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.

ANSWERS TO QUESTIONS (1)

- Who gave the accused a telnet/ftp account?

  ANSWER: Jeremy (from diary)

- What's the username/password for the account?

  ANSWER: gnome / gnome123

- What relevant file transfers appear in the network traces?

  ANSWER:

  > **rhino1.jpg, rhino3.jpg in rhino.log trace**
  > **[FTP transfers]**
  >
  > **rhino2.jpg in contraband.zip file from rhino.log trace [encrypted, pw = monkey]**
  >
  > **rhino4.jpg, rhino5.gif in rhino2.log**
  > **[HTTP transfers]**
  >
  > **An executable "rhino.exe" in rhino3.log**
  > **[HTTP transfer]**

ANSWERS TO QUESTIONS (2)

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

  ANSWER: Suspect tossed it into the Mississippi River (from diary)

- What happened to the USB key?

  ANSWER: Suspect reformatted it—possibly at Radio Shack--hoping not to overwrite the "good" stuff. Source: diary.

ANSWERS TO QUESTIONS (3)

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

  ANSWER:

  Directly, several reasonable gumbo recipes… ☺

  Must use file carving (Foremost, Scalpel, WinHex, or FTK) to retrieve evidence:

  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

  Word document "diary.doc" contains some answers to the questions

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

  ANSWER:

  At least one thing:

  rhino2.jpg carved from USBKEY is same as rhino2.jpg in zip file from network trace.

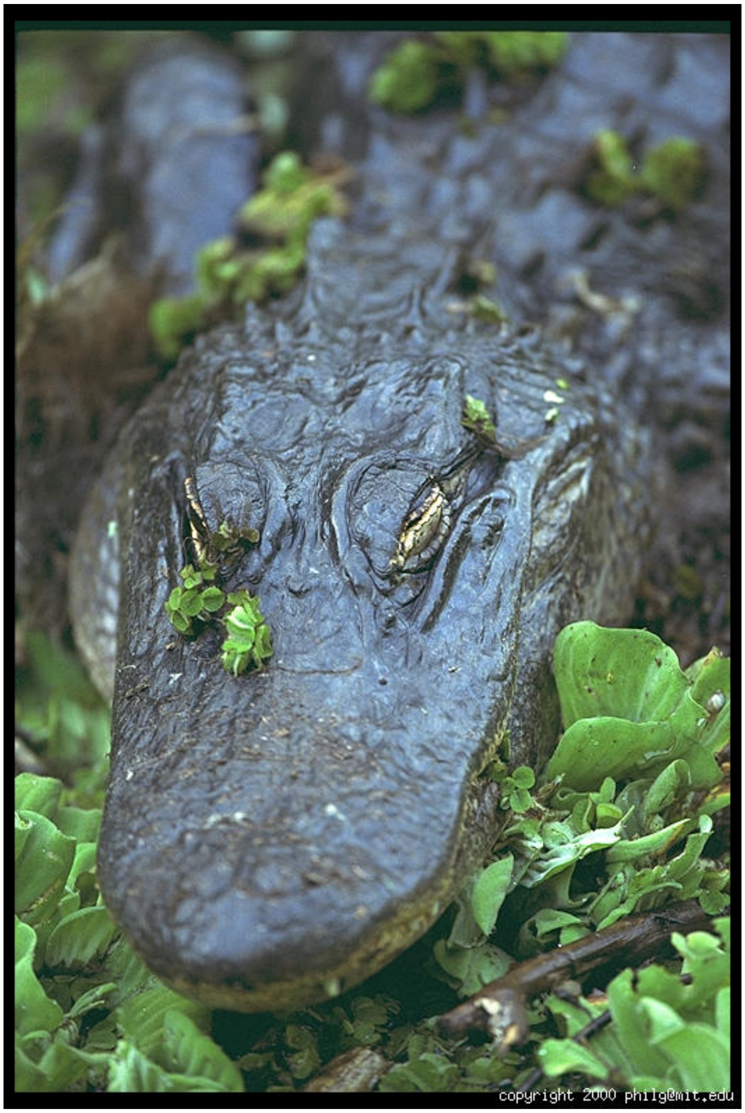
Summary:

10 unique rhino images can be recovered.

SOLUTION (1)

Carve:

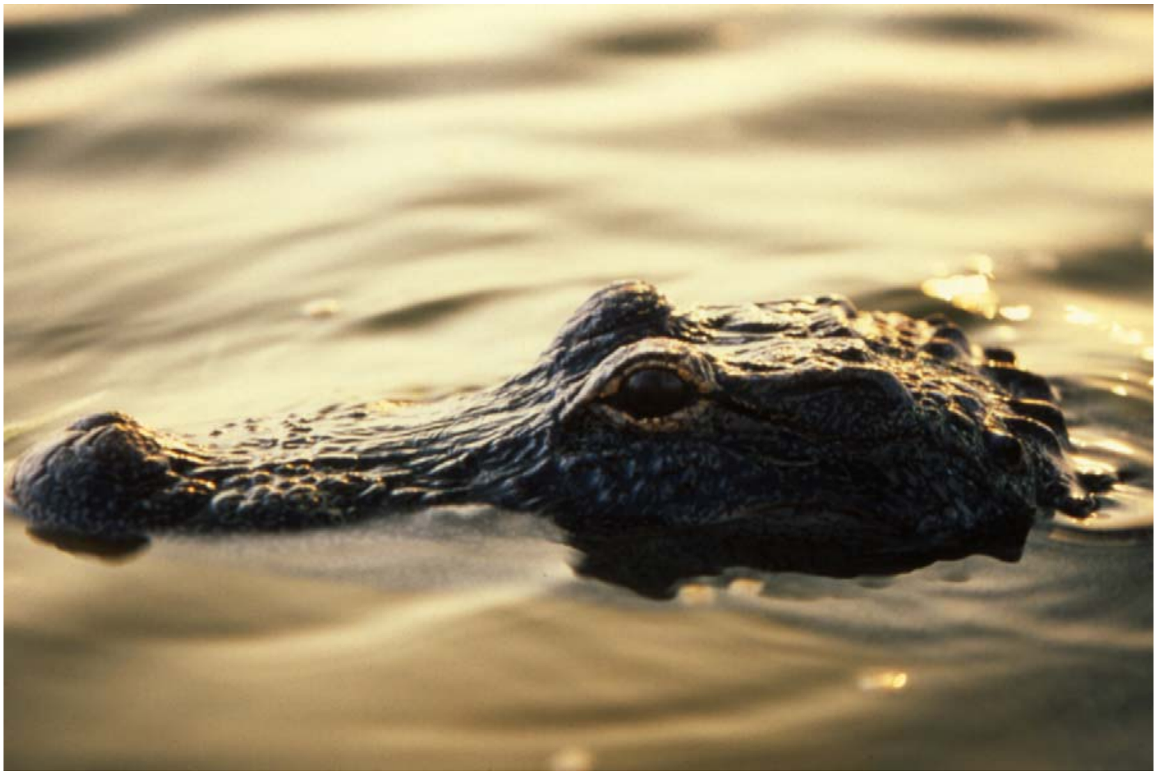
alligator1.jpg
MD5: ee67d8bef72f9b63fa93dc9ea1bb833a



SOLUTION (2)

Carve:

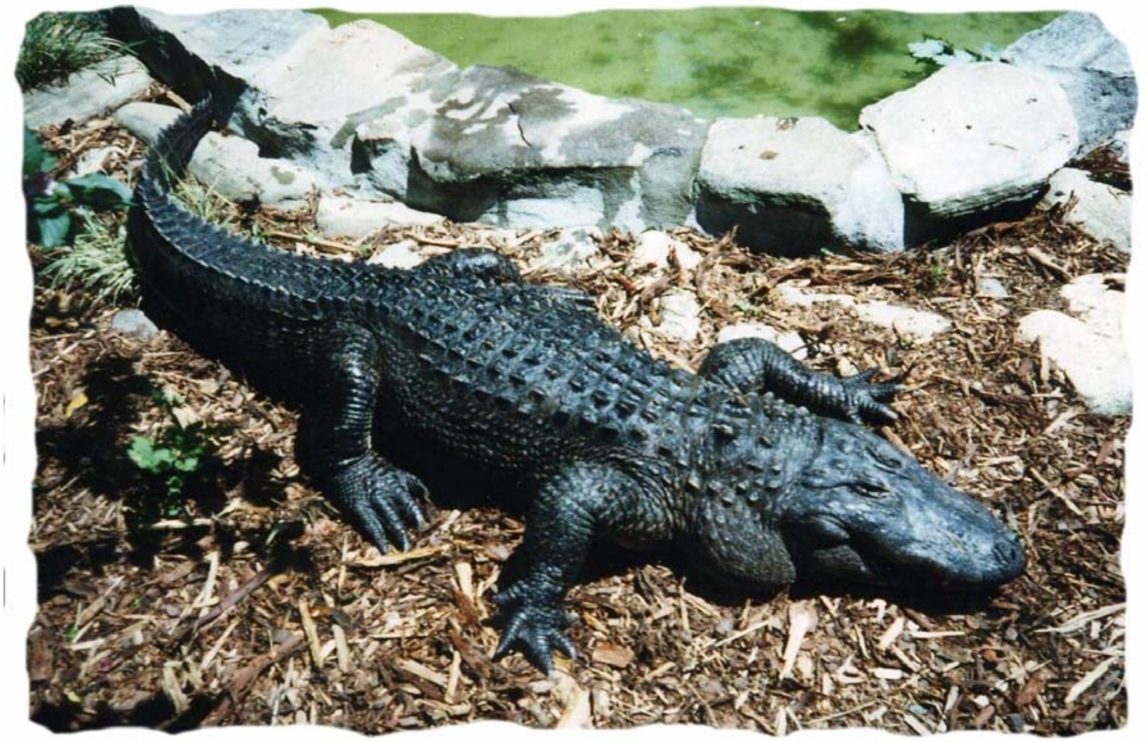
alligator2.jpg
MD5: 4d37a1033450b8cc96ffd1564829d321



SOLUTION (3)

Carve:

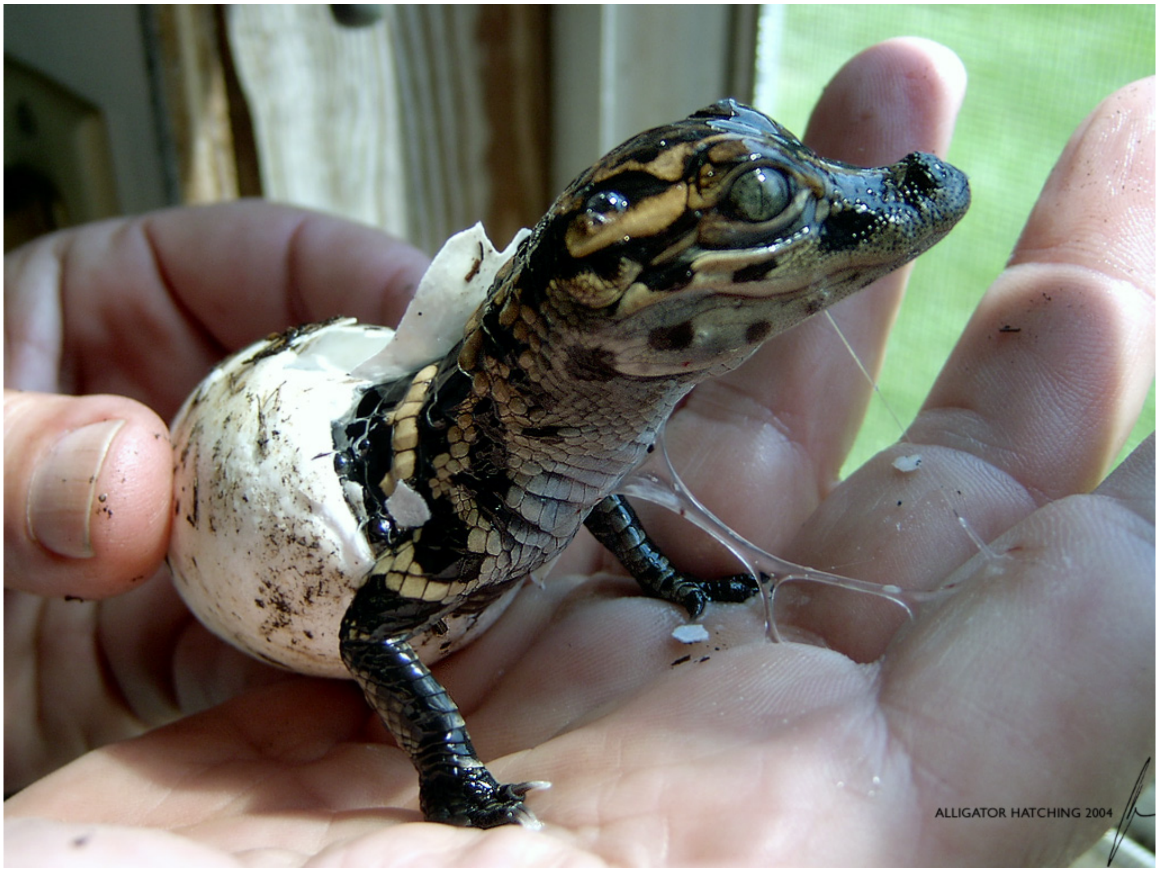
alligator3.jpg
MD5: 6bd0e9bd4fb4a738f9ca4c351a853281



SOLUTION (4)

Carve:

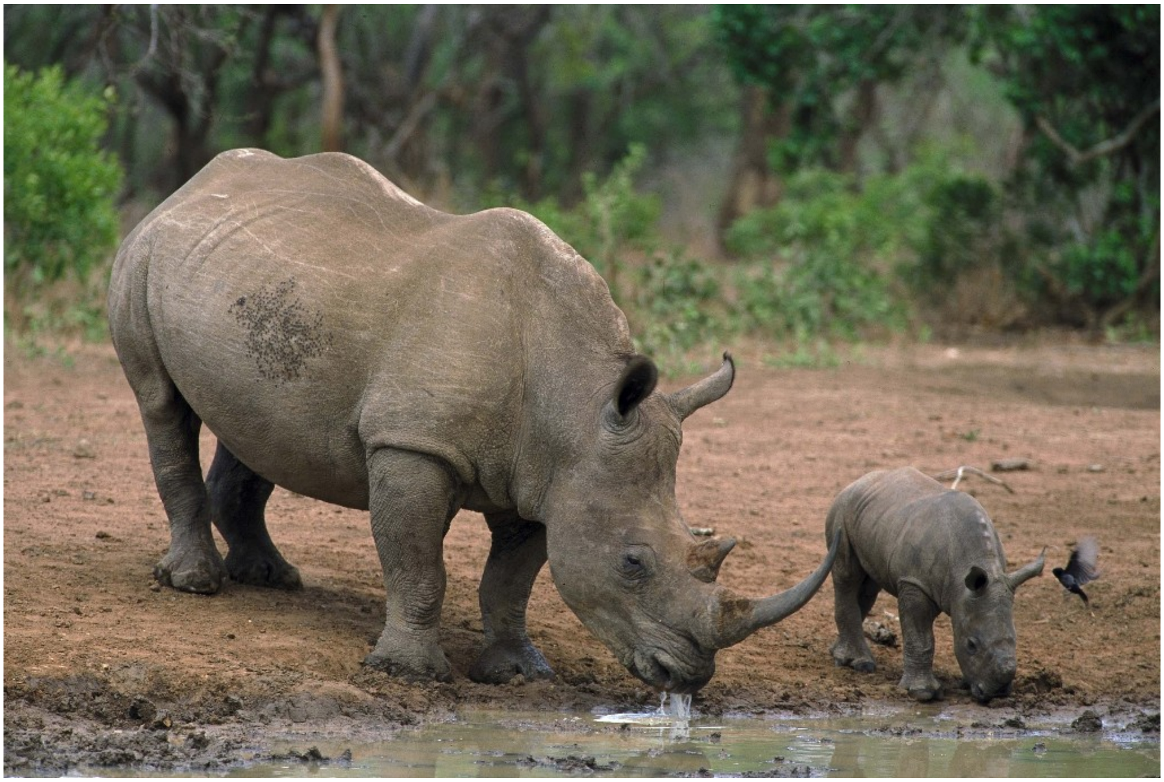
alligator4.jpg
MD5: f1bbcd31cd33badc65ca3d1d781f57fa



