

MD .ARAFAT ISLAM

IT-17008

Course Code : ICT-3208

Ping information & captured packet: ping 8.8.8.8 in powershell

Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

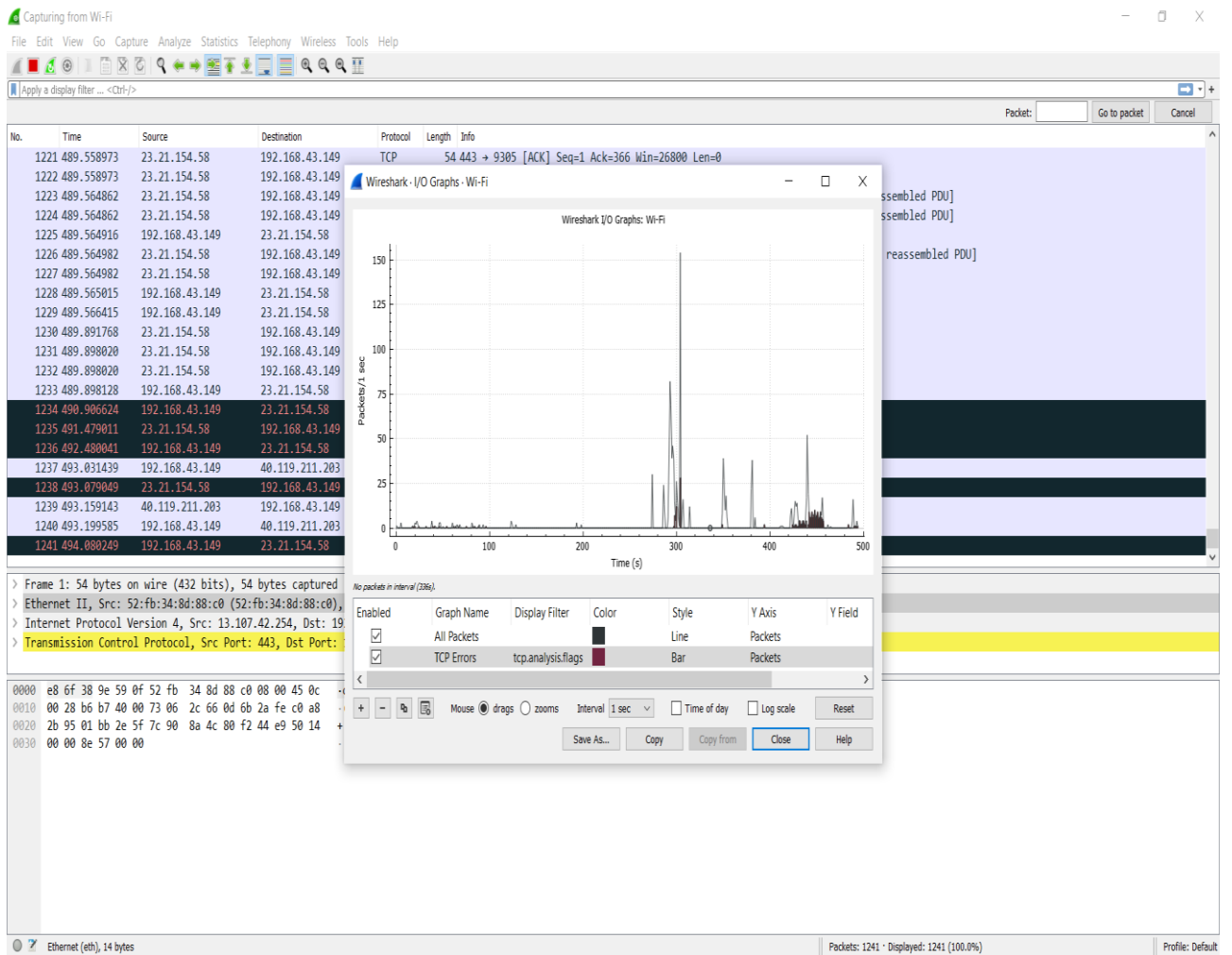
Try the new cross-platform PowerShell <https://aka.ms/pscore6>

