COMPUTER NETWORKS

LAB – 2

Name: Naga Tharun Makkena

Roll No: SE20UCSE105

Section: CSE-2

---

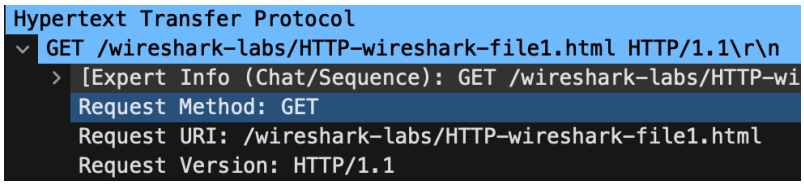
1. Wireshark_HTTP_v7.0 lab sheet

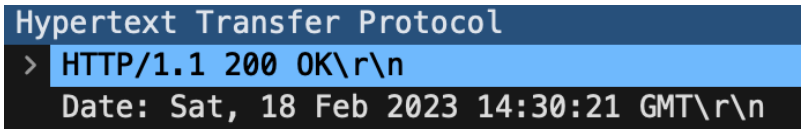
```
No.     Time           Source                Destination           Protocol Length Info
     82 11.042329      10.59.193.228         128.119.245.12        HTTP     544    GET /
wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 82: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface en0, id 0
Ethernet II, Src: Apple_ee:13:09 (bc:d0:74:ee:13:09), Dst: Cisco_6a:af:79 (84:80:2d:6a:af:79)
Internet Protocol Version 4, Src: 10.59.193.228, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 530
    Identification: 0x0000 (0)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xf742 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.59.193.228
    Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 50575, Dst Port: 80, Seq: 1, Ack: 1, Len: 490
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/
1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/110.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 90]
    [Next request in frame: 92]
```

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Ans: HTTP version of browser: 1.1

HTTP version of server: 1.1





2. What languages (if any) does your browser indicate that it can accept to the server?

Ans:

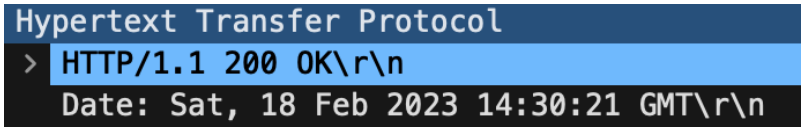
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Ans: IP address of computer: 10.59.193.228

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

4. What is the status code returned from the server to your browser?

Ans: Status code: **200**



5. When was the HTML file that you are retrieving last modified at the server?

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

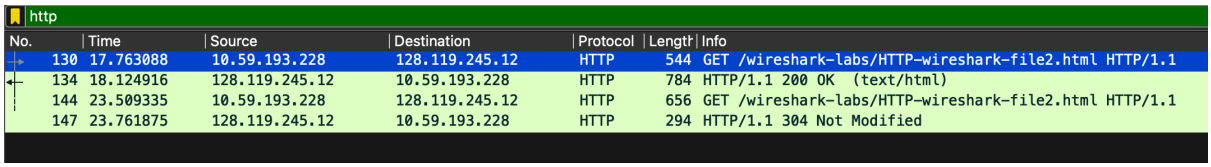
6. How many bytes of content are being returned to your browser?

Ans: **128 bytes** of content.

```
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
```

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

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



8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

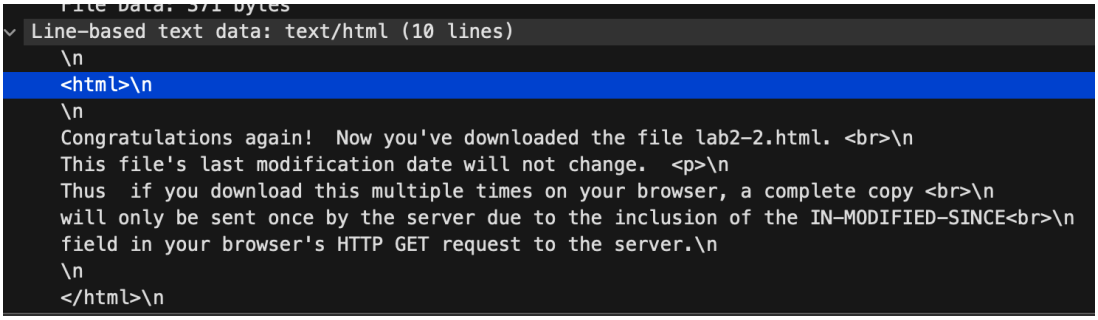
Ans: There is **no "IF-MODIFIED-SINCE" line** in the first HTTP GET request.

