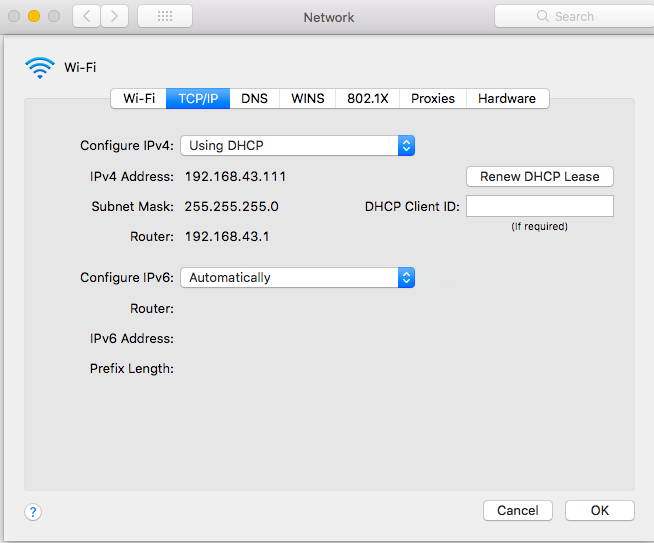
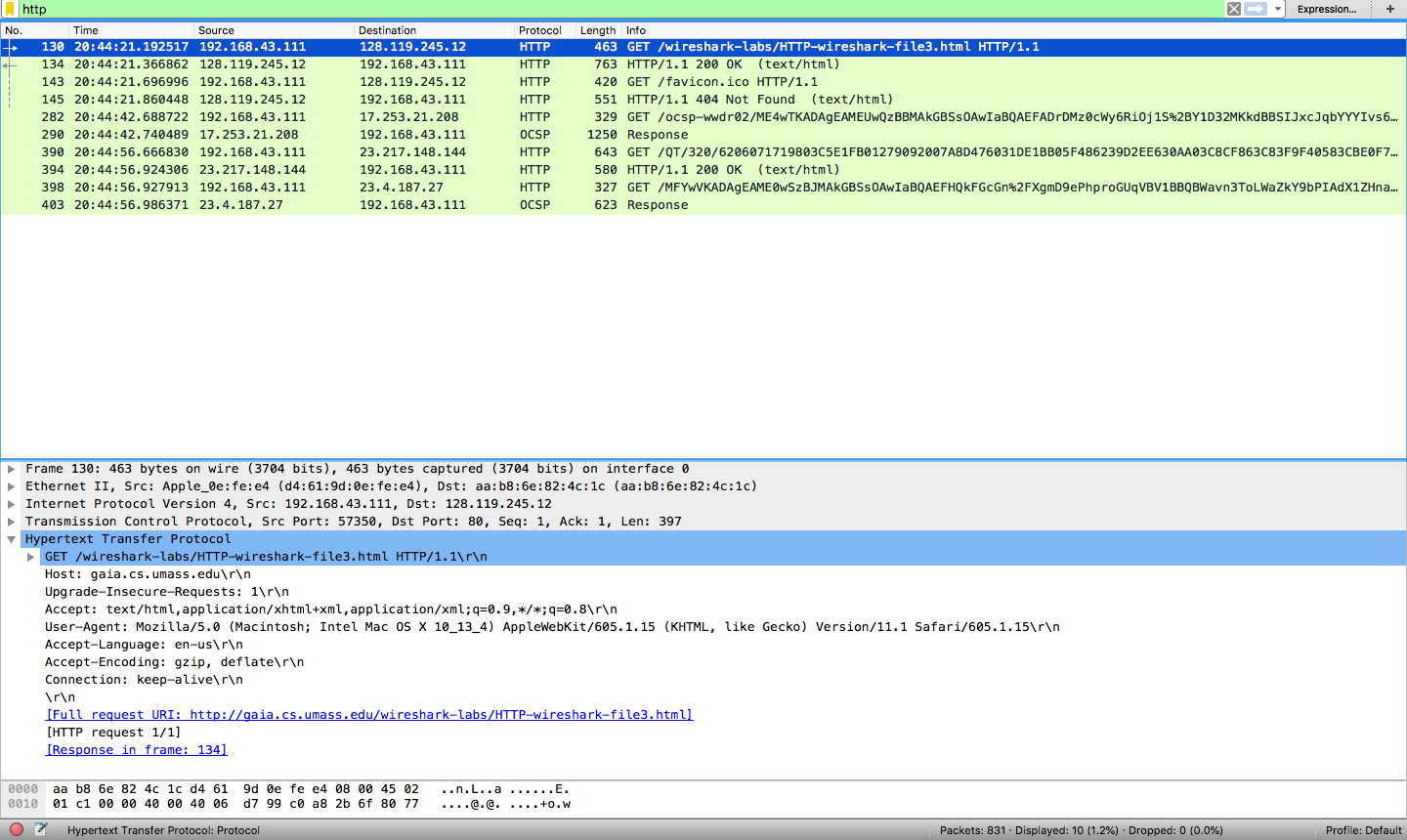
Name: Yohannes woldegerima

Final Lab



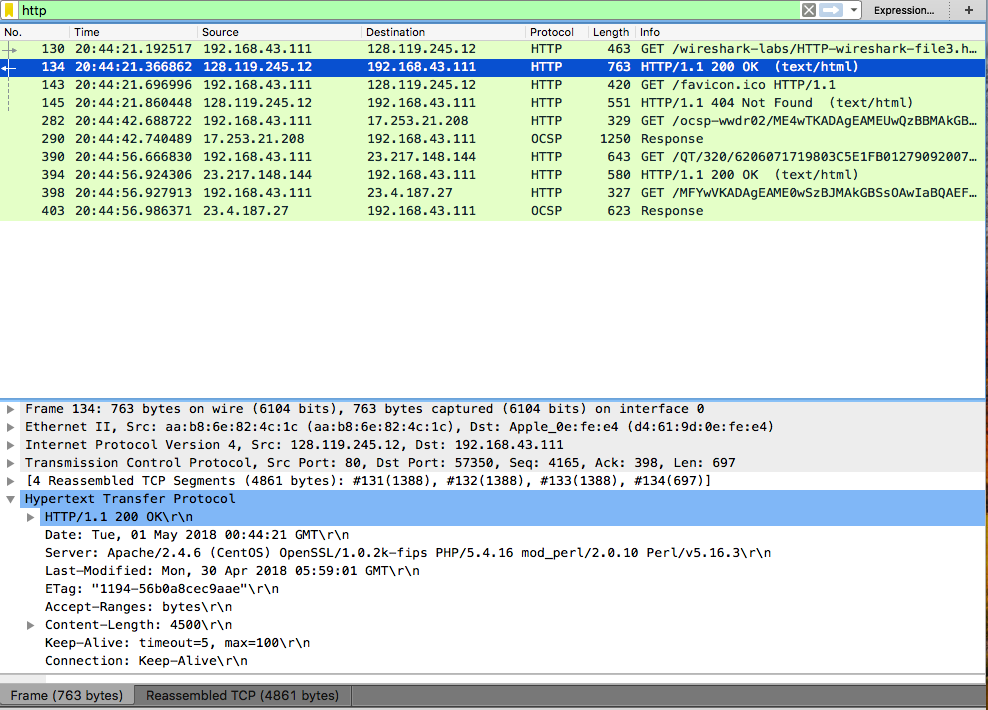
1. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

It Sent 1 GET request to the server, The packet number is 130.



