Ivan Cruz

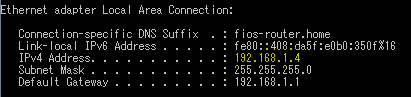
Prof. Waziri

IT-520

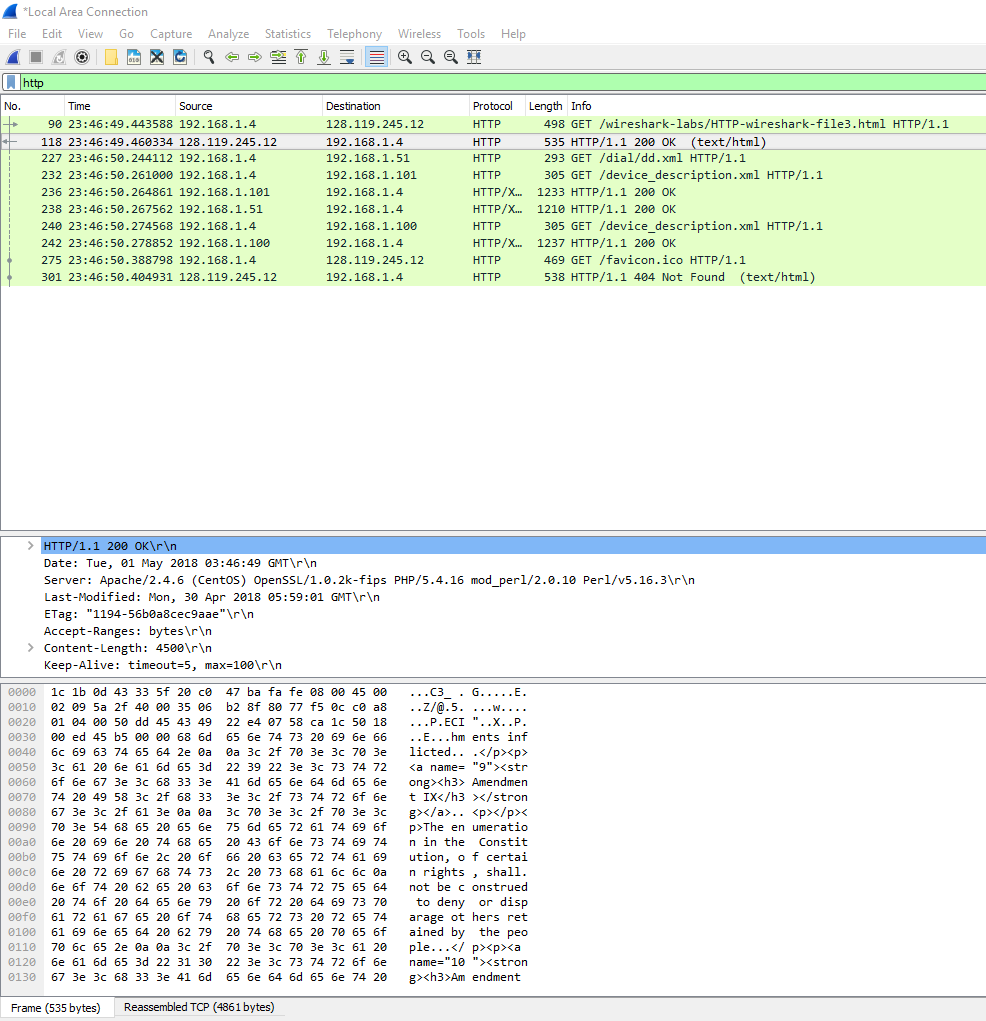
May 1st, 2018

Lab Final

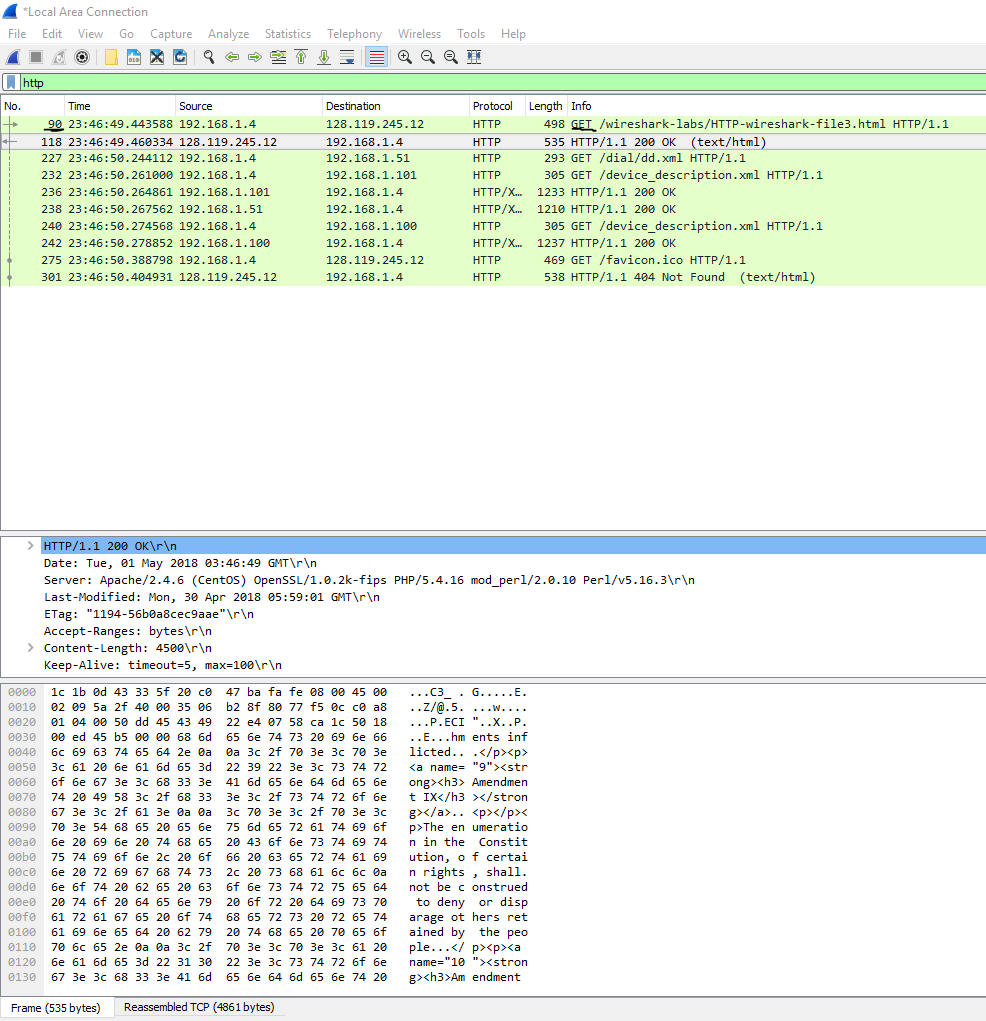
My computer’s IPv4 is 192.168.1.4



1. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill of Rights?
2. 5 HTTP GET Requests were sent.

