

CNS Lab on WireShark

Date: 28/08/2022

Id: 2022PIS5083

Name: SUMITRA SHARMA

Branch: M.Tech (Computer Science and Information Security)

Batch: 2022-2024

Networks Assignment:

ICMP protocol analysis prerequisites:-

```
Microsoft Windows [Version 10.0.19043.1889]
(c) Microsoft Corporation. All rights reserved.

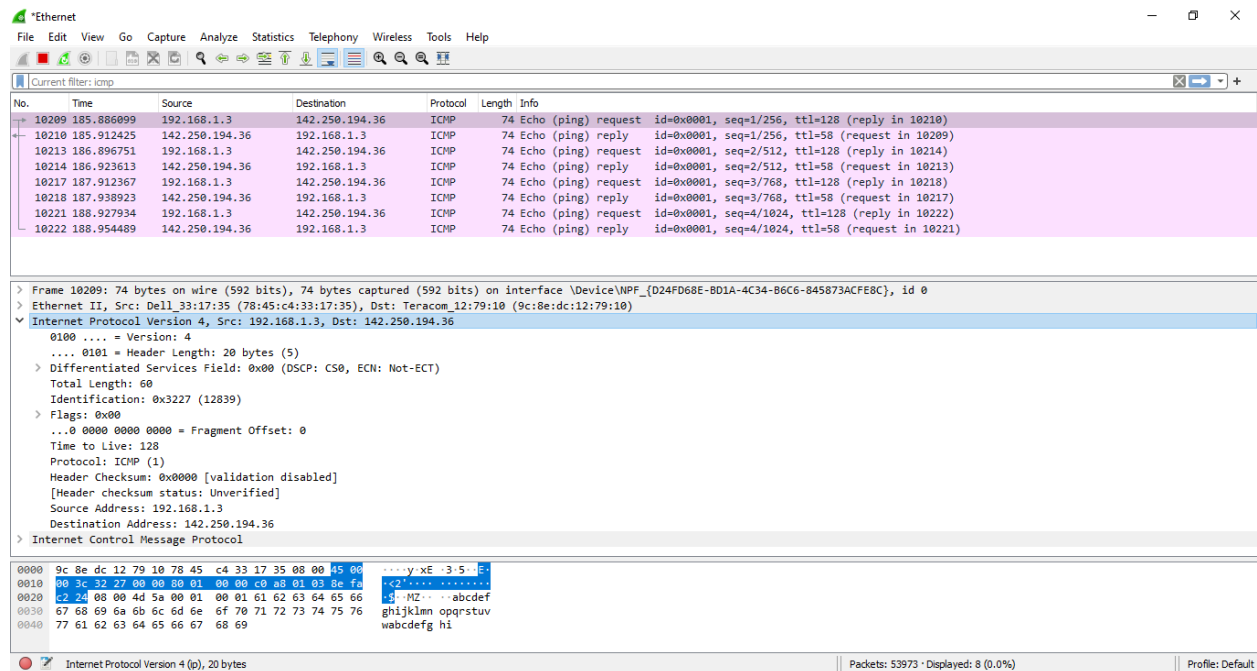
C:\Users\Cute Nose>ping www.google.com

Pinging www.google.com [142.250.194.36] with 32 bytes of data:
Reply from 142.250.194.36: bytes=32 time=26ms TTL=58
Reply from 142.250.194.36: bytes=32 time=27ms TTL=58
Reply from 142.250.194.36: bytes=32 time=26ms TTL=58
Reply from 142.250.194.36: bytes=32 time=26ms TTL=58

Ping statistics for 142.250.194.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 27ms, Average = 26ms
```

(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?

Solution: 192.168.1.3



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

Solution: ICMP (1)

Wireshark packet capture showing ICMP Echo (ping) request and reply. The packet list shows a request from 192.168.1.3 to 142.250.194.36. The packet details pane shows the Internet Protocol Version 4 header with a length of 60 bytes and the Internet Control Message Protocol (ICMP) header. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
10209	185.886099	192.168.1.3	142.250.194.36	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 10210)
10210	185.912425	142.250.194.36	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=58 (request in 10209)
10213	186.896751	192.168.1.3	142.250.194.36	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 10214)
10214	186.923613	142.250.194.36	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=58 (request in 10213)
10217	187.912367	192.168.1.3	142.250.194.36	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 10218)
10218	187.938923	142.250.194.36	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=58 (request in 10217)
10221	188.927934	192.168.1.3	142.250.194.36	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 10222)
10222	188.954489	142.250.194.36	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=58 (request in 10221)

Frame 10209: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D24FD68E-BD1A-4C34-B6C6-845873ACF8C}, id 0
Ethernet II, Src: Dell_33:17:35 (78:45:c4:33:17:35), Dst: Teracom_12:79:10 (9c:8e:dc:12:79:10)
Internet Protocol Version 4, Src: 192.168.1.3, Dst: 142.250.194.36
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0x3227 (12839)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.3
Destination Address: 142.250.194.36
Internet Control Message Protocol

0000 9c 8e dc 12 79 10 78 45 c4 33 17 35 08 00 45 00x.E.3.5..E-
0010 00 3c 32 27 00 00 00 01 00 00 c0 a8 01 03 8e fa ..<2'.....
0020 c2 24 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66 \$.MZ...abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Protocol (p.proto), 1 byte | Packets: 53235 • Displayed: 8 (0.0%) | Profile: Default

(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.

Solution: IP header length = 20 bytes (as seen in screenshot)

Payload bytes: 40 (total length 60 - the 20 header bytes = 40)

Wireshark packet capture showing ICMP Echo (ping) request and reply. The packet list shows a request from 192.168.1.3 to 142.250.194.36. The packet details pane shows the Internet Protocol Version 4 header with a length of 60 bytes and the Internet Control Message Protocol (ICMP) header. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
10209	185.886099	192.168.1.3	142.250.194.36	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 10210)
10210	185.912425	142.250.194.36	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=58 (request in 10209)
10213	186.896751	192.168.1.3	142.250.194.36	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 10214)
10214	186.923613	142.250.194.36	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=58 (request in 10213)
10217	187.912367	192.168.1.3	142.250.194.36	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 10218)
10218	187.938923	142.250.194.36	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=58 (request in 10217)
10221	188.927934	192.168.1.3	142.250.194.36	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 10222)
10222	188.954489	142.250.194.36	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=58 (request in 10221)

Frame 10209: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D24FD68E-BD1A-4C34-B6C6-845873ACF8C}, id 0
Ethernet II, Src: Dell_33:17:35 (78:45:c4:33:17:35), Dst: Teracom_12:79:10 (9c:8e:dc:12:79:10)
Internet Protocol Version 4, Src: 192.168.1.3, Dst: 142.250.194.36
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0x3227 (12839)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.3
Destination Address: 142.250.194.36
Internet Control Message Protocol

0000 9c 8e dc 12 79 10 78 45 c4 33 17 35 08 00 45 00x.E.3.5..E-
0010 00 3c 32 27 00 00 00 01 00 00 c0 a8 01 03 8e fa ..<2'.....
0020 c2 24 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66 \$.MZ...abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Header length in 32-bit words (p.hdr_len), 1 byte | Packets: 54931 • Displayed: 8 (0.0%) | Profile: Default

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

Solution: No, the IP datagram has not been fragmented. Observe the More fragments field. Notice that it is not set, indicating no more fragments will follow.

Wireshark packet capture showing an ICMP Echo (ping) request and reply. The packet list shows packet 10209 as the ICMP Echo (ping) request. The packet details pane shows the IP header and ICMP header for packet 10209. The 'More fragments' field is set to 'Not set'.

