

IoT and Edge Computing Assignment

Submitted By: Vignesh [AM.SC.P2MCA23039]

Amrita School of Computing, Amrita University, Amritapuri

Handled By: Jinesh Sir

15/02/2024

Networking Part

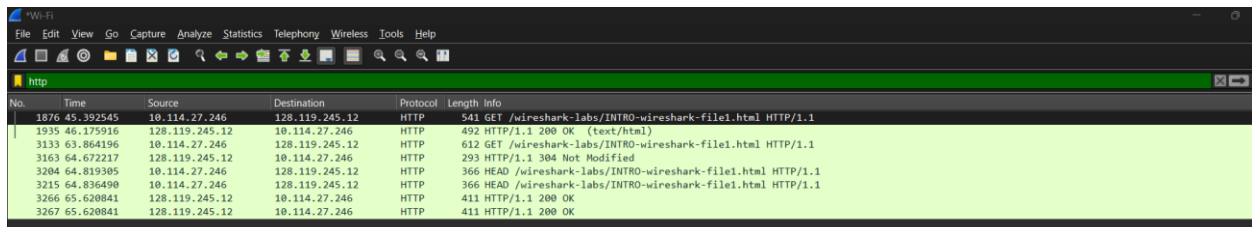
Assignments related to Intro, TCP, UDP, IP through Wireshark.

Introduction Part-1

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

Solution: TCP, UDP, HTTP, DNS, ARP, IMAP, TLSV1.2, (Any 3 possible protocols will be accepted.)

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.



The screenshot shows the Wireshark interface with a packet capture of an HTTP GET request and its corresponding OK response. The packet list pane is visible, showing the following details:

No.	Time	Source	Destination	Protocol	Length	Info
1876	45.392545	10.114.27.246	128.119.245.12	HTTP	541	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
1935	46.175916	128.119.245.12	10.114.27.246	HTTP	492	HTTP/1.1 200 OK (text/html)
3133	63.864196	10.114.27.246	128.119.245.12	HTTP	612	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
3163	64.672237	128.119.245.12	10.114.27.246	HTTP	293	HTTP/1.1 304 Not Modified
3204	64.819385	10.114.27.246	128.119.245.12	HTTP	366	HEAD /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
3215	64.836490	10.114.27.246	128.119.245.12	HTTP	366	HEAD /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
3266	65.620841	128.119.245.12	10.114.27.246	HTTP	411	HTTP/1.1 200 OK
3267	65.620841	128.119.245.12	10.114.27.246	HTTP	411	HTTP/1.1 200 OK

According to the screenshot, the time interval between the HTTP GET message and HTTP OK message is $46.175916s - 45.392545s = 0.783371s$

3. What is the Internet address of gaia.cs.umass.edu? What is the Internet address of your computer?

Solution: gaia.cs.umass.edu: 128.119.245.12

My computer: xxx.xxx.xxx.xxx

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK.

Solution: The screenshot of HTTP GET and OK message:

No.	Time	Source	Destination	Protocol	Length	Info
1876	45.392545	10.114.27.246	128.119.245.12	HTTP	541	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
1935	46.175916	128.119.245.12	10.114.27.246	HTTP	492	HTTP/1.1 200 OK (text/html)
3133	63.864196	10.114.27.246	128.119.245.12	HTTP	612	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
3163	64.672217	128.119.245.12	10.114.27.246	HTTP	293	HTTP/1.1 304 Not Modified
3204	64.819305	10.114.27.246	128.119.245.12	HTTP	366	HEAD /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
3215	64.836498	10.114.27.246	128.119.245.12	HTTP	366	HEAD /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
3266	65.620841	128.119.245.12	10.114.27.246	HTTP	411	HTTP/1.1 200 OK
3267	65.620841	128.119.245.12	10.114.27.246	HTTP	411	HTTP/1.1 200 OK

▼ Frame 1876: 541 bytes on wire (4328 bits), 541 bytes captured (4328 bits) on interface \Device\NPF_{97120B9C-EDE0-4236-A5B3-B8483800ED9A}, id 0