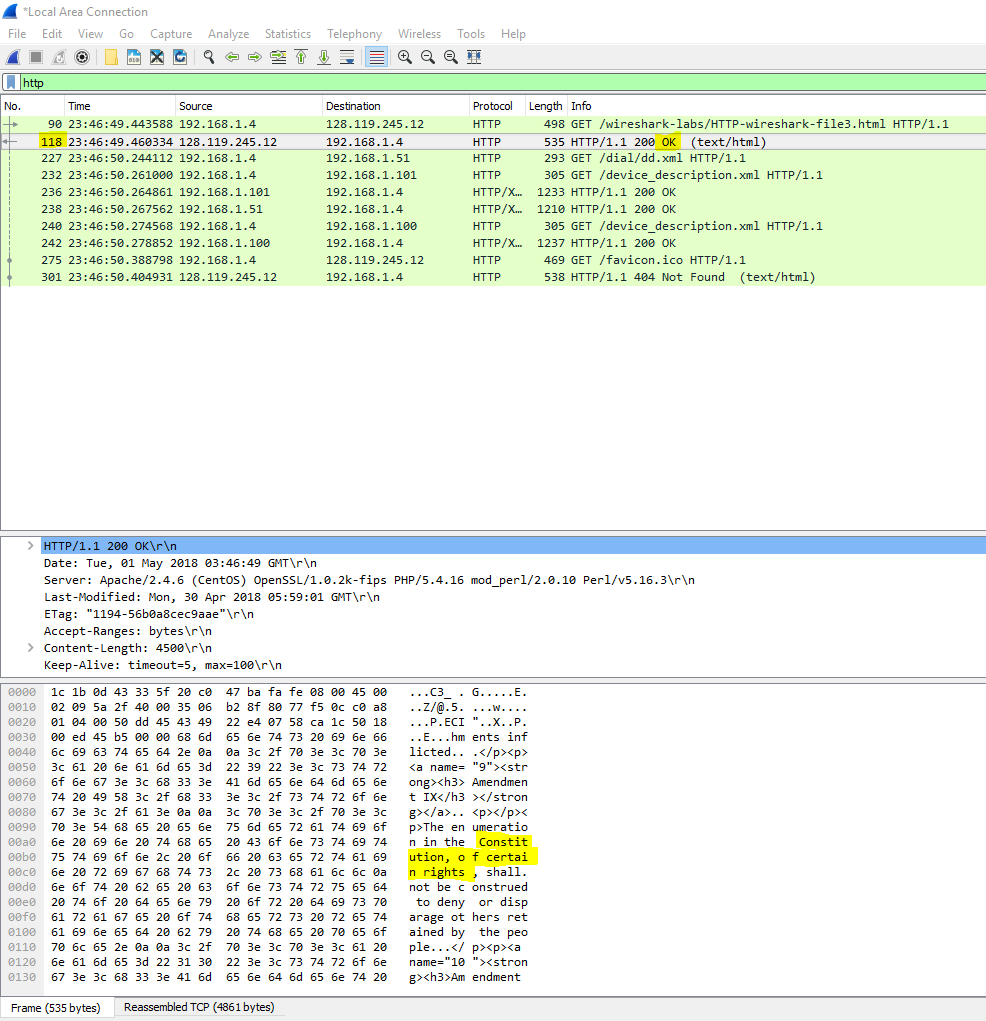


1. The packet number for the Bill of Rights HTTP GET message is 90.



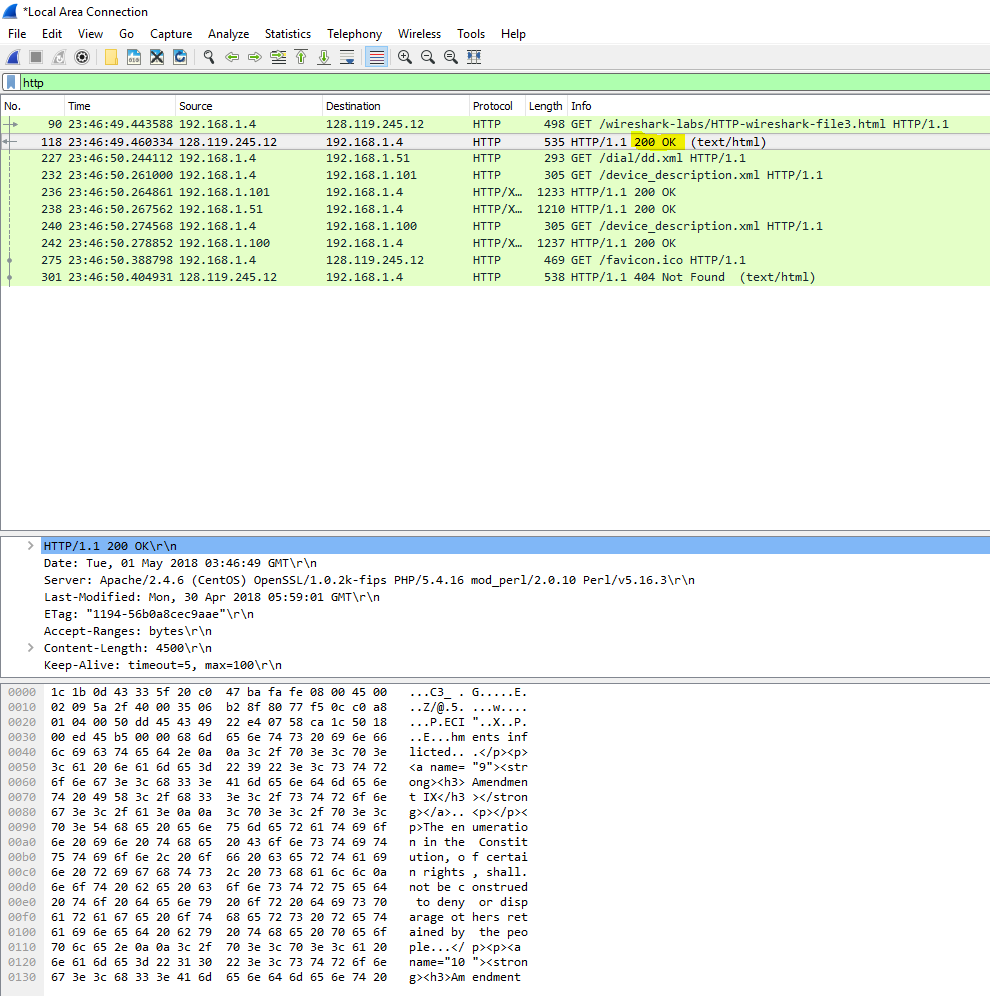
1. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

* The packet number to the response was 118.

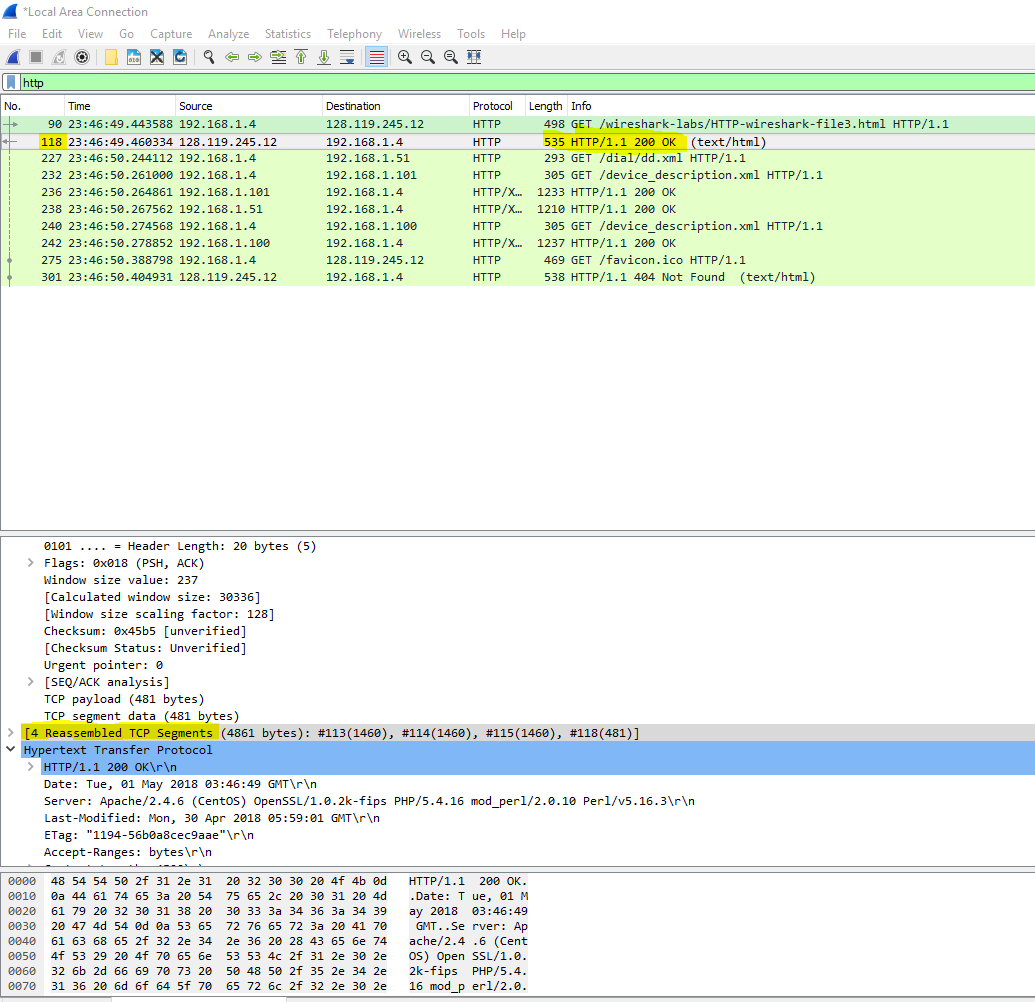


1. What is the status code and phrase in the response?

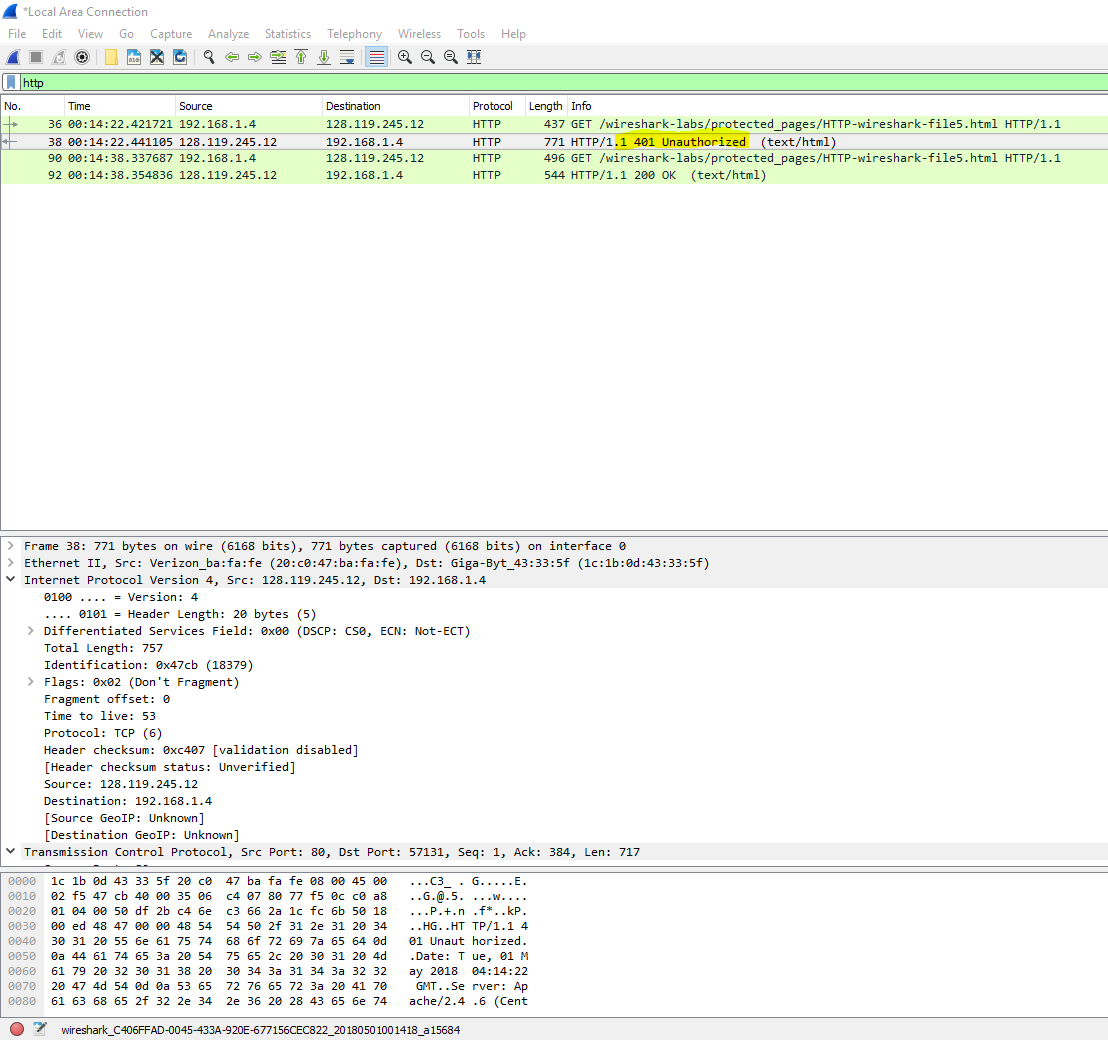
* The status code and phrase of the response was, “200 OK.”