1st GET request

```
No.     Time           Source                Destination           Protocol Length Info
    130 17.763088      10.59.193.228         128.119.245.12        HTTP     544    GET /
wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Frame 130: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface en0, id 0
Ethernet II, Src: Apple_ee:13:09 (bc:d0:74:ee:13:09), Dst: Cisco_6a:af:79 (84:80:2d:6a:af:79)
Internet Protocol Version 4, Src: 10.59.193.228, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50636, Dst Port: 80, Seq: 1, Ack: 1, Len: 490
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/110.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 134]
```

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Ans: Text returned in response to the first GET



10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?

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

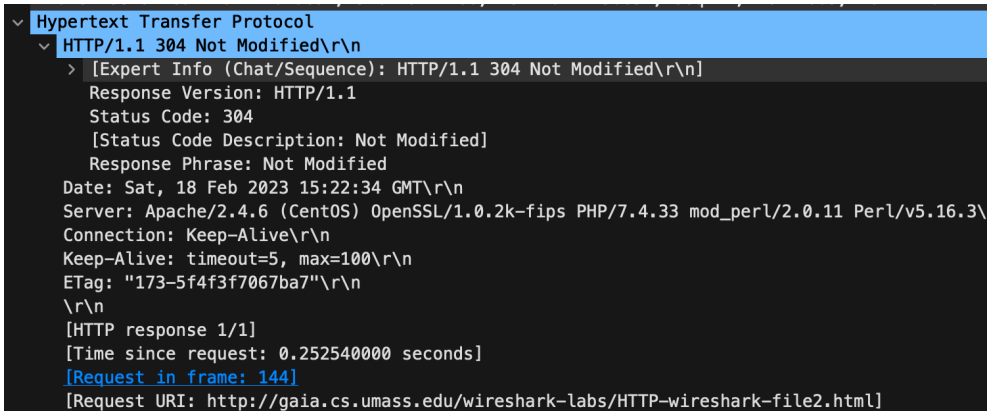
```
No.     Time           Source                Destination           Protocol Length Info
    144 23.509335      10.59.193.228         128.119.245.12        HTTP     656    GET /
wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Frame 144: 656 bytes on wire (5248 bits), 656 bytes captured (5248 bits) on interface en0, id 0
Ethernet II, Src: Apple_ee:13:09 (bc:d0:74:ee:13:09), Dst: Cisco_6a:af:79 (84:80:2d:6a:af:79)
Internet Protocol Version 4, Src: 10.59.193.228, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50637, Dst Port: 80, Seq: 1, Ack: 1, Len: 602
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/110.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    If-None-Match: "173-5f4f3f7067ba7"\r\n
    If-Modified-Since: Sat, 18 Feb 2023 06:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 147]
```

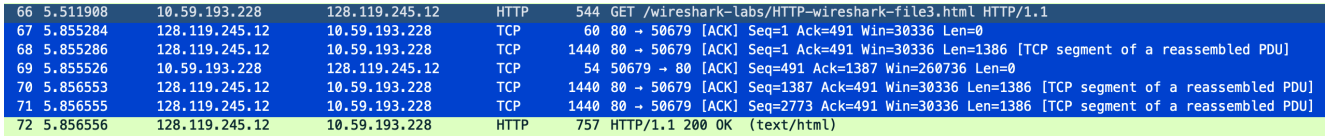
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Ans: HTTP status code: **204**

Phrase: "**Not Modified**"

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





12. 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?

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

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

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

Ans: Packet **68**

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

Ans: Status code: **200**

Phrase: "**OK**"

```
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
```

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

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

They are 68, 70, 71 in the trace.

