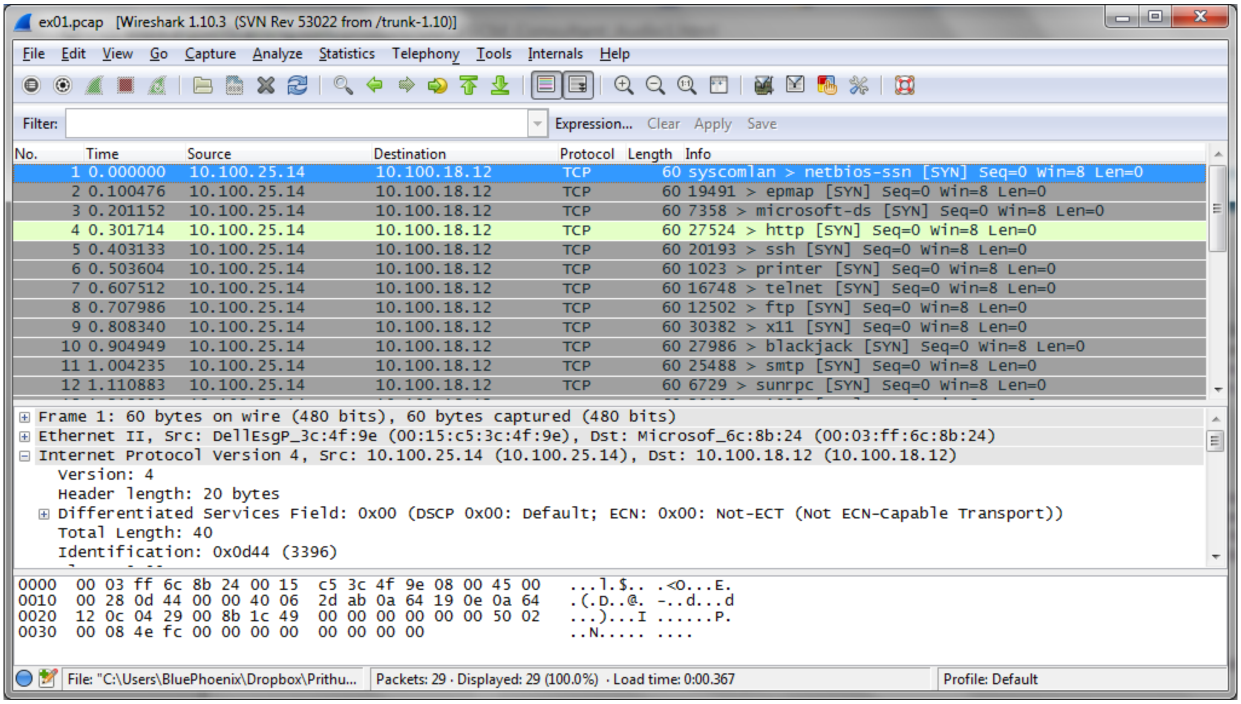
Rahul Prithu - CSCI395 – Lab 7

Answer 1:

By looking at the packets and its info, we can tell right away that there are suspicious network activities. After analyzing the available information, we can tell that that *DellEsgP_3c:4f:9e* is doing a port scanning *Microsof_6c:8b:24*, as there are multiple activities on a number of ports. Another activity that raises suspicions is, the user used ssh, and then telnet, and then file transfer.


ex01.pcap [Wireshark 1.10.3 (SVN Rev 53022 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time      Source         Destination    Protocol Length Info
    1 0.000000  10.100.25.14   10.100.18.12   TCP         60 syscomlan > netbios-ssn [SYN] Seq=0 Win=8 Len=0
    2 0.100476  10.100.25.14   10.100.18.12   TCP         60 19491 > epmap [SYN] Seq=0 Win=8 Len=0
    3 0.201152  10.100.25.14   10.100.18.12   TCP         60 7358 > microsoft-ds [SYN] Seq=0 Win=8 Len=0
    4 0.301714  10.100.25.14   10.100.18.12   TCP         60 27524 > http [SYN] Seq=0 Win=8 Len=0
    5 0.403133  10.100.25.14   10.100.18.12   TCP         60 20193 > ssh [SYN] Seq=0 Win=8 Len=0
    6 0.503604  10.100.25.14   10.100.18.12   TCP         60 1023 > printer [SYN] Seq=0 Win=8 Len=0
    7 0.607512  10.100.25.14   10.100.18.12   TCP         60 16748 > telnet [SYN] Seq=0 Win=8 Len=0
    8 0.707986  10.100.25.14   10.100.18.12   TCP         60 12502 > ftp [SYN] Seq=0 Win=8 Len=0
    9 0.808340  10.100.25.14   10.100.18.12   TCP         60 30382 > x11 [SYN] Seq=0 Win=8 Len=0
   10 0.904949  10.100.25.14   10.100.18.12   TCP         60 27986 > blackjack [SYN] Seq=0 Win=8 Len=0
   11 1.004235  10.100.25.14   10.100.18.12   TCP         60 25488 > smtp [SYN] Seq=0 Win=8 Len=0
   12 1.110883  10.100.25.14   10.100.18.12   TCP         60 6729 > sunrpc [SYN] Seq=0 Win=8 Len=0
```

