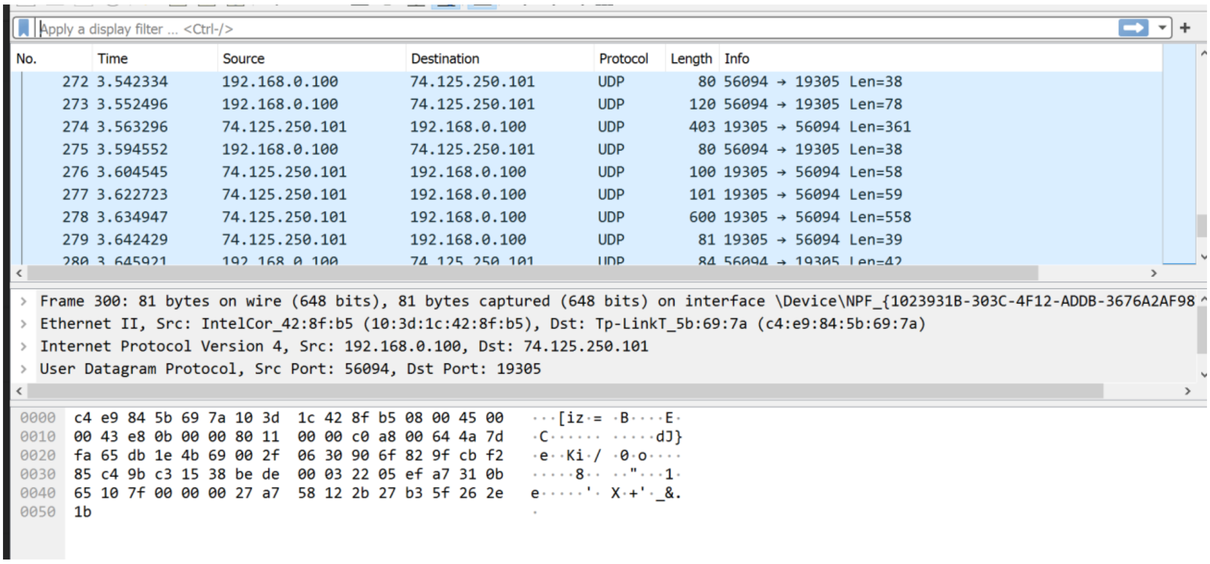
Practical 2

Date:- 07/08/21
Roll No:- 19BCE248
Course No:- 2CS502 Computer Networks

AIM: Explore Packet capture tool (Wireshark) to capture and analyse various types of network packets.

