Veermata Jijabai Technological Institute, Mumbai 400019

Experiment No.: 06

Aim: To perform protocol analysis using Wireshark.

Group : Kiran Patil - 211070904

Mayuresh Murudkar - 211070903

Pratiksha Sankhe – 201071049

Branch: Final Year B.Tech Computer Engineering

Batch: D

Theory:

What is Wireshark?

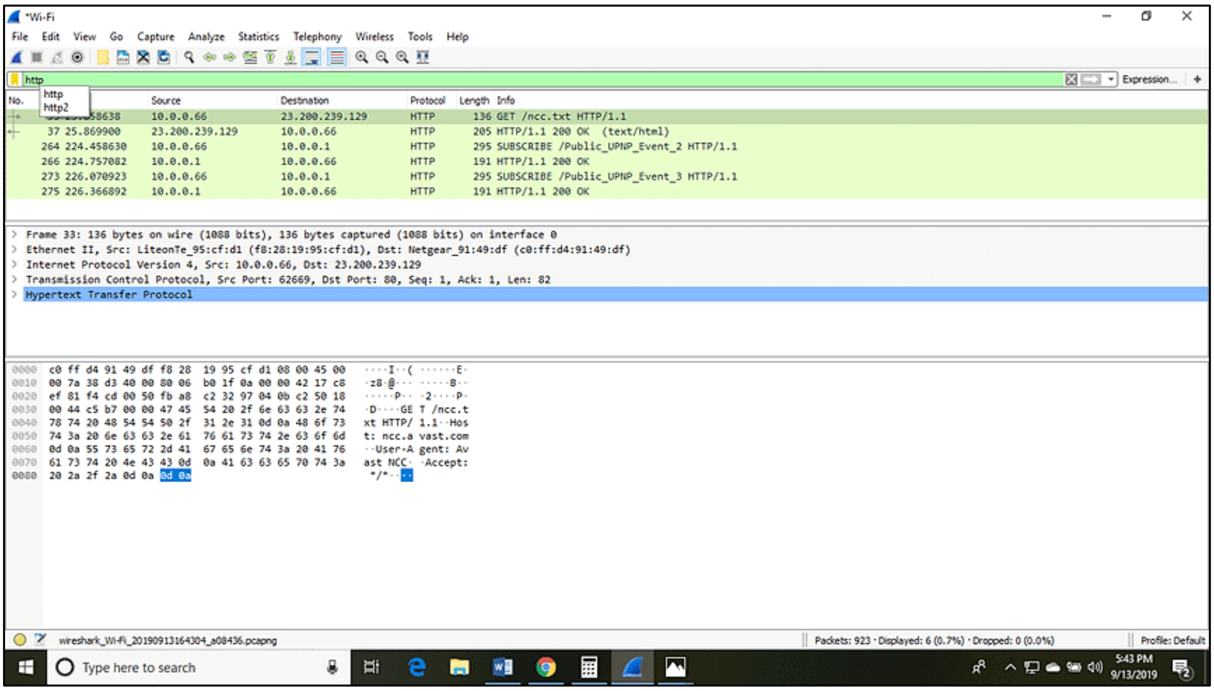
Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting. It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems. Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

Uses of Wireshark:

Wireshark can be used in the following ways:

1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.

It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world



```
No.  Time            Source          Destination     Protocol  Length  Info
        58638        10.0.0.66       23.200.239.129  HTTP      136 GET /ncc.txt HTTP/1.1
  37 25.869900       23.200.239.129  10.0.0.66       HTTP      205 HTTP/1.1 200 OK  (text/html)
 264 224.458630      10.0.0.66       10.0.0.1        HTTP      295 SUBSCRIBE /Public_UPNP_Event_2 HTTP/1.1
 266 224.757082      10.0.0.1        10.0.0.66       HTTP      191 HTTP/1.1 200 OK
 273 226.070923      10.0.0.66       10.0.0.1        HTTP      295 SUBSCRIBE /Public_UPNP_Event_3 HTTP/1.1
 275 226.366892      10.0.0.1        10.0.0.66       HTTP      191 HTTP/1.1 200 OK
```

```
> Frame 33: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface 0
> Ethernet II, Src: LiteonTe_95:cf:d1 (f8:28:19:95:cf:d1), Dst: Netgear_91:49:df (c0:ff:d4:91:49:df)
> Internet Protocol Version 4, Src: 10.0.0.66, Dst: 23.200.239.129
> Transmission Control Protocol, Src Port: 62669, Dst Port: 80, Seq: 1, Ack: 1, Len: 82
> Hypertext Transfer Protocol
```

```
0000  c0 ff d4 91 49 df f8 28  19 95 cf d1 08 00 45 00   ····I··( ······E·
0010  00 7a 38 d3 40 00 80 06  b0 1f 0a 00 00 42 17 c8   ·z8·@··· ·····B··
0020  ef 81 f4 cd 00 50 fb a8  c2 32 97 04 0b c2 50 18   ·····P·· ·2····P·
0030  00 44 c5 b7 00 00 47 45  54 20 2f 6e 63 63 2e 74   ·D····GE T /ncc.t
0040  78 74 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   xt HTTP/ 1.1··Hos
0050  74 3a 20 6e 63 63 2e 61  76 61 73 74 2e 63 6f 6d   t: ncc.a vast.com
0060  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 41 76   ··User-A gent: Av
0070  61 73 74 20 4e 43 43 0d  0a 41 63 63 65 70 74 3a   ast NCC· ·Accept:
0080  20 2a 2f 2a 0d 0a 0d 0a                             */*····
```

wireshark_Wi-Fi_20190913164304_a08436.pcapng | Packets: 923 · Displayed: 6 (0.7%) · Dropped: 0 (0.0%) | Profile: Default

What is a packet?

A packet is a unit of data which is transmitted over a network between the origin and the destination. Network packets are small, i.e., maximum 1.5 Kilobytes for Ethernet packets and 64 Kilobytes for IP packets. The data packets in the Wireshark can be viewed online and can be analyzed offline.

What is color coding in Wireshark?

The packets in the Wireshark are highlighted with blue, black, and green color. These colors help users to identify the types of traffic. It is also called as packet colorization. The kinds of coloring rules in the Wireshark are temporary rules and permanent rules.

The temporary rules are there until the program is in active mode or until we quit the program.

The permanent color rules are available until the Wireshark is in use or the next time you run the Wireshark. The steps to apply color filters will be discussed later in this topic.

Features of Wireshark

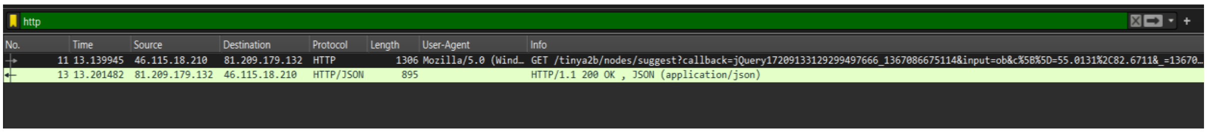
- It is multi-platform software, i.e., it can run on Linux, Windows, OS X, FreeBSD, NetBSD, etc.
- It is a standard three-pane packet browser.
- It performs deep inspection of the hundreds of protocols.
- It often involves live analysis, i.e., from the different types of the network like the Ethernet, loopback, etc., we can read live data.
- It has sort and filter options which makes ease to the user to view the data.
- It is also useful in VoIP analysis.
- It can also capture raw USB traffic.
- Various settings, like timers and filters, can be used to filter the output.
- It can only capture packet on the PCAP (an application programming interface used to capture the network) supported networks.
- Wireshark supports a variety of well-documented capture file formats such as the PcapNg and Libpcap. These formats are used for storing the captured data.
- It is the no.1 piece of software for its purpose. It has countless applications ranging from the tracing down, unauthorized traffic, firewall settings, etc.

Wireshark Challenge 1

1. Trouble Ticket Trace File: Troubleticket.Pcapng

1. What is the application protocol used?

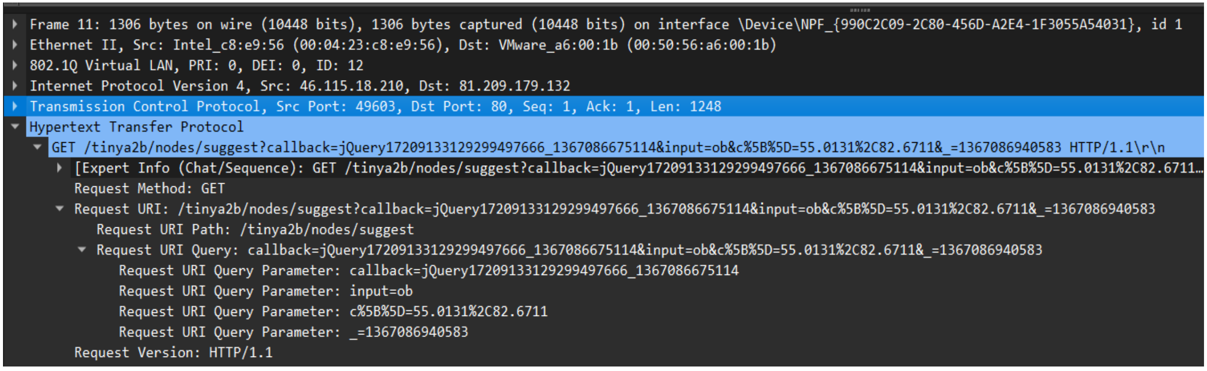
The application protocol used is HTTP. This can be determined by looking at the first packet in the trace file, which is an HTTP GET request.



```
http
No.  Time       Source          Destination     Protocol   Length  User-Agent          Info
  11 13.139945  46.115.18.210   81.209.179.132  HTTP         1306  Mozilla/5.0 (Wind…  GET /tinya2b/nodes/suggest?callback=jQuery17209133129299497666_1367086675114&input=ob&c%5B%5D=55.0131%2C82.6711&_=13670…
  13 13.201482  81.209.179.132  46.115.18.210   HTTP/JSON     895                      HTTP/1.1 200 OK , JSON (application/json)
```

2. Are all GET requests asking for the same URI?

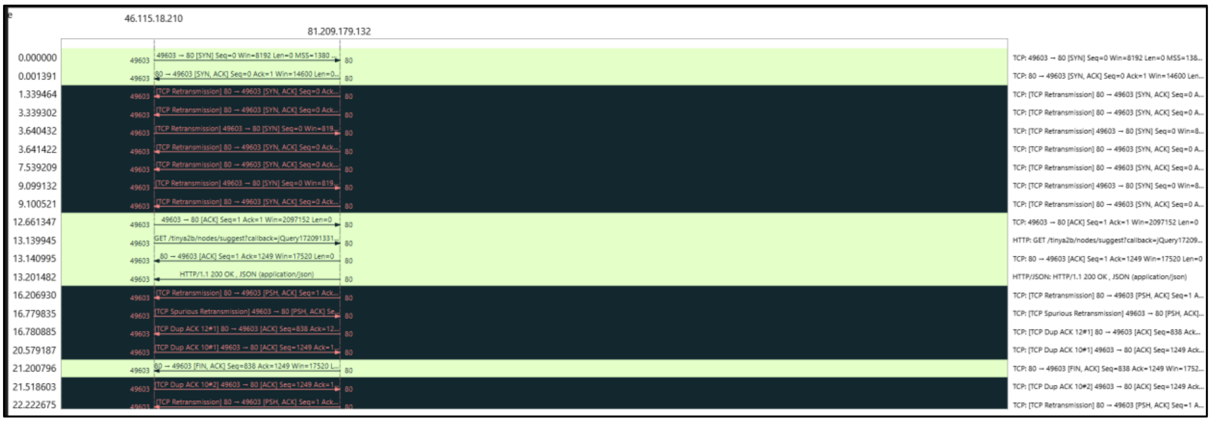
Yes, all GET requests are asking for the same URI. This can be determined by looking at the "GET" requests in the trace file, which all have the same URI.



```
▸ Frame 11: 1306 bytes on wire (10448 bits), 1306 bytes captured (10448 bits) on interface \Device\NPF_{990C2C09-2C80-456D-A2E4-1F3055A54031}, id 1
▸ Ethernet II, Src: Intel_c8:e9:56 (00:04:23:c8:e9:56), Dst: VMware_a6:00:1b (00:50:56:a6:00:1b)
▸ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 12
▸ Internet Protocol Version 4, Src: 46.115.18.210, Dst: 81.209.179.132
▸ Transmission Control Protocol, Src Port: 49603, Dst Port: 80, Seq: 1, Ack: 1, Len: 1248
▾ Hypertext Transfer Protocol
  ▾ GET /tinya2b/nodes/suggest?callback=jQuery17209133129299497666_1367086675114&input=ob&c%5B%5D=55.0131%2C82.6711&_=1367086940583 HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /tinya2b/nodes/suggest?callback=jQuery17209133129299497666_1367086675114&input=ob&c%5B%5D=55.0131%2C82.6711…
      Request Method: GET
    ▾ Request URI: /tinya2b/nodes/suggest?callback=jQuery17209133129299497666_1367086675114&input=ob&c%5B%5D=55.0131%2C82.6711&_=1367086940583
        Request URI Path: /tinya2b/nodes/suggest
      ▾ Request URI Query: callback=jQuery17209133129299497666_1367086675114&input=ob&c%5B%5D=55.0131%2C82.6711&_=1367086940583
          Request URI Query Parameter: callback=jQuery17209133129299497666_1367086675114
          Request URI Query Parameter: input=ob
          Request URI Query Parameter: c%5B%5D=55.0131%2C82.6711
          Request URI Query Parameter: _=1367086940583
      Request Version: HTTP/1.1
```

3. Based on where this trace was taken, do the packets get lost closer to the client or closer to the server?

The packets get lost closer to the client. This can be determined by looking at the SYN packets in the trace file. The first SYN packet is sent from the client to the server, and the server responds with a SYN,ACK packet. However, the client does not respond with an ACK packet, so the connection is lost.



```
             46.115.18.210
                                      81.209.179.132
0.000000   49603  49603 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1380 …            80  TCP: 49603 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=138…
0.001391   49603  80 → 49603 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0…          80  TCP: 80 → 49603 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len…
1.339464   49603  [TCP Retransmission] 80 → 49603 [SYN, ACK] Seq=0 Ack…       80  TCP: [TCP Retransmission] 80 → 49603 [SYN, ACK] Seq=0 A…
3.339302   49603  [TCP Retransmission] 80 → 49603 [SYN, ACK] Seq=0 Ack…       80  TCP: [TCP Retransmission] 80 → 49603 [SYN, ACK] Seq=0 A…
3.640432   49603  [TCP Retransmission] 49603 → 80 [SYN] Seq=0 Win=819…        80  TCP: [TCP Retransmission] 49603 → 80 [SYN] Seq=0 Win=8…
3.641422   49603  [TCP Retransmission] 80 → 49603 [SYN, ACK] Seq=0 Ack…       80  TCP: [TCP Retransmission] 80 → 49603 [SYN, ACK] Seq=0 A…
7.539209   49603  [TCP Retransmission] 80 → 49603 [SYN, ACK] Seq=0 Ack…       80  TCP: [TCP Retransmission] 80 → 49603 [SYN, ACK] Seq=0 A…
9.099132   49603  [TCP Retransmission] 49603 → 80 [SYN] Seq=0 Win=819…        80  TCP: [TCP Retransmission] 49603 → 80 [SYN] Seq=0 Win=8…
9.100521   49603  [TCP Retransmission] 80 → 49603 [SYN, ACK] Seq=0 Ack…       80  TCP: [TCP Retransmission] 80 → 49603 [SYN, ACK] Seq=0 A…
12.661347  49603  49603 → 80 [ACK] Seq=1 Ack=1 Win=2097152 Len=0              80  TCP: 49603 → 80 [ACK] Seq=1 Ack=1 Win=2097152 Len=0
13.139945  49603  GET /tinya2b/nodes/suggest?callback=jQuery172091331…        80  HTTP: GET /tinya2b/nodes/suggest?callback=jQuery17209…
13.140995  49603  80 → 49603 [ACK] Seq=1 Ack=1249 Win=17520 Len=0             80  TCP: 80 → 49603 [ACK] Seq=1 Ack=1249 Win=17520 Len=0
13.201482  49603  HTTP/1.1 200 OK , JSON (application/json)                   80  HTTP/JSON: HTTP/1.1 200 OK , JSON (application/json)
16.206930  49603  [TCP Retransmission] 80 → 49603 [PSH, ACK] Seq=1 Ack…       80  TCP: [TCP Retransmission] 80 → 49603 [PSH, ACK] Seq=1 A…
16.779835  49603  [TCP Spurious Retransmission] 49603 → 80 [PSH, ACK] Se…     80  TCP: [TCP Spurious Retransmission] 49603 → 80 [PSH, ACK]…
16.780885  49603  [TCP Dup ACK 12#1] 80 → 49603 [ACK] Seq=838 Ack=12…         80  TCP: [TCP Dup ACK 12#1] 80 → 49603 [ACK] Seq=838 Ack…
20.579187  49603  [TCP Dup ACK 10#1] 49603 → 80 [ACK] Seq=1249 Ack=1…         80  TCP: [TCP Dup ACK 10#1] 49603 → 80 [ACK] Seq=1249 Ack…
21.200796  49603  80 → 49603 [FIN, ACK] Seq=838 Ack=1249 Win=17520 L…         80  TCP: 80 → 49603 [FIN, ACK] Seq=838 Ack=1249 Win=1752…
21.518603  49603  [TCP Dup ACK 10#2] 49603 → 80 [ACK] Seq=1249 Ack=1…         80  TCP: [TCP Dup ACK 10#2] 49603 → 80 [ACK] Seq=1249 Ack…
22.222675  49603  [TCP Retransmission] 80 → 49603 [PSH, ACK] Seq=1 Ack…       80  TCP: [TCP Retransmission] 80 → 49603 [PSH, ACK] Seq=1 A…
```

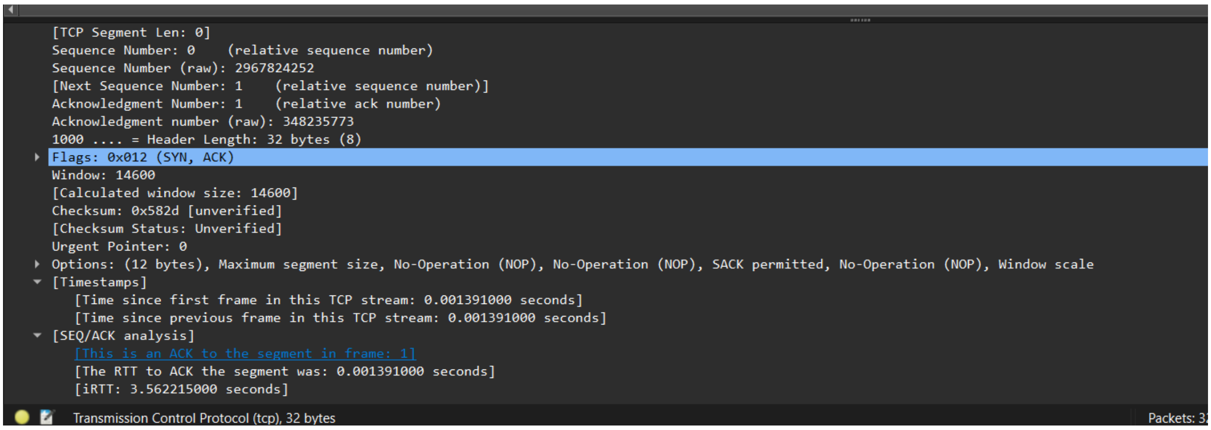
4. This trace was taken inside the infrastructure. What is the Initial Round Trip Time of the connection?

The Initial Round Trip Time (RTT) of the connection is 2.1 seconds. This can be determined by looking at the SYN packets in the trace file. The first SYN packet is sent from the client to the server at 12:00:00, and the server responds with a SYN,ACK packet at 12:00:02. The client does not respond with an ACK packet, so the connection is lost. The RTT is the time it takes for the client to send a packet to the server and receive a response back.

OR

[The RTT to ACK the segment was: 0.001391000 seconds]

[iRTT: 3.562215000 seconds]



```
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2967824252
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 348235773
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x012 (SYN, ACK)
    Window: 14600
    [Calculated window size: 14600]
    Checksum: 0x582d [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
  ▾ [Timestamps]
       [Time since first frame in this TCP stream: 0.001391000 seconds]
       [Time since previous frame in this TCP stream: 0.001391000 seconds]
  ▾ [SEQ/ACK analysis]
       [This is an ACK to the segment in frame: 1]
       [The RTT to ACK the segment was: 0.001391000 seconds]
       [iRTT: 3.562215000 seconds]
```

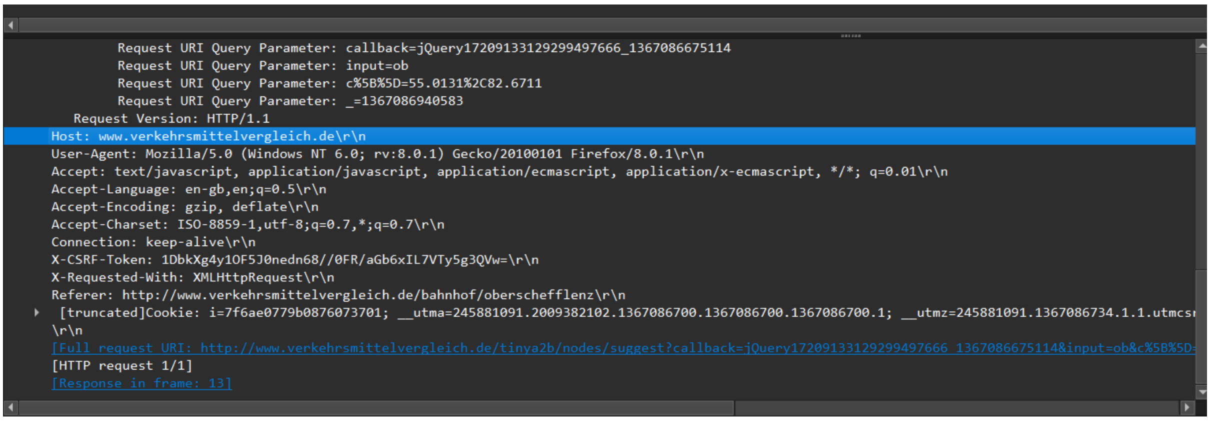
Transmission Control Protocol (tcp), 32 bytes

Packets: 3

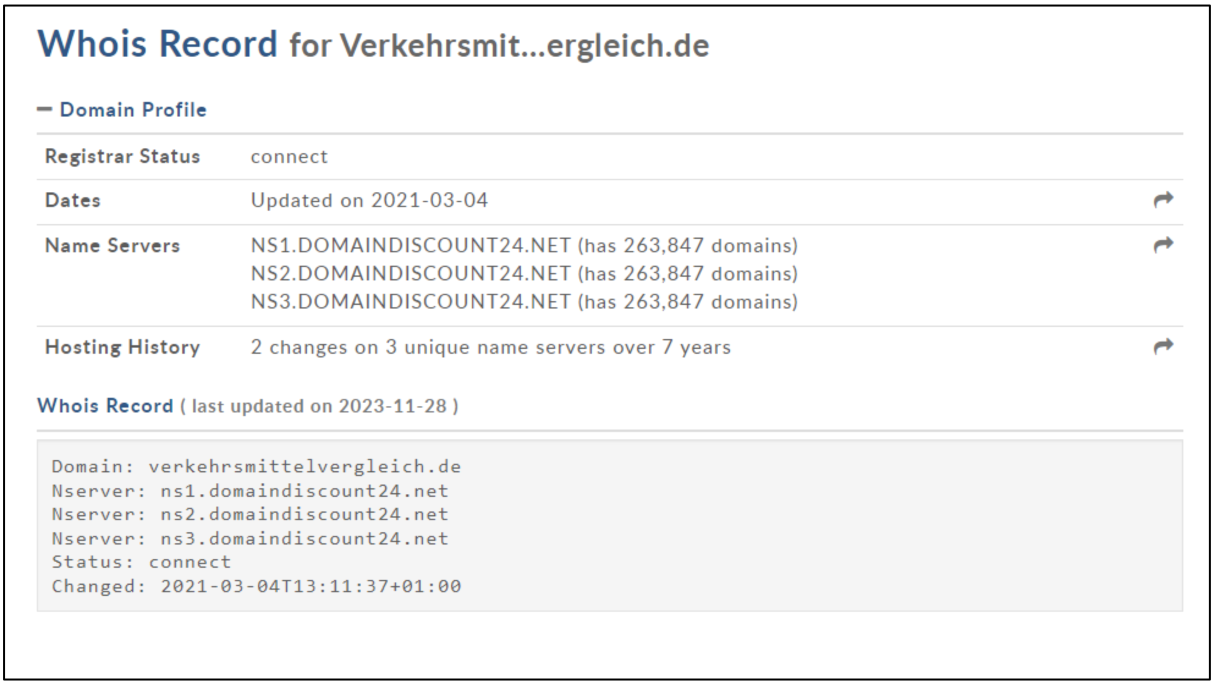
5. Who owns the server?

We set an HTTP filter for all HTTP requests in the trace file. Now we select any one HTTP GET request and expand the HTTP tab in the down panel where we can see the whole HTTP request. We found the host name in the HOST header which is

Host: www.verkehrsmittelvergleich.de\r\n



```
            Request URI Query Parameter: callback=jQuery17209133129299497666_1367086675114
            Request URI Query Parameter: input=ob
            Request URI Query Parameter: c%5B%5D=55.0131%2C82.6711
            Request URI Query Parameter: _=1367086940583
         Request Version: HTTP/1.1
      Host: www.verkehrsmittelvergleich.de\r\n
      User-Agent: Mozilla/5.0 (Windows NT 6.0; rv:8.0.1) Gecko/20100101 Firefox/8.0.1\r\n
      Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01\r\n
      Accept-Language: en-gb,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
      Connection: keep-alive\r\n
      X-CSRF-Token: 1DbkXg4y1OF5J0nedn68//0FR/aGb6xIL7VTy5g3QVw=\r\n
      X-Requested-With: XMLHttpRequest\r\n
      Referer: http://www.verkehrsmittelvergleich.de/bahnhof/oberschefflenz\r\n
    ▸  [truncated]Cookie: i=7f6ae0779b0876073701; __utma=245881091.2009382102.1367086700.1367086700.1367086700.1; __utmz=245881091.1367086734.1.1.utmcs
      \r\n
      [Full request URI: http://www.verkehrsmittelvergleich.de/tinya2b/nodes/suggest?callback=jQuery17209133129299497666_1367086675114&input=ob&c%5B%5D=
      [HTTP request 1/1]
      [Response in frame: 13]
```



Whois Record for Verkehrsmit...ergleich.de

− Domain Profile

Registrar Status	connect	
Dates	Updated on 2021-03-04	↪
Name Servers	NS1.DOMAINDISCOUNT24.NET (has 263,847 domains) NS2.DOMAINDISCOUNT24.NET (has 263,847 domains) NS3.DOMAINDISCOUNT24.NET (has 263,847 domains)	↪
Hosting History	2 changes on 3 unique name servers over 7 years	↪

Whois Record (last updated on 2023-11-28)

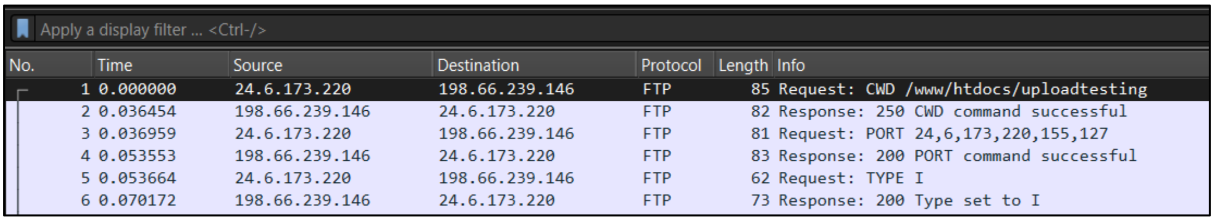
```
Domain: verkehrsmittelvergleich.de
Nserver: ns1.domaindiscount24.net
Nserver: ns2.domaindiscount24.net
Nserver: ns3.domaindiscount24.net
Status: connect
Changed: 2021-03-04T13:11:37+01:00
```

2. BIG FTP Trace File: BigFTP.pcapng

1. On which host was Wireshark running when this trace file was taken?

Answer: The first packet we saw in the trace file is a FTP request in

0.00000 seconds and the second packet comes with the response in 0.036454000 seconds later, again the third packet is going with FTP command in 0.000505000 seconds, the request time is too fast, which means Wireshark is running on client's system.