```
⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: DellEsgP_3c:4f:9e (00:15:c5:3c:4f:9e), Dst: Microsof_6c:8b:24 (00:03:ff:6c:8b:24)
⊟ Internet Protocol Version 4, Src: 10.100.25.14 (10.100.25.14), Dst: 10.100.18.12 (10.100.18.12)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 40
    Identification: 0x0d44 (3396)
```

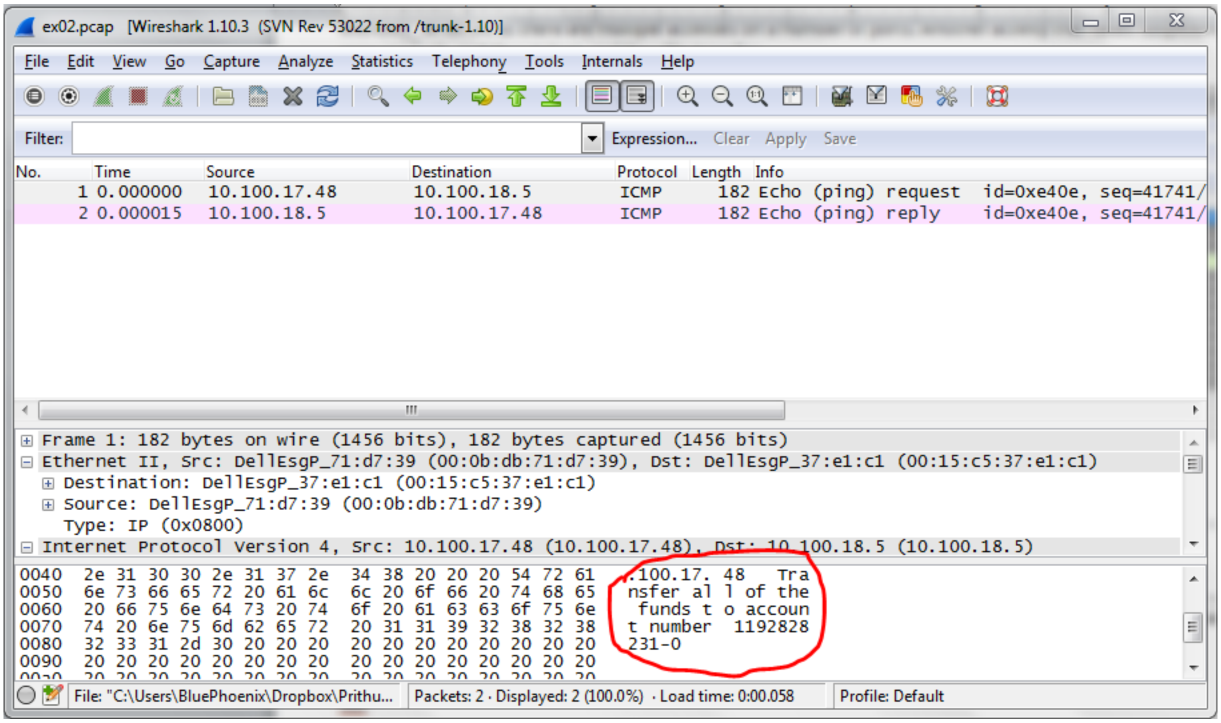
```
0000  00 03 ff 6c 8b 24 00 15  c5 3c 4f 9e 08 00 45 00   ...l.$.. .<O...E.
0010  00 28 0d 44 00 00 40 06  2d ab 0a 64 19 0e 0a 64   .(.D..@. -..d...d
0020  12 0c 04 29 00 8b 1c 49  00 00 00 00 00 00 50 02   ...)...I ......P.
0030  00 08 4e fc 00 00 00 00  00 00 00 00               ..N..... ....
```

File: "C:\Users\BluePhoenix\Dropbox\Prithu... Packets: 29 · Displayed: 29 (100.0%) · Load time: 0:00.367 Profile: Default

Also blackjack? Very suspicious in my book!

Answer 2:

Looking at the two pings..we get the the message "Transfer all of the funds to account number 1192828231-0. Someone somewhere is transferring some-sum of money to somebody. It's not only suspicious, but hints something illegal.

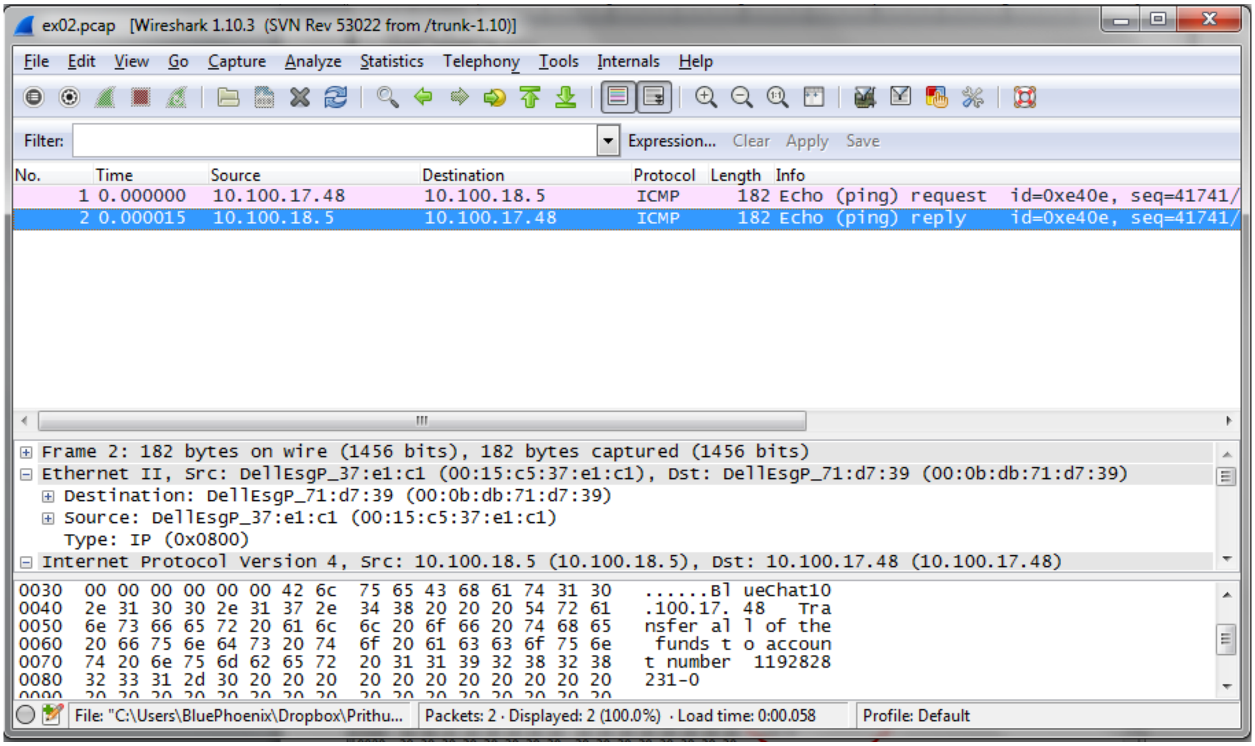

