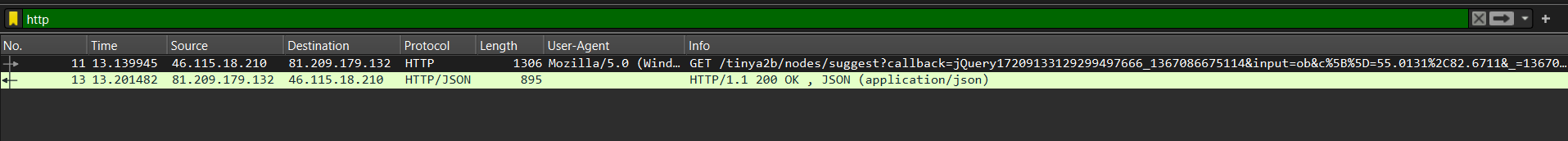
**1. TROUBLE TICKET Trace File: TroubleTicket.pcapng**

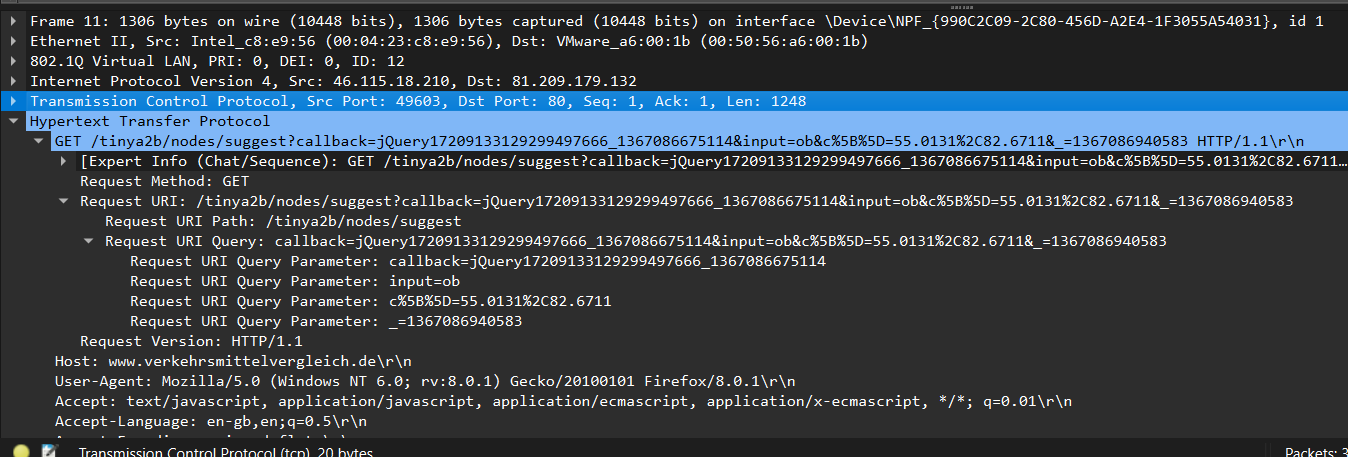
1. What is the application protocol used?

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.



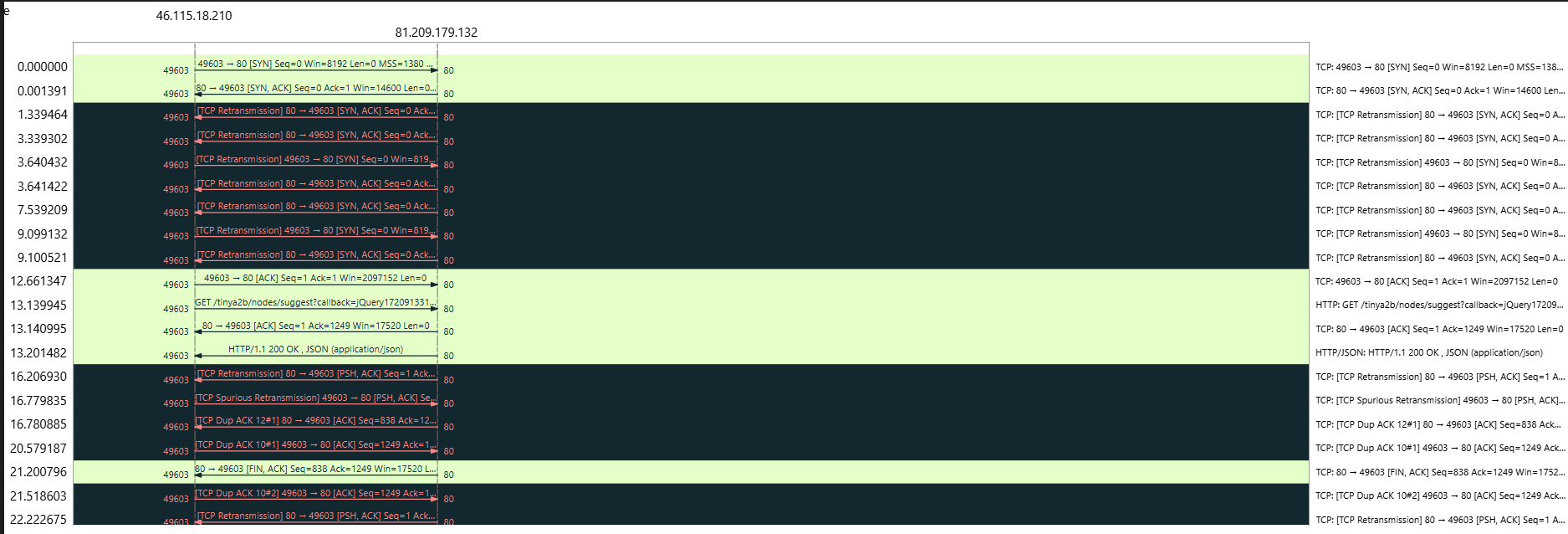
2. Are all GET requests asking for the same URI?

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.



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.



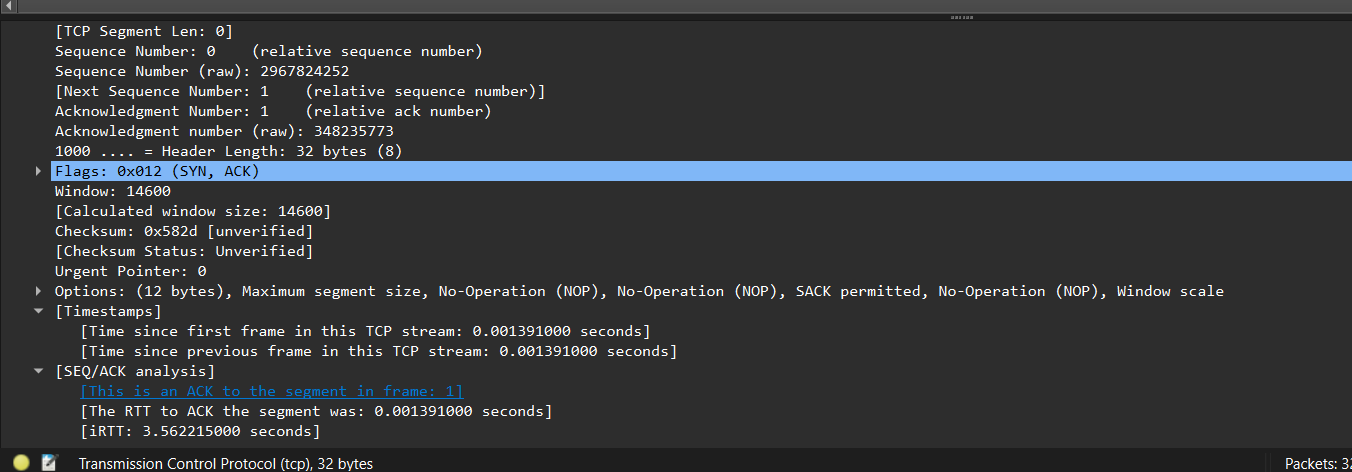
4. This trace was taken inside the infrastructure. What is the Initial Round Trip Time of the connection?

