Wenjie Xu Wireshark Final Exam

Instructions:

• This exam is due on May 1st, 2018 at 6:30 pm (beginning of class). I will NOT accept any submission after the specified date and time. If you have an excuse, let me know on time. (However, if it is an emergency, we can work it out. I might request for a proof.)

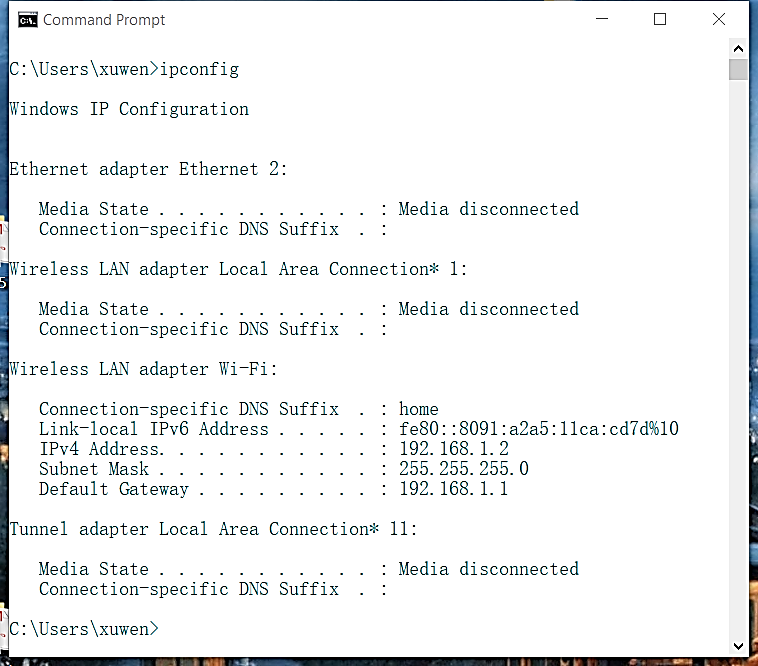
• For every response, you should take a screenshot and type the answer. I will NOT grade any question that does not have a screenshot, and a written response. Don’t expect me to look for the answers from the screenshot. TYPE it. Partial answers will not be graded.

• Before you begin, take a screenshot and type your computer’s IP address. If your IP changed at any point. Then you must retake the screenshot and TYPE the IP address again. (Example, if today you answered question 1, 2, and 3 using IP 10.10.10.1, and tomorrow your IP changed to 10.30.20.19. You can continue; but, you MUST take another screenshot for the new IP. If you fail to do this, I will not grade any subsequent questions.)

• If you can’t afford printing, let me know on time. We can work something out. However, if you choose not to print till the last minute, and encounter errors on the day of submission. Then I can’t help you.

• If a question is not clear, make note of it, and we will discuss it in the next class.

• Email me if you have any concerns.



My computer IP address:

192.168.1.2

Visit: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

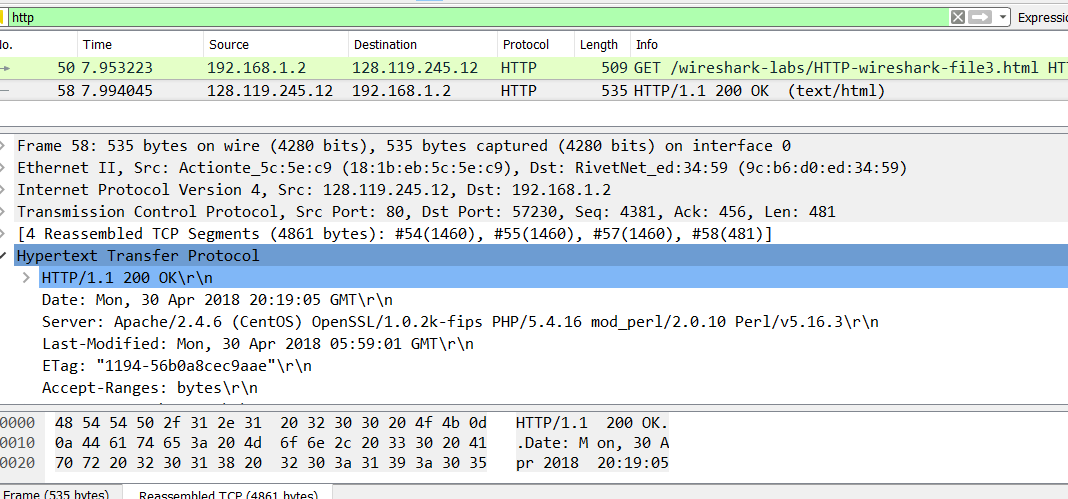
1. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

Answer: My browser sent 1 HTTP GET request. The packet 50 contains the GET message for the file link.



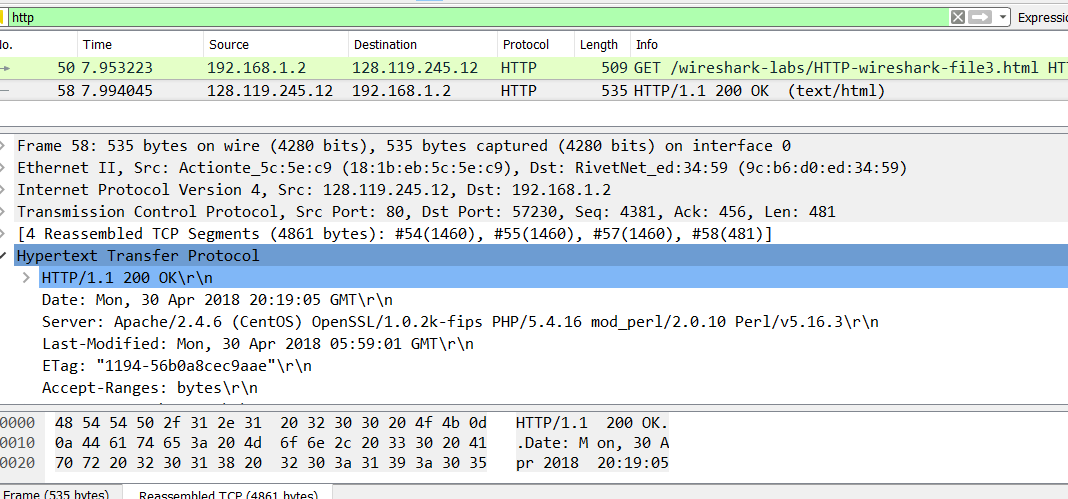
2. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Answer: Packet 58 contains the status code and phrase related with the response to the browser request.



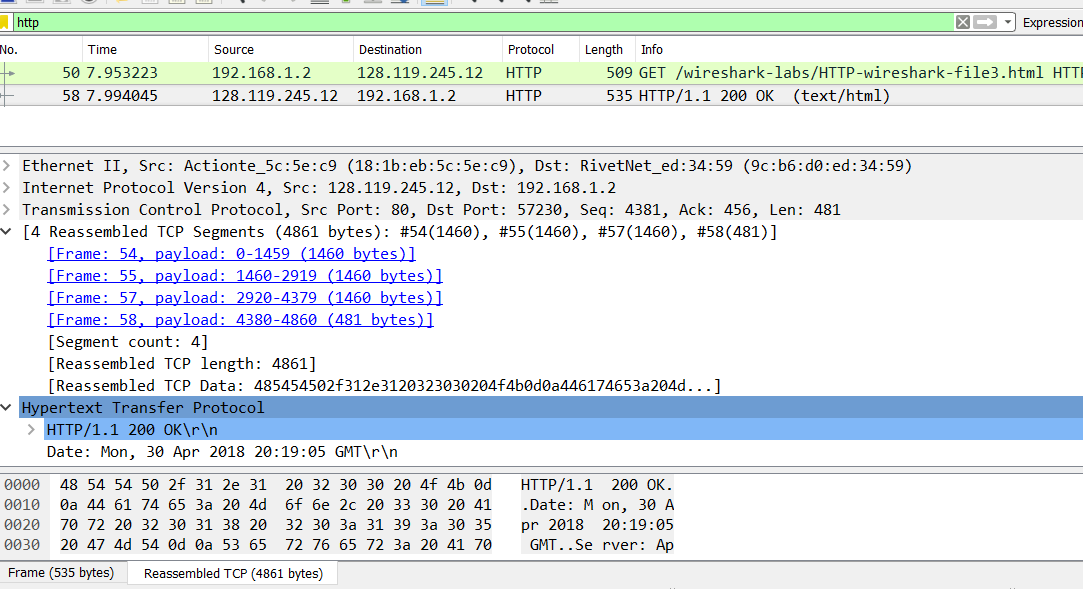
3. What is the status code and phrase in the response?

Answer: The status code and phrase in the response is 200 ok



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

Answer: There are 4 TCP needed to carry the single HTTP response and the corresponding text.

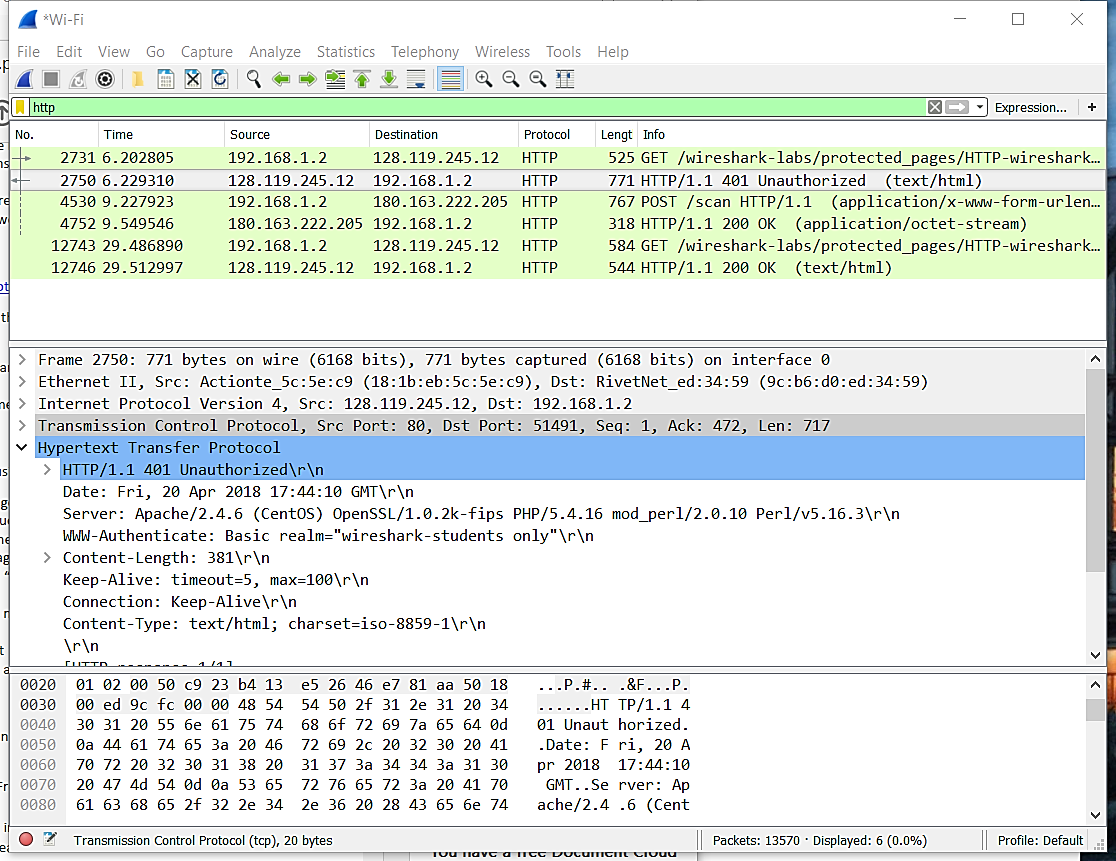


Visit: http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html

The username is “wireshark-students” (without the quotes), and the password is “network

