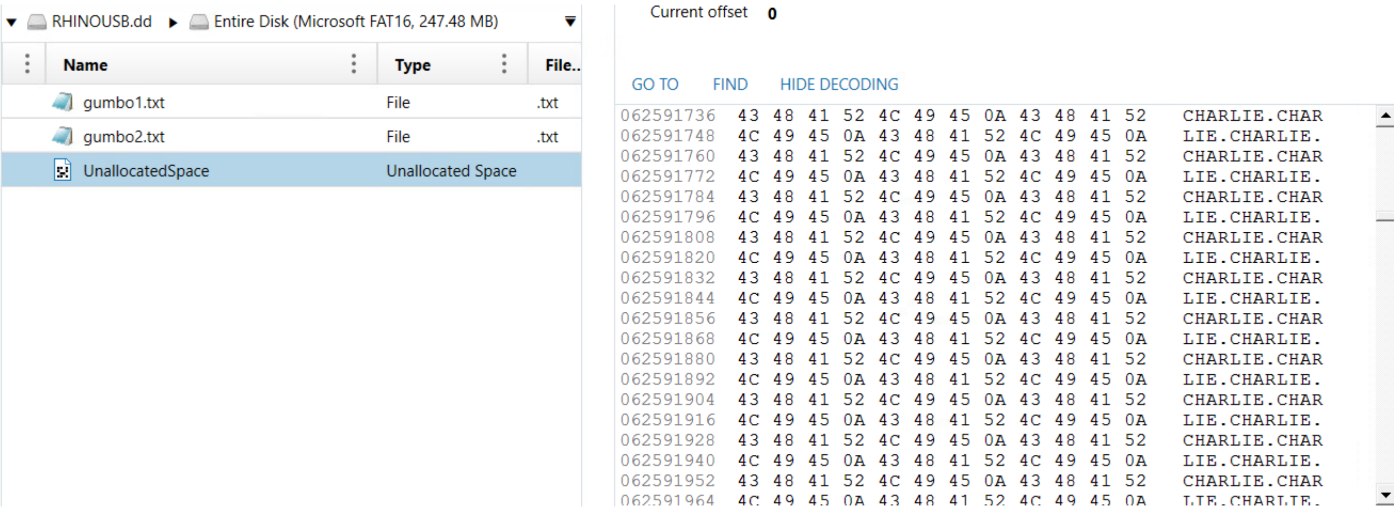
RHINOUSB.dd

PREVIEW

FIND

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 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 Radio Shack.



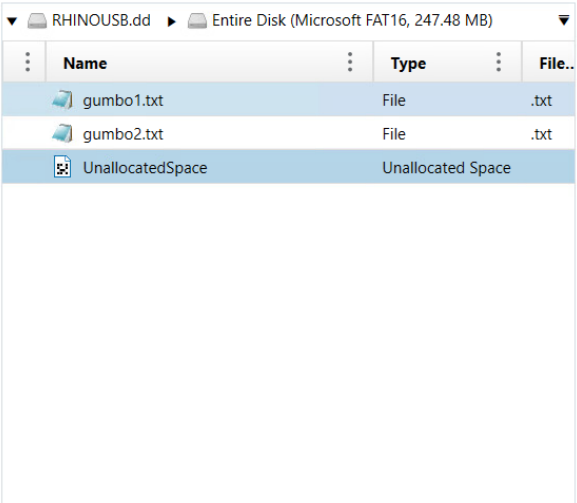
RHINOUSB.dd ▸ Entire Disk (Microsoft FAT16, 247.48 MB)

Name	Type	File..
gumbo1.txt	File	.txt
gumbo2.txt	File	.txt
UnallocatedSpace	Unallocated Space	