ex02.pcap [Wireshark 1.10.3 (SVN Rev 53022 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time      Source         Destination    Protocol Length Info
    1 0.000000  10.100.17.48   10.100.18.5    ICMP       182 Echo (ping) request  id=0xe40e, seq=41741/
    2 0.000015  10.100.18.5    10.100.17.48   ICMP       182 Echo (ping) reply    id=0xe40e, seq=41741/
```

```
⊞ Frame 1: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits)
⊟ Ethernet II, Src: DellEsgP_71:d7:39 (00:0b:db:71:d7:39), Dst: DellEsgP_37:e1:c1 (00:15:c5:37:e1:c1)
  ⊞ Destination: DellEsgP_37:e1:c1 (00:15:c5:37:e1:c1)
  ⊞ Source: DellEsgP_71:d7:39 (00:0b:db:71:d7:39)
    Type: IP (0x0800)
⊟ Internet Protocol Version 4, Src: 10.100.17.48 (10.100.17.48), Dst: 10.100.18.5 (10.100.18.5)
```

```
0040  2e 31 30 30 2e 31 37 2e  34 38 20 20 20 54 72 61   .100.17. 48   Tra
0050  6e 73 66 65 72 20 61 6c  6c 20 6f 66 20 74 68 65   nsfer al l of the
0060  20 66 75 6e 64 73 20 74  6f 20 61 63 63 6f 75 6e    funds t o accoun
0070  74 20 6e 75 6d 62 65 72  20 31 31 39 32 38 32 38   t number  1192828
0080  32 33 31 2d 30 20 20 20  20 20 20 20 20 20 20 20   231-0
0090  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
```

