**COMPUTER NETWORKS**

**LAB – 2**

Name: Naga Tharun Makkena

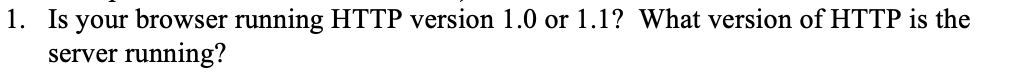
Roll No: SE20UCSE105

Section: CSE-2

1. **Wireshark\_HTTP\_v7.0 lab sheet**

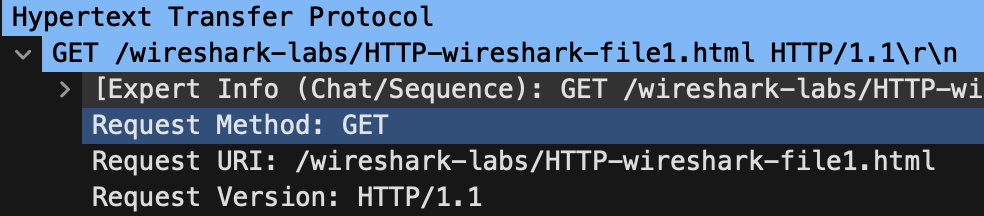
--------------------------------------------------------------------------------------------------------------------------------------

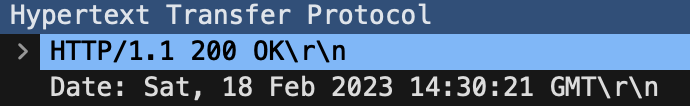


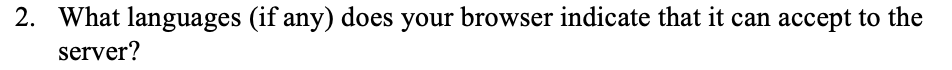


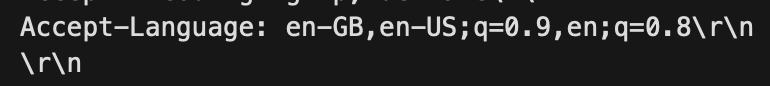
Ans: HTTP version of browser: 1.1

HTTP version of server: 1.1







Ans: 



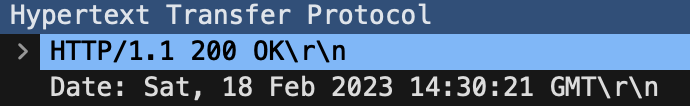
Ans: IP address of computer: 10.59.193.228

IP address of gaia.cs.umass.edu server: 128.119.245.12



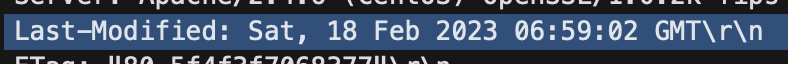


Ans: Status code: **200**



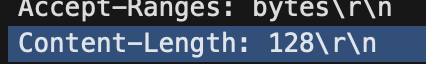


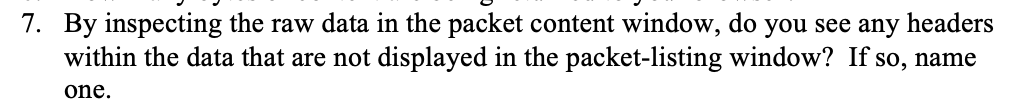
Ans: File last modified: Sat, 18 Feb 2023 06:59:02 GMT



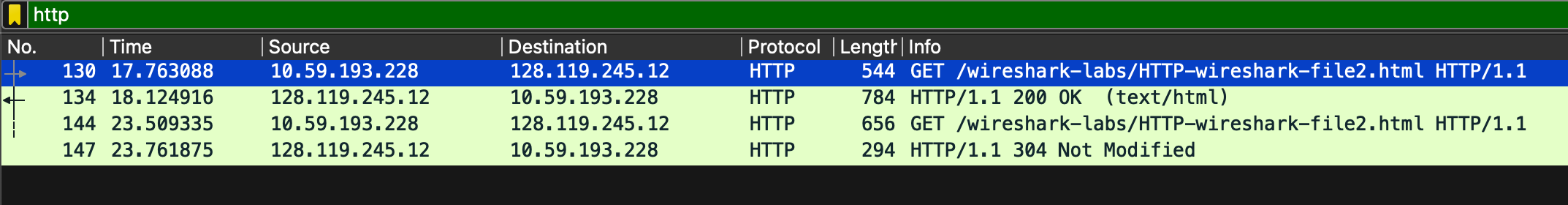


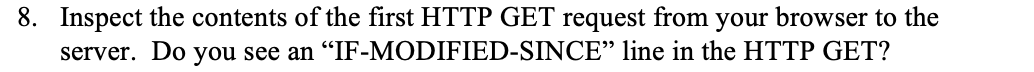
Ans: **128 bytes** of content.





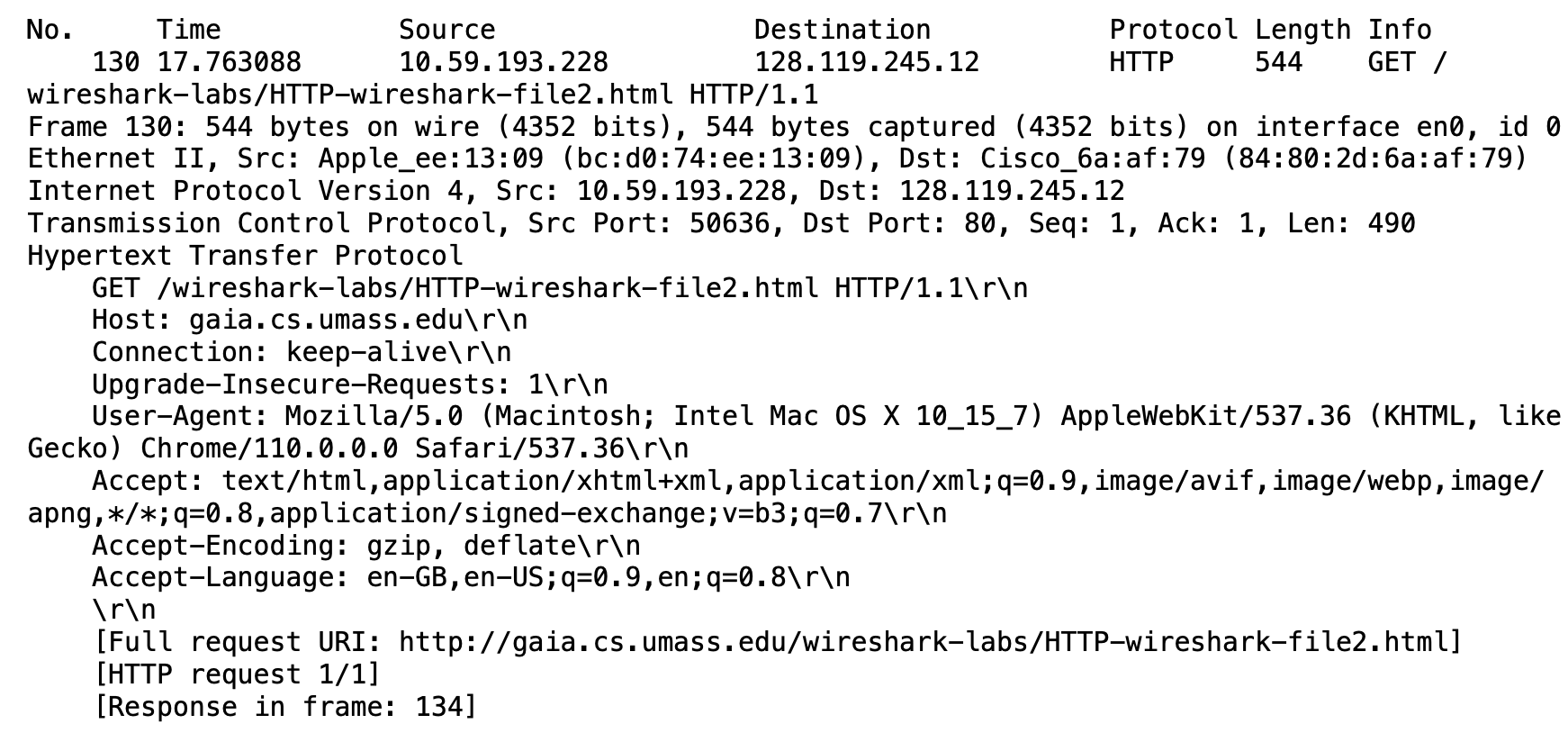
Ans: **No**, I don’t see any in the HTTP message.