SOLUTION (5)

Carve:

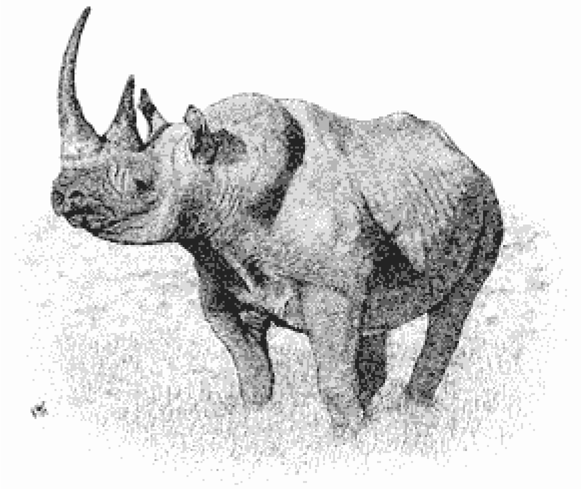
rhino2.jpg
MD5:ed870202082ea4fd8f5488533a561b35



SOLUTION (6)

Carve:

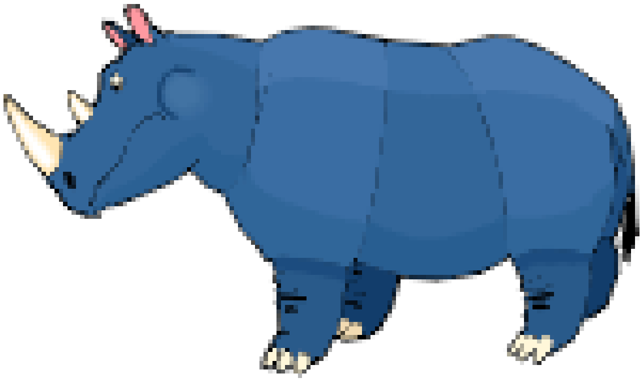
rhino8.gif
MD5: 76610b7bdb85e5f65e96df3f7e417a74



SOLUTION (7)

Carve:

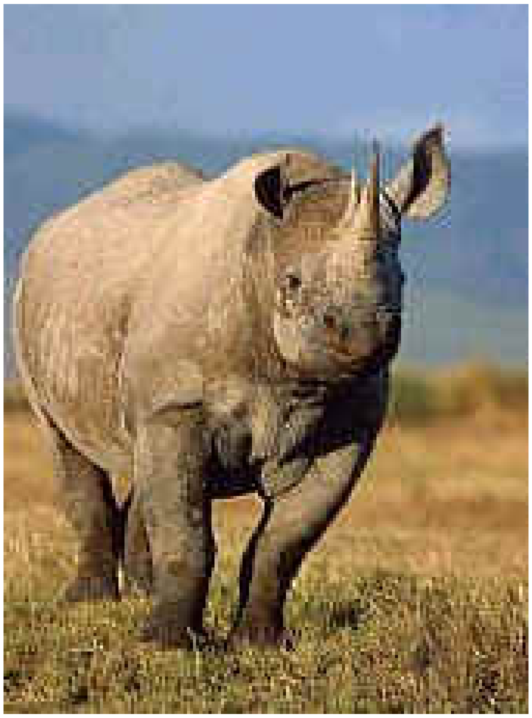
rhino9.gif
MD5: d03dc23d4ec39e4d16da3c46d2932d62



SOLUTION (8)

Carve:

rhino10.jpg
MD5: ca03f2eed3db06a82a8a31b3a3defa24



SOLUTION (9)

stegdetect on the carved JPG files:

```
# stegdetect *.jpg
File aa 0001.jpg : negative
Corrupt JPEG data: 8 extraneous bytes before…
File aa 0002.jpg : jphide(*)
File aa 0003.jpg : skipped (false positive likely)
File aa 0004.jpg : negative
File aa 0005.jpg : negative
Corrupt JPEG data: 198 extraneous bytes before…
File aa 0006.jpg : negative
File aa 0007.jpg : negative
```

stegbreak:

```
# stegbreak -f words -r rules.ini *.jpg
…
…
File aa 0003.jpg : jphide[v5](gator)
File aa 0002.jpg : jphide[v5](gumbo)
…

…
Processed 2 files, found 2 embeddings.
Time: 3 seconds: Cracks: 19769,   6589.7 c/s
```

SOLUTION (10)

jpseek on the JPGs w/ stego:

```
C:\temp\crap>\stego\jphide\jpseek "File aa 0002.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: <gumbo>

C:\temp\crap>\stego\jphide\jpseek "File aa 0003.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: <gator>
```

SOLUTION (11)

alligator2.jpg

[illegible]

MD5:87018ef0cfdb91[illegible]18d92efeb9c19338

SOLUTION (12)

alligator3.jpg

[illegible]

MD5: 63a39823f80b3[illegible]2dcd112158b55011

SOLUTION (13)

Carve:

diary.doc
MD5: 4227284fc2e03b7d7d5ca1fe23855afb

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.

My mother and I have a unique relationship. Chasing Amy - *whimpers* By all accounts i should have liked this film. Their relationship was a failure! All other IB families are trying to keep their kid in IB.. trying to encourage their kid to do good.. mine is trying to make me quit. Anyway, this one is someone she was involved with in high school who says he's been trying to find her all these years and finally tracked her down. So seeing how I am scared of pitch black darkness I got up and was trying to see what made the power go out, and my parents got up and joined me with flashlights and candles. I handed in the damn homework, which was really quite stupid for all those who do know how to use the damn computer. He turned back to me, completely sober, completely serious and replied - 'No, I don't dislike you, I'm just scared of you.' I stared at him in disbelief for a moment or two or three - scared of me?

There truly are buckets of phenomenal things to be amazed by, and thankful for.

Stocklos and Andrew were only there for one of the nights I was.

Then there was one 4th of July when we had just moved to a big new house in the country & we were flat busted, so we had no funds to celebrate. But Jon and been watching the encounter and remained at bay purposely in order to let me say what I had to say to Andrew. I am so excited about the trip... and so excited that Jen and Nicole are going... and so excited that we are going to both Wolves games while we are there. And she attempted lying to me about going Hong Kong together. And look, it's very difficult to work both sides of the aisle.