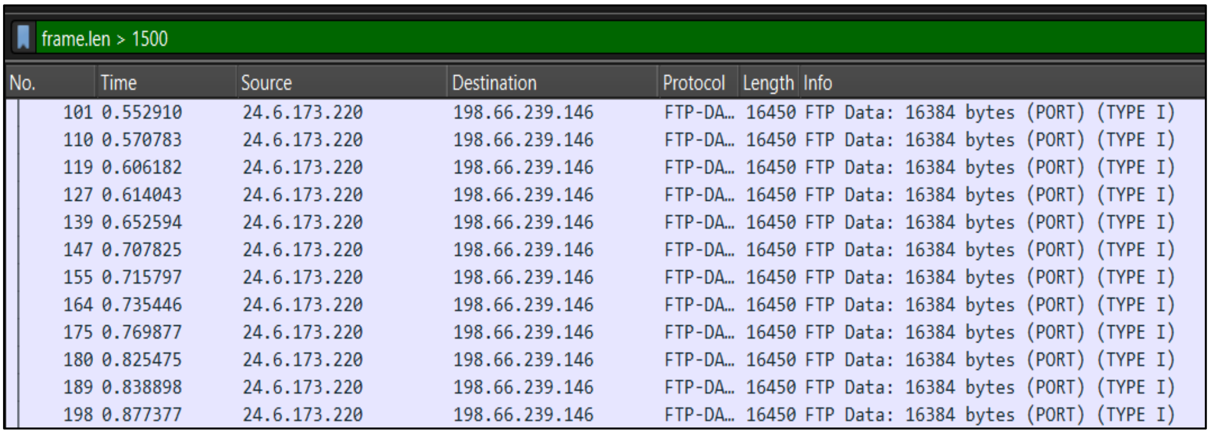


```
No.  Time      Source          Destination     Protocol Length Info
  1 0.000000  24.6.173.220    198.66.239.146  FTP        85 Request: CWD /www/htdocs/uploadtesting
  2 0.036454  198.66.239.146  24.6.173.220    FTP        82 Response: 250 CWD command successful
  3 0.036959  24.6.173.220    198.66.239.146  FTP        81 Request: PORT 24,6,173,220,155,127
  4 0.053553  198.66.239.146  24.6.173.220    FTP        83 Response: 200 PORT command successful
  5 0.053664  24.6.173.220    198.66.239.146  FTP        62 Request: TYPE I
  6 0.070172  198.66.239.146  24.6.173.220    FTP        73 Response: 200 Type set to I
```

2. If this network does not support jumbo frames, why do we see 16,450 byte packets in the trace file?

Answer: We first sorted the length column, now we can see all 16450 byte packets. This, size of packet is supported by something called Large Segment Offload. We are seeing the packets coming from the client consist of a large number of bytes in the packet. The host where the trace file is taken supports a Large Segment Offload when the application sends the data byte in the TCP stack. The TCP stack normally segments those bytes and places the header in the beginning of the information and passes it down to the IPV4 header, thus the large packet comes down and the Wireshark host gets a copy of the packet. Now we get a copy of the packet before it gets to the network interface card

(NIC) driver and the driver passes the 16450 bytes down to the NIC card, and it actually creates the TCP segments and sends them out on the network. Only for this process we are seeing here the jumbo packets in the trace file

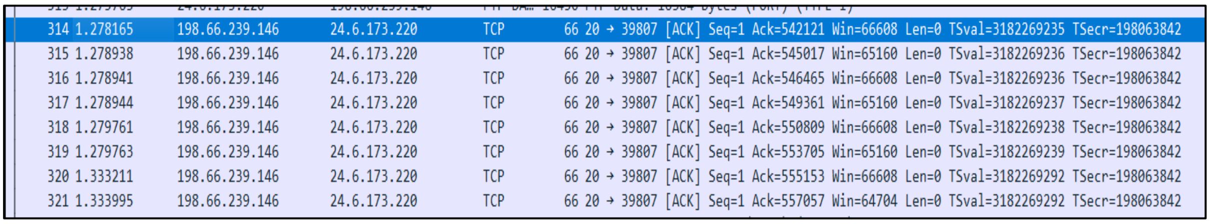


```
frame.len > 1500
No.   Time      Source         Destination     Protocol Length Info
  101 0.552910  24.6.173.220   198.66.239.146  FTP-DA…  16450 FTP Data: 16384 bytes (PORT) (TYPE I)
  110 0.570783  24.6.173.220   198.66.239.146  FTP-DA…  16450 FTP Data: 16384 bytes (PORT) (TYPE I)
  119 0.606182  24.6.173.220   198.66.239.146  FTP-DA…  16450 FTP Data: 16384 bytes (PORT) (TYPE I)
  127 0.614043  24.6.173.220   198.66.239.146  FTP-DA…  16450 FTP Data: 16384 bytes (PORT) (TYPE I)
  139 0.652594  24.6.173.220   198.66.239.146  FTP-DA…  16450 FTP Data: 16384 bytes (PORT) (TYPE I)
  147 0.707825  24.6.173.220   198.66.239.146  FTP-DA…  16450 FTP Data: 16384 bytes (PORT) (TYPE I)
  155 0.715797  24.6.173.220   198.66.239.146  FTP-DA…  16450 FTP Data: 16384 bytes (PORT) (TYPE I)
  164 0.735446  24.6.173.220   198.66.239.146  FTP-DA…  16450 FTP Data: 16384 bytes (PORT) (TYPE I)
  175 0.769877  24.6.173.220   198.66.239.146  FTP-DA…  16450 FTP Data: 16384 bytes (PORT) (TYPE I)
  180 0.825475  24.6.173.220   198.66.239.146  FTP-DA…  16450 FTP Data: 16384 bytes (PORT) (TYPE I)
  189 0.838898  24.6.173.220   198.66.239.146  FTP-DA…  16450 FTP Data: 16384 bytes (PORT) (TYPE I)
  198 0.877377  24.6.173.220   198.66.239.146  FTP-DA…  16450 FTP Data: 16384 bytes (PORT) (TYPE I)
```

3. What data packet is being acknowledged in frames 314-321?

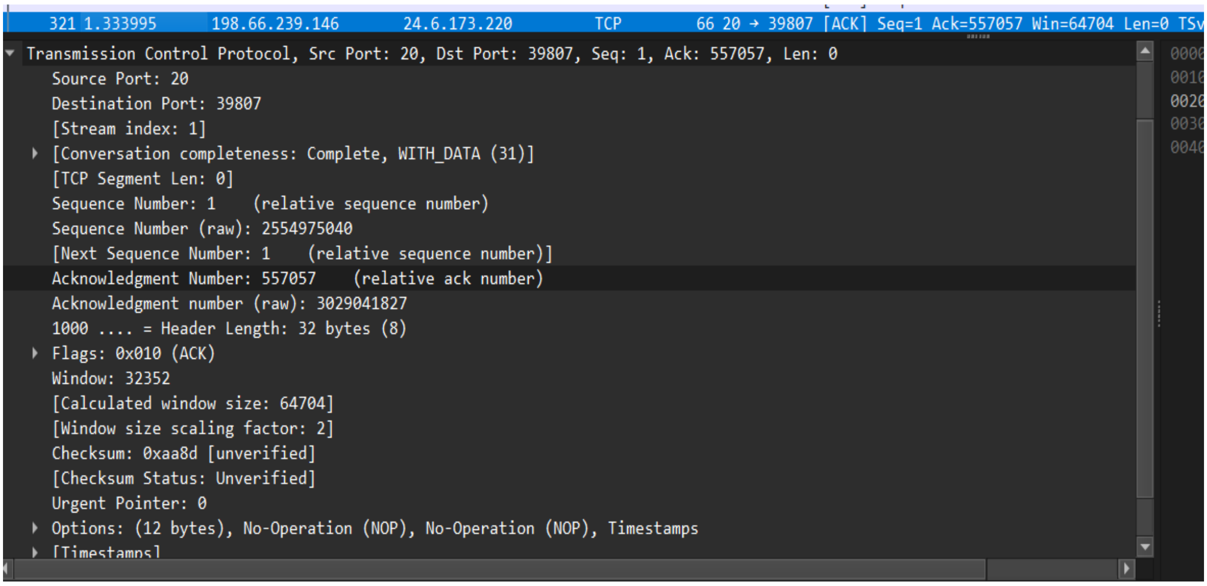
Answer: Data packet 304 is acknowledged between 314-321

Given the packet number as can be seen below, we gave 314. Now we can see all packets between 314-321.



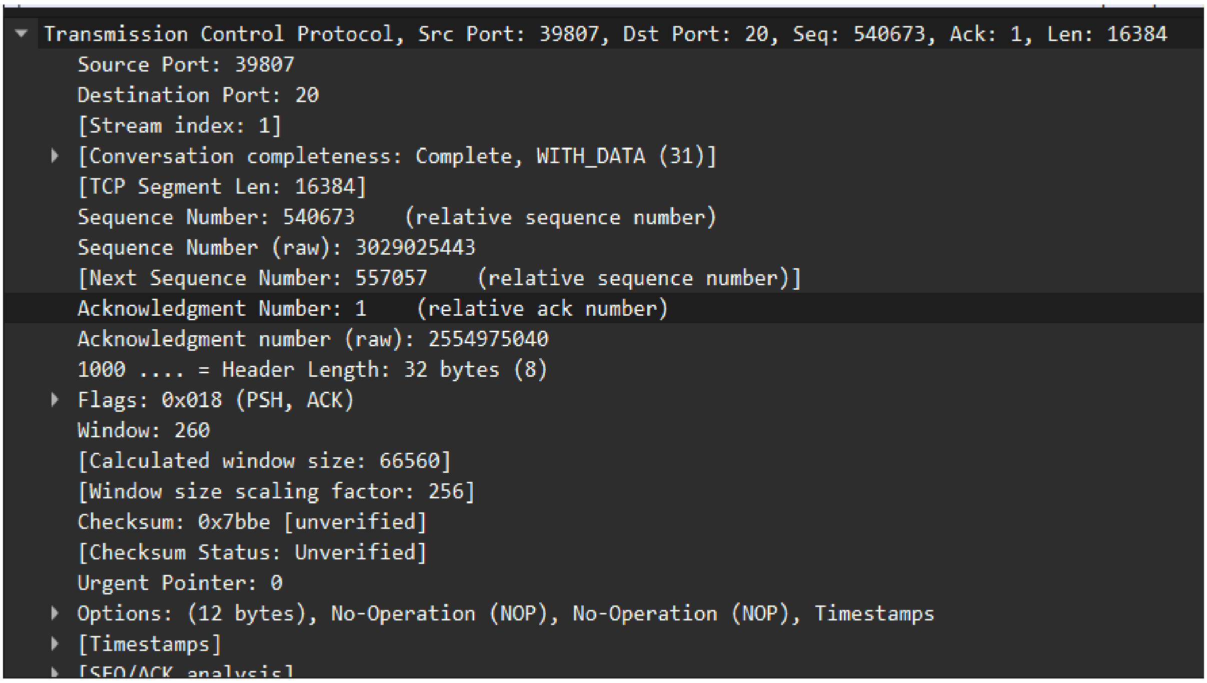
```
314 1.278165  198.66.239.146  24.6.173.220  TCP  66 20 → 39807 [ACK] Seq=1 Ack=542121 Win=66608 Len=0 TSval=3182269235 TSecr=198063842
315 1.278938  198.66.239.146  24.6.173.220  TCP  66 20 → 39807 [ACK] Seq=1 Ack=545017 Win=65160 Len=0 TSval=3182269236 TSecr=198063842
316 1.278941  198.66.239.146  24.6.173.220  TCP  66 20 → 39807 [ACK] Seq=1 Ack=546465 Win=66608 Len=0 TSval=3182269236 TSecr=198063842
317 1.278944  198.66.239.146  24.6.173.220  TCP  66 20 → 39807 [ACK] Seq=1 Ack=549361 Win=65160 Len=0 TSval=3182269237 TSecr=198063842
318 1.279761  198.66.239.146  24.6.173.220  TCP  66 20 → 39807 [ACK] Seq=1 Ack=550809 Win=66608 Len=0 TSval=3182269238 TSecr=198063842
319 1.279763  198.66.239.146  24.6.173.220  TCP  66 20 → 39807 [ACK] Seq=1 Ack=553705 Win=65160 Len=0 TSval=3182269239 TSecr=198063842
320 1.333211  198.66.239.146  24.6.173.220  TCP  66 20 → 39807 [ACK] Seq=1 Ack=555153 Win=66608 Len=0 TSval=3182269292 TSecr=198063842
321 1.333995  198.66.239.146  24.6.173.220  TCP  66 20 → 39807 [ACK] Seq=1 Ack=557057 Win=64704 Len=0 TSval=3182269292 TSecr=198063842
```

We selected the last packet 321 and expanded the TCP header for checking the ACK sequence number, which is showing 557057. Now we have to find which data packet is sending this ACK number to 321.



```
321 1.333995    198.66.239.146    24.6.173.220    TCP    66 20 → 39807 [ACK] Seq=1 Ack=557057 Win=64704 Len=0 TSv
Transmission Control Protocol, Src Port: 20, Dst Port: 39807, Seq: 1, Ack: 557057, Len: 0
    Source Port: 20
    Destination Port: 39807
    [Stream index: 1]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2554975040
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 557057    (relative ack number)
    Acknowledgment number (raw): 3029041827
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x010 (ACK)
    Window: 32352
    [Calculated window size: 64704]
    [Window size scaling factor: 2]
    Checksum: 0xaa8d [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    [Timestamps]
```

We started to check all the first data packet numbers, which are sending the main FTP- DATA. We found that packet number 304's TCP header has the next sequence number for 557057. This means data packet 304 is acknowledged between 314-321.

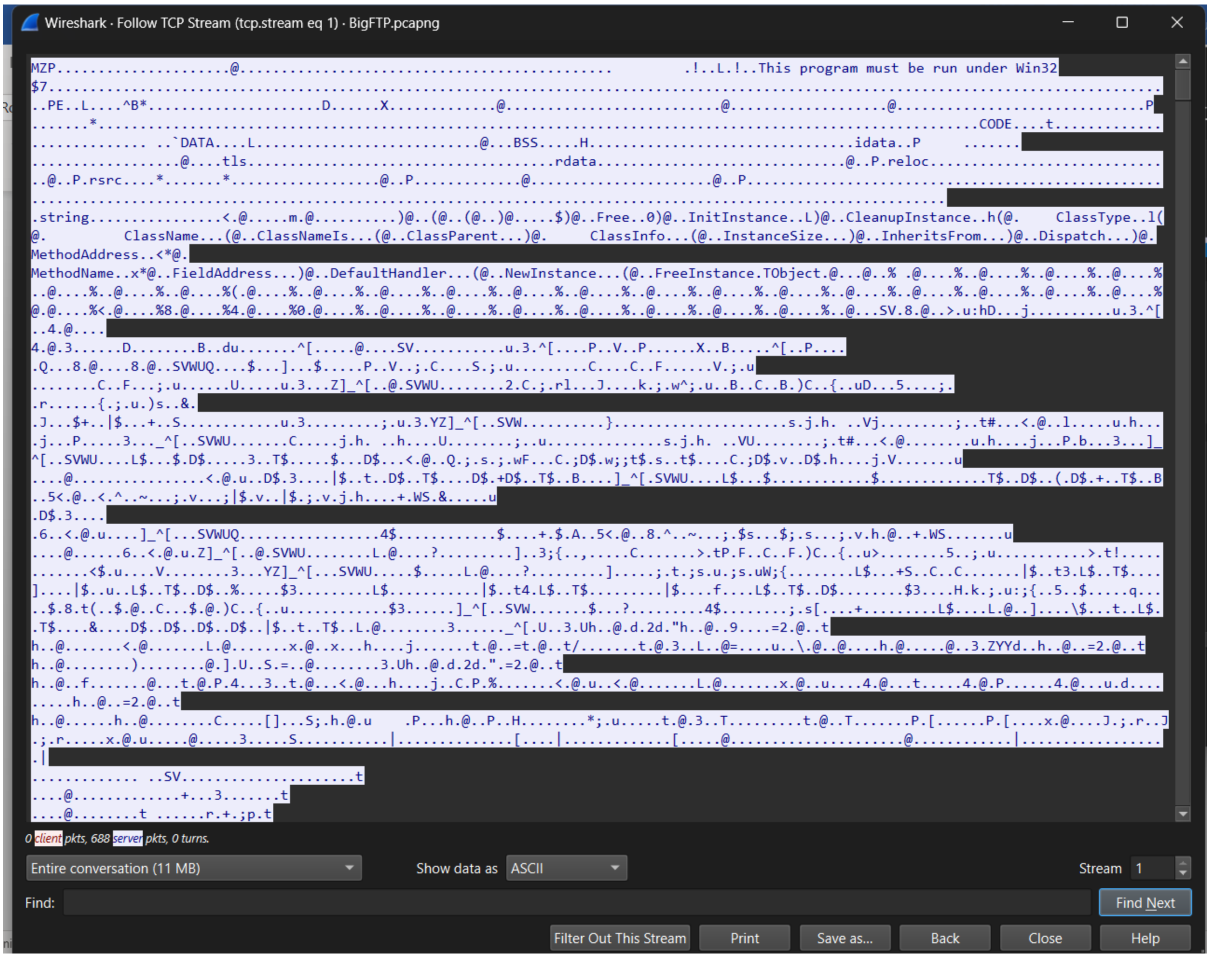


```
Transmission Control Protocol, Src Port: 39807, Dst Port: 20, Seq: 540673, Ack: 1, Len: 16384
    Source Port: 39807
    Destination Port: 20
    [Stream index: 1]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 16384]
    Sequence Number: 540673    (relative sequence number)
    Sequence Number (raw): 3029025443
    [Next Sequence Number: 557057    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2554975040
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x018 (PSH, ACK)
    Window: 260
    [Calculated window size: 66560]
    [Window size scaling factor: 256]
    Checksum: 0x7bbe [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    [Timestamps]
    [SEQ/ACK analysis]
```

4. Why can’t you view the reassembled .jpg file that is uploaded in thistrace file?

Answer: We selected a data packet and right clicked on it then selected Follow TCP stream.

Inside the TCP stream it is showing the RAW data and it doesn’t look like an image file. There is a message showing that this program must be run under win32 and also some kind of source code is showing. It means it is a Windows executable program.



Wireshark · Follow TCP Stream (tcp.stream eq 1) · BigFTP.pcapng

```
MZP....................@.........................................         .!..L.!..This program must be run under Win32
$7........................................................................................................................
..PE..L....^B*....................D......X............@.........................@..................@.............................P
.......*...............................................................................................CODE....t............
.............. ..`DATA....L..........................@...BSS.....H...............................idata..P     .......
..................@....tls...................................rdata.............................@..P.reloc..........................
..@..P.rsrc....*.......*..................@..P............@......................@..P.........................................
..............................................................................................................
.string................<.@.....m.@..........)@..(@..(@..)@.....$)@..Free..0)@..InitInstance..L)@..CleanupInstance..h(@.    ClassType..l(
@.          ClassName...(@..ClassNameIs...(@..ClassParent...)@.     ClassInfo...(@..InstanceSize...)@..InheritsFrom...)@..Dispatch...)@.
MethodAddress..<*@.
MethodName..x*@..FieldAddress...)@..DefaultHandler...(@..NewInstance...(@..FreeInstance.TObject.@...@..% .@....%..@....%..@....%..@....%
..@....%..@....%..@....%(.@....%..@....%..@....%..@....%..@....%..@....%..@....%..@....%..@....%..@....%..@....%..@....%..@....%..@....%
@.@....%<.@....%8.@....%4.@....%0.@....%..@....%..@....%..@....%..@....%..@....%..@....%..@....%..@...SV.8.@..>.u:hD...j..........u.3.^[
..4.@....
4.@.3......D........B..du.......^[.....@....SV...........u.3.^[....P..V..P......X..B.....^[..P....
.Q...8.@....8.@..SVWUQ....$...]...$.....P..V..;.C....S.;.u.........C....C..F......V.;.u
........C..F...;.u......U.....u.3...Z]_^[..@.SVWU........2.C.;.rl...J....k.;.w^;.u..B..C..B.)C..{..uD...5....;.
.r......{.;.u.)s..&.
.J...$+..|$...+..S............u.3.........;.u.3.YZ]_^[..SVW..........}.....................s.j.h. ..Vj.........;..t#...<.@..l.....u.h...
.j...P.....3..._^[..SVWU.......C.....j.h. ..h....U........;..u..............s.j.h. ..VU........;.t#...<.@........u.h....j...P.b...3...]_
^[..SVWU....L$...$.D$.....3..T$.....$...D$...<.@..Q.;.s.;.wF...C.;D$.w;;t$.s..t$....C.;D$.v..D$.h....j.V.......u
....@...............<.@.u..D$.3....|$..t..D$..T$....D$.+D$..T$..B....]_^[.SVWU....L$...$............$............T$..D$..(.D$.+..T$..B
..5<.@..<.^..~...;.v...;|$.v..|$.;.v.j.h....+.WS.&.....u
.D$.3....
.6..<.@.u....]_^[...SVWUQ.................4$...........$....+.$.A..5<.@..8.^..~...;.$s...$;.s...;.v.h.@..+.WS.......u
....@......6..<.@.u.Z]_^[..@.SVWU........L.@....?.........]..3;{..,.....C.......>.tP.F..C..F.)C..{..u>........5..;.u...........>.t!.....
.......<$.u....V........3...YZ]_^[...SVWU.....$.....L.@....?.........].....;.t.;s.u.;s.uW;{.........L$...+S..C..C.......|$..t3.L$..T$....
]....|$..u..L$..T$..D$..%.....$3.........L$...........|$..t4.L$..T$.........|$....f....L$..T$..D$........$3....H.k.;.u:;{..5..$.....q...
..$.8.t(..$.@..C...$.@.)C..{..u............$3......]_^[..SVW.......$...?.........4$........;.s[....+.........L$....L.@..]....\$...t..L$.
.T$....&....D$..D$..D$..D$..|$..t..T$..L.@........3......_^[.U..3.Uh..@.d.2d."h..@..9....=2.@..t
h..@.......<.@.......L.@.......x.@..x...h....j.......t.@..=t.@..t/.......t.@.3..L..@=....u..\.@..@....h.@.....@..3.ZYYd..h..@..=2.@..t
h..@........).......@.].U..S.=..@........3.Uh..@.d.2d.".=2.@..t
h..@..f.......@...t.@.P.4...3..t.@...<.@...h....j..C.P.%.......<.@.u..<.@.......L.@.......x.@..u....4.@...t.....4.@.P......4.@...u.d....
.....h..@..=2.@..t
h..@......h..@........C.....[]...S;.h.@.u    .P...h.@..P..H........*;.u.....t.@.3..T.........t.@..T.......P.[......P.[....x.@....J.;.r..J
.;.r.....x.@.u.....@.....3.....S...........|.............[....|............[.....@.....................@............|................
.|
............ ..SV.....................t
....@............+...3.......t
....@........t ......r.+.;p.t
```

0 client pkts, 688 server pkts, 0 turns.

Entire conversation (11 MB)

Show data as ASCII

Stream 1

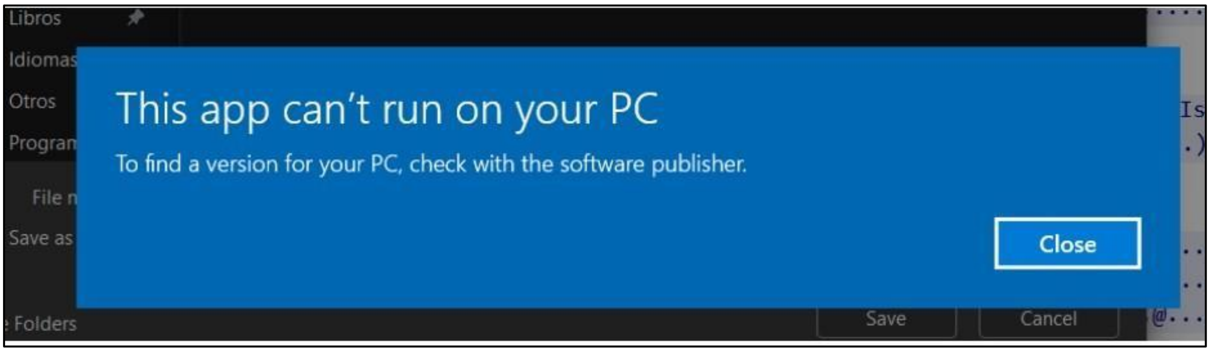
Find:

5. What is the true purpose of kidsatbeach.jpg?

Answer : In the previous challenge we saw that the jpg file was actually an exe file. So we saved the file in exe format. Then we executed it

File name: bigftp.exe

This application was not supported in Windows Operating System.



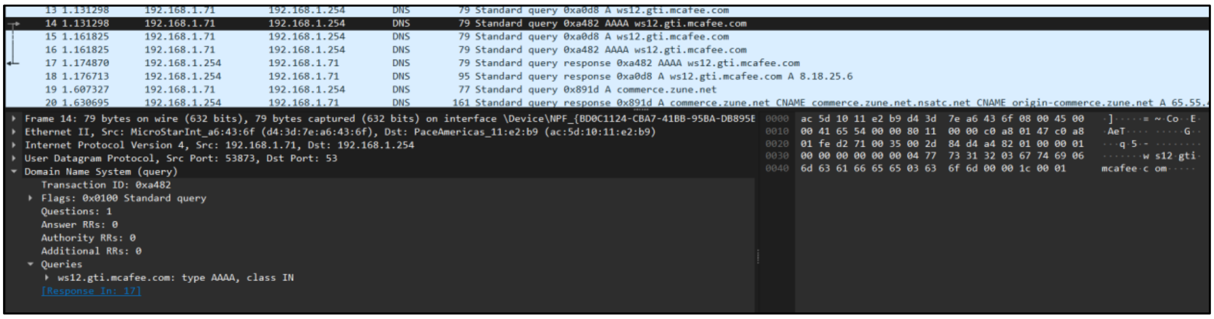
This app can't run on your PC

To find a version for your PC, check with the software publisher.

3. PAID TO PLAY Trace File: AllPlayNoWork.pcapng

1. For what server did the client try to resolve an IPv6 address?

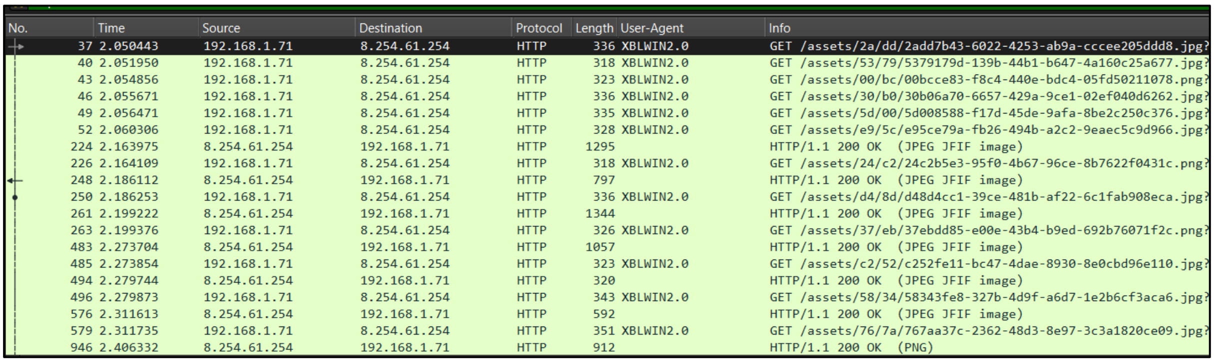
The client tried to resolve an IPv6 address for the server ws12.gti.mcafee.com. This can be determined by looking at the DNS query in the trace file, which has a value of AAAA and is trying to resolve the hostname ws12.gti.mcafee.com



```
13 1.131298   192.168.1.71    192.168.1.254   DNS    79 Standard query 0xa0d8 A ws12.gti.mcafee.com
14 1.131298   192.168.1.71    192.168.1.254   DNS    79 Standard query 0xa482 AAAA ws12.gti.mcafee.com
15 1.161825   192.168.1.71    192.168.1.254   DNS    79 Standard query 0xa0d8 A ws12.gti.mcafee.com
16 1.161825   192.168.1.71    192.168.1.254   DNS    79 Standard query 0xa482 AAAA ws12.gti.mcafee.com
17 1.174870   192.168.1.254   192.168.1.71    DNS    79 Standard query response 0xa482 AAAA ws12.gti.mcafee.com
18 1.176713   192.168.1.254   192.168.1.71    DNS    95 Standard query response 0xa0d8 A ws12.gti.mcafee.com A 8.18.25.6
19 1.607327   192.168.1.71    192.168.1.254   DNS    77 Standard query 0x891d A commerce.zune.net
20 1.630695   192.168.1.254   192.168.1.71    DNS   161 Standard query response 0x891d A commerce.zune.net CNAME commerce.zune.net.nsatc.net CNAME origin-commerce.zune.net A 65.55.

Frame 14: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{BD0C1124-CBA7-41BB-95BA-DB895E
Ethernet II, Src: MicroStarInt_a6:43:6f (d4:3d:7e:a6:43:6f), Dst: PaceAmericas_11:e2:b9 (ac:5d:10:11:e2:b9)
Internet Protocol Version 4, Src: 192.168.1.71, Dst: 192.168.1.254
User Datagram Protocol, Src Port: 53873, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0xa482
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    ws12.gti.mcafee.com: type AAAA, class IN
  [Response In: 17]

0000  ac 5d 10 11 e2 b9 d4 3d  7e a6 43 6f 08 00 45 00   ·]·····=~·Co··E·
0010  00 41 65 54 00 00 80 11  00 00 c0 a8 01 47 c0 a8   ·AeT·········G··
0020  01 fe d2 71 00 35 00 2d  84 d4 a4 82 01 00 00 01   ···q·5·-········
0030  00 00 00 00 00 00 04 77  73 31 32 03 67 74 69 06   ·······w s12·gti·
0040  6d 63 61 66 65 65 03 63  6f 6d 00 00 1c 00 01      mcafee·c om·····
```

2. What operating system do you think the client is running?

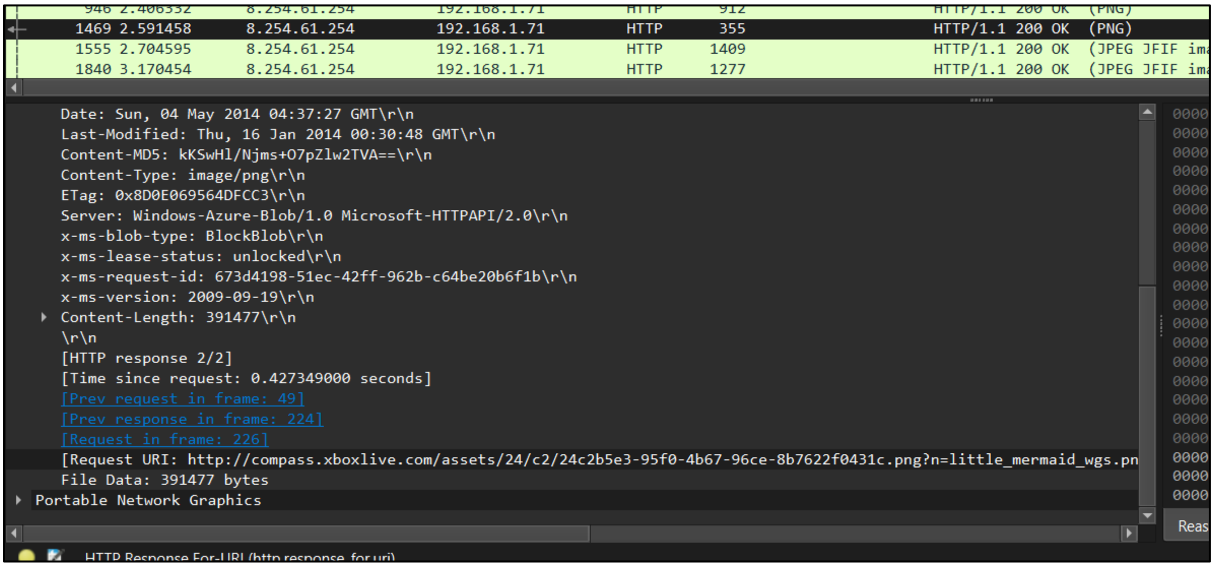
The client is running Windows 7. This can be determined by looking at the User-Agent field in the HTTP GET request, which has the value of Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729).



