Alisha Kamat (201071010)
Kunal Agarwal (201070074)
Sanskruti Mahajan (201071012)

LAB ASSIGNMENT 6

AIM:

To perform protocol analysis using wireshark.

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.
6. 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.

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.

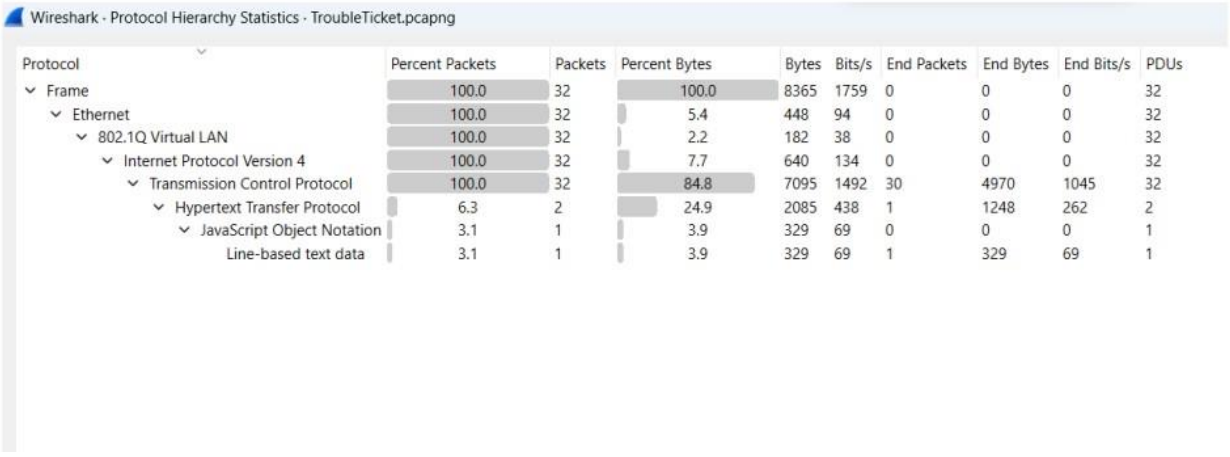
Features of Wireshark

- 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

Trouble Ticket Trace File: TroubleTicket.pcapng

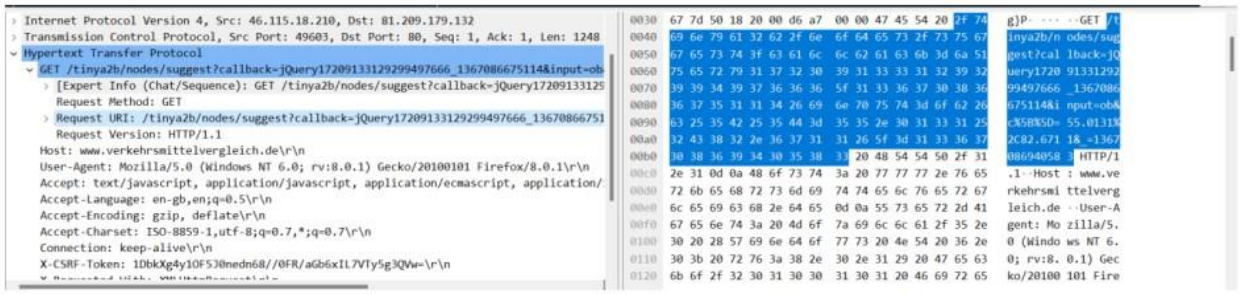
1. What is the application protocol used? Answer: HTTP


Wireshark · Protocol Hierarchy Statistics · TroubleTicket.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	32	100.0	8365	1759	0	0	0	32
Ethernet	100.0	32	5.4	448	94	0	0	0	32
802.1Q Virtual LAN	100.0	32	2.2	182	38	0	0	0	32
Internet Protocol Version 4	100.0	32	7.7	640	134	0	0	0	32
Transmission Control Protocol	100.0	32	84.8	7095	1492	30	4970	1045	32
Hypertext Transfer Protocol	6.3	2	24.9	2085	438	1	1248	262	2
JavaScript Object Notation	3.1	1	3.9	329	69	0	0	0	1
Line-based text data	3.1	1	3.9	329	69	1	329	69	1

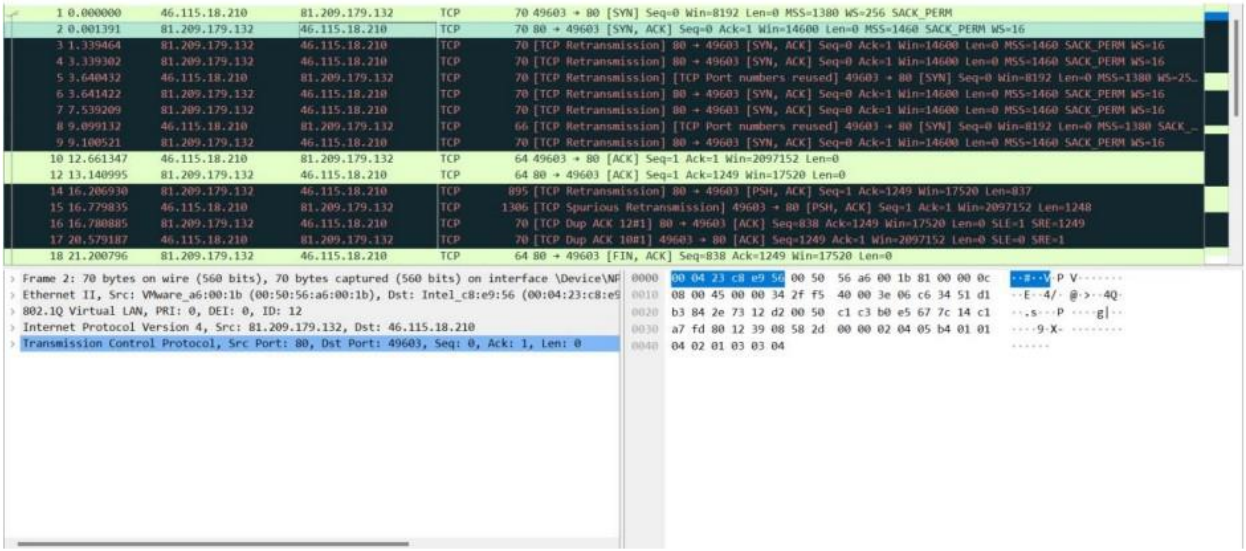
2. Are all GET requests asking for the same URI?

Answer: Yes, as we can see all the GET requests have the same URI ie sr. no. 11, 15, 21 Packets.



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

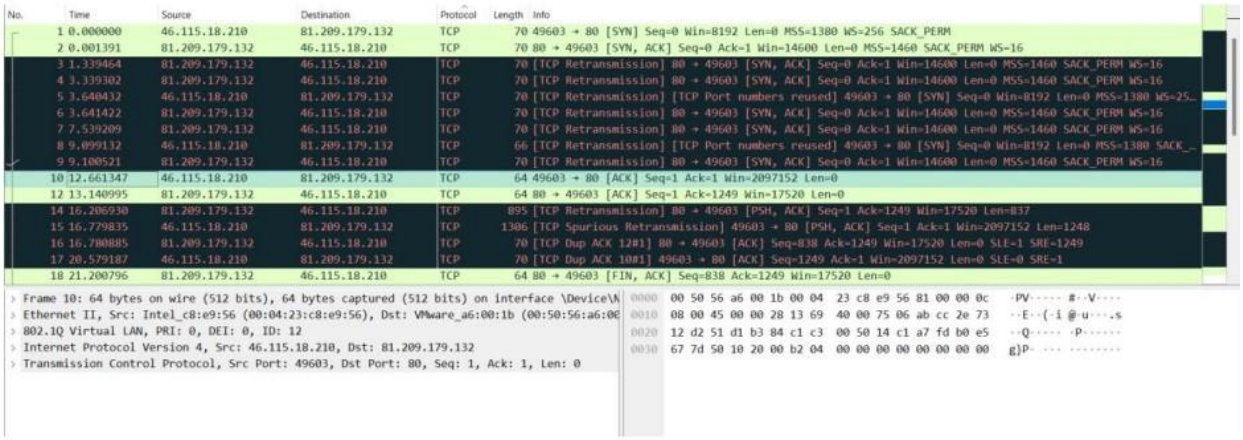
Answer: Connection is lost near the client as it is not responding to SYN, ACK sent by server



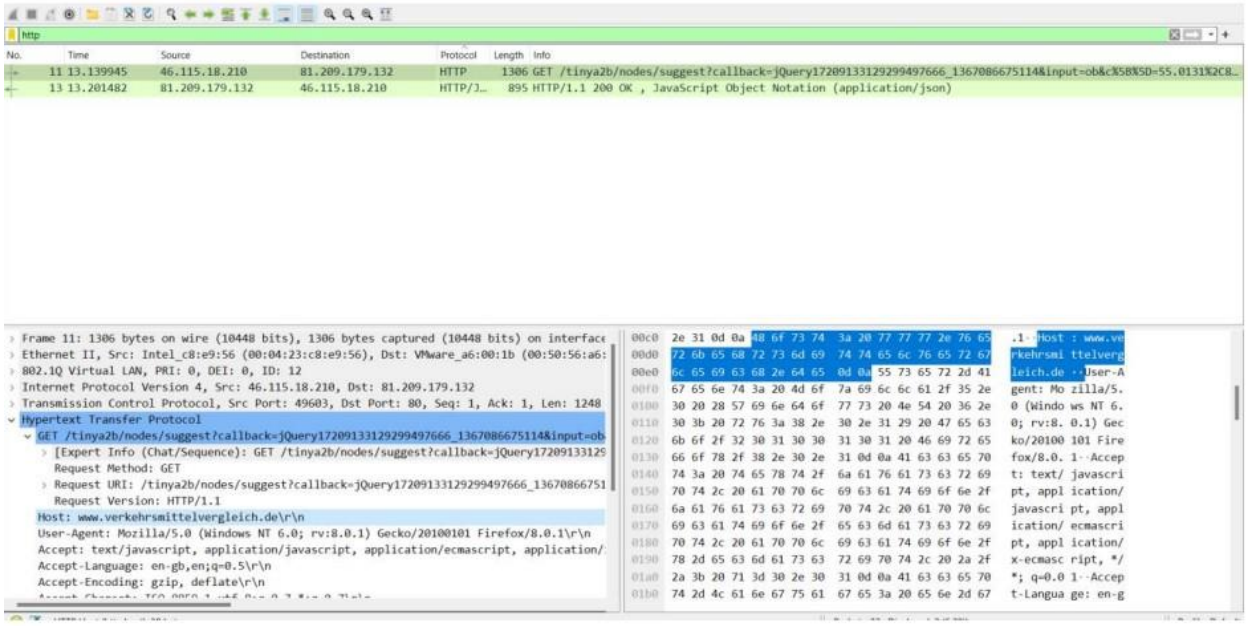
4. This trace was taken inside the infrastructure. What is the Initial Round Trip Time of the connection?

Answer: RTT refers to the time taken by a network request to reach a destination and to revert back to the original source. In case of wireshark, we can assume the time taken for a 3-way handshake is the same as RTT.

We have set the reference time as packet 8 relative time for packet 10 is 3.562215



5. Who owns the server?
   Answer: 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 www.verkehrsmittelvergleich.de



DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup

Home > Whois Lookup > VerkehrsmittelVergleich.de

Whois Record for Verkehrsmit...ergleich.de

Domain Profile

Registrar Status	connect
Dates	Updated on 2021-03-04
Name Servers	NS1.DOMAINDISCOUNT24.NET (has 279,498 domains) NS2.DOMAINDISCOUNT24.NET (has 279,498 domains) NS3.DOMAINDISCOUNT24.NET (has 279,498 domains)
Tech Contact	—
Hosting History	2 changes on 3 unique name servers over 6 years

Website

Website Title	None given.

Whois Record (last updated on 2022-10-14)

```
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
```

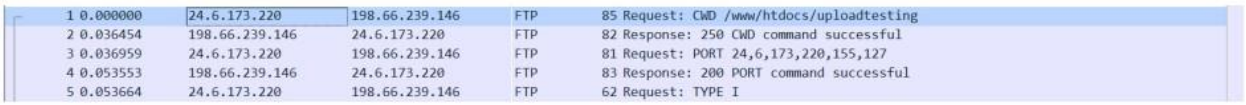
```
root@LAPTOP-K61BR036:/mnt/c/users/aryan# whois verkehrsmittelvergleich.de
% Restricted rights.
%
% Terms and Conditions of Use
%
% The above data may only be used within the scope of technical or
% administrative necessities of Internet operation or to remedy legal
% problems.
% The use for other purposes, in particular for advertising, is not permitted.
%
% The DENIC whois service on port 43 doesn't disclose any information concerning
% the domain holder, general request and abuse contact.
% This information can be obtained through use of our web-based whois service
% available at the DENIC website:
% http://www.denic.de/en/domains/whois-service/web-whois.html
%
%

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
root@LAPTOP-K61BR036:/mnt/c/users/aryan#
```

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.

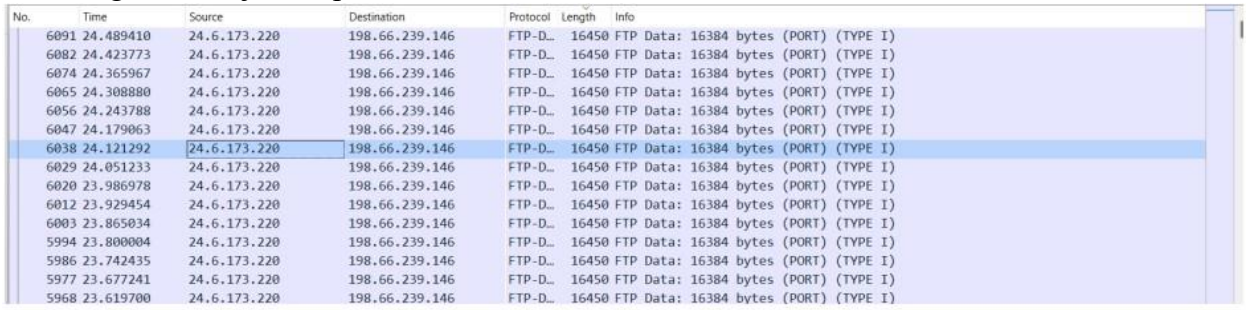


1	0.000000	24.6.173.220	198.66.239.146	FTP	85 Request: CWD /www/htdocs/uploadtesting
2	0.036454	198.66.239.146	24.6.173.220	FTP	82 Response: 250 CWD command successful
3	0.036959	24.6.173.220	198.66.239.146	FTP	81 Request: PORT 24,6,173,220,155,127
4	0.053553	198.66.239.146	24.6.173.220	FTP	83 Response: 200 PORT command successful
5	0.053664	24.6.173.220	198.66.239.146	FTP	62 Request: TYPE I

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

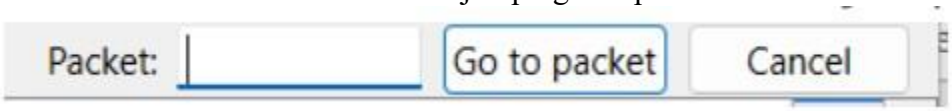
(NIC) driver and the driver passes the 16450 bytes down to the NIC card, and it actually creates the TCP segments and sends them out on the network. Only for this process we are seeing here the jumbo packets in the trace file



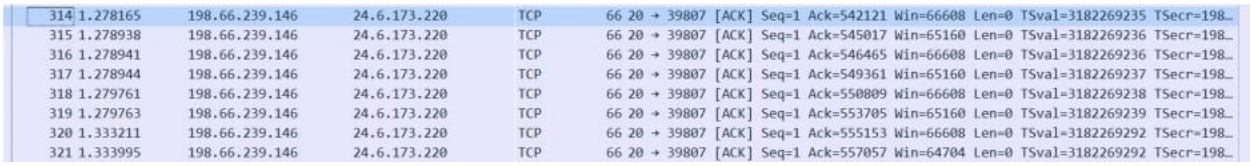
No.	Time	Source	Destination	Protocol	Length	Info
6091	24.489410	24.6.173.220	198.66.239.146	FTP-D…	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6082	24.423773	24.6.173.220	198.66.239.146	FTP-D…	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6074	24.365967	24.6.173.220	198.66.239.146	FTP-D…	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6065	24.308880	24.6.173.220	198.66.239.146	FTP-D…	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6056	24.243788	24.6.173.220	198.66.239.146	FTP-D…	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6047	24.179063	24.6.173.220	198.66.239.146	FTP-D…	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6038	24.121292	24.6.173.220	198.66.239.146	FTP-D…	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6029	24.051233	24.6.173.220	198.66.239.146	FTP-D…	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6020	23.986978	24.6.173.220	198.66.239.146	FTP-D…	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6012	23.929454	24.6.173.220	198.66.239.146	FTP-D…	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
6003	23.865034	24.6.173.220	198.66.239.146	FTP-D…	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
5994	23.800004	24.6.173.220	198.66.239.146	FTP-D…	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
5986	23.742435	24.6.173.220	198.66.239.146	FTP-D…	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
5977	23.677241	24.6.173.220	198.66.239.146	FTP-D…	16450	FTP Data: 16384 bytes (PORT) (TYPE I)
5968	23.619700	24.6.173.220	198.66.239.146	FTP-D…	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
Select Go and then Go to Packet for jumping into packet number 314.

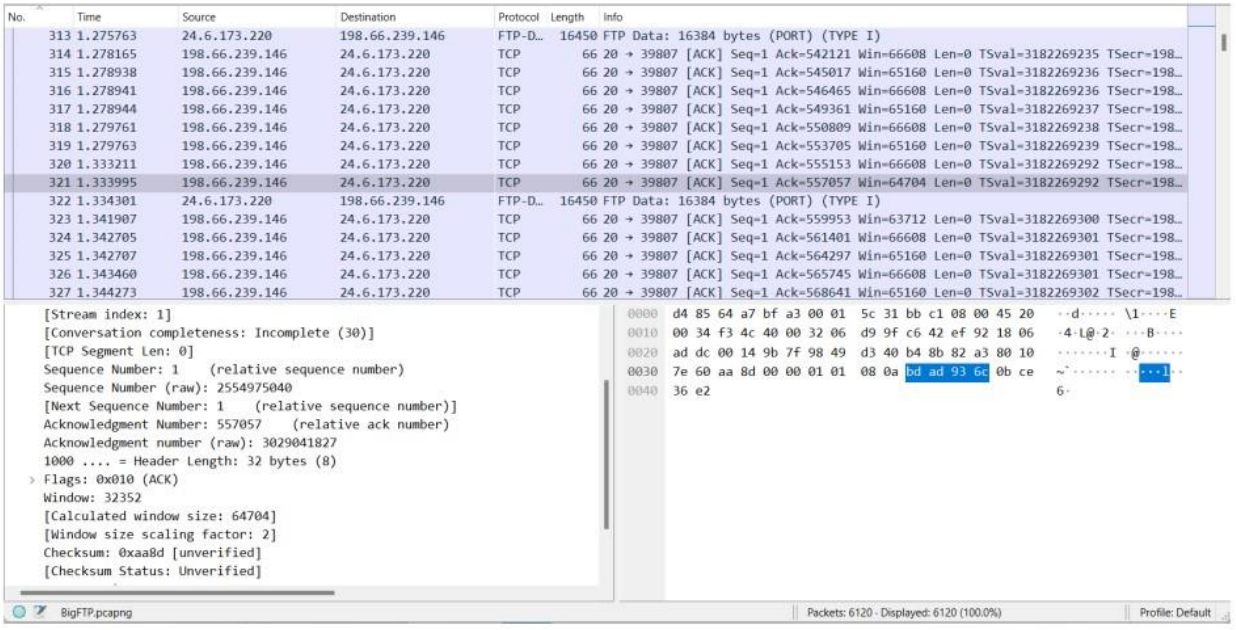


Given the packet number as can be seen below, we gave 314. Now we can see all packets between 314-321.

