COMPUTER NETWORKS AND SECURITY LABORATORY

Assignment No. 13

NAME :- OJUS P. JAISWAL

ROLL NO. :- TACO19108

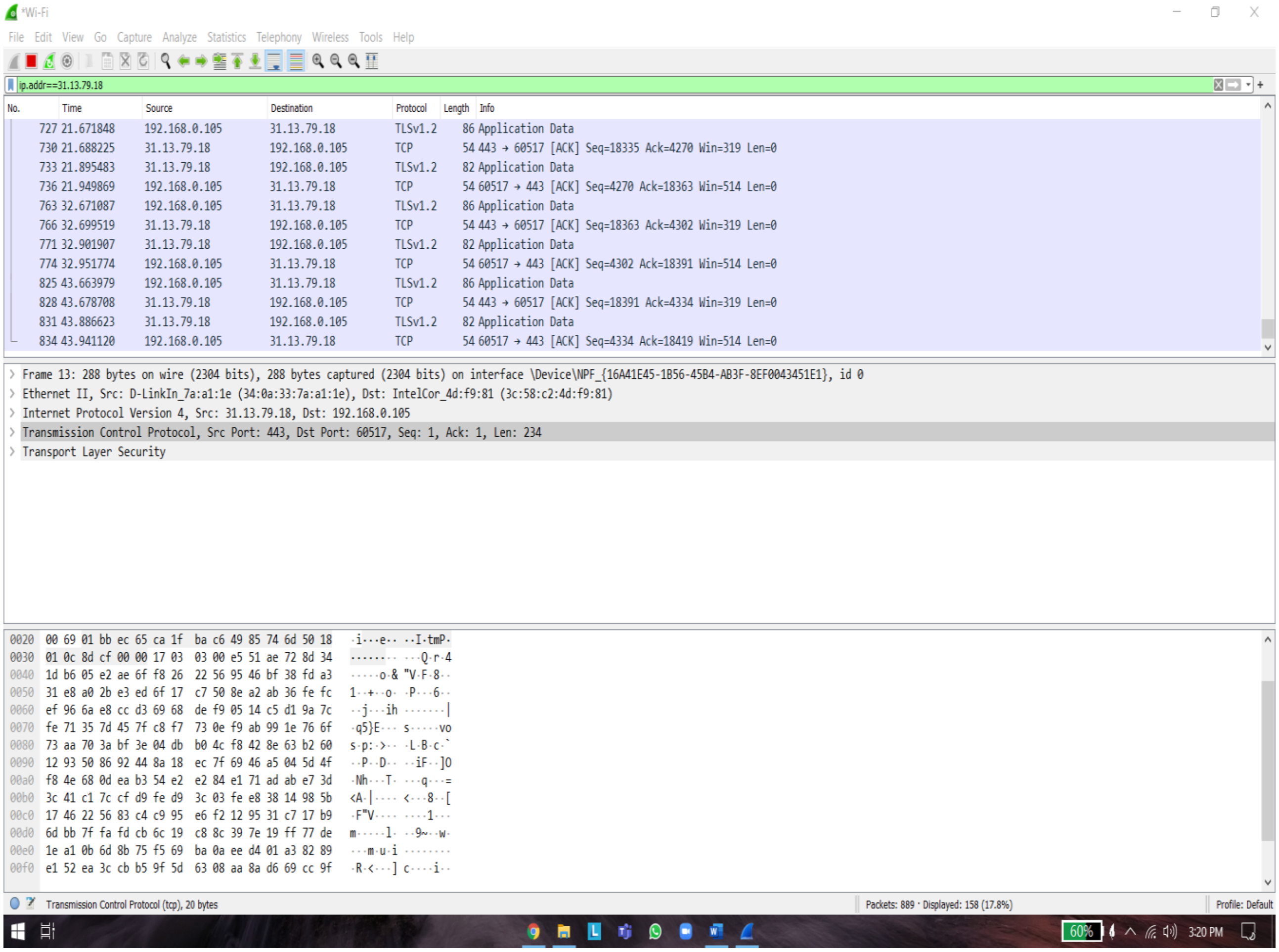
YEAR AND DIV :- TE A

Ques :- Capture packets using Wireshark, write the exact packet capture filter expressions to accomplish the following and save the output in file :

1. Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account

Solution :-

Packet capture filter expression : ip.addr==31.13.79.18



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

ip.addr==31.13.79.18

```
No.     Time       Source          Destination     Protocol  Length Info
    727 21.671848  192.168.0.105   31.13.79.18     TLSv1.2     86 Application Data
    730 21.688225  31.13.79.18     192.168.0.105   TCP         54 443 → 60517 [ACK] Seq=18335 Ack=4270 Win=319 Len=0
    733 21.895483  31.13.79.18     192.168.0.105   TLSv1.2     82 Application Data
    736 21.949869  192.168.0.105   31.13.79.18     TCP         54 60517 → 443 [ACK] Seq=4270 Ack=18363 Win=514 Len=0
    763 32.671087  192.168.0.105   31.13.79.18     TLSv1.2     86 Application Data
    766 32.699519  31.13.79.18     192.168.0.105   TCP         54 443 → 60517 [ACK] Seq=18363 Ack=4302 Win=319 Len=0
    771 32.901907  31.13.79.18     192.168.0.105   TLSv1.2     82 Application Data
    774 32.951774  192.168.0.105   31.13.79.18     TCP         54 60517 → 443 [ACK] Seq=4302 Ack=18391 Win=514 Len=0
    825 43.663979  192.168.0.105   31.13.79.18     TLSv1.2     86 Application Data
    828 43.678708  31.13.79.18     192.168.0.105   TCP         54 443 → 60517 [ACK] Seq=18391 Ack=4334 Win=319 Len=0
    831 43.886623  31.13.79.18     192.168.0.105   TLSv1.2     82 Application Data
    834 43.941120  192.168.0.105   31.13.79.18     TCP         54 60517 → 443 [ACK] Seq=4334 Ack=18419 Win=514 Len=0
```

```
> Frame 13: 288 bytes on wire (2304 bits), 288 bytes captured (2304 bits) on interface \Device\NPF_{16A41E45-1B56-45B4-AB3F-8EF0043451E1}, id 0
> Ethernet II, Src: D-LinkIn_7a:a1:1e (34:0a:33:7a:a1:1e), Dst: IntelCor_4d:f9:81 (3c:58:c2:4d:f9:81)
> Internet Protocol Version 4, Src: 31.13.79.18, Dst: 192.168.0.105
> Transmission Control Protocol, Src Port: 443, Dst Port: 60517, Seq: 1, Ack: 1, Len: 234
> Transport Layer Security
```