No.	Time	Source	Destination	Protocol	Length	Info
10206	185.728716	172.217.167.234	192.168.1.3	UDP	67	443 → 62001 Len=25
10207	185.802679	192.168.1.3	192.168.1.1	DNS	74	Standard query 0x0202 A www.google.com
10208	185.833147	192.168.1.1	192.168.1.3	DNS	90	Standard query response 0x0202 A www.google.com A 142.250.194.36
10209	185.886099	192.168.1.3	142.250.194.36	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 10210)
10210	185.912425	142.250.194.36	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=58 (request in 10209)
10211	186.131089	192.168.1.3	172.217.167.234	UDP	75	62001 → 443 Len=33
10212	186.166256	172.217.167.234	192.168.1.3	UDP	67	443 → 62001 Len=25

Frame 10209: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D24FD68E-BD1A-4C34-B6C6-845873ACF8C}, id 0
Ethernet II, Src: Dell_33:17:35 (78:45:c4:33:17:35), Dst: Teracom_12:79:10 (9c:8e:dc:12:79:10)
Internet Protocol Version 4, Src: 192.168.1.3, Dst: 142.250.194.36
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0x3227 (12839)
Flags: 0x00
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..0... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.3
Destination Address: 142.250.194.36
> Internet Control Message Protocol

0000 9c 8e dc 12 79 10 78 45 c4 33 17 35 08 00 45 00xE .3.5..E.
0010 00 3c 32 27 00 00 01 00 00 c0 a8 01 03 8e fa <2" ..
0020 c2 24 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66 \$.MZ.. ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

More fragments (p.flags.mf), 1 byte | Packets: 69502 • Displayed: 69502 (100.0%) | Profile: Default

(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?

Solution: Identification field.

The top screenshot shows a packet capture in Wireshark. The packet list on the left shows a selected ICMP Echo (ping) request (No. 10209). The packet details pane on the right shows the structure of the ICMP Echo request, including the Identification field (0x3227) and the Echo data (74 bytes). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

The bottom screenshot shows a packet capture in Wireshark. The packet list on the left shows a selected ICMP Echo (ping) reply (No. 10213). The packet details pane on the right shows the structure of the ICMP Echo reply, including the Identification field (0x3228) and the Echo data (74 bytes). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

(f) Which fields stay constant? 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 (www.google .com 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)
- TTL (remains same in my test) because it represents the maximum number of IP routers that the packet can go through before being discarded.

The following fields change:

- Identification field is incrementing (each IP datagram has a different ID). The identification field changes for all the ICMP TTL-exceeded replies **because the identification field is a unique value**. When two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram.

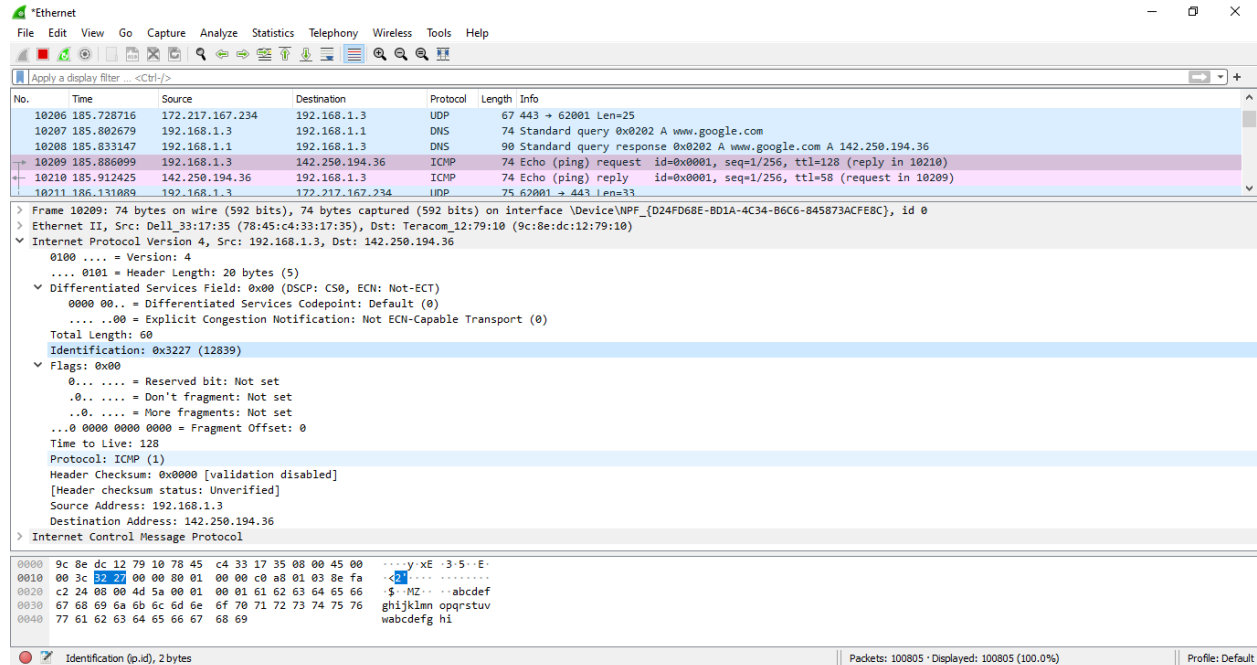
(g) Describe the pattern you see in the values in the Identification field of the IP datagram.

Solution: According to the below table. We can conclude that in the series of IP datagram ping request packets the identification field increments by 1. But in the series of IP datagram ping reply packets the identification field remains the same.

Packet no.	Request Identification field	Reply Identification field
1.	0x3227 (12839)	0x000 (0)
2.	0x3228 (12840)	0x000 (0)
3.	0x3229 (12841)	0x000 (0)
4.	0x322a (12842)	0x000 (0)

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

Solution: Identification field = 0x3227 (12839), TTL field = 128.



(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?

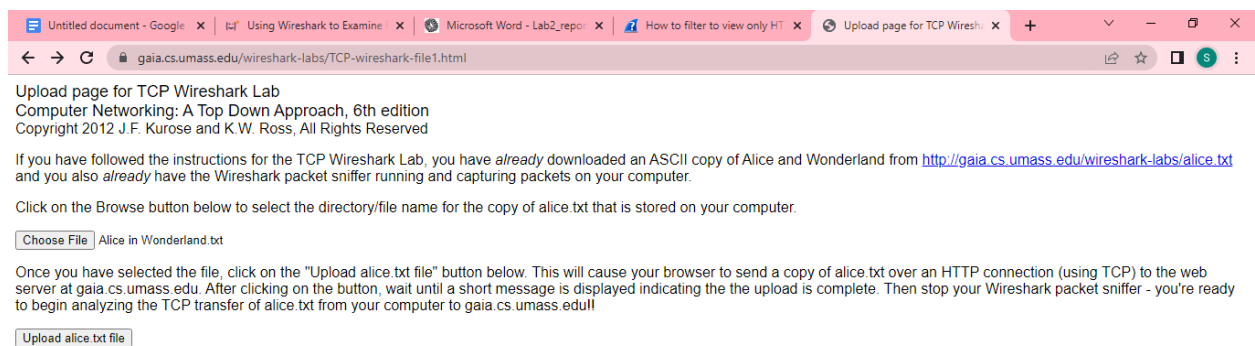
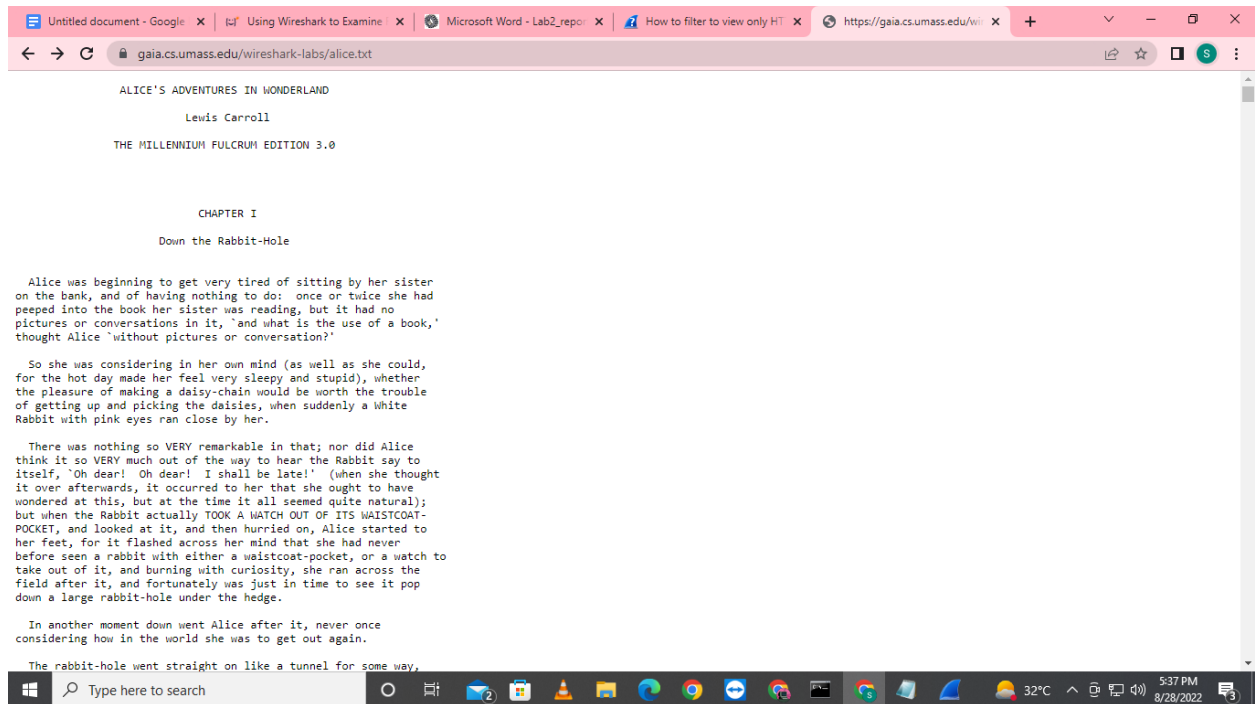
Solution: Yes, the values for Identification field and TTL remain unchanged for all of the ICMP TTL-exceeded replies sent to my computer because it represents the maximum number of IP routers that the packet can go through before being discarded.