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

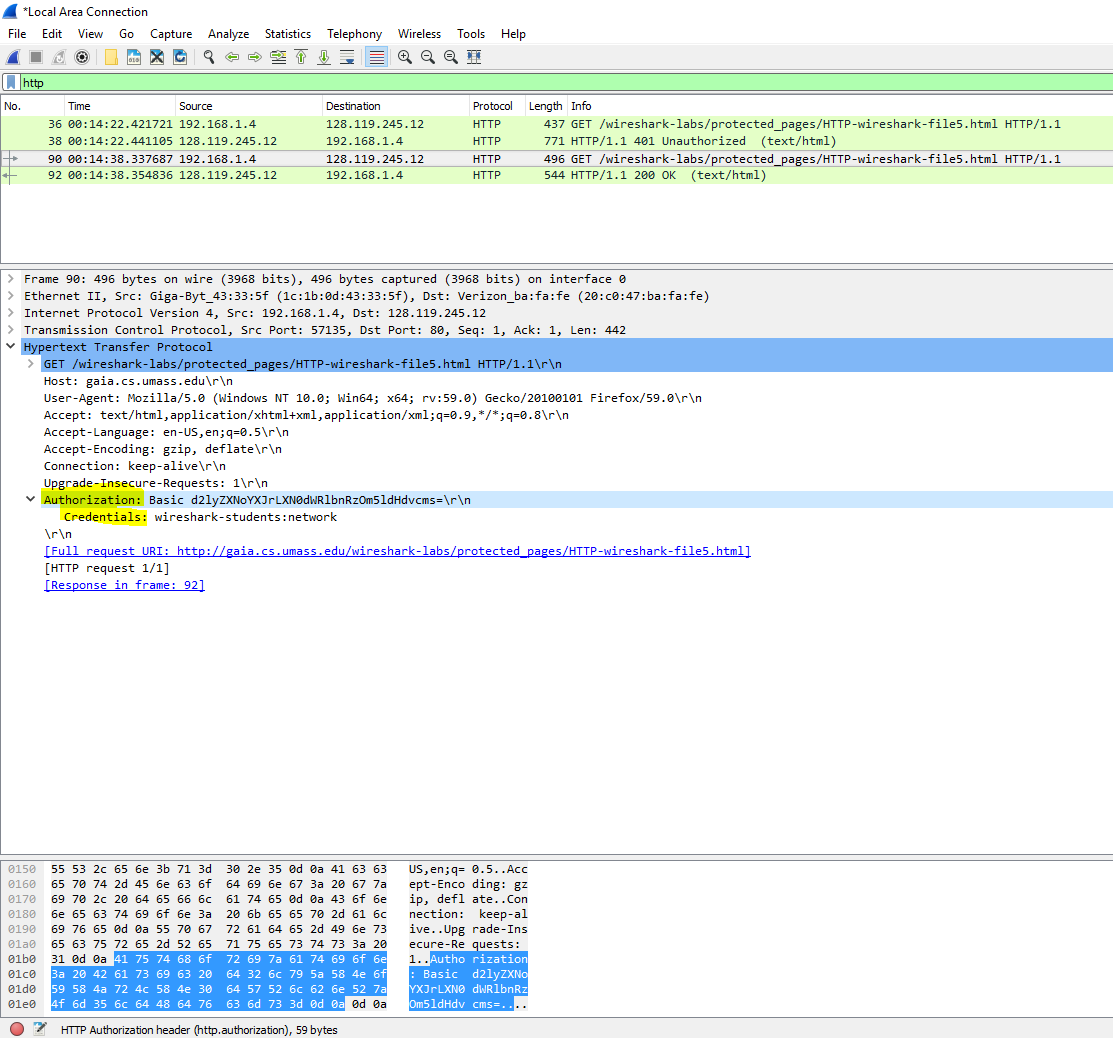
* 4 TCP segments were needed to send the data 

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

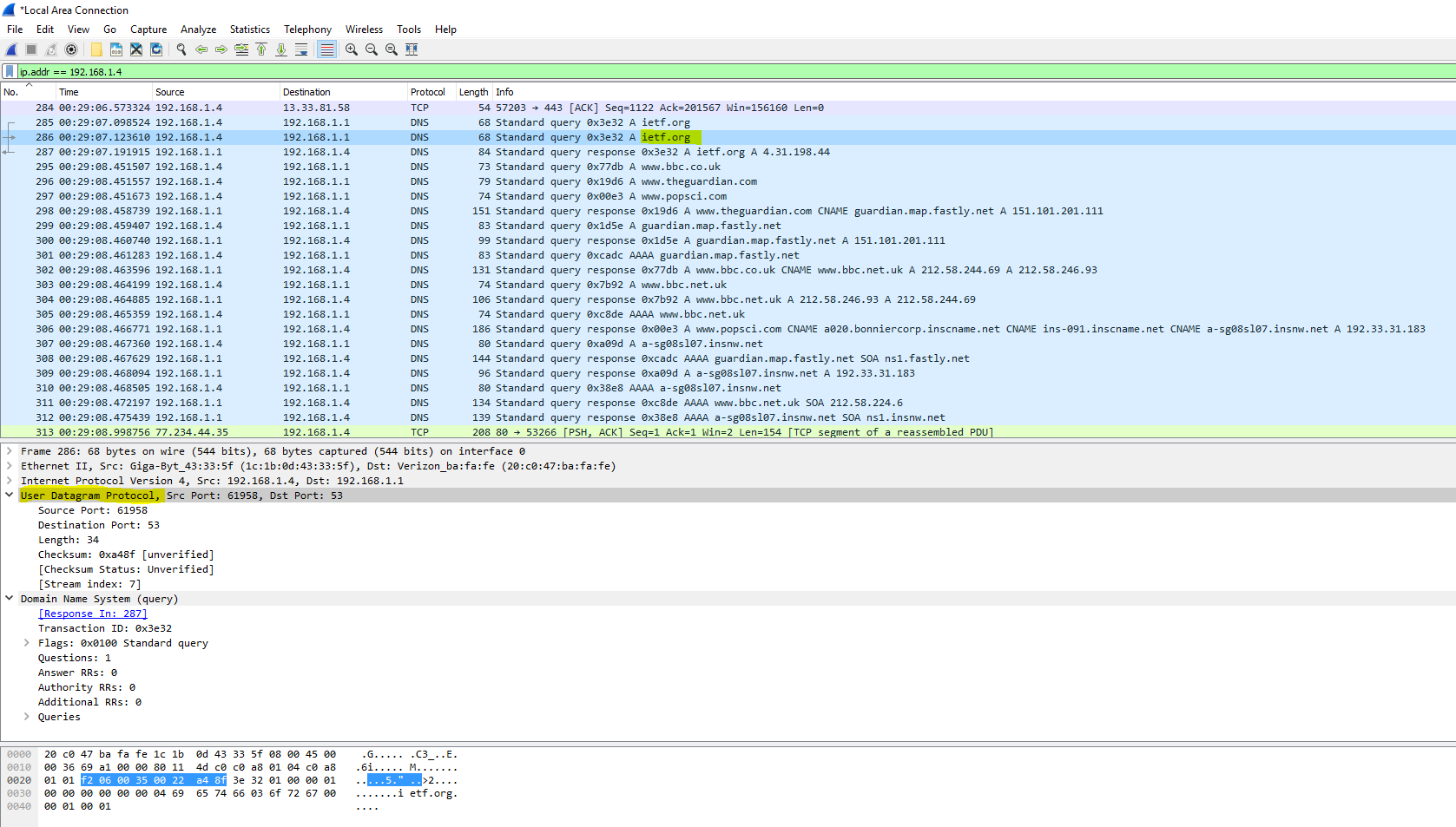
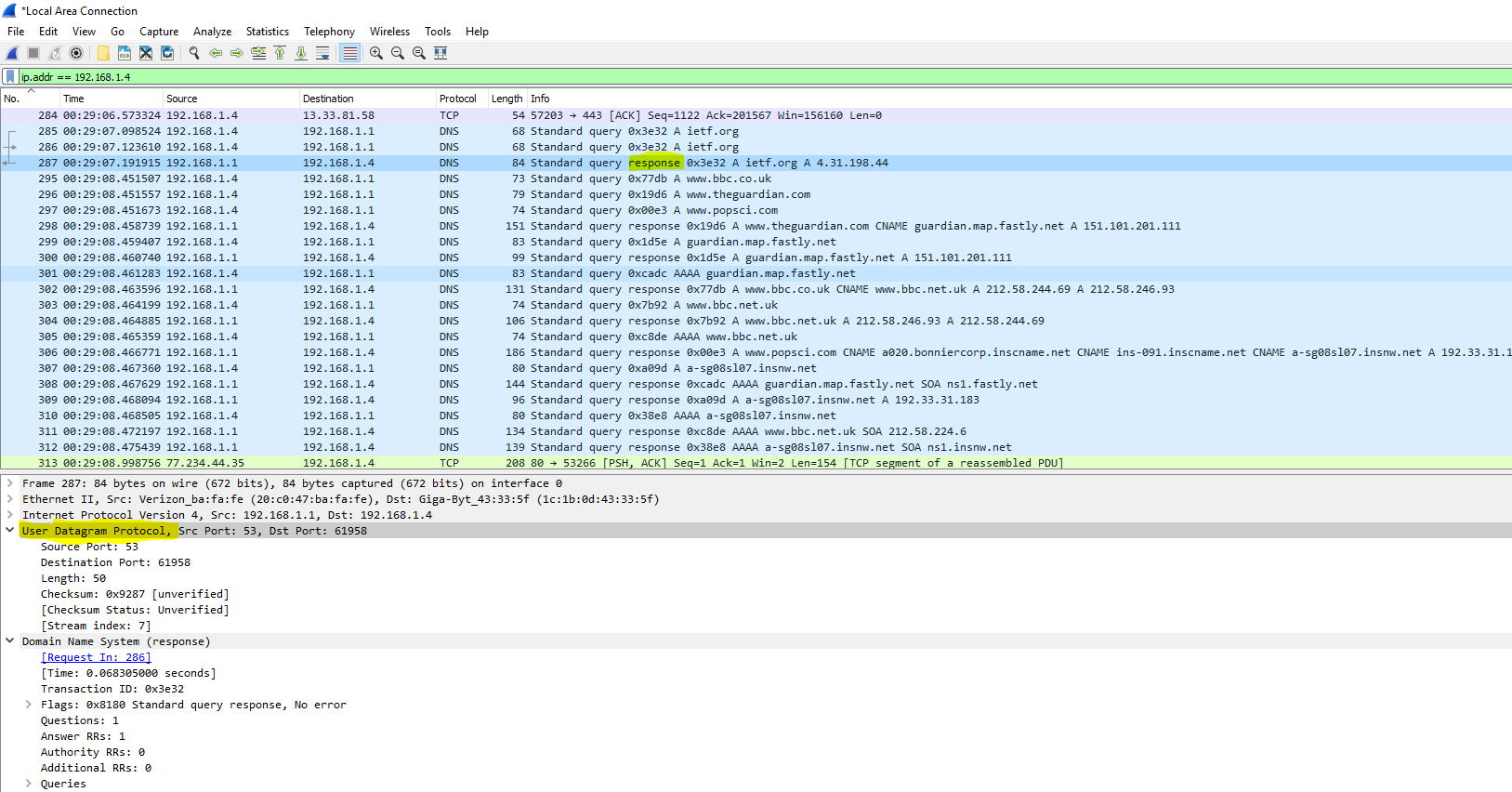
* The first response was: “401 Unauthorized” 

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

* An authorization with the Credentials for accessing the website was added to the 2nd HTTP GET message.

