

Name:- MOHAMMED TOUSIF
Roll No:- CB.EN.P2CYS22008

ANALYZING TRANSPORT LAYER PROTOCOLS USING WIRESHARK

Date :- 27-10-2022

Aim :- To analyze Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) using wireshark.

Tools Required :- Windows OS , CMD with Administrator privilege , Wireshark.

Procedure :-

Opening “tcp” pcap file in wireshark.

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

IP address of gaia.cs.umass.edu

```
C:\WINDOWS\system32>nslookup gaia.cs.umass.edu
Server: prithvi.amritanet.edu
Address: 172.17.18.2

Non-authoritative answer:
Name: gaia.cs.umass.edu
Address: 128.119.245.12

C:\WINDOWS\system32>
```

Source and Destination addresses:

192.168.1.102	128.119.245.12	TCP	62 1161 → 80 [SYN]
128.119.245.12	192.168.1.102	TCP	62 80 → 1161 [SYN,
192.168.1.102	128.119.245.12	TCP	54 1161 → 80 [ACK]
192.168.1.102	128.119.245.12	TCP	619 1161 → 80 [PSH,
192.168.1.102	128.119.245.12	TCP	1514 1161 → 80 [PSH,

b. What is the IP address of `gaia.cs.umass.edu`? On what port number is it sending and receiving TCP segments for this connection?

IP address : 128.119.245.12

	1161	80
	80	1161
	1161	80
	1161	80
	1161	80

c. 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?

Sequence Number : 0

Length	Info	Srcport	Destport
62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM	1161	80
62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM	80	1161

SYN Segment

```

Flags: 0x002 (SYN)
  000. .... = Reserved: Not set
  ...0 .... = Accurate ECN: Not set
  .... 0... = Congestion Window Reduced: Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...0 .... = Acknowledgment: Not set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
  .... .... ...0 = Fin: Not set

```

d. 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?

```
[SYN] Seq=0 Win=16384 Len=0
[SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
[ACK] Seq=1 Ack=1 Win=1752 Len=0
```

Sequence Number of SYNACK : 0

Acknowledgement of SYNACK : 1

gaia.cs.umass.edu determined the ACK value by incrementing 1 to the sequence value as a part of TCP communication .

What is it in the segment that identifies the segment as a SYNACK segment?

```
▼ Flags: 0x012 (SYN, ACK)
  000. .... = Reserved: Not set
  ...0 .... = Accurate ECN: Not set
  .... 0... = Congestion Window Reduced: Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...1 = Acknowledgment: Set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
  .... .... ...0 = Fin: Not set
```

e. 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.

Sequence No of TCP containing HTTP POST command : 1

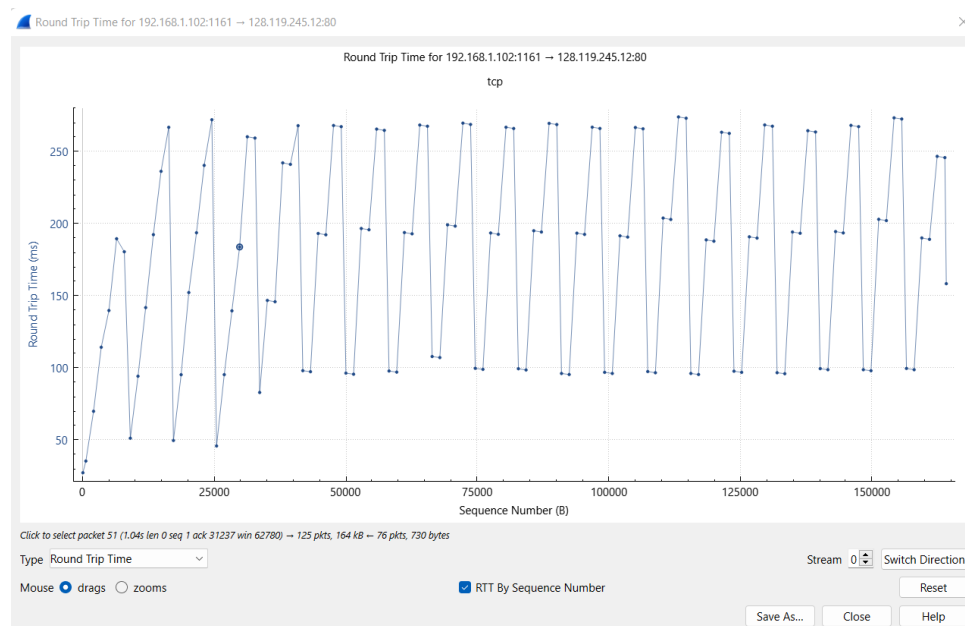
```

TCP 619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
Wireshark · Packet 4 · tcp

> Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 1, Ack: 1, Len: 565
  Source Port: 1161
  Destination Port: 80
  [Stream index: 0]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 565]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 232129013
  [Next Sequence Number: 566 (relative sequence number)]

