Firstly, we fetch the ip address of Facebook using either of the following 2 methods: (Type on your terminal):

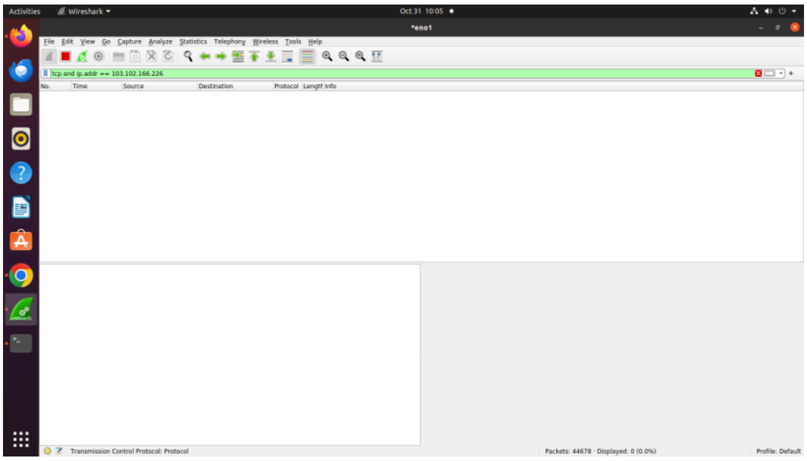
- ping www.facebook.com

OR

- host www.facebook.com

The above mentioned steps will give you the ip address of your site.
Now, open the wireshark application and choose eno1 as capturing option and write the following command :
tcp && ip.addr == <address of site you received from your terminal>

Now, there might a case, you may get the following blank outputs (as shown in the following two images):


Activities
Wireshark
Oct 31 10:05
*eno1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

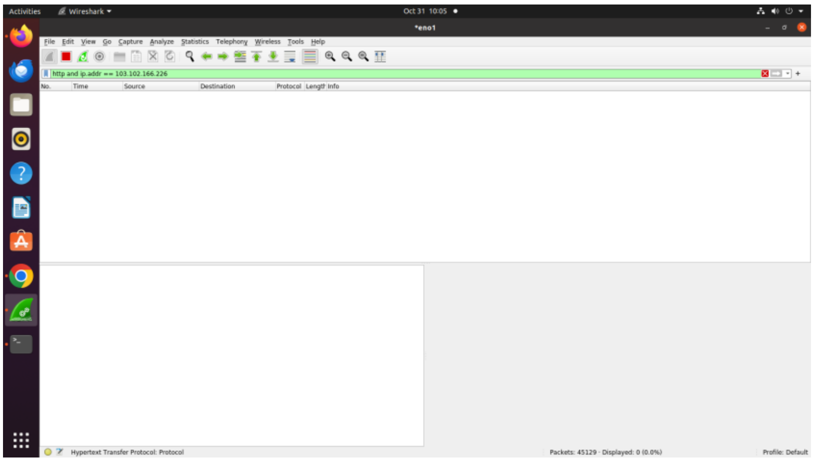
tcp and ip.addr == 103.102.166.226

No. Time Source Destination Protocol Length Info

Transmission Control Protocol: Protocol

Packets: 44678 · Displayed: 0 (0.0%)

Profile: Default


Activities
Wireshark
Oct 31 10:05
*eno1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http and ip.addr == 103.102.166.226

No. Time Source Destination Protocol Length Info

Hypertext Transfer Protocol: Protocol

Packets: 45129 · Displayed: 0 (0.0%)

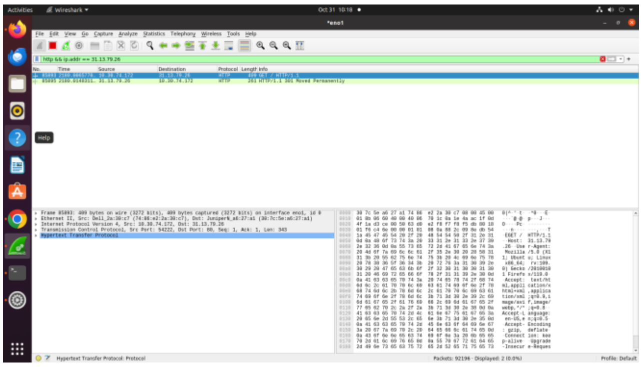
Profile: Default

In this case, you need to note that here your site is using ICMP protocol and not tcp and http as required in our case. This happens because as there are n number of address associated with a single site (in our case facebook), the address you fetched from the terminal is using ICMP protocol rather than tcp and http.

