# Module B8: File Recovery from Intercept Network Traffic Log.

## Pre-requisite Knowledge and Skills:

1. Understand basic of internet/network communication

## Learning Objectives

1. Understand the basic of internet communications.
2. Understand the risks of communication through internet.
3. Be exposed to methodology on communication interception and traffic log analysis.

## Recommended Running Environment/Tools:

1. Windows OS
2. Wireshark
3. xvi32.exe (the xvi32 folder)

## Material:

1. rhino.log
2. rhino2.log

## Video Lecture:

1. Network File Recovery

## Lab Assessment:

1. Network File Recovery Quiz

## Acknowledgement:

The log files, rhino.log and rhino2.log, are obtained from DFRWS 2005 Rodeo Challenge, https://www.dfrws.org/search

## Lab Instructions:

### 1. Scenario Description

You are chatting with your friends and transferred pictures by using a popular application (which uses ftp and http, a faked scenario). However, someone intercept your traffic by sniffing the communication signals and dumped into a few log files

- What you need to worry about?
- Can that person get the pictures you sent to your friends?
- How about login username and password?

**Tasks**

- Giving rhino.log and rhino2.log and wireshark tool
- Looking for password and user through FTP protocol
- Recover raw FTP transferred data (FTPData protocol, rhino.log)
    - Rhino1.jpg
- Recover http transferred data (rhino2.log, and xvi32.exe to edit)
    - Rhino4.jpg

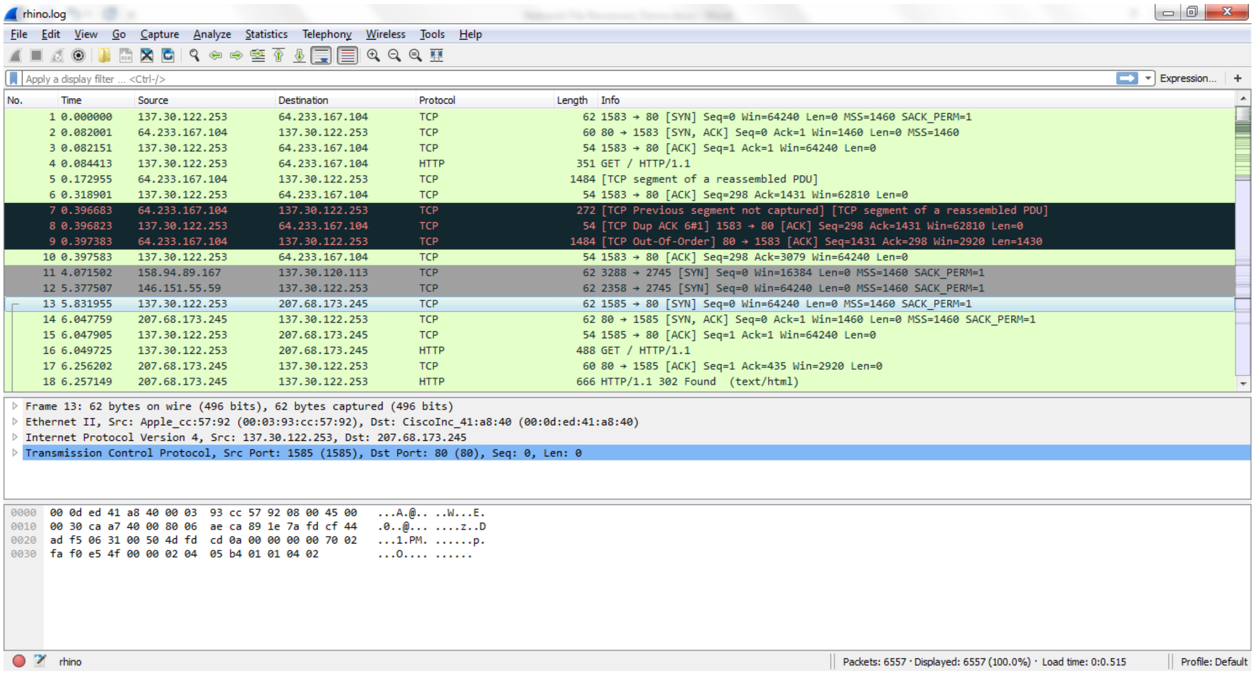
## 2. Assessment

- Recover a rhino5.gif file from the http transferred data (rhino2.log, the file signature is GIF89a).

## 3. Step by Step Instructions

### FTP Transmitted File Recovery

1. Load traffic log file into Wireshark for traffic analysis


rhino.log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

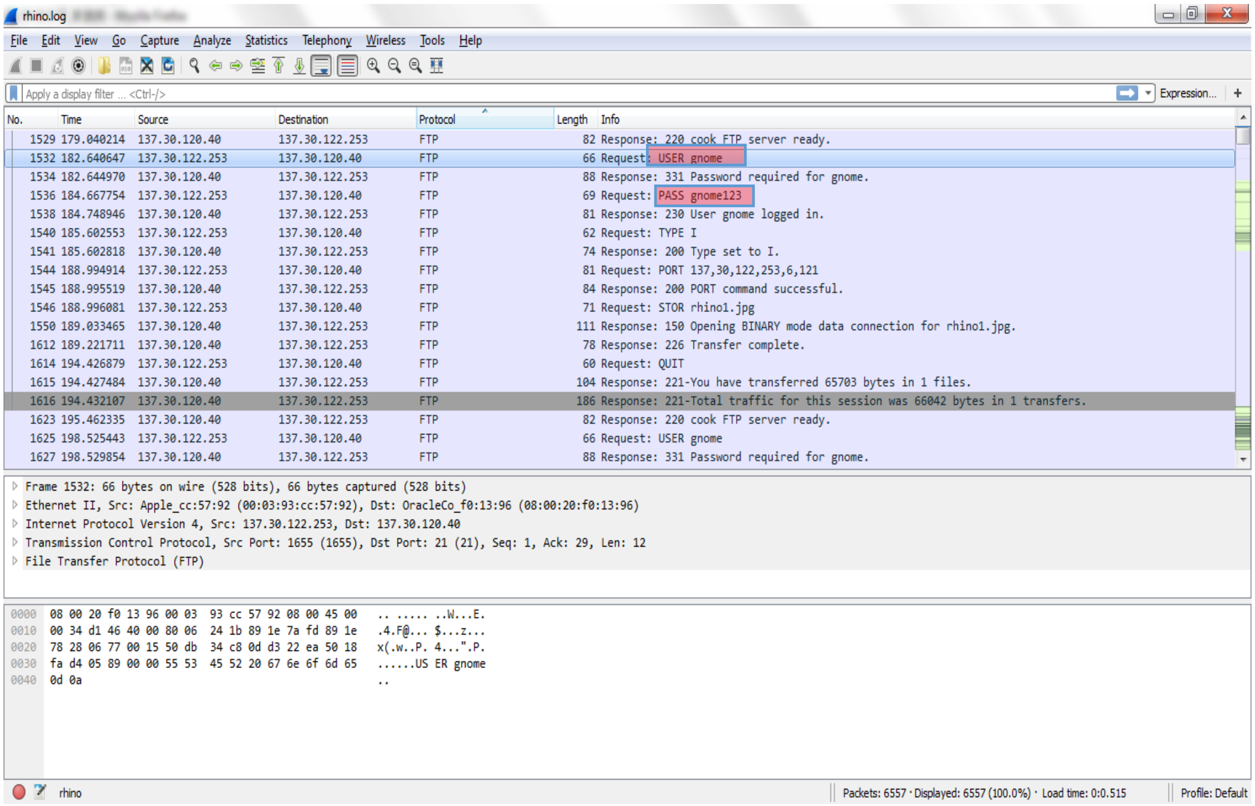
```
No.   Time      Source          Destination     Protocol  Length Info
    1 0.000000  137.30.122.253  64.233.167.104  TCP           62 1583 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
    2 0.082001  64.233.167.104  137.30.122.253  TCP           60 80 → 1583 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460
    3 0.082151  137.30.122.253  64.233.167.104  TCP           54 1583 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
    4 0.084413  137.30.122.253  64.233.167.104  HTTP         351 GET / HTTP/1.1
    5 0.172955  64.233.167.104  137.30.122.253  TCP         1484 [TCP segment of a reassembled PDU]
    6 0.318901  137.30.122.253  64.233.167.104  TCP           54 1583 → 80 [ACK] Seq=298 Ack=1431 Win=62810 Len=0
    7 0.396683  64.233.167.104  137.30.122.253  TCP          272 [TCP Previous segment not captured] [TCP segment of a reassembled PDU]
    8 0.396823  137.30.122.253  64.233.167.104  TCP           54 [TCP Dup ACK 6#1] 1583 → 80 [ACK] Seq=298 Ack=1431 Win=62810 Len=0
    9 0.397383  64.233.167.104  137.30.122.253  TCP         1484 [TCP Out-Of-Order] 80 → 1583 [ACK] Seq=1431 Ack=298 Win=2920 Len=1430
   10 0.397583  137.30.122.253  64.233.167.104  TCP           54 1583 → 80 [ACK] Seq=298 Ack=3079 Win=64240 Len=0
   11 4.071502  158.94.89.167   137.30.120.113  TCP           62 3288 → 2745 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
   12 5.377507  146.151.55.59   137.30.122.253  TCP           62 2358 → 2745 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
   13 5.831955  137.30.122.253  207.68.173.245  TCP           62 1585 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
   14 6.047759  207.68.173.245  137.30.122.253  TCP           62 80 → 1585 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460 SACK_PERM=1
   15 6.047905  137.30.122.253  207.68.173.245  TCP           54 1585 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   16 6.049725  137.30.122.253  207.68.173.245  HTTP         488 GET / HTTP/1.1
   17 6.256202  207.68.173.245  137.30.122.253  TCP           60 80 → 1585 [ACK] Seq=1 Ack=435 Win=2920 Len=0
   18 6.257149  207.68.173.245  137.30.122.253  HTTP         666 HTTP/1.1 302 Found  (text/html)
```

```
▷ Frame 13: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▷ Ethernet II, Src: Apple_cc:57:92 (00:03:93:cc:57:92), Dst: CiscoInc_41:a8:40 (00:0d:ed:41:a8:40)
▷ Internet Protocol Version 4, Src: 137.30.122.253, Dst: 207.68.173.245
▷ Transmission Control Protocol, Src Port: 1585 (1585), Dst Port: 80 (80), Seq: 0, Len: 0
```

```
0000  00 0d ed 41 a8 40 00 03  93 cc 57 92 08 00 45 00   ...A.@.. ..W...E.
0010  00 30 ca a7 40 00 80 06  ae ca 89 1e 7a fd cf 44   .0..@... ....z..D
0020  ad f5 06 31 00 50 4d fd  cd 0a 00 00 00 00 70 02   ...1.PM. ......p.
0030  fa f0 e5 4f 00 00 02 04  05 b4 01 01 04 02         ...O.... ......
```

```
rhino    Packets: 6557 · Displayed: 6557 (100.0%) · Load time: 0:0.515    Profile: Default
```