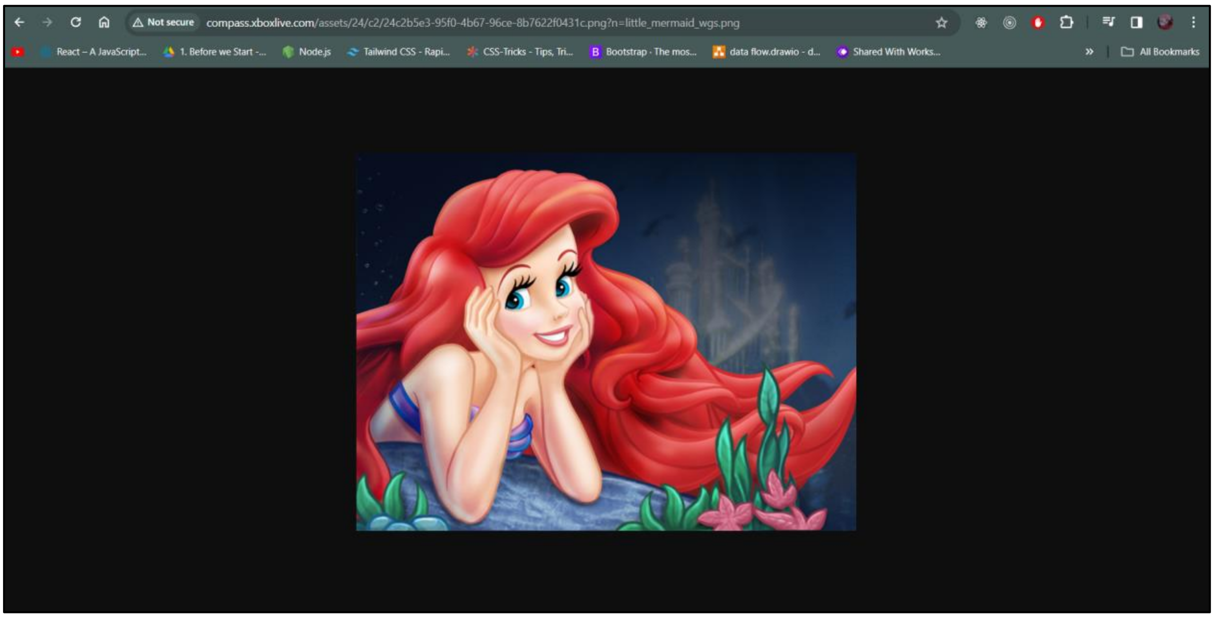
```
No.      Time       Source          Destination     Protocol Length User-Agent   Info
    37 2.050443   192.168.1.71    8.254.61.254    HTTP       336 XBLWIN2.0    GET /assets/2a/dd/2add7b43-6022-4253-ab9a-cccee205ddd8.jpg?
    40 2.051950   192.168.1.71    8.254.61.254    HTTP       318 XBLWIN2.0    GET /assets/53/79/5379179d-139b-44b1-b647-4a160c25a677.jpg?
    43 2.054856   192.168.1.71    8.254.61.254    HTTP       323 XBLWIN2.0    GET /assets/00/bc/00bcce83-f8c4-440e-bdc4-05fd50211078.png?
    46 2.055671   192.168.1.71    8.254.61.254    HTTP       336 XBLWIN2.0    GET /assets/30/b0/30b06a70-6657-429a-9ce1-02ef040d6262.jpg?
    49 2.056471   192.168.1.71    8.254.61.254    HTTP       335 XBLWIN2.0    GET /assets/5d/00/5d008588-f17d-45de-9afa-8be2c250c376.jpg?
    52 2.060306   192.168.1.71    8.254.61.254    HTTP       328 XBLWIN2.0    GET /assets/e9/5c/e95ce79a-fb26-494b-a2c2-9eaec5c9d966.jpg?
   224 2.163975   8.254.61.254    192.168.1.71    HTTP      1295              HTTP/1.1 200 OK  (JPEG JFIF image)
   226 2.164109   192.168.1.71    8.254.61.254    HTTP       318 XBLWIN2.0    GET /assets/24/c2/24c2b5e3-95f0-4b67-96ce-8b7622f0431c.png?
   248 2.186112   8.254.61.254    192.168.1.71    HTTP       797              HTTP/1.1 200 OK  (JPEG JFIF image)
   250 2.186253   192.168.1.71    8.254.61.254    HTTP       336 XBLWIN2.0    GET /assets/d4/8d/d48d4cc1-39ce-481b-af22-6c1fab908eca.jpg?
   261 2.199222   8.254.61.254    192.168.1.71    HTTP      1344              HTTP/1.1 200 OK  (JPEG JFIF image)
   263 2.199376   192.168.1.71    8.254.61.254    HTTP       326 XBLWIN2.0    GET /assets/37/eb/37ebdd85-e00e-43b4-b9ed-692b76071f2c.png?
   483 2.273704   8.254.61.254    192.168.1.71    HTTP      1057              HTTP/1.1 200 OK  (JPEG JFIF image)
   485 2.273854   192.168.1.71    8.254.61.254    HTTP       323 XBLWIN2.0    GET /assets/c2/52/c252fe11-bc47-4dae-8930-8e0cbd96e110.jpg?
   494 2.279744   8.254.61.254    192.168.1.71    HTTP       320              HTTP/1.1 200 OK  (JPEG JFIF image)
   496 2.279873   192.168.1.71    8.254.61.254    HTTP       343 XBLWIN2.0    GET /assets/58/34/58343fe8-327b-4d9f-a6d7-1e2b6cf3aca6.jpg?
   576 2.311613   8.254.61.254    192.168.1.71    HTTP       592              HTTP/1.1 200 OK  (JPEG JFIF image)
   579 2.311735   192.168.1.71    8.254.61.254    HTTP       351 XBLWIN2.0    GET /assets/76/7a/767aa37c-2362-48d3-8e97-3c3a1820ce09.jpg?
   946 2.406332   8.254.61.254    192.168.1.71    HTTP       912              HTTP/1.1 200 OK  (PNG)
```

3. What is the color of the mermaid’s hair?

The color of the mermaid's hair is red. This can be determined by looking at the image of the mermaid in the trace file, which has red hair.



```
     946 2.406332     8.254.61.254          192.168.1.71          HTTP      912          HTTP/1.1 200 OK  (PNG)
    1469 2.591458     8.254.61.254          192.168.1.71          HTTP      355          HTTP/1.1 200 OK  (PNG)
    1555 2.704595     8.254.61.254          192.168.1.71          HTTP     1409          HTTP/1.1 200 OK  (JPEG JFIF ima
    1840 3.170454     8.254.61.254          192.168.1.71          HTTP     1277          HTTP/1.1 200 OK  (JPEG JFIF ima

      Date: Sun, 04 May 2014 04:37:27 GMT\r\n
      Last-Modified: Thu, 16 Jan 2014 00:30:48 GMT\r\n
      Content-MD5: kKSwHl/Njms+O7pZlw2TVA==\r\n
      Content-Type: image/png\r\n
      ETag: 0x8D0E069564DFCC3\r\n
      Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0\r\n
      x-ms-blob-type: BlockBlob\r\n
      x-ms-lease-status: unlocked\r\n
      x-ms-request-id: 673d4198-51ec-42ff-962b-c64be20b6f1b\r\n
      x-ms-version: 2009-09-19\r\n
    > Content-Length: 391477\r\n
      \r\n
      [HTTP response 2/2]
      [Time since request: 0.427349000 seconds]
      [Prev request in frame: 49]
      [Prev response in frame: 224]
      [Request in frame: 226]
      [Request URI: http://compass.xboxlive.com/assets/24/c2/24c2b5e3-95f0-4b67-96ce-8b7622f0431c.png?n=little_mermaid_wgs.pn
      File Data: 391477 bytes
  > Portable Network Graphics
```



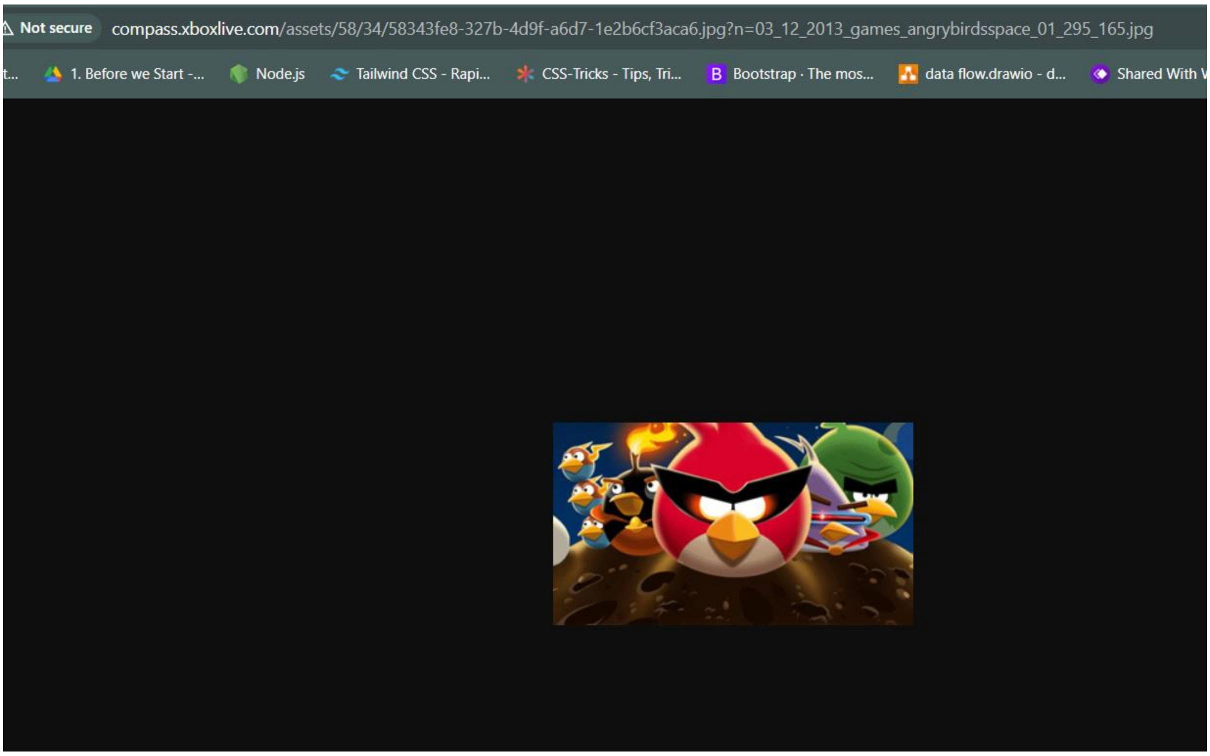
4. What classic games did the user learn about? (Name all of them.)

The user learned about the following classic games:

- Royal Envoy 2
- Istunt 2
- Uno and friends
- Angry bird space
- Harvest 1
- Hydro Thunder Hurricane
- Big Buck Hunter
- Alpha jax 1
- Bejeweled

5. Which Angry Birds edition did the user learn about?

The user learned about the Angry Birds Rio edition. This can be determined by looking at the image of the Angry Birds Rio logo in the trace file.


Not secure
compass.xboxlive.com/assets/58/34/58343fe8-327b-4d9f-a6d7-1e2b6cf3aca6.jpg?n=03_12_2013_games_angrybirdsspace_01_295_165.jpg
t...
1. Before we Start -...
Node.js
Tailwind CSS - Rapi...
CSS-Tricks - Tips, Tri...
Bootstrap · The mos...
data flow.drawio - d...
Shared With V

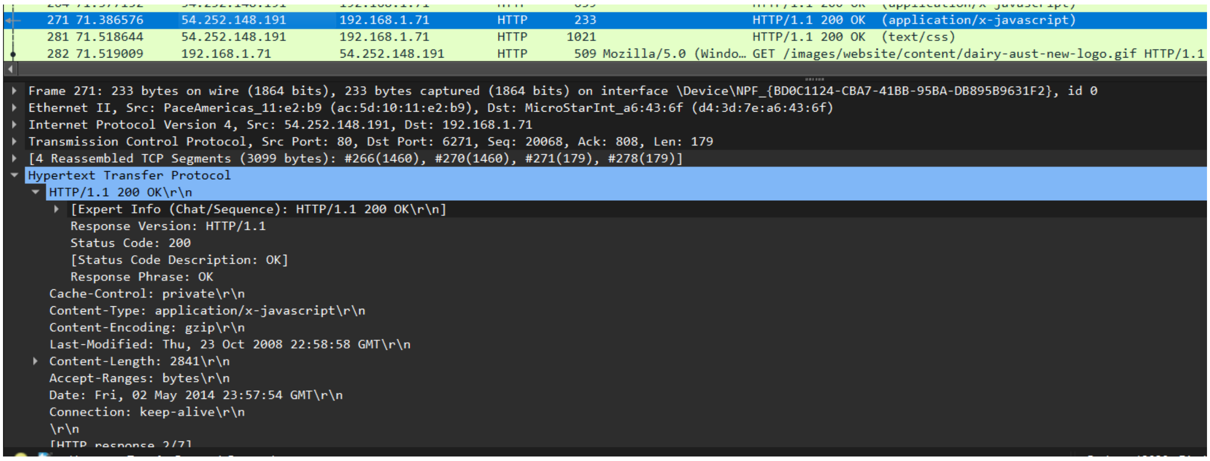
4. BROWSING BUDDY Trace File: BrowsingAlong.pcapng

1. What version of dumpcap was used to capture this trace file?

The version of dumpcap used to capture this trace file is not explicitly indicated in the capture file. However, based on the file format and capture options, it is likely that version 1.4 or later was used.

2.Which frame contains the 200 OK response to the GET request for /scripts/AC_OETags.js?

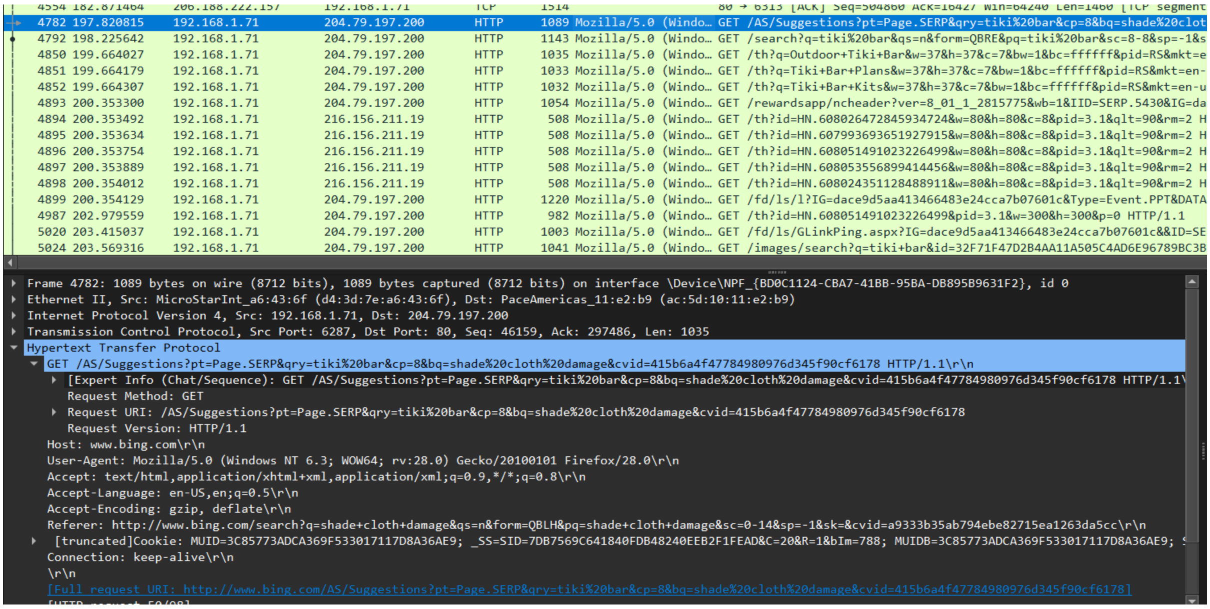
Frame 271 contains the 200 OK response to the GET request for /scripts/AC_OETags.js. This can be determined by looking at the HTTP responses in the trace file and identifying the one that has a status code of 200 and a request URI of /scripts/AC_OETags.js.



```
  271 71.386576   54.252.148.191     192.168.1.71       HTTP      233                         HTTP/1.1 200 OK  (application/x-javascript)
  281 71.518644   54.252.148.191     192.168.1.71       HTTP     1021                         HTTP/1.1 200 OK  (text/css)
  282 71.519009   192.168.1.71       54.252.148.191     HTTP      509 Mozilla/5.0 (Windo… GET /images/website/content/dairy-aust-new-logo.gif HTTP/1.1

Frame 271: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits) on interface \Device\NPF_{BD0C1124-CBA7-41BB-95BA-DB895B9631F2}, id 0
Ethernet II, Src: PaceAmericas_11:e2:b9 (ac:5d:10:11:e2:b9), Dst: MicroStarInt_a6:43:6f (d4:3d:7e:a6:43:6f)
Internet Protocol Version 4, Src: 54.252.148.191, Dst: 192.168.1.71
Transmission Control Protocol, Src Port: 80, Dst Port: 6271, Seq: 20068, Ack: 808, Len: 179
[4 Reassembled TCP Segments (3099 bytes): #266(1460), #270(1460), #271(179), #278(179)]
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Cache-Control: private\r\n
  Content-Type: application/x-javascript\r\n
  Content-Encoding: gzip\r\n
  Last-Modified: Thu, 23 Oct 2008 22:58:58 GMT\r\n
  Content-Length: 2841\r\n
  Accept-Ranges: bytes\r\n
  Date: Fri, 02 May 2014 23:57:54 GMT\r\n
  Connection: keep-alive\r\n
  \r\n
  [HTTP response 2/7]
```

3. In what kind of "bar" is the client interested?

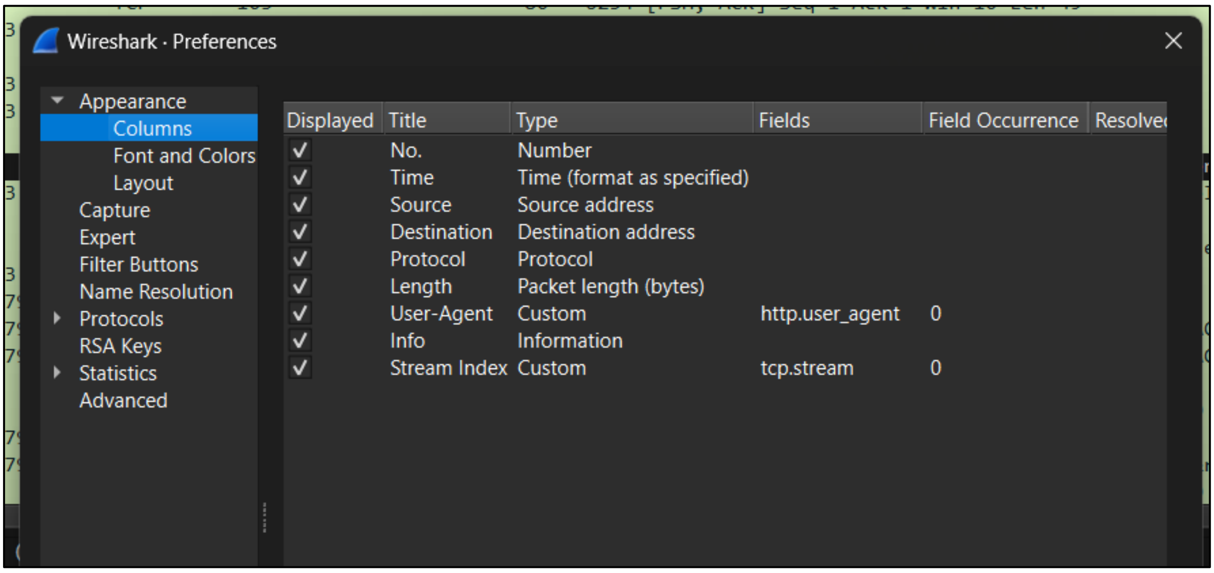
Tiki bar



```
 4554 182.871464 206.188.222.157   192.168.1.71      TCP      1514                         80 → 6313 [ACK] Seq=504860 Ack=16427 Win=64240 Len=1460 [TCP segment
 4782 197.820815 192.168.1.71      204.79.197.200    HTTP     1089 Mozilla/5.0 (Windo… GET /AS/Suggestions?pt=Page.SERP&qry=tiki%20bar&cp=8&bq=shade%20clot
 4792 198.225642 192.168.1.71      204.79.197.200    HTTP     1143 Mozilla/5.0 (Windo… GET /search?q=tiki%20bar&qs=n&form=QBRE&pq=tiki%20bar&sc=8-8&sp=-1&s
 4850 199.664027 192.168.1.71      204.79.197.200    HTTP     1035 Mozilla/5.0 (Windo… GET /th?q=Outdoor+Tiki+Bar&w=37&h=37&c=7&bw=1&bc=ffffff&pid=RS&mkt=e
 4851 199.664179 192.168.1.71      204.79.197.200    HTTP     1033 Mozilla/5.0 (Windo… GET /th?q=Tiki+Bar+Plans&w=37&h=37&c=7&bw=1&bc=ffffff&pid=RS&mkt=en-
 4852 199.664307 192.168.1.71      204.79.197.200    HTTP     1032 Mozilla/5.0 (Windo… GET /th?q=Tiki+Bar+Kits&w=37&h=37&c=7&bw=1&bc=ffffff&pid=RS&mkt=en-u
 4893 200.353300 192.168.1.71      204.79.197.200    HTTP     1054 Mozilla/5.0 (Windo… GET /rewardsapp/ncheader?ver=8_01_1_2815775&wb=1&IID=SERP.5430&IG=da
 4894 200.353492 192.168.1.71      216.156.211.19    HTTP      508 Mozilla/5.0 (Windo… GET /th?id=HN.608026472845934724&w=80&h=80&c=8&pid=3.1&qlt=90&rm=2 H
 4895 200.353634 192.168.1.71      216.156.211.19    HTTP      508 Mozilla/5.0 (Windo… GET /th?id=HN.607993693651927915&w=80&h=80&c=8&pid=3.1&qlt=90&rm=2 H
 4896 200.353754 192.168.1.71      216.156.211.19    HTTP      508 Mozilla/5.0 (Windo… GET /th?id=HN.608051491023226499&w=80&h=80&c=8&pid=3.1&qlt=90&rm=2 H
 4897 200.353889 192.168.1.71      216.156.211.19    HTTP      508 Mozilla/5.0 (Windo… GET /th?id=HN.608053556899414456&w=80&h=80&c=8&pid=3.1&qlt=90&rm=2 H
 4898 200.354012 192.168.1.71      216.156.211.19    HTTP      508 Mozilla/5.0 (Windo… GET /th?id=HN.608024351128488911&w=80&h=80&c=8&pid=3.1&qlt=90&rm=2 H
 4899 200.354129 192.168.1.71      204.79.197.200    HTTP     1220 Mozilla/5.0 (Windo… GET /fd/ls/l?IG=dace9d5aa413466483e24cca7b07601c&Type=Event.PPT&DATA
 4987 202.979559 192.168.1.71      204.79.197.200    HTTP      982 Mozilla/5.0 (Windo… GET /th?id=HN.608051491023226499&pid=3.1&w=300&h=300&p=0 HTTP/1.1
 5020 203.415037 192.168.1.71      204.79.197.200    HTTP     1003 Mozilla/5.0 (Windo… GET /fd/ls/GLinkPing.aspx?IG=dace9d5aa413466483e24cca7b07601c&&ID=SE
 5024 203.569316 192.168.1.71      204.79.197.200    HTTP     1041 Mozilla/5.0 (Windo… GET /images/search?q=tiki+bar&id=32F71F47D2B4AA11A505C4AD6E96789BC3B

Frame 4782: 1089 bytes on wire (8712 bits), 1089 bytes captured (8712 bits) on interface \Device\NPF_{BD0C1124-CBA7-41BB-95BA-DB895B9631F2}, id 0
Ethernet II, Src: MicroStarInt_a6:43:6f (d4:3d:7e:a6:43:6f), Dst: PaceAmericas_11:e2:b9 (ac:5d:10:11:e2:b9)
Internet Protocol Version 4, Src: 192.168.1.71, Dst: 204.79.197.200
Transmission Control Protocol, Src Port: 6287, Dst Port: 80, Seq: 46159, Ack: 297486, Len: 1035
Hypertext Transfer Protocol
  GET /AS/Suggestions?pt=Page.SERP&qry=tiki%20bar&cp=8&bq=shade%20cloth%20damage&cvid=415b6a4f47784980976d345f90cf6178 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /AS/Suggestions?pt=Page.SERP&qry=tiki%20bar&cp=8&bq=shade%20cloth%20damage&cvid=415b6a4f47784980976d345f90cf6178 HTTP/1.1\
    Request Method: GET
    Request URI: /AS/Suggestions?pt=Page.SERP&qry=tiki%20bar&cp=8&bq=shade%20cloth%20damage&cvid=415b6a4f47784980976d345f90cf6178
    Request Version: HTTP/1.1
  Host: www.bing.com\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:28.0) Gecko/20100101 Firefox/28.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Referer: http://www.bing.com/search?q=shade+cloth+damage&qs=n&form=QBLH&pq=shade+cloth+damage&sc=0-14&sp=-1&sk=&cvid=a9333b35ab794ebe82715ea1263da5cc\r\n
  [truncated]Cookie: MUID=3C85773ADCA369F533017117D8A36AE9; _SS=SID=7DB7569C641840FDB48240EEB2F1FEAD&C=20&R=1&bIm=788; MUIDB=3C85773ADCA369F533017117D8A36AE9; S
  Connection: keep-alive\r\n
  \r\n
  [Full request URI: http://www.bing.com/AS/Suggestions?pt=Page.SERP&qry=tiki%20bar&cp=8&bq=shade%20cloth%20damage&cvid=415b6a4f47784980976d345f90cf6178]
  [HTTP request 50/98]
```

4. Which TCP stream experienced the most Retransmissions?

TCP stream 14 experienced the most retransmissions, with a total of 5 retransmissions. This can be determined by analyzing the TCP retransmission information in the trace file.



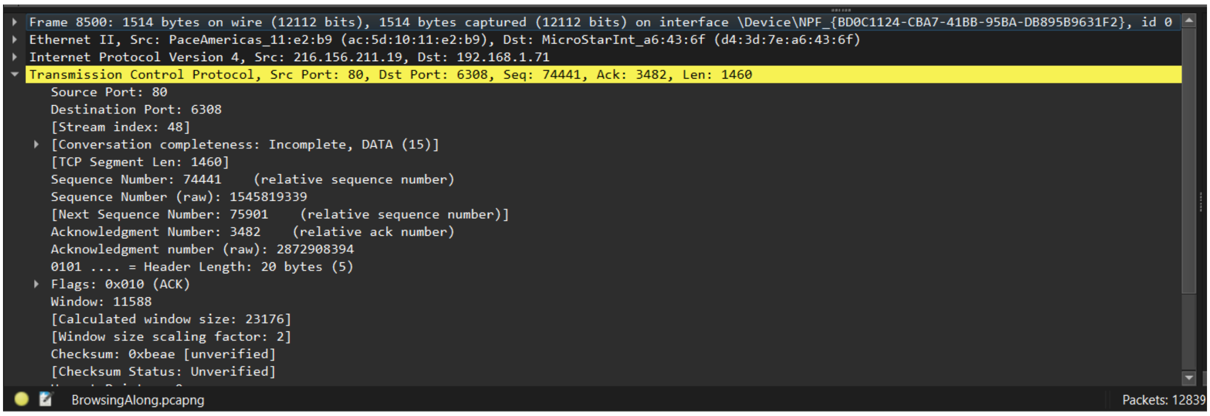
Displayed	Title	Type	Fields	Field Occurrence	Resolve
✓	No.	Number			
✓	Time	Time (format as specified)			
✓	Source	Source address			
✓	Destination	Destination address			
✓	Protocol	Protocol			
✓	Length	Packet length (bytes)			
✓	User-Agent	Custom	http.user_agent	0	
✓	Info	Information			
✓	Stream Index	Custom	tcp.stream	0	

5. Frame 8500 is a retransmission triggered by duplicate ACKs. Why isn't it marked as a Fast Retransmission?

Frame 8500 is not marked as a Fast Retransmission because it was triggered by duplicate ACKs, not by three consecutive ACKs for the same unacknowledged segment. Fast Retransmissions are specifically designed to handle situations where three ACKs are received for the same unacknowledged segment, indicating that the segment is likely lost and needs to be retransmitted quickly. Duplicate ACKs, on the other hand, suggest that the segment may have been delayed or reordered, and a Fast Retransmission may not be necessary.

OR

We can see that there are two duplicate ACK packets before frame 8500. If there are two duplicate ACKs in the reverse direction and if the packet occurs within 20ms of the last duplicate ACK then it will be considered as fast retransmission. Using timestamp of 8500 it was more than 20 ms longer than the previous frame. So, it isn't a fast retransmission.

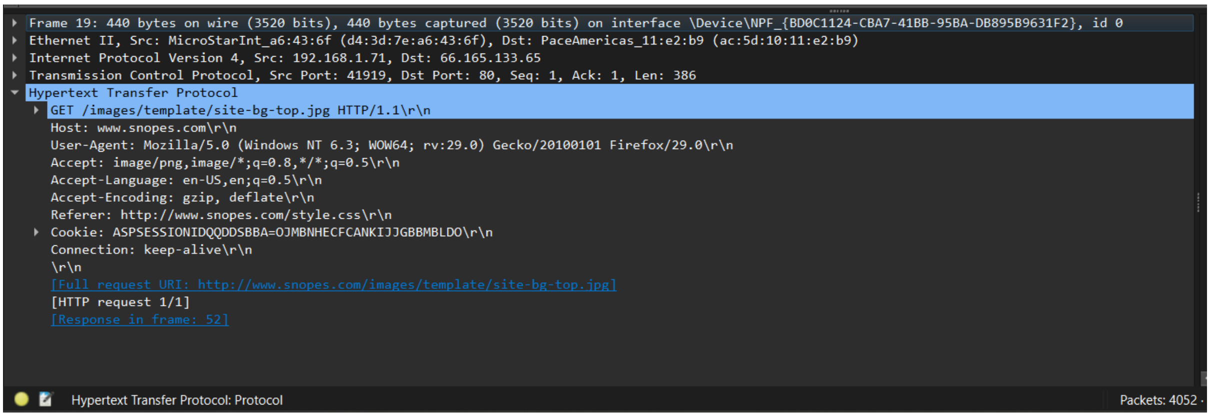


```
Frame 8500: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{BD0C1124-CBA7-41BB-95BA-DB895B9631F2}, id 0
Ethernet II, Src: PaceAmericas_11:e2:b9 (ac:5d:10:11:e2:b9), Dst: MicroStarInt_a6:43:6f (d4:3d:7e:a6:43:6f)
Internet Protocol Version 4, Src: 216.156.211.19, Dst: 192.168.1.71
Transmission Control Protocol, Src Port: 80, Dst Port: 6308, Seq: 74441, Ack: 3482, Len: 1460
    Source Port: 80
    Destination Port: 6308
    [Stream index: 48]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 1460]
    Sequence Number: 74441    (relative sequence number)
    Sequence Number (raw): 1545819339
    [Next Sequence Number: 75901    (relative sequence number)]
    Acknowledgment Number: 3482    (relative ack number)
    Acknowledgment number (raw): 2872908394
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
    Window: 11588
    [Calculated window size: 23176]
    [Window size scaling factor: 2]
    Checksum: 0xbeae [unverified]
    [Checksum Status: Unverified]
```

5. OUCH! Trace File: AskSnopes.pcapng

1. What web server software is used by www.snopes.com?

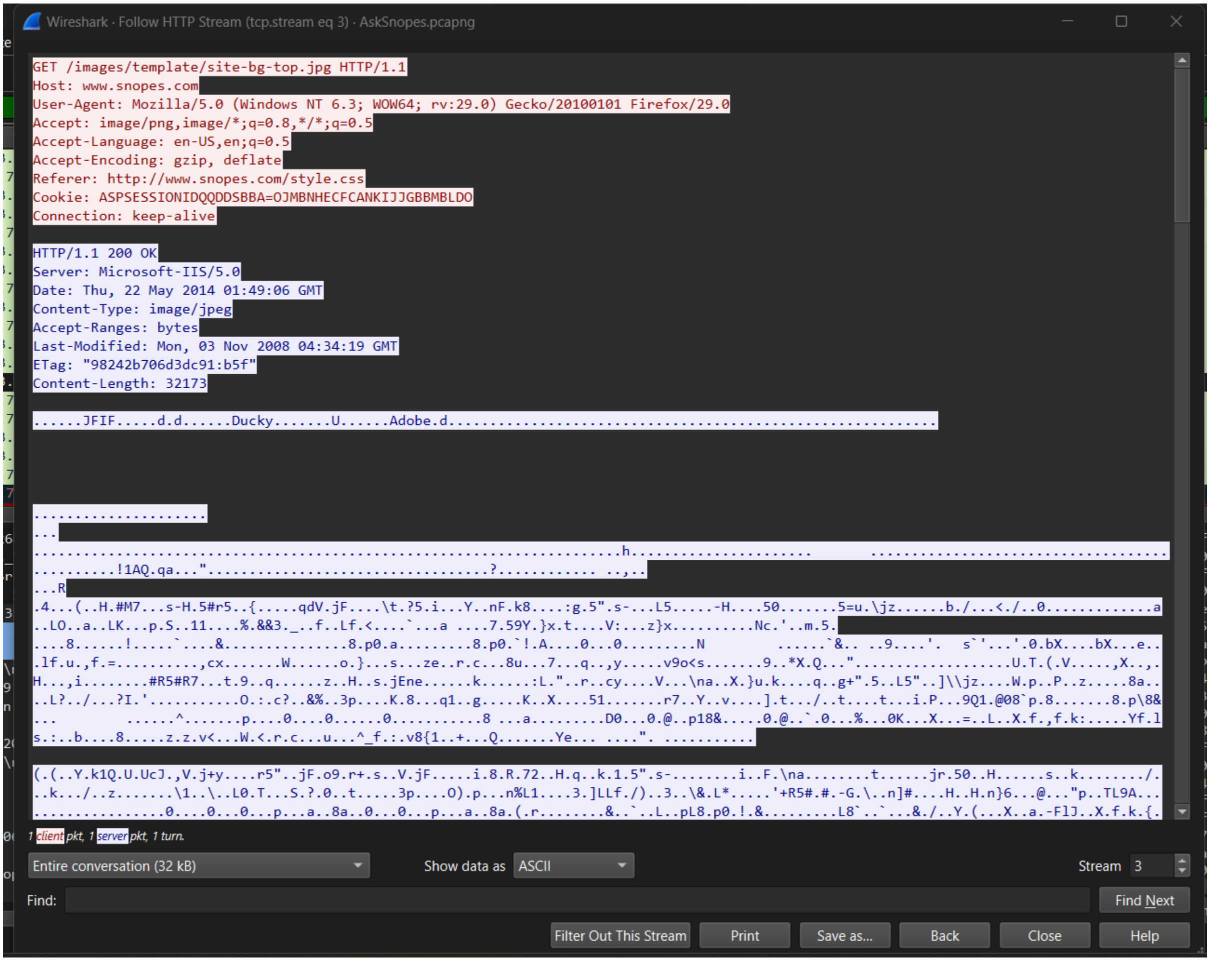
The web server software used by www.snopes.com is Microsoft-IIS/5.0. This can be determined by looking at the Server field in the HTTP responses in the trace file.



```
▸ Frame 19: 440 bytes on wire (3520 bits), 440 bytes captured (3520 bits) on interface \Device\NPF_{BD0C1124-CBA7-41BB-95BA-DB895B9631F2}, id 0
▸ Ethernet II, Src: MicroStarInt_a6:43:6f (d4:3d:7e:a6:43:6f), Dst: PaceAmericas_11:e2:b9 (ac:5d:10:11:e2:b9)
▸ Internet Protocol Version 4, Src: 192.168.1.71, Dst: 66.165.133.65
▸ Transmission Control Protocol, Src Port: 41919, Dst Port: 80, Seq: 1, Ack: 1, Len: 386
▾ Hypertext Transfer Protocol
  ▸ GET /images/template/site-bg-top.jpg HTTP/1.1\r\n
    Host: www.snopes.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0\r\n
    Accept: image/png,image/*;q=0.8,*/*;q=0.5\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://www.snopes.com/style.css\r\n
  ▸ Cookie: ASPSESSIONIDQQDDSBBA=OJMBNHECFCANKIJJGBBMBLDO\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://www.snopes.com/images/template/site-bg-top.jpg]
    [HTTP request 1/1]
    [Response in frame: 52]
```