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

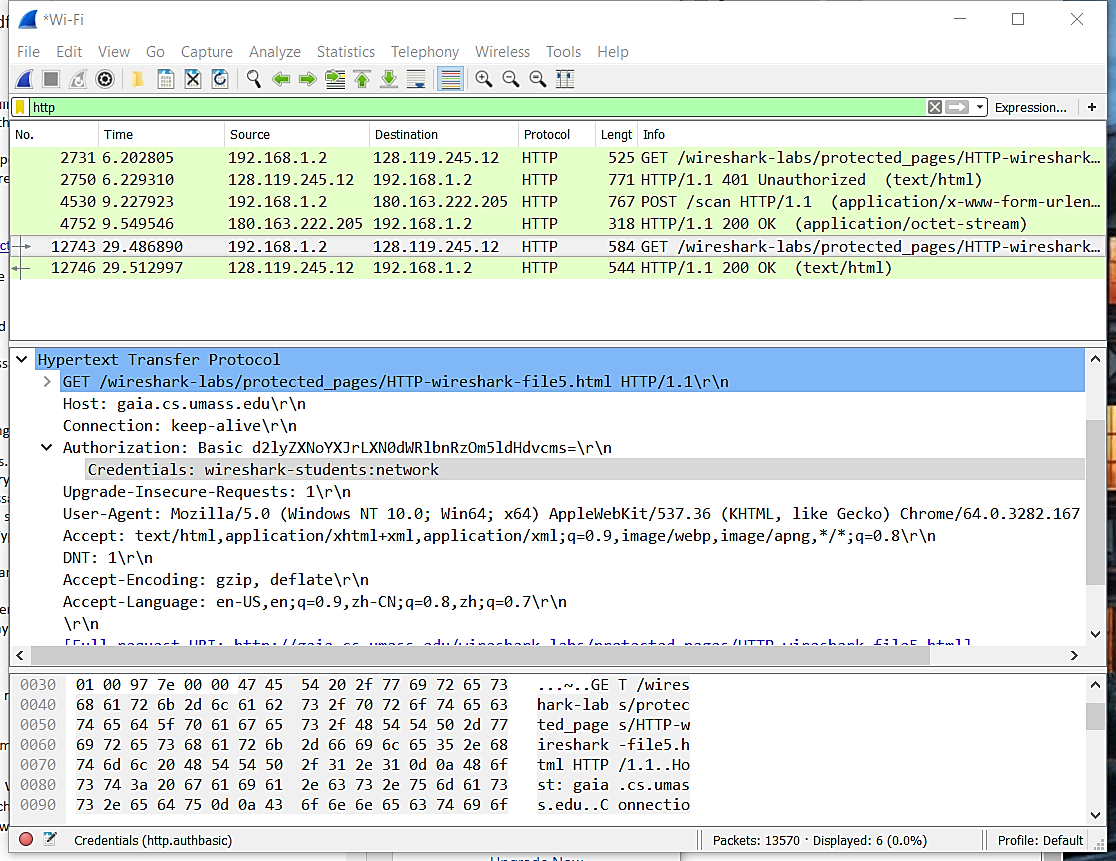
Answer: The server’s response to the initial GET message is 401 Unauthorized.



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

Answer: The new field is the Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n

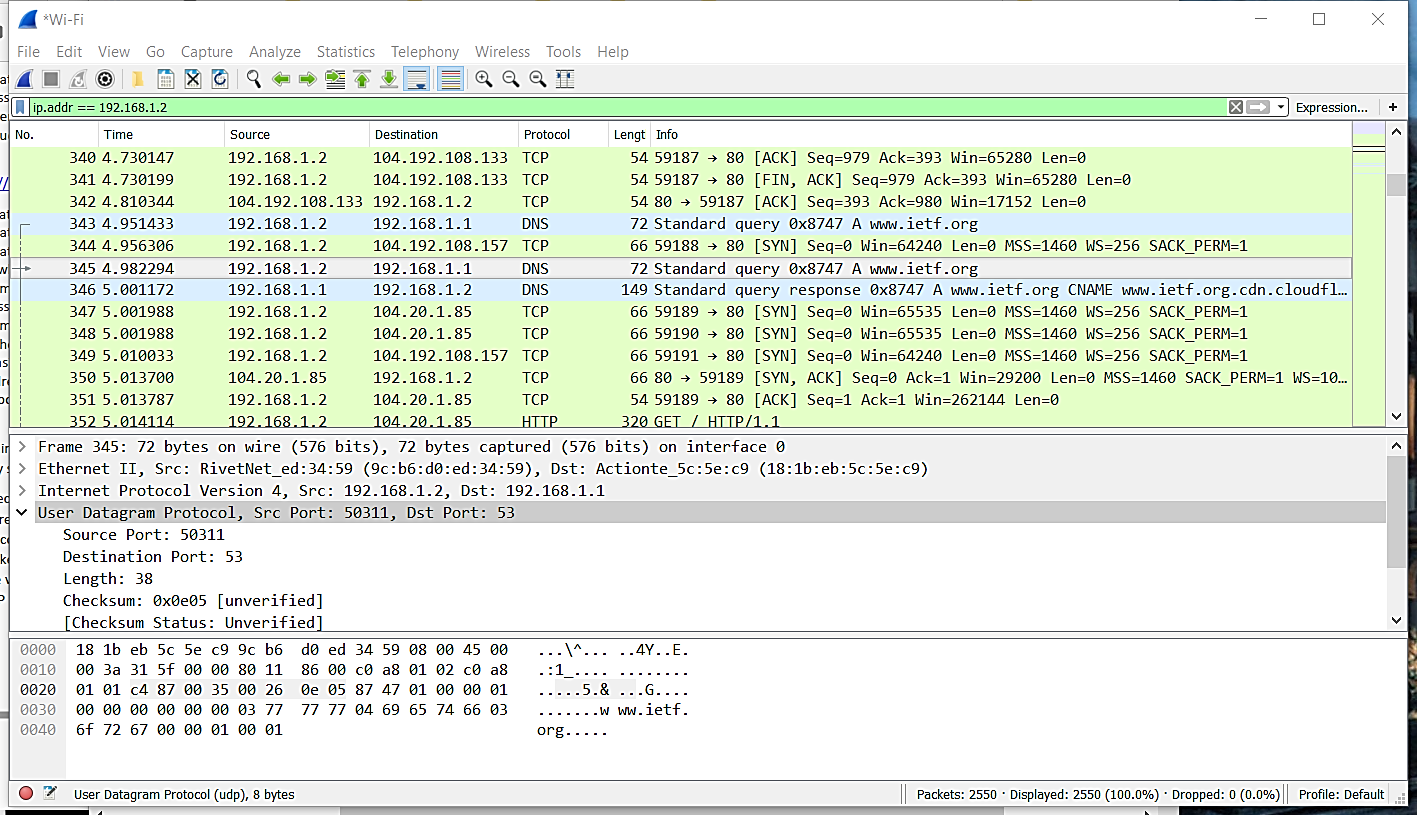
Credentials: wireshark-students:network which indicates the user name and the password.

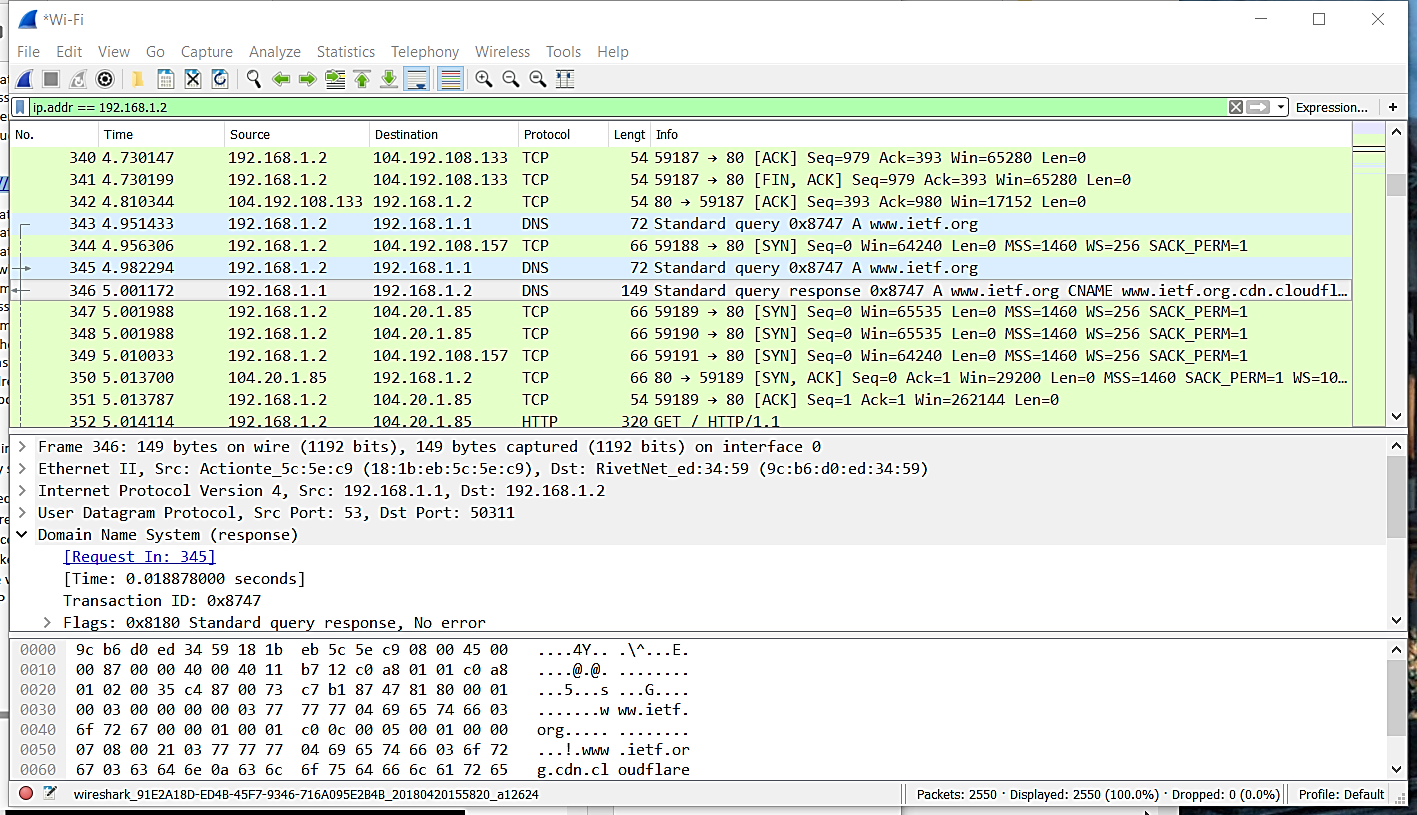


Visit: http://www.ietf.org (Hint: Filter Wireshark using “ip addr == your IP”)