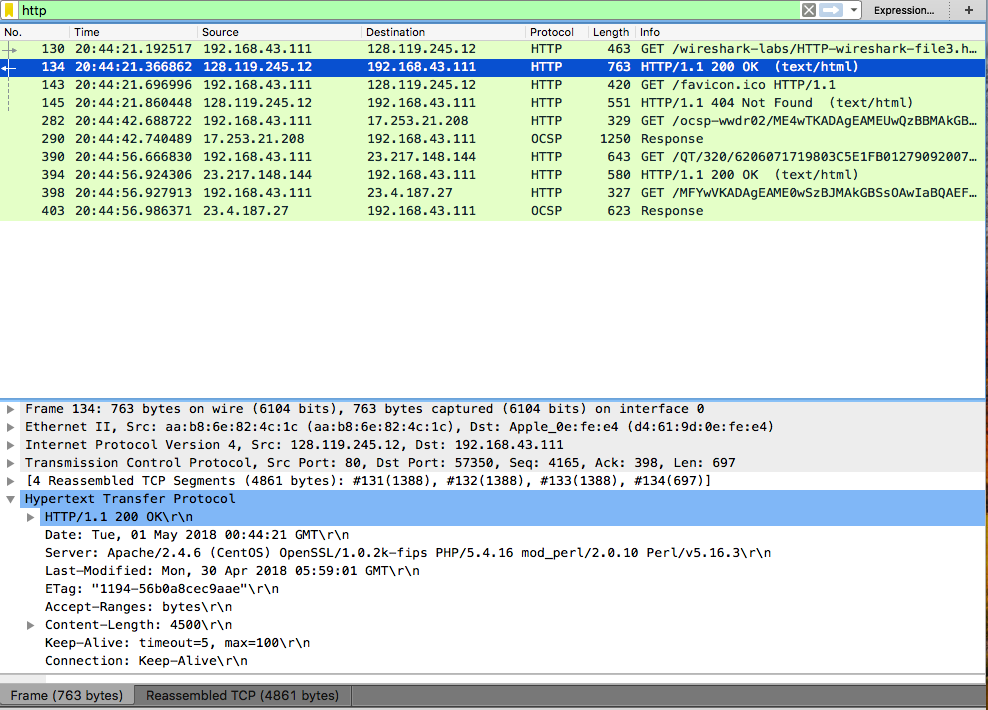
1. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

The packet that contains the status code and phrase that the server sent is 134.



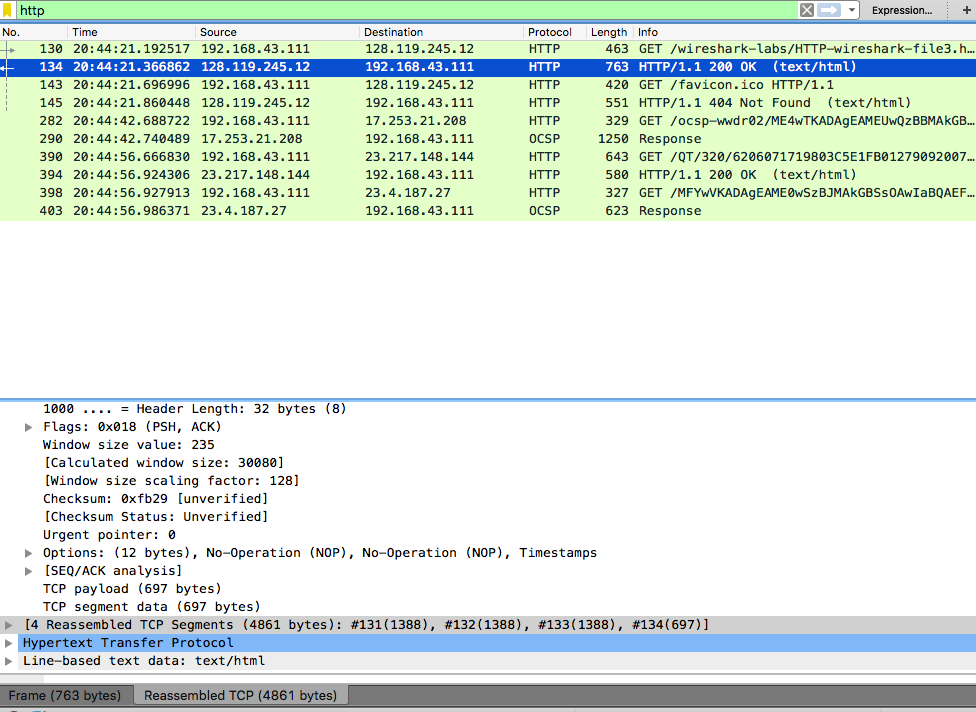
1. What is the status code and phrase in the response?

The status code and phrase in the response is 200 OK



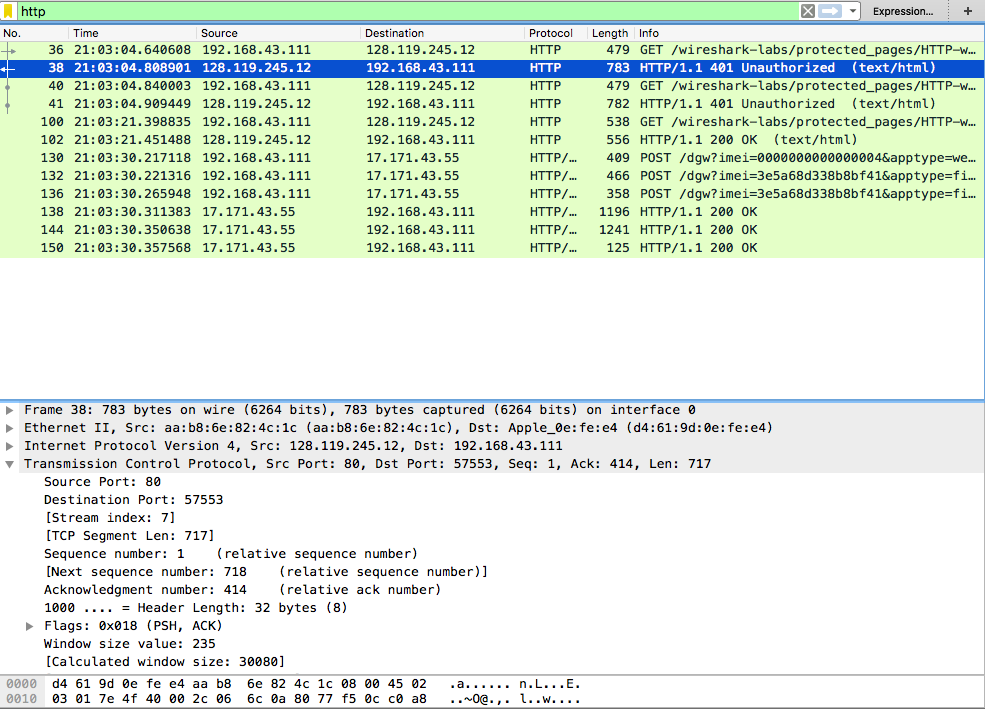
1. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