Section number: 1

- Interface id: 0 (\Device\NPF_{97120B9C-EDE0-4236-A5B3-B8483800ED9A})
- Encapsulation type: Ethernet (1)
- Arrival Time: Feb 15, 2024 14:51:27.458976000 India Standard Time
- UTC Arrival Time: Feb 15, 2024 09:21:27.458976000 UTC
- Epoch Arrival Time: 1707988887.458976000
- [Time shift for this packet: 0.000000000 seconds]
- [Time delta from previous captured frame: 0.003485000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 45.392545000 seconds]
- Frame Number: 1876
- Frame Length: 541 bytes (4328 bits)
- Capture Length: 541 bytes (4328 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:tcp:http]
- [Coloring Rule Name: HTTP]
- [Coloring Rule String: http || tcp.port == 80 || http2]
- Ethernet II, Src: Intel_d5:36:80 (0c:54:15:d5:36:80), Dst: Fortinet_09:00:1a (00:09:0f:09:00:1a)
- Internet Protocol Version 4, Src: 10.114.27.246, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 50755, Dst Port: 80, Seq: 1, Ack: 1, Len: 487
- ▼ Hypertext Transfer Protocol
 - GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
 - Request Method: GET
 - Request URI: /wireshark-labs/INTRO-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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0\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-US,en;q=0.9\r\n
 - \r\n
 - [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
 - [HTTP request 1/1]

TCP Part-II

1. What is the IP address of the client (the initiator of this TCP connection), and what is the server's IP address? From which port the client initiates the connection, and what is the port number used for this connection on the server side?

► Frame 1876: 541 bytes on wire (4328 bits), 541 bytes captured (4328 bits) on interface \Device\NPF_{97120B9C-EDE0-4236-A5B3-B8483800ED9A}, id 0

► Ethernet II, Src: Intel_d5:36:80 (0c:54:15:d5:36:80), Dst: Fortinet_09:00:1a (00:09:0f:09:00:1a)

► Internet Protocol Version 4, Src: 10.114.27.246, Dst: 128.119.245.12

► Transmission Control Protocol, Src Port: 50755, Dst Port: 80, Seq: 1, Ack: 1, Len: 487

▼ Hypertext Transfer Protocol

- GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
 - Request Method: GET
 - Request URI: /wireshark-labs/INTRO-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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0\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-US,en;q=0.9\r\n
 - \r\n
 - [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
 - [HTTP request 1/1]

Client:

IP address: 10.114.27.246

Port: 50755

```

▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.114.27.246
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50755, Seq: 1, Ack: 488, Len: 438
▼ Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  ▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Date: Thu, 15 Feb 2024 09:21:16 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 15 Feb 2024 06:59:02 GMT\r\n
    ETag: "51-61166299576e0"\r\n
    Accept-Ranges: bytes\r\n
  ▶ Content-Length: 81\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.783371000 seconds]
  [Request in frame: 1876]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
  File Data: 81 bytes
▶ Line-based text data: text/html (3 lines)

```

Server:

IP address: 128.119.245.12

Port: 80

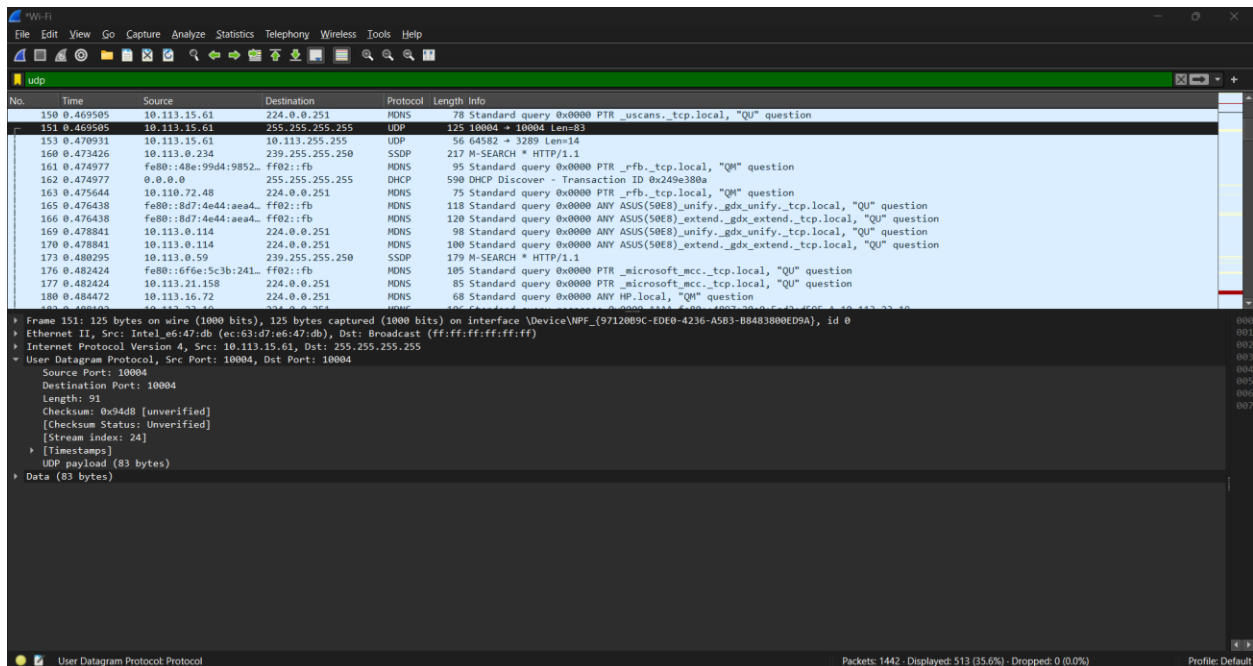
UDP Part-III

1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

Solution:

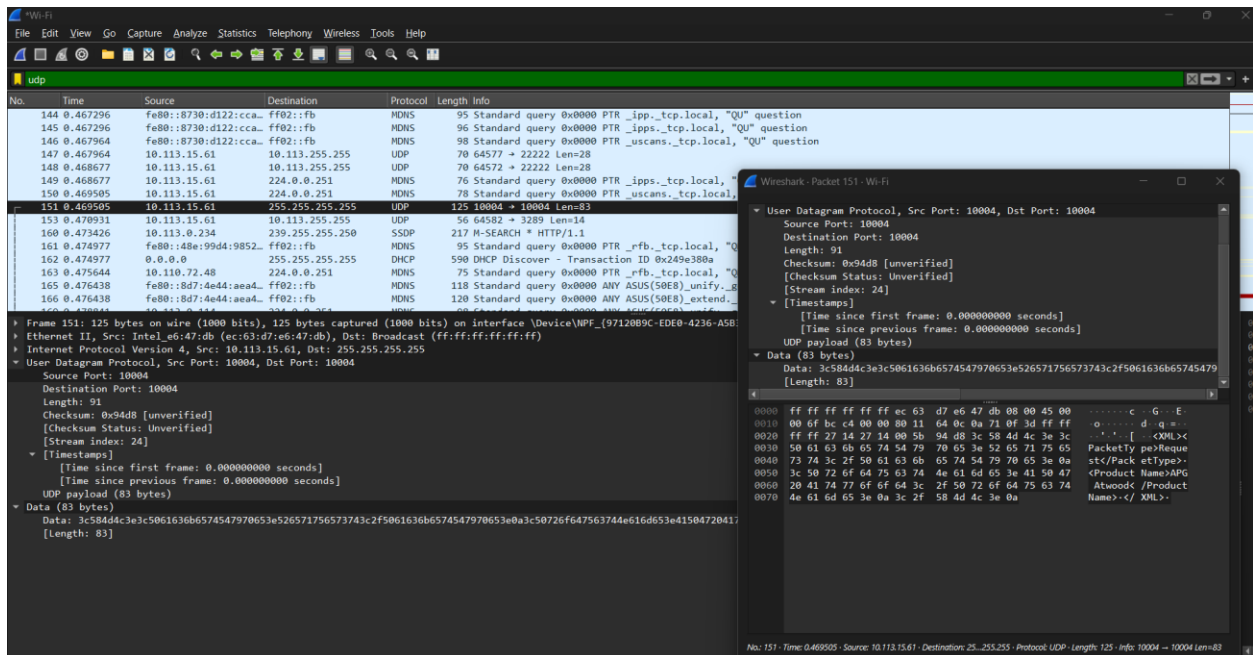
UDP header contains 4 fields:

1. source port;
2. destination port;
3. length;
4. checksum



2. 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.

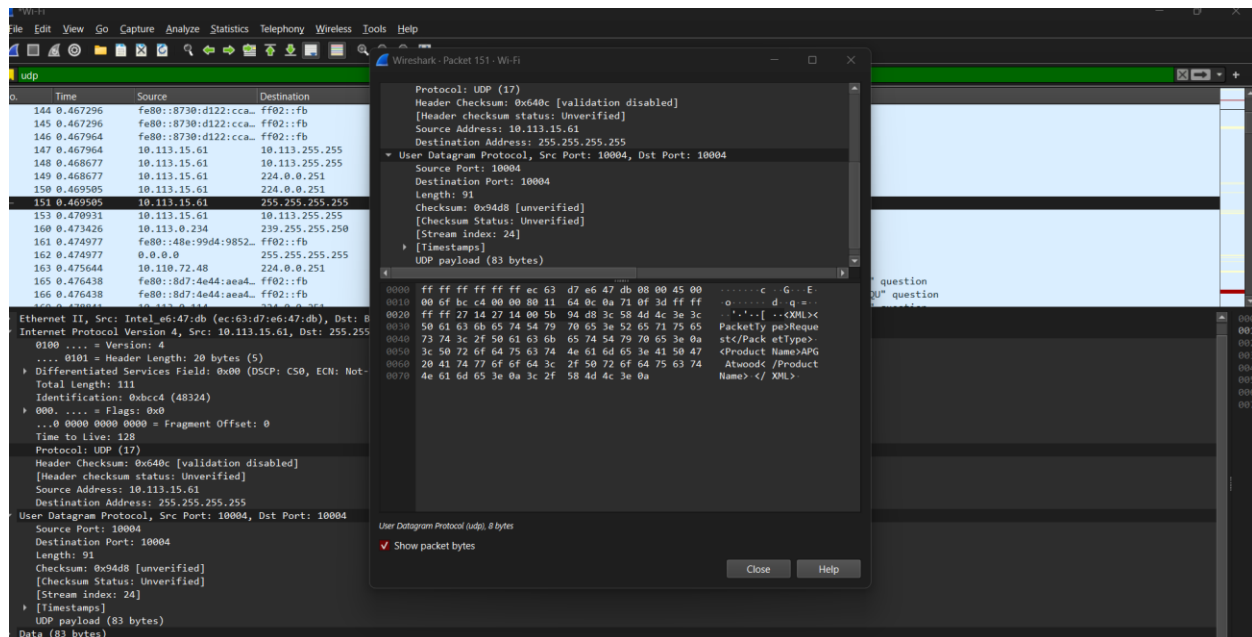
Solution: The UDP header has a fixed length of 8 bytes. Each of these 4 header fields is 2 bytes long



3. The value in the Length field is the length of what? (You can consult the text for this answer). What is the length of UDP payload for your selected packet.

Solution: The length field specifies the number of bytes in the UDP segment (header plus data). An explicit length value is needed since the size of the data field may differ from one UDP segment to the next.

The length of UDP payload for selected packet is 83 bytes. 91 bytes - 8 bytes = 83 bytes.