FTP protocol analysis prerequisites:-

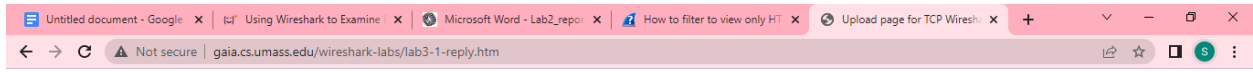
```
C:\Users\Cute Nose>ftp gaia.cs.umass.edu
Connected to gaia.cs.umass.edu.
220 (vsFTPd 3.0.2)
200 Always in UTF8 mode.
User (gaia.cs.umass.edu:(none)): _
```

TCP protocol analysis prerequisites:-

Download the below file and save as “Alice in Wonderland”.



Restart Wireshark and then after upload the file.



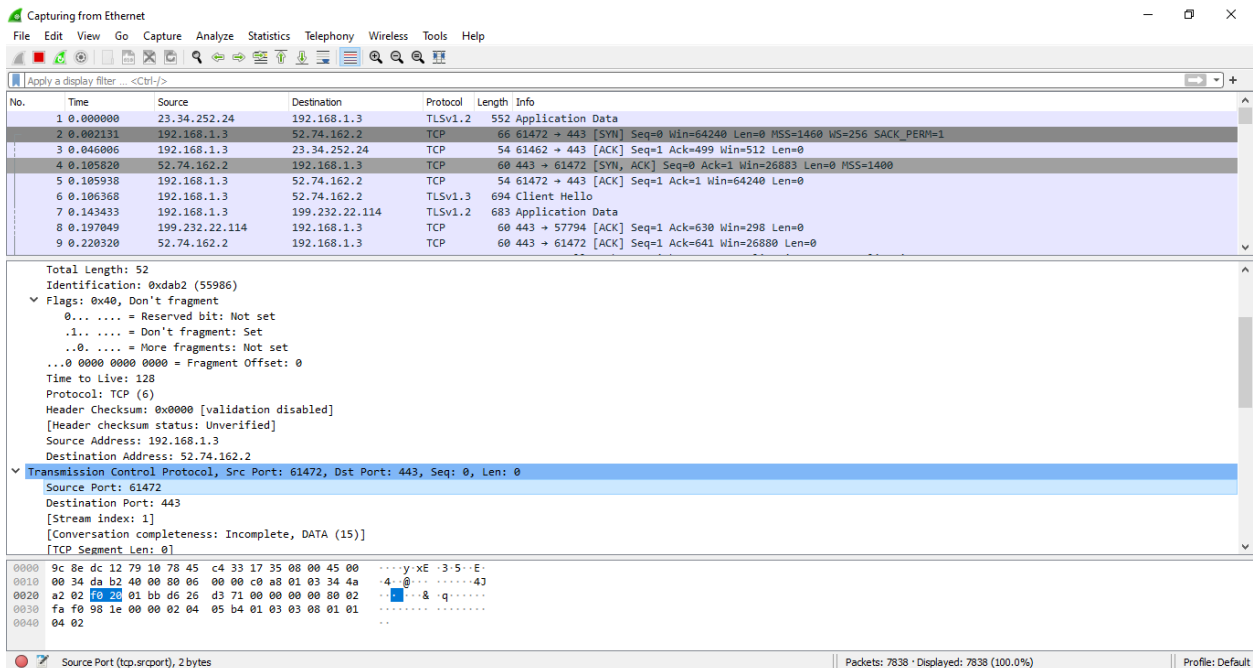
Congratulations!

You've now transferred a copy of alice.txt from your computer to gaia.cs.umass.edu. You should now stop Wireshark packet capture. It's time to start analyzing the captured Wireshark packets!

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

Solution: Src IP address = 192.168.1.3

Src Port = 61472



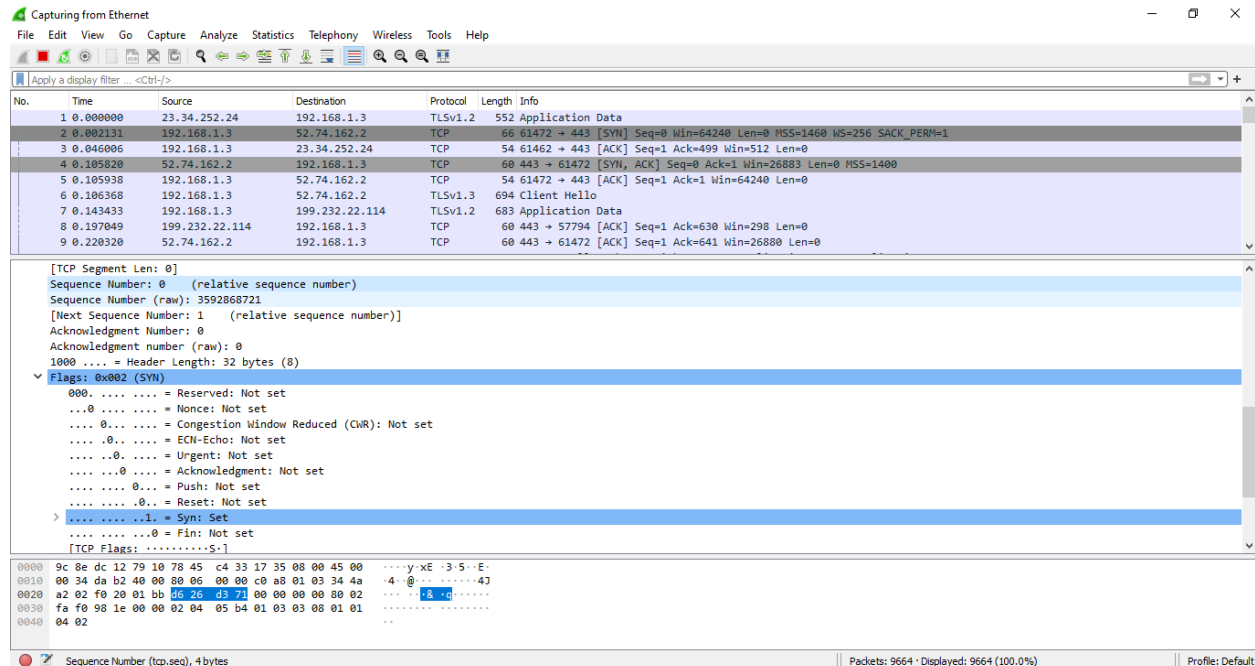
(k) What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

Solution: Sequence Number is a 32-bit field that holds a number for the first byte sent in a particular segment. This number helps in the identification of the messages received in order.