To resolve this problem:
Enter the following command:
tcp && ip.addr == <ip address of your system>
This will give you a list of all the ip addresses that are using TCP protocol on your machine.
Here’s a tip, most of the time Facebook uses ip address that starts with 31.xx.xx.xx
Search this ip address in the list of ip addresses that are displayed after executing above command.

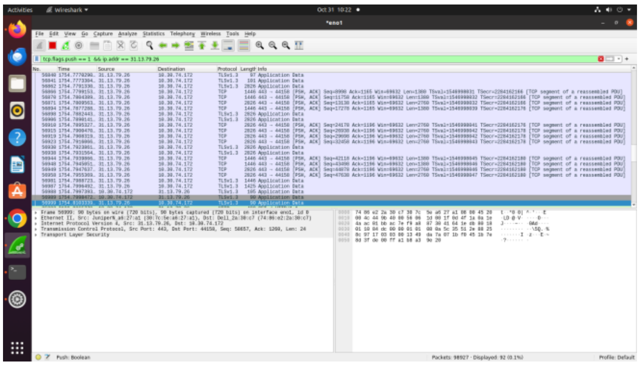
Now the procedure is simple, jus use the above address 31.xx.xx.xx in further procedure ahead:
a. Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account using:
 tcp && ip.addr == <ip address of facebook in your case> (eg. 31.13.79.26)
b. Capture all HTTP traffic to/from Facebook (other website), when you log in to your Facebook account using:
 http && ip.addr == 31.13.79.26
c. 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:
 tcp.flags.syn == 1 && ip.addr == 31.13.79.26
 tcp.flags.push == 1 && ip.addr == 31.13.79.26
 tcp.flags.reset == 1 && ip.addr == 31.13.79.26

Refer the following images:



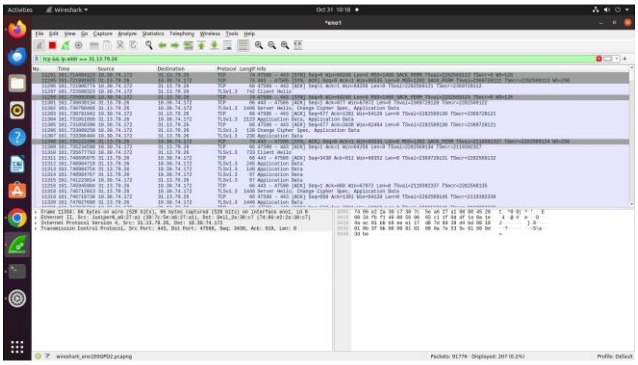
```
http && ip.addr == 31.13.79.26
```

```
Packets: 92196 · Displayed: 2 (0.0%)
```



```
tcp.flags.push == 1  && ip.addr == 31.13.79.26
```

```
Packets: 98927 · Displayed: 92 (0.1%)
```


Activities
Wireshark ▾
Oct 31 10:18 ●
*eno1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