Current offset 0

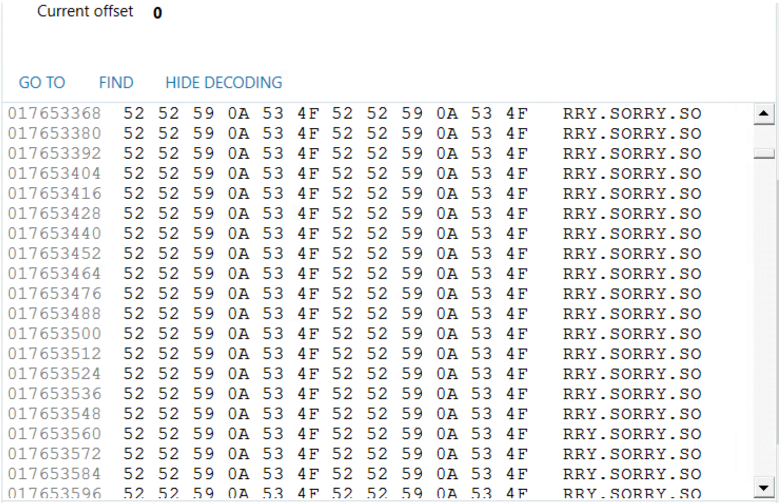
GO TO FIND HIDE DECODING

```
062591736  43 48 41 52 4C 49 45 0A 43 48 41 52   CHARLIE.CHAR
062591748  4C 49 45 0A 43 48 41 52 4C 49 45 0A   LIE.CHARLIE.
062591760  43 48 41 52 4C 49 45 0A 43 48 41 52   CHARLIE.CHAR
062591772  4C 49 45 0A 43 48 41 52 4C 49 45 0A   LIE.CHARLIE.
062591784  43 48 41 52 4C 49 45 0A 43 48 41 52   CHARLIE.CHAR
062591796  4C 49 45 0A 43 48 41 52 4C 49 45 0A   LIE.CHARLIE.
062591808  43 48 41 52 4C 49 45 0A 43 48 41 52   CHARLIE.CHAR
062591820  4C 49 45 0A 43 48 41 52 4C 49 45 0A   LIE.CHARLIE.
062591832  43 48 41 52 4C 49 45 0A 43 48 41 52   CHARLIE.CHAR
062591844  4C 49 45 0A 43 48 41 52 4C 49 45 0A   LIE.CHARLIE.
062591856  43 48 41 52 4C 49 45 0A 43 48 41 52   CHARLIE.CHAR
062591868  4C 49 45 0A 43 48 41 52 4C 49 45 0A   LIE.CHARLIE.
062591880  43 48 41 52 4C 49 45 0A 43 48 41 52   CHARLIE.CHAR
062591892  4C 49 45 0A 43 48 41 52 4C 49 45 0A   LIE.CHARLIE.
062591904  43 48 41 52 4C 49 45 0A 43 48 41 52   CHARLIE.CHAR
062591916  4C 49 45 0A 43 48 41 52 4C 49 45 0A   LIE.CHARLIE.
062591928  43 48 41 52 4C 49 45 0A 43 48 41 52   CHARLIE.CHAR
062591940  4C 49 45 0A 43 48 41 52 4C 49 45 0A   LIE.CHARLIE.
062591952  43 48 41 52 4C 49 45 0A 43 48 41 52   CHARLIE.CHAR
062591964  4C 49 45 0A 43 48 41 52 4C 49 45 0A   LIE.CHARLIE.
```



RHINOUSB.dd ▸ Entire Disk (Microsoft FAT16, 247.48 MB)

Name	Type	File..
gumbo1.txt	File	.txt
gumbo2.txt	File	.txt
UnallocatedSpace	Unallocated Space	



Current offset 0

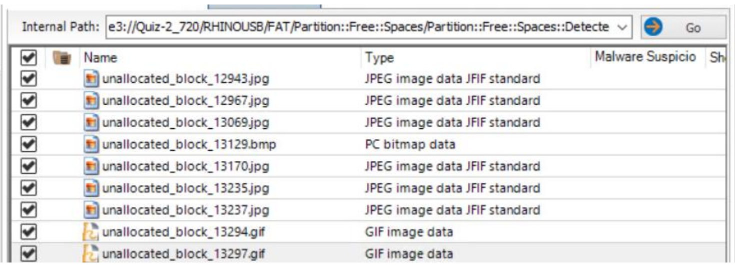
```
017653368  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653380  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653392  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653404  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653416  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653428  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653440  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653452  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653464  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653476  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653488  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653500  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653512  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653524  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653536  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653548  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653560  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653572  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653584  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
017653596  52 52 59 0A 53 4F 52 52 59 0A 53 4F   RRY.SORRY.SO
```

6. What is recoverable from the *dd* image of the USB key?

Answer: Based on the provided data, here's what was recoverable from the RHINOUSB.dd image of the USB key:

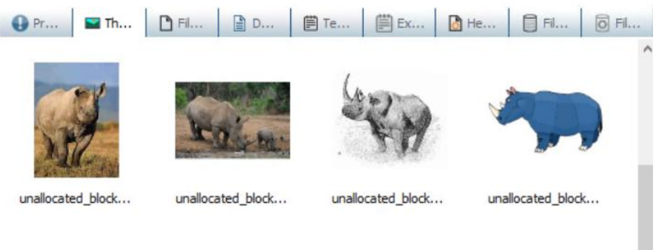
- **Undeleted Files:**
  - **gumbo1.txt and gumbo2.txt**: These text files, containing gumbo recipes, were directly recoverable as they were not deleted from the USB key.
- **Recovered Images (using Paraben):**
  - **rhino6.jpg**: Extracted from f0103704.jpg using steganography with the password "gumbo."
  - **rhino7.jpg**: Extracted from f0104520.jpg using steganography with the password "gator."
  - **rhino2.jpg, rhino8.gif, rhino9.gif, rhino10.jpg**: Directly recovered through file carving.
  - **alligator1.jpg, alligator5.jpg**: Carved from the drive but are irrelevant to the investigation.
- **Recovered Document:**
  - **she said in February at the age of 74.doc**: A Word document potentially containing answers or information relevant to the case.

➢ **Explanation:** The presence of rhinoceros images hidden within seemingly innocuous image files (alligator2.jpg and alligator3.jpg) using steganography, along with the directly recovered rhinoceroses' images and the potentially relevant Word document, suggests an attempt to conceal data on the USB key. The fact that the USB key was reformatted further supports this conclusion. However, the successful recovery of these files highlights the effectiveness of forensic tools and techniques, such as file carving and steganography analysis, in uncovering hidden or deleted data.