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]

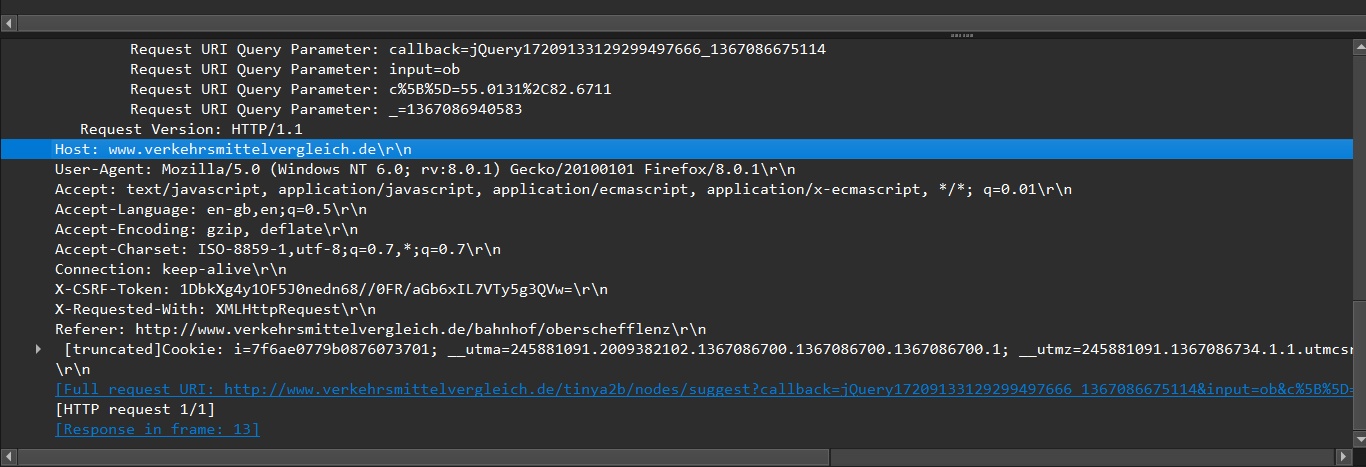
[iRTT: 3.562215000 seconds]



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](http://www.verkehrsmittelvergleich.de\r\n)

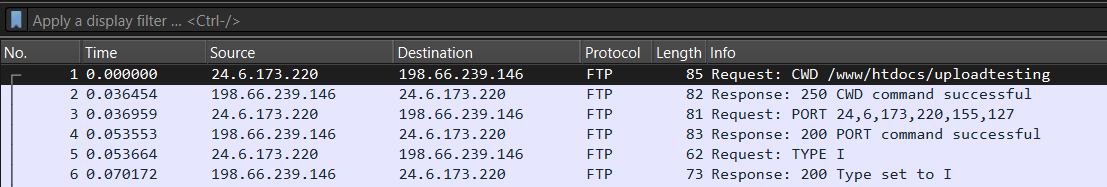




**2. BIG FTP Trace File: BigFTP.pcapng**

* 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

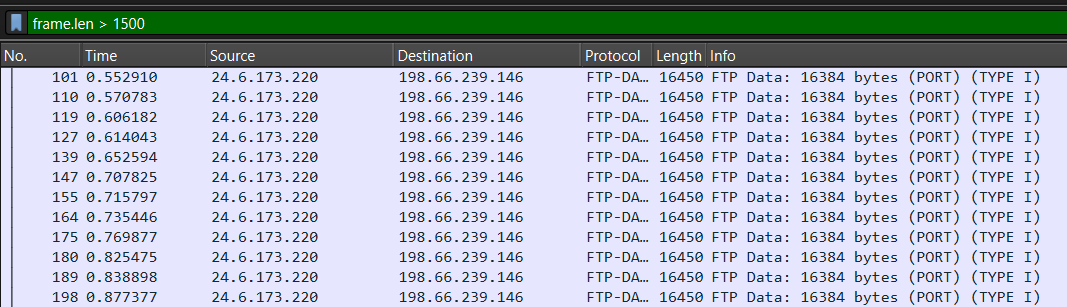
0.00000 seconds and the second packet comes with the response in 0.036454000 seconds later, again the third packet is going with FTP command in 0.000505000 seconds, the request time is too fast, which means Wireshark is running on client’s system.



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

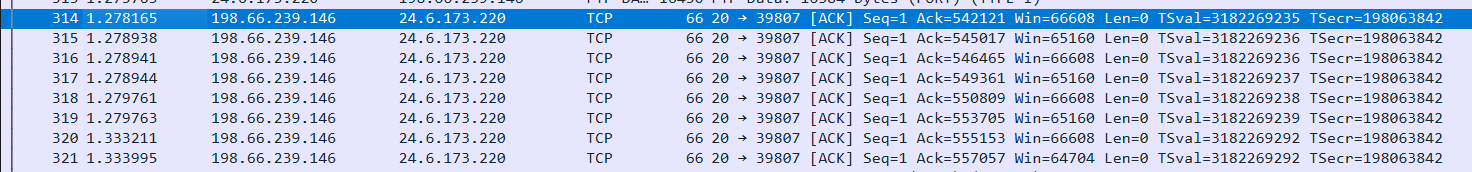
Answer: We first sorted the length column, now we can see all 16450 byte packets. This, size of packet is supported by something called Large Segment Offload. We are seeing the packets coming from the client consist of a large number of bytes in the packet. The host where the trace file is taken supports 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

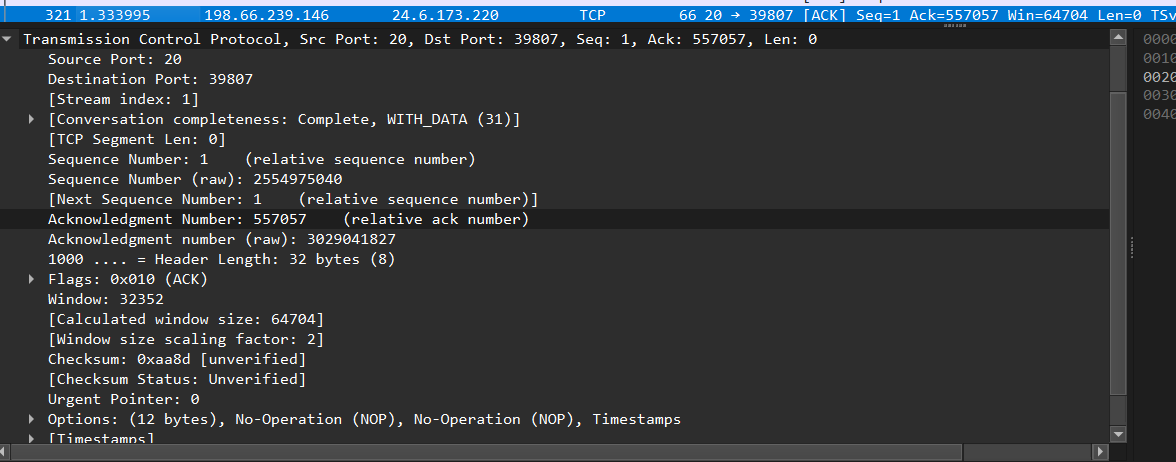


* 1. What data packet is being acknowledged in frames 314-321? Answer: Data packet 304 is acknowledged between 314-321

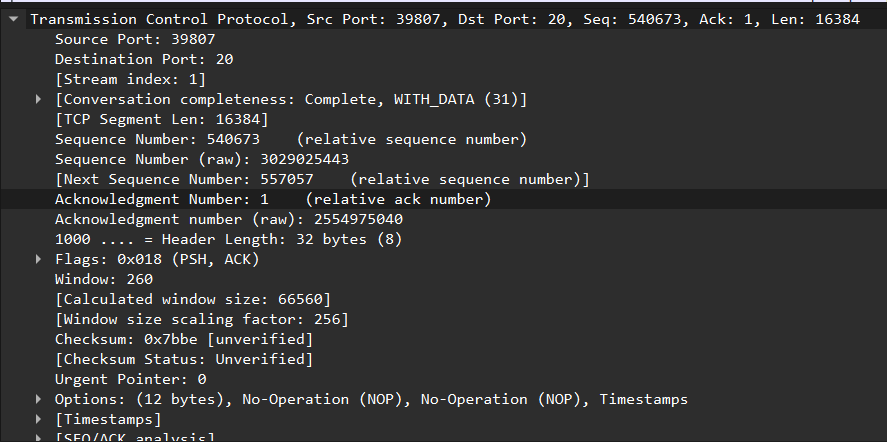
Given the packet number as can be seen below, we gave 314. Now we can see all packets between 314-321.