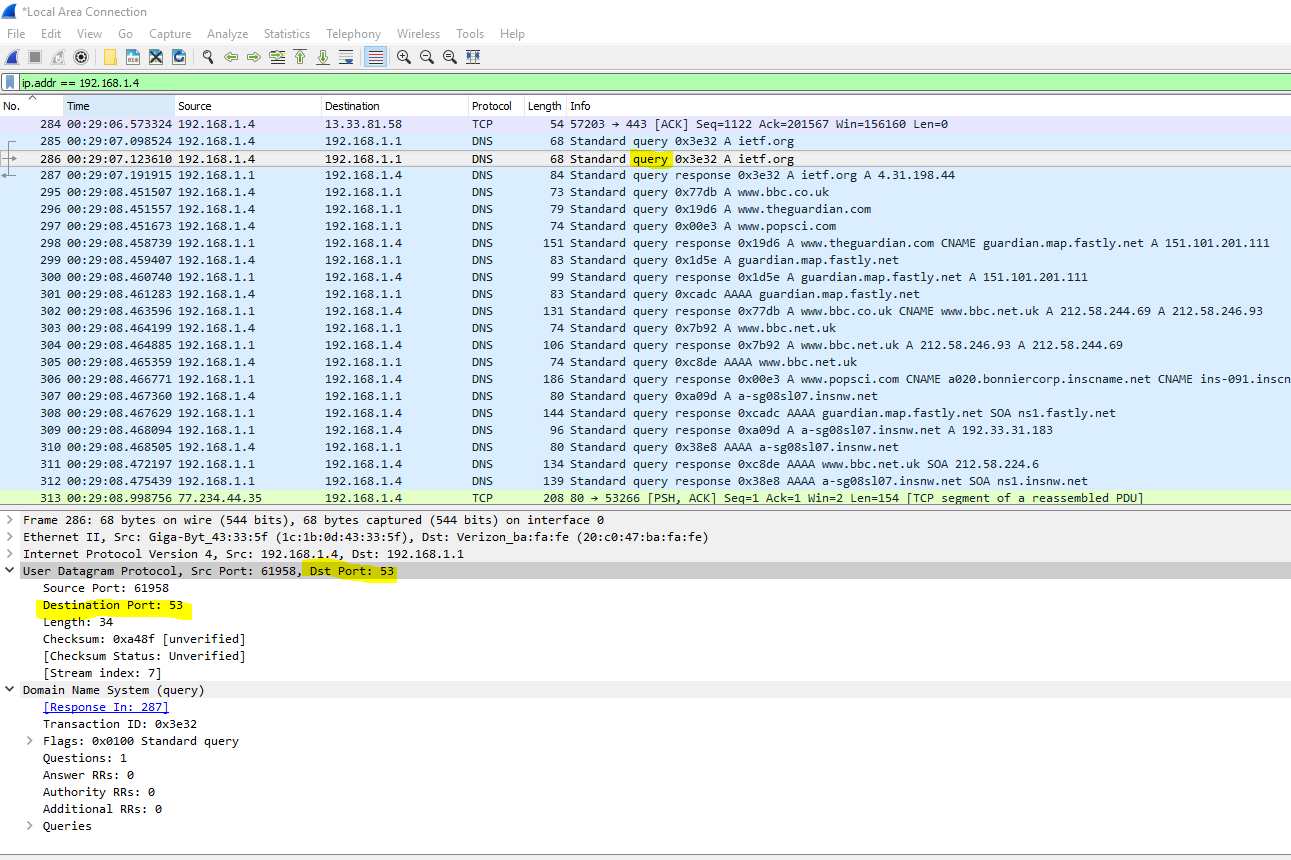


1. Locate the DNS query and response messages. Are they sent over UDP or TCP?

* Both DNS query and the Response message are sent over UDP.  

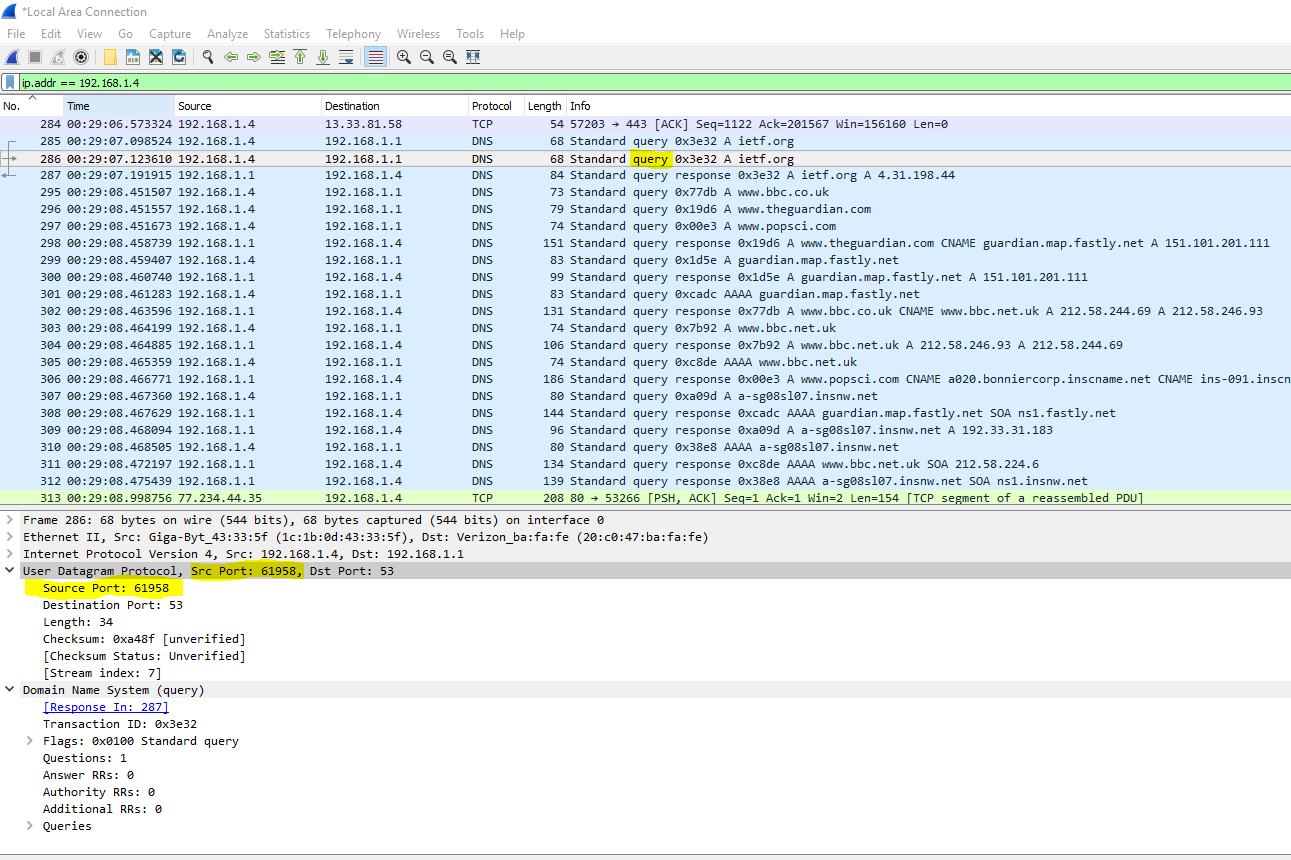
1. What is the destination port for the DNS query message?

* The Destination port of the DNS query message is 53



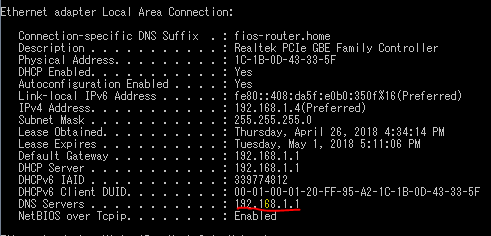
1. What is the source port of DNS response message?