There are 4 TCP segments to carry the response



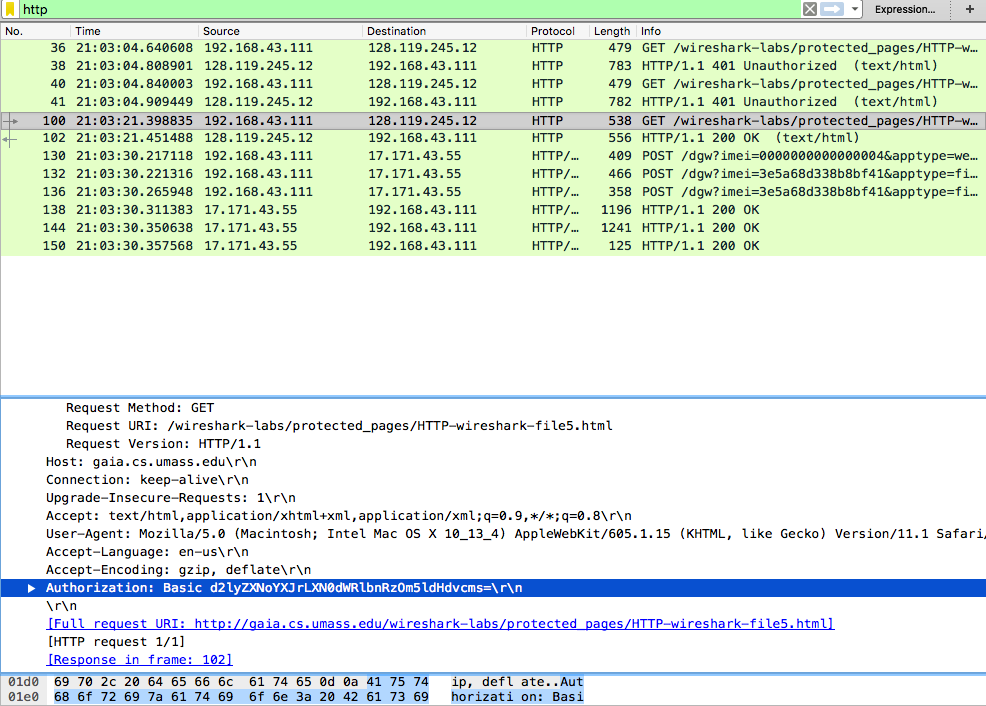
1. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?

The first response is 401 unauthorized



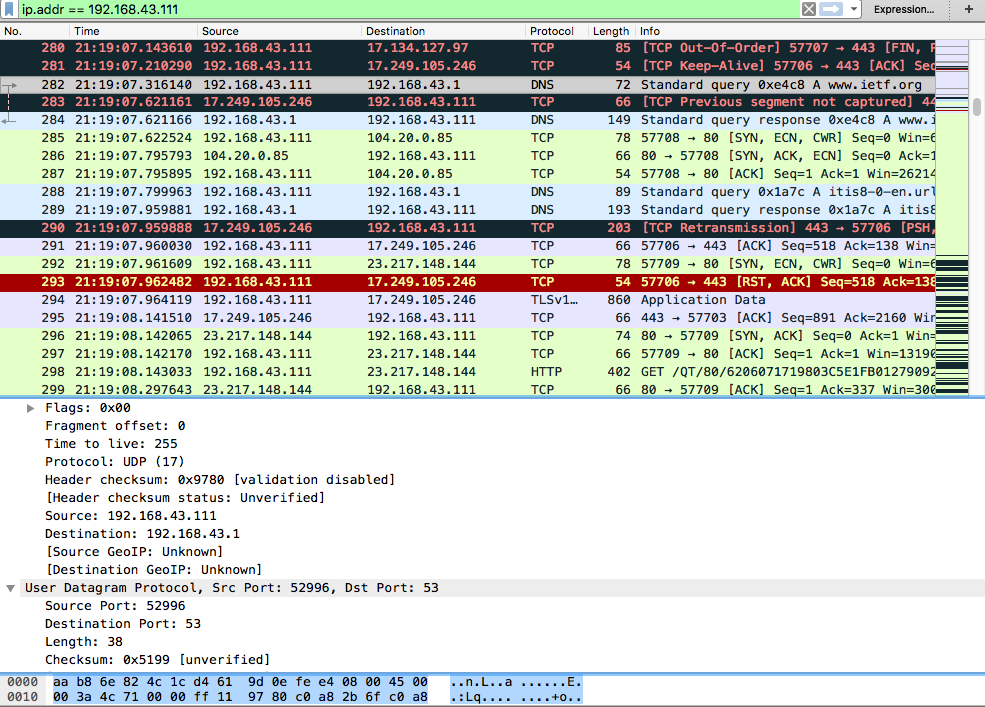
1. When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

For the second time it still got the 401 unautorized, but for the third time it includes the authorization



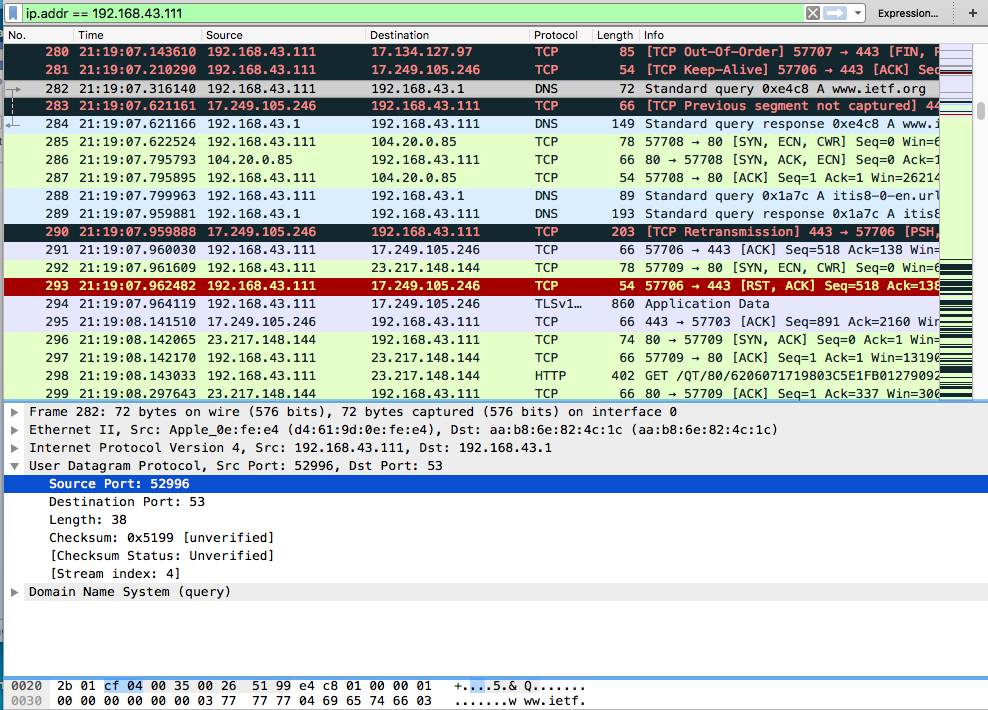
1. Locate the DNS query and response messages. Are they sent over UDP or TCP?

They are sent over UDP



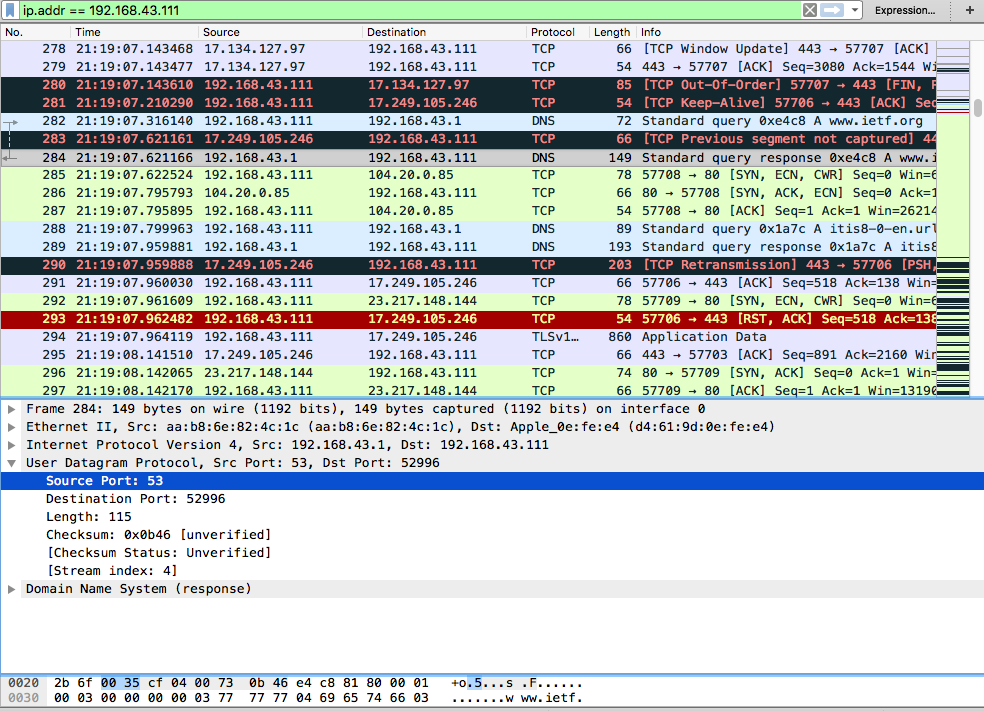
1. What is the destination port for the DNS query message?

