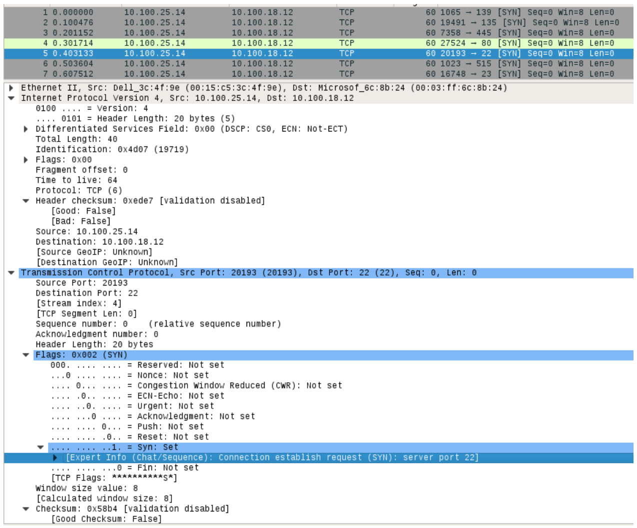
Christopher Mayol

Ex01.pcap



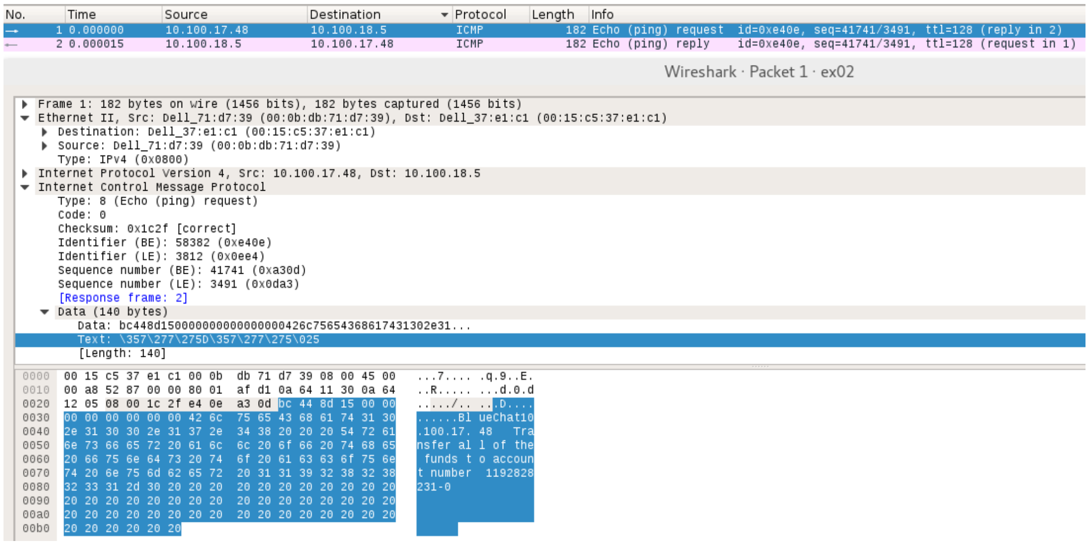
```
 1 0.000000   10.100.25.14   10.100.18.12   TCP     60 1065 → 139 [SYN] Seq=0 Win=8 Len=0
 2 0.100476   10.100.25.14   10.100.18.12   TCP     60 19491 → 135 [SYN] Seq=0 Win=8 Len=0
 3 0.201152   10.100.25.14   10.100.18.12   TCP     60 7358 → 445 [SYN] Seq=0 Win=8 Len=0
 4 0.301714   10.100.25.14   10.100.18.12   TCP     60 27524 → 80 [SYN] Seq=0 Win=8 Len=0
 5 0.403133   10.100.25.14   10.100.18.12   TCP     60 20193 → 22 [SYN] Seq=0 Win=8 Len=0
 6 0.503604   10.100.25.14   10.100.18.12   TCP     60 1023 → 515 [SYN] Seq=0 Win=8 Len=0
 7 0.607512   10.100.25.14   10.100.18.12   TCP     60 16748 → 23 [SYN] Seq=0 Win=8 Len=0
▶ Ethernet II, Src: Dell_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, Dst: 10.100.18.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x4d07 (19719)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
  ▼ Header checksum: 0xede7 [validation disabled]
      [Good: False]
      [Bad: False]
    Source: 10.100.25.14
    Destination: 10.100.18.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ Transmission Control Protocol, Src Port: 20193 (20193), Dst Port: 22 (22), Seq: 0, Len: 0
    Source Port: 20193
    Destination Port: 22
    [Stream index: 4]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 20 bytes
  ▼ Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ▼ .... .... ..1. = Syn: Set
      ▶ [Expert Info (Chat/Sequence): Connection establish request (SYN): server port 22]
      .... .... ...0 = Fin: Not set
      [TCP Flags: **********S*]
    Window size value: 8
    [Calculated window size: 8]
  ▼ Checksum: 0x58b4 [validation disabled]
      [Good Checksum: False]
```

We have a connection between the source (10.100.25.14) computer and a destination (10.100.18.12) server.