Sequence number (relative) = 0

Sequence number (raw) = 3592868721

The first TCP datagram for the ftp session initiation only sets **SYN** bit to **1**.



(I) 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?

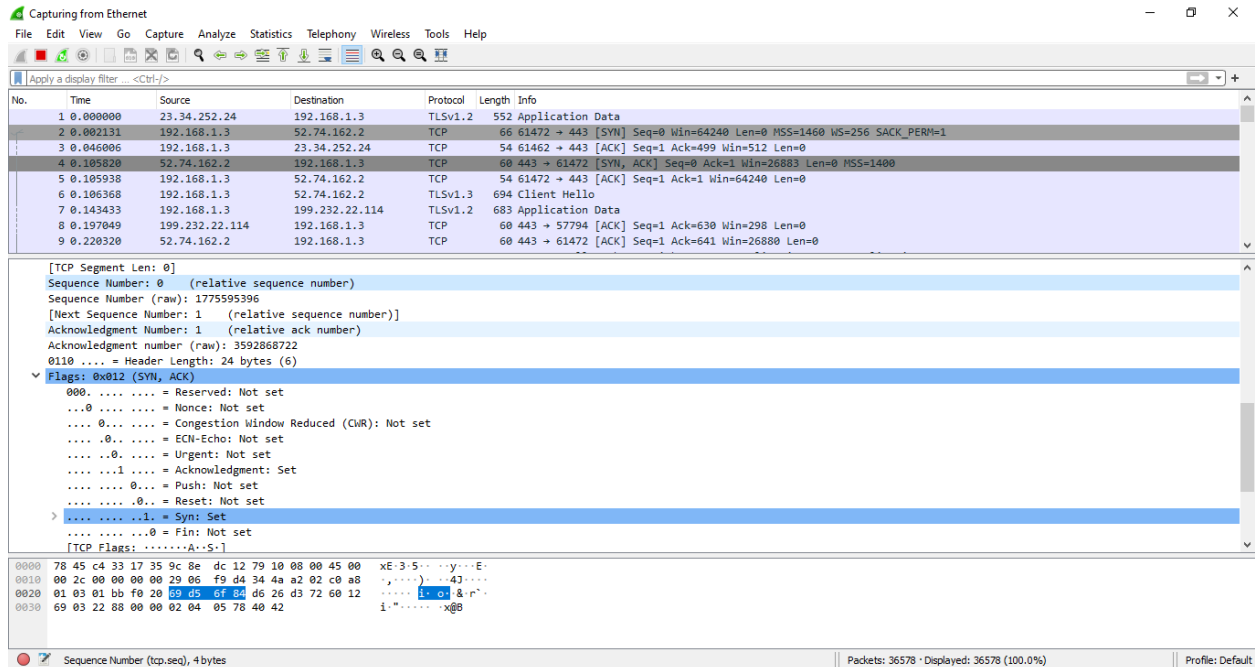
Solution: Sequence number (relative) = 0

Sequence number (raw) = 1775595396

Acknowledgement number (relative) = 1

Acknowledgement number (raw) = 3592868722. The value of the ACKnowledgement field in the SYNACK segment is determined by gaia.cs.umass.edu **by adding 1 to the initial sequence number of SYN segment from the client computer** (i.e. the sequence number of the SYN segment initiated by the client computer is 0).

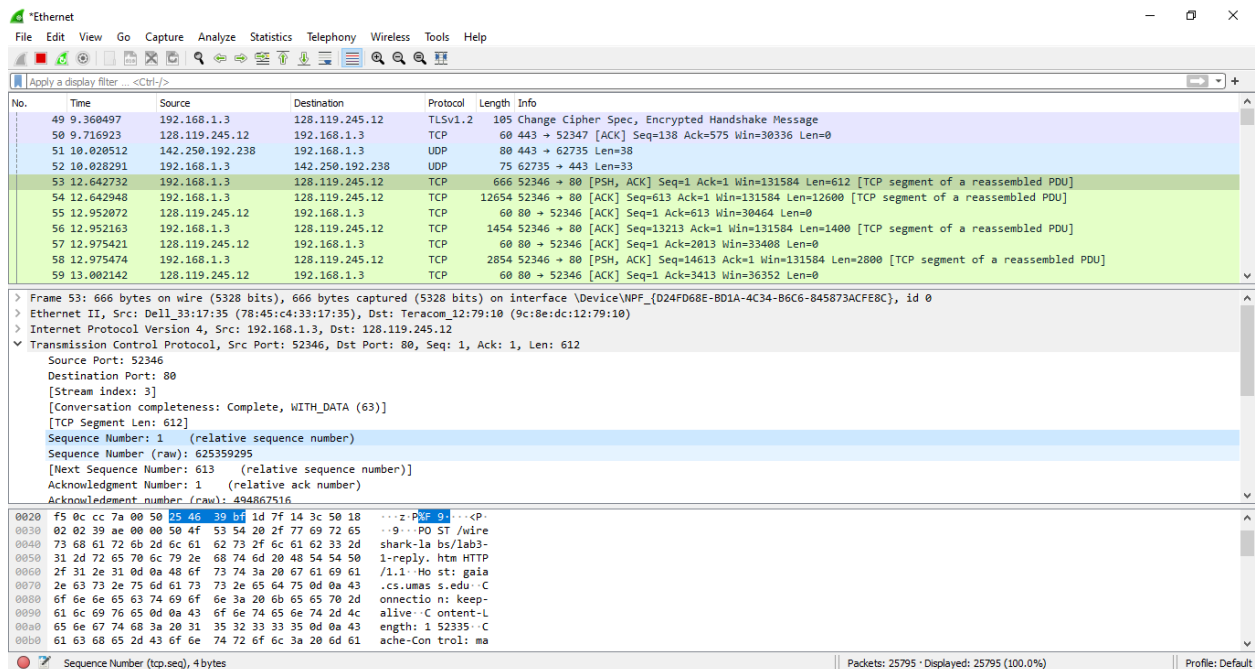
The TCP datagram for the ftp sets **SYN & ACK** bit to **1**.



(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.