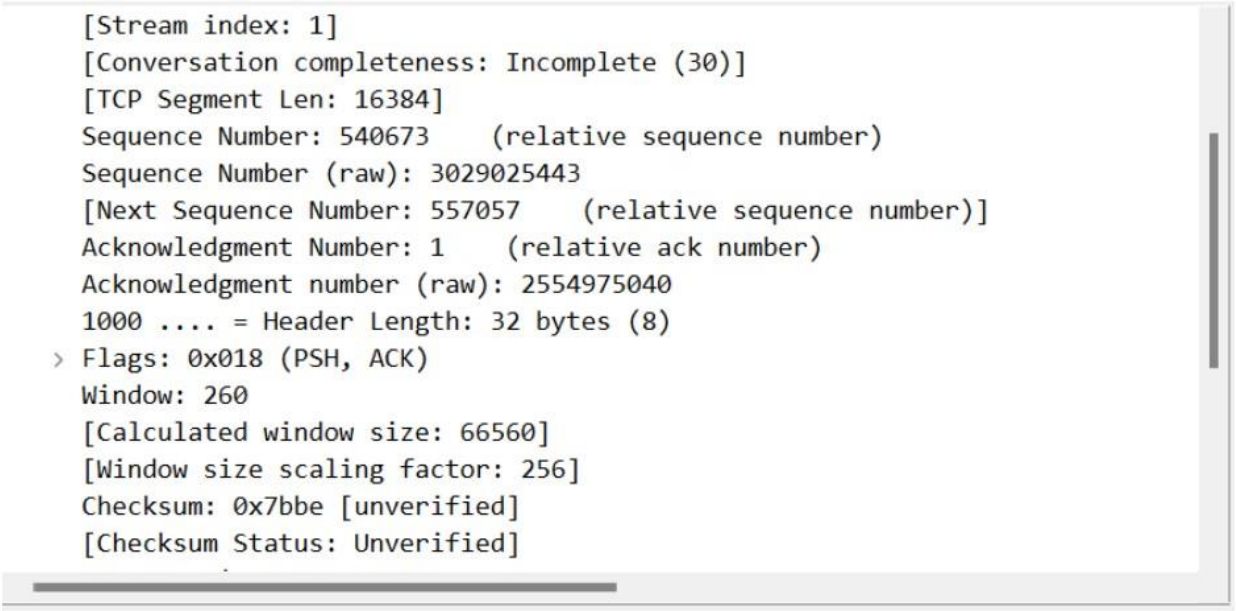


314	1.278165	198.66.239.146	24.6.173.220	TCP	66 20 → 39807 [ACK] Seq=1 Ack=542121 Win=66608 Len=0 TSval=3182269235 TSecr=198…
315	1.278938	198.66.239.146	24.6.173.220	TCP	66 20 → 39807 [ACK] Seq=1 Ack=545017 Win=65160 Len=0 TSval=3182269236 TSecr=198…
316	1.278941	198.66.239.146	24.6.173.220	TCP	66 20 → 39807 [ACK] Seq=1 Ack=546465 Win=66608 Len=0 TSval=3182269236 TSecr=198…
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=198…
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=198…
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=198…
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=198…
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=198…

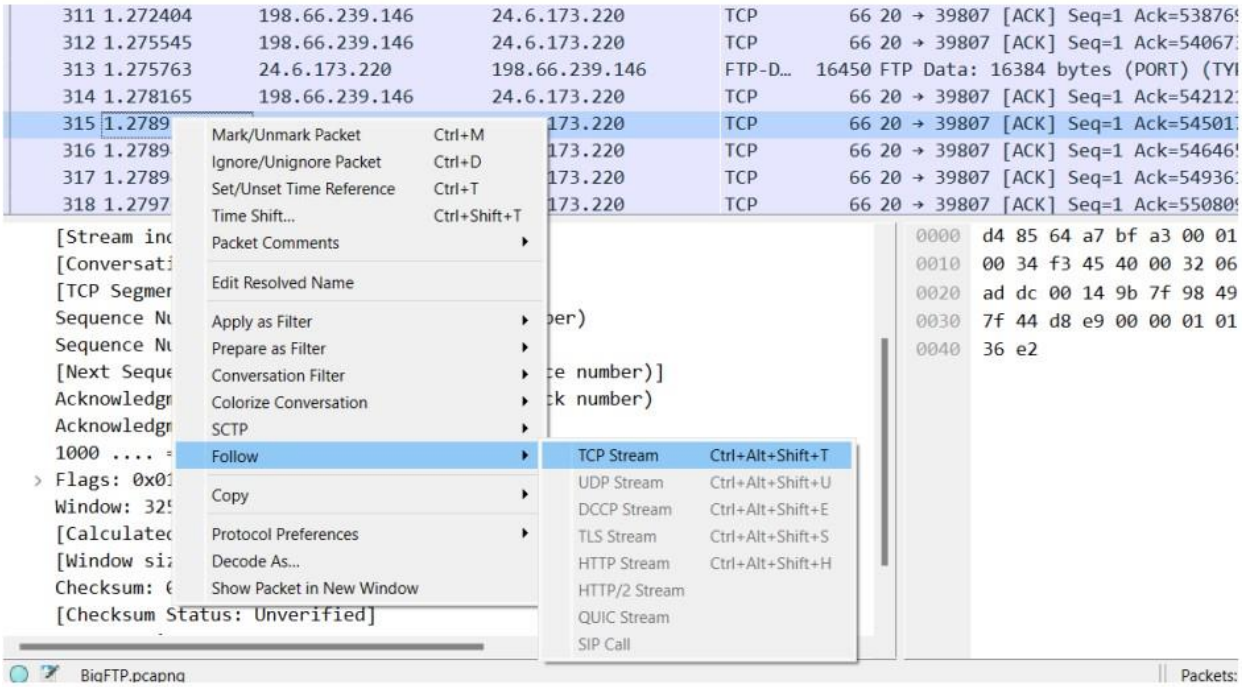
We selected the last packet 321 and expanded the TCP header for checking the ACK sequence number, which is showing 557057. Now we have to find which data packet is sending this ACK number to 321.



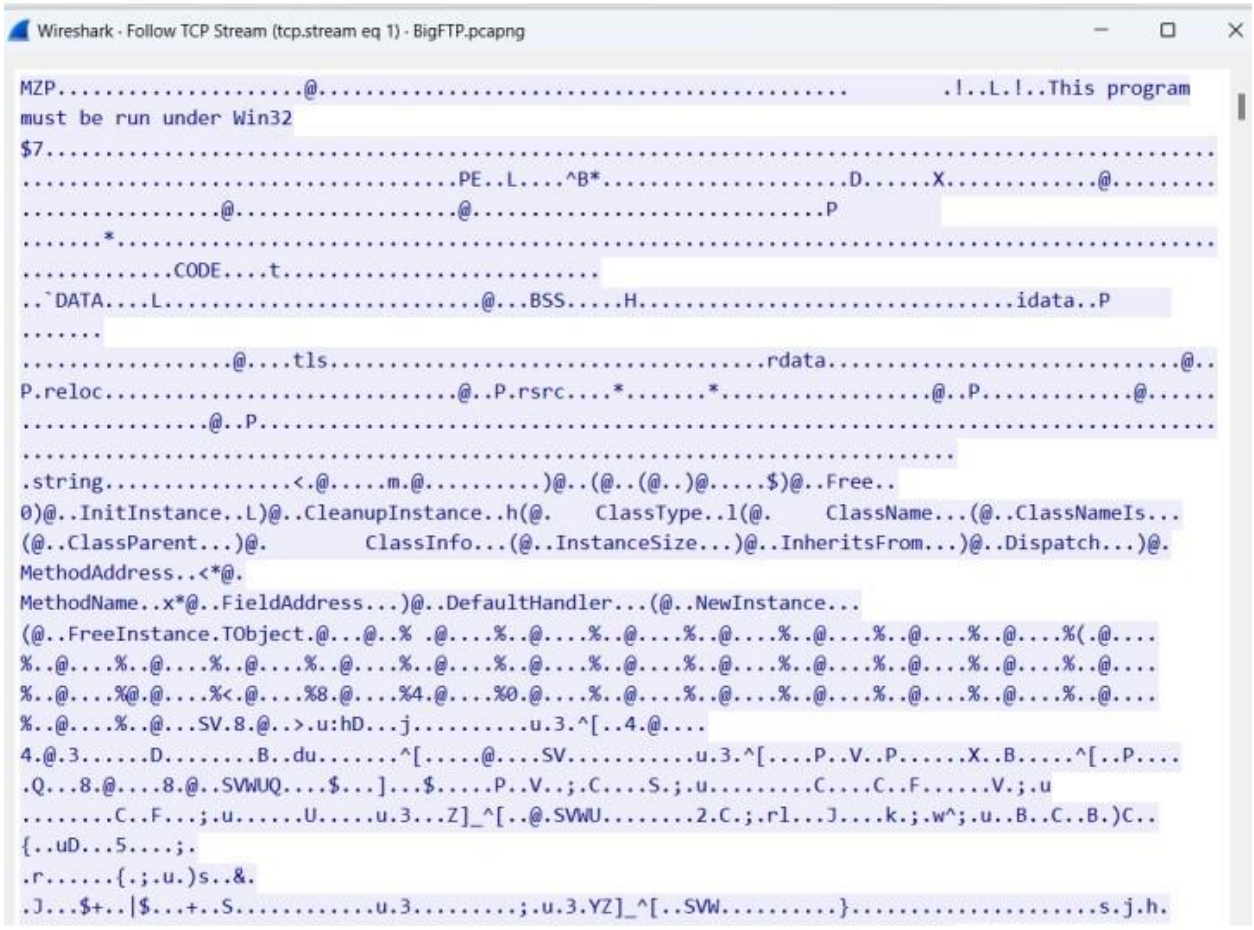
We started to check all the first data packet numbers, which are sending the main FTP-DATA. We found that packet number 304's TCP header has the next sequence number for 557057. This means data packet 304 is acknowledged between 314-321.



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.

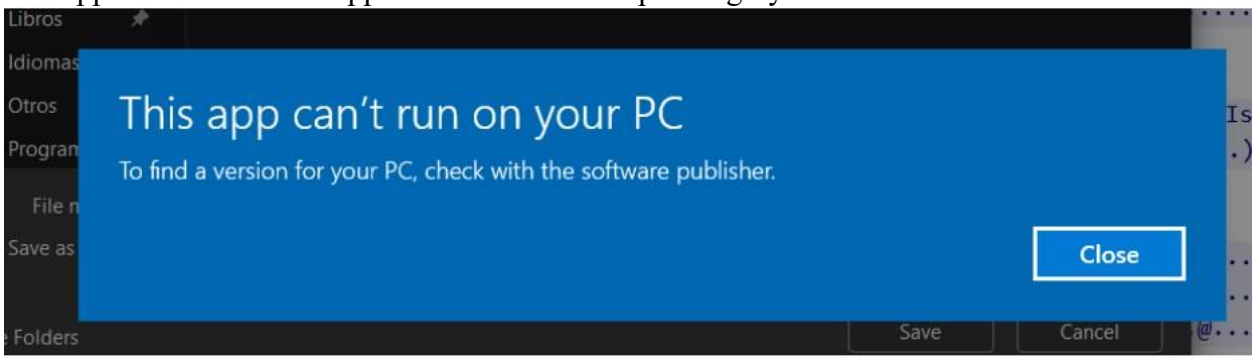


Inside the TCP stream it is showing the RAW data and it doesn't look like an image file. There is a message showing that this program must be run under win32 and also some kind of source code is showing. It means it is a Windows executable program.



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

This application was not supported in Windows Operating System.

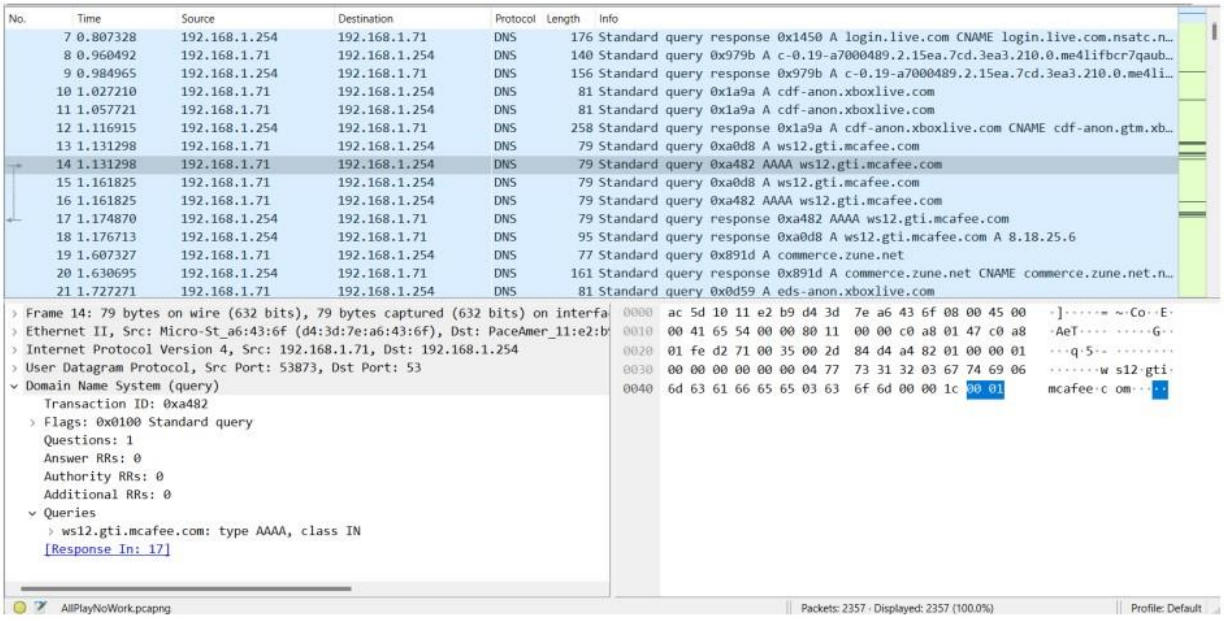


PAID TO PLAY Trace File: AllPlayNoWork.pcapng

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

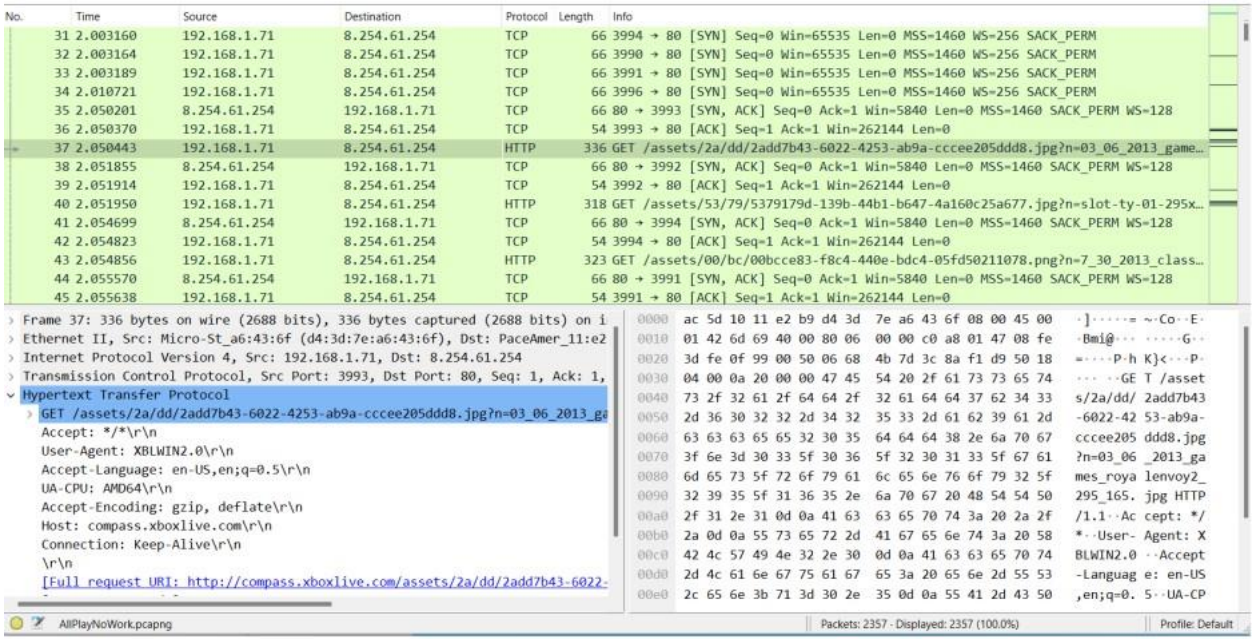
The IPv6 resolution process tries to look for AAAA in the DNS query type

Answer: ws12.gti.mcafee.com

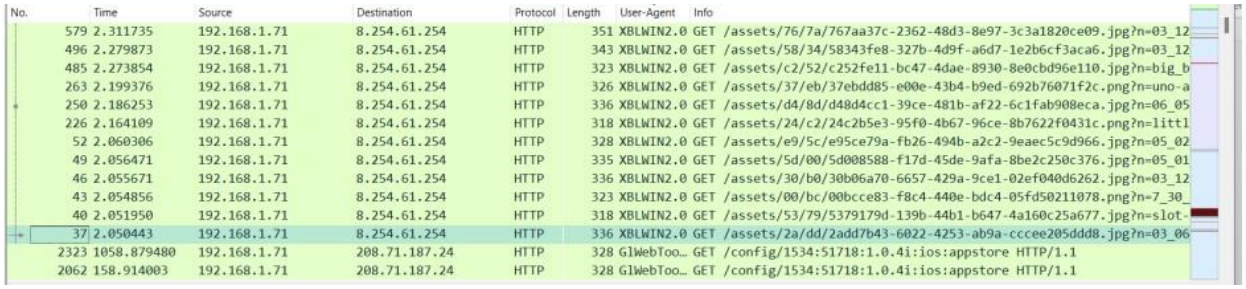


2. What operating system do you think the client is running?

Answer: Windows 8

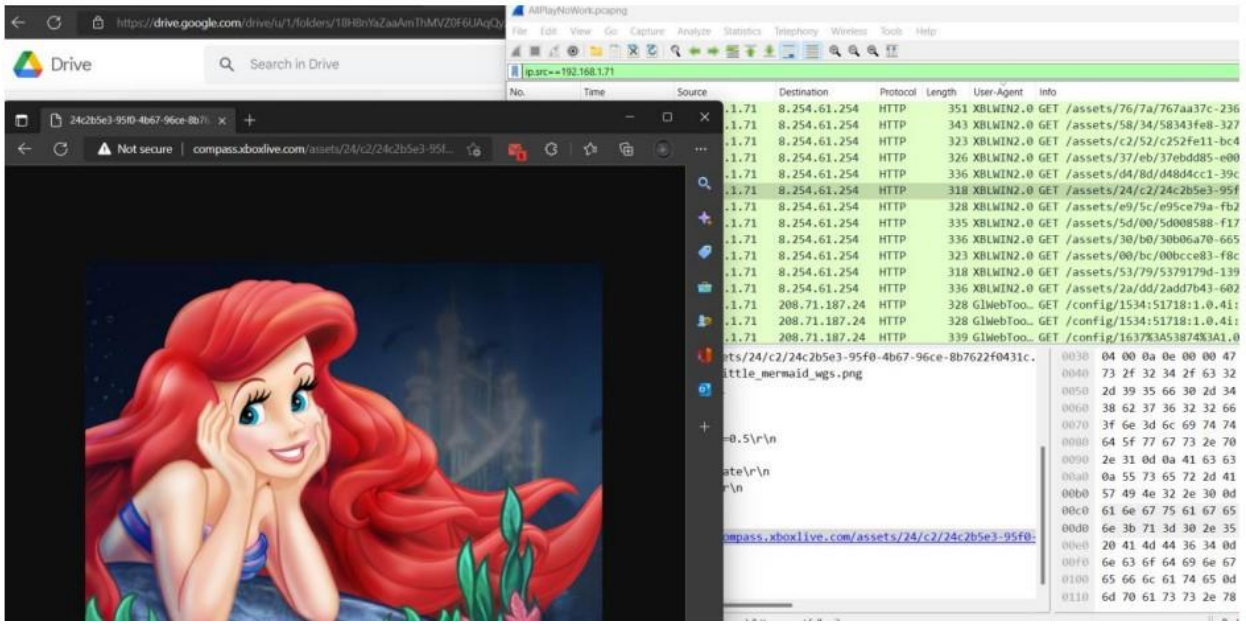


Right click on the user agent and click “apply as column”