The Destination Port is 52996



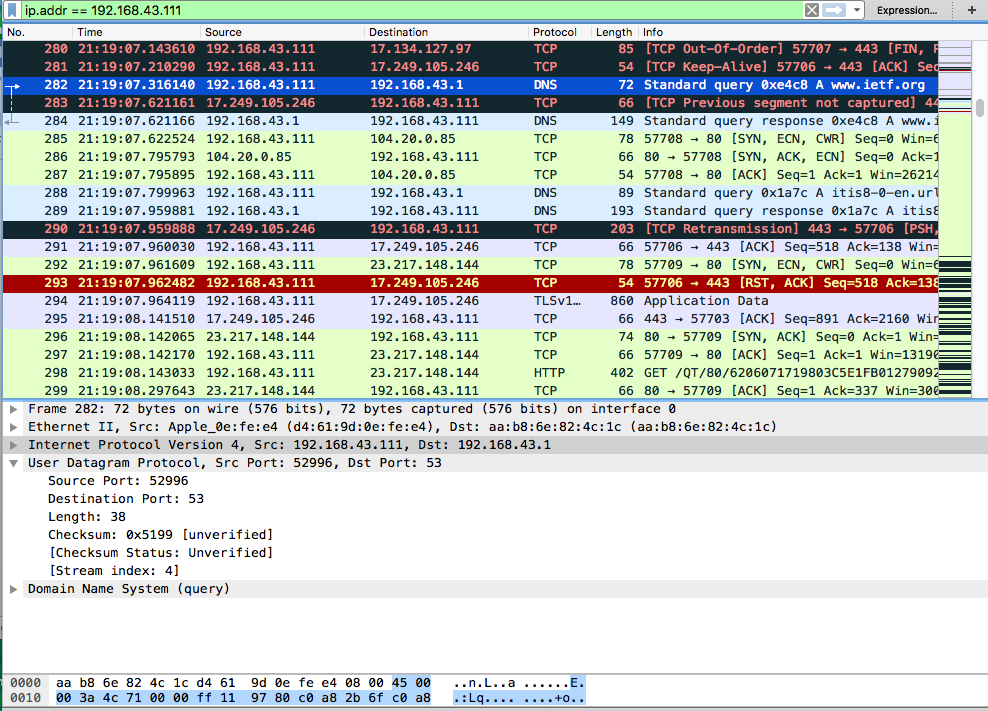
1. What is the source port of DNS response message?

The Source port for the response message is 53



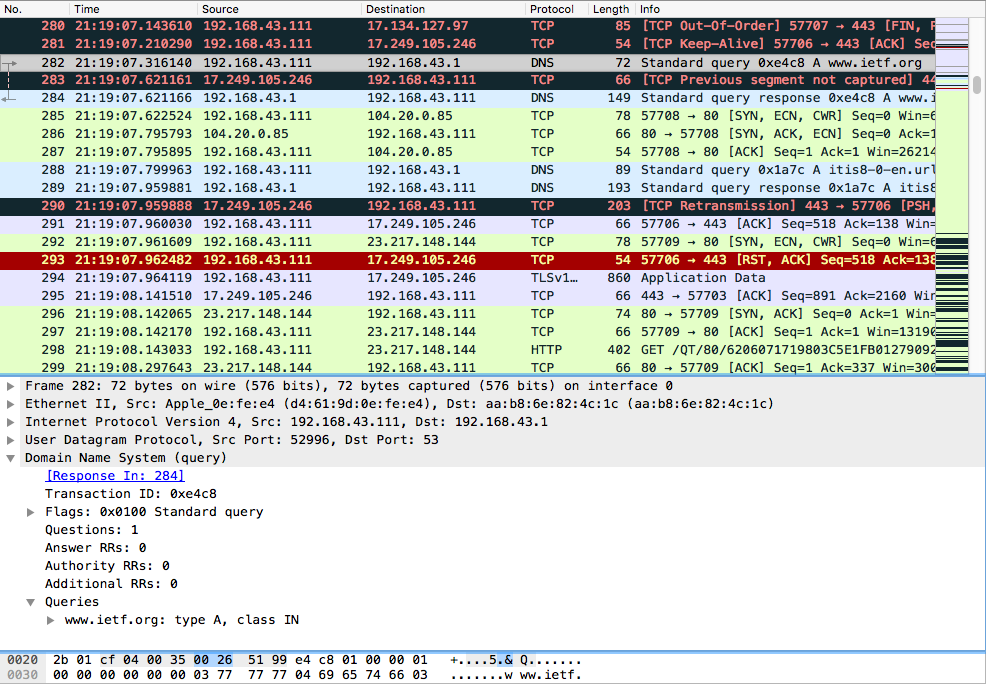
1. To what IP address is the DNS query message sent?

The destination IP is 192.168.43.1 which is the router



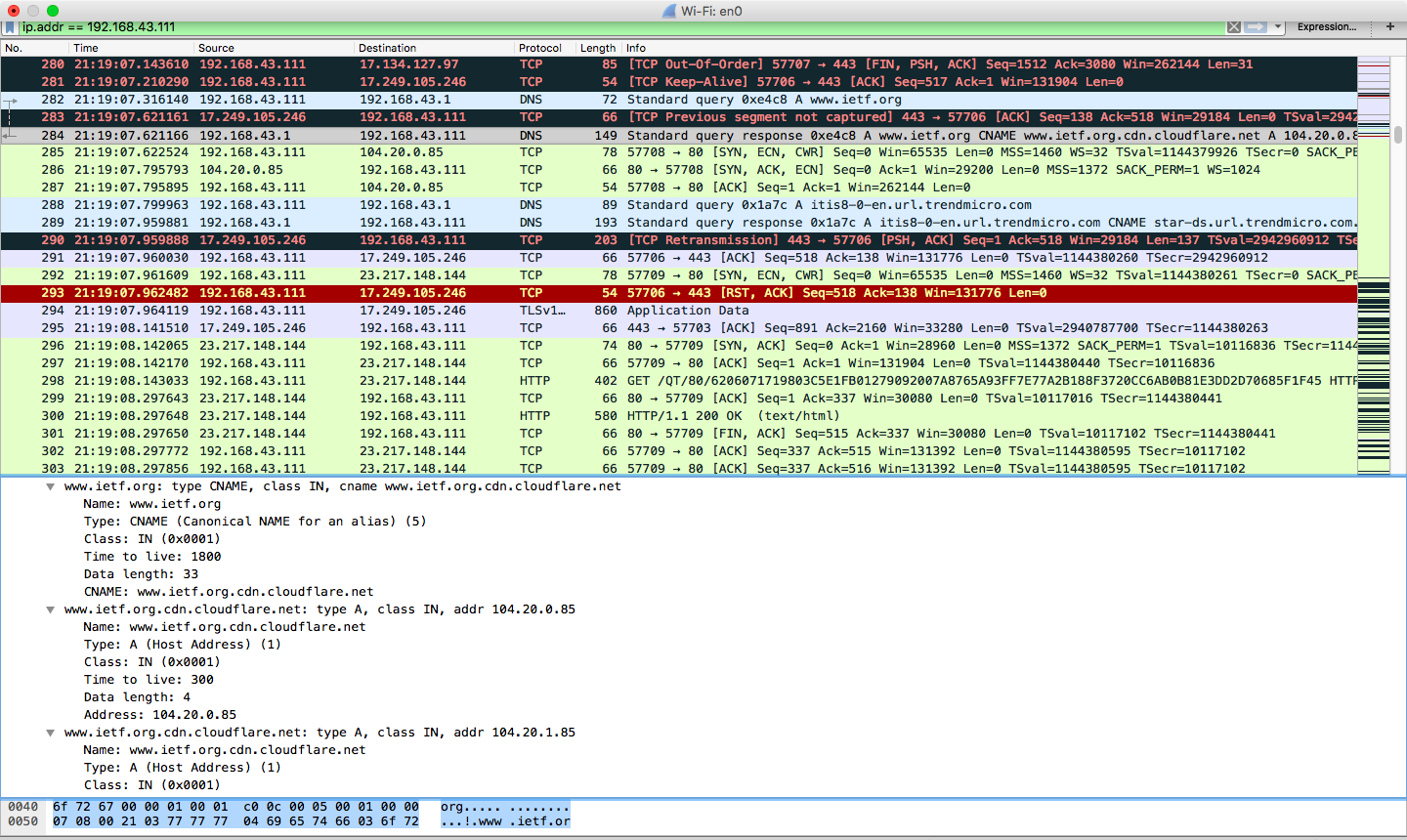
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The type is A and it does not have any answers