Solution: Sequence number (relative) = 1

Sequence number (raw) = 625359295



(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

Solution:

Segment no.	Sequence number	Send time	Received time	RTT
1.	1	4.0255		4.0255
2.	613	4.02571	4.33484	0.30913
3.	13213	4.334931	4.358189	0.023258
4.	14613	4.358242	4.38491	0.26668
5.	17413	4.384987	4.413993	0.29006
6.	20213	4.414054	4.437691	0.023637

According to the formula: $\text{EstimatedRTT} = 0.875 * \text{EstimatedRTT} + 0.125 * \text{SampleRTT}$

EstimatedRTT after the receipt of the ACK of segment 1:

EstimatedRTT = RTT for Segment 1 = 0.095674 s

EstimatedRTT after the receipt of the ACK of segment 2:

EstimatedRTT = 0.30913 s

EstimatedRTT after the receipt of the ACK of segment 3:

EstimatedRTT = $0.875 * 0.30913 + 0.125 * 0.023258 = 0.273396$ s

EstimatedRTT after the receipt of the ACK of segment 4:

EstimatedRTT = $0.875 * 0.273396 + 0.125 * 0.26668 = 0.2725565$ s

EstimatedRTT after the receipt of the ACK of segment 5:

EstimatedRTT = $0.875 * 0.2725565 + 0.125 * 0.29006 = 0.2747444375$ s

EstimatedRTT after the receipt of the ACK of segment 5:

EstimatedRTT = $0.875 * 0.2747444375 + 0.125 * 0.023637 = 0.2433560078$ s

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

Solution: The length of the first TCP segment is 612 bytes, the length of the second TCP segment is 12600 bytes, the length of the third TCP segment is 1400 bytes. The length of each of the remaining TCP segments is 2800 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
51	10.020512	142.250.192.238	192.168.1.3	UDP	80	443 → 62735 Len=38
52	10.028291	192.168.1.3	142.250.192.238	UDP	75	62735 → 443 Len=33
53	12.642732	192.168.1.3	128.119.245.12	TCP	666	52346 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=612 [TCP segment of a reassembled PDU]
54	12.642948	192.168.1.3	128.119.245.12	TCP	12654	52346 → 80 [ACK] Seq=613 Ack=1 Win=131584 Len=12600 [TCP segment of a reassembled PDU]
55	12.952072	128.119.245.12	192.168.1.3	TCP	60	80 → 52346 [ACK] Seq=1 Ack=613 Win=30464 Len=0
56	12.952163	192.168.1.3	128.119.245.12	TCP	1454	52346 → 80 [ACK] Seq=13213 Ack=1 Win=131584 Len=1400 [TCP segment of a reassembled PDU]
57	12.975421	128.119.245.12	192.168.1.3	TCP	60	80 → 52346 [ACK] Seq=1 Ack=2013 Win=33408 Len=0
58	12.975474	192.168.1.3	128.119.245.12	TCP	2854	52346 → 80 [PSH, ACK] Seq=14613 Ack=1 Win=131584 Len=2800 [TCP segment of a reassembled PDU]
59	13.002142	128.119.245.12	192.168.1.3	TCP	60	80 → 52346 [ACK] Seq=1 Ack=3413 Win=36352 Len=0
60	13.002219	192.168.1.3	128.119.245.12	TCP	2854	52346 → 80 [ACK] Seq=17413 Ack=1 Win=131584 Len=2800 [TCP segment of a reassembled PDU]
61	13.031225	128.119.245.12	192.168.1.3	TCP	60	80 → 52346 [ACK] Seq=1 Ack=4813 Win=39296 Len=0

> Frame 53: 666 bytes on wire (5328 bits), 666 bytes captured (5328 bits) on interface \Device\NPF_{D24FD68E-BD1A-4C34-B6C6-845873ACFE8C}, id 0
 > Ethernet II, Src: Dell_33:17:35 (78:45:c4:33:17:35), Dst: Teracom_12:79:10 (9c:8e:dc:12:79:10)
 > Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
 > Transmission Control Protocol, Src Port: 52346, Dst Port: 80, Seq: 1, Ack: 1, Len: 612
 Source Port: 52346
 Destination Port: 80
 [Stream index: 3]
 [Conversation completeness: Complete, WITH_DATA (63)]
 [TCP Segment Len: 612]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 625359295
 [Next Sequence Number: 613 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment Number (raw): 494867516

0000 f5 0c cc 7a 00 50 25 46 39 bf 1d 7f 14 3c 18 ...:PXf 9...<
 0030 02 02 39 ae 00 50 4f 53 54 20 2f 77 69 72 65 ...9...PO ST /wire
 0040 73 68 61 72 6b 2d 6c 61 62 73 2f 6c 61 62 33 2d shark-la bs/lab3-
 0050 31 2d 72 65 70 6c 79 2e 68 74 6d 20 48 54 54 50 1-reply. htm HTTP
 0060 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 67 61 69 61 /1.1..Ho st: gaia
 0070 2e 63 73 2e 75 6d 61 73 73 2e 65 64 75 0d 0a 43 .cs.umass.edu..C
 0080 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d connectio n: keep-
 0090 61 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c allive..C content-L
 00a0 65 6e 67 74 68 3a 20 31 35 32 33 33 35 0d 0a 43 emgth: 1 52335..C
 00b0 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 acHe-Cont rol: ma

(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?

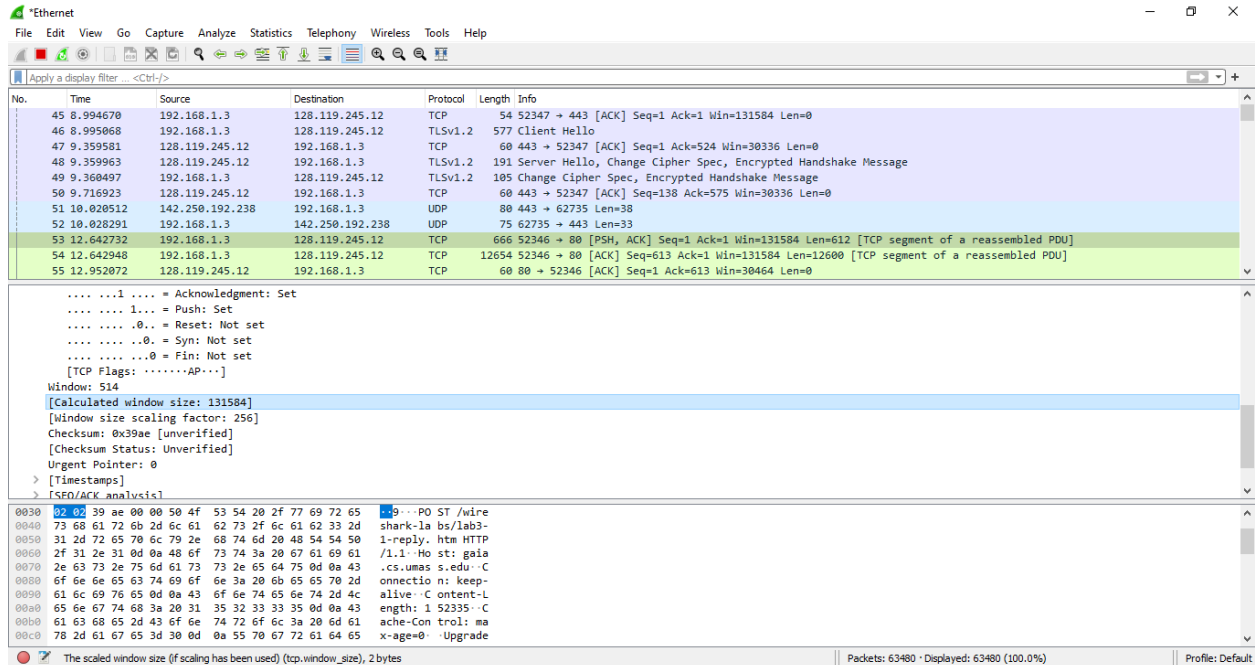
Solution: The minimum amount of available buffer space advertised at the received for the entire trace is indicated first ACK from the server, its value is 30464 bytes (shown in above figure).