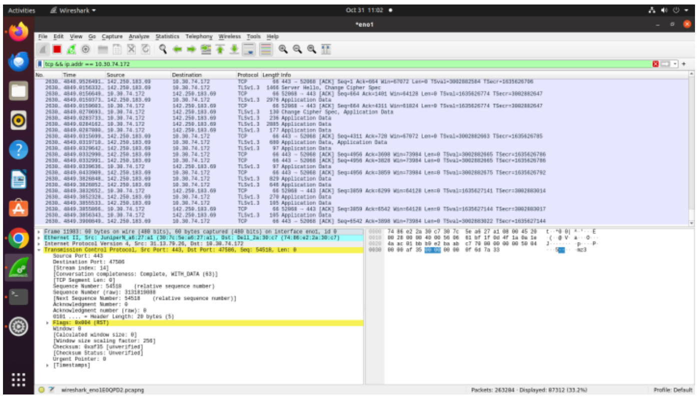
```
tcp && ip.addr == 31.13.79.26

No.   Time          Source        Destination   Protocol Length Info
11291 161.714484123 10.30.74.172  31.13.79.26   TCP      74 47586 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2282569113 TSecr=0 WS=128
11295 161.721891925 31.13.79.26   10.30.74.172  TCP      74 443 → 47586 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1392 SACK_PERM TSval=2369728112 TSecr=2282569113 WS=256
11296 161.721906774 10.30.74.172  31.13.79.26   TCP      66 47586 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2282569121 TSecr=2369728112
11297 161.722600323 10.30.74.172  31.13.79.26   TLSv1.3  742 Client Hello
11299 161.725003096 10.30.74.172  31.13.79.26   TCP      74 47598 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2282569124 TSecr=0 WS=128
11301 161.730030134 31.13.79.26   10.30.74.172  TCP      66 443 → 47586 [ACK] Seq=1 Ack=677 Win=67072 Len=0 TSval=2369728120 TSecr=2282569122
11302 161.730760466 31.13.79.26   10.30.74.172  TLSv1.3  1466 Server Hello, Change Cipher Spec, Application Data
11303 161.730781942 10.30.74.172  31.13.79.26   TCP      66 47586 → 443 [ACK] Seq=677 Ack=1381 Win=64128 Len=0 TSval=2282569130 TSecr=2369728121
11304 161.731051055 31.13.79.26   10.30.74.172  TLSv1.3  2123 Application Data, Application Data
11305 161.731056390 10.30.74.172  31.13.79.26   TCP      66 47586 → 443 [ACK] Seq=677 Ack=3430 Win=62464 Len=0 TSval=2282569130 TSecr=2369728121
11306 161.733089250 10.30.74.172  31.13.79.26   TLSv1.3  130 Change Cipher Spec, Application Data
11307 161.733306404 10.30.74.172  31.13.79.26   TLSv1.3  236 Application Data
11308 161.735222396 31.13.79.26   10.30.74.172  TCP      74 443 → 47598 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1392 SACK_PERM TSval=2119392327 TSecr=2282569124 WS=256
11309 161.735234500 10.30.74.172  31.13.79.26   TCP      66 47598 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2282569134 TSecr=2119392327
11310 161.735677793 10.30.74.172  31.13.79.26   TLSv1.3  733 Client Hello
11311 161.740095075 31.13.79.26   10.30.74.172  TCP      66 443 → 47586 [ACK] Seq=3430 Ack=912 Win=68352 Len=0 TSval=2369728131 TSecr=2282569132
11312 161.740984718 31.13.79.26   10.30.74.172  TLSv1.3  245 Application Data
11313 161.740984754 31.13.79.26   10.30.74.172  TLSv1.3  140 Application Data
11314 161.740984767 31.13.79.26   10.30.74.172  TLSv1.3  97 Application Data
11315 161.741223814 10.30.74.172  31.13.79.26   TLSv1.3  97 Application Data
11316 161.745946984 31.13.79.26   10.30.74.172  TCP      66 443 → 47598 [ACK] Seq=1 Ack=668 Win=67072 Len=0 TSval=2119392337 TSecr=2282569135
11318 161.746713913 31.13.79.26   10.30.74.172  TLSv1.3  1466 Server Hello, Change Cipher Spec, Application Data
11319 161.746718730 10.30.74.172  31.13.79.26   TCP      66 47598 → 443 [ACK] Seq=668 Ack=1381 Win=64128 Len=0 TSval=2282569146 TSecr=2119392338
11320 161.747027688 31.13.79.26   10.30.74.172  TLSv1.3  1446 Application Data

› Frame 11304: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eno1, id 0
› Ethernet II, Src: JuniperN_a6:27:a1 (30:7c:5e:a6:27:a1), Dst: Dell_2a:30:c7 (74:86:e2:2a:30:c7)
› Internet Protocol Version 4, Src: 31.13.79.26, Dst: 10.30.74.172
› Transmission Control Protocol, Src Port: 443, Dst Port: 47586, Seq: 3430, Ack: 919, Len: 0

0000  74 86 e2 2a 30 c7 30 7c  5e a6 27 a1 08 00 45 20
0010  00 34 fb f1 40 00 56 06  65 c1 1f 0d 4f 1a 0a 1e
0020  4a ac 01 bb b9 ee e1 17  d8 7d 69 38 d4 bd 80 10
0030  01 0b 3f 0b 00 00 01 01  08 0a 7e 53 5c 61 88 bd
0040  30 be

wireshark_eno1E0QPD2.pcapng          Packets: 91776 · Displayed: 207 (0.2%)          Profile: Default
```