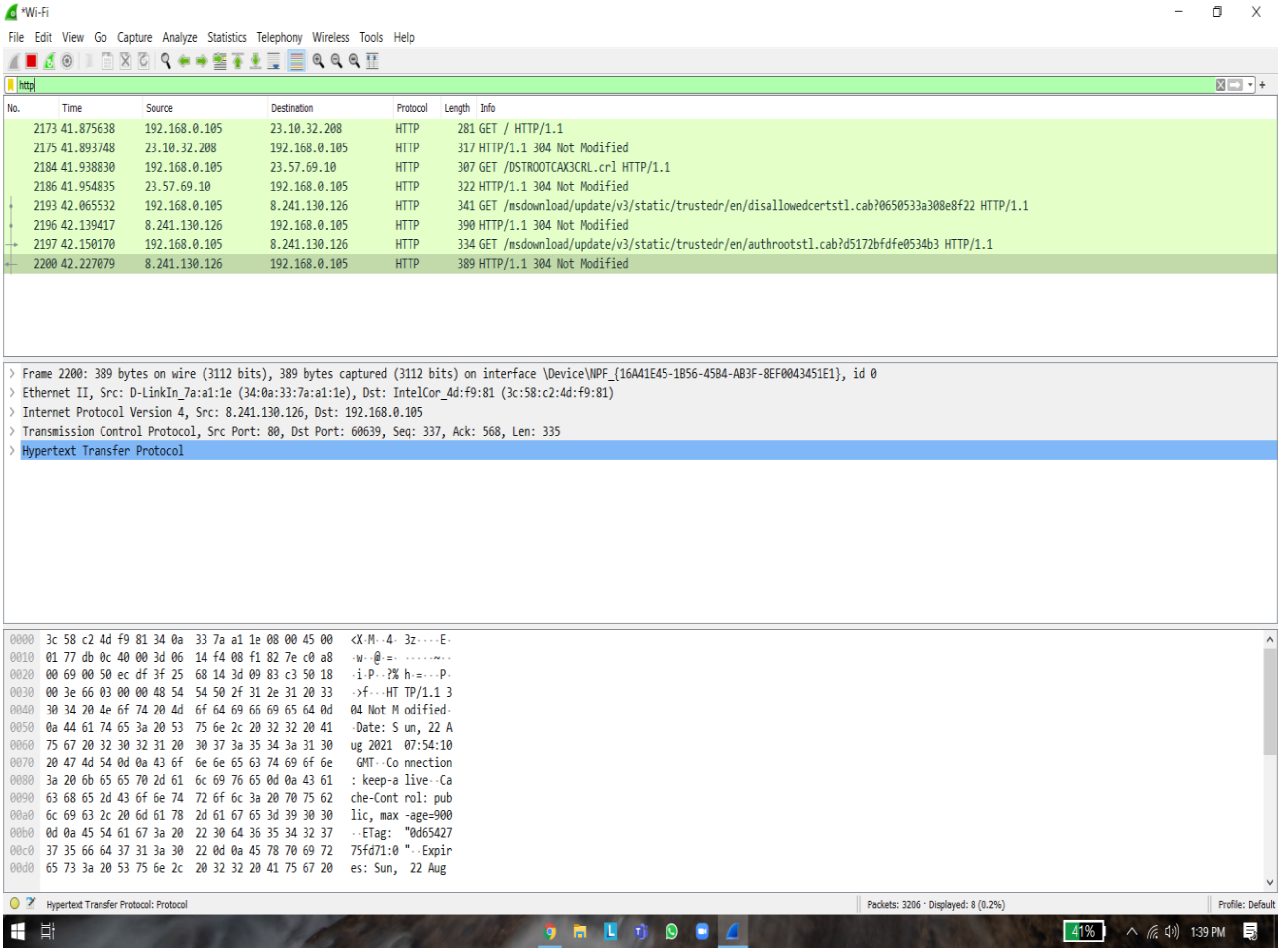
```
0020  00 69 01 bb ec 65 ca 1f  ba c6 49 85 74 6d 50 18   ·i···e·· ··I·tmP·
0030  01 0c 8d cf 00 00 17 03  03 00 e5 51 ae 72 8d 34   ········ ···Q·r·4
0040  1d b6 05 e2 ae 6f f8 26  22 56 95 46 bf 38 fd a3   ·····o·& "V·F·8··
0050  31 e8 a0 2b e3 ed 6f 17  c7 50 8e a2 ab 36 fe fc   1··+··o· ·P···6··
0060  ef 96 6a e8 cc d3 69 68  de f9 05 14 c5 d1 9a 7c   ··j···ih ·······|
0070  fe 71 35 7d 45 7f c8 f7  73 0e f9 ab 99 1e 76 6f   ·q5}E··· s·····vo
0080  73 aa 70 3a bf 3e 04 db  b0 4c f8 42 8e 63 b2 60   s·p:·>·· ·L·B·c·`
0090  12 93 50 86 92 44 8a 18  ec 7f 69 46 a5 04 5d 4f   ··P··D·· ··iF··]O
00a0  f8 4e 68 0d ea b3 54 e2  e2 84 e1 71 ad ab e7 3d   ·Nh···T· ···q···=
00b0  3c 41 c1 7c cf d9 fe d9  3c 03 fe e8 38 14 98 5b   <A·|···· <···8··[
00c0  17 46 22 56 83 c4 c9 95  e6 f2 12 95 31 c7 17 b9   ·F"V···· ····1···
00d0  6d bb 7f fa fd cb 6c 19  c8 8c 39 7e 19 ff 77 de   m·····l· ··9~··w·
00e0  1e a1 0b 6d 8b 75 f5 69  ba 0a ee d4 01 a3 82 89   ···m·u·i ········
00f0  e1 52 ea 3c cb b5 9f 5d  63 08 aa 8a d6 69 cc 9f   ·R·<···] c····i··
```

Transmission Control Protocol (tcp), 20 bytes   Packets: 889 · Displayed: 158 (17.8%)   Profile: Default