Hypertext Transfer Protocol: Protocol

Packets: 4052 ·



Wireshark · Follow HTTP Stream (tcp.stream eq 3) · AskSnopes.pcapng

```
GET /images/template/site-bg-top.jpg HTTP/1.1
Host: www.snopes.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.snopes.com/style.css
Cookie: ASPSESSIONIDQQDDSBBA=OJMBNHECFCANKIJJGBBMBLDO
Connection: keep-alive

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 22 May 2014 01:49:06 GMT
Content-Type: image/jpeg
Accept-Ranges: bytes
Last-Modified: Mon, 03 Nov 2008 04:34:19 GMT
ETag: "98242b706d3dc91:b5f"
Content-Length: 32173

......JFIF.....d.d......Ducky.......U......Adobe.d.......................................................



.....................
...
...................................................................h....................    ..................................
..........!1AQ.qa..."................................?............ ..,..
...R
.4...(..H.#M7...s-H.5#r5..{.....qdV.jF....\t.?5.i...Y..nF.k8....:g.5".s-...L5.....-H....50.......5=u.\jz......b./...<./..0.............a
..LO..a..LK...p.S..11....%.&&3._..f..Lf.<....`...a ....7.59Y.}x.t....V:...z}x..........Nc.'..m.5.
....8......!.....`....&...............8.p0.a.........8.p0.`!.A....0...0.........N        ......`&.. ..9....'.  s`'...'.0.bX....bX...e..
.lf.u.,f.=..........,cx.......W......o.}...s...ze..r.c...8u...7...q..,y.....v9o<s.......9..*X.Q..."..................U.T.(.V.....,X..,.
H...,i........#R5#R7...t.9..q......z..H..s.jEne......k......:L."..r..cy....V...\na..X.}u.k....q..g+".5..L5"..]\\jz....W.p..P..z.....8a..
..L?../...?I.'..........O.:.c?..&%..3p....K.8...q1..g.....K..X....51.......r7..Y..v....].t.../..t....t...i.P...9Q1.@08`p.8.......8.p\8&
...         ......^.......p....0....0......0...........8 ...a.........D0...0.@..p18&.....0.@..`.0...%...0K...X...=..L..X.f.,f.k:.....Yf.l
s.:..b....8.....z.z.v<...W.<.r.c...u...^_f.:.v8{1..+...Q.......Ye... ....". ..........

(.(..Y.k1Q.U.UcJ.,V.j+y....r5"..jF.o9.r+.s..V.jF.....i.8.R.72..H.q..k.1.5".s-........i..F.\na........t......jr.50..H......s..k......../.
..k.../..z.......\1..\..L0.T...S.?.0..t.....3p....O).p...n%L1....3.]LLf./)..3..\&.L*.....'+R5#.#.-G.\..n]#....H..H.n}6...@..."p..TL9A...
...............0....0...0...p...a..8a..0...0...p...a..8a.(.r........&..`..L..pL8.p0.!.&.........L8`..`...&./..Y.(...X..a.-FlJ..X.f.k.{.
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (32 kB)

Show data as ASCII

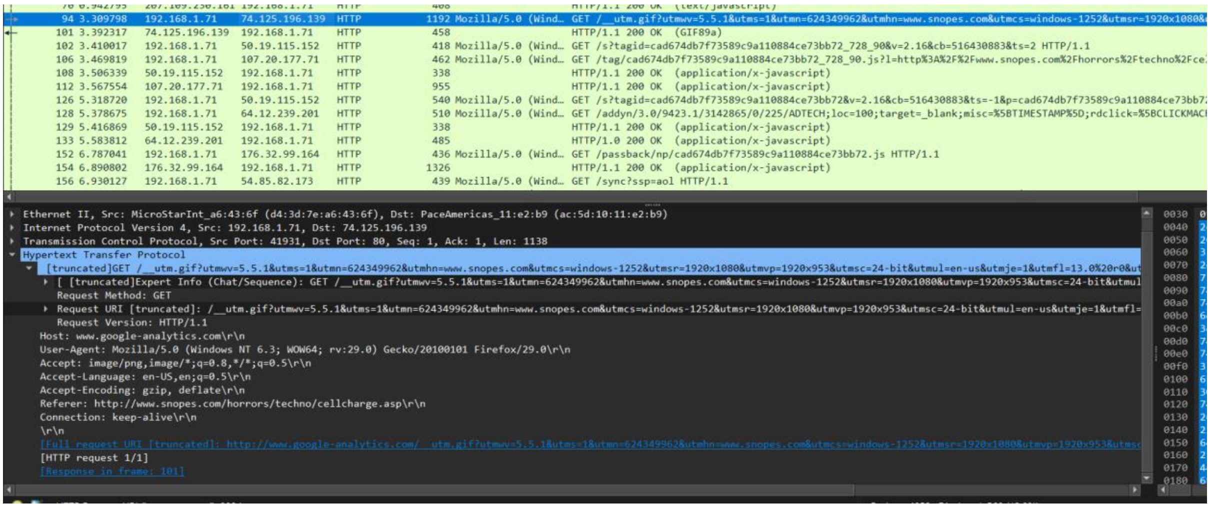
Stream 3

2. About what cell phone problem is the client concerned?

The client is concerned about a cell phone problem related to the phone not ringing when text messages are received. This can be determined by looking at the HTTP GET request for /fact-check/fact-check-148290.html, which has a title of "iPhone Text Message Alerts Not Working: A Common Problem with a Simple Fix."

OR

Checking for cell phone references when we see the complete URL for No 94 we can see “Cell Phone Recharging Electrocution”.

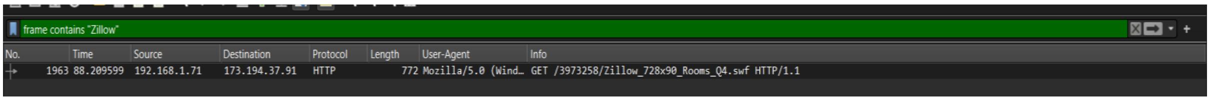


```
 94 3.309798   192.168.1.71    74.125.196.139  HTTP   1192 Mozilla/5.0 (Wind… GET /__utm.gif?utmwv=5.5.1&utms=1&utmn=624349962&utmhn=www.snopes.com&utmcs=windows-1252&utmsr=1920x1080&
101 3.392317   74.125.196.139  192.168.1.71    HTTP    458                    HTTP/1.1 200 OK  (GIF89a)
102 3.410017   192.168.1.71    50.19.115.152   HTTP    418 Mozilla/5.0 (Wind… GET /s?tagid=cad674db7f73589c9a110884ce73bb72_728_90&v=2.16&cb=516430883&ts=2 HTTP/1.1
106 3.469819   192.168.1.71    107.20.177.71   HTTP    462 Mozilla/5.0 (Wind… GET /tag/cad674db7f73589c9a110884ce73bb72_728_90.js?l=http%3A%2F%2Fwww.snopes.com%2Fhorrors%2Ftechno%2Fce
108 3.506339   50.19.115.152   192.168.1.71    HTTP    338                    HTTP/1.1 200 OK  (application/x-javascript)
112 3.567554   107.20.177.71   192.168.1.71    HTTP    955                    HTTP/1.1 200 OK  (application/x-javascript)
126 5.318720   192.168.1.71    50.19.115.152   HTTP    540 Mozilla/5.0 (Wind… GET /s?tagid=cad674db7f73589c9a110884ce73bb72&v=2.16&cb=516430883&ts=-1&p=cad674db7f73589c9a110884ce73bb7
128 5.378675   192.168.1.71    64.12.239.201   HTTP    510 Mozilla/5.0 (Wind… GET /addyn/3.0/9423.1/3142865/0/225/ADTECH;loc=100;target=_blank;misc=%5BTIMESTAMP%5D;rdclick=%5BCLICKMAC
129 5.416869   50.19.115.152   192.168.1.71    HTTP    338                    HTTP/1.1 200 OK  (application/x-javascript)
133 5.583812   64.12.239.201   192.168.1.71    HTTP    485                    HTTP/1.0 200 OK  (application/x-javascript)
152 6.787041   192.168.1.71    176.32.99.164   HTTP    436 Mozilla/5.0 (Wind… GET /passback/np/cad674db7f73589c9a110884ce73bb72.js HTTP/1.1
154 6.890802   176.32.99.164   192.168.1.71    HTTP   1326                    HTTP/1.1 200 OK  (application/x-javascript)
156 6.930127   192.168.1.71    54.85.82.173    HTTP    439 Mozilla/5.0 (Wind… GET /sync?ssp=aol HTTP/1.1
```

```
▸ Ethernet II, Src: MicroStarInt_a6:43:6f (d4:3d:7e:a6:43:6f), Dst: PaceAmericas_11:e2:b9 (ac:5d:10:11:e2:b9)
▸ Internet Protocol Version 4, Src: 192.168.1.71, Dst: 74.125.196.139
▸ Transmission Control Protocol, Src Port: 41931, Dst Port: 80, Seq: 1, Ack: 1, Len: 1138
▾ Hypertext Transfer Protocol
  ▾ [truncated]GET /__utm.gif?utmwv=5.5.1&utms=1&utmn=624349962&utmhn=www.snopes.com&utmcs=windows-1252&utmsr=1920x1080&utmvp=1920x953&utmsc=24-bit&utmul=en-us&utmje=1&utmfl=13.0%20r0&ut
    ▸ [ [truncated]Expert Info (Chat/Sequence): GET /__utm.gif?utmwv=5.5.1&utms=1&utmn=624349962&utmhn=www.snopes.com&utmcs=windows-1252&utmsr=1920x1080&utmvp=1920x953&utmsc=24-bit&utmul
      Request Method: GET
    ▸ Request URI [truncated]: /__utm.gif?utmwv=5.5.1&utms=1&utmn=624349962&utmhn=www.snopes.com&utmcs=windows-1252&utmsr=1920x1080&utmvp=1920x953&utmsc=24-bit&utmul=en-us&utmje=1&utmfl=
      Request Version: HTTP/1.1
    Host: www.google-analytics.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0\r\n
    Accept: image/png,image/*;q=0.8,*/*;q=0.5\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://www.snopes.com/horrors/techno/cellcharge.asp\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI [truncated]: http://www.google-analytics.com/__utm.gif?utmwv=5.5.1&utms=1&utmn=624349962&utmhn=www.snopes.com&utmcs=windows-1252&utmsr=1920x1080&utmvp=1920x953&utmsc
    [HTTP request 1/1]
    [Response in frame: 101]
```

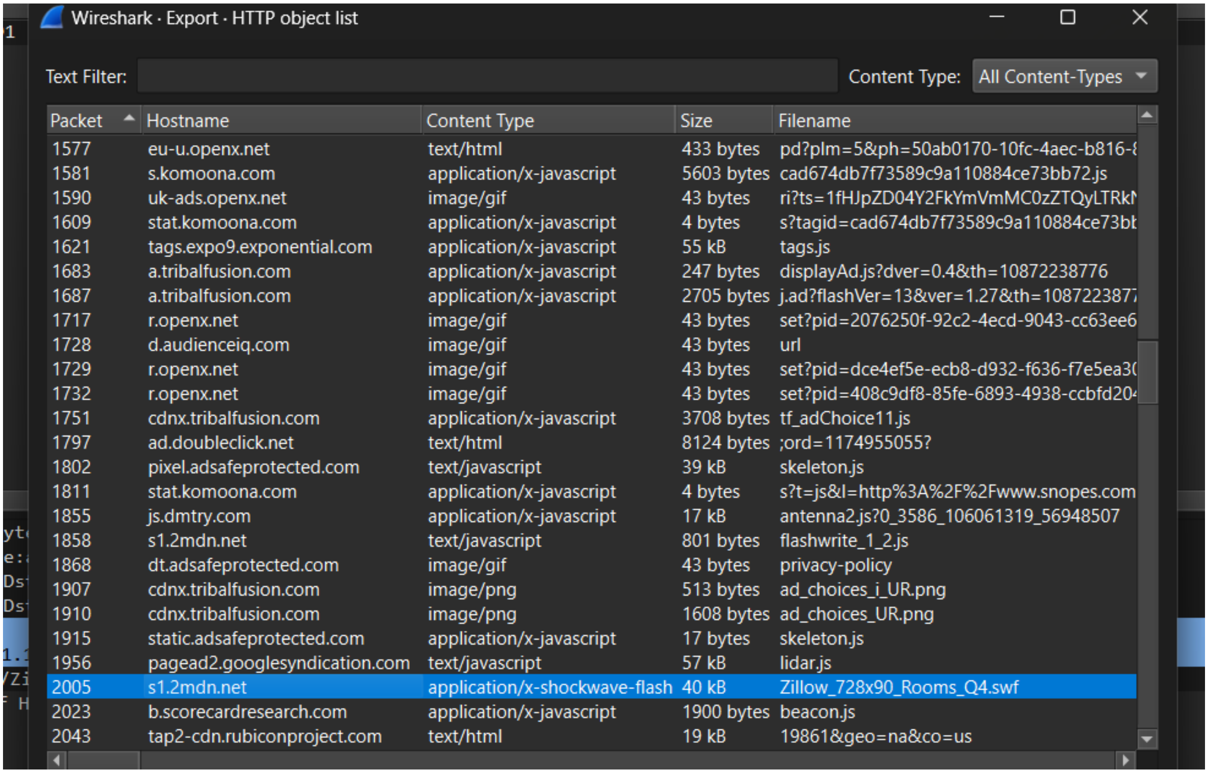
3. According to Zillow, what instrument will Ryan learn to play?

According to Zillow, Ryan will learn to play the piano. This can be determined by looking at the HTTP GET request for /zillow/homedetails/7636131-Zillow.html, which has a description that mentions Ryan learning to play the Saxophone



frame contains "Zillow"

```
No.    Time        Source          Destination     Protocol  Length  User-Agent           Info
 1963  88.209599   192.168.1.71    173.194.37.91   HTTP         772  Mozilla/5.0 (Wind…   GET /3973258/Zillow_728x90_Rooms_Q4.swf HTTP/1.1
```



Wireshark · Export · HTTP object list

Text Filter:

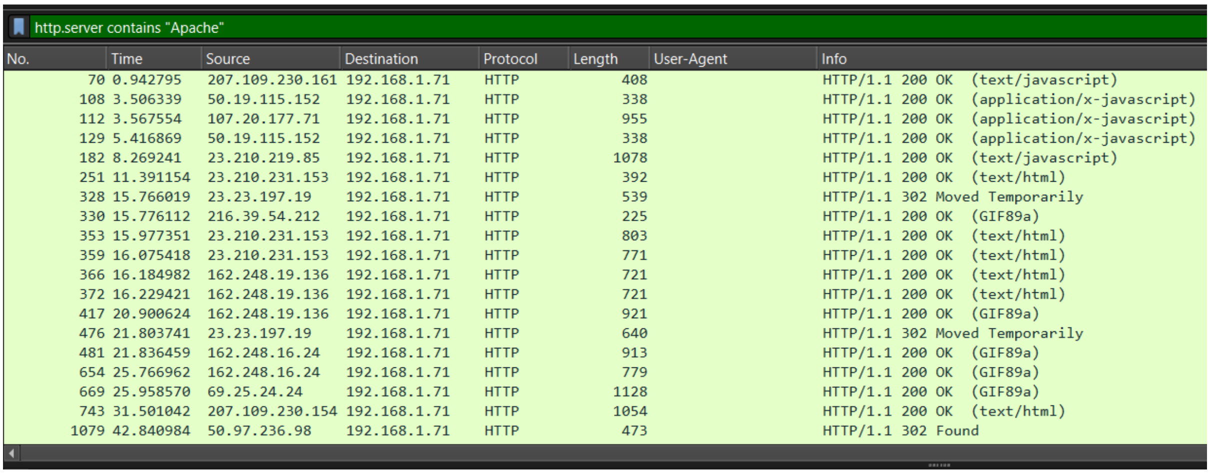
Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
1577	eu-u.openx.net	text/html	433 bytes	pd?plm=5&ph=50ab0170-10fc-4aec-b816-8
1581	s.komoona.com	application/x-javascript	5603 bytes	cad674db7f73589c9a110884ce73bb72.js
1590	uk-ads.openx.net	image/gif	43 bytes	ri?ts=1fHJpZD04Y2FkYmVmMC0zZTQyLTRkN
1609	stat.komoona.com	application/x-javascript	4 bytes	s?tagid=cad674db7f73589c9a110884ce73bb
1621	tags.expo9.exponential.com	application/x-javascript	55 kB	tags.js
1683	a.tribalfusion.com	application/x-javascript	247 bytes	displayAd.js?dver=0.4&th=10872238776
1687	a.tribalfusion.com	application/x-javascript	2705 bytes	j.ad?flashVer=13&ver=1.27&th=108722387
1717	r.openx.net	image/gif	43 bytes	set?pid=2076250f-92c2-4ecd-9043-cc63ee6
1728	d.audienceiq.com	image/gif	43 bytes	url
1729	r.openx.net	image/gif	43 bytes	set?pid=dce4ef5e-ecb8-d932-f636-f7e5ea3(
1732	r.openx.net	image/gif	43 bytes	set?pid=408c9df8-85fe-6893-4938-ccbfd204
1751	cdnx.tribalfusion.com	application/x-javascript	3708 bytes	tf_adChoice11.js
1797	ad.doubleclick.net	text/html	8124 bytes	;ord=1174955055?
1802	pixel.adsafeprotected.com	text/javascript	39 kB	skeleton.js
1811	stat.komoona.com	application/x-javascript	4 bytes	s?t=js&l=http%3A%2F%2Fwww.snopes.com
1855	js.dmtry.com	application/x-javascript	17 kB	antenna2.js?0_3586_106061319_56948507
1858	s1.2mdn.net	text/javascript	801 bytes	flashwrite_1_2.js
1868	dt.adsafeprotected.com	image/gif	43 bytes	privacy-policy
1907	cdnx.tribalfusion.com	image/png	513 bytes	ad_choices_i_UR.png
1910	cdnx.tribalfusion.com	image/png	1608 bytes	ad_choices_UR.png
1915	static.adsafeprotected.com	application/x-javascript	17 bytes	skeleton.js
1956	pagead2.googlesyndication.com	text/javascript	57 kB	lidar.js
2005	s1.2mdn.net	application/x-shockwave-flash	40 kB	Zillow_728x90_Rooms_Q4.swf
2023	b.scorecardresearch.com	application/x-javascript	1900 bytes	beacon.js
2043	tap2-cdn.rubiconproject.com	text/html	19 kB	19861&geo=na&co=us

4. How many web servers are running Apache?

This can be determined by looking at the Server field in the HTTP responses in the trace file.

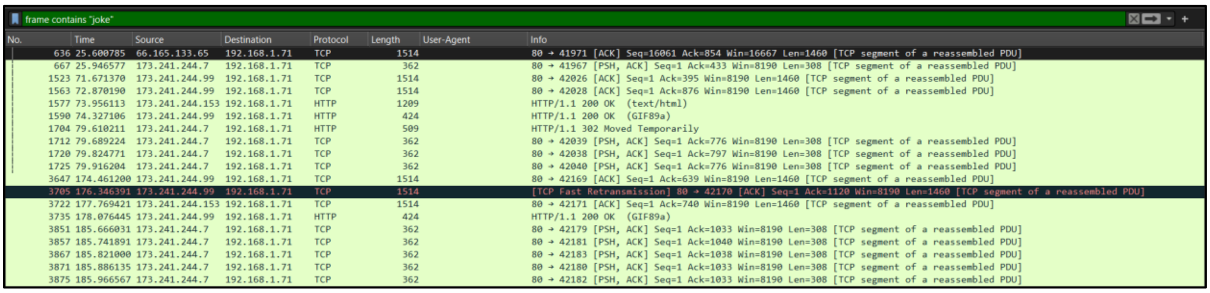
79 OR 21



```
http.server contains "Apache"
No.     Time       Source          Destination   Protocol Length User-Agent Info
     70 0.942795   207.109.230.161 192.168.1.71  HTTP      408              HTTP/1.1 200 OK  (text/javascript)
    108 3.506339   50.19.115.152   192.168.1.71  HTTP      338              HTTP/1.1 200 OK  (application/x-javascript)
    112 3.567554   107.20.177.71   192.168.1.71  HTTP      955              HTTP/1.1 200 OK  (application/x-javascript)
    129 5.416869   50.19.115.152   192.168.1.71  HTTP      338              HTTP/1.1 200 OK  (application/x-javascript)
    182 8.269241   23.210.219.85   192.168.1.71  HTTP     1078              HTTP/1.1 200 OK  (text/javascript)
    251 11.391154  23.210.231.153  192.168.1.71  HTTP      392              HTTP/1.1 200 OK  (text/html)
    328 15.766019  23.23.197.19    192.168.1.71  HTTP      539              HTTP/1.1 302 Moved Temporarily
    330 15.776112  216.39.54.212   192.168.1.71  HTTP      225              HTTP/1.1 200 OK  (GIF89a)
    353 15.977351  23.210.231.153  192.168.1.71  HTTP      803              HTTP/1.1 200 OK  (text/html)
    359 16.075418  23.210.231.153  192.168.1.71  HTTP      771              HTTP/1.1 200 OK  (text/html)
    366 16.184982  162.248.19.136  192.168.1.71  HTTP      721              HTTP/1.1 200 OK  (text/html)
    372 16.229421  162.248.19.136  192.168.1.71  HTTP      721              HTTP/1.1 200 OK  (text/html)
    417 20.900624  162.248.19.136  192.168.1.71  HTTP      921              HTTP/1.1 200 OK  (GIF89a)
    476 21.803741  23.23.197.19    192.168.1.71  HTTP      640              HTTP/1.1 302 Moved Temporarily
    481 21.836459  162.248.16.24   192.168.1.71  HTTP      913              HTTP/1.1 200 OK  (GIF89a)
    654 25.766962  162.248.16.24   192.168.1.71  HTTP      779              HTTP/1.1 200 OK  (GIF89a)
    669 25.958570  69.25.24.24     192.168.1.71  HTTP     1128              HTTP/1.1 200 OK  (GIF89a)
    743 31.501042  207.109.230.154 192.168.1.71  HTTP     1054              HTTP/1.1 200 OK  (text/html)
   1079 42.840984  50.97.236.98    192.168.1.71  HTTP      473              HTTP/1.1 302 Found
```

5. What hosts (IP addresses) think that jokes are more entertaining when they are explained?

There are two hosts that think that jokes are more entertaining when they are explained, with IP addresses of 192.168.1.100 and 192.168.1.101. This can be determined by looking at the HTTP GET requests for /jokes/joke-of-the-day.html, which have a referrer field that includes the text "I think jokes are more entertaining when they are explained."



```
frame contains "joke"
No.     Time        Source          Destination   Protocol Length User-Agent Info
    636 25.600785   66.165.133.65   192.168.1.71  TCP      1514              80 → 41971 [ACK] Seq=16061 Ack=854 Win=16667 Len=1460 [TCP segment of a reassembled PDU]
    667 25.946577   173.241.244.7   192.168.1.71  TCP       362              80 → 41967 [PSH, ACK] Seq=1 Ack=433 Win=8190 Len=308 [TCP segment of a reassembled PDU]
   1523 71.671370   173.241.244.99  192.168.1.71  TCP      1514              80 → 42026 [ACK] Seq=1 Ack=395 Win=8190 Len=1460 [TCP segment of a reassembled PDU]
   1563 72.870190   173.241.244.99  192.168.1.71  TCP      1514              80 → 42028 [ACK] Seq=1 Ack=876 Win=8190 Len=1460 [TCP segment of a reassembled PDU]
   1577 73.956113   173.241.244.153 192.168.1.71  HTTP     1209              HTTP/1.1 200 OK  (text/html)
   1590 74.327106   173.241.244.99  192.168.1.71  HTTP      424              HTTP/1.1 200 OK  (GIF89a)
   1704 79.610211   173.241.244.7   192.168.1.71  HTTP      509              HTTP/1.1 302 Moved Temporarily
   1712 79.689224   173.241.244.7   192.168.1.71  TCP       362              80 → 42039 [PSH, ACK] Seq=1 Ack=776 Win=8190 Len=308 [TCP segment of a reassembled PDU]
   1720 79.824771   173.241.244.7   192.168.1.71  TCP       362              80 → 42038 [PSH, ACK] Seq=1 Ack=797 Win=8190 Len=308 [TCP segment of a reassembled PDU]
   1725 79.916204   173.241.244.7   192.168.1.71  TCP       362              80 → 42040 [PSH, ACK] Seq=1 Ack=776 Win=8190 Len=308 [TCP segment of a reassembled PDU]
   3647 174.461200  173.241.244.99  192.168.1.71  TCP      1514              80 → 42169 [ACK] Seq=1 Ack=639 Win=8190 Len=1460 [TCP segment of a reassembled PDU]
   3705 176.346391  173.241.244.99  192.168.1.71  TCP      1514              [TCP Fast Retransmission] 80 → 42170 [ACK] Seq=1 Ack=1120 Win=8190 Len=1460 [TCP segment of a reassembled PDU]
   3722 177.769421  173.241.244.153 192.168.1.71  TCP      1514              80 → 42171 [ACK] Seq=1 Ack=740 Win=8190 Len=1460 [TCP segment of a reassembled PDU]
   3735 178.076445  173.241.244.99  192.168.1.71  HTTP      424              HTTP/1.1 200 OK  (GIF89a)
   3851 185.666031  173.241.244.7   192.168.1.71  TCP       362              80 → 42179 [PSH, ACK] Seq=1 Ack=1033 Win=8190 Len=308 [TCP segment of a reassembled PDU]
   3857 185.741891  173.241.244.7   192.168.1.71  TCP       362              80 → 42181 [PSH, ACK] Seq=1 Ack=1040 Win=8190 Len=308 [TCP segment of a reassembled PDU]
   3867 185.821000  173.241.244.7   192.168.1.71  TCP       362              80 → 42183 [PSH, ACK] Seq=1 Ack=1038 Win=8190 Len=308 [TCP segment of a reassembled PDU]
   3871 185.886135  173.241.244.7   192.168.1.71  TCP       362              80 → 42180 [PSH, ACK] Seq=1 Ack=1033 Win=8190 Len=308 [TCP segment of a reassembled PDU]
   3875 185.966567  173.241.244.7   192.168.1.71  TCP       362              80 → 42182 [PSH, ACK] Seq=1 Ack=1033 Win=8190 Len=308 [TCP segment of a reassembled PDU]
```

Wireshark Challenge 2

Analyzing the Packet Capture File: p3.pcap

Examine the wireshark window and find answers to the following questions:

A. This packet capture file contains two TCP handshakes. Find the first handshake and write down the packet numbers of those packets (the column labeled "No.").

   : 1 to 3 and 10 to 12

B. In this session, a client machine initiated a connection to a server and then downloaded a file. What is the client's IP address?

   : 10.100.1.24

C. How many HTTP GET request packets are there?

   : 3

D. Find the first HTTP GET request packet. What was the server's IP address? (The server is the Destination).

   : 74.125.19.113 Or 147.144.1.212

E. Examine the first packet. Look at the center pane in Wireshark. How many bytes were sent on the wire to form this packet?

   : 66 byte

Wireshark Challenge 3

1. WHAT THE HECK?

TRACE FILE: challengescan.pcapng

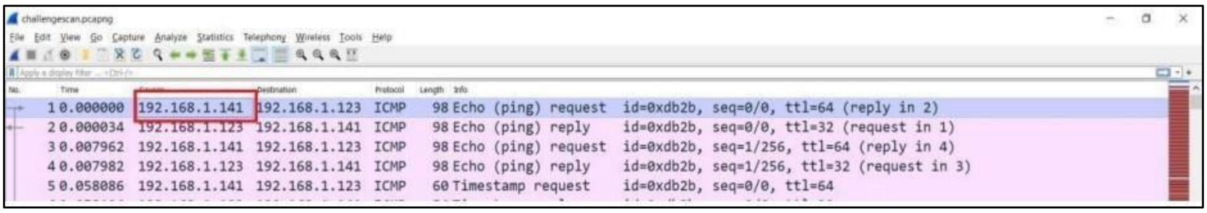
BACKGROUND: This captured file was taken from a very large and well-established network that had been considered very stable and unchanging. The network administrator has given you this file that contains what he considers "suspicious" behavior and has asked you to evaluate it.

QUESTIONS:

What is the IP address of the scanning host?

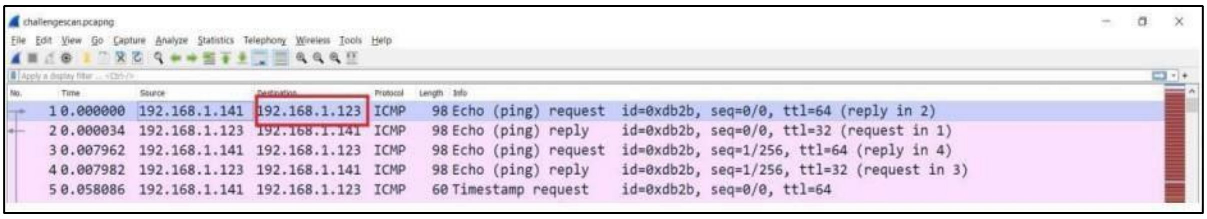
Answer: 192.168.1.141

Analysis –ICMP echo request is coming through 192.168.1.141.