No.	Time	Source	Destination	Protocol	Length	Info
62	4.228597	10.59.193.228	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
67	4.554182	128.119.245.12	10.59.193.228	HTTP	1355	HTTP/1.1 200 OK (text/html)
70	4.580369	10.59.193.228	128.119.245.12	HTTP	490	GET /pearson.png HTTP/1.1
78	4.860613	128.119.245.12	10.59.193.228	HTTP	893	HTTP/1.1 200 OK (PNG)
83	4.895141	10.59.193.228	178.79.137.164	HTTP	457	GET /8E_cover_small.jpg HTTP/1.1
89	5.195911	178.79.137.164	10.59.193.228	HTTP	225	HTTP/1.1 301 Moved Permanently

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

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**

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

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

No.	Time	Source	Destination	Protocol	Length	Info
57	2.833018	10.59.193.228	128.119.245.12	HTTP	560	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
60	3.098589	128.119.245.12	10.59.193.228	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
236	19.969848	10.59.193.228	128.119.245.12	HTTP	645	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
239	20.403307	128.119.245.12	10.59.193.228	HTTP	544	HTTP/1.1 200 OK (text/html)

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

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**"

```
Status Code: 401
[Status Code Description: Unauthorized]
Response Phrase: Unauthorized
```

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

Ans: It included "**Authorization: Basic"** field.

```
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
```

2. 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.

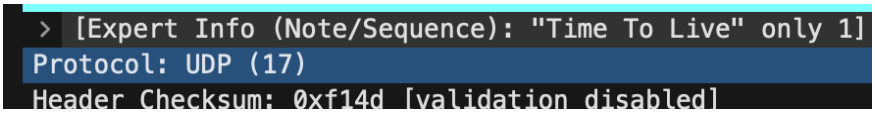
```
No.     Time           Source                Destination           Protocol Length Info
     15 4.430033       10.59.193.228         128.119.245.12        UDP      70     34499 →
33435 Len=28
Frame 15: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0
Ethernet II, Src: Apple_ee:13:09 (bc:d0:74:ee:13:09), Dst: Cisco_6a:af:79 (84:80:2d:6a:af:79)
Internet Protocol Version 4, Src: 10.59.193.228, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x86c4 (34500)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0xf14d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.59.193.228
    Destination Address: 128.119.245.12
User Datagram Protocol, Src Port: 34499, Dst Port: 33435
    Source Port: 34499
    Destination Port: 33435
    Length: 36
    Checksum: 0xb4a3 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 6]
    [Timestamps]
    UDP payload (28 bytes)
Data (28 bytes)
0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0010  00 00 00 00 00 00 00 00 00 00 00 00               ............
```

1. What is the IP address of your computer?

Ans: IP address: **10.59.193.228**

2. Within the IP packet header, what is the value in the upper layer protocol field?

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



3. How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*? Explain how you determined the number of payload bytes.

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**

```
    .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSC
  Total Length: 56
```

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

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

```
000. .... = Flags: 0x0
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
```

5. Which fields in the IP datagram *always* change from one datagram to the next within this series of ICMP messages sent by your computer?

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

6. Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?

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

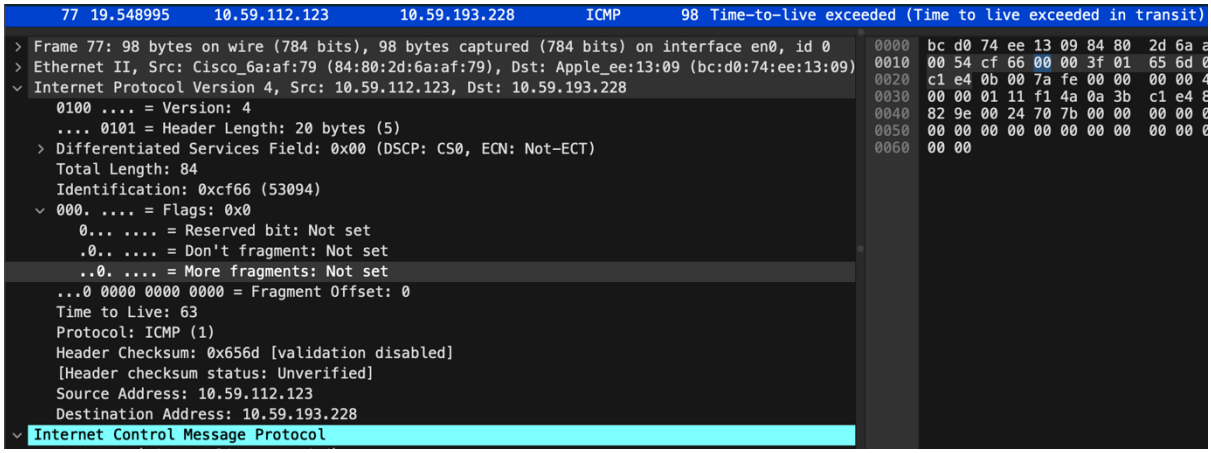
The fields that must stay constant are: **Version, header length, differentiated services, destination IP, source IP, upper layer protocol.**