They connection type is a TCP connection and in a TCP connection we start a connection with a 3- way handshake, we request a connection with SYN message, then the server acknowledges the request by sending a ACK message reply, and we then ACK that we received the ACK from the server.

This is clearly not the case in this connection. First, thing we see is pretty obvious the server is not replying to the client with acknowledgments. The client is attacking the server with a SYN Flood. The attacker floods the server with requests, initially the server replied to the syn request with an ack but the attacker ignores the ack and instead sends syn requests to the server. Since the server is expecting for an ack the server won’t respond causing a denial of service to the other clients trying to communicate with the server.

Ex02.pcap



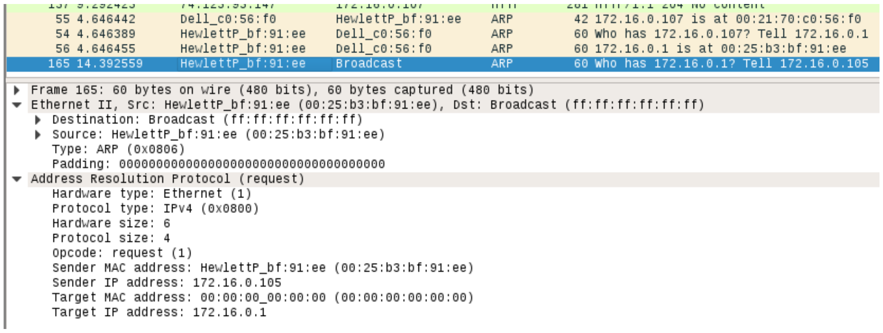
```
No.  Time        Source          Destination      Protocol  Length  Info
   1 0.000000    10.100.17.48    10.100.18.5      ICMP         182 Echo (ping) request  id=0xe40e, seq=41741/3491, ttl=128 (reply in 2)
   2 0.000015    10.100.18.5     10.100.17.48     ICMP         182 Echo (ping) reply    id=0xe40e, seq=41741/3491, ttl=128 (request in 1)
```

Wireshark · Packet 1 · ex02

```
▶ Frame 1: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits)
▼ Ethernet II, Src: Dell_71:d7:39 (00:0b:db:71:d7:39), Dst: Dell_37:e1:c1 (00:15:c5:37:e1:c1)
  ▶ Destination: Dell_37:e1:c1 (00:15:c5:37:e1:c1)
  ▶ Source: Dell_71:d7:39 (00:0b:db:71:d7:39)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 10.100.17.48, Dst: 10.100.18.5
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x1c2f [correct]
    Identifier (BE): 58382 (0xe40e)
    Identifier (LE): 3812 (0x0ee4)
    Sequence number (BE): 41741 (0xa30d)
    Sequence number (LE): 3491 (0x0da3)
    [Response frame: 2]
  ▼ Data (140 bytes)
      Data: bc448d1500000000000000000426c75654368617431302e31...
      Text: \357\277\275D\357\277\275\025
      [Length: 140]

0000  00 15 c5 37 e1 c1 00 0b  db 71 d7 39 08 00 45 00   ...7.... .q.9..E.
0010  00 a8 52 87 00 00 80 01  af d1 0a 64 11 30 0a 64   ..R..... ...d.0.d
0020  12 05 08 00 1c 2f e4 0e  a3 0d bc 44 8d 15 00 00   ...../.. ..D....
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
00a0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00b0  20 20 20 20 20 20
```

