**Wireshark Final Exam**

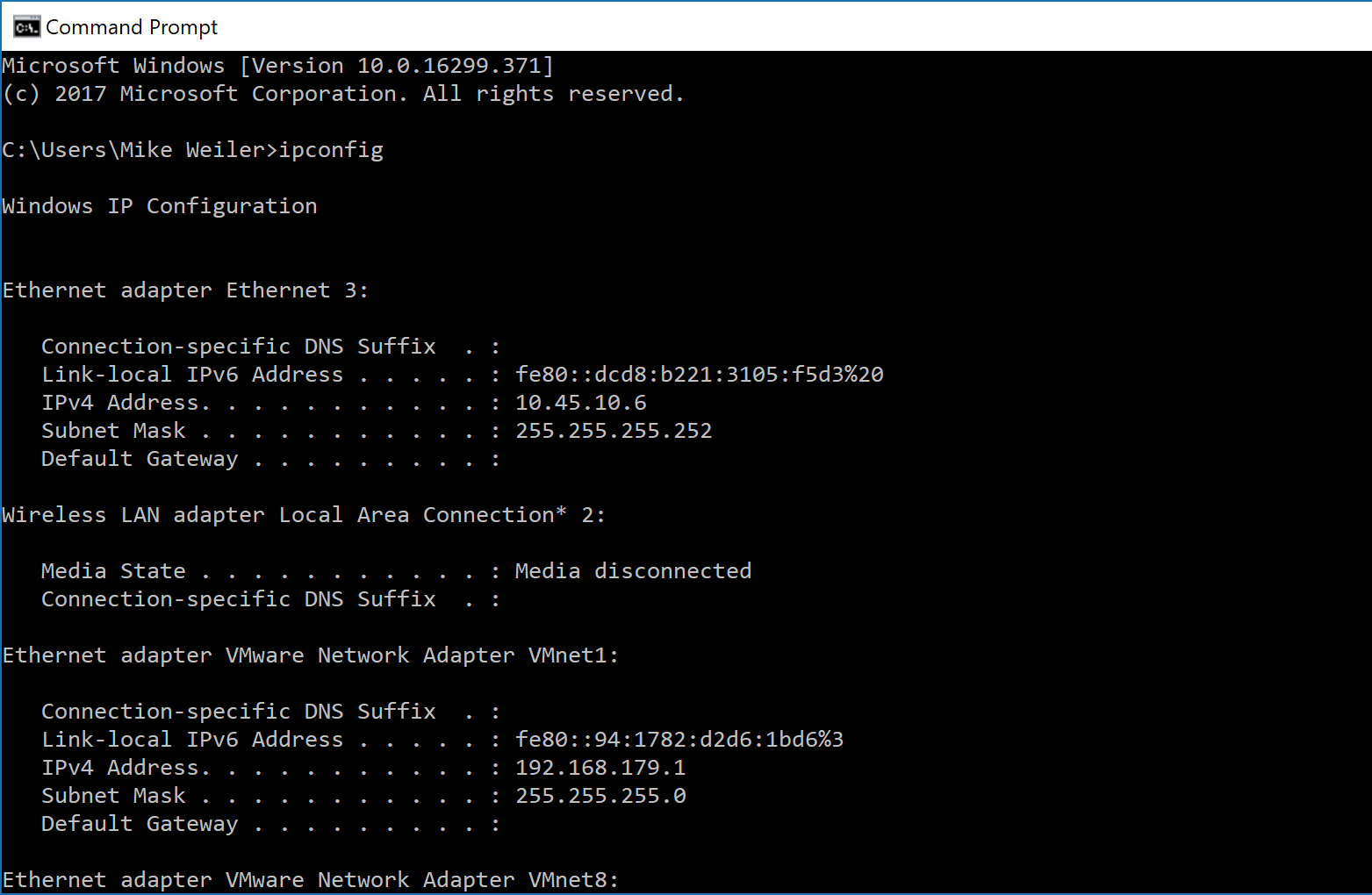
**IT 520-A – Enterprise Infrastructure & Networks**

**Due Date: May 1st, 2018**

**Michael Weiler**

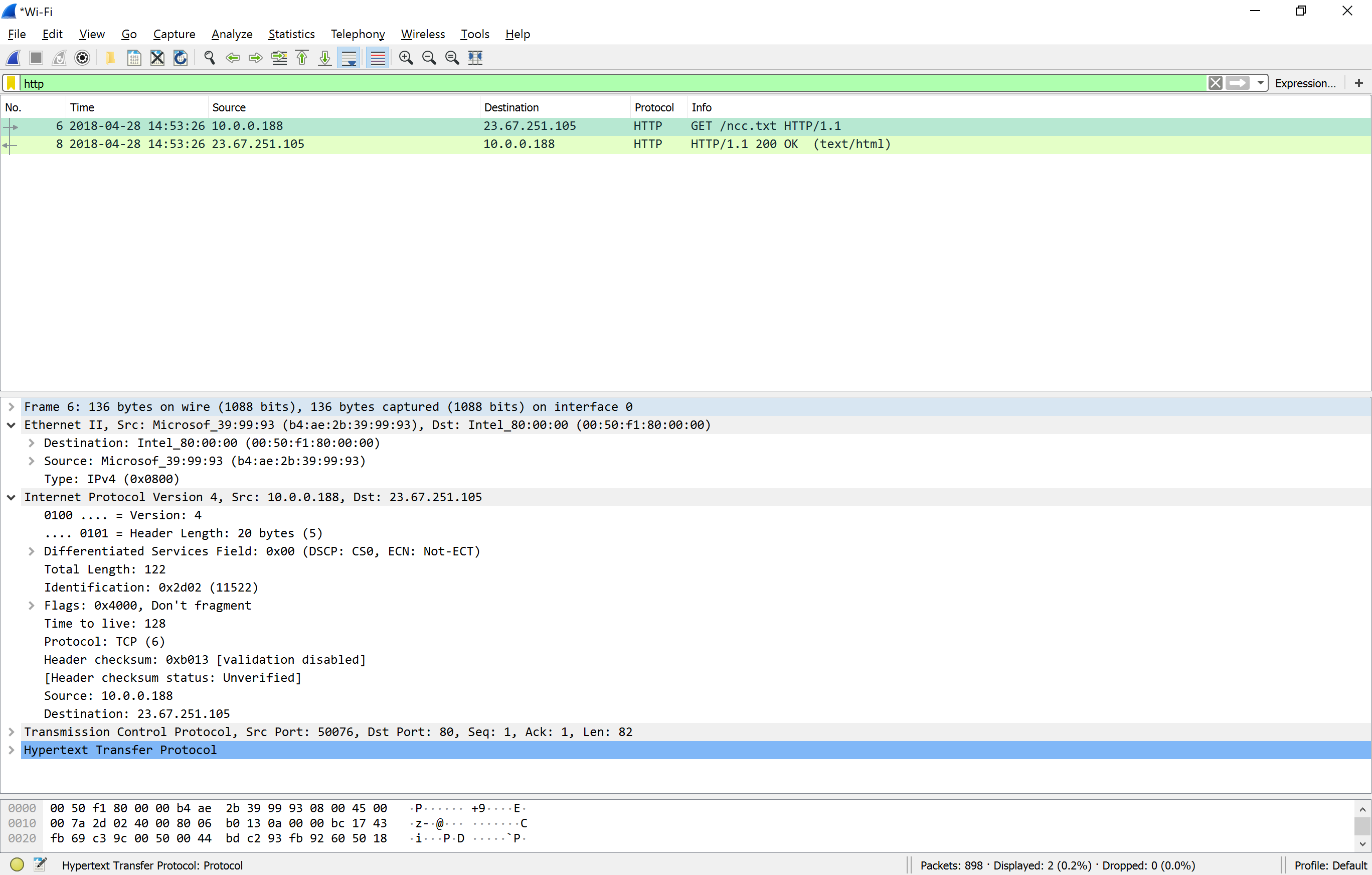
Instructions:

• 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.)