- ## Capturing Data Packets

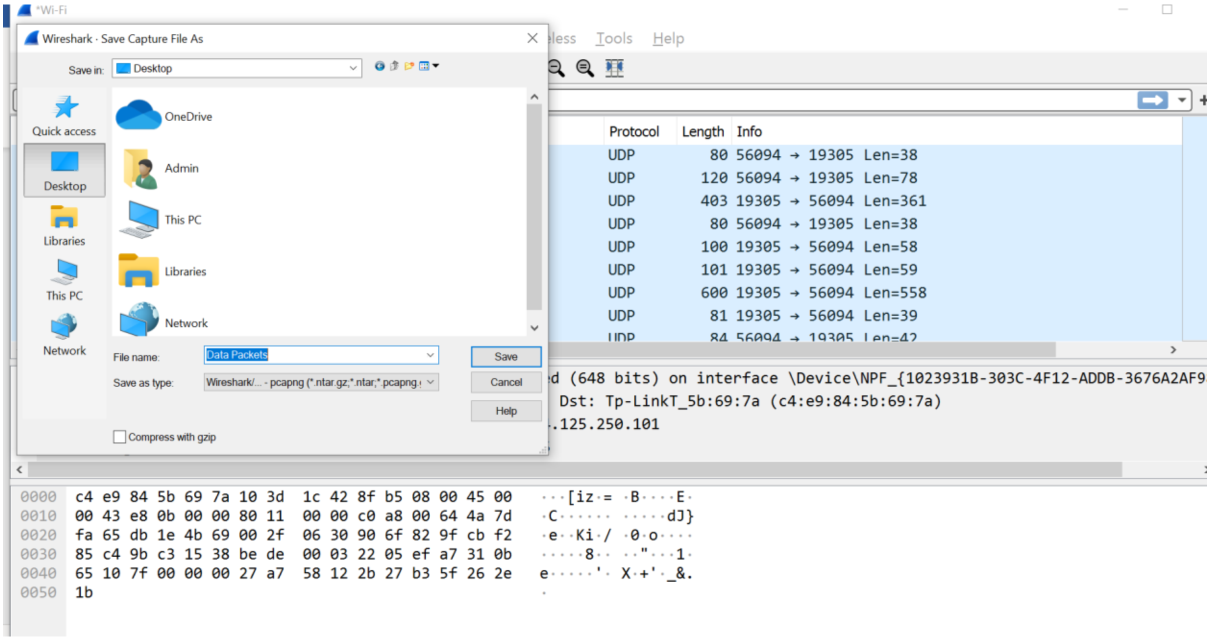


```
No.      Time         Source            Destination       Protocol  Length Info
     272 3.542334     192.168.0.100     74.125.250.101    UDP         80 56094 → 19305 Len=38
     273 3.552496     192.168.0.100     74.125.250.101    UDP        120 56094 → 19305 Len=78
     274 3.563296     74.125.250.101    192.168.0.100     UDP        403 19305 → 56094 Len=361
     275 3.594552     192.168.0.100     74.125.250.101    UDP         80 56094 → 19305 Len=38
     276 3.604545     74.125.250.101    192.168.0.100     UDP        100 19305 → 56094 Len=58
     277 3.622723     74.125.250.101    192.168.0.100     UDP        101 19305 → 56094 Len=59
     278 3.634947     74.125.250.101    192.168.0.100     UDP        600 19305 → 56094 Len=558
     279 3.642429     74.125.250.101    192.168.0.100     UDP         81 19305 → 56094 Len=39
     280 3.645921     192.168.0.100     74.125.250.101    UDP         84 56094 → 19305 Len=42
```

```
> Frame 300: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_{1023931B-303C-4F12-ADDB-3676A2AF98
> Ethernet II, Src: IntelCor_42:8f:b5 (10:3d:1c:42:8f:b5), Dst: Tp-LinkT_5b:69:7a (c4:e9:84:5b:69:7a)
> Internet Protocol Version 4, Src: 192.168.0.100, Dst: 74.125.250.101
> User Datagram Protocol, Src Port: 56094, Dst Port: 19305
```

```
0000  c4 e9 84 5b 69 7a 10 3d  1c 42 8f b5 08 00 45 00   ···[iz·= ·B····E·
0010  00 43 e8 0b 00 00 80 11  00 00 c0 a8 00 64 4a 7d   ·C······ ·····dJ}
0020  fa 65 db 1e 4b 69 00 2f  06 30 90 6f 82 9f cb f2   ·e··Ki·/ ·0·o····
0030  85 c4 9b c3 15 38 be de  00 03 22 05 ef a7 31 0b   ·····8·· ··"···1·
0040  65 10 7f 00 00 00 27 a7  58 12 2b 27 b3 5f 26 2e   e·····'· X·+'·_&.
0050  1b                                                 ·
```