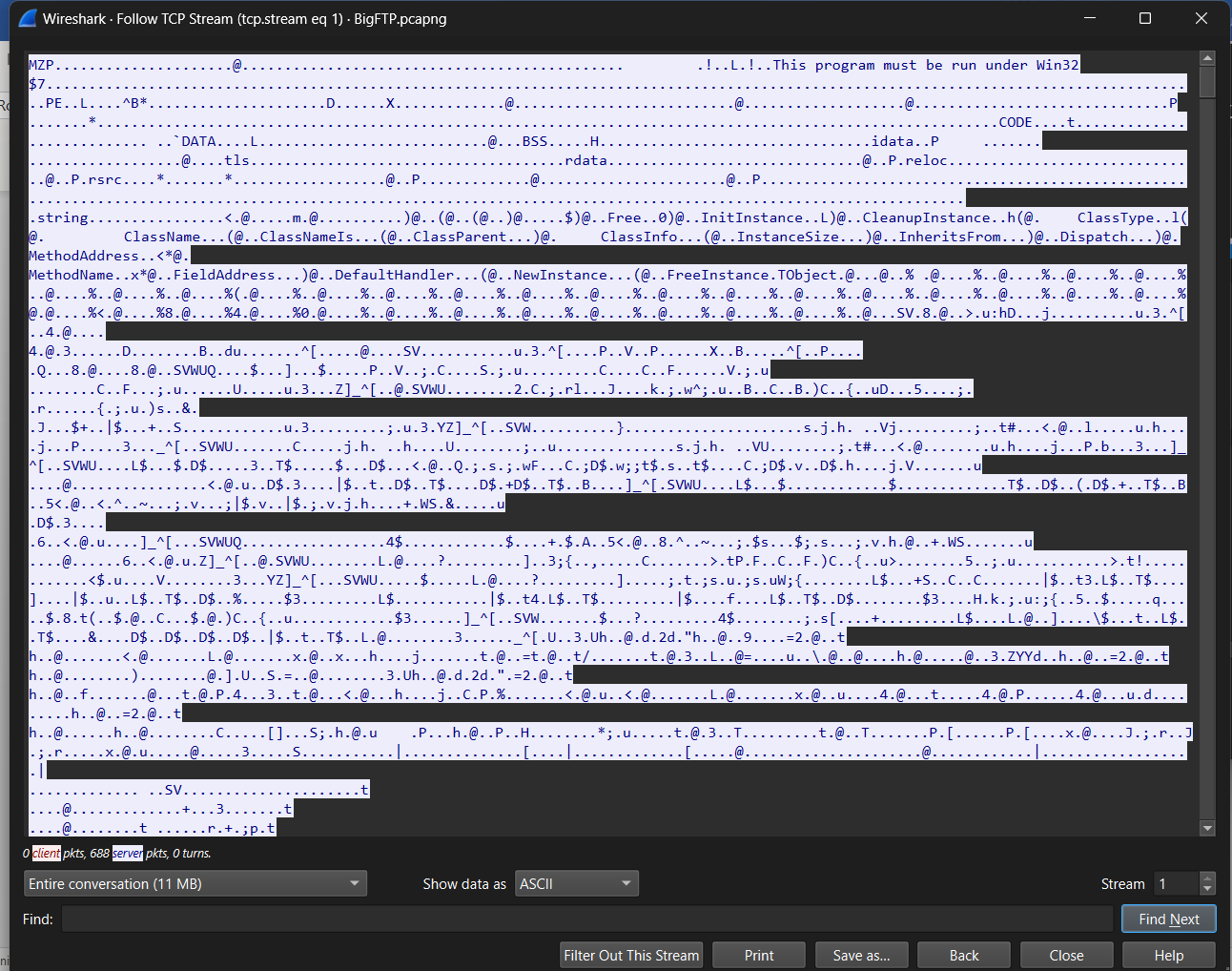
We selected the last packet 321 and expanded the TCP header for checking the ACK sequence number, which is showing 557057. Now we have to find which data packet is sending this ACK number to 321.



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.



* 1. 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.

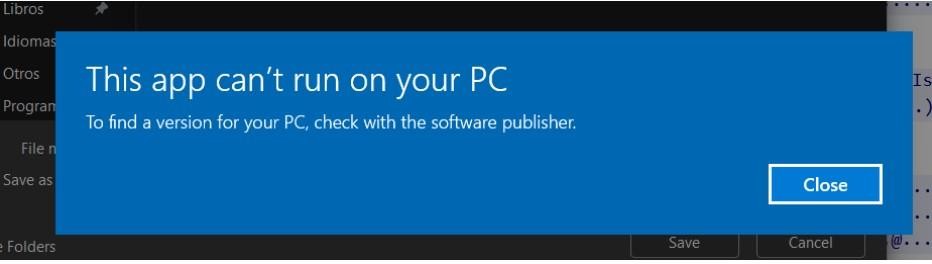
* 1. What is the true purpose of kidsatbeach.jpg?

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



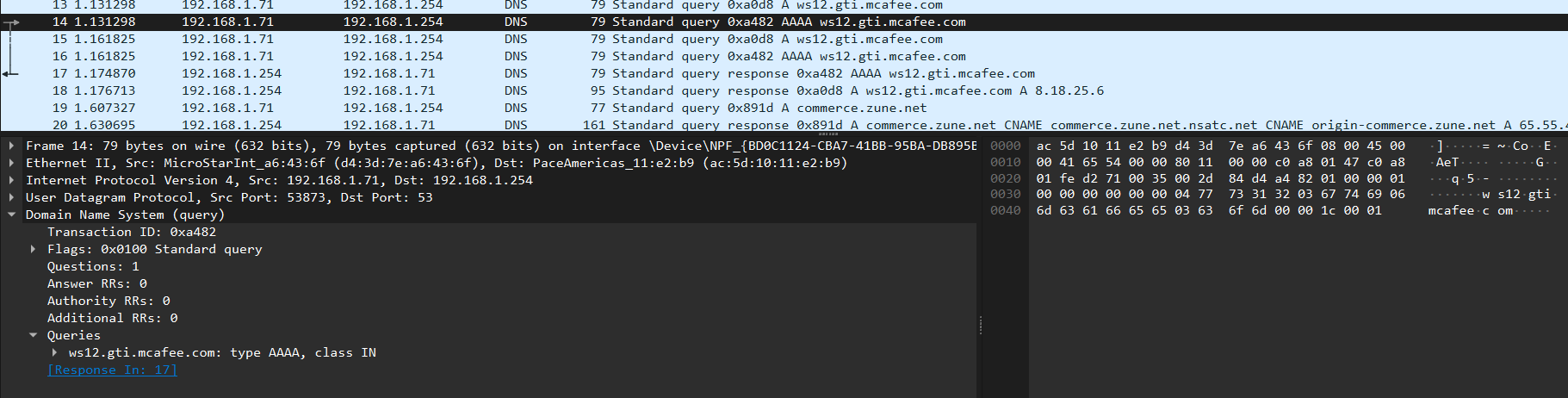
This application was not supported in Windows Operating System.



