United International University

Assignment 01

Submitted by:

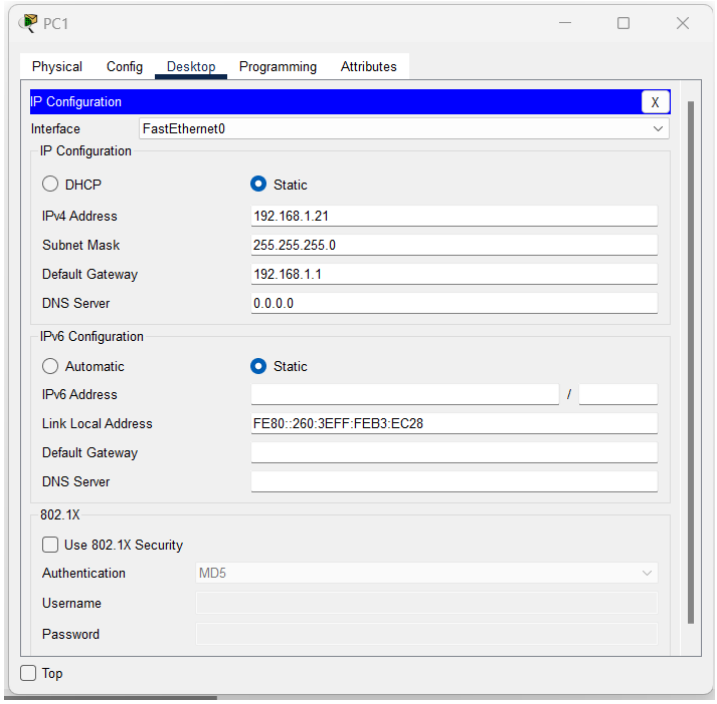
Azizul Islam Nayem (011201262)