4. What is the maximum number of bytes that can be included in a UDP payload?

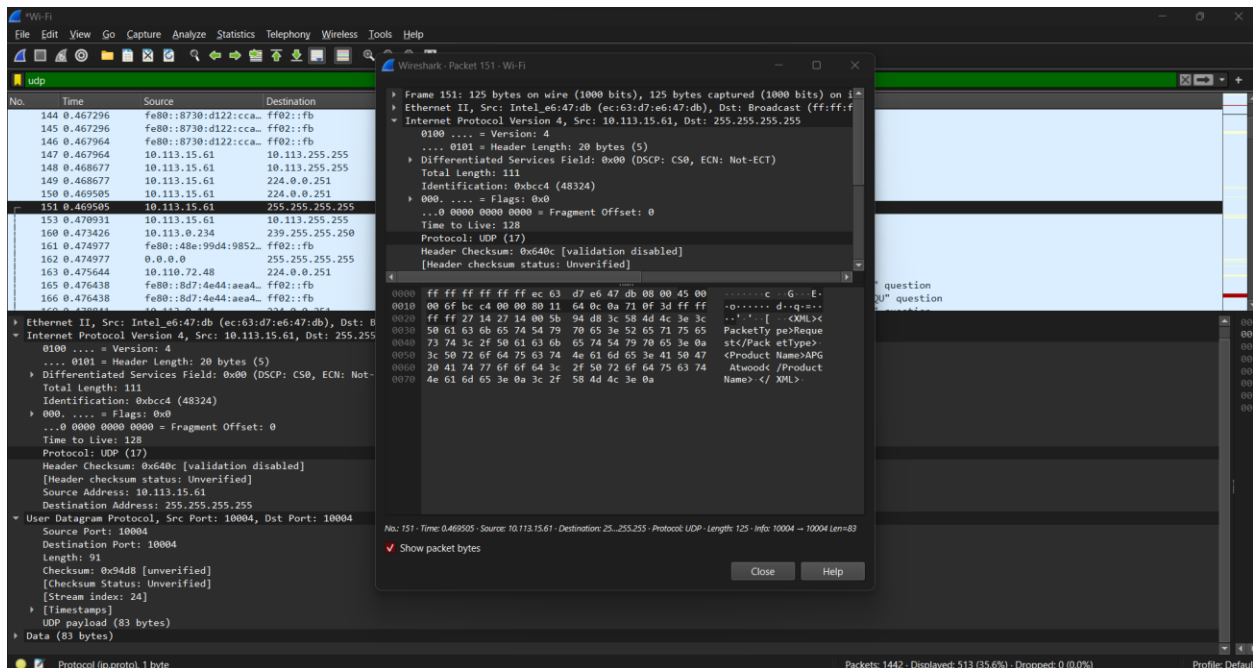
Solution: The maximum number of bytes that can be included in a UDP payload is $(2^{16} - 1)$ bytes plus the header bytes. This gives 65535 bytes - 8 bytes = 65527 bytes.

5. What is the largest possible source port number?

Solution: The largest possible source port number is $(2^{16} - 1) = 65535$.

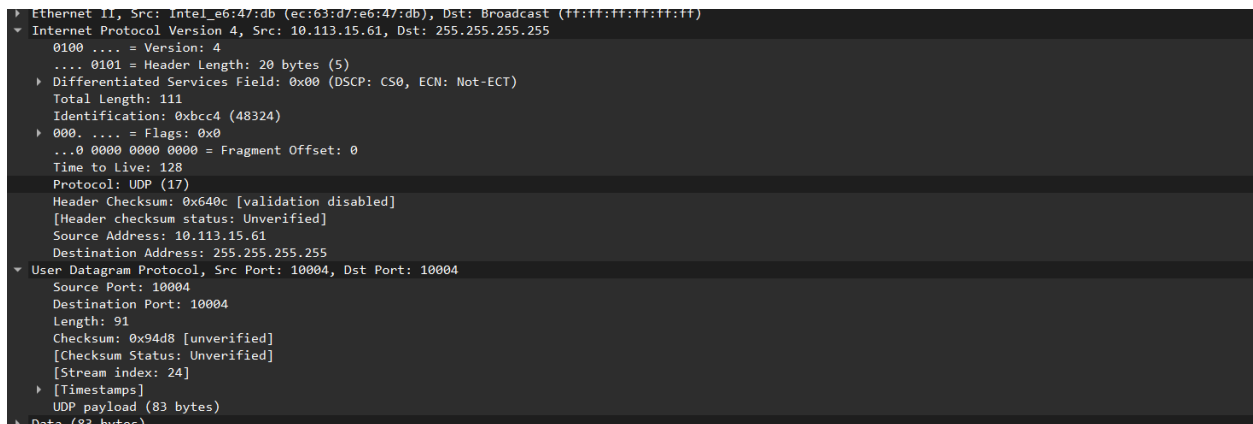
6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. (To answer this question, you'll need to look into the IP header.)