2. Capture all HTTP traffic to/from Facebook, when you log in to your Facebook account

Solution :-

Packet capture filter expression : http


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
41%
1:39 PM

http

```
No.     Time       Source          Destination     Protocol  Length Info
   2173 41.875638  192.168.0.105   23.10.32.208    HTTP      281 GET / HTTP/1.1
   2175 41.893748  23.10.32.208    192.168.0.105   HTTP      317 HTTP/1.1 304 Not Modified
   2184 41.938830  192.168.0.105   23.57.69.10     HTTP      307 GET /DSTROOTCAX3CRL.crl HTTP/1.1
   2186 41.954835  23.57.69.10     192.168.0.105   HTTP      322 HTTP/1.1 304 Not Modified
   2193 42.065532  192.168.0.105   8.241.130.126   HTTP      341 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?0650533a308e8f22 HTTP/1.1
   2196 42.139417  8.241.130.126   192.168.0.105   HTTP      390 HTTP/1.1 304 Not Modified
   2197 42.150170  192.168.0.105   8.241.130.126   HTTP      334 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?d5172bfdfe0534b3 HTTP/1.1
   2200 42.227079  8.241.130.126   192.168.0.105   HTTP      389 HTTP/1.1 304 Not Modified
```

```
> Frame 2200: 389 bytes on wire (3112 bits), 389 bytes captured (3112 bits) on interface \Device\NPF_{16A41E45-1B56-45B4-AB3F-8EF0043451E1}, id 0
> Ethernet II, Src: D-LinkIn_7a:a1:1e (34:0a:33:7a:a1:1e), Dst: IntelCor_4d:f9:81 (3c:58:c2:4d:f9:81)
> Internet Protocol Version 4, Src: 8.241.130.126, Dst: 192.168.0.105
> Transmission Control Protocol, Src Port: 80, Dst Port: 60639, Seq: 337, Ack: 568, Len: 335
> Hypertext Transfer Protocol
```

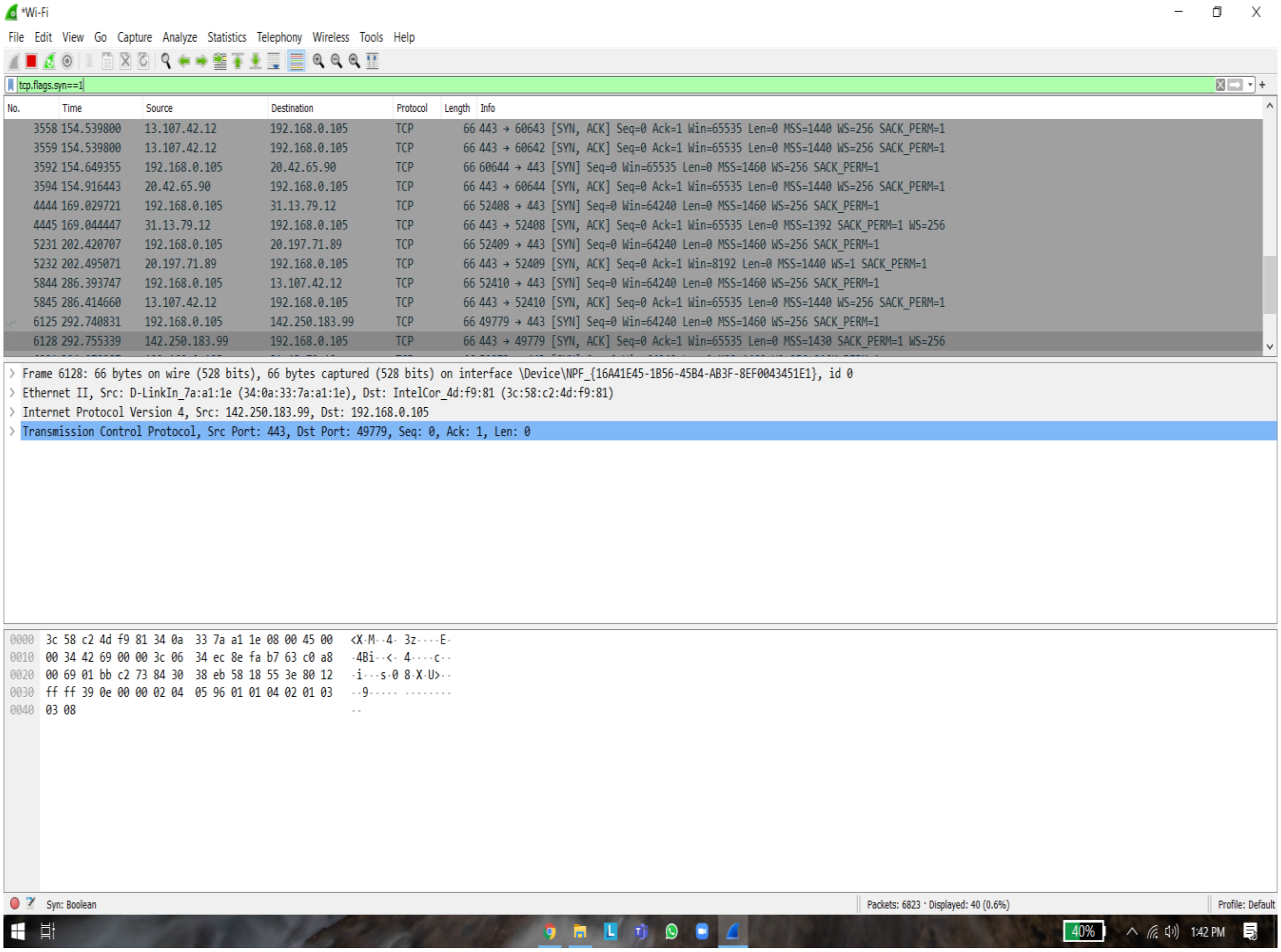
```
0000  3c 58 c2 4d f9 81 34 0a  33 7a a1 1e 08 00 45 00   <X·M··4· 3z····E·
0010  01 77 db 0c 40 00 3d 06  14 f4 08 f1 82 7e c0 a8   ·w··@·=· ·····~··
0020  00 69 00 50 ec df 3f 25  68 14 3d 09 83 c3 50 18   ·i·P··?% h·=···P·
0030  00 3e 66 03 00 00 48 54  54 50 2f 31 2e 31 20 33   ·>f···HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified·
0050  0a 44 61 74 65 3a 20 53  75 6e 2c 20 32 32 20 41   ·Date: S un, 22 A
0060  75 67 20 32 30 32 31 20  30 37 3a 35 34 3a 31 30   ug 2021  07:54:10
0070  20 47 4d 54 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e    GMT··Co nnection
0080  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
0090  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 70 75 62   che-Cont rol: pub
00a0  6c 69 63 2c 20 6d 61 78  2d 61 67 65 3d 39 30 30   lic, max -age=900
00b0  0d 0a 45 54 61 67 3a 20  22 30 64 36 35 34 32 37   ··ETag:  "0d65427
00c0  37 35 66 64 37 31 3a 30  22 0d 0a 45 78 70 69 72   75fd71:0 "··Expir
00d0  65 73 3a 20 53 75 6e 2c  20 32 32 20 41 75 67 20   es: Sun,  22 Aug
```

Hypertext Transfer Protocol: Protocol | Packets: 3206 · Displayed: 8 (0.2%) | Profile: Default

3. Write a DISPLAY filter expression to count all TCP packets (captured under item #1) that have the flags SYN, PSH, and RST set. Show the fraction of packets that had each flag set.