```

f. Plot the RTT graph using Wireshark.



g. What is the length of each of the first six TCP segments (HTTP POST)?

Length of first six TCP segments :

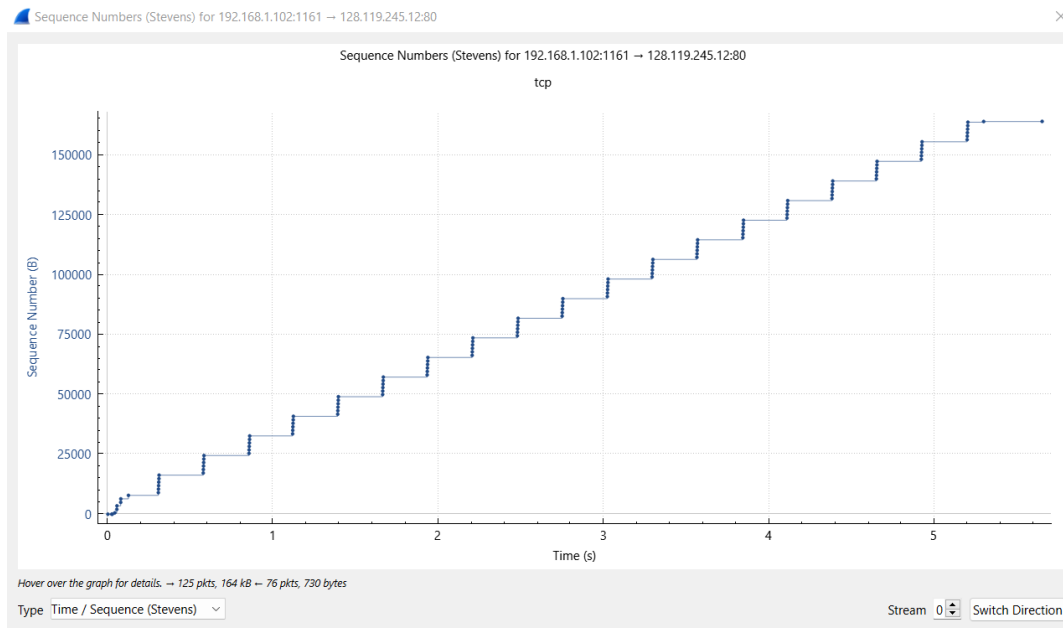
565 , 1460 , 1460 , 1460 , 1460 , 1460

Time	Protocol	Length	Info
0.245.12	HTTP	104	POST /etherreal-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
3.1.102	HTTP	784	HTTP/1.1 200 OK (text/html)

Wireshark · Packet 199 · tcp

> Frame 199: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
 > Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
 > Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
 > Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164041, Ack: 1, Len: 50
 > [122 Reassembled TCP Segments (164090 bytes): #4(565), #5(1460), #7(1460), #8(1460), #10(1460), #11(1460), #13(1147),
 > Hypertext Transfer Protocol
 > MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "-----265001916915724"

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



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

Throughput = Total amount of Data transferred / Total time taken

619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=50 [TCP segment of a reassembled PDU]

TCP	60	80 → 1161 [ACK] Seq=1	Ack=164091	Win=62780	Len=0
-----	----	-----------------------	------------	-----------	-------