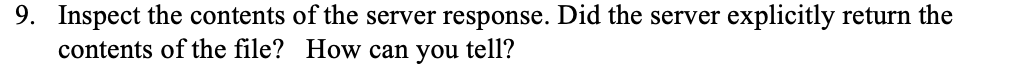


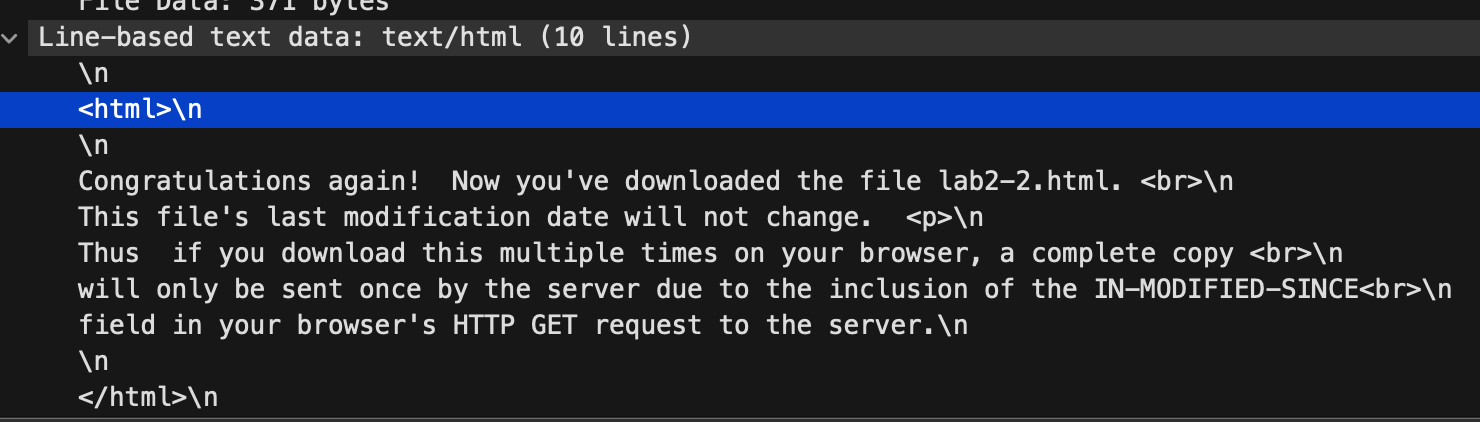


Ans: There is **no “IF-MODIFIED-SINCE” line** in the first HTTP GET request.

**1st GET request**

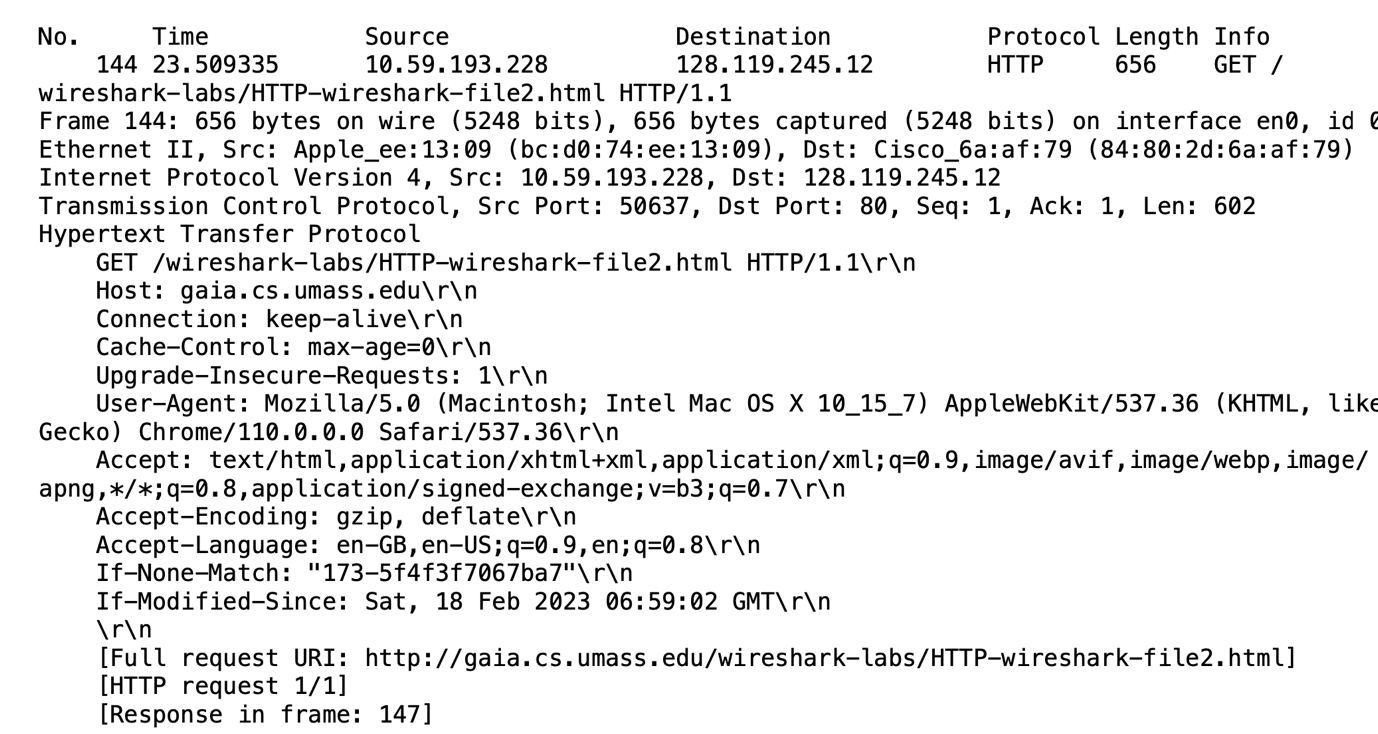


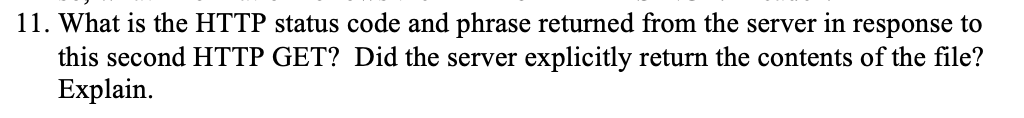


Ans: Text returned in response to the first GET 



Ans: **Yes, “IF-MODIFIED-SINCE” line is found** in the 2nd HTTP GET request. It has the information of the time the file was last accessed which is stored in cache.