2. Identify clear text user name and password for FTP login


rhino.log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

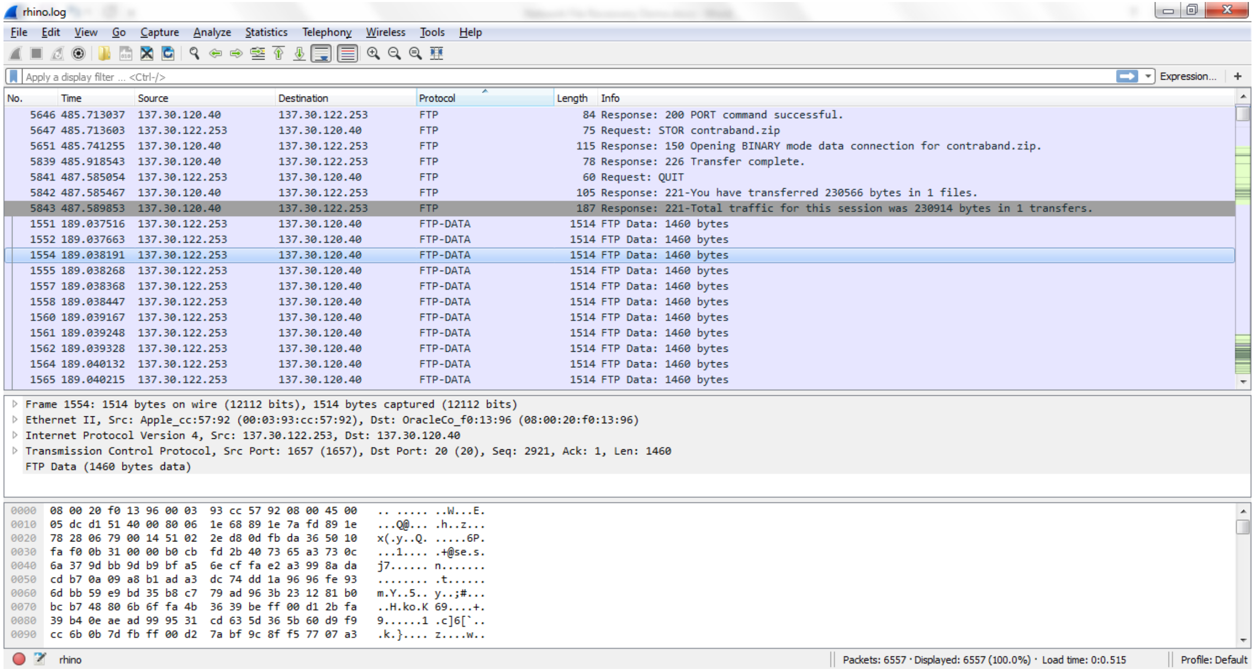
```
No.  Time        Source          Destination     Protocol  Length Info
1529 179.040214  137.30.120.40   137.30.122.253  FTP           82 Response: 220 cook FTP server ready.
1532 182.640647  137.30.122.253  137.30.120.40   FTP           66 Request: USER gnome
1534 182.644970  137.30.120.40   137.30.122.253  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: OracleCo_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 (1655), Dst Port: 21 (21), Seq: 1, Ack: 29, Len: 12
▷ File Transfer Protocol (FTP)
```

```
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                                              ..
```

```
rhino        Packets: 6557 · Displayed: 6557 (100.0%) · Load time: 0:0.515        Profile: Default
```

3. Locate FTP-DATA protocol – the first file transferred by FTP-DATA protocol


rhino.log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

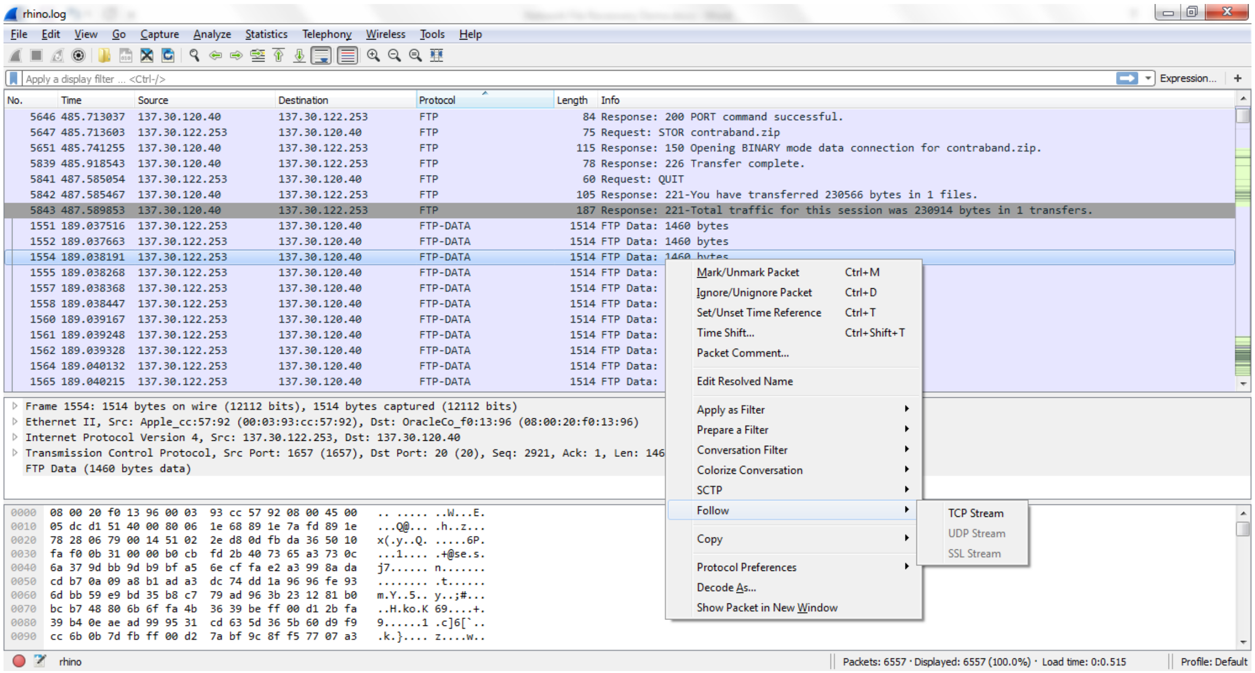
```
No.  Time        Source          Destination     Protocol  Length Info
5646 485.713037  137.30.120.40   137.30.122.253  FTP           84 Response: 200 PORT command successful.
5647 485.713603  137.30.122.253  137.30.120.40   FTP           75 Request: STOR contraband.zip
5651 485.741255  137.30.120.40   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.
1551 189.037516  137.30.122.253  137.30.120.40   FTP-DATA    1514 FTP Data: 1460 bytes
1552 189.037663  137.30.122.253  137.30.120.40   FTP-DATA    1514 FTP Data: 1460 bytes
1554 189.038191  137.30.122.253  137.30.120.40   FTP-DATA    1514 FTP Data: 1460 bytes
1555 189.038268  137.30.122.253  137.30.120.40   FTP-DATA    1514 FTP Data: 1460 bytes
1557 189.038368  137.30.122.253  137.30.120.40   FTP-DATA    1514 FTP Data: 1460 bytes
1558 189.038447  137.30.122.253  137.30.120.40   FTP-DATA    1514 FTP Data: 1460 bytes
1560 189.039167  137.30.122.253  137.30.120.40   FTP-DATA    1514 FTP Data: 1460 bytes
1561 189.039248  137.30.122.253  137.30.120.40   FTP-DATA    1514 FTP Data: 1460 bytes
1562 189.039328  137.30.122.253  137.30.120.40   FTP-DATA    1514 FTP Data: 1460 bytes
1564 189.040132  137.30.122.253  137.30.120.40   FTP-DATA    1514 FTP Data: 1460 bytes
1565 189.040215  137.30.122.253  137.30.120.40   FTP-DATA    1514 FTP Data: 1460 bytes
```

```
▷ Frame 1554: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
▷ Ethernet II, Src: Apple_cc:57:92 (00:03:93:cc:57:92), Dst: OracleCo_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: 1657 (1657), Dst Port: 20 (20), Seq: 2921, Ack: 1, Len: 1460
  FTP Data (1460 bytes data)
```

```
0000  08 00 20 f0 13 96 00 03  93 cc 57 92 08 00 45 00   .. ..... ..W...E.
0010  05 dc d1 51 40 00 80 06  1e 68 89 1e 7a fd 89 1e   ...Q@... .h..z...
0020  78 28 06 79 00 14 51 02  2e d8 0d fb da 36 50 10   x(.y..Q. .....6P.
0030  fa f0 0b 31 00 00 b0 cb  fd 2b 40 73 65 a3 73 0c   ...1.... .+@se.s.
0040  6a 37 9d bb 9d b9 bf a5  6e cf fa e2 a3 99 8a da   j7...... n.......
0050  cd b7 0a 09 a8 b1 ad a3  dc 74 dd 1a 96 96 fe 93   ........ .t......
0060  6d bb 59 e9 bd 35 b8 c7  79 ad 96 3b 23 12 81 b0   m.Y..5.. y..;#...
0070  bc b7 48 80 6b 6f fa 4b  36 39 be ff 00 d1 2b fa   ..H.ko.K 69....+.
0080  39 b4 0e ae ad 99 95 31  cd 63 5d 36 5b 60 d9 f9   9......1 .c]6[`..
0090  cc 6b 0b 7d fb ff 00 d2  7a bf 9c 8f f5 77 07 a3   .k.}.... z....w..
```

```
rhino        Packets: 6557 · Displayed: 6557 (100.0%) · Load time: 0:0.515        Profile: Default
```

4. Right click and choose follow TCP stream --- to recover a file transmitted by FTP-DATA


rhino.log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
TCP Stream
UDP Stream
SSL Stream
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
rhino
Packets: 6557 · Displayed: 6557 (100.0%) · Load time: 0:0.515
Profile: Default