Solution :-

Packet capture filter expression : tcp.flags.syn==1



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

```
tcp.flags.syn==1
```

```
No.   Time        Source          Destination     Protocol Length Info
 3558 154.539800  13.107.42.12    192.168.0.105   TCP      66 443 → 60643 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
 3559 154.539800  13.107.42.12    192.168.0.105   TCP      66 443 → 60642 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
 3592 154.649355  192.168.0.105   20.42.65.90     TCP      66 60644 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 3594 154.916443  20.42.65.90     192.168.0.105   TCP      66 443 → 60644 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
 4444 169.029721  192.168.0.105   31.13.79.12     TCP      66 52408 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 4445 169.044447  31.13.79.12     192.168.0.105   TCP      66 443 → 52408 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1392 SACK_PERM=1 WS=256
 5231 202.420707  192.168.0.105   20.197.71.89    TCP      66 52409 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 5232 202.495071  20.197.71.89    192.168.0.105   TCP      66 443 → 52409 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=1 SACK_PERM=1
 5844 286.393747  192.168.0.105   13.107.42.12    TCP      66 52410 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 5845 286.414660  13.107.42.12    192.168.0.105   TCP      66 443 → 52410 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
 6125 292.740831  192.168.0.105   142.250.183.99  TCP      66 49779 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 6128 292.755339  142.250.183.99  192.168.0.105   TCP      66 443 → 49779 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
```

```
> Frame 6128: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{16A41E45-1B56-45B4-AB3F-8EF0043451E1}, id 0
> Ethernet II, Src: D-LinkIn_7a:a1:1e (34:0a:33:7a:a1:1e), Dst: IntelCor_4d:f9:81 (3c:58:c2:4d:f9:81)
> Internet Protocol Version 4, Src: 142.250.183.99, Dst: 192.168.0.105
> Transmission Control Protocol, Src Port: 443, Dst Port: 49779, Seq: 0, Ack: 1, Len: 0
```

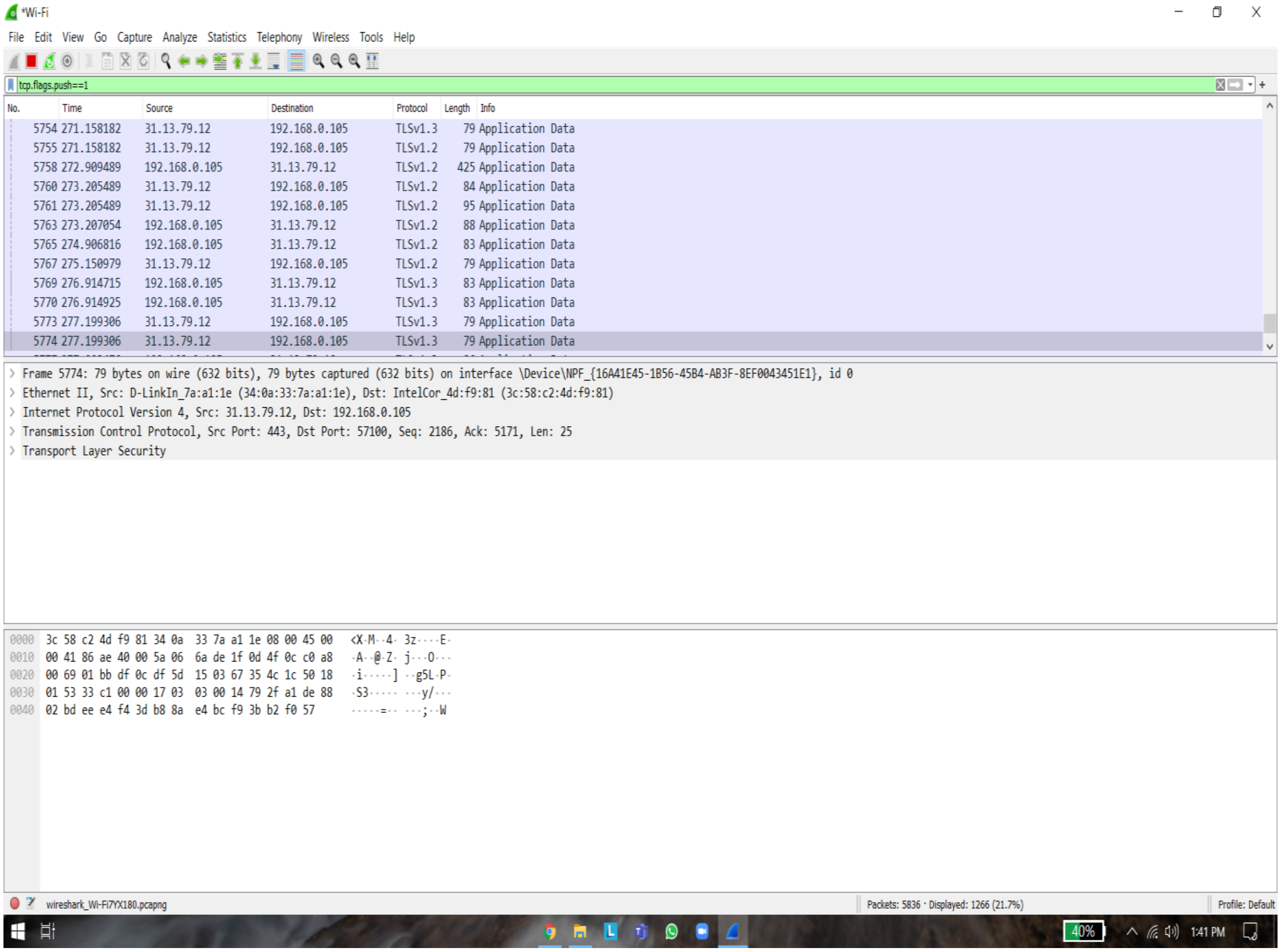
```
0000  3c 58 c2 4d f9 81 34 0a  33 7a a1 1e 08 00 45 00   <X·M··4· 3z····E·
0010  00 34 42 69 00 00 3c 06  34 ec 8e fa b7 63 c0 a8   ·4Bi··<· 4····c··
0020  00 69 01 bb c2 73 84 30  38 eb 58 18 55 3e 80 12   ·i···s·0 8·X·U>··
0030  ff ff 39 0e 00 00 02 04  05 96 01 01 04 02 01 03   ··9····· ········
0040  03 08                                              ··
```