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.

7. Describe the pattern you see in the values in the Identification field of the IP datagram

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



8. What is the value in the Identification field and the TTL field?

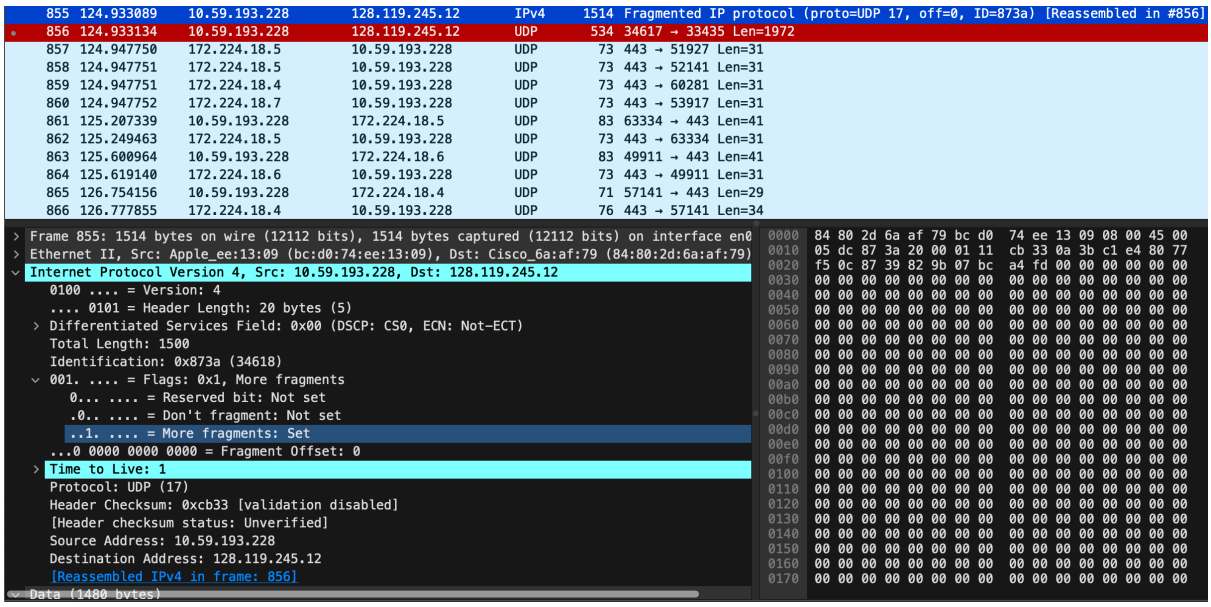
Ans: Identification: 0xcf66 (53094)

Time to live (TTL): 63

9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

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.



10. Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 2000. Has that message been fragmented across more than one IP datagram? [Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the *ip-ethereal-trace-1*packet trace. If your computer has an Ethernet interface, a packet size of 2000 *should* cause fragmentation.[3]]