* The Source port of the DNS query is 61958

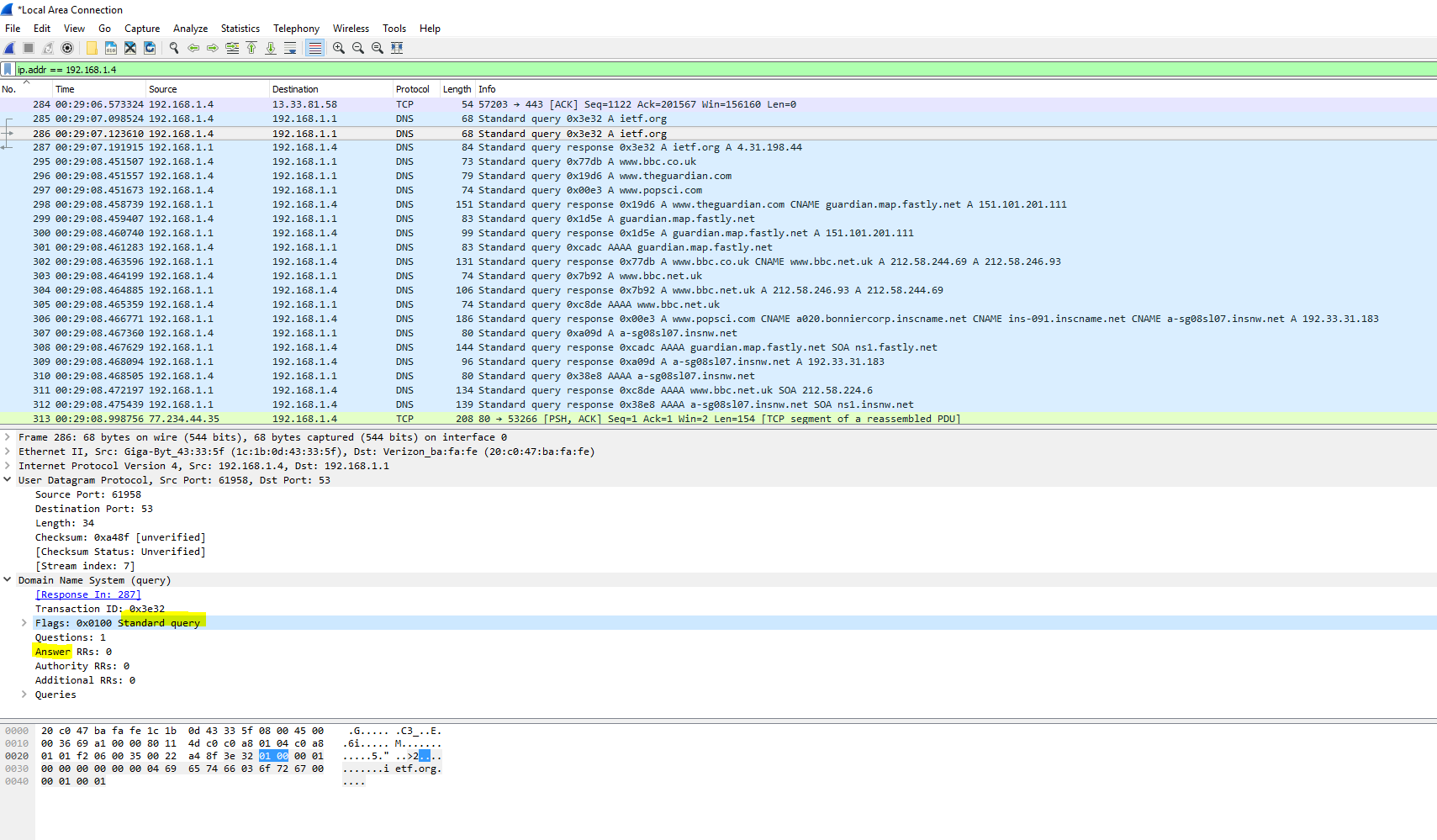


1. To what IP address is the DNS query message sent?

* The destination is 192.168.1.1 which is my local DNS

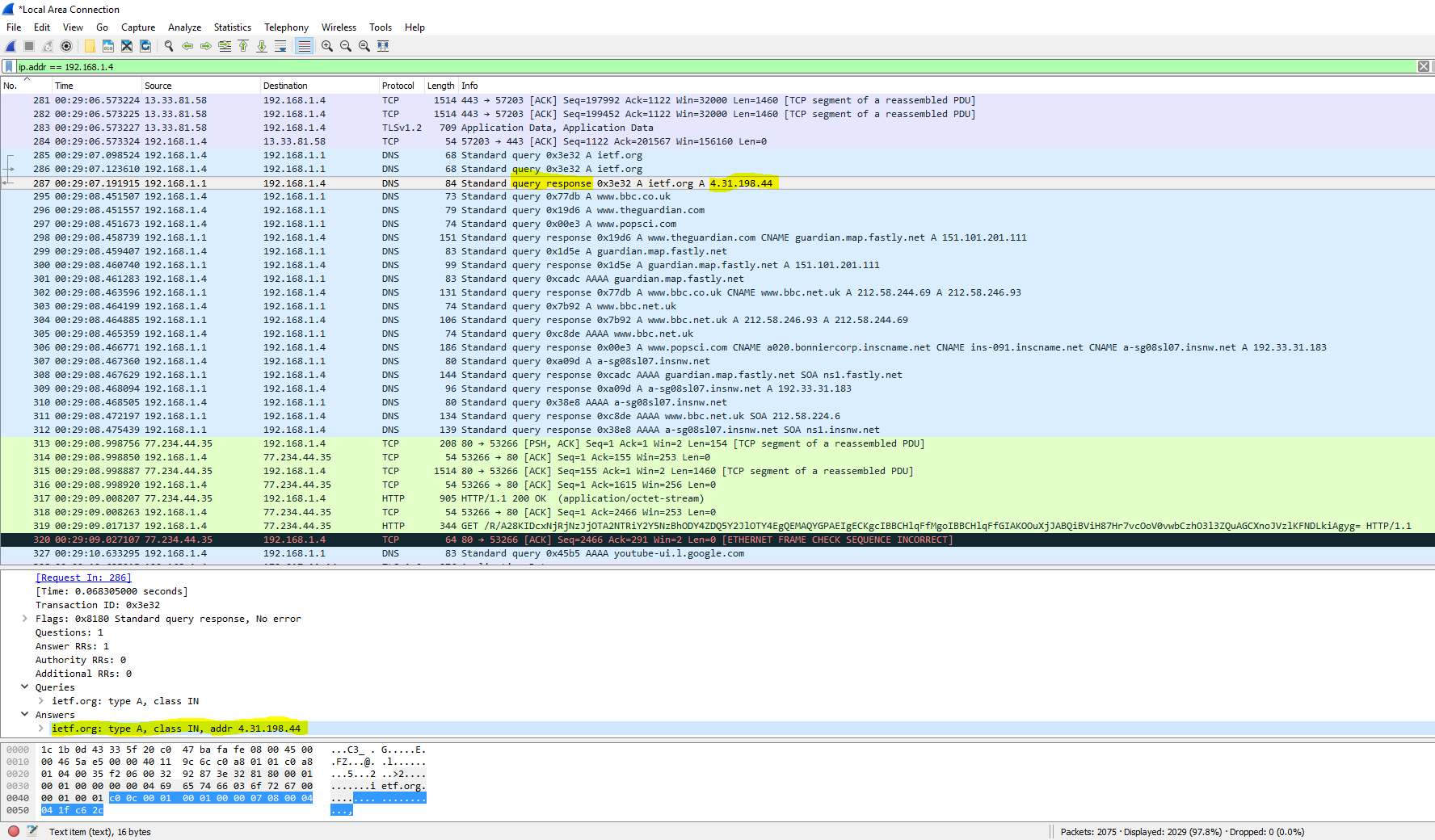


1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

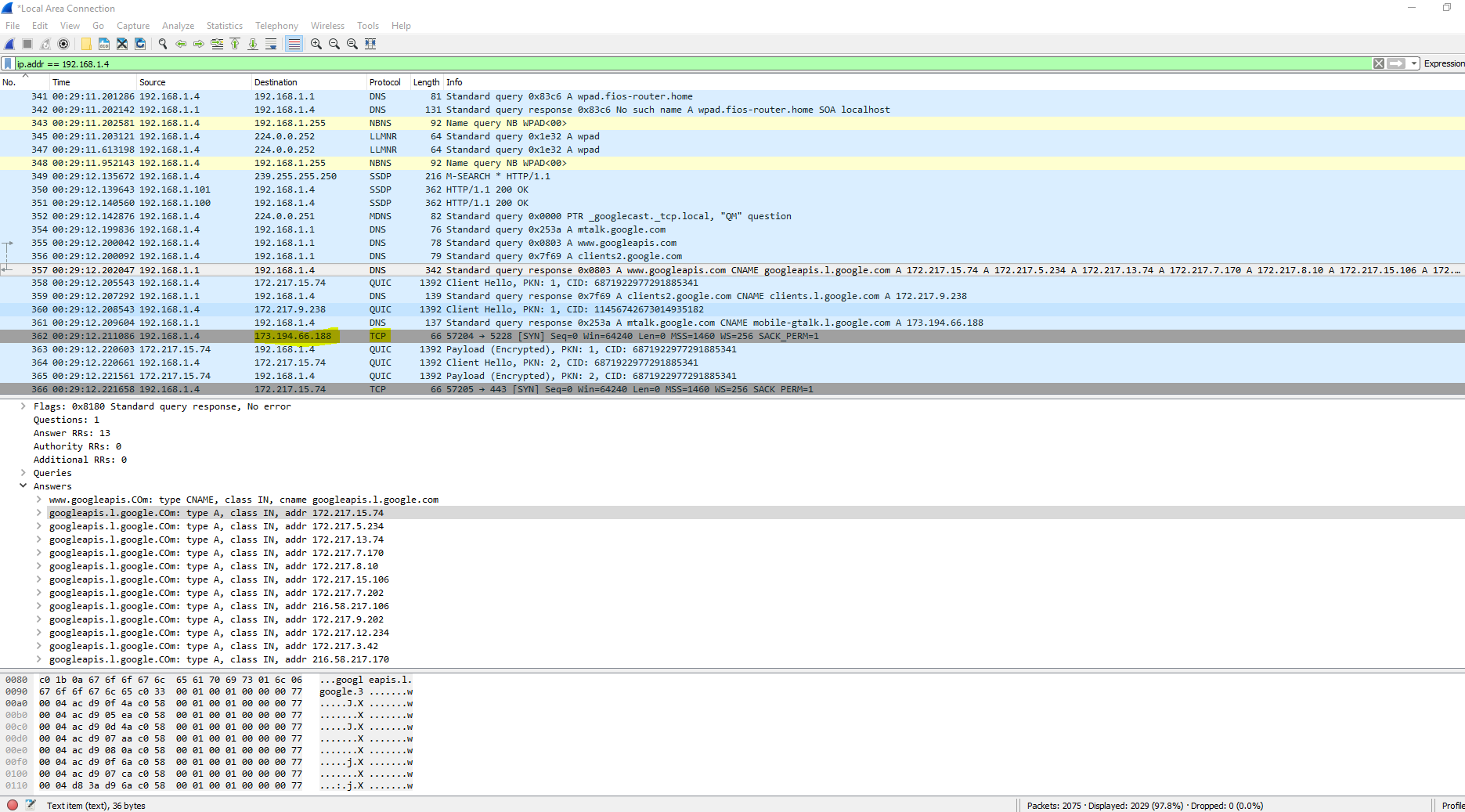
* The message is a Standard query with 0 answers. 

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

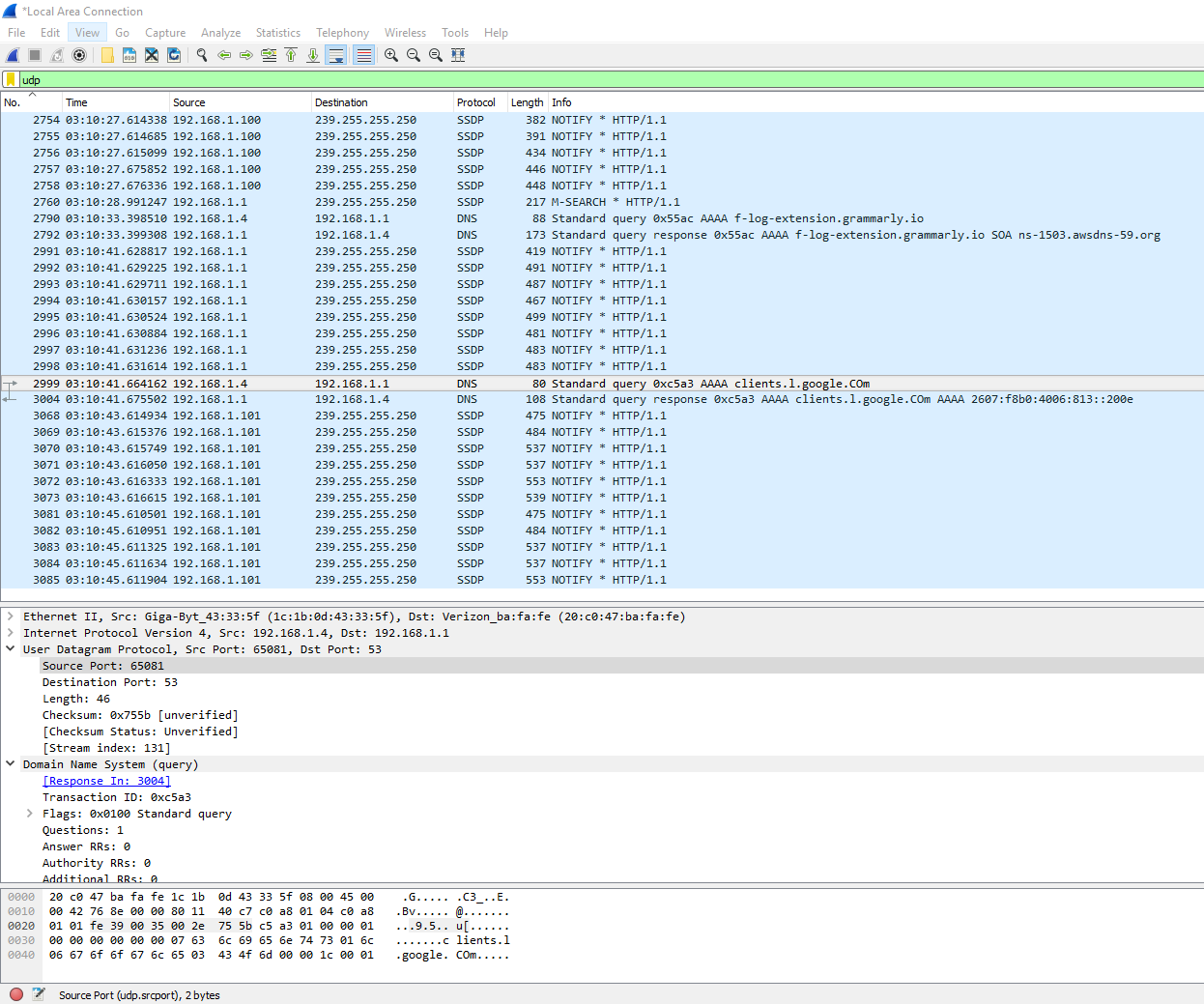
* In the response message, there is 1 Answer. The answer contains the name, type, class, and IP address of the website. (ietf.org, type A, class IN, and IP address 4.31.198.44)



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?