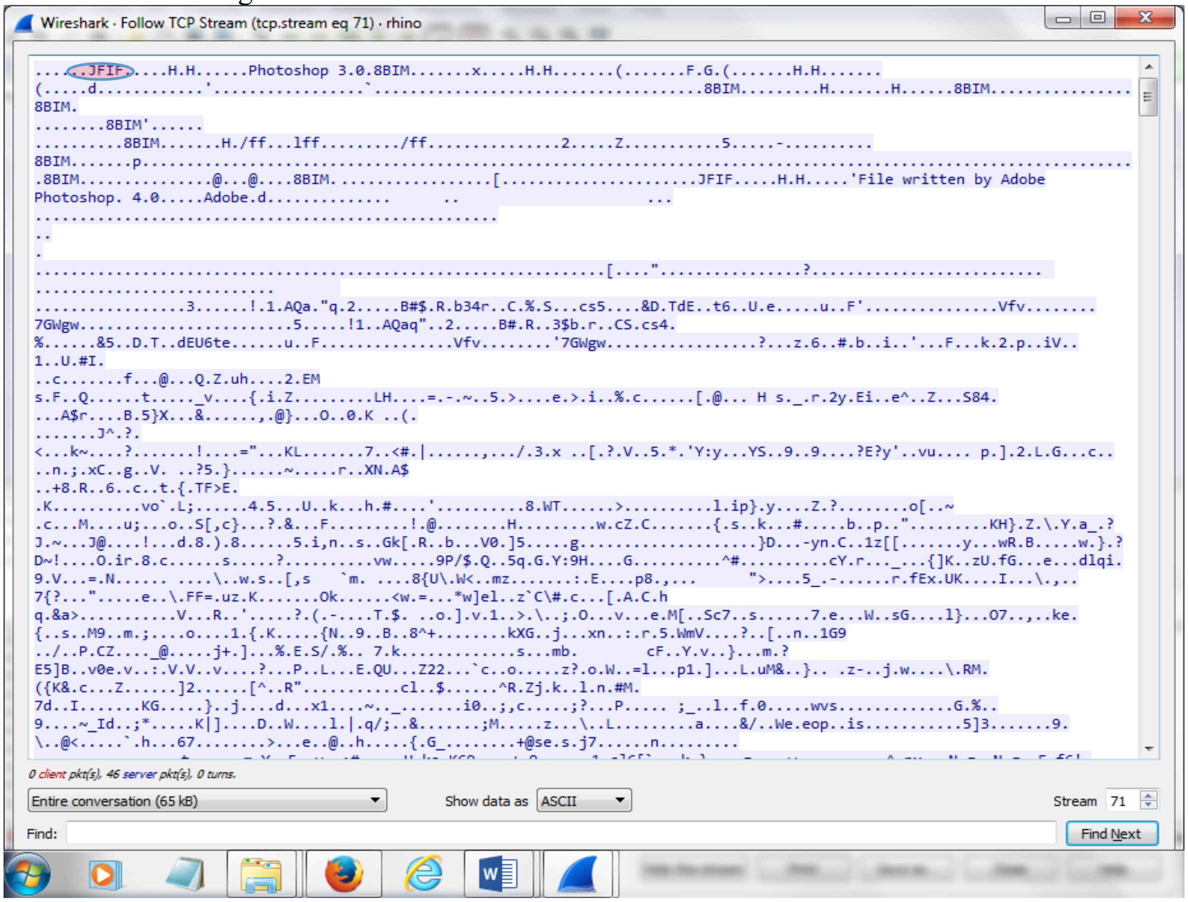
```
No.  Time        Source          Destination     Protocol   Length Info
5646 485.713037  137.30.120.40   137.30.122.253  FTP          84 Response: 200 PORT command successful.
5647 485.713603  137.30.122.253  137.30.120.40   FTP          75 Request: STOR contraband.zip
5651 485.741255  137.30.120.40   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.
1551 189.037516  137.30.122.253  137.30.120.40   FTP-DATA   1514 FTP Data: 1460 bytes
1552 189.037663  137.30.122.253  137.30.120.40   FTP-DATA   1514 FTP Data: 1460 bytes
1554 189.038191  137.30.122.253  137.30.120.40   FTP-DATA   1514 FTP Data: 1460 bytes
1555 189.038268  137.30.122.253  137.30.120.40   FTP-DATA   1514 FTP Data:
1557 189.038368  137.30.122.253  137.30.120.40   FTP-DATA   1514 FTP Data:
1558 189.038447  137.30.122.253  137.30.120.40   FTP-DATA   1514 FTP Data:
1560 189.039167  137.30.122.253  137.30.120.40   FTP-DATA   1514 FTP Data:
1561 189.039248  137.30.122.253  137.30.120.40   FTP-DATA   1514 FTP Data:
1562 189.039328  137.30.122.253  137.30.120.40   FTP-DATA   1514 FTP Data:
1564 189.040132  137.30.122.253  137.30.120.40   FTP-DATA   1514 FTP Data:
1565 189.040215  137.30.122.253  137.30.120.40   FTP-DATA   1514 FTP Data:
```

```
▷ Frame 1554: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
▷ Ethernet II, Src: Apple_cc:57:92 (00:03:93:cc:57:92), Dst: OracleCo_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: 1657 (1657), Dst Port: 20 (20), Seq: 2921, Ack: 1, Len: 146
  FTP Data (1460 bytes data)
```

```
0000  08 00 20 f0 13 96 00 03  93 cc 57 92 08 00 45 00   .. ..... ..W...E.
0010  05 dc d1 51 40 00 80 06  1e 68 89 1e 7a fd 89 1e   ...Q@... .h..z...
0020  78 28 06 79 00 14 51 02  2e d8 0d fb da 36 50 10   x(.y..Q. .....6P.
0030  fa f0 0b 31 00 00 b0 cb  fd 2b 40 73 65 a3 73 0c   ...1.... .+@se.s.
0040  6a 37 9d bb 9d b9 bf a5  6e cf fa e2 a3 99 8a da   j7...... n.......
0050  cd b7 0a 09 a8 b1 ad a3  dc 74 dd 1a 96 96 fe 93   ........ .t......
0060  6d bb 59 e9 bd 35 b8 c7  79 ad 96 3b 23 12 81 b0   m.Y..5.. y..;#...
0070  bc b7 48 80 6b 6f fa 4b  36 39 be ff 00 d1 2b fa   ..H.ko.K 69....+.
0080  39 b4 0e ae ad 99 95 31  cd 63 5d 36 5b 60 d9 f9   9......1 .c]6[`..
0090  cc 6b 0b 7d fb ff 00 d2  7a bf 9c 8f f5 77 07 a3   .k.}.... z....w..
```

5. The raw file recovered—file transferred by FTP-DATA

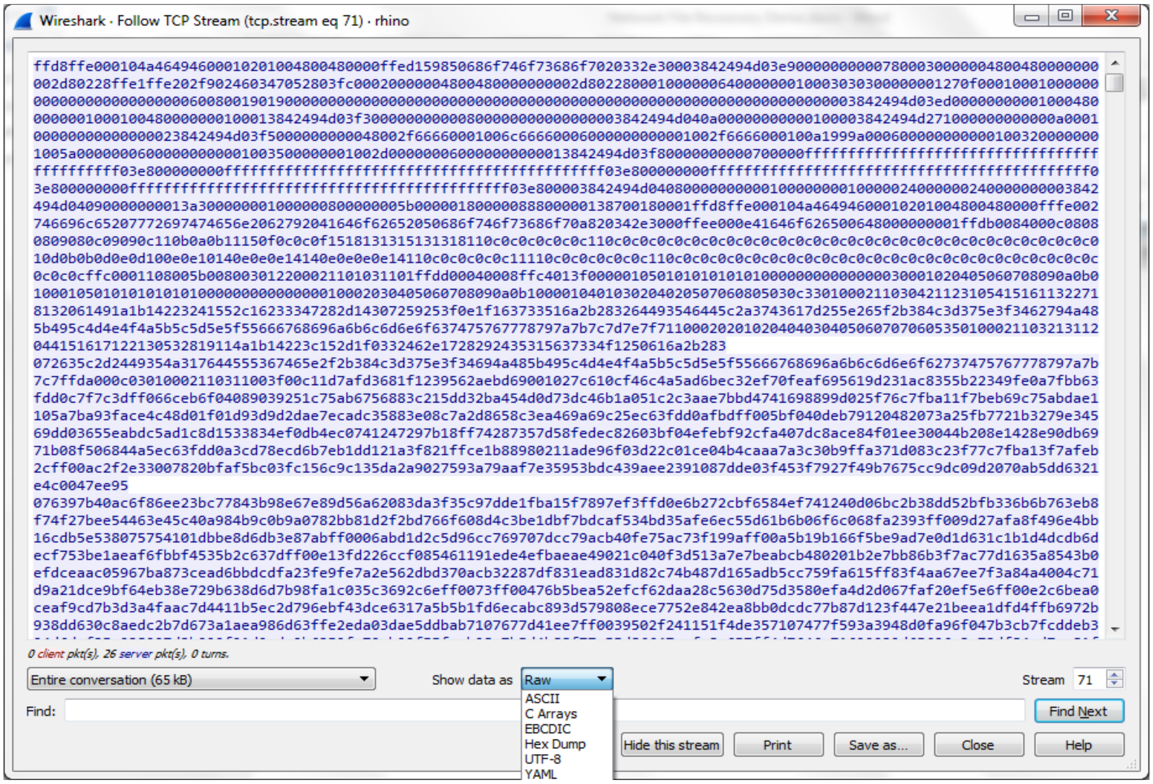
Note the JFIF file signature from BYTE 6 to BYTE 9


Wireshark · Follow TCP Stream (tcp.stream eq 71) · rhino
Entire conversation (65 kB)
Show data as
ASCII
Stream
71
Find:
Find Next

```
......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$r....B.5}X...&......,.@}...O..0.K ..(.
.......J^.?.
<...k~....?.......!....="...KL.......7..<#.|......,.../.3.x ..[.?.V..5.*.'Y:y...YS..9..9....?E?y'..vu.... p.].2.L.G...c..
..n.;.xC..g..V. ..?5.}......~.....r..XN.A$
..+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...V0.]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.....}..j....d...x1....~.._........i0..;,c.....;?...P.....  ;_..l..f.0.....wvs.............G.%..
9....~_Id..;*.....K|]....D..W....l.|.q/;..&.......;M.....z...\..L..........a....&/..We.eop..is...........5]3.......9.
\..@<.....`.h...67.........>...e..@..h.....{.G_.........+@se.s.j7......n.........
```