- ## Saving Data Packets



File name: Data Packets

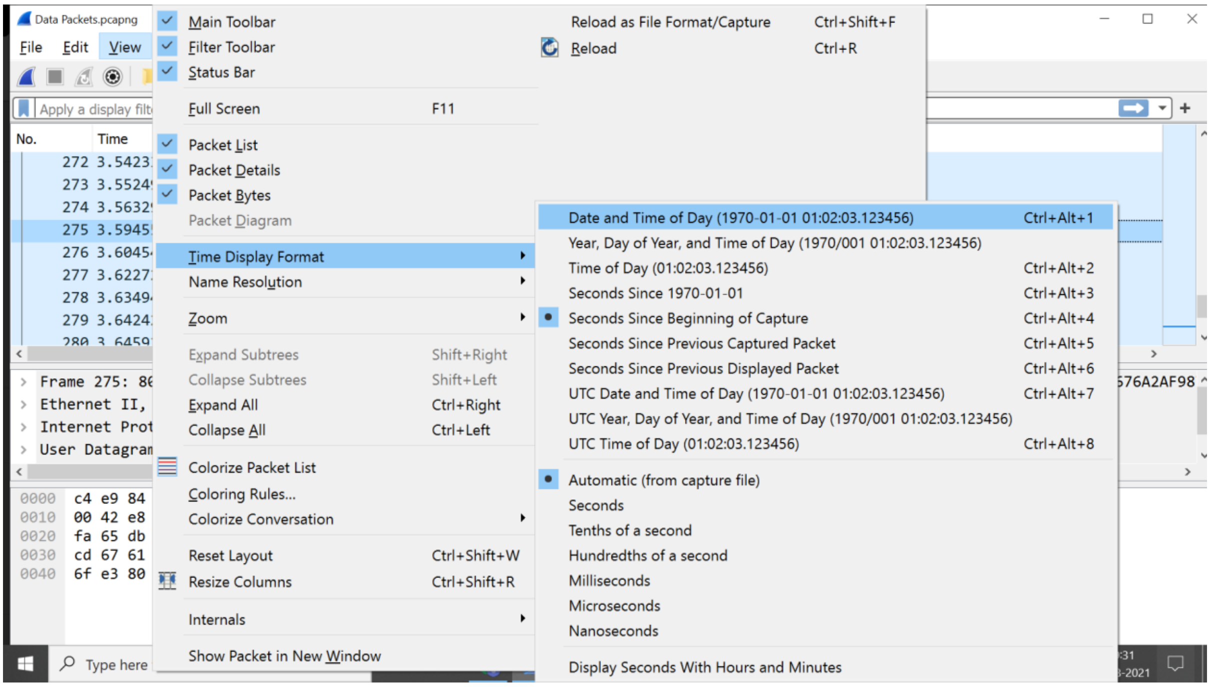
Save as type: Wireshark/... - pcapng (*.ntar.gz;*.ntar;*.pcapng.(

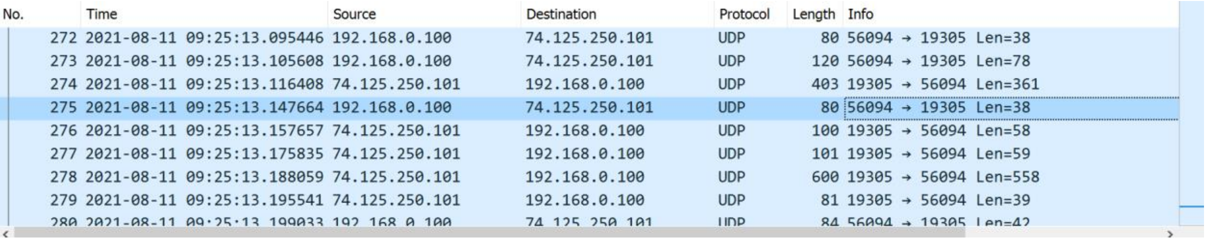
```
Protocol  Length Info
UDP           80 56094 → 19305 Len=38
UDP          120 56094 → 19305 Len=78
UDP          403 19305 → 56094 Len=361
UDP           80 56094 → 19305 Len=38
UDP          100 19305 → 56094 Len=58
UDP          101 19305 → 56094 Len=59
UDP          600 19305 → 56094 Len=558
UDP           81 19305 → 56094 Len=39
UDP           84 56094 → 19305 Len=42
```

```
d (648 bits) on interface \Device\NPF_{1023931B-303C-4F12-ADDB-3676A2AF9
 Dst: Tp-LinkT_5b:69:7a (c4:e9:84:5b:69:7a)
.125.250.101
```

```
0000  c4 e9 84 5b 69 7a 10 3d  1c 42 8f b5 08 00 45 00   ···[iz·= ·B····E·
0010  00 43 e8 0b 00 00 80 11  00 00 c0 a8 00 64 4a 7d   ·C······ ·····dJ}
0020  fa 65 db 1e 4b 69 00 2f  06 30 90 6f 82 9f cb f2   ·e··Ki·/ ·0·o····
0030  85 c4 9b c3 15 38 be de  00 03 22 05 ef a7 31 0b   ·····8·· ··"···1·
0040  65 10 7f 00 00 27 a7 58  12 2b 27 b3 5f 26 2e      e·····'· X·+'·_&.
0050  1b                                                 ·
```