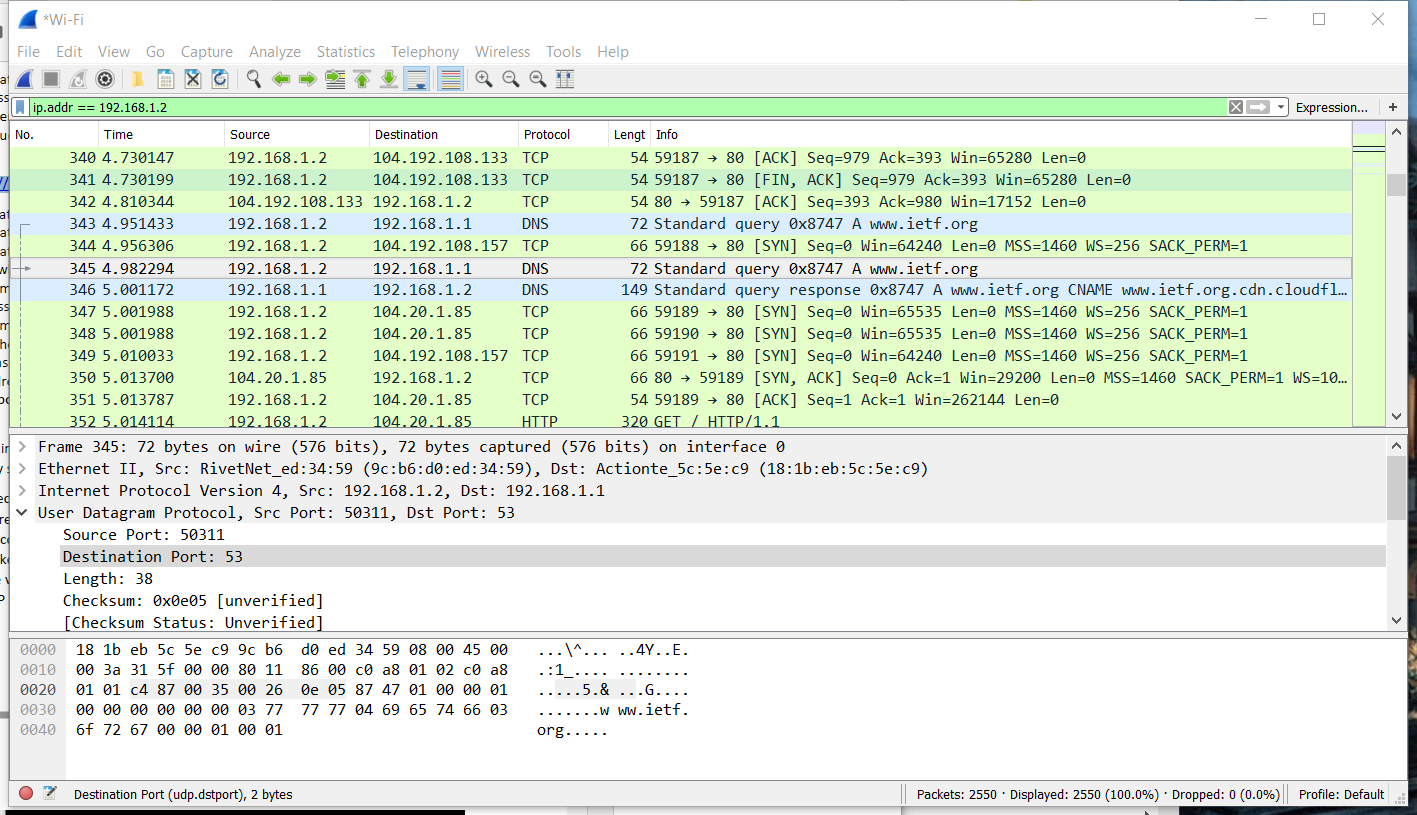
7. Locate the DNS query and response messages. Are they sent over UDP or TCP?

Answer: DNS query message is packet 345, response massage is packet 346. They are sent over UDP.