*0 client pkt(s), 46 server pkt(s), 0 turns.*

6. Save the file to a RAW format



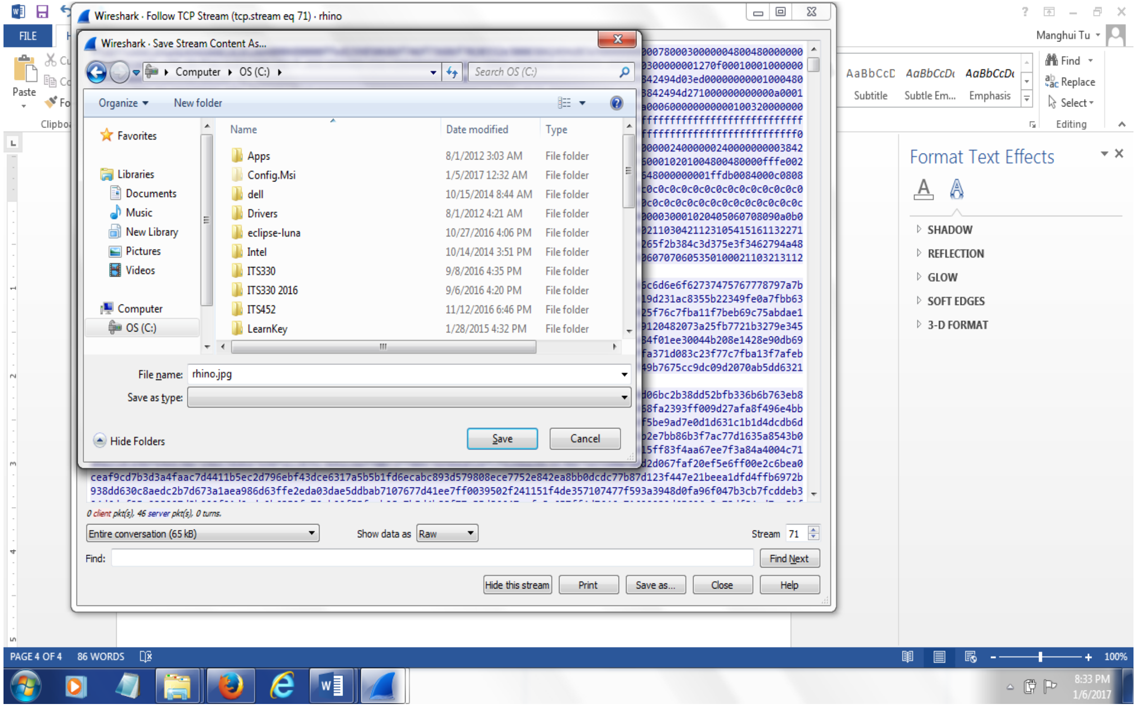
Wireshark · Follow TCP Stream (tcp.stream eq 71) · rhino

```
ffd8ffe000104a46494600010201004800480000ffed159850686f746f73686f7020332e30003842494d03e9000000000007800030000004800480000000
002d80228ffe1ffe202f902460347052803fc00020000004800480000000002d80228000100000064000000010003030300000001270f00010001000000
0000000000000000006008001901900000000000000000000000000000000000000000000000000000000000000003842494d03ed0000000001000480
000000100010048000000010001384249d03f3000000000080000000000000003842494d040a0000000000010003842494d2710000000000000a0001
000000000000002384249d03f50000000000048002f66660001006c666600060000000000001002f6666000100a1999a00060000000000000100320000000
1005a00000006000000000000100350000000001002d000000060000000000013842494d03f80000000000700000ffffffffffffffffffffffffffffffff
fffffffff03e800000000ffffffffffffffffffffffffffffffffffffffffffffff03e800000000ffffffffffffffffffffffffffffffffffffffffffffffff0
3e800000000ffffffffffffffffffffffffffffffffffffffffffffff03e80003842494d04080000000000010000000010000240000000240000000003842
494d04090000000000013a30000000100000080000005b000001800000888000001387001800 01ffd8ffe000104a46494600010201004800480000fffe002
746696c6520777269747474656e2062792041646f62652050686f746f73686f70a820342e3000ffee000e41646f626500648000000001ffdb0084000c0808
0809080c09090c110b0a0b11150f0c0c0f151813131515131318110c0c0c0c0c110c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0
10d0b0b0d0e0d100e0e10140e0e0e14140e0e0e0e14110c0c0c0c0c11110c0c0c0c0c110c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c
0c0c0cffc0001108005b008003012200021101031101ffdd00040008ffc4013f000001050101010101010000000000000003000102040506070809 0a0b0
100010501010101010100000000000000010002030405060708090a0b1000010401030204020507060805030c33010002110304211231054151611322 71
8132061491a1b14223241552c16233347282d14307259253f0e1f163733516a2b283264493546445c2a3743617d255e265f2b384c3d375e3f3462794a48
5b495c4d4e4f4a5b5c5d5e5f55666768696a6b6c6d6e6f637475767778797a7b7c7d7e7f711000202010204040304050607070605350100021103213112
04415161712213053281911 4a1b14223c152d1f0332462e1728292435315637334f1250616a2b283
072635c2d2449354a317644555367465e2f2b384c3d375e3f34694a485b495c4d4e4f4a5b5c5d5e5f55666768696a6b6c6d6e6f627374757677787 97a7b
7c7ffda000c03010002110311003f00c11d7afd3681f1239562aebd69001027c610cf46c4a5ad6bec32ef70feaf695619d231ac8355b22349fe0a7fbb63
fdd0c7f7c3dff066ceb6f04089039251c75ab6756883c215dd32ba454d0d73dc46b1a051c2c3aae7bbd4741698899d025f76c7fba11f7beb69c75abdae1
105a7ba93face4c48d01f01d93d9d2dae7ecadc35883e08c7a2d8658c3ea469a69c25ec63fdd0afbdff005bf040deb79120482073a25fb7721b3279e345
69dd03655eabdc5ad1c8d1533834ef0db4ec0741247297b18ff74287357d58fedec82603bf04efebf92cfa407dc8ace84f01ee30044b208e1428e90db69
71b08f506844a5ec63fdd0a3cd78ecd6b7eb1dd121a3f821ffce1b88980211ade96f03d22c01ce04b4caaa7a3c30b9ffa371d083c23f77c7fba13f7afeb
2cff00ac2f2e33007820bfaf5bc03fc156c9c135da2a9027593a79aaf7e35953bdc439aee2391087dde03f453f7927f49b7675cc9dc09d2070ab5dd6321
e4c0047ee95
076397b40ac6f86ee23bc77843b98e67e89d56a62083da3f35c97dde1fba15f7897ef3ffd0e6b272cbf6584ef741240d06bc2b38dd52bfb336b6b763eb8
f74f27bee54463e45c40a984b9c0b9a0782bb81d2f2bd766f608d4c3be1dbf7bdcaf534bd35afe6ec55d61b6b06f6c068fa2393ff009d27afa8f496e4bb
16cdb5e538075754101dbbe8d6db3e87abff0006abd1d2c5d96cc769707dcc79acb40fe75ac73f199aff00a5b19b166f5be9ad7e0d1d631c1b1d4dcdb6d
ecf753be1aeaf6fbbf4535b2c637dff00e13fd226ccf085461191ede4efbaeae49021c040f3d513a7e7beabcb480201b2e7bb86b3f7ac77d1635a8543b0
efdceaac05967ba873cead6bbdcdfa23fe9fe7a2e562dbd370acb32287df831ead831d82c74b487d165adb5cc759fa615ff83f4aa67ee7f3a84a4004c71
d9a21dce9bf64eb38e729b638d6d7b98fa1c035c3692c6eff0073ff00476b5bea52efcf62daa28c5630d75d3580efa4d2d067faf20ef5e6ff00e2c6bea0
ceaf9cd7b3d3a4faac7d4411b5ec2d796ebf43dce6317a5b5b1fd6ecabc893d579808ece7752e842ea8bb0dcdc77b87d123f447e21beea1dfd4ffb6972b
938dd630c8aedc2b7d673a1aea986d63ffe2eda03dae5ddbab7107677d41ee7ff0039502f241151f4de357107477f593a3948d0fa96f047b3cb7fcddeb3
```

*0 client pkt(s), 26 server pkt(s), 0 turns.*

Entire conversation (65 kB) | Show data as: Raw | Stream: 71

7. Save file as rhino.jpg –



Wireshark · Follow TCP Stream (tcp.stream eq 71) · rhino

Wireshark · Save Stream Content As...

Computer ▸ OS (C:) ▸

| Name | Date modified | Type |
|---|---|---|
| Apps | 8/1/2012 3:03 AM | File folder |
| Config.Msi | 1/5/2017 12:32 AM | File folder |
| dell | 10/15/2014 8:44 AM | File folder |
| Drivers | 8/1/2012 4:21 AM | File folder |
| eclipse-luna | 10/27/2016 4:06 PM | File folder |
| Intel | 10/14/2014 3:51 PM | File folder |
| ITS330 | 9/8/2016 4:35 PM | File folder |
| ITS330 2016 | 9/6/2016 4:20 PM | File folder |
| ITS452 | 11/12/2016 6:46 PM | File folder |
| LearnKey | 1/28/2015 4:32 PM | File folder |