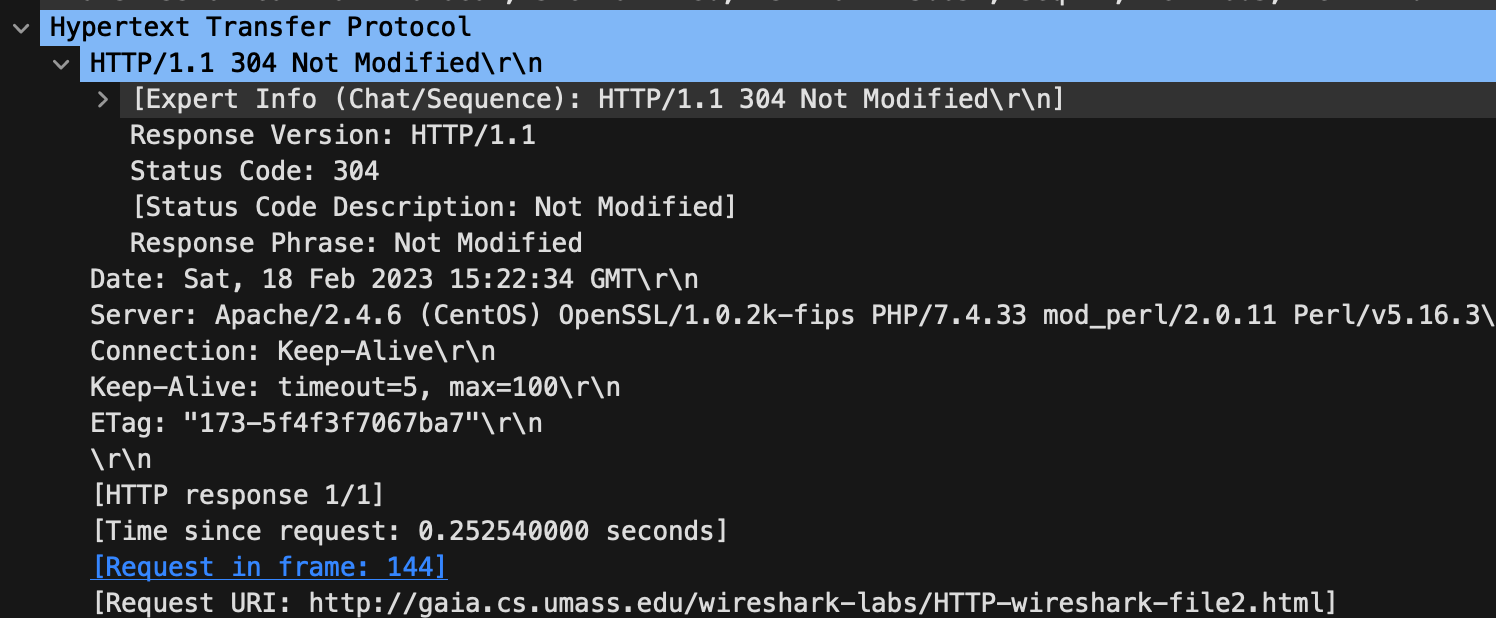
**2nd GET request** 

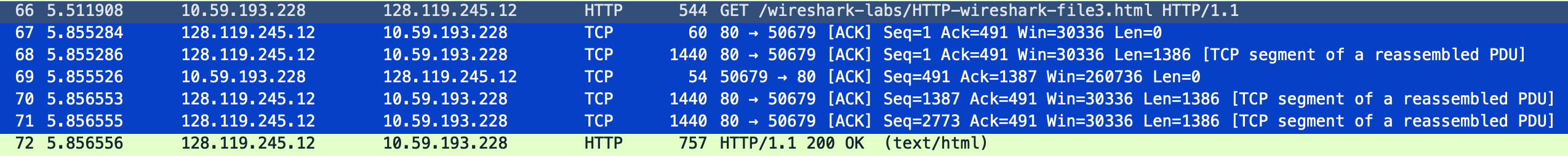


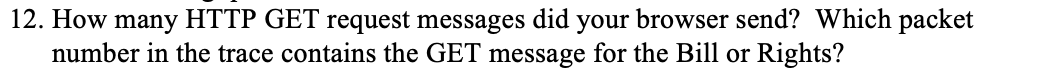
Ans: HTTP status code: **204**

Phrase: “**Not Modified**”

**No contents are returned** as the contents of the file is not modified.

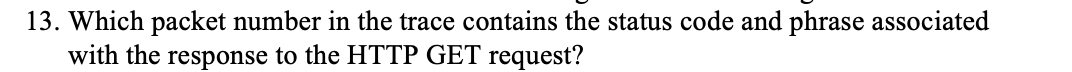






Ans: Number of HTTP GET request messages browser sent: **1**

Packet number that contains GET message for the Bills or Rights: **66**

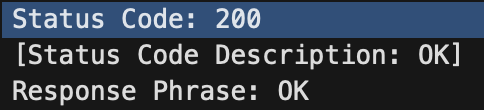


Ans: Packet **68**



Ans: Status code: **200**

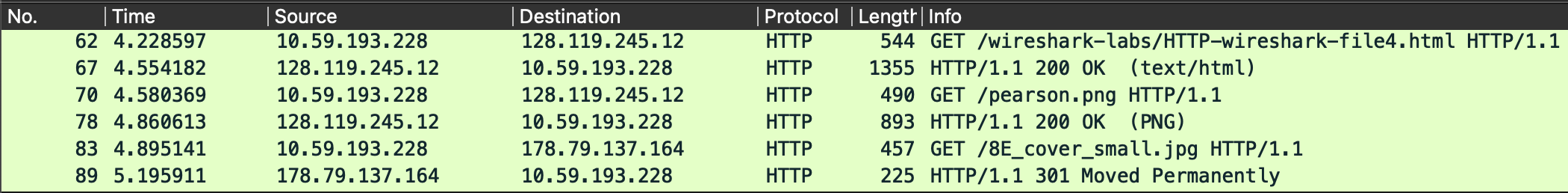
Phrase: “**OK**”

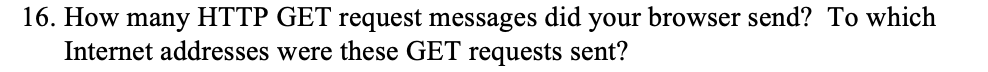




Ans: Number of data containing TCP segments needed: **3 packets**

**They are 68, 70, 71 in the trace.**



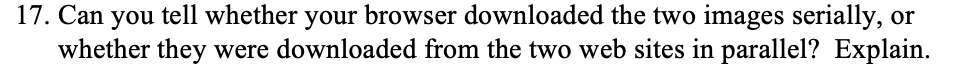


Ans: **Three HTTP GET request messages** are sent by the browser.

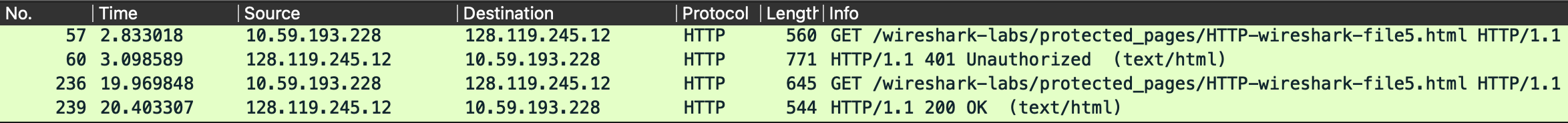
Packet 62 in trace for **getting the base file** to internet address: **128.119.245.12**

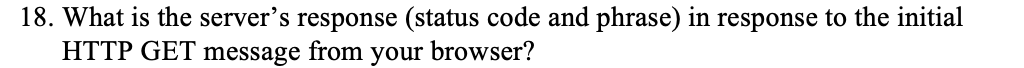
Packet 70 in trace **to** **get the pearson logo** to internet address: **128.119.245.12**

Packet 83 in trace **to get the image of 5th edition book cover** to internet address: **178.79.137.164**



Ans: The downloads from the two websites occurred in **parallel**.

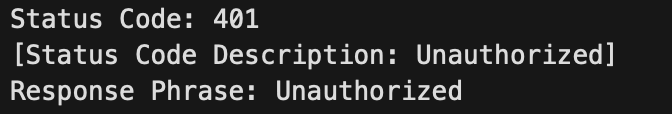


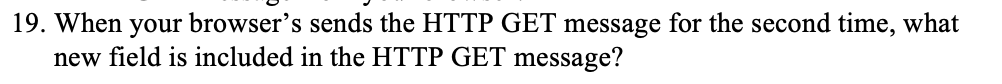


Ans: The first GET request is from packet 57 in trace. And the first REPLY is packet 60 in the trace.

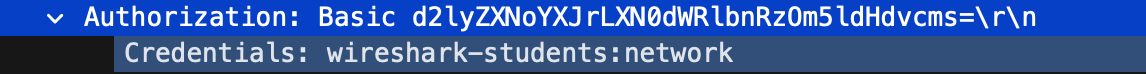
Status code: **401**

Phrase: “**Unauthorized**”





Ans: It included “**Authorization: Basic”** field.