1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

It has three answers, the first one shows the Canonical Name and address for the intended website. The second and third one shows the address of the website



1. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

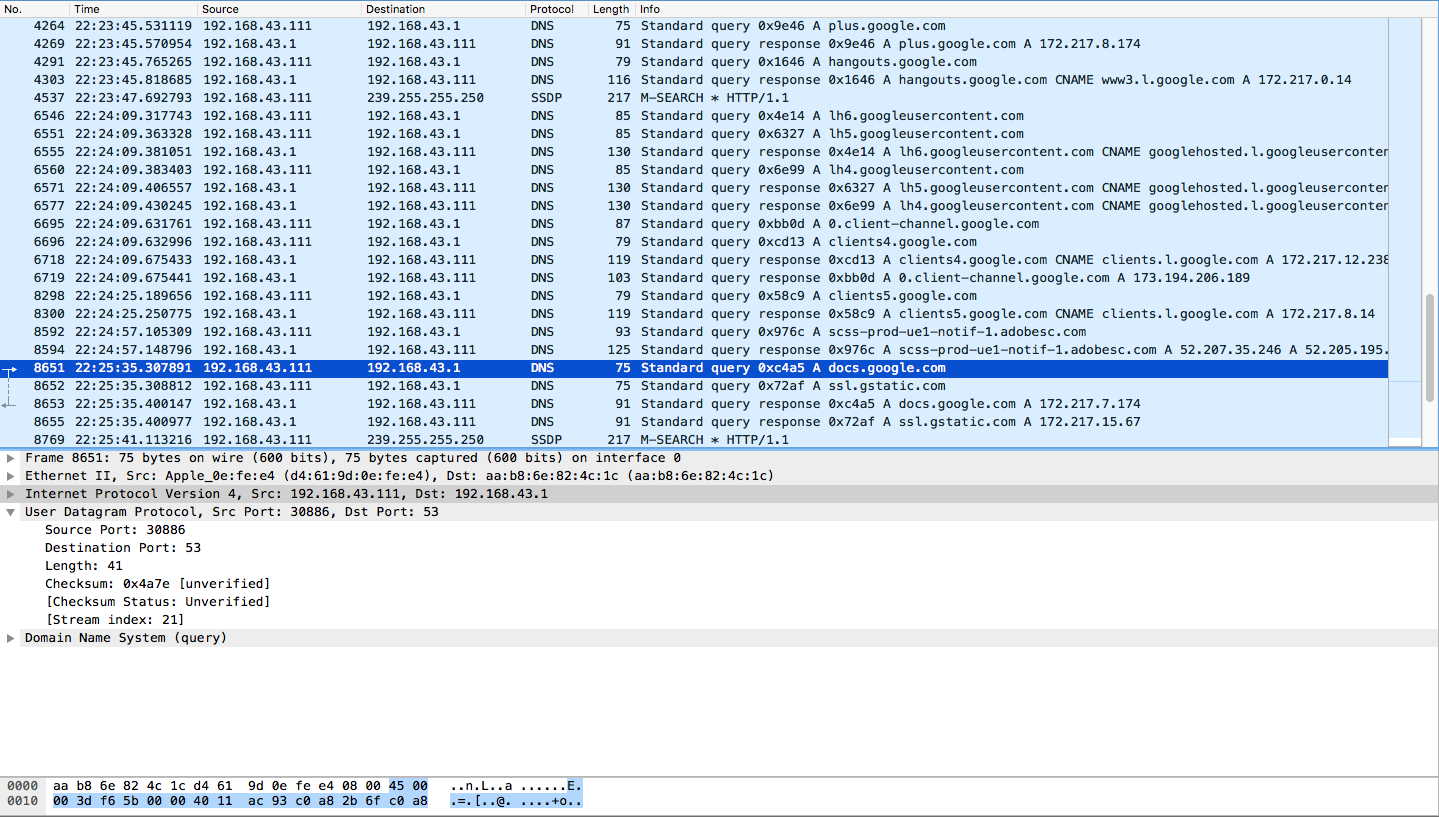
The destination IP is the same as the IP address of my computer



1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header.