It might last. MILLER, who actually taught my HIS 102 class last semester, and he was the last class I had last time, and the first class this time.

I've been so caught up in all this craziness going on and such!

This can be a very uncomfortable moment if someone walks in and busts you.

I haven't brought it up to Amanda, but Stephen knows how uncomfortable it is. It's all uncomfortable and awkward.

And it's so easy, we're an Irish family and all that implies.

So in honor of better times: heres something I wrote a year ago, a moment from a night that Brady and I spent together last winter...

Sarah and I took a break after extensive arguing, where she proceeded to date my closest friend and housemate from Miami. After much haranguing from my father, my sisters, brother, nieces and I begrudgingly agreed to sing carols and whatnot, in unison and harmony, at our hüge Christmas party under the name, The Family Songsters. You know, what will people remember years from now as hip?

All the card schools in every corner of the earth - and all that's in between - are they just a game of chance? This was foretold and all that goes along with it. I always had the feeling that he was going to turn on me one day and that I was being set up for the kill, but the moment never came. Sometimes I have to bribe Big Mike with a bottle of vodka to drive over in his van so I can collect an item that's too big to fit into my 13-year-old Mazda hatchback. I grunted, growled and prepared to tell the offending party that I was BUSY when I glanced up and saw the SN glaring at me from the new window... And then getting her to arrange a time with Lynn, so that I can tell her just with me and Tal there. Its quite a good show, although there are some problems with it: um, guys, could you lay off on the slow-motion-with-morbid-period-appropriate-soundtrack routine when tying up the end of the episode? Had a session with my therapist, Kim, on Monday as per usual. To spend some time with friends? At heart and core were a lot alike, we just get there at slightly different ways some times. Science has proven that people of different races are that way because of the climate.

Not many people got the angle I did during the ceremony, to see the way they were smiling, the way that they looked at each other, but if anyone was dense enough to miss it before, they would have figured it out from seeing that. I feel, so, so what’s the word... ah yes annoyed with people who think that i am something that I'm not when i barely even know them. I was told I bird walk, it means like, talking about something, going off on a tangent and talking about something completely different, then going back to what i was talking about before like I haven’t been ranting about something else for the last 5 minutes. A complete 180 from last week and the week before, I think it has something to do with the fact I haven't seen/talked to Gus since last Tuesday.

In a way I don't even want to write here cos she might come and read it then not write herself but at the same time I've been thinking in diary entry since about 10:30pm when the distractions stopped.

I don't know what to say to him.

I don't know what I'll be feeling tomorrow night at this time, all alone with no cable and no gas and no internet access, but thats okay.

I still have to tell my Tom & Jerry story... probably tomorrow if I have time.

Feeling certain there was a curse upon my head, I gave up, returned home, and took a shower.

Do you have to be a gold member to put in background pics??

A little background: When I was 14, I had eye surgery to correct a birth defect. When I called them the other day to find out when they were open, I got someone very, very stern. And they sent a snotty fool down from Buffalo to run the store. However, after a while of dealing with her crap, management decided they wanted some more room in the store to put...whatever. 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 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.

SOLUTION (14)

Network Traces

(3) files recoverable from “rhino.log”:

rhino1.jpg
rhino3.jpg
contraband.zip   (FTP TRANSFERS)

(2) files recoverable from “rhino2.log”

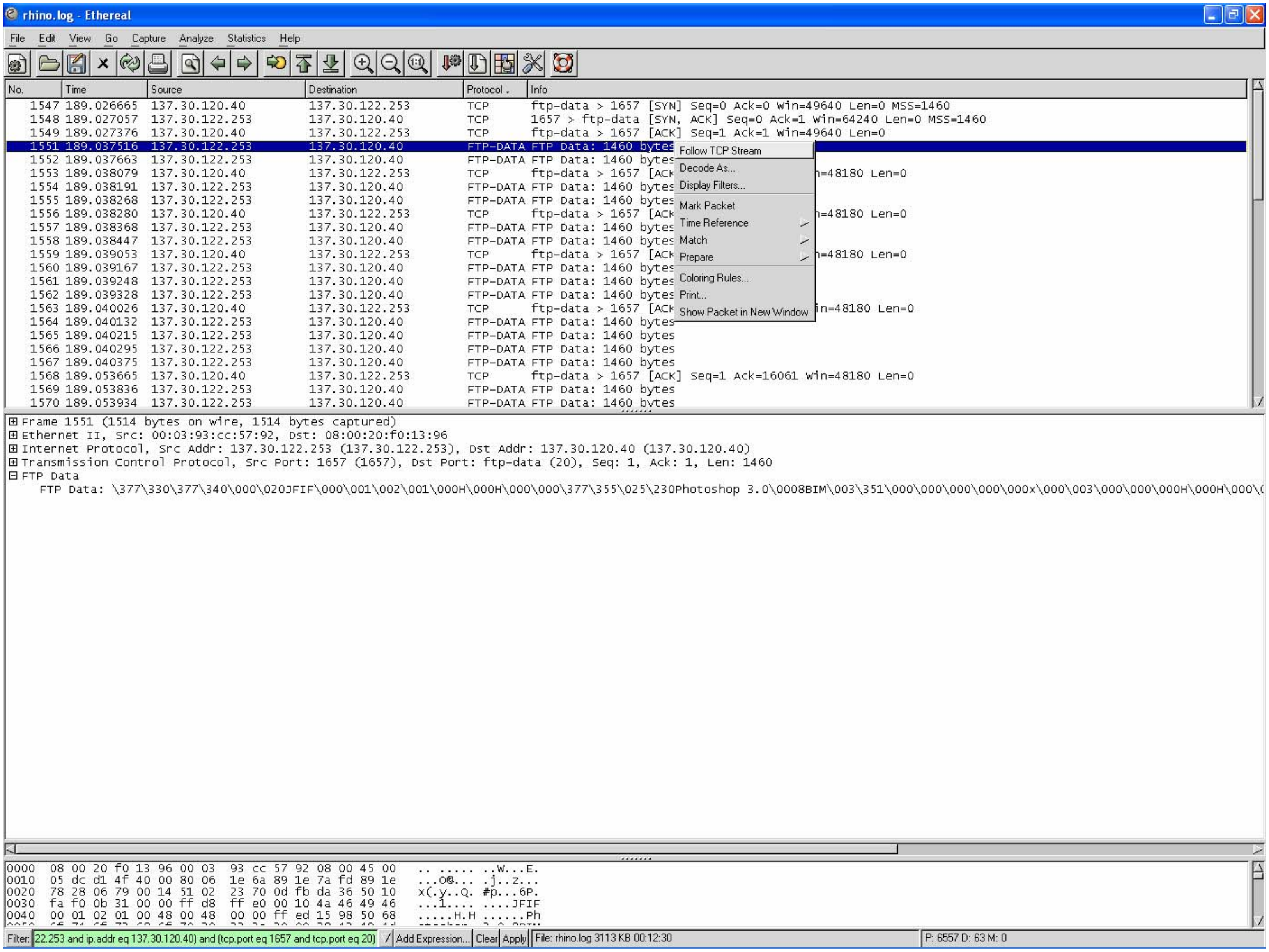
rhino4.jpg
rhino5.gif   (HTTP transfers)

(1) file recoverable from “rhino3.log”

rhino.exe
[Early version of MS DISKPART]