Syn: Boolean

Packets: 6823 · Displayed: 40 (0.6%)

Profile: Default

Packet capture filter expression : tcp.flags.push==1



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

tcp.flags.push==1

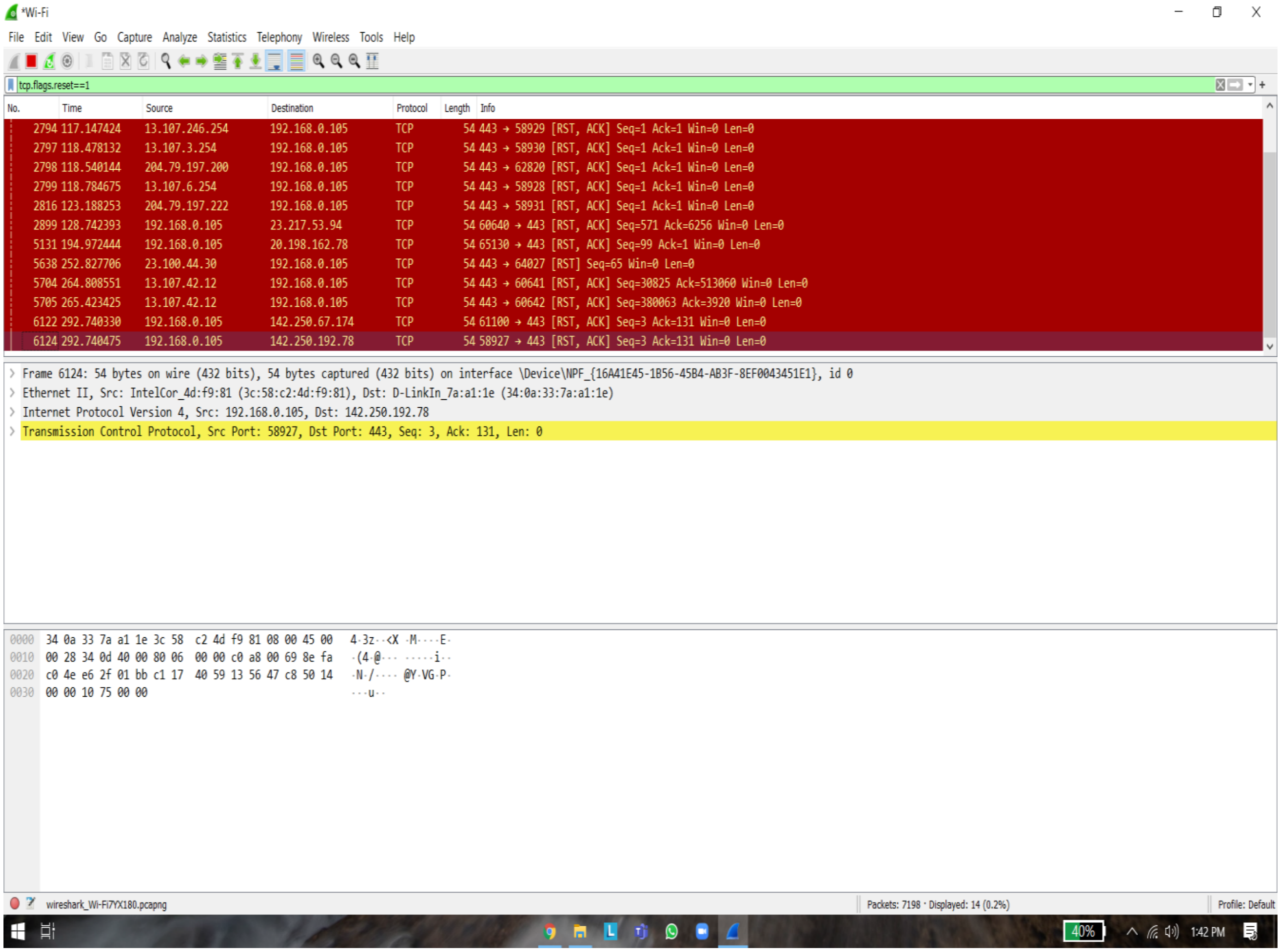
```
No.   Time        Source         Destination    Protocol Length Info
 5754 271.158182  31.13.79.12    192.168.0.105  TLSv1.3    79 Application Data
 5755 271.158182  31.13.79.12    192.168.0.105  TLSv1.2    79 Application Data
 5758 272.909489  192.168.0.105  31.13.79.12    TLSv1.2   425 Application Data
 5760 273.205489  31.13.79.12    192.168.0.105  TLSv1.2    84 Application Data
 5761 273.205489  31.13.79.12    192.168.0.105  TLSv1.2    95 Application Data
 5763 273.207054  192.168.0.105  31.13.79.12    TLSv1.2    88 Application Data
 5765 274.906816  192.168.0.105  31.13.79.12    TLSv1.2    83 Application Data
 5767 275.150979  31.13.79.12    192.168.0.105  TLSv1.2    79 Application Data
 5769 276.914715  192.168.0.105  31.13.79.12    TLSv1.3    83 Application Data
 5770 276.914925  192.168.0.105  31.13.79.12    TLSv1.3    83 Application Data
 5773 277.199306  31.13.79.12    192.168.0.105  TLSv1.3    79 Application Data
 5774 277.199306  31.13.79.12    192.168.0.105  TLSv1.3    79 Application Data
```

```
> Frame 5774: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{16A41E45-1B56-45B4-AB3F-8EF0043451E1}, id 0
> Ethernet II, Src: D-LinkIn_7a:a1:1e (34:0a:33:7a:a1:1e), Dst: IntelCor_4d:f9:81 (3c:58:c2:4d:f9:81)
> Internet Protocol Version 4, Src: 31.13.79.12, Dst: 192.168.0.105
> Transmission Control Protocol, Src Port: 443, Dst Port: 57100, Seq: 2186, Ack: 5171, Len: 25
> Transport Layer Security
```

```
0000  3c 58 c2 4d f9 81 34 0a  33 7a a1 1e 08 00 45 00   <X·M··4· 3z····E·
0010  00 41 86 ae 40 00 5a 06  6a de 1f 0d 4f 0c c0 a8   ·A··@·Z· j···O···
0020  00 69 01 bb df 0c df 5d  15 03 67 35 4c 1c 50 18   ·i·····] ··g5L·P·
0030  01 53 33 c1 00 00 17 03  03 00 14 79 2f a1 de 88   ·S3····· ···y/···
0040  02 bd ee e4 f4 3d b8 8a  e4 bc f9 3b b2 f0 57      ·····=·· ···;··W
```

wireshark_Wi-Fi7YX180.pcapng | Packets: 5836 · Displayed: 1266 (21.7%) | Profile: Default