No.	Time	Source	Destination	Protocol	Length	Info
47	9.359581	128.119.245.12	192.168.1.3	TCP	60	443 → 52347 [ACK] Seq=1 Ack=524 Win=30336 Len=0
48	9.359963	128.119.245.12	192.168.1.3	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
49	9.360497	192.168.1.3	128.119.245.12	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
50	9.716923	128.119.245.12	192.168.1.3	TCP	60	443 → 52347 [ACK] Seq=138 Ack=575 Win=30336 Len=0
51	10.020512	142.250.192.238	192.168.1.3	UDP	80	443 → 62735 Len=38
52	10.028291	192.168.1.3	142.250.192.238	UDP	75	62735 → 443 Len=33
53	12.642732	192.168.1.3	128.119.245.12	TCP	666	52346 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=612 [TCP segment of a reassembled PDU]
54	12.642948	192.168.1.3	128.119.245.12	TCP	12654	52346 → 80 [ACK] Seq=613 Ack=1 Win=131584 Len=12600 [TCP segment of a reassembled PDU]
55	12.952072	128.119.245.12	192.168.1.3	TCP	60	80 → 52346 [ACK] Seq=1 Ack=613 Win=30464 Len=0
56	12.952163	192.168.1.3	128.119.245.12	TCP	1454	52346 → 80 [ACK] Seq=13213 Ack=1 Win=131584 Len=1400 [TCP segment of a reassembled PDU]
57	12.975421	128.119.245.12	192.168.1.3	TCP	60	80 → 52346 [ACK] Seq=1 Ack=2013 Win=33408 Len=0

.....1..... = Acknowledgment: Set
0... = Push: Not set
0... = Reset: Not set
0... = Syn: Not set
0... = Fin: Not set
 [TCP Flags:A....]
 Window: 238
 [Calculated window size: 30464]
 [Window size scaling factor: 128]
 Checksum: 0x17c8 [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 > [Timestamps]
 > [SFD/ACK analysis]

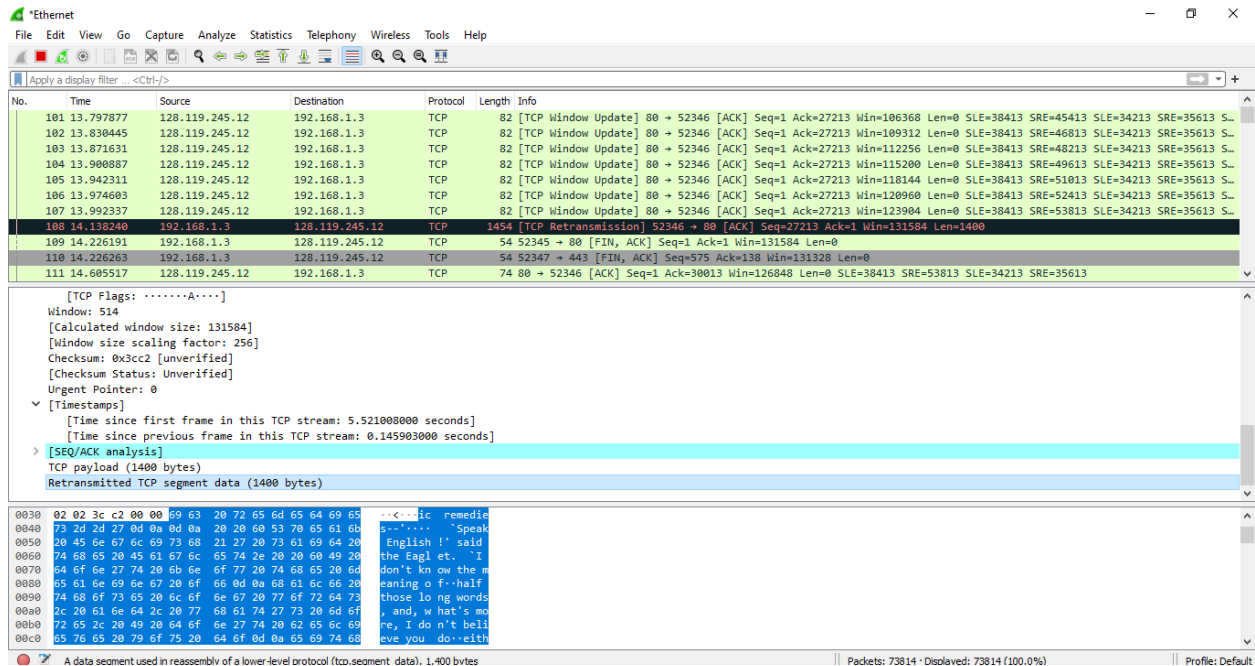
0000 78 45 c4 33 17 35 9c 8e dc 12 79 10 08 00 45 00 xE3 5...y...E-
 0010 00 28 0e f3 00 00 26 06 4e ae 80 77 f5 0c c0 a8 -(....& N..w...
 0020 01 03 00 50 cc 7a 1d 7f 14 3c 25 46 3c 23 50 10 ...P..z...<%F#P-
 0030 80 ee 17 c8 00 00 01 01 08 0a bf 8b

This receiver window grows until it reaches the maximum receiver buffer size of 131584 bytes. According to the trace, the sender is never throttled due to the lack of receiver buffer space.



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

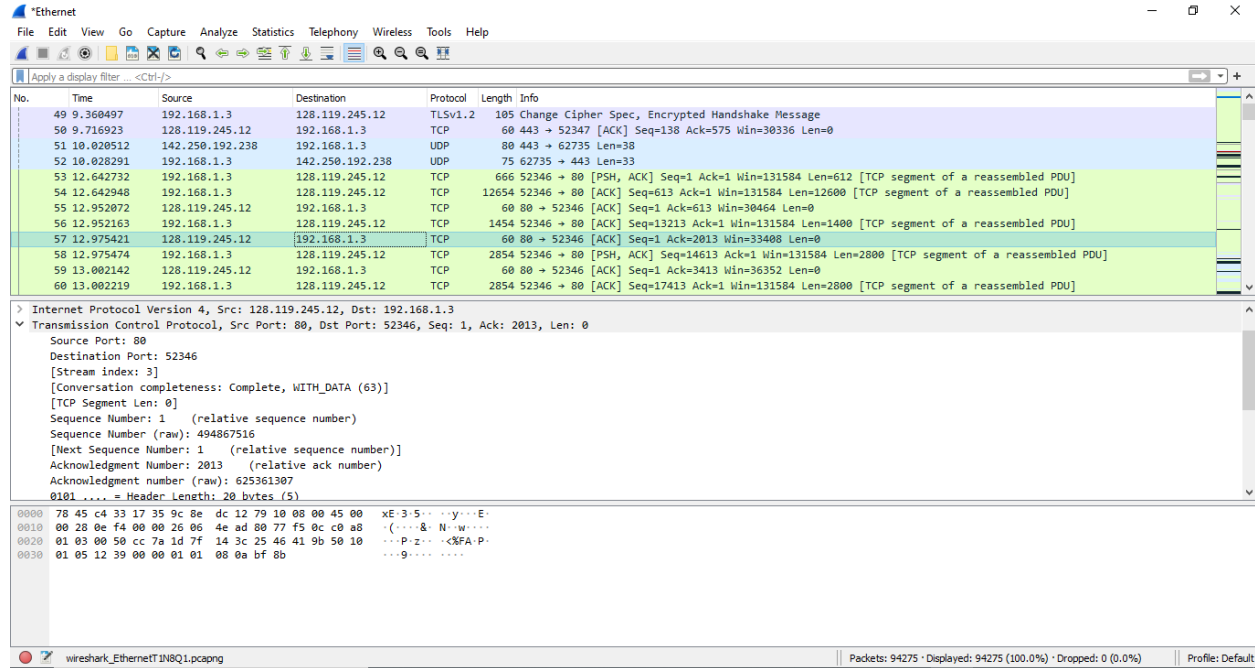
Solution: Yes, there are retransmitted segments in the trace file. When an outbound segment is handed down to an IP and there's no acknowledgment for the data before TCP's automatic timer expires, the segment is retransmitted.



(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).

Solution: The difference between the acknowledged sequence numbers of two consecutive ACKs indicates the data received by the server between these two ACKs. The receiver is ACKing every other segment. For example, segment of No. 57 acknowledged data with $2013 - 613 = 1400$ bytes.