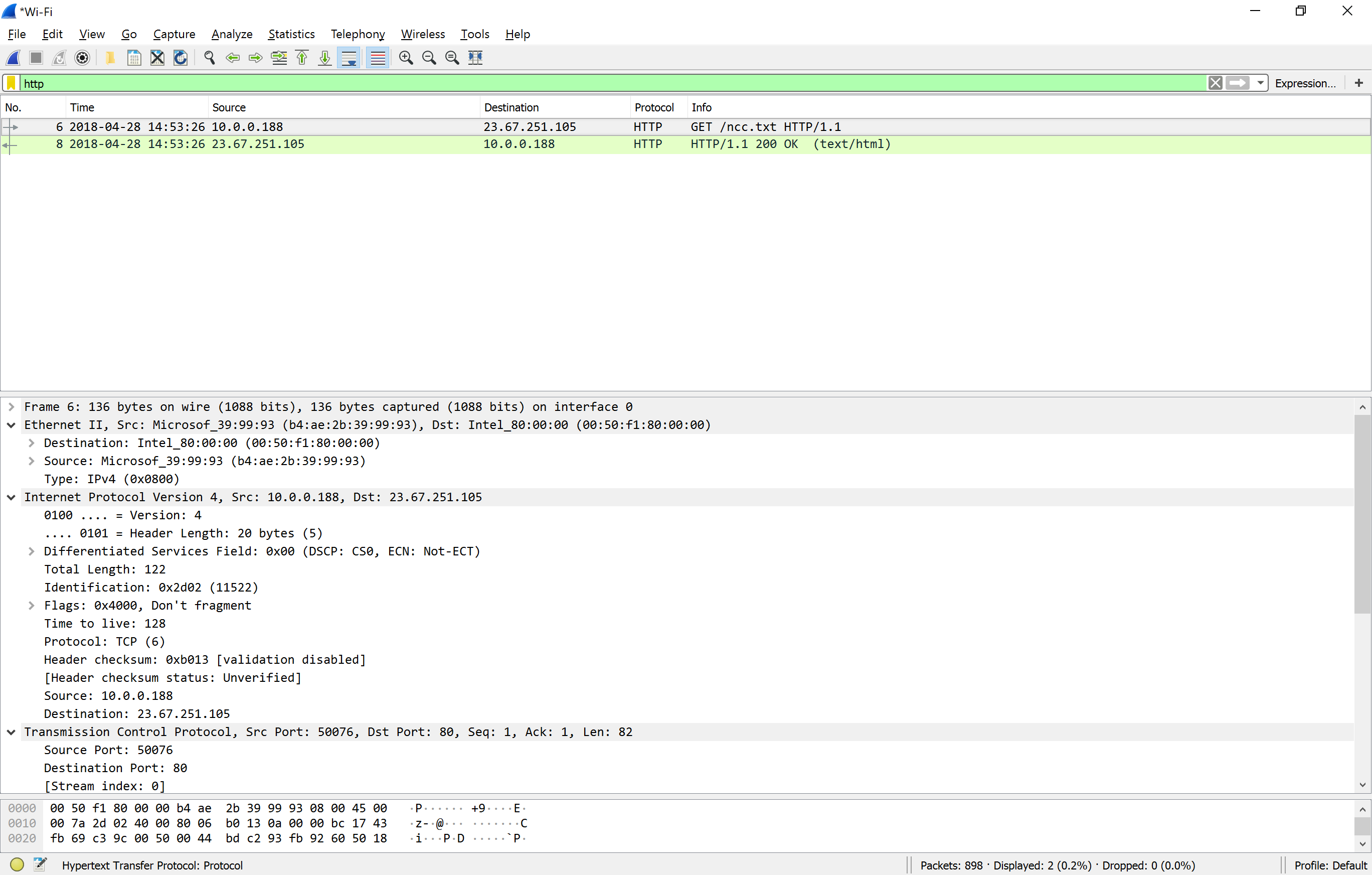


Visit: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

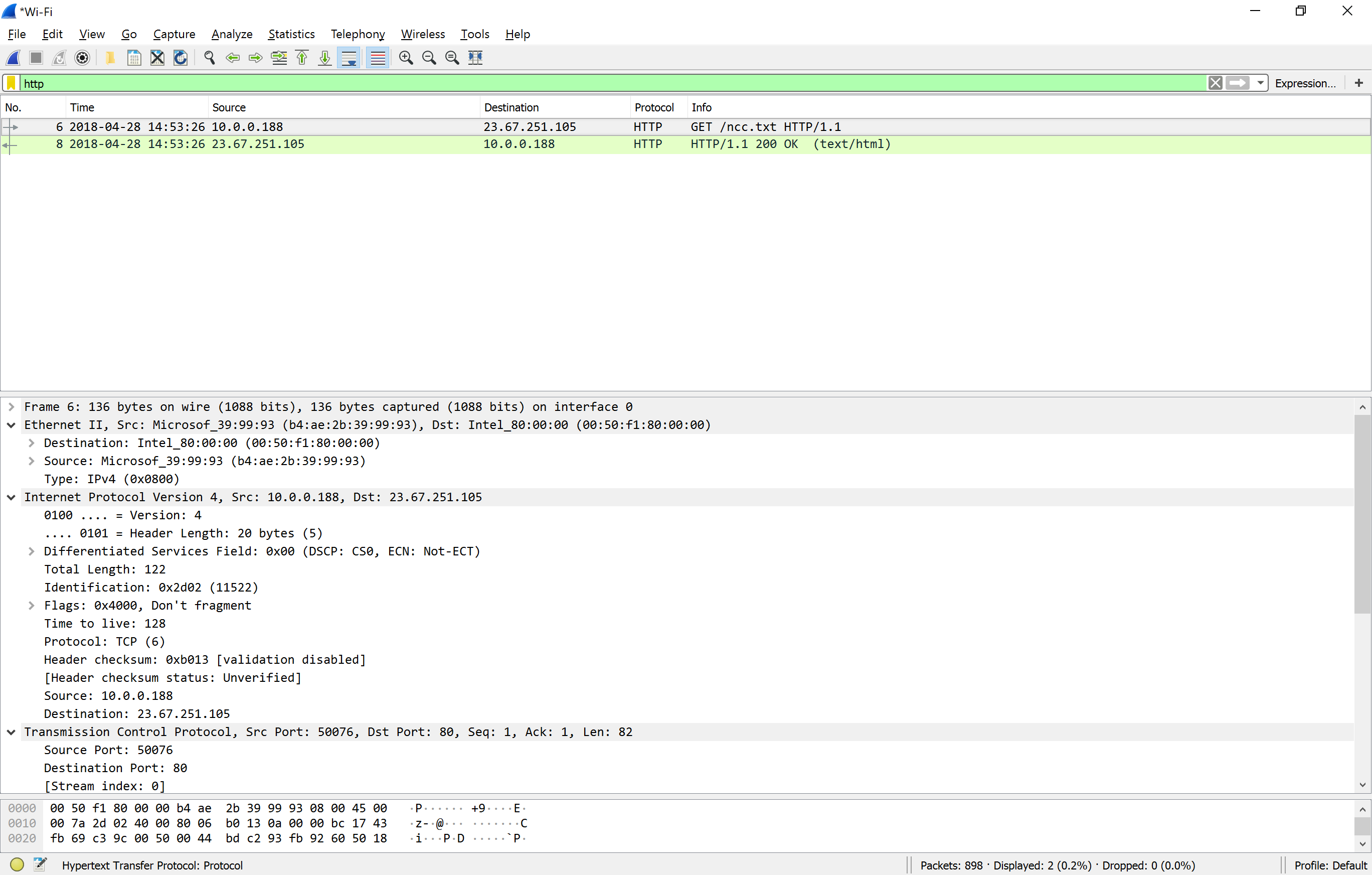
1. How many HTTP GET request messages did your browser send? **1** Which packet number in the trace contains the GET message for the Bill or Rights? **6**



1. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request? **8**



1. What is the status code and phrase in the response? **8** **2018-04-28 14:53:26 23.67.251.105 10.0.0.188 HTTP HTTP/1.1 200 OK (text/html)**