Course Title: Computer Networks

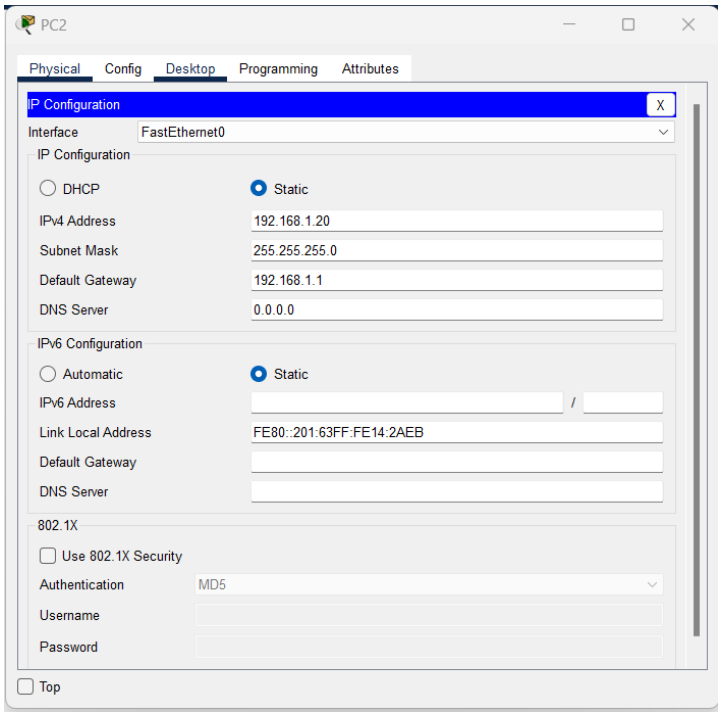
Course Code: CSE 3711

Department of Computer Science & Engineering

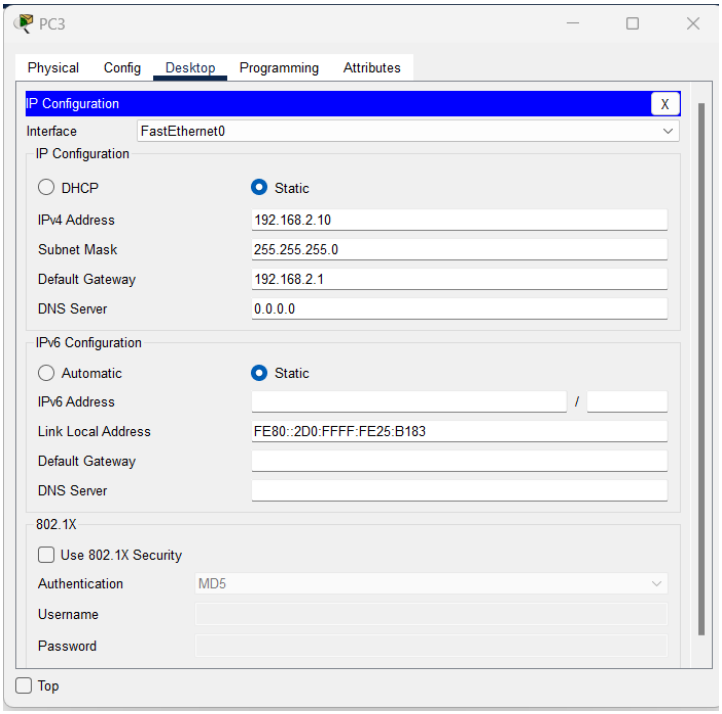
Question 2



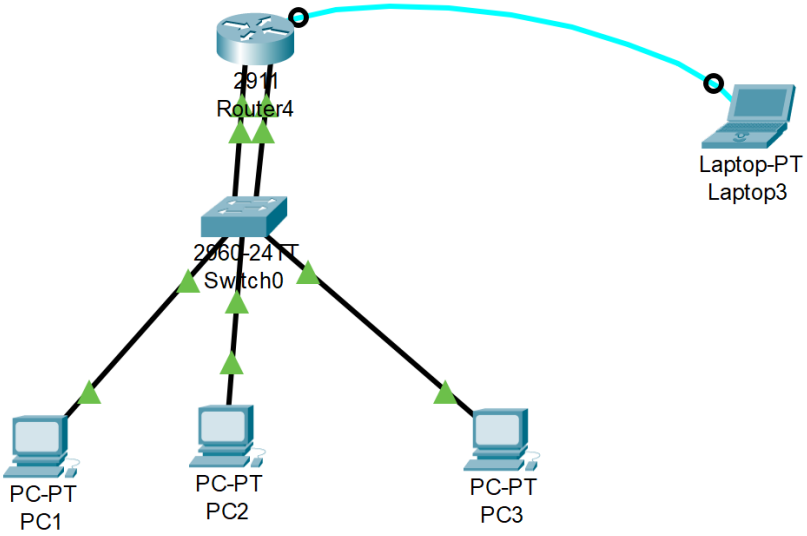
Ip configuration for PC1



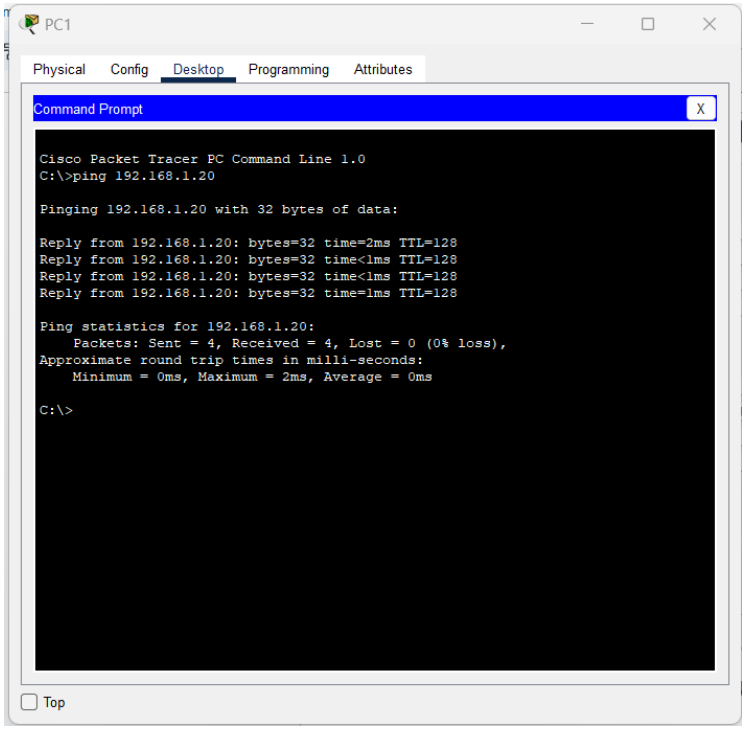
Ip configuration for PC2



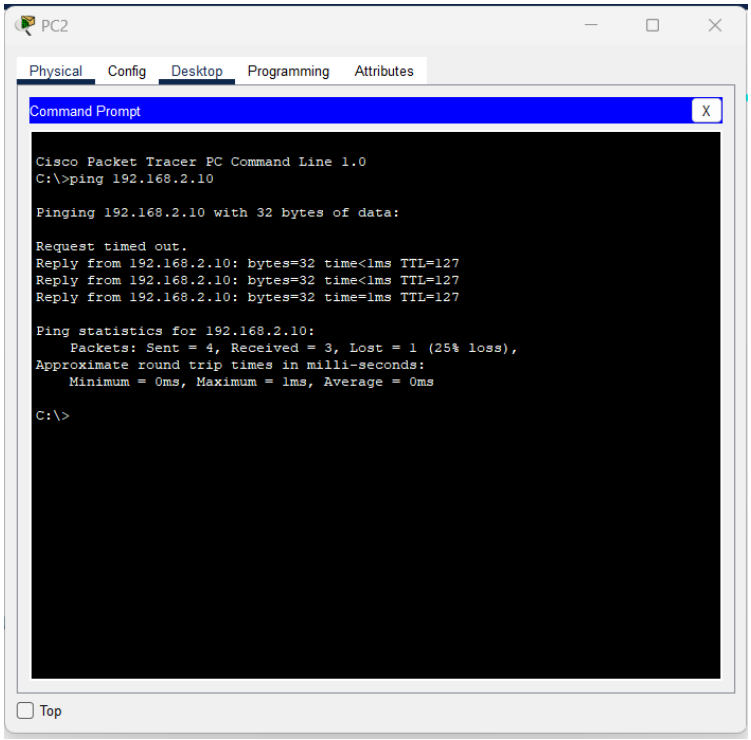
Ip configuration for PC3



Whole network configuration



Verify connectivity between the computers by pinging PC2 from PC1



Verify connectivity between the computers by pinging PC3 from PC2

Question 1

Step 1:

Wireshark · Capture File Properties · Wi-Fi 2

Details

File

Name:	C:\Users\DCL\AppData\Local\Temp\wireshark_Wi-Fi 2MYADA2.pcapng
Length:	433 kB
Hash (SHA256):	3b9f009f2e6a15d1e6ffa7f2d9a5f4ffef491da4e483952e8aecda856449b88d
Hash (RIPEMD160):	a05fc777486b2b2fe23ceaa0aea50cc81bd76bc6
Hash (SHA1):	30c3a3dea78a818f0742dc7850f1bbb616a7c6a6
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2023-08-28 01:33:17
Last packet:	2023-08-28 01:33:35
Elapsed:	00:00:17

Capture

Hardware:	Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz (with SSE4.2)
OS:	64-bit Windows 11 (22H2), build 22621
Application:	Dumpcap (Wireshark) 4.0.8 (v4.0.8-0-g81696bb74857)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Wi-Fi 2	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	972	972 (100.0%)	—
Time span, s	17.460	17.460	—
Average pps	55.7	55.7	—
Average packet size, B	412	412	—
Bytes	400829	400829 (100.0%)	0
Average bytes/s	22 k	22 k	—
Average bits/s	183 k	183 k	—

a) The number of packets captured during the capture session are 972.

Wireshark · Protocol Hierarchy Statistics · Wi-Fi 2

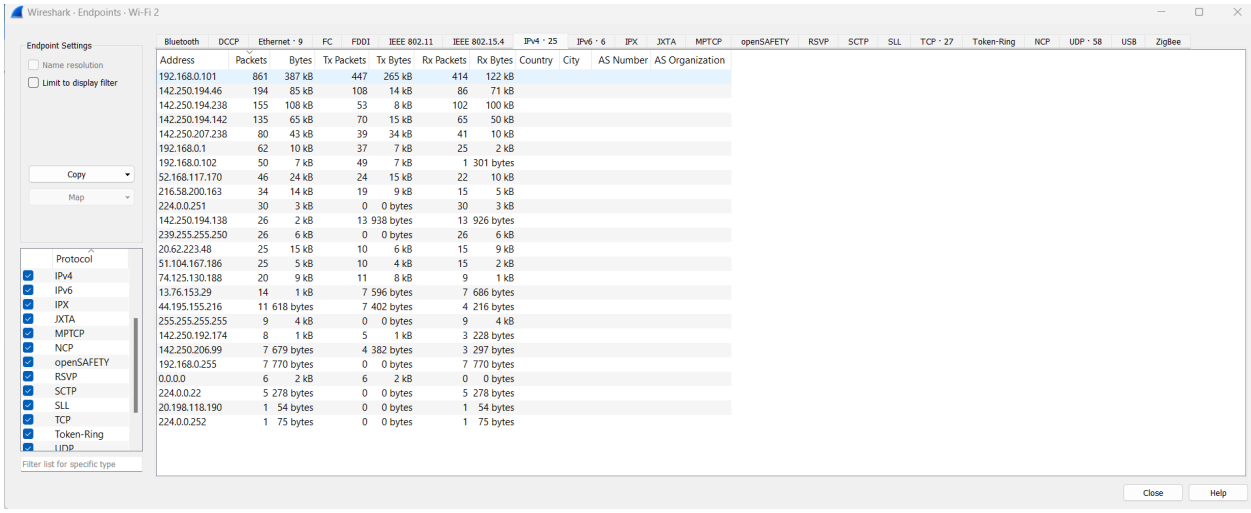
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	972	100.0	400829	183 k	0	0	0	972
Ethernet	100.0	972	3.4	13608	6234	0	0	0	972
Internet Protocol Version 6	1.6	16	0.2	640	293	0	0	0	16
User Datagram Protocol	0.8	8	0.0	64	29	0	0	0	8
Multicast Domain Name System	0.8	8	0.1	320	146	8	320	146	8
Internet Control Message Protocol v6	0.8	8	0.1	224	102	8	224	102	8
Internet Protocol Version 4	94.5	919	4.6	18400	8430	0	0	0	919
User Datagram Protocol	40.3	392	0.8	3136	1436	0	0	0	392
Simple Service Discovery Protocol	2.7	26	1.1	4550	2084	26	4550	2084	26
QUIC IETF	6.5	63	8.3	33206	15 k	63	28484	13 k	67
NetBIOS Name Service	0.7	7	0.1	476	218	7	476	218	7
Multicast Domain Name System	3.2	31	0.5	1963	899	31	1963	899	31
Link-local Multicast Name Resolution	0.1	1	0.0	33	15	1	33	15	1
Dynamic Host Configuration Protocol	0.9	9	0.9	3576	1638	9	3576	1638	9
Domain Name System	6.1	59	1.3	5267	2413	59	5267	2413	59
Data	20.2	196	26.0	104026	47 k	196	104026	47 k	196
Transmission Control Protocol	53.7	522	53.3	213587	97 k	374	144071	66 k	522
Transport Layer Security	15.2	148	40.7	163277	74 k	148	146533	67 k	150
Internet Group Management Protocol	0.5	5	0.0	88	40	5	88	40	5
Address Resolution Protocol	3.8	37	0.3	1036	474	37	1036	474	37