PS C:\windows\system32> ping 255.255.255.255
Ping request could not find host 255.255.255.255. Please check the name and try again.
PS C:\windows\system32> ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=262ms TTL=112
Reply from 8.8.8.8: bytes=32 time=55ms TTL=112
Reply from 8.8.8.8: bytes=32 time=55ms TTL=112
Reply from 8.8.8.8: bytes=32 time=66ms TTL=112

Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 55ms, Maximum = 262ms, Average = 109ms
PS C:\windows\system32>

1	192.168.43.149	13.107.4.254	TCP	54 6208 → 443 [ACK] Seq=452
1	192.168.43.149	13.107.4.254	TLSv1.2	92 Application Data
5	13.107.4.254	192.168.43.149	TCP	92 [TCP Retransmission] 443
5	13.107.4.254	192.168.43.149	TLSv1.2	544 Application Data
5	13.107.4.254	192.168.43.149	TLSv1.2	230 Application Data
5	13.107.4.254	192.168.43.149	TLSv1.2	92 Application Data
5	13.107.4.254	192.168.43.149	TLSv1.2	92 Application Data
0	192.168.43.149	13.107.4.254	TCP	54 6206 → 443 [ACK] Seq=674
2	192.168.43.149	13.107.4.254	TLSv1.2	92 Application Data
8	13.107.4.254	192.168.43.149	TCP	54 443 → 6206 [ACK] Seq=117
5	13.107.4.254	192.168.43.149	TCP	54 [TCP Previous segment no
5	13.107.4.254	192.168.43.149	TCP	92 [TCP Retransmission] 443
1	192.168.43.149	13.107.4.254	TCP	54 6208 → 443 [ACK] Seq=490
83	192.168.43.149	8.8.8.8	ICMP	74 Echo (ping) request id=
27	8.8.8.8	192.168.43.149	ICMP	74 Echo (ping) reply id=
19	192.168.43.149	8.8.8.8	ICMP	74 Echo (ping) request id=
46	8.8.8.8	192.168.43.149	ICMP	74 Echo (ping) reply id=
05	192.168.43.149	8.8.8.8	ICMP	74 Echo (ping) request id=
02	8.8.8.8	192.168.43.149	ICMP	74 Echo (ping) reply id=
82	192.168.43.149	40.90.189.152	TLSv1.2	153 Application Data
97	40.90.189.152	192.168.43.149	TLSv1.2	223 Application Data
50	192.168.43.149	40.90.189.152	TCP	54 1887 → 443 [ACK] Seq=100
95	192.168.43.149	8.8.8.8	ICMP	74 Echo (ping) request id=
49	8.8.8.8	192.168.43.149	ICMP	74 Echo (ping) reply id=
12	Chongqin_9e:59:0f	52:fb:34:8d:88:c0	ARP	42 Who has 192.168.43.174?
67	52:fb:34:8d:88:c0	Chongqin_9e:59:0f	ARP	42 192.168.43.174 is at 52:



The protocol information :