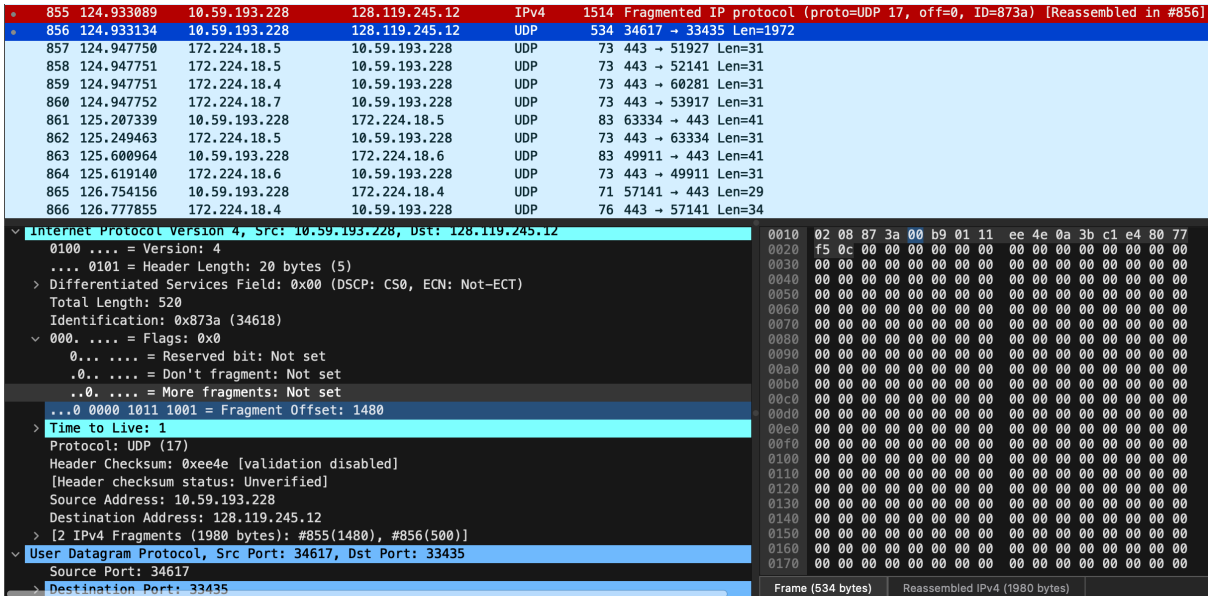
Ans: Yes, this packet has been fragmented across more than one datagram.

11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP 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.



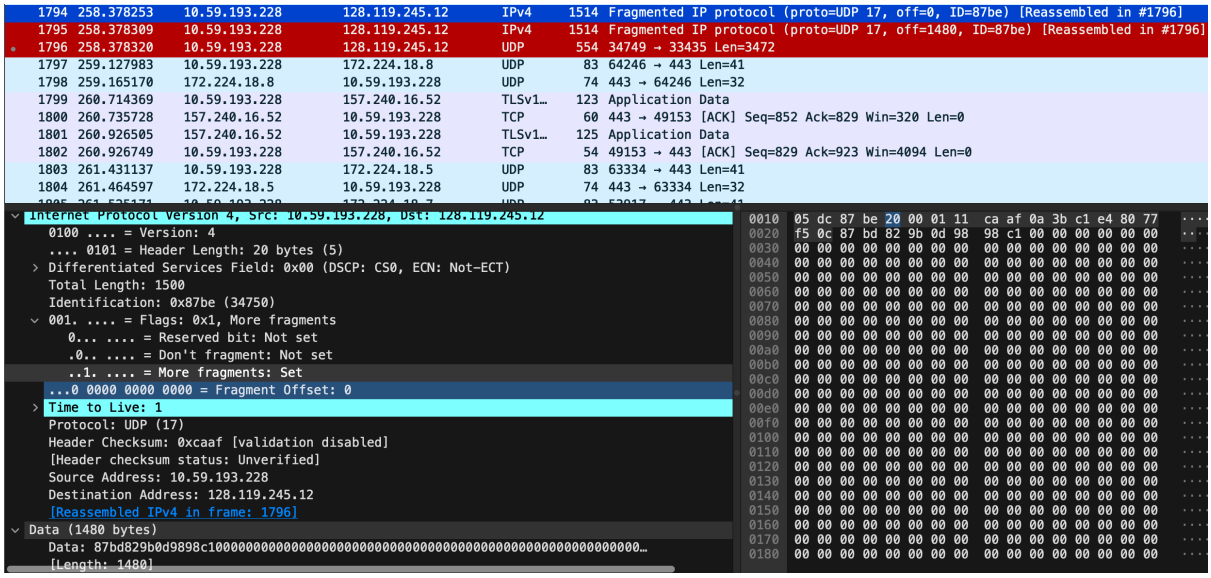
12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

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**.

