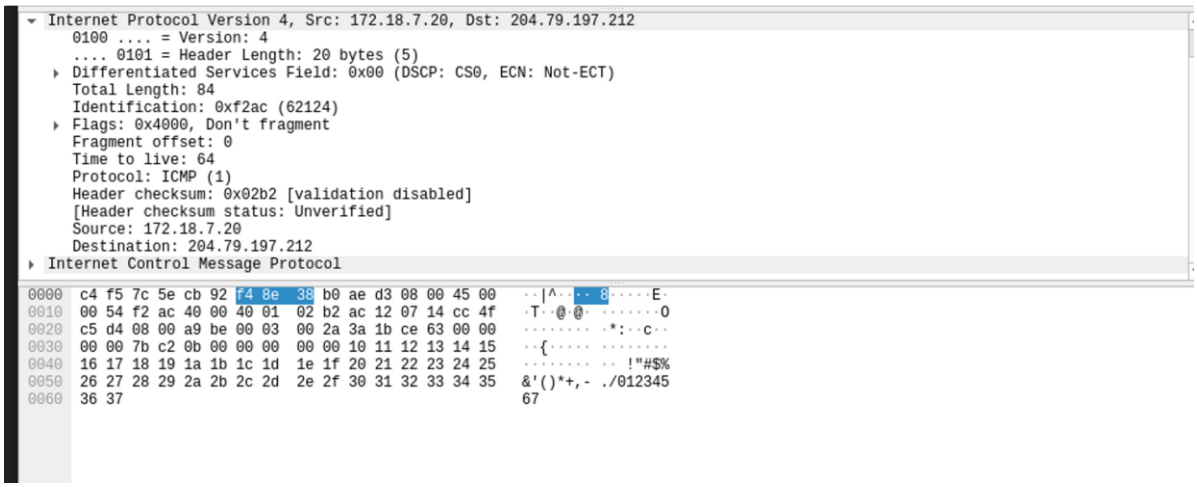
os lab 2(security)
TANMAY MITTAL
2020UCP1795

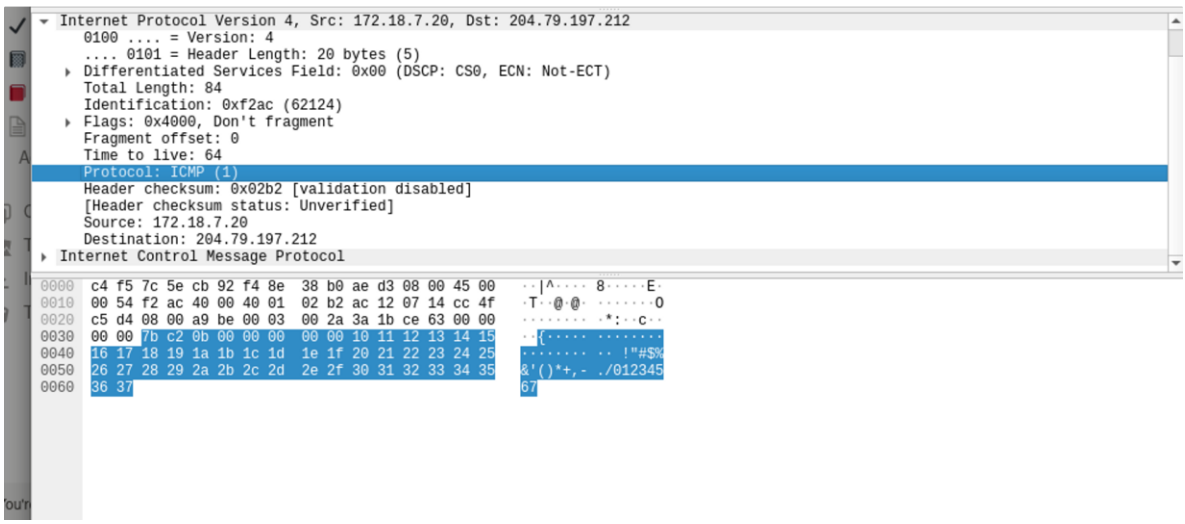
(a) Select the first ICMP Echo Request message sent by your computer, and expand the Internet
Protocol part of the packet in the packet details window. What is the IP address of your
computer?