Solution: Use ethereal to carve FTP/HTTP data streams

FTP is easier. For HTTP, need to trim HTTP header.



```
No.     Time        Source          Destination     Protocol . Info
   1547 189.026665  137.30.120.40   137.30.122.253  TCP      ftp-data > 1657 [SYN] Seq=0 Ack=0 Win=49640 Len=0 MSS=1460
   1548 189.027057  137.30.122.253  137.30.120.40   TCP      1657 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   1549 189.027376  137.30.120.40   137.30.122.253  TCP      ftp-data > 1657 [ACK] Seq=1 Ack=1 Win=49640 Len=0
   1551 189.037516  137.30.122.253  137.30.120.40   FTP-DATA FTP Data: 1460 bytes
   1552 189.037663  137.30.122.253  137.30.120.40   FTP-DATA FTP Data: 1460 bytes
   1553 189.038079  137.30.120.40   137.30.122.253  TCP      ftp-data > 1657 [ACK                     n=48180 Len=0
   1554 189.038191  137.30.122.253  137.30.120.40   FTP-DATA FTP Data: 1460 bytes
   1555 189.038268  137.30.122.253  137.30.120.40   FTP-DATA FTP Data: 1460 bytes
   1556 189.038280  137.30.120.40   137.30.122.253  TCP      ftp-data > 1657 [ACK                     n=48180 Len=0
   1557 189.038368  137.30.122.253  137.30.120.40   FTP-DATA FTP Data: 1460 bytes
   1558 189.038447  137.30.122.253  137.30.120.40   FTP-DATA FTP Data: 1460 bytes
   1559 189.039053  137.30.120.40   137.30.122.253  TCP      ftp-data > 1657 [ACK                     n=48180 Len=0
   1560 189.039167  137.30.122.253  137.30.120.40   FTP-DATA FTP Data: 1460 bytes
   1561 189.039248  137.30.122.253  137.30.120.40   FTP-DATA FTP Data: 1460 bytes
   1562 189.039328  137.30.122.253  137.30.120.40   FTP-DATA FTP Data: 1460 bytes
   1563 189.040026  137.30.120.40   137.30.122.253  TCP      ftp-data > 1657 [ACK                     in=48180 Len=0
   1564 189.040132  137.30.122.253  137.30.120.40   FTP-DATA FTP Data: 1460 bytes
   1565 189.040215  137.30.122.253  137.30.120.40   FTP-DATA FTP Data: 1460 bytes
   1566 189.040295  137.30.122.253  137.30.120.40   FTP-DATA FTP Data: 1460 bytes
   1567 189.040375  137.30.122.253  137.30.120.40   FTP-DATA FTP Data: 1460 bytes
   1568 189.053665  137.30.120.40   137.30.122.253  TCP      ftp-data > 1657 [ACK] Seq=1 Ack=16061 Win=48180 Len=0
   1569 189.053836  137.30.122.253  137.30.120.40   FTP-DATA FTP Data: 1460 bytes
   1570 189.053934  137.30.122.253  137.30.120.40   FTP-DATA FTP Data: 1460 bytes
```

```
⊞ Frame 1551 (1514 bytes on wire, 1514 bytes captured)
⊞ Ethernet II, Src: 00:03:93:cc:57:92, Dst: 08:00:20:f0:13:96
⊞ Internet Protocol, Src Addr: 137.30.122.253 (137.30.122.253), Dst Addr: 137.30.120.40 (137.30.120.40)
⊞ Transmission Control Protocol, Src Port: 1657 (1657), Dst Port: ftp-data (20), Seq: 1, Ack: 1, Len: 1460
⊟ FTP Data
    FTP Data: \377\330\377\340\000\020JFIF\000\001\002\001\000H\000H\000\000\377\355\025\230Photoshop 3.0\0008BIM\003\351\000\000\000\000\000x\000\003\000\000\000H\000H\000\(
```

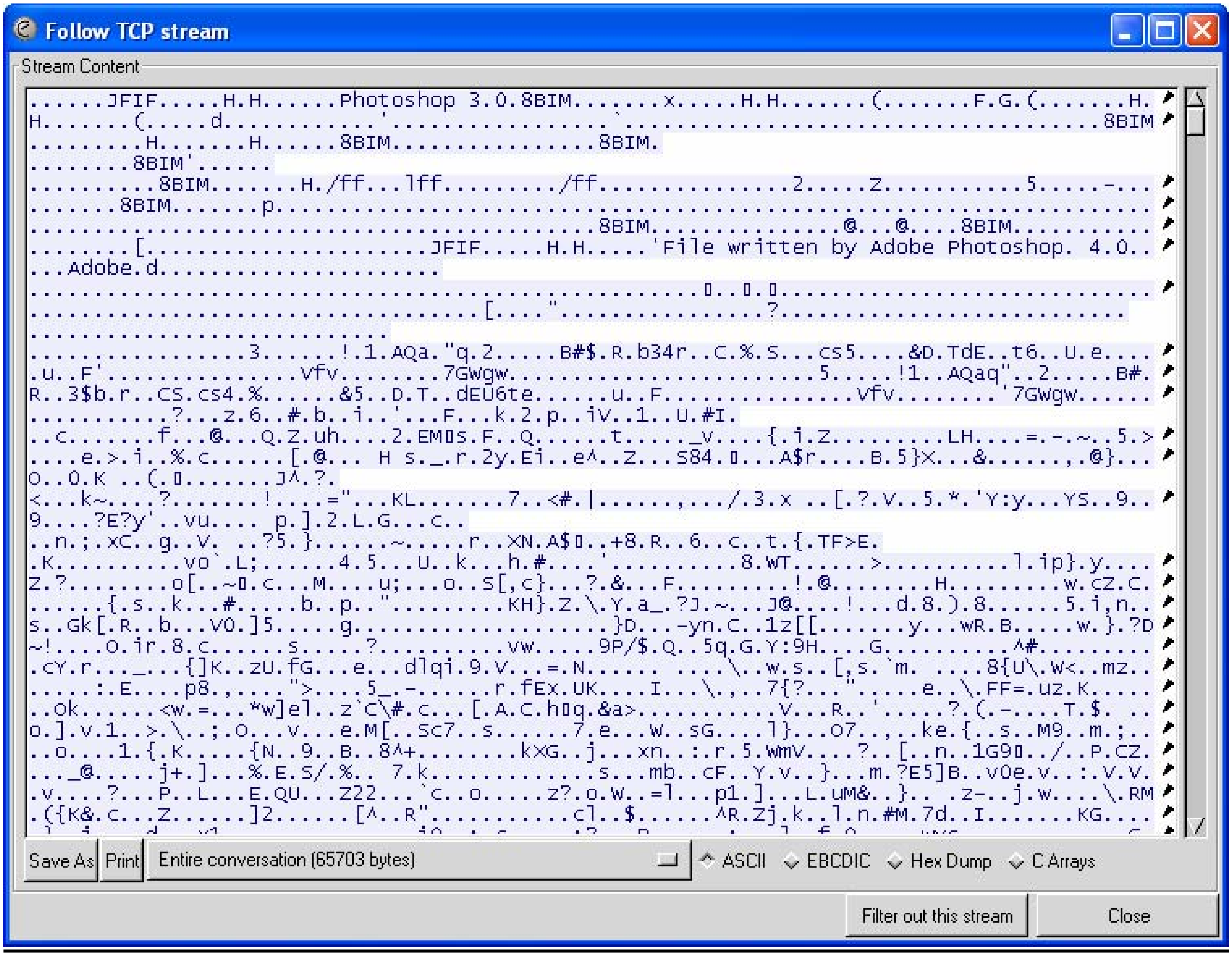
```
0000   08 00 20 f0 13 96 00 03  93 cc 57 92 08 00 45 00   .. ..... ..W...E.
0010   05 dc d1 4f 40 00 80 06  1e 6a 89 1e 7a fd 89 1e   ...O@... .j..z...
0020   78 28 06 79 00 14 51 02  23 70 0d fb da 36 50 10   x(.y..Q. #p...6P.
0030   fa f0 0b 31 00 00 ff d8  ff e0 00 10 4a 46 49 46   ...1.... ....JFIF
0040   00 01 02 01 00 48 00 48  00 00 ff ed 15 98 50 68   .....H.H ......Ph
```