File name: rhino.jpg

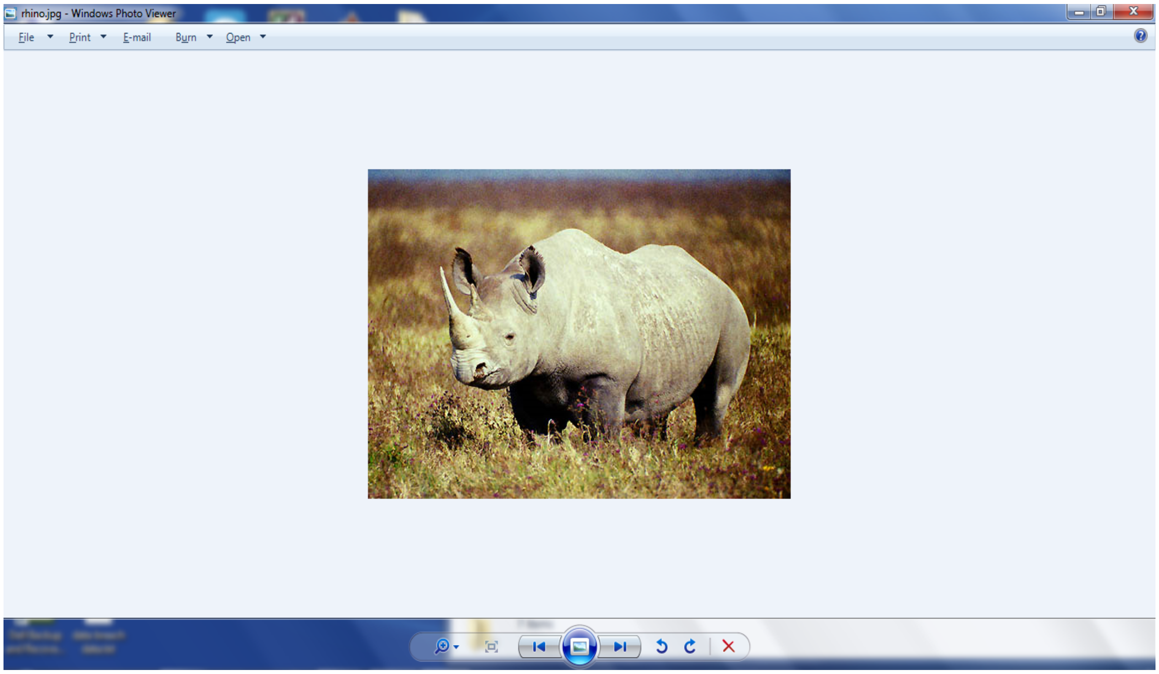
Save as type:

ceaf9cd7b3d3a4faac7d4411b5ec2d796ebf43dce6317a5b5b1fd6ecabc893d579808ece7752e842ea8bb0dcdc77b87d123f447e21beea1dfd4ffb6972b
938dd630c8aedc2b7d673a1aea986d63ffe2eda03dae5ddbab7107677d41ee7ff0039502f241151f4de357107477f593a3948d0fa96f047b3cb7fcddeb3

*0 client pkt(s), 46 server pkt(s), 0 turns.*

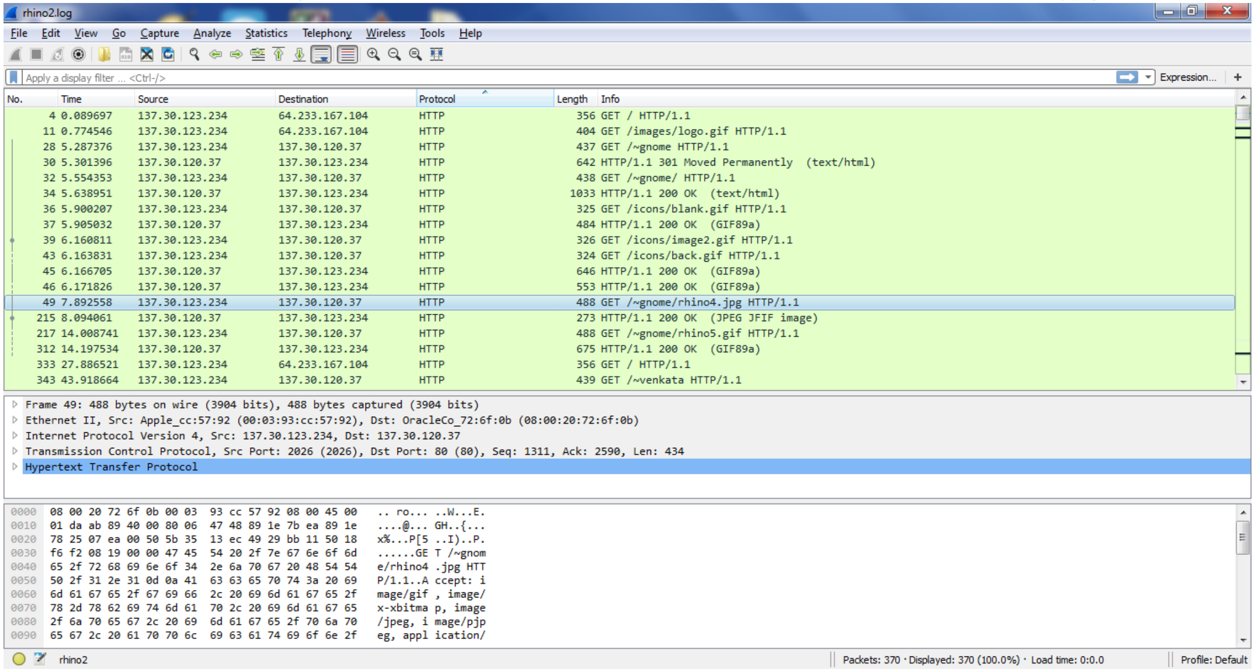
Entire conversation (65 kB) | Show data as: Raw | Stream: 71

8. Locate the file rhino.jpg and double click



## HTTP Transmitted File Recovery

1. Open rhino2.log file in Wireshark and sort http protocol, and locate rhino4.jpg

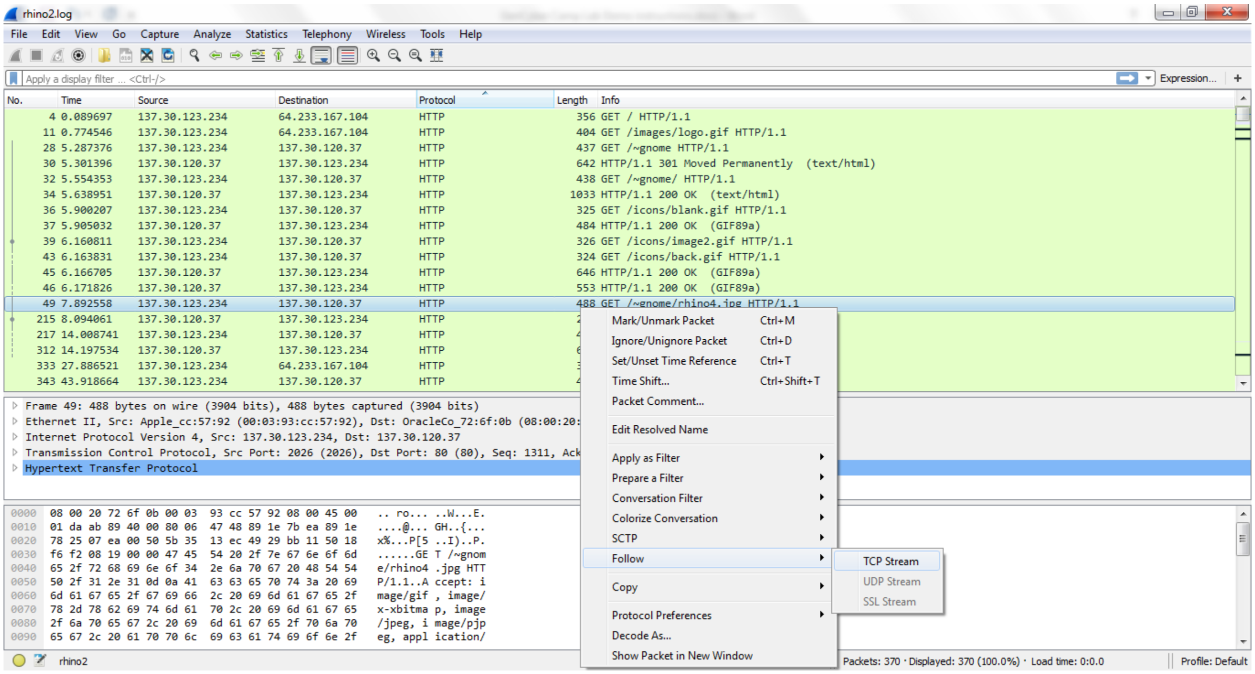


| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 4 | 0.089697 | 137.30.123.234 | 64.233.167.104 | HTTP | 356 | GET / HTTP/1.1 |
| 11 | 0.774546 | 137.30.123.234 | 64.233.167.104 | HTTP | 404 | GET /images/logo.gif HTTP/1.1 |
| 28 | 5.287376 | 137.30.123.234 | 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) |
| 333 | 27.886521 | 137.30.123.234 | 64.233.167.104 | HTTP | 356 | GET / HTTP/1.1 |
| 343 | 43.918664 | 137.30.123.234 | 137.30.120.37 | HTTP | 439 | GET /~venkata HTTP/1.1 |

```
▷ Frame 49: 488 bytes on wire (3904 bits), 488 bytes captured (3904 bits)
▷ Ethernet II, Src: Apple_cc:57:92 (00:03:93:cc:57:92), Dst: OracleCo_72:6f:0b (08:00:20:72:6f:0b)
▷ Internet Protocol Version 4, Src: 137.30.123.234, Dst: 137.30.120.37
▷ Transmission Control Protocol, Src Port: 2026 (2026), Dst Port: 80 (80), Seq: 1311, Ack: 2590, Len: 434
▷ Hypertext Transfer Protocol
```