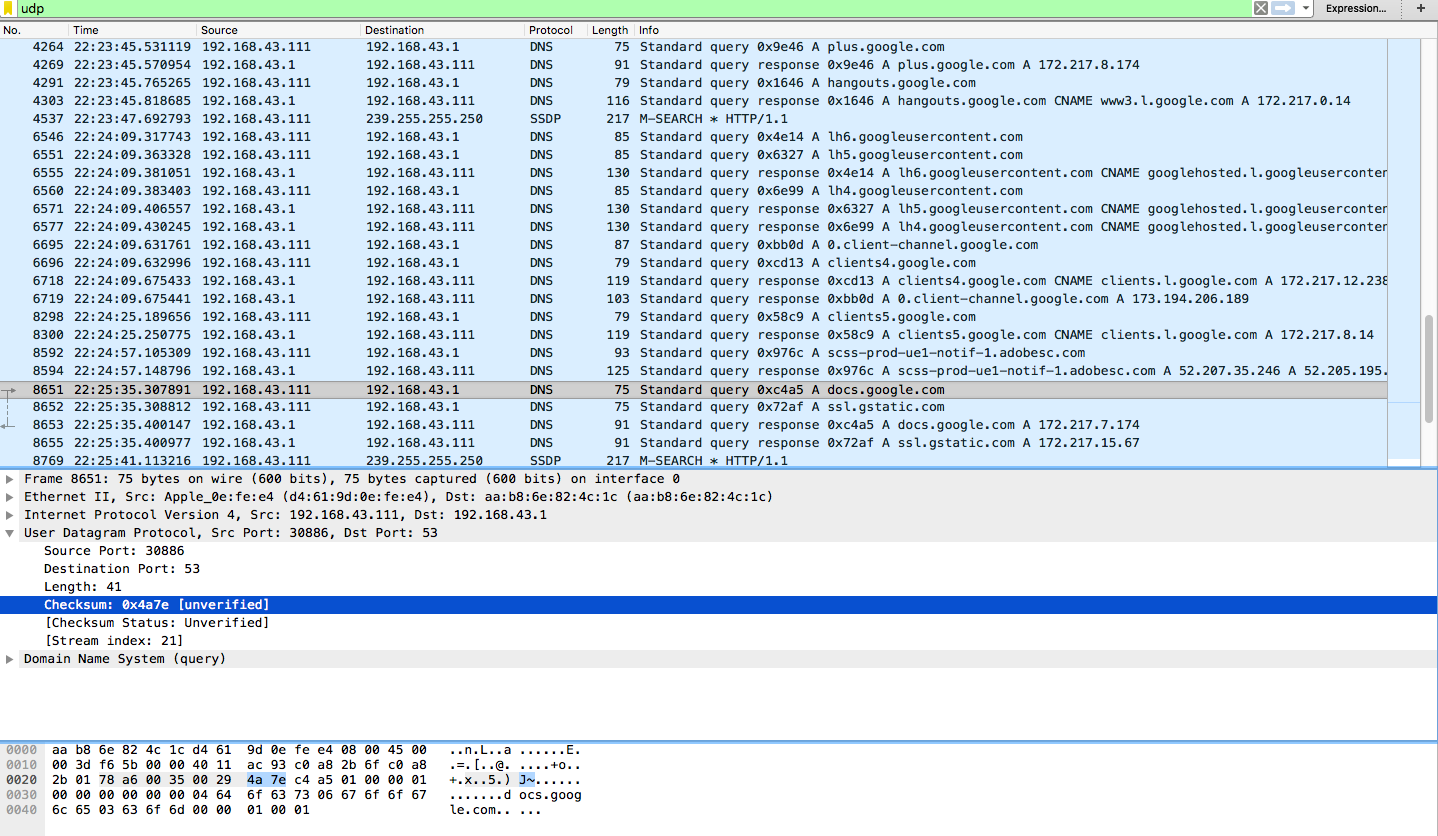
The UDP header contains 4 fields.

Source port, Destination port, length, and checksum



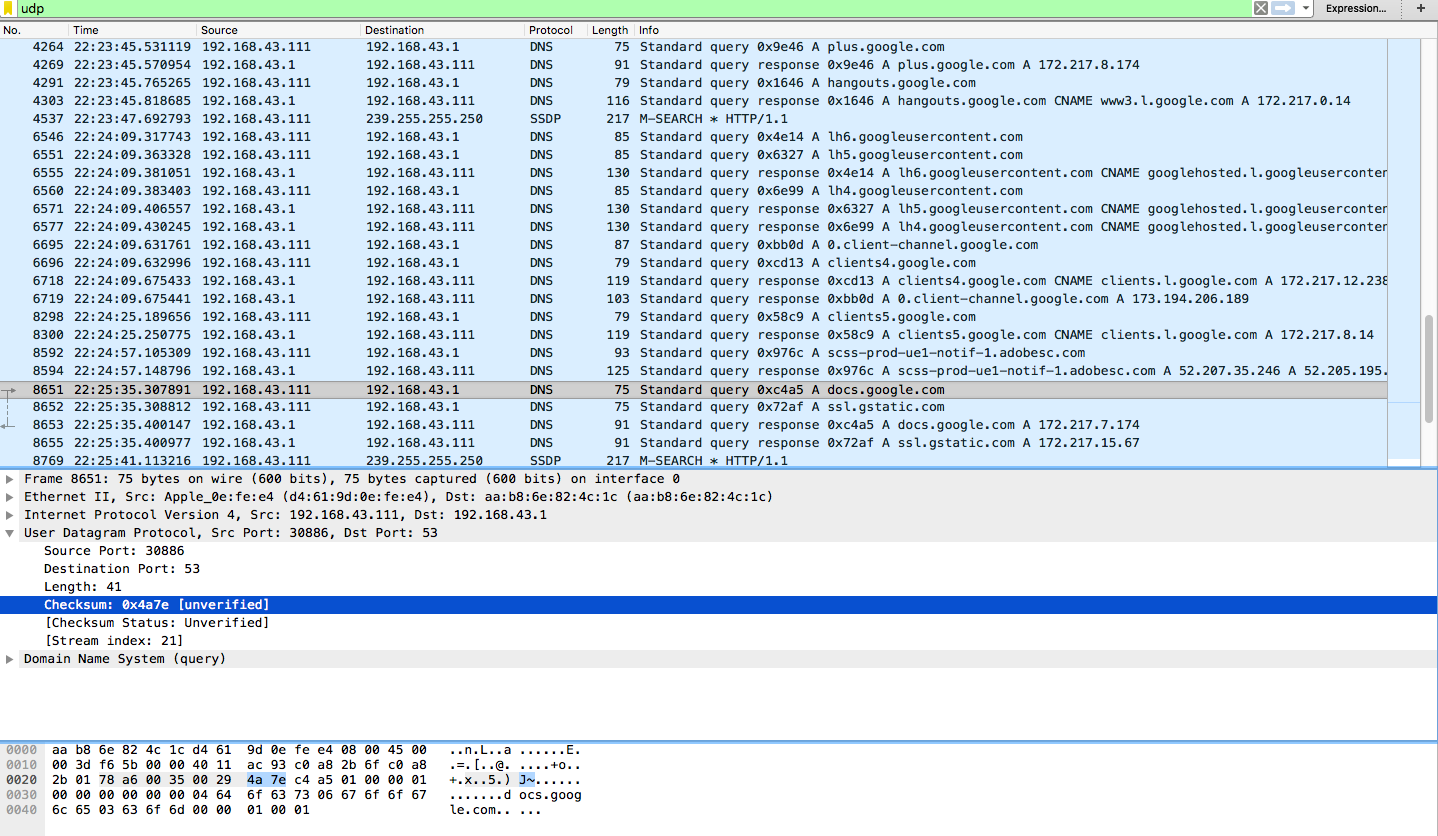
1. By consulting the displayed information in Wireshark’s packet content field for this packet, determine the length (in bytes) of each of the UDP header.

The UDP headers are 2 bytes long

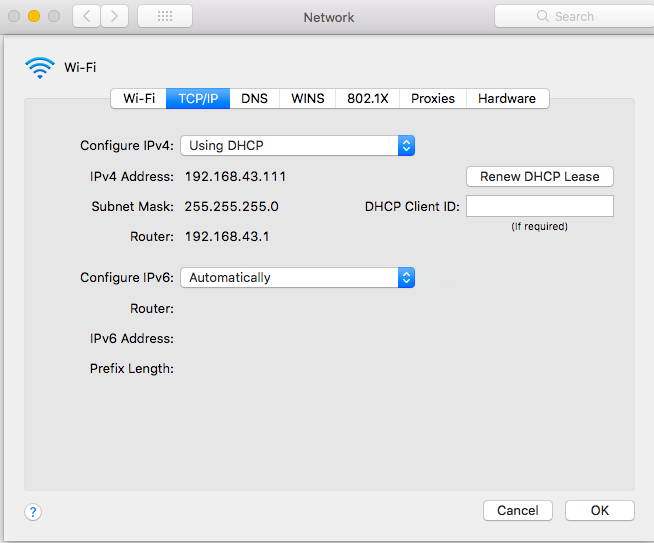


1. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.

The value in the length field, in the example below it is 41, is the sum of the 8 header bytes and the remaining data bytes encapsulated in the packet.