ans: IP address is 172.18.7.20



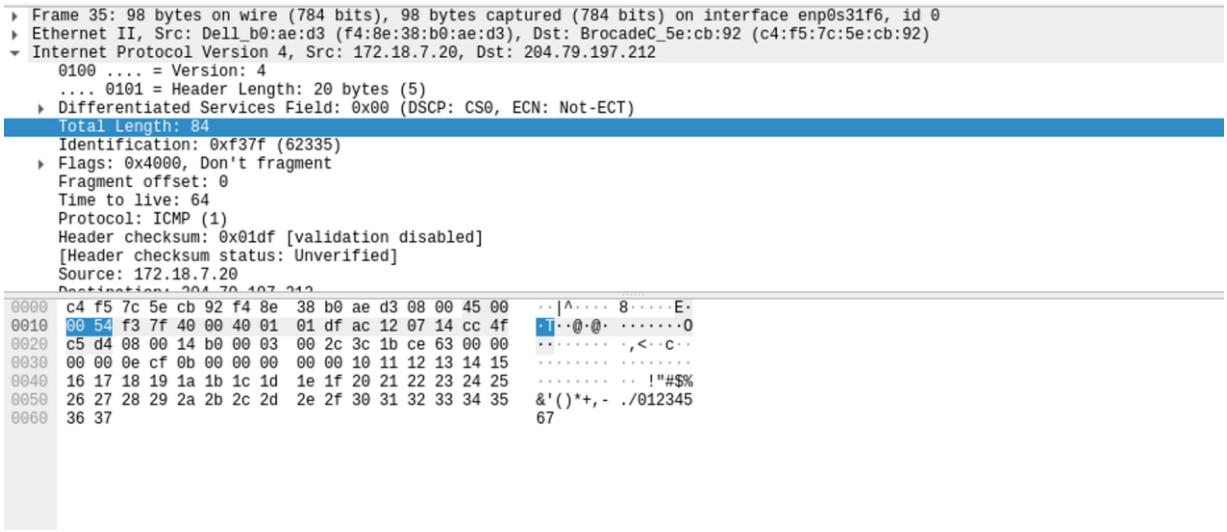
(b) Within the IP packet header, what is the value in the upper layer protocol field?

soln:



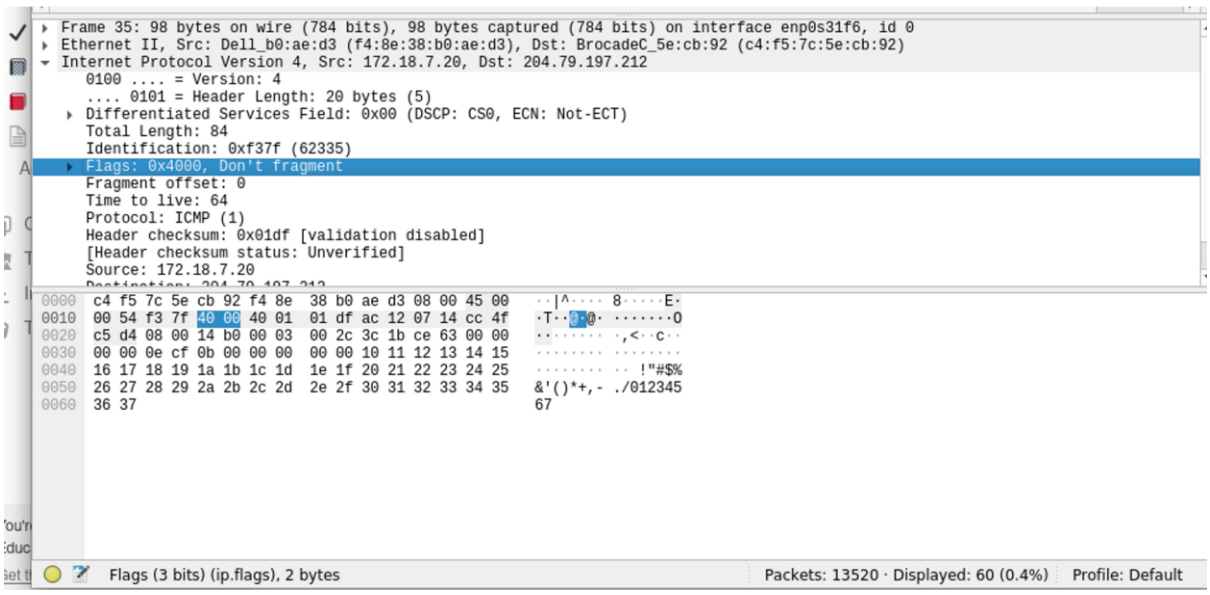
(c) How many bytes are in the IP header? How many bytes are in the payload of the IP datagram?
Explain how you determined the number of payload bytes.

soln:



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

soln:



(e) Which fields in the IP datagram always change from one datagram to the next within this series
of ICMP messages sent by your computer?

soln: identification, time to live and checksum are change

(f) Which fields stay constant? Which of the fields must stay constant? Which fields must change?
Why?

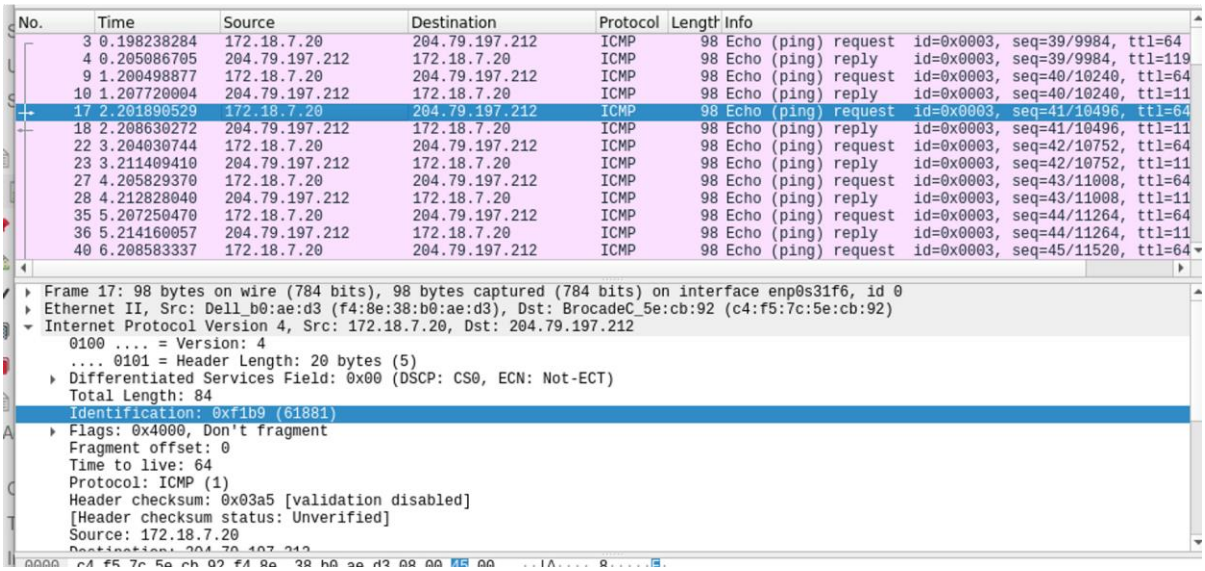
soln:

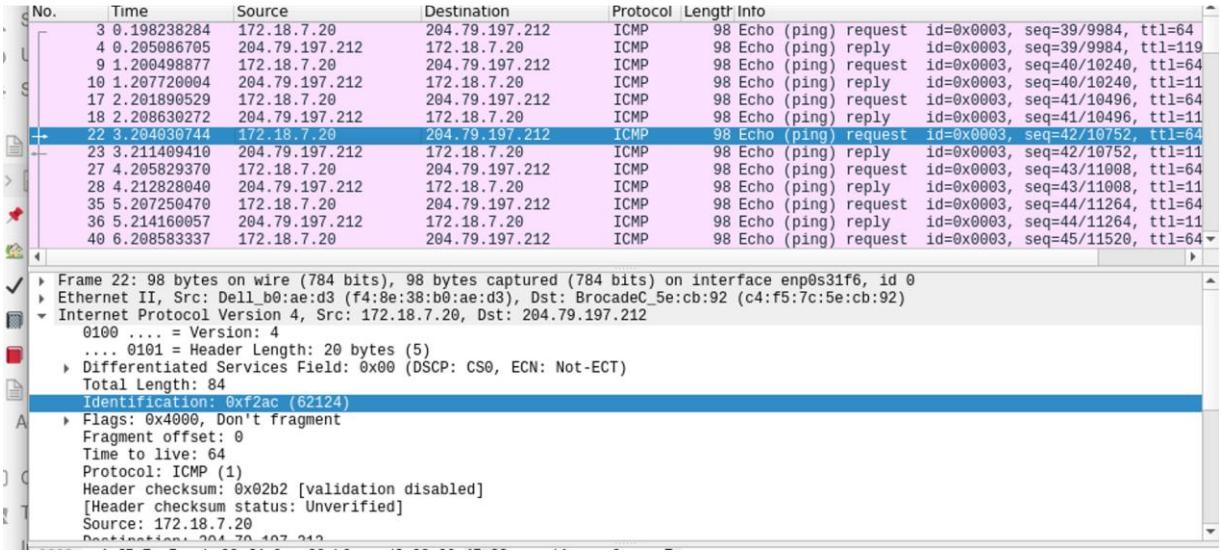
field that are constant are source IP(sending req from same source), destination IP(recieving reply from destination), upper layer protocol(until we change our protocol)

field that must change are

(g) Describe the pattern you see in the values in the Identification field of the IP datagram

soln:





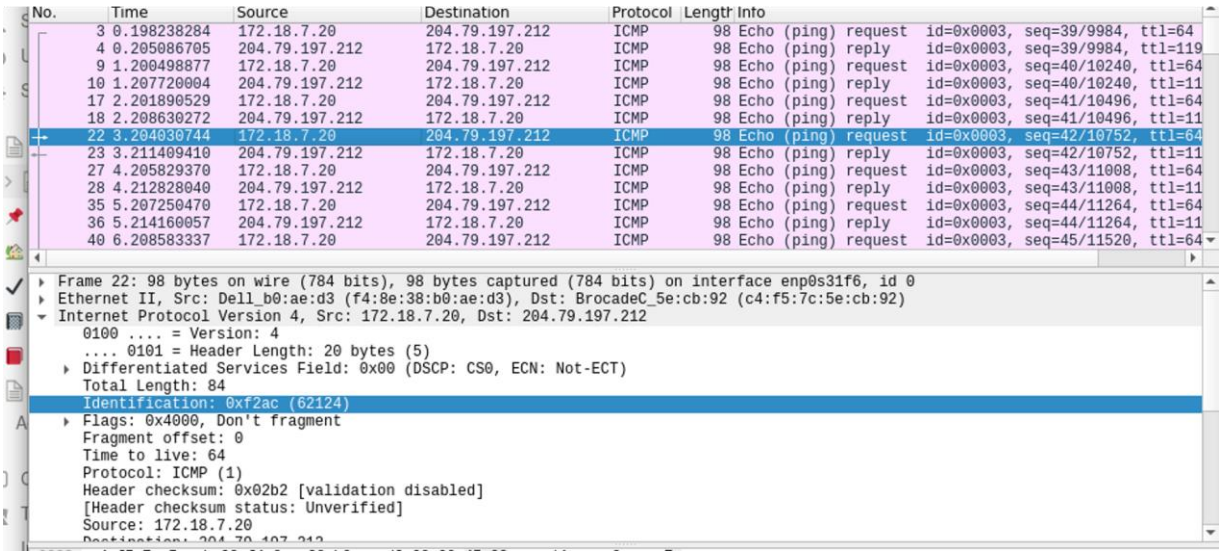
No.	Time	Source	Destination	Protocol	Length	Info
3	0.198238284	172.18.7.20	204.79.197.212	ICMP	98	Echo (ping) request id=0x0003, seq=39/9984, ttl=64
4	0.205086705	204.79.197.212	172.18.7.20	ICMP	98	Echo (ping) reply id=0x0003, seq=39/9984, ttl=119
9	1.200498877	172.18.7.20	204.79.197.212	ICMP	98	Echo (ping) request id=0x0003, seq=40/10240, ttl=64
10	1.207720004	204.79.197.212	172.18.7.20	ICMP	98	Echo (ping) reply id=0x0003, seq=40/10240, ttl=11
17	2.201890529	172.18.7.20	204.79.197.212	ICMP	98	Echo (ping) request id=0x0003, seq=41/10496, ttl=64
18	2.208630272	204.79.197.212	172.18.7.20	ICMP	98	Echo (ping) reply id=0x0003, seq=41/10496, ttl=11
22	3.204030744	172.18.7.20	204.79.197.212	ICMP	98	Echo (ping) request id=0x0003, seq=42/10752, ttl=64
23	3.211409410	204.79.197.212	172.18.7.20	ICMP	98	Echo (ping) reply id=0x0003, seq=42/10752, ttl=11
27	4.205829370	172.18.7.20	204.79.197.212	ICMP	98	Echo (ping) request id=0x0003, seq=43/11008, ttl=64
28	4.212828040	204.79.197.212	172.18.7.20	ICMP	98	Echo (ping) reply id=0x0003, seq=43/11008, ttl=11
35	5.207250470	172.18.7.20	204.79.197.212	ICMP	98	Echo (ping) request id=0x0003, seq=44/11264, ttl=64
36	5.214160057	204.79.197.212	172.18.7.20	ICMP	98	Echo (ping) reply id=0x0003, seq=44/11264, ttl=11
40	6.208583337	172.18.7.20	204.79.197.212	ICMP	98	Echo (ping) request id=0x0003, seq=45/11520, ttl=64

```
Frame 22: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s31f6, id 0
Ethernet II, Src: Dell_b0:ae:d3 (f4:8e:38:b0:ae:d3), Dst: BrocadeC_5e:cb:92 (c4:f5:7c:5e:cb:92)
Internet Protocol Version 4, Src: 172.18.7.20, Dst: 204.79.197.212
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xf2ac (62124)
  Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x02b2 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.18.7.20
```

(h) What is the value in the Identification field and the TTL field?

soln:

identification:- 62124 and TTL(time to live) 64.



No.	Time	Source	Destination	Protocol	Length	Info
3	0.198238284	172.18.7.20	204.79.197.212	ICMP	98	Echo (ping) request id=0x0003, seq=39/9984, ttl=64
4	0.205086705	204.79.197.212	172.18.7.20	ICMP	98	Echo (ping) reply id=0x0003, seq=39/9984, ttl=119
9	1.200498877	172.18.7.20	204.79.197.212	ICMP	98	Echo (ping) request id=0x0003, seq=40/10240, ttl=64
10	1.207720004	204.79.197.212	172.18.7.20	ICMP	98	Echo (ping) reply id=0x0003, seq=40/10240, ttl=11
17	2.201890529	172.18.7.20	204.79.197.212	ICMP	98	Echo (ping) request id=0x0003, seq=41/10496, ttl=64
18	2.208630272	204.79.197.212	172.18.7.20	ICMP	98	Echo (ping) reply id=0x0003, seq=41/10496, ttl=11
22	3.204030744	172.18.7.20	204.79.197.212	ICMP	98	Echo (ping) request id=0x0003, seq=42/10752, ttl=64
23	3.211409410	204.79.197.212	172.18.7.20	ICMP	98	Echo (ping) reply id=0x0003, seq=42/10752, ttl=11
27	4.205829370	172.18.7.20	204.79.197.212	ICMP	98	Echo (ping) request id=0x0003, seq=43/11008, ttl=64
28	4.212828040	204.79.197.212	172.18.7.20	ICMP	98	Echo (ping) reply id=0x0003, seq=43/11008, ttl=11
35	5.207250470	172.18.7.20	204.79.197.212	ICMP	98	Echo (ping) request id=0x0003, seq=44/11264, ttl=64
36	5.214160057	204.79.197.212	172.18.7.20	ICMP	98	Echo (ping) reply id=0x0003, seq=44/11264, ttl=11
40	6.208583337	172.18.7.20	204.79.197.212	ICMP	98	Echo (ping) request id=0x0003, seq=45/11520, ttl=64

```
Frame 22: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s31f6, id 0
Ethernet II, Src: Dell_b0:ae:d3 (f4:8e:38:b0:ae:d3), Dst: BrocadeC_5e:cb:92 (c4:f5:7c:5e:cb:92)
Internet Protocol Version 4, Src: 172.18.7.20, Dst: 204.79.197.212
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xf2ac (62124)
  Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x02b2 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.18.7.20
```