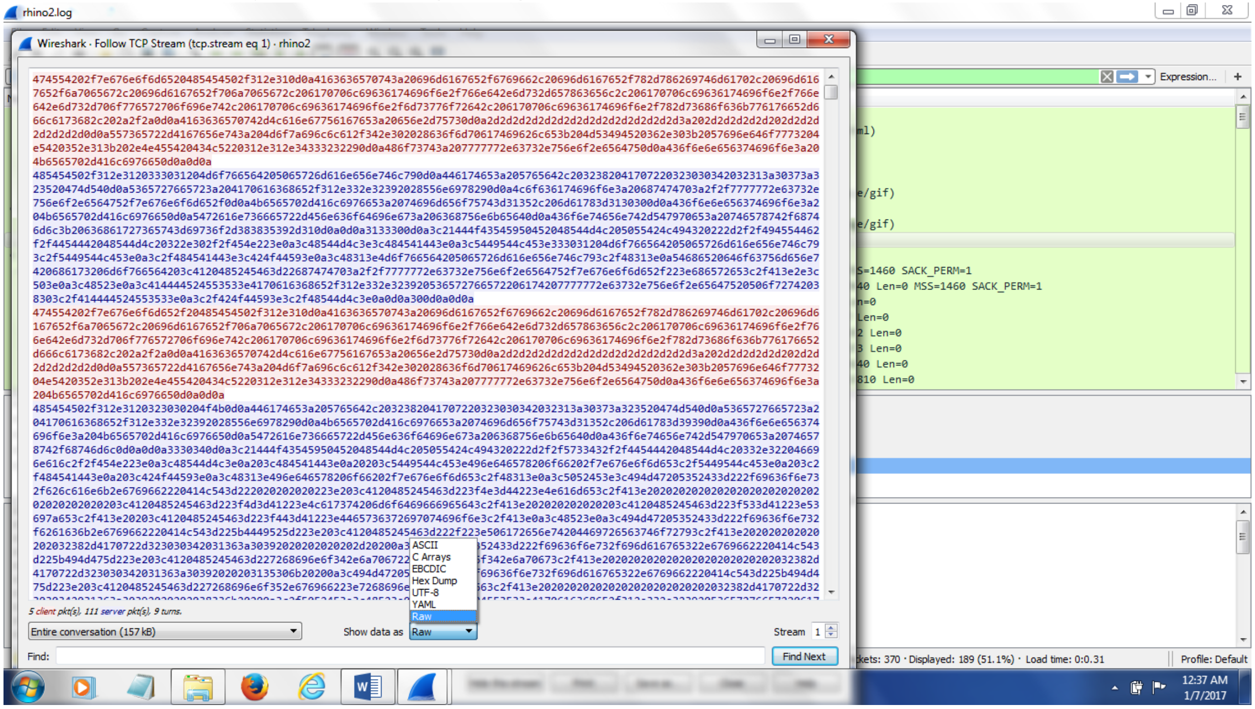
```
0000  08 00 20 72 6f 0b 00 03  93 cc 57 92 08 00 45 00   .. ro... ..W...E.
0010  01 da ab 89 40 00 80 06  47 48 89 1e 7b ea 89 1e   ....@... GH..{...
0020  78 25 07 ea 00 50 5b 35  13 ec 49 29 bb 11 50 18   x%...P[5 ..I)..P.
0030  f6 f2 08 19 00 00 47 45  54 20 2f 7e 67 6e 6f 6d   ......GE T /~gnom
0040  65 2f 72 68 69 6e 6f 34  2e 6a 70 67 20 48 54 54   e/rhino4 .jpg HTT
0050  50 2f 31 2e 31 0d 0a 41  63 63 65 70 74 3a 20 69   P/1.1..A ccept: i
0060  6d 61 67 65 2f 67 69 66  2c 20 69 6d 61 67 65 2f   mage/gif , image/
0070  78 2d 78 62 69 74 6d 61  70 2c 20 69 6d 61 67 65   x-xbitma p, image
0080  2f 6a 70 65 67 2c 20 69  6d 61 67 65 2f 70 6a 70   /jpeg, i mage/pjp
0090  65 67 2c 20 61 70 70 6c  69 63 61 74 69 6f 6e 2f   eg, appl ication/
```

2. Follow TCP stream to recover this file


rhino2.log
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream
UDP Stream
SSL Stream
rhino2
Packets: 370 · Displayed: 370 (100.0%) · Load time: 0:0.0
Profile: Default

```
No.   Time        Source           Destination      Protocol  Length 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
  217 14.008741   137.30.123.234   137.30.120.37    HTTP
  312 14.197534   137.30.120.37    137.30.123.234   HTTP
  333 27.886521   137.30.123.234   64.233.167.104   HTTP
  343 43.918664   137.30.123.234   137.30.120.37    HTTP

▷ Frame 49: 488 bytes on wire (3904 bits), 488 bytes captured (3904 bits)
▷ Ethernet II, Src: Apple_cc:57:92 (00:03:93:cc:57:92), Dst: OracleCo_72:6f:0b (08:00:20:
▷ Internet Protocol Version 4, Src: 137.30.123.234, Dst: 137.30.120.37
▷ Transmission Control Protocol, Src Port: 2026 (2026), Dst Port: 80 (80), Seq: 1311, Ack
▷ Hypertext Transfer Protocol

0000  08 00 20 72 6f 0b 00 03  93 cc 57 92 08 00 45 00   .. ro... ..W...E.
0010  01 da ab 89 40 00 80 06  47 48 89 1e 7b ea 89 1e   ....@... GH..{...
0020  78 25 07 ea 00 50 5b 35  13 ec 49 29 bb 11 50 18   x%...P[5 ..I)..P.
0030  f6 f2 08 19 00 00 47 45  54 20 2f 7e 67 6e 6f 6d   ......GE T /~gnom
0040  65 2f 72 68 69 6e 6f 34  2e 6a 70 67 20 48 54 54   e/rhino4 .jpg HTT
0050  50 2f 31 2e 31 0d 0a 41  63 63 65 70 74 3a 20 69   P/1.1..A ccept: i
0060  6d 61 67 65 2f 67 69 66  2c 20 69 6d 61 67 65 2f   mage/gif , image/
0070  78 2d 78 62 69 74 6d 61  70 2c 20 69 6d 61 67 65   x-xbitma p, image
0080  2f 6a 70 65 67 2c 20 69  6d 61 67 65 2f 70 6a 70   /jpeg, i mage/pjp
0090  65 67 2c 20 61 70 70 6c  69 63 61 74 69 6f 6e 2f   eg, appl ication/
```

3. Save the file as raw to rhino4.jpg, compare the raw format and ASCII format (http? Not JFIF from byte 6 at the beginning)



```
474554202f7e676e6f6d6520485454502f312e310d0a4163636570743a20696d6167652f6769662c20696d6167652f782d786269746d61702c20696d616
7652f6a7065672c20696d6167652f706a7065672c206170706c69636174696f6e2f766e642e6d732d657863656c2c206170706c69636174696f6e2f766e
642e6d732d706f776572706f696e742c206170706c69636174696f6e2f6d73776f72642c206170706c69636174696f6e2f782d73686f636b776176652d6
66c6173682c202a2f2a0d0a4163636570742d4c616e67756167653a20656e2d75730d0a2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d3a202d2d2d2d2d202d2d2d
2d2d2d2d0d0a557365722d4167656e743a204d6f7a696c6c612f342e302028636f6d70617469626c653b204d53494520362e303b2057696e646f7773204
e5420352e313b202e4e455420434c5220312e312e34333232290d0a486f73743a207777772e63732e756e6f2e6564750d0a436f6e6e656374696f6e3a20
4b6565702d416c6976650d0a0d0a
485454502f312e3120333031204d6f766564205065726d616e656e746c790d0a446174653a205765642c2032382041707220323030342032313a30373a3
23520474d540d0a5365727665723a204170616368652f312e332e32392028556e6978290d0a4c6f636174696f6e3a20687474703a2f2f7777772e63732e
756e6f2e6564752f7e676e6f6d652f0d0a4b6565702d416c6976653a2074696d656f75743d31352c206d61783d3130300d0a436f6e6e656374696f6e3a2
04b6565702d416c6976650d0a5472616e736665722d456e636f64696e673a206368756e6b65640d0a436f6e74656e742d547970653a20746578742f6874
6d6c3b20636861727365743d69736f2d383835392d310d0a0d0a3133300d0a3c21444f43545950452048544d4c205055424c494320222d2f2f494554462
f2f4454442048544d4c20322e302f2f454e223e0a3c48544d4c3e3c484541443e0a3c5449544c453e333031204d6f766564205065726d616e656e746c79
3c2f5449544c453e0a3c2f484541443e3c424f44593e0a3c48313e4d6f766564205065726d616e656e746c793c2f48313e0a54686520646f63756d656e7
420686173206d6f766564203c4120485245463d22687474703a2f2f7777772e63732e756e6f2e6564752f7e676e6f6d652f223e686572653c2f413e2e3c
503e0a3c48523e0a3c414444524553533e4170616368652f312e332e3239205365727665722061742077777772e63732e756e6f2e65647520506f7274203
8303c2f414444524553533e0a3c2f424f44593e3c2f48544d4c3e0a0d0a300d0a0d0a
474554202f7e676e6f6d652f20485454502f312e310d0a4163636570743a20696d6167652f6769662c20696d6167652f782d786269746d61702c20696d6
167652f6a7065672c20696d6167652f706a7065672c206170706c69636174696f6e2f766e642e6d732d657863656c2c206170706c69636174696f6e2f76
6e642e6d732d706f776572706f696e742c206170706c69636174696f6e2f6d73776f72642c206170706c69636174696f6e2f782d73686f636b776176652
d666c6173682c202a2f2a0d0a4163636570742d4c616e67756167653a20656e2d75730d0a2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d3a202d2d2d2d2d202d2d
2d2d2d2d2d0d0a557365722d4167656e743a204d6f7a696c6c612f342e302028636f6d70617469626c653b204d53494520362e303b2057696e646f77732
04e5420352e313b202e4e455420434c5220312e312e34333232290d0a486f73743a207777772e63732e756e6f2e6564750d0a436f6e6e656374696f6e3a
204b6565702d416c6976650d0a0d0a
485454502f312e3120323030204f4b0d0a446174653a205765642c2032382041707220323030342032313a30373a323520474d540d0a5365727665723a2
04170616368652f312e332e32392028556e6978290d0a4b6565702d416c6976653a2074696d656f75743d31352c206d61783d39390d0a436f6e6e656374
696f6e3a204b6565702d416c6976650d0a5472616e736665722d456e636f64696e673a206368756e6b65640d0a436f6e74656e742d547970653a2074657
8742f68746d6c0d0a0d0a3330340d0a3c21444f43545950452048544d4c205055424c494320222d2f2f5733432f2f4454442048544d4c20332e32204669
6e616c2f2f454e223e0a3c48544d4c3e0a203c484541443e0a20203c5449544c453e496e646578206f66202f7e676e6f6d653c2f5449544c453e0a203c2
f484541443e0a203c424f44593e0a3c48313e496e646578206f66202f7e676e6f6d653c2f48313e0a3c5052453e3c494d47205352433d222f69636f6e73
2f626c616e6b2e6769662220414c543d22202020202020223e203c4120485245463d223f4e3d44223e4e616d653c2f413e2020202020202020202020202020202
0202020202020203c4120485245463d223f4d3d41223e4c617374206d6f6469666965643c2f413e202020202020203c4120485245463d223f533d41223e53
697a653c2f413e20203c4120485245463d223f443d41223e4465736372697074696f6e3c2f413e0a3c48523e0a3c494d47205352433d222f69636f6e732
f6261636b2e6769662220414c543d225b4449525d223e203c4120485245463d222f223e506172656e74204469726563746f72793c2f413e20202020202020
202032382d4170722d323030342031363a30392020202020202020202d20200a3              52433d222f69636f6e732f696d616765322e6769662220414c543
d225b494d475d223e203c4120485245463d227268696e6f342e6a706722              f342e6a70673c2f413e20202020202020202020202020202020202032382d
4170722d323030342031363a303920202031353036b20200a3c494d47205              f69636f6e732f696d616765322e6769662220414c543d225b494d4
75d223e203c4120485245463d227268696e6f352e676966223e7268696e6              63c2f413e20202020202020202020202020202020202032382d4170722d32
```