No display filter.

Close Copy Help

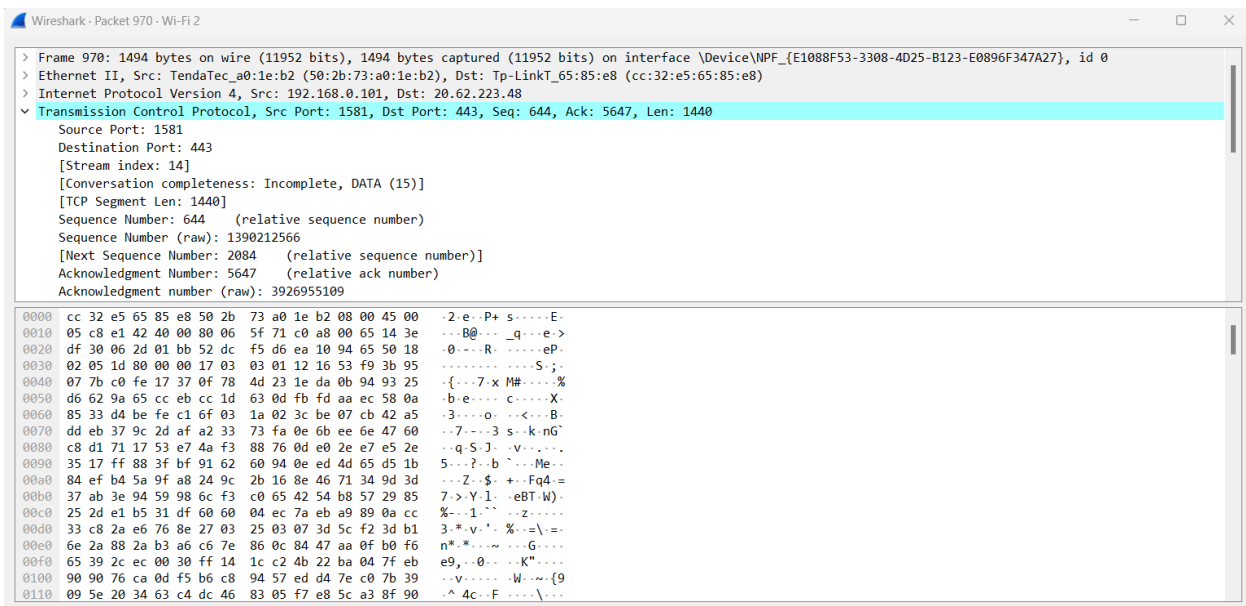
b) The most common protocol in the captured traffic is TCP the percentage is about 53.7 and it is under IPV4.

c)

