



United International University

**Assignment 01**

Submitted by:

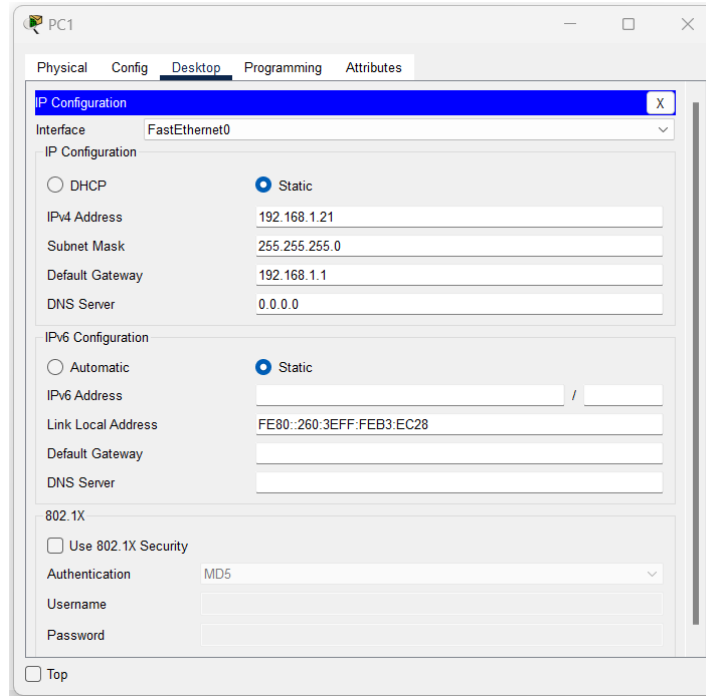
Azizul Islam Nayem (011201262)

Course Title: Computer Networks

Course Code: CSE 3711

Department of Computer Science &  
Engineering

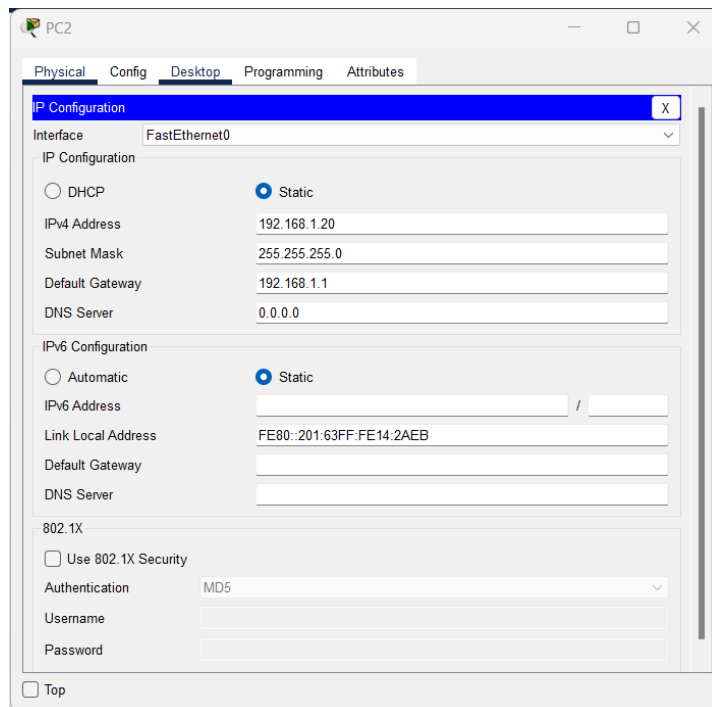
## Question 2



The screenshot shows the 'IP Configuration' window for PC1. The 'Interface' is set to 'FastEthernet0'. Under 'IP Configuration', 'Static' is selected. The IPv4 Address is 192.168.1.21, Subnet Mask is 255.255.255.0, Default Gateway is 192.168.1.1, and DNS Server is 0.0.0.0. Under 'IPv6 Configuration', 'Static' is selected. The IPv6 Address is empty, Link Local Address is FE80::260:3EFF:FEB3:EC28, Default Gateway is empty, and DNS Server is empty. Under '802.1X', 'Use 802.1X Security' is unchecked, Authentication is MD5, Username is empty, and Password is empty. A 'Top' button is at the bottom left.

Field	Value
Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.1.21
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0
IPv6 Configuration	
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	
Link Local Address	FE80::260:3EFF:FEB3:EC28
Default Gateway	
DNS Server	
802.1X	
<input type="checkbox"/> Use 802.1X Security	
Authentication	MD5
Username	
Password	