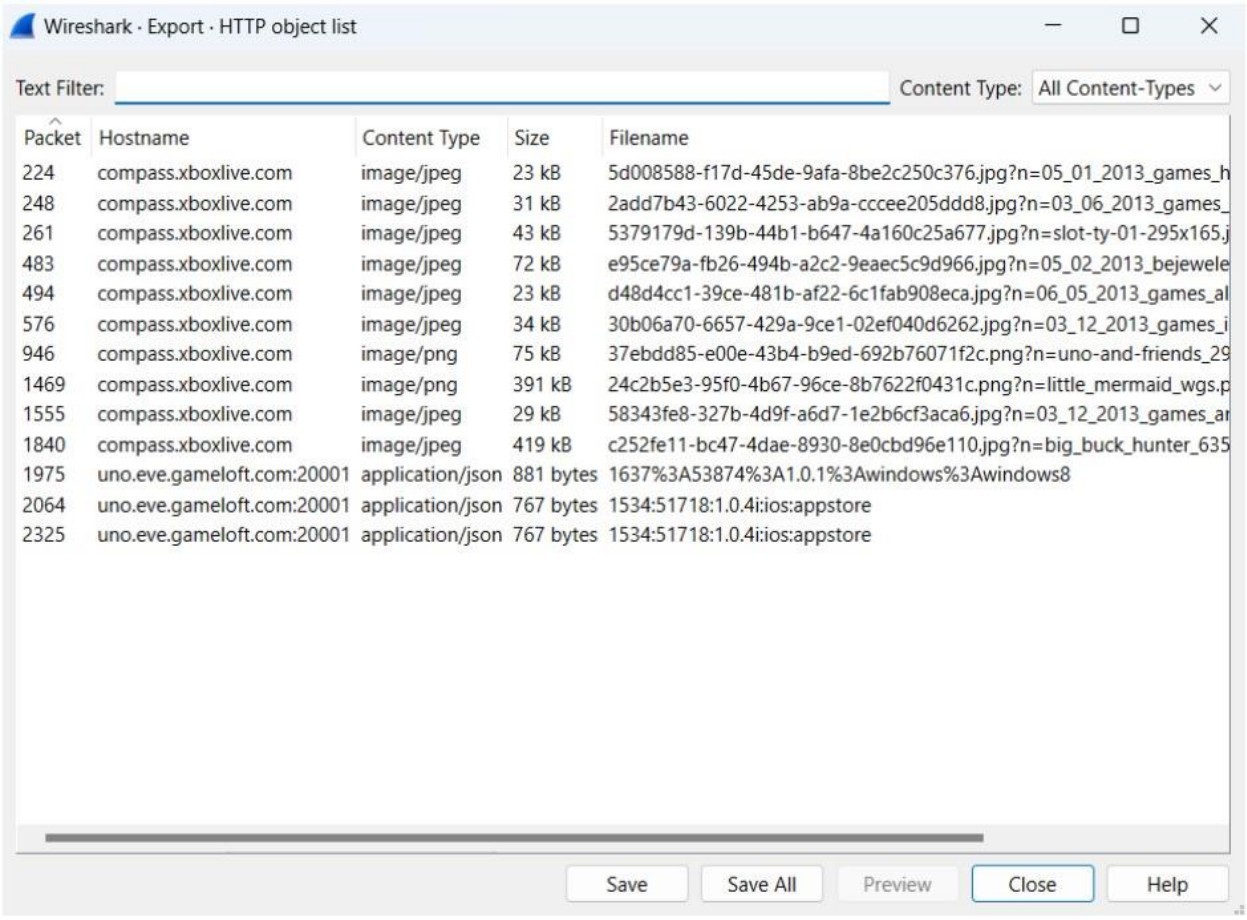


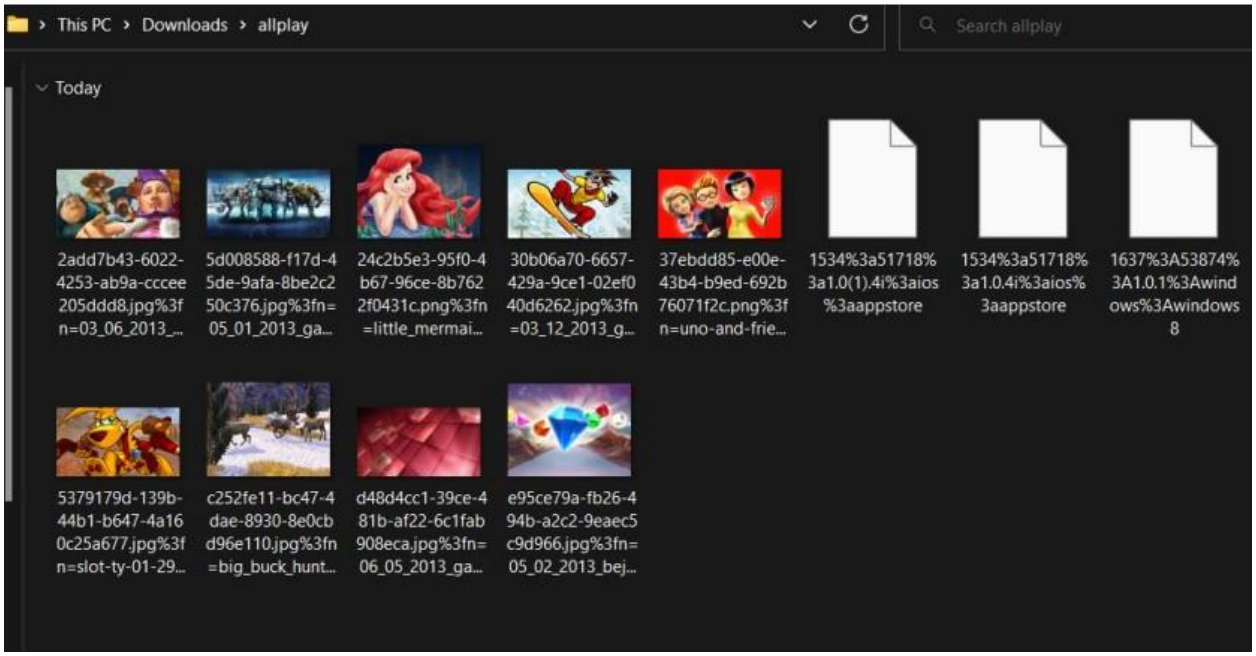
No.	Time	Source	Destination	Protocol	Length	User-Agent	Info
579	2.311735	192.168.1.71	8.254.61.254	HTTP	351	XBLWIN2.0	GET /assets/76/7a/767aa37c-2362-48d3-8e97-3c3a1820ce09.jpg?n=03_12
496	2.279873	192.168.1.71	8.254.61.254	HTTP	343	XBLWIN2.0	GET /assets/58/34/58343fe8-327b-4d9f-a6d7-1e2b6cf3aca6.jpg?n=03_12
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?n=big_b
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?n=uno-a
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?n=06_05
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?n=littl
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?n=05_02
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?n=05_01
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?n=03_12
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?n=7_30_
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?n=slot-
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?n=03_06
2323	1058.879480	192.168.1.71	208.71.187.24	HTTP	328	GlWebToo…	GET /config/1534:51718:1.0.4i:ios:appstore HTTP/1.1
2062	158.914003	192.168.1.71	208.71.187.24	HTTP	328	GlWebToo…	GET /config/1534:51718:1.0.4i:ios:appstore HTTP/1.1

3. What is the color of the mermaid's hair?
Answer: Reddish-orange

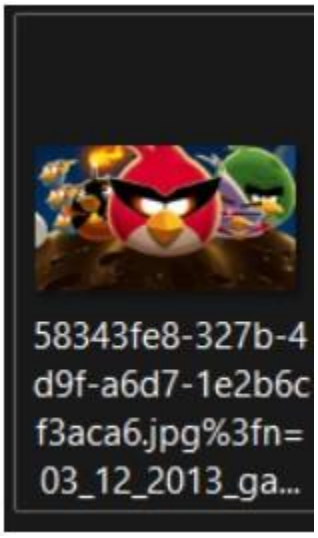


4. What classic games did the user learn about?
Answer: Games: Solitaire, Pac-Man, Mahjong, BigBuck etc:


Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Packet Hostname Content Type Size Filename
224 compass.xboxlive.com image/jpeg 23 kB 5d008588-f17d-45de-9afa-8be2c250c376.jpg?n=05_01_2013_games_h
248 compass.xboxlive.com image/jpeg 31 kB 2add7b43-6022-4253-ab9a-cccee205ddd8.jpg?n=03_06_2013_games_
261 compass.xboxlive.com image/jpeg 43 kB 5379179d-139b-44b1-b647-4a160c25a677.jpg?n=slot-ty-01-295x165.j
483 compass.xboxlive.com image/jpeg 72 kB e95ce79a-fb26-494b-a2c2-9eaec5c9d966.jpg?n=05_02_2013_bejewele
494 compass.xboxlive.com image/jpeg 23 kB d48d4cc1-39ce-481b-af22-6c1fab908eca.jpg?n=06_05_2013_games_al
576 compass.xboxlive.com image/jpeg 34 kB 30b06a70-6657-429a-9ce1-02ef040d6262.jpg?n=03_12_2013_games_i
946 compass.xboxlive.com image/png 75 kB 37ebdd85-e00e-43b4-b9ed-692b76071f2c.png?n=uno-and-friends_29
1469 compass.xboxlive.com image/png 391 kB 24c2b5e3-95f0-4b67-96ce-8b7622f0431c.png?n=little_mermaid_wgs.p
1555 compass.xboxlive.com image/jpeg 29 kB 58343fe8-327b-4d9f-a6d7-1e2b6cf3aca6.jpg?n=03_12_2013_games_ar
1840 compass.xboxlive.com image/jpeg 419 kB c252fe11-bc47-4dae-8930-8e0cbd96e110.jpg?n=big_buck_hunter_635
1975 uno.eve.gameloft.com:20001 application/json 881 bytes 1637%3A53874%3A1.0.1%3Awindows%3Awindows8
2064 uno.eve.gameloft.com:20001 application/json 767 bytes 1534:51718:1.0.4i:ios:appstore
2325 uno.eve.gameloft.com:20001 application/json 767 bytes 1534:51718:1.0.4i:ios:appstore
Save
Save All
Preview
Close
Help

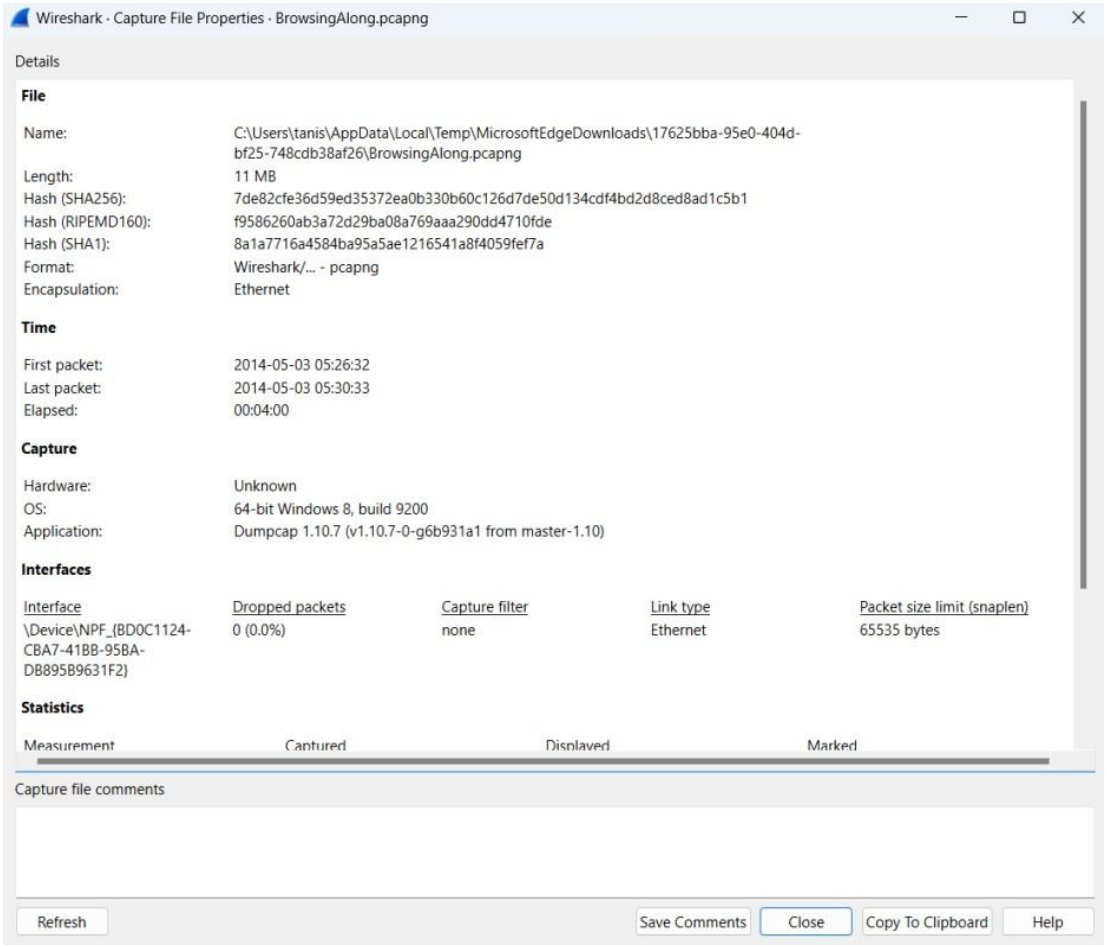

This PC › Downloads › allplay
Search allplay
Today
2add7b43-6022-4253-ab9a-cccee205ddd8.jpg%3fn=03_06_2013_...
5d008588-f17d-45de-9afa-8be2c250c376.jpg%3fn=05_01_2013_ga...
24c2b5e3-95f0-4b67-96ce-8b7622f0431c.png%3fn=little_mermai...
30b06a70-6657-429a-9ce1-02ef040d6262.jpg%3fn=03_12_2013_g...
37ebdd85-e00e-43b4-b9ed-692b76071f2c.png%3fn=uno-and-frie...
1534%3a51718%3a1.0(1).4i%3aios%3aappstore
1534%3a51718%3a1.0.4i%3aios%3aappstore
1637%3A53874%3A1.0.1%3Awindows%3Awindows8
5379179d-139b-44b1-b647-4a160c25a677.jpg%3fn=slot-ty-01-29...
c252fe11-bc47-4dae-8930-8e0cbd96e110.jpg%3fn=big_buck_hunt...
d48d4cc1-39ce-481b-af22-6c1fab908eca.jpg%3fn=06_05_2013_ga...
e95ce79a-fb26-494b-a2c2-9eaec5c9d966.jpg%3fn=05_02_2013_bej...

5. Which Angry Birds edition did the user learn about?
Answer: Angry Birds Space Edition



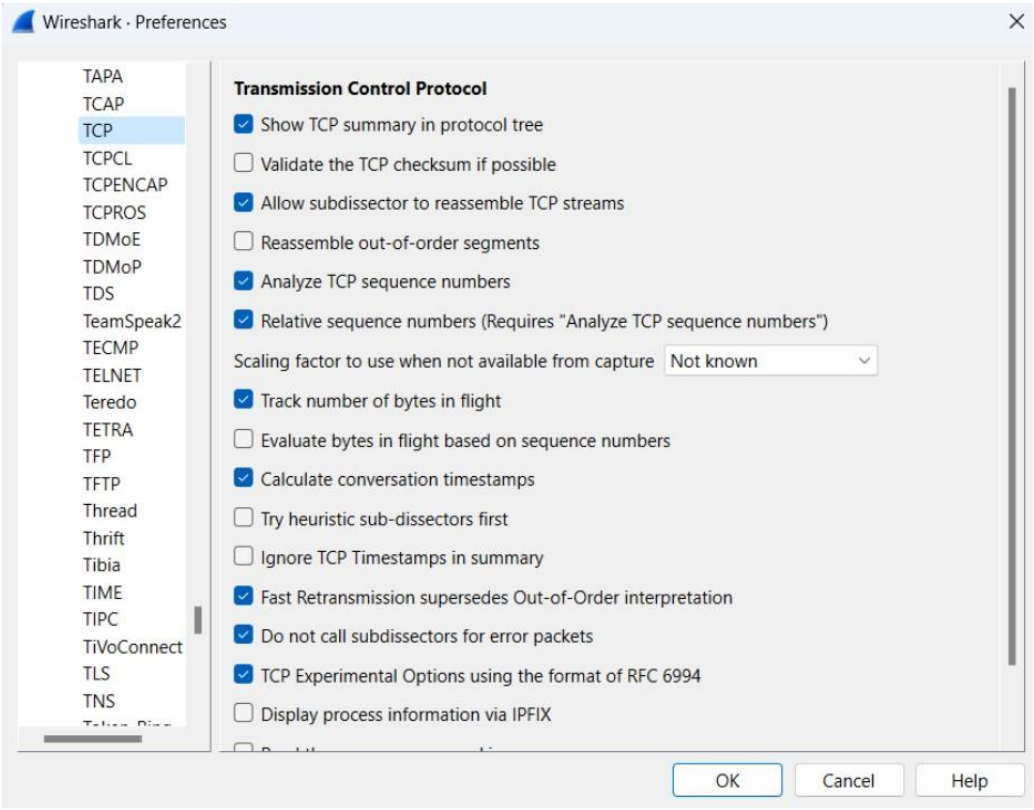
BROWSING BUDDY Trace File: BrowsingAlong.pcapng

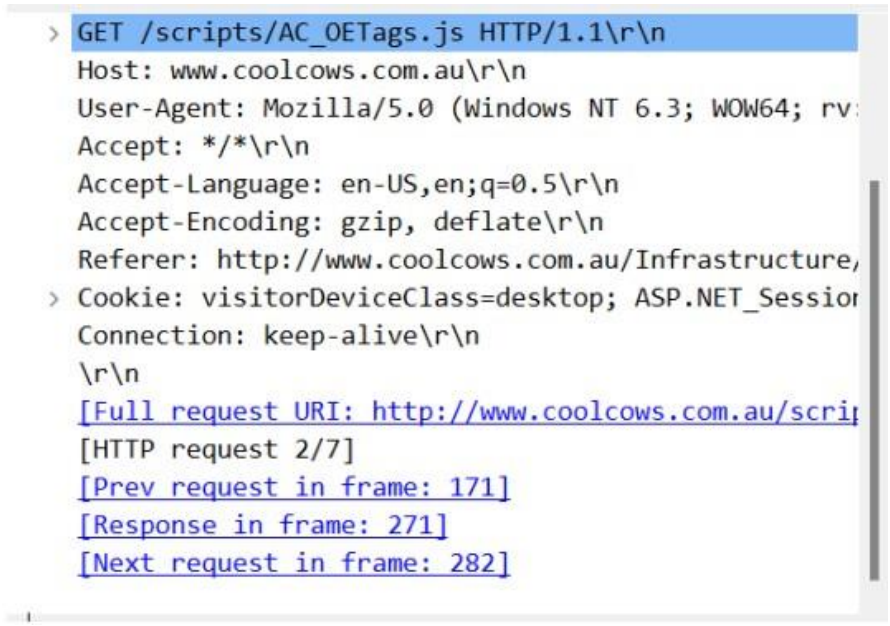
1. What version of dumpcap was used to capture this trace file?
Answer: Dumpcap 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)



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

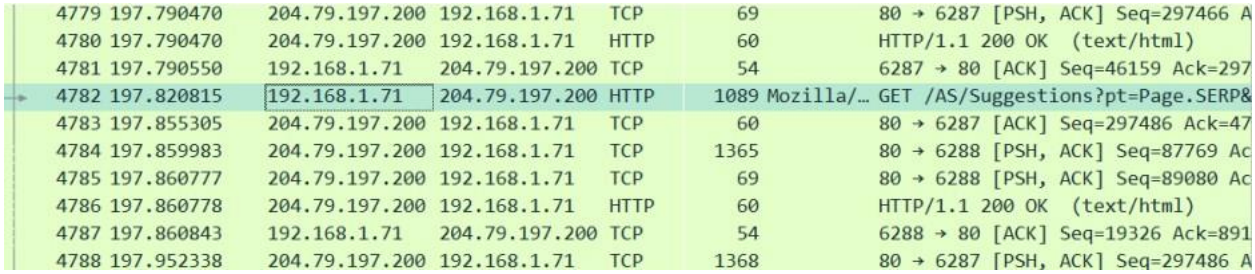
Answer: 266


Wireshark · Preferences
TAPA
TCAP
TCP
TCPCL
TCPENCAP
TCPROS
TDMoE
TDMoP
TDS
TeamSpeak2
TECMP
TELNET
Teredo
TETRA
TFP
TFTP
Thread
Thrift
Tibia
TIME
TIPC
TiVoConnect
TLS
TNS
Transmission Control Protocol
Show TCP summary in protocol tree
Validate the TCP checksum if possible
Allow subdissector to reassemble TCP streams
Reassemble out-of-order segments
Analyze TCP sequence numbers
Relative sequence numbers (Requires "Analyze TCP sequence numbers")
Scaling factor to use when not available from capture
Not known
Track number of bytes in flight
Evaluate bytes in flight based on sequence numbers
Calculate conversation timestamps
Try heuristic sub-dissectors first
Ignore TCP Timestamps in summary
Fast Retransmission supersedes Out-of-Order interpretation
Do not call subdissectors for error packets
TCP Experimental Options using the format of RFC 6994
Display process information via IPFIX
OK
Cancel
Help