Solution: The IP protocol number for UDP is 0x11 hex, which is 17 in decimal value.



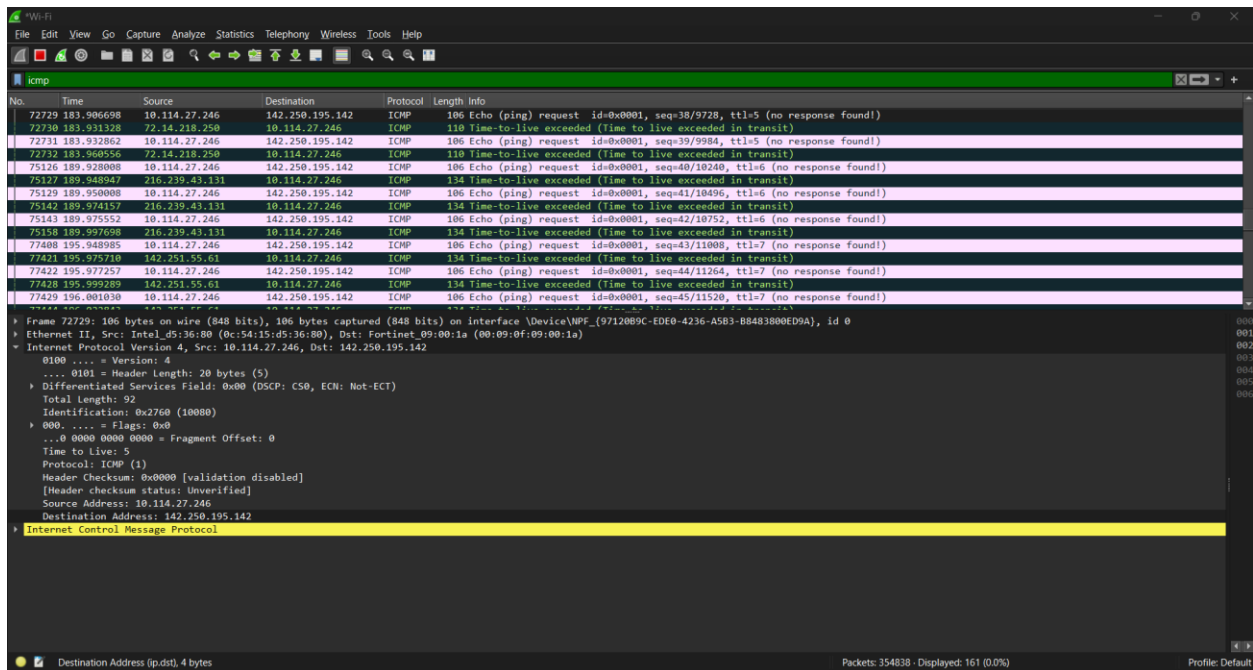
7. Examine a pair of UDP packets in which the first packet is sent by your host and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets.

Solution: The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and conversely the destination port of the UDP packet sent by the host is the same as the source port of the reply packet.