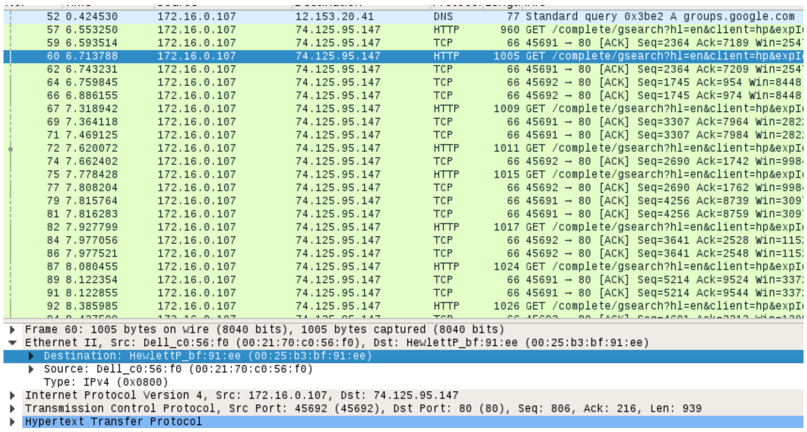
We can see that the connection is a ICMP connection type. ICMP is usually used by routers to report error messages to the client. ICMP uses echo packets for communication. Analysing the echo message we see that the employees have been communicating. “BlueChat101001748 Transfer all of the funds to account 1192828231-0”. The employees have created a ICMP tunnel which allows them to communicate from this port by injecting their messages into echo packets. This also allows them to avoid firewall detection.

Ex03.pcap



```
 157 9.292425    74.125.93.147      172.16.0.107       HTTP      261 HTTP/1.1 204 No Content
  55 4.646442    Dell_c0:56:f0      HewlettP_bf:91:ee  ARP        42 172.16.0.107 is at 00:21:70:c0:56:f0
  54 4.646389    HewlettP_bf:91:ee  Dell_c0:56:f0      ARP        60 Who has 172.16.0.107? Tell 172.16.0.1
  56 4.646455    HewlettP_bf:91:ee  Dell_c0:56:f0      ARP        60 172.16.0.1 is at 00:25:b3:bf:91:ee
 165 14.392559   HewlettP_bf:91:ee  Broadcast          ARP        60 Who has 172.16.0.1? Tell 172.16.0.105

▶ Frame 165: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▼ Ethernet II, Src: HewlettP_bf:91:ee (00:25:b3:bf:91:ee), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Source: HewlettP_bf:91:ee (00:25:b3:bf:91:ee)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▼ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HewlettP_bf:91:ee (00:25:b3:bf:91:ee)
    Sender IP address: 172.16.0.105
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.16.0.1
```

We notice an ARP connection between a Dell computer and an HP computer. In packet 54 HP computer request for the pc who has ip address of 172.16.0.107. In packet 55, the Dell computer replies to the request with confirmation and mac address.



```
52 0.424530   172.16.0.107   12.153.20.41    DNS     77 Standard query 0x3be2 A groups.google.com
57 6.553250   172.16.0.107   74.125.95.147   HTTP   960 GET /complete/gsearch?hl=en&client=hp&expI
59 6.593514   172.16.0.107   74.125.95.147   TCP     66 45691 → 80 [ACK] Seq=2364 Ack=7189 Win=254
60 6.713788   172.16.0.107   74.125.95.147   HTTP  1005 GET /complete/gsearch?hl=en&client=hp&expI
62 6.743231   172.16.0.107   74.125.95.147   TCP     66 45691 → 80 [ACK] Seq=2364 Ack=7209 Win=254
64 6.759845   172.16.0.107   74.125.95.147   TCP     66 45692 → 80 [ACK] Seq=1745 Ack=954 Win=8448
66 6.886155   172.16.0.107   74.125.95.147   TCP     66 45692 → 80 [ACK] Seq=1745 Ack=974 Win=8448
67 7.318942   172.16.0.107   74.125.95.147   HTTP  1009 GET /complete/gsearch?hl=en&client=hp&expI
69 7.364118   172.16.0.107   74.125.95.147   TCP     66 45691 → 80 [ACK] Seq=3307 Ack=7964 Win=282
71 7.469125   172.16.0.107   74.125.95.147   TCP     66 45691 → 80 [ACK] Seq=3307 Ack=7984 Win=282
72 7.620072   172.16.0.107   74.125.95.147   HTTP  1011 GET /complete/gsearch?hl=en&client=hp&expI
74 7.662402   172.16.0.107   74.125.95.147   TCP     66 45692 → 80 [ACK] Seq=2690 Ack=1742 Win=998
75 7.778428   172.16.0.107   74.125.95.147   HTTP  1015 GET /complete/gsearch?hl=en&client=hp&expI
77 7.808204   172.16.0.107   74.125.95.147   TCP     66 45692 → 80 [ACK] Seq=2690 Ack=1762 Win=998
79 7.815764   172.16.0.107   74.125.95.147   TCP     66 45691 → 80 [ACK] Seq=4256 Ack=8739 Win=309
81 7.816283   172.16.0.107   74.125.95.147   TCP     66 45691 → 80 [ACK] Seq=4256 Ack=8759 Win=309
82 7.927799   172.16.0.107   74.125.95.147   HTTP  1017 GET /complete/gsearch?hl=en&client=hp&expI
84 7.977056   172.16.0.107   74.125.95.147   TCP     66 45692 → 80 [ACK] Seq=3641 Ack=2528 Win=115
86 7.977521   172.16.0.107   74.125.95.147   TCP     66 45692 → 80 [ACK] Seq=3641 Ack=2548 Win=115
87 8.080455   172.16.0.107   74.125.95.147   HTTP  1024 GET /complete/gsearch?hl=en&client=hp&expI
89 8.122354   172.16.0.107   74.125.95.147   TCP     66 45691 → 80 [ACK] Seq=5214 Ack=9524 Win=337
91 8.122855   172.16.0.107   74.125.95.147   TCP     66 45691 → 80 [ACK] Seq=5214 Ack=9544 Win=337
92 8.385985   172.16.0.107   74.125.95.147   HTTP  1026 GET /complete/gsearch?hl=en&client=hp&expI

▶ Frame 60: 1005 bytes on wire (8040 bits), 1005 bytes captured (8040 bits)
▼ Ethernet II, Src: Dell_c0:56:f0 (00:21:70:c0:56:f0), Dst: HewlettP_bf:91:ee (00:25:b3:bf:91:ee)
  ▶ Destination: HewlettP_bf:91:ee (00:25:b3:bf:91:ee)
  ▶ Source: Dell_c0:56:f0 (00:21:70:c0:56:f0)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 172.16.0.107, Dst: 74.125.95.147
▶ Transmission Control Protocol, Src Port: 45692 (45692), Dst Port: 80 (80), Seq: 806, Ack: 216, Len: 939
▶ Hypertext Transfer Protocol
```