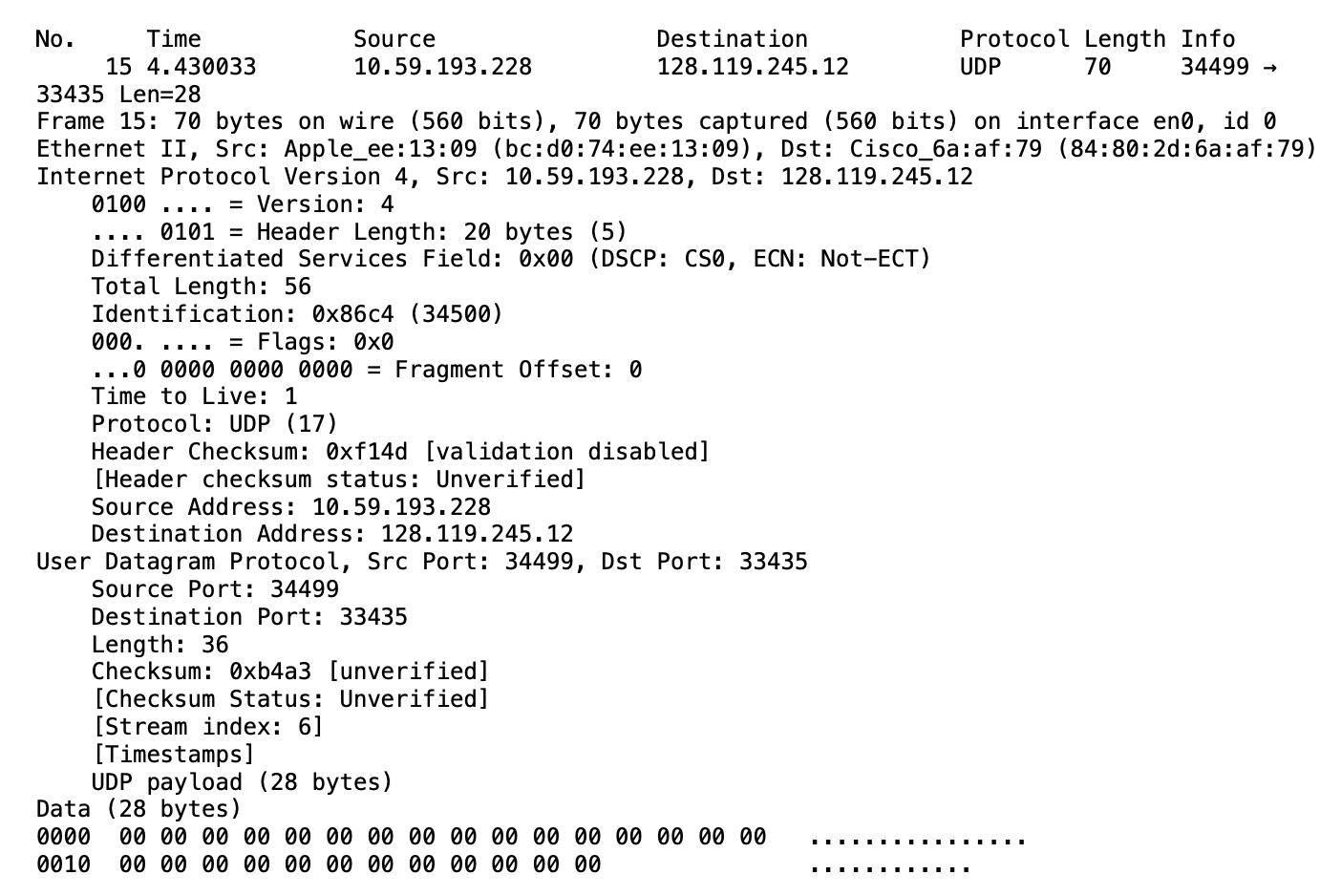


1. **Wireshark\_IP\_v7.0 lab sheet**

--------------------------------------------------------------------------------------------------------------------------------------

Being a mac system, a series of UDP segment is visible but not ICMP Echo Request.

Attaching the print of the data of 1st UDP packet.

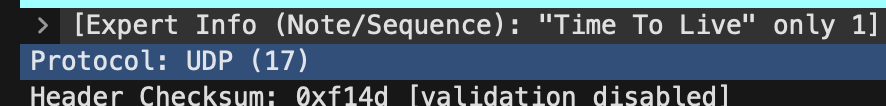


1. 

Ans: IP address: **10.59.193.228**



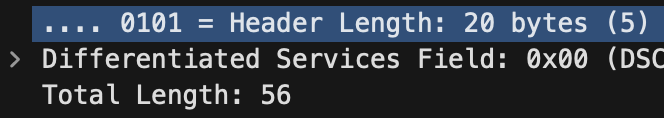
Ans: The upper layer protocol field is: **UDP (17)**

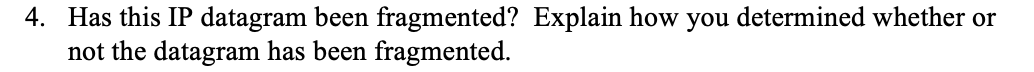




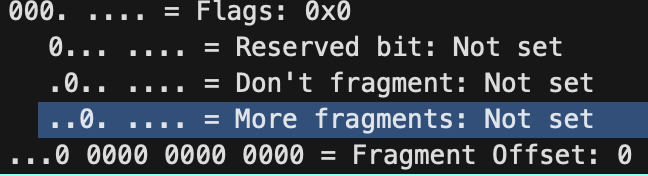
Ans: Number of bytes in IP header: **20 bytes.** Total length: **56 bytes.**

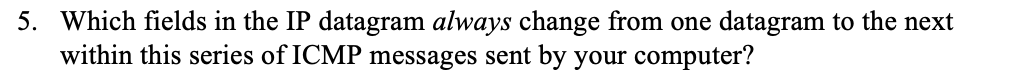
Then the **payload is: total length – bytes in IP header = 36 bytes**

****

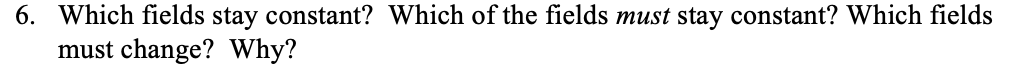


Ans: The more fragments bit is 0, so the datagram is **not fragmented**.





Ans: **Identification, Time to live, Header checksum** always change.

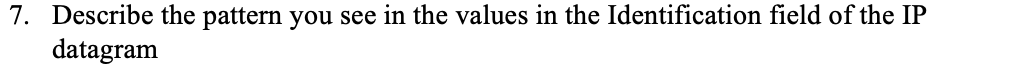


Ans: The fields that stay constant are: **Version, header length, differentiated services, destination IP, source IP, upper layer protocol.**

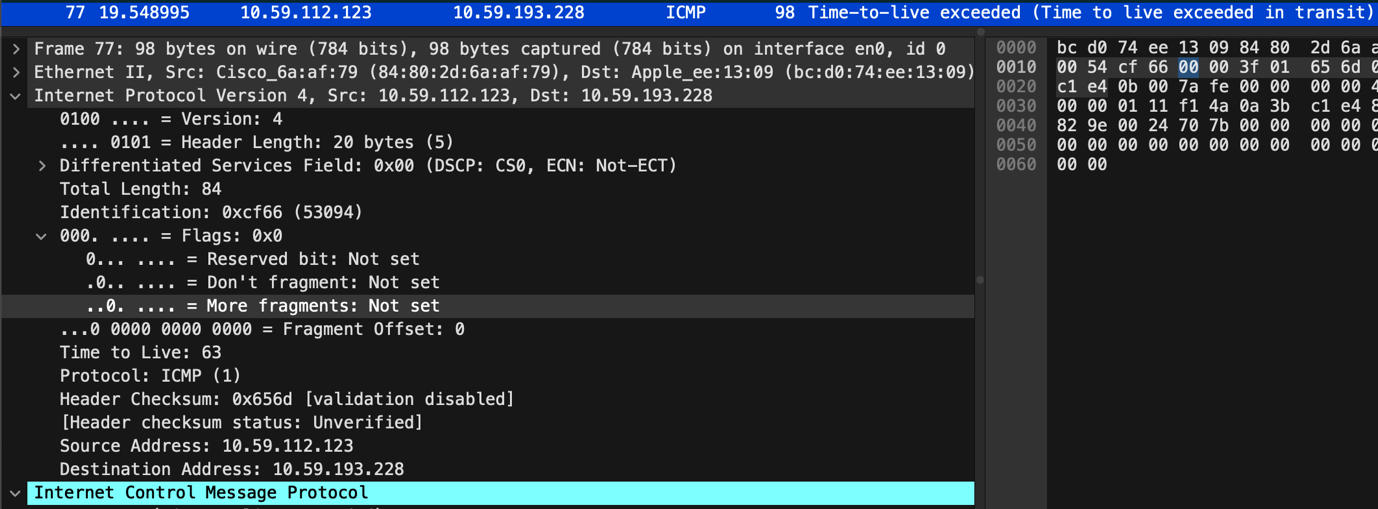
The fields that must stay constant are: **Version, header length, differentiated services, destination IP, source IP, upper layer protocol.**

The fields that must change are: **Identification, Time to live, Header checksum.**

**Because each IP packet must have different id, traceroute increments each subsequent packet, as the header changes checksum must also change.**



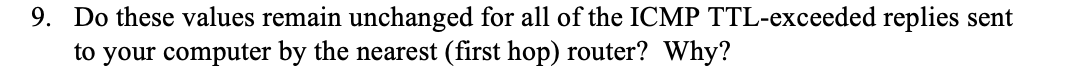
Ans: The value in the Identification field **increments** with each UDP request.