File: "C:\Users\BluePhoenix\Dropbox\Prithu... Packets: 2 · Displayed: 2 (100.0%) · Load time: 0:00.058 Profile: Default

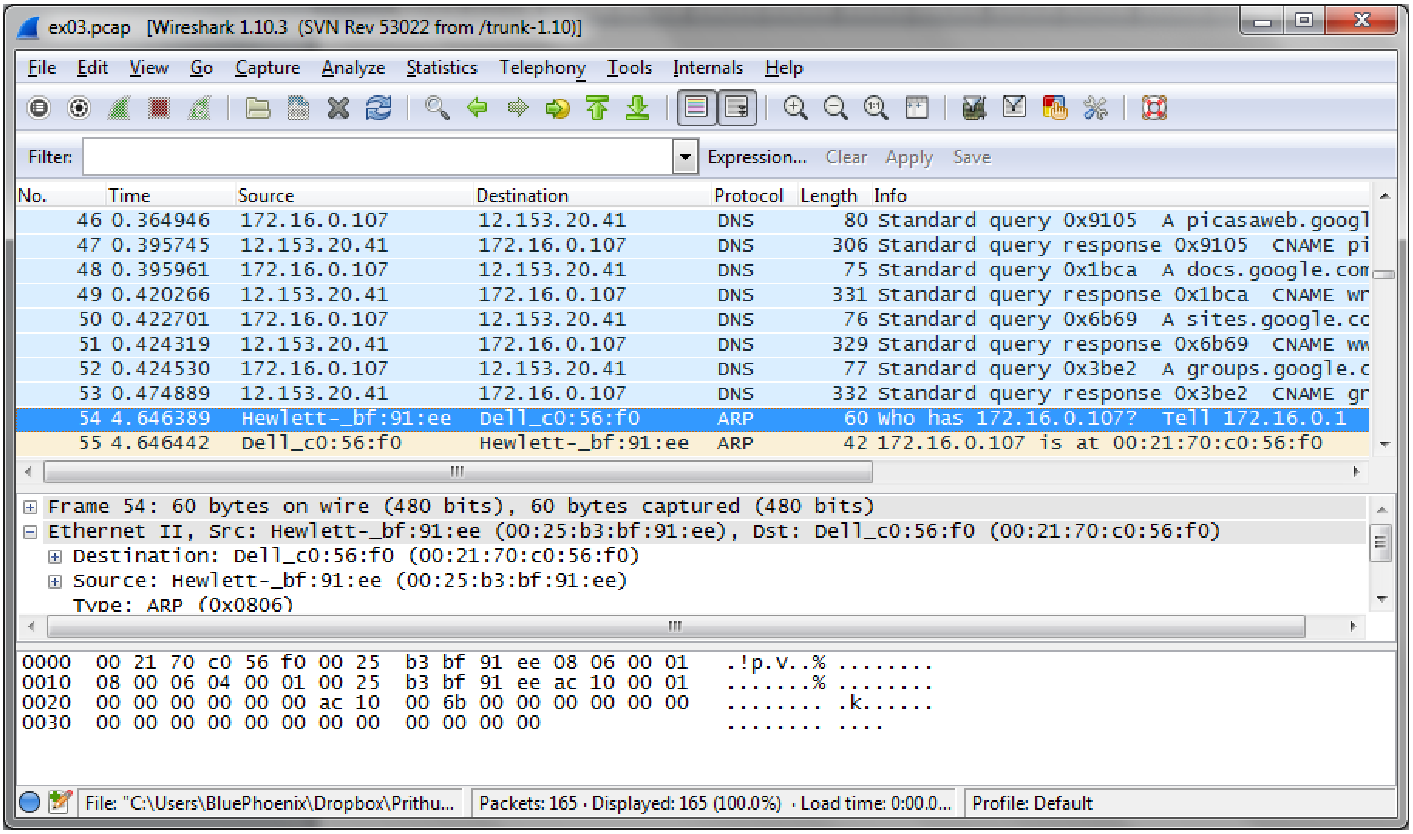


```
ex02.pcap  [Wireshark 1.10.3  (SVN Rev 53022 from /trunk-1.10)]

No.     Time        Source           Destination      Protocol Length Info
      1 0.000000    10.100.17.48     10.100.18.5      ICMP        182 Echo (ping) request  id=0xe40e, seq=41741/
      2 0.000015    10.100.18.5      10.100.17.48     ICMP        182 Echo (ping) reply    id=0xe40e, seq=41741/

⊞ Frame 2: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits)
⊟ Ethernet II, Src: DellEsgP_37:e1:c1 (00:15:c5:37:e1:c1), Dst: DellEsgP_71:d7:39 (00:0b:db:71:d7:39)
  ⊞ Destination: DellEsgP_71:d7:39 (00:0b:db:71:d7:39)
  ⊞ Source: DellEsgP_37:e1:c1 (00:15:c5:37:e1:c1)
    Type: IP (0x0800)
⊟ Internet Protocol Version 4, Src: 10.100.18.5 (10.100.18.5), Dst: 10.100.17.48 (10.100.17.48)

0030  00 00 00 00 00 00 42 6c  75 65 43 68 61 74 31 30   ......Bl ueChat10
0040  2e 31 30 30 2e 31 37 2e  34 38 20 20 20 54 72 61   .100.17. 48   Tra
0050  6e 73 66 65 72 20 61 6c  6c 20 6f 66 20 74 68 65   nsfer al l of the
0060  20 66 75 6e 64 73 20 74  6f 20 61 63 63 6f 75 6e    funds t o accoun
0070  74 20 6e 75 6d 62 65 72  20 31 31 39 32 38 32 38   t number  1192828
0080  32 33 31 2d 30 20 20 20  20 20 20 20 20 20 20 20   231-0
0090  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20

File: "C:\Users\BluePhoenix\Dropbox\Prithu...   Packets: 2 · Displayed: 2 (100.0%) · Load time: 0:00.058   Profile: Default
```

Money, the root of all evil!

Answer 3:

Analyzing the packets one by one, we see that packets 1-to-53 are between *Dell_c0:56:f0* and *Cisco_31:07:33*. However, when we arrive at packet #54, the consistent pattern between the user and router changes. We see that *Hewlett-_bf:91:ee* makes ARP requests. We can then see that this series of packets from Hewlett is doing as a man-in-the-middle attack and intercepting *Dell_c0:56:f0*'s activities.