13. What fields change in the IP header between the first and second fragment?

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



14. How many fragments were created from the original datagram?

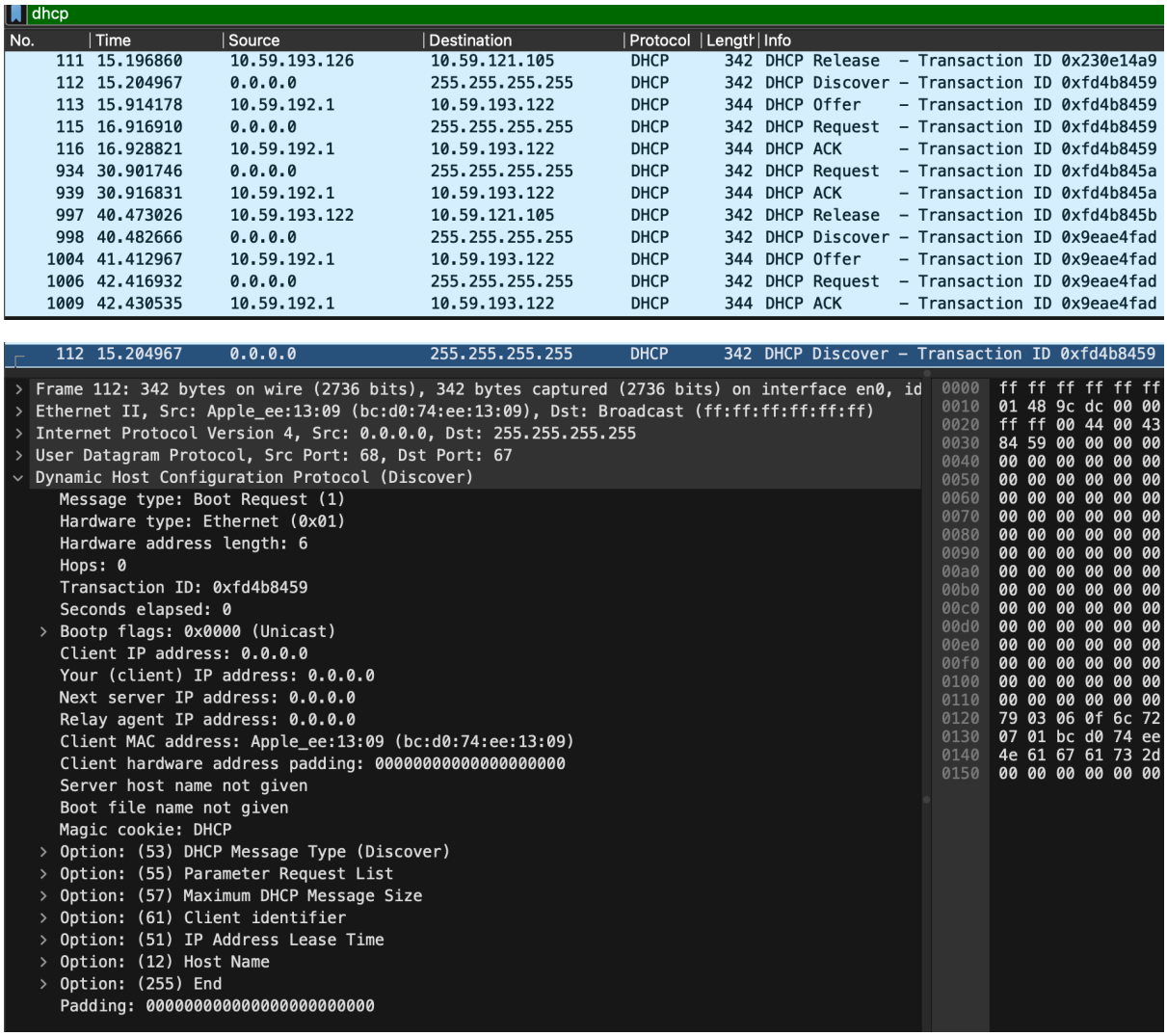
Ans: **Three fragments** are created from the original datagram after switching to 3500.