```
No.  Time      Source         Destination    Protocol Length Info
   1 0.000000  192.168.1.141  192.168.1.123  ICMP     98 Echo (ping) request  id=0xdb2b, seq=0/0, ttl=64 (reply in 2)
   2 0.000034  192.168.1.123  192.168.1.141  ICMP     98 Echo (ping) reply    id=0xdb2b, seq=0/0, ttl=32 (request in 1)
   3 0.007962  192.168.1.141  192.168.1.123  ICMP     98 Echo (ping) request  id=0xdb2b, seq=1/256, ttl=64 (reply in 4)
   4 0.007982  192.168.1.123  192.168.1.141  ICMP     98 Echo (ping) reply    id=0xdb2b, seq=1/256, ttl=32 (request in 3)
   5 0.058086  192.168.1.141  192.168.1.123  ICMP     60 Timestamp request    id=0xdb2b, seq=0/0, ttl=64
```

What is the IP address of the target host? Answer: 192.168.1.123

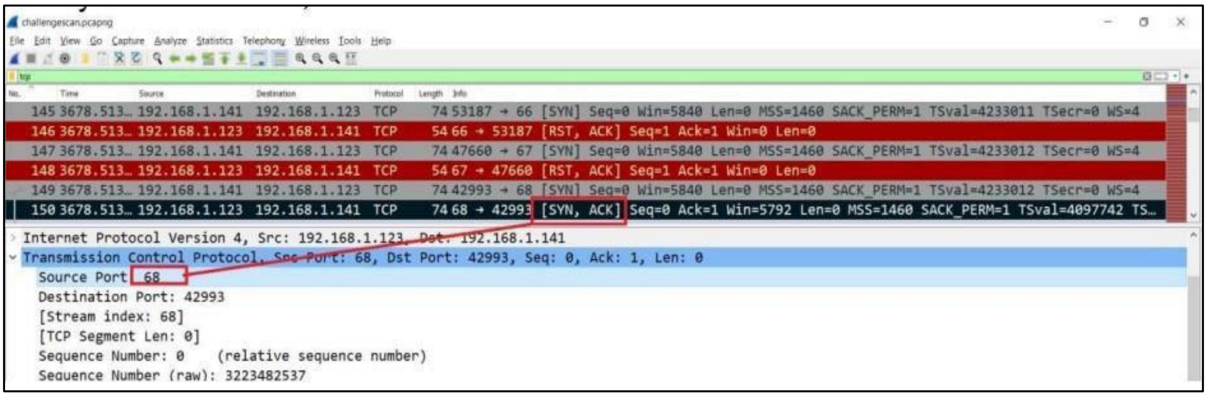


```
No.  Time      Source         Destination    Protocol Length Info
   1 0.000000  192.168.1.141  192.168.1.123  ICMP     98 Echo (ping) request  id=0xdb2b, seq=0/0, ttl=64 (reply in 2)
   2 0.000034  192.168.1.123  192.168.1.141  ICMP     98 Echo (ping) reply    id=0xdb2b, seq=0/0, ttl=32 (request in 1)
   3 0.007962  192.168.1.141  192.168.1.123  ICMP     98 Echo (ping) request  id=0xdb2b, seq=1/256, ttl=64 (reply in 4)
   4 0.007982  192.168.1.123  192.168.1.141  ICMP     98 Echo (ping) reply    id=0xdb2b, seq=1/256, ttl=32 (request in 3)
   5 0.058086  192.168.1.141  192.168.1.123  ICMP     60 Timestamp request    id=0xdb2b, seq=0/0, ttl=64
```

Which TCP port opens on the target?

Answer: Port 68

Analysis: Find SYN,ACK Packet and its source host

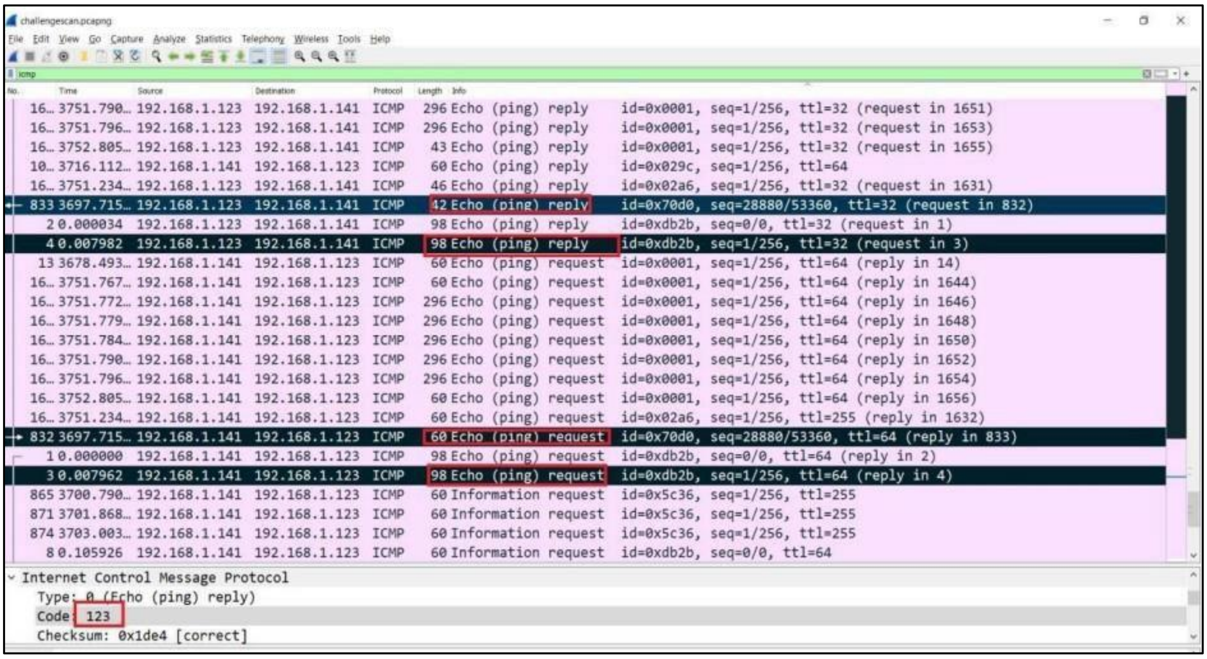


```
tcp
No.  Time        Source         Destination    Protocol Length Info
 145 3678.513... 192.168.1.141  192.168.1.123  TCP      74 53187 → 66 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=4233011 TSecr=0 WS=4
 146 3678.513... 192.168.1.123  192.168.1.141  TCP      54 66 → 53187 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 147 3678.513... 192.168.1.141  192.168.1.123  TCP      74 47660 → 67 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=4233012 TSecr=0 WS=4
 148 3678.513... 192.168.1.123  192.168.1.141  TCP      54 67 → 47660 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 149 3678.513... 192.168.1.141  192.168.1.123  TCP      74 42993 → 68 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=4233012 TSecr=0 WS=4
 150 3678.513... 192.168.1.123  192.168.1.141  TCP      74 68 → 42993 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4097742 TS...

> Internet Protocol Version 4, Src: 192.168.1.123, Dst: 192.168.1.141
v Transmission Control Protocol, Src Port: 68, Dst Port: 42993, Seq: 0, Ack: 1, Len: 0
    Source Port: 68
    Destination Port: 42993
    [Stream index: 68]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3223482537
```

Which ICMP packets contain non-standard Type/Code numbers?

Answer: Code 123

Analysis: After checking all ICMP packets, the selected 4 packets had code 123. Others had 0 and 3


challengescan.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info

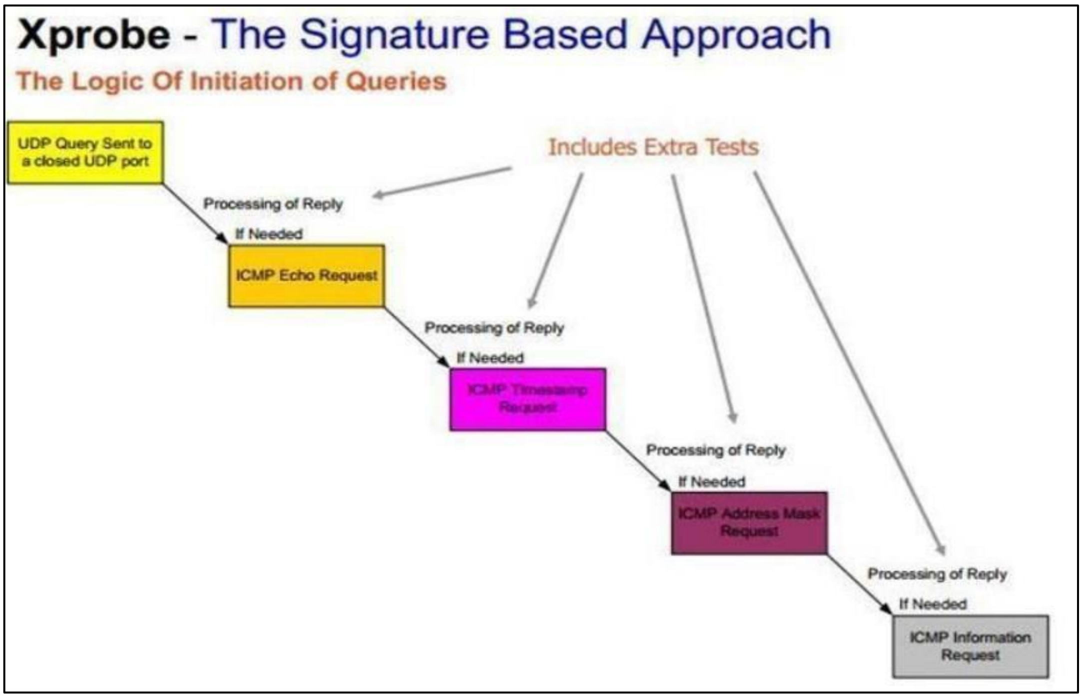
```
   16… 3751.790… 192.168.1.123 192.168.1.141 ICMP 296 Echo (ping) reply     id=0x0001, seq=1/256, ttl=32 (request in 1651)
   16… 3751.796… 192.168.1.123 192.168.1.141 ICMP 296 Echo (ping) reply     id=0x0001, seq=1/256, ttl=32 (request in 1653)
   16… 3752.805… 192.168.1.123 192.168.1.141 ICMP  43 Echo (ping) reply     id=0x0001, seq=1/256, ttl=32 (request in 1655)
   10… 3716.112… 192.168.1.141 192.168.1.123 ICMP  60 Echo (ping) reply     id=0x029c, seq=1/256, ttl=64
   16… 3751.234… 192.168.1.123 192.168.1.141 ICMP  46 Echo (ping) reply     id=0x02a6, seq=1/256, ttl=32 (request in 1631)
  833 3697.715… 192.168.1.123 192.168.1.141 ICMP  42 Echo (ping) reply     id=0x70d0, seq=28880/53360, ttl=32 (request in 832)
    2 0.000034  192.168.1.123 192.168.1.141 ICMP  98 Echo (ping) reply     id=0xdb2b, seq=0/0, ttl=32 (request in 1)
    4 0.007982  192.168.1.123 192.168.1.141 ICMP  98 Echo (ping) reply     id=0xdb2b, seq=1/256, ttl=32 (request in 3)
   13 3678.493… 192.168.1.141 192.168.1.123 ICMP  60 Echo (ping) request   id=0x0001, seq=1/256, ttl=64 (reply in 14)
   16… 3751.767… 192.168.1.141 192.168.1.123 ICMP  60 Echo (ping) request   id=0x0001, seq=1/256, ttl=64 (reply in 1644)
   16… 3751.772… 192.168.1.141 192.168.1.123 ICMP 296 Echo (ping) request   id=0x0001, seq=1/256, ttl=64 (reply in 1646)
   16… 3751.779… 192.168.1.141 192.168.1.123 ICMP 296 Echo (ping) request   id=0x0001, seq=1/256, ttl=64 (reply in 1648)
   16… 3751.784… 192.168.1.141 192.168.1.123 ICMP 296 Echo (ping) request   id=0x0001, seq=1/256, ttl=64 (reply in 1650)
   16… 3751.790… 192.168.1.141 192.168.1.123 ICMP 296 Echo (ping) request   id=0x0001, seq=1/256, ttl=64 (reply in 1652)
   16… 3751.796… 192.168.1.141 192.168.1.123 ICMP 296 Echo (ping) request   id=0x0001, seq=1/256, ttl=64 (reply in 1654)
   16… 3752.805… 192.168.1.141 192.168.1.123 ICMP  60 Echo (ping) request   id=0x0001, seq=1/256, ttl=64 (reply in 1656)
   16… 3751.234… 192.168.1.141 192.168.1.123 ICMP  60 Echo (ping) request   id=0x02a6, seq=1/256, ttl=255 (reply in 1632)
  832 3697.715… 192.168.1.141 192.168.1.123 ICMP  60 Echo (ping) request   id=0x70d0, seq=28880/53360, ttl=64 (reply in 833)
    1 0.000000  192.168.1.141 192.168.1.123 ICMP  98 Echo (ping) request   id=0xdb2b, seq=0/0, ttl=64 (reply in 2)
    3 0.007962  192.168.1.141 192.168.1.123 ICMP  98 Echo (ping) request   id=0xdb2b, seq=1/256, ttl=64 (reply in 4)
  865 3700.790… 192.168.1.141 192.168.1.123 ICMP  60 Information request   id=0x5c36, seq=1/256, ttl=255
  871 3701.868… 192.168.1.141 192.168.1.123 ICMP  60 Information request   id=0x5c36, seq=1/256, ttl=255
  874 3703.003… 192.168.1.141 192.168.1.123 ICMP  60 Information request   id=0x5c36, seq=1/256, ttl=255
    8 0.105926  192.168.1.141 192.168.1.123 ICMP  60 Information request   id=0xdb2b, seq=0/0, ttl=64
```

```
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 123
  Checksum: 0x1de4 [correct]
```

What software is used to scan the target?

Answer: Xprobe

Analysis:

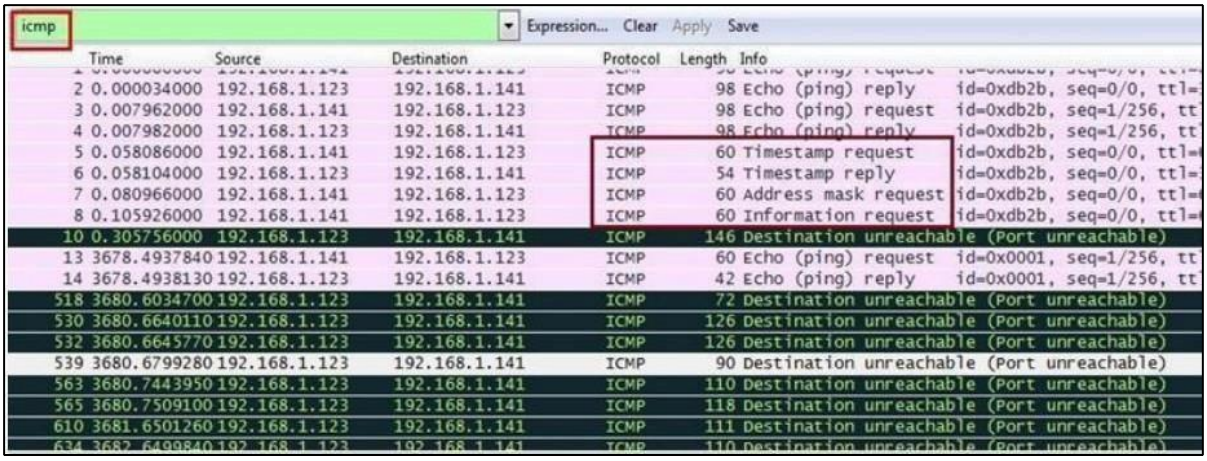


Xprobe - The Signature Based Approach

The Logic Of Initiation of Queries

As can be seen in the above diagram, it is an ICMP based scan and the first request is an ICMP echo request; after that it sends the ICMP timestamp request, then it sends the

ICMP address mask request, and at last it sends the ICMP information request. The same pattern is also available in the trace file where we applied the filter for ICMP packets.



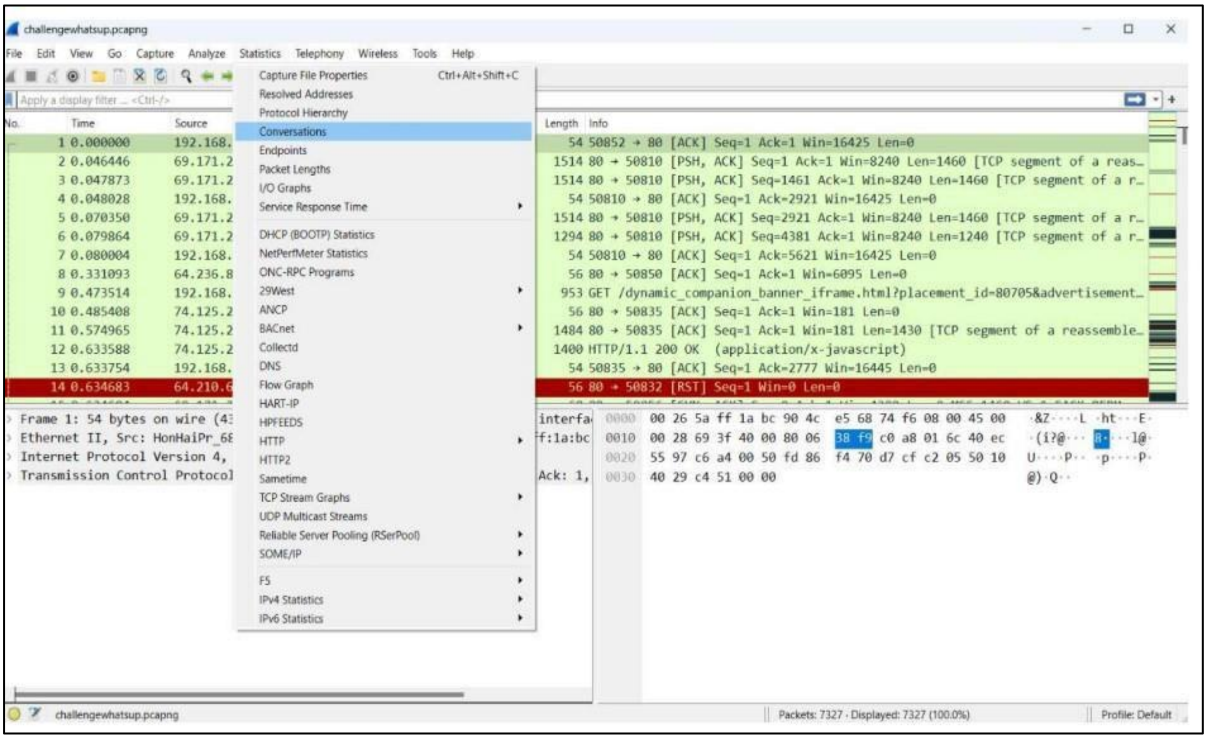
```
    Time          Source         Destination    Protocol Length Info
  2 0.000034000   192.168.1.123  192.168.1.141  ICMP       98 Echo (ping) reply      id=0xdb2b, seq=0/0, ttl=
  3 0.007962000   192.168.1.141  192.168.1.123  ICMP       98 Echo (ping) request    id=0xdb2b, seq=1/256, tt
  4 0.007982000   192.168.1.123  192.168.1.141  ICMP       98 Echo (ping) reply      id=0xdb2b, seq=1/256, tt
  5 0.058086000   192.168.1.141  192.168.1.123  ICMP       60 Timestamp request      id=0xdb2b, seq=0/0, ttl=
  6 0.058104000   192.168.1.123  192.168.1.141  ICMP       54 Timestamp reply        id=0xdb2b, seq=0/0, ttl=
  7 0.080966000   192.168.1.141  192.168.1.123  ICMP       60 Address mask request   id=0xdb2b, seq=0/0, ttl=
  8 0.105926000   192.168.1.141  192.168.1.123  ICMP       60 Information request    id=0xdb2b, seq=0/0, ttl=
 10 0.305756000   192.168.1.123  192.168.1.141  ICMP      146 Destination unreachable (Port unreachable)
 13 3678.4937840  192.168.1.141  192.168.1.123  ICMP       60 Echo (ping) request    id=0x0001, seq=1/256, tt
 14 3678.4938130  192.168.1.123  192.168.1.141  ICMP       42 Echo (ping) reply      id=0x0001, seq=1/256, tt
518 3680.6034700  192.168.1.123  192.168.1.141  ICMP       72 Destination unreachable (Port unreachable)
530 3680.6640110  192.168.1.123  192.168.1.141  ICMP      126 Destination unreachable (Port unreachable)
532 3680.6645770  192.168.1.123  192.168.1.141  ICMP      126 Destination unreachable (Port unreachable)
539 3680.6799280  192.168.1.123  192.168.1.141  ICMP       90 Destination unreachable (Port unreachable)
563 3680.7443950  192.168.1.123  192.168.1.141  ICMP      110 Destination unreachable (Port unreachable)
565 3680.7509100  192.168.1.123  192.168.1.141  ICMP      118 Destination unreachable (Port unreachable)
610 3681.6501260  192.168.1.123  192.168.1.141  ICMP      111 Destination unreachable (Port unreachable)
634 3682.6499840  192.168.1.123  192.168.1.141  ICMP      110 Destination unreachable (Port unreachable)
```

Cursed

How many different IP hosts is Scott's machine communicating with?

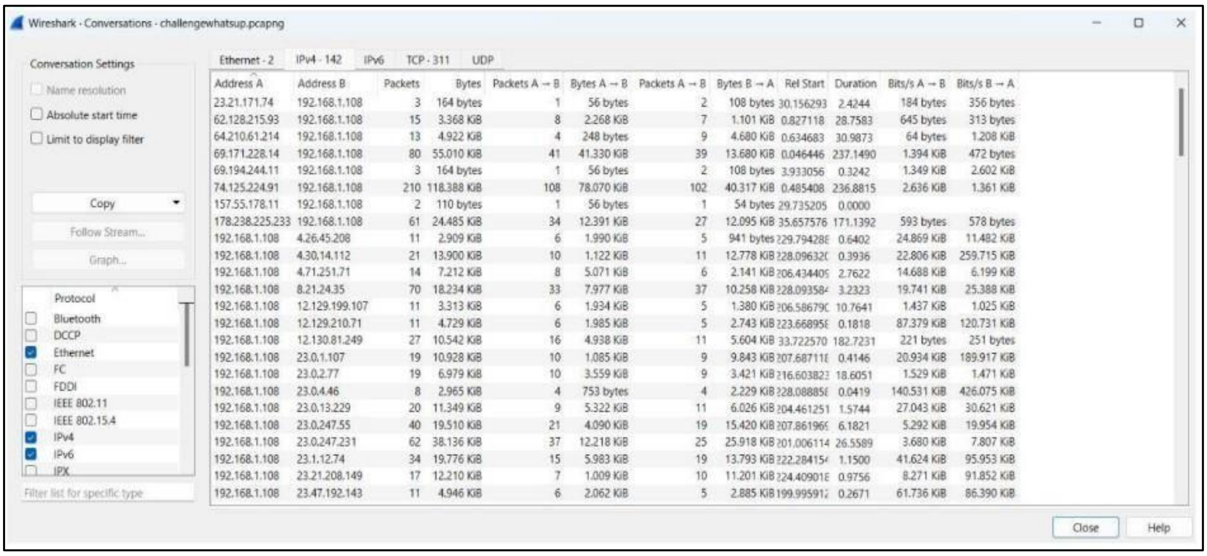
Answer: 142

First we have to check the communication which can be seen by opening Statistics > Conversations



```
No.  Time      Source        Length Info
  1 0.000000  192.168.         54 50852 → 80 [ACK] Seq=1 Ack=1 Win=16425 Len=0
  2 0.046446  69.171.2       1514 80 → 50810 [PSH, ACK] Seq=1 Ack=1 Win=8240 Len=1460 [TCP segment of a reas…
  3 0.047873  69.171.2       1514 80 → 50810 [PSH, ACK] Seq=1461 Ack=1 Win=8240 Len=1460 [TCP segment of a r…
  4 0.048028  192.168.         54 50810 → 80 [ACK] Seq=1 Ack=2921 Win=16425 Len=0
  5 0.070350  69.171.2       1514 80 → 50810 [PSH, ACK] Seq=2921 Ack=1 Win=8240 Len=1460 [TCP segment of a r…
  6 0.079864  69.171.2       1294 80 → 50810 [PSH, ACK] Seq=4381 Ack=1 Win=8240 Len=1240 [TCP segment of a r…
  7 0.080004  192.168.         54 50810 → 80 [ACK] Seq=1 Ack=5621 Win=16425 Len=0
  8 0.331093  64.236.8         56 80 → 50850 [ACK] Seq=1 Ack=1 Win=6095 Len=0
  9 0.473514  192.168.        953 GET /dynamic_companion_banner_iframe.html?placement_id=80705&advertisement…
 10 0.485408  74.125.2         56 80 → 50835 [ACK] Seq=1 Ack=1 Win=181 Len=0
 11 0.574965  74.125.2       1484 80 → 50835 [ACK] Seq=1 Ack=1 Win=181 Len=1430 [TCP segment of a reassemble…
 12 0.633588  74.125.2       1400 HTTP/1.1 200 OK  (application/x-javascript)
 13 0.633754  192.168.         54 50835 → 80 [ACK] Seq=1 Ack=2777 Win=16445 Len=0
 14 0.634683  64.210.6         56 80 → 50832 [RST] Seq=1 Win=0 Len=0

> Frame 1: 54 bytes on wire (4…        interfa…
> Ethernet II, Src: HonHaiPr_6…        …f:1a:bc
> Internet Protocol Version 4,
> Transmission Control Protocol        Ack: 1,

0000  00 26 5a ff 1a bc 90 4c  e5 68 74 f6 08 00 45 00   ·&Z····L ·ht···E·
0010  00 28 69 3f 40 00 80 06  38 f9 c0 a8 01 6c 40 ec   ·(i?@··· 8····l@·
0020  55 97 c6 a4 00 50 fd 86  f4 70 d7 cf c2 05 50 10   U····P·· ·p····P·
0030  40 29 c4 51 00 00                                  @)·Q··
```

Then we can select the Ipv4 tab and see the count is 142 which means that there are 142 Ips communicating with Scott’s machine.



Wireshark · Conversations · challengewhatsup.pcapng
Copy
Follow Stream...
Graph...
Filter list for specific type
Close
Help

Conversation Settings

☐ Name resolution
☐ Absolute start time
☐ Limit to display filter

Protocol
☐ Bluetooth
☐ DCCP
☑ Ethernet
☐ FC
☐ FDDI
☐ IEEE 802.11
☐ IEEE 802.15.4
☑ IPv4
☑ IPv6
☐ IPX

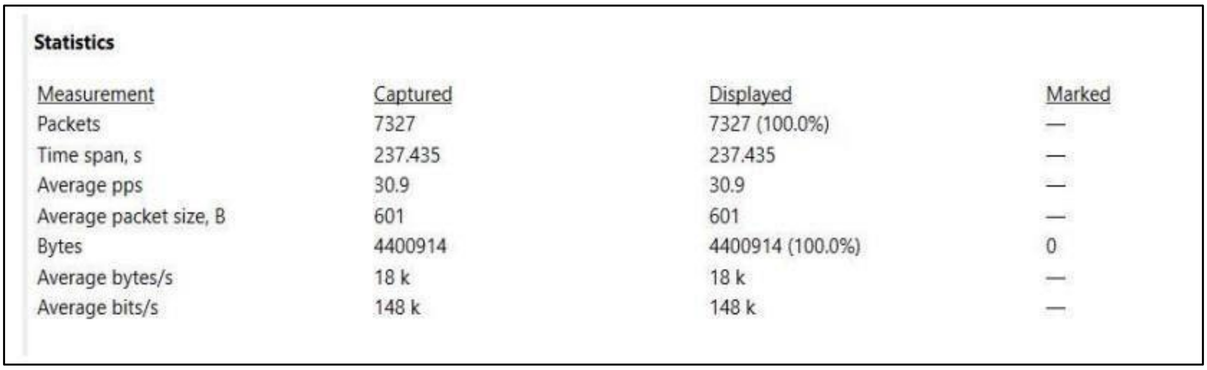
Ethernet · 2 | IPv4 · 142 | IPv6 | TCP · 311 | UDP

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets A → B	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
23.21.171.74	192.168.1.108	3	164 bytes	1	56 bytes	2	108 bytes	30.156293	2.4244	184 bytes	356 bytes
62.128.215.93	192.168.1.108	15	3.368 KiB	8	2.268 KiB	7	1.101 KiB	0.827118	28.7583	645 bytes	313 bytes
64.210.61.214	192.168.1.108	13	4.922 KiB	4	248 bytes	9	4.680 KiB	0.634683	30.9873	64 bytes	1.208 KiB
69.171.228.14	192.168.1.108	80	55.010 KiB	41	41.330 KiB	39	13.680 KiB	0.046446	237.1490	1.394 KiB	472 bytes
69.194.244.11	192.168.1.108	3	164 bytes	1	56 bytes	2	108 bytes	3.933056	0.3242	1.349 KiB	2.602 KiB
74.125.224.91	192.168.1.108	210	118.388 KiB	108	78.070 KiB	102	40.317 KiB	0.485408	236.8815	2.636 KiB	1.361 KiB
157.55.178.11	192.168.1.108	2	110 bytes	1	56 bytes	1	54 bytes	29.735205	0.0000		
178.238.225.233	192.168.1.108	61	24.485 KiB	34	12.391 KiB	27	12.095 KiB	35.657576	171.1392	593 bytes	578 bytes
192.168.1.108	4.26.45.208	11	2.909 KiB	6	1.990 KiB	5	941 bytes	229.79428	0.6402	24.869 KiB	11.482 KiB
192.168.1.108	4.30.14.112	21	13.900 KiB	10	1.122 KiB	11	12.778 KiB	228.09632	0.3936	22.806 KiB	259.715 KiB
192.168.1.108	4.71.251.71	14	7.212 KiB	8	5.071 KiB	6	2.141 KiB	206.43440	2.7622	14.688 KiB	6.199 KiB
192.168.1.108	8.21.24.35	70	18.234 KiB	33	7.977 KiB	37	10.258 KiB	228.09358	3.2323	19.741 KiB	25.388 KiB
192.168.1.108	12.129.199.107	11	3.313 KiB	6	1.934 KiB	5	1.380 KiB	206.58679	10.7641	1.437 KiB	1.025 KiB
192.168.1.108	12.129.210.71	11	4.729 KiB	6	1.985 KiB	5	2.743 KiB	223.66895	0.1818	87.379 KiB	120.731 KiB
192.168.1.108	12.130.81.249	27	10.542 KiB	16	4.938 KiB	11	5.604 KiB	33.722570	182.7231	221 bytes	251 bytes
192.168.1.108	23.0.1.107	19	10.928 KiB	10	1.085 KiB	9	9.843 KiB	207.68711	0.4146	20.934 KiB	189.917 KiB
192.168.1.108	23.0.2.77	19	6.979 KiB	10	3.559 KiB	9	3.421 KiB	216.60382	18.6051	1.529 KiB	1.471 KiB
192.168.1.108	23.0.4.46	8	2.965 KiB	4	753 bytes	4	2.229 KiB	228.08885	0.0419	140.531 KiB	426.075 KiB
192.168.1.108	23.0.13.229	20	11.349 KiB	9	5.322 KiB	11	6.026 KiB	204.461251	1.5744	27.043 KiB	30.621 KiB
192.168.1.108	23.0.247.55	40	19.510 KiB	21	4.090 KiB	19	15.420 KiB	207.86196	6.1821	5.292 KiB	19.954 KiB
192.168.1.108	23.0.247.231	62	38.136 KiB	37	12.218 KiB	25	25.918 KiB	201.006114	26.5589	3.680 KiB	7.807 KiB
192.168.1.108	23.1.12.74	34	19.776 KiB	15	5.983 KiB	19	13.793 KiB	222.28415	1.1500	41.624 KiB	95.953 KiB
192.168.1.108	23.21.208.149	17	12.210 KiB	7	1.009 KiB	10	11.201 KiB	224.40901	0.9756	8.271 KiB	91.852 KiB
192.168.1.108	23.47.192.143	11	4.946 KiB	6	2.062 KiB	5	2.885 KiB	199.99591	0.2671	61.736 KiB	86.390 KiB

What is the average packets per second rate seen in this trace file?

Answer: 30.9

We can check out the packets rate per second from the summary options. Select > Statistics> Capture File Properties And as shown below, we can see the average packets rate per second



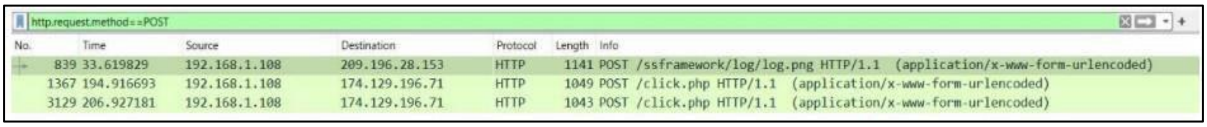
Statistics

Measurement	Captured	Displayed	Marked
Packets	7327	7327 (100.0%)	—
Time span, s	237.435	237.435	—
Average pps	30.9	30.9	—
Average packet size, B	601	601	—
Bytes	4400914	4400914 (100.0%)	0
Average bytes/s	18 k	18 k	—
Average bits/s	148 k	148 k	—

How many HTTP POST requests did Scott’s machine send?

Answer: 3

We applied a filter i.e. http.request.method == POST to filter only POST requests

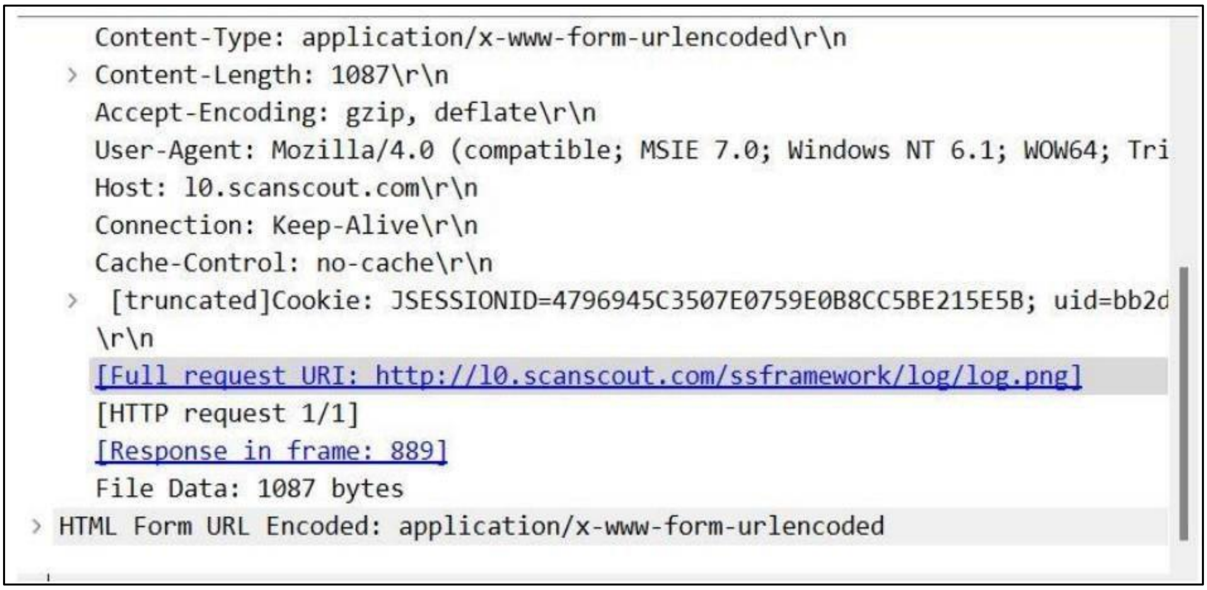