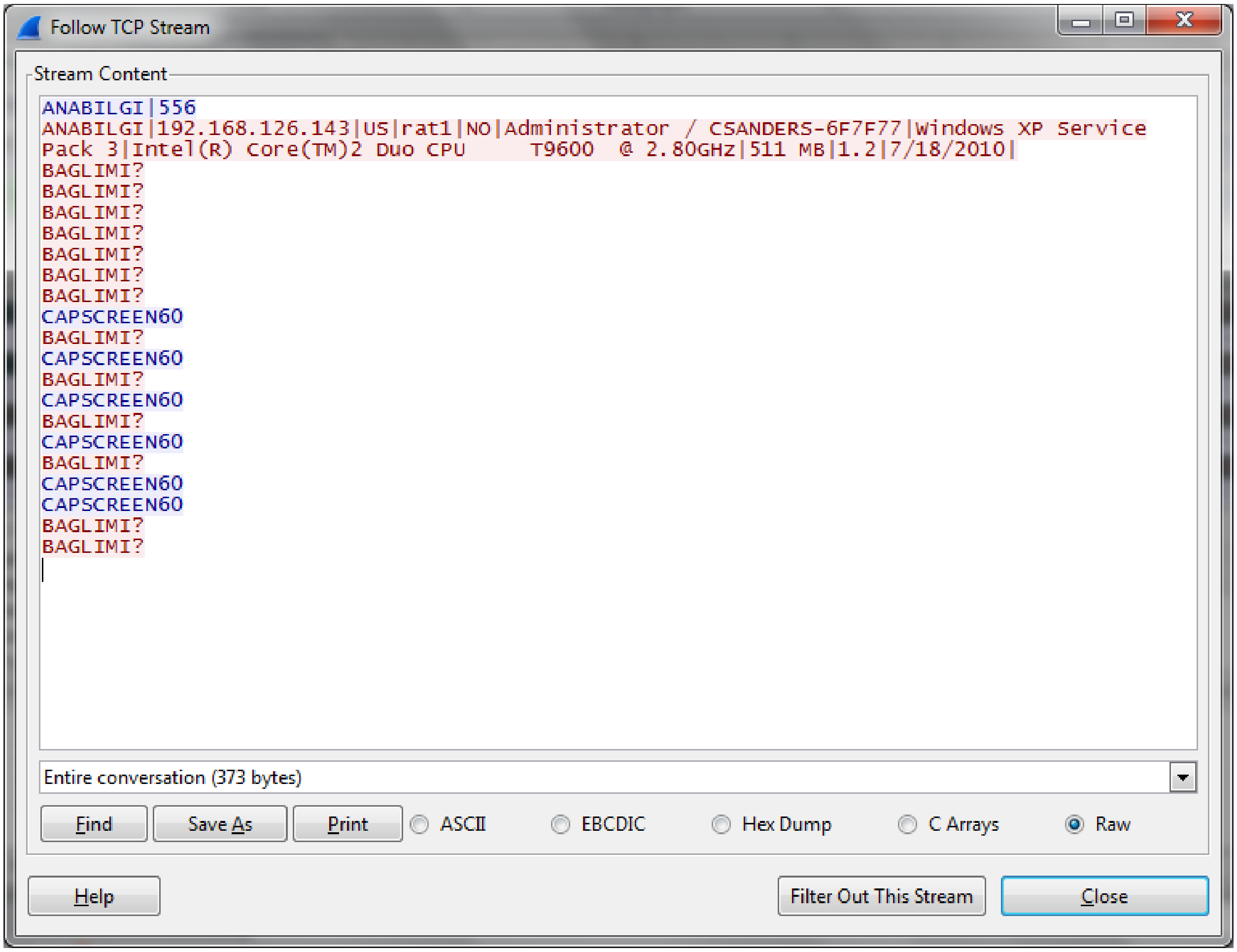
```
ex03.pcap  [Wireshark 1.10.3  (SVN Rev 53022 from /trunk-1.10)]

No.     Time        Source             Destination        Protocol Length Info
     46 0.364946    172.16.0.107       12.153.20.41       DNS          80 Standard query 0x9105  A picasaweb.googl
     47 0.395745    12.153.20.41       172.16.0.107       DNS         306 Standard query response 0x9105  CNAME pi
     48 0.395961    172.16.0.107       12.153.20.41       DNS          75 Standard query 0x1bca  A docs.google.com
     49 0.420266    12.153.20.41       172.16.0.107       DNS         331 Standard query response 0x1bca  CNAME wr
     50 0.422701    172.16.0.107       12.153.20.41       DNS          76 Standard query 0x6b69  A sites.google.cc
     51 0.424319    12.153.20.41       172.16.0.107       DNS         329 Standard query response 0x6b69  CNAME ww
     52 0.424530    172.16.0.107       12.153.20.41       DNS          77 Standard query 0x3be2  A groups.google.c
     53 0.474889    12.153.20.41       172.16.0.107       DNS         332 Standard query response 0x3be2  CNAME gr
     54 4.646389    Hewlett-_bf:91:ee  Dell_c0:56:f0      ARP          60 Who has 172.16.0.107?  Tell 172.16.0.1
     55 4.646442    Dell_c0:56:f0      Hewlett-_bf:91:ee  ARP          42 172.16.0.107 is at 00:21:70:c0:56:f0

⊞ Frame 54: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊟ Ethernet II, Src: Hewlett-_bf:91:ee (00:25:b3:bf:91:ee), Dst: Dell_c0:56:f0 (00:21:70:c0:56:f0)
  ⊞ Destination: Dell_c0:56:f0 (00:21:70:c0:56:f0)
  ⊞ Source: Hewlett-_bf:91:ee (00:25:b3:bf:91:ee)
    Type: ARP (0x0806)

0000  00 21 70 c0 56 f0 00 25  b3 bf 91 ee 08 06 00 01   .!p.V..% ........
0010  08 00 06 04 00 01 00 25  b3 bf 91 ee ac 10 00 01   .......% ........
0020  00 00 00 00 00 00 ac 10  00 6b 00 00 00 00 00 00   ........ .k......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....

File: "C:\Users\BluePhoenix\Dropbox\Prithu...   Packets: 165 · Displayed: 165 (100.0%) · Load time: 0:00.0...   Profile: Default
```

Wolf in sheep's clothing!

Answer 4:

Searching for *ANABILGI/ANA BILGI*, turns out two packets, but they don't contain any useful information.