Filter: 22.253 and ip.addr eq 137.30.120.40) and (tcp.port eq 1657 and tcp.port eq 20)

File: rhino.log 3113 KB 00:12:30

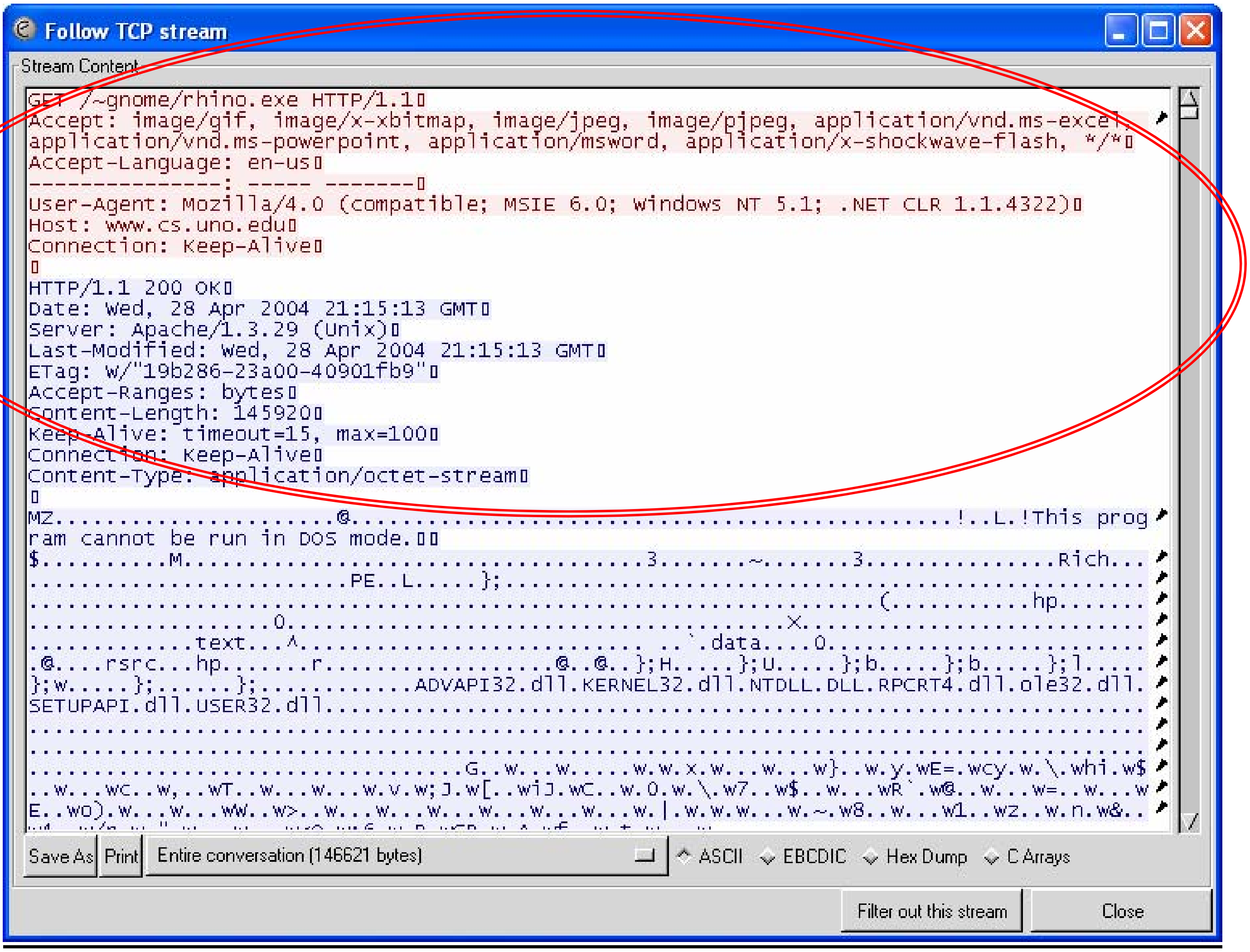
P: 6557 D: 63 M: 0

FTP



```
......JFIF.....H.H......Photoshop 3.0.8BIM........x.....H.H.......(.......F.G.(.......H.
H.......(.....d...........'...................`...........................8BIM
.........H.......H......8BIM.................8BIM.
........8BIM'......
..........8BIM.......H./ff...lff........./ff...............2.....Z...........5.....-...
.......8BIM.......p.....................................................................
.................................................8BIM...............@...@....8BIM..........
........[......................JFIF.....H.H.....'File written by Adobe Photoshop. 4.0..
...Adobe.d.....................
..........................................................□..□.□.............................
...................................[....".................?..............................
............................
.................3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE..t6..U.e....
.u..F'..............Vfv........7Gwgw.........................5.....!1..AQaq"..2.....B#.
R..3$b.r..CS.cs4.%......&5..D.T..dEU6te......u..F................Vfv........'7Gwgw......
...........?...z.6..#.b..i..'...F...k.2.p..iV..1..U.#I.
..c.......f...@...Q.Z.uh....2.EM□s.F..Q......t....._v....{.i.Z.........LH....=.-.~..5.>
....e.>.i..%.c......[.@...  H s._.r.2y.Ei..e^..Z...S84.□...A$r....B.5}X...&......,.@}...
O..O.K  ..(.□.......J^.?.
<...k~....?.......!....="...KL.......7..<#.|........,.../.3.x  ..[.?.V..5.*.'Y:y...YS..9..
9....?E?y'..vu....  p.].2.L.G...c..
..n.;.xC..g..V.  ..?5.}.......~.....r..XN.A$□..+8.R..6..c..t.{.TF>E.
.K..........vo`.L;......4.5...U..k...h.#....'..........8.WT.......>..........l.ip}.y....
Z.?........o[..~□.c...M....u;...o..S[,c}...?.&...F.........!.@........H.........w.cZ.C.
......{.s..k...#.....b..p.."..........KH}.Z.\.Y.a_.?J.~...J@....!...d.8.).8......5.i,n..
s..Gk[.R..b...VO.]5.....g......................}D...-yn.C..1z[[.......y...wR.B.....w.}.?D
~!....O.ir.8.c......s.....?..........vw.....9P/$.Q..5q.G.Y:9H....G..........^#.........
.cY.r...._...{]K..zU.fG...e...dlqi.9.V...=.N......  ....\..w.s..[,s.`m.  ....8{U\.W<..mz..
......:.E....p8.,.....">....5_.-......r.fEx.UK....I....\.,..7{?...".....e..\.FF=.uz.K.....
..Ok......<w.=...*w]el..z`C\#.c...[.A.C.h□q.&a>...........V...R..'.....?.(.-....T.$.  ..
o.].v.1..>.\..;.O...v....e.M[..Sc7..s......7.e...W..sG....l}...O7..,...ke.{..s..M9..m.;..
..o....1.{.K.....{N..9..B..8^+.........kXG..j...xn..:.r.5.wmV....?..[..n..1G9□../..P.CZ.
...._@.....j+.]...%.E.S/.%..  7.k..............s...mb..cF..Y.v..}...m.?E5]B..v0e.v...:.V.V.
.v....?...P..L...E.QU...Z22....`c..o.....z?.o.W..=l...p1.]...L.uM&..}..  .z-..j.w....\.RM
.({K&.c...Z.......]2.......[^..R"............cl..$.......^R.Zj.k..l.n.#M.7d..I.........KG....
```
]