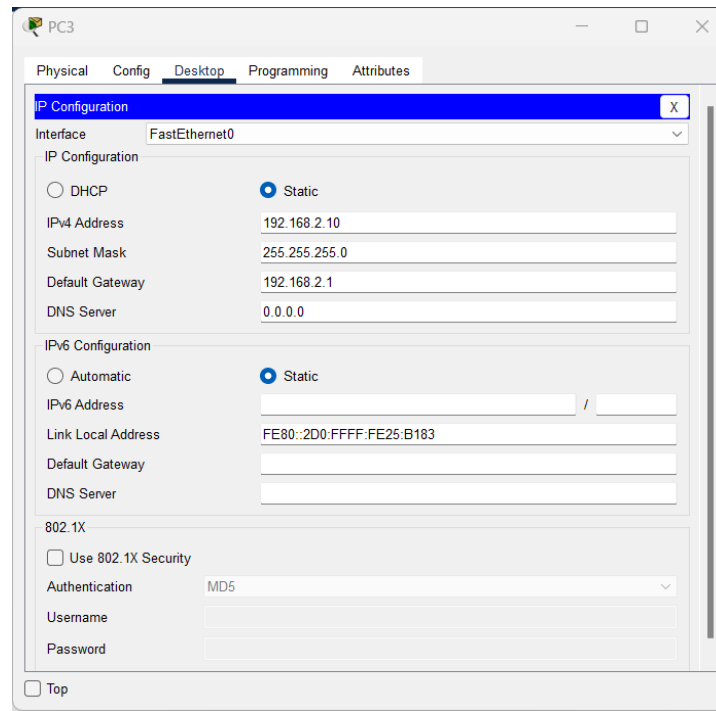
Ip configuration for PC1



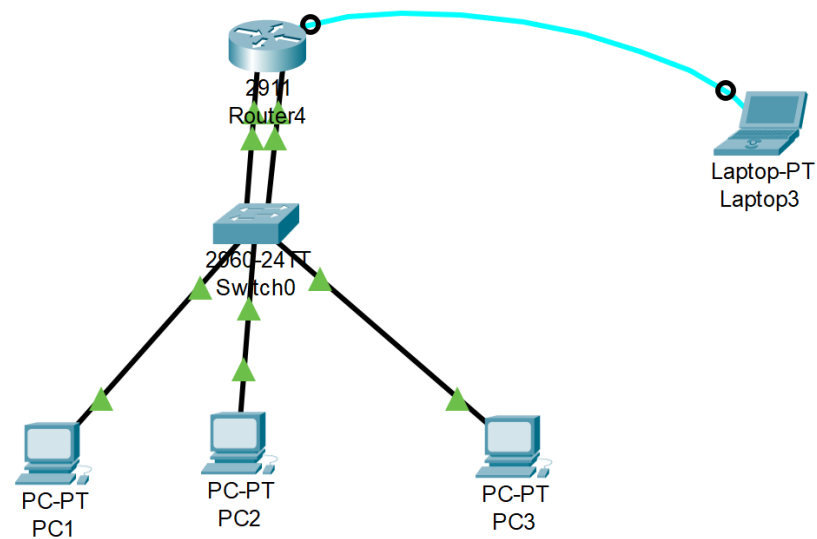
The screenshot shows the 'IP Configuration' window for PC2. The 'Interface' is set to 'FastEthernet0'. Under 'IP Configuration', 'Static' is selected. The IPv4 Address is 192.168.1.20, Subnet Mask is 255.255.255.0, Default Gateway is 192.168.1.1, and DNS Server is 0.0.0.0. Under 'IPv6 Configuration', 'Static' is selected. The IPv6 Address is empty, Link Local Address is FE80::201:63FF:FE14:2AEB, Default Gateway is empty, and DNS Server is empty. Under '802.1X', 'Use 802.1X Security' is unchecked, Authentication is MD5, Username is empty, and Password is empty. A 'Top' button is at the bottom left.

Field	Value
Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.1.20
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0
IPv6 Configuration	
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	
Link Local Address	FE80::201:63FF:FE14:2AEB
Default Gateway	
DNS Server	
802.1X	
<input type="checkbox"/> Use 802.1X Security	
Authentication	MD5
Username	
Password	