**3. PAID TO PLAY Trace File: AllPlayNoWork.pcapng**

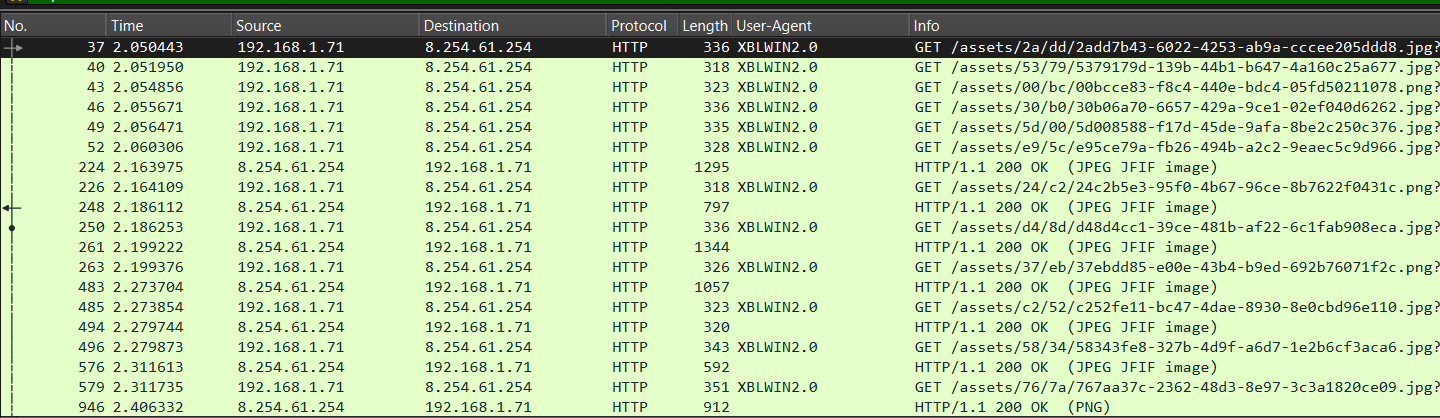
1. For what server did the client try to resolve an IPv6 address?

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



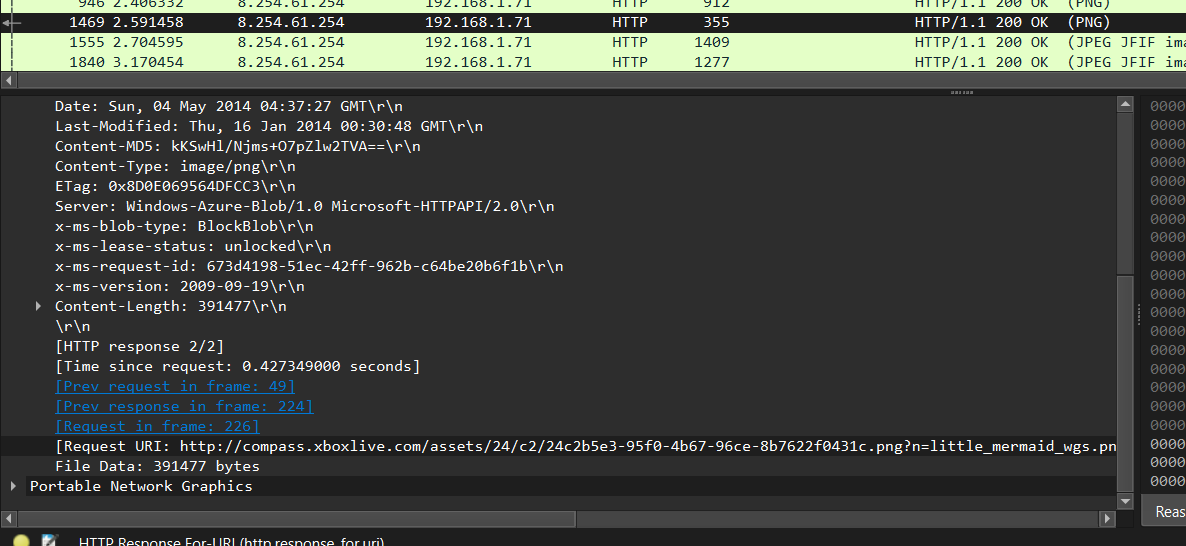
2. What operating system do you think the client is running?

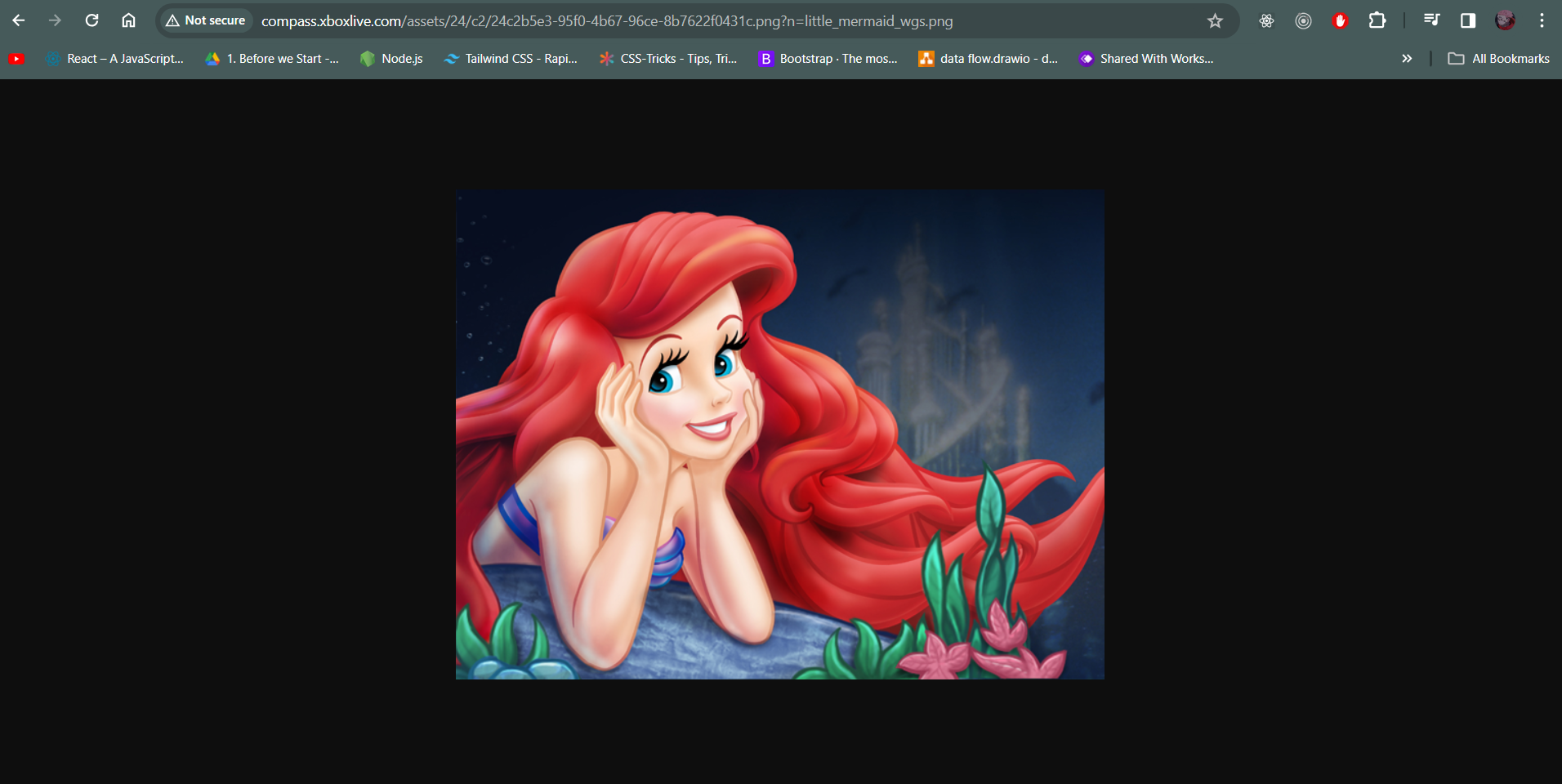
The client is running Windows 7. This can be determined by looking at the User-Agent field in the HTTP GET request, which has the value of Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729).