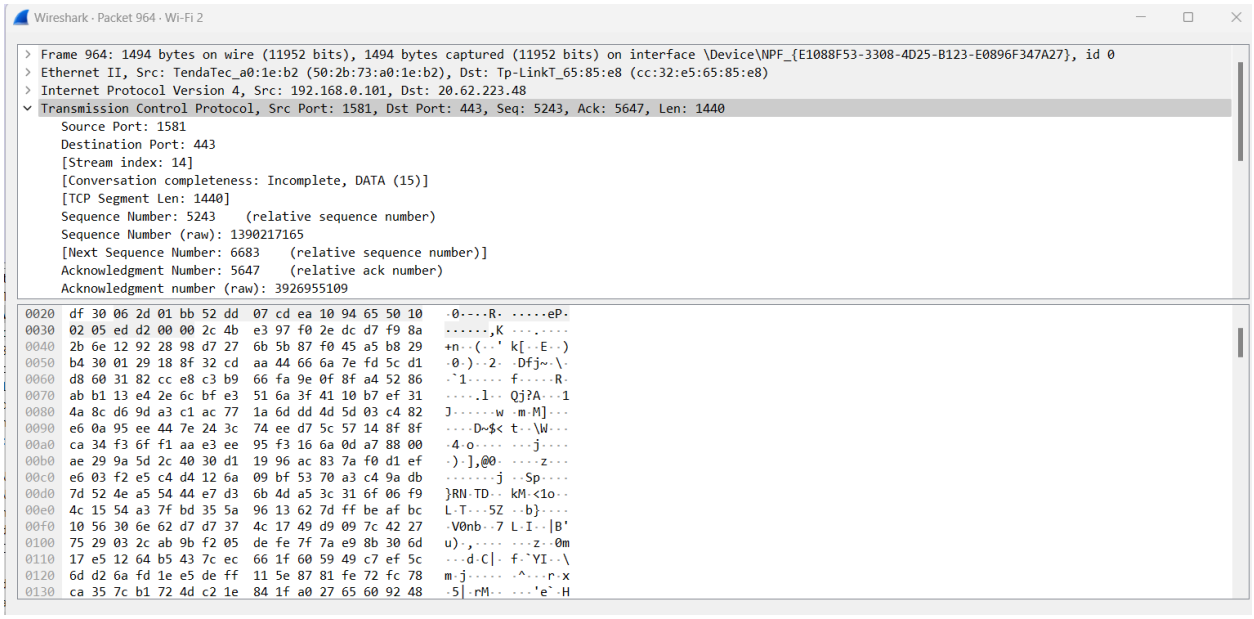


Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
192.168.0.101	861	387 kB	447	265 kB	414	122 kB				
142.250.194.46	194	85 kB	108	14 kB	86	71 kB				
142.250.194.238	155	108 kB	53	8 kB	102	100 kB				
142.250.194.142	135	65 kB	70	15 kB	65	50 kB				
142.250.207.238	80	43 kB	39	34 kB	41	10 kB				
192.168.0.1	62	10 kB	37	7 kB	25	2 kB				
192.168.0.102	50	7 kB	49	7 kB	1	301 bytes				
52.168.117.170	46	24 kB	24	15 kB	22	10 kB				
216.58.200.163	34	14 kB	19	9 kB	15	5 kB				
224.0.0.251	30	3 kB	0	0 bytes	30	3 kB				
142.250.194.138	26	2 kB	13	938 bytes	13	926 bytes				
239.255.255.250	26	6 kB	0	0 bytes	26	6 kB				
20.62.223.48	25	15 kB	10	6 kB	15	9 kB				
51.104.167.186	25	5 kB	10	4 kB	15	2 kB				
74.125.130.188	20	9 kB	11	8 kB	9	1 kB				
13.76.153.29	14	1 kB	7	596 bytes	7	686 bytes				
44.195.155.216	11	618 bytes	7	402 bytes	4	216 bytes				
255.255.255.255	9	4 kB	0	0 bytes	9	4 kB				
142.250.192.174	8	1 kB	5	1 kB	3	228 bytes				
142.250.206.99	7	679 bytes	4	382 bytes	3	297 bytes				
192.168.0.255	7	770 bytes	0	0 bytes	7	770 bytes				
0.0.0.0	6	2 kB	6	2 kB	0	0 bytes				
224.0.0.22	5	278 bytes	0	0 bytes	5	278 bytes				
20.198.118.190	1	54 bytes	0	0 bytes	1	54 bytes				
224.0.0.252	1	75 bytes	0	0 bytes	1	75 bytes				

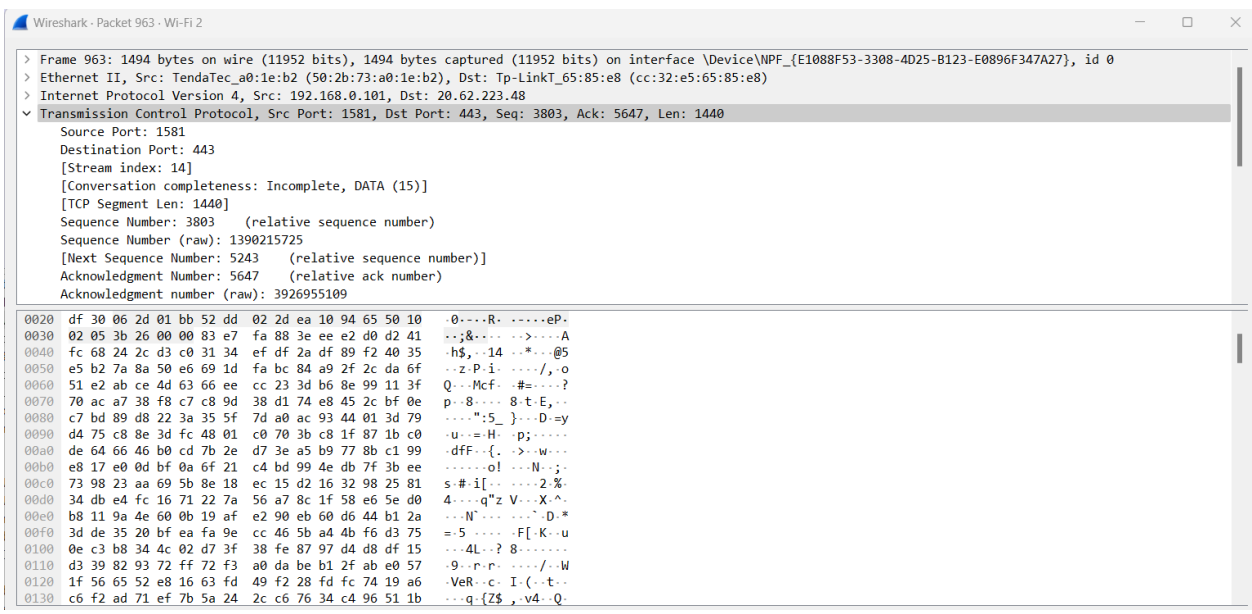
Sorting the endpoints based on the number of packets or bytes transferred.



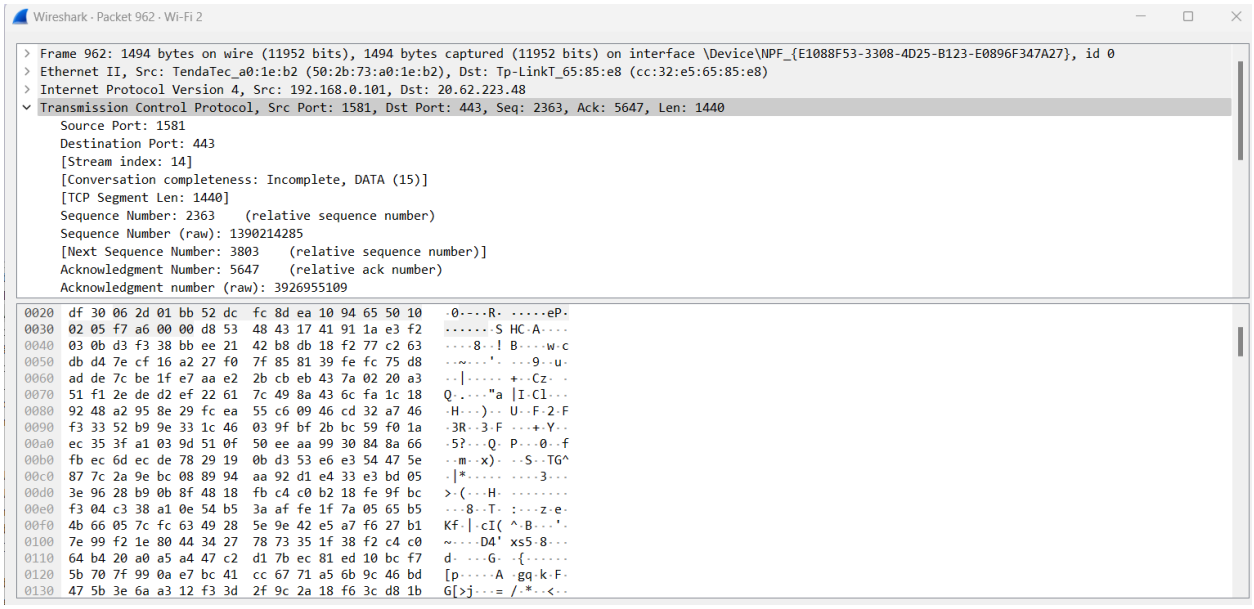
1st network connection among top 5 connection based on length