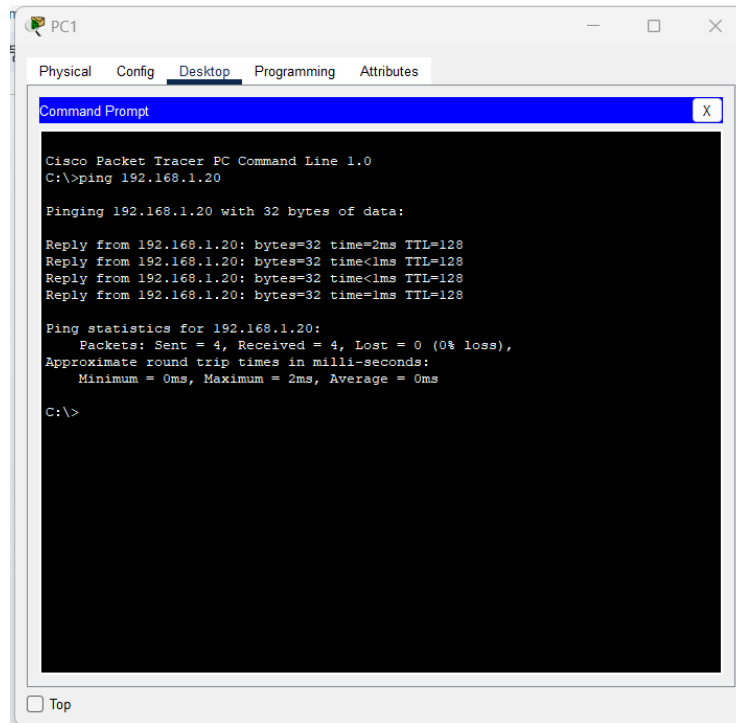
Ip configuration for PC2



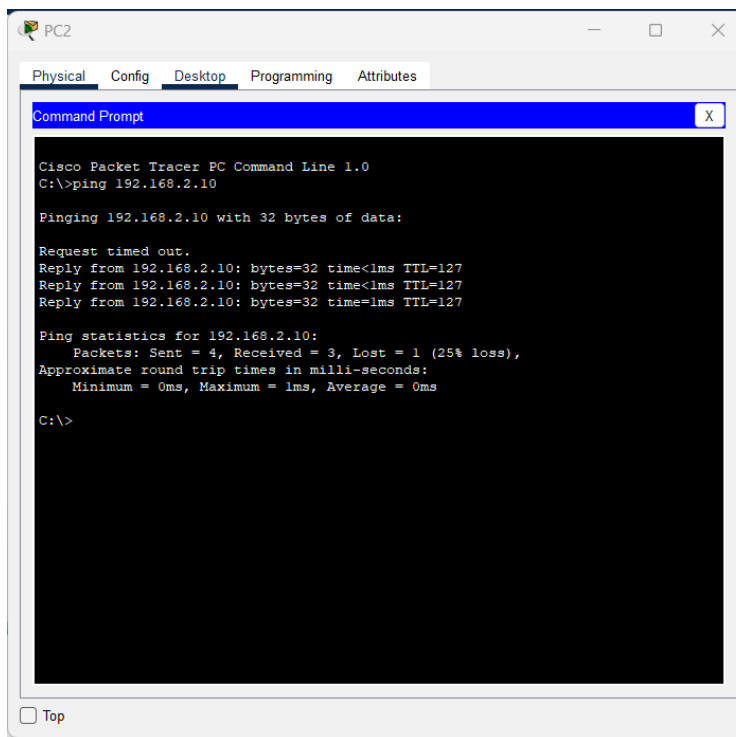
Ip configuration for PC3



Whole network configuration



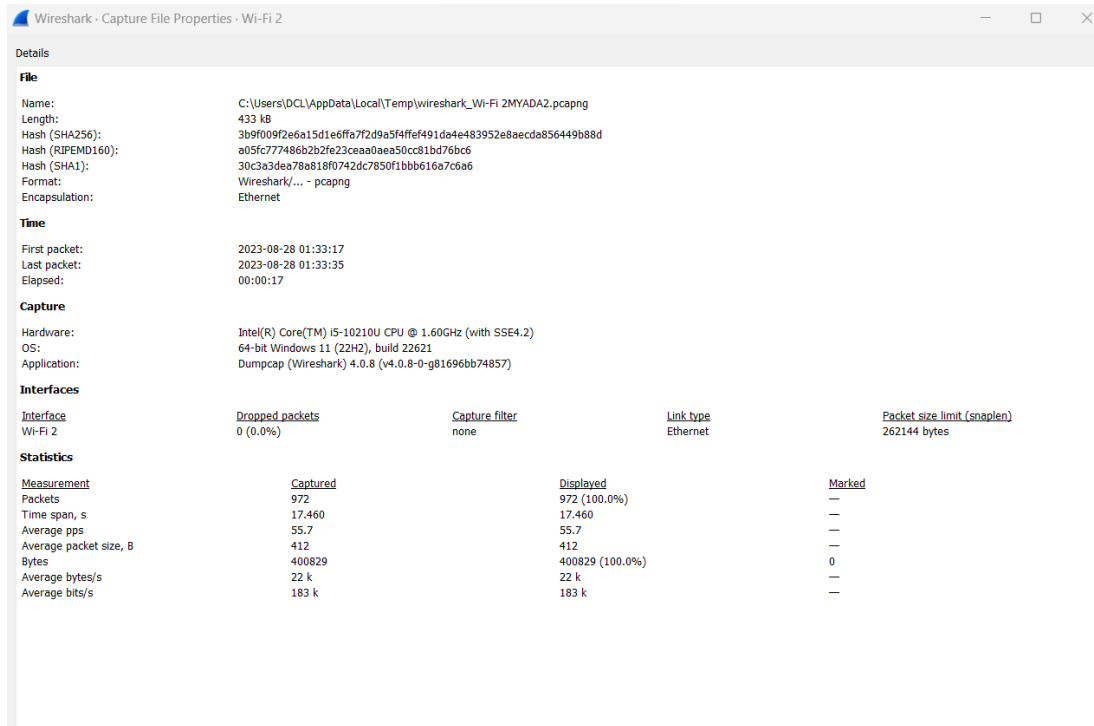
Verify connectivity between the computers by pinging PC2 from PC1