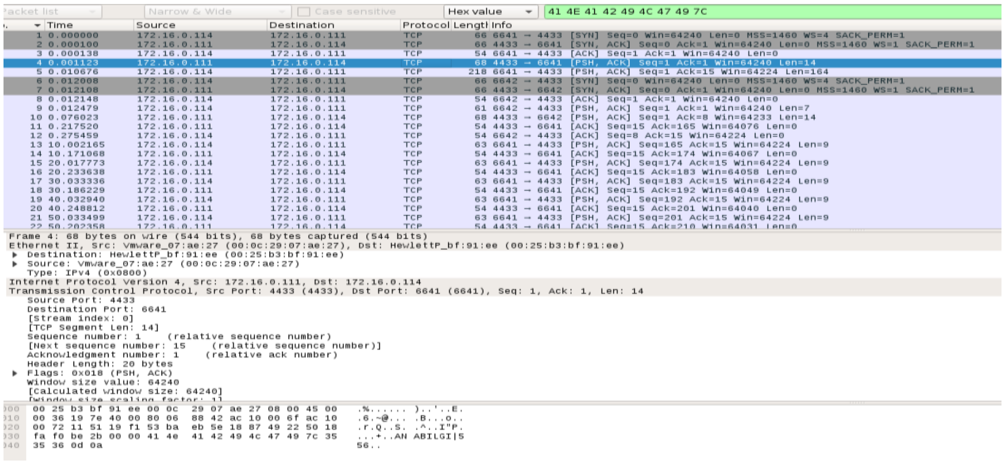
After the 56 packet we see that the hp computer is receiving all the packets from the dell computer.

The hp pc has performed ARP spoofing attack, basically linking his mac address to the dell's ip address, creating a man in the middle attack.

After, in packet 165 we see the attacker change his ip address from 172.16.0.1 to 172.16.0.5 and

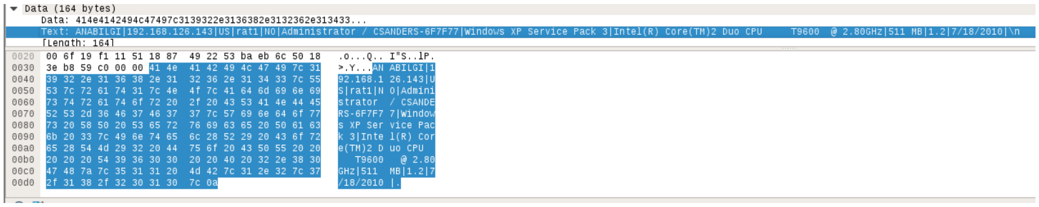
Broadcasting to see who has its previous ip address.