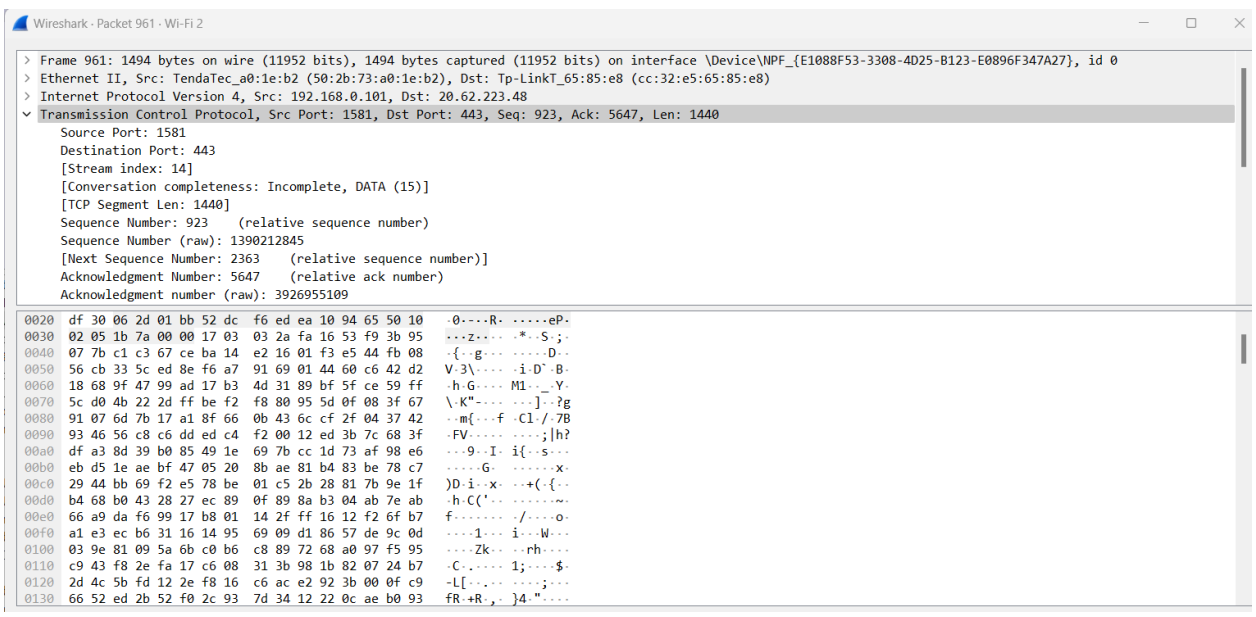
2nd network connection among top 5 connection based on length



3rd network connection among top 5 connection based on length



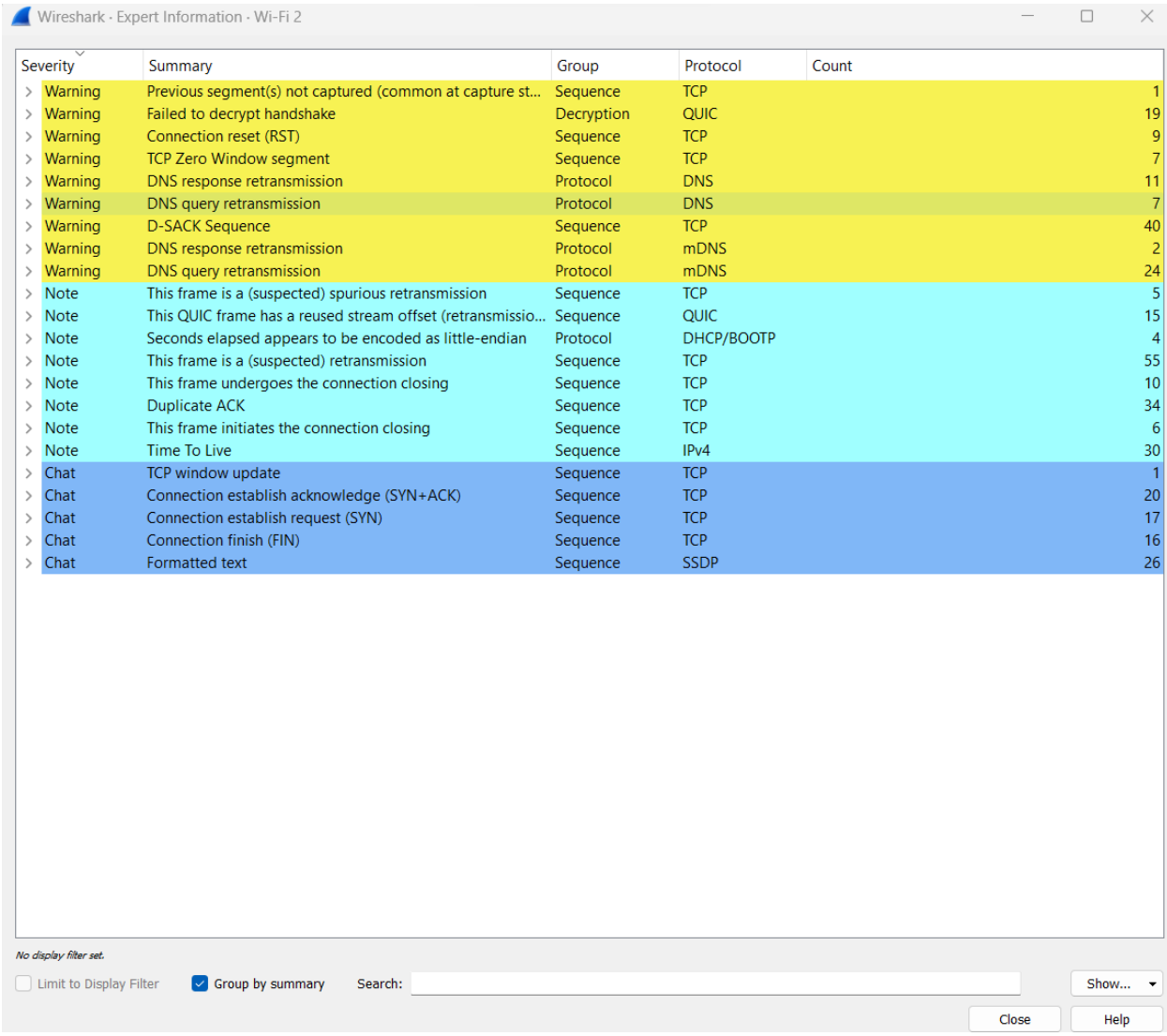
4th network connection among top 5 connection based on length



5th network connection among top 5 connection based on length

Step 2:

a)