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

soln:

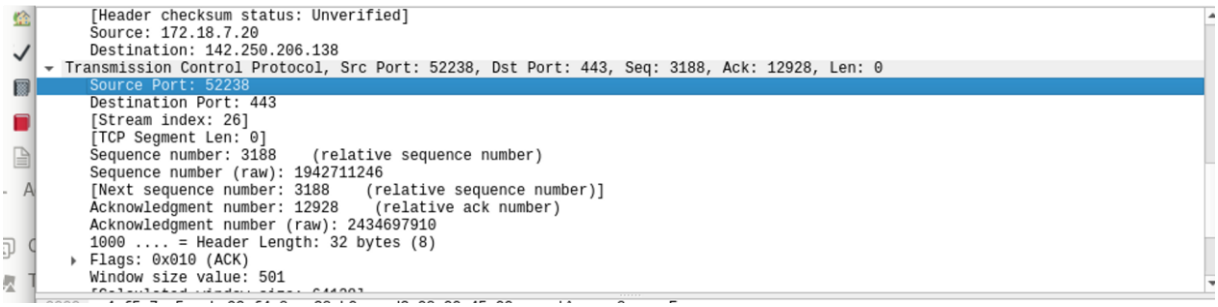
the TTL field remains unchanged because the TTL for the first router is always the same.

(j) What is the IP address and TCP port number used by your client computer (source) to transfer the file ?

soln:

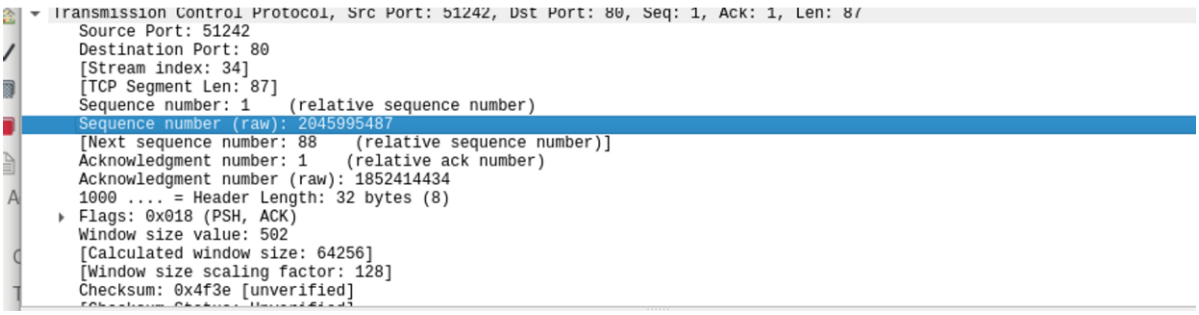
ip address : 172.18.7.20

tcp port no. : 52238



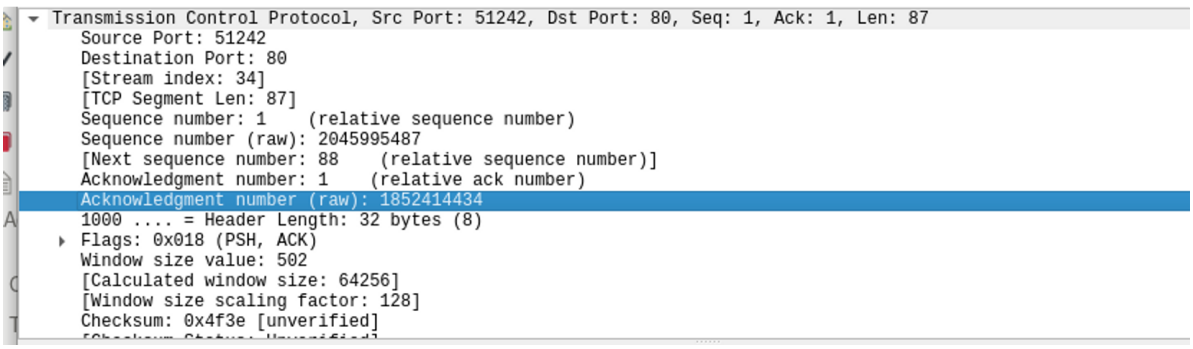
(k) What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection
between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the
segment as a SYN segment?

soln:



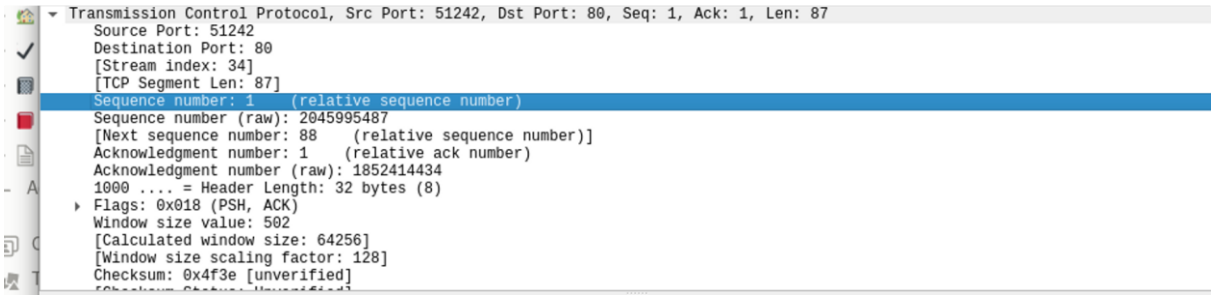
(l) What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client
computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK
segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that
identifies the segment as a SYNACK segment?

sol: the syn acknoledgement sent by cs.mass.edu to the client is 1.