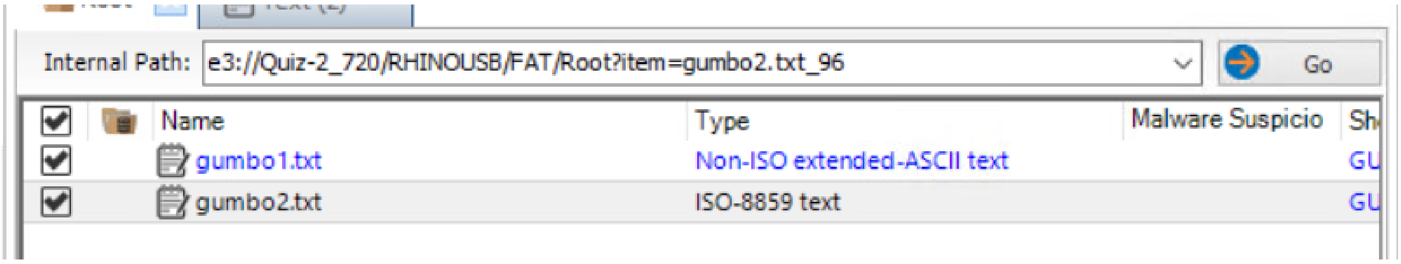


Internal Path: e3://Quiz-2_720/RHINOUSB/FAT/Partition::Free::Spaces/Partition::Free::Spaces::Detecte

☑	Name	Type	Malware Suspicio	Sh
☑	unallocated_block_12943.jpg	JPEG image data JFIF standard		
☑	unallocated_block_12967.jpg	JPEG image data JFIF standard		
☑	unallocated_block_13069.jpg	JPEG image data JFIF standard		
☑	unallocated_block_13129.bmp	PC bitmap data		
☑	unallocated_block_13170.jpg	JPEG image data JFIF standard		
☑	unallocated_block_13235.jpg	JPEG image data JFIF standard		
☑	unallocated_block_13237.jpg	JPEG image data JFIF standard		
☑	unallocated_block_13294.gif	GIF image data		
☑	unallocated_block_13297.gif	GIF image data		

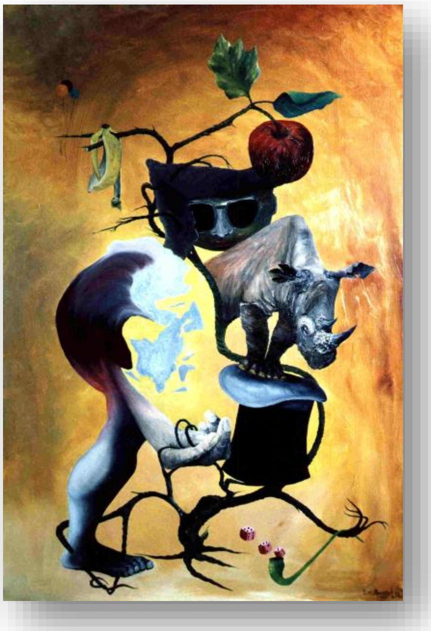


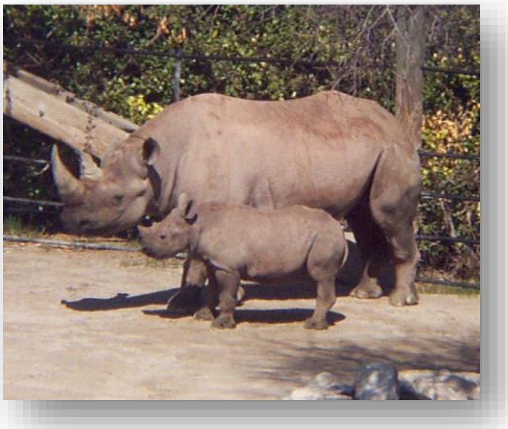
- **Evidence**:
  - **Path**: e3://Quiz-2_720/RHINOUSB/FAT/Root?item=gumbo2.txt_96

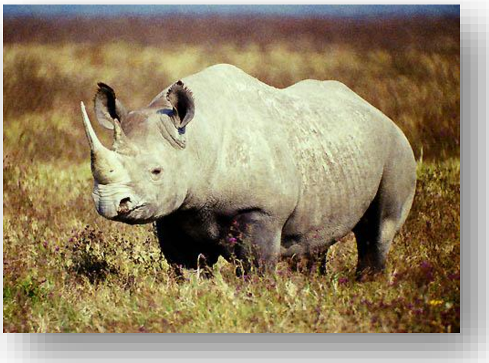


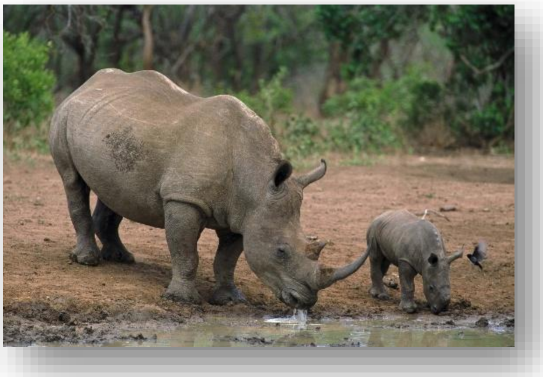
Internal Path: e3://Quiz-2_720/RHINOUSB/FAT/Root?item=gumbo2.txt_96 Go

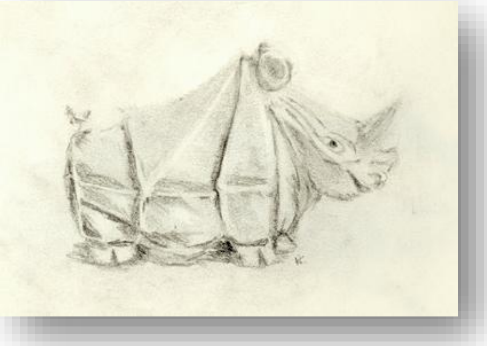
☑	Name	Type	Malware Suspicio	Sh
☑	gumbo1.txt	Non-ISO extended-ASCII text		GU
☑	gumbo2.txt	ISO-8859 text		GU

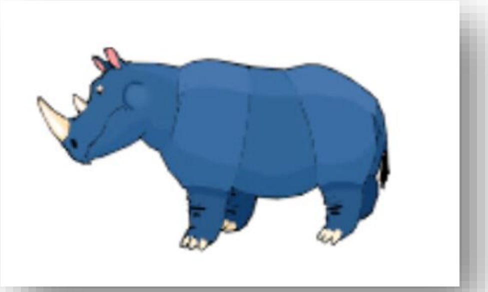


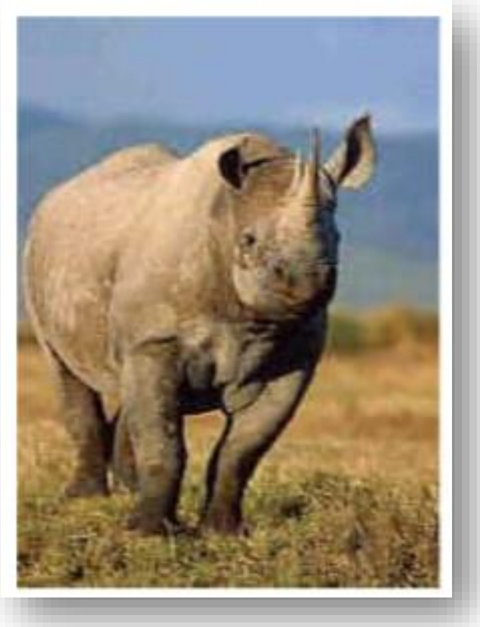


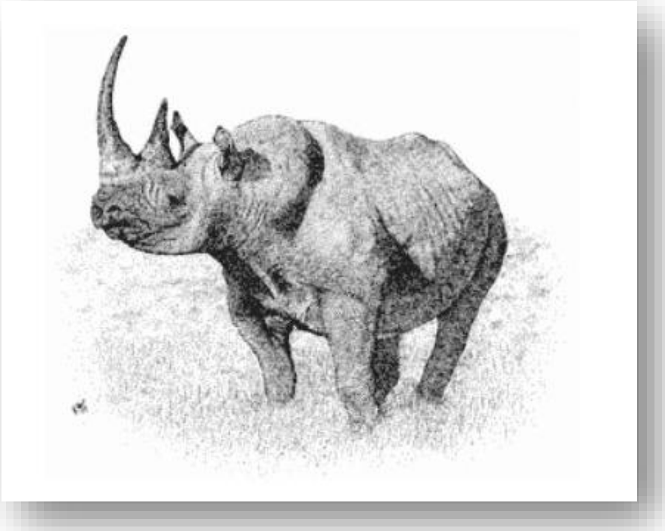


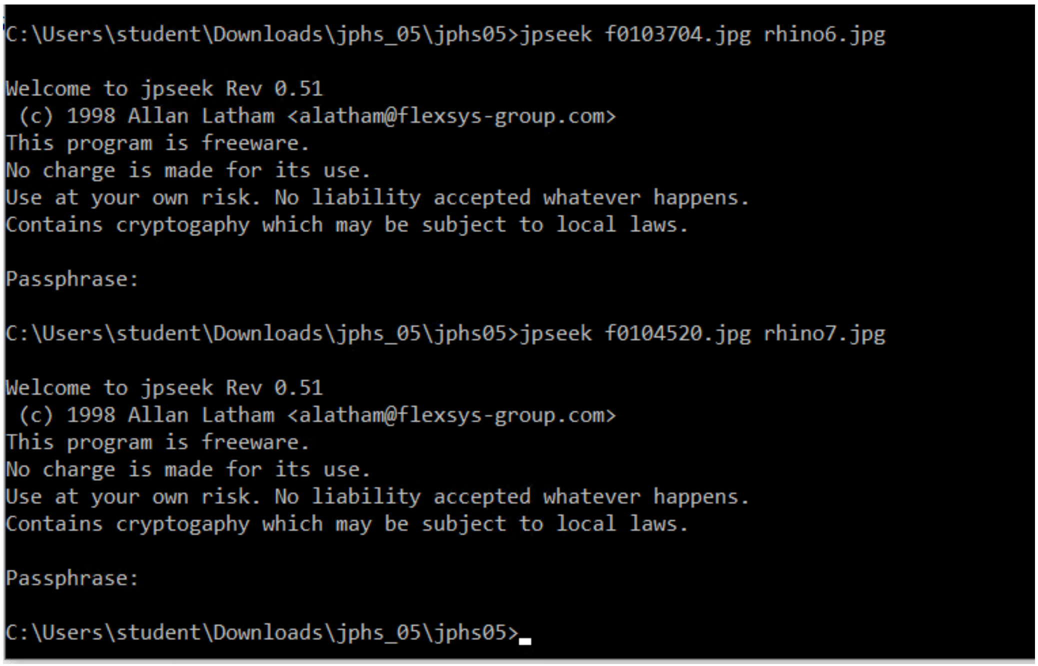




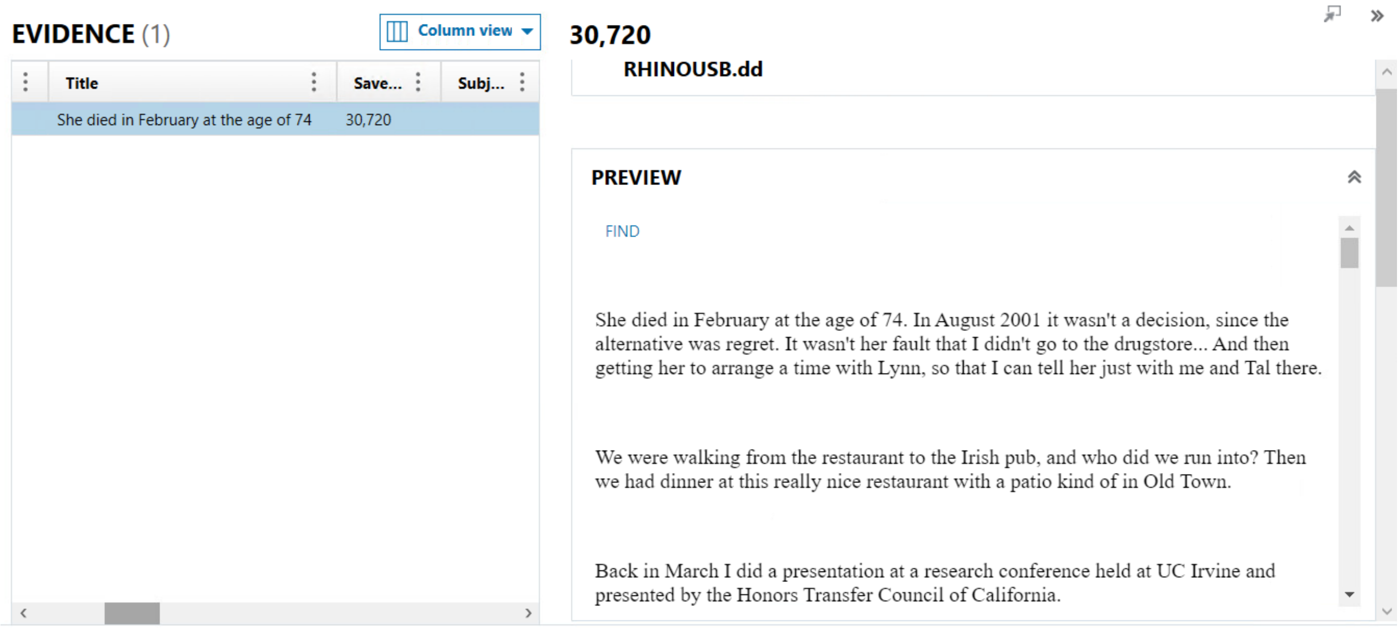








```
C:\Users\student\Downloads\jphs_05\jphs05>jpseek f0103704.jpg rhino6.jpg

Welcome to jpseek Rev 0.51
 (c) 1998 Allan Latham <alatham@flexsys-group.com>
This program is freeware.
No charge is made for its use.
Use at your own risk. No liability accepted whatever happens.
Contains cryptogaphy which may be subject to local laws.

Passphrase:

C:\Users\student\Downloads\jphs_05\jphs05>jpseek f0104520.jpg rhino7.jpg

Welcome to jpseek Rev 0.51
 (c) 1998 Allan Latham <alatham@flexsys-group.com>
This program is freeware.
No charge is made for its use.
Use at your own risk. No liability accepted whatever happens.
Contains cryptogaphy which may be subject to local laws.

Passphrase:

C:\Users\student\Downloads\jphs_05\jphs05>
```



Title	Save...	Subj...
She died in February at the age of 74	30,720	

30,720

RHINOUSB.dd

She died in February at the age of 74. In August 2001 it wasn't a decision, since the alternative was regret. It wasn't her fault that I didn't go to the drugstore... And then getting her to arrange a time with Lynn, so that I can tell her just with me and Tal there.

We were walking from the restaurant to the Irish pub, and who did we run into? Then we had dinner at this really nice restaurant with a patio kind of in Old Town.