Activities
Wireshark ▾
Oct 31 11:02 ●
*eno1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

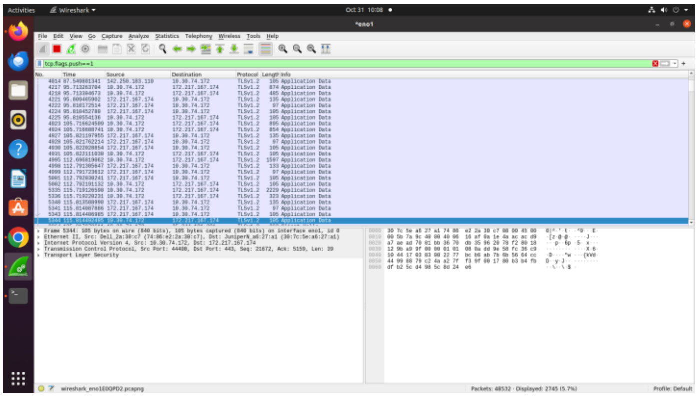
```
tcp && ip.addr == 10.30.74.172

No.    Time           Source          Destination     Protocol Length Info
2630…  4848.9526491…  142.250.183.69  10.30.74.172    TCP      66 443 → 52068 [ACK] Seq=1 Ack=664 Win=67072 Len=0 TSval=3002882584 TSecr=1635626706
2630…  4849.0156332…  142.250.183.69  10.30.74.172    TLSv1.3  1466 Server Hello, Change Cipher Spec
2630…  4849.0156649…  10.30.74.172    142.250.183.69  TCP      66 52068 → 443 [ACK] Seq=664 Ack=1401 Win=64128 Len=0 TSval=1635626774 TSecr=3002882647
2630…  4849.0159373…  142.250.183.69  10.30.74.172    TLSv1.3  2976 Application Data
2630…  4849.0159683…  10.30.74.172    142.250.183.69  TCP      66 52068 → 443 [ACK] Seq=664 Ack=4311 Win=61824 Len=0 TSval=1635626774 TSecr=3002882647
2630…  4849.0270693…  10.30.74.172    142.250.183.69  TLSv1.3  130 Change Cipher Spec, Application Data
2630…  4849.0283733…  10.30.74.172    142.250.183.69  TLSv1.3  236 Application Data
2630…  4849.0284162…  10.30.74.172    142.250.183.69  TLSv1.3  2085 Application Data
2630…  4849.0287080…  10.30.74.172    142.250.183.69  TLSv1.3  177 Application Data
2630…  4849.0315699…  142.250.183.69  10.30.74.172    TCP      66 443 → 52068 [ACK] Seq=4311 Ack=728 Win=67072 Len=0 TSval=3002882663 TSecr=1635626785
2630…  4849.0319710…  142.250.183.69  10.30.74.172    TLSv1.3  680 Application Data, Application Data
2630…  4849.0329642…  142.250.183.69  10.30.74.172    TLSv1.3  97 Application Data
2630…  4849.0332990…  142.250.183.69  10.30.74.172    TCP      66 443 → 52068 [ACK] Seq=4956 Ack=3698 Win=73984 Len=0 TSval=3002882665 TSecr=1635626786
2630…  4849.0332991…  142.250.183.69  10.30.74.172    TCP      66 443 → 52068 [ACK] Seq=4956 Ack=3828 Win=73984 Len=0 TSval=3002882665 TSecr=1635626786
2630…  4849.0339636…  10.30.74.172    142.250.183.69  TLSv1.3  97 Application Data
2630…  4849.0433909…  142.250.183.69  10.30.74.172    TCP      66 443 → 52068 [ACK] Seq=4956 Ack=3859 Win=73984 Len=0 TSval=3002882675 TSecr=1635626792