I took a break and started again but It’s the same router



1. Explain what happened in Figure 1. (pay close attention to the command.)

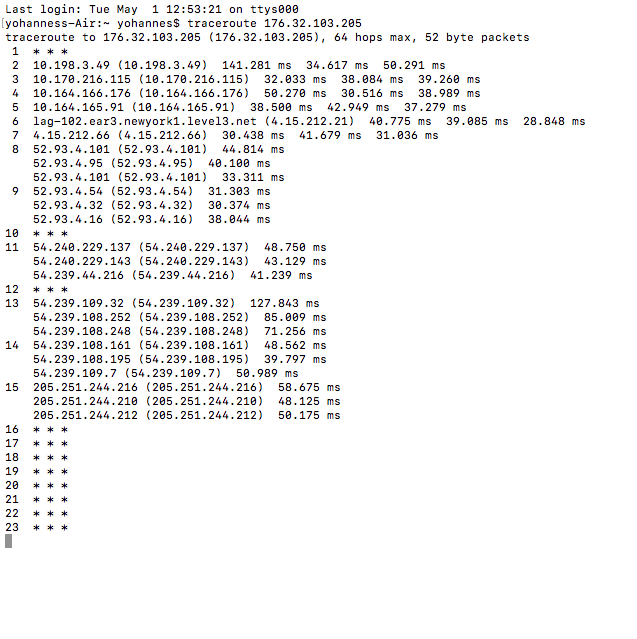
The figure shows the roundtrip time it took the pinged website from the computer, this shows if the website is up and running. It also check the speed of the website.

1. Which protocol is used to carry out the instruction in Figure 1.

The protocol it uses is the ICMP.

1. Who owns the IP?

Amazon owns the IP

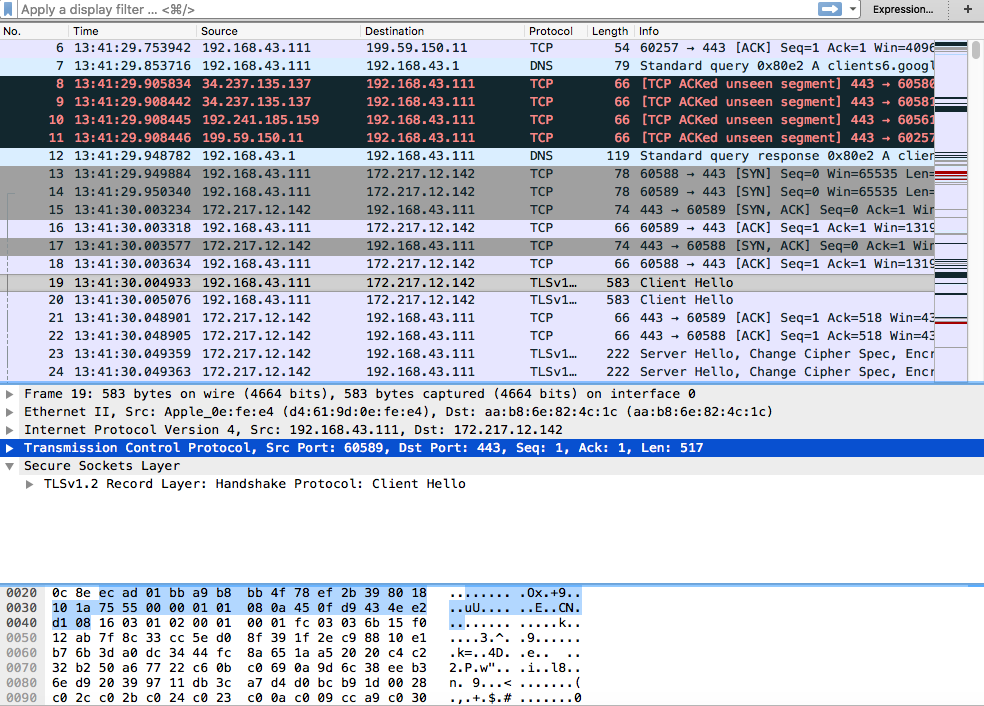


1. In addition to a screenshot, in a tabular form, list all the hops between your computer’s IP and the IP address in Figure 1. The table should include the owner, and location of the IP address.

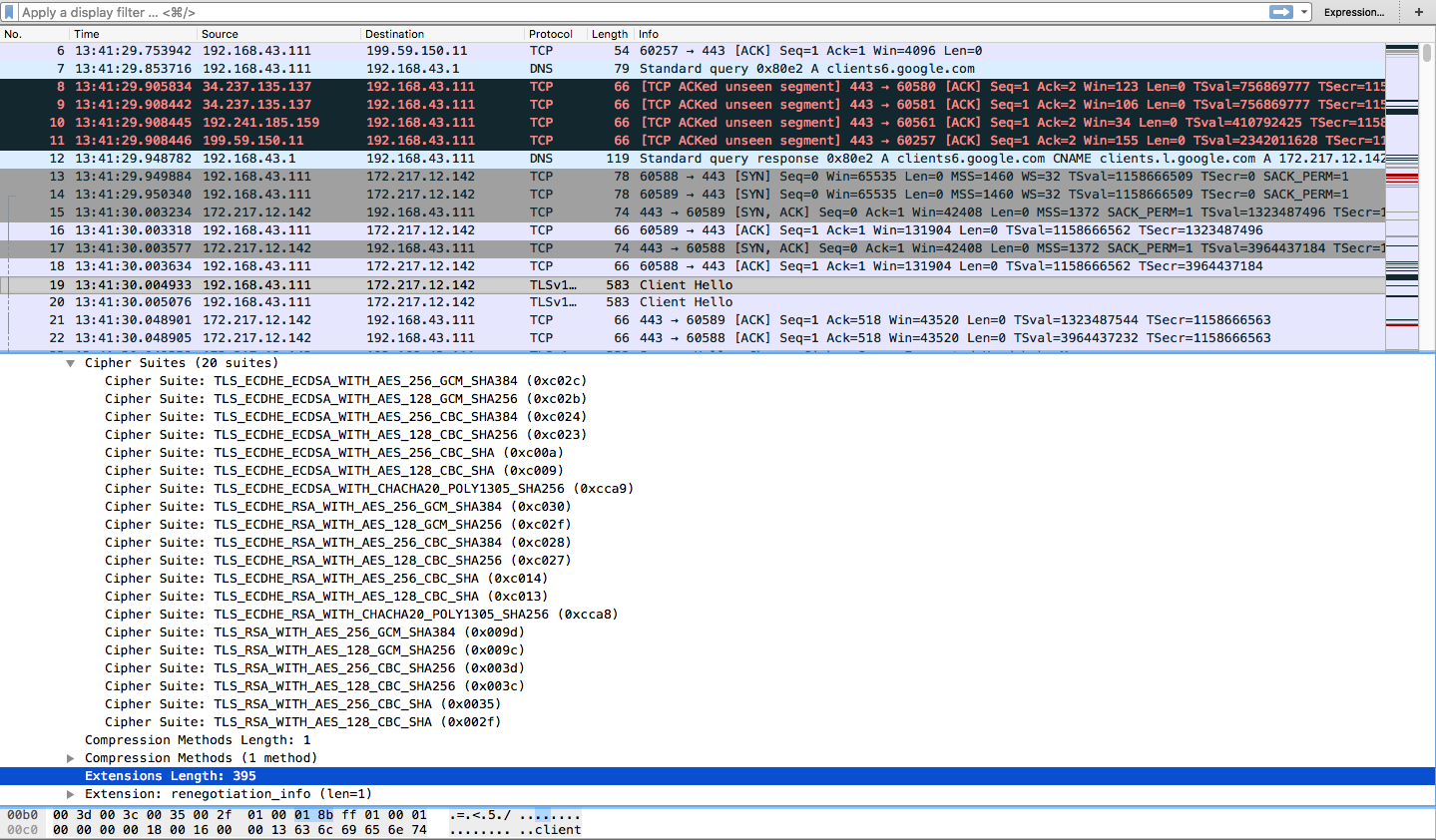
|  |  |  |
| --- | --- | --- |
| IP address | Location | Owner |
| 10.198.3.49 | IP not found (private) | Not found (private) |
| 10.170.216.115 | IP not found (private) | Not found (private) |
| 10.164.166.176 | IP not found (private) | Not found (private) |
| 10.164.165.91 | IP not found (private) | Not found (private) |
| 4.15.212.21 | New York | Level 3 Parent, LLC |
| 4.15.212.66 | New York | Level 3 Parent, LLC |
| 52.93.4.101 | Ashburn, Virginia | Amazon.com |
| 52.93.4.95 | Ashburn, Virginia | Amazon.com |
| 52.93.4.101 | Ashburn, Virginia | Amazon.com |
| 52.93.4.54 | Ashburn, Virginia | Amazon.com |
| 52.93.4.32 | Ashburn, Virginia | Amazon.com |
| 52.93.4.16 | Ashburn, Virginia | Amazon.com |
| 54.240.229.137 | Ashburn, Virginia | Amazon.com |
| 54.240.229.143 | Ashburn, Virginia | Amazon.com |
| 54.239.44.216 | Ashburn, Virginia | Amazon.com |
| 54.239.109.32 | Ashburn, Virginia | Amazon.com |
| 54.239.108.252 | Ashburn, Virginia | Amazon.com |
| 54.239.108.248 | Ashburn, Virginia | Amazon.com |
| 54.239.108.161 | Ashburn, Virginia | Amazon.com |
| 54.239.108.195 | Ashburn, Virginia | Amazon.com |
| 54.239.109.7 | Ashburn, Virginia | Amazon.com |
| 205.251.244.216 | Ashburn, Virginia | Amazon.com |
| 205.251.244.210 | Ashburn, Virginia | Amazon.com |
| 205.251.244.212 | Ashburn, Virginia | Amazon.com |