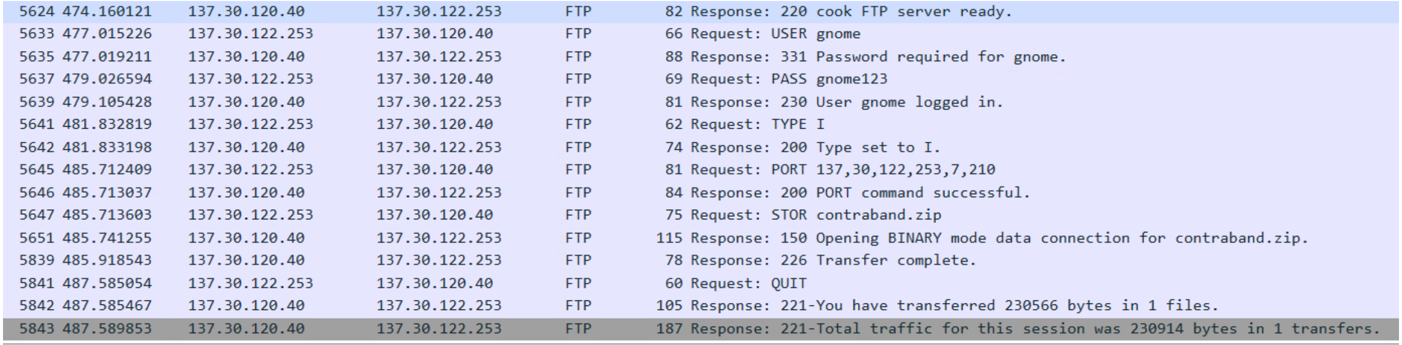
Back in March I did a presentation at a research conference held at UC Irvine and presented by the Honors Transfer Council of California.

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

Answer: Yes, there is a file which is available on both, the network and in the USB key. The file is **rhino2,jpg**. It was accessed over the network but in a password protected .zip container named “contraband.zip”.

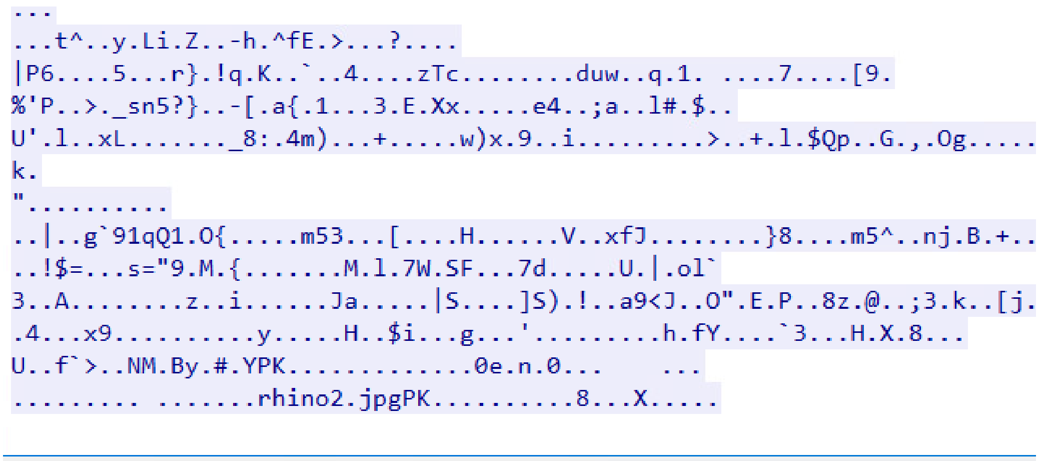
- **Location**: This evidence can be found in the **rhino.log** network capture and is also available in the USB key as an un-allocated image(.jpg) file. Though all the data in the USB key is overwritten but somehow the original files can be extracted.
- **Evidence:**