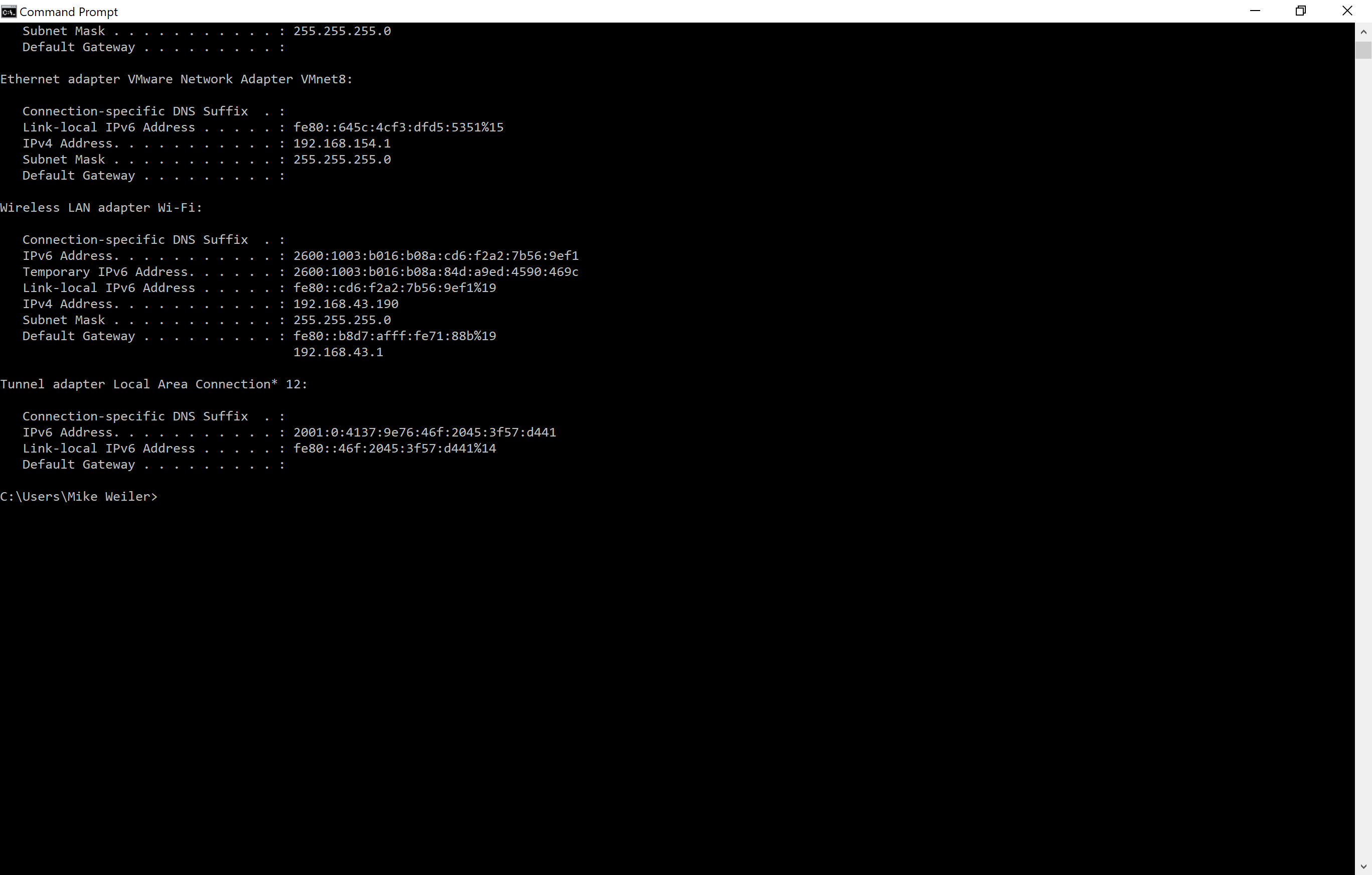


1. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights? **151**

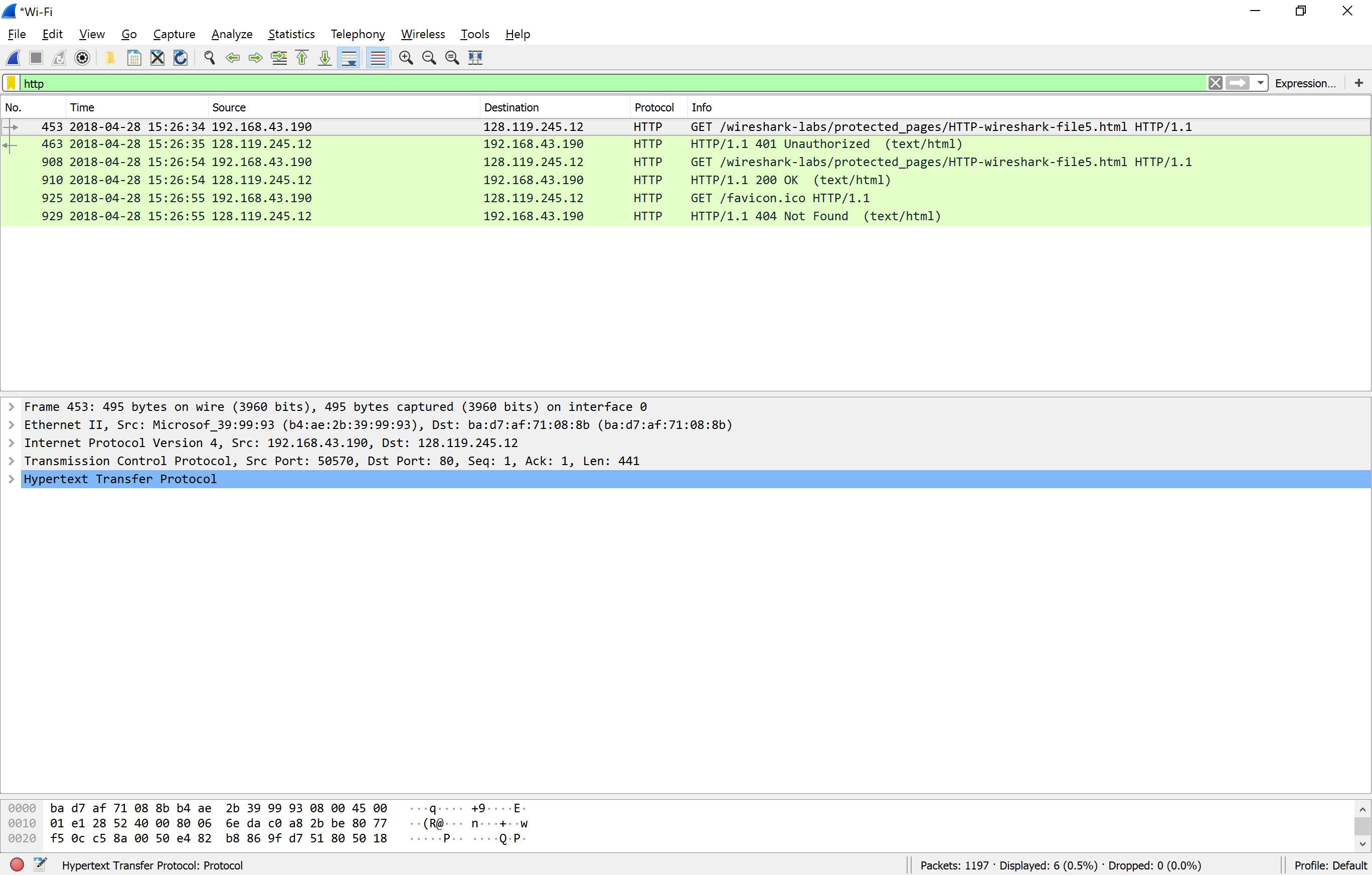


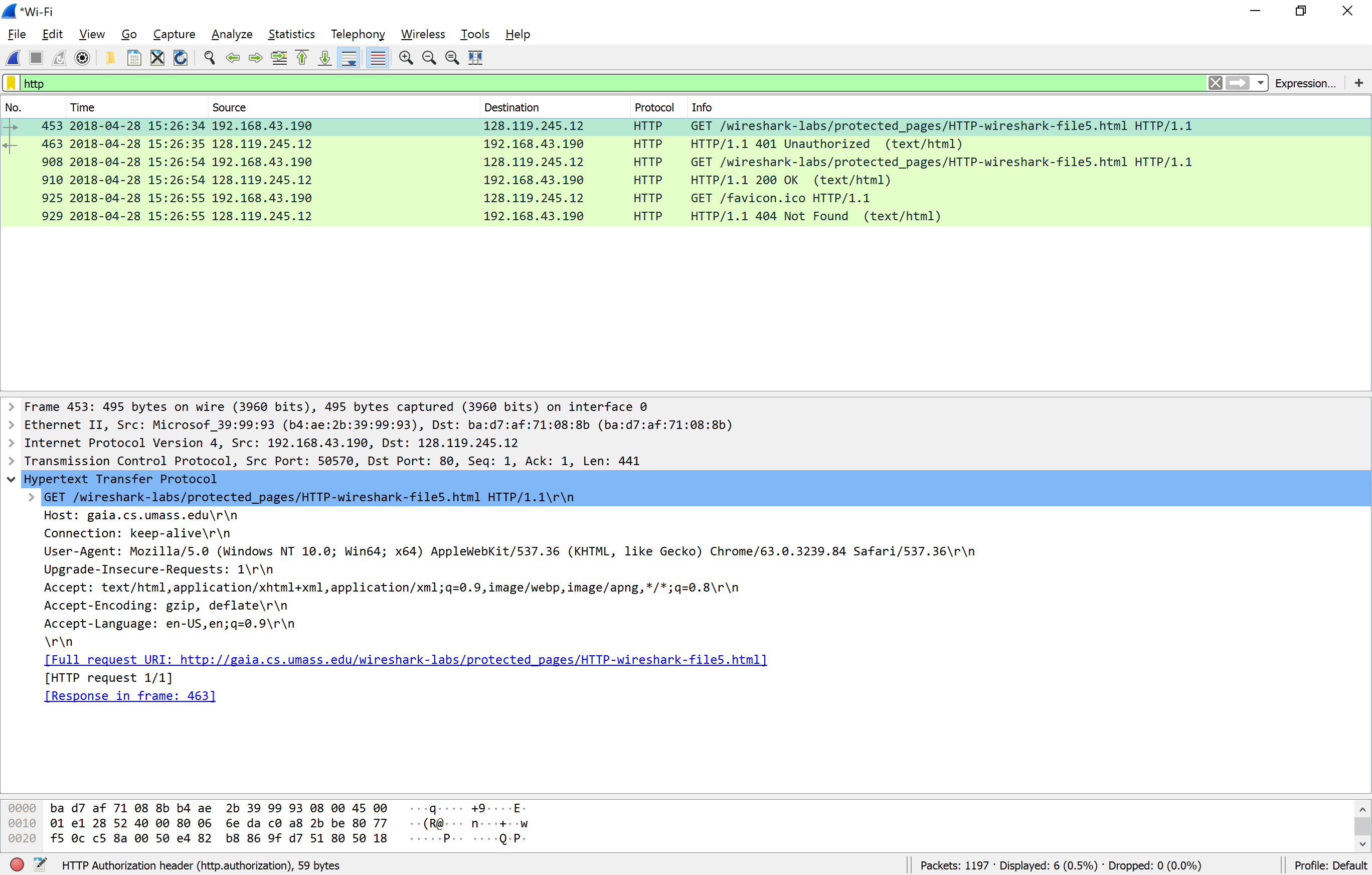
Visit: http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html

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

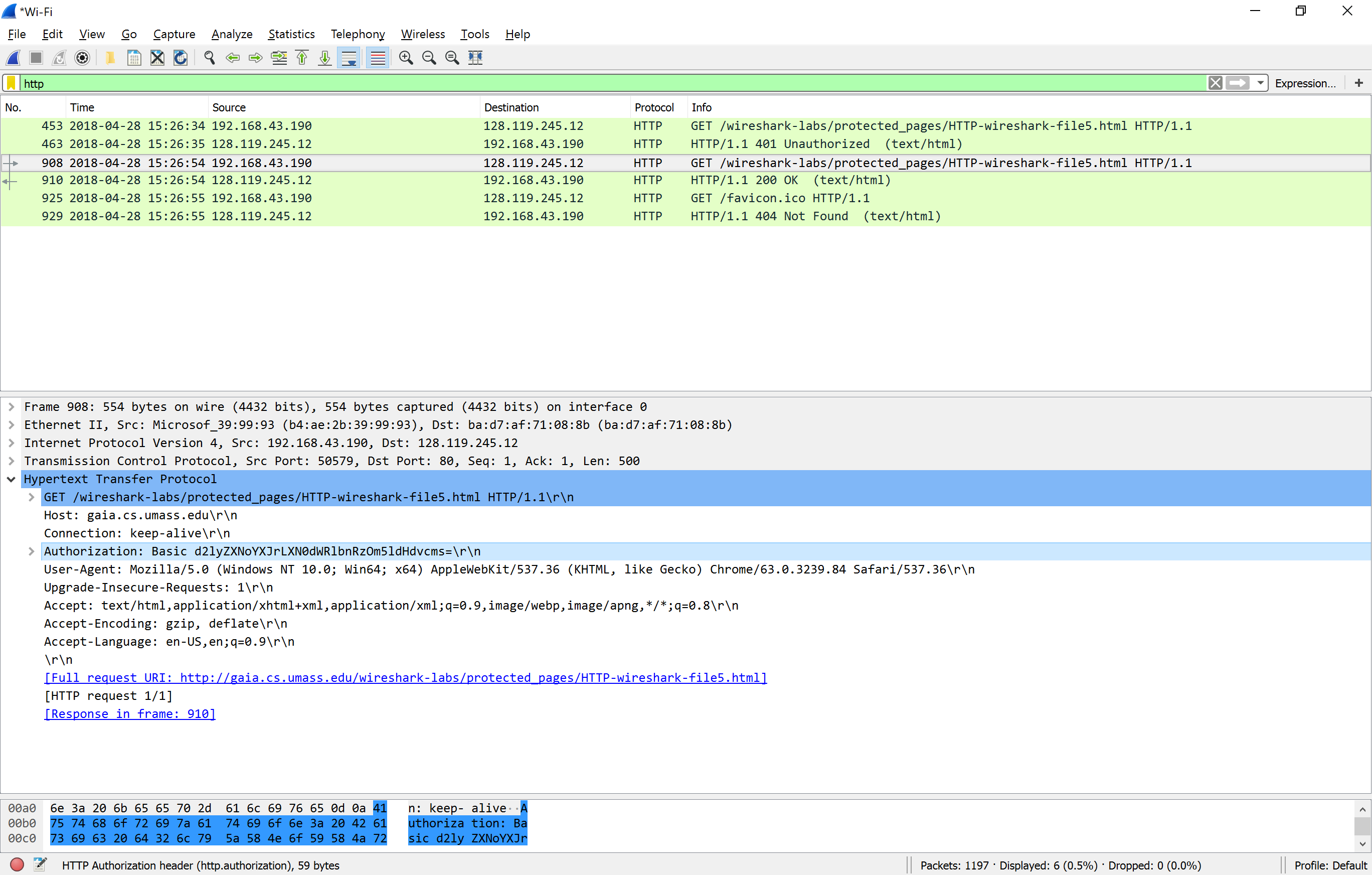


1. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser? **463 2018-04-28 15:26:35 128.119.245.12 192.168.43.190 HTTP HTTP/1.1 401 Unauthorized (text/html)**