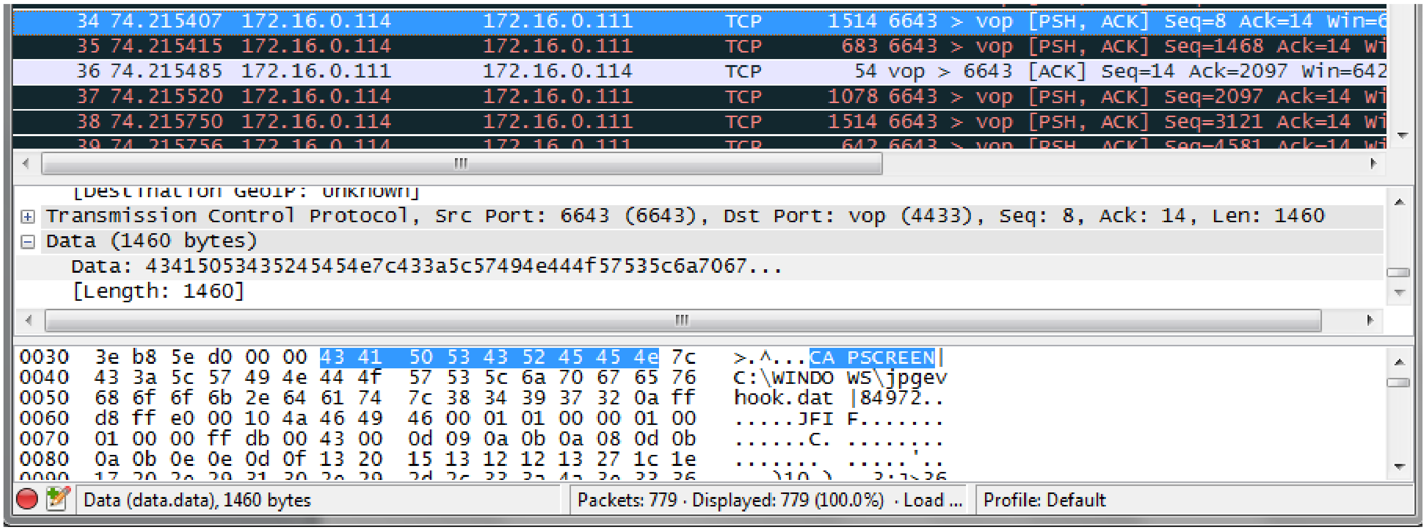
However going through some of the packets, some things stick out..some packets have *BAGLIMI?*
Doing a “Follow TCP Stream”, we can see that all the strings there.



```
ANABILGI|556
ANABILGI|192.168.126.143|US|rat1|NO|Administrator / CSANDERS-6F7F77|Windows XP Service
Pack 3|Intel(R) Core(TM)2 Duo CPU     T9600  @ 2.80GHz|511 MB|1.2|7/18/2010|
BAGLIMI?
BAGLIMI?
BAGLIMI?
BAGLIMI?
BAGLIMI?
BAGLIMI?
BAGLIMI?
CAPSCREEN60
BAGLIMI?
CAPSCREEN60
BAGLIMI?
CAPSCREEN60
BAGLIMI?
CAPSCREEN60
BAGLIMI?
CAPSCREEN60
CAPSCREEN60
BAGLIMI?
BAGLIMI?
```

Entire conversation (373 bytes)

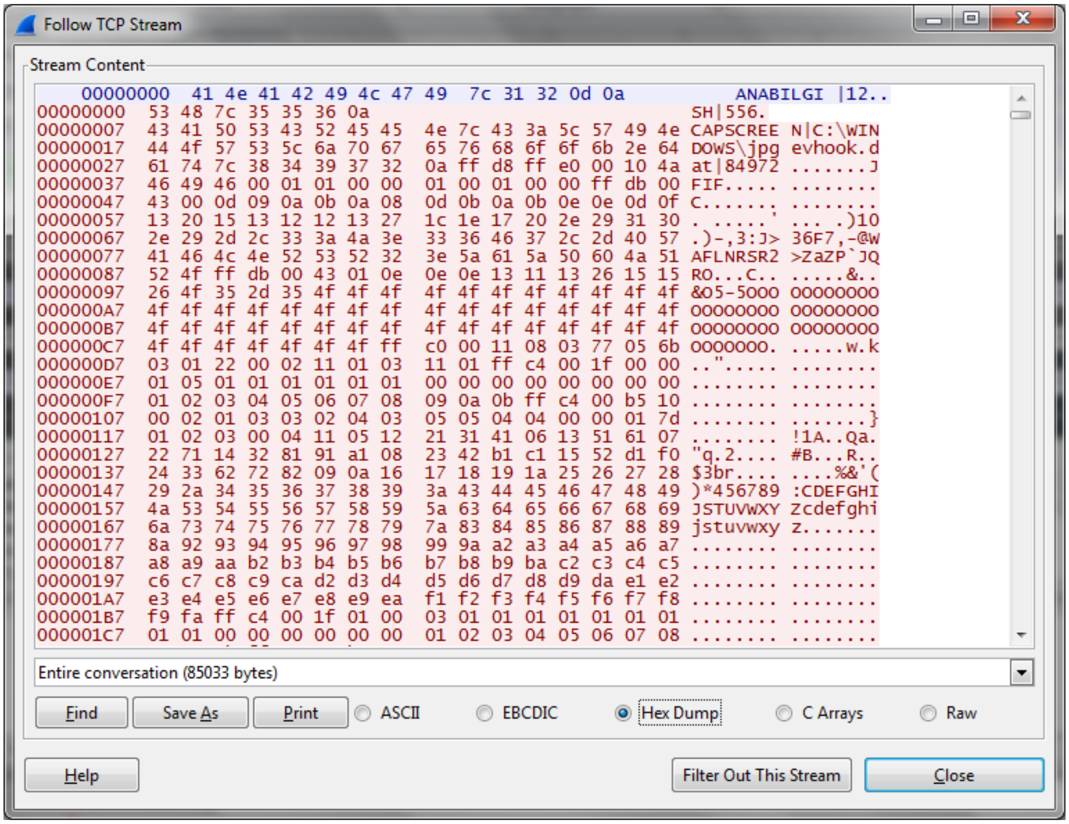
After searching through these strings, we found out that packets containing the string *CAPSCREEN* (Not *CAPSREEN60*), contains some hexadecimal information. Upon further review of the packets, we can see that these packets contain JPG headers.



```
34 74.215407  172.16.0.114     172.16.0.111     TCP     1514 6643 > vop [PSH, ACK] Seq=8 Ack=14 Win=6
35 74.215415  172.16.0.114     172.16.0.111     TCP      683 6643 > vop [PSH, ACK] Seq=1468 Ack=14 Wi
36 74.215485  172.16.0.111     172.16.0.114     TCP       54 vop > 6643 [ACK] Seq=14 Ack=2097 Win=642
37 74.215520  172.16.0.114     172.16.0.111     TCP     1078 6643 > vop [PSH, ACK] Seq=2097 Ack=14 Wi
38 74.215750  172.16.0.114     172.16.0.111     TCP     1514 6643 > vop [PSH, ACK] Seq=3121 Ack=14 Wi
39 74.215756  172.16.0.114     172.16.0.111     TCP      642 6643 > vop [PSH, ACK] Seq=4581 Ack=14 Wi

    [Destination GeoIP: Unknown]
⊞ Transmission Control Protocol, Src Port: 6643 (6643), Dst Port: vop (4433), Seq: 8, Ack: 14, Len: 1460
⊟ Data (1460 bytes)
    Data: 434150534352454e7c433a5c57494e444f57535c6a7067...
    [Length: 1460]

0030  3e b8 5e d0 00 00 43 41  50 53 43 52 45 45 4e 7c   >.^...CA PSCREEN|
0040  43 3a 5c 57 49 4e 44 4f  57 53 5c 6a 70 67 65 76   C:\WINDO WS\jpgev
0050  68 6f 6f 6b 2e 64 61 74  7c 38 34 39 37 32 0a ff   hook.dat |84972..
0060  d8 ff e0 00 10 4a 46 49  46 00 01 01 00 00 01 00   .....JFI F.......
0070  01 00 00 ff db 00 43 00  0d 09 0a 0b 0a 08 0d 0b   ......C. ........
0080  0a 0b 0e 0e 0d 0f 13 20  15 13 12 12 13 27 1c 1e   .......  .....'..
```