GET /scripts/AC_OETags.js HTTP/1.1\r\n
Host: www.coolcows.com.au\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv
Accept: */*\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Referer: http://www.coolcows.com.au/Infrastructure,
Cookie: visitorDeviceClass=desktop; ASP.NET_Sessio
Connection: keep-alive\r\n
\r\n
[Full request URI: http://www.coolcows.com.au/scri
[HTTP request 2/7]
[Prev request in frame: 171]
[Response in frame: 271]
[Next request in frame: 282]

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

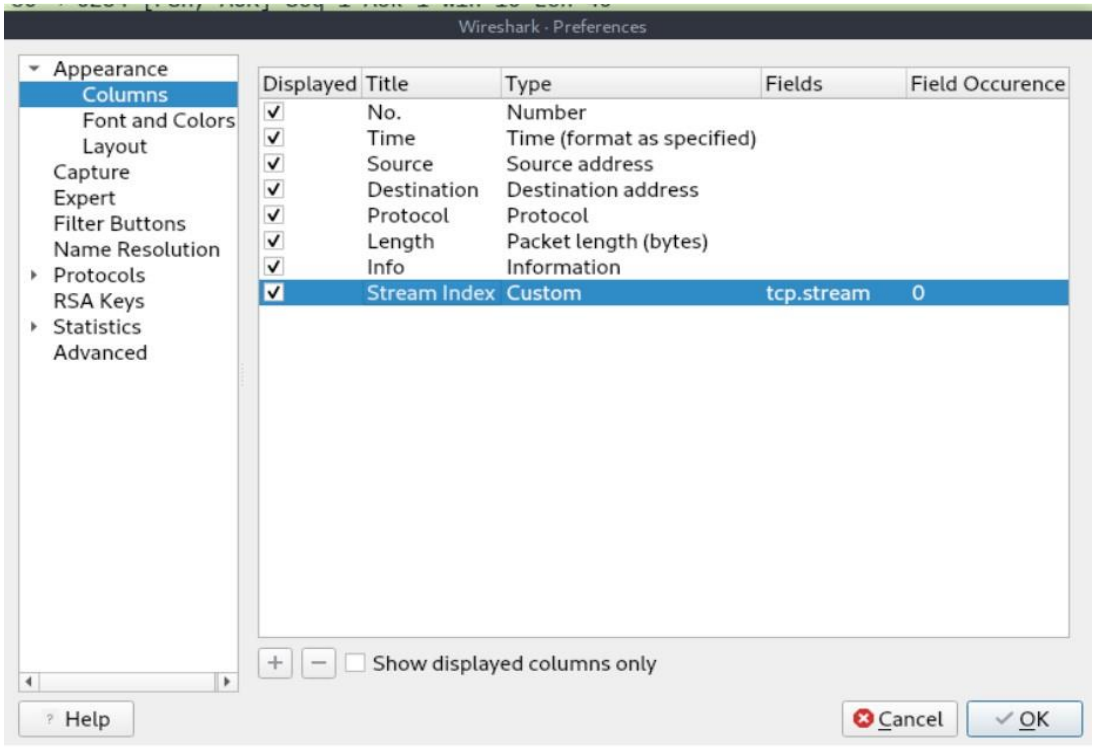
Answer: tiki bar

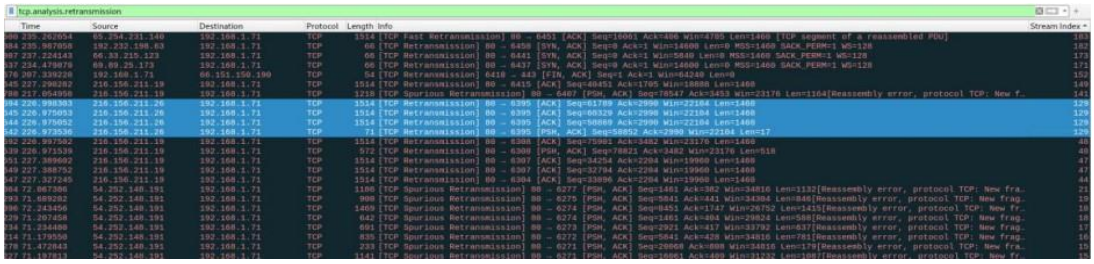


4779	197.790470	204.79.197.200	192.168.1.71	TCP	69	80 → 6287 [PSH, ACK] Seq=297466 A
4780	197.790470	204.79.197.200	192.168.1.71	HTTP	60	HTTP/1.1 200 OK (text/html)
4781	197.790550	192.168.1.71	204.79.197.200	TCP	54	6287 → 80 [ACK] Seq=46159 Ack=297
4782	197.820815	192.168.1.71	204.79.197.200	HTTP	1089 Mozilla/…	GET /AS/Suggestions?pt=Page.SERP&
4783	197.855305	204.79.197.200	192.168.1.71	TCP	60	80 → 6287 [ACK] Seq=297486 Ack=47
4784	197.859983	204.79.197.200	192.168.1.71	TCP	1365	80 → 6288 [PSH, ACK] Seq=87769 Ac
4785	197.860777	204.79.197.200	192.168.1.71	TCP	69	80 → 6288 [PSH, ACK] Seq=89080 Ac
4786	197.860778	204.79.197.200	192.168.1.71	HTTP	60	HTTP/1.1 200 OK (text/html)
4787	197.860843	192.168.1.71	204.79.197.200	TCP	54	6288 → 80 [ACK] Seq=19326 Ack=891
4788	197.952338	204.79.197.200	192.168.1.71	TCP	1368	80 → 6287 [PSH, ACK] Seq=297486 A

4. Which TCP stream experienced the most Retransmissions?

Answer: 129

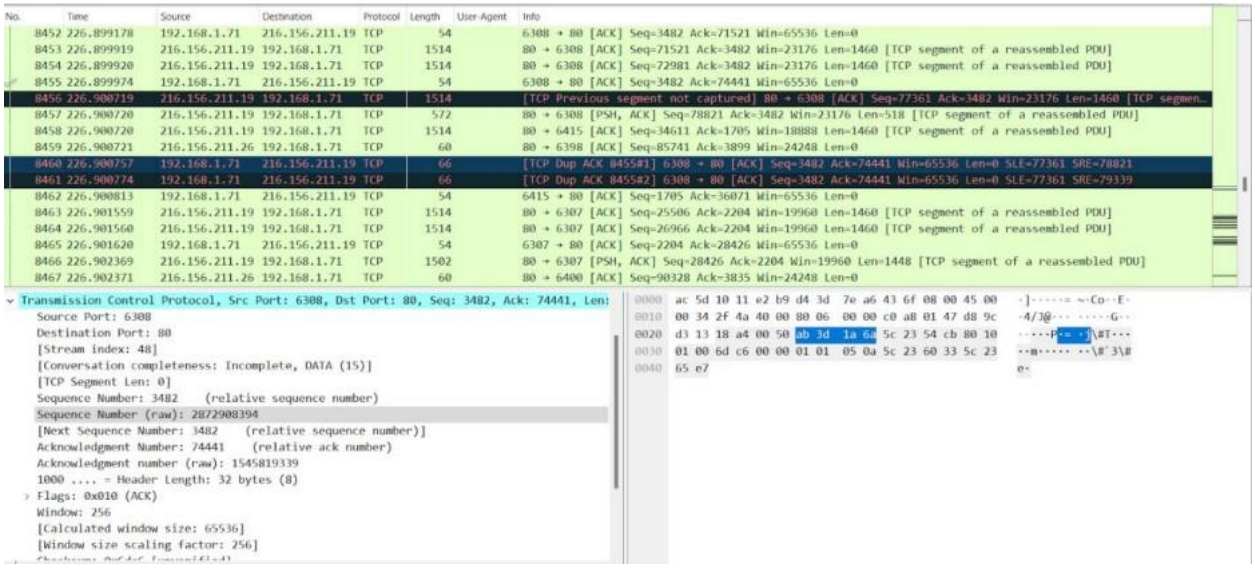




5. Frame 8500 is a retransmission triggered by duplicate ACKs. Why isn’tit marked as a Fast Retransmission?

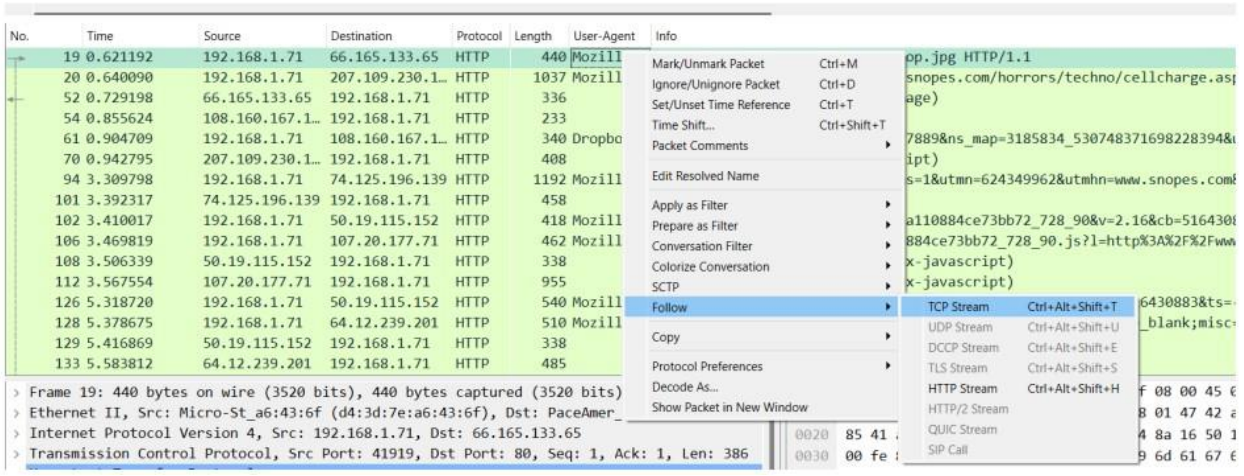
Answer: We can see that there are two duplicate ACK packets before frame 8500. If there are two duplicate ACKs in the reverse direction and if the packet occurs within 20ms of the last duplicate ACK then it will be considered as fast retransmission. Using a

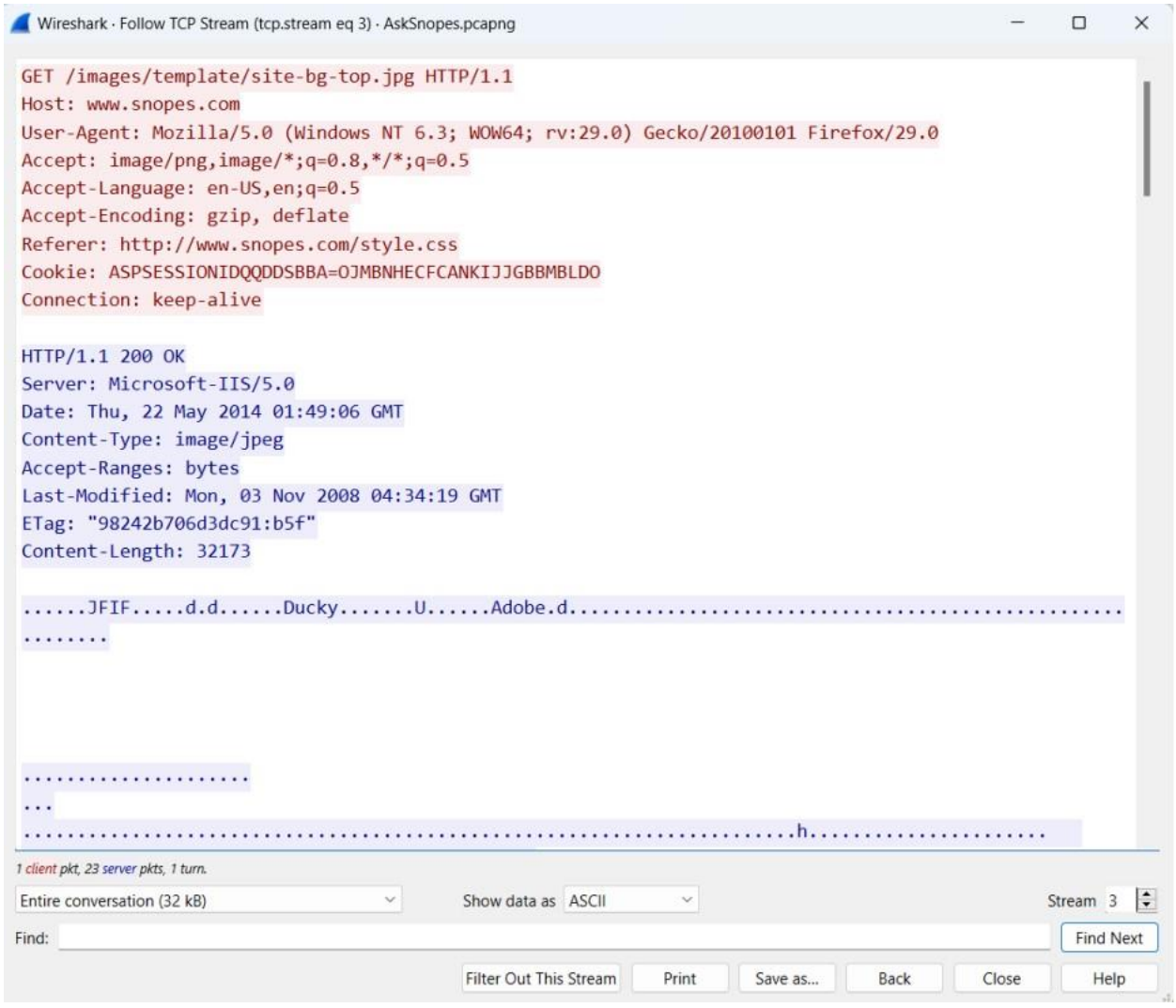
timestamp of 8500 it was more than 20 ms longer than the previous frame. So, it isn't a fast retransmission.



OUCH! Trace File: AskSnopes.pcapng

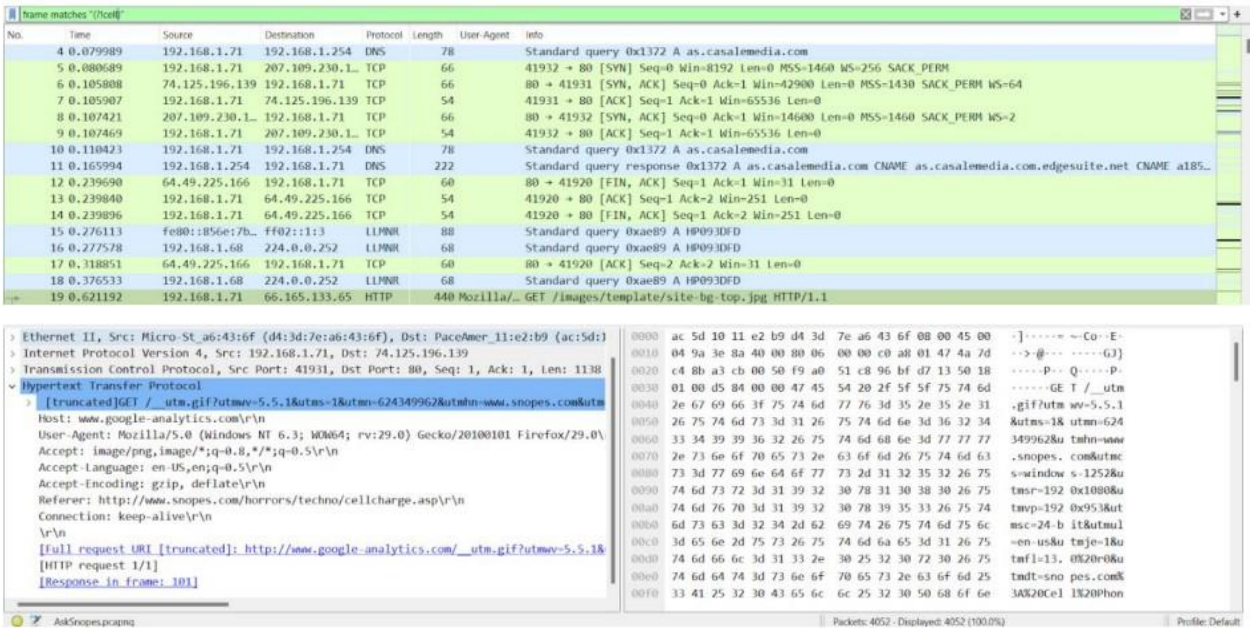
1. What web server software is used by www.snopes.com? Answer: Microsoft-IIS/5.0