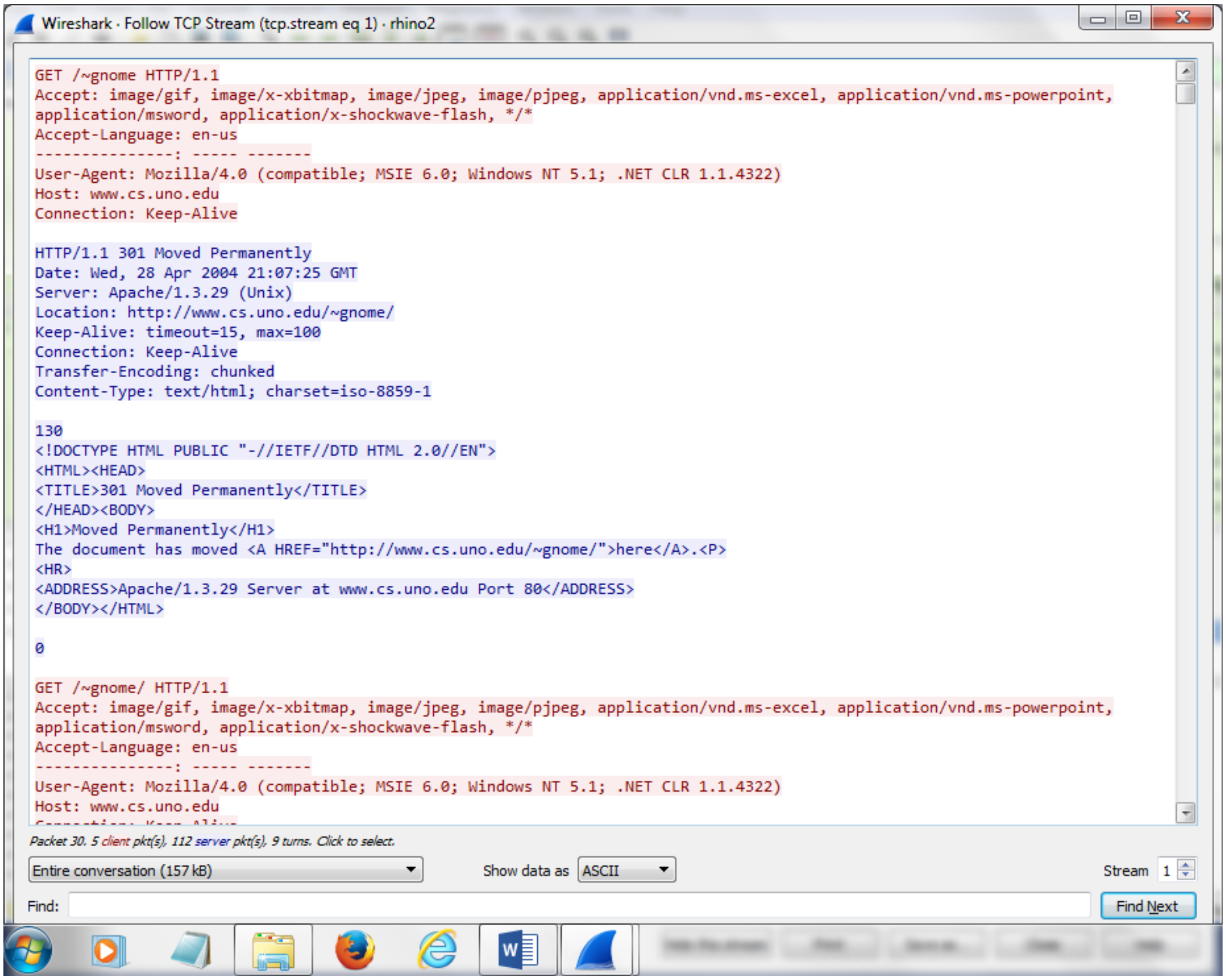
*5 client pkt(s), 111 server pkt(s), 9 turns.*

Entire conversation (157 kB)

Show data as: Raw

Stream: 1

Find:

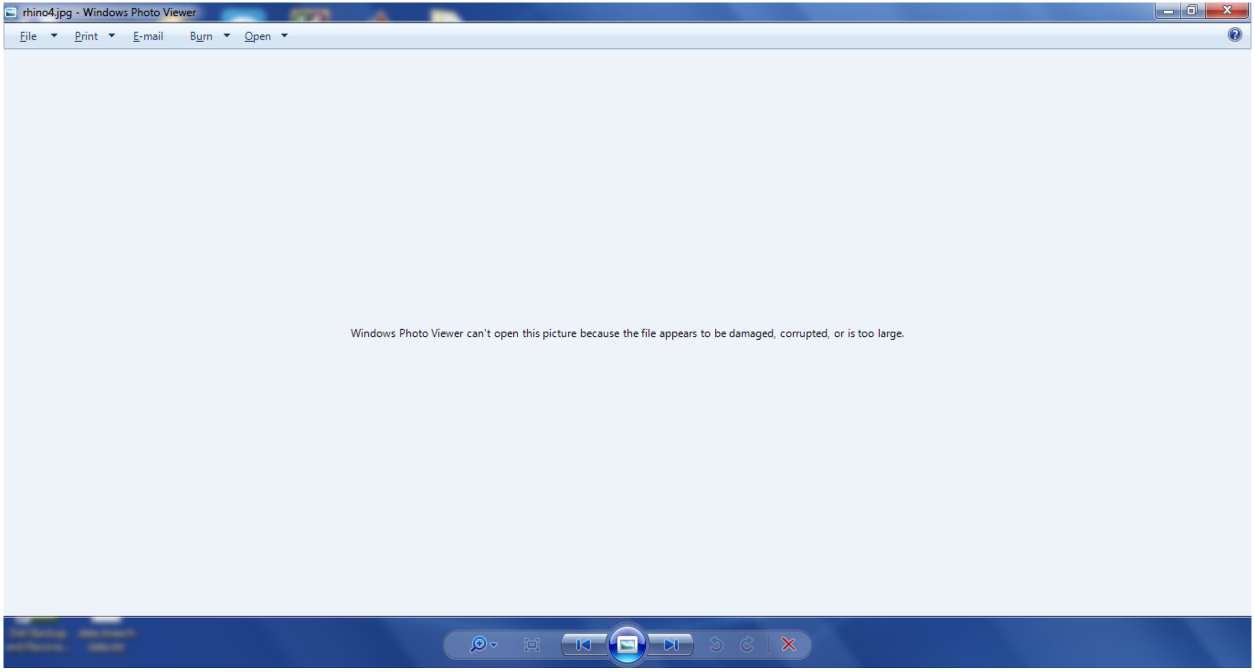


```
GET /~gnome HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, application/x-shockwave-flash, */*
Accept-Language: en-us
---------------: ----- -------
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Host: www.cs.uno.edu
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Date: Wed, 28 Apr 2004 21:07:25 GMT
Server: Apache/1.3.29 (Unix)
Location: http://www.cs.uno.edu/~gnome/
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1

130
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>301 Moved Permanently</TITLE>
</HEAD><BODY>
<H1>Moved Permanently</H1>
The document has moved <A HREF="http://www.cs.uno.edu/~gnome/">here</A>.<P>
<HR>
<ADDRESS>Apache/1.3.29 Server at www.cs.uno.edu Port 80</ADDRESS>
</BODY></HTML>

0

GET /~gnome/ 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
```

Packet 30. 5 client pkt(s), 112 server pkt(s), 9 turns. Click to select.

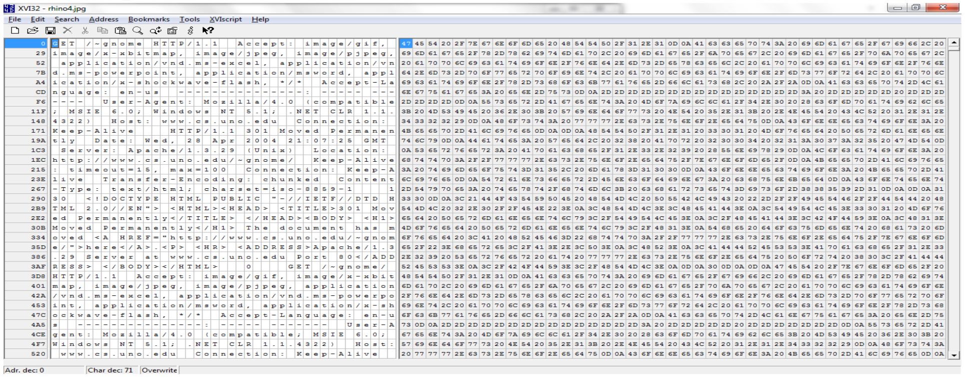
Entire conversation (157 kB) Show data as ASCII Stream 1

4. Double click on the rhino4.jpg file, you cannot view the file

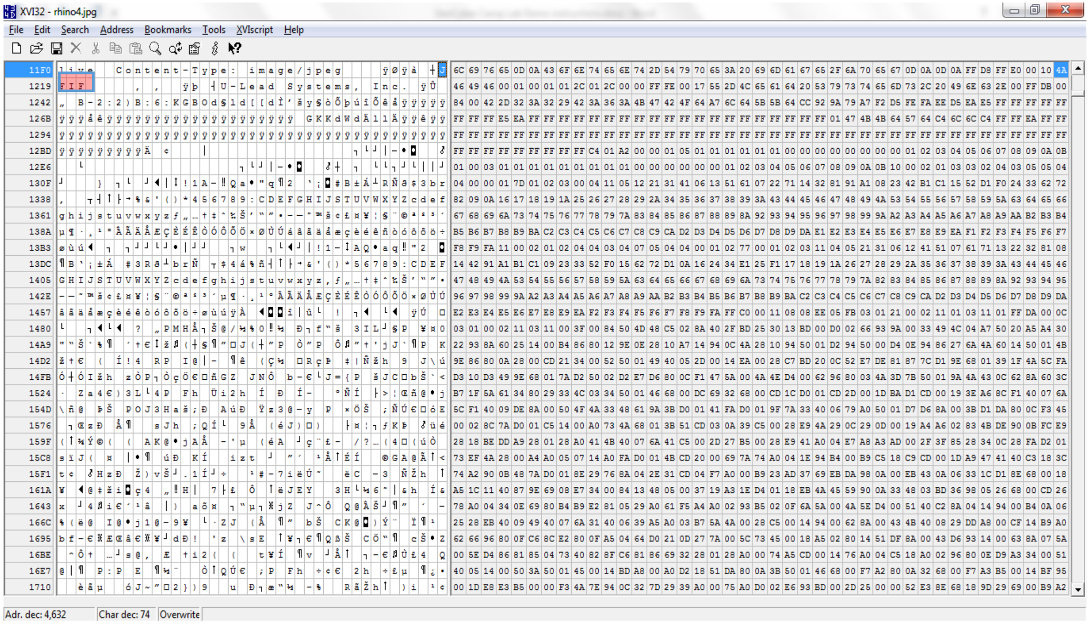


Windows Photo Viewer can't open this picture because the file appears to be damaged, corrupted, or is too large.