Data (data.data), 1460 bytes | Packets: 779 · Displayed: 779 (100.0%) · Load ... | Profile: Default

Packets 34, 158, 282, 407, 533, and 654 all have the same things on them.

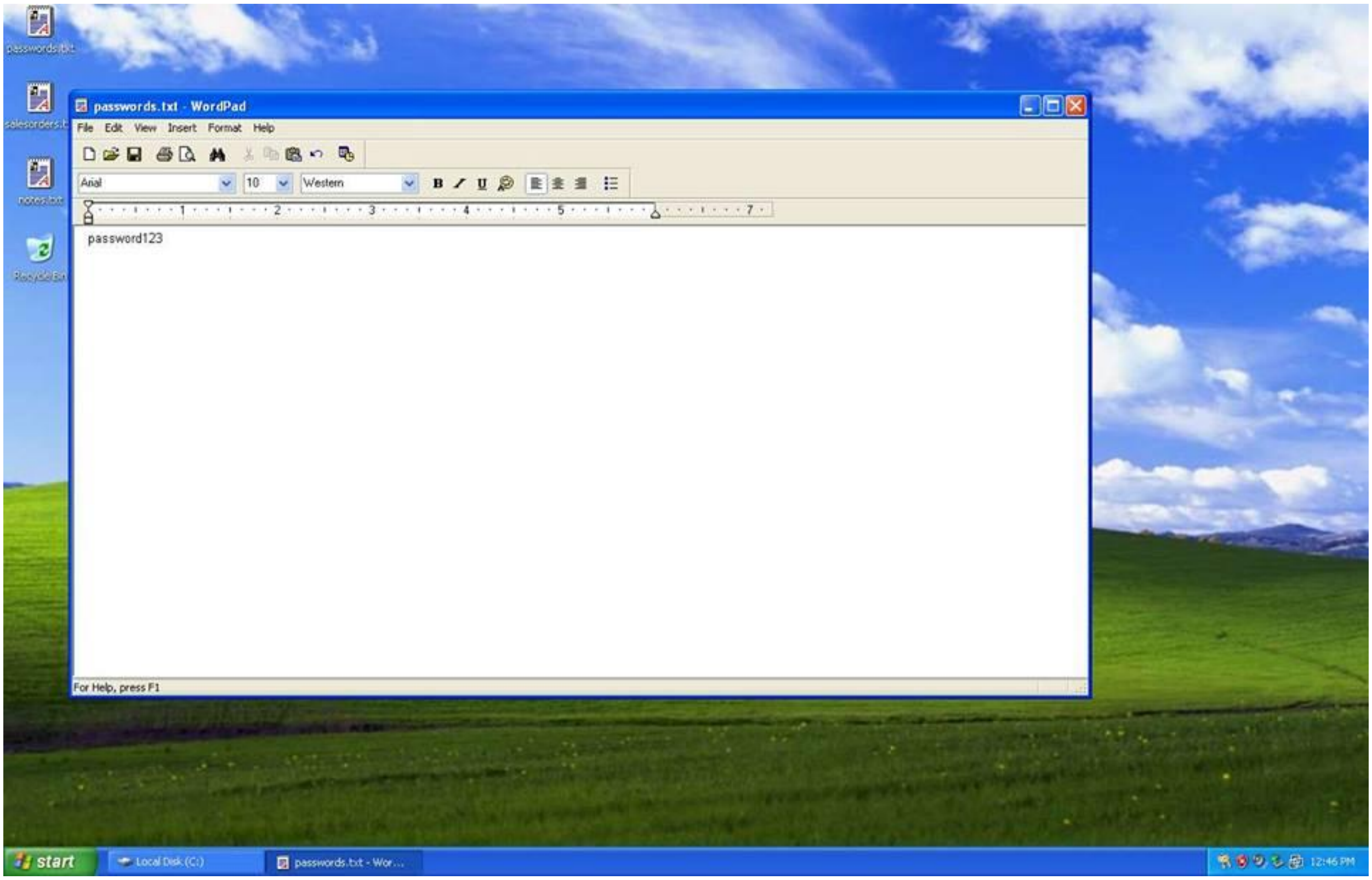


```
    00000000  41 4e 41 42 49 4c 47 49  7c 31 32 0d 0a          ANABILGI |12..
00000000  53 48 7c 35 35 36 0a                             SH|556.
00000007  43 41 50 53 43 52 45 45  4e 7c 43 3a 5c 57 49 4e CAPSCREE N|C:\WIN
00000017  44 4f 57 53 5c 6a 70 67  65 76 68 6f 6f 6b 2e 64 DOWS\jpg evhook.d
00000027  61 74 7c 38 34 39 37 32  0a ff d8 ff e0 00 10 4a at|84972 .......J
00000037  46 49 46 00 01 01 00 00  01 00 01 00 00 ff db 00 FIF..... ........
00000047  43 00 0d 09 0a 0b 0a 08  0d 0b 0a 0b 0e 0e 0d 0f C....... ........
00000057  13 20 15 13 12 12 13 27  1c 1e 17 20 2e 29 31 30 . .....' ... .)10
00000067  2e 29 2d 2c 33 3a 4a 3e  33 36 46 37 2c 2d 40 57 .)-,3:J> 36F7,-@W
00000077  41 46 4c 4e 52 53 52 32  3e 5a 61 5a 50 60 4a 51 AFLNRSR2 >ZaZP`JQ
00000087  52 4f ff db 00 43 01 0e  0e 0e 13 11 13 26 15 15 RO...C.. .....&..
00000097  26 4f 35 2d 35 4f 4f 4f  4f 4f 4f 4f 4f 4f 4f 4f &O5-5OOO OOOOOOOO
000000A7  4f 4f 4f 4f 4f 4f 4f 4f  4f 4f 4f 4f 4f 4f 4f 4f OOOOOOOO OOOOOOOO
000000B7  4f 4f 4f 4f 4f 4f 4f 4f  4f 4f 4f 4f 4f 4f 4f 4f OOOOOOOO OOOOOOOO
000000C7  4f 4f 4f 4f 4f 4f 4f ff  c0 00 11 08 03 77 05 6b OOOOOOO. .....w.k
000000D7  03 01 22 00 02 11 01 03  11 01 ff c4 00 1f 00 00 .."..... ........
000000E7  01 05 01 01 01 01 01 01  00 00 00 00 00 00 00 00 ........ ........
000000F7  01 02 03 04 05 06 07 08  09 0a 0b ff c4 00 b5 10 ........ ........