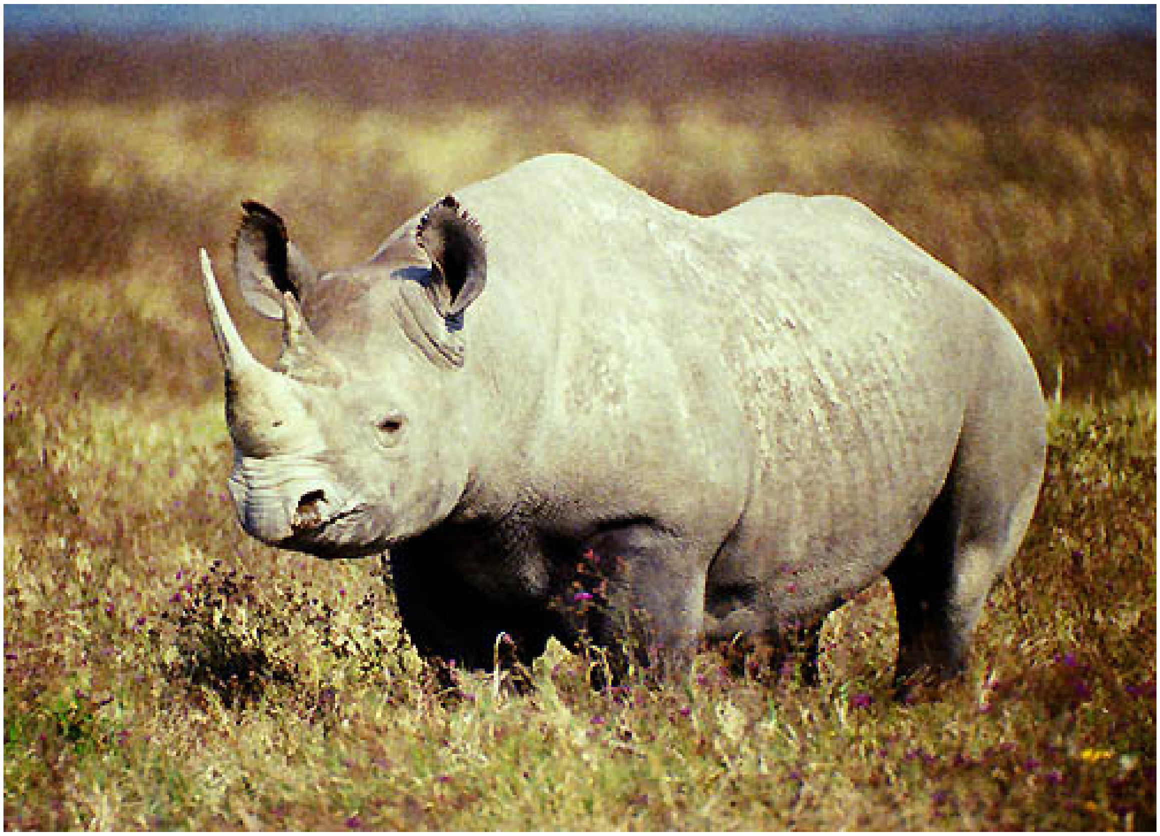
HTTP



```
GET /~gnome/rhino.exe HTTP/1.1▯
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel,
application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */*▯
Accept-Language: en-us▯
---------------: ----- -------▯
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)▯
Host: www.cs.uno.edu▯
Connection: Keep-Alive▯
▯
HTTP/1.1 200 OK▯
Date: Wed, 28 Apr 2004 21:15:13 GMT▯
Server: Apache/1.3.29 (Unix)▯
Last-Modified: Wed, 28 Apr 2004 21:15:13 GMT▯
ETag: W/"19b286-23a00-40901fb9"▯
Accept-Ranges: bytes▯
Content-Length: 145920▯
Keep-Alive: timeout=15, max=100▯
Connection: Keep-Alive▯
Content-Type: application/octet-stream▯
▯
MZ.....................@...........................................!..L.!This prog
ram cannot be run in DOS mode.▯▯
$.........M........................................3.......~.......3...............Rich...
.........................PE..L.....};..................................................
..................................................................(...........hp.......
..................0.........................................X.........................
.............text...^........................  ..`.data....0..........................
.@....rsrc...hp.......r..................@..@..};H.....};U.....};b.....};b.....};l.....
};w.....};......};............ADVAPI32.dll.KERNEL32.dll.NTDLL.DLL.RPCRT4.dll.ole32.dll.
SETUPAPI.dll.USER32.dll.................................................................
........................................................................................
........................................................................................
.................................G..w...w.....w.w.x.w...w...w}..w.y.wE=.wcy.w.\.whi.w$
..w...wc..w,..wT..w...w...w.v.w;J.w[..wiJ.wC..w.0.w.\.w7..w$..w...wR`.w@..w...w=..w...w
E..wo).w...w...ww..w>..w...w...w...w...w...w...w.|.w.w.w...w.~.w8..w...w1..wz..w.n.w&..
```

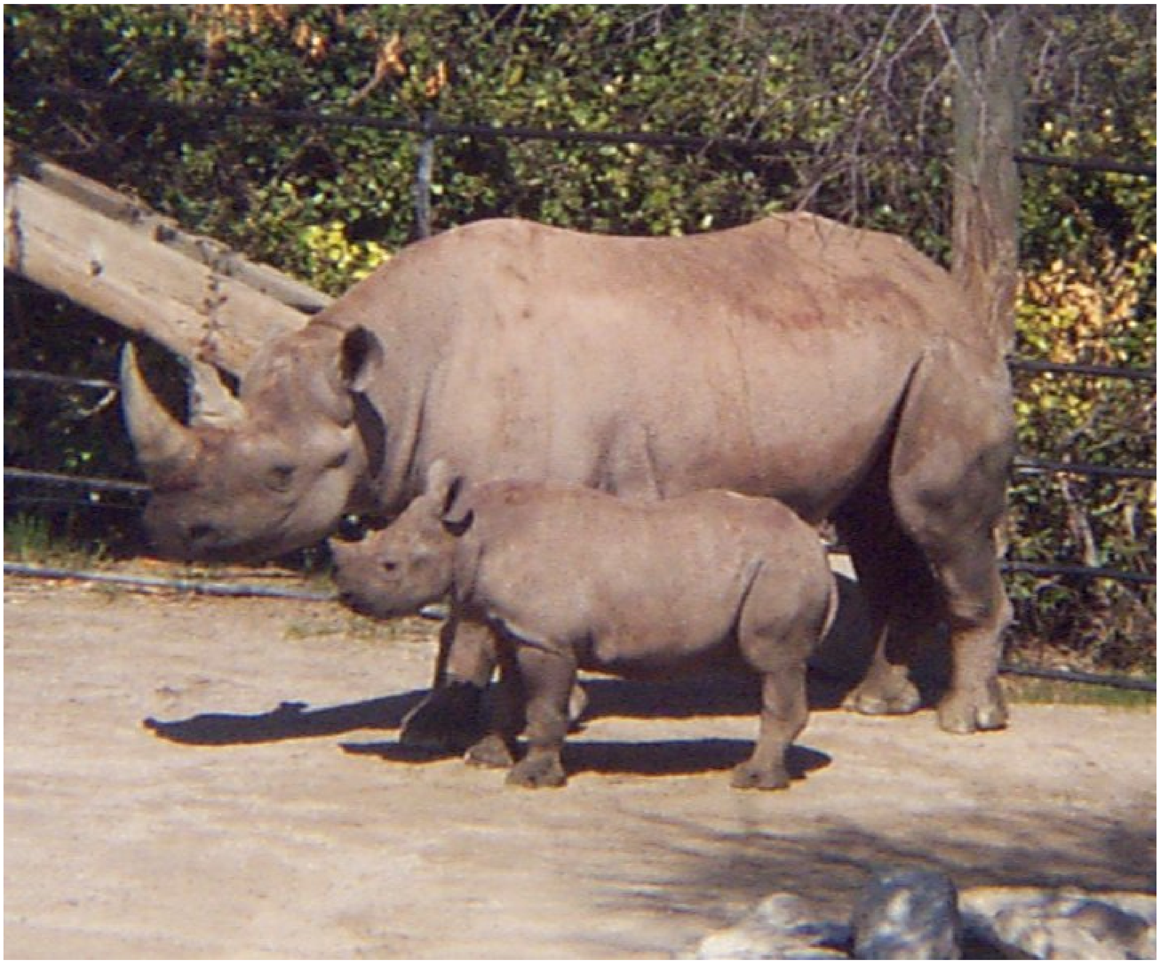
SOLUTION (15)