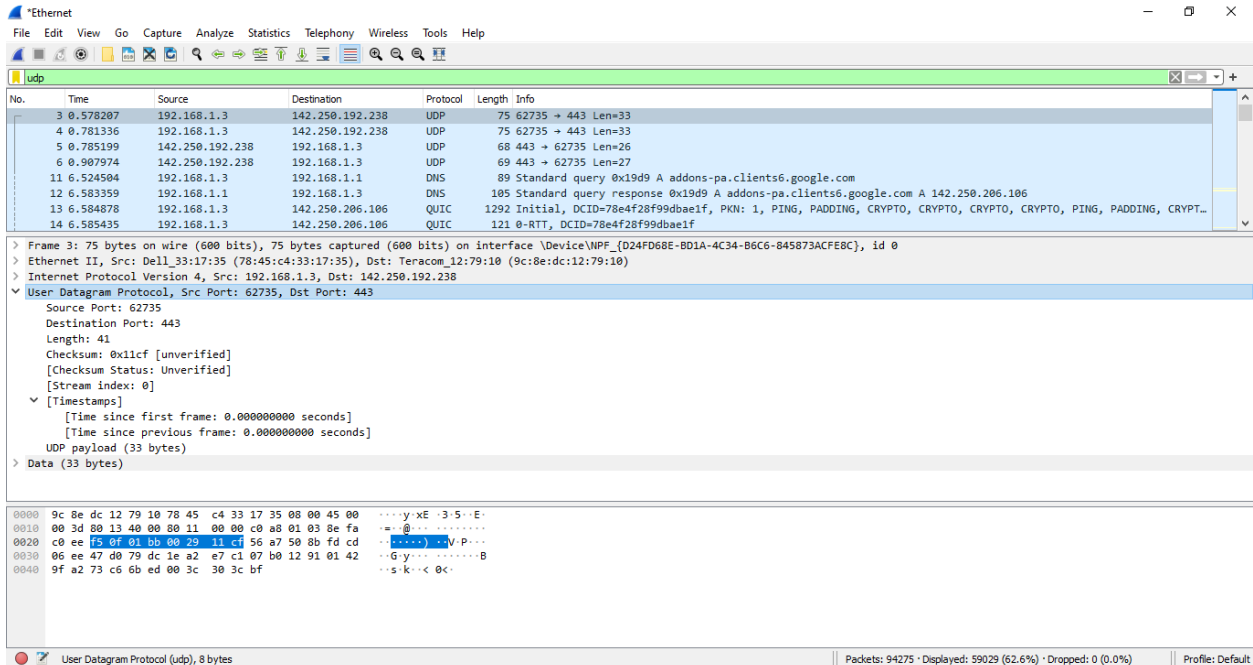


(s) What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

Solution: The alice.txt on the hard drive is 152,138 bytes, and the download time is 4.025500000(First TCP segment) - 0.000043000(last ACK) = 4.025457 second. Therefore, the throughput for the TCP connection is computed as $152,138 / 4.025457 = 37,793.969728$ bytes/second.

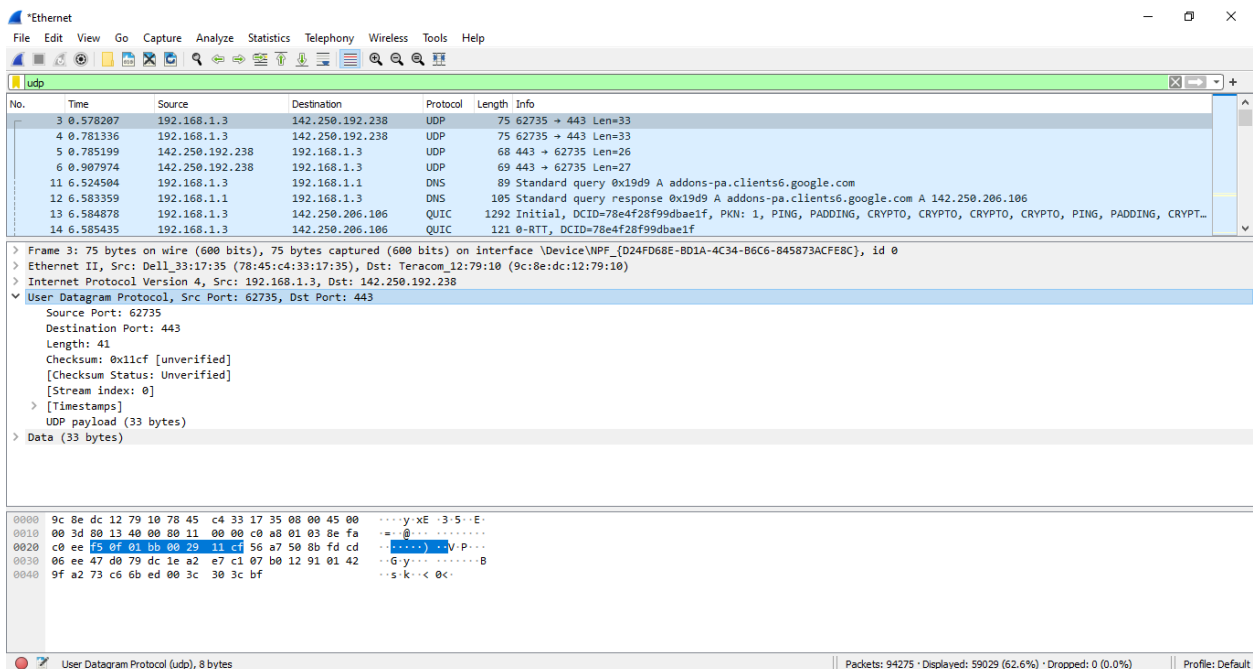
(t) Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

Solution: Source Port, Destination Port, Length, Checksum.



(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.

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

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 33 bytes. 41 bytes - 8 bytes = 33 bytes.

The screenshot shows a Wireshark packet capture of a UDP segment. The packet list at the top shows a UDP packet with length 443. The packet details pane shows the UDP header with source port 62735, destination port 443, and length 41. The packet bytes pane shows the raw data of the UDP segment.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.578207	192.168.1.3	142.250.192.238	UDP	75	62735 → 443 Len=33
4	0.781336	192.168.1.3	142.250.192.238	UDP	75	62735 → 443 Len=33
5	0.785199	142.250.192.238	192.168.1.3	UDP	68	443 → 62735 Len=26
6	0.907974	142.250.192.238	192.168.1.3	UDP	69	443 → 62735 Len=27
11	6.524504	192.168.1.3	192.168.1.1	DNS	89	Standard query 0x19d9 A addons-pa.clients6.google.com
12	6.583359	192.168.1.1	192.168.1.3	DNS	105	Standard query response 0x19d9 A addons-pa.clients6.google.com A 142.250.206.106
13	6.584878	192.168.1.3	142.250.206.106	QUIC	1292	Initial, DCID=78e4f28f99dbae1f, PKN: 1, PING, PADDING, CRYPTO, CRYPTO, CRYPTO, CRYPTO, PING, PADDING, CRYPTO...
14	6.585435	192.168.1.3	142.250.206.106	QUIC	121	0-RTT, DCID=78e4f28f99dbae1f

Frame 3: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{D24FD68E-BD1A-4C34-B6C6-845873ACFE8C}, id 0
 Ethernet II, Src: Dell_33:17:35 (78:45:c4:33:17:35), Dst: Teracom_12:79:10 (9c:8e:dc:12:79:10)
 Internet Protocol Version 4, Src: 192.168.1.3, Dst: 142.250.192.238
 User Datagram Protocol, Src Port: 62735, Dst Port: 443
 Source Port: 62735
 Destination Port: 443
 Length: 41
 Checksum: 0x11cf [unverified]
 [Checksum Status: Unverified]
 [Stream index: 0]
 [Timestamps]
 UDP payload (33 bytes)
 Data (33 bytes)

0000 9c 8e dc 12 79 10 78 45 c4 33 17 35 00 00 45 00xE-35-E-
 0010 00 3d 80 13 40 00 80 11 00 00 c0 a8 01 03 8e fa@.....
 0020 c0 ee f5 0f 01 bb 00 29 11 cf 56 a7 50 8b fd cdV-P...
 0030 06 ee 47 d0 79 dc 1e a2 e7 c1 07 b0 12 91 01 42 ...G-y.....B
 0040 9f a2 73 c6 6b ed 00 3c 30 3c bfs-k<<0k

(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)

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.