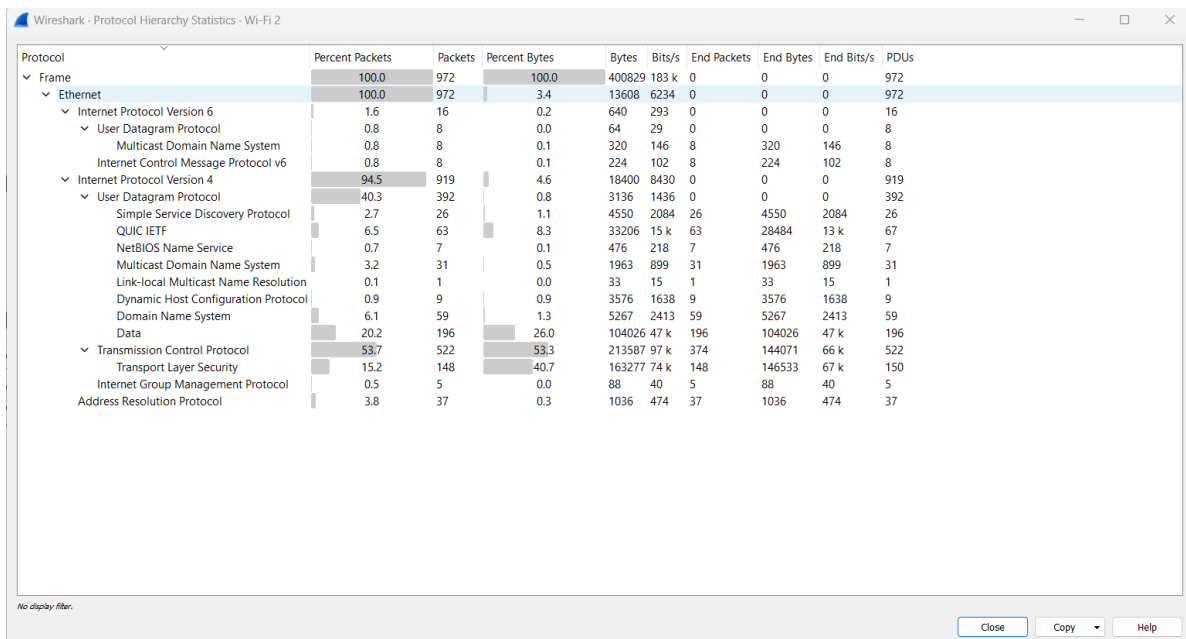
Verify connectivity between the computers by pinging PC3 from PC2

# Question 1

## Step 1:



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



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				
20.190.118.190	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.

```

> Frame 970: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{E1088F53-3308-4D25-B123-E0896F347A27}, id 0
> Ethernet II, Src: TendaTec_a0:1e:b2 (50:2b:73:a0:1e:b2), Dst: Tp-LinkT_65:85:e8 (cc:32:e5:65:85:e8)
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 20.62.223.48
< Transmission Control Protocol, Src Port: 1581, Dst Port: 443, Seq: 644, Ack: 5647, Len: 1440
  Source Port: 1581
  Destination Port: 443
  [Stream index: 14]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 1440]
  Sequence Number: 644 (relative sequence number)
  Sequence Number (raw): 1390212566
  [Next Sequence Number: 2084 (relative sequence number)]
  Acknowledgment Number: 5647 (relative ack number)
  Acknowledgment number (raw): 3926955109
  
```

1st network connection among top 5 connection based on length

```
Wireshark - Packet 964 - Wi-Fi 2

> Frame 964: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{E1088F53-3308-4D25-B123-E0896F347A27}, id 0
> Ethernet II, Src: TendaTec_a0:1e:b2 (50:2b:73:a0:1e:b2), Dst: Tp-LinkT_65:85:e8 (cc:32:e5:65:85:e8)
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 20.62.223.48
> Transmission Control Protocol, Src Port: 1581, Dst Port: 443, Seq: 5243, Ack: 5647, Len: 1440
  Source Port: 1581
  Destination Port: 443
  [Stream index: 14]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 1440]
  Sequence Number: 5243 (relative sequence number)
  Sequence Number (raw): 1390217165
  [Next Sequence Number: 6683 (relative sequence number)]
  Acknowledgment Number: 5647 (relative ack number)
  Acknowledgment number (raw): 3926955109

0020 df 30 06 2d 01 bb 52 dd 07 cd ea 10 94 65 50 10 .0---R. ....eP.
0030 02 05 ed d2 00 00 2c 4b e3 97 f0 2e dc d7 f9 8a .....K .....
0040 2b 6e 12 92 28 98 d7 27 6b 5b 87 f0 45 a5 b8 29 +-n-(-' k[...E...
0050 b4 30 01 29 18 8f 32 cd aa 44 66 6a 7e fd 5c d1 .0)-.2- Dfj-.\.
0060 d8 60 31 82 cc e8 c3 b9 66 fa 9e 0f 8f a4 52 86 ^1-----f-----R-
0070 ab b1 13 e4 2e 6c bf e3 51 6a 3f 41 10 b7 ef 31 .....l---Qj?A---1
0080 4a 8c d6 9d a3 c1 ac 77 1a 6d dd 4d 5d 03 c4 82 }-----w -m-M]---
0090 e6 0a 95 ee 4a 7e 24 3c 74 ee d7 5c 57 14 8f 8f ....D-$< t-.\W---
00a0 ca 34 f3 6f f1 aa e3 ee 95 f3 16 6a 0d a7 88 00 .4-o-----j-----
00b0 ae 29 9a 5d 2c 40 30 d1 19 96 ac 83 7a f0 d1 ef .)-,]@0-----z---
00c0 e6 03 f2 e5 c4 d4 12 6a 09 bf 53 70 a3 c4 9a db .....j-----Sp---
00d0 7d 52 4e a5 54 44 e7 d3 6b 4d a5 3c 31 6f 06 f9 }RN-TD...kM<1o...
00e0 4c 15 54 a3 7f bd 35 5a 96 13 62 7d ff be af bc L.T...5Z ..b]....
00f0 10 56 30 6e 62 d7 d7 37 4c 17 49 d9 09 7c 42 27 .\0nb...7 L-I...[B'
0100 75 29 03 2c ab 9b f2 05 de fe 7f 7a e9 8b 30 6d u),.....z---0m
0110 17 e5 12 64 b5 43 7c ec 66 1f 60 59 49 c7 ef 5c ...d-C]...f-`YI-.\
0120 6d d2 6a fd 1e e5 de ff 11 5e 87 81 fe 72 fc 78 m-j-----^-----r-x
0130 ca 35 7c b1 72 4d c2 1e 84 1f a0 27 65 60 92 48 .5]-rM-----'e'-H
```