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.





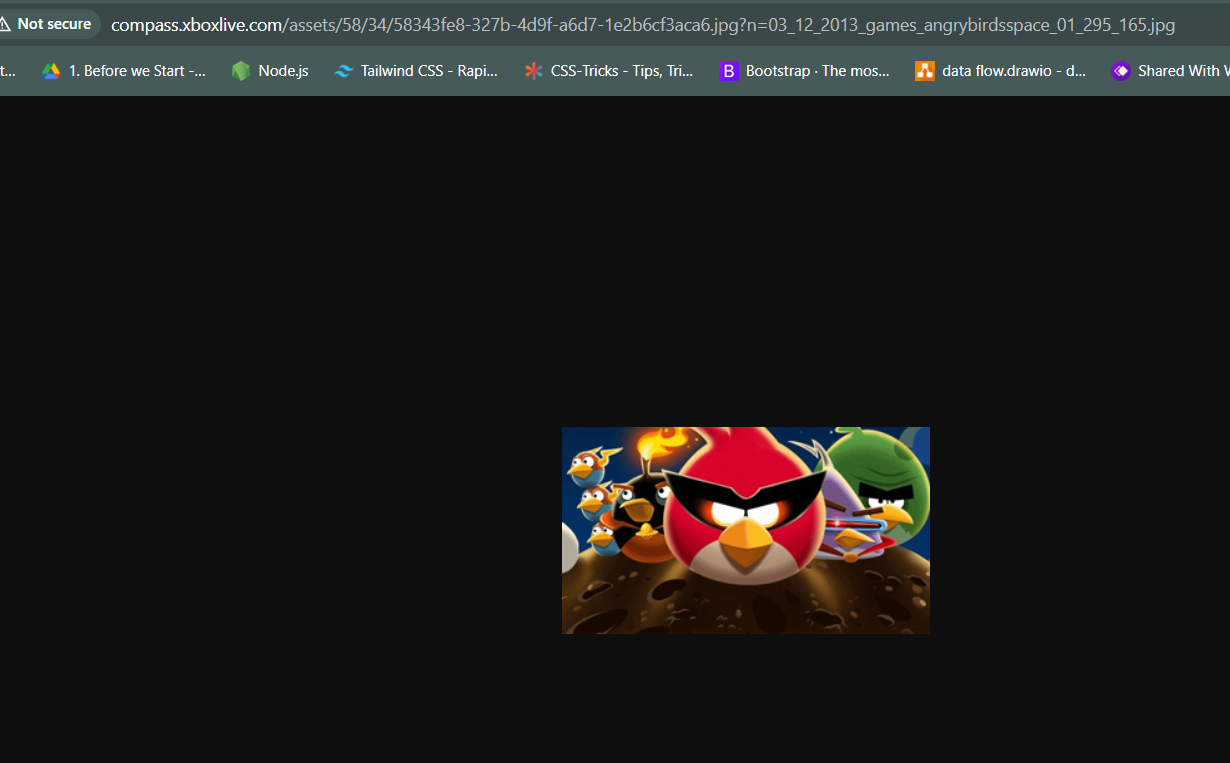
4. What classic games did the user learn about? (Name all of them.)

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.



**4. BROWSING BUDDY Trace File: BrowsingAlong.pcapng**

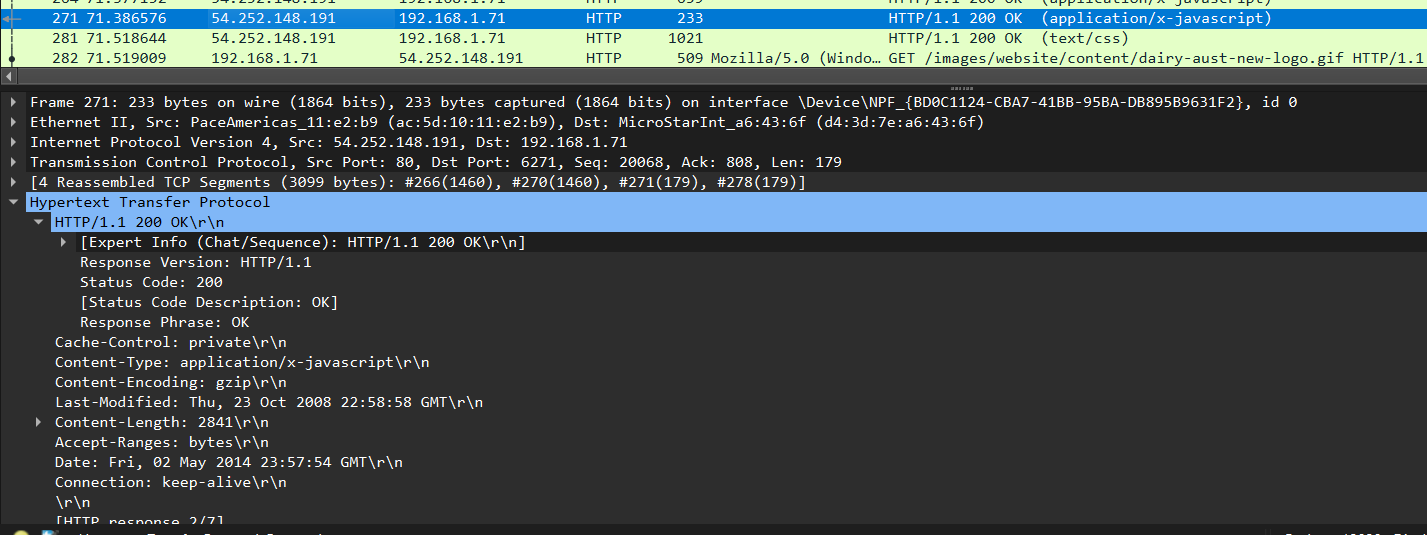
Sure, here are the answers to your questions based on the provided capture file:

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

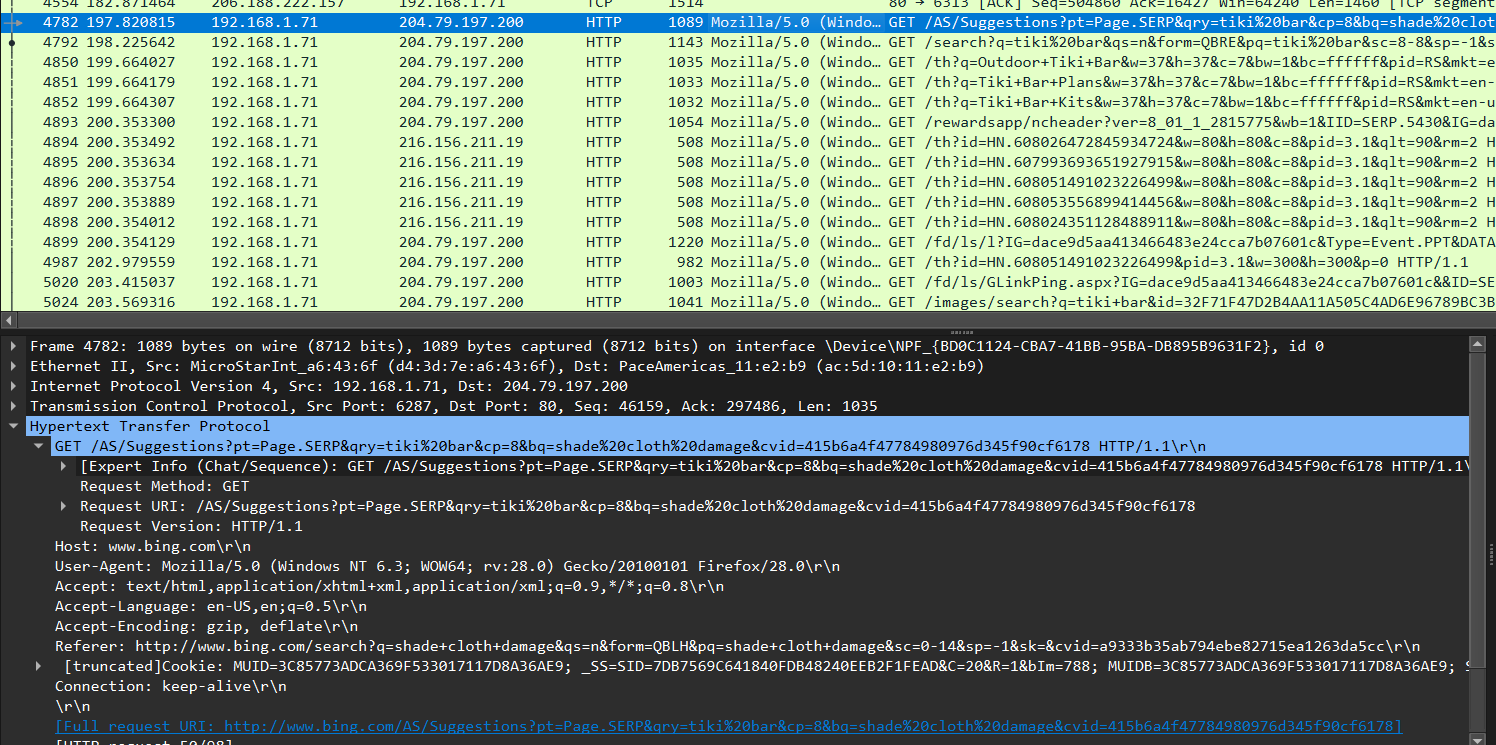
The version of dumpcap used to capture this trace file is not explicitly indicated in the capture file. However, based on the file format and capture options, it is likely that version 1.4 or later was used.

1. 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.

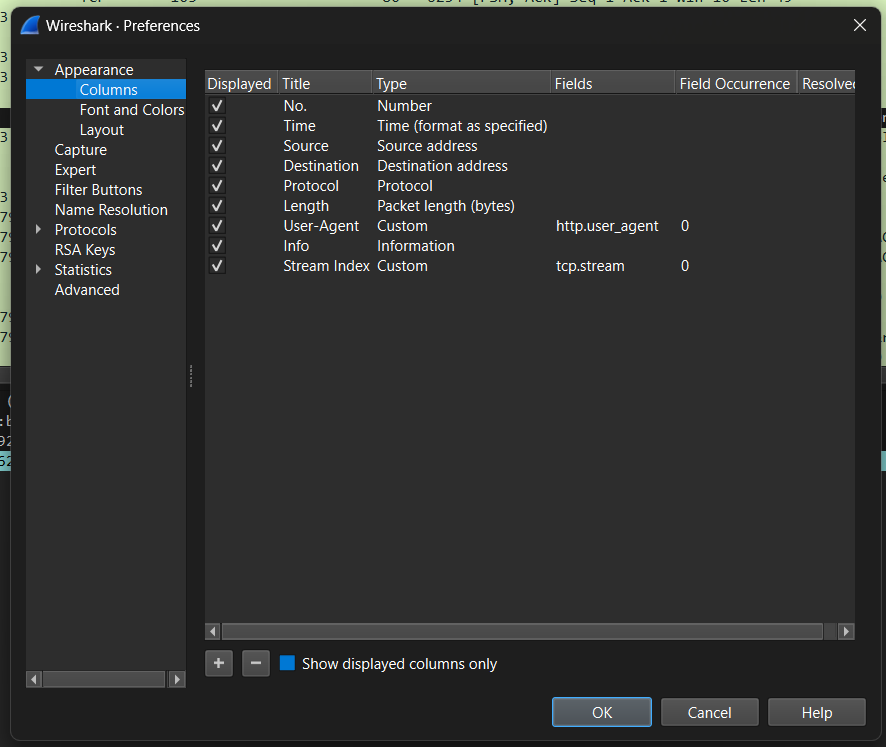


1. In what kind of “bar” is the client interested?

Tiki bar

1. 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.

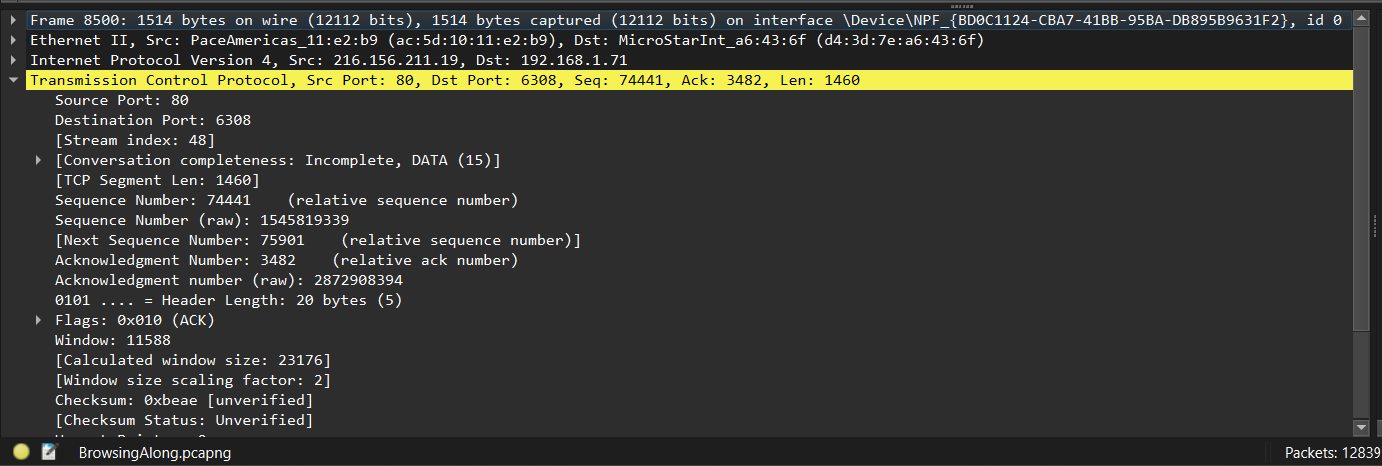


1. Frame 8500 is a retransmission triggered by duplicate ACKs. Why isn’t it marked as a Fast Retransmission?

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.