rhino1.jpg
MD5: d5a83cde0131c3a034e5a0d3bd94b3c9



SOLUTION (16)

rhino3.jpg
MD5: b058218ea0060092d4e01ef3d7a3b815



SOLUTION (17)

ZIP file carved from FTP data stream:

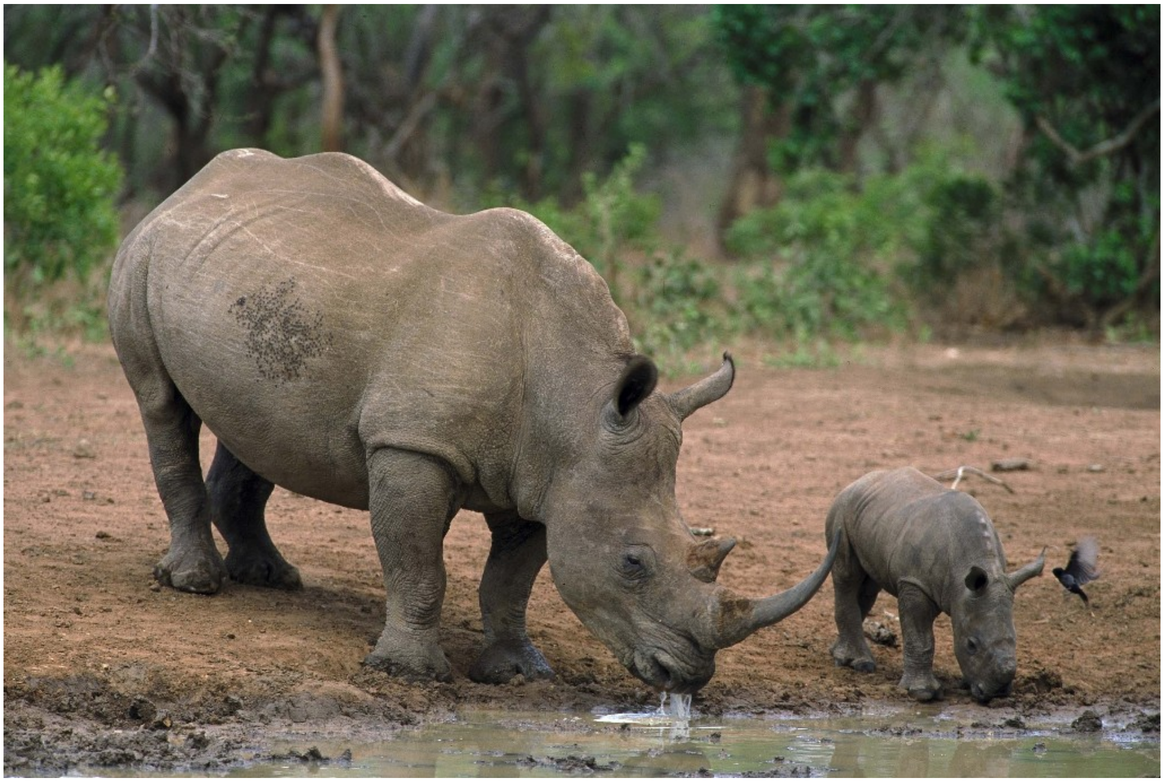
```
# unzip -v contraband.zip
Archive:  contraband.zip
 Length   Method    Size  Ratio   Date    Time    CRC-32    Name
--------  ------  ------- -----   ----    ----    ------    ----
  230665  Defl:N   230436   0%  04-26-04 17:00   936ebe65  rhino2.jpg
--------          -------  ---                             -------
  230665           230436   0%                             1 file

# unzip contraband.zip
Archive:  contraband.zip
[contraband.zip] rhino2.jpg password: <monkey>
```

(Use a password cracker)

SOLUTION (18)

rhino2.jpg
MD5:ed870202082ea4fd8f5488533a561b35



(matches image carved from USB key)

SOLUTION (19)

rhino.exe
MD5:d62d9989535c4c8db14e50b58c9f25a0

```
Microsoft DiskPart version 1.0
Copyright (C) 1999-2001 Microsoft Corporation.
On computer: TASSO

DISKPART> HELP

Microsoft DiskPart version 1.0

ADD         - Add a mirror to a simple volume.
ACTIVE      - Activates the current basic partition.
ASSIGN      - Assign a drive letter or mount point to…
BREAK       - Break a mirror set.
CLEAN       - Clear the configuration information, or all…
CONVERT     - Converts between different disk formats.
CREATE      - Create a volume or partition.
DELETE      - Delete an object.
DETAIL      - Provide details about an object.
EXIT        - Exit DiskPart
EXTEND      - Extend a volume.
HELP        - Prints a list of commands.
IMPORT      - Imports a disk group.
LIST        - Prints out a list of objects.
ONLINE      - Online a disk that is currently marked…
REM         - Does nothing. Used to comment scripts.
REMOVE      - Remove a drive letter or mount point assignment.
RESCAN      - Rescan the computer looking for disks…
RETAIN      - Place a retainer partition under a simple…
SELECT      - Move the focus to an object.

DISKPART>
```

SOLUTION (20)

Username/password for account “gnome” can be found by opening rhino.log (the first network trace), sorting packets in ascending order by protocol, then examining the telnet packets 1203-1247.

-------------STOP-----------

EVIDENCE FROM NETWORK TRACES:

rhino1.jpg, rhino3.jpg in rhino.log trace
[FTP transfers]

rhino2.jpg in contraband.zip file from rhino.log trace [encrypted, password = monkey]

rhino4.jpg, rhino5.gif in rhino2.log [HTTP transfer]

“rhino.exe” from rhino3.log
[Early version of MS DISKPART]

EVIDENCE FROM USB KEY dd IMAGE:

USB key containing images was reformatted

Now, only two gumbo recipes are undeleted

File carving results:

rhino6.jpg in alligator2.jpg

[stego jphide, password = gator]

rhino7.jpg in alligator3.jpg

[stego jphide, password = gumbo]

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

alligator1.jpg, alligator5.jpg are carve-able but irrelevant

“diary.doc” contains some answers to the questions

-----------PRIVATE-----------

Tools to install:

Linux:

tcpdump, ethereal
stegdetect/stegbreak, jphide/jpseek
zip cracker
foremost or scalpel file carvers
Sleuthkit

Windows:

windump, ethereal
stegdetect/stegbreak, jphide/jpseek
Paraben or similar for password cracking
foremost or scalpel file carvers
FTK and/or WinHex