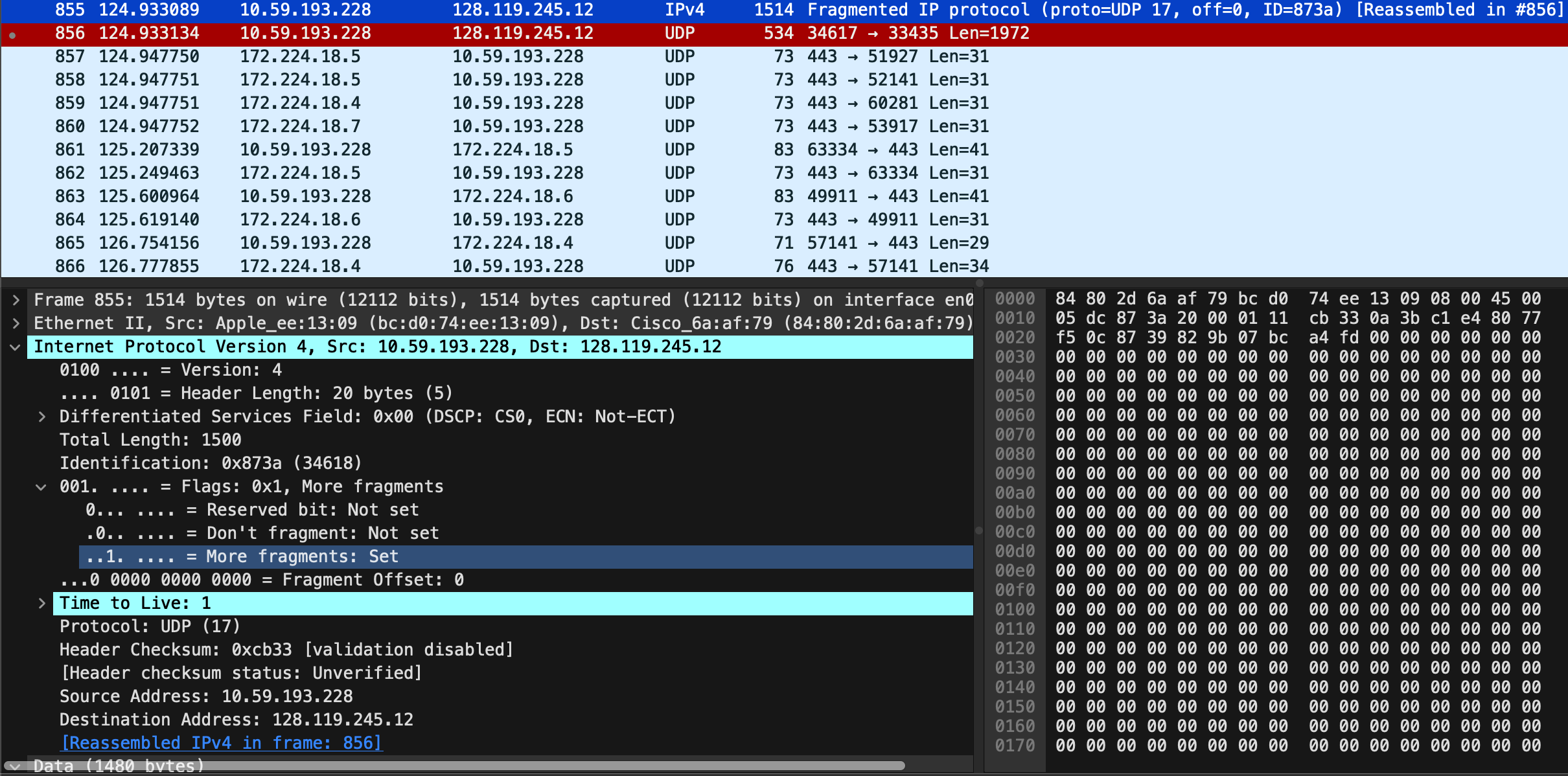
Ans: Identification: 0xcf66 (53094)

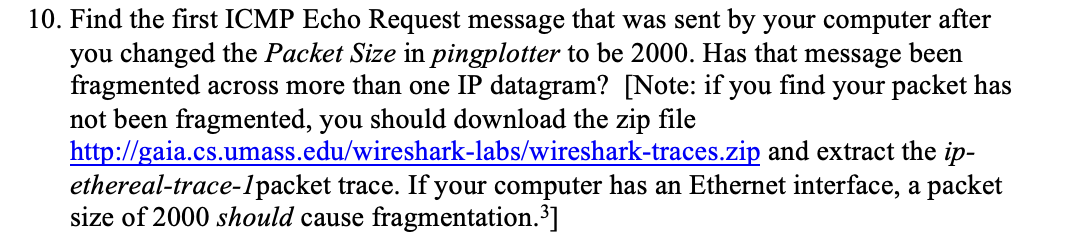
Time to live (TTL): 63



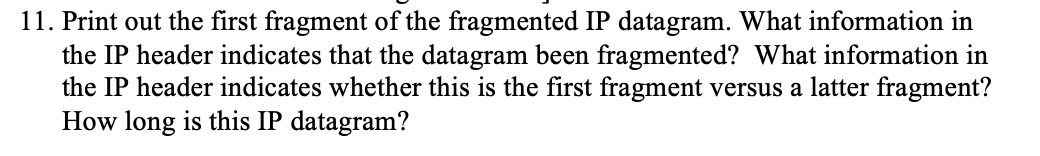
Ans: The **identification field value changes** for every reply as it is unique. When more IP datagrams have same identification field that means they are fragments of a single large IP datagram.

The **TTL field remains constant** for the nearest (first hop) router.





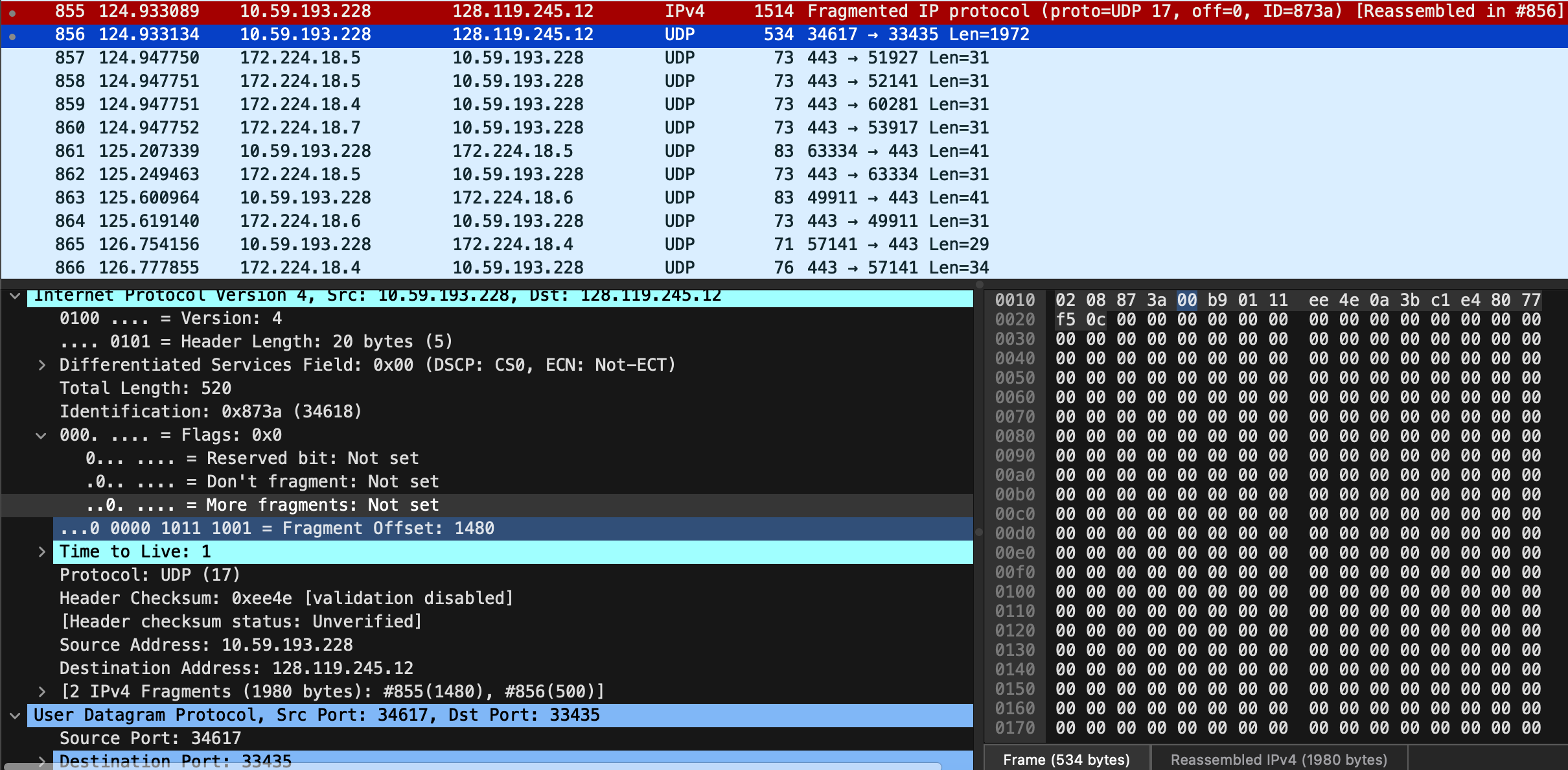
Ans: Yes, this packet has been fragmented across more than one datagram.