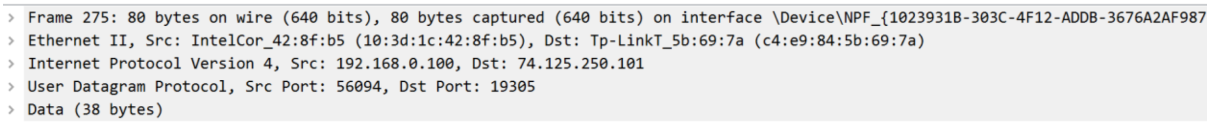
- Changing Date and Time Format


Data Packets.pcapng
File Edit View
Apply a display filt
No. Time
272 3.5423
273 3.5524
274 3.5632
275 3.5945
276 3.6045
277 3.6227
278 3.6349
279 3.6424
280 3.6459
Frame 275: 8(
Ethernet II,
Internet Prot
User Datagram
0000 c4 e9 84
0010 00 42 e8
0020 fa 65 db
0030 cd 67 61
0040 6f e3 80
Type here
Main Toolbar
Filter Toolbar
Status Bar
Full Screen F11
Packet List
Packet Details
Packet Bytes
Packet Diagram
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout Ctrl+Shift+W
Resize Columns Ctrl+Shift+R
Internals
Show Packet in New Window
Reload as File Format/Capture Ctrl+Shift+F
Reload Ctrl+R
Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+1
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
Time of Day (01:02:03.123456) Ctrl+Alt+2
Seconds Since 1970-01-01 Ctrl+Alt+3
● Seconds Since Beginning of Capture Ctrl+Alt+4
Seconds Since Previous Captured Packet Ctrl+Alt+5
Seconds Since Previous Displayed Packet Ctrl+Alt+6
UTC Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+7
UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
UTC Time of Day (01:02:03.123456) Ctrl+Alt+8
● Automatic (from capture file)
Seconds
Tenths of a second
Hundredths of a second
Milliseconds
Microseconds
Nanoseconds
Display Seconds With Hours and Minutes
576A2AF98



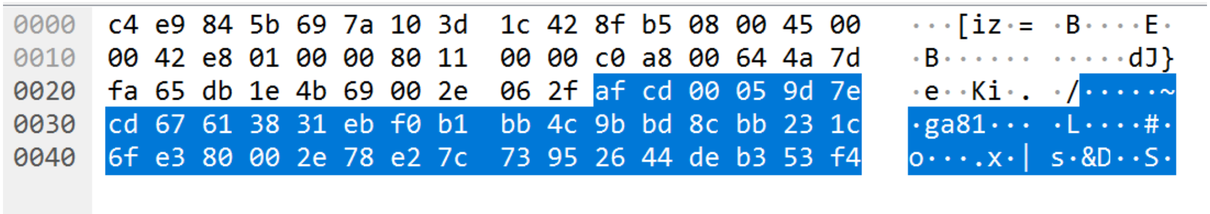
```
No.  Time                       Source         Destination    Protocol Length Info
 272 2021-08-11 09:25:13.095446 192.168.0.100  74.125.250.101 UDP          80 56094 → 19305 Len=38
 273 2021-08-11 09:25:13.105608 192.168.0.100  74.125.250.101 UDP         120 56094 → 19305 Len=78
 274 2021-08-11 09:25:13.116408 74.125.250.101 192.168.0.100  UDP         403 19305 → 56094 Len=361
 275 2021-08-11 09:25:13.147664 192.168.0.100  74.125.250.101 UDP          80 56094 → 19305 Len=38
 276 2021-08-11 09:25:13.157657 74.125.250.101 192.168.0.100  UDP         100 19305 → 56094 Len=58
 277 2021-08-11 09:25:13.175835 74.125.250.101 192.168.0.100  UDP         101 19305 → 56094 Len=59
 278 2021-08-11 09:25:13.188059 74.125.250.101 192.168.0.100  UDP         600 19305 → 56094 Len=558
 279 2021-08-11 09:25:13.195541 74.125.250.101 192.168.0.100  UDP          81 19305 → 56094 Len=39
 280 2021-08-11 09:25:13.199033 192.168.0.100  74.125.250.101 UDP          84 56094 → 19305 Len=42
```