Wireshark · Expert Information · Wi-Fi 2

Severity	Summary	Group	Protocol	Count
Warning	Previous segment(s) not captured (common at capture st...	Sequence	TCP	1
Warning	Failed to decrypt handshake	Decryption	QUIC	19
Warning	Connection reset (RST)	Sequence	TCP	9
Warning	TCP Zero Window segment	Sequence	TCP	7
Warning	DNS response retransmission	Protocol	DNS	11
Warning	DNS query retransmission	Protocol	DNS	7
Warning	D-SACK Sequence	Sequence	TCP	40
Warning	DNS response retransmission	Protocol	mDNS	2
Warning	DNS query retransmission	Protocol	mDNS	24
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	5
Note	This QUIC frame has a reused stream offset (retransmissio...	Sequence	QUIC	15
Note	Seconds elapsed appears to be encoded as little-endian	Protocol	DHCP/BOOTP	4
Note	This frame is a (suspected) retransmission	Sequence	TCP	55
Note	This frame undergoes the connection closing	Sequence	TCP	10
Note	Duplicate ACK	Sequence	TCP	34
Note	This frame initiates the connection closing	Sequence	TCP	6
Note	Time To Live	Sequence	IPv4	30
Chat	TCP window update	Sequence	TCP	1
Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP	20
Chat	Connection establish request (SYN)	Sequence	TCP	17
Chat	Connection finish (FIN)	Sequence	TCP	16
Chat	Formatted text	Sequence	SSDP	26

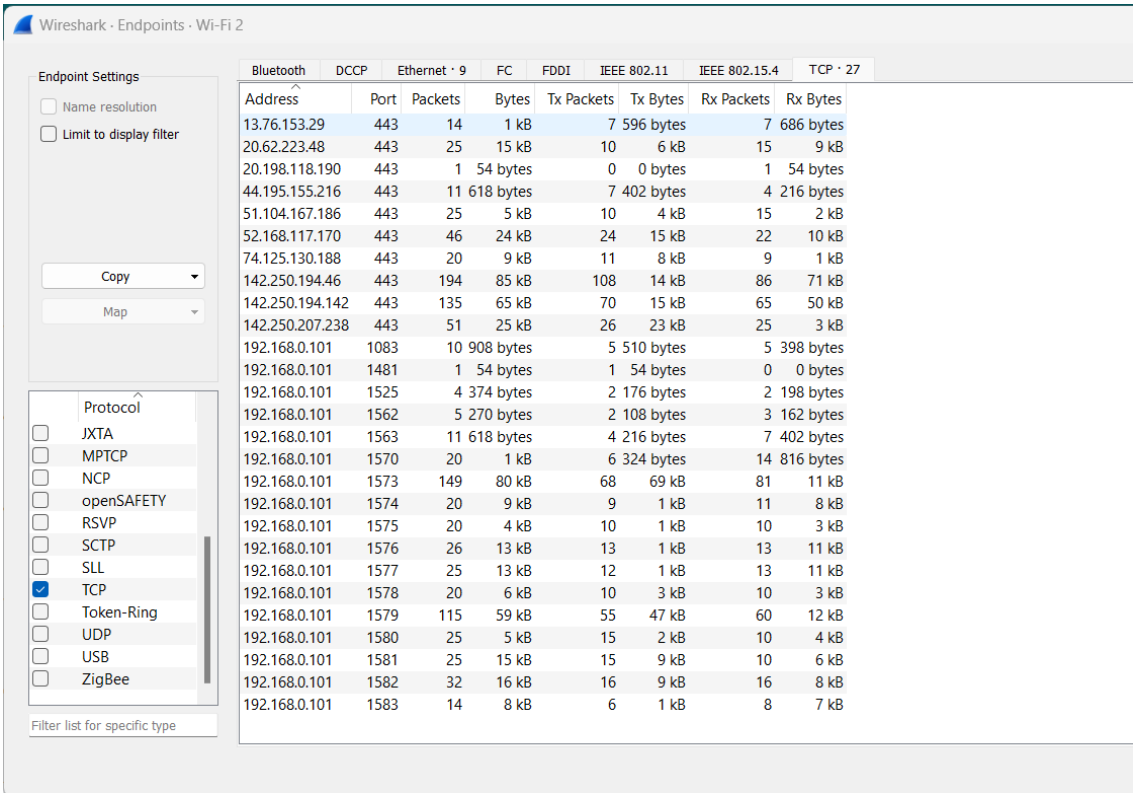
No display filter set.

Limit to Display Filter Group by summary Search: Show...

Close Help

I chose TCP protocol here because from the expert summary i can see that TCP is most used protocol . Besides, TCP is designed to ensure reliable and ordered delivery of data between two devices on a network. It achieves this through various mechanisms like acknowledgment of received data, retransmission of lost packets, and flow control to prevent overwhelming the recipient. TCP is a connection-oriented protocol, meaning it establishes a connection between sender and receiver before data transmission.

b)



Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
13.76.153.29	443	14	1 kB	7	596 bytes	7	686 bytes
20.62.223.48	443	25	15 kB	10	6 kB	15	9 kB
20.198.118.190	443	1	54 bytes	0	0 bytes	1	54 bytes
44.195.155.216	443	11	618 bytes	7	402 bytes	4	216 bytes
51.104.167.186	443	25	5 kB	10	4 kB	15	2 kB
52.168.117.170	443	46	24 kB	24	15 kB	22	10 kB
74.125.130.188	443	20	9 kB	11	8 kB	9	1 kB
142.250.194.46	443	194	85 kB	108	14 kB	86	71 kB
142.250.194.142	443	135	65 kB	70	15 kB	65	50 kB
142.250.207.238	443	51	25 kB	26	23 kB	25	3 kB
192.168.0.101	1083	10	908 bytes	5	510 bytes	5	398 bytes
192.168.0.101	1481	1	54 bytes	1	54 bytes	0	0 bytes
192.168.0.101	1525	4	374 bytes	2	176 bytes	2	198 bytes
192.168.0.101	1562	5	270 bytes	2	108 bytes	3	162 bytes
192.168.0.101	1563	11	618 bytes	4	216 bytes	7	402 bytes
192.168.0.101	1570	20	1 kB	6	324 bytes	14	816 bytes
192.168.0.101	1573	149	80 kB	68	69 kB	81	11 kB
192.168.0.101	1574	20	9 kB	9	1 kB	11	8 kB
192.168.0.101	1575	20	4 kB	10	1 kB	10	3 kB
192.168.0.101	1576	26	13 kB	13	1 kB	13	11 kB
192.168.0.101	1577	25	13 kB	12	1 kB	13	11 kB
192.168.0.101	1578	20	6 kB	10	3 kB	10	3 kB
192.168.0.101	1579	115	59 kB	55	47 kB	60	12 kB
192.168.0.101	1580	25	5 kB	15	2 kB	10	4 kB
192.168.0.101	1581	25	15 kB	15	9 kB	10	6 kB
192.168.0.101	1582	32	16 kB	16	9 kB	16	8 kB
192.168.0.101	1583	14	8 kB	6	1 kB	8	7 kB

The common port numbers used by the TCP protocol is 443.