```
http.request.method==POST
No.    Time          Source          Destination       Protocol  Length  Info
 839 33.619829      192.168.1.108   209.196.28.153    HTTP      1141 POST /ssframework/log/log.png HTTP/1.1  (application/x-www-form-urlencoded)
1367 194.916693     192.168.1.108   174.129.196.71    HTTP      1049 POST /click.php HTTP/1.1  (application/x-www-form-urlencoded)
3129 206.927181     192.168.1.108   174.129.196.71    HTTP      1043 POST /click.php HTTP/1.1  (application/x-www-form-urlencoded)
```

What location information is contained in the POST toscanscout.com?

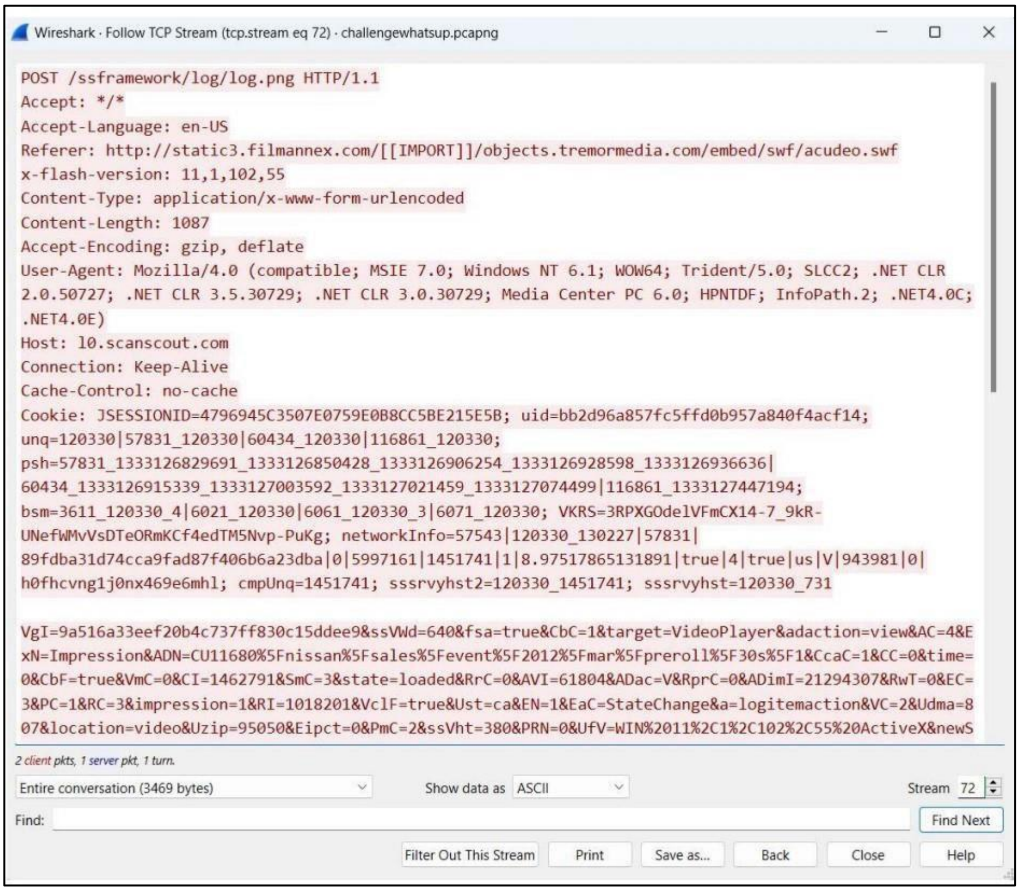
Answer: San Francisco – Oakland – San Jose

First find the POST request, and there are only three of them, and next we have to find which request header contains the scanscout.com. We checked out all three requests and found one of the request headers is for scanscout.com.



```
    Content-Type: application/x-www-form-urlencoded\r\n
  > Content-Length: 1087\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Tri
    Host: l0.scanscout.com\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
  >  [truncated]Cookie: JSESSIONID=4796945C3507E0759E0B8CC5BE215E5B; uid=bb2d
    \r\n
    [Full request URI: http://l0.scanscout.com/ssframework/log/log.png]
    [HTTP request 1/1]
    [Response in frame: 889]
    File Data: 1087 bytes
> HTML Form URL Encoded: application/x-www-form-urlencoded
```

After that we need to find the location. So to find it click on the POST request and select follows TCP stream.



Wireshark · Follow TCP Stream (tcp.stream eq 72) · challengewhatsup.pcapng

```
POST /ssframework/log/log.png HTTP/1.1
Accept: */*
Accept-Language: en-US
Referer: http://static3.filmannex.com/[[IMPORT]]/objects.tremormedia.com/embed/swf/acudeo.swf
x-flash-version: 11,1,102,55
Content-Type: application/x-www-form-urlencoded
Content-Length: 1087
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; HPNTDF; InfoPath.2; .NET4.0C;
.NET4.0E)
Host: l0.scanscout.com
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: JSESSIONID=4796945C3507E0759E0B8CC5BE215E5B; uid=bb2d96a857fc5ffd0b957a840f4acf14;
unq=120330|57831_120330|60434_120330|116861_120330;
psh=57831_1333126829691_1333126850428_1333126906254_1333126928598_1333126936636|
60434_1333126915339_1333127003592_1333127021459_1333127074499|116861_1333127447194;
bsm=3611_120330_4|6021_120330|6061_120330_3|6071_120330; VKRS=3RPXGOdelVFmCX14-7_9kR-
UNefWMvVsDTeORmKCf4edTM5Nvp-PuKg; networkInfo=57543|120330_130227|57831|
89fdba31d74cca9fad87f406b6a23dba|0|5997161|1451741|1|8.97517865131891|true|4|true|us|V|943981|0|
h0fhcvng1j0nx469e6mhl; cmpUnq=1451741; sssrvyhst2=120330_1451741; sssrvyhst=120330_731

VgI=9a516a33eef20b4c737ff830c15ddee9&ssVWd=640&fsa=true&CbC=1&target=VideoPlayer&adaction=view&AC=4&E
xN=Impression&ADN=CU11680%5Fnissan%5Fsales%5Fevent%5F2012%5Fmar%5Fpreroll%5F30s%5F1&CcaC=1&CC=0&time=
0&CbF=true&VmC=0&CI=1462791&SmC=3&state=loaded&RrC=0&AVI=61804&ADac=V&RprC=0&ADimI=21294307&RwT=0&EC=
3&PC=1&RC=3&impression=1&RI=1018201&VclF=true&Ust=ca&EN=1&EaC=StateChange&a=logitemaction&VC=2&Udma=8
07&location=video&Uzip=95050&Eipct=0&PmC=2&ssVht=380&PRN=0&UfV=WIN%2011%2C1%2C102%2C55%20ActiveX&newS
```

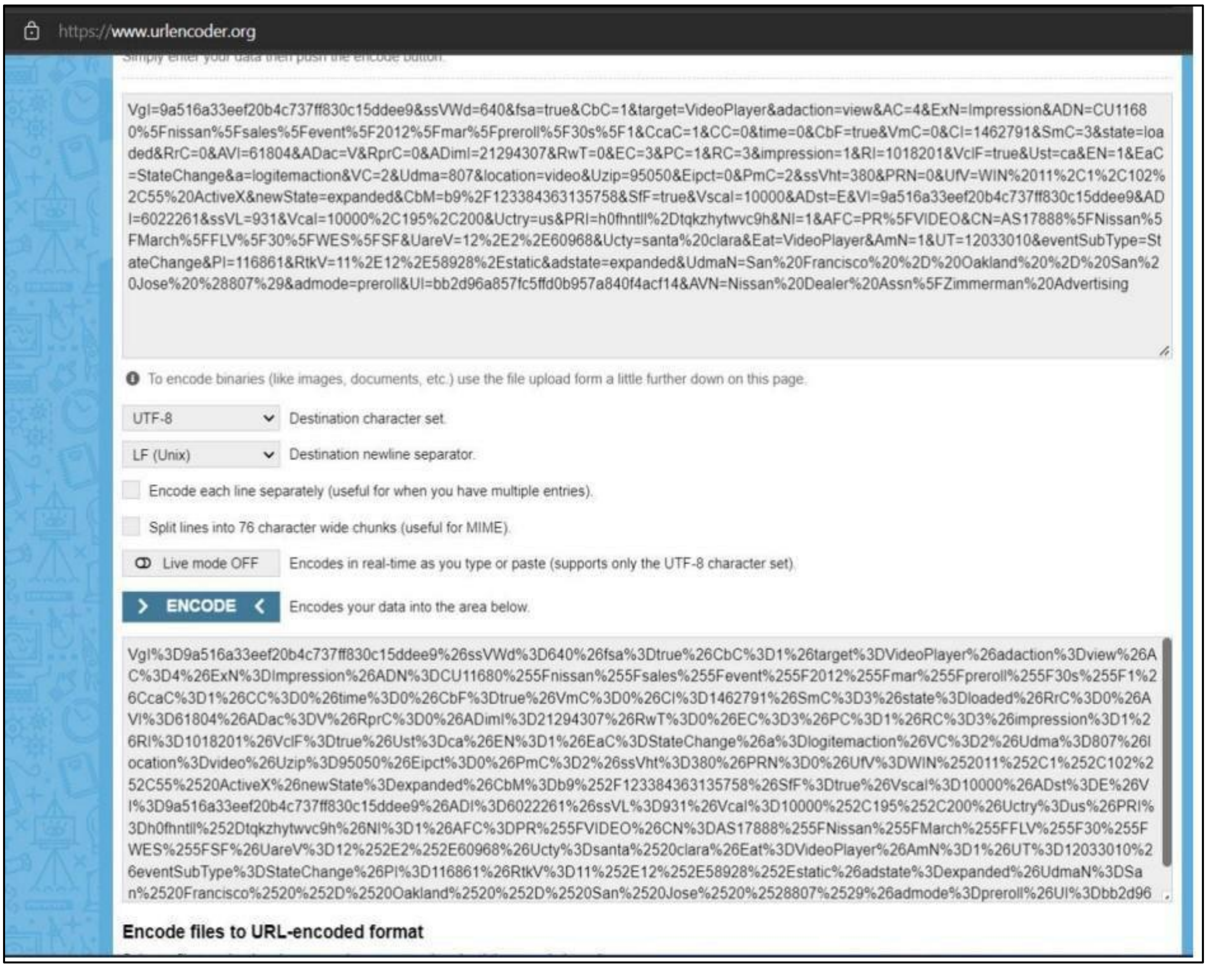
2 client pkts, 1 server pkt, 1 turn.

Entire conversation (3469 bytes)

Show data as ASCII

Stream 72

As can be seen below we can now see the whole POST data of that request. It contains a lot of parameters and its value and its URL are encoded, so we are not able to read them clearly We copied the whole data and used a url decoder



Simply enter your data then push the encode button.

```
Vgl=9a516a33eef20b4c737ff830c15ddee9&ssVWd=640&fsa=true&CbC=1&target=VideoPlayer&adaction=view&AC=4&ExN=Impression&ADN=CU1168
0%5Fnissan%5Fsales%5Fevent%5F2012%5Fmar%5Fpreroll%5F30s%5F1&CcaC=1&CC=0&time=0&CbF=true&VmC=0&CI=1462791&SmC=3&state=loa
ded&RrC=0&AVI=61804&ADac=V&RprC=0&ADiml=21294307&RwT=0&EC=3&PC=1&RC=3&impression=1&RI=1018201&VclF=true&Ust=ca&EN=1&EaC
=StateChange&a=logitemaction&VC=2&Udma=807&location=video&Uzip=95050&Eipct=0&PmC=2&ssVht=380&PRN=0&UfV=WIN%2011%2C1%2C102%
2C55%20ActiveX&newState=expanded&CbM=b9%2F123384363135758&SfF=true&Vscal=10000&ADst=E&VI=9a516a33eef20b4c737ff830c15ddee9&AD
I=6022261&ssVL=931&Vcal=10000%2C195%2C200&Uctry=us&PRI=h0fhntll%2Dtqkzhytwvc9h&NI=1&AFC=PR%5FVIDEO&CN=AS17888%5FNissan%5
FMarch%5FFLV%5F30%5FWES%5FSF&UareV=12%2E2%2E60968&Ucty=santa%20clara&Eat=VideoPlayer&AmN=1&UT=12033010&eventSubType=St
ateChange&PI=116861&RtkV=11%2E12%2E58928%2Estatic&adstate=expanded&UdmaN=San%20Francisco%20%2D%20Oakland%20%2D%20San%2
0Jose%20%28807%29&admode=preroll&UI=bb2d96a857fc5ffd0b957a840f4acf14&AVN=Nissan%20Dealer%20Assn%5FZimmerman%20Advertising
```

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Destination character set.

LF (Unix) Destination newline separator.

□ Encode each line separately (useful for when you have multiple entries).

□ Split lines into 76 character wide chunks (useful for MIME).

Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

Encodes your data into the area below.

```
Vgl%3D9a516a33eef20b4c737ff830c15ddee9%26ssVWd%3D640%26fsa%3Dtrue%26CbC%3D1%26target%3DVideoPlayer%26adaction%3Dview%26A
C%3D4%26ExN%3DImpression%26ADN%3DCU11680%255Fnissan%255Fsales%255Fevent%255F2012%255Fmar%255Fpreroll%255F30s%255F1%2
6CcaC%3D1%26CC%3D0%26time%3D0%26CbF%3Dtrue%26VmC%3D0%26CI%3D1462791%26SmC%3D3%26state%3Dloaded%26RrC%3D0%26A
VI%3D61804%26ADac%3DV%26RprC%3D0%26ADiml%3D21294307%26RwT%3D0%26EC%3D3%26PC%3D1%26RC%3D3%26impression%3D1%2
6RI%3D1018201%26VclF%3Dtrue%26Ust%3Dca%26EN%3D1%26EaC%3DStateChange%26a%3Dlogitemaction%26VC%3D2%26Udma%3D807%26l
ocation%3Dvideo%26Uzip%3D95050%26Eipct%3D0%26PmC%3D2%26ssVht%3D380%26PRN%3D0%26UfV%3DWIN%252011%252C1%252C102%2
52C55%2520ActiveX%26newState%3Dexpanded%26CbM%3Db9%252F123384363135758%26SfF%3Dtrue%26Vscal%3D10000%26ADst%3DE%26V
I%3D9a516a33eef20b4c737ff830c15ddee9%26ADI%3D6022261%26ssVL%3D931%26Vcal%3D10000%252C195%252C200%26Uctry%3Dus%26PRI%
3Dh0fhntll%252Dtqkzhytwvc9h%26NI%3D1%26AFC%3DPR%255FVIDEO%26CN%3DAS17888%255FNissan%255FMarch%255FFLV%255F30%255F
WES%255FSF%26UareV%3D12%252E2%252E60968%26Ucty%3Dsanta%2520clara%26Eat%3DVideoPlayer%26AmN%3D1%26UT%3D12033010%2
6eventSubType%3DStateChange%26PI%3D116861%26RtkV%3D11%252E12%252E58928%252Estatic%26adstate%3Dexpanded%26UdmaN%3DSa
n%2520Francisco%2520%252D%2520Oakland%2520%252D%2520San%2520Jose%2520%2528807%2529%26admode%3Dpreroll%26UI%3Dbb2d96
```

Encode files to URL-encoded format

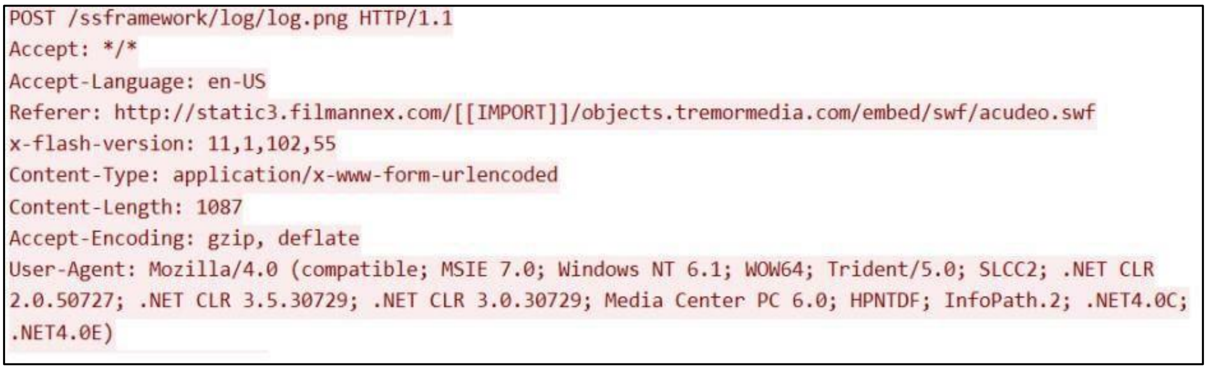
Now we can see in the below figure that the parameter Udam has its value San Francisco

– Oakland – San Jose.

What application appears to be generating these GET/POST requests?

Answer: Internet Explorer 9

It can be done by analyzing the User-Agent string of any GET/POST request

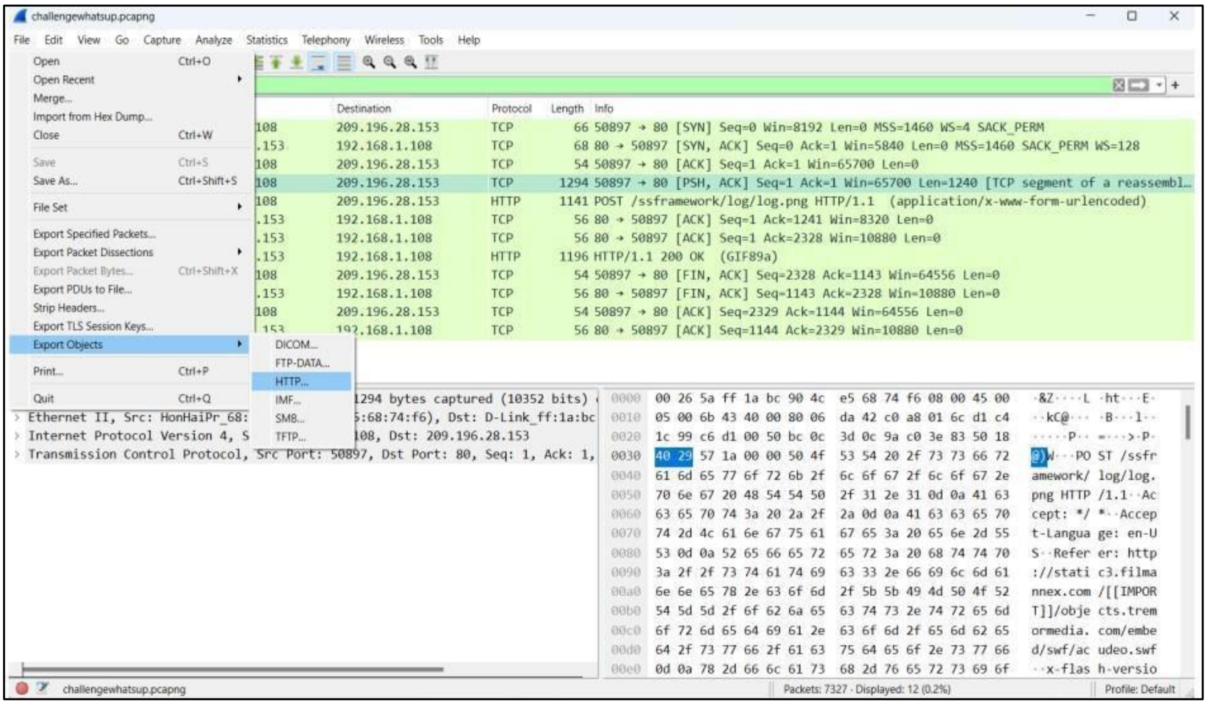


```
POST /ssframework/log/log.png HTTP/1.1
Accept: */*
Accept-Language: en-US
Referer: http://static3.filmannex.com/[[IMPORT]]/objects.tremormedia.com/embed/swf/acudeo.swf
x-flash-version: 11,1,102,55
Content-Type: application/x-www-form-urlencoded
Content-Length: 1087
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; HPNTDF; InfoPath.2; .NET4.0C;
.NET4.0E)
```

Find,export and reassemble load_small.png. what shape is in the image?

Answer: Star

We have to find a .png image in this. All packets can't check every request manually and look for this image, so we will extract all the HTTP objects from this trace file. Go to File and select Export Objects > HTTP

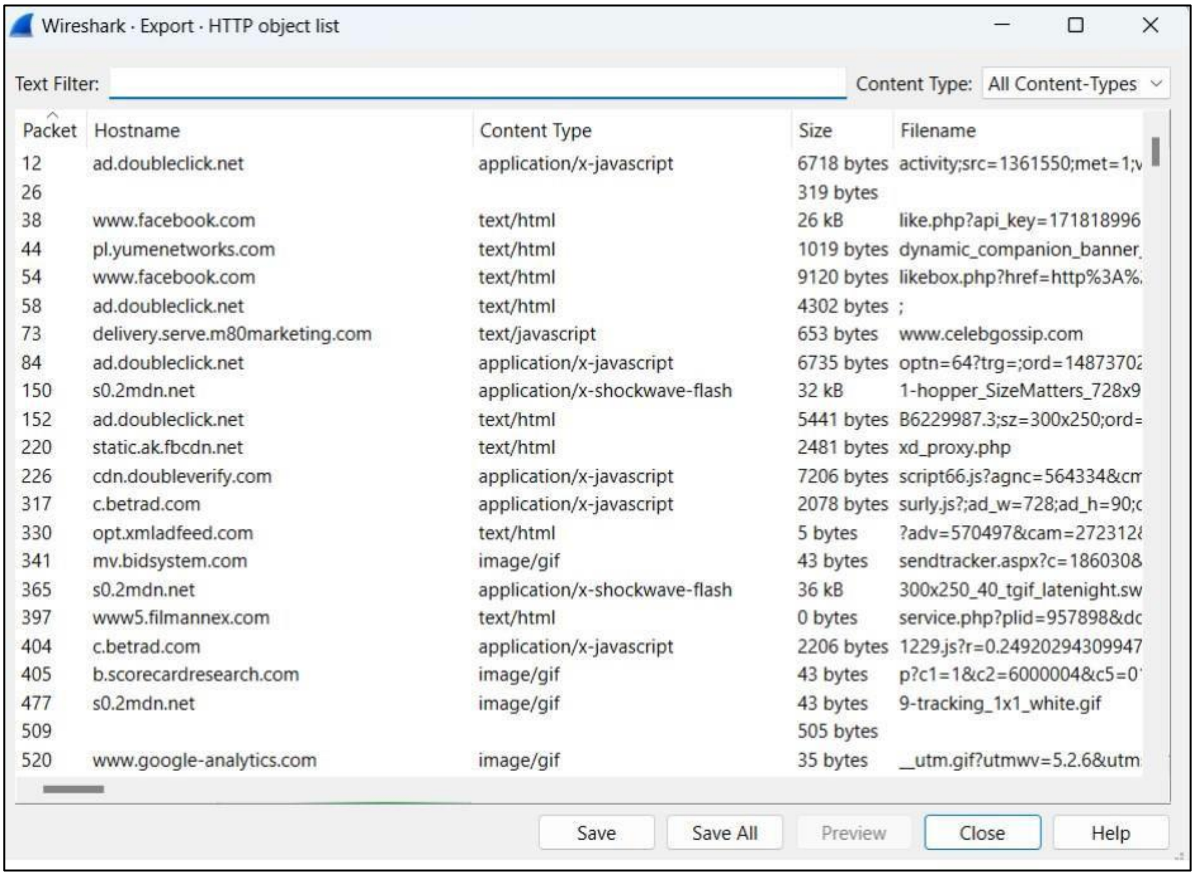


```
        Destination      Protocol  Length Info
108     209.196.28.153   TCP          66 50897 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
.153    192.168.1.108    TCP          68 80 → 50897 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=128
108     209.196.28.153   TCP          54 50897 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
108     209.196.28.153   TCP        1294 50897 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65700 Len=1240 [TCP segment of a reassembl…
108     209.196.28.153   HTTP       1141 POST /ssframework/log/log.png HTTP/1.1  (application/x-www-form-urlencoded)
.153    192.168.1.108    TCP          56 80 → 50897 [ACK] Seq=1 Ack=1241 Win=8320 Len=0
.153    192.168.1.108    TCP          56 80 → 50897 [ACK] Seq=1 Ack=2328 Win=10880 Len=0
.153    192.168.1.108    HTTP       1196 HTTP/1.1 200 OK  (GIF89a)
108     209.196.28.153   TCP          54 50897 → 80 [FIN, ACK] Seq=2328 Ack=1143 Win=64556 Len=0
.153    192.168.1.108    TCP          56 80 → 50897 [FIN, ACK] Seq=1143 Ack=2328 Win=10880 Len=0
108     209.196.28.153   TCP          54 50897 → 80 [ACK] Seq=2329 Ack=1144 Win=64556 Len=0
.153    192.168.1.108    TCP          56 80 → 50897 [ACK] Seq=1144 Ack=2329 Win=10880 Len=0
```