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

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

(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).

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

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. The bottom pane shows the detailed view of the selected packet (No. 3), which is a UDP packet. The packet details are as follows:

No.	Time	Source	Destination	Protocol	Length	Info
3	0.578207	192.168.1.3	142.250.192.238	UDP	75	62735 → 443 Len=33
4	0.781336	192.168.1.3	142.250.192.238	UDP	75	62735 → 443 Len=33
5	0.785199	142.250.192.238	192.168.1.3	UDP	68	443 → 62735 Len=26
6	0.907974	142.250.192.238	192.168.1.3	UDP	69	443 → 62735 Len=27
11	6.524504	192.168.1.3	192.168.1.1	DNS	89	Standard query 0x19d9 A addons-pa.clients6.google.com
12	6.583359	192.168.1.1	192.168.1.3	DNS	105	Standard query response 0x19d9 A addons-pa.clients6.google.com A 142.250.206.106
13	6.584878	192.168.1.3	142.250.206.106	QUIC	1292	Initial, DCID=78e4f28f99dbae1f, PKN: 1, PING, PADDING, CRYPTO, CRYPTO, CRYPTO, CRYPTO, PING, PADDING, CRYPT...
14	6.585435	192.168.1.3	142.250.206.106	QUIC	121	0-RTT, DCID=78e4f28f99dbae1f

The detailed view of the selected packet (No. 3) shows the following structure:

- Frame 3: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{D24FD68E-BD1A-4C34-B6C6-845873ACFE8C}, id 0
- Ethernet II, Src: Dell_33:17:35 (78:45:c4:33:17:35), Dst: Teracom_12:79:10 (9c:8e:dc:12:79:10)
- Internet Protocol Version 4, Src: 192.168.1.3, Dst: 142.250.192.238
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 61
 - Identification: 0x8013 (32787)
 - Flags: 0x40, Don't fragment
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 128
 - Protocol: UDP (17)
 - Header Checksum: 0x0000 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.1.3
 - Destination Address: 142.250.192.238
- User Datagram Protocol, Src Port: 62735, Dst Port: 443
 - 0000 9c 8e dc 12 79 10 78 45 c4 33 17 35 08 00 45 00 ...y.xE 3 5 E
 - 0010 00 3d 00 13 40 00 00 00 00 c0 a8 01 03 8e fa ...@ ...
 - 0020 c0 ee f5 0f 01 bb 00 29 11 cf 56 a7 50 80 fd cd ...P...
 - 0030 06 ee 47 00 79 dc 1e a2 e7 c1 07 b0 12 91 01 42 ...G y ... B
 - 0040 9f a2 73 c6 6b ed 00 3c 30 3c bf ...s k < 0 c

(z) Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second 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.

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
3	0.578207	192.168.1.3	142.250.192.238	UDP	75	62735 → 443 Len=33
4	0.781336	192.168.1.3	142.250.192.238	UDP	75	62735 → 443 Len=33
5	0.785199	142.250.192.238	192.168.1.3	UDP	68	443 → 62735 Len=26
6	0.907974	142.250.192.238	192.168.1.3	UDP	69	443 → 62735 Len=27
11	6.524504	192.168.1.3	192.168.1.1	DNS	89	Standard query 0x19d9 A addons-pa.clients6.google.com
12	6.583359	192.168.1.1	192.168.1.3	DNS	105	Standard query response 0x19d9 A addons-pa.clients6.google.com A 142.250.206.106
13	6.584878	192.168.1.3	142.250.206.106	QUIC	1292	Initial, DCID=78e4f28f99dbae1f, PKN: 1, PING, PADDING, CRYPTO, CRYPTO, PING, PADDING, CRYPT...
14	6.585435	192.168.1.3	142.250.206.106	QUIC	121	0-RTT, DCID=78e4f28f99dbae1f

> Frame 4: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{D24FD68E-BD1A-4C34-B6C6-845873ACFE8C}, id 0

> Ethernet II, Src: Dell_33:17:35 (78:45:c4:33:17:35), Dst: Teracom_12:79:10 (9c:8e:dc:12:79:10)

> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 142.250.192.238

> User Datagram Protocol, Src Port: 62735, Dst Port: 443

Source Port: 62735

Destination Port: 443

Length: 41

Checksum: 0x11cf [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

> [Timestamps]

UDP payload (33 bytes)

> Data (33 bytes)

0000 9c 8e dc 12 79 10 78 45 c4 33 17 35 08 00 45 00xE:3:5...E-

0010 00 20 00 14 40 00 00 11 00 00 c0 a8 01 03 8e fa@.....

0020 c0 ee f5 0f 01 bb 00 29 11 cf 5e a7 50 80 fd cdP.....

0030 06 ee 47 d7 58 02 0a 66 fc 3e be 75 39 c3 07 bcG.X:f->u9...

0040 89 c5 9f 8d 7f 05 50 86 f8 f6 3aP.....

Source Port (udp.srcport), 2 bytes

Packets: 94275 · Displayed: 59029 (62.6%) · Dropped: 0 (0.0%)

Profile: Default

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
3	0.578207	192.168.1.3	142.250.192.238	UDP	75	62735 → 443 Len=33
4	0.781336	192.168.1.3	142.250.192.238	UDP	75	62735 → 443 Len=33
5	0.785199	142.250.192.238	192.168.1.3	UDP	68	443 → 62735 Len=26
6	0.907974	142.250.192.238	192.168.1.3	UDP	69	443 → 62735 Len=27
11	6.524504	192.168.1.3	192.168.1.1	DNS	89	Standard query 0x19d9 A addons-pa.clients6.google.com
12	6.583359	192.168.1.1	192.168.1.3	DNS	105	Standard query response 0x19d9 A addons-pa.clients6.google.com A 142.250.206.106
13	6.584878	192.168.1.3	142.250.206.106	QUIC	1292	Initial, DCID=78e4f28f99dbae1f, PKN: 1, PING, PADDING, CRYPTO, CRYPTO, CRYPTO, PING, PADDING, CRYPT...
14	6.585435	192.168.1.3	142.250.206.106	QUIC	121	0-RTT, DCID=78e4f28f99dbae1f

> Frame 5: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{D24FD68E-BD1A-4C34-B6C6-845873ACFE8C}, id 0

> Ethernet II, Src: Teracom_12:79:10 (9c:8e:dc:12:79:10), Dst: Dell_33:17:35 (78:45:c4:33:17:35)

> Internet Protocol Version 4, Src: 142.250.192.238, Dst: 192.168.1.3

> User Datagram Protocol, Src Port: 443, Dst Port: 62735

Source Port: 443

Destination Port: 62735

Length: 34

Checksum: 0xf8f8 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

> [Timestamps]

UDP payload (26 bytes)

> Data (26 bytes)

0000 78 45 c4 33 17 35 9c 8e dc 12 79 10 08 00 45 00 xE:3:5...y...E-

0010 00 36 00 00 00 00 3a 11 6f 23 8e fa c0 ee c0 a86.....c#.....

0020 01 03 01 05 f5 0f 00 22 f8 f8 5c 2b 8b 74 14 d41.....\+t...

0030 9b 30 46 25 a8 17 c5 f3 6e 55 03 08 77 87 1a d60F.....nU...w...

0040 81 d6 2c eb;

Source Port (udp.srcport), 2 bytes

Packets: 94275 · Displayed: 59029 (62.6%) · Dropped: 0 (0.0%)

Profile: Default