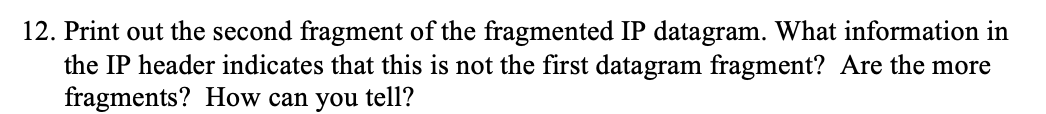


Ans: The **More fragments field is set** indicating that the **packet is fragmented**.

The **Fragment offset is set to 0** meaning it is **the 1st fragment**.

The fragment has a **total length: 1500** including the header.



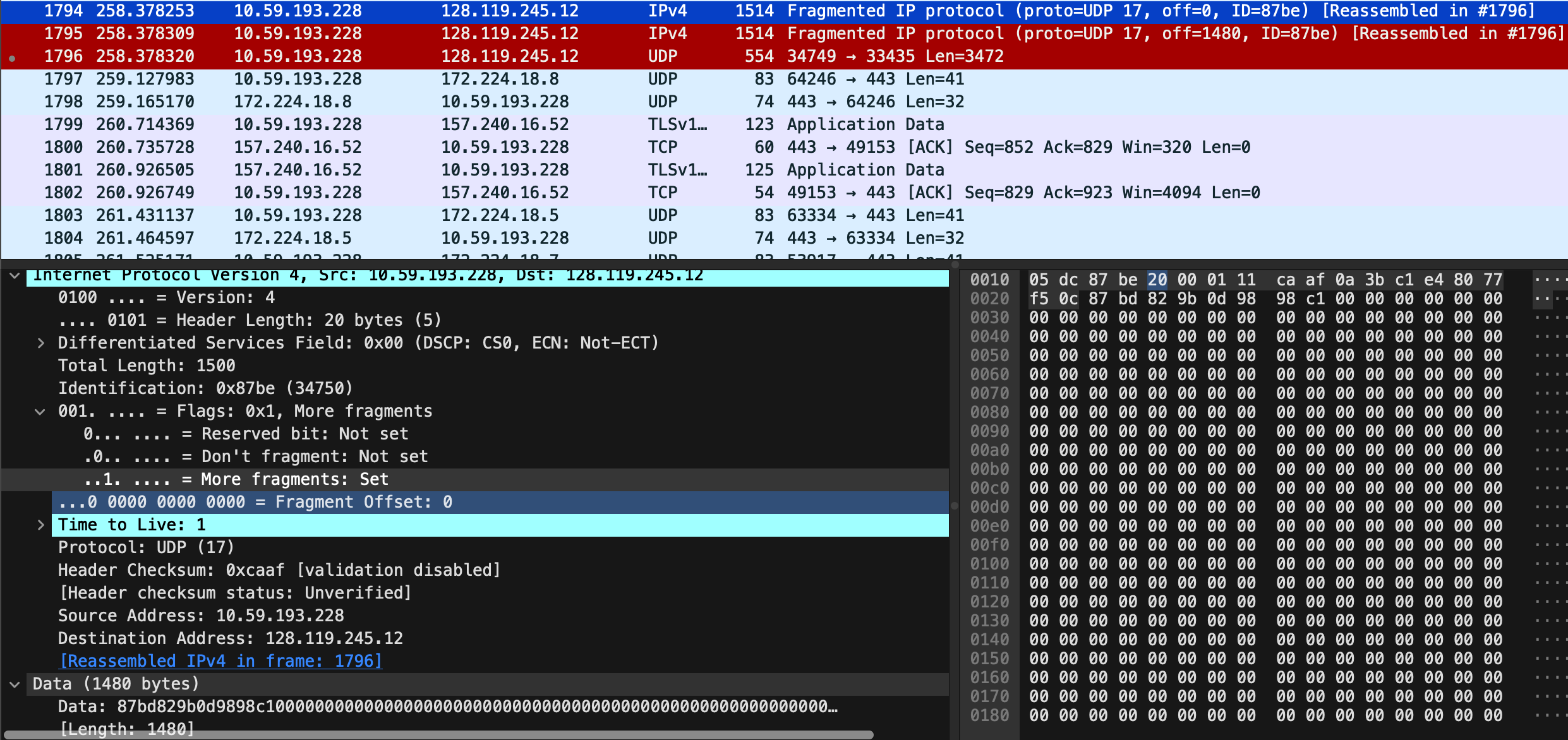


Ans: The **fragment offset is set to 1480** meaning it is **not the first fragment**.

The **More fragments field is not set** meaning it is the **last fragment**.



Ans: **Total length, flags, checksum, fragment offset**.





Ans: **Three fragments** are created from the original datagram after switching to 3500.



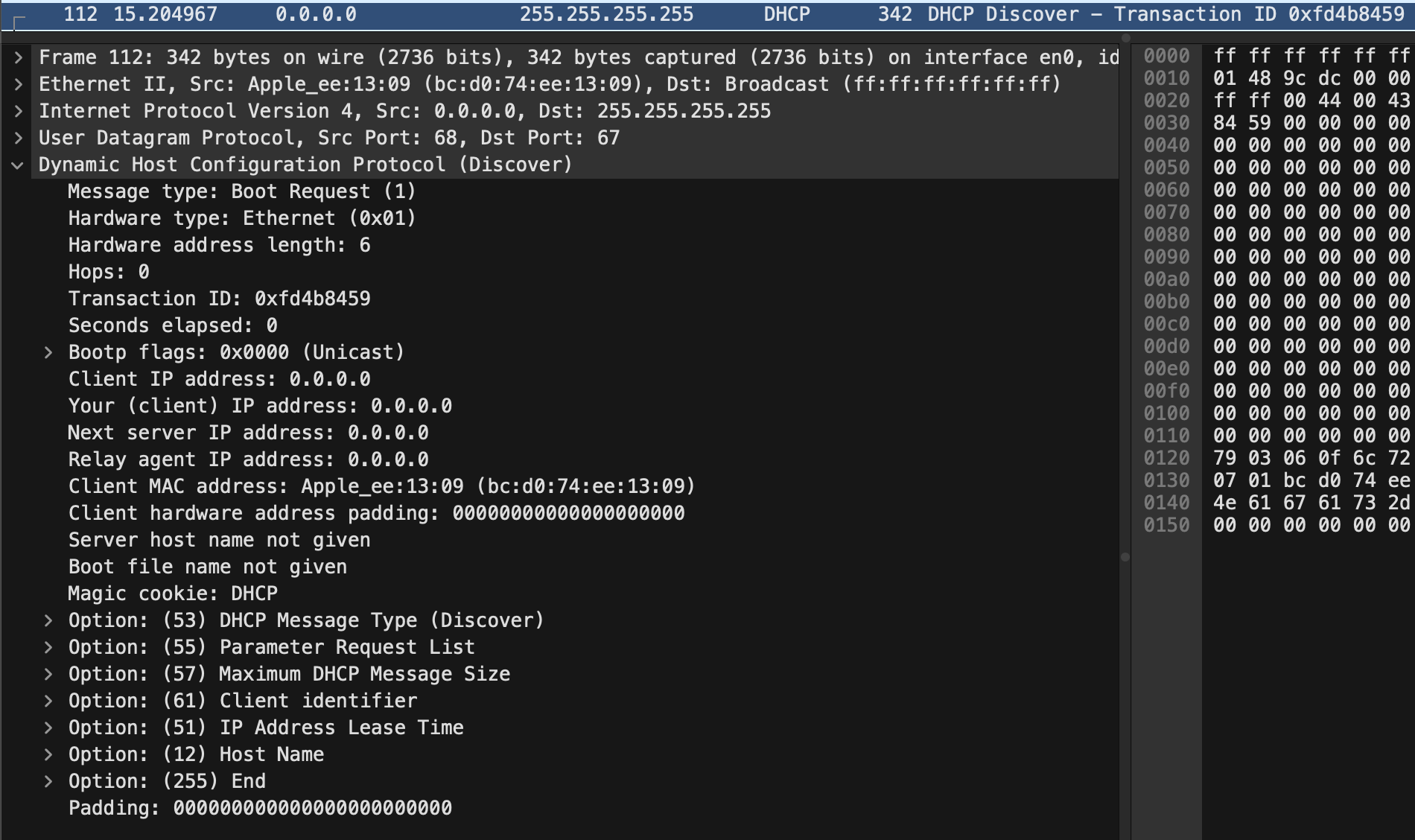
Ans: First 2 packets: have same total length: 1500, more fragments: 1 but the last packet has total length: 540, more fragments: 0.