## 2nd network connection among top 5 connection based on length

```
Wireshark - Packet 963 - Wi-Fi 2

> Frame 963: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{E1088F53-3308-4D25-B123-E0896F347A27}, id 0
> Ethernet II, Src: TendaTec_a0:1e:b2 (50:2b:73:a0:1e:b2), Dst: Tp-LinkT_65:85:e8 (cc:32:e5:65:85:e8)
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 20.62.223.48
> Transmission Control Protocol, Src Port: 1581, Dst Port: 443, Seq: 3803, Ack: 5647, Len: 1440
  Source Port: 1581
  Destination Port: 443
  [Stream index: 14]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 1440]
  Sequence Number: 3803 (relative sequence number)
  Sequence Number (raw): 1390215725
  [Next Sequence Number: 5243 (relative sequence number)]
  Acknowledgment Number: 5647 (relative ack number)
  Acknowledgment number (raw): 3926955109

0020 df 30 06 2d 01 bb 52 dd 02 2d ea 10 94 65 50 10 .0---R. ....eP.
0030 02 05 3b 26 00 00 83 e7 fa 88 3e ee e2 d0 d2 41 .;8;....>....A
0040 fc 68 24 2c d3 c0 31 34 ef df 2a df 89 f2 40 35 .h$,..14 ..*...@5
0050 e5 b2 7a 8a 50 e6 69 1d fa bc 84 a9 2f 2c da 6f .-z-P-i-...-/..o
0060 51 e2 ab ce 4d 63 66 ee cc 23 3d b6 8e 99 11 3f Q...Mc f-#=-...?
0070 70 ac a7 38 f8 c7 c8 9d 38 d1 74 e8 45 2c bf 0e p-8...-8-t:E,-?
0080 c7 bd 89 d8 22 3a 35 5f 7d a0 ac 93 44 01 3d 79 .....5_ }...D=y
0090 d4 75 c8 8e 3d fc 48 01 c0 70 3b c8 1f 87 1b c0 .u-=-H- p;-...
00a0 de 64 66 46 b0 cd 7b 2e d7 3e a5 b9 77 8b c1 99 .dff-{-.->-w-...
00b0 e8 17 e0 0d bf 0a 6f 21 c4 bd 99 4e db 7f 3b ee .....ol-...N-;-
00c0 73 98 23 aa 69 5b 8e 18 ec 15 d2 16 32 98 25 81 s#-i[-...-2-%-
00d0 34 db e4 fc 16 71 22 7a 56 a7 8c 1f 58 e6 5e d0 4...q"z V-.-X^.-
00e0 b8 11 9a 4e 60 0b 19 af e2 90 eb 60 d6 44 b1 2a ...N"-...-D-*
00f0 3d de 35 20 bf ea fa 9e cc 46 5b a4 4b f6 d3 75 =5 .....-F[-K-..u
0100 0e c3 b8 34 4c 02 d7 3f 38 fe 87 97 d4 d8 df 15 ...4L...? 8-.....
0110 d3 39 82 93 72 ff 72 f3 a0 da be b1 2f ab e0 57 .9-.-r-.-/-W
0120 1f 56 65 52 e8 16 63 fd 49 f2 28 fd fc 74 19 a6 .Ver-.-c- I-(-t-..
0130 c6 f2 ad 71 ef 7b 5a 24 2c c6 76 34 c4 96 51 1b ...q-{Z$, -v4-Q-
```