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl>

No.	Time	Source	Destination	Protocol	Length	Info
297	113.111546	8.8.8.8	192.168.43.149	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=112 (request in 296)
298	114.061105	192.168.43.149	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 299)
299	114.116402	8.8.8.8	192.168.43.149	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=112 (request in 298)
300	114.716382	192.168.43.149	40.90.189.152	TLSv1.2	153	Application Data
301	114.817397	40.90.189.152	192.168.43.149	TLSv1.2	223	Application Data
302	114.857550	192.168.43.149	40.90.189.152	TCP	54	1887 → 443 [ACK] Seq=100 Ack=170 Win=251 Len=0
303	115.065595	192.168.43.149	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (reply in 304)
304	115.132149	8.8.8.8	192.168.43.149	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=112 (request in 303)
305	116.567012	Chongqin_9e:59:0f	52:fb:34:8d:88:c0	ARP	42	Who has 192.168.43.174? Tell 192.168.43.149
306	116.706767	52:fb:34:8d:88:c0	Chongqin_9e:59:0f	ARP	42	192.168.43.174 is at 52:fb:34:8d:88:c0
307	130.578272	23.23.176.28	192.168.43.149	TLSv1.2	85	Application Data
308	130.578788	192.168.43.149	23.23.176.28	TLSv1.2	89	Application Data
309	131.040023	23.23.176.28	192.168.43.149	TCP	54	443 → 6152 [ACK] Seq=94 Ack=106 Win=266 Len=0
310	142.921723	52:fb:34:8d:88:c0	Chongqin_9e:59:0f	ARP	42	Who has 192.168.43.149? Tell 192.168.43.174
311	142.921747	Chongqin_9e:59:0f	52:fb:34:8d:88:c0	ARP	42	192.168.43.149 is at e8:6f:38:9e:59:0f
312	157.600714	192.168.43.149	192.168.43.255	NBNS	92	Name query NB LAPTOP-HUA55H06<1c>
313	158.350700	192.168.43.149	192.168.43.255	NBNS	92	Name query NB LAPTOP-HUA55H06<1c>
314	159.101135	192.168.43.149	192.168.43.255	NBNS	92	Name query NB LAPTOP-HUA55H06<1c>
315	190.497508	23.23.176.28	192.168.43.149	TLSv1.2	85	Application Data
316	190.498472	192.168.43.149	23.23.176.28	TLSv1.2	89	Application Data

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{21180162-8CC1-44A6-98AE-3A3176C8B304}, id 0

> Ethernet II, Src: Chongqin_9e:59:0f (e8:6f:38:9e:59:0f), Dst: 52:fb:34:8d:88:c0 (52:fb:34:8d:88:c0)

> Internet Protocol Version 4, Src: 192.168.43.149, Dst: 117.18.237.29

▼ Transmission Control Protocol, Src Port: 6207, Dst Port: 80, Seq: 0, Len: 0

Source Port: 6207

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

Sequence number (raw): 2889874799

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 0

Acknowledgment number (raw): 0

1000 = Header Length: 32 bytes (8)

```
0000 52 fb 34 8d 88 c0 e8 6f 38 9e 59 0f 08 00 45 00  R 4 ... 8 Y ... E .
0010 00 34 f2 34 40 00 80 06 ba 21 c0 a8 2b 95 75 12  .4 .@ ... .! .+ u .
0020 ed 1d 18 3f 00 50 ac 3f fd 6f 00 00 00 00 00 02  ...? .P ? .o .....
0030 fa f0 63 73 00 00 02 04 05 b4 01 03 03 08 01 01  ..CS .....
0040 04 02 ..
```

Transmission Control Protocol (tcp), 32 bytes

Packets: 376 • Displayed: 376 (100.0%)

Profile: Default

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



Apply a display filter <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1328	541.745119	52.158.208.111	192.168.43.149	TCP	66	443 → 9306 [FIN, ACK] Seq=4484 Ack=5824 Win=261888 Len=0 TSval=1073507752 TSecr=5459024
1329	541.745156	192.168.43.149	52.158.208.111	TCP	66	9306 → 443 [ACK] Seq=5824 Ack=4485 Win=65536 Len=0 TSval=5459370 TSecr=1073507752
1330	544.115195	192.168.43.149	172.217.163.170	TCP	54	9307 → 443 [FIN, ACK] Seq=1736 Ack=8705 Win=65536 Len=0
1331	544.240252	172.217.163.170	192.168.43.149	TCP	54	443 → 9307 [FIN, ACK] Seq=8705 Ack=1737 Win=64000 Len=0
1332	544.240338	192.168.43.149	172.217.163.170	TCP	54	9307 → 443 [ACK] Seq=1737 Ack=8706 Win=65536 Len=0

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{2118D162-8CC1-44A6-98AE-3A3176C8B3D4}, id 0