Ex04.pcap

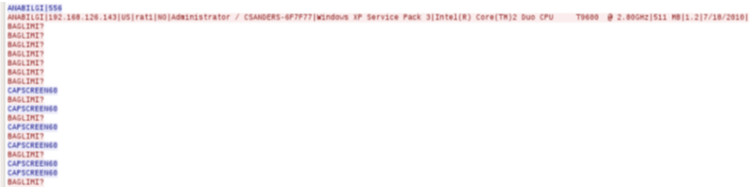


```
Packet list | Narrow & Wide | □ Case sensitive | Hex value | 41 4E 41 42 49 4C 47 49 7C

 No.  Time        Source         Destination    Protocol Length Info
  1 0.000000    172.16.0.114   172.16.0.111   TCP     66 6641 → 4433 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=4 SACK_PERM=1
  2 0.000100    172.16.0.111   172.16.0.114   TCP     66 4433 → 6641 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM=1
  3 0.000138    172.16.0.114   172.16.0.111   TCP     54 6641 → 4433 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  4 0.001123    172.16.0.111   172.16.0.114   TCP     68 4433 → 6641 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=14
  5 0.010676    172.16.0.114   172.16.0.111   TCP    218 6641 → 4433 [PSH, ACK] Seq=1 Ack=15 Win=64224 Len=164
  6 0.012008    172.16.0.114   172.16.0.111   TCP     66 6642 → 4433 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=4 SACK_PERM=1
  7 0.012108    172.16.0.111   172.16.0.114   TCP     66 4433 → 6642 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM=1
  8 0.012148    172.16.0.114   172.16.0.111   TCP     54 6642 → 4433 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  9 0.012479    172.16.0.114   172.16.0.111   TCP     61 6642 → 4433 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=7
 10 0.076023    172.16.0.111   172.16.0.114   TCP     68 4433 → 6642 [PSH, ACK] Seq=1 Ack=8 Win=64233 Len=14
 11 0.217520    172.16.0.111   172.16.0.114   TCP     54 4433 → 6641 [ACK] Seq=15 Ack=165 Win=64076 Len=0
 12 0.275459    172.16.0.114   172.16.0.111   TCP     54 6642 → 4433 [ACK] Seq=8 Ack=15 Win=64224 Len=0
 13 10.002165   172.16.0.114   172.16.0.111   TCP     63 6641 → 4433 [PSH, ACK] Seq=165 Ack=15 Win=64224 Len=9
 14 10.171068   172.16.0.111   172.16.0.114   TCP     54 4433 → 6641 [ACK] Seq=15 Ack=174 Win=64067 Len=0
 15 20.017773   172.16.0.114   172.16.0.111   TCP     63 6641 → 4433 [PSH, ACK] Seq=174 Ack=15 Win=64224 Len=9
 16 20.233638   172.16.0.111   172.16.0.114   TCP     54 4433 → 6641 [ACK] Seq=15 Ack=183 Win=64058 Len=0
 17 30.033336   172.16.0.114   172.16.0.111   TCP     63 6641 → 4433 [PSH, ACK] Seq=183 Ack=15 Win=64224 Len=9
 18 30.186229   172.16.0.111   172.16.0.114   TCP     54 4433 → 6641 [ACK] Seq=15 Ack=192 Win=64049 Len=0
 19 40.032940   172.16.0.114   172.16.0.111   TCP     63 6641 → 4433 [PSH, ACK] Seq=192 Ack=15 Win=64224 Len=9
 20 40.248812   172.16.0.111   172.16.0.114   TCP     54 4433 → 6641 [ACK] Seq=15 Ack=201 Win=64040 Len=0
 21 50.033499   172.16.0.114   172.16.0.111   TCP     63 6641 → 4433 [PSH, ACK] Seq=201 Ack=15 Win=64224 Len=9
 22 50.202358   172.16.0.111   172.16.0.114   TCP     54 4433 → 6641 [ACK] Seq=15 Ack=210 Win=64031 Len=0

Frame 4: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
Ethernet II, Src: Vmware_07:ae:27 (00:0c:29:07:ae:27), Dst: HewlettP_bf:91:ee (00:25:b3:bf:91:ee)
 ▶ Destination: HewlettP_bf:91:ee (00:25:b3:bf:91:ee)
 ▶ Source: Vmware_07:ae:27 (00:0c:29:07:ae:27)
   Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.16.0.111, Dst: 172.16.0.114
Transmission Control Protocol, Src Port: 4433 (4433), Dst Port: 6641 (6641), Seq: 1, Ack: 1, Len: 14
   Source Port: 4433
   Destination Port: 6641
   [Stream index: 0]
   [TCP Segment Len: 14]
   Sequence number: 1    (relative sequence number)
   [Next sequence number: 15    (relative sequence number)]
   Acknowledgment number: 1    (relative ack number)
   Header Length: 20 bytes
 ▶ Flags: 0x018 (PSH, ACK)
   Window size value: 64240
   [Calculated window size: 64240]
   [Window size scaling factor: 1]

000  00 25 b3 bf 91 ee 00 0c  29 07 ae 27 08 00 45 00   .%...... )..'..E.
010  00 36 19 7e 40 00 80 06  88 42 ac 10 00 6f ac 10   .6.~@... .B...o..
020  00 72 11 51 19 f1 53 ba  eb 5e 18 87 49 22 50 18   .r.Q..S. .^..I"P.
030  fa f0 be 2b 00 00 41 4e  41 42 49 4c 47 49 7c 35   ...+..AN ABILGI|5
040  35 36 0d 0a                                        56..
```