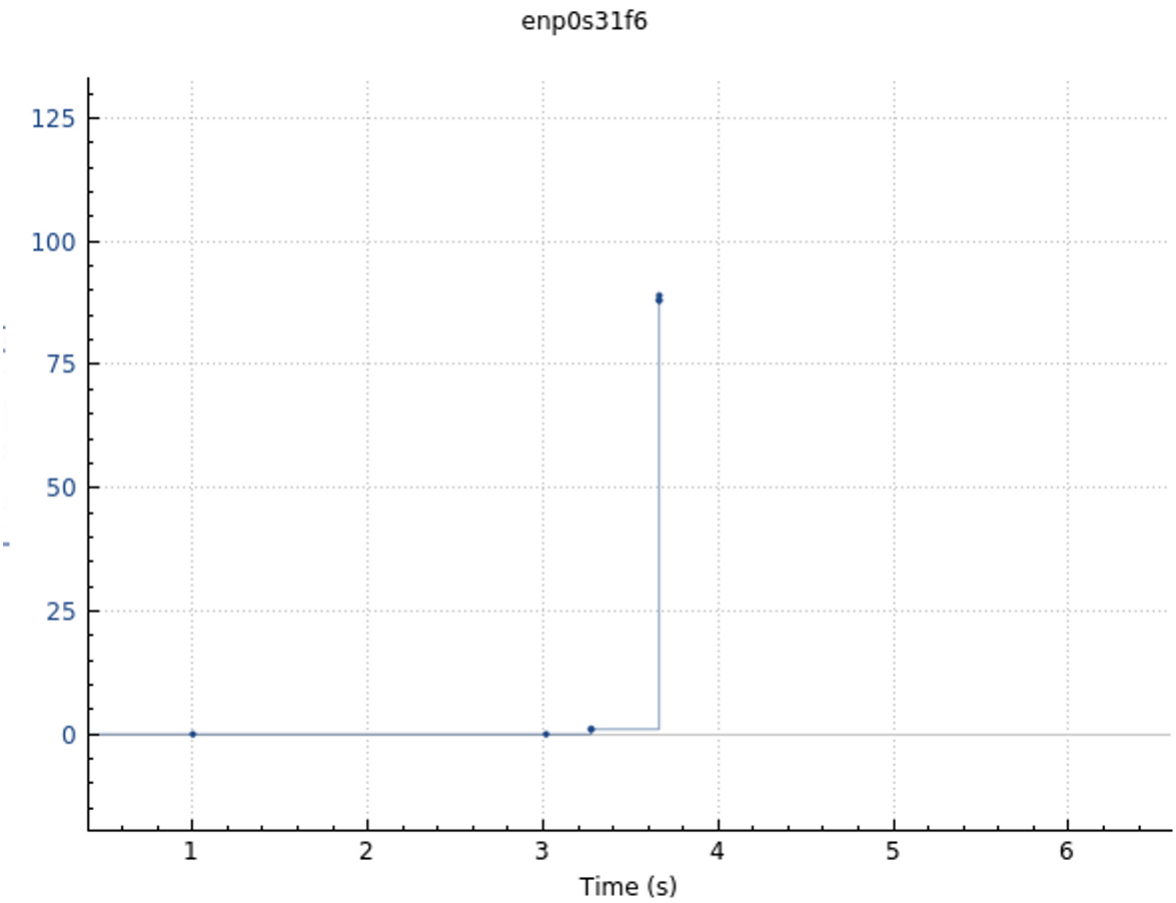


(m) What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the
bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

soln :



(n) Consider the TCP segment containing the HTTP POST as the first segment in the TCP
connection. What are the sequence numbers of the first six segments in the TCP connection
(including the segment containing the HTTP POST)? At what time was each segment sent?
When was the ACK for each segment received? Given the difference between when each TCP
segment was sent, and when its acknowledgement was received, what is the RTT value for each
of the six segments? What is the EstimatedRTT value



soln:

(o) What is the length of each of the first six TCP segments?

soln: 148, 87, 104, 147, 92

(p) What is the minimum amount of available buffer space advertised at the received for the entire
trace? Does the lack of receiver buffer space ever throttle the sender?

soln: it's calculated window size is (5840). lack of buffer space means the packet is recieved as it is.

(q) Are there any retransmitted segments in the trace file? What did you check for (in the trace) in
order to answer this question?