## 3rd network connection among top 5 connection based on length

```
Wireshark - Packet 962 - Wi-Fi 2

> Frame 962: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{E1088F53-3308-4D25-B123-E0896F347A27}, id 0
> Ethernet II, Src: TendaTec_a0:1e:b2 (50:2b:73:a0:1e:b2), Dst: Tp-LinkT_65:85:e8 (cc:32:e5:65:85:e8)
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 20.62.223.48
> Transmission Control Protocol, Src Port: 1581, Dst Port: 443, Seq: 2363, Ack: 5647, Len: 1440
  Source Port: 1581
  Destination Port: 443
  [Stream index: 14]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 1440]
  Sequence Number: 2363 (relative sequence number)
  Sequence Number (raw): 1390214285
  [Next Sequence Number: 3803 (relative sequence number)]
  Acknowledgment Number: 5647 (relative ack number)
  Acknowledgment number (raw): 3926955109

0020 d f 30 06 2d 01 bb 52 dc f6 8d ea 10 94 65 50 10 .0---R- .....eP.
0030 02 05 f7 a6 00 00 d8 53 48 43 17 41 91 1a e3 f2 .....S HC A---
0040 03 0b d3 f3 38 bb ee 21 42 b8 db 18 f2 77 c2 63 ---8--! B---w-c
0050 db d4 7e cf 16 a2 27 f0 7f 85 81 39 fe fc 75 d8 ---w---'---9---u-
0060 ad de 7c be 1f e7 aa e2 2b cb eb 43 7a 02 20 a3 -[]-----+--Cz---
0070 51 f1 2e de d2 ef 22 61 7c 49 8a 43 6c fa 1c 18 Q-----"a [I C1---
0080 92 48 a2 95 8e 29 fc ea 55 c6 09 46 cd 32 a7 46 -H---)---U---F-2-F
0090 f3 33 52 b9 9e 33 1c 46 03 9f bf 2b bc 59 f0 1a -3R--3-F---+Y---
00a0 ec 35 3f a1 03 9d 51 0f 50 ee aa 99 30 84 8a 66 -5?---Q- P---0---f
00b0 fb ec 6d ec de 78 29 19 0b d3 53 e6 e3 54 47 5e --m-x)---S---TG^
00c0 87 7c 2a 9e bc 08 89 94 aa 92 d1 e4 33 e3 bd 05 -[]*-----3---
00d0 3e 96 28 b9 b0 8f 48 18 fb c4 c0 b2 18 fe 9f bc >(-...H-.....
00e0 f3 04 c3 38 a1 0e 54 b5 3a af fe 1f 7a 05 65 b5 --8---T---:---z-e-
00f0 4b 66 05 7c fc 63 49 28 5e 9e 42 e5 a7 f6 27 b1 Kf-[]-cI( ^B---'
0100 7e 99 f2 1e 80 44 34 27 78 73 35 1f 38 f2 c4 c0 ~---D4' xs5-8---
0110 64 b4 20 a0 a5 a4 47 c2 d1 7b ec 81 ed 10 bc f7 d---G---{-----
0120 5b 70 7f 99 0a e7 bc 41 cc 67 71 a5 6b 9c 46 bd [p-----A gq-k-F-
0130 47 5b 3e 6a a3 12 f3 3d 2f 9c 2a 18 f6 3c d8 1b G[>j---= /-*-<-<---
```