> Ethernet II, Src: 52:fb:34:8d:88:c0 (52:fb:34:8d:88:c0), Dst: Chongqin_9e:59:0f (e8:6f:38:9e:59:0f)

> Internet Protocol Version 4, Src: 13.107.42.254, Dst: 192.168.43.149

▼ Transmission Control Protocol, Src Port: 443, Dst Port: 11871, Seq: 1, Ack: 1, Len: 0

Source Port: 443

Destination Port: 11871

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 2089847372

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 2163361001

0101 = Header Length: 20 bytes (5)

> Flags: 0x014 (RST, ACK)

Window size value: 0

[Calculated window size: 0]

[Window size scaling factor: -1 (unknown)]

Checksum: 0x8e57 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

> [Timestamps]

Port Security Hashing Algorithm:

0030	00 3e 91 f2 00 00 26 ca 79 60 65 b3 35 d0 4c 4e	·>·-·-·&· y`e·5·LN
0040	e1 22 1b 71 b5 c3 40 9b 24 82 82 92 3d 51 3c ea	·"·q·-·@· \$·-·-·=Q<·
0050	44 4a 06 f5 b2 03 53 92 c7 dd 8e 34 39 82 22 26	DJ·-·-·S· -·-·49·"&
0060	23 85 17 a0 81 01 bc 00 6b b0 d4 70 3b 7b 71 61	#·-·-·-·-· k·-·p;{qa
0070	c0 b1 6a a0 1a 1e c1 71 95 dc 4e 54 0f 22 d0 80	·-·j·-·-·q ·-·NT·"-·
0080	bd ab b9 b5 d7 5d b4 81 f1 ac 13 44 c0 c3 19 e8	·-·-·-·]·-· -·-·D·-·-·
0090	49 c1 59 94 0f 0e 0d d4 d9 a3 f8 23 5f a3 0f 9c	I·Y·-·-·-· -·-·#_·-·-·
00a0	63 0b 57 65 f4 55 34 7d 98 0a 21 e2 13 d5 aa 81	c·We·U4} ·-·!·-·-·-·
00b0	ea 05 78 1d ee a2 91 6e 61 63 27 49 b2 1f 9e 96	·-·x·-·-·-·n ac'I·-·-·
00c0	71 6f 52 bb 80 bc e8 60 d8 a6 4e 76 29 b0 0d 38	qoR·-·-·-·` ·-·Nv)·-·8
00d0	4e 11 cc 59 68 4d a4 37 0c c9 fb ac 5c d3 d0 2a	N·-·YhM·7 ·-·-·-·\·-·*
00e0	b9 25 4b 69 bb 97 9c f9 f7 43 3a a2 98 0e 51 52	·%Ki·-·-·-· ·-·C:·-·-·QR
00f0	5a 8e c9 f4 6a bf 3a 0f 59 25 1a 88 6f f6 b0 c2	Z·-·-·j·-·-·: Y%·-·-·o·-·-·
0100	50 1c da 8d 5c 85 22 99 96 f4 c0 76 c2 2c 1a f7	P·-·-·\·-·"- ·-·-·v·-·-·,
0110	51 fd 66 f1 c8 42 59 9e da 5b f8 80 a3 2b 0c 70	Q·f·-·BY· ·-·[·-·-·-·+·p
0120	b9 78 9b 3b 55 98 6c 79 09 d8 c6 cf b9 51 60 9e	·x·-·;U·ly ·-·-·-·-·Q`·
0130	52 f6 ca 15 c0 07 90 66 f9 0d 13 16 c0 05 4d e2	R·-·-·-·-·f ·-·-·-·-·M·
0140	5d 4a 53 5e b9 22 fb 30 ed 81 7e e5 92 4f 06 28]JS^·"-·0 ·-·~·-·-·0·(