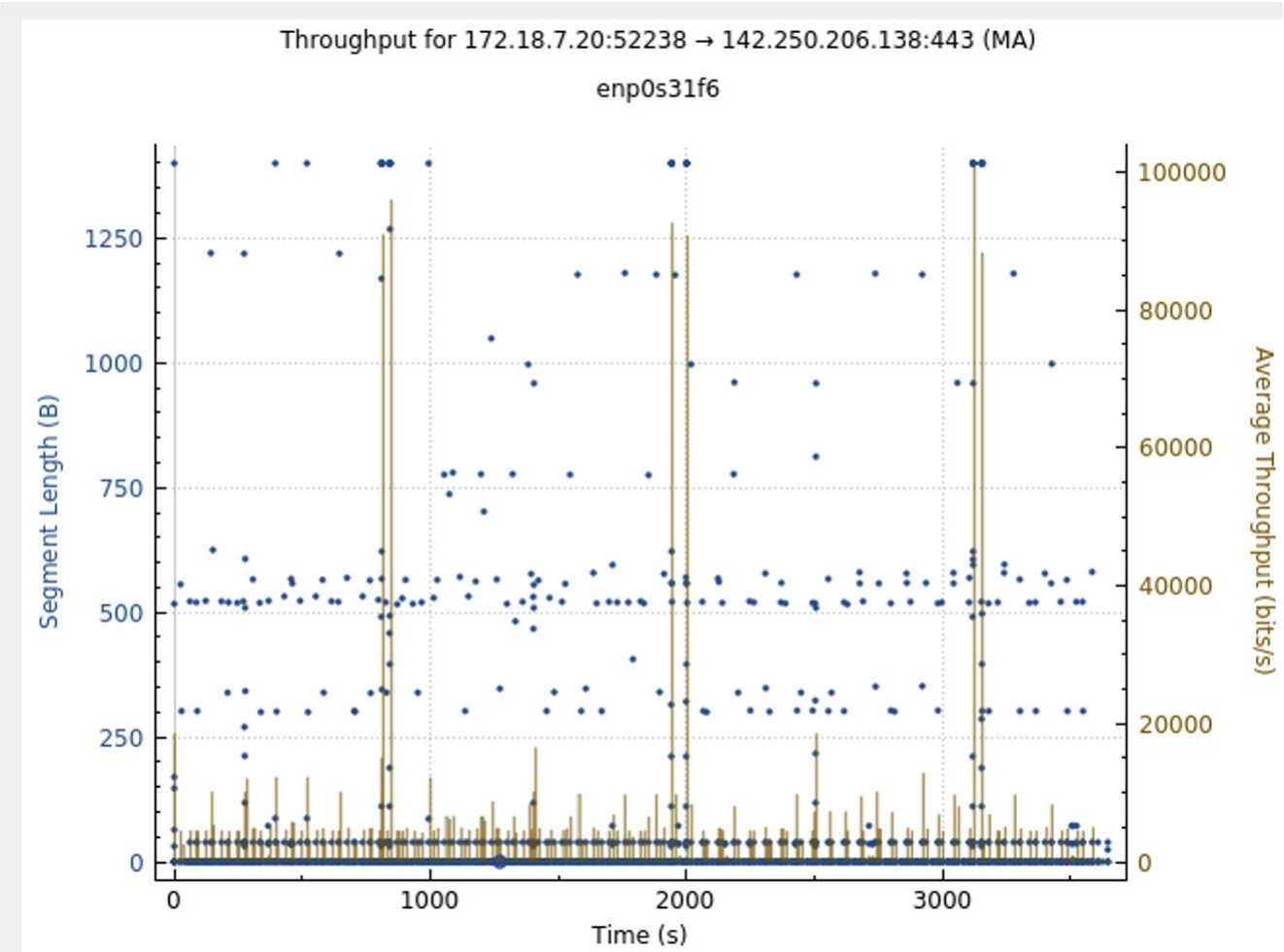
soln: there are none, to check re-transmission , we would check for repeating segment numbers.

(r) How much data does the receiver typically acknowledge in an ACK? Can you identify cases
where the receiver is ACKing every other received segment (see Table 3.2 on page 250 in the
text).

soln: 1500 bytes on average are getting acknowledge in an TCP-ACk packet.

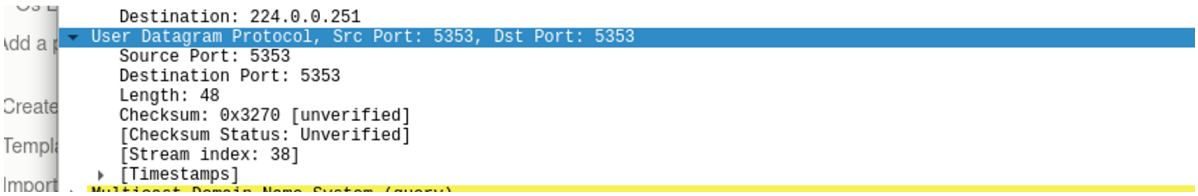
(s) What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how
you calculated this value.

soln: statistics → tcp stream graph → throughput



(t) 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.

soln:



(u) 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.

soln: 8 bytes each headr files is a byte long.

(v) The value in the Length field is the length of what? (You can consult the text for this answer).
Verify your claim with your captured UDP packet.

soln: length of field specified is no. of the udp segment (header+data).