Packet capture filter expression : tcp.flags.reset==1



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

```
tcp.flags.reset==1
```

```
No.   Time        Source          Destination     Protocol Length Info
 2794 117.147424  13.107.246.254  192.168.0.105   TCP      54 443 → 58929 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 2797 118.478132  13.107.3.254    192.168.0.105   TCP      54 443 → 58930 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 2798 118.540144  204.79.197.200  192.168.0.105   TCP      54 443 → 62820 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 2799 118.784675  13.107.6.254    192.168.0.105   TCP      54 443 → 58928 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 2816 123.188253  204.79.197.222  192.168.0.105   TCP      54 443 → 58931 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 2899 128.742393  192.168.0.105   23.217.53.94    TCP      54 60640 → 443 [RST, ACK] Seq=571 Ack=6256 Win=0 Len=0
 5131 194.972444  192.168.0.105   20.198.162.78   TCP      54 65130 → 443 [RST, ACK] Seq=99 Ack=1 Win=0 Len=0
 5638 252.827706  23.100.44.30    192.168.0.105   TCP      54 443 → 64027 [RST] Seq=65 Win=0 Len=0
 5704 264.808551  13.107.42.12    192.168.0.105   TCP      54 443 → 60641 [RST, ACK] Seq=30825 Ack=513060 Win=0 Len=0
 5705 265.423425  13.107.42.12    192.168.0.105   TCP      54 443 → 60642 [RST, ACK] Seq=380063 Ack=3920 Win=0 Len=0
 6122 292.740330  192.168.0.105   142.250.67.174  TCP      54 61100 → 443 [RST, ACK] Seq=3 Ack=131 Win=0 Len=0
 6124 292.740475  192.168.0.105   142.250.192.78  TCP      54 58927 → 443 [RST, ACK] Seq=3 Ack=131 Win=0 Len=0
```

```
> Frame 6124: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{16A41E45-1B56-45B4-AB3F-8EF0043451E1}, id 0
> Ethernet II, Src: IntelCor_4d:f9:81 (3c:58:c2:4d:f9:81), Dst: D-LinkIn_7a:a1:1e (34:0a:33:7a:a1:1e)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 142.250.192.78
> Transmission Control Protocol, Src Port: 58927, Dst Port: 443, Seq: 3, Ack: 131, Len: 0
```

```
0000  34 0a 33 7a a1 1e 3c 58  c2 4d f9 81 08 00 45 00   4·3z··<X ·M····E·
0010  00 28 34 0d 40 00 80 06  00 00 c0 a8 00 69 8e fa   ·(4·@··· ·····i··
0020  c0 4e e6 2f 01 bb c1 17  40 59 13 56 47 c8 50 14   ·N·/···· @Y·VG·P·
0030  00 00 10 75 00 00                                  ···u··
```

wireshark_Wi-Fi7YX180.pcapng

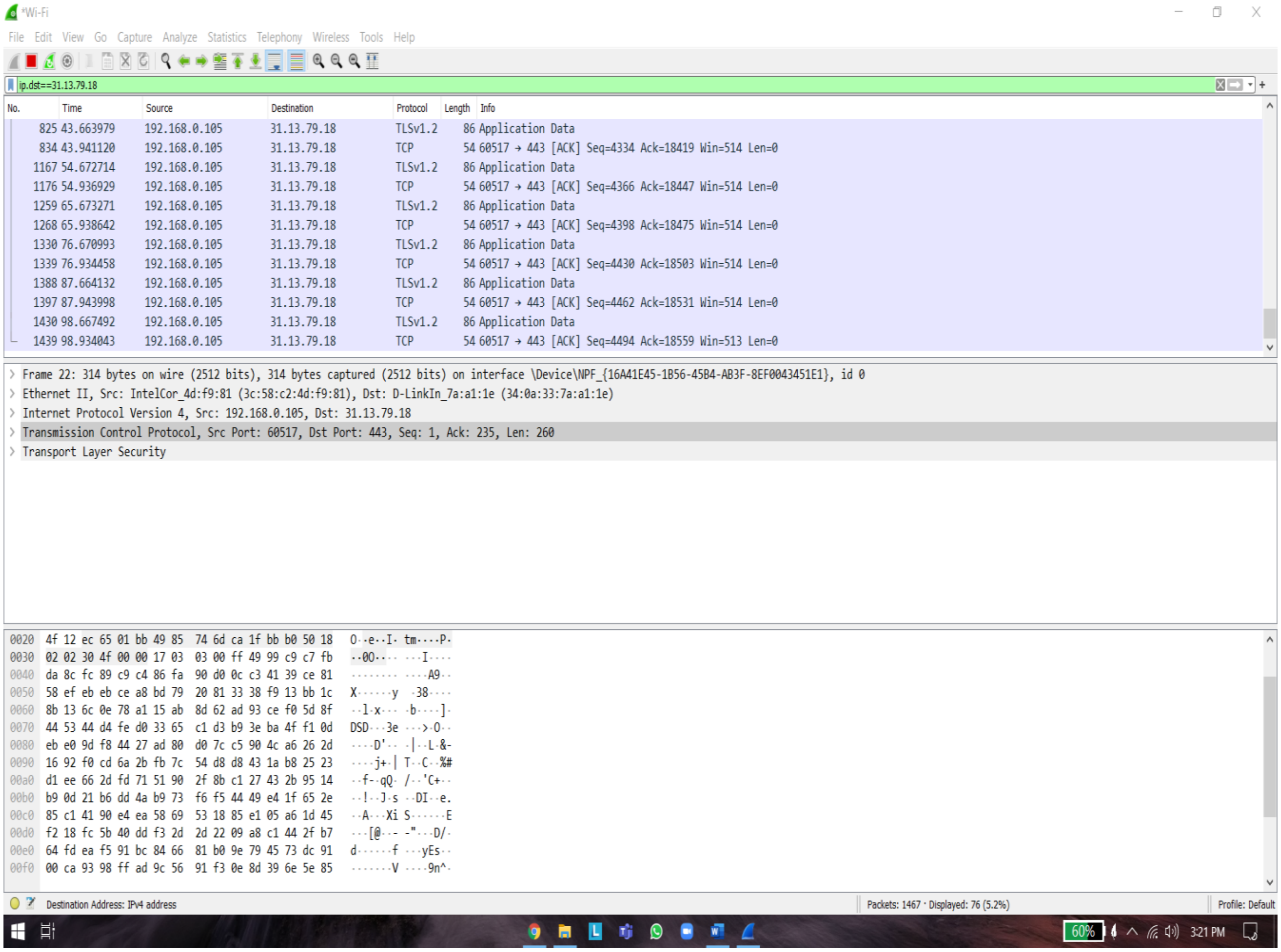
Packets: 7198 · Displayed: 14 (0.2%)