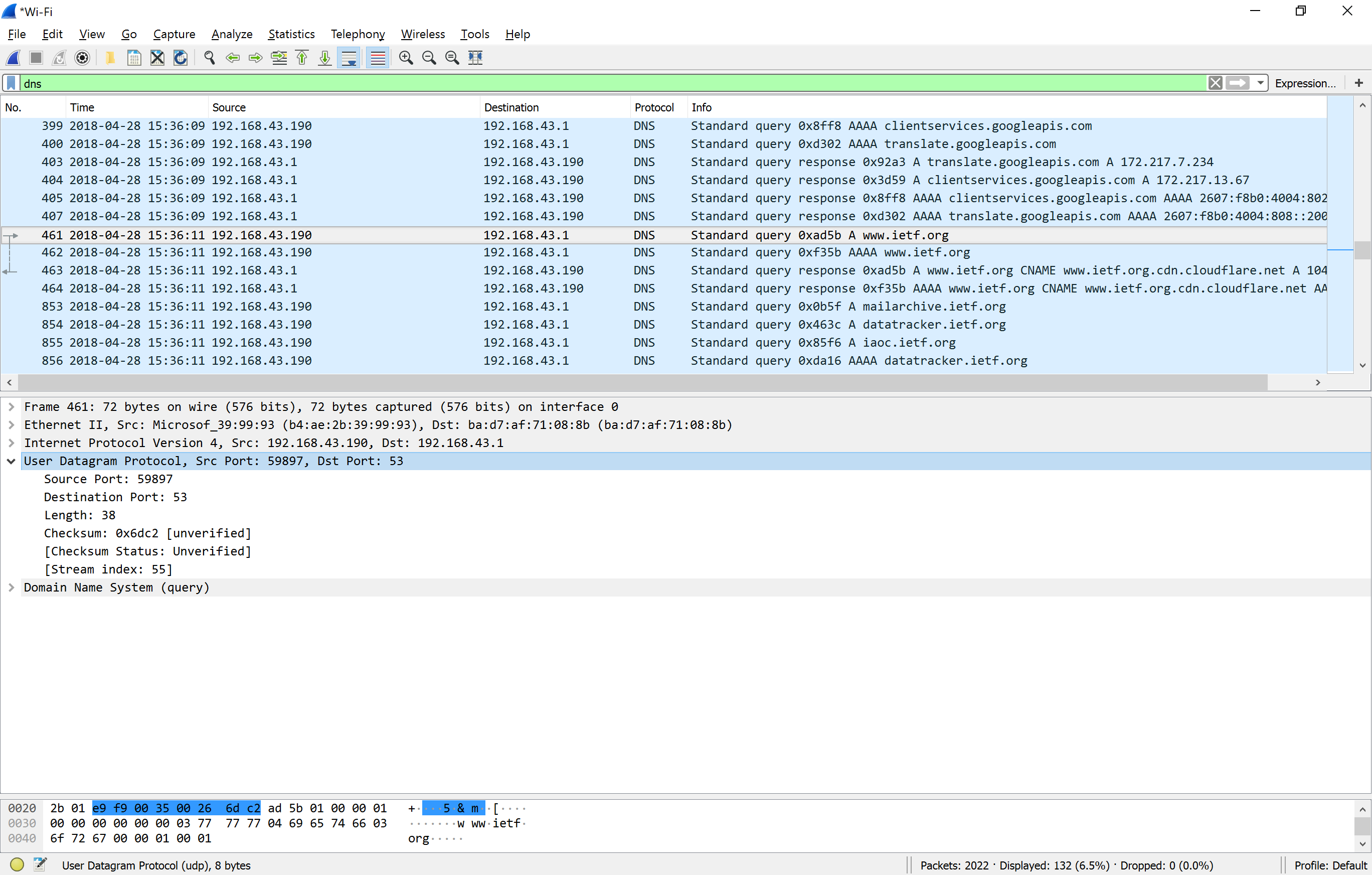


1. When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message? **An AUTHORIZATION: Basic**

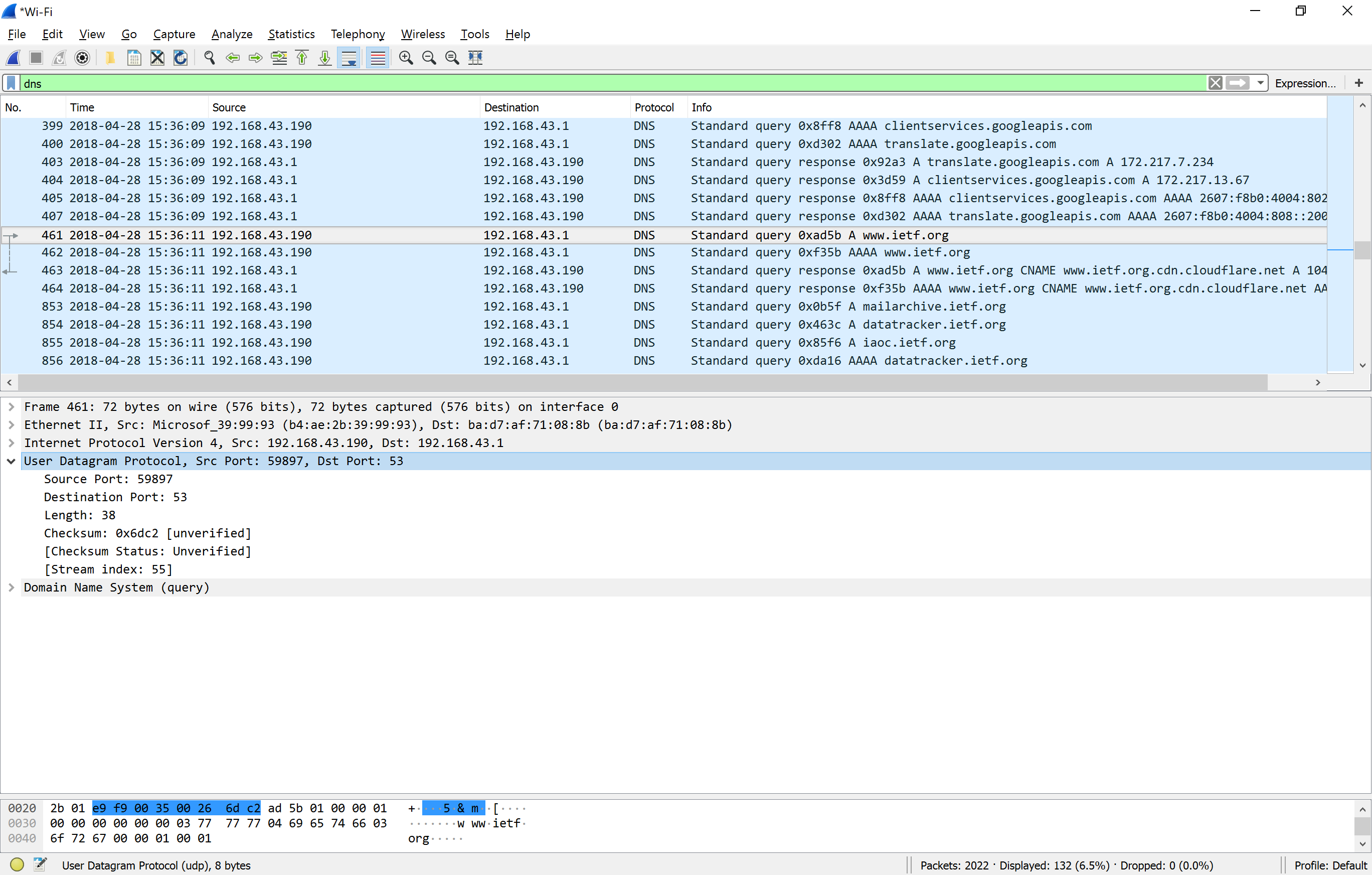


Visit: http://www.ietf.org (Hint: Filter Wireshark using “ip addr == your IP”)

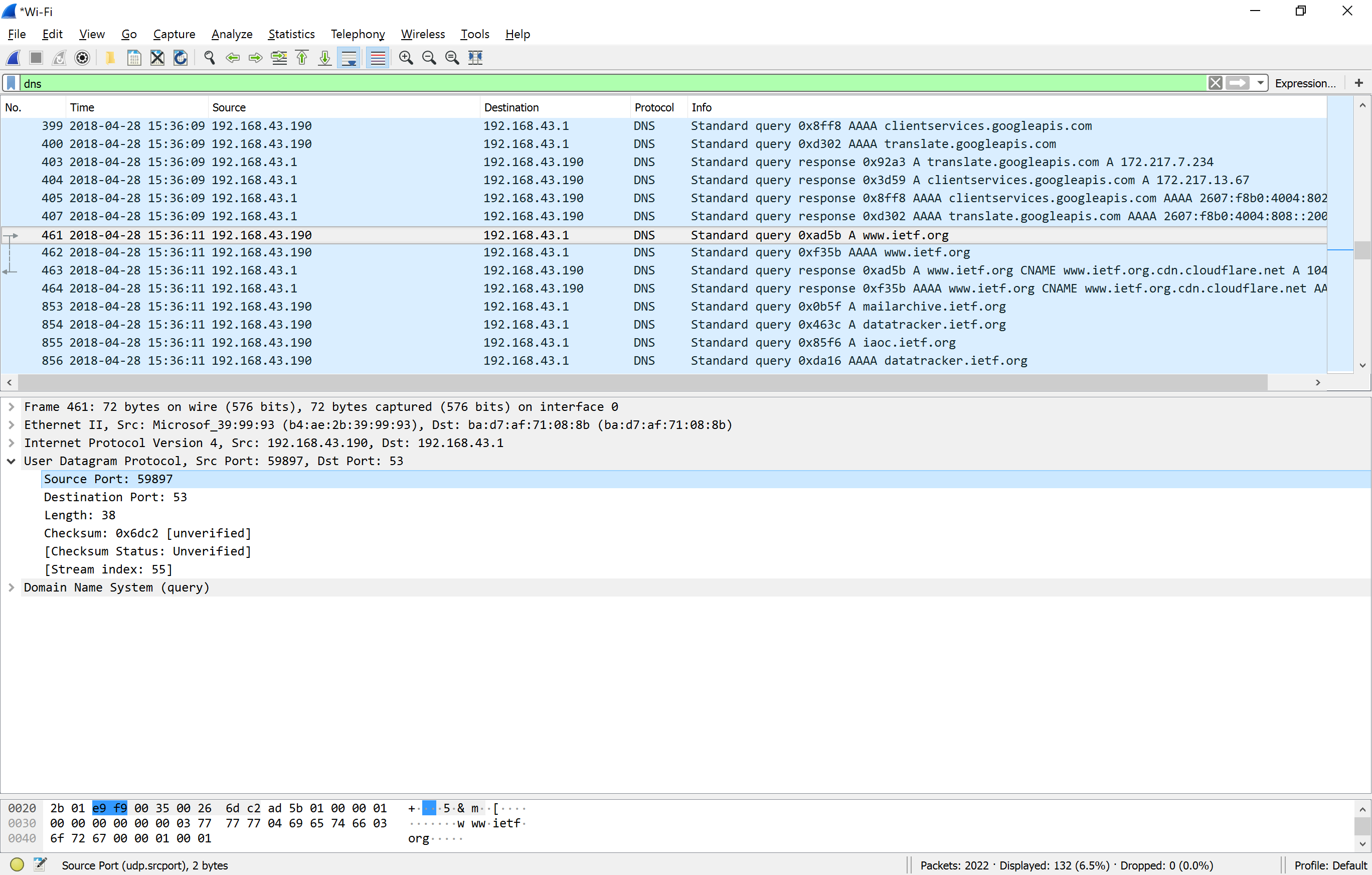
1. Locate the DNS query and response messages. Are they sent over UDP or TCP? **UDP**



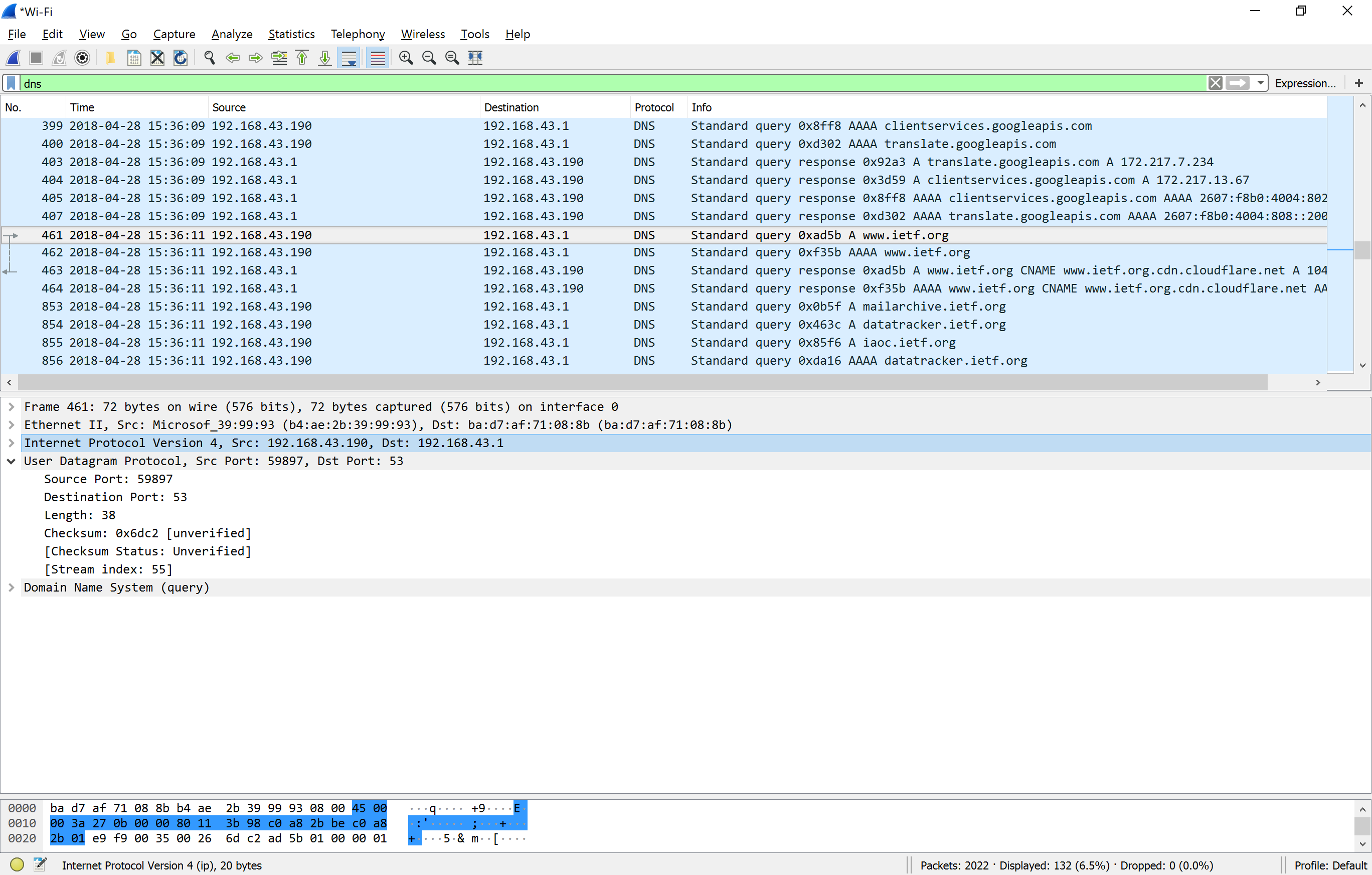
1. What is the destination port for the DNS query message? **53**