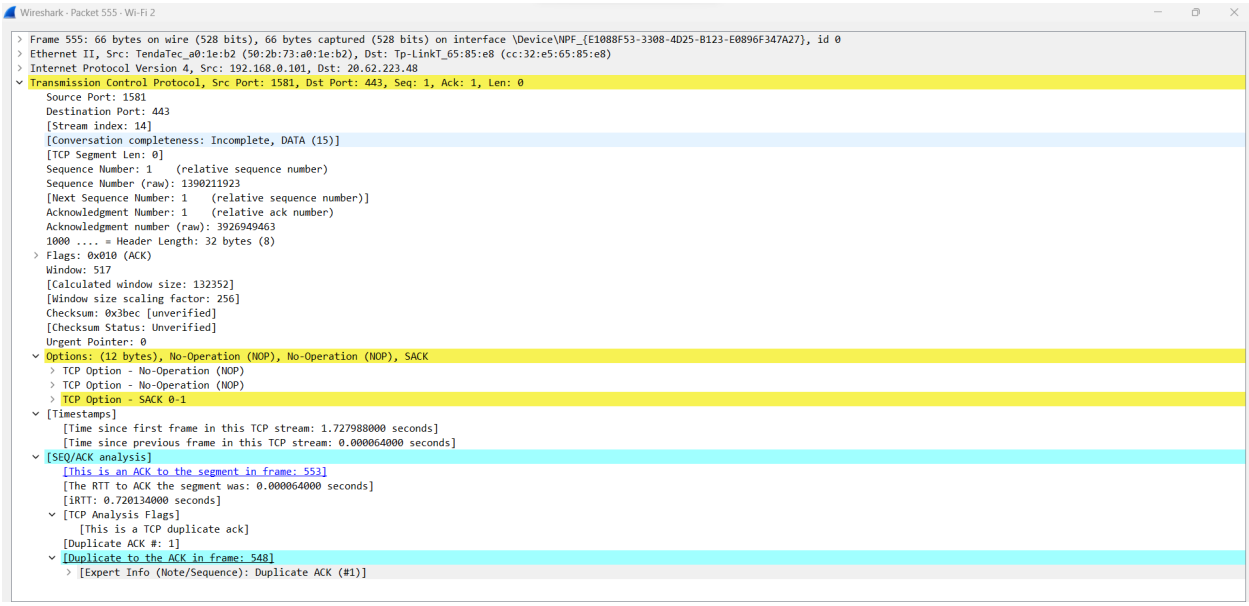
c)

```
Wireshark · Packet 553 · Wi-Fi 2
> Frame 553: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{E1088F53-3308-4D25-B123-E0896F347A27}, id 0
> Ethernet II, Src: Tp-LinkT_65:85:e8 (cc:32:e5:65:85:e8), Dst: TendaTec_a0:1e:b2 (50:2b:73:a0:1e:b2)
> Internet Protocol Version 4, Src: 20.62.223.48, Dst: 192.168.0.101
v Transmission Control Protocol, Src Port: 443, Dst Port: 1581, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 1581
    [Stream index: 14]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3926949462
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1390211923
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x0929 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  v Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
    > TCP Option - Maximum segment size: 1440 bytes
    > TCP Option - No-Operation (NOP)
    > TCP Option - No-Operation (NOP)
    > TCP Option - SACK permitted
    > TCP Option - No-Operation (NOP)
    > TCP Option - Window scale: 7 (multiply by 128)
  v [Timestamps]
      [Time since first frame in this TCP stream: 1.727924000 seconds]
      [Time since previous frame in this TCP stream: 0.008148000 seconds]
  v [SEQ/ACK analysis]
      [iRTT: 0.720134000 seconds]
    v [TCP Analysis Flags]
      > [Expert Info (Note/Sequence): This frame is a (suspected) retransmission]
        [The RTO for this segment was: 0.008322000 seconds]
        [RTO based on delta from frame: 545]
```

Packet 553 is a SYN-ACK packet in a TCP communication. It originates from source IP 20.62.223.48 on port 443 and is destined for IP 192.168.0.101 on port 1581. The sequence number is set to 0 (relative), and the acknowledgment number is 1. The packet bears the flags 0*012, indicating both SYN and ACK. This packet signifies the response to a connection initiation request. It acknowledges the receipt of a SYN packet, confirms its readiness to establish a connection, and offers its sequence number for data transmission.

```
Wireshark · Packet 554 · Wi-Fi 2
> Frame 554: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{E1088F53-3308-4D25-B123-E0896F347A27}, id 0
> Ethernet II, Src: Tp-LinkT_65:85:e8 (cc:32:e5:65:85:e8), Dst: TendaTec_a0:1e:b2 (50:2b:73:a0:1e:b2)
> Internet Protocol Version 4, Src: 51.104.167.186, Dst: 192.168.0.101
v Transmission Control Protocol, Src Port: 443, Dst Port: 1580, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 1580
    [Stream index: 13]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1575930513
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 245205698
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0x091e [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  v Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    > TCP Option - Maximum segment size: 1440 bytes
    > TCP Option - No-Operation (NOP)
    > TCP Option - Window scale: 8 (multiply by 256)
    > TCP Option - No-Operation (NOP)
    > TCP Option - No-Operation (NOP)
    > TCP Option - SACK permitted
  v [Timestamps]
      [Time since first frame in this TCP stream: 3.660981000 seconds]
      [Time since previous frame in this TCP stream: 0.060871000 seconds]
  v [SEQ/ACK analysis]
      [iRTT: 0.951080000 seconds]
    v [TCP Analysis Flags]
      > [Expert Info (Note/Sequence): This frame is a (suspected) retransmission]
        [The RTO for this segment was: 0.062862000 seconds]
        [RTO based on delta from frame: 520]
```

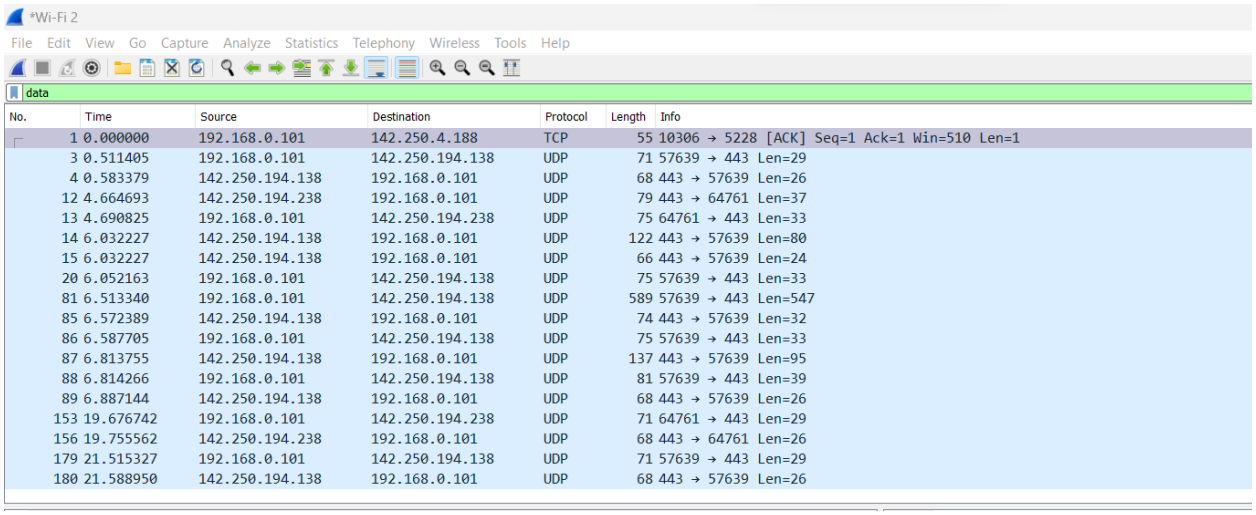
Packet 554 represents a TCP connection initiation from source IP 51.104.167.186 to destination IP 192.168.0.101. The source port 443 indicates an HTTPS connection, and the destination port 1580 designates a specific service. The packet carries a SYN-ACK flag combination, indicating a response to a previous SYN request. The Sequence Number is 0 (relative), and the Acknowledgment Number is 1, signifying that the sender acknowledges the initial SYN and is ready to establish the connection. The packet's significance lies in acknowledging the request to establish a connection and initiating the negotiation process for secure data exchange over HTTPS.