- Package Details

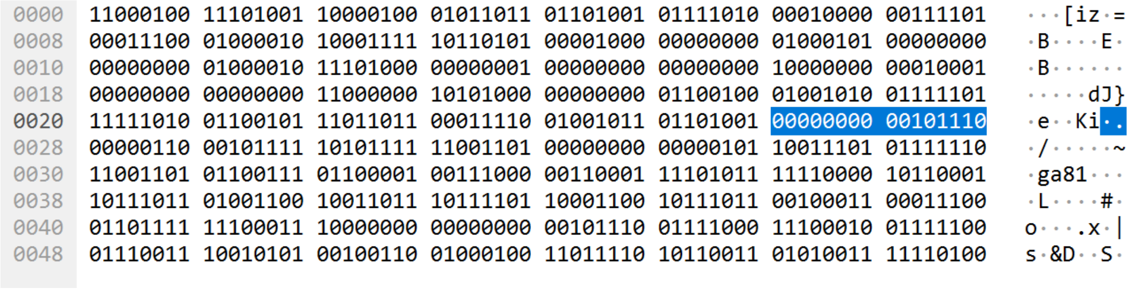


```
> Frame 275: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{1023931B-303C-4F12-ADDB-3676A2AF987
> Ethernet II, Src: IntelCor_42:8f:b5 (10:3d:1c:42:8f:b5), Dst: Tp-LinkT_5b:69:7a (c4:e9:84:5b:69:7a)
> Internet Protocol Version 4, Src: 192.168.0.100, Dst: 74.125.250.101
> User Datagram Protocol, Src Port: 56094, Dst Port: 19305
> Data (38 bytes)
```

- Package Bytes

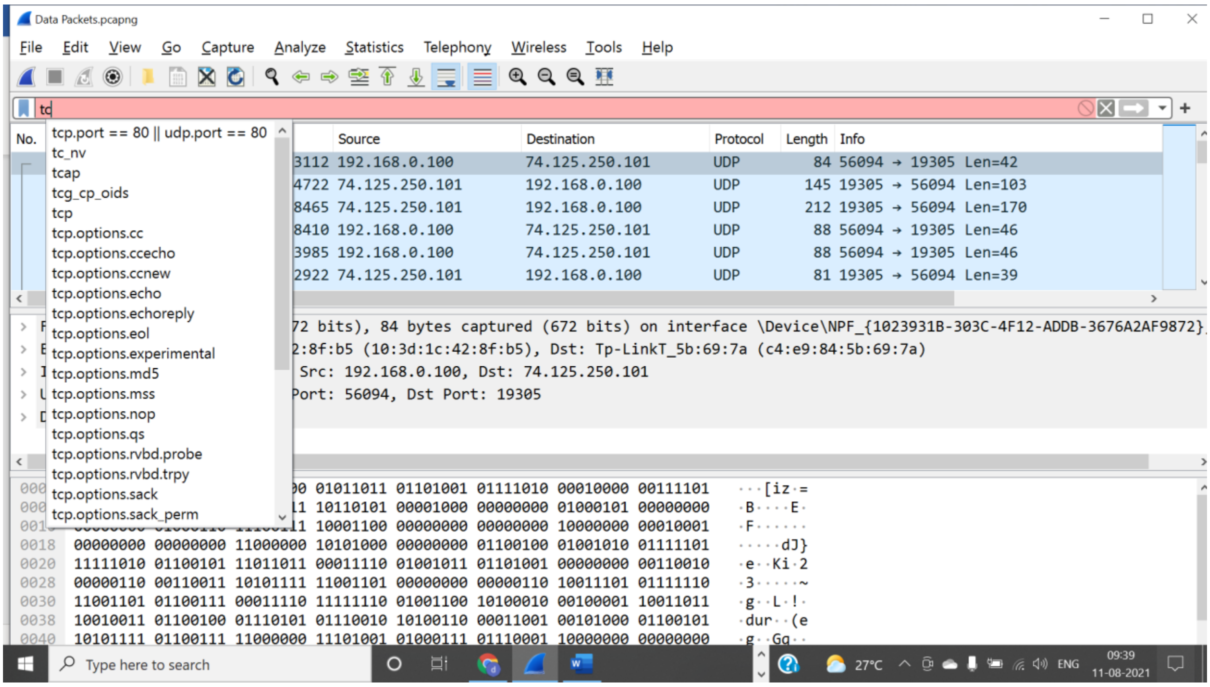


```
0000  c4 e9 84 5b 69 7a 10 3d  1c 42 8f b5 08 00 45 00   ···[iz·= ·B····E·
0010  00 42 e8 01 00 00 80 11  00 00 c0 a8 00 64 4a 7d   ·B······ ·····dJ}
0020  fa 65 db 1e 4b 69 00 2e  06 2f af cd 00 05 9d 7e   ·e··Ki·. ·/·····~
0030  cd 67 61 38 31 eb f0 b1  bb 4c 9b bd 8c bb 23 1c   ·ga81··· ·L····#·
0040  6f e3 80 00 2e 78 e2 7c  73 95 26 44 de b3 53 f4   o···.x·| s·&D··S·
```



```
0000  11000100 11101001 10000100 01011011 01101001 01111010 00010000 00111101   ···[iz·=
0008  00011100 01000010 10001111 10110101 00001000 00000000 01000101 00000000   ·B····E·
0010  00000000 01000010 11101000 00000001 00000000 00000000 10000000 00010001   ·B······
0018  00000000 00000000 11000000 10101000 00000000 01100100 01001010 01111101   ·····dJ}
0020  11111010 01100101 11011011 00011110 01001011 01101001 00000000 00101110   ·e··Ki·.
0028  00000110 00101111 10101111 11001101 00000000 00000101 10011101 01111110   ·/·····~
0030  11001101 01100111 01100001 00111000 00110001 11101011 11110000 10110001   ·ga81···
0038  10111011 01001100 10011011 10111101 10001100 10111011 00100011 00011100   ·L····#·
0040  01101111 11100011 10000000 00000000 00101110 01111000 11100010 01111100   o···.x·|
0048  01110011 10010101 00100110 01000100 11011110 10110011 01010011 11110100   s·&D··S·
```