Finding the packet with the string remote access trojan we can confirm that we have been compromised.



```
▼ Data (164 bytes)
    Data: 414e4142494c47497c3139322e3136382e3132362e313433...
    Text: 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|\n
    [Length: 164]

0020  00 6f 19 f1 11 51 18 87  49 22 53 ba eb 6c 50 18   .o...Q.. I"S..lP.
0030  3e b8 59 c0 00 00 41 4e  41 42 49 4c 47 49 7c 31   >.Y...AN ABILGI|1
0040  39 32 2e 31 36 38 2e 31  32 36 2e 31 34 33 7c 55   92.168.1 26.143|U
0050  53 7c 72 61 74 31 7c 4e  4f 7c 41 64 6d 69 6e 69   S|rat1|N O|Admini
0060  73 74 72 61 74 6f 72 20  2f 20 43 53 41 4e 44 45   strator  / CSANDE
0070  52 53 2d 36 46 37 46 37  37 7c 57 69 6e 64 6f 77   RS-6F7F7 7|Window
0080  73 20 58 50 20 53 65 72  76 69 63 65 20 50 61 63   s XP Ser vice Pac
0090  6b 20 33 7c 49 6e 74 65  6c 28 52 29 20 43 6f 72   k 3|Inte l(R) Cor
00a0  65 28 54 4d 29 32 20 44  75 6f 20 43 50 55 20 20   e(TM)2 D uo CPU
00b0  20 20 20 54 39 36 30 30  20 20 40 20 32 2e 38 30      T9600   @ 2.80
00c0  47 48 7a 7c 35 31 31 20  4d 42 7c 31 2e 32 7c 37   GHz|511  MB|1.2|7
00d0  2f 31 38 2f 32 30 31 30  7c 0a                     /18/2010 |.
```