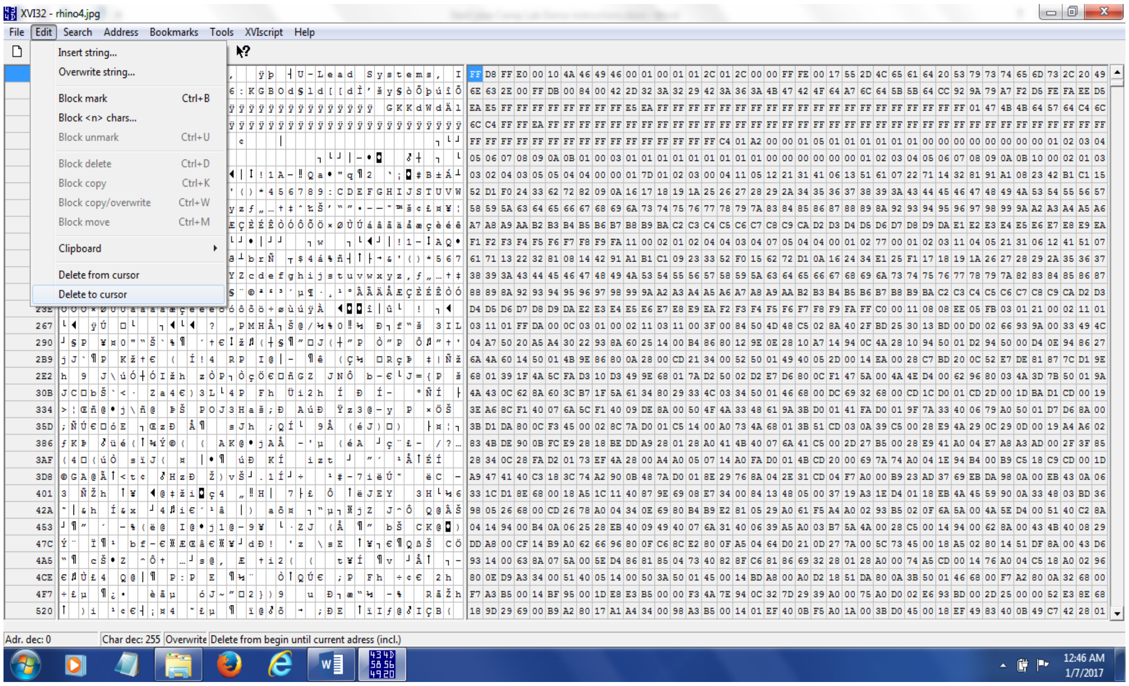
5. Open the file in a hex editor, xvi32



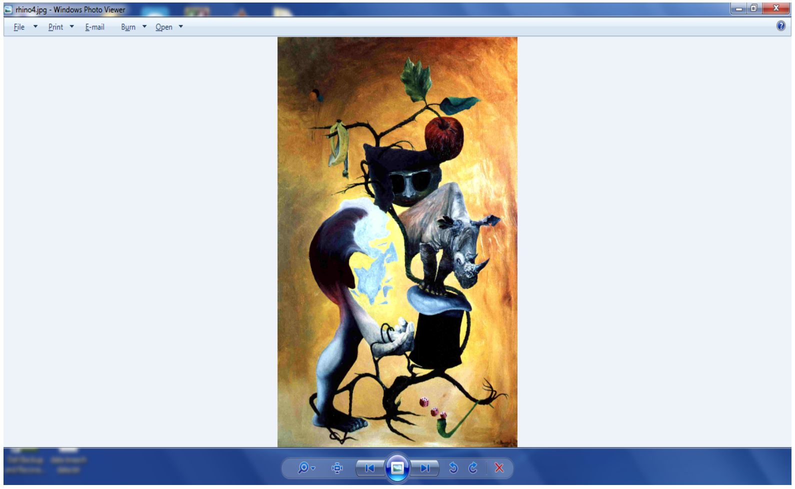
6. Search IFIF by using xvi search tab, you locate the JFIF file signature



7. Cut the http header, by using xvi/edit/**delete to cursor** (the last menu option)

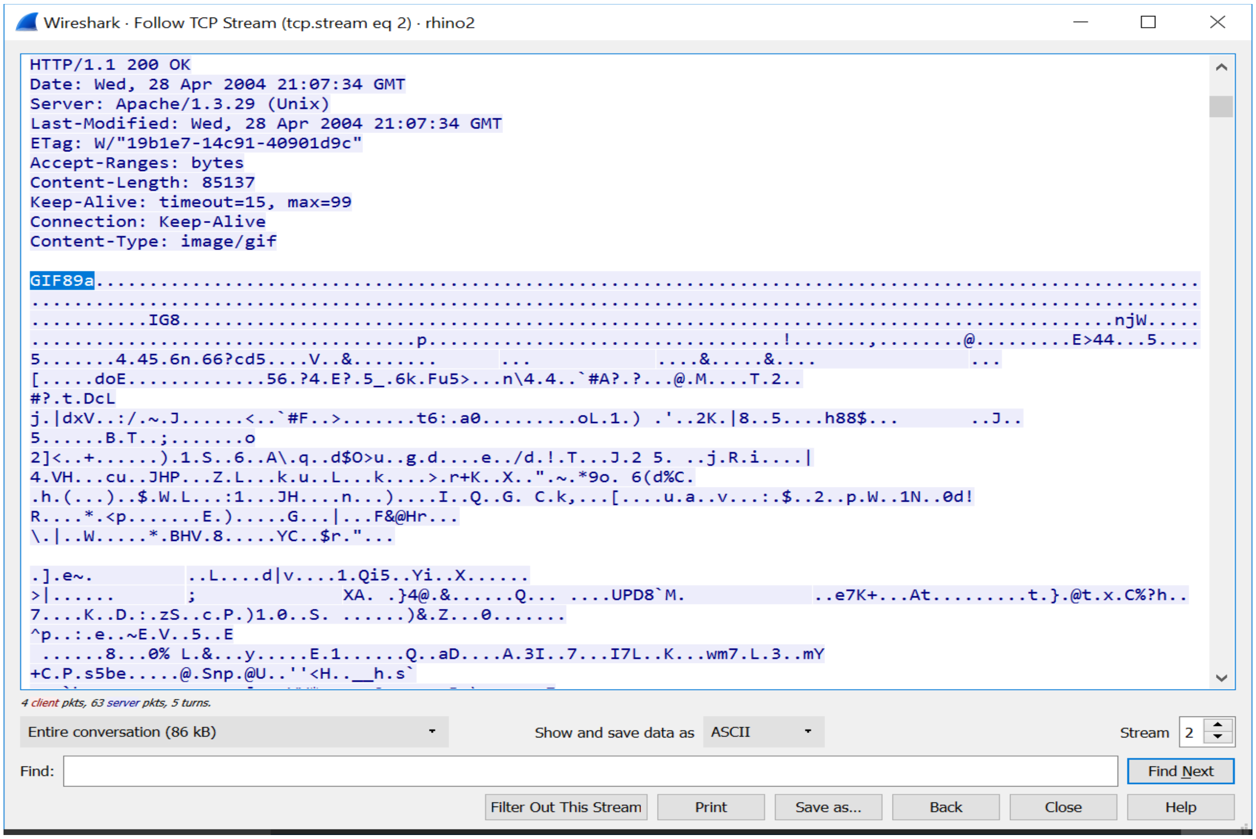


8. Go to the rhino4.jpg file and double click



## Assessment Hints

The ASCII view of the data (file) received from the session. Note the file signature GIF89a



```
HTTP/1.1 200 OK
Date: Wed, 28 Apr 2004 21:07:34 GMT
Server: Apache/1.3.29 (Unix)
Last-Modified: Wed, 28 Apr 2004 21:07:34 GMT
ETag: W/"19b1e7-14c91-40901d9c"
Accept-Ranges: bytes
Content-Length: 85137
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Content-Type: image/gif

GIF89a.......................................................................................................
.............................................................................................................
...........IG8.......................................................................................njW.....
....................................p.................................!.......,........@.........E>44...5....
5.......4.45.6n.66?cd5....V..&........           ...              ....&.....&....              ...
[.....doE............56.?4.E?.5_.6k.Fu5>...n\4.4..`#A?.?...@.M....T.2..
#?.t.DcL
j.|dxV..:/.~.J......<..`#F..>.......t6:.a0.........oL.1.) .'..2K.|8..5....h88$...      ..J..
5......B.T..;.......o
2]<..+......).1.S..6..A\.q..d$O>u..g.d....e../d.!.T...J.2 5. ..j.R.i....|
4.VH...cu..JHP...Z.L...k.u..L...k....>.r+K..X..".~.*9o. 6(d%C.
.h.(...)..$.W.L...:1...JH....n...)....I..Q..G. C.k,...[....u.a..v...:.$..2..p.W..1N..0d!
R....*.<p.......E.).....G...|...F&@Hr...
\.|..W.....*.BHV.8.....YC..$r."...

.].e~.          ..L....d|v....1.Qi5..Yi..X......
>|......        ;             XA. .}4@.&......Q... ....UPD8`M.           ..e7K+...At.........t.}.@t.x.C%?h..
7....K..D.:.zS..c.P.)1.0..S. ......)&.Z...0.......
^p..:.e..~E.V..5..E
 ......8...0% L.&...y.....E.1......Q..aD....A.3I..7...I7L..K...wm7.L.3..mY
+C.P.s5be.....@.Snp.@U..''<H..__h.s`
```

4 client pkts, 63 server pkts, 5 turns.

Entire conversation (86 kB)

Show and save data as: ASCII

Stream: 2

Find:

The picture recovered for assessment (rhino5.gif)