- Applying Filters



Data Packets.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search
27°C
ENG
09:39
11-08-2021

tc

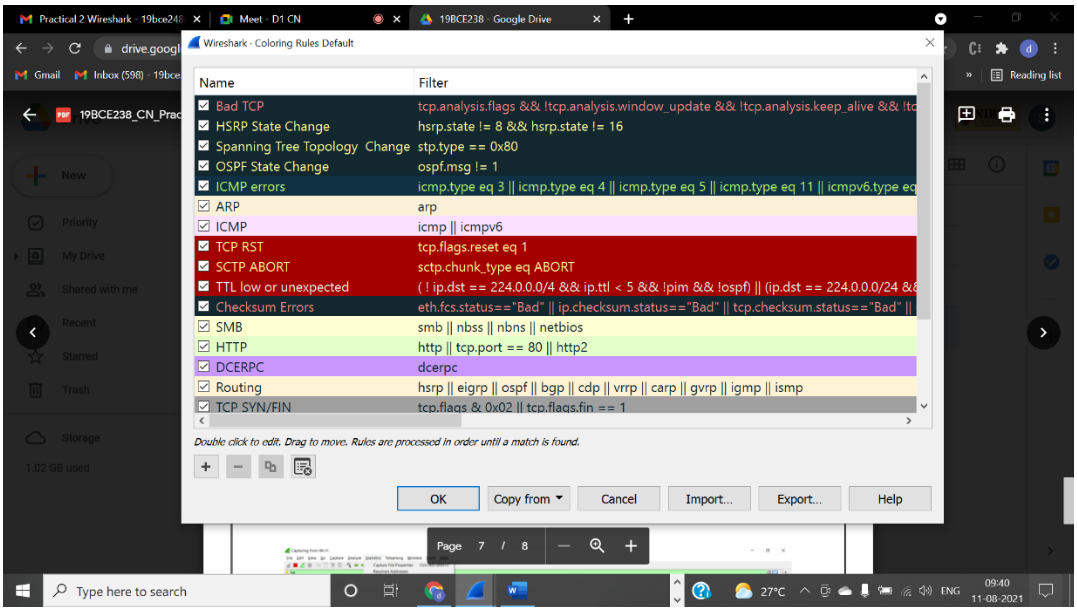
```
tcp.port == 80 || udp.port == 80
tc_nv
tcap
tcg_cp_oids
tcp
tcp.options.cc
tcp.options.ccecho
tcp.options.ccnew
tcp.options.echo
tcp.options.echoreply
tcp.options.eol
tcp.options.experimental
tcp.options.md5
tcp.options.mss
tcp.options.nop
tcp.options.qs
tcp.options.rvbd.probe
tcp.options.rvbd.trpy
tcp.options.sack
tcp.options.sack_perm
```

```
No.       Source          Destination     Protocol  Length Info
    3112 192.168.0.100   74.125.250.101  UDP          84 56094 → 19305 Len=42
    4722 74.125.250.101  192.168.0.100   UDP         145 19305 → 56094 Len=103
    8465 74.125.250.101  192.168.0.100   UDP         212 19305 → 56094 Len=170
    8410 192.168.0.100   74.125.250.101  UDP          88 56094 → 19305 Len=46
    3985 192.168.0.100   74.125.250.101  UDP          88 56094 → 19305 Len=46
    2922 74.125.250.101  192.168.0.100   UDP          81 19305 → 56094 Len=39
```

```
> F 72 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{1023931B-303C-4F12-ADDB-3676A2AF9872}
> E 2:8f:b5 (10:3d:1c:42:8f:b5), Dst: Tp-LinkT_5b:69:7a (c4:e9:84:5b:69:7a)
> I  Src: 192.168.0.100, Dst: 74.125.250.101
> U Port: 56094, Dst Port: 19305
> D
```

```
000  0 01011011 01101001 01111010 00010000 00111101   ···[iz·=
000  11 10110101 00001000 00000000 01000101 00000000   ·B····E·
001  11 10001100 00000000 00000000 10000000 00010001   ·F······
0018  00000000 00000000 11000000 10101000 00000000 01100100 01001010 01111101   ·····dJ}
0020  11111010 01100101 11011011 00011110 01001011 01101001 00000000 00110010   ·e··Ki·2
0028  00000110 00110011 10101111 11001101 00000000 00000110 10011101 01111110   ·3·····~
0030  11001101 01100111 00011110 11111110 01001100 10100010 00100001 10011011   ·g··L·!·
0038  10010011 01100100 01110101 01110010 10100110 00011001 00101000 01100101   ·dur··(e
0040  10101111 01100111 11000000 11101001 01000111 01110001 10000000 00000000   ·g··Gq··
```