00000107  00 02 01 03 03 02 04 03  05 05 04 04 00 00 01 7d ........ .......}
00000117  01 02 03 00 04 11 05 12  21 31 41 06 13 51 61 07 ........ !1A..Qa.
00000127  22 71 14 32 81 91 a1 08  23 42 b1 c1 15 52 d1 f0 "q.2.... #B...R..
00000137  24 33 62 72 82 09 0a 16  17 18 19 1a 25 26 27 28 $3br.... ....%&'(
00000147  29 2a 34 35 36 37 38 39  3a 43 44 45 46 47 48 49 )*456789 :CDEFGHI
00000157  4a 53 54 55 56 57 58 59  5a 63 64 65 66 67 68 69 JSTUVWXY Zcdefghi
00000167  6a 73 74 75 76 77 78 79  7a 83 84 85 86 87 88 89 jstuvwxy z.......
00000177  8a 92 93 94 95 96 97 98  99 9a a2 a3 a4 a5 a6 a7 ........ ........
00000187  a8 a9 aa b2 b3 b4 b5 b6  b7 b8 b9 ba c2 c3 c4 c5 ........ ........
00000197  c6 c7 c8 c9 ca d2 d3 d4  d5 d6 d7 d8 d9 da e1 e2 ........ ........
000001A7  e3 e4 e5 e6 e7 e8 e9 ea  f1 f2 f3 f4 f5 f6 f7 f8 ........ ........
000001B7  f9 fa ff c4 00 1f 01 00  03 01 01 01 01 01 01 01 ........ ........
000001C7  01 01 00 00 00 00 00 00  01 02 03 04 05 06 07 08 ........ ........
```

Entire conversation (85033 bytes)

Interesting note: ANABILGI exists in all the six packets, but didn't come up during the search.

After saving the Hex dump/packet info dump, and removing everything from the top before the JPG header begins, we were able to extract six jpgs, which reveals the fact that there is indeed a malware in the computer that is sending screen shots. Not only that, the user's password has been compromised, as evident from one of the images!



password123

"password123" is a bad password-practice. Even a little hacking program could've gotten in.