0150	f8 3f e0 f0 33 30 5c 7b cc 59 49 1b 80 de 91 c0	·?·-·-·30\{ ·-·YI·-·-·-·
0160	74 3a a6 f0 05 a4 2f 82 6b 82 84 32 d0 91 65 d9	t:·-·-·-·/· k·-·2·-·e·
0170	84 b0 d0 11 26 d8 18 49 e3 ad a7 98 e3 36 96 ed	·-·-·-·&·-·-·I ·-·-·-·-·6·-·
0180	71 91 c6 20 c5 ea 95 0d 2c 28 3e 46 d9 7c 10 00	q·-· -·-·-·-·,(>F· ·-·
0190	c3 f1 f0 cb ac 38 fc ed 5d f6 46 c8 3b 71 59 16	·-·-·-·8·-·-·]·-·F·-·;qY·
01a0	55 41 31 74 ba 4a 99 42 46 a7 09 91 f7 e5 b5 b0	UA1t·J·B F·-·-·-·-·-·
01b0	d9 86 82 79 fb 26 9e 94 03 4a df f7 ac fb 55 9e	·-·-·y·&·-·-· ·-·J·-·-·-·U·
01c0	26 3b f5 41 37 a7 c5 b8 2b 39 c9 41 5c 26 5f 51	&;·A7·-·-· +9·A\&_Q
01d0	81 c6 3c 65 40 f9 d8 b9 77 78 86 7b ea 0a fc ae	·-·<e@·-·-· wx·{·-·-·-·
01e0	bb 36 68 18 e2 b3 3b 44 c7 6d 40 fa 0b 1e d9 3d	·6h·-·-·;D ·-·m@·-·-·-·=
01f0	01 4c 91 87 60 83 36 37 7a bc 78 a0 38 27 a3 c3	·L·-·-·`·67 z·x·8'·-·
0200	4a 0e ca 5f d8 0e 25 f0 b0 af 22 4d 12 b7 ba 20	J·-·-·_·-·-·%·-·-· "M·-·-·
0210	29 2d 4b e5 2a 93 84 4c 4e 3b 52 e7 57 d2 86 b9)·-·K·*·-·-·L N;R·W·-·-·
0220	4b df 44 61 d6 9b c8 61 93 00 6c 42 58 af 38 65	K·Da·-·-·-·a ·-·-·lBX·8e
0230	f5 c0 8f ee 01 ad 9f 1b 99 a8 02 9a e2 89 7c 60	·-·-·-·-·-·-·-·-· `
0240	36 03 aa c4 65 d0 11 f9 3c 8a 33 00 b5 b2 d8 b2	6·-·-·e·-·-· <·3·-·-·-·
0250	bc 96 f2 9f d3 94 17 a5 48 b1 d2 46 c3 d1 c5 70	·-·-·-·-·-·-· H·-·F·-·-·p
0260	b4 07 02 ed 69 83 96 b8 cd 43 b8 d4 55 ee dd d0	·-·-·-·i·-·-· ·-·C·-·U·-·
0270	19 85 0c 3d 5b 3d 16 e4 37 aa ab 16 38 7d 3d 06	·-·-·-·=[·-·-· 7·-·-·8}·-·=
0280	00 82 43 a4 de 45 c9 8c 22 79 d7 29 68 7c 74 3f	·-·C·-·E·-·-· "y·)h t?
0290	b0 e5 ed cb c3 cd ea 92 8d d0 5d 00 0a 06 0c bc	·-·-·-·-·-·-·-·-·]·-·-·-·-·
02a0	43 77 f0 39 b4 95 3a 5c ff 95 53 86 0b 49 c3 90	Cw·9·-·-·:\ ·-·-·S·-·-·I·
02b0	21 d6 f7 1f fe c4 03 a0 47 70 94 ad d0 5b 6b e7	!·-·-·-·-·-· Gp·-·-·[k·
02c0	78 39 15 aa 3c 59 53 d3 04 00 df 4c 0d 2f 86 2a	x9·-·-·<YS· -·-·-·L·-/·*
02d0	d9 49 0b 8a 6b d7 30 4f ae 7c df 24 43 01 aa 1a	·I·-·-·k·00 ·-· ·-·\$C·-·-·
02e0	a8 40 b1 3f f0 46 f8 74 06 a3 88 b2 1c 0c 09 7e	·@·-·?·F·t ·-·-·-·-·-·~