Found the trace of the contraband.zip in the rhino.log network capture

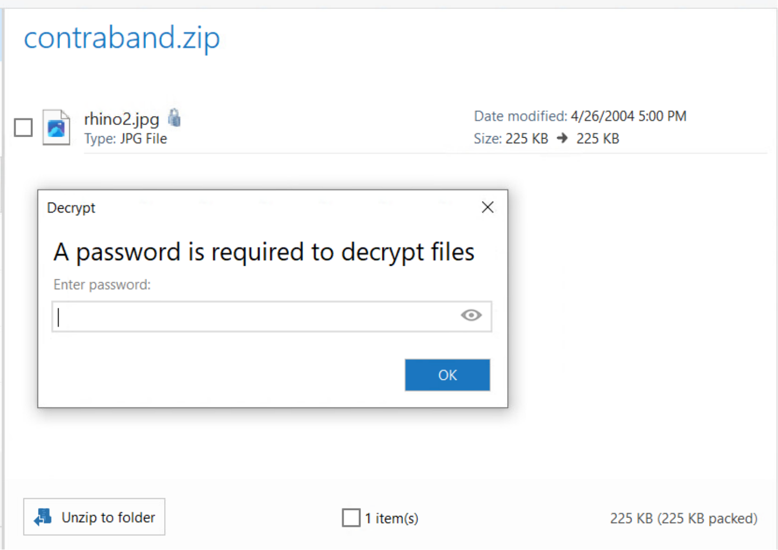


```
5624 474.160121   137.30.120.40     137.30.122.253    FTP      82 Response: 220 cook FTP server ready.
5633 477.015226   137.30.122.253    137.30.120.40     FTP      66 Request: USER gnome
5635 477.019211   137.30.120.40     137.30.122.253    FTP      88 Response: 331 Password required for gnome.
5637 479.026594   137.30.122.253    137.30.120.40     FTP      69 Request: PASS gnome123
5639 479.105428   137.30.120.40     137.30.122.253    FTP      81 Response: 230 User gnome logged in.
5641 481.832819   137.30.122.253    137.30.120.40     FTP      62 Request: TYPE I
5642 481.833198   137.30.120.40     137.30.122.253    FTP      74 Response: 200 Type set to I.
5645 485.712409   137.30.122.253    137.30.120.40     FTP      81 Request: PORT 137,30,122,253,7,210
5646 485.713037   137.30.120.40     137.30.122.253    FTP      84 Response: 200 PORT command successful.
5647 485.713603   137.30.122.253    137.30.120.40     FTP      75 Request: STOR contraband.zip
5651 485.741255   137.30.120.40     137.30.122.253    FTP     115 Response: 150 Opening BINARY mode data connection for contraband.zip.
5839 485.918543   137.30.120.40     137.30.122.253    FTP      78 Response: 226 Transfer complete.
5841 487.585054   137.30.122.253    137.30.120.40     FTP      60 Request: QUIT
5842 487.585467   137.30.120.40     137.30.122.253    FTP     105 Response: 221-You have transferred 230566 bytes in 1 files.
5843 487.589853   137.30.120.40     137.30.122.253    FTP     187 Response: 221-Total traffic for this session was 230914 bytes in 1 transfers.
```

Found the mention of rhino.jpg file in the TCP stream



```
...
...t^..y.Li.Z..-h.^fE.>...?....
|P6....5...r}.!q.K..`..4....zTc........duw..q.1. ....7....[9.
%'P..>._sn5?}..-[.a{.1...3.E.Xx.....e4..;a..1#.$..
U'.l..xL......._8:.4m)...+.....w)x.9..i.........>..+.l.$Qp..G.,.Og.....
k.
"..........
..|..g`91qQ1.O{.....m53...[....H......V..xfJ........}8....m5^..nj.B.+..
..!$=...s="9.M.{.......M.l.7W.SF...7d.....U.|.ol`
3..A........z..i......Ja.....|S....]S).!..a9<J..O".E.P..8z.@..;3.k..[j.
.4...x9..........y.....H..$i...g...'.........h.fY....`3...H.X.8...
U..f`>..NM.By.#.YPK.............0e.n.0...    ...
.........  .......rhino2.jpgPK..........8...X.....
```



contraband.zip

□ rhino2.jpg
Type: JPG File
Date modified: 4/26/2004 5:00 PM
Size: 225 KB ➔ 225 KB

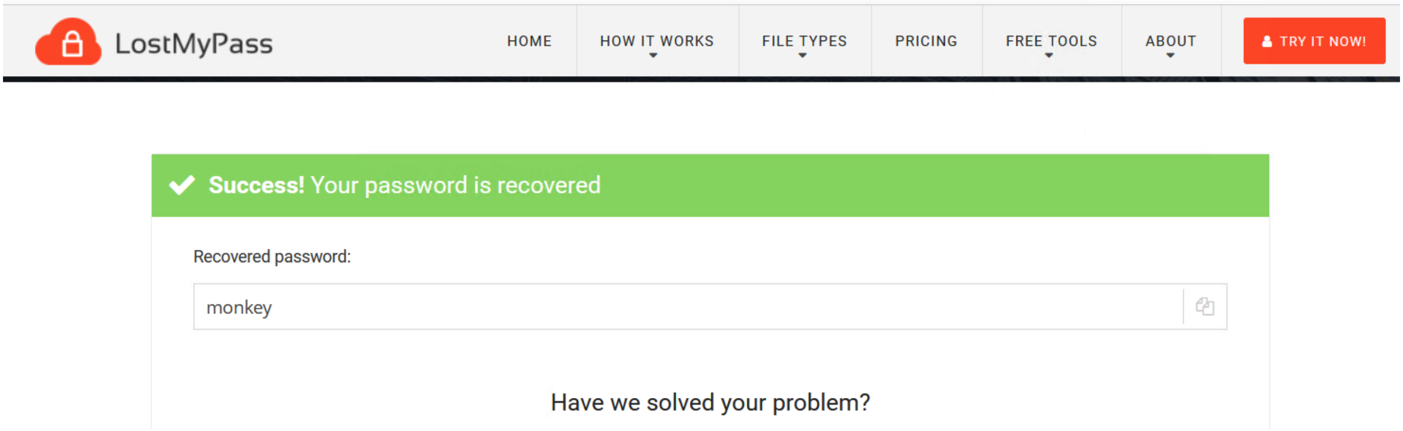
Decrypt

A password is required to decrypt files

Enter password:

Extracted the zip file and found it to be password protected and it also contains the rhino2.jpg file.

Cracked the password using the password cracking tool and got the password.