- Coloring Rules

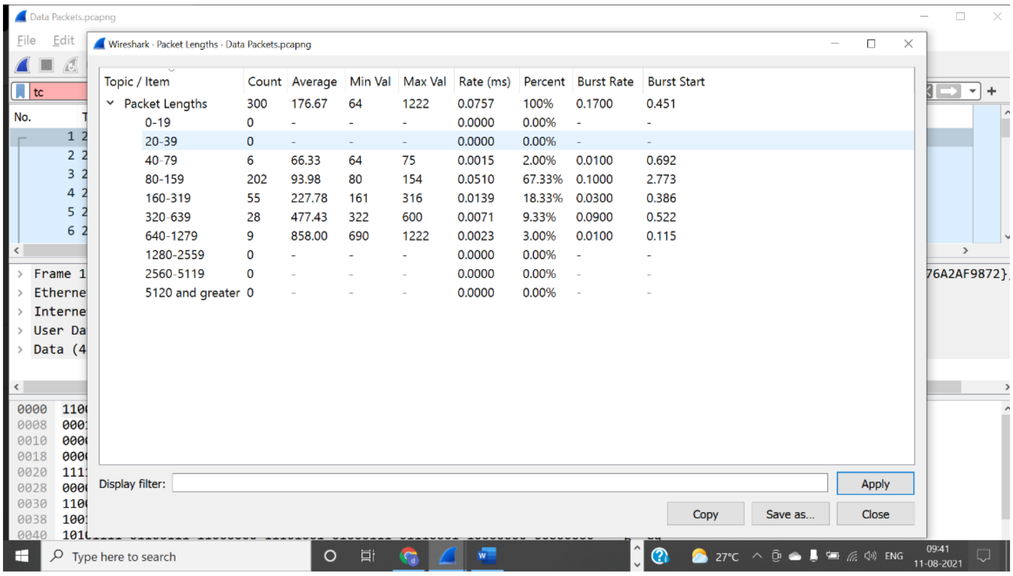


Wireshark · Coloring Rules Default

Name	Filter
☑ Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tc
☑ HSRP State Change	hsrp.state != 8 && hsrp.state != 16
☑ Spanning Tree Topology Change	stp.type == 0x80
☑ OSPF State Change	ospf.msg != 1
☑ ICMP errors	icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq
☑ ARP	arp
☑ ICMP	icmp || icmpv6
☑ TCP RST	tcp.flags.reset eq 1
☑ SCTP ABORT	sctp.chunk_type eq ABORT
☑ TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 &&
☑ Checksum Errors	eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" ||
☑ SMB	smb || nbss || nbns || netbios
☑ HTTP	http || tcp.port == 80 || http2
☑ DCERPC	dcerpc
☑ Routing	hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
☑ TCP SYN/FIN	tcp.flags & 0x02 || tcp.flags.fin == 1

Double click to edit. Drag to move. Rules are processed in order until a match is found.