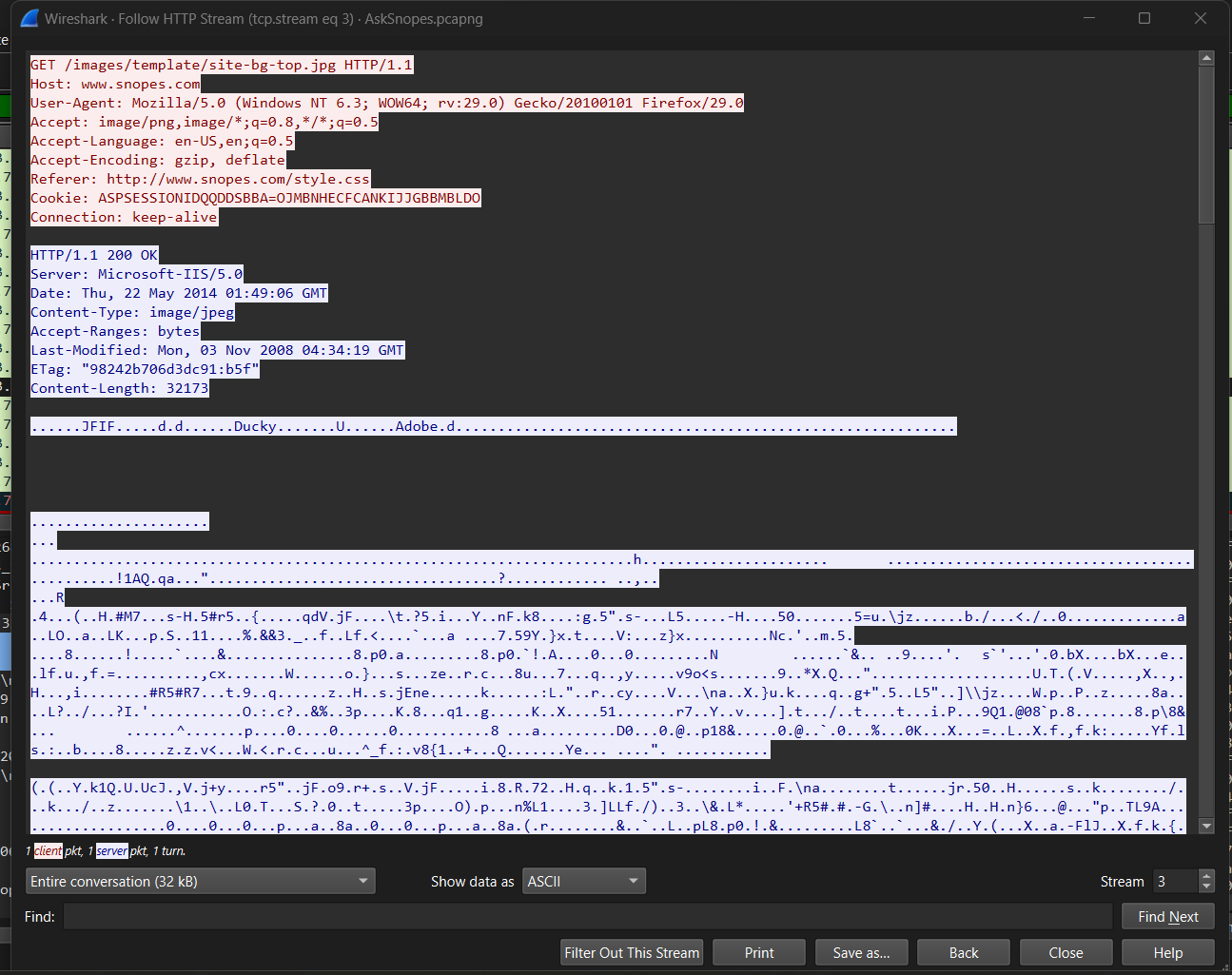
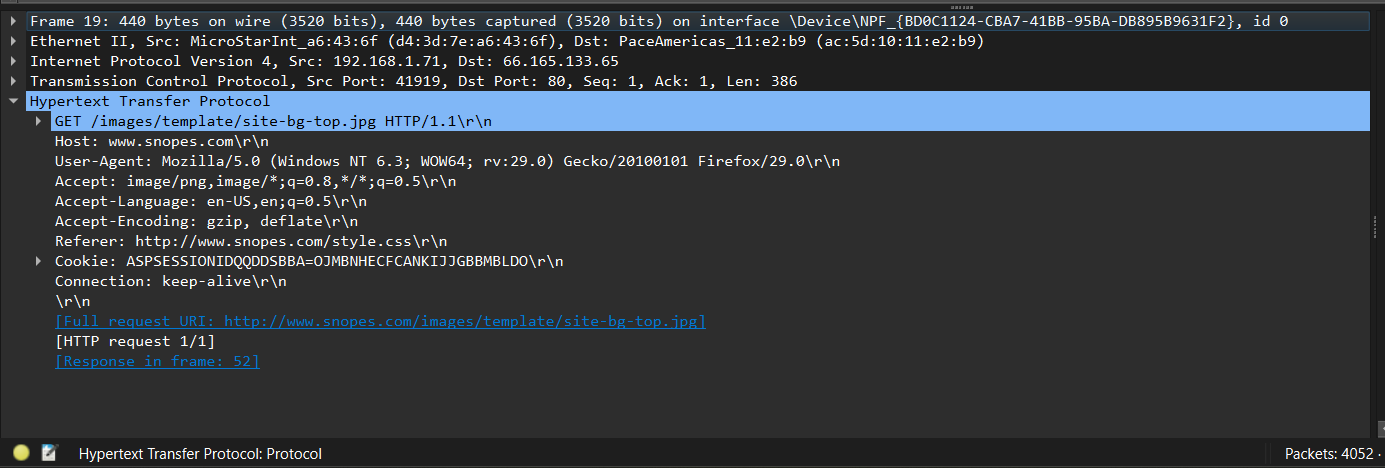


5. OUCH! Trace File: AskSnopes.pcapng

Sure, here are the answers to your questions based on the provided capture file:

1. What web server software is used by [www.snopes.com](https://www.snopes.com/)?

The web server software used by [www.snopes.com](https://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.

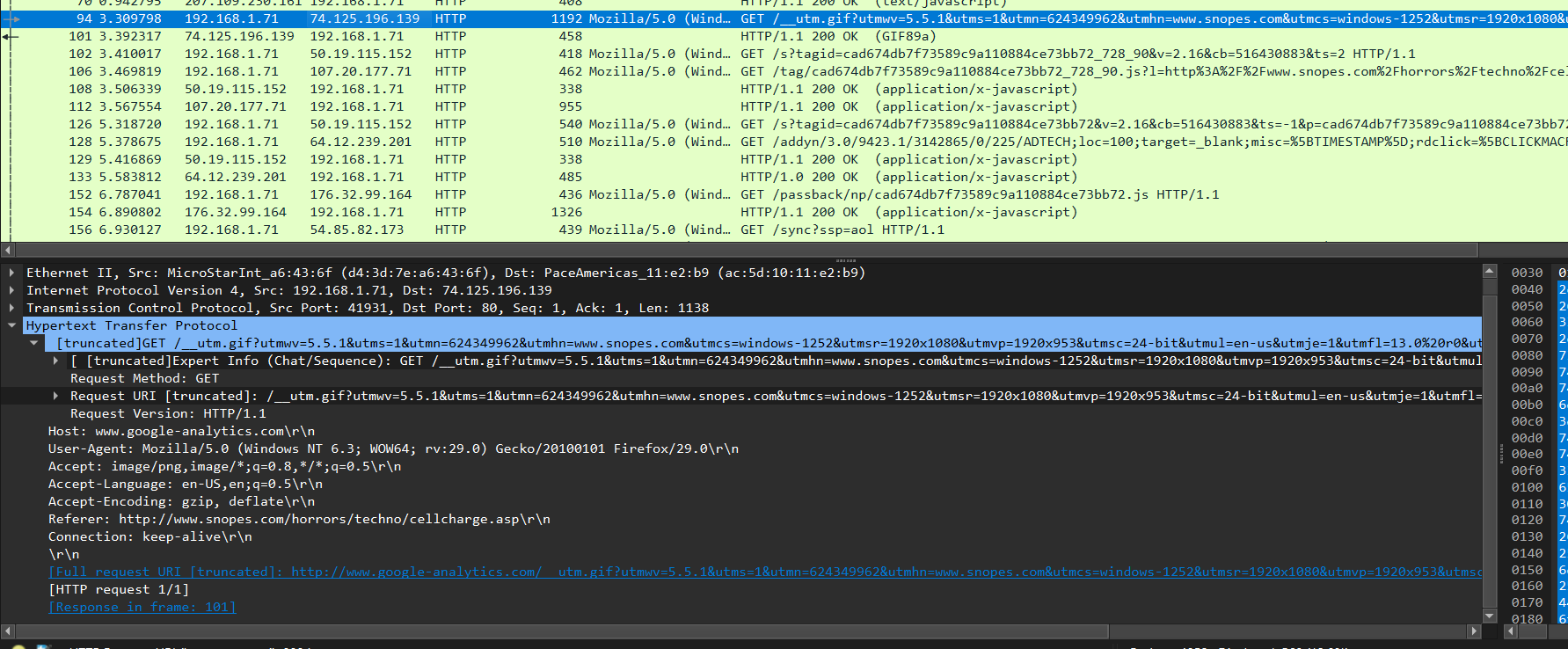


1. About what cell phone problem is the client concerned?

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."