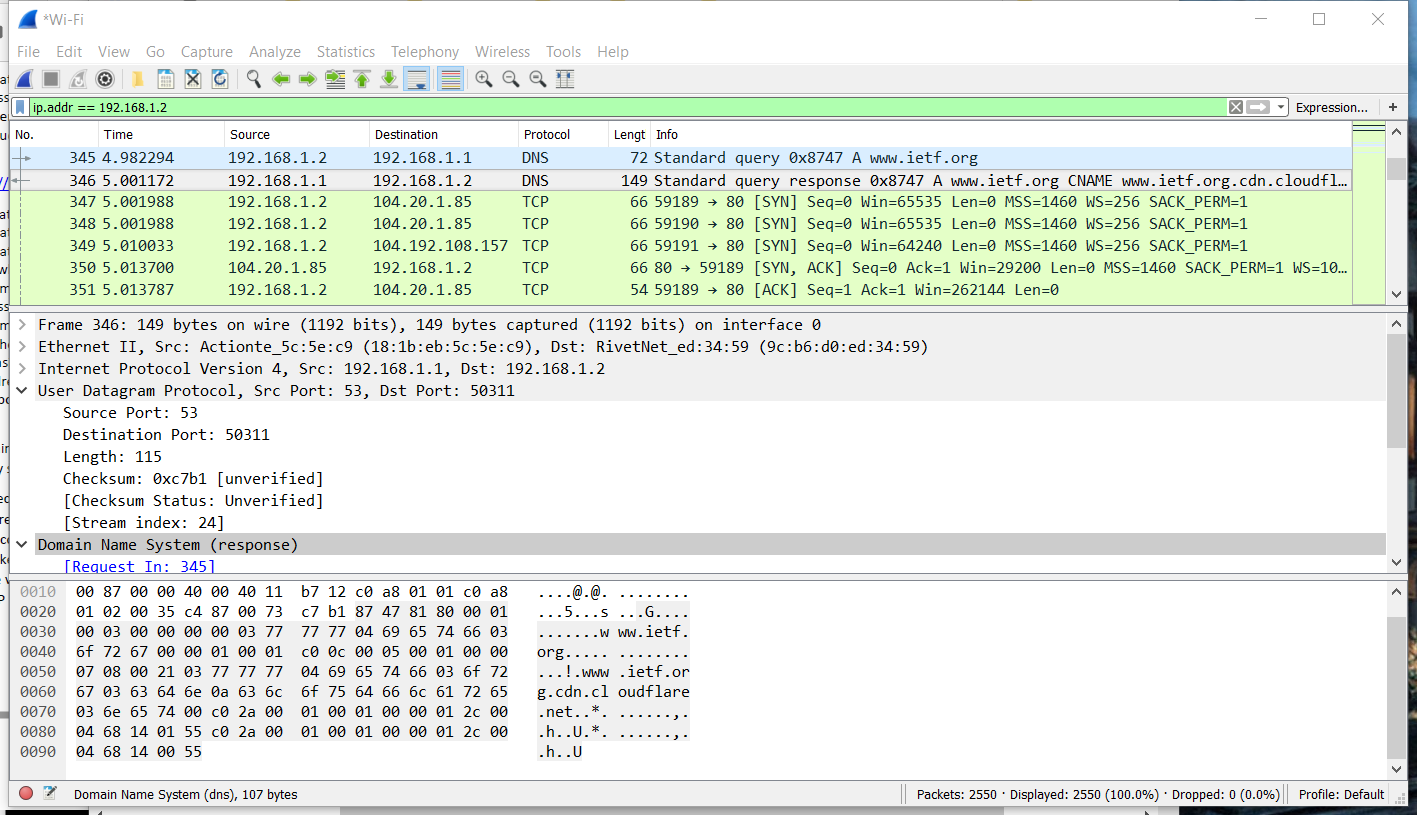


8. What is the destination port for the DNS query message?

Answer: the destination port for the DNS (IP 192.186.1.1) query message is 53

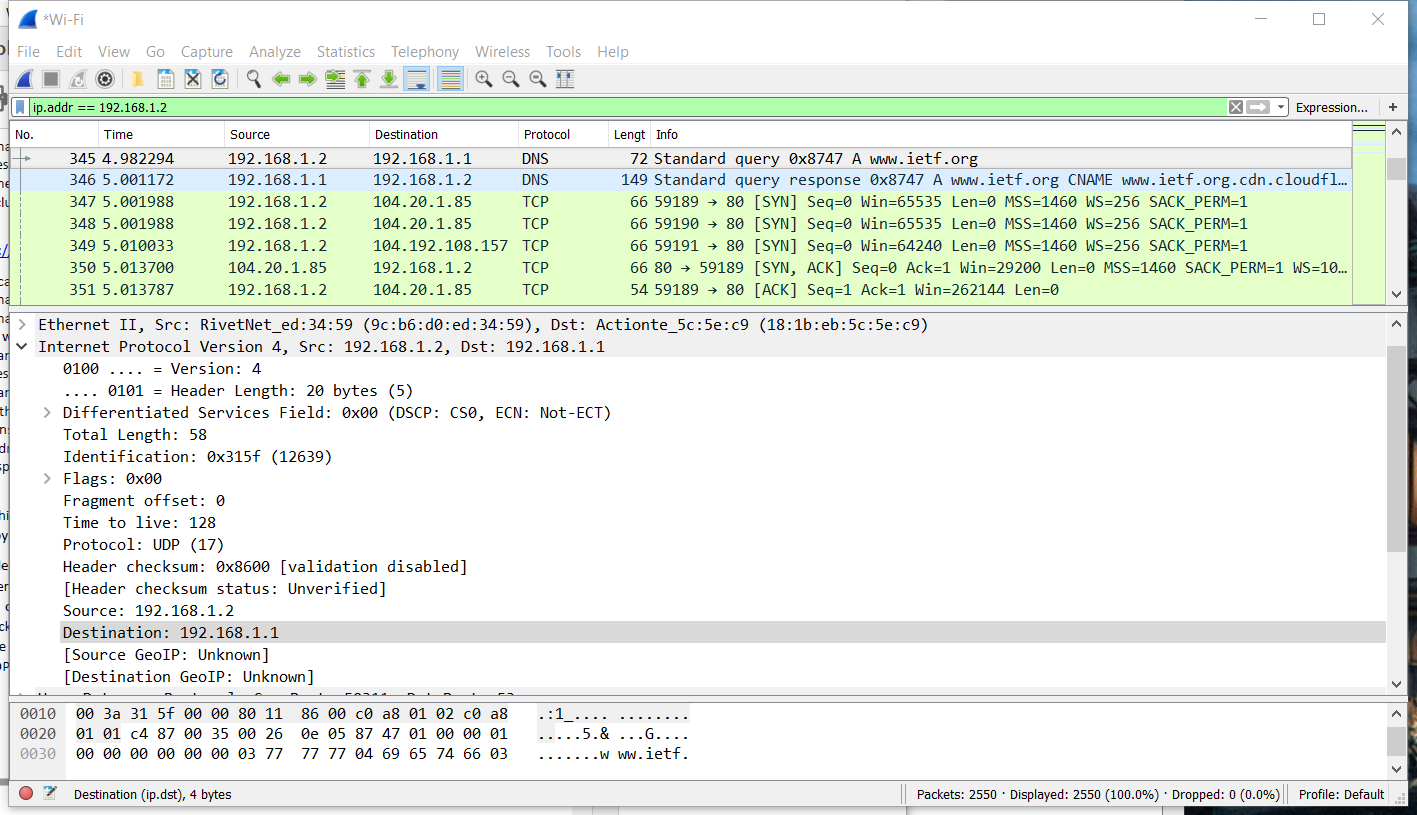
9. What is the source port of DNS response message?

Answer: The source port of DNS (IP 192.186.1.1) response message is 53



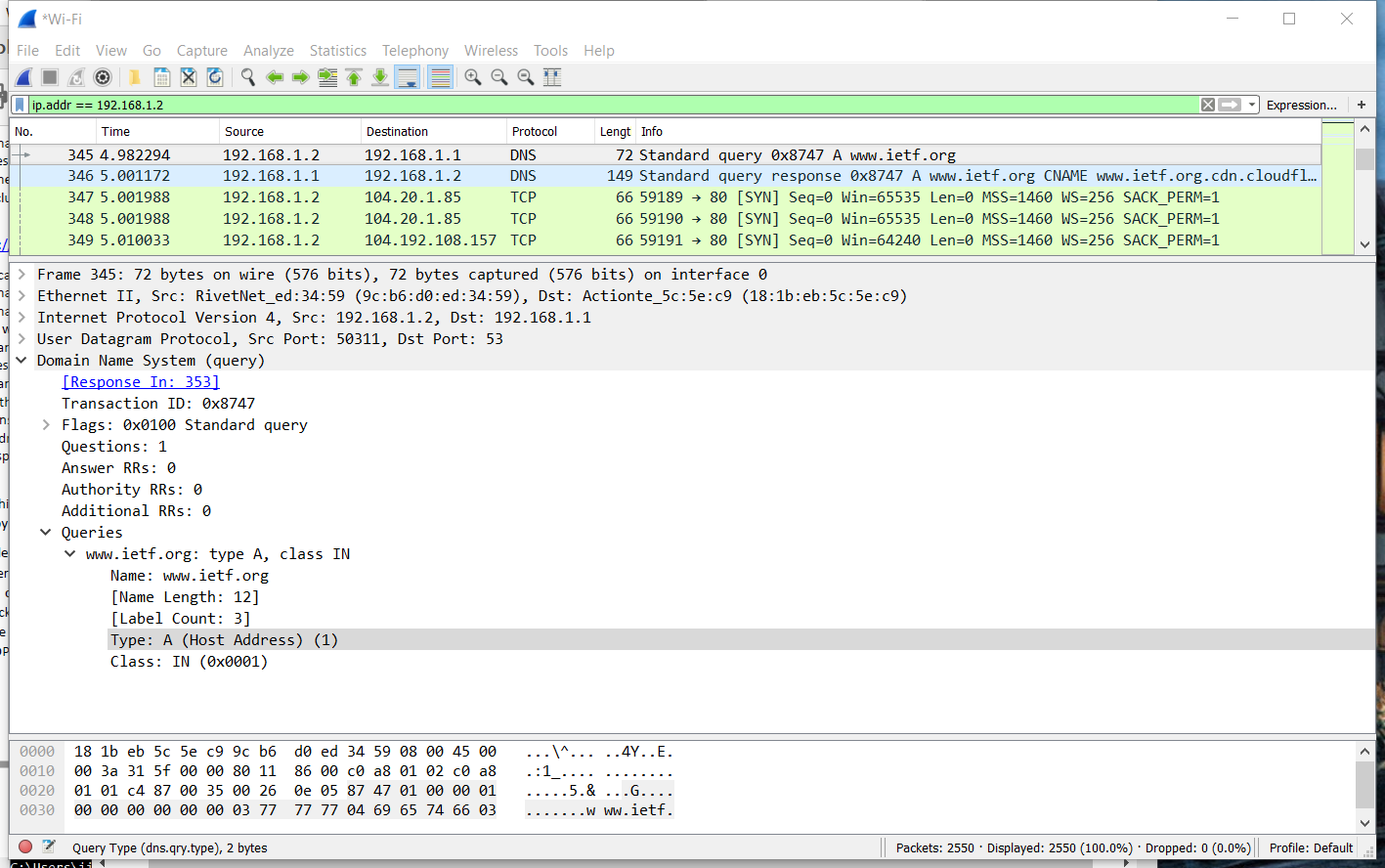
10. To what IP address is the DNS query message sent?

Answer: DNS query message is sent to IP address 192.186.1.1



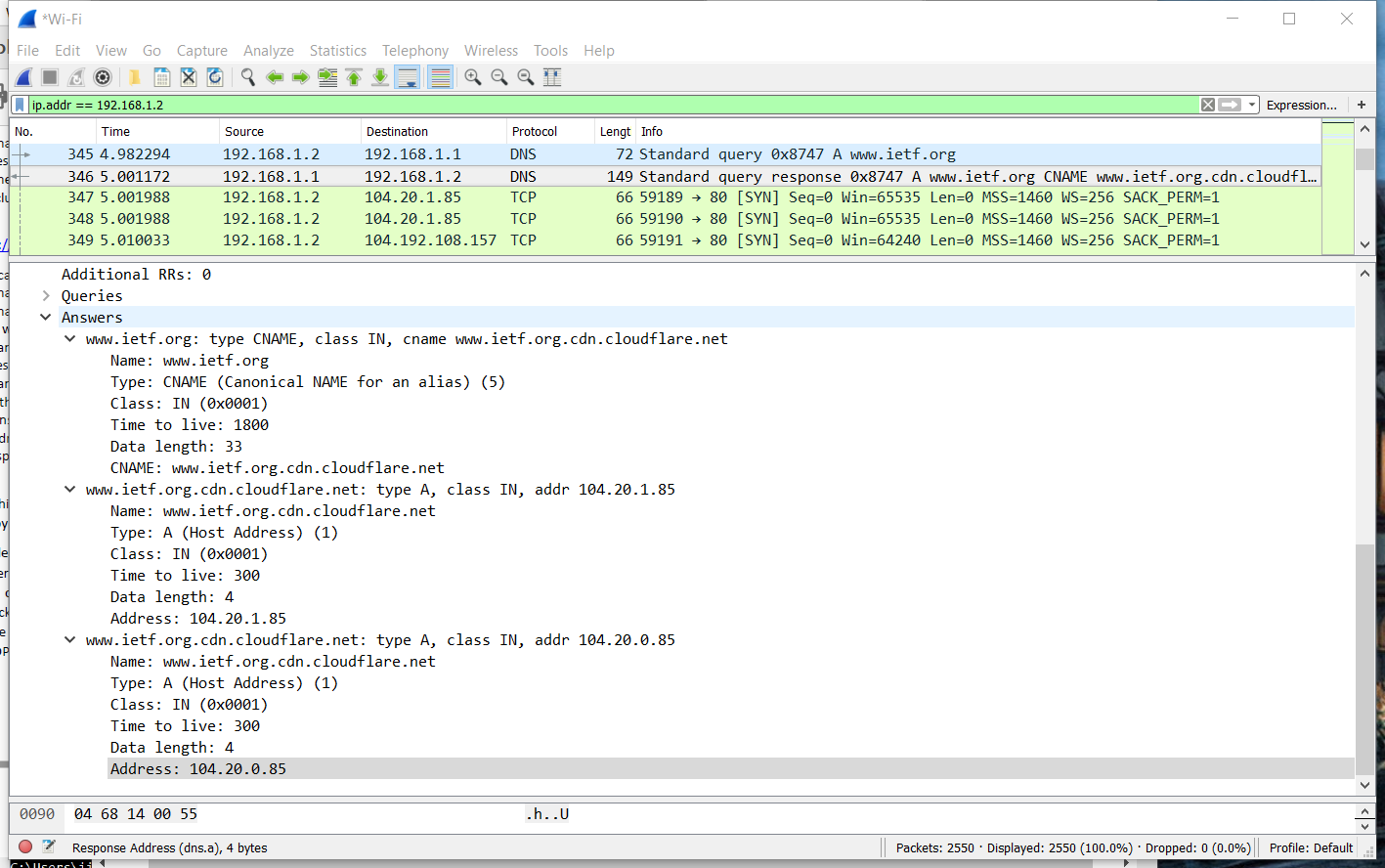
11. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: The type of DNS query is type A (host address). The query message has no “answers”