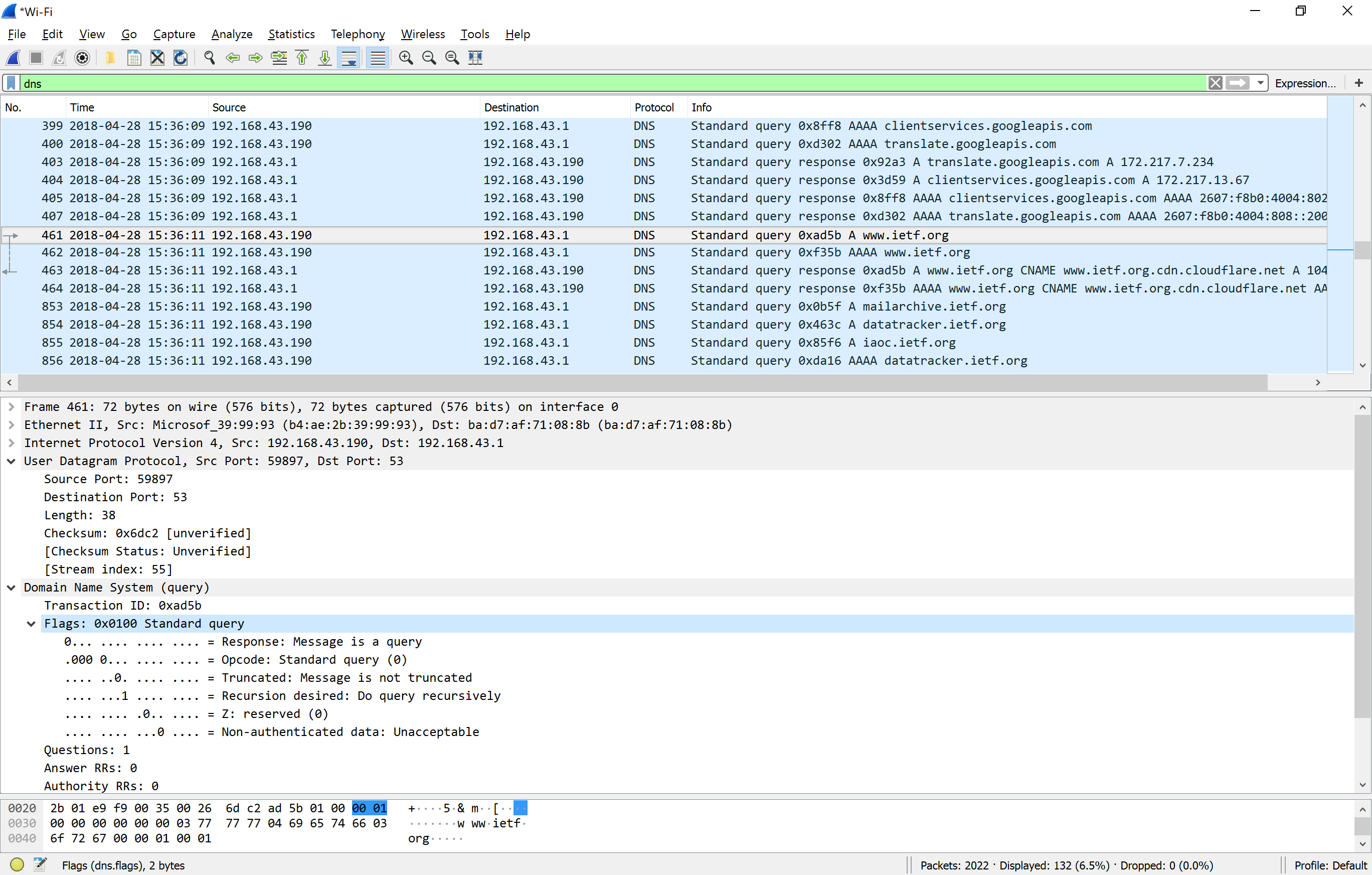
1. What is the source port of DNS response message? **59897**



1. To what IP address is the DNS query message sent? **192.168.43.1**



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



1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? **3 Answers**

**Name**

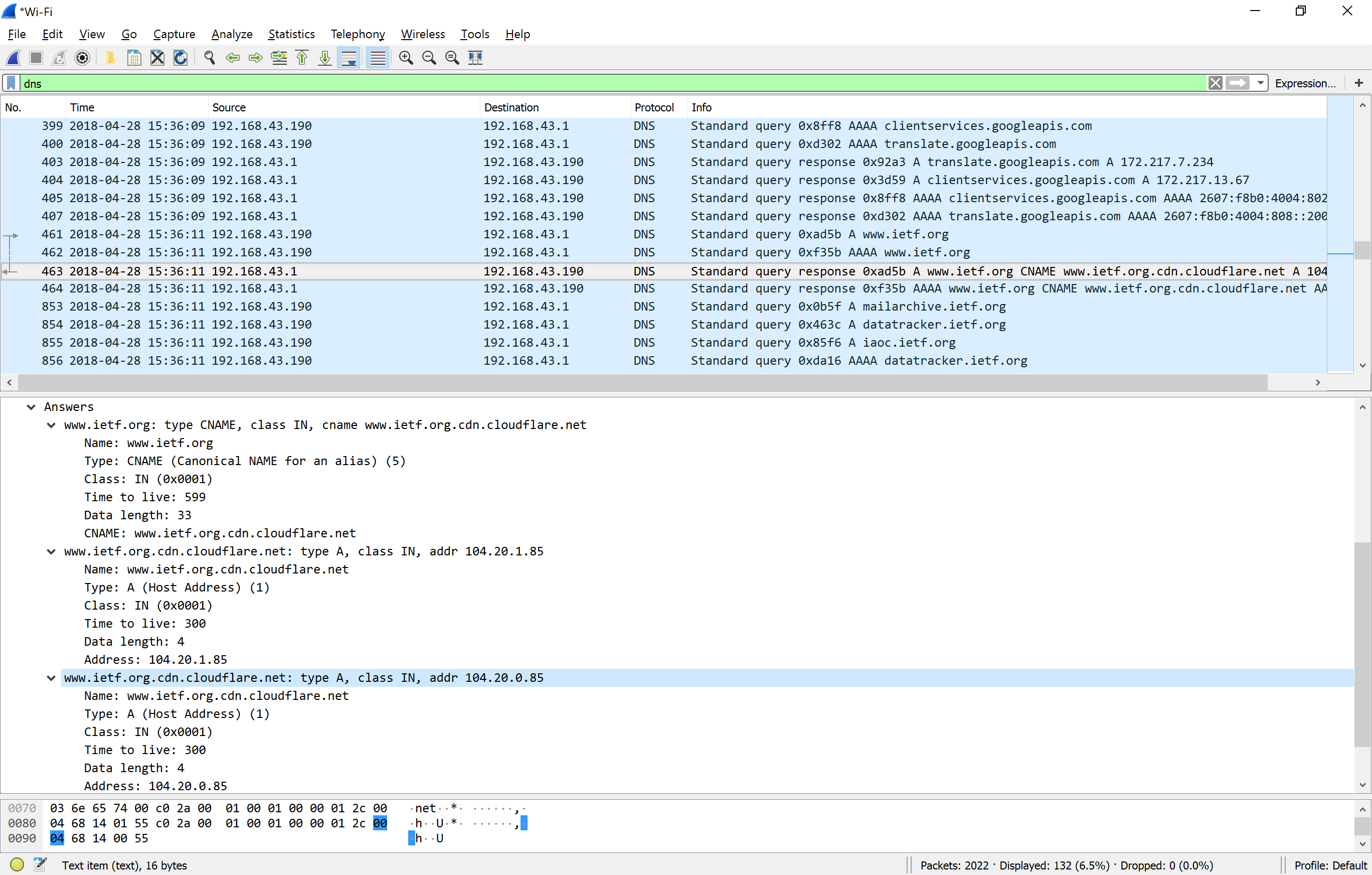
**Type: Host address**

**Class: (IN) inet**

**Time to live**

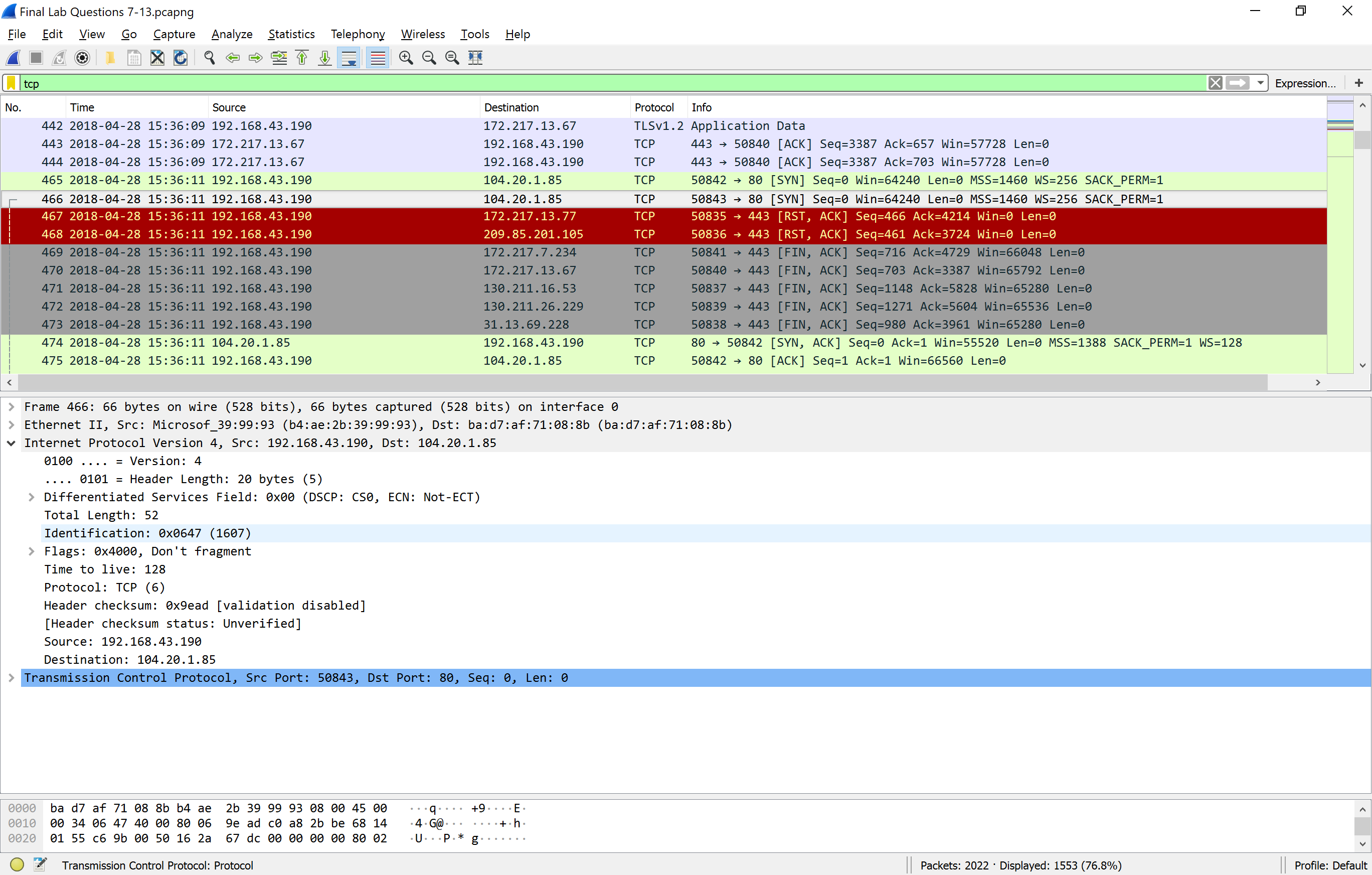
**Data length**

**Address**



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? :