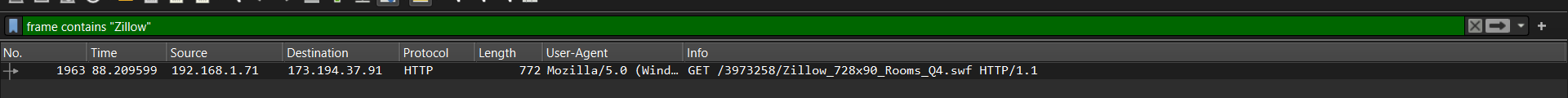
OR

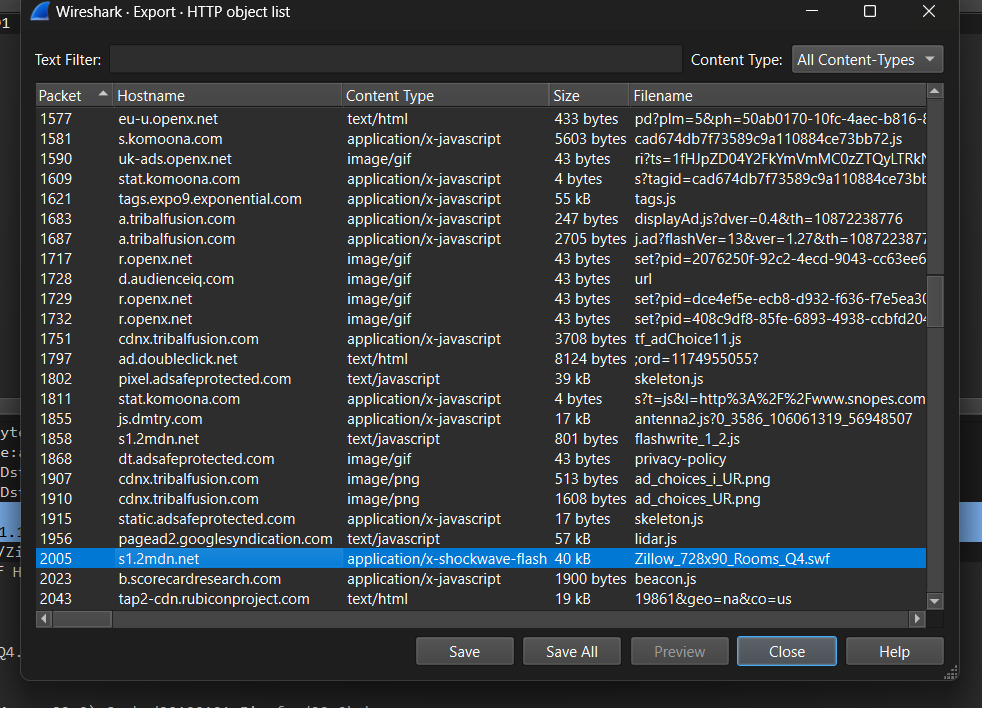
Checking for cell phone references when we see the complete URL for No 94 we can see “Cell Phone Recharging Electrocution”.



1. 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



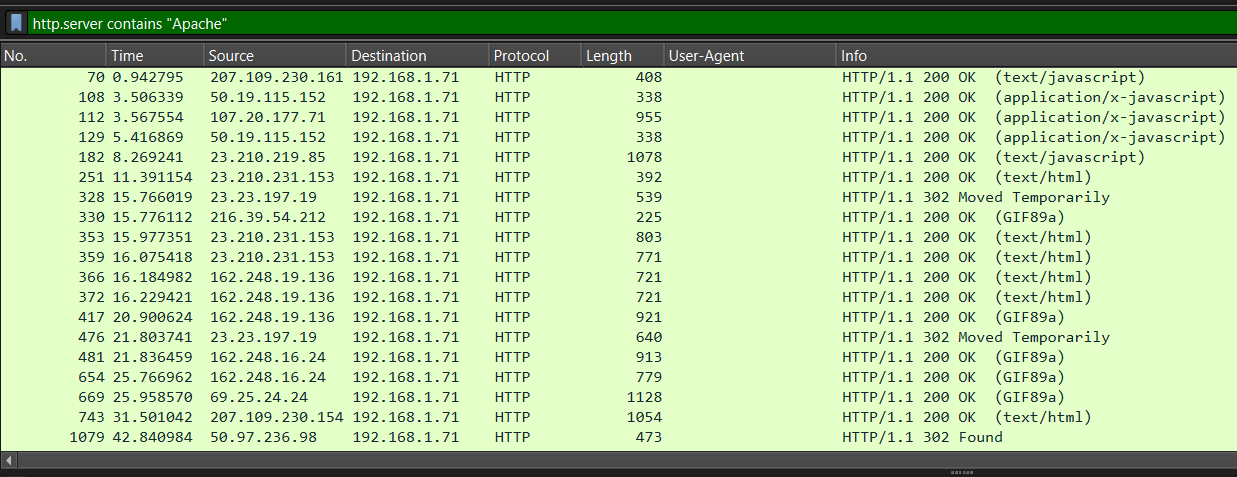




1. How many web servers are running Apache?

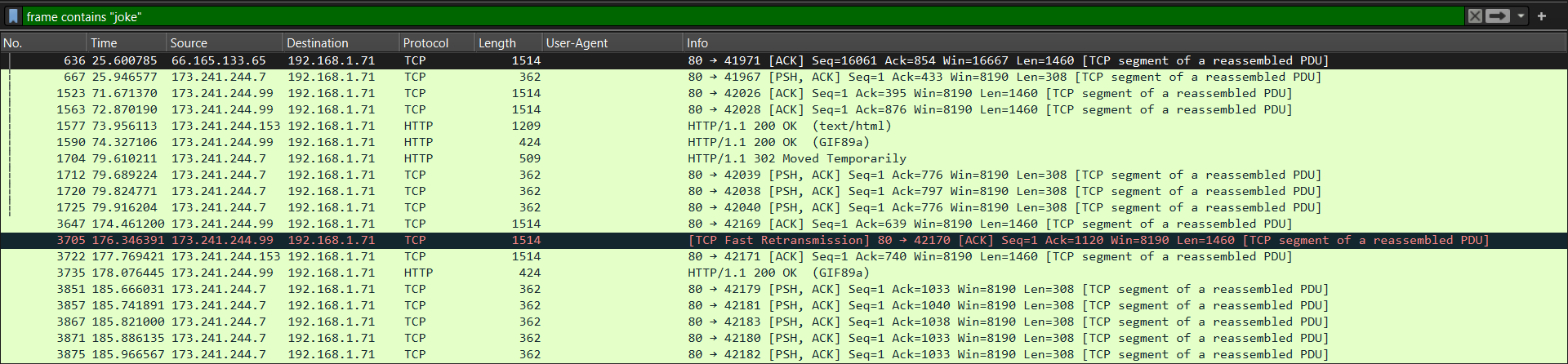
This can be determined by looking at the Server field in the HTTP responses in the trace file.

79 OR 21



1. 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."



**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