2630…  4849.3826848…  142.250.183.69  10.30.74.172    TLSv1.3  829 Application Data
2630…  4849.3826852…  142.250.183.69  10.30.74.172    TLSv1.3  646 Application Data
2630…  4849.3832652…  10.30.74.172    142.250.183.69  TCP      66 52068 → 443 [ACK] Seq=3859 Ack=6299 Win=64128 Len=0 TSval=1635627141 TSecr=3002883014
2630…  4849.3852328…  142.250.183.69  10.30.74.172    TLSv1.3  270 Application Data
2630…  4849.3855533…  142.250.183.69  10.30.74.172    TLSv1.3  105 Application Data
2630…  4849.3855866…  10.30.74.172    142.250.183.69  TCP      66 52068 → 443 [ACK] Seq=3859 Ack=6542 Win=64128 Len=0 TSval=1635627144 TSecr=3002883017
2630…  4849.3856343…  10.30.74.172    142.250.183.69  TLSv1.3  105 Application Data
2630…  4849.3900849…  142.250.183.69  10.30.74.172    TCP      66 443 → 52068 [ACK] Seq=6542 Ack=3898 Win=73984 Len=0 TSval=3002883022 TSecr=1635627144

› Frame 11983: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eno1, id 0
› Ethernet II, Src: JuniperN_a6:27:a1 (30:7c:5e:a6:27:a1), Dst: Dell_2a:30:c7 (74:86:e2:2a:30:c7)
› Internet Protocol Version 4, Src: 31.13.79.26, Dst: 10.30.74.172
⌄ Transmission Control Protocol, Src Port: 443, Dst Port: 47586, Seq: 54518, Len: 0
    Source Port: 443
    Destination Port: 47586
    [Stream index: 14]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 54518    (relative sequence number)
    Sequence Number (raw): 3131819888
    [Next Sequence Number: 54518    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    0101 .... = Header Length: 20 bytes (5)
  › Flags: 0x004 (RST)
    Window: 0
    [Calculated window size: 0]
    [Window size scaling factor: 256]
    Checksum: 0xaf35 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › [Timestamps]

0000  74 86 e2 2a 30 c7 30 7c  5e a6 27 a1 08 00 45 20
0010  00 28 00 00 40 00 56 06  61 bf 1f 0d 4f 1a 0a 1e
0020  4a ac 01 bb b9 e2 ba ab  c7 70 00 00 00 00 50 04
0030  00 00 af 35 00 00 00 00  0f 6d 7a 33

wireshark_eno1E0QPD2.pcapng          Packets: 263284 · Displayed: 87312 (33.2%)          Profile: Default
```


Activities
Wireshark ▾
Oct 31 10:08 ●
*eno1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

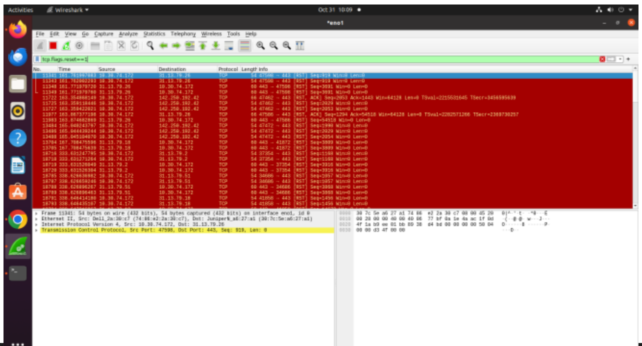
```
tcp.flags.push==1

No.  Time           Source          Destination     Protocol Length Info
4014 87.549801341   142.250.183.110 10.30.74.172    TLSv1.2  105 Application Data
4217 95.713263704   10.30.74.172    172.217.167.174 TLSv1.2  874 Application Data
4218 95.713304673   10.30.74.172    172.217.167.174 TLSv1.2  485 Application Data
4221 95.809465902   172.217.167.174 10.30.74.172    TLSv1.2  135 Application Data
4222 95.810172514   172.217.167.174 10.30.74.172    TLSv1.2  97 Application Data
4224 95.810452780   172.217.167.174 10.30.74.172    TLSv1.2  105 Application Data
4225 95.810554136   10.30.74.172    172.217.167.174 TLSv1.2  105 Application Data
4923 105.716624589  10.30.74.172    172.217.167.174 TLSv1.2  805 Application Data
4924 105.716688741  10.30.74.172    172.217.167.174 TLSv1.2  854 Application Data
4927 105.821197955  172.217.167.174 10.30.74.172    TLSv1.2  135 Application Data
4928 105.821762214  172.217.167.174 10.30.74.172    TLSv1.2  97 Application Data
4930 105.822028854  172.217.167.174 10.30.74.172    TLSv1.2  105 Application Data
4931 105.822111030  10.30.74.172    172.217.167.174 TLSv1.2  105 Application Data
4995 112.696819062  10.30.74.172    172.217.167.174 TLSv1.2  1597 Application Data
4998 112.791305647  172.217.167.174 10.30.74.172    TLSv1.2  133 Application Data
4999 112.791723612  172.217.167.174 10.30.74.172    TLSv1.2  97 Application Data
5001 112.792038241  172.217.167.174 10.30.74.172    TLSv1.2  105 Application Data
5002 112.792191132  10.30.74.172    172.217.167.174 TLSv1.2  105 Application Data
5335 115.719120590  10.30.74.172    172.217.167.174 TLSv1.2  2229 Application Data
5336 115.719220231  10.30.74.172    172.217.167.174 TLSv1.2  323 Application Data
5340 115.813580998  172.217.167.174 10.30.74.172    TLSv1.2  135 Application Data
5341 115.814087886  172.217.167.174 10.30.74.172    TLSv1.2  97 Application Data
5343 115.814406985  172.217.167.174 10.30.74.172    TLSv1.2  105 Application Data
5344 115.814492495  10.30.74.172    172.217.167.174 TLSv1.2  105 Application Data

› Frame 5344: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface eno1, id 0
› Ethernet II, Src: Dell_2a:30:c7 (74:86:e2:2a:30:c7), Dst: JuniperN_a6:27:a1 (30:7c:5e:a6:27:a1)
› Internet Protocol Version 4, Src: 10.30.74.172, Dst: 172.217.167.174
› Transmission Control Protocol, Src Port: 44400, Dst Port: 443, Seq: 21672, Ack: 5159, Len: 39
› Transport Layer Security

0000  30 7c 5e a6 27 a1 74 86  e2 2a 30 c7 08 00 45 00
0010  00 5b 7a 9c 40 00 40 06  16 af 0a 1e 4a ac ac d9
0020  a7 ae ad 70 01 bb 36 70  db 35 96 20 78 f2 80 18
0030  12 9b a9 9f 00 00 01 01  08 0a dd 9e 58 fc 36 c9
0040  10 44 17 03 03 00 22 77  bc b6 ab 7b 6b 56 64 cc
0050  44 99 88 79 c2 4a a2 7f  f3 9f 00 17 80 b3 b4 fb
0060  df b2 5c d4 98 5c 8d 24  e6

wireshark_eno1E0QPD2.pcapng          Packets: 48532 · Displayed: 2745 (5.7%)          Profile: Default
```


Activities
Wireshark ▾
Oct 31 10:09 ●
*eno1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

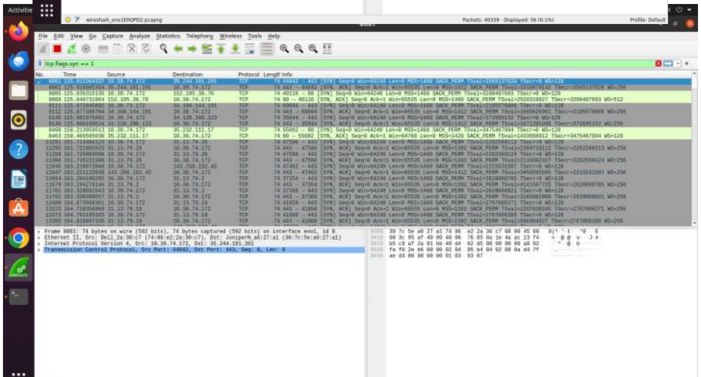
```
tcp.flags.reset==1

No.   Time          Source        Destination    Protocol Length Info
11341 161.761997883 10.30.74.172  31.13.79.26    TCP      54 47598 → 443 [RST] Seq=919 Win=0 Len=0
11343 161.762002283 10.30.74.172  31.13.79.26    TCP      54 47598 → 443 [RST] Seq=919 Win=0 Len=0
11348 161.771979720 31.13.79.26   10.30.74.172   TCP      60 443 → 47598 [RST] Seq=3691 Win=0 Len=0
11349 161.771979760 31.13.79.26   10.30.74.172   TCP      60 443 → 47598 [RST] Seq=3691 Win=0 Len=0
11722 163.354868149 10.30.74.172  142.250.192.42 TCP      66 47462 → 443 [RST, ACK] Seq=2053 Ack=1443 Win=64128 Len=0 TSval=2215531645 TSecr=3456595639
11725 163.358118446 10.30.74.172  142.250.192.42 TCP      54 47462 → 443 [RST] Seq=2029 Win=0 Len=0
11727 163.358422021 10.30.74.172  142.250.192.42 TCP      54 47462 → 443 [RST] Seq=2053 Win=0 Len=0
11977 163.867377198 10.30.74.172  31.13.79.26    TCP      66 47586 → 443 [RST, ACK] Seq=1294 Ack=54518 Win=64128 Len=0 TSval=2282571266 TSecr=2369730257
11983 163.874882889 31.13.79.26   10.30.74.172   TCP      60 443 → 47586 [RST] Seq=54518 Win=0 Len=0
13484 165.040243797 10.30.74.172  142.250.192.42 TCP      54 47472 → 443 [RST] Seq=1990 Win=0 Len=0
13486 165.044430244 10.30.74.172  142.250.192.42 TCP      54 47472 → 443 [RST] Seq=2029 Win=0 Len=0
13488 165.045104070 10.30.74.172  142.250.192.42 TCP      54 47472 → 443 [RST] Seq=2054 Win=0 Len=0
13704 167.708475596 31.13.79.18   10.30.74.172   TCP      60 443 → 41872 [RST] Seq=3889 Win=0 Len=0
13705 167.708475639 31.13.79.18   10.30.74.172   TCP      60 443 → 41872 [RST] Seq=3889 Win=0 Len=0
18716 333.631247795 10.30.74.172  31.13.79.2     TCP      54 37354 → 443 [RST] Seq=1168 Win=0 Len=0
18718 333.631271264 10.30.74.172  31.13.79.2     TCP      54 37354 → 443 [RST] Seq=1168 Win=0 Len=0
18719 333.631520849 31.13.79.2    10.30.74.172   TCP      60 443 → 37354 [RST] Seq=3916 Win=0 Len=0
18720 333.631520884 31.13.79.2    10.30.74.172   TCP      60 443 → 37354 [RST] Seq=3916 Win=0 Len=0
18785 338.626630082 10.30.74.172  31.13.79.51    TCP      54 34686 → 443 [RST] Seq=1057 Win=0 Len=0
18787 338.626659246 10.30.74.172  31.13.79.51    TCP      54 34686 → 443 [RST] Seq=1057 Win=0 Len=0
18788 338.628896267 31.13.79.51   10.30.74.172   TCP      60 443 → 34686 [RST] Seq=3868 Win=0 Len=0
18789 338.628896463 31.13.79.51   10.30.74.172   TCP      60 443 → 34686 [RST] Seq=3868 Win=0 Len=0
18791 338.646414180 10.30.74.172  31.13.79.18    TCP      54 41858 → 443 [RST] Seq=1456 Win=0 Len=0
18793 338.646435187 10.30.74.172  31.13.79.18    TCP      54 41858 → 443 [RST] Seq=1456 Win=0 Len=0

› Frame 11341: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eno1, id 0
› Ethernet II, Src: Dell_2a:30:c7 (74:86:e2:2a:30:c7), Dst: JuniperN_a6:27:a1 (30:7c:5e:a6:27:a1)
› Internet Protocol Version 4, Src: 10.30.74.172, Dst: 31.13.79.26
› Transmission Control Protocol, Src Port: 47598, Dst Port: 443, Seq: 919, Len: 0

0000  30 7c 5e a6 27 a1 74 86  e2 2a 30 c7 08 00 45 20
0010  00 28 00 00 40 00 40 06  77 bf 0a 1e 4a ac 1f 0d
0020  4f 1a b9 ee 01 bb 89 38  d4 bd 00 00 00 00 50 04
0030  00 00 d3 4f 00 00

wireshark_eno1E0QPD2.pcapng          Packets: 49339 · Displayed: 56 (0.1%)          Profile: Default
```


Activitie
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags.syn == 1

No.   Time          Source          Destination     Protocol Length Info
8081  125.812384337 10.30.74.172    35.244.181.201  TCP      74 44842 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1565137020 TSecr=0 WS=128
8082  125.816085054 35.244.181.201  10.30.74.172    TCP      74 443 → 44842 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=3310970142 TSecr=1565137020 WS=256
8085  125.836315135 10.30.74.172    152.195.38.76   TCP      74 40116 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3200497693 TSecr=0 WS=128
8088  125.840731064 152.195.38.76   10.30.74.172    TCP      74 80 → 40116 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=2520310027 TSecr=3200497693 WS=512
8111  125.872845092 10.30.74.172    34.160.144.191  TCP      74 60694 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2105570806 TSecr=0 WS=128
8112  125.877398764 34.160.144.191  10.30.74.172    TCP      74 443 → 60694 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=1665626961 TSecr=2105570806 WS=256
8145  125.981075661 10.30.74.172    34.120.208.123  TCP      74 35044 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=372695152 TSecr=0 WS=128
8148  125.988189524 34.120.208.123  10.30.74.172    TCP      74 443 → 35044 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=3471285396 TSecr=372695152 WS=256
8460  150.213959513 10.30.74.172    35.232.111.17   TCP      74 55082 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3475467994 TSecr=0 WS=128
8463  150.466565030 35.232.111.17   10.30.74.172    TCP      74 80 → 55082 [SYN, ACK] Seq=0 Ack=1 Win=64768 Len=0 MSS=1420 SACK_PERM TSval=1433058912 TSecr=3475467994 WS=128
11291 161.714484123 10.30.74.172    31.13.79.26     TCP      74 47586 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2282569113 TSecr=0 WS=128
11295 161.721891925 31.13.79.26     10.30.74.172    TCP      74 443 → 47586 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1392 SACK_PERM TSval=2369728112 TSecr=2282569113 WS=256
11299 161.725003096 10.30.74.172    31.13.79.26     TCP      74 47598 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2282569124 TSecr=0 WS=128
11308 161.735222396 31.13.79.26     10.30.74.172    TCP      74 443 → 47598 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1392 SACK_PERM TSval=2119392327 TSecr=2282569124 WS=256
11645 163.216673948 10.30.74.172    142.250.192.42  TCP      74 47462 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2215531507 TSecr=0 WS=128
11647 163.221122038 142.250.192.42  10.30.74.172    TCP      74 443 → 47462 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=3456595505 TSecr=2215531507 WS=256
11664 163.264100265 10.30.74.172    31.13.79.2      TCP      74 37354 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2628068785 TSecr=0 WS=128
11679 163.294278146 31.13.79.2      10.30.74.172    TCP      74 443 → 37354 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1392 SACK_PERM TSval=4141597725 TSecr=2628068785 WS=256
11701 163.320091643 10.30.74.172    31.13.79.2      TCP      74 37366 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2628068821 TSecr=0 WS=128
11702 163.330469557 31.13.79.2      10.30.74.172    TCP      74 443 → 37366 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1392 SACK_PERM TSval=3165082909 TSecr=2628068821 WS=256
12400 164.073668361 10.30.74.172    31.13.79.18     TCP      74 41858 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2767066271 TSecr=0 WS=128
13223 164.728356069 31.13.79.18     10.30.74.172    TCP      74 443 → 41858 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1392 SACK_PERM TSval=2207638345 TSecr=2767066271 WS=256
13373 164.792165325 10.30.74.172    31.13.79.18     TCP      74 41868 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2767066380 TSecr=0 WS=128
13385 164.816097306 31.13.79.18     10.30.74.172    TCP      74 443 → 41868 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1392 SACK_PERM TSval=586064027 TSecr=2767066380 WS=256

› Frame 8081: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eno1, id 0
› Ethernet II, Src: Dell_2a:30:c7 (74:86:e2:2a:30:c7), Dst: JuniperN_a6:27:a1 (30:7c:5e:a6:27:a1)
› Internet Protocol Version 4, Src: 10.30.74.172, Dst: 35.244.181.201
› Transmission Control Protocol, Src Port: 44842, Dst Port: 443, Seq: 0, Len: 0

0000  30 7c 5e a6 27 a1 74 86  e2 2a 30 c7 08 00 45 00
0010  00 3c 05 af 40 00 40 06  76 85 0a 1e 4a ac 23 f4
0020  b5 c9 af 2a 01 bb 40 d4  62 d5 00 00 00 00 a0 02
0030  fa f0 2e b6 00 00 02 04  05 b4 04 02 08 0a d4 7f
0040  ae d4 00 00 00 00 01 03  03 07
```