**It corresponds to the first IP address provided in the DNS response message.**

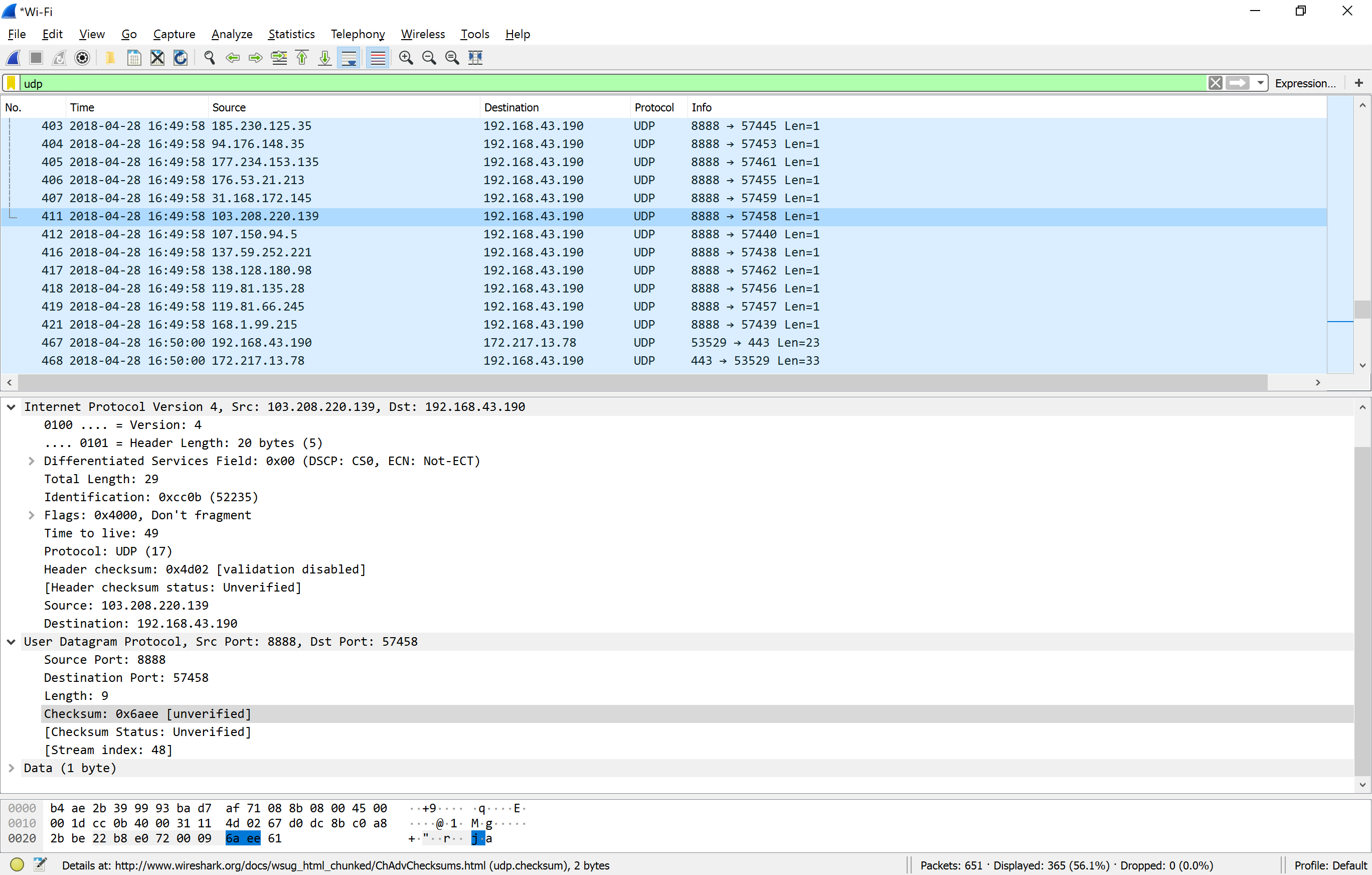


Do something that will cause your host to send and receive UDP packets. (example: use SNMP protocol by sending an email).

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

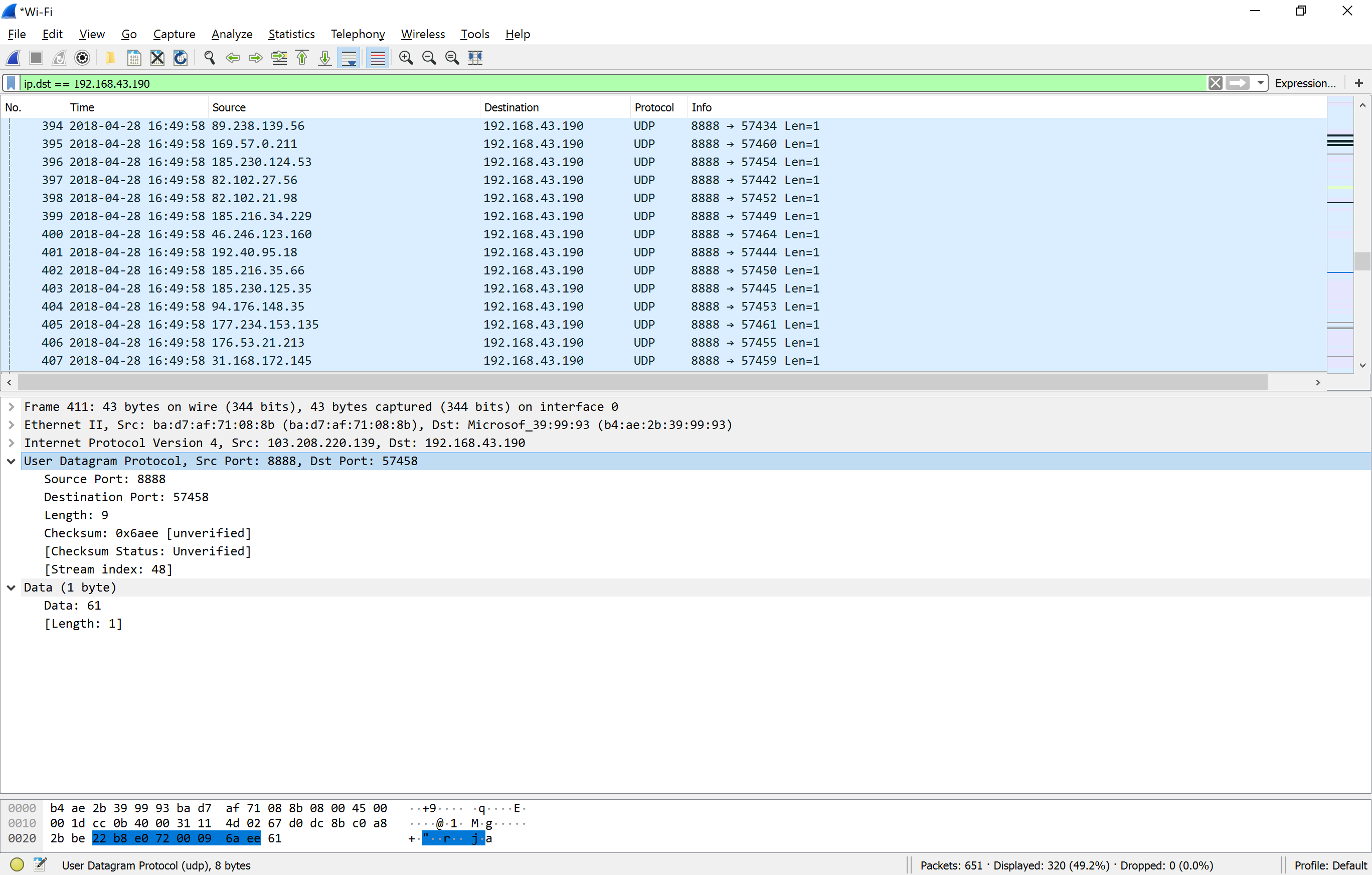
**4**

**1. Source port 2. Destination port 3. Length 4. Checksum**

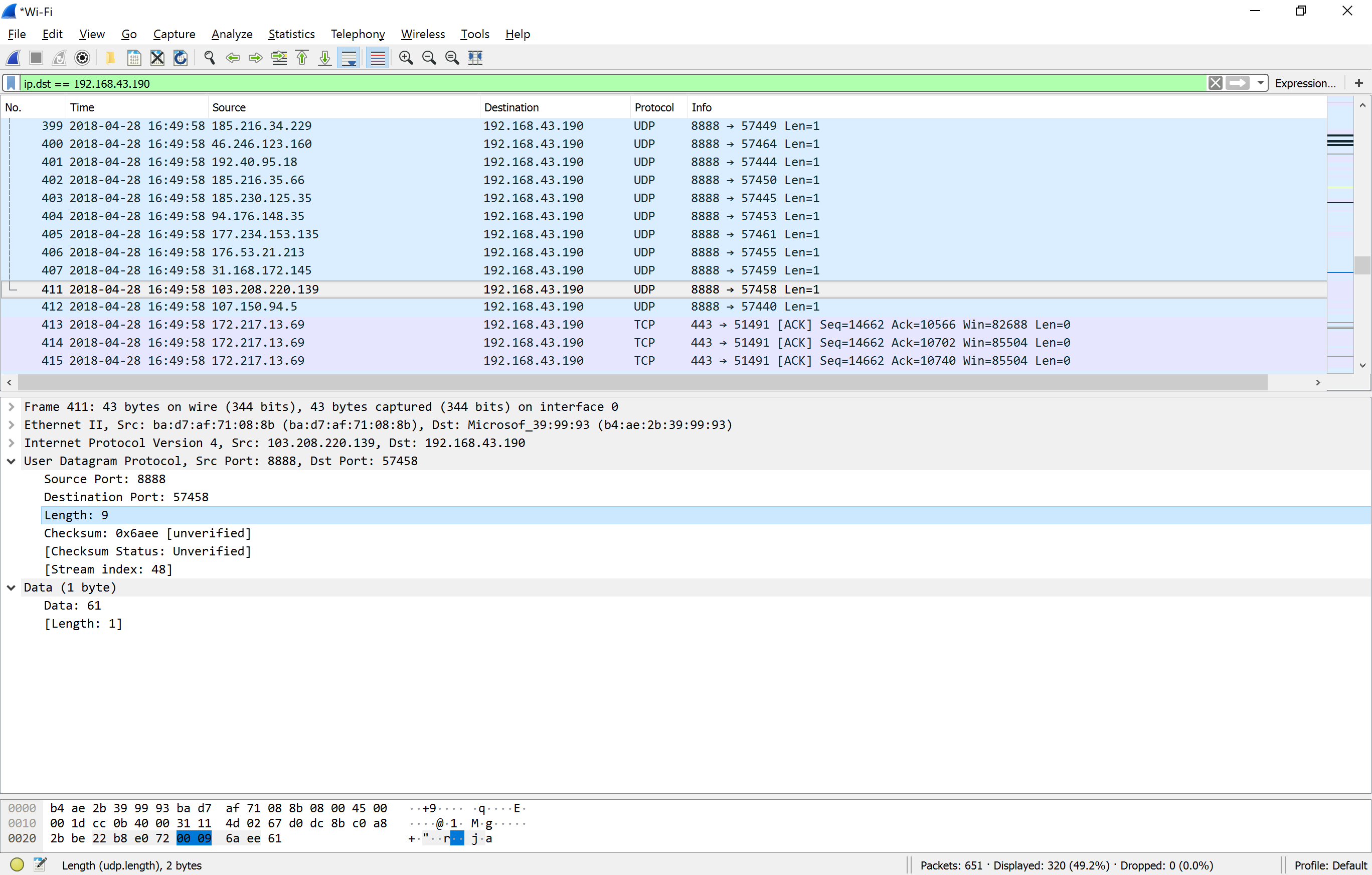


1. By consulting the displayed information in Wireshark’s packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

**The UDP header is 8 bytes (see circle below). Each field is 2 bytes long**



1. The value in the Length field is the length of what? Verify your claim with your captured UDP packet. **9 see circle below**



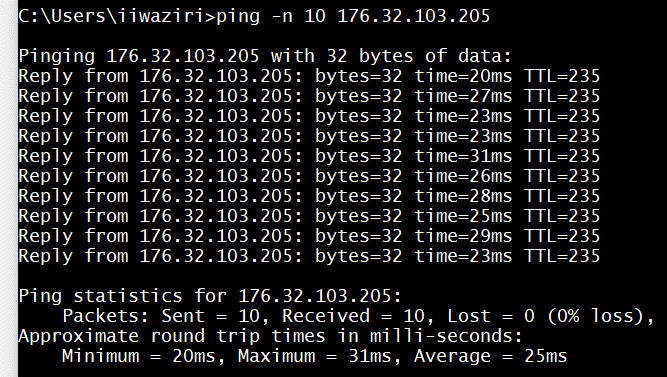


Figure 1

Use Figure 1 above to answer question 17 - 25

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

**The ping command was used in the Command Prompt to test the ability of the source computer “iiwasiri” to reach a specified destination computer/IP of 176.32.103.205. Simply put, this command is usually used to verify that a computer can communicate with another over a network…. HOWEVER the -n was used to specify the number of echo requests to send. In this case it was 10.**

