

# Facebook Packets Captured:

1. Select search box
2. Add condition ip.addr == 157.240.16.16
3. Take screenshot

Activities Wireshark Dec 3 21:13 \*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==157.240.16.16

No.	Time	Source	Destination	Protocol	Length	Info
3295	18.79055899	157.240.16.16	192.168.219.175	TCP	76	443 → 43990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1
3296	18.79051521	192.168.219.175	157.240.16.16	TCP	68	43990 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=325515638
3297	18.79060945	192.168.219.175	157.240.16.16	TLSv1.3	585	Client Hello
3298	18.79250240	157.240.16.16	192.168.219.175	TCP	68	443 → 43990 [ACK] Seq=1 Ack=518 Win=6400 Len=0 TSval=11040977
3299	18.80229857	157.240.16.16	192.168.219.175	TLSv1.3	2435	Server Hello, Change Cipher Spec, Application Data, Application Data
3210	18.80231512	192.168.219.175	157.240.16.16	TCP	68	43990 → 443 [ACK] Seq=518 Ack=2368 Win=61952 Len=0 TSval=3255
3211	18.80448923	192.168.219.175	157.240.16.16	TLSv1.3	132	Change Cipher Spec, Application Data
3212	18.80464869	192.168.219.175	157.240.16.16	TLSv1.3	932	Application Data
3213	18.80858466	157.240.16.16	192.168.219.175	TCP	68	443 → 43990 [ACK] Seq=2368 Ack=1446 Win=7680 Len=0 TSval=1104
3214	18.811211595	157.240.16.16	192.168.219.175	TLSv1.3	237	Application Data
3215	18.811217901	192.168.219.175	157.240.16.16	TCP	68	43990 → 443 [ACK] Seq=1446 Ack=2537 Win=64000 Len=0 TSval=325
3216	19.05017261	157.240.16.16	192.168.219.175	TLSv1.3	902	Application Data
3218	19.05023952	192.168.219.175	157.240.16.16	TCP	68	43990 → 443 [ACK] Seq=1446 Ack=2771 Win=63872 Len=0 TSval=325
3233	19.05081696	157.240.16.16	192.168.219.175	TLSv1.3	324	Application Data
3256	19.050832761	157.240.16.16	192.168.219.175	TCP	68	443 → 43990 [ACK] Seq=2771 Ack=1702 Win=9472 Len=0 TSval=1104
3261	19.253106178	157.240.16.16	192.168.219.175	TLSv1.3	98	Application Data
3262	19.253139717	192.168.219.175	157.240.16.16	TCP	68	43990 → 443 [ACK] Seq=1702 Ack=2801 Win=64128 Len=0 TSval=325
4285	24.429679669	192.168.219.175	157.240.16.16	TLSv1.3	153	Application Data
4286	24.429986239	192.168.219.175	157.240.16.16	TLSv1.3	213	Application Data
4287	24.430243489	192.168.219.175	157.240.16.16	TLSv1.3	111	Application Data
4289	24.454060875	192.168.219.175	157.240.16.16	TLSv1.3	293	Application Data
4290	24.454401330	192.168.219.175	157.240.16.16	TLSv1.3	153	Application Data
4291	24.454707954	192.168.219.175	157.240.16.16	TLSv1.3	169	Application Data
4292	24.455139134	192.168.219.175	157.240.16.16	TLSv1.3	120	Application Data
4293	24.455489615	192.168.219.175	157.240.16.16	TLSv1.3	124	Application Data
4294	24.455745233	157.240.16.16	192.168.219.175	TCP	68	443 → 43990 [ACK] Seq=2801 Ack=2110 Win=11136 Len=0 TSval=110
4295	24.456211092	157.240.16.16	192.168.219.175	TCP	68	443 → 43990 [ACK] Seq=2801 Ack=2195 Win=11136 Len=0 TSval=110
4296	24.456883230	157.240.16.16	192.168.219.175	TCP	68	443 → 43990 [ACK] Seq=2801 Ack=2287 Win=11136 Len=0 TSval=110
4297	24.456883395	157.240.16.16	192.168.219.175	TCP	68	443 → 43990 [ACK] Seq=2801 Ack=2330 Win=11136 Len=0 TSval=110
4298	24.456883423	157.240.16.16	192.168.219.175	TCP	68	443 → 43990 [ACK] Seq=2801 Ack=2395 Win=11136 Len=0 TSval=110
4299	24.456883423	157.240.16.16	192.168.219.175	TCP	68	443 → 43990 [ACK] Seq=2801 Ack=2395 Win=11136 Len=0 TSval=110
4302	24.607311996	192.168.219.175	157.240.16.16	TLSv1.3	287	Application Data
4303	24.607479992	192.168.219.175	157.240.16.16	TLSv1.3	444	Application Data, Application Data, Application Data
4305	24.611387709	157.240.16.16	192.168.219.175	TLSv1.3	128	Application Data, Application Data
4306	24.611387851	157.240.16.16	192.168.219.175	TLSv1.3	98	Application Data

Frame 3204: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0

- Linux cooked capture
- Internet Protocol Version 4, Src: 192.168.219.175, Dst: 157.240.16.16
- Transmission Control Protocol, Src Port: 43990, Dst Port: 443, Seq: 0, Len: 0

0000 00 04 00 01 00 06 a0 51 0b 5e 28 fe 00 60 08 00 .....Q^H....