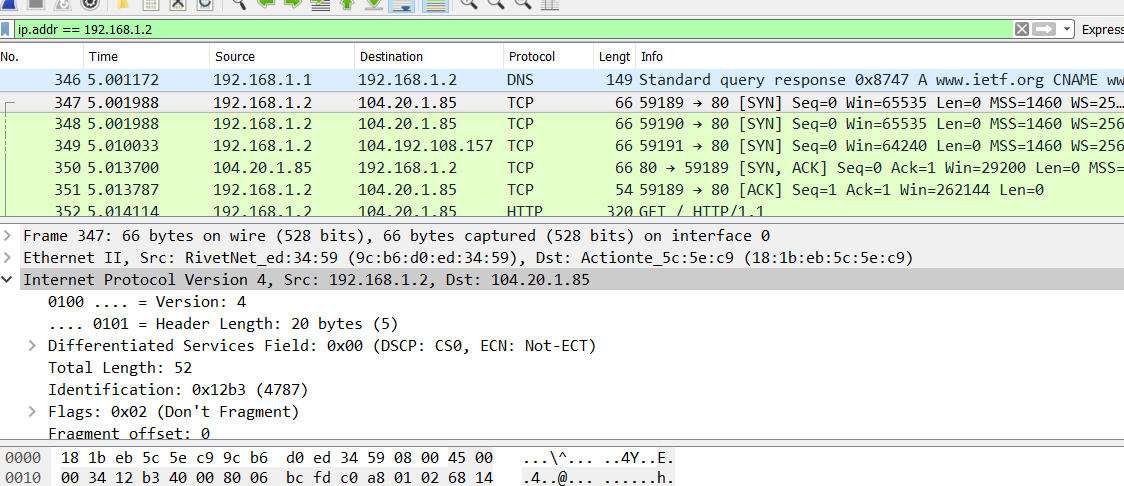


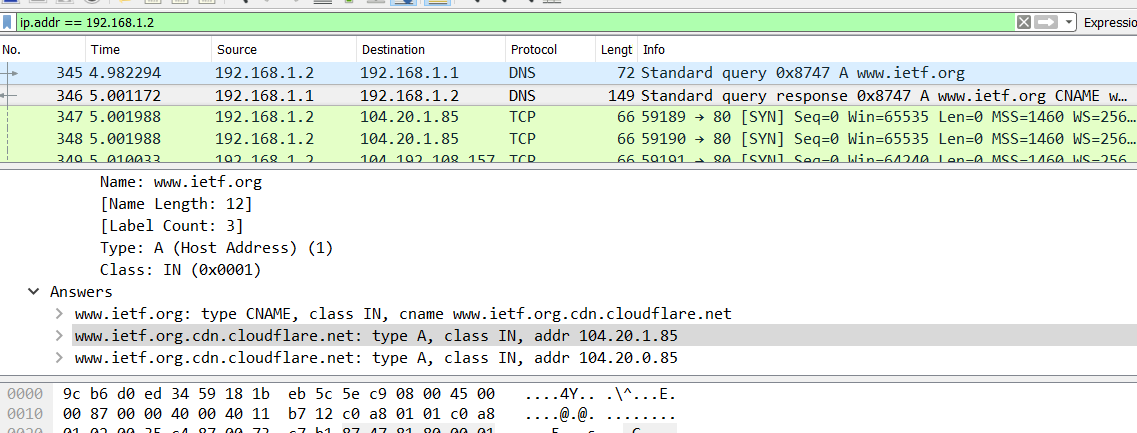
12. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Answer: There are 3 “answers” in the DNS response message. Each answer contains the domain name, type, class, time to live, data length, CName or IP address.



13. 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?

Answer: Yes, the destination IP address of the SYN packet is 104.20.1.85, the same as the second answer in the DNS response message.

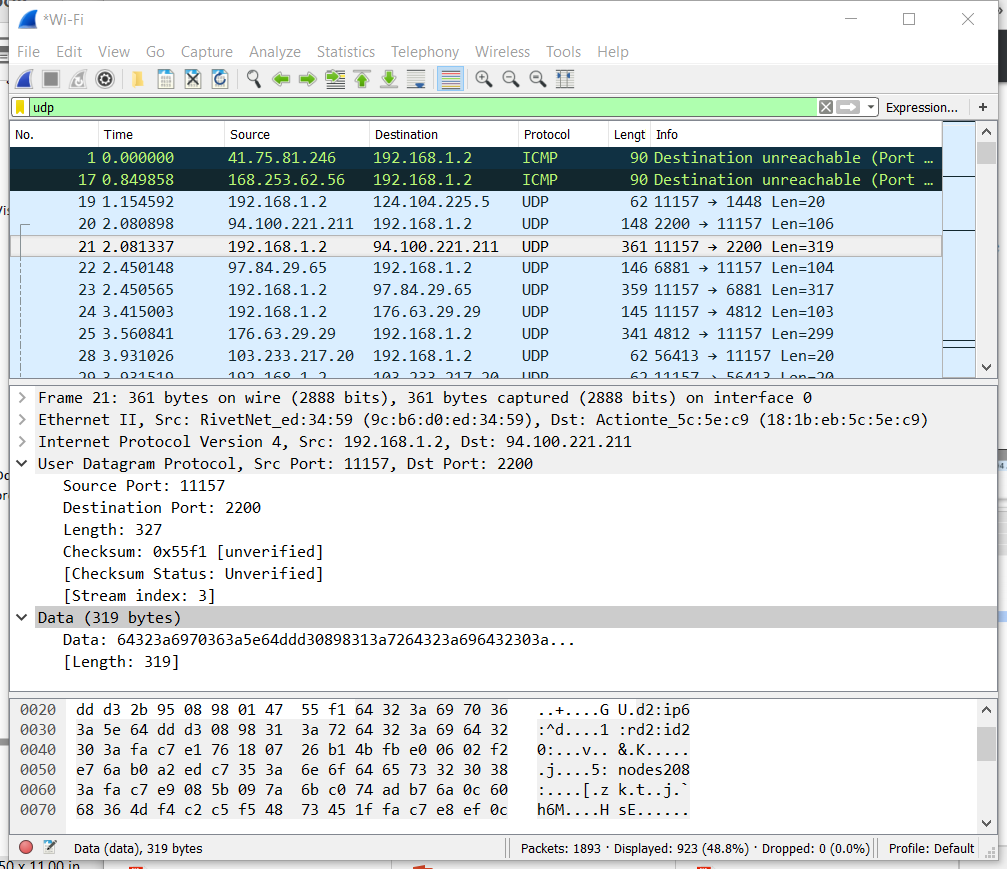
SYN packet IP address of the destination

DNS response message answer

Do something that will cause your host to send and receive UDP packets. (example: use SNMP protocol by sending an email).

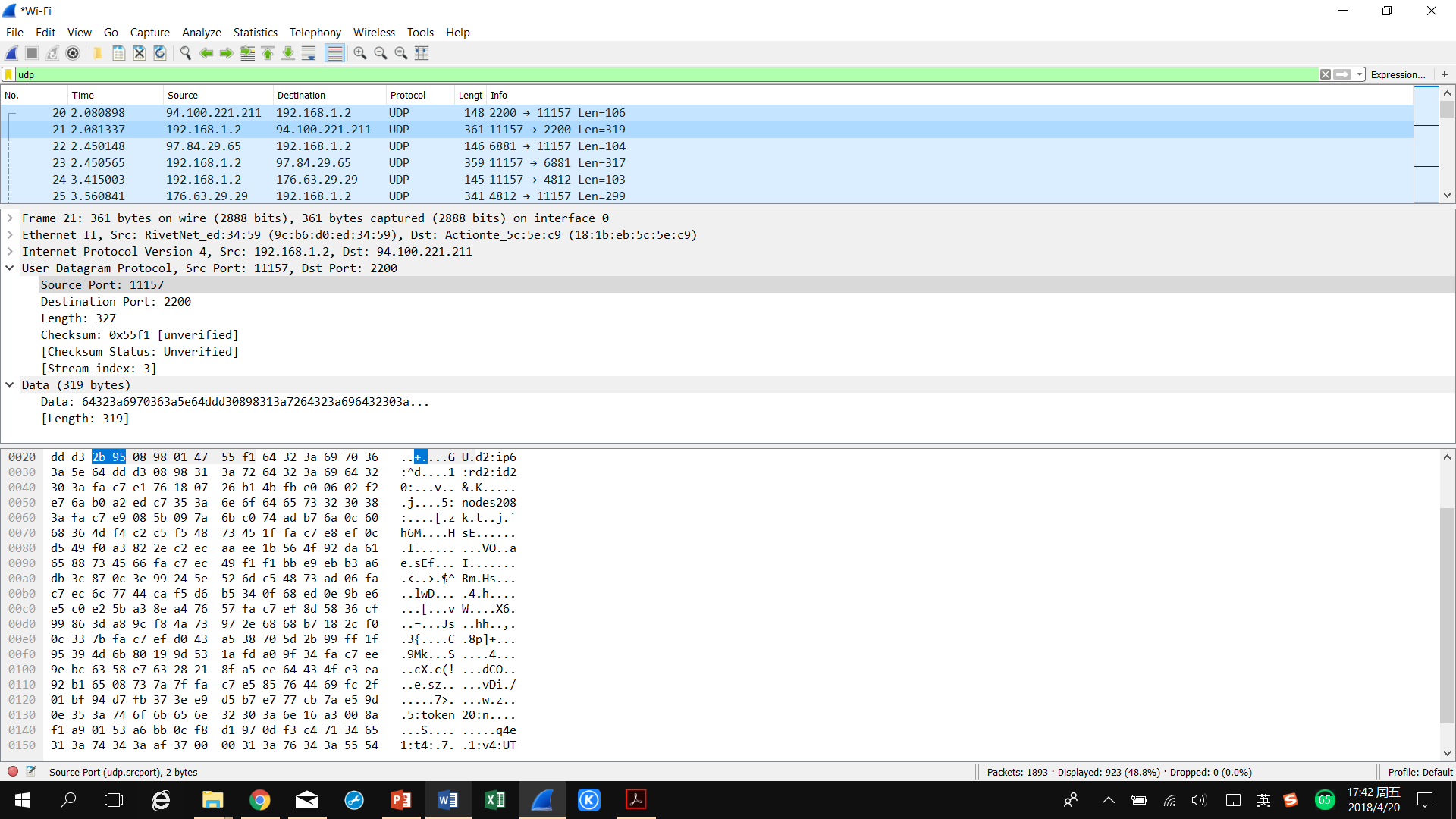
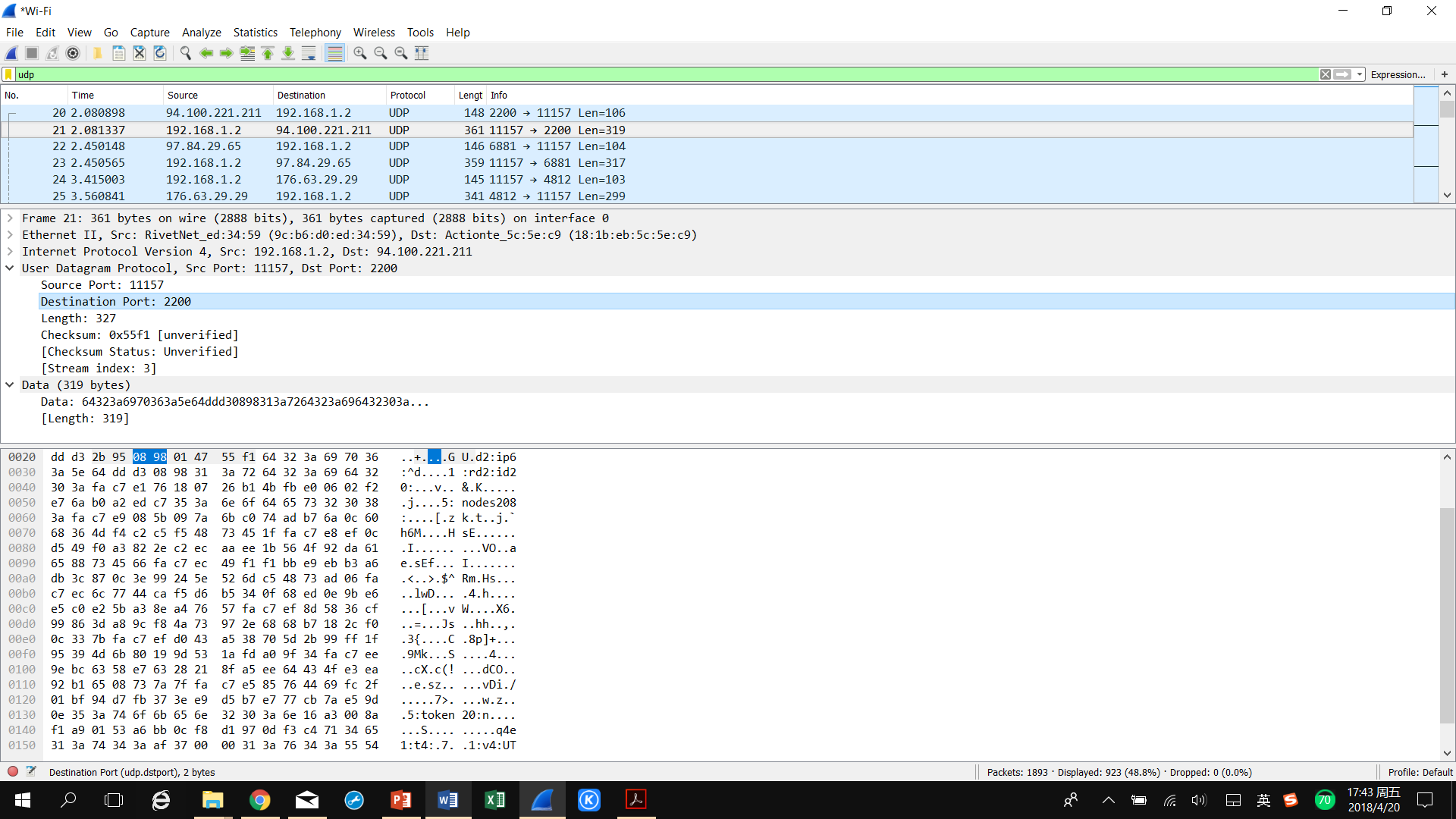
14. Select *one* UDP packet from your trace. From this packet, determine how many fields there are in the UDP header