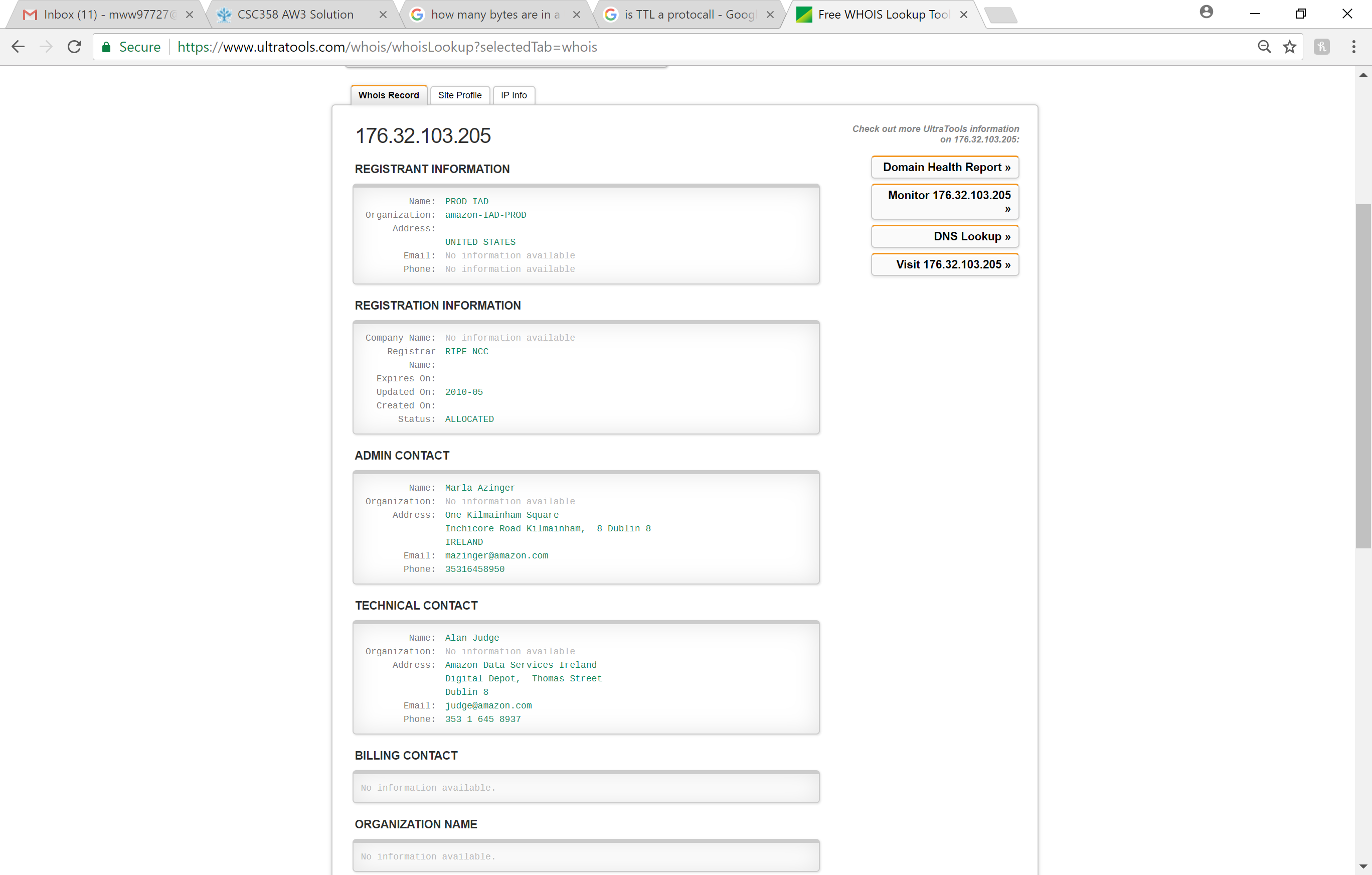
18. Which protocol is used to carry out the instruction in Figure 1.

**Time To Live (TTL) is a value in an Internet Protocol (IP) packet that tells a network router whether or not the packet has been in the network too long and should be discarded. Therefor, the answer is Internet Protocol (IP)**

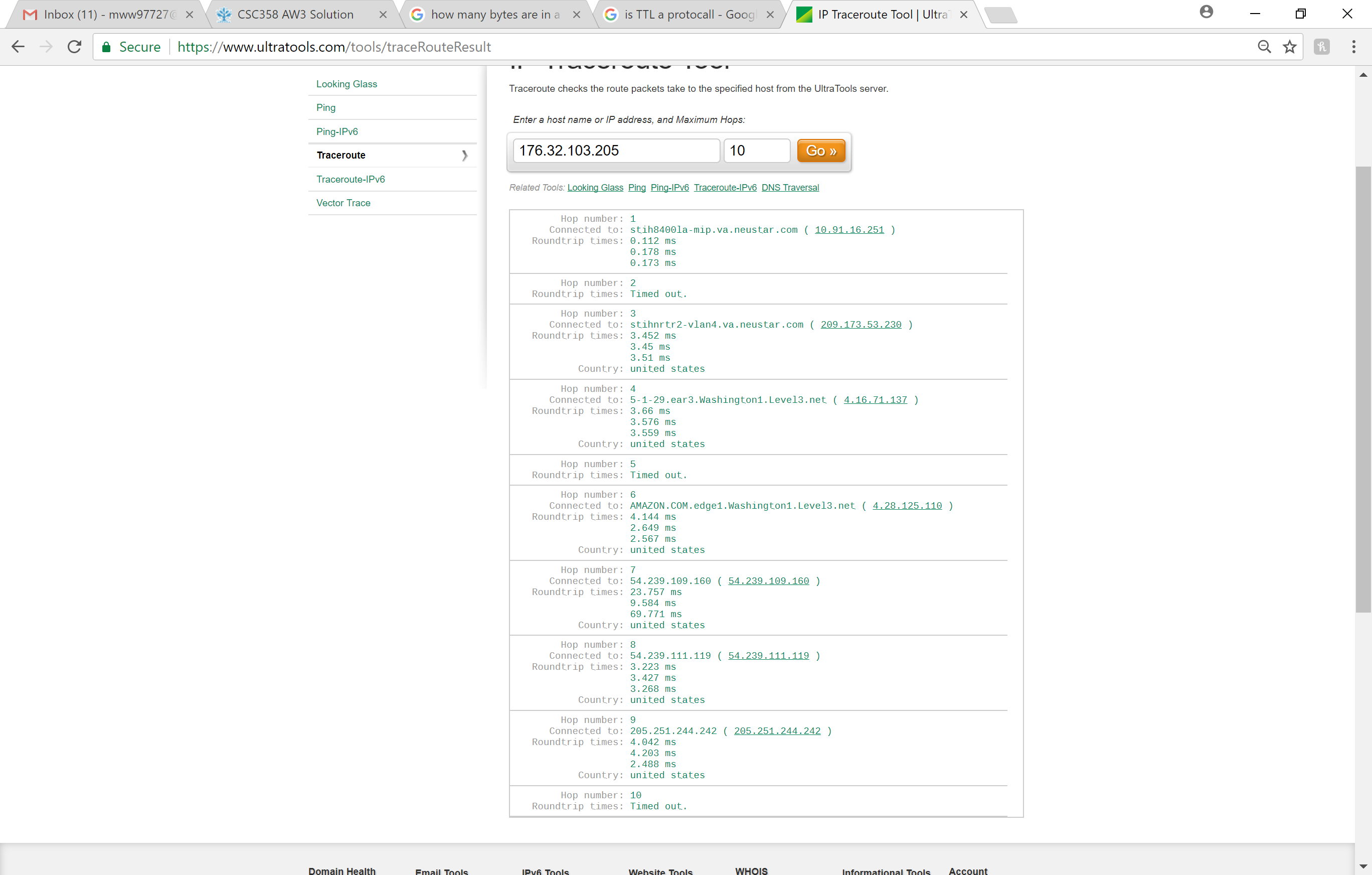
19. Who owns the IP?

Search 176.32.103.205

**Amazon**

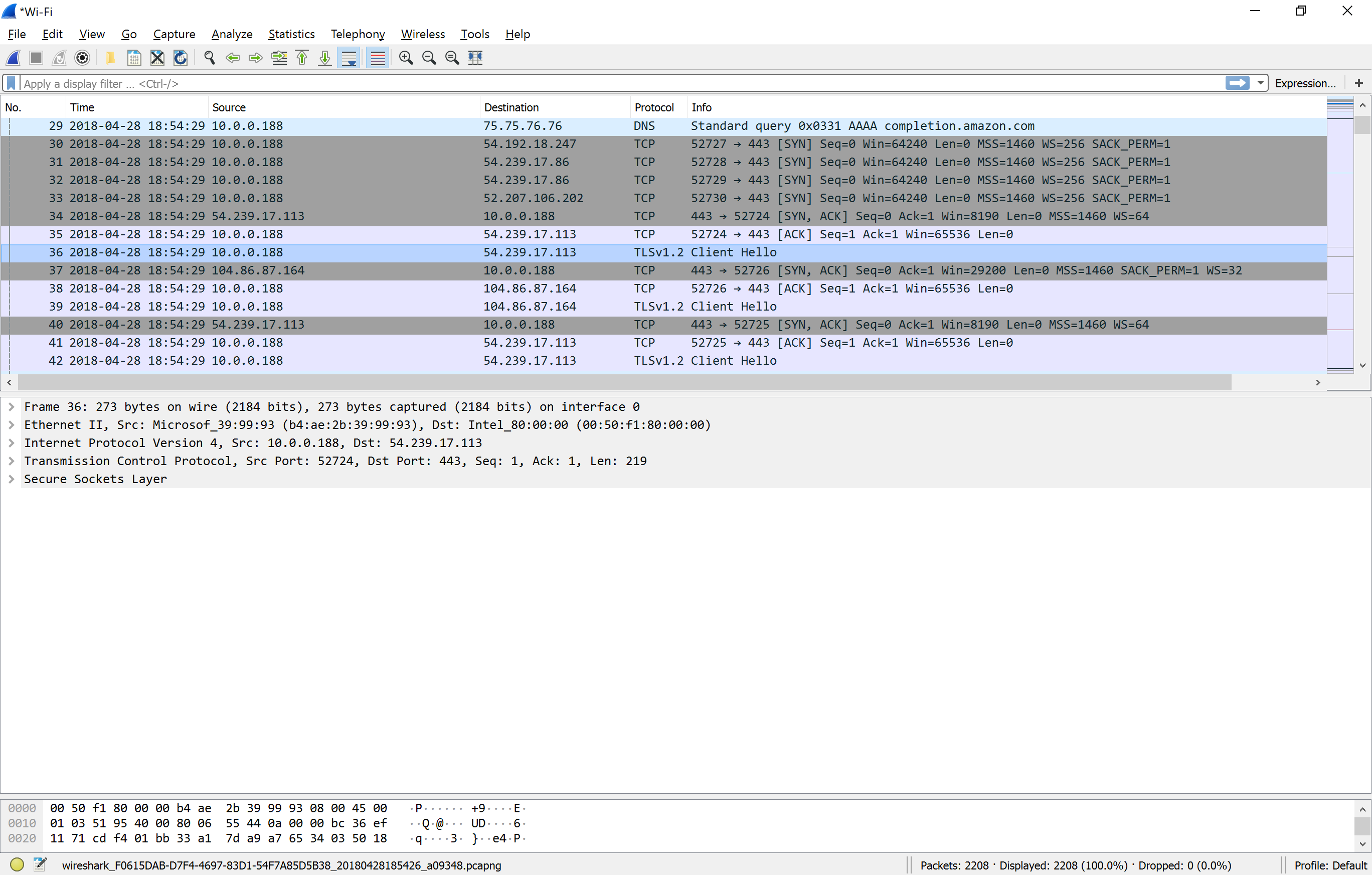


20. In addition to a screenshot, in a tabular form, list all the hops between your computer’s IP and the IP address in Figure 1. The table should include the owner, and location of the IP address.