Different Statistics:

Wi-Fi file capture

Wireshark · Capture File Properties · Wi-Fi

Details

File

Name:

C:\Users\USER\AppData\Local\Temp\wireshark_Wi-Fi_20200804211509_a01608.pcapng

Length:

24 kB

Hash (SHA256):

4a3e04fe356cd42feec021b0783dfd5fe39b096c76f1d7ead62b2fcea15c3b89

Hash (RIPEMD160):

c09df01ea64e532c2fed5079cee65dd1a640a9cb

Hash (SHA1):

e231768d84970f9830ff8449ad51c083aa64de6e

Format:

Wireshark/... - pcapng

Encapsulation:

Ethernet

Time

First packet:

2020-08-04 21:15:18

Last packet:

2020-08-04 21:15:44

Elapsed:

00:00:26

Capture

Hardware:

Intel(R) Core(TM) i3-10110U CPU @ 2.10GHz (with SSE4.2)

OS:

64-bit Windows 10 (1909), build 18363

Application:

Dumpcap (Wireshark) 3.2.5 (v3.2.5-0-ged20ddea8138)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Wi-Fi	Unknown	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	106	106 (100.0%)	—
Time span, s	26.030	26.030	—
Average pps	4.1	4.1	—
Average packet size, B	190	190	—
Bytes	20135	20135 (100.0%)	0
Average bytes/s	773	773	—
Average bits/s	6188	6188	—

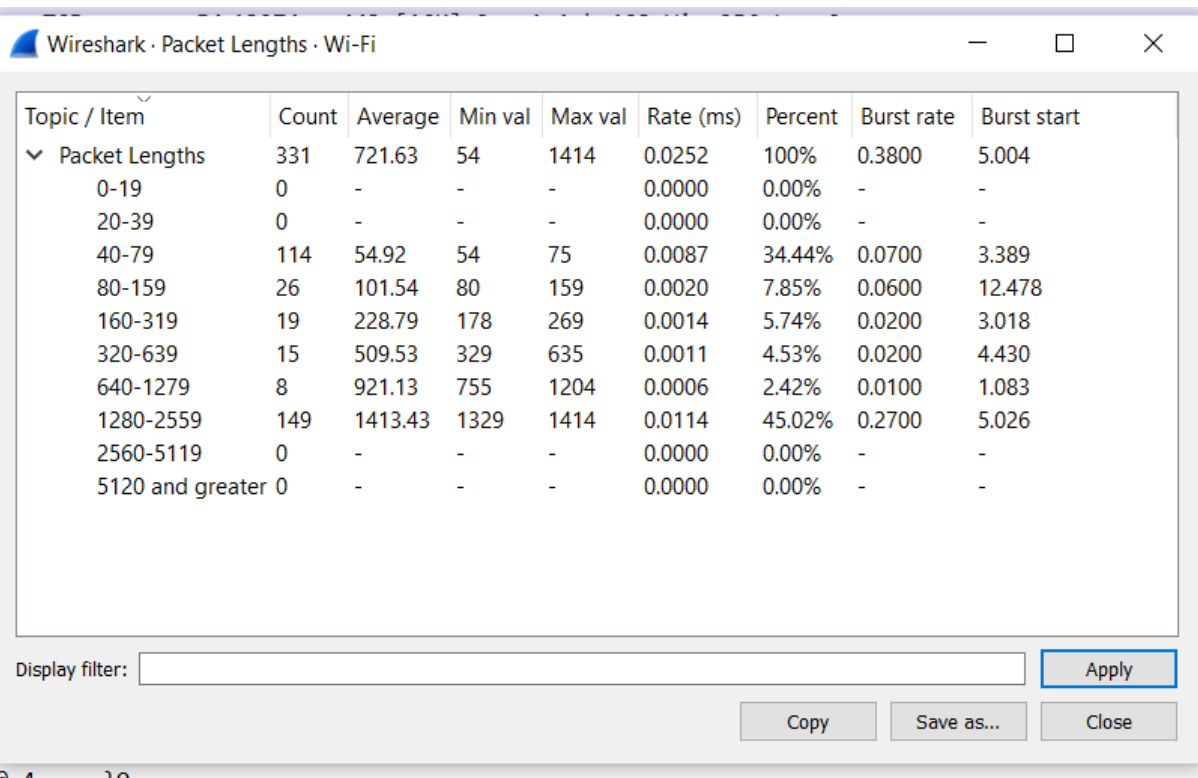
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	739	100.0	330333	11 k	0	0	0
▼ Ethernet	100.0	739	3.1	10346	345	0	0	0
▼ Internet Protocol Version 4	99.2	733	4.4	14660	489	0	0	0
▼ User Datagram Protocol	5.3	39	0.1	312	10	0	0	0
Simple Service Discovery Protocol	1.1	8	0.4	1392	46	8	1392	46
NetBIOS Name Service	2.0	15	0.2	750	25	15	750	25
Domain Name System	2.2	16	0.2	825	27	16	825	27
▼ Transmission Control Protocol	93.9	694	91.4	301880	10 k	462	229342	7661
Transport Layer Security	30.7	227	86.0	284244	9496	222	231373	7729
Data	1.4	10	0.0	10	0	10	10	0
Address Resolution Protocol	0.8	6	0.1	168	5	6	168	5