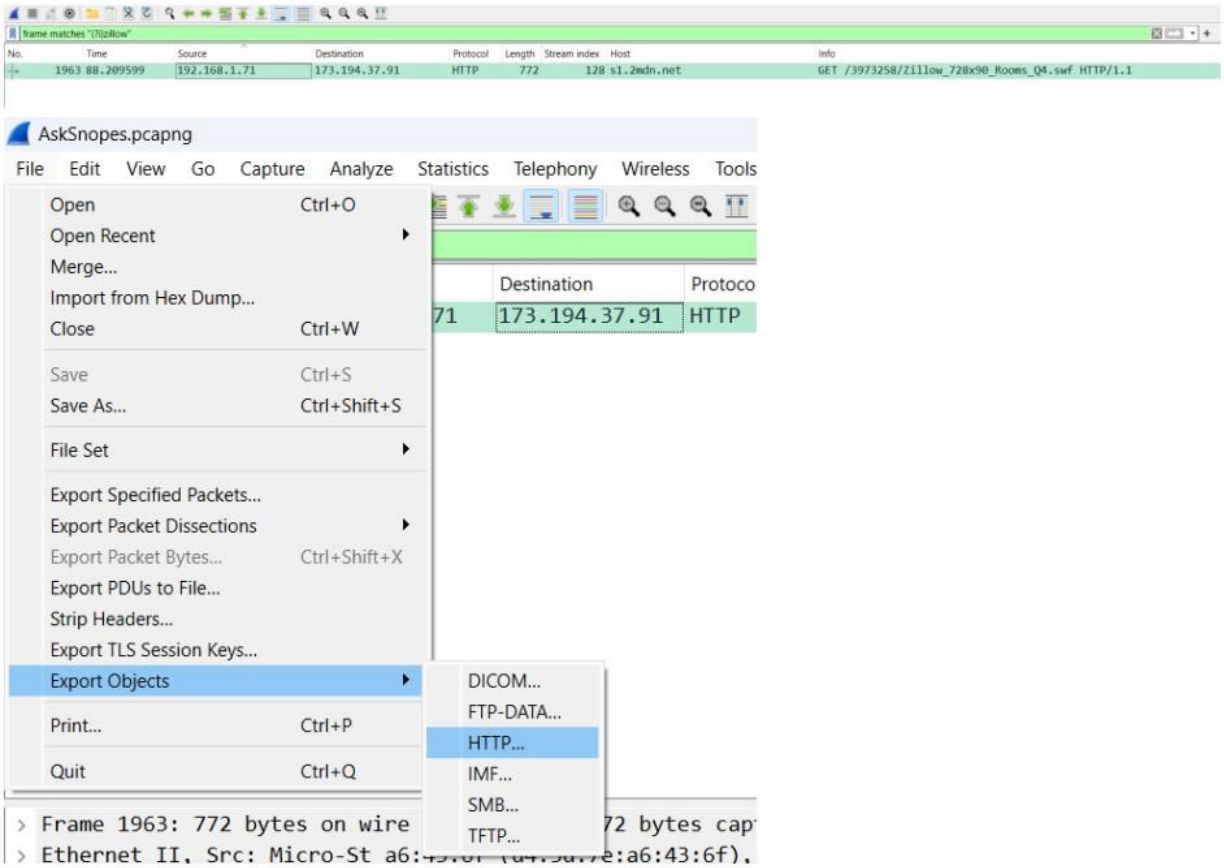


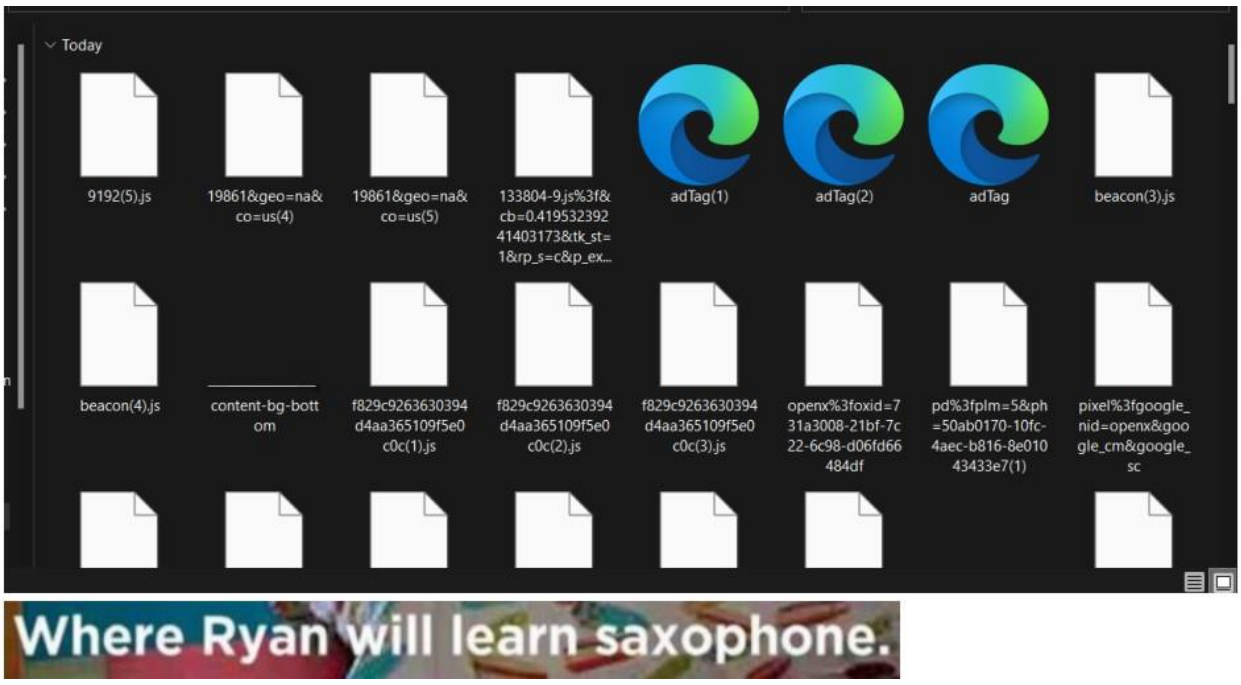
2. What cell phone problem is the client concerned?

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

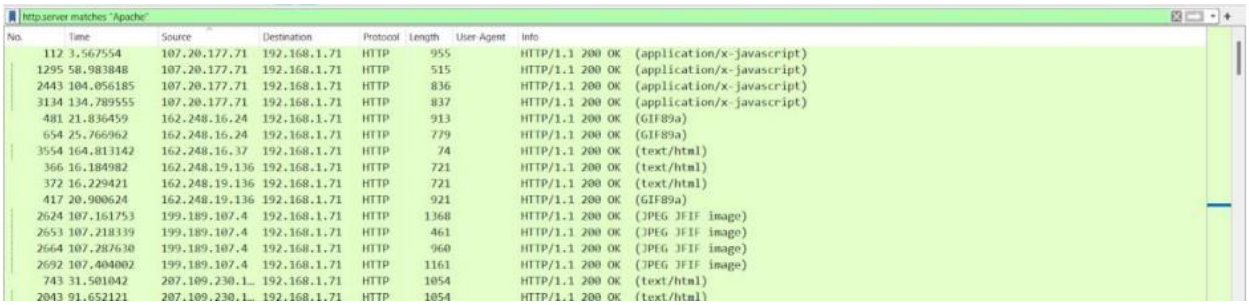


3. According to Zillow, what instrument will Ryan learn to play?
Answer: Saxophone





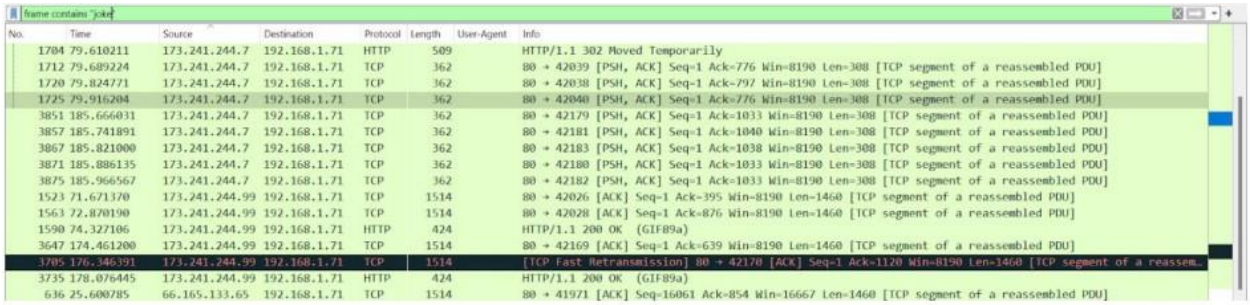
4. How many web servers are running Apache?
Answer: 21



Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets A → B	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.71	23.23.197.19	2	1.151 KiB	13	15.38%	0	0 bytes	2	1.151 KiB	14.871442	9.0852	0 bytes	1.014 KiB
192.168.1.71	23.210.219.85	6	6.316 KiB	56	10.71%	0	0 bytes	6	6.316 KiB	7.762760	161.9039	0 bytes	319 bytes
192.168.1.71	23.210.231.153	12	6.019 KiB	314	3.82%	0	0 bytes	12	6.019 KiB	10.694794	184.0216	0 bytes	267 bytes
192.168.1.71	50.19.115.152	13	4.291 KiB	50	26.00%	0	0 bytes	13	4.291 KiB	2.871487	177.3290	0 bytes	198 bytes
192.168.1.71	50.97.236.98	2	1.712 KiB	36	5.56%	0	0 bytes	2	1.712 KiB	42.700396	67.8534	0 bytes	206 bytes
192.168.1.71	50.116.194.21	1	1.021 KiB	11	9.09%	0	0 bytes	1	1.021 KiB	76.690824	5.3140	0 bytes	1.536 KiB
192.168.1.71	50.116.194.28	1	527 bytes	11	9.09%	0	0 bytes	1	527 bytes	79.809615	5.3124	0 bytes	793 bytes
192.168.1.71	54.243.109.84	1	609 bytes	11	9.09%	0	0 bytes	1	609 bytes	106.497568	59.9250	0 bytes	81 bytes
192.168.1.71	63.135.172.251	2	837 bytes	14	14.29%	0	0 bytes	2	837 bytes	106.780786	6.3934	0 bytes	1.022 KiB
192.168.1.71	69.25.24.24	13	14.672 KiB	143	9.09%	0	0 bytes	13	14.672 KiB	24.755133	149.4709	0 bytes	804 bytes
192.168.1.71	69.25.24.26	3	3.015 KiB	30	10.00%	0	0 bytes	3	3.015 KiB	42.755805	97.9370	0 bytes	252 bytes
192.168.1.71	107.20.177.71	4	3.069 KiB	29	13.79%	0	0 bytes	4	3.069 KiB	2.911223	191.8342	0 bytes	131 bytes
192.168.1.71	162.248.16.24	2	1.652 KiB	24	8.33%	0	0 bytes	2	1.652 KiB	21.300858	4.4916	0 bytes	2.942 KiB
192.168.1.71	162.248.16.37	1	74 bytes	32	3.13%	0	0 bytes	1	74 bytes	153.981593	10.8567	0 bytes	54 bytes
192.168.1.71	162.248.19.136	3	2.308 KiB	42	7.14%	0	0 bytes	3	2.308 KiB	14.992486	8.9642	0 bytes	2.059 KiB
192.168.1.71	207.109.230.154	3	3.088 KiB	44	6.82%	0	0 bytes	3	3.088 KiB	31.446135	115.1637	0 bytes	219 bytes
192.168.1.71	207.109.230.161	2	1.146 KiB	30	6.67%	0	0 bytes	2	1.146 KiB	0.080689	171.0507	0 bytes	54 bytes
192.168.1.71	207.109.230.187	3	2.965 KiB	42	7.14%	0	0 bytes	3	2.965 KiB	130.470514	64.2095	0 bytes	378 bytes
192.168.1.71	216.39.54.212	1	225 bytes	12	8.33%	0	0 bytes	1	225 bytes	14.893408	1.0217	0 bytes	1.720 KiB
199.189.107.4	192.168.1.71	4	3.857 KiB	209	1.91%	4	3.857 KiB	0	0 bytes	3.194677	109.2084	289 bytes	0 bytes

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

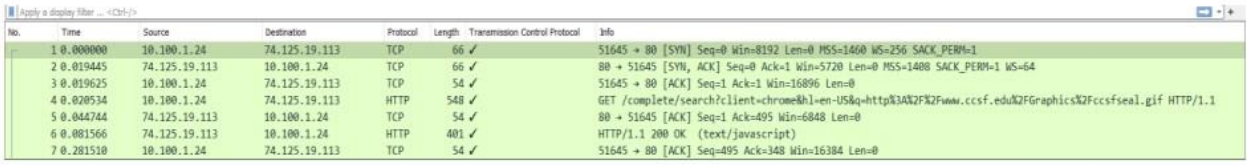
Answer: 173.241.244.7, 173.241.244.99, 173.241.244.153



Wireshark Challenge 2

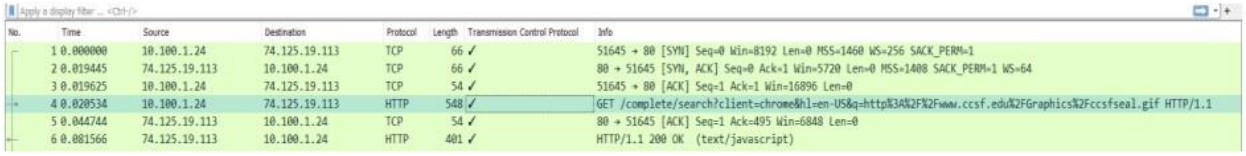
Examine the wireshark window and find answers to the following questions:

1. This packet capture file contains two TCP handshakes. Find the firsthandshake and write down the packet numbers of those packets (the column labeled "No."). Ans: Packets: 1, 2 and 3



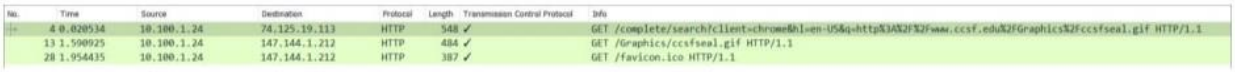
No.	Time	Source	Destination	Protocol	Length	Transmission Control Protocol	Info
1	0.000000	10.100.1.24	74.125.19.113	TCP	66 ✓		51645 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.019445	74.125.19.113	10.100.1.24	TCP	66 ✓		80 → 51645 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1408 SACK_PERM=1 WS=64
3	0.019625	10.100.1.24	74.125.19.113	TCP	54 ✓		51645 → 80 [ACK] Seq=1 Ack=1 Win=16896 Len=0
4	0.020534	10.100.1.24	74.125.19.113	HTTP	548 ✓		GET /complete/search?client=chrome&hl=en-US&q=http%3A%2F%2Fwww.ccsf.edu%2FGraphics%2Fccsfseal.gif HTTP/1.1
5	0.044744	74.125.19.113	10.100.1.24	TCP	54 ✓		80 → 51645 [ACK] Seq=1 Ack=495 Win=6848 Len=0
6	0.081566	74.125.19.113	10.100.1.24	HTTP	401 ✓		HTTP/1.1 200 OK (text/javascript)
7	0.281510	10.100.1.24	74.125.19.113	TCP	54 ✓		51645 → 80 [ACK] Seq=495 Ack=348 Win=16384 Len=0

2. In this session, a client machine initiated a connection to a server andthen downloaded a file. What is the client's IP address?
Ans: 10.100.1.24



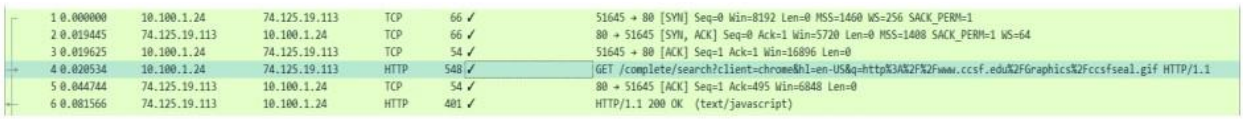
No.	Time	Source	Destination	Protocol	Length	Transmission Control Protocol	Info
1	0.000000	10.100.1.24	74.125.19.113	TCP	66 ✓		51645 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.019445	74.125.19.113	10.100.1.24	TCP	66 ✓		80 → 51645 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1408 SACK_PERM=1 WS=64
3	0.019625	10.100.1.24	74.125.19.113	TCP	54 ✓		51645 → 80 [ACK] Seq=1 Ack=1 Win=16896 Len=0
4	0.020534	10.100.1.24	74.125.19.113	HTTP	548 ✓		GET /complete/search?client=chrome&hl=en-US&q=http%3A%2F%2Fwww.ccsf.edu%2FGraphics%2Fccsfseal.gif HTTP/1.1
5	0.044744	74.125.19.113	10.100.1.24	TCP	54 ✓		80 → 51645 [ACK] Seq=1 Ack=495 Win=6848 Len=0
6	0.081566	74.125.19.113	10.100.1.24	HTTP	401 ✓		HTTP/1.1 200 OK (text/javascript)

3. How many HTTP GET request packets are there?Ans: 3



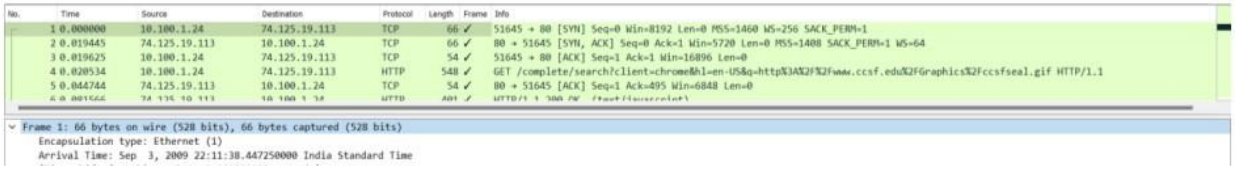
No.	Time	Source	Destination	Protocol	Length	Transmission Control Protocol	Info
4	0.020534	10.100.1.24	74.125.19.113	HTTP	548 ✓		GET /complete/search?client=chrome&hl=en-US&q=http%3A%2F%2Fwww.ccsf.edu%2FGraphics%2Fccsfseal.gif HTTP/1.1
13	1.590925	10.100.1.24	147.144.1.212	HTTP	484 ✓		GET /Graphics/ccsfseal.gif HTTP/1.1
28	1.954435	10.100.1.24	147.144.1.212	HTTP	387 ✓		GET /favicon.ico HTTP/1.1

4. Find the first HTTP GET request packet. What was the server's IPaddress? (The server is the Destination).
Ans: 74.125.19.113



No.	Time	Source	Destination	Protocol	Length	Transmission Control Protocol	Info
1	0.000000	10.100.1.24	74.125.19.113	TCP	66 ✓		51645 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.019445	74.125.19.113	10.100.1.24	TCP	66 ✓		80 → 51645 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1408 SACK_PERM=1 WS=64
3	0.019625	10.100.1.24	74.125.19.113	TCP	54 ✓		51645 → 80 [ACK] Seq=1 Ack=1 Win=16896 Len=0
4	0.020534	10.100.1.24	74.125.19.113	HTTP	548 ✓		GET /complete/search?client=chrome&hl=en-US&q=http%3A%2F%2Fwww.ccsf.edu%2FGraphics%2Fccsfseal.gif HTTP/1.1
5	0.044744	74.125.19.113	10.100.1.24	TCP	54 ✓		80 → 51645 [ACK] Seq=1 Ack=495 Win=6848 Len=0
6	0.081566	74.125.19.113	10.100.1.24	HTTP	401 ✓		HTTP/1.1 200 OK (text/javascript)

5. Examine the first packet. Look at the center pane in Wireshark. Howmany bytes were sent on the wire to form this packet?
Ans: 66 bytes



No.	Time	Source	Destination	Protocol	Length	Frame	Info
1	0.000000	10.100.1.24	74.125.19.113	TCP	66 ✓		51645 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.019445	74.125.19.113	10.100.1.24	TCP	66 ✓		80 → 51645 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1408 SACK_PERM=1 WS=64
3	0.019625	10.100.1.24	74.125.19.113	TCP	54 ✓		51645 → 80 [ACK] Seq=1 Ack=1 Win=16896 Len=0
4	0.020534	10.100.1.24	74.125.19.113	HTTP	548 ✓		GET /complete/search?client=chrome&hl=en-US&q=http%3A%2F%2Fwww.ccsf.edu%2FGraphics%2Fccsfseal.gif HTTP/1.1
5	0.044744	74.125.19.113	10.100.1.24	TCP	54 ✓		80 → 51645 [ACK] Seq=1 Ack=495 Win=6848 Len=0

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Sep 3, 2009 22:11:38.447250000 India Standard Time

Wireshark Challenge 3 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:

1. 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.

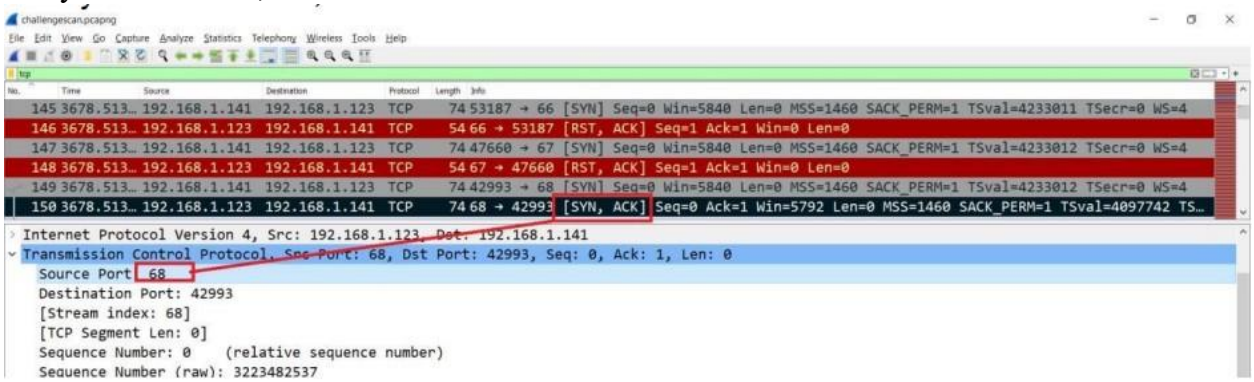
2. What is the IP address of the target host?