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. **1.2**



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

**Cipher Suites (14 suites)**

**Cipher Suite: Reserved (GREASE) (0xcaca)**

**Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)**

**Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)**

**Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc02c)**

**Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)**

**Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcca9)**

**Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcca8)**

**Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc013)**

**Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xc014)**

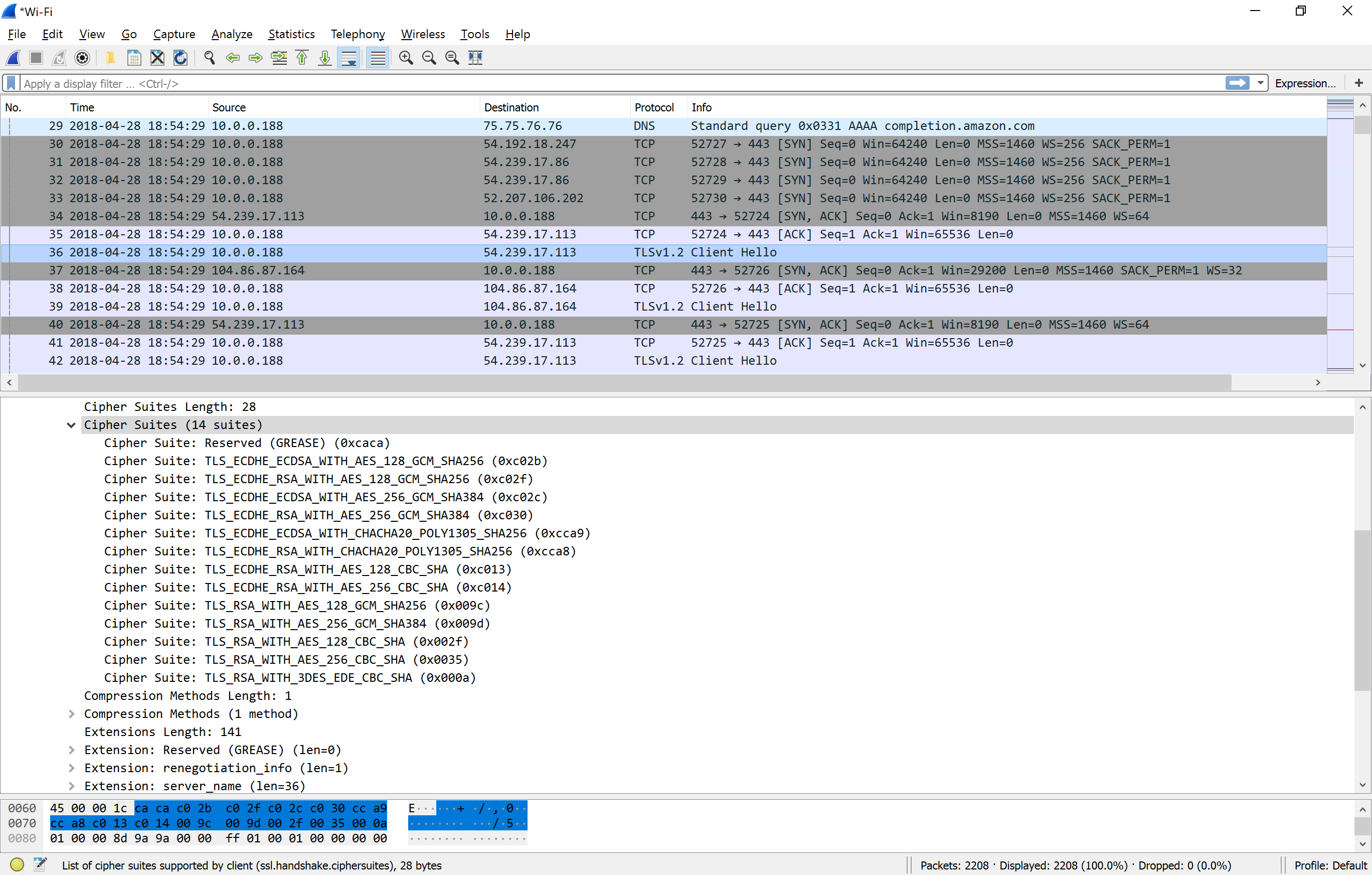
**Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0x009c)**

**Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x009d)**

**Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002f)**

**Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)**

**Cipher Suite: TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x000a)**



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

**443**

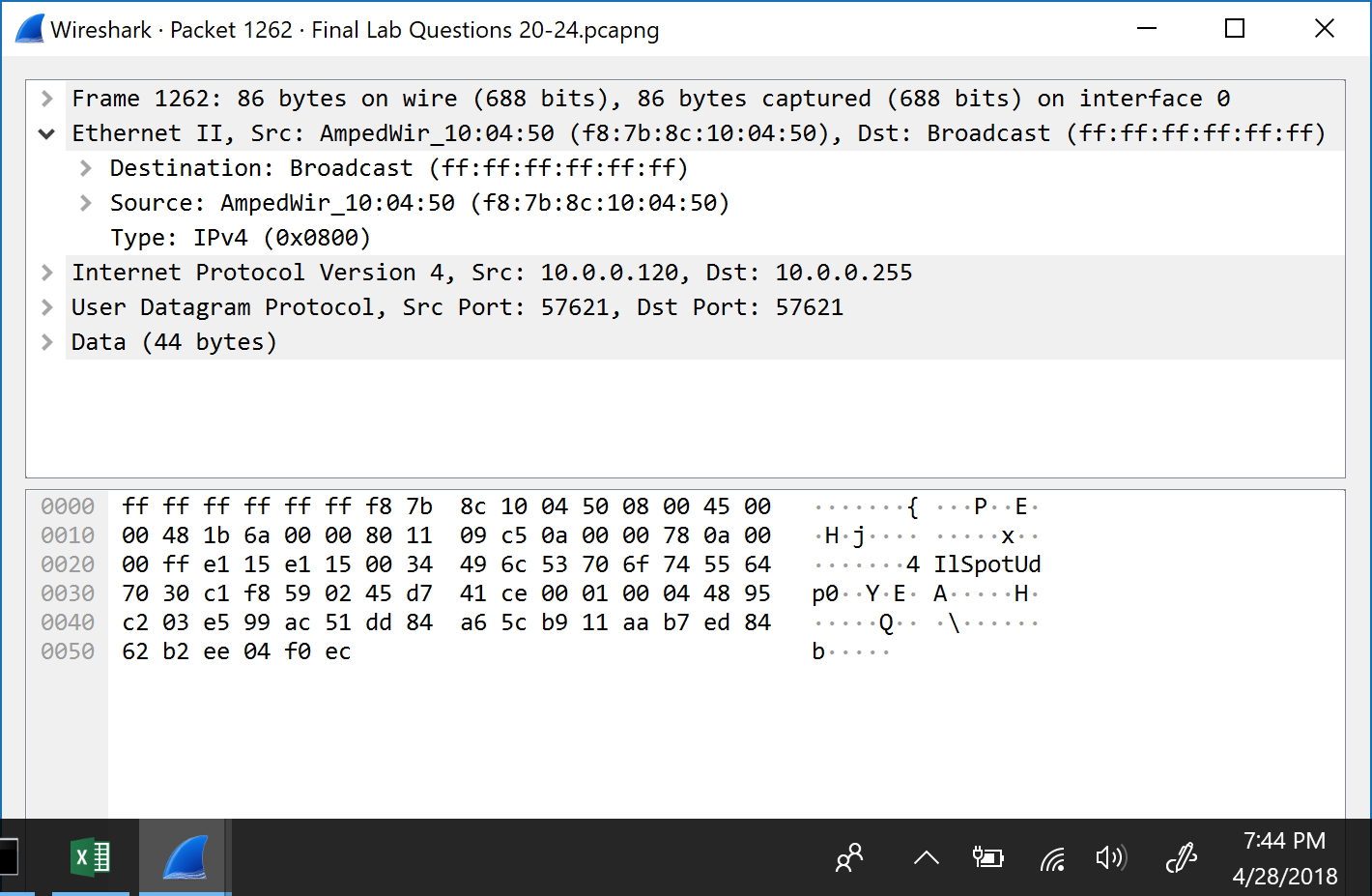
**It is using it because 443 is a known TCP port for TLS traffic**



24. What are the source and destination MAC address? (My machine and router????

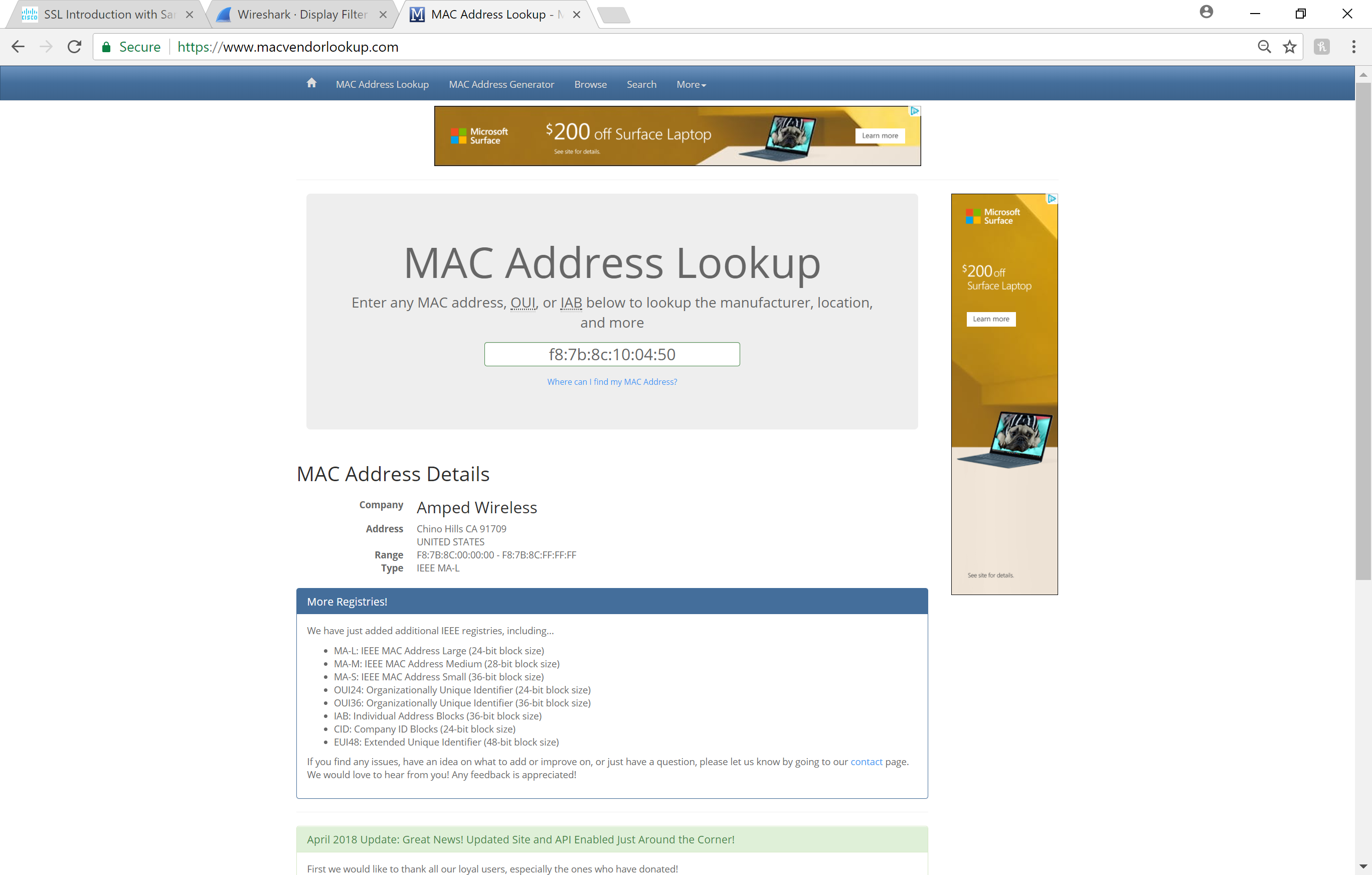
**Source f8:7b:8c:10:04:50**

**Destination ff:ff:ff:ff:ff:ff**



25. 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).

**Amped Wireless**



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. INCLUDE THE FINAL

**Under usmnco**