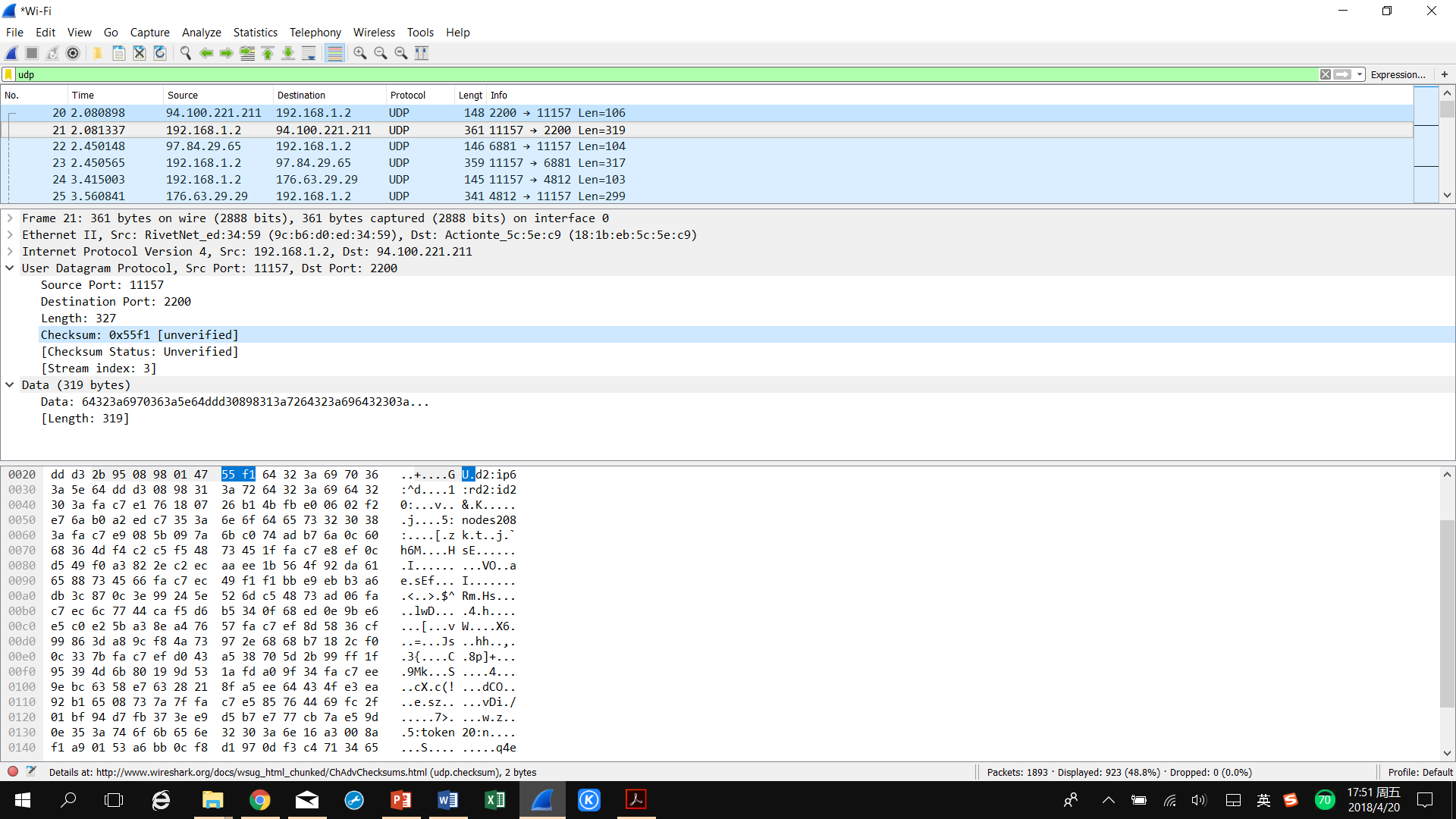
Answer: UDP header contains 4 fields: 1. source port; 2. destination port; 3. length; 4. Checksum

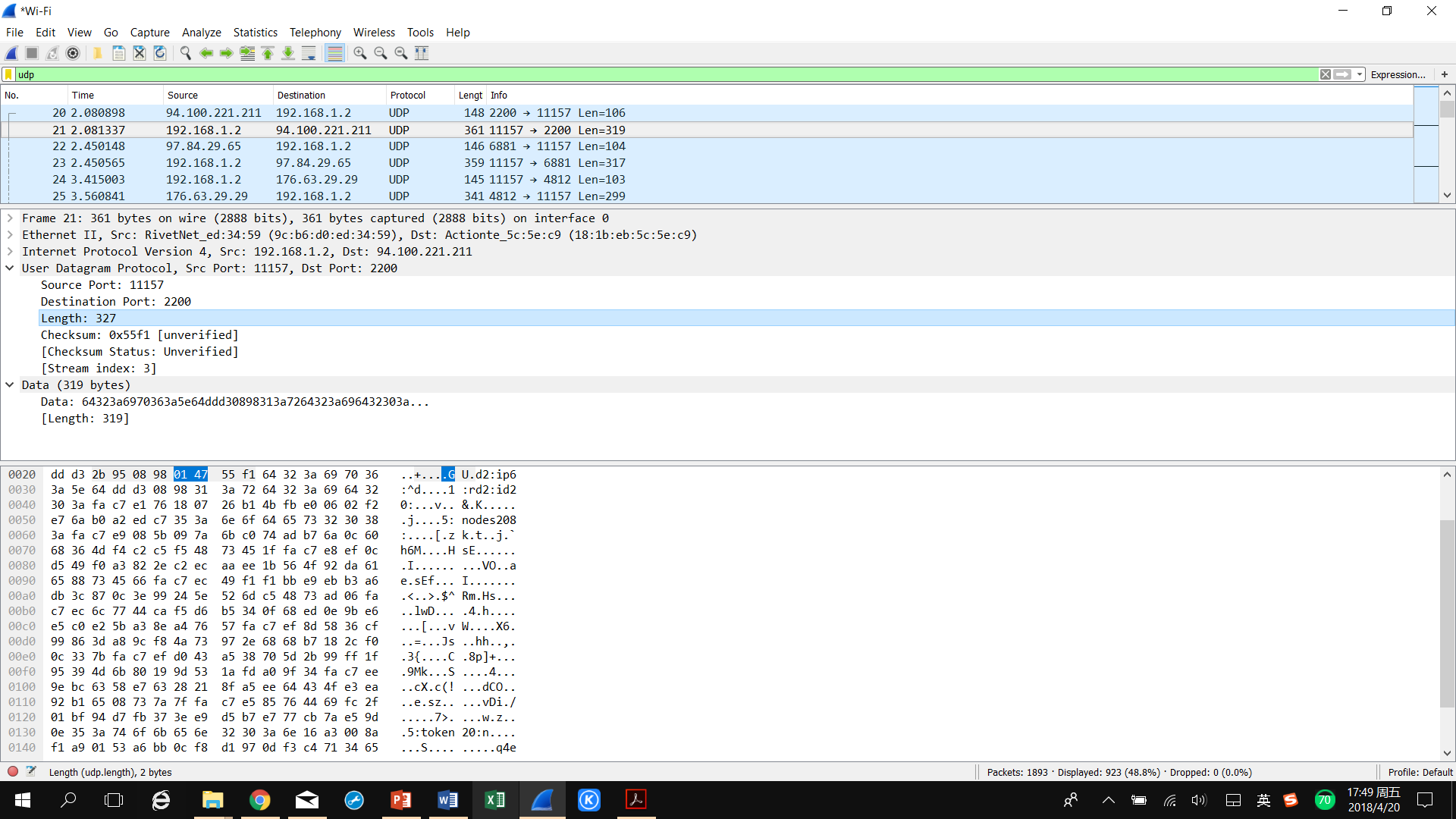


15. By consulting the displayed information in Wireshark’s packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

Answer: In Packet 21, the length of source port, destination port, length and checksum each equals 2 bytes. And the length of UDP header fields is 8 bytes total.

 Source port Destination Port



Length Checksum

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

Answer: the values indicates the UDP segment (payload + header) is 327 bytes long.

The payload of data equals 319 bytes. Each field in the UDP header is 2 bytes, and the UDP header all adds up to 8 bytes. Therefore, the total length of the UDP segment equals 327 bytes (319 + 8).

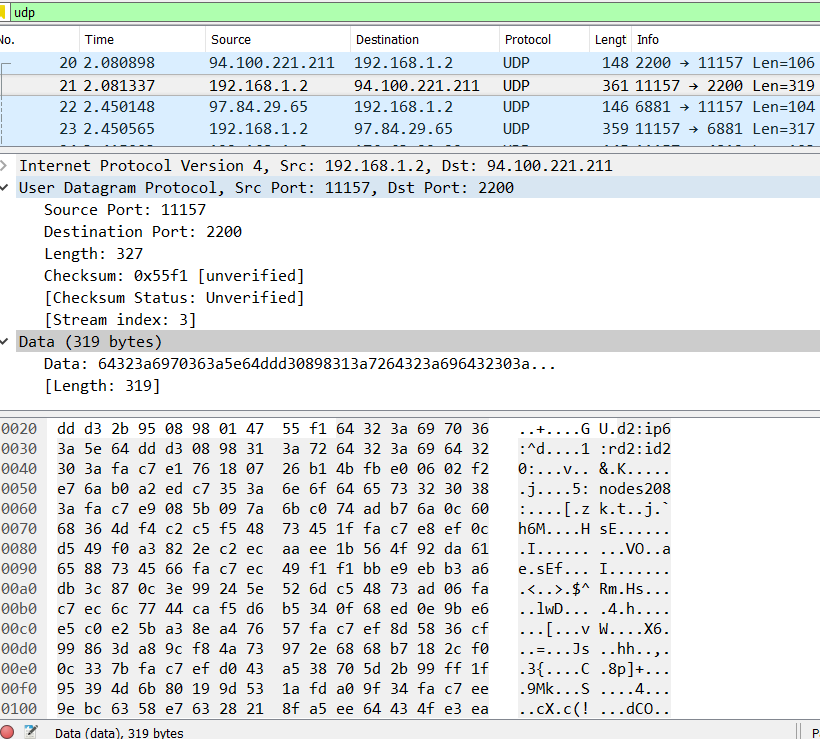




Figure 1

Use Figure 1 above to answer question 17 - 25

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

Answer: The command ‘ping -n 10 176.32.103.205’ is to verify IP- level connectivity and determine response time between the destination device and source device over the network by sending 10 ICMP Echo requests to the destination IP address 176.32.103.205.

In the figure 1, the Ping command works much like a sonar echo-location, sending a small packet of information containing an ICMP ECHO\_REQUEST to the specified device whose IP address, in this case, is 176.32.103.205, then the specified device sends an ECHO\_REPLY packet in return.

On the other hand, the IP address 127.0.0.1 is set by convention to always indicate the source computer. Therefore, a ping to that address will always ping the source. This provides the most basic test of the source local communications.

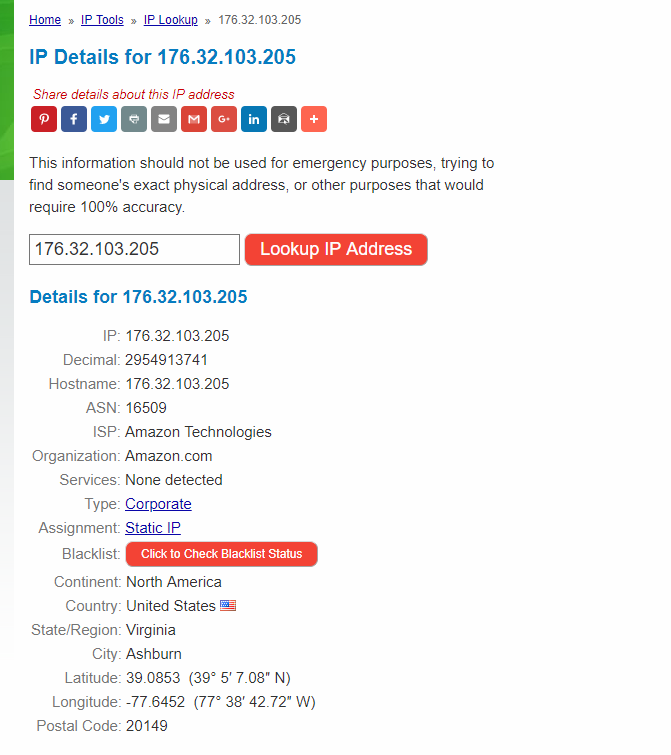
Moreover, the ping also includes the reaction time of the connection–how fast the source device gets a response after it sent out a request.

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

Answer: The protocol used is ICMP, standing for Internet Control Message Protocol.

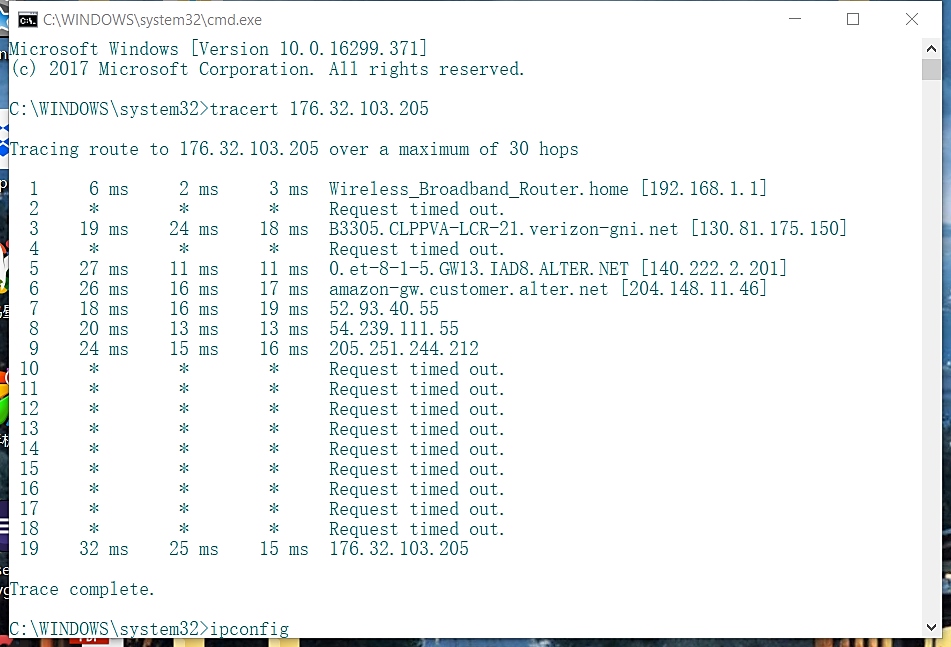
19. Who owns the IP?

Answer: Amazon.com owns the IP.



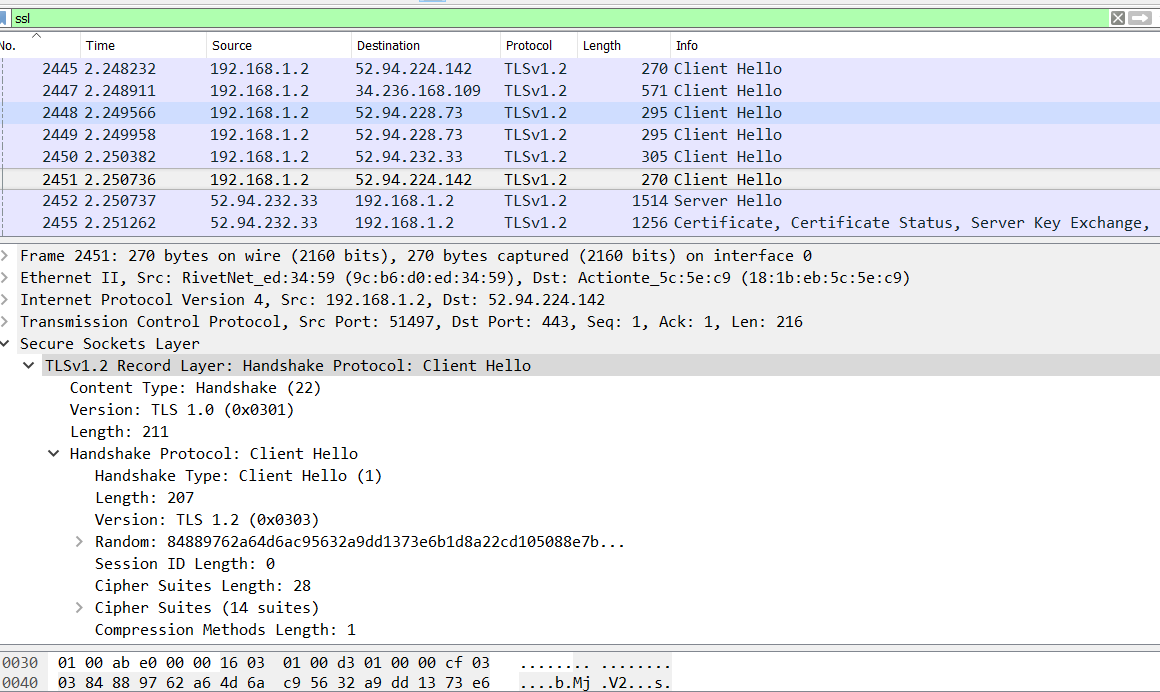
20. In addition to a screenshot, in a tabular form, list all the hops between your computer’s IP and the IP address in Figure 1. The table should include the owner, and location of the IP address.