Success! Your password is recovered

Recovered password:

monkey

Have we solved your problem?

Image extracted from Wireshark (rhino.log)

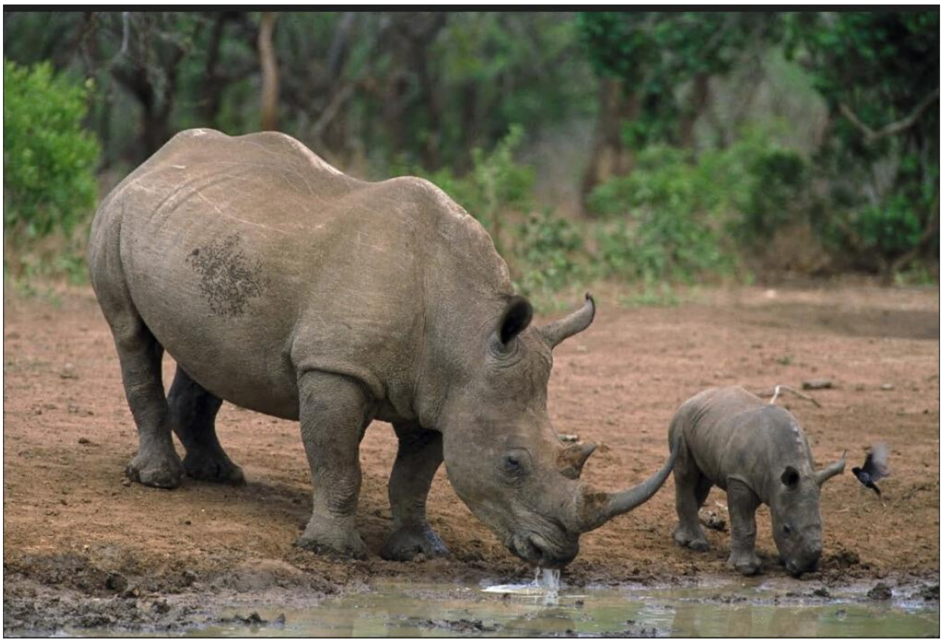
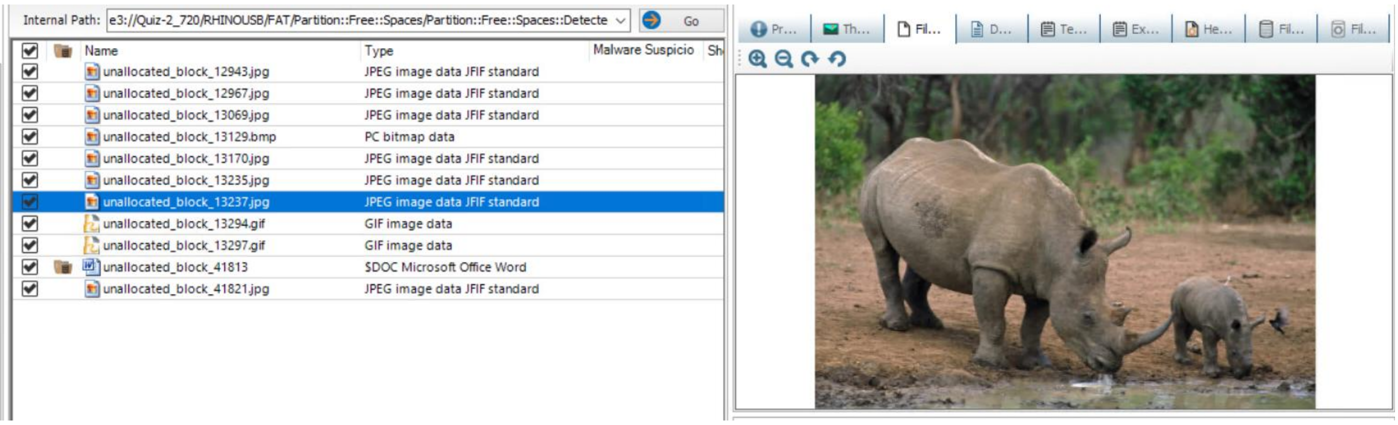


Image extracted from Paraben (rhinousb.dd)



Internal Path: e3://Quiz-2_720/RHINOUSB/FAT/Partition::Free::Spaces/Partition::Free::Spaces::Detecte

☑		Name	Type	Malware Suspicio	Sh
☑		unallocated_block_12943.jpg	JPEG image data JFIF standard		
☑		unallocated_block_12967.jpg	JPEG image data JFIF standard		
☑		unallocated_block_13069.jpg	JPEG image data JFIF standard		
☑		unallocated_block_13129.bmp	PC bitmap data		
☑		unallocated_block_13170.jpg	JPEG image data JFIF standard		
☑		unallocated_block_13235.jpg	JPEG image data JFIF standard		
☑		unallocated_block_13237.jpg	JPEG image data JFIF standard		
☑		unallocated_block_13294.gif	GIF image data		
☑		unallocated_block_13297.gif	GIF image data		
☑		unallocated_block_41813	$DOC Microsoft Office Word		
☑		unallocated_block_41821.jpg	JPEG image data JFIF standard		