#### 4th network connection among top 5 connection based on length

```
Wireshark - Packet 961 - Wi-Fi 2

> Frame 961: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{E1088F53-3308-4D25-B123-E0896F347A27}, id 0
> Ethernet II, Src: TendaTec_a0:1e:b2 (50:2b:73:a0:1e:b2), Dst: Tp-LinkT_65:85:e8 (cc:32:e5:65:85:e8)
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 20.62.223.48
> Transmission Control Protocol, Src Port: 1581, Dst Port: 443, Seq: 923, Ack: 5647, Len: 1440
  Source Port: 1581
  Destination Port: 443
  [Stream index: 14]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 1440]
  Sequence Number: 923 (relative sequence number)
  Sequence Number (raw): 1390212845
  [Next Sequence Number: 2363 (relative sequence number)]
  Acknowledgment Number: 5647 (relative ack number)
  Acknowledgment number (raw): 3926955109

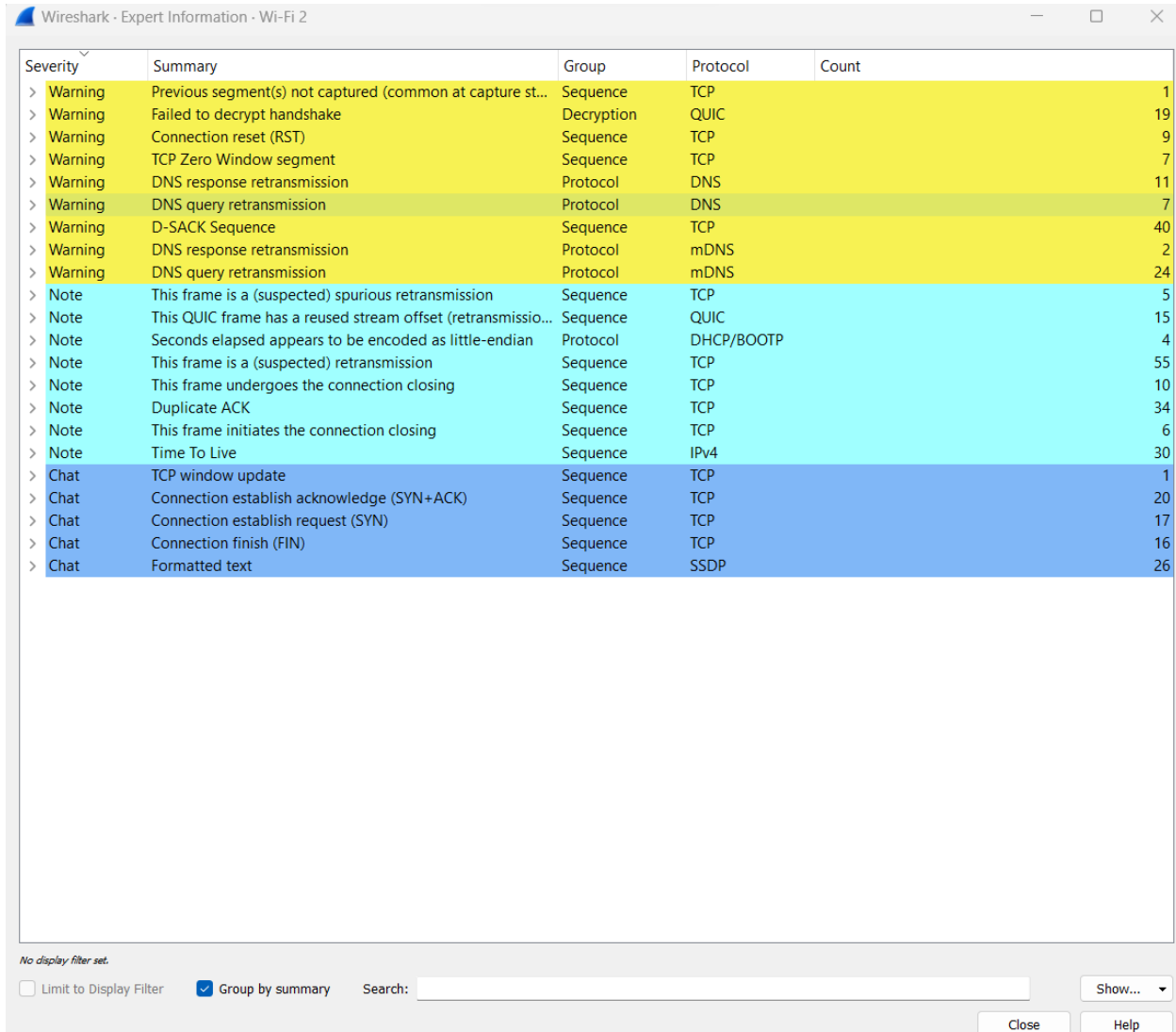
0020 d f 30 06 2d 01 bb 52 dc f6 8d ea 10 94 65 50 10 .0---R- .....eP.
0030 02 05 1b 7a 00 00 17 03 03 2a fa 16 53 f9 3b 95 ...Z---*---S-;-
0040 07 7b c1 c3 67 ce ba 14 e2 16 01 f3 e5 44 fb 08 -{-g-----D--
0050 56 cb 33 5c ed 8e f6 a7 91 69 01 44 60 c6 42 d2 V-3\----i-D'-B-
0060 18 68 9f 47 99 ad 17 b3 4d 31 89 bf 5f ce 59 ff -h-G-----M1---Y-
0070 5c d0 4b 22 2d ff be f2 f8 80 95 5d 0f 08 3f 67 \-K'-----]-?g
0080 91 07 6d 7b 17 a1 8f 66 0b 43 6c cf 2f 04 37 42 -m{---f-C1-/7B
0090 93 46 56 c8 c6 dd ed c4 f2 00 12 ed 3b 7c 68 3f -FV-----;|h?
00a0 df a3 8d 39 b0 85 49 1e 69 7b cc 1d 73 af 98 e6 ---9---I- i{--s---
00b0 eb d5 1e ae bf 47 05 20 8b ae 81 b4 83 be 78 c7 -----G-----x-
00c0 29 44 bb 69 f2 e5 78 be 01 c5 2b 28 81 7b 9e 1f )D-i--x---+(-{-
00d0 b4 68 b0 43 28 27 ec 89 0f 89 8a b3 04 ab 7e ab -h-C('-----
00e0 66 a9 da f6 99 17 b8 01 14 2f ff 16 12 f2 6f b7 f-----/----o-
00f0 a1 e3 ec b6 31 16 14 95 69 09 d1 86 57 de 9c 0d ----1---i--W---
0100 03 9e 81 09 5a 6b c0 b6 c8 89 72 68 a0 97 f5 95 ---Zk-----rh---
0110 c9 43 f8 2e fa 17 c6 08 31 3b 98 1b 82 07 24 b7 -C-----1;---$-
0120 2d 4c 5b fd 12 2e f8 16 c6 ac e2 92 3b 00 0f c9 -L[-----;---
0130 66 52 ed 2b 52 f0 2c 93 7d 34 12 22 0c ae b0 93 fR+R,--.4"----
```

#### 5th network connection among top 5 connection based on length



## Step 2:

a)



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)

Wireshark · Endpoints · Wi-Fi 2

Endpoint Settings

☐ Name resolution

☐ Limit to display filter

Copy

Map

Protocol

☐ JXTA

☐ MPTCP

☐ NCP

☐ openSAFETY

☐ RSVP

☐ SCTP

☐ SLL

☒ TCP

☐ Token-Ring

☐ UDP

☐ USB

☐ ZigBee

Filter list for specific type

Bluetooth	DCCP	Ethernet · 9	FC	FDDI	IEEE 802.11	IEEE 802.15.4	TCP · 27
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