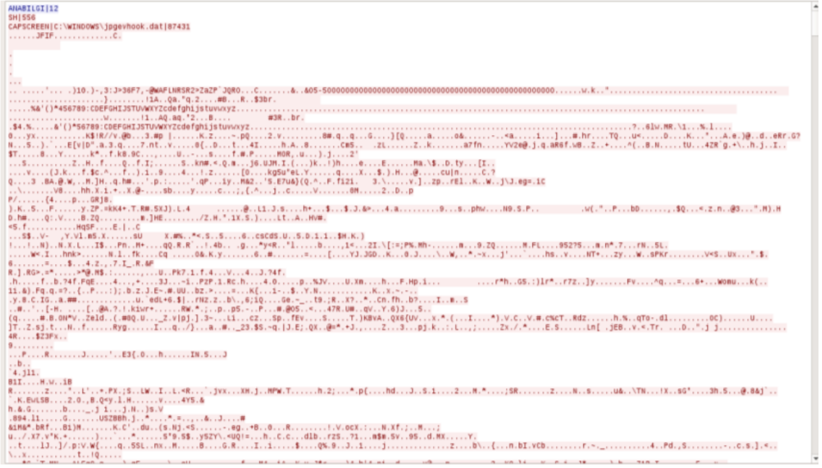
```
ANABILGI|556
ANABILGI|192.168.126.143|US|rat1|NO|Administrator / CSANDERS-6F7F77|Windows XP Service Pack 3|Intel(R) Core(TM)2 Duo CPU     T9600  @ 2.80GHz|511 MB|1.2|7/18/2010|
BAGLIMI?
BAGLIMI?
BAGLIMI?
BAGLIMI?
BAGLIMI?
BAGLIMI?
BAGLIMI?
CAPSCREEN60
BAGLIMI?
CAPSCREEN60
BAGLIMI?
CAPSCREEN60
BAGLIMI?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

Tcp stream

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|

We can see that the attacker stole information details about our system.

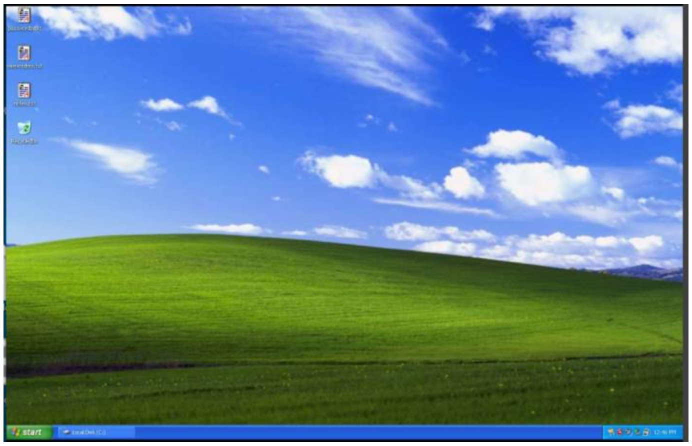
Another Tcp stream we find the data of a jpeg file.

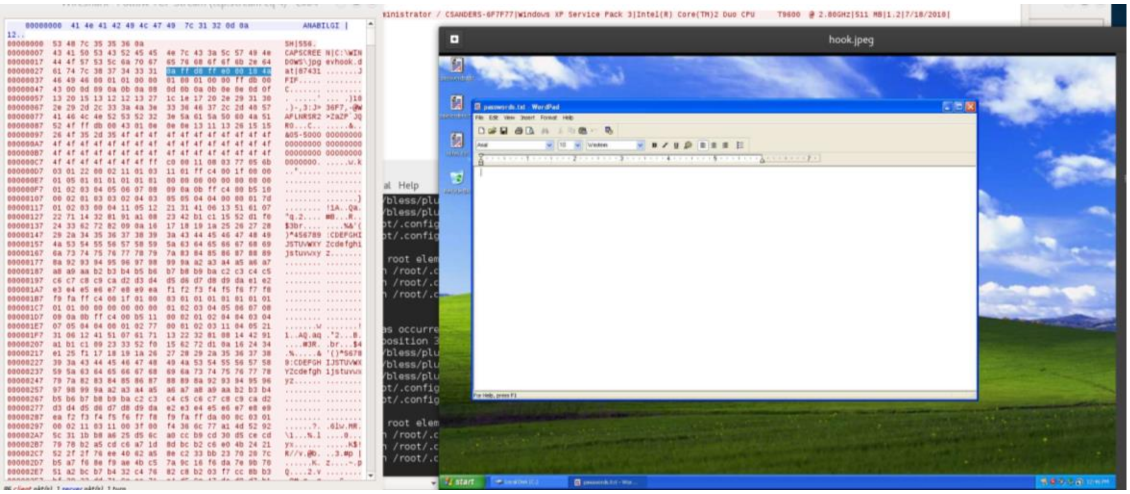


```
ANABILGI|12
SH|556
CAPSCREEN|C:\WINDOWS\jpgevhook.dat|87431
.......JFIF..............C.
.
.
.
...
.. ......'.... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C........&..&05-5000000000000000000000000000000
.........................}.........!1A..Qa."q.2....#B...R..$3br.
.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
.........................w........!1..AQ.aq.'2...B....        #3R..br.
.$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
0...yx............K$!R//v.@b...3.#p |......K.Z....~.pQ....2.v..........8#.q..q...G....}[Q.....a.
N...5..).`...E[v|D".a.3.q....7.nt..v.....0{..D...t...4I.....h.A..8.......Cm5..   .ZL.......Z..k.
$T.....8...Y......k*..f.k8.9C...,.....U..-....s....f.#.P.....MOR,.u...).j....2'
```

Dumping the raw data to a hex editor we recover the file by fixing the signature header and footer

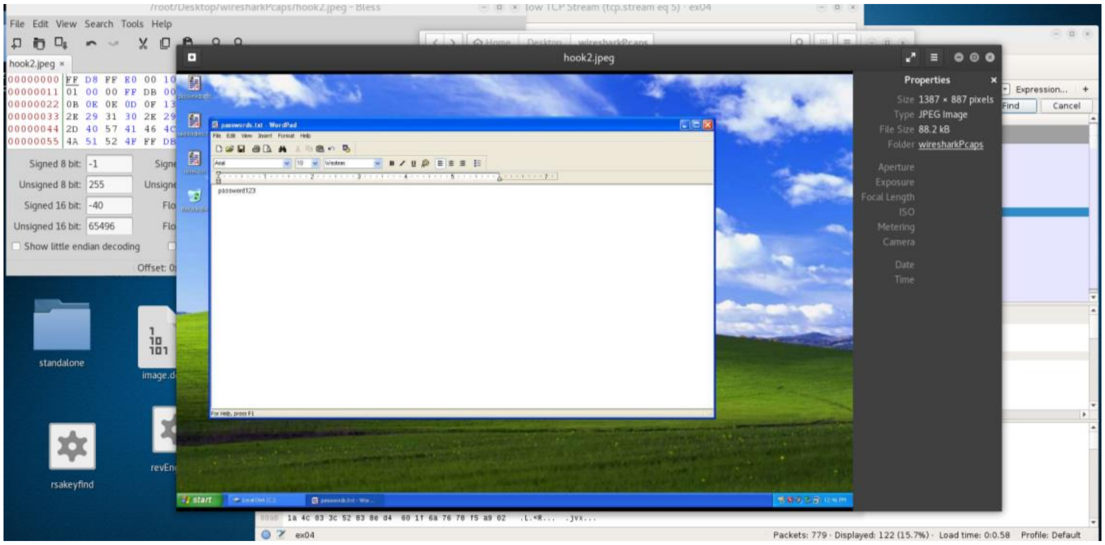
Erasing any data before the header signature 0xffh 0xd8 0xffh we recover the image file