This packet, sent from source IP 192.168.0.101 to destination IP 20.62.223.48, signifies an acknowledgment in an established TCP connection. The sequence number indicates that this is the first data segment relative to the initial sequence number, and the acknowledgment number confirms that the sender has received data up to sequence number 1. The ACK flag (0x010) affirms the successful receipt of data. This packet's significance lies in its role within the ongoing data exchange, ensuring the reliable flow of information between the sender and the receiver over TCP.

Step 3:

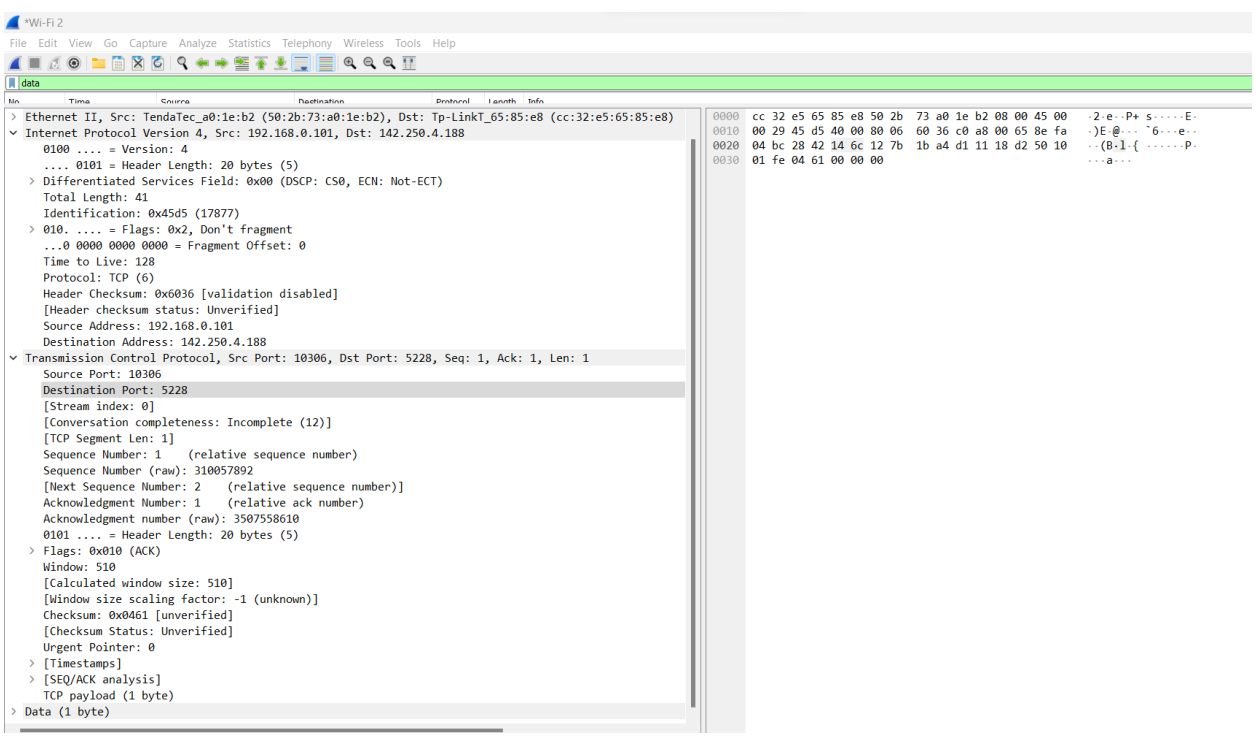
a)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.101	142.250.4.188	TCP	55	10306 → 5228 [ACK] Seq=1 Ack=1 Win=510 Len=1
3	0.511405	192.168.0.101	142.250.194.138	UDP	71	57639 → 443 Len=29
4	0.583379	142.250.194.138	192.168.0.101	UDP	68	443 → 57639 Len=26
12	4.664693	142.250.194.238	192.168.0.101	UDP	79	443 → 64761 Len=37
13	4.690825	192.168.0.101	142.250.194.238	UDP	75	64761 → 443 Len=33
14	6.032227	142.250.194.138	192.168.0.101	UDP	122	443 → 57639 Len=80
15	6.032227	142.250.194.138	192.168.0.101	UDP	66	443 → 57639 Len=24
20	6.052163	192.168.0.101	142.250.194.138	UDP	75	57639 → 443 Len=33
81	6.513340	192.168.0.101	142.250.194.138	UDP	589	57639 → 443 Len=547
85	6.572389	142.250.194.138	192.168.0.101	UDP	74	443 → 57639 Len=32
86	6.587705	192.168.0.101	142.250.194.138	UDP	75	57639 → 443 Len=33
87	6.813755	142.250.194.138	192.168.0.101	UDP	137	443 → 57639 Len=95
88	6.814266	192.168.0.101	142.250.194.138	UDP	81	57639 → 443 Len=39
89	6.887144	142.250.194.138	192.168.0.101	UDP	68	443 → 57639 Len=26
153	19.676742	192.168.0.101	142.250.194.238	UDP	71	64761 → 443 Len=29
156	19.755562	142.250.194.238	192.168.0.101	UDP	68	443 → 64761 Len=26
179	21.515327	192.168.0.101	142.250.194.138	UDP	71	57639 → 443 Len=29
180	21.588950	142.250.194.138	192.168.0.101	UDP	68	443 → 57639 Len=26

Yes, I observe unusual network traffic here.

b)



In this scenario, the anomaly originates from source IP 192.168.0.101 and targets destination IP 142.250.4.188. The packet has a length of 41 bytes and utilizes the TCP protocol. Notably, the sequence number is 1, the acknowledgement number is 1, and the flags indicate an ACKnowledgment (0x010). The TCP payload, albeit minimal at just 1 byte, contributes to this anomaly's distinctive characteristics.

c)

To further investigate anomalies, analyze packet payloads and network behavior for unusual patterns, leveraging intrusion detection systems and behavioral analysis tools. Implement segmentation, update firewalls, and collaborate with experts to validate findings. For mitigation, isolate affected systems, enact incident response plans, and share insights with stakeholders to enhance future security strategies.

—----------END OF THE DOCUMENT—----------