**Fragment offset and header checksum** changes for all three fragments.

1. **Wireshark\_DHCP\_v7.0 lab sheet**

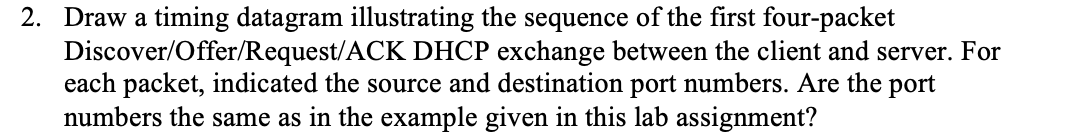
--------------------------------------------------------------------------------------------------------------------------------------



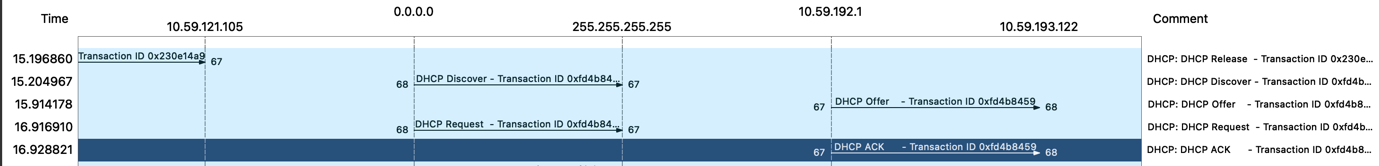




Ans: DHCP messages are sent over **UDP**.



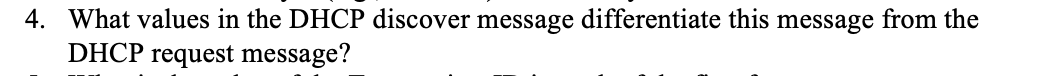
Ans: The port numbers are **67, 68**. They are the same in the lab.

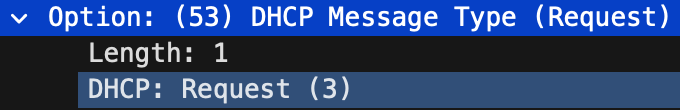
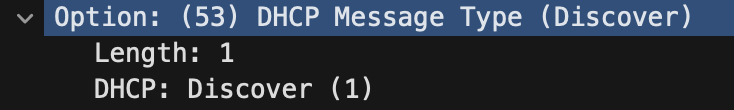


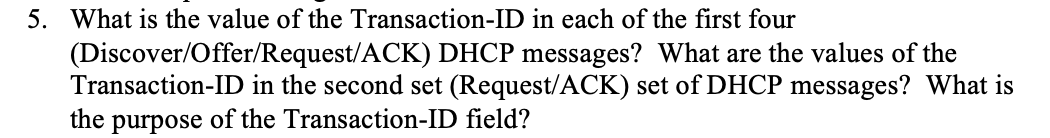


Ans: The link-layer address of my host is **bc:d0:74:ee:13:09**

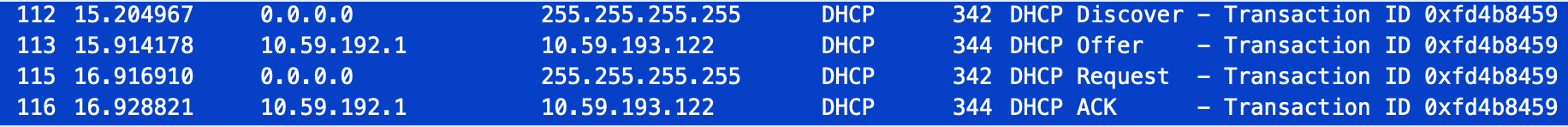




Ans: **Option 53** in DHCP request differs between Request and Discover.



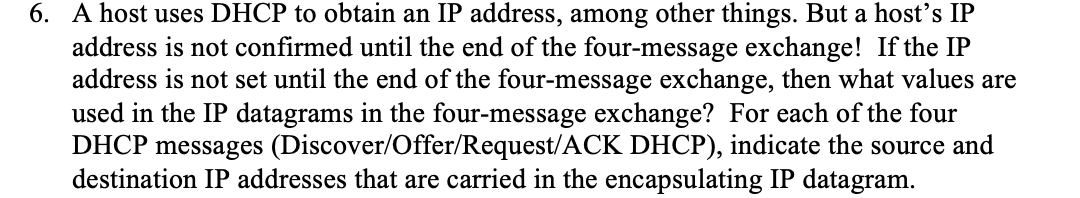
Ans: First 4 (Discover/Offer/Request/ACK) DHCP messages transaction id: 0xfd4b8459



Transaction id of second set (Request/ACK) DHCP messages id: 0xfd4b845a



Transaction id is used to differentiate between different client requests during the request process.



Ans: Source:

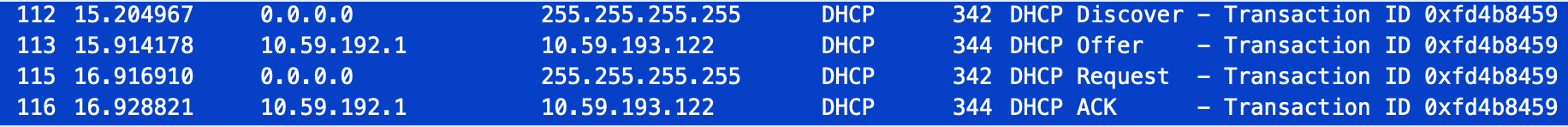
Discover, Request: 0.0.0.0

Offer, ACK: 10.59.192.1

Destination:

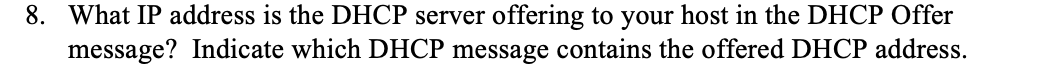
Discover, Request: 255.255.255.255

Offer, ACK: 10.59.193.122



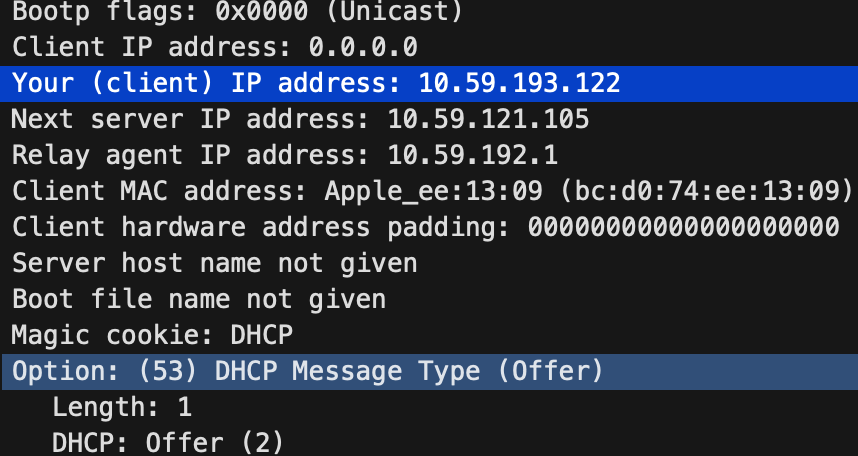


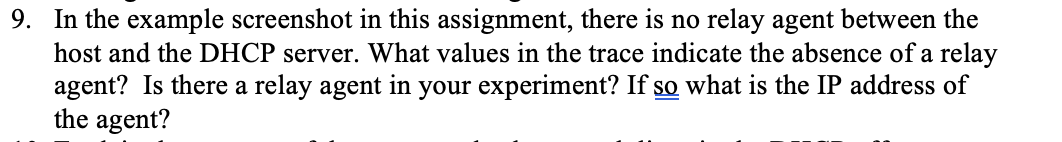
Ans: IP address of my DHCP server: **10.59.191.1**