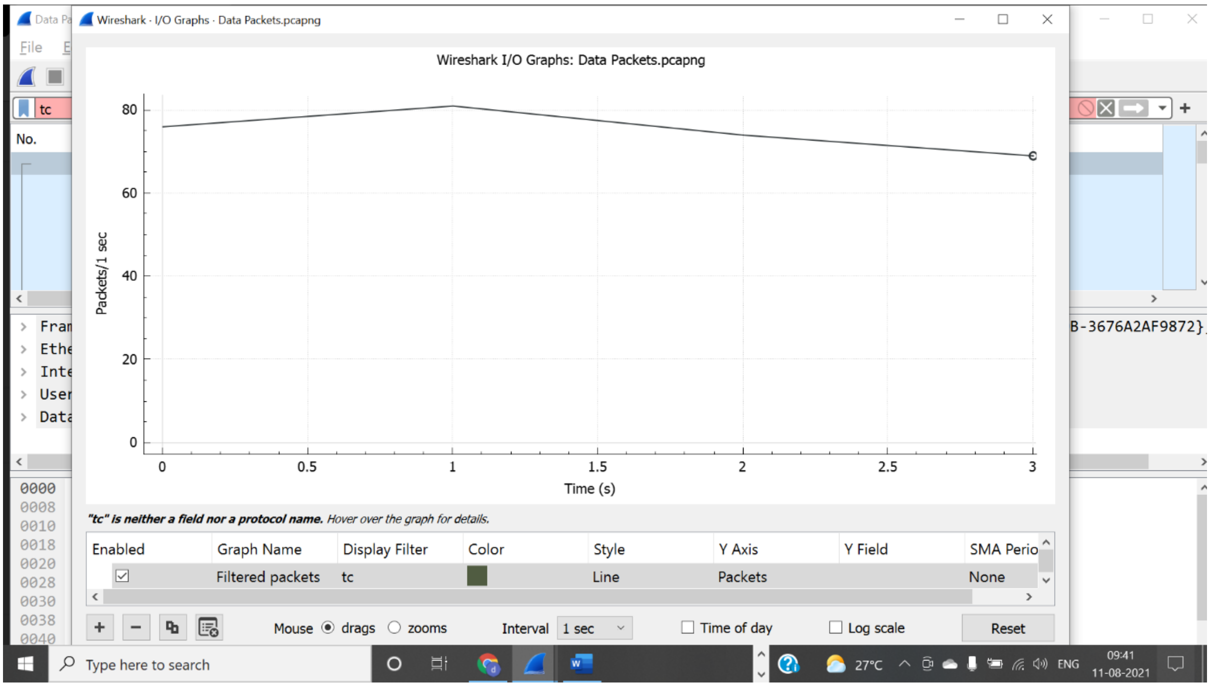
- Wireshark Statistics



Wireshark · Packet Lengths · Data Packets.pcapng

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	300	176.67	64	1222	0.0757	100%	0.1700	0.451
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	6	66.33	64	75	0.0015	2.00%	0.0100	0.692
80-159	202	93.98	80	154	0.0510	67.33%	0.1000	2.773
160-319	55	227.78	161	316	0.0139	18.33%	0.0300	0.386
320-639	28	477.43	322	600	0.0071	9.33%	0.0900	0.522
640-1279	9	858.00	690	1222	0.0023	3.00%	0.0100	0.115
1280-2559	0	-	-	-	0.0000	0.00%	-	-
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Display filter:



"tc" is neither a field nor a protocol name. *Hover over the graph for details.*

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Perio
☑	Filtered packets	tc	🟩	Line	Packets		None

Mouse ● drags ○ zooms   Interval 1 sec   □ Time of day   □ Log scale   Reset