15. What fields change in the IP header among the fragments?

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.

3. Wireshark_DHCP_v7.0 lab sheet



dhcp

No.	Time	Source	Destination	Protocol	Length	Info
111	15.196860	10.59.193.126	10.59.121.105	DHCP	342	DHCP Release - Transaction ID 0x230e14a9
112	15.204967	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xfd4b8459
113	15.914178	10.59.192.1	10.59.193.122	DHCP	344	DHCP Offer - Transaction ID 0xfd4b8459
115	16.916910	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xfd4b8459
116	16.928821	10.59.192.1	10.59.193.122	DHCP	344	DHCP ACK - Transaction ID 0xfd4b8459
934	30.901746	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xfd4b845a
939	30.916831	10.59.192.1	10.59.193.122	DHCP	344	DHCP ACK - Transaction ID 0xfd4b845a
997	40.473026	10.59.193.122	10.59.121.105	DHCP	342	DHCP Release - Transaction ID 0xfd4b845b
998	40.482666	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x9eae4fad
1004	41.412967	10.59.192.1	10.59.193.122	DHCP	344	DHCP Offer - Transaction ID 0x9eae4fad
1006	42.416932	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x9eae4fad
1009	42.430535	10.59.192.1	10.59.193.122	DHCP	344	DHCP ACK - Transaction ID 0x9eae4fad

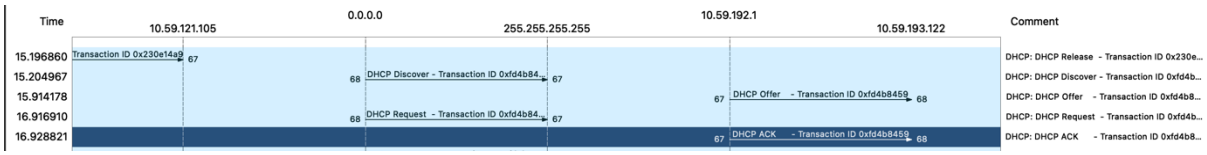

```
  112 15.204967    0.0.0.0          255.255.255.255  DHCP     342 DHCP Discover - Transaction ID 0xfd4b8459

> Frame 112: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id
> Ethernet II, Src: Apple_ee:13:09 (bc:d0:74:ee:13:09), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xfd4b8459
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Apple_ee:13:09 (bc:d0:74:ee:13:09)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (55) Parameter Request List
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (51) IP Address Lease Time
  > Option: (12) Host Name
  > Option: (255) End
    Padding: 000000000000000000000000

0000  ff ff ff ff ff ff
0010  01 48 9c dc 00 00
0020  ff ff 00 44 00 43
0030  84 59 00 00 00 00
0040  00 00 00 00 00 00
0050  00 00 00 00 00 00
0060  00 00 00 00 00 00
0070  00 00 00 00 00 00
0080  00 00 00 00 00 00
0090  00 00 00 00 00 00
00a0  00 00 00 00 00 00
00b0  00 00 00 00 00 00
00c0  00 00 00 00 00 00
00d0  00 00 00 00 00 00
00e0  00 00 00 00 00 00
00f0  00 00 00 00 00 00
0100  00 00 00 00 00 00
0110  00 00 00 00 00 00
0120  79 03 06 0f 6c 72
0130  07 01 bc d0 74 ee
0140  4e 61 67 61 73 2d
0150  00 00 00 00 00 00
```

1. Are DHCP messages sent over UDP or TCP?

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

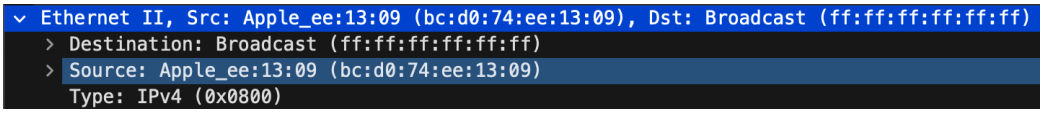
2. Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?