✓ Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)
 Encapsulation type: Ethernet (1)
 Arrival Time: Aug 21, 2004 19:14:20.596858000 India Standard Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1093095860.596858000 seconds
 [Time delta from previous captured frame: 0.003212000 seconds]
 [Time delta from previous displayed frame: 0.003212000 seconds]
 [Time since reference or first frame: 0.026477000 seconds]
 Frame Number: 4

Frame 202: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
 Encapsulation type: Ethernet (1)
 Arrival Time: Aug 21, 2004 19:14:26.026211000 India Standard Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1093095866.026211000 seconds
 [Time delta from previous captured frame: 0.007943000 seconds]
 [Time delta from previous displayed frame: 0.007943000 seconds]
 [Time since reference or first frame: 5.455830000 seconds]
 Frame Number: 202
 Frame Length: 60 bytes (480 bits)

$164090 / 5.429353 = 30,222.754$ bytes per second
 30.222 kilobytes/second

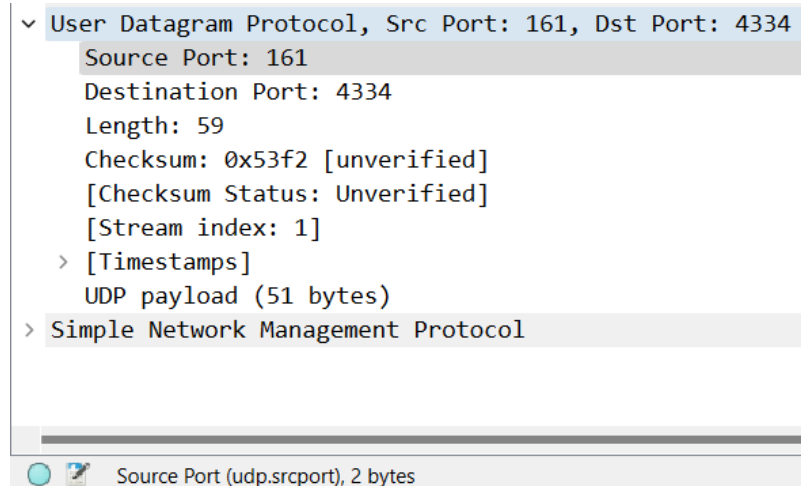
Opening the “udp” pcap file.

j. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. Name these fields.

✓ User Datagram Protocol, Src Port: 137, Dst Port: 137
 Source Port: 137
 Destination Port: 137
 Length: 70
 Checksum: 0x3eea [unverified]
 [Checksum Status: Unverified]
 [Stream index: 11]
 > [Timestamps]
 UDP payload (62 bytes)

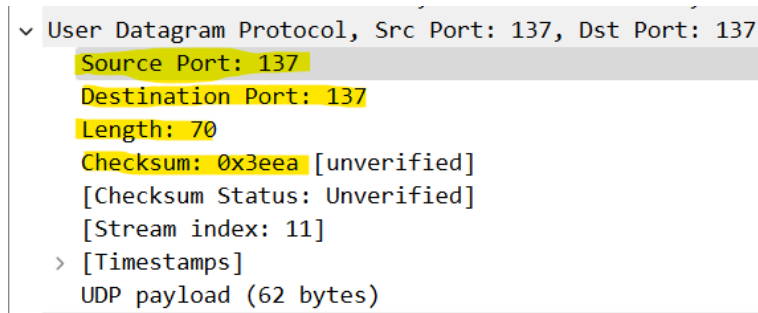
Source Port , Destination Port , Length , Checksum

k. 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.



Source Port : 2 Bytes
Destination Port : 2 Bytes
Length : 2 Bytes
Checksum : 2 Bytes

l. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.



Length : 70

UDP payload + Header length = Length
62 + 8 = 70

m. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation.

```

Internet Protocol Version 4, Src: 192.168.1.102, [
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0,
    Total Length: 90
    Identification: 0x030c (780)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]

```

Protocol No for UDP is : 17

Hexadecimal Notation : 11

n. 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.

Destination	Protocol	Length	Info	Srcport	Destport
192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0	4334	161
192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0	161	4334

Sourceport : 4334

Destination port : 161

Result :- Analyzing TCP and UDP protocols using wireshark is successfully done.