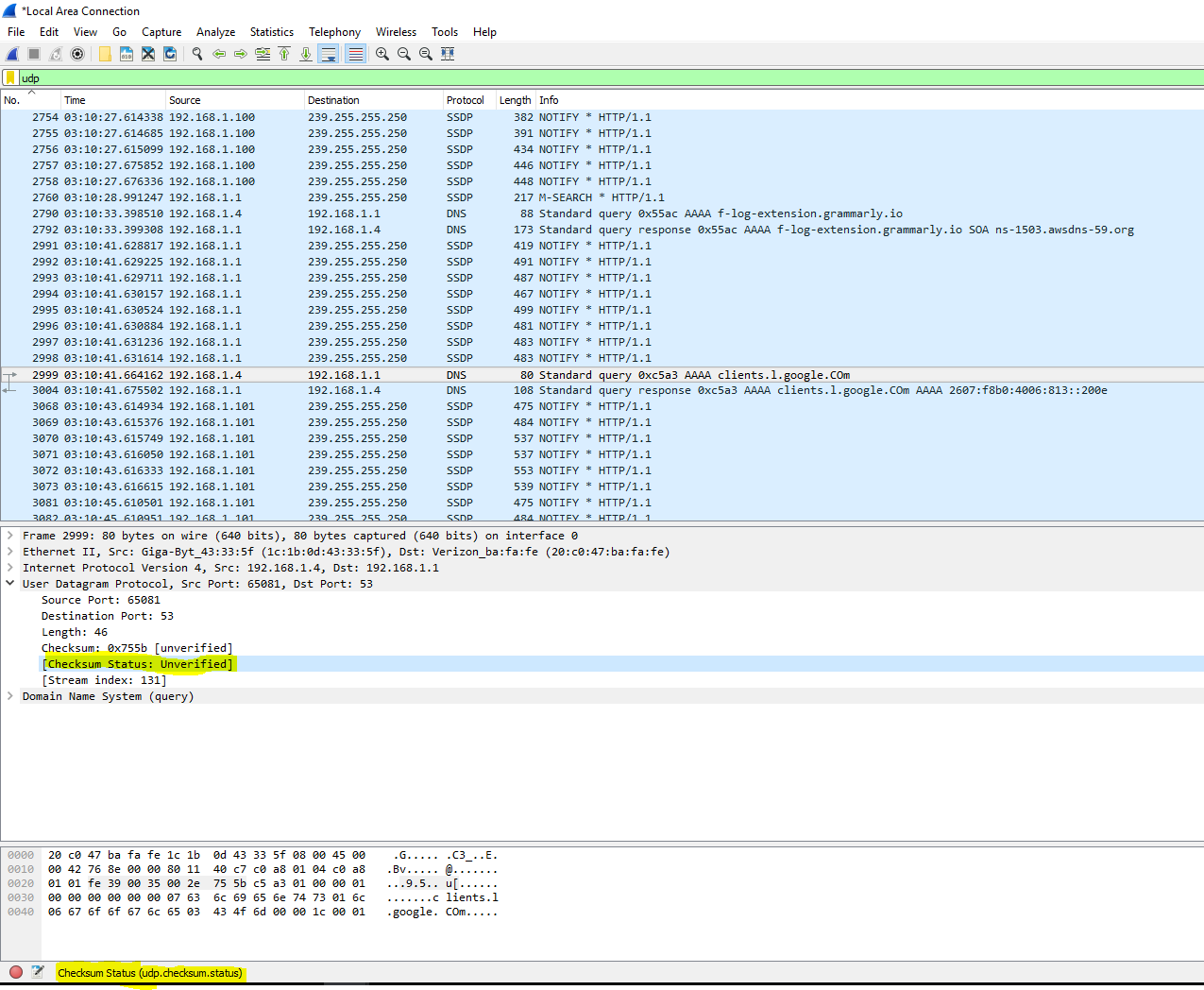
* The IP address found in the DNS response for ieft.org was not the same destination IP address for the next TCP SYN packet. The destination was 173.194.66.188, a google server, while the first query response contained an IP address of 4.31.198.44.

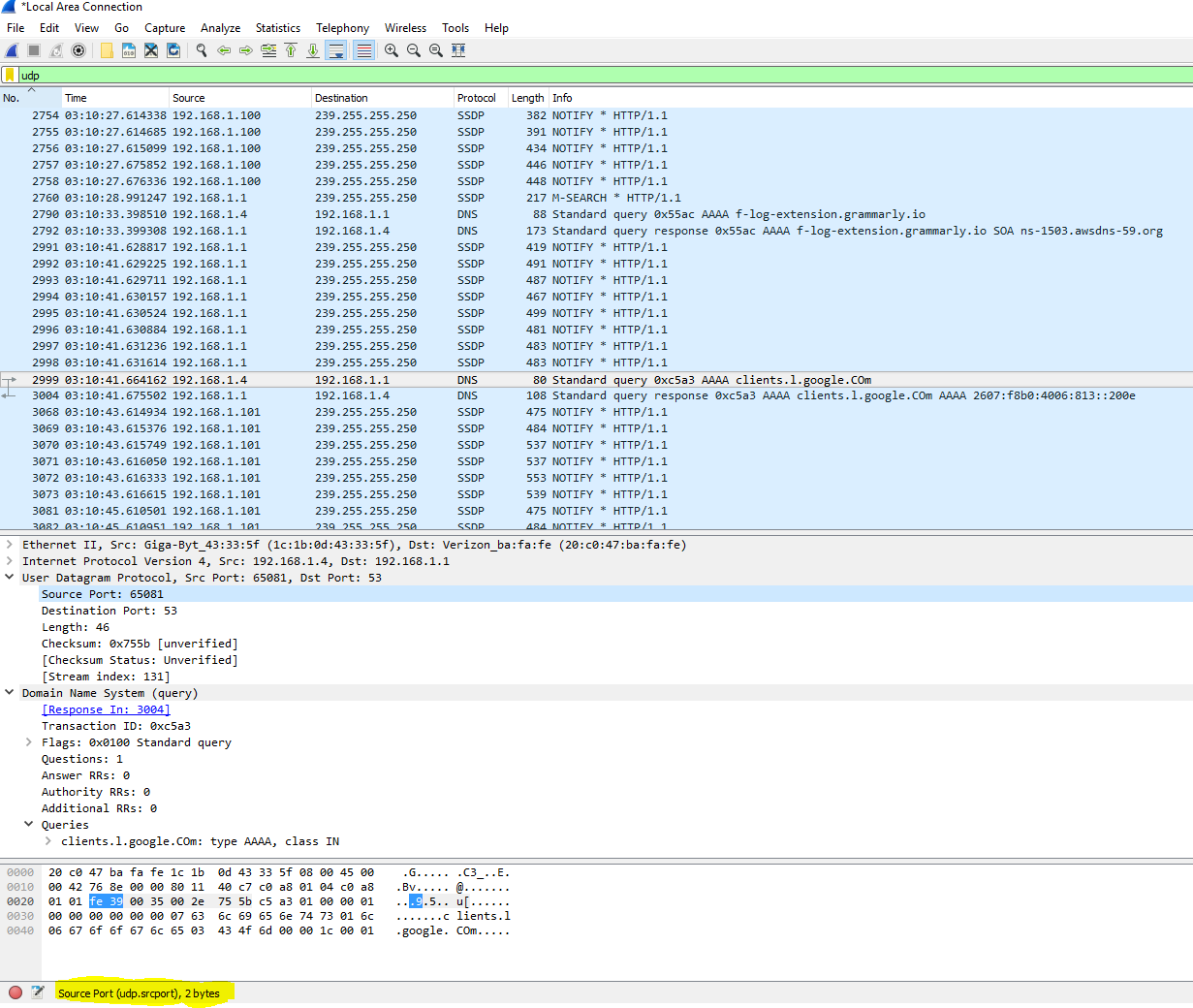
1. Select *one* UDP packet from your trace. From this packet, determine how many fields there are in the UDP header

* There are 6 fields within the UDP section of the packet: Source port, Destination port, Length, Checksum, Checksum Status, and Stream index. 

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 fields.