|  |  |  |  |
| --- | --- | --- | --- |
| Hop Count | IP address | IP Owner | Location |
| 1 | 192.168.1.1 | Internet Assigned Numbers Authority | CA, USA |
| 2 | Request timed out | N/A | N/A |
| 3 | 130.81.175.150 | MCI Communications Services, Inc. d/b/a Verizon Business | VA, USA |
| 4 | Request timed out | N/A | N/A |
| 5 | 140.222.2.201 | ANS CO+RE Systems, Inc. | NY, USA |
| 6 | 204.148.11.46 | ANS Communications, Inc | VA, USA |
| 7 | 52.93.40.55 | Amazon Technologies Inc. | WA, USA |
| 8 | 54.239.111.55 | Amazon Technologies Inc. | WA, USA |
| 9 | 205.251.244.212 | Amazon.com, Inc. | WA, USA |
| 10 | Request timed out | N/A | N/A |
| 11 | Request timed out | N/A | N/A |
| 12 | Request timed out | N/A | N/A |
| 13 | Request timed out | N/A | N/A |
| 14 | Request timed out | N/A | N/A |
| 15 | Request timed out | N/A | N/A |
| 16 | Request timed out | N/A | N/A |
| 17 | Request timed out | N/A | N/A |
| 18 | Request timed out | N/A | N/A |
| 19 | 176.32.103.205 | Amazon.com | VA, USA |



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

Answer: The version of TLS is TLSv1.2

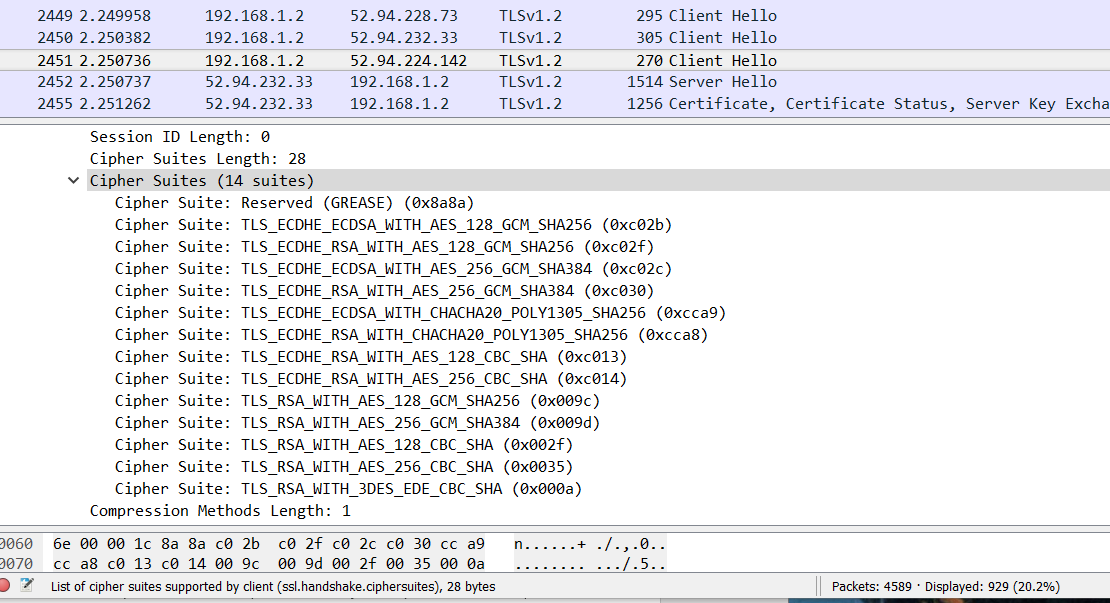


22. List all the algorithms listed in the Cipher Suite of the “Client Hello” packet in 21.

Answer: ECDHE\_ECDSA, ECDHE\_RSA, RSA,

AES, CHACHA20\_POLY1305, AES, 3DES

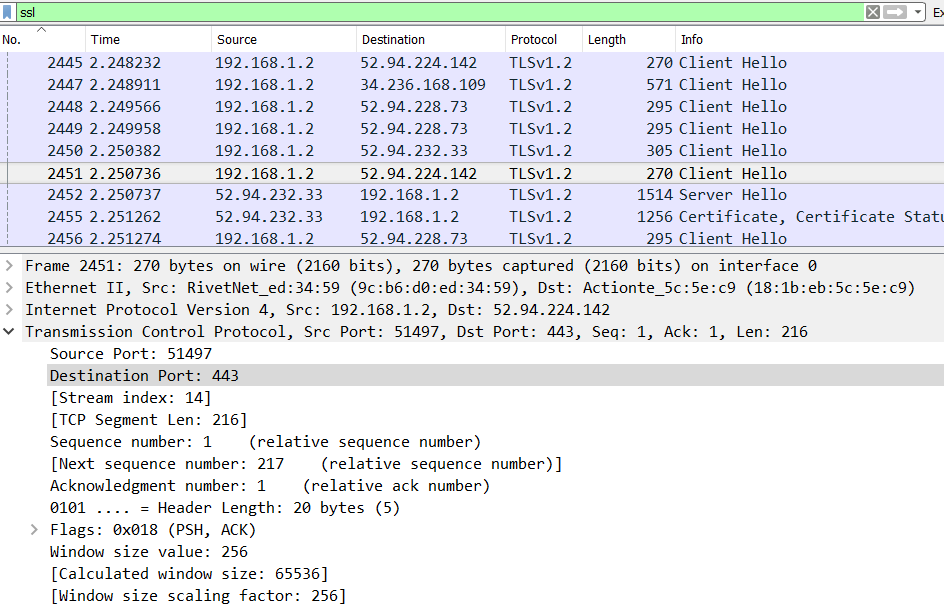
SHA



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

Answer: The TCP port number is 443.

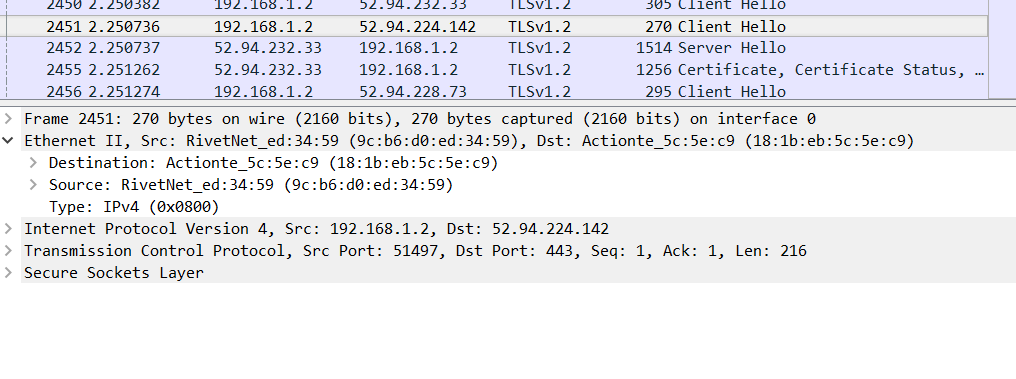
TCP port 443 is the standard TCP port that is used for website which use SSL. In the case of https, Netscape chose 443 to be the default port used by secure http because the port was not being used for any other purpose at the time.



24. What are the source and destination MAC address?

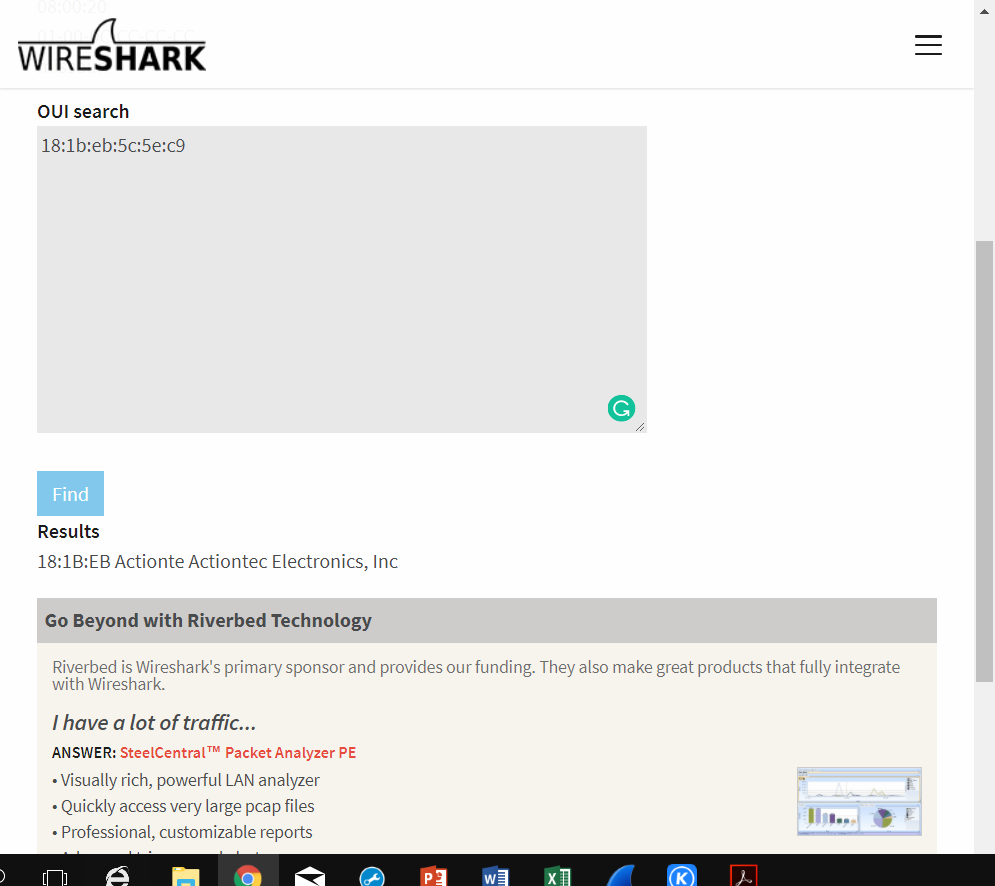
Answer: Source MAC address is 9c:b6:d0:ed:34:59

Destination MAC address is 18:1b:eb:5c:5e:c9



25. 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).

Answer: Actiontec Electronics, Inc



Extra Credit: (3 Marks)

Make a GitHub account and create a repository. Name the repo “wireshark\_labs”. Add **all the labs** you did in this class (both **Wireshark saved files** and **submitted reports**). Add your GitHub username to the end of this lab or email it to me.

GitHub username: wenjie01

https://github.com/wenjie01/wireshark\_labs