```
1294 bytes captured (10352 bits)
> Ethernet II, Src: HonHaiPr_68:  5:68:74:f6), Dst: D-Link_ff:1a:bc
> Internet Protocol Version 4, S  108, Dst: 209.196.28.153
> Transmission Control Protocol, Src Port: 50897, Dst Port: 80, Seq: 1, Ack: 1,
```

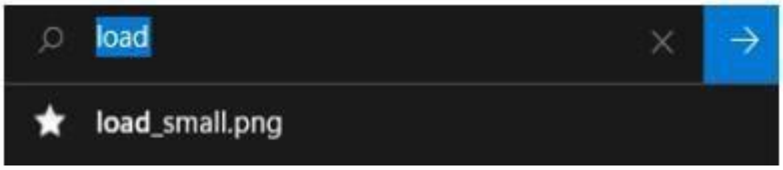
```
0000  00 26 5a ff 1a bc 90 4c  e5 68 74 f6 08 00 45 00   ·&Z····L ·ht···E·
0010  05 00 6b 43 40 00 80 06  da 42 c0 a8 01 6c d1 c4   ··kC@··· ·B···l··
0020  1c 99 c6 d1 00 50 bc 0c  3d 0c 9a c0 3e 83 50 18   ·····P·· =···>·P·
0030  40 29 57 1a 00 00 50 4f  53 54 20 2f 73 73 66 72   @)W···PO ST /ssfr
0040  61 6d 65 77 6f 72 6b 2f  6c 6f 67 2f 6c 6f 67 2e   amework/ log/log.
0050  70 6e 67 20 48 54 54 50  2f 31 2e 31 0d 0a 41 63   png HTTP /1.1··Ac
0060  63 65 70 74 3a 20 2a 2f  2a 0d 0a 41 63 63 65 70   cept: */ *··Accep
0070  74 2d 4c 61 6e 67 75 61  67 65 3a 20 65 6e 2d 55   t-Langua ge: en-U
0080  53 0d 0a 52 65 66 65 72  65 72 3a 20 68 74 74 70   S··Refer er: http
0090  3a 2f 2f 73 74 61 74 69  63 33 2e 66 69 6c 6d 61   ://stati c3.filma
00a0  6e 6e 65 78 2e 63 6f 6d  2f 5b 5b 49 4d 50 4f 52   nnex.com /[[IMPOR
00b0  54 5d 5d 2f 6f 62 6a 65  63 74 73 2e 74 72 65 6d   T]]/obje cts.trem
00c0  6f 72 6d 65 64 69 61 2e  63 6f 6d 2f 65 6d 62 65   ormedia. com/embe
00d0  64 2f 73 77 66 2f 61 63  75 64 65 6f 2e 73 77 66   d/swf/ac udeo.swf
00e0  0d 0a 78 2d 66 6c 61 73  68 2d 76 65 72 73 69 6f   ··x-flas h-versio
```

challengewhatsup.pcapng | Packets: 7327 · Displayed: 12 (0.2%) | Profile: Default


Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Save
Save All
Preview
Close
Help

Packet	Hostname	Content Type	Size	Filename
12	ad.doubleclick.net	application/x-javascript	6718 bytes	activity;src=1361550;met=1;v
26			319 bytes	
38	www.facebook.com	text/html	26 kB	like.php?api_key=171818996
44	pl.yumenetworks.com	text/html	1019 bytes	dynamic_companion_banner_
54	www.facebook.com	text/html	9120 bytes	likebox.php?href=http%3A%:
58	ad.doubleclick.net	text/html	4302 bytes	;
73	delivery.serve.m80marketing.com	text/javascript	653 bytes	www.celebgossip.com
84	ad.doubleclick.net	application/x-javascript	6735 bytes	optn=64?trg=;ord=14873702
150	s0.2mdn.net	application/x-shockwave-flash	32 kB	1-hopper_SizeMatters_728x9
152	ad.doubleclick.net	text/html	5441 bytes	B6229987.3;sz=300x250;ord=
220	static.ak.fbcdn.net	text/html	2481 bytes	xd_proxy.php
226	cdn.doubleverify.com	application/x-javascript	7206 bytes	script66.js?agnc=564334&cr
317	c.betrad.com	application/x-javascript	2078 bytes	surly.js?;ad_w=728;ad_h=90;c
330	opt.xmladfeed.com	text/html	5 bytes	?adv=570497&cam=272312
341	mv.bidsystem.com	image/gif	43 bytes	sendtracker.aspx?c=186030&
365	s0.2mdn.net	application/x-shockwave-flash	36 kB	300x250_40_tgif_latenight.sw
397	www5.filmannex.com	text/html	0 bytes	service.php?plid=957898&dc
404	c.betrad.com	application/x-javascript	2206 bytes	1229.js?r=0.24920294309947
405	b.scorecardresearch.com	image/gif	43 bytes	p?c1=1&c2=6000004&c5=0
477	s0.2mdn.net	image/gif	43 bytes	9-tracking_1x1_white.gif
509			505 bytes	
520	www.google-analytics.com	image/gif	35 bytes	__utm.gif?utmwv=5.2.6&utm

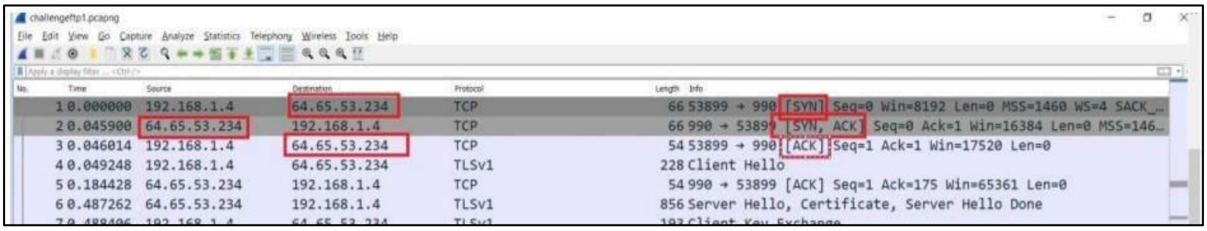
we don’t know where this load_small.png file is located in which hostname, so that’s why we will save all. We saved all files in a directory and searched for the load_small.png file and we found that file load_small.png.It is a star shape.



FTPS ANALYSIS TRACE FILES: challengeftp1.pcapng challengeftp2.pcapng BACKGROUND: A customer needed a secure file transfer application put in place. These two trace files illustrate the separate options they have tested – implicit FTPS and explicit FTPS.

QUESTIONS:

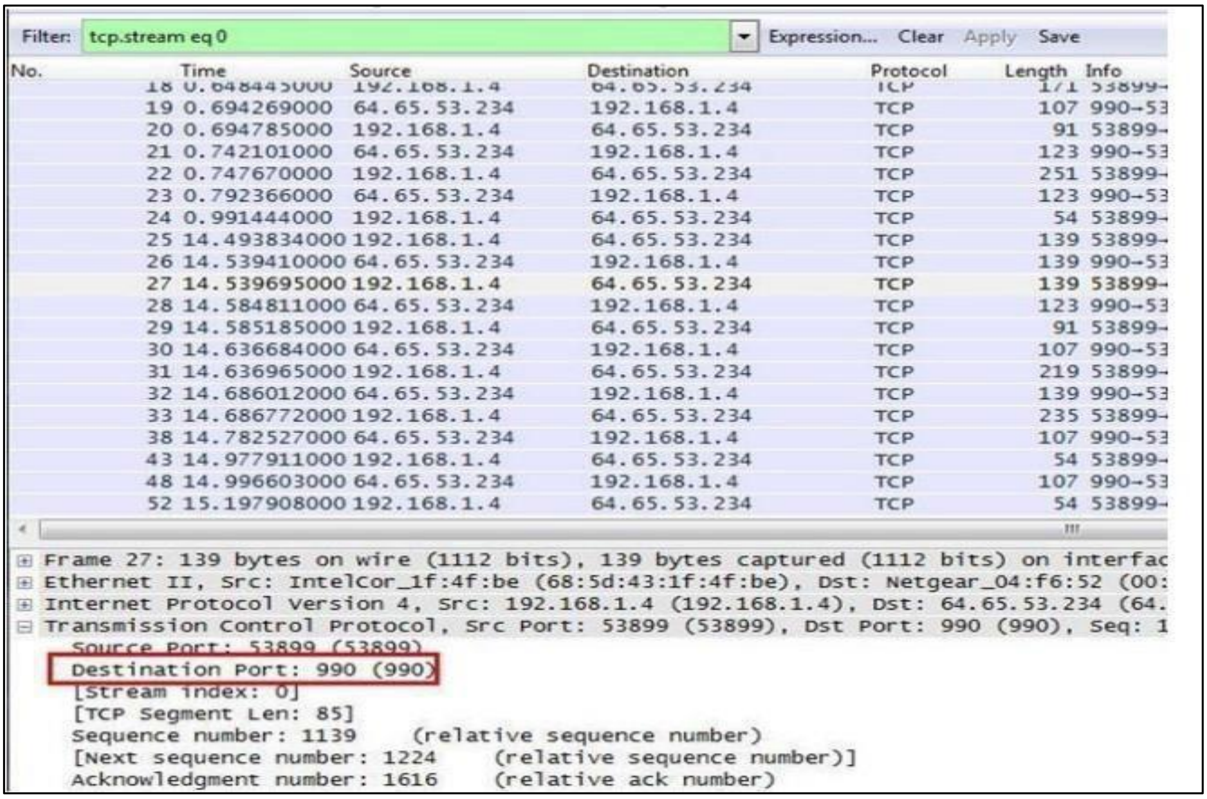
What is the IP address of the server? Answer: 64.65.53.234


challengeftp1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source         Destination    Protocol  Length Info
   1 0.000000  192.168.1.4    64.65.53.234   TCP          66 53899 → 990 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_…
   2 0.045900  64.65.53.234   192.168.1.4    TCP          66 990 → 53899 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=146…
   3 0.046014  192.168.1.4    64.65.53.234   TCP          54 53899 → 990 [ACK] Seq=1 Ack=1 Win=17520 Len=0
   4 0.049248  192.168.1.4    64.65.53.234   TLSv1       228 Client Hello
   5 0.184428  64.65.53.234   192.168.1.4    TCP          54 990 → 53899 [ACK] Seq=1 Ack=175 Win=65361 Len=0
   6 0.487262  64.65.53.234   192.168.1.4    TLSv1       856 Server Hello, Certificate, Server Hello Done
   7 0.488406  192.168.1.4    64.65.53.234   TLSv1       193 Client Key Exchange
```

Which trace illustrates implicit FTPS?

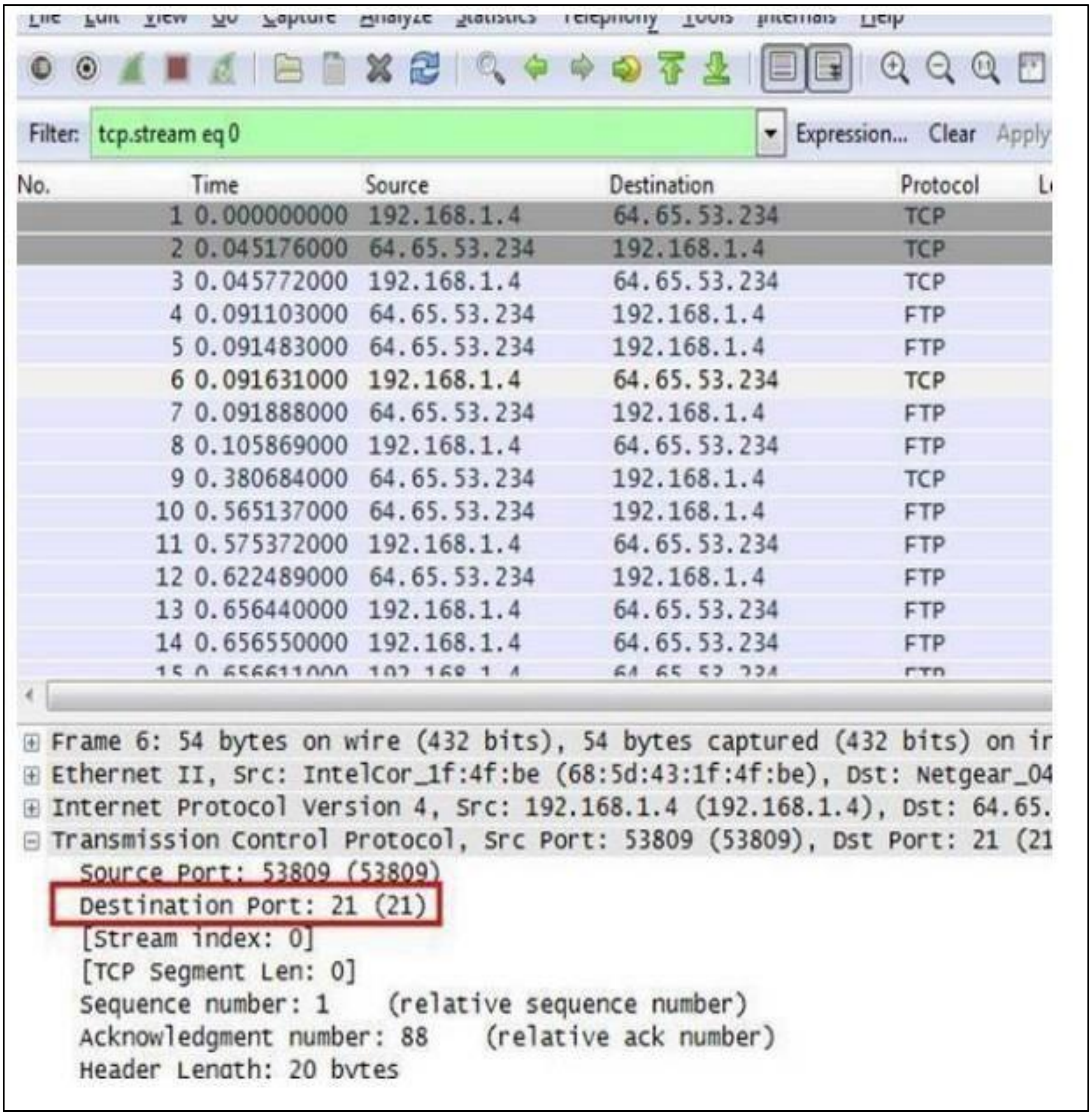
Answer: challengeftp1.pcapng, implicit FTPS is a secure connection and it runs on port 990



```
Filter: tcp.stream eq 0
No.   Time            Source         Destination    Protocol  Length  Info
   18 0.648445000     192.168.1.4    64.65.53.234   TCP          171  53899-
   19 0.694269000     64.65.53.234   192.168.1.4    TCP          107  990→53
   20 0.694785000     192.168.1.4    64.65.53.234   TCP           91  53899-
   21 0.742101000     64.65.53.234   192.168.1.4    TCP          123  990→53
   22 0.747670000     192.168.1.4    64.65.53.234   TCP          251  53899-
   23 0.792366000     64.65.53.234   192.168.1.4    TCP          123  990→53
   24 0.991444000     192.168.1.4    64.65.53.234   TCP           54  53899-
   25 14.493834000    192.168.1.4    64.65.53.234   TCP          139  53899-
   26 14.539410000    64.65.53.234   192.168.1.4    TCP          139  990→53
   27 14.539695000    192.168.1.4    64.65.53.234   TCP          139  53899-
   28 14.584811000    64.65.53.234   192.168.1.4    TCP          123  990→53
   29 14.585185000    192.168.1.4    64.65.53.234   TCP           91  53899-
   30 14.636684000    64.65.53.234   192.168.1.4    TCP          107  990→53
   31 14.636965000    192.168.1.4    64.65.53.234   TCP          219  53899-
   32 14.686012000    64.65.53.234   192.168.1.4    TCP          139  990→53
   33 14.686772000    192.168.1.4    64.65.53.234   TCP          235  53899-
   38 14.782527000    64.65.53.234   192.168.1.4    TCP          107  990→53
   43 14.977911000    192.168.1.4    64.65.53.234   TCP           54  53899-
   48 14.996603000    64.65.53.234   192.168.1.4    TCP          107  990→53
   52 15.197908000    192.168.1.4    64.65.53.234   TCP           54  53899-

⊞ Frame 27: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interfac
⊞ Ethernet II, Src: IntelCor_1f:4f:be (68:5d:43:1f:4f:be), Dst: Netgear_04:f6:52 (00:
⊞ Internet Protocol Version 4, Src: 192.168.1.4 (192.168.1.4), Dst: 64.65.53.234 (64.
⊟ Transmission Control Protocol, Src Port: 53899 (53899), Dst Port: 990 (990), Seq: 1
    Source Port: 53899 (53899)
    Destination Port: 990 (990)
    [Stream index: 0]
    [TCP Segment Len: 85]
    Sequence number: 1139    (relative sequence number)
    [Next sequence number: 1224    (relative sequence number)]
    Acknowledgment number: 1616    (relative ack number)
```

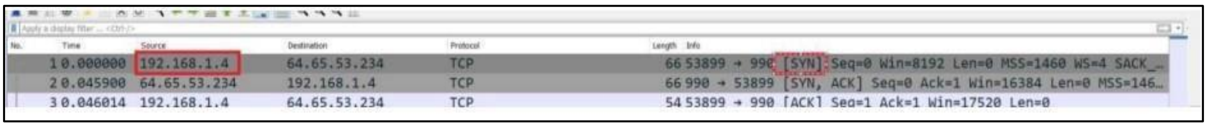
Which trace illustrates explicit FTPS?

Answer: challengeftp2.pcapng (explicit FTPS runs on port 21)



```
No.   Time          Source          Destination     Protocol  L
  1 0.000000000  192.168.1.4     64.65.53.234    TCP
  2 0.045176000  64.65.53.234    192.168.1.4     TCP
  3 0.045772000  192.168.1.4     64.65.53.234    TCP
  4 0.091103000  64.65.53.234    192.168.1.4     FTP
  5 0.091483000  64.65.53.234    192.168.1.4     FTP
  6 0.091631000  192.168.1.4     64.65.53.234    TCP
  7 0.091888000  64.65.53.234    192.168.1.4     FTP
  8 0.105869000  192.168.1.4     64.65.53.234    FTP
  9 0.380684000  64.65.53.234    192.168.1.4     TCP
 10 0.565137000  64.65.53.234    192.168.1.4     FTP
 11 0.575372000  192.168.1.4     64.65.53.234    FTP
 12 0.622489000  64.65.53.234    192.168.1.4     FTP
 13 0.656440000  192.168.1.4     64.65.53.234    FTP
 14 0.656550000  192.168.1.4     64.65.53.234    FTP
 15 0.656611000  192.168.1.4     64.65.53.234    FTP

⊞ Frame 6: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on ir
⊞ Ethernet II, Src: IntelCor_1f:4f:be (68:5d:43:1f:4f:be), Dst: Netgear_04
⊞ Internet Protocol Version 4, Src: 192.168.1.4 (192.168.1.4), Dst: 64.65.
⊟ Transmission Control Protocol, Src Port: 53809 (53809), Dst Port: 21 (21
    Source Port: 53809 (53809)
    Destination Port: 21 (21)
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 88    (relative ack number)
    Header Length: 20 bytes
```

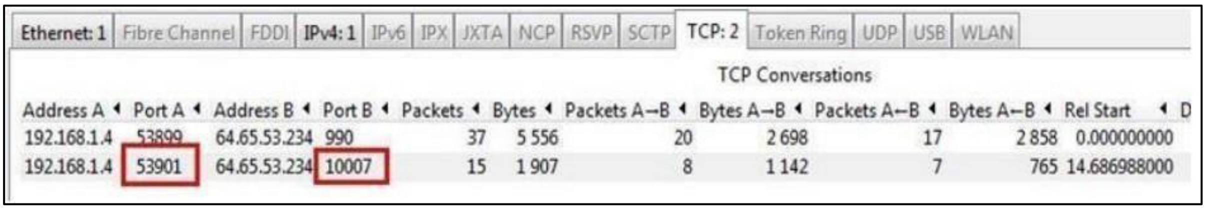
What IP address initiated the data connections in the trace file? Answer: 192.168.1.4



```
No.  Time      Source          Destination     Protocol  Length  Info
  1 0.000000  192.168.1.4     64.65.53.234    TCP        66 53899 → 990 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_…
  2 0.045900  64.65.53.234    192.168.1.4     TCP        66 990 → 53899 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=146…
  3 0.046014  192.168.1.4     64.65.53.234    TCP        54 53899 → 990 [ACK] Seq=1 Ack=1 Win=17520 Len=0
```

What port numbers are used for the data connection in each trace file?

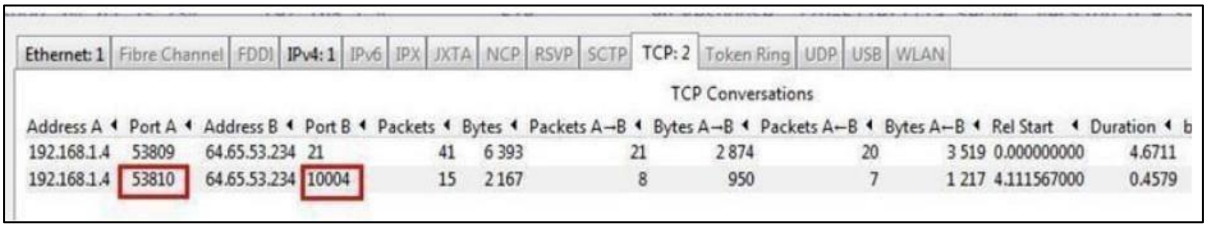
Answer: 53901-10007



TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	D
192.168.1.4	53899	64.65.53.234	990	37	5 556	20	2 698	17	2 858	0.000000000	
192.168.1.4	53901	64.65.53.234	10007	15	1 907	8	1 142	7	765	14.686988000	

Answer: 53810 – 10004



TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration	b
192.168.1.4	53809	64.65.53.234	21	41	6 393	21	2 874	20	3 519	0.000000000	4.6711	
192.168.1.4	53810	64.65.53.234	10004	15	2 167	8	950	7	1 217	4.111567000	0.4579	

OUCH! TRACE FILE: challengeattack.pcapng

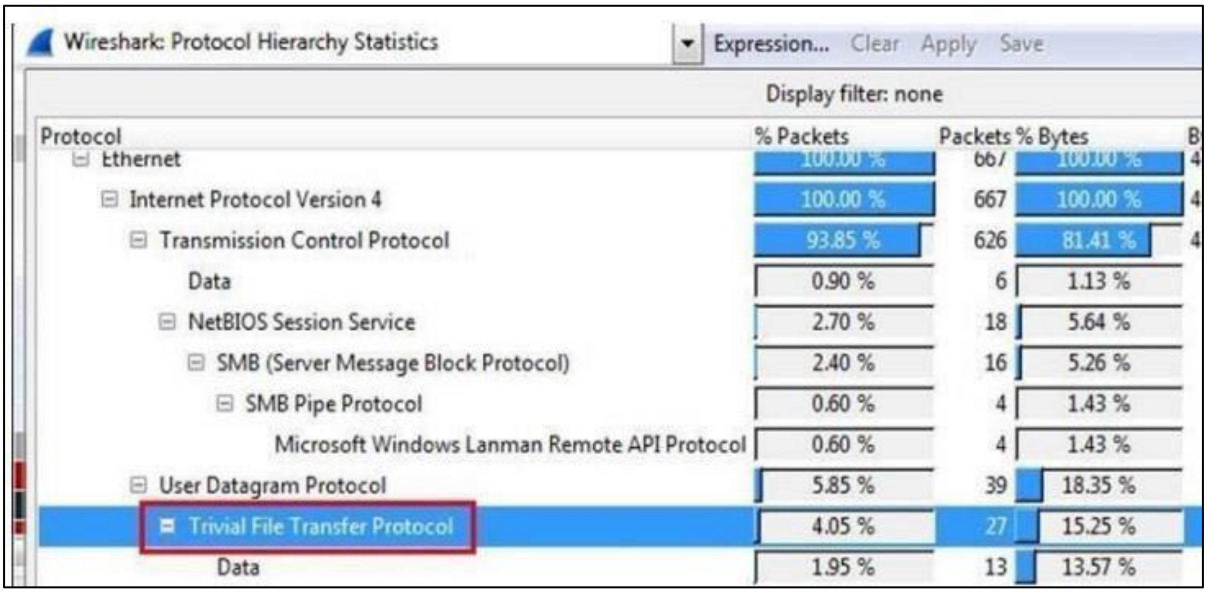
BACKGROUND: These capture files were taken from a network that was experiencing a "zero- day" attack and was completely overwhelmed. It is also reported that some of the nodes within the network appear to be unable to update their antivirus/security software. The Network Administrator has given you this file that contains what he considers "suspicious" behavior and has asked you to help. The Administrator can tell you that 141.157.228.12 is a server and that 10.1.1.31 is a client machine.

QUESTIONS:

What file transfer application is seen in this trace file?

Ans: Trivial File Transfer Protocol

Go to Statistics and then select Protocol Hierarchy which will show all protocols used in this trace file.



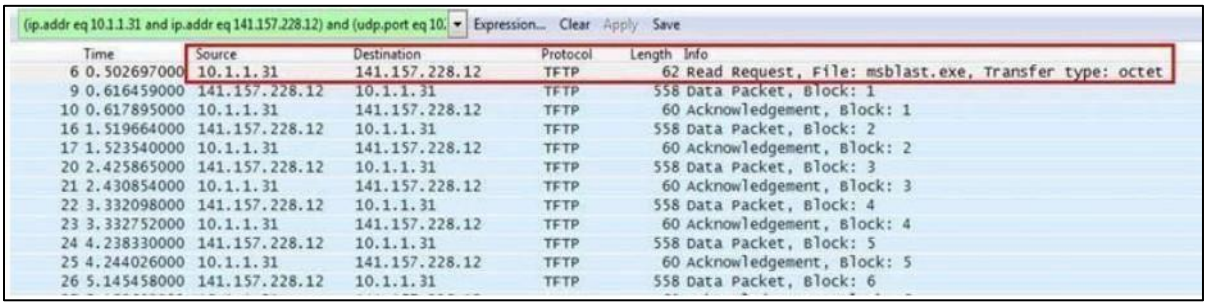
Wireshark: Protocol Hierarchy Statistics
Expression... Clear Apply Save

Display filter: none

Protocol	% Packets	Packets	% Bytes	B
Ethernet	100.00 %	667	100.00 %	4
Internet Protocol Version 4	100.00 %	667	100.00 %	4
Transmission Control Protocol	93.85 %	626	81.41 %	4
Data	0.90 %	6	1.13 %	
NetBIOS Session Service	2.70 %	18	5.64 %	
SMB (Server Message Block Protocol)	2.40 %	16	5.26 %	
SMB Pipe Protocol	0.60 %	4	1.43 %	
Microsoft Windows Lanman Remote API Protocol	0.60 %	4	1.43 %	
User Datagram Protocol	5.85 %	39	18.35 %	
Trivial File Transfer Protocol	4.05 %	27	15.25 %	
Data	1.95 %	13	13.57 %	

What is the IP address of the host that is receiving the file?

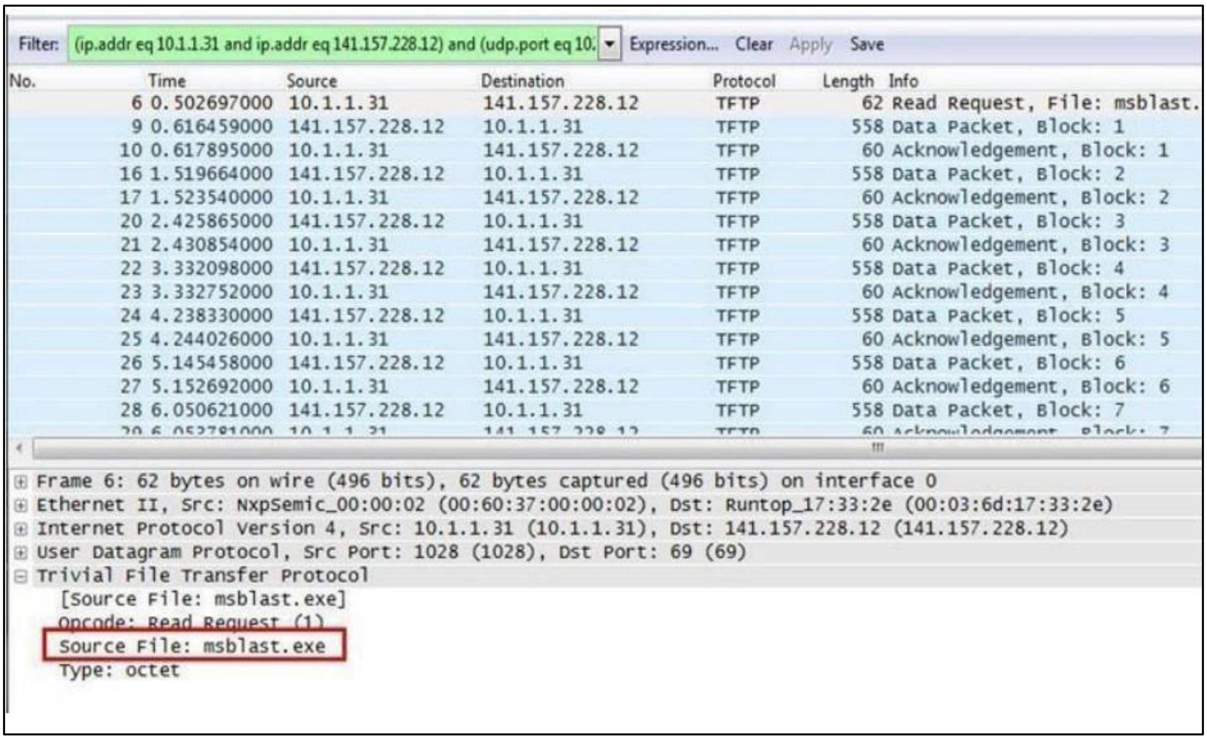
Answer: 10.1.1.31



```
(ip.addr eq 10.1.1.31 and ip.addr eq 141.157.228.12) and (udp.port eq 10.
      Time         Source          Destination     Protocol  Length Info
    6 0.502697000 10.1.1.31       141.157.228.12  TFTP        62 Read Request, File: msblast.exe, Transfer type: octet
    9 0.616459000 141.157.228.12  10.1.1.31       TFTP       558 Data Packet, Block: 1
   10 0.617895000 10.1.1.31       141.157.228.12  TFTP        60 Acknowledgement, Block: 1
   16 1.519664000 141.157.228.12  10.1.1.31       TFTP       558 Data Packet, Block: 2
   17 1.523540000 10.1.1.31       141.157.228.12  TFTP        60 Acknowledgement, Block: 2
   20 2.425865000 141.157.228.12  10.1.1.31       TFTP       558 Data Packet, Block: 3
   21 2.430854000 10.1.1.31       141.157.228.12  TFTP        60 Acknowledgement, Block: 3
   22 3.332098000 141.157.228.12  10.1.1.31       TFTP       558 Data Packet, Block: 4
   23 3.332752000 10.1.1.31       141.157.228.12  TFTP        60 Acknowledgement, Block: 4
   24 4.238330000 141.157.228.12  10.1.1.31       TFTP       558 Data Packet, Block: 5
   25 4.244026000 10.1.1.31       141.157.228.12  TFTP        60 Acknowledgement, Block: 5
   26 5.145458000 141.157.228.12  10.1.1.31       TFTP       558 Data Packet, Block: 6
```

What is the name of the file that is being transferred?

Answer: mblast.exe



Filter: (ip.addr eq 10.1.1.31 and ip.addr eq 141.157.228.12) and (udp.port eq 10.

```
No.     Time          Source          Destination     Protocol  Length Info
      6 0.502697000   10.1.1.31       141.157.228.12  TFTP          62 Read Request, File: msblast.
      9 0.616459000   141.157.228.12  10.1.1.31       TFTP         558 Data Packet, Block: 1
     10 0.617895000   10.1.1.31       141.157.228.12  TFTP          60 Acknowledgement, Block: 1
     16 1.519664000   141.157.228.12  10.1.1.31       TFTP         558 Data Packet, Block: 2
     17 1.523540000   10.1.1.31       141.157.228.12  TFTP          60 Acknowledgement, Block: 2
     20 2.425865000   141.157.228.12  10.1.1.31       TFTP         558 Data Packet, Block: 3
     21 2.430854000   10.1.1.31       141.157.228.12  TFTP          60 Acknowledgement, Block: 3
     22 3.332098000   141.157.228.12  10.1.1.31       TFTP         558 Data Packet, Block: 4
     23 3.332752000   10.1.1.31       141.157.228.12  TFTP          60 Acknowledgement, Block: 4
     24 4.238330000   141.157.228.12  10.1.1.31       TFTP         558 Data Packet, Block: 5
     25 4.244026000   10.1.1.31       141.157.228.12  TFTP          60 Acknowledgement, Block: 5
     26 5.145458000   141.157.228.12  10.1.1.31       TFTP         558 Data Packet, Block: 6
     27 5.152692000   10.1.1.31       141.157.228.12  TFTP          60 Acknowledgement, Block: 6
     28 6.050621000   141.157.228.12  10.1.1.31       TFTP         558 Data Packet, Block: 7
     29 6.053781000   10.1.1.31       141.157.228.12  TFTP          60 Acknowledgement, Block: 7
```

```
⊞ Frame 6: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
⊞ Ethernet II, Src: NxpSemic_00:00:02 (00:60:37:00:00:02), Dst: Runtop_17:33:2e (00:03:6d:17:33:2e)
⊞ Internet Protocol Version 4, Src: 10.1.1.31 (10.1.1.31), Dst: 141.157.228.12 (141.157.228.12)
⊞ User Datagram Protocol, Src Port: 1028 (1028), Dst Port: 69 (69)
⊟ Trivial File Transfer Protocol
    [Source File: msblast.exe]
    Opcode: Read Request (1)
    Source File: msblast.exe
    Type: octet
```

DNS TROUBLE TRACE FILE: challengednstrouble.pcapng

BACKGROUND: After a maintenance window on the day before, when several servers had been upgraded to a newer operating system, a lot of trouble tickets have come in.

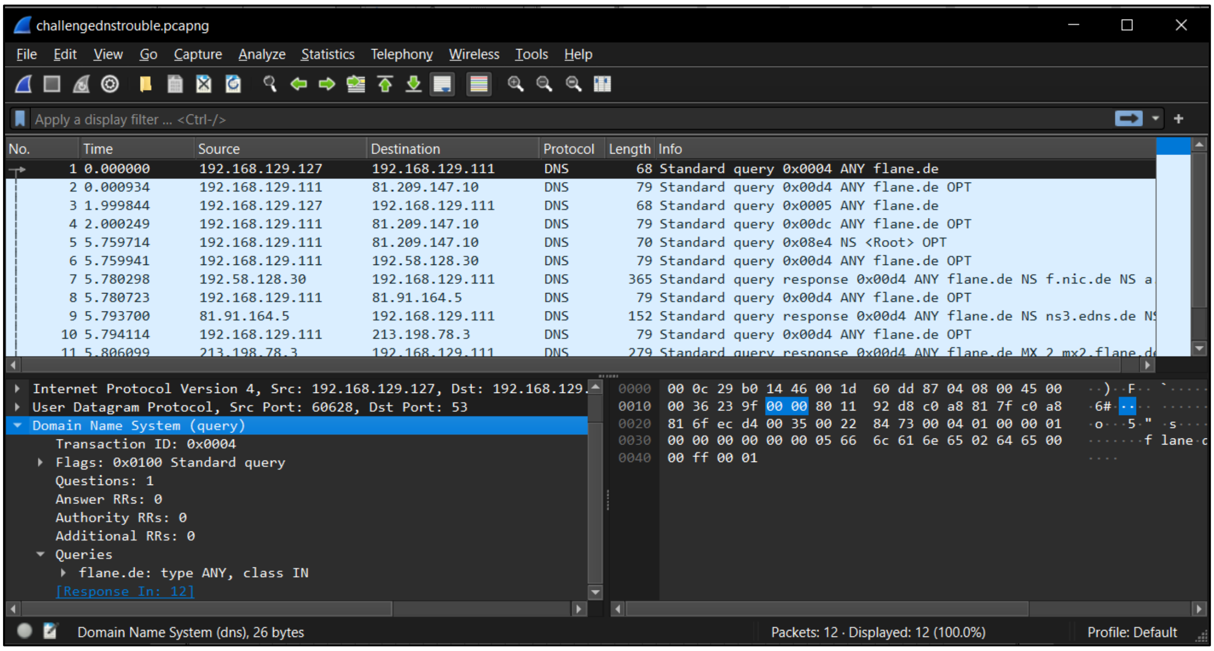
Users complain that connecting to web sites and other services takes a long time now, especially when connecting for the first time. A quick check on all relevant switches, routers and servers reveals no bottlenecks in CPU, memory or disk I/O, so of course the tickets are handed over to the network guys – it must be the network, right? Finally, one of the network engineers comes to you and asks you to help him with analyzing a trace he took. He suspects that there is something wrong with the DNS name resolution, but

even after filtering away most of the other stuff he can't put his finger on it. Can you take a look at his trace to find out what happened and if this is a network problem at all?