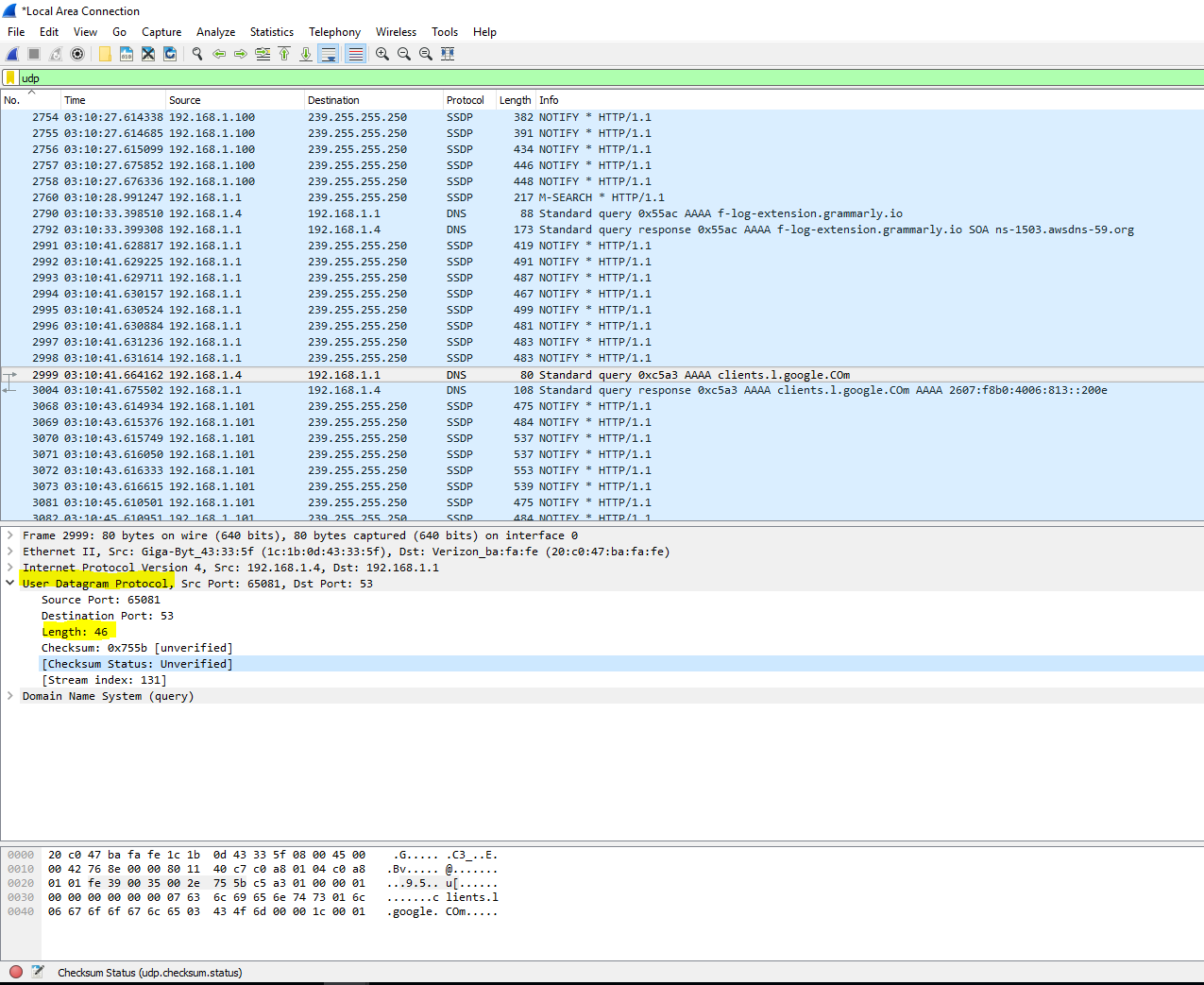
* Checksum Status and Stream index contained were unknown



* The rest were 2 bytes each. The screenshot shows the first field, source port, as proof.
* 

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

* The length field is the UDP header bytes and payload data bytes.



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

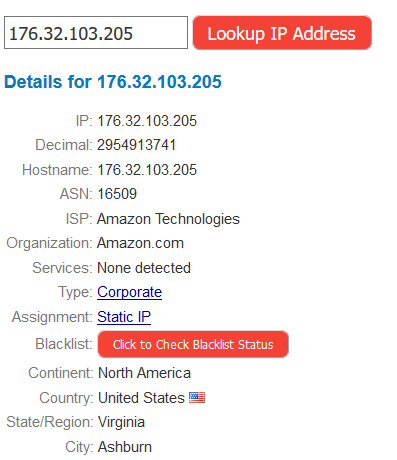
* The ping command sends packets of data to a specified address. These packets are sent back and tells the user the round-trip time and whether the packet was lost.
* In Figure 1, the user used the ping -n 10 command: the -n is the count value of pings that are going to be sent to the specified address, in this case 10, to IP address 176.32.103.205. The user received all 10 packets back and the average round trip time was 25 ms.

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

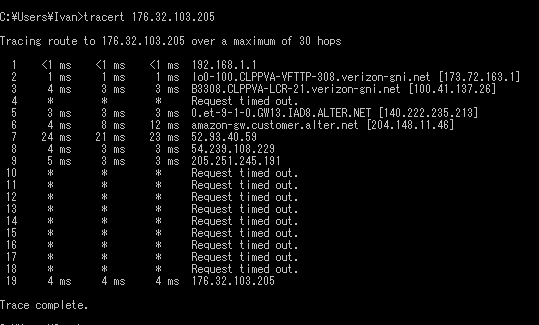
* Internet Control Message Protocol (ICMP) is used for the ping command

1. Who owns the IP?

* Amazon owns the IP

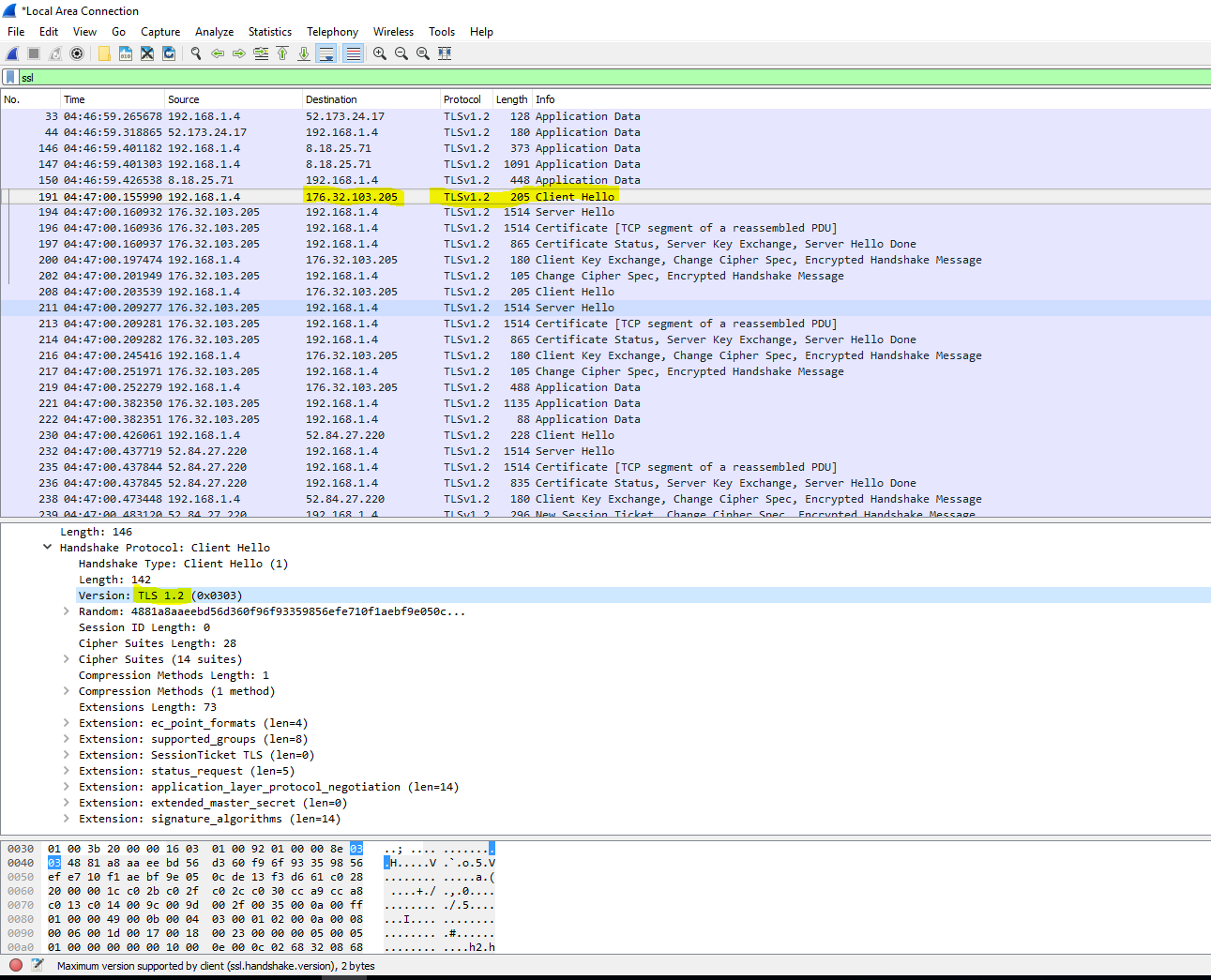


1. In addition to a screenshot, in a tabular form, list all the hops between your computer’s IP and the IP address in Figure 1. The table should include the owner, and location of the IP address.



|  |  |  |  |
| --- | --- | --- | --- |
| Hop # | IP Address | Owner | Location |
| 1 | 192.168.1.1 | Ivan Cruz | Culpeper, VA |
| 2 | 173.72.163.1 | Verizon Fios | Culpeper, VA |
| 3 | 100.41.137.26 | Verizon Internet Services | Culpeper, VA |
| 4 | Request timed out | | |
| 5 | 140.222.235.213 | ANS CO+RE System | Purchase, NY |
| 6 | 204.148.11.46 | Verizon Business | Los Angeles, CA |
| 7 | 52.93.40.59 | Amazon.com | Seattle, WA |
| 8 | 54.239.108.229 | Amazon.com | Ashburn, VA |
| 9 | 205.251.245.191 | Amazon.com | Ashburn, VA |
| 10-18 | Request timed out | | |
| 19 | 176.32.103.205 | Amazon Technologies | Ashburn, VA |

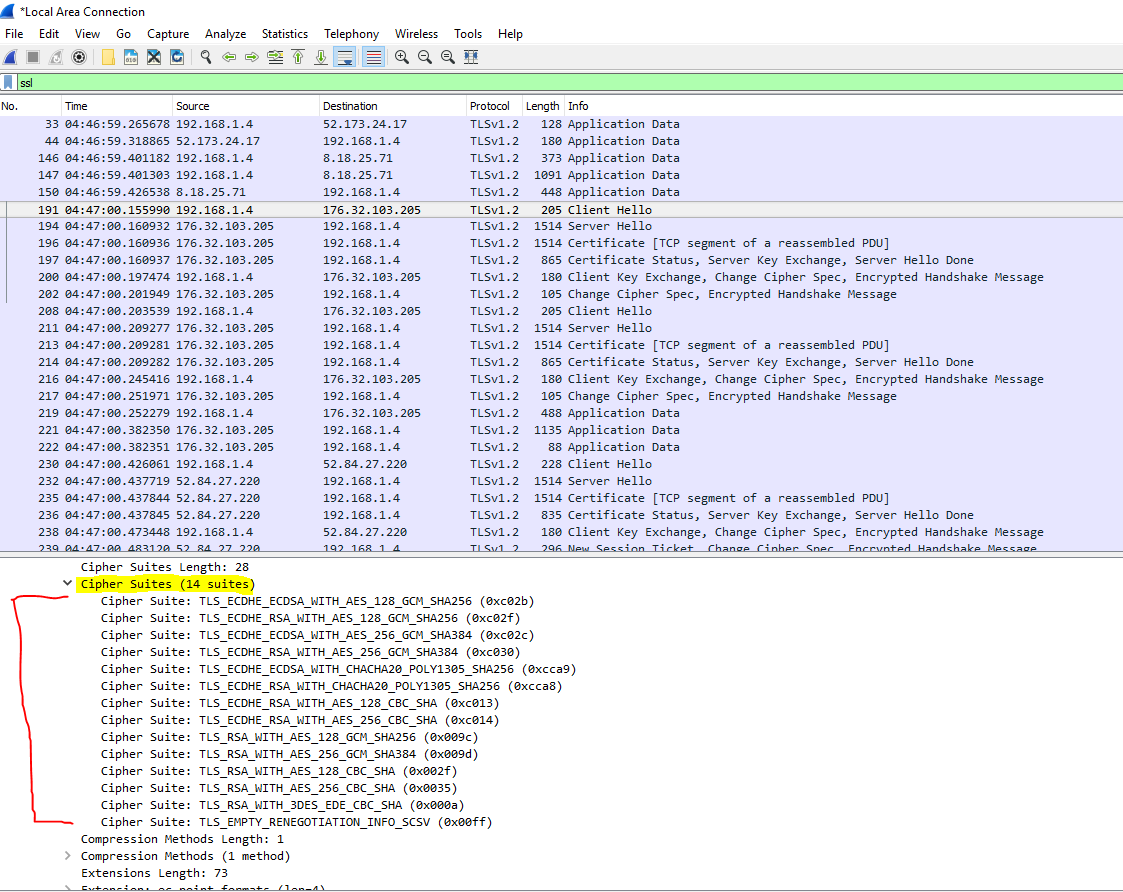
1. What version of TLS does the IP above use? Hint: Visit the website of the owners IP address, and capture the “Client Hello” packet.