IP Part-IV

1. Select the first ICMP Echo Request message sent by your computer, expand the Internet Protocol part of the packet in the packet details window, and print this.



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

Solution: ICMP (1)

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.

Solution:

Header bytes: 20 (as seen in screenshot)

Payload bytes: 72 (total length 92 minus the 20 header bytes = 72)

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

Solution:

From the previous screenshot, we do not see any IPv4 fragments. We will see these later when we transmit longer ICMP echo requests.

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?

Solution:

Identification field is incrementing.

Time to live is also incrementing

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

Solution:

The following fields remain constant:

- version (IPv4 always used)
- header length (doesn't change since we are always using IPv4)
- source IP (my computer's IP address doesn't change)
- destination IP (usc.edu's IP address doesn't change)
- differentiated services (same protocol every time)
- upper layer protocol (same protocol every time)
- header checksum (verification disabled in my tests)

The following fields change:

- Identification field is incrementing (each IP datagram has a different ID)
- Time to live is also incrementing (this is how trace route works, as discussed in the assignment)

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

Solution: They are incrementing with each datagram

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

Solution:

My nearest hop router was 10.114.27.246.

From the screenshot below, we see that

- 120-bytes pings: Identification = 43860 and TTL = 255

No.	Time	Source	Destination	Protocol	Length	Info
27418	68.964075	10.114.0.1	10.114.27.246	ICMP	94	Destination unreachable (Host unreachable)
27495	69.153667	10.114.0.1	10.114.27.246	ICMP	94	Destination unreachable (Host unreachable)
29895	73.163579	10.114.0.1	10.114.27.246	ICMP	94	Destination unreachable (Host unreachable)
38528	76.943802	10.114.0.1	10.114.27.246	ICMP	94	Destination unreachable (Host unreachable)
31958	80.244852	10.114.0.1	10.114.27.246	ICMP	94	Destination unreachable (Host unreachable)
36490	91.499872	10.114.27.246	216.58.200.142	ICMP	106	Echo (ping) request id=0x0001, seq=1/256, ttl=1 (no response found!)
36434	91.515340	10.114.0.1	10.114.27.246	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
36435	91.516914	10.114.27.246	216.58.200.142	ICMP	106	Echo (ping) request id=0x0001, seq=2/512, ttl=1 (no response found!)
36436	91.517952	10.114.0.1	10.114.27.246	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
36437	91.519051	10.114.27.246	216.58.200.142	ICMP	106	Echo (ping) request id=0x0001, seq=3/768, ttl=1 (no response found!)
36438	91.520078	10.114.0.1	10.114.27.246	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
38649	97.488444	10.114.27.246	216.58.200.142	ICMP	106	Echo (ping) request id=0x0001, seq=4/1024, ttl=2 (no response found!)
38650	97.493851	117.193.77.225	10.114.27.246	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
38651	97.495453	10.114.27.246	216.58.200.142	ICMP	106	Echo (ping) request id=0x0001, seq=5/1280, ttl=2 (no response found!)
38652	97.499275	117.193.77.225	10.114.27.246	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Layer	Length	Info
Frame 36438: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{97120B9C-EDE0-4236-ASB3-BB483800ED9A}, id 0		
Ethernet II, Src: Fortinet_09:00:1a (00:09:0f:09:00:1a), Dst: Intel_d5:36:80 (0c:54:15:d5:36:80)		
Internet Protocol Version 4, Src: 10.114.0.1, Dst: 10.114.27.246		
0100 = Version: 4		
.... 0101 = Header Length: 20 bytes (5)		
... Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)		
Total Length: 120		
Identification: 0xab54 (43860)		
0000 = Flags: 0x0		
...0 0000 0000 0000 = Fragment Offset: 0		
Time to Live: 255		
Protocol: ICMP (1)		
Header Checksum: 0xde95 [validation disabled]		
[Header checksum status: Unverified]		
Source Address: 10.114.0.1		
Destination Address: 10.114.27.246		
Internet Control Message Protocol		

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?

Solution: In my test, these fields did not change.