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



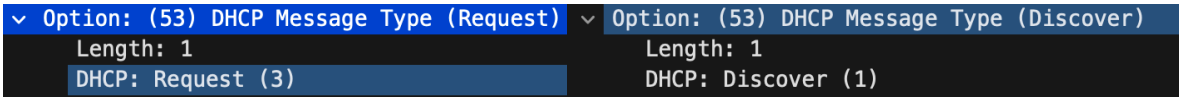
3. What is the link-layer (e.g., Ethernet) address of your host?

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



4. What values in the DHCP discover message differentiate this message from the DHCP request message?

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



5. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?

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.

6. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

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

```
112 15.204967    0.0.0.0          255.255.255.255    DHCP     342 DHCP Discover - Transaction ID 0xfd4b8459
113 15.914178    10.59.192.1      10.59.193.122      DHCP     344 DHCP Offer    - Transaction ID 0xfd4b8459
115 16.916910    0.0.0.0          255.255.255.255    DHCP     342 DHCP Request  - Transaction ID 0xfd4b8459
116 16.928821    10.59.192.1      10.59.193.122      DHCP     344 DHCP ACK      - Transaction ID 0xfd4b8459
```

7. What is the IP address of your DHCP server?

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

8. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.

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

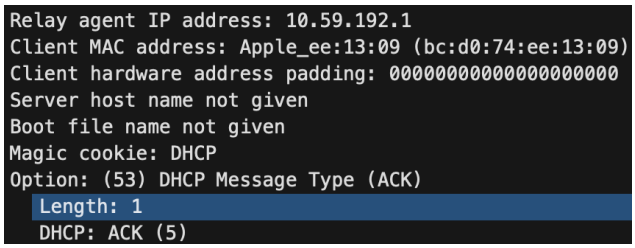
DHCP offer message offered DHCP address.

```
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 10.59.193.122
Next server IP address: 10.59.121.105
Relay agent IP address: 10.59.192.1
Client MAC address: Apple_ee:13:09 (bc:d0:74:ee:13:09)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Offer)
   Length: 1
   DHCP: Offer (2)
```

9. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?

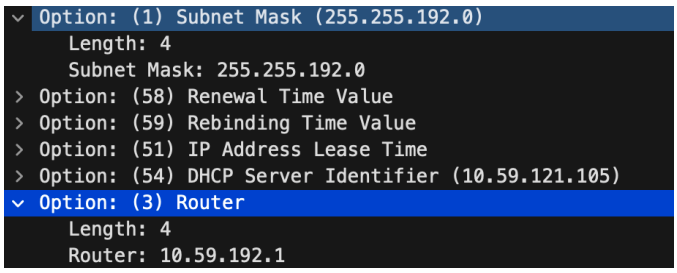
Ans: In the screenshot the relay agent IP address is: 0.0.0.0 this indicates there is no DHCP relay used.

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



10. Explain the purpose of the router and subnet mask lines in the DHCP offer message.

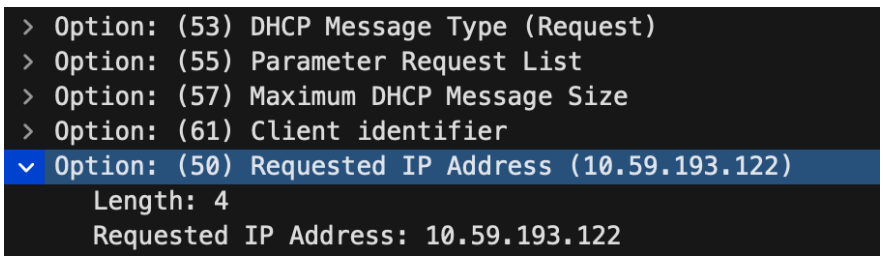
Ans: The subnet mask line tells the client which subnet mask to use. The router line indicates the client what its default gateway should be.



11. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?

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

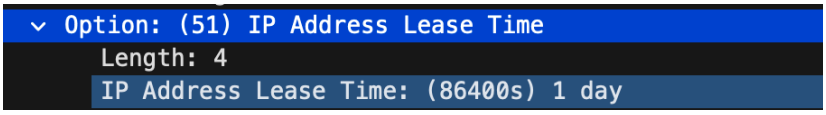
Client's response in **option 50 of the request message**.



12. Explain the purpose of the lease time. How long is the lease time in your experiment?

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.**



13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?

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.

14. Clear the *bootp* filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.

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.