* 176.32.103.205 uses TLS version 1.2

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

* There is a total of 14 different combinations of algorithms (Cipher Suites)

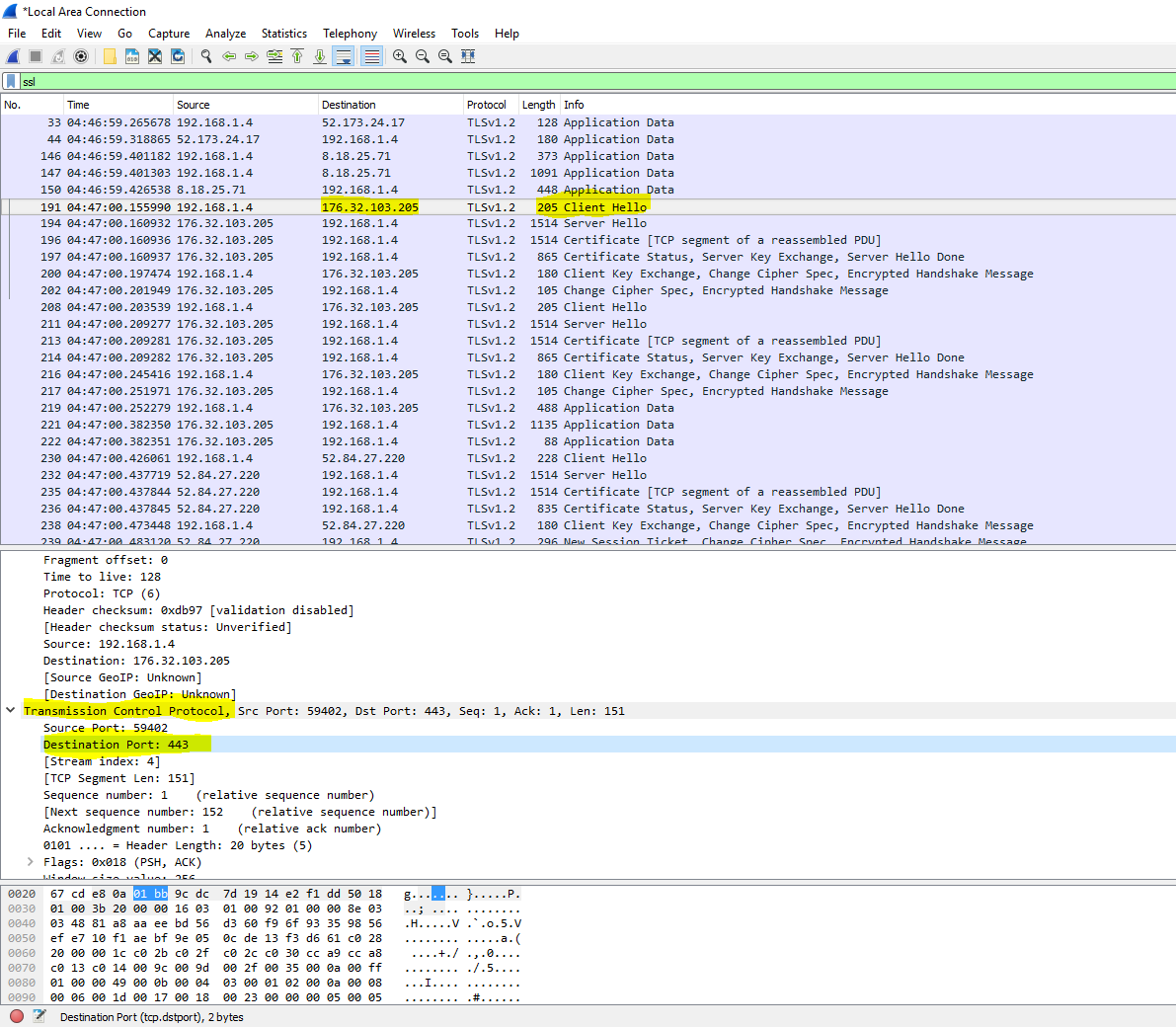
1. TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
2. TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
3. TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
4. TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
5. TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256
6. TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256
7. TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
8. TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
9. TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
10. TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
11. TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
12. TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
13. TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
14. TLS\_EMPTY\_RENEGOTIATION\_INFO\_SCSV



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

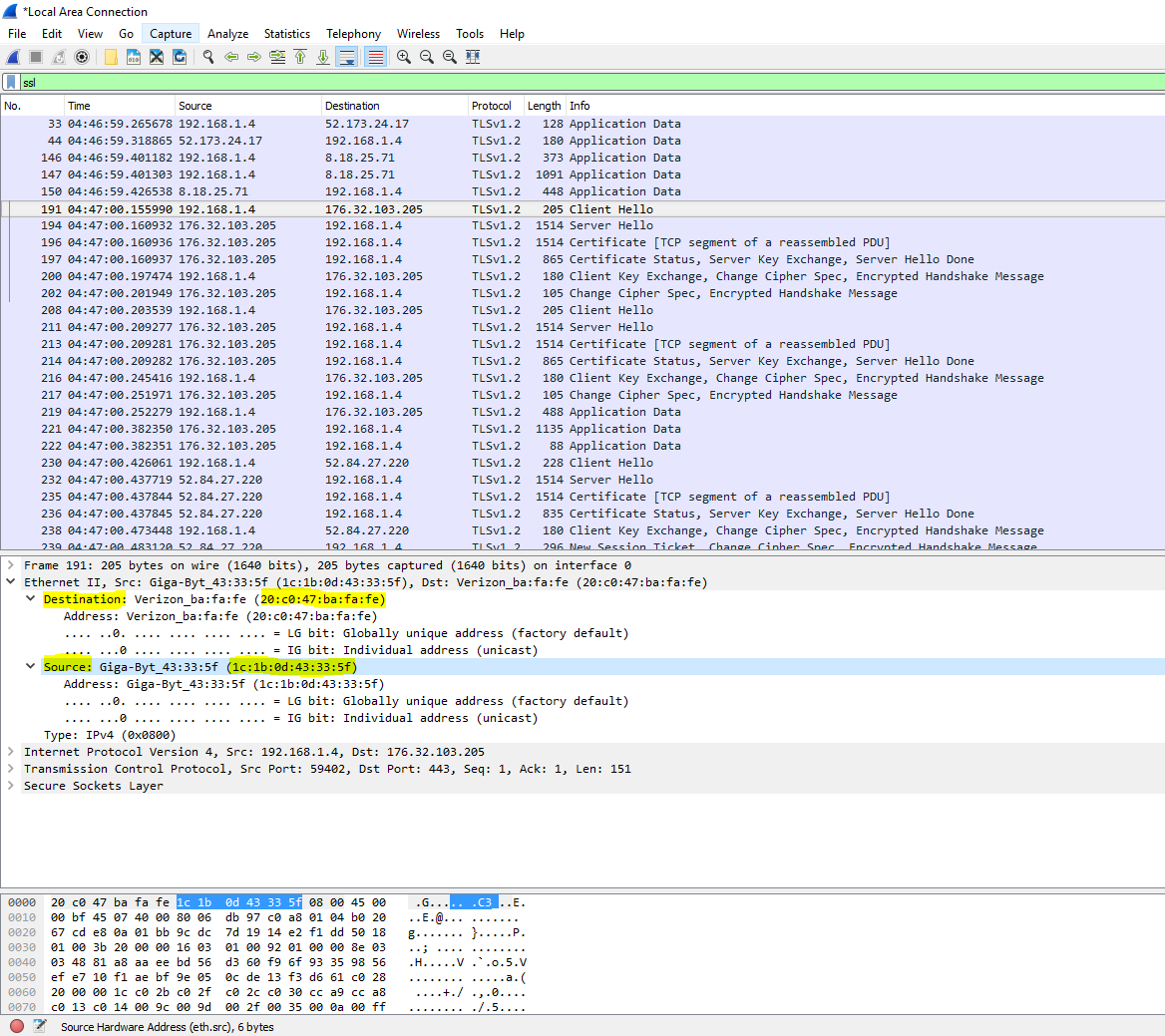
number?

* The “Client Hello” packet uses port number 443 because it is using HTTPS and not regular HTTP (port 80). Amazon uses HTTPS to secure their customer’s data.



1. What are the source and destination MAC address?

* The Source MAC address is 1c:1b:0d:43:33:5f
* The Destination MAC address is 20:c0:47:ba:fa:fe

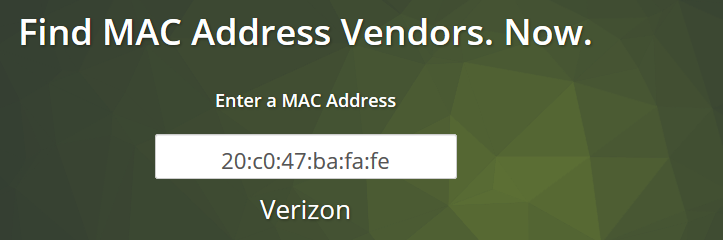


1. Identify the company that manufactured the network cards with the MAC address identified in 8 above. (Hint: there are a lot of websites you can use to lookup MAC address, just like you would for an IP).

* Giga-Byte Technology manufactured the Source machine’s network card



* Verizon is the company that manufactured the Destination machine’s network card



Extra Credit:

GitHub link: <https://github.com/ivangcruz/wireshark_labs>