DNS

Wireshark · DNS · Wi-Fi								
Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ Total Packets	24				0.0006	100%	0.0400	42.542
▼ rcode	24				0.0006	100.00%	0.0400	42.542
No error	24				0.0006	100.00%	0.0400	42.542
▼ opcodes	24				0.0006	100.00%	0.0400	42.542
Standard query	24				0.0006	100.00%	0.0400	42.542
▼ Query/Response	24				0.0006	100.00%	0.0400	42.542
Response	12				0.0003	50.00%	0.0200	42.600
Query	12				0.0003	50.00%	0.0200	42.542
▼ Query Type	24				0.0006	100.00%	0.0400	42.542
A (Host Address)	24				0.0006	100.00%	0.0400	42.542
▼ Class	24				0.0006	100.00%	0.0400	42.542
IN	24				0.0006	100.00%	0.0400	42.542
▼ Service Stats	0				0.0000	100%	-	-
request-response time (secs)	11	0.08	0.050018	0.148524	0.0003		0.0200	42.600
no. of unsolicited responses	0				0.0000		-	-

Display filter:

Apply



Protocol have been used:

Wireshark · IP Protocol Types · Wi-Fi

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ IP Protocol Types	516				0.0049	100%	0.3800	5.004
UDP	21				0.0002	4.07%	0.0200	0.569
TCP	495				0.0047	95.93%	0.3800	5.004

Display filter:

Apply Copy Save as... Close

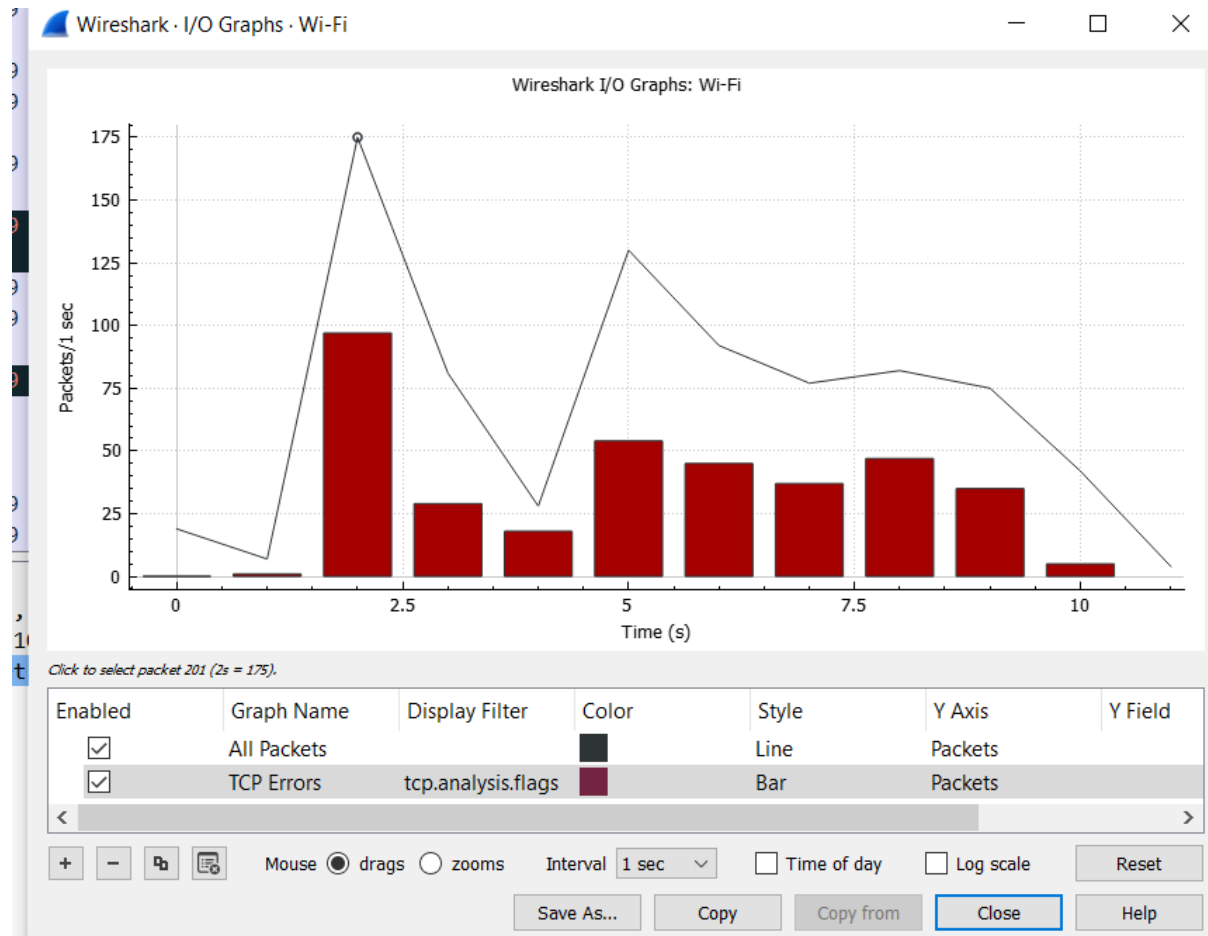
Wireshark · Destinations and Ports · Wi-Fi

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ Destinations and Ports	501				0.0093	100%	0.3800	5.004
▼ 74.125.68.188	1				0.0000	0.20%	0.0100	13.368
▼ TCP	1				0.0000	100.00%	0.0100	13.368
5228	1				0.0000	100.00%	0.0100	13.368
▼ 74.125.24.189	6				0.0001	1.20%	0.0200	19.972
▼ TCP	6				0.0001	100.00%	0.0200	19.972
443	6				0.0001	100.00%	0.0200	19.972
▼ 40.119.211.203	5				0.0001	1.00%	0.0100	2.393
▼ TCP	5				0.0001	100.00%	0.0100	2.393
443	5				0.0001	100.00%	0.0100	2.393
▼ 34.237.189.140	1				0.0000	0.20%	0.0100	51.481
▼ TCP	1				0.0000	100.00%	0.0100	51.481
443	1				0.0000	100.00%	0.0100	51.481
▼ 239.255.255.250	4				0.0001	0.80%	0.0100	9.565
▼ UDP	4				0.0001	100.00%	0.0100	9.565

Display filter:

Apply Copy Save as... Close

Error & Success Rates:



Real time Response:

