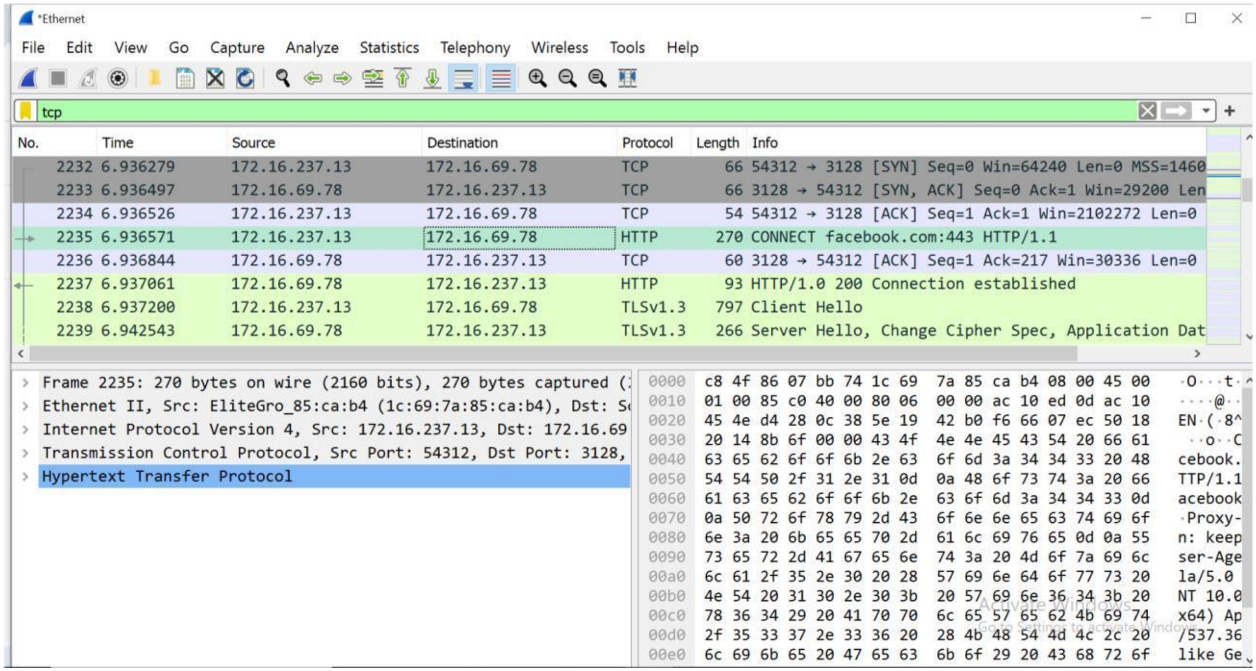
Name: Vedant Sanjay Dhamale
Roll No. 2337015
Title: Capture packets using Wireshark, write the exact packet capture filter expressions to accomplish. Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account .

Output:-

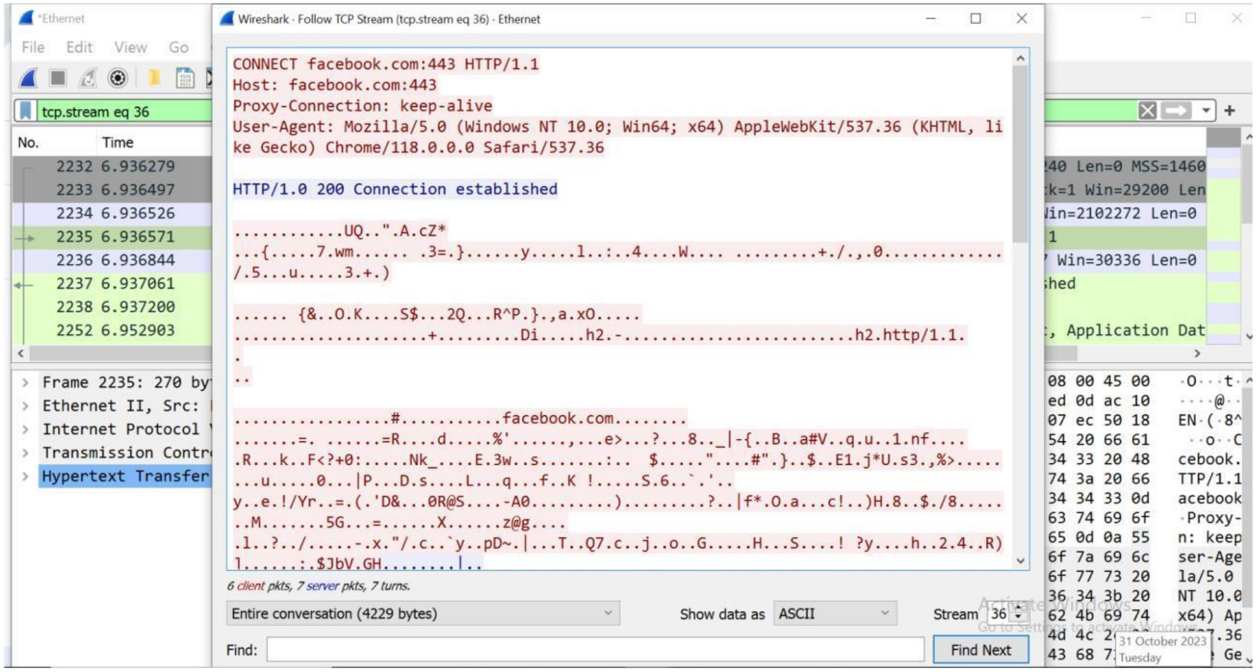

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

```
No.   Time        Source          Destination     Protocol  Length Info
2232 6.936279   172.16.237.13   172.16.69.78    TCP        66 54312 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2233 6.936497   172.16.69.78    172.16.237.13   TCP        66 3128 → 54312 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len
2234 6.936526   172.16.237.13   172.16.69.78    TCP        54 54312 → 3128 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
2235 6.936571   172.16.237.13   172.16.69.78    HTTP      270 CONNECT facebook.com:443 HTTP/1.1
2236 6.936844   172.16.69.78    172.16.237.13   TCP        60 3128 → 54312 [ACK] Seq=1 Ack=217 Win=30336 Len=0
2237 6.937061   172.16.69.78    172.16.237.13   HTTP       93 HTTP/1.0 200 Connection established
2238 6.937200   172.16.237.13   172.16.69.78    TLSv1.3   797 Client Hello
2239 6.942543   172.16.69.78    172.16.237.13   TLSv1.3   266 Server Hello, Change Cipher Spec, Application Dat
```

```
> Frame 2235: 270 bytes on wire (2160 bits), 270 bytes captured (:
> Ethernet II, Src: EliteGro_85:ca:b4 (1c:69:7a:85:ca:b4), Dst: S
> Internet Protocol Version 4, Src: 172.16.237.13, Dst: 172.16.69
> Transmission Control Protocol, Src Port: 54312, Dst Port: 3128,
> Hypertext Transfer Protocol
```

```
0000  c8 4f 86 07 bb 74 1c 69  7a 85 ca b4 08 00 45 00   ·O···t·
0010  01 00 85 c0 40 00 80 06  00 00 ac 10 ed 0d ac 10   ····@··
0020  45 4e d4 28 0c 38 5e 19  42 b0 f6 66 07 ec 50 18   EN·(·8^
0030  20 14 8b 6f 00 00 43 4f  4e 4e 45 43 54 20 66 61    ··o··C
0040  63 65 62 6f 6f 6b 2e 63  6f 6d 3a 34 34 33 20 48   cebook.
0050  54 54 50 2f 31 2e 31 0d  0a 48 6f 73 74 3a 20 66   TTP/1.1
0060  61 63 65 62 6f 6f 6b 2e  63 6f 6d 3a 34 34 33 0d   acebook
0070  0a 50 72 6f 78 79 2d 43  6f 6e 6e 65 63 74 69 6f   ·Proxy-
0080  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep
0090  73 65 72 2d 41 67 65 6e  74 3a 20 4d 6f 7a 69 6c   ser-Age
00a0  6c 61 2f 35 2e 30 20 28  57 69 6e 64 6f 77 73 20   la/5.0
00b0  4e 54 20 31 30 2e 30 3b  20 57 69 6e 36 34 3b 20   NT 10.0
00c0  78 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   x64) Ap
00d0  2f 35 33 37 2e 33 36 20  28 4b 48 54 4d 4c 2c 20   /537.36
00e0  6c 69 6b 65 20 47 65 63  6b 6f 29 20 43 68 72 6f   like Ge
```



tcp.stream eq 36

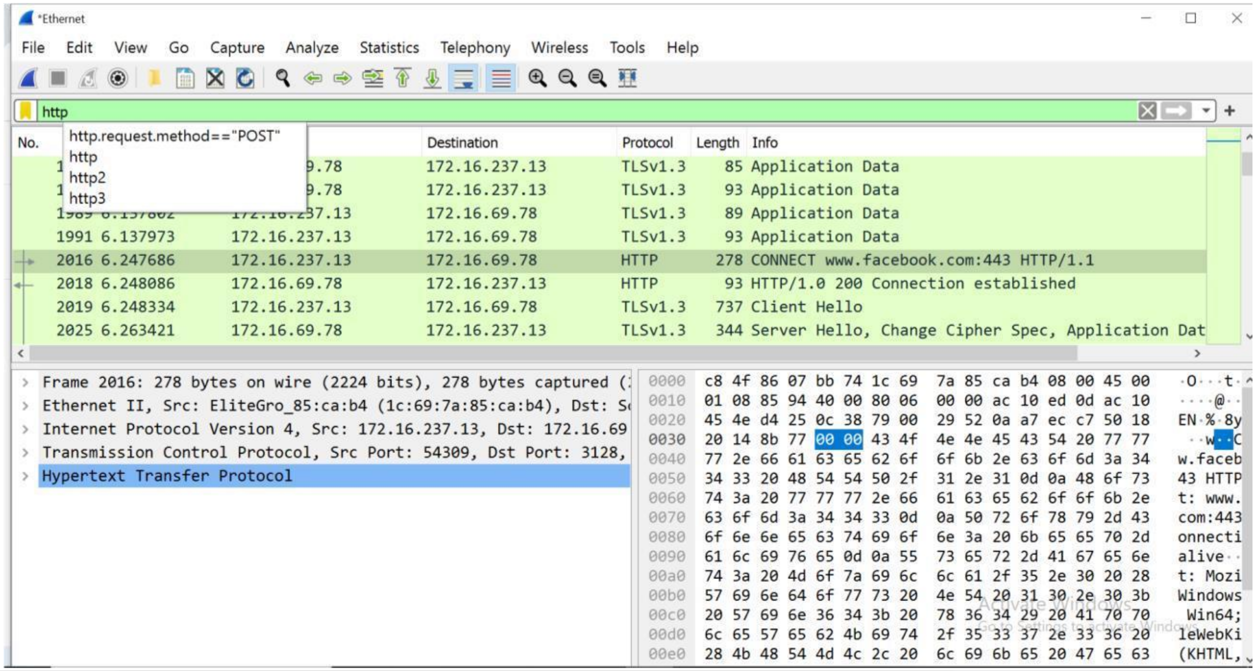
```
CONNECT facebook.com:443 HTTP/1.1
Host: facebook.com:443
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
ke Gecko) Chrome/118.0.0.0 Safari/537.36

HTTP/1.0 200 Connection established

...........UQ..".A.cZ*
...{.....7.wm...... .3=.}......y.....l..:..4....W.... .........+./.,.0............
/.5...u.....3.+.)

...... {&..O.K....S$...2Q...R^P.}.,a.xO.....
....................+.........Di.....h2.-.........................h2.http/1.1.
.
..

................#..........facebook.com........
.......=. ......=R....d.....%'.......,...e>...?...8.._|-{..B..a#V..q.u..1.nf....
.R...k..F<?+0:.....Nk_....E.3w..s.......:..  $....."....#".}..$..E1.j*U.s3.,%>.....
...u.....0...|P...D.s....L...q...f..K !.....S.6..`.'..
y..e.!/Yr..=.(.'D&...0R@S....-A0.........).........?..|f*.O.a...c!..)H.8..$./8.....
..M.......5G...=......X......z@g....
.l..?../.....-.x."/.c..`y..pD~.|...T..Q7.c..j..o..G.....H...S....! ?y....h..2.4..R)
l......:.$JbV.GH........|..
```

6 client pkts, 7 server pkts, 7 turns.

Entire conversation (4229 bytes)   Show data as ASCII   Stream 36

Find: Find Next

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

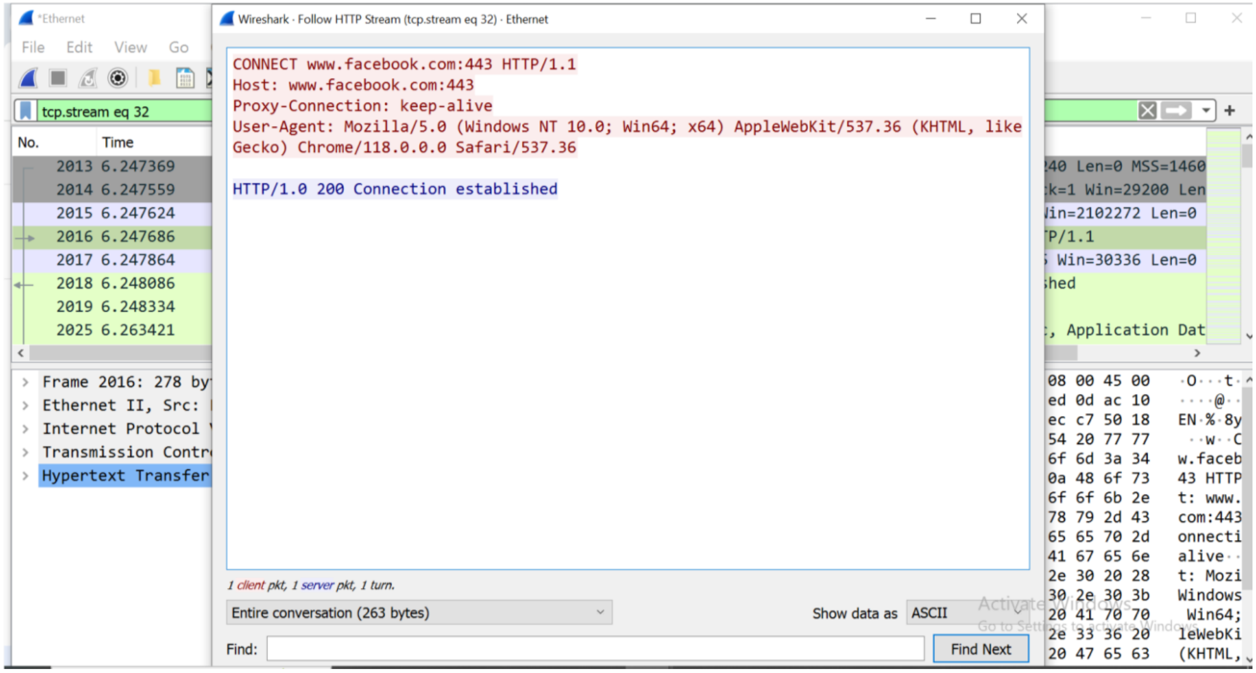


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http.request.method=="POST"
http
http2
http3

```
No.                            Destination      Protocol  Length Info
 1            ...9.78          172.16.237.13    TLSv1.3    85 Application Data
 1            ...9.78          172.16.237.13    TLSv1.3    93 Application Data
 1989 6.137862  172.16.237.13  172.16.69.78     TLSv1.3    89 Application Data
 1991 6.137973  172.16.237.13  172.16.69.78     TLSv1.3    93 Application Data
 2016 6.247686  172.16.237.13  172.16.69.78     HTTP      278 CONNECT www.facebook.com:443 HTTP/1.1
 2018 6.248086  172.16.69.78   172.16.237.13    HTTP       93 HTTP/1.0 200 Connection established
 2019 6.248334  172.16.237.13  172.16.69.78     TLSv1.3   737 Client Hello
 2025 6.263421  172.16.69.78   172.16.237.13    TLSv1.3   344 Server Hello, Change Cipher Spec, Application Dat
```

```
> Frame 2016: 278 bytes on wire (2224 bits), 278 bytes captured (
> Ethernet II, Src: EliteGro_85:ca:b4 (1c:69:7a:85:ca:b4), Dst: S
> Internet Protocol Version 4, Src: 172.16.237.13, Dst: 172.16.69
> Transmission Control Protocol, Src Port: 54309, Dst Port: 3128,
> Hypertext Transfer Protocol
```

```
0000  c8 4f 86 07 bb 74 1c 69  7a 85 ca b4 08 00 45 00   ·O···t·
0010  01 08 85 94 40 00 80 06  00 00 ac 10 ed 0d ac 10   ····@··
0020  45 4e d4 25 0c 38 79 00  29 52 0a a7 ec c7 50 18   EN·%·8y
0030  20 14 8b 77 00 00 43 4f  4e 4e 45 43 54 20 77 77    ··w··C
0040  77 2e 66 61 63 65 62 6f  6f 6b 2e 63 6f 6d 3a 34   w.faceb
0050  34 33 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   43 HTTP
0060  74 3a 20 77 77 77 2e 66  61 63 65 62 6f 6f 6b 2e   t: www.
0070  63 6f 6d 3a 34 34 33 0d  0a 50 72 6f 78 79 2d 43   com:443
0080  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnecti
0090  61 6c 69 76 65 0d 0a 55  73 65 72 2d 41 67 65 6e   alive··
00a0  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozi
00b0  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows
00c0  20 57 69 6e 36 34 3b 20  78 36 34 29 20 41 70 70    Win64;
00d0  6c 65 57 65 62 4b 69 74  2f 35 33 37 2e 33 36 20   leWebKi
00e0  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65 20 47 65 63   (KHTML,
```



*Ethernet
File Edit View Go
tcp.stream eq 32
Wireshark · Follow HTTP Stream (tcp.stream eq 32) · Ethernet

```
No.  Time
2013 6.247369                    ...40 Len=0 MSS=1460
2014 6.247559                    ...k=1 Win=29200 Len
2015 6.247624                    ...Win=2102272 Len=0
2016 6.247686                    ...P/1.1
2017 6.247864                    ... Win=30336 Len=0
2018 6.248086                    ...hed
2019 6.248334
2025 6.263421                    ..., Application Dat

> Frame 2016: 278 by
> Ethernet II, Src:
> Internet Protocol
> Transmission Contr
> Hypertext Transfer
```

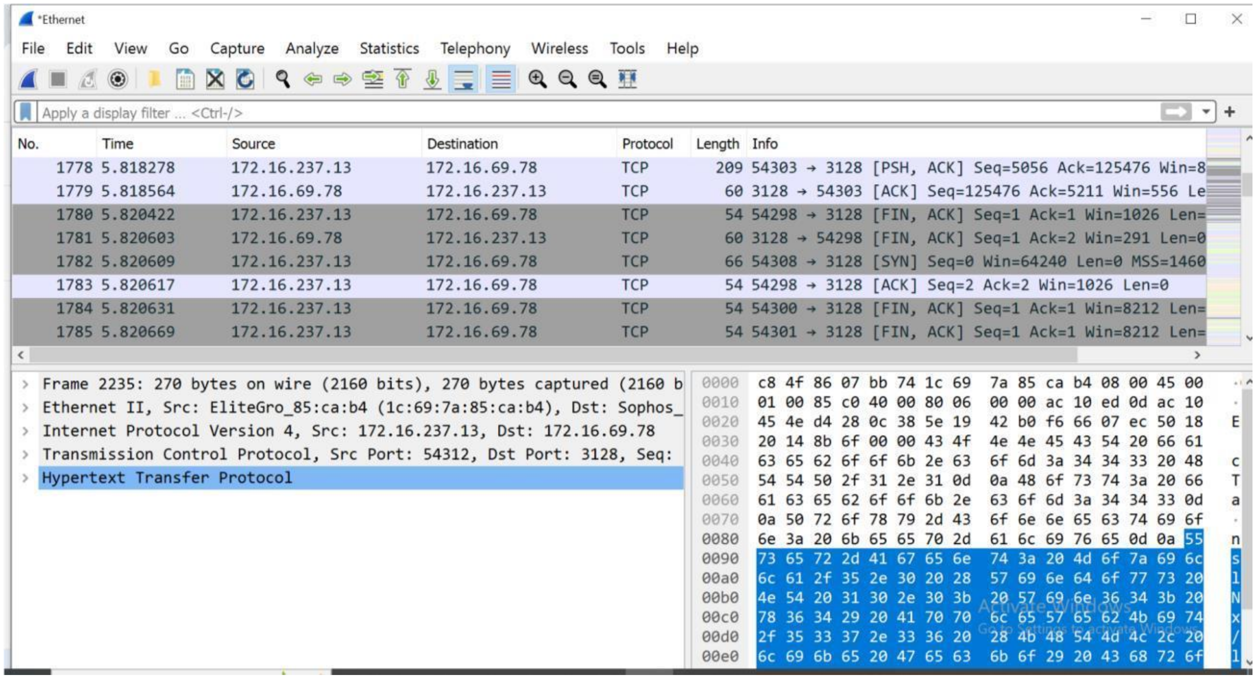
```
CONNECT www.facebook.com:443 HTTP/1.1
Host: www.facebook.com:443
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/118.0.0.0 Safari/537.36

HTTP/1.0 200 Connection established
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (263 bytes)　Show data as ASCII

Find: 　Find Next

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.

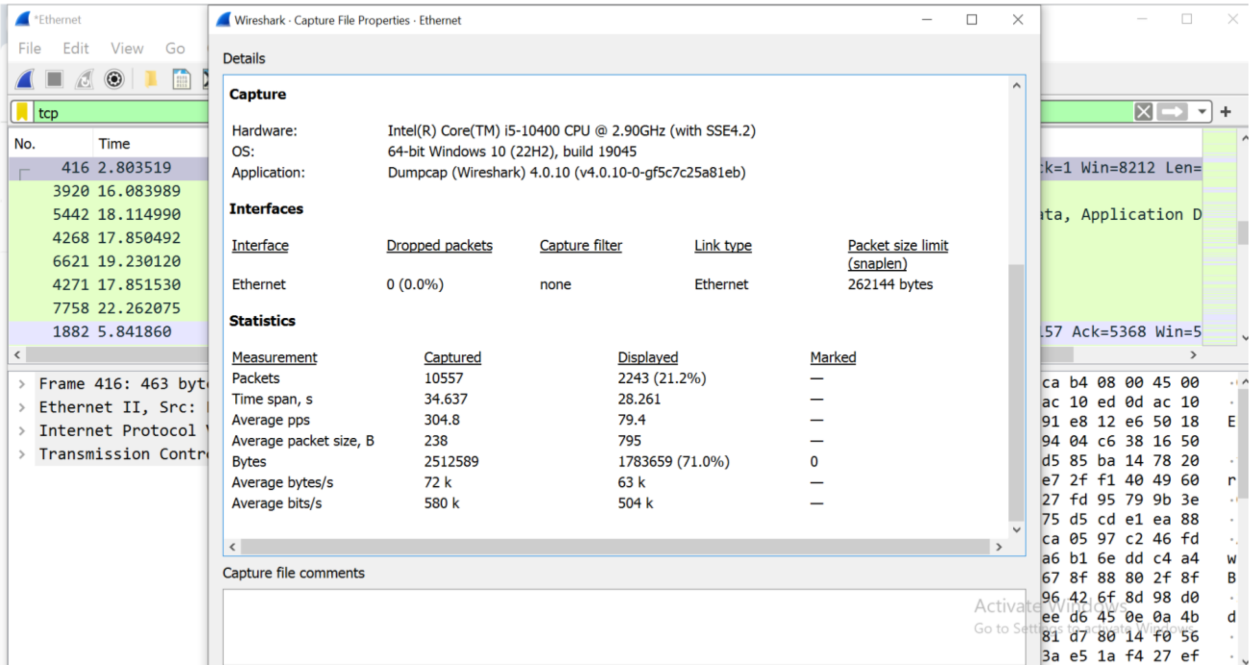

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source          Destination     Protocol Length Info
 1778 5.818278  172.16.237.13   172.16.69.78    TCP      209 54303 → 3128 [PSH, ACK] Seq=5056 Ack=125476 Win=8
 1779 5.818564  172.16.69.78    172.16.237.13   TCP       60 3128 → 54303 [ACK] Seq=125476 Ack=5211 Win=556 Le
 1780 5.820422  172.16.237.13   172.16.69.78    TCP       54 54298 → 3128 [FIN, ACK] Seq=1 Ack=1 Win=1026 Len=
 1781 5.820603  172.16.69.78    172.16.237.13   TCP       60 3128 → 54298 [FIN, ACK] Seq=1 Ack=2 Win=291 Len=0
 1782 5.820609  172.16.237.13   172.16.69.78    TCP       66 54308 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
 1783 5.820617  172.16.237.13   172.16.69.78    TCP       54 54298 → 3128 [ACK] Seq=2 Ack=2 Win=1026 Len=0
 1784 5.820631  172.16.237.13   172.16.69.78    TCP       54 54300 → 3128 [FIN, ACK] Seq=1 Ack=1 Win=8212 Len=
 1785 5.820669  172.16.237.13   172.16.69.78    TCP       54 54301 → 3128 [FIN, ACK] Seq=1 Ack=1 Win=8212 Len=
```

```
> Frame 2235: 270 bytes on wire (2160 bits), 270 bytes captured (2160 b
> Ethernet II, Src: EliteGro_85:ca:b4 (1c:69:7a:85:ca:b4), Dst: Sophos_
> Internet Protocol Version 4, Src: 172.16.237.13, Dst: 172.16.69.78
> Transmission Control Protocol, Src Port: 54312, Dst Port: 3128, Seq:
> Hypertext Transfer Protocol
```

```
0000  c8 4f 86 07 bb 74 1c 69  7a 85 ca b4 08 00 45 00
0010  01 00 85 c0 40 00 80 06  00 00 ac 10 ed 0d ac 10
0020  45 4e d4 28 0c 38 5e 19  42 b0 f6 66 07 ec 50 18   E
0030  20 14 8b 6f 00 00 43 4f  4e 4e 45 43 54 20 66 61
0040  63 65 62 6f 6f 6b 2e 63  6f 6d 3a 34 34 33 20 48   c
0050  54 54 50 2f 31 2e 31 0d  0a 48 6f 73 74 3a 20 66   T
0060  61 63 65 62 6f 6f 6b 2e  63 6f 6d 3a 34 34 33 0d   a
0070  0a 50 72 6f 78 79 2d 43  6f 6e 6e 65 63 74 69 6f
0080  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n
0090  73 65 72 2d 41 67 65 6e  74 3a 20 4d 6f 7a 69 6c   s
00a0  6c 61 2f 35 2e 30 20 28  57 69 6e 64 6f 77 73 20   l
00b0  4e 54 20 31 30 2e 30 3b  20 57 69 6e 36 34 3b 20   N
00c0  78 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   x
00d0  2f 35 33 37 2e 33 36 20  28 4b 48 54 4d 4c 2c 20   /
00e0  6c 69 6b 65 20 47 65 63  6b 6f 29 20 43 68 72 6f   l
```

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



tcp

```
No.   Time
  416 2.803519
 3920 16.083989
 5442 18.114990
 4268 17.850492
 6621 19.230120
 4271 17.851530
 7758 22.262075
 1882 5.841860
```

```
> Frame 416: 463 byt
> Ethernet II, Src:
> Internet Protocol
> Transmission Contr
```

```
k=1 Win=8212 Len=
ta, Application D
57 Ack=5368 Win=5
```

```
ca b4 08 00 45 00
ac 10 ed 0d ac 10
91 e8 12 e6 50 18   E
94 04 c6 38 16 50
d5 85 ba 14 78 20
e7 2f f1 40 49 60   r
27 fd 95 79 9b 3e
75 d5 cd e1 ea 88
ca 05 97 c2 46 fd
a6 b1 6e dd c4 a4   w
67 8f 88 80 2f 8f   B
96 42 6f 8d 98 d0
ee d6 45 0e 0a 4b   d
81 d7 80 14 f0 56
3a e5 1a f4 27 ef
```

Capture

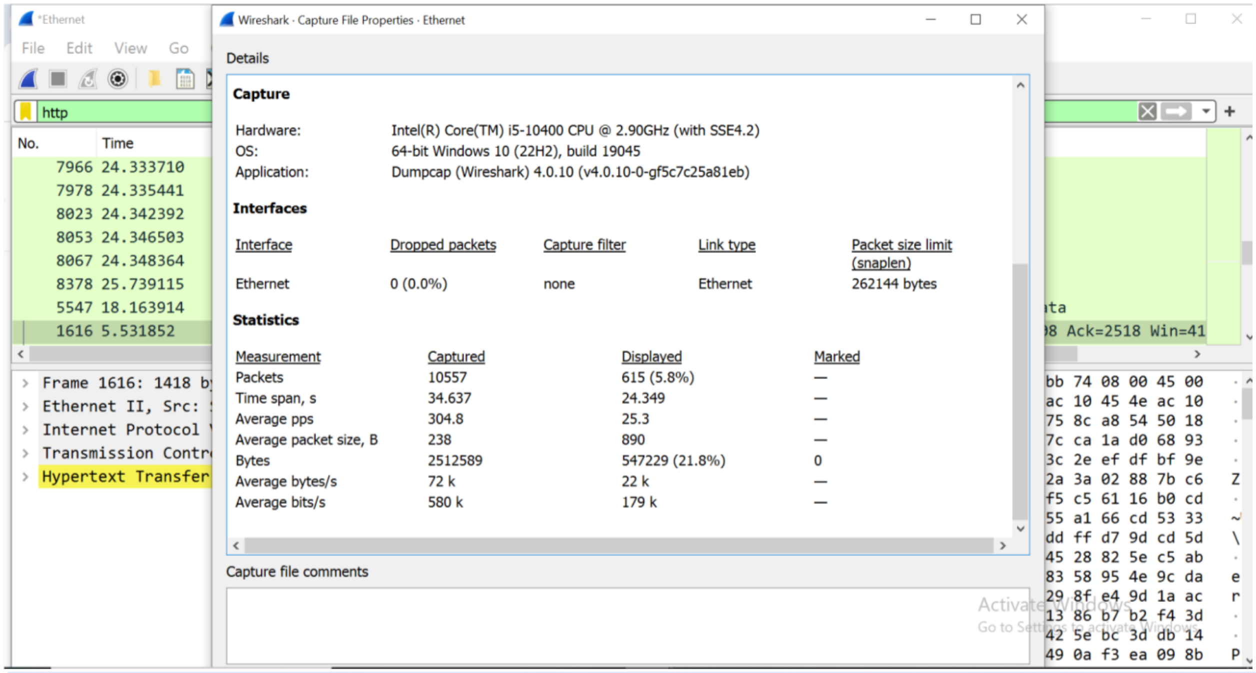
Hardware:	Intel(R) Core(TM) i5-10400 CPU @ 2.90GHz (with SSE4.2)
OS:	64-bit Windows 10 (22H2), build 19045
Application:	Dumpcap (Wireshark) 4.0.10 (v4.0.10-0-gf5c7c25a81eb)

Interfaces

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

Statistics

Measurement	Captured	Displayed	Marked
Packets	10557	2243 (21.2%)	—
Time span, s	34.637	28.261	—
Average pps	304.8	79.4	—
Average packet size, B	238	795	—
Bytes	2512589	1783659 (71.0%)	0
Average bytes/s	72 k	63 k	—
Average bits/s	580 k	504 k	—



```
No.       Time
    7966 24.333710
    7978 24.335441
    8023 24.342392
    8053 24.346503
    8067 24.348364
    8378 25.739115
    5547 18.163914
    1616 5.531852
```

```
ata
98 Ack=2518 Win=41
```

```
> Frame 1616: 1418 by
> Ethernet II, Src: 
> Internet Protocol 
> Transmission Contr
> Hypertext Transfer
```

```
bb 74 08 00 45 00   ·
ac 10 45 4e ac 10   ·
75 8c a8 54 50 18   ·
7c ca 1a d0 68 93   ·
3c 2e ef df bf 9e   ·
2a 3a 02 88 7b c6   Z
f5 c5 61 16 b0 cd   ·
55 a1 66 cd 53 33   ~
dd ff d7 9d cd 5d   \
45 28 82 5e c5 ab   ·
83 58 95 4e 9c da   e
29 8f e4 9d 1a ac   r
13 86 b7 b2 f4 3d   ·
42 5e bc 3d db 14   ·
49 0a f3 ea 09 8b   P
```

Details

Capture

Hardware:	Intel(R) Core(TM) i5-10400 CPU @ 2.90GHz (with SSE4.2)
OS:	64-bit Windows 10 (22H2), build 19045
Application:	Dumpcap (Wireshark) 4.0.10 (v4.0.10-0-gf5c7c25a81eb)

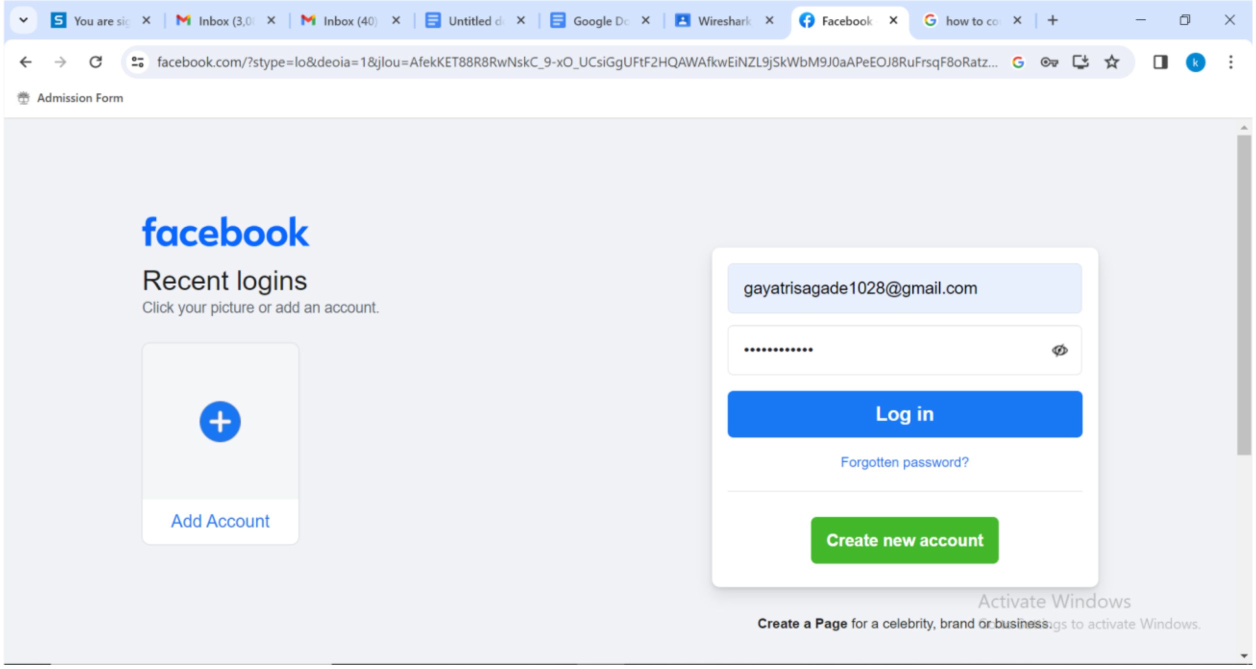
Interfaces

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

Statistics

Measurement	Captured	Displayed	Marked
Packets	10557	615 (5.8%)	—
Time span, s	34.637	24.349	—
Average pps	304.8	25.3	—
Average packet size, B	238	890	—
Bytes	2512589	547229 (21.8%)	0
Average bytes/s	72 k	22 k	—
Average bits/s	580 k	179 k	—

Capture file comments



facebook.com/?stype=lo&deoia=1&jlou=AfekKET88R8RwNskC_9-xO_UCsiGgUFtF2HQAWAfkwEiNZL9jSkWbM9J0aAPeEOJ8RuFrsqF8oRatz...

Recent logins

Click your picture or add an account.

gayatrisagade1028@gmail.com

•••••••••••••

Create a Page for a celebrity, brand or business.