Profile: Default

4. Count how many TCP packets you received from / sent to Face book, and how many of each were also HTTP packets.

Solution :-

Packet capture filter expression : ip.dst==31.13.79.18



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

```
ip.dst==31.13.79.18
```

```
No.   Time        Source         Destination   Protocol  Length Info
  825 43.663979   192.168.0.105  31.13.79.18   TLSv1.2   86 Application Data
  834 43.941120   192.168.0.105  31.13.79.18   TCP       54 60517 → 443 [ACK] Seq=4334 Ack=18419 Win=514 Len=0
 1167 54.672714   192.168.0.105  31.13.79.18   TLSv1.2   86 Application Data
 1176 54.936929   192.168.0.105  31.13.79.18   TCP       54 60517 → 443 [ACK] Seq=4366 Ack=18447 Win=514 Len=0
 1259 65.673271   192.168.0.105  31.13.79.18   TLSv1.2   86 Application Data
 1268 65.938642   192.168.0.105  31.13.79.18   TCP       54 60517 → 443 [ACK] Seq=4398 Ack=18475 Win=514 Len=0
 1330 76.670993   192.168.0.105  31.13.79.18   TLSv1.2   86 Application Data
 1339 76.934458   192.168.0.105  31.13.79.18   TCP       54 60517 → 443 [ACK] Seq=4430 Ack=18503 Win=514 Len=0
 1388 87.664132   192.168.0.105  31.13.79.18   TLSv1.2   86 Application Data
 1397 87.943998   192.168.0.105  31.13.79.18   TCP       54 60517 → 443 [ACK] Seq=4462 Ack=18531 Win=514 Len=0
 1430 98.667492   192.168.0.105  31.13.79.18   TLSv1.2   86 Application Data
 1439 98.934043   192.168.0.105  31.13.79.18   TCP       54 60517 → 443 [ACK] Seq=4494 Ack=18559 Win=513 Len=0
```

```
> Frame 22: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits) on interface \Device\NPF_{16A41E45-1B56-45B4-AB3F-8EF0043451E1}, id 0
> Ethernet II, Src: IntelCor_4d:f9:81 (3c:58:c2:4d:f9:81), Dst: D-LinkIn_7a:a1:1e (34:0a:33:7a:a1:1e)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 31.13.79.18
> Transmission Control Protocol, Src Port: 60517, Dst Port: 443, Seq: 1, Ack: 235, Len: 260
> Transport Layer Security
```