Answer: 192.168.1.123

3. Which TCP port opens on the target?

Answer: Port 68

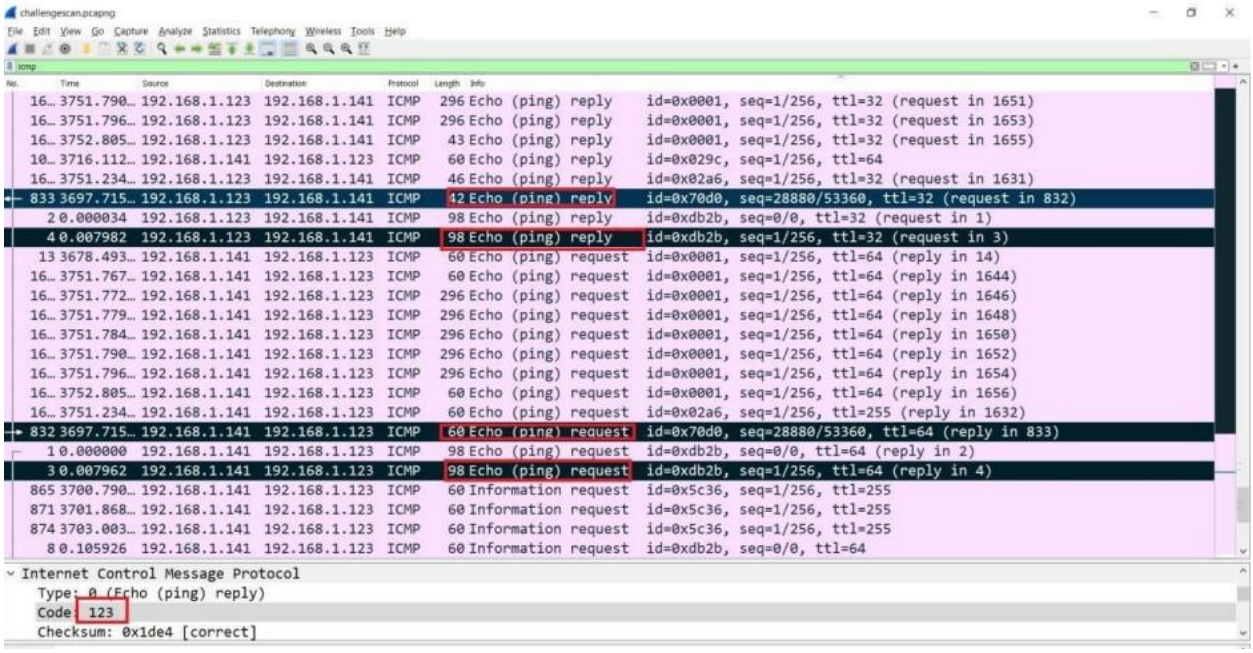
Analysis: Find SYN,ACK Packet and its source host



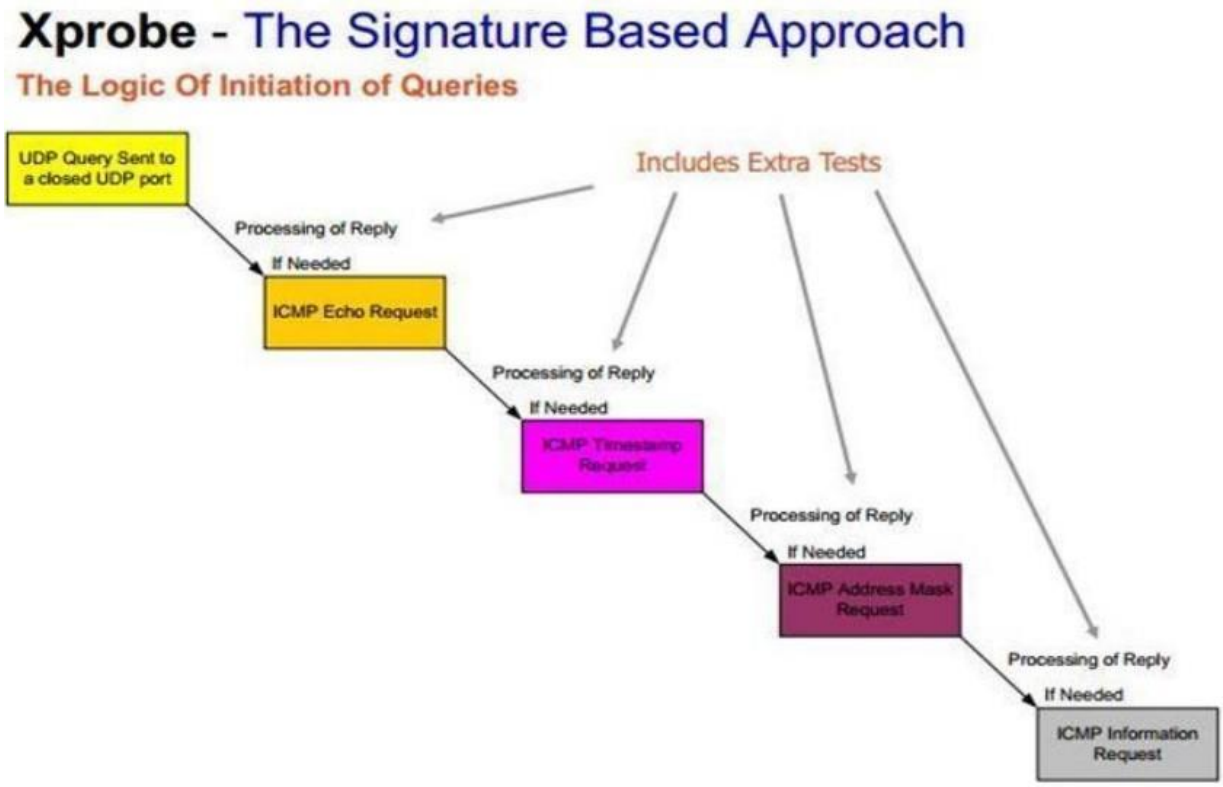
4. Which ICMP packets contain non-standard Type/Code numbers?

Answer: Code 123

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

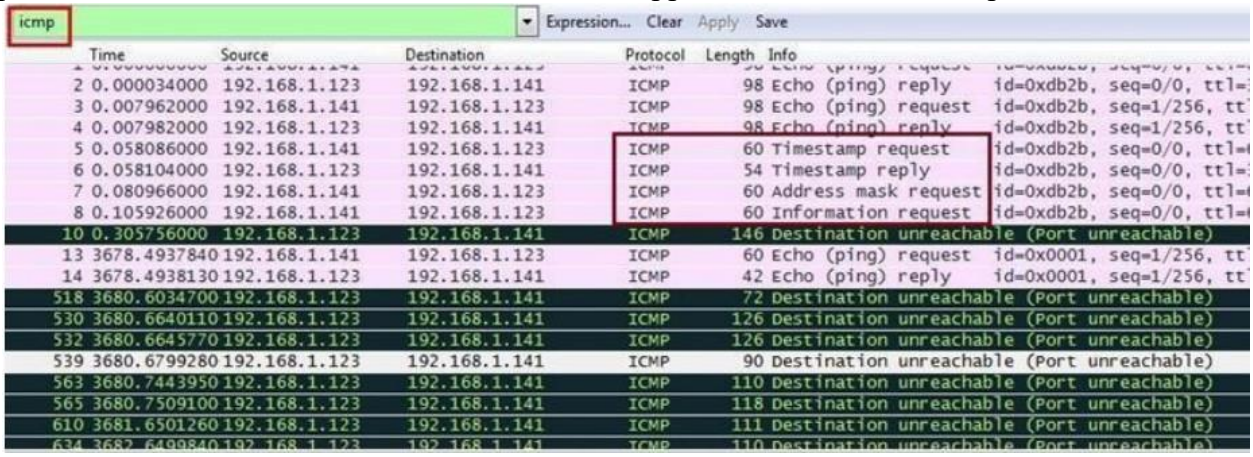


5. What software is used to scan the target?
Answer: Xprobe
Analysis:



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.

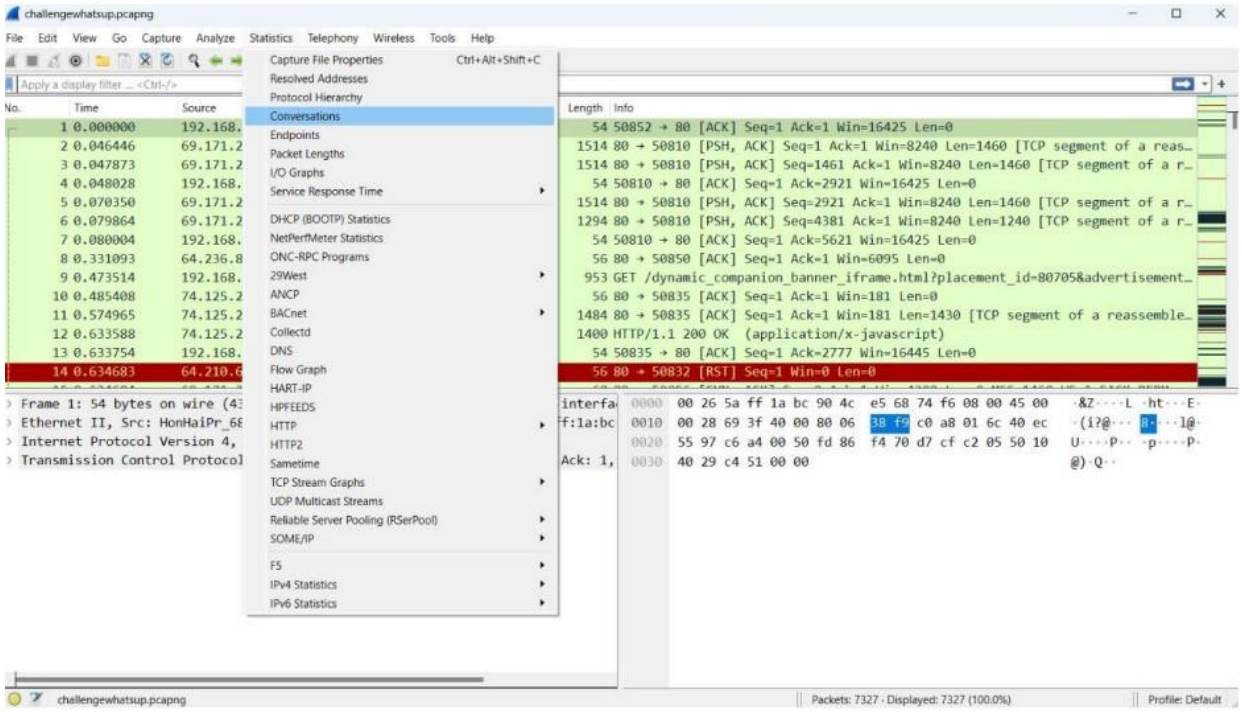


Cursed

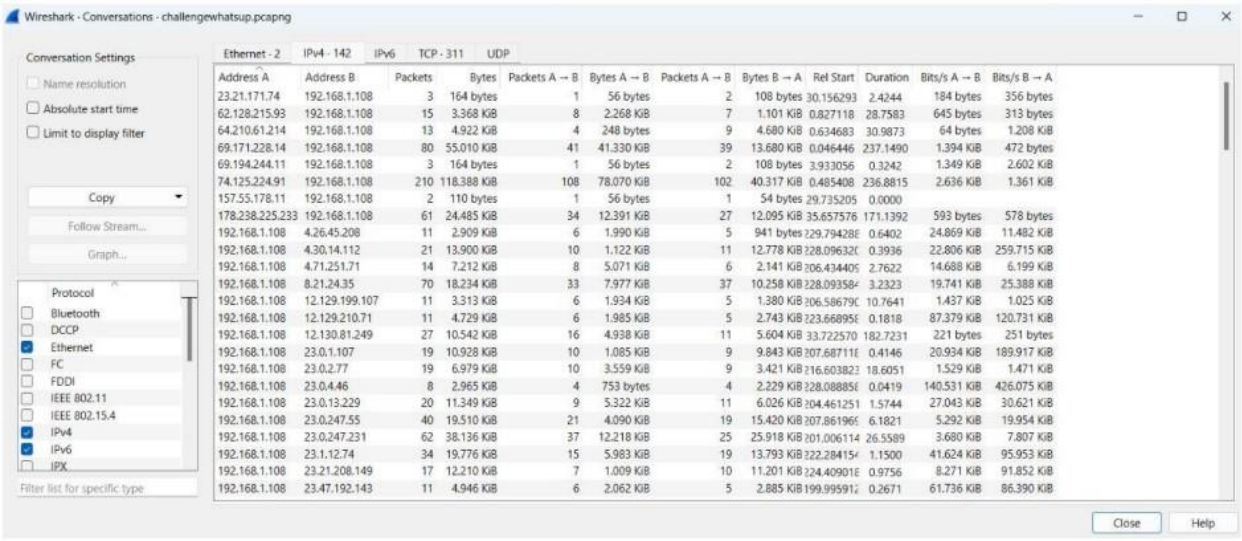
1. How many different IP hosts is Scott's machine communicating with?

Answer: 142

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



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.



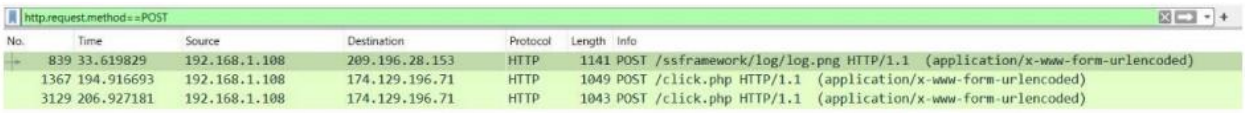
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets A → B	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
23.21.171.74	192.168.1.108	3	164 bytes	1	56 bytes	2	108 bytes	30.156293	2.4244	184 bytes	356 bytes
62.128.215.93	192.168.1.108	15	3.368 KiB	8	2.268 KiB	7	1.101 KiB	0.827118	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	229.79428E	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	206.434405	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	207.68711E	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	216.603822	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	224.409016	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	199.995912	0.2671	61.736 KiB	86.390 KiB

2. 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

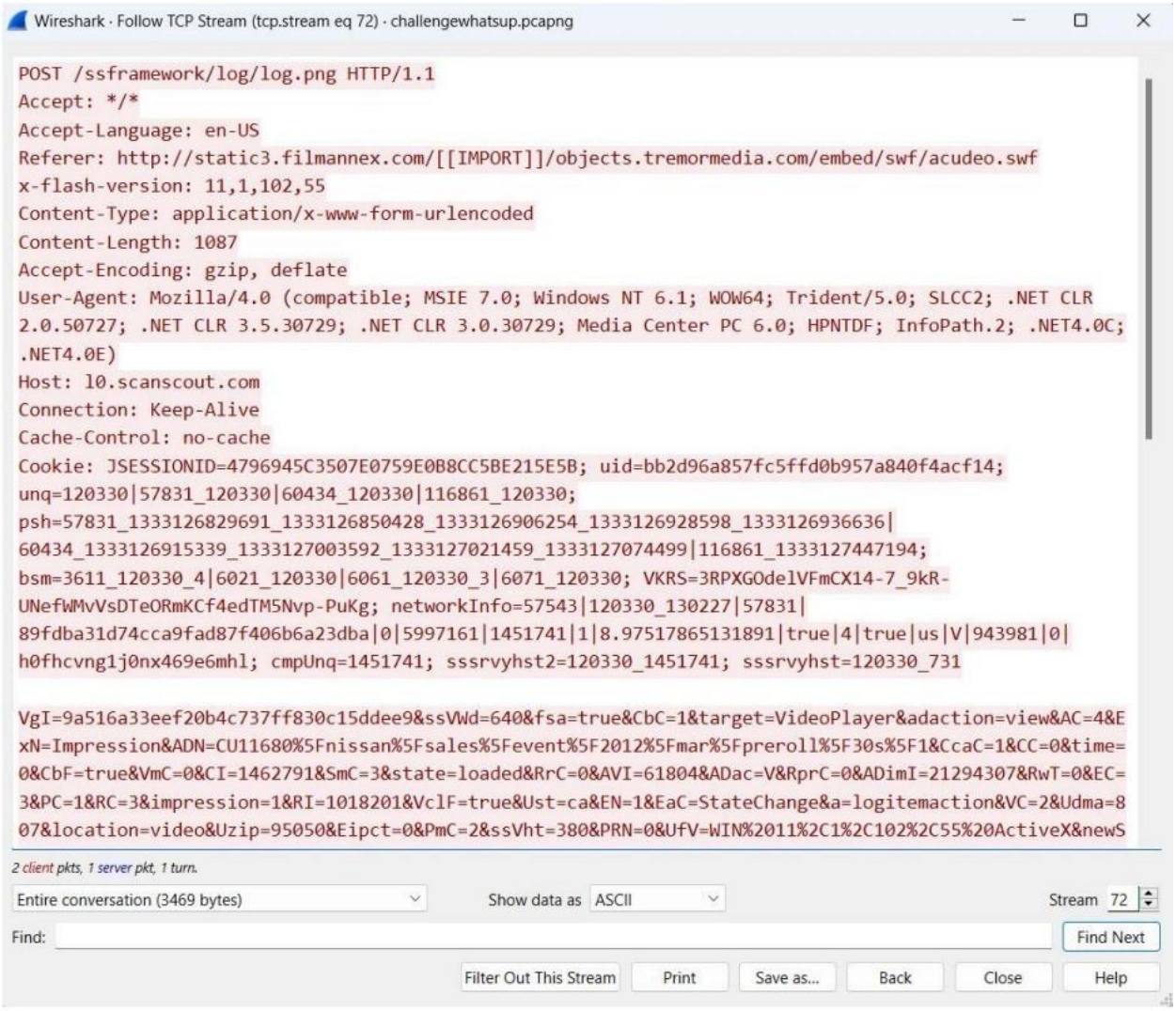
Measurement	Captured	Displayed	Marked
Packets	7327	7327 (100.0%)	—
Time span, s	237.435	237.435	—
Average pps	30.9	30.9	—
Average packet size, B	601	601	—
Bytes	4400914	4400914 (100.0%)	0
Average bytes/s	18 k	18 k	—
Average bits/s	148 k	148 k	—

3. 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

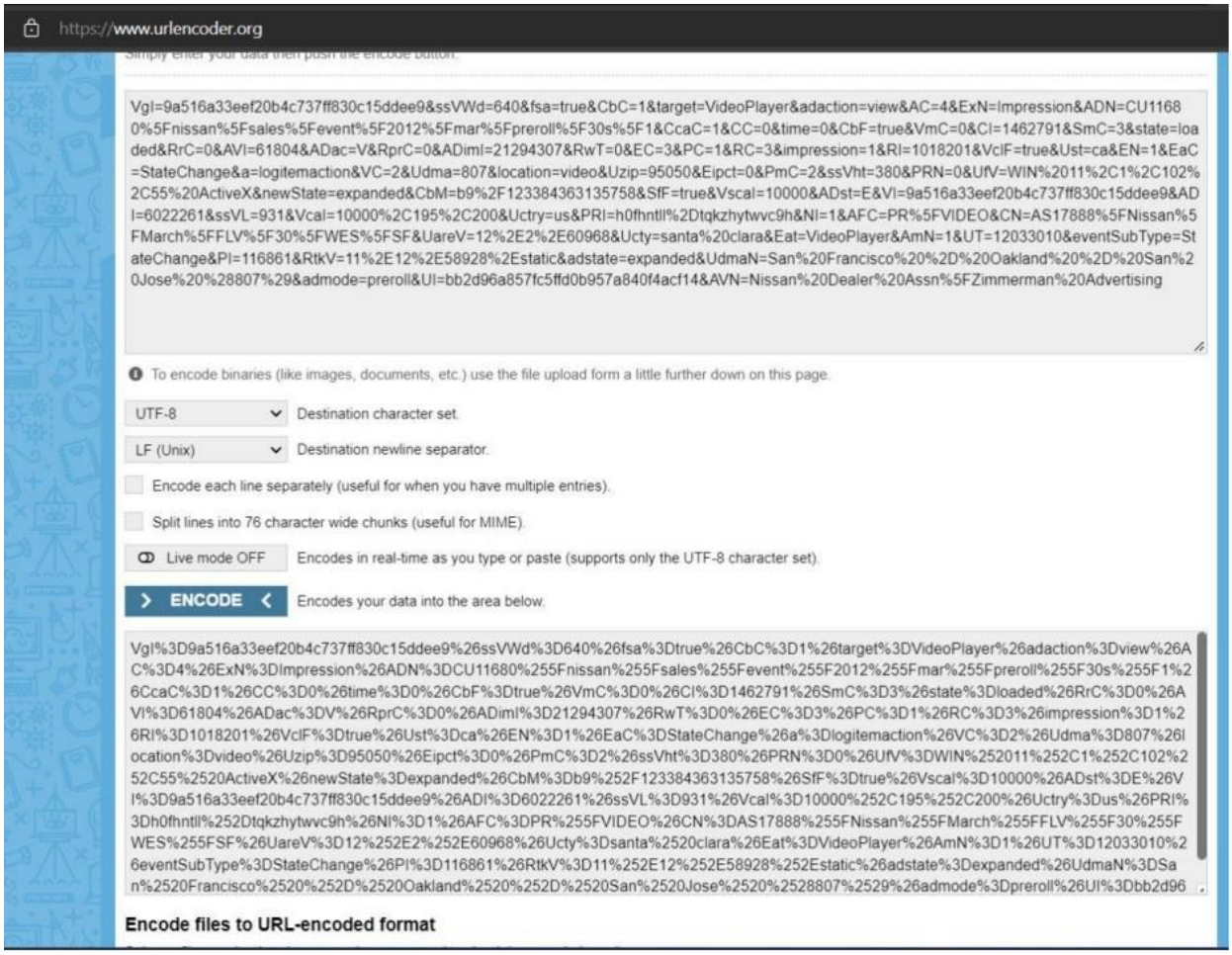


4. What location information is contained in the POST toscanscout.com?
Answer: San Francisco – Oakland – San Jose
First find the POST request, and there are only three of them, and next we have to find which request header contains the scanscout.com. We checked out all three requests and found one of the request headers is for scanscout.com.