Ans: IP address offered by DHCP server is: **10.59.193.122**

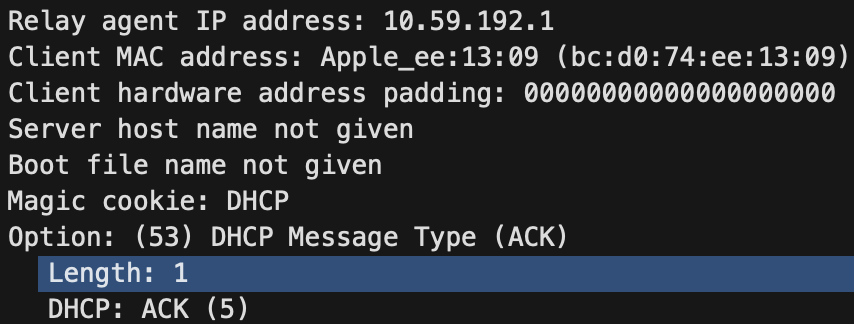
**DHCP offer** message offered DHCP address.

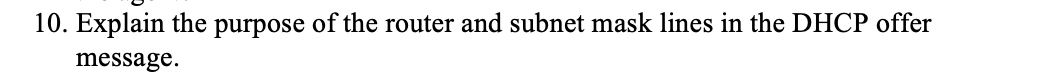




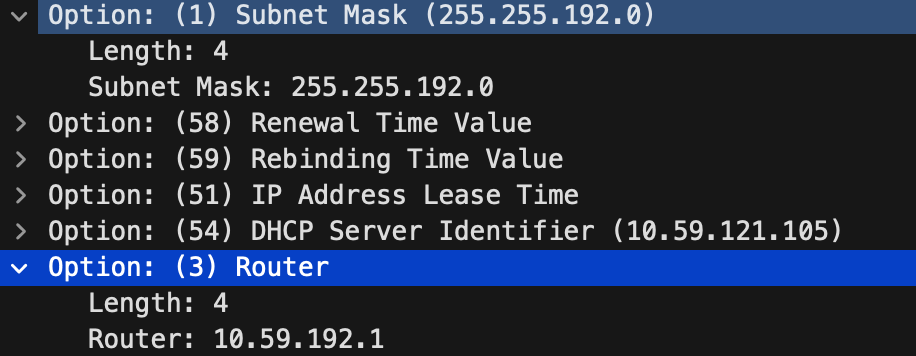
Ans: In the screenshot the relay agent IP address is: 0.0.0.0 this indicates there is no DHCP relay used.

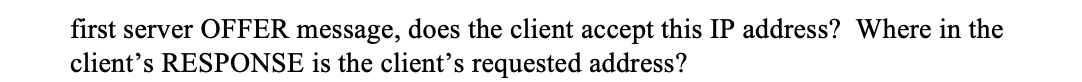
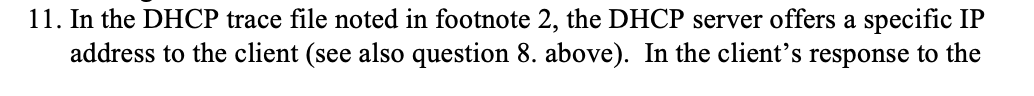
In my experiment the relay agent IP address is: **10.59.191.1**





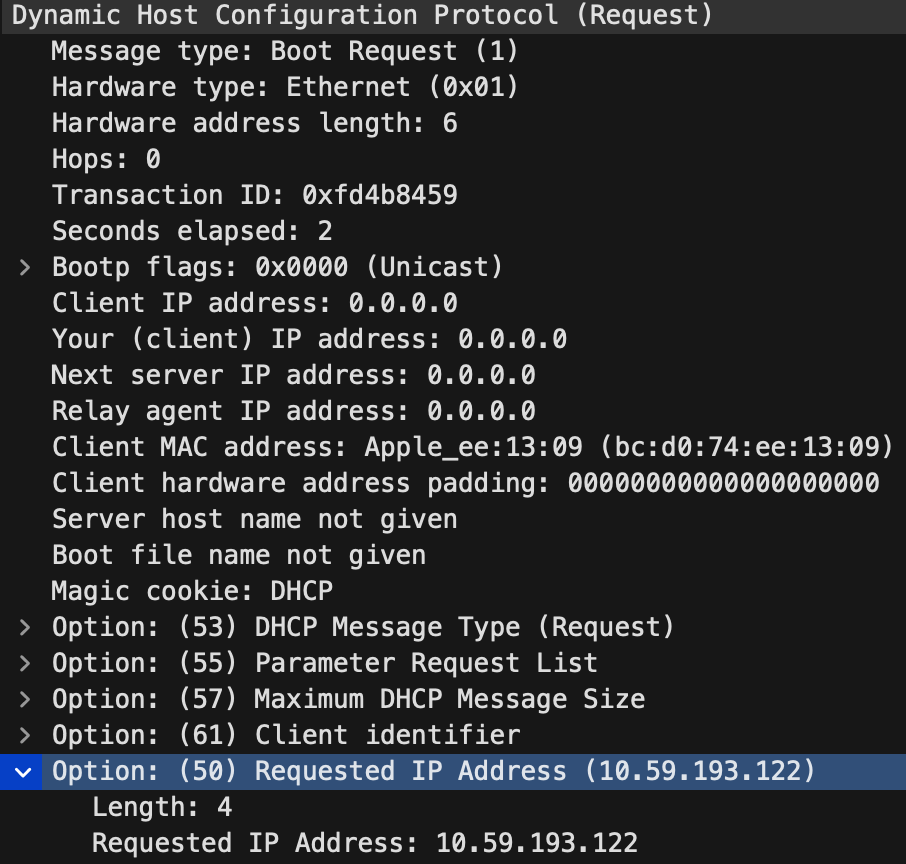
Ans: The subnet mask line tells the client which subnet mask to use. The router line indicates the client what its default gateway should be.





Ans: Client accepts the IP address offered by the DHCP server.

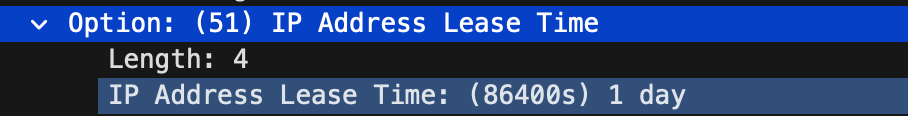
Client’s response in **option 50 of the request message**.

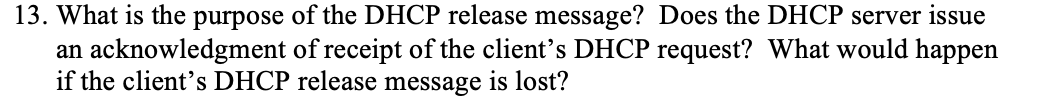




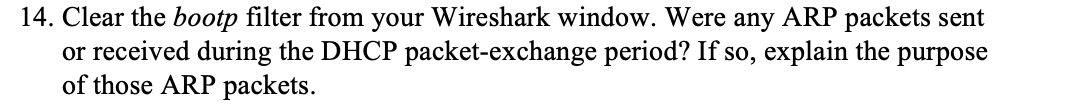
Ans: Lease time is the amount of time the DHCP server assigns an IP address to a client. The IP address is not assigned to any other client unless the lease time is over or the client gives up the IP address. After the lease time is over, the IP address is auto assigned to another client.

Lease time in my experiment is: **1 day.**





Ans: DHCP release message is sent to cancel the lease on the IP address given by the DHCP server. It is sent by the client. The DHCP server does not issue any acknowledgement of the DHCP release message. If the message is lost, the server has to wait till the lease time to be over to reuse the IP address for another client.



Ans: Yes, the ARP requests are made by the DHCP server. Before offering an IP address to a client, the server makes an ARP request to check if the IP address is already in use by any other client or workstation.