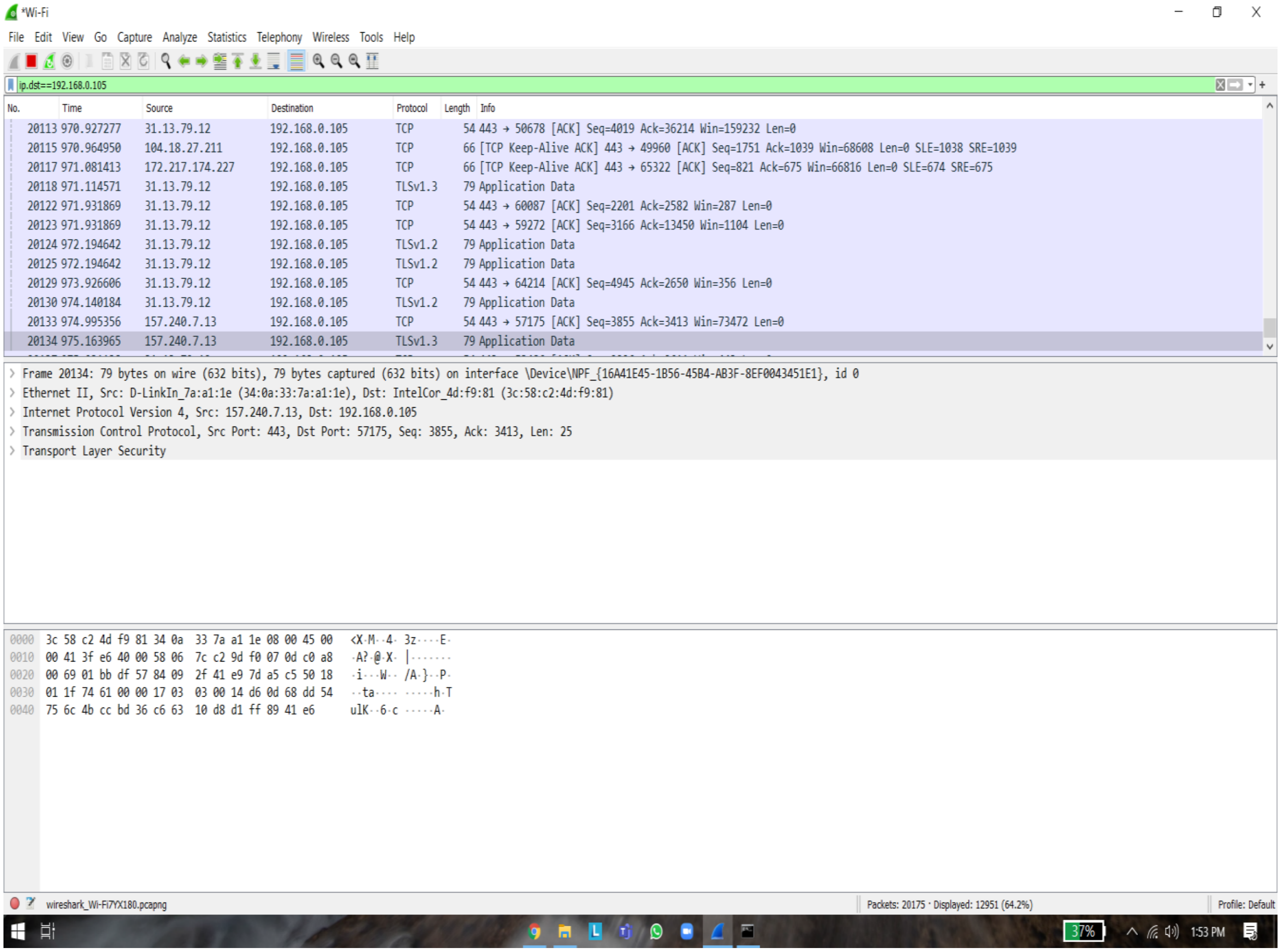
```
0020  4f 12 ec 65 01 bb 49 85  74 6d ca 1f bb b0 50 18   O··e··I· tm····P·
0030  02 02 30 4f 00 00 17 03  03 00 ff 49 99 c9 c7 fb   ··0O···· ···I····
0040  da 8c fc 89 c9 c4 86 fa  90 d0 0c c3 41 39 ce 81   ········ ····A9··
0050  58 ef eb eb ce a8 bd 79  20 81 33 38 f9 13 bb 1c   X······y  ·38····
0060  8b 13 6c 0e 78 a1 15 ab  8d 62 ad 93 ce f0 5d 8f   ··l·x··· ·b····]·
0070  44 53 44 d4 fe d0 33 65  c1 d3 b9 3e ba 4f f1 0d   DSD···3e ···>·O··
0080  eb e0 9d f8 44 27 ad 80  d0 7c c5 90 4c a6 26 2d   ····D'·· ·|··L·&-
0090  16 92 f0 cd 6a 2b fb 7c  54 d8 d8 43 1a b8 25 23   ····j+·| T··C··%#
00a0  d1 ee 66 2d fd 71 51 90  2f 8b c1 27 43 2b 95 14   ··f-·qQ· /··'C+··
00b0  b9 0d 21 b6 dd 4a b9 73  f6 f5 44 49 e4 1f 65 2e   ··!··J·s ··DI··e.
00c0  85 c1 41 90 e4 ea 58 69  53 18 85 e1 05 a6 1d 45   ··A···Xi S······E
00d0  f2 18 fc 5b 40 dd f3 2d  2d 22 09 a8 c1 44 2f b7   ···[@··- -"···D/·
00e0  64 fd ea f5 91 bc 84 66  81 b0 9e 79 45 73 dc 91   d······f ···yEs··
00f0  00 ca 93 98 ff ad 9c 56  91 f3 0e 8d 39 6e 5e 85   ·······V ····9n^·
```

Destination Address: IPv4 address

Packets: 1467 · Displayed: 76 (5.2%)

Profile: Default

Packet capture filter expression : ip.dst==192.168.0.105



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

ip.dst==192.168.0.105

```
No.   Time        Source           Destination     Protocol Length Info
20113 970.927277  31.13.79.12      192.168.0.105   TCP      54 443 → 50678 [ACK] Seq=4019 Ack=36214 Win=159232 Len=0
20115 970.964950  104.18.27.211    192.168.0.105   TCP      66 [TCP Keep-Alive ACK] 443 → 49960 [ACK] Seq=1751 Ack=1039 Win=68608 Len=0 SLE=1038 SRE=1039
20117 971.081413  172.217.174.227  192.168.0.105   TCP      66 [TCP Keep-Alive ACK] 443 → 65322 [ACK] Seq=821 Ack=675 Win=66816 Len=0 SLE=674 SRE=675
20118 971.114571  31.13.79.12      192.168.0.105   TLSv1.3  79 Application Data
20122 971.931869  31.13.79.12      192.168.0.105   TCP      54 443 → 60087 [ACK] Seq=2201 Ack=2582 Win=287 Len=0
20123 971.931869  31.13.79.12      192.168.0.105   TCP      54 443 → 59272 [ACK] Seq=3166 Ack=13450 Win=1104 Len=0
20124 972.194642  31.13.79.12      192.168.0.105   TLSv1.2  79 Application Data
20125 972.194642  31.13.79.12      192.168.0.105   TLSv1.2  79 Application Data
20129 973.926606  31.13.79.12      192.168.0.105   TCP      54 443 → 64214 [ACK] Seq=4945 Ack=2650 Win=356 Len=0
20130 974.140184  31.13.79.12      192.168.0.105   TLSv1.2  79 Application Data
20133 974.995356  157.240.7.13     192.168.0.105   TCP      54 443 → 57175 [ACK] Seq=3855 Ack=3413 Win=73472 Len=0
20134 975.163965  157.240.7.13     192.168.0.105   TLSv1.3  79 Application Data
```

```
> Frame 20134: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{16A41E45-1B56-45B4-AB3F-8EF0043451E1}, id 0
> Ethernet II, Src: D-LinkIn_7a:a1:1e (34:0a:33:7a:a1:1e), Dst: IntelCor_4d:f9:81 (3c:58:c2:4d:f9:81)
> Internet Protocol Version 4, Src: 157.240.7.13, Dst: 192.168.0.105
> Transmission Control Protocol, Src Port: 443, Dst Port: 57175, Seq: 3855, Ack: 3413, Len: 25
> Transport Layer Security
```

```
0000  3c 58 c2 4d f9 81 34 0a  33 7a a1 1e 08 00 45 00   <X·M··4· 3z····E·
0010  00 41 3f e6 40 00 58 06  7c c2 9d f0 07 0d c0 a8   ·A?·@·X· |·······
0020  00 69 01 bb df 57 84 09  2f 41 e9 7d a5 c5 50 18   ·i···W·· /A·}··P·
0030  01 1f 74 61 00 00 17 03  03 00 14 d6 0d 68 dd 54   ··ta···· ·····h·T
0040  75 6c 4b cc bd 36 c6 63  10 d8 d1 ff 89 41 e6      ulK··6·c ·····A·
```

wireshark_Wi-Fi7YX180.pcapng   Packets: 20175 · Displayed: 12951 (64.2%)   Profile: Default