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



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.



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

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

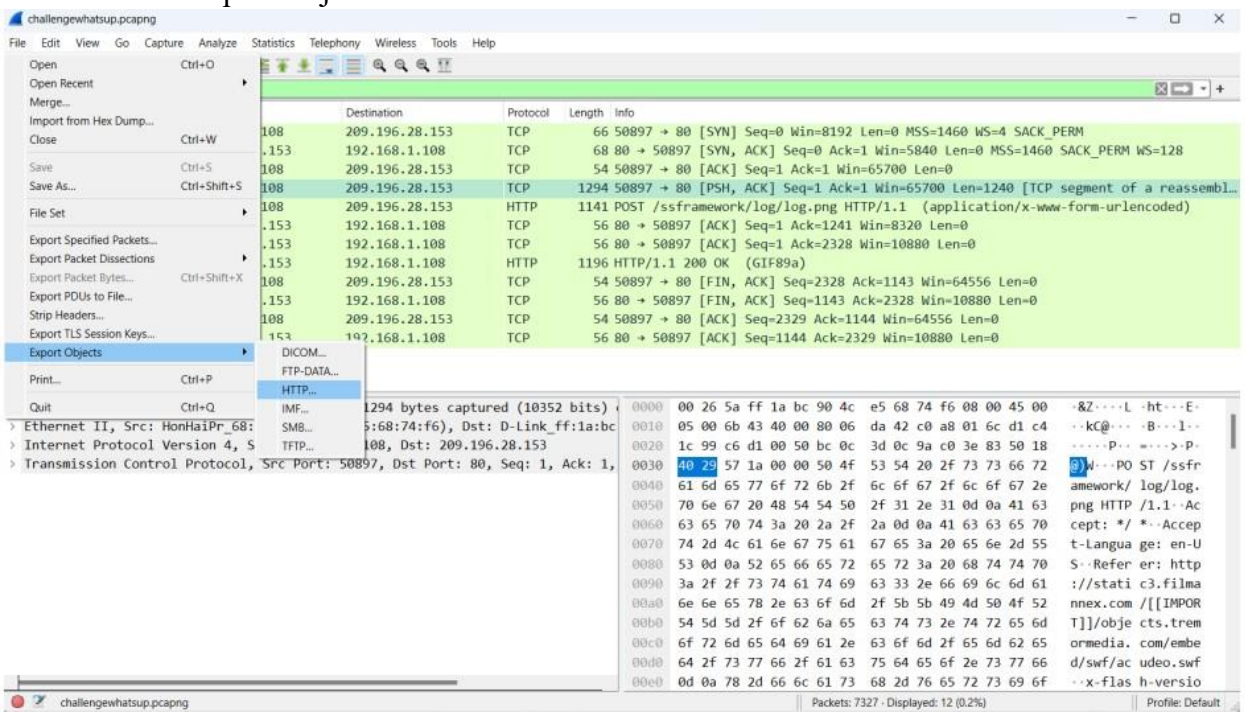
Answer: Internet Explorer 9
It can be done by analyzing the User-Agent string of any GET/POST request

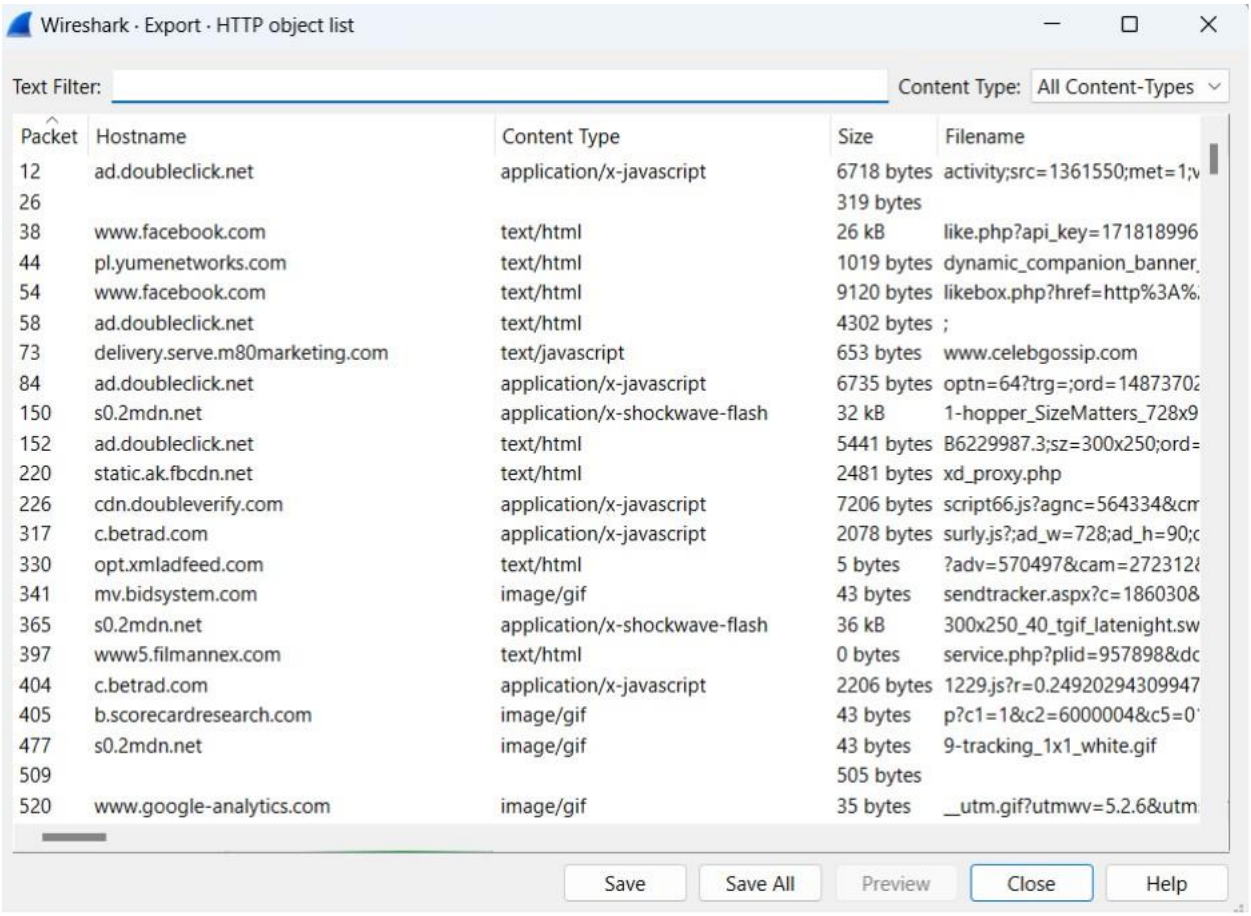
```
POST /ssframework/log/log.png HTTP/1.1
Accept: */*
Accept-Language: en-US
Referer: http://static3.filmannex.com/[[IMPORT]]/objects.tremormedia.com/embed/swf/acudeo.swf
x-flash-version: 11,1,102,55
Content-Type: application/x-www-form-urlencoded
Content-Length: 1087
Accept-Encoding: gzip, deflate
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)
```

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

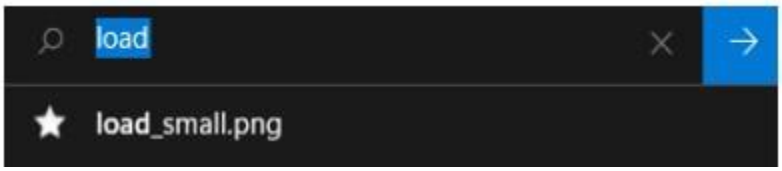
Answer: Star

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





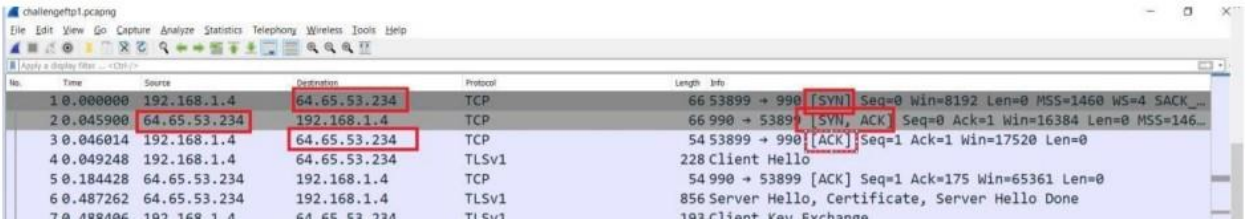
we don't know where this load_small.png file is located in which hostname, so that's why we will save all. We saved all files in a directory and searched for the load_small.png file and we found that file load_small.png.It is a star shape.



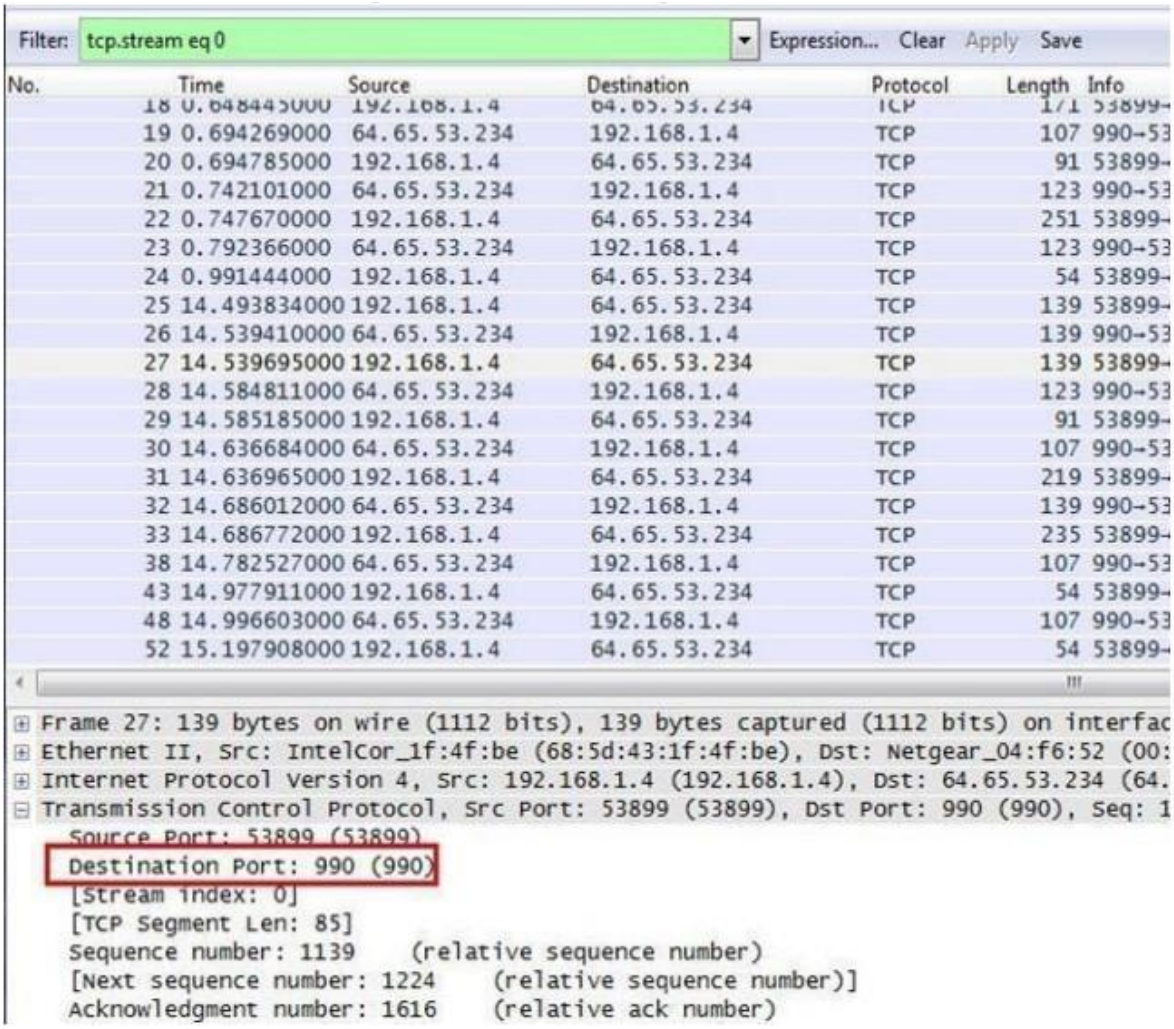
FTPS ANALYSIS TRACE FILES: challengeftp1.pcapng challengeftp2.pcapng
BACKGROUND: A customer needed a secure file transfer application put in place. These two trace files illustrate the separate options they have tested – implicit FTPS and explicit FTPS.

QUESTIONS:

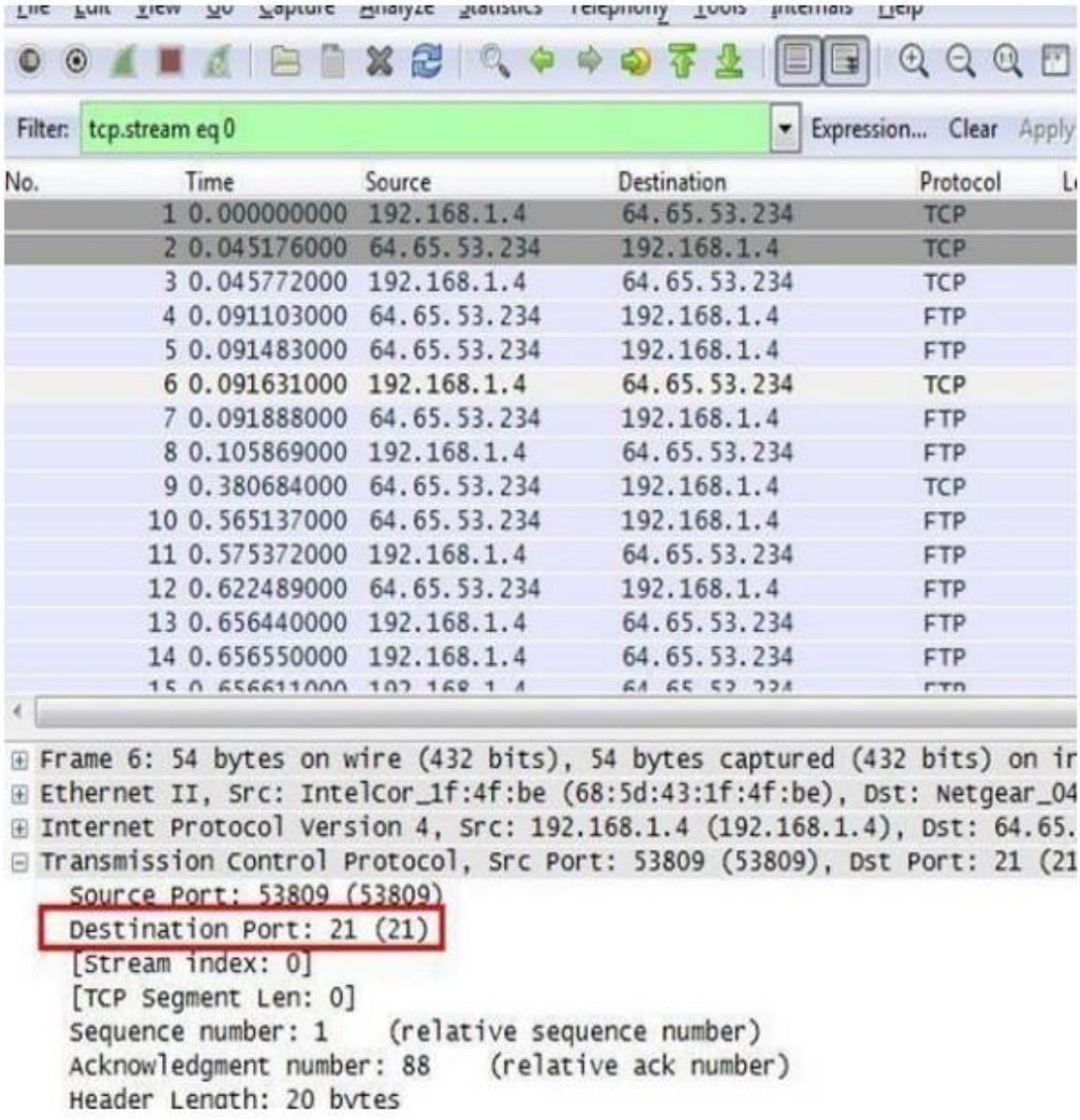
1. What is the IP address of the server?
Answer: 64.65.53.234



2. Which trace illustrates implicit FTPS?
Answer: challengeftp1.pcapng, implicit FTPS is a secure connection and it runs on port 990

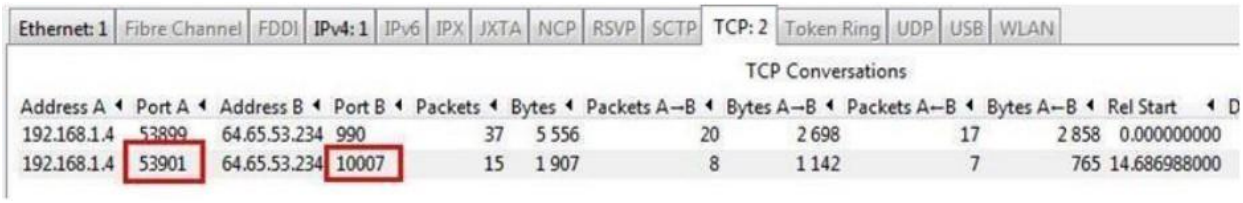


3. Which trace illustrates explicit FTPS?
Answer: challengeftp2.pcapng (explicit FTPS runs on port 21)



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

5.What port numbers are used for the data connection in each trace file?
Answer: 53901-10007

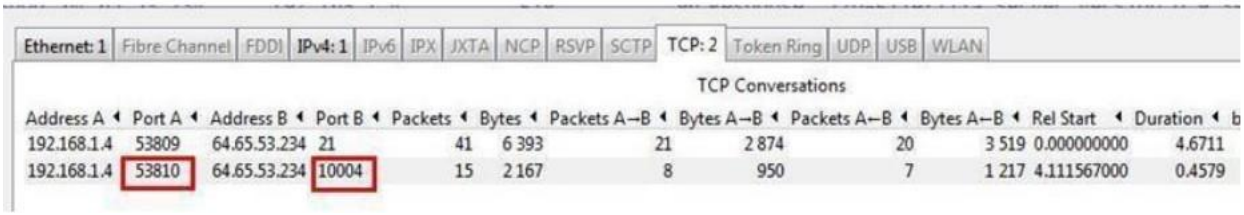


Ethernet: 1 | Fibre Channel | FDDI | IPv4: 1 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 2 | Token Ring | UDP | USB | WLAN

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



Ethernet: 1 | Fibre Channel | FDDI | IPv4: 1 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 2 | Token Ring | UDP | USB | WLAN