```
    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 37 34 33 31  0a ff d8 ff e0 00 10 4a  at|87431 .......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  ........ ........
000001D7  09 0a 0b ff c4 00 b5 11  00 02 01 02 04 04 03 04  ........ ........
000001E7  07 05 04 04 00 01 02 77  00 01 02 03 11 04 05 21  .......w .......!
000001F7  31 06 12 41 51 07 61 71  13 22 32 81 08 14 42 91  1..AQ.aq ."2...B.
00000207  a1 b1 c1 09 23 33 52 f0  15 62 72 d1 0a 16 24 34  ....#3R. .br...$4
00000217  e1 25 f1 17 18 19 1a 26  27 28 29 2a 35 36 37 38  .%.....& '()*5678
00000227  39 3a 43 44 45 46 47 48  49 4a 53 54 55 56 57 58  9:CDEFGH IJSTUVWX
00000237  59 5a 63 64 65 66 67 68  69 6a 73 74 75 76 77 78  YZcdefgh ijstuvwx
00000247  79 7a 82 83 84 85 86 87  88 89 8a 92 93 94 95 96  yz...... ........
00000257  97 98 99 9a a2 a3 a4 a5  a6 a7 a8 a9 aa b2 b3 b4  ........ ........
00000267  b5 b6 b7 b8 b9 ba c2 c3  c4 c5 c6 c7 c8 c9 ca d2  ........ ........
00000277  d3 d4 d5 d6 d7 d8 d9 da  e2 e3 e4 e5 e6 e7 e8 e9  ........ ........
00000287  ea f2 f3 f4 f5 f6 f7 f8  f9 fa ff da 00 0c 03 01  ........ ........
00000297  00 02 11 03 11 00 3f 00  f4 36 6c 77 a1 4d 52 92  ......?. .6lw.MR.
000002A7  5c 31 1b b8 a6 25 d5 6c  a0 cc b9 cd 30 d5 ce cd  \1...%.l ....0...
000002B7  79 78 b2 a5 cd c6 a7 1d  8d bc b2 c6 e0 4b 24 21  yx...... .....K$!
000002C7  52 2f 2f 76 ee 40 62 a5  8e c2 33 bb 23 70 28 7c  R//v.@b. ..3.#p (|
000002D7  b5 a7 f6 8e f9 ae 4b c5  7a 9c 16 f6 da 7e 9b 70  ......K. z....~.p
000002E7  51 a2 bc b7 b4 32 c4 76  82 c8 b2 03 f7 cc 8b b3  Q....2.v ........
```

```
ministrator / CSANDERS-6F7F77|Windows XP Service Pack 3|Intel(R) Core(TM)2 Duo CPU     T9600  @ 2.80GHz|511 MB|1.2|7/18/2010|
```



```
00000000 FF D8 FF E0 00 10
00000011 01 00 00 FF DB 00
00000022 0B 0E 0E 0D 0F 13
00000033 2E 29 31 30 2E 29
00000044 2D 40 57 41 46 4C
00000055 4A 51 52 4F FF DB
```

Signed 8 bit: -1

Unsigned 8 bit: 255

Signed 16 bit: -40

Unsigned 16 bit: 65496

□ Show little endian decoding

password123

Size 1387 × 887 pixels

Type JPEG Image

File Size 88.2 kB

Folder wiresharkPcaps

Packets: 779 · Displayed: 122 (15.7%) · Load time: 0:0.58   Profile: Default

We have recover various image files and we can see that one of the image file is a screenshot of a passwords.txt file, containing the password: “password123”

So, the attacker was able to steal the password!