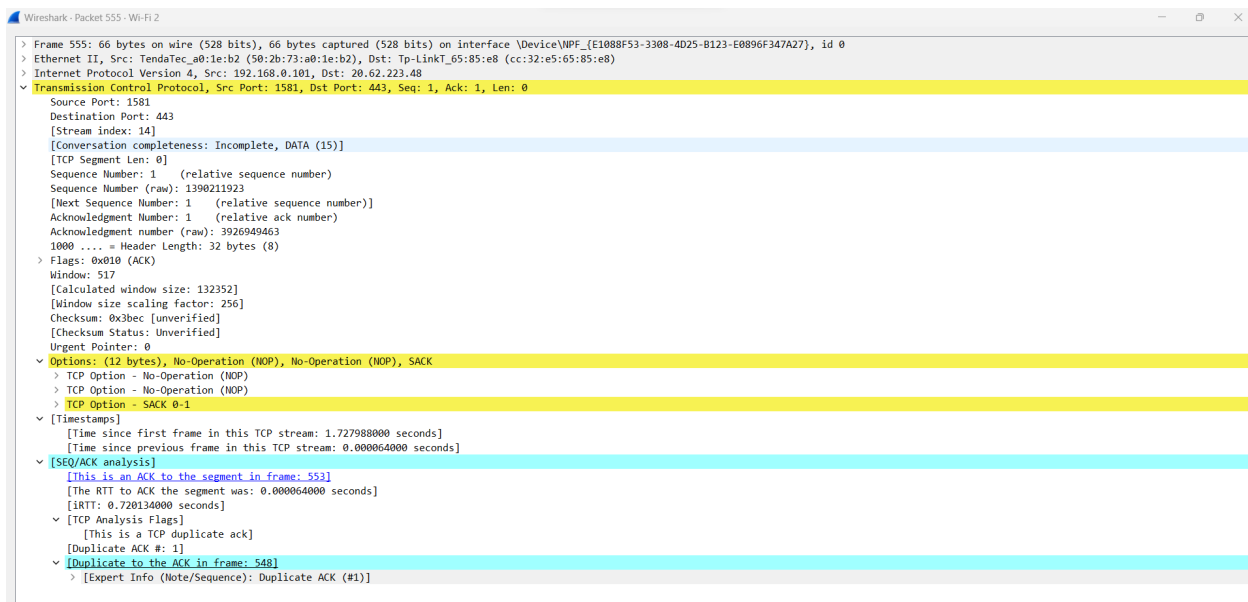
```
> Frame 553: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{E1088F53-3308-4D25-B123-E0896F347A27}, id 0
> Ethernet II, Src: Tp-LinkT_65:85:e8 (cc:32:e5:65:85:e8), Dst: TendaTec_a0:1e:b2 (50:2b:73:a0:1e:b2)
> Internet Protocol Version 4, Src: 20.62.223.48, Dst: 192.168.0.101
> 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
  > 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)
  > [Timestamps]
    [Time since first frame in this TCP stream: 1.727924000 seconds]
    [Time since previous frame in this TCP stream: 0.008148000 seconds]
  > [SEQ/ACK analysis]
    [IRTT: 0.720134000 seconds]
    > [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
> 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
  > 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
  > [Timestamps]
    [Time since first frame in this TCP stream: 3.660981000 seconds]
    [Time since previous frame in this TCP stream: 0.060871000 seconds]
  > [SEQ/ACK analysis]
    [IRTT: 0.951080000 seconds]
    > [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)

*Wi-Fi 2						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
data						
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)

*Wi-Fi 2						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
data						
No.	Time	Source	Destination	Protocol	Length	Info
Ethernet II, Src: TendaTec_a0:1e:b2 (50:2b:73:a0:1e:b2), Dst: Tp-LinkT_65:85:e8 (cc:32:e5:65:85:e8)						
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 142.250.4.188						
0100 .... = Version: 4						
... 0101 = Header Length: 20 bytes (5)						
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 41						
Identification: 0x45d5 (17877)						
010. .... = Flags: 0x2, Don't fragment						
...0 0000 0000 0000 = Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
Header Checksum: 0x6036 [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 192.168.0.101						
Destination Address: 142.250.4.188						
Transmission Control Protocol, Src Port: 10306, Dst Port: 5228, Seq: 1, Ack: 1, Len: 1						
Source Port: 10306						
Destination Port: 5228						
[Stream index: 0]						
[Conversation completeness: Incomplete (12)]						
[TCP Segment Len: 1]						
Sequence Number: 1 (relative sequence number)						
Sequence Number (raw): 310057892						
[Next Sequence Number: 2 (relative sequence number)]						
Acknowledgment Number: 1 (relative ack number)						
Acknowledgment number (raw): 3507558610						
0101 .... = Header Length: 20 bytes (5)						
Flags: 0x010 (ACK)						
Window: 510						
[Calculated window size: 510]						
[Window size scaling factor: -1 (unknown)]						
Checksum: 0x8461 [unverified]						
[Checksum Status: Unverified]						
Urgent Pointer: 0						
[Timestamps]						
[SEQ/ACK analysis]						
TCP payload (1 byte)						
Data (1 byte)						
0000	cc 32 e5 65 85 e8 50 2b 73 a0 1e b2 08 00 45 00	.2.e..P+s.....E..				
0010	00 29 45 d5 40 00 80 06 60 36 c0 a8 00 65 8e fa	.)E@...`6....e..				
0020	04 bc 28 42 14 6c 12 7b 1b a4 d1 11 18 d2 50 10	..(B.l.( .....P..				
0030	01 fe 04 61 00 00 00	...a...				

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-----