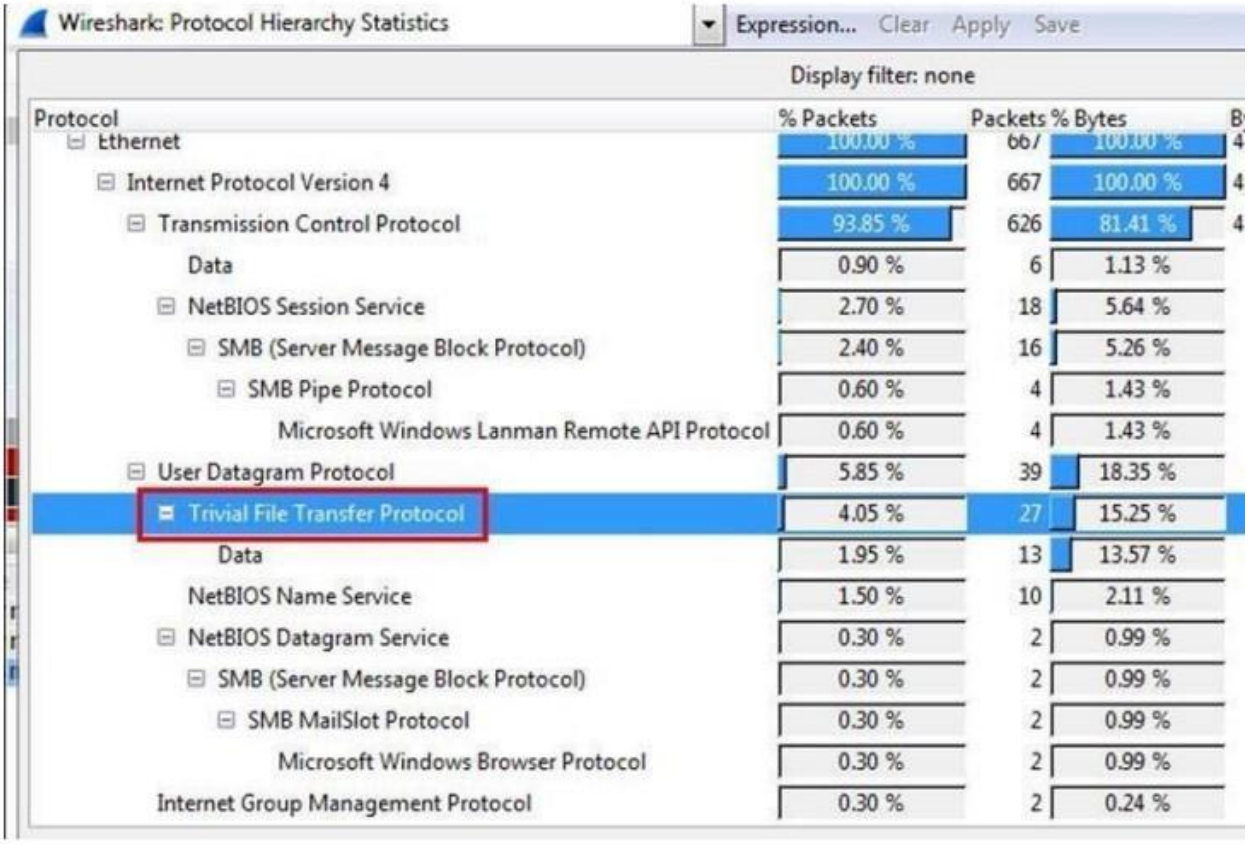
TCP Conversations

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	

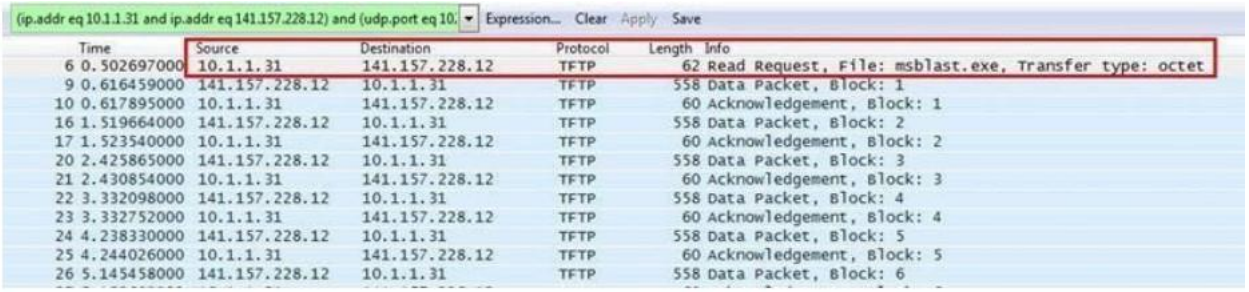
OUCH! TRACE FILE: challengeattack.pcapng
BACKGROUND: These capture files were taken from a network that was experiencing a "zero- day" attack and was completely overwhelmed. It is also reported that some of the nodes within the network appear to be unable to update their antivirus/security software. 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:

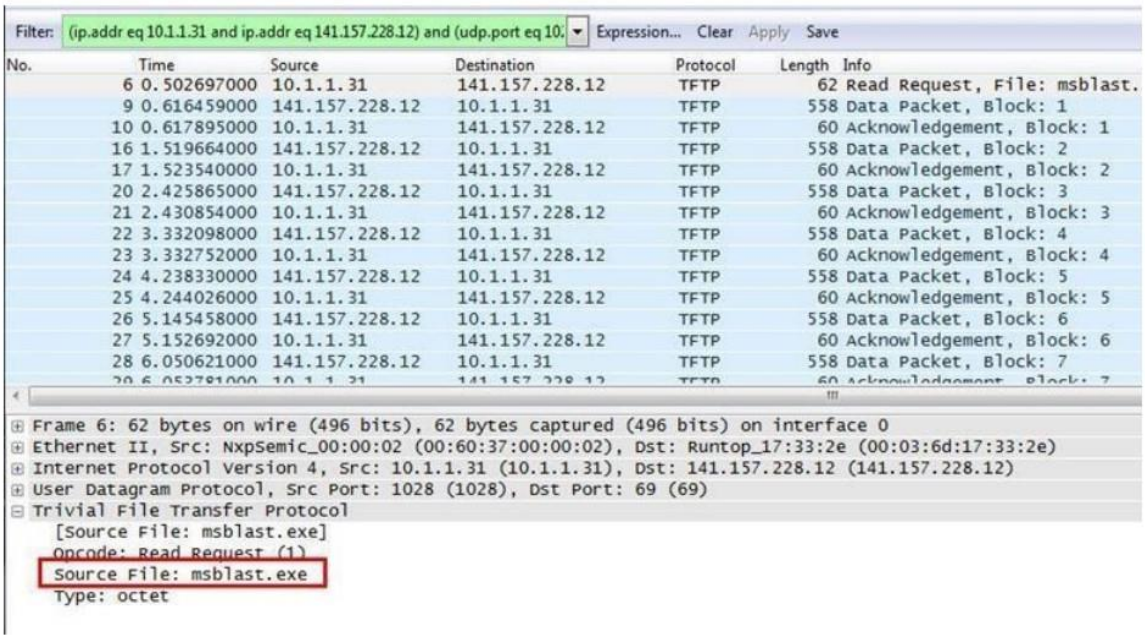
1. What file transfer application is seen in this trace file?
Ans: Trivial File Transfer Protocol
Go to Statistics and then select Protocol Hierarchy which will show all protocols used in this trace file.



2. What is the IP address of the host that is receiving the file?
Answer: 10.1.1.31



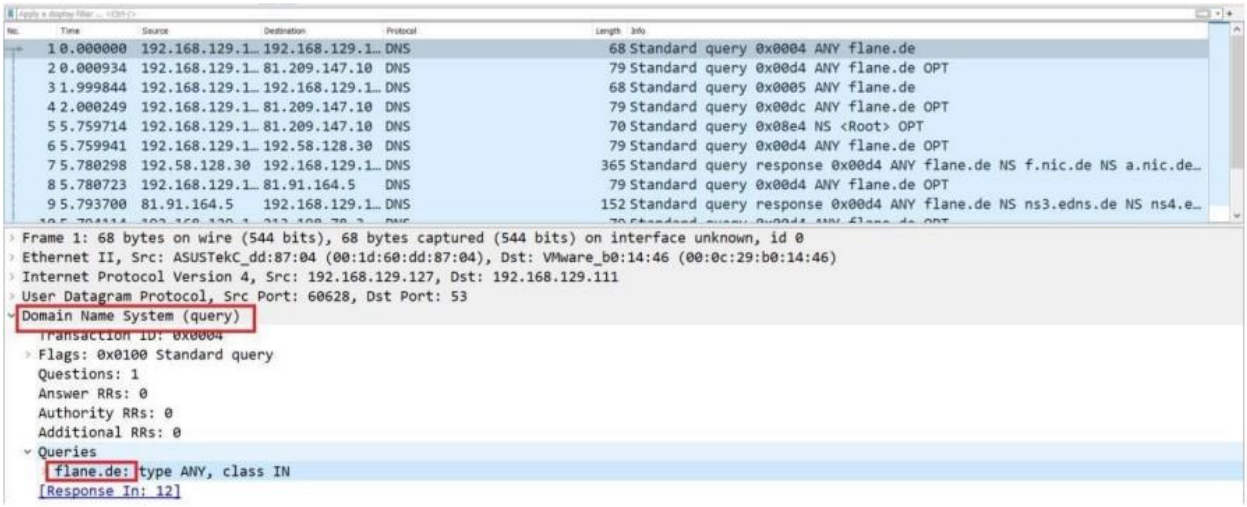
3. What is the name of the file that is being transferred?
Answer: mblast.exe



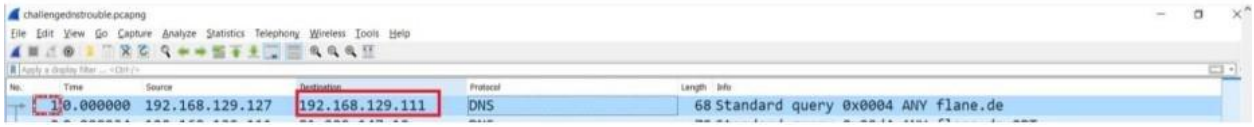
DNS TROUBLE TRACE FILE: challengednstrouble.pcapng
BACKGROUND: After a maintenance window on the day before, when several servers had been upgraded to a newer operating system, a lot of trouble tickets have come in. Users complain that connecting to web sites and other services takes a long time now, 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:

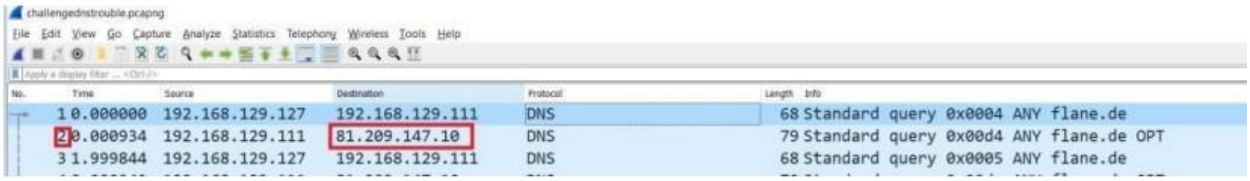
1. What FQDN is the client attempting to resolve?
Answer: flane.de



2.To what IP address is the first recursive DNS query sent? Ans: 192.168.129.111.



3. To what IP address is the second recursive DNS query sent?
Answer: 81.209.147.10

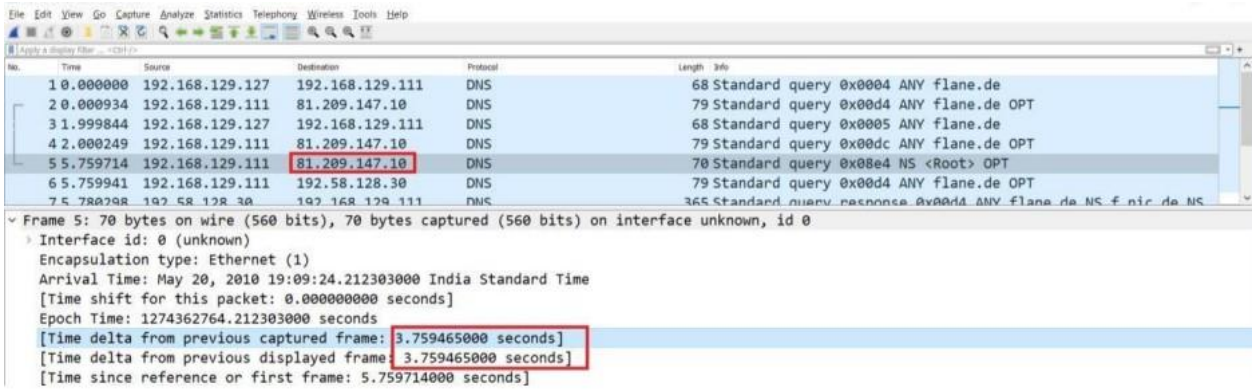


4. The trace file includes authoritative DNS servers responsible for whattop level country code domain?

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

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

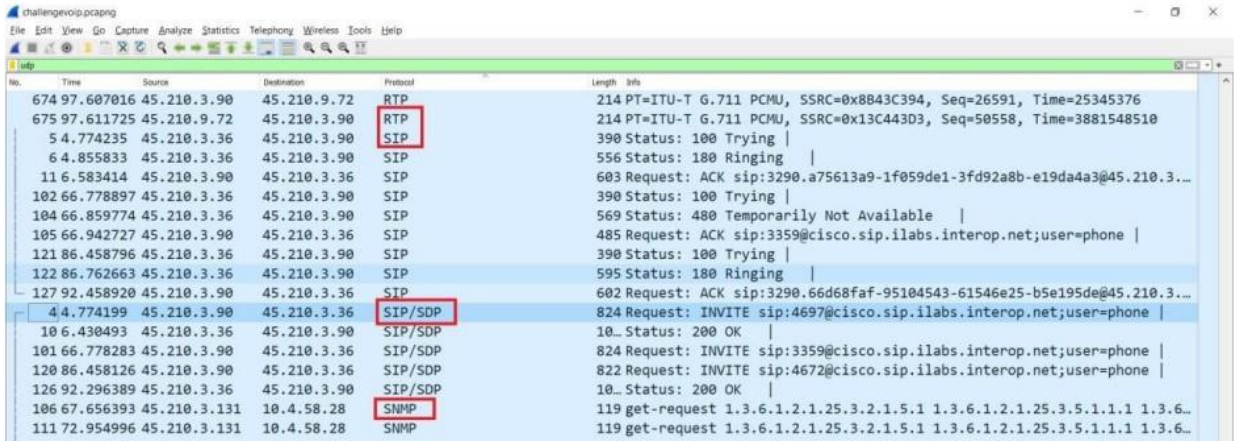
Answer: 81.209.147.10



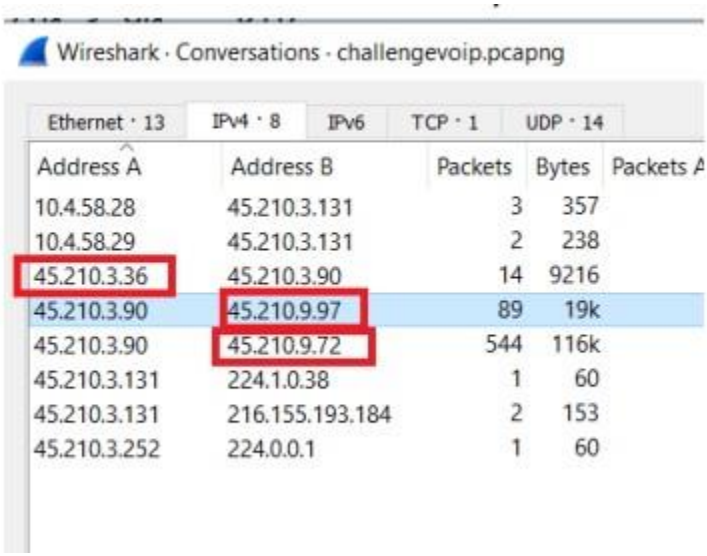
VOIP RECONSTRUCTION TRACE FILES: challengevoip.pcapng
BACKGROUND: This captured file was collected from a recently installed VoIP network that is experiencing performance issues, and you have been asked to evaluate it and recommend corrective action.

QUESTIONS:

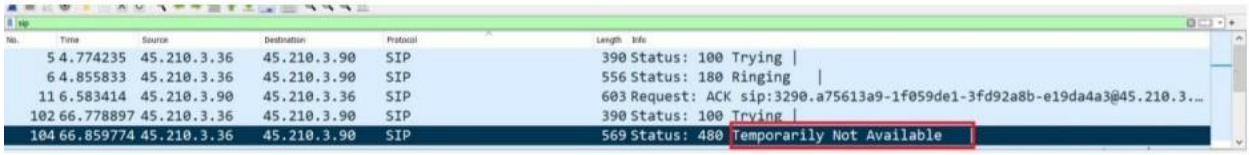
1. What three UDP-based protocols are used for the VoIP call and call setup?
Answer: SIP, SDP, RTP, SNMP



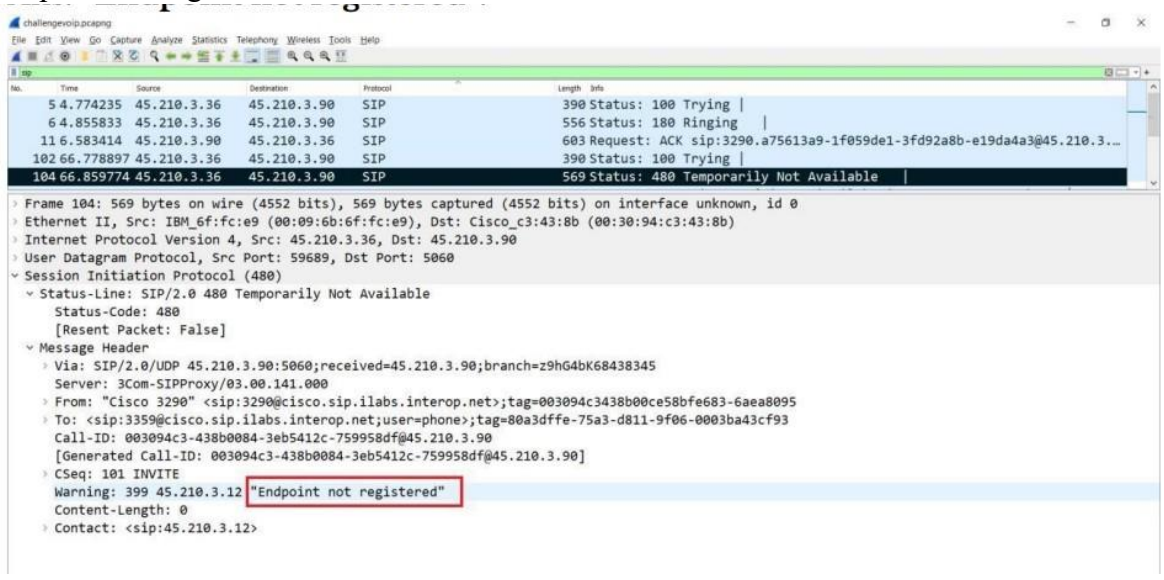
2.With what three IP addresses is 45.210.3.90 communicating?
Answer: 45.210.3.36, 45.210.3.97, 45.210.3.72



3.What SIP error code is seen in this trace file?
Answer: Error code 480



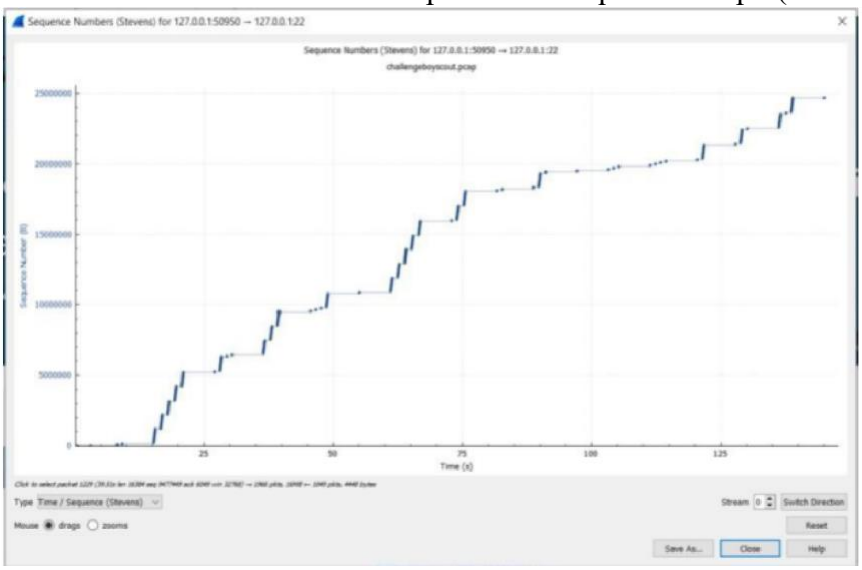
4.What is the stated cause of this SIP error? Ans:
“Endpoint not registered”.



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).



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

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