(w) What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer
to this question can be determined by your answer to 2. above)

soln: 65535 -8= 65527 bytes

(x) What is the largest possible source port number? (Hint: see the hint in 4.)

soln: 65535

(y) 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 Protocol field of the IP datagram
containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).

soln:

LAB-2

1. select first ICMP Echo request. what is the IP addr of your computer

According to result. The IP addr of my PC is 210.212.97.174

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

According to result, within IP packet header the value in upper layer protocol field is ICMP(1)

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

According to result
Header Length :20 bytes
Total length: 84.-

Payload : 84 - 20 = 64 bytes

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

∴ More fragment (MF) bit is not zero under flags section
∴ It is not fragementable

2. Which field in the IP datagram always change from one datagram to next within this series of ICMP messages

According to observation
Time to leave & header checksum always change

2. What field stay constant? which of the fields must stay constant? Which field must change? Why?

The field that stay constant:
- Version (∵ we are using IPV4)
- header length (∵ they are UDP packets)
- Source IP (since all packet are sent from my computer)
- destination IP (∵ we are sending to same host)
- Differentiated Services (∵ all packets are UDP)
- Upper layer protocol (∵ these are UDP packets)

The fields that must stay constant are:

version (∵ we are using IPV4)
header length (∵ there are UDP packets)
source IP (∵ all pkts are sent from my computer)
destination IP (∵ we are sending to same host)
Differentiated services (∵ all packets are UDP)
upper layer protocol (∵ since there are UDP packets)

The fields that must change are:

Identification (IP packets have different id's)
Time to live (traceroute increments each packet)
Header checksum (∵ header changes)

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

It is fragmented across more than one IP datagram

Q Print out first fragment of IP datagram. What information in IP header has been fragmented? How long is this IP datagram

Acc. to observation:
The flags bit more fragments is set means datagram is fragmented.
The fragment offset is 0, we know this is first fragment.
Total Length: 455

Q12 Point out second fragment of fragmented IP datagram. What information in IP header indicates that this is not first datagram fragment? Are there more fragments

Acc. to observation, this is not first fragment offset is 1480 and this should be last fragment; since status of more fragment flag is not set.

Q13 Value of Identification in TTL field?
Identification: 29033
TTL : 50

Q14 Do these values remain unchanged for all ICMP TTL-exceeded replies sent to your computer by nearest router?

The Identification field changes for all ICMP TTL-exceeded replies because Identification field is unique value. When two or more

IP datagrams have same identification value
it means are fragments of single large IP datagram.

The TTL field remains unchanged because the TTL for first hop router is always the same

Q What is IP address and TCP port number used by your client compute to gaia.cs.umass.edu
Source Port: 443
Destination Port: 43998

Q12 What is sequence no. of TCP SYN BW client computer? What is segment that identifies segment as a SYN segment

The sequence number of TCP SYN segment is 0 since it is used to initate the TCP connection BW the client computer & gaia.cs.umass.edu, According to result, in flags section syn flag is set to 1 which indicates this segment is SYN segment

Q.13 What is sequence number of SYNACK segment sent by gaia.cs.umass.edu to client computer in reply to SYN? How did gaia.cs.edu identifies segment as SYNACK segment?

Value of SYNACK segment: 0
Value of Acknowledgment field: 1
determined by gaia.cs.umass.edu

Q What is sequence no. of TCP segment containing HTTP Post command, you'll need to dig into the packet content field with it's DATA field?

Segment no. 6 contains HTTP post, sequence number of this segment is 1.

Q Consider TCP segment containing HTTP Post as first segment ... Given the difference what is estimated RTT value.

According to given figures segment 1-6 are no. 6, 7, 8, 9, 11
Acknowledments 1-6 are 10, 12, 13, 16, 19 & 22

Segment #	Sent time	ACK received time	RTT
segment 1	0.27125700	0,368d31000	0.095674
segment 2	0,27142500	0,367289000	0095864
segment 3	0,271970	0,368617000	0,09682
segment 4	0,271960	0.36 995 20000	0,098154
segment 5	0.367081	0,47996500	0,112684
segment 6	0.3687100	0.48249200	0,113781

4 what is length of each of first six TCP segments?

The length of first six tcp segments is 1337 and of following five segments is 1448 bytes.

5 What is minimum buffer advertised at the received for entire trace? Does lack of receive space ever throttle to senders?

Minimum buffer: 5792 bytes
Grows till it reaches: 62780 bytes.

6 Are there any retransmitted segments in trace file? what do you check to answer?

No retransmitted segments: time sequence graph (tcptrace)

7 How much data receiver acknowledge in ACK?
Refer ex: segment No. 13 acknowledged data with 1430 bytes

8 what is throughput for TCP connection? Explain.

$$\text{Throughput} = \frac{\text{first seq. no of A}}{\text{last ACK}} = \frac{152138}{1.307471} = 116319.60 \text{ bytes/sec}$$

9 Select one UDP packet from your trace? Det no. of fields? Header contains 4 field: source port, dest^n port, length & checksum

10 By Det. length of each UDP header fields?
UDP header has fixed length of 8 bytes. Each 4 header fields is 2 bytes long

Q Det length of UDP payload
length of payload: 40 - 8 = 32 bytes

Q What is max bytes included in UDP payload?
$(2^{16}-1)$ bytes plus header = 65527 bytes

Q What is largest possible source port number?
Largest port Number = $(2^{16}-1)$ = 65535

Q What is protool number for UDP? Both in hex & dec
IP protool number for UDP 0x11 hex, which is
17 in dec value

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

The source packet of UDP sent by host is same destination port of reply packets & conversly true.