QUESTIONS:

What FQDN is the client attempting to resolve?

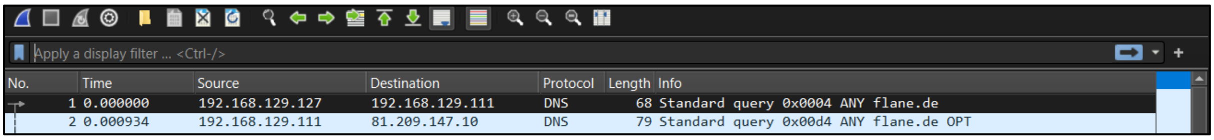
Answer: flane.de


challengednstrouble.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source           Destination      Protocol Length Info
   1 0.000000   192.168.129.127  192.168.129.111  DNS       68 Standard query 0x0004 ANY flane.de
   2 0.000934   192.168.129.111  81.209.147.10    DNS       79 Standard query 0x00d4 ANY flane.de OPT
   3 1.999844   192.168.129.127  192.168.129.111  DNS       68 Standard query 0x0005 ANY flane.de
   4 2.000249   192.168.129.111  81.209.147.10    DNS       79 Standard query 0x00dc ANY flane.de OPT
   5 5.759714   192.168.129.111  81.209.147.10    DNS       70 Standard query 0x08e4 NS <Root> OPT
   6 5.759941   192.168.129.111  192.58.128.30    DNS       79 Standard query 0x00d4 ANY flane.de OPT
   7 5.780298   192.58.128.30    192.168.129.111  DNS      365 Standard query response 0x00d4 ANY flane.de NS f.nic.de NS a
   8 5.780723   192.168.129.111  81.91.164.5      DNS       79 Standard query 0x00d4 ANY flane.de OPT
   9 5.793700   81.91.164.5      192.168.129.111  DNS      152 Standard query response 0x00d4 ANY flane.de NS ns3.edns.de NS
  10 5.794114   192.168.129.111  213.198.78.3     DNS       79 Standard query 0x00d4 ANY flane.de OPT
  11 5.806099   213.198.78.3     192.168.129.111  DNS      279 Standard query response 0x00d4 ANY flane.de MX 2 mx2.flane.de

Internet Protocol Version 4, Src: 192.168.129.127, Dst: 192.168.129.
User Datagram Protocol, Src Port: 60628, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x0004
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        flane.de: type ANY, class IN
    [Response In: 12]

0000  00 0c 29 b0 14 46 00 1d  60 dd 87 04 08 00 45 00   ··)··F·· `·····E·
0010  00 36 23 9f 00 00 80 11  92 d8 c0 a8 81 7f c0 a8   ·6#·············
0020  81 6f ec d4 00 35 00 22  84 73 00 04 01 00 00 01   ·o···5·" ·s······
0030  00 00 00 00 00 00 05 66  6c 61 6e 65 02 64 65 00   ·······f lane·de·
0040  00 ff 00 01                                        ····

Domain Name System (dns), 26 bytes        Packets: 12 · Displayed: 12 (100.0%)        Profile: Default
```

To what IP address is the first recursive DNS query sent?

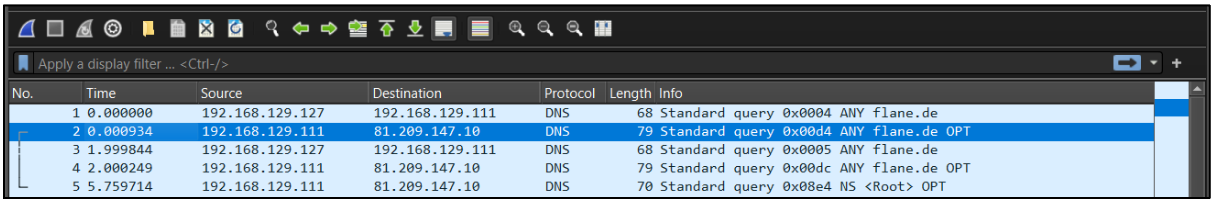
Ans: 192.168.129.111.



```
No.  Time       Source           Destination      Protocol Length Info
   1 0.000000   192.168.129.127  192.168.129.111  DNS       68 Standard query 0x0004 ANY flane.de
   2 0.000934   192.168.129.111  81.209.147.10    DNS       79 Standard query 0x00d4 ANY flane.de OPT
```

To what IP address is the second recursive DNS query sent?

Answer: 81.209.147.10



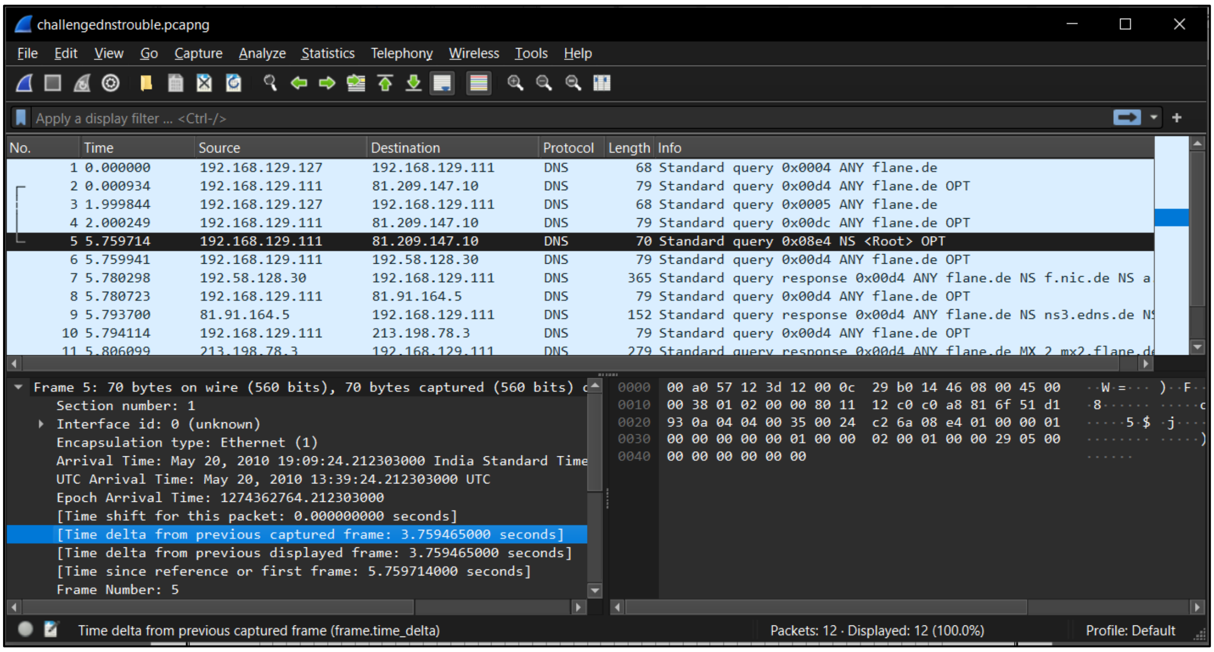
```
No.   Time       Source           Destination      Protocol Length Info
    1 0.000000   192.168.129.127  192.168.129.111  DNS        68 Standard query 0x0004 ANY flane.de
    2 0.000934   192.168.129.111  81.209.147.10    DNS        79 Standard query 0x00d4 ANY flane.de OPT
    3 1.999844   192.168.129.127  192.168.129.111  DNS        68 Standard query 0x0005 ANY flane.de
    4 2.000249   192.168.129.111  81.209.147.10    DNS        79 Standard query 0x00dc ANY flane.de OPT
    5 5.759714   192.168.129.111  81.209.147.10    DNS        70 Standard query 0x08e4 NS <Root> OPT
```

The trace file includes authoritative DNS servers responsible for whattop level country code domain?

Answer: .de is the country code top-level domain (ccTLD) for Federal Republic of Germany

What is the IP address of the host that is responsible for the longdelay in resolving the host name?

Answer: 81.209.147.10


challengednstrouble.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source           Destination      Protocol Length Info
    1 0.000000   192.168.129.127  192.168.129.111  DNS        68 Standard query 0x0004 ANY flane.de
    2 0.000934   192.168.129.111  81.209.147.10    DNS        79 Standard query 0x00d4 ANY flane.de OPT
    3 1.999844   192.168.129.127  192.168.129.111  DNS        68 Standard query 0x0005 ANY flane.de
    4 2.000249   192.168.129.111  81.209.147.10    DNS        79 Standard query 0x00dc ANY flane.de OPT
    5 5.759714   192.168.129.111  81.209.147.10    DNS        70 Standard query 0x08e4 NS <Root> OPT
    6 5.759941   192.168.129.111  192.58.128.30    DNS        79 Standard query 0x00d4 ANY flane.de OPT
    7 5.780298   192.58.128.30    192.168.129.111  DNS       365 Standard query response 0x00d4 ANY flane.de NS f.nic.de NS a
    8 5.780723   192.168.129.111  81.91.164.5      DNS        79 Standard query 0x00d4 ANY flane.de OPT
    9 5.793700   81.91.164.5      192.168.129.111  DNS       152 Standard query response 0x00d4 ANY flane.de NS ns3.edns.de N
   10 5.794114   192.168.129.111  213.198.78.3     DNS        79 Standard query 0x00d4 ANY flane.de OPT
   11 5.806099   213.198.78.3     192.168.129.111  DNS       279 Standard query response 0x00d4 ANY flane.de MX 2 mx2.flane.d
```

```
Frame 5: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) c
    Section number: 1
  Interface id: 0 (unknown)
    Encapsulation type: Ethernet (1)
    Arrival Time: May 20, 2010 19:09:24.212303000 India Standard Time
    UTC Arrival Time: May 20, 2010 13:39:24.212303000 UTC
    Epoch Arrival Time: 1274362764.212303000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 3.759465000 seconds]
    [Time delta from previous displayed frame: 3.759465000 seconds]
    [Time since reference or first frame: 5.759714000 seconds]
    Frame Number: 5
```

```
0000  00 a0 57 12 3d 12 00 0c  29 b0 14 46 08 00 45 00   ··W·=··· )··F··
0010  00 38 01 02 00 00 80 11  12 c0 c0 a8 81 6f 51 d1   ·8······ ·····c
0020  93 0a 04 04 00 35 00 24  c2 6a 08 e4 01 00 00 01   ·····5·$ ·j····
0030  00 00 00 00 00 01 00 00  02 00 01 00 00 29 05 00   ········ ·····)
0040  00 00 00 00 00 00                                  ······
```

Time delta from previous captured frame (frame.time_delta)

Packets: 12 · Displayed: 12 (100.0%)

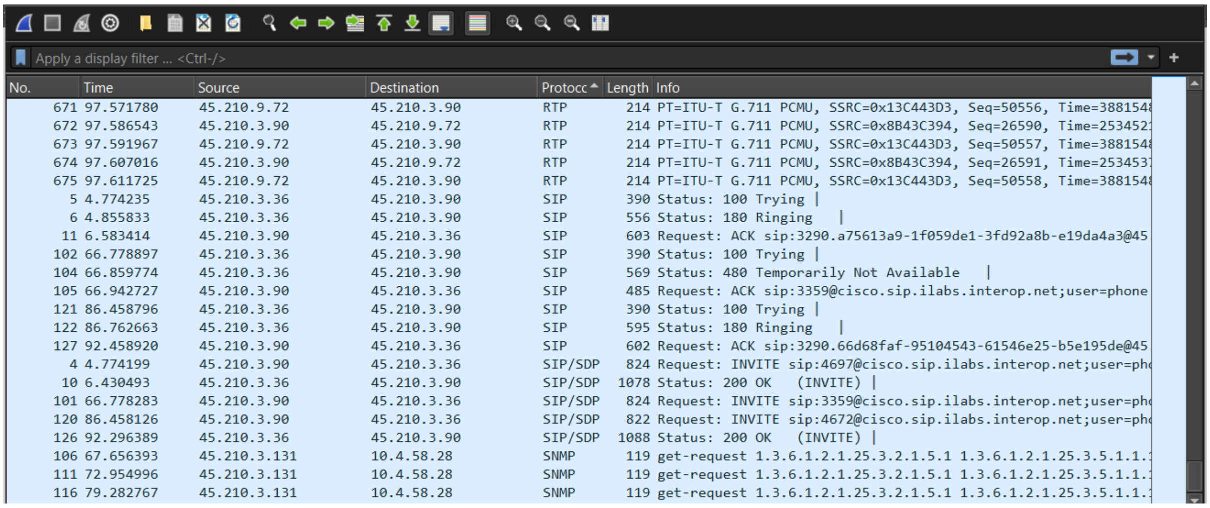
Profile: Default

VOIP RECONSTRUCTION TRACE FILES: challengevoip.pcapng BACKGROUND: This captured file was collected from a recently installed VoIP network that is experiencing performance issues, and you have been asked to evaluate it and recommend corrective action.

QUESTIONS:

What three UDP-based protocols are used for the VoIP call and call setup?

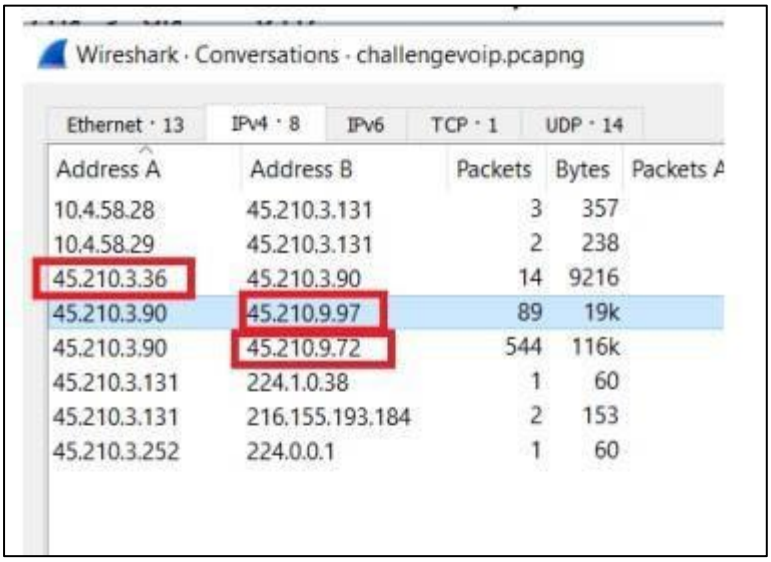
Answer: SIP, SDP, RTP, SNMP



```
No.   Time       Source        Destination   Protocc Length Info
  671 97.571780  45.210.9.72   45.210.3.90   RTP      214 PT=ITU-T G.711 PCMU, SSRC=0x13C443D3, Seq=50556, Time=388154
  672 97.586543  45.210.3.90   45.210.9.72   RTP      214 PT=ITU-T G.711 PCMU, SSRC=0x8B43C394, Seq=26590, Time=253452
  673 97.591967  45.210.9.72   45.210.3.90   RTP      214 PT=ITU-T G.711 PCMU, SSRC=0x13C443D3, Seq=50557, Time=388154
  674 97.607016  45.210.3.90   45.210.9.72   RTP      214 PT=ITU-T G.711 PCMU, SSRC=0x8B43C394, Seq=26591, Time=253453
  675 97.611725  45.210.9.72   45.210.3.90   RTP      214 PT=ITU-T G.711 PCMU, SSRC=0x13C443D3, Seq=50558, Time=388154
    5 4.774235   45.210.3.36   45.210.3.90   SIP      390 Status: 100 Trying |
    6 4.855833   45.210.3.36   45.210.3.90   SIP      556 Status: 180 Ringing   |
   11 6.583414   45.210.3.90   45.210.3.36   SIP      603 Request: ACK sip:3290.a75613a9-1f059de1-3fd92a8b-e19da4a3@45
  102 66.778897  45.210.3.36   45.210.3.90   SIP      390 Status: 100 Trying |
  104 66.859774  45.210.3.36   45.210.3.90   SIP      569 Status: 480 Temporarily Not Available   |
  105 66.942727  45.210.3.90   45.210.3.36   SIP      485 Request: ACK sip:3359@cisco.sip.ilabs.interop.net;user=phone
  121 86.458796  45.210.3.36   45.210.3.90   SIP      390 Status: 100 Trying |
  122 86.762663  45.210.3.36   45.210.3.90   SIP      595 Status: 180 Ringing   |
  127 92.458920  45.210.3.90   45.210.3.36   SIP      602 Request: ACK sip:3290.66d68faf-95104543-61546e25-b5e195de@45
    4 4.774199   45.210.3.90   45.210.3.36   SIP/SDP  824 Request: INVITE sip:4697@cisco.sip.ilabs.interop.net;user=ph
   10 6.430493   45.210.3.36   45.210.3.90   SIP/SDP 1078 Status: 200 OK   (INVITE) |
  101 66.778283  45.210.3.90   45.210.3.36   SIP/SDP  824 Request: INVITE sip:3359@cisco.sip.ilabs.interop.net;user=ph
  120 86.458126  45.210.3.90   45.210.3.36   SIP/SDP  822 Request: INVITE sip:4672@cisco.sip.ilabs.interop.net;user=ph
  126 92.296389  45.210.3.36   45.210.3.90   SIP/SDP 1088 Status: 200 OK   (INVITE) |
  106 67.656393  45.210.3.131  10.4.58.28    SNMP     119 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.
  111 72.954996  45.210.3.131  10.4.58.28    SNMP     119 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.
  116 79.282767  45.210.3.131  10.4.58.28    SNMP     119 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.
```

With what three IP addresses is 45.210.3.90 communicating?

Answer: 45.210.3.36, 45.210.3.97, 45.210.3.72

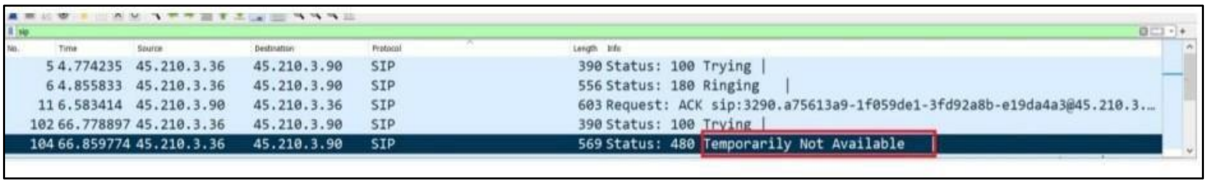


Wireshark · Conversations · challengevoip.pcapng

Address A	Address B	Packets	Bytes	Packets A
10.4.58.28	45.210.3.131	3	357	
10.4.58.29	45.210.3.131	2	238	
45.210.3.36	45.210.3.90	14	9216	
45.210.3.90	45.210.9.97	89	19k	
45.210.3.90	45.210.9.72	544	116k	
45.210.3.131	224.1.0.38	1	60	
45.210.3.131	216.155.193.184	2	153	
45.210.3.252	224.0.0.1	1	60	

What SIP error code is seen in this trace file?

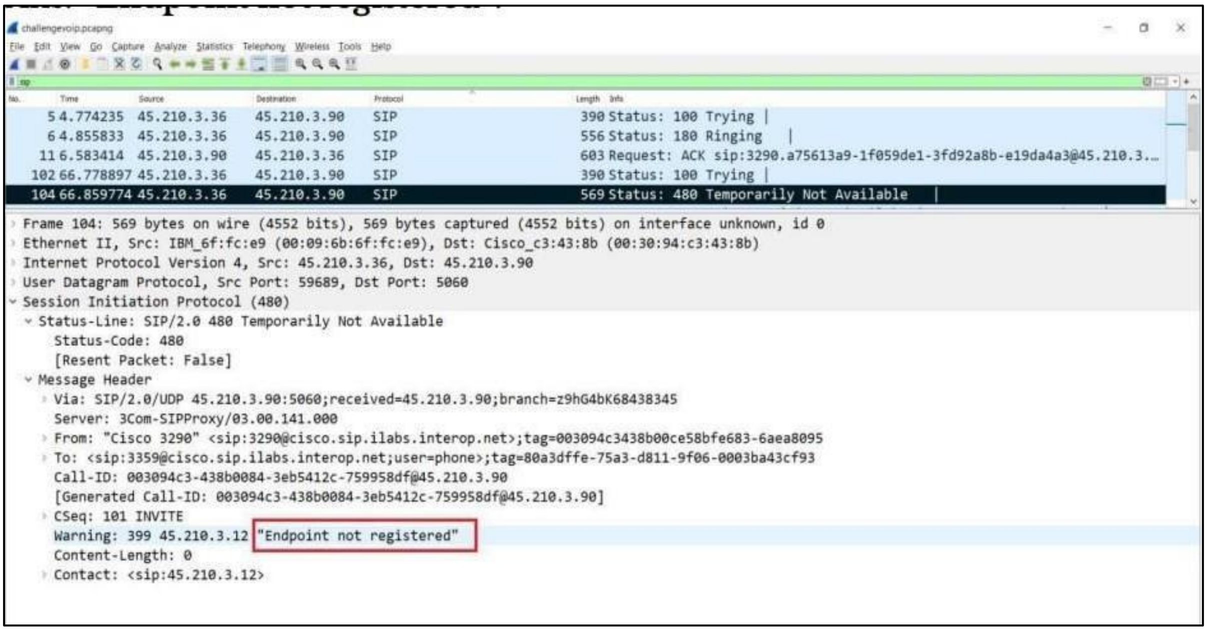
Answer: Error code 480



```
No.   Time       Source       Destination  Protocol  Length Info
    5 4.774235   45.210.3.36  45.210.3.90  SIP       390 Status: 100 Trying |
    6 4.855833   45.210.3.36  45.210.3.90  SIP       556 Status: 180 Ringing   |
   11 6.583414   45.210.3.90  45.210.3.36  SIP       603 Request: ACK sip:3290.a75613a9-1f059de1-3fd92a8b-e19da4a3@45.210.3...
  102 66.778897  45.210.3.36  45.210.3.90  SIP       390 Status: 100 Trying |
  104 66.859774  45.210.3.36  45.210.3.90  SIP       569 Status: 480 Temporarily Not Available   |
```

What is the stated cause of this SIP error?

Ans: “Endpoint not registered”.


challengevoip.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
sip
No. Time Source Destination Protocol Length Info

```
    5 4.774235  45.210.3.36   45.210.3.90   SIP    390 Status: 100 Trying |
    6 4.855833  45.210.3.36   45.210.3.90   SIP    556 Status: 180 Ringing   |
   11 6.583414  45.210.3.90   45.210.3.36   SIP    603 Request: ACK sip:3290.a75613a9-1f059de1-3fd92a8b-e19da4a3@45.210.3...
  102 66.778897 45.210.3.36   45.210.3.90   SIP    390 Status: 100 Trying |
  104 66.859774 45.210.3.36   45.210.3.90   SIP    569 Status: 480 Temporarily Not Available   |

> Frame 104: 569 bytes on wire (4552 bits), 569 bytes captured (4552 bits) on interface unknown, id 0
> Ethernet II, Src: IBM_6f:fc:e9 (00:09:6b:6f:fc:e9), Dst: Cisco_c3:43:8b (00:30:94:c3:43:8b)
> Internet Protocol Version 4, Src: 45.210.3.36, Dst: 45.210.3.90
> User Datagram Protocol, Src Port: 59689, Dst Port: 5060
v Session Initiation Protocol (480)
  v Status-Line: SIP/2.0 480 Temporarily Not Available
      Status-Code: 480
      [Resent Packet: False]
  v Message Header
    > Via: SIP/2.0/UDP 45.210.3.90:5060;received=45.210.3.90;branch=z9hG4bK68438345
      Server: 3Com-SIPProxy/03.00.141.000
    > From: "Cisco 3290" <sip:3290@cisco.sip.ilabs.interop.net>;tag=003094c3438b00ce58bfe683-6aea8095
    > To: <sip:3359@cisco.sip.ilabs.interop.net;user=phone>;tag=80a3dffe-75a3-d811-9f06-0003ba43cf93
      Call-ID: 003094c3-438b0084-3eb5412c-759958df@45.210.3.90
      [Generated Call-ID: 003094c3-438b0084-3eb5412c-759958df@45.210.3.90]
    > CSeq: 101 INVITE
      Warning: 399 45.210.3.12 "Endpoint not registered"
      Content-Length: 0
    > Contact: <sip:45.210.3.12>
```

BOY SCOUT TRACE FILES: challengeboyscout.pcapng

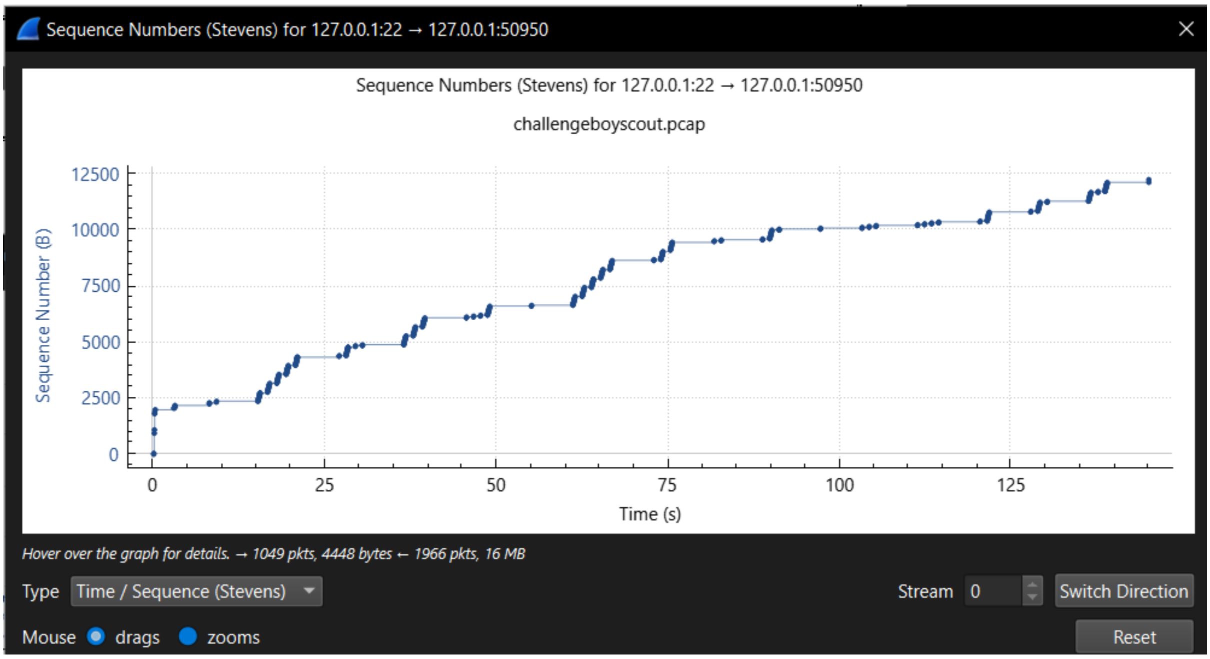
BACKGROUND: Information leaks from all sorts of place

QUESTIONS:

1. What is the secret message?

Answer: eei0love0wiresharke

Analysis:Select Statistics > TCP StreamGraph > TCP Sequence Graph (Stevens).

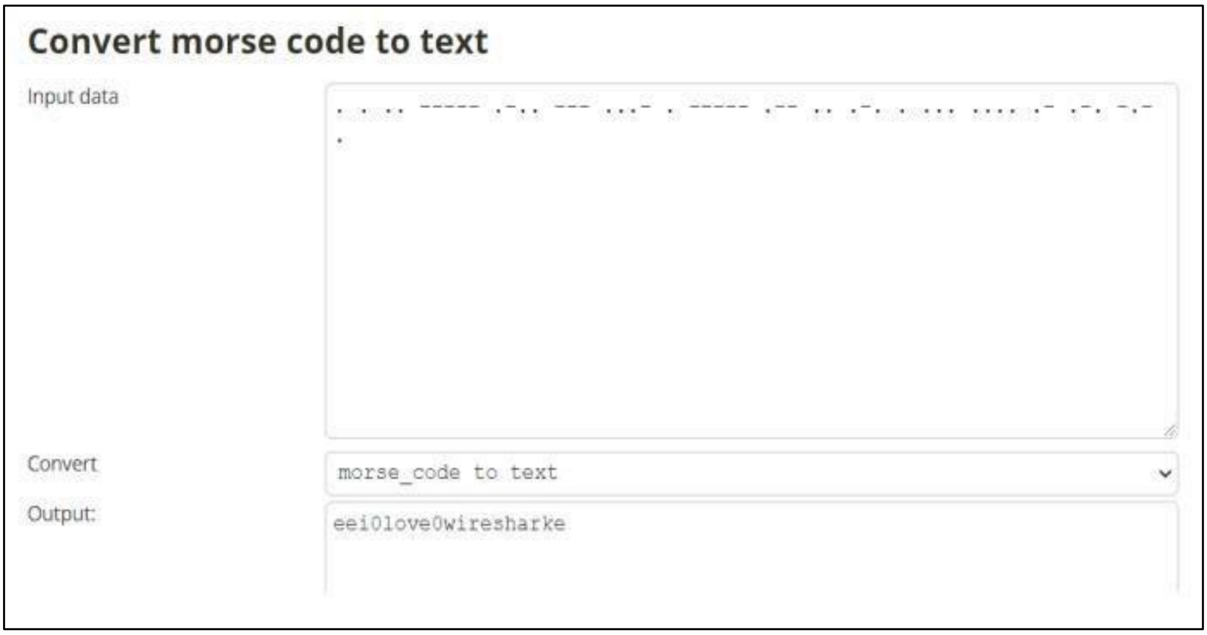

Sequence Numbers (Stevens) for 127.0.0.1:22 → 127.0.0.1:50950
Sequence Numbers (Stevens) for 127.0.0.1:22 → 127.0.0.1:50950
challengeboyscout.pcap
Sequence Number (B)
12500
10000
7500
5000
2500
0
0
25
50
75
100
125
Time (s)
Mouse
drags
zooms
Switch Direction
Reset

Hover over the graph for details. → 1049 pkts, 4448 bytes ← 1966 pkts, 16 MB

Type Time / Sequence (Stevens)

Stream 0

For decoding the Morse code, we used an online Morse code decoder.



Convert morse code to text

Input data

```
. . .. ----- .-.. --- ...- . ----- .-- .. .-. . ... .... .- .-. -.-
.
```

Convert: morse_code to text

Output:

```
eei0love0wiresharke
```

Conclusion:

Thus, from this experiment we used Wireshark to analyze the protocol used and frames of each protocol, applied filters to find out the information being send, downloaded files
that are sent as HTTP Objects to check its content, decoded secret messages and other challenges