1. What version of TLS does the IP above use? Hint: Visit the website of the owners IP address, and capture the “Client Hello” packet.

The TLS version is TLSv1.2



1. List all the algorithms listed in the Cipher Suite of the “Client Hello” packet in 21.



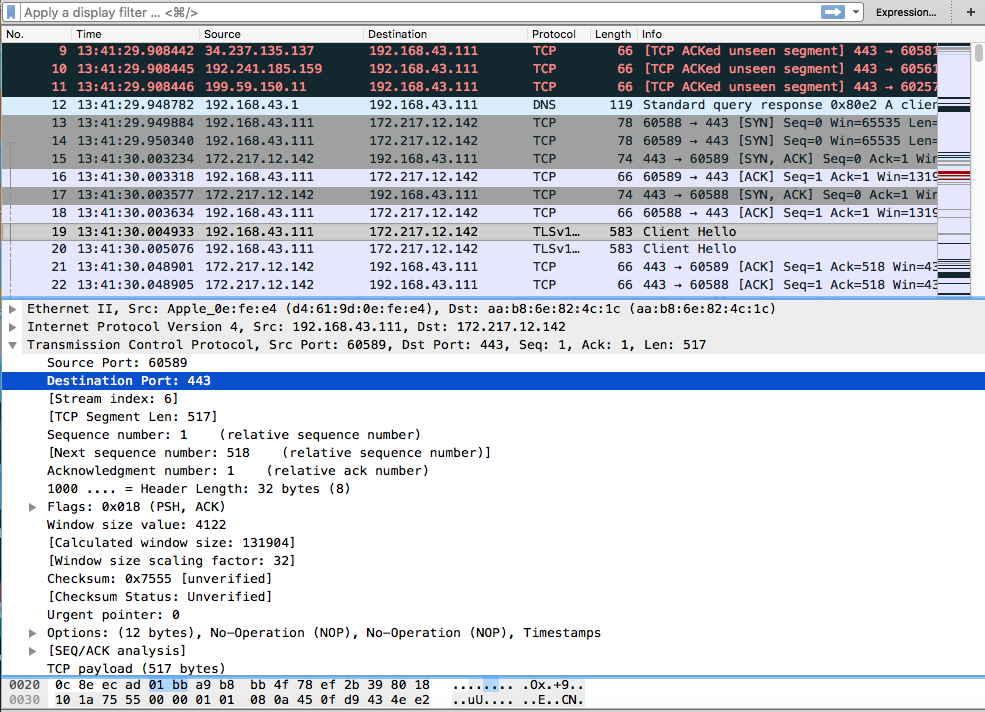
Public key algorithm: ECDHE\_ECDSA, ECDHE\_RSA, RSA

Symmetric‐key algorithm: AES\_256\_GCM, AES\_128\_GCM, AES\_128\_CBC, AES\_256\_CBC, CHACHA20\_POLY1305

Hash algorithm: SHA384, SHA256, SHA

1. What TCP port number is used by the “Client Hello” packet, and why is it using that port number?

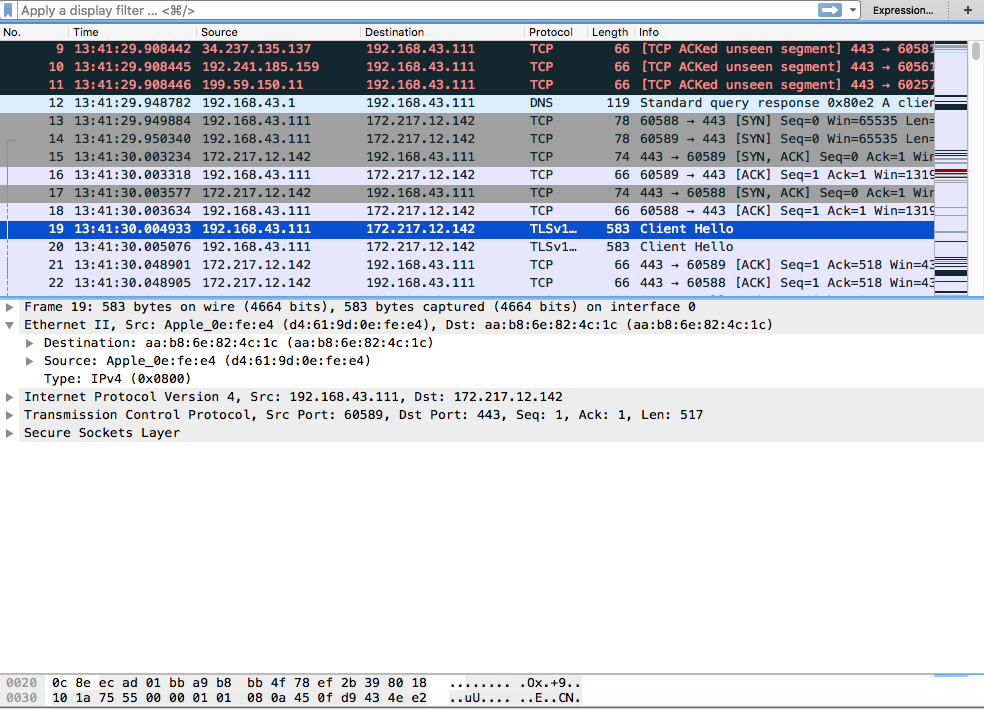
The destination port number used is 443, it is used because It is a secured website.



1. What are the source and destination MAC address?

Source Mac address - d4:61:9d:0e:fe:e4

Destination Mac address- aa:b8:6e:82:4c:1c



1. Identify the company that manufactured the network cards with the MAC address identified in 24 above. (Hint: there are a lot of websites you can use to lookup MAC address, just like you would for an IP).

-For the destination MAC it is Drã¤gerwerk Ag & Co. Kg Aa

-For the Source MAC it is Fe Global Hong Kong Limited