0010 45 00 00 3c 89 b3 40 00 40 06 60 b0 c0 a8 0b a7 E<<0 0 f....

0020 90 f0 50 50 a0 52 05 00 64 7b 00 00 00 00 00 ---R0{.....

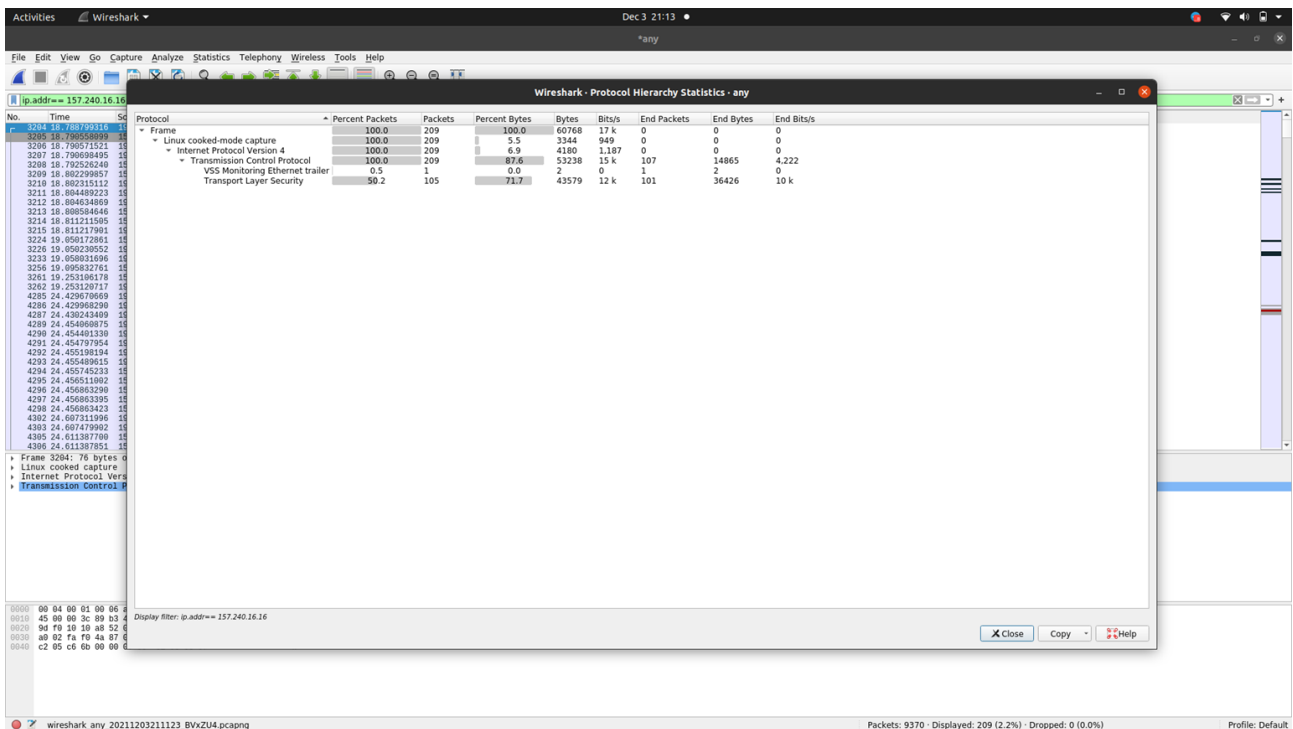
0030 a0 02 fa f0 4a 07 00 00 02 04 05 04 04 02 08 0a ---J.....

0040 c2 05 c6 c6 00 00 00 00 01 03 03 07 ---k.....

wireshark\_any\_2021120321123\_BVxZU4.pcapng Packets: 9370 - Displayed: 209 (2.2%) - Dropped: 0 (0.0%) Profile: Default

## PROTOCOL HIERARCHY STATS for packets captured

1. Go to statistics
2. Go to protocol hierarchy stats
3. Take screenshot



## Transport Layer Security Over Facebook Packets

1. Select search box
2. Add filters ip.addr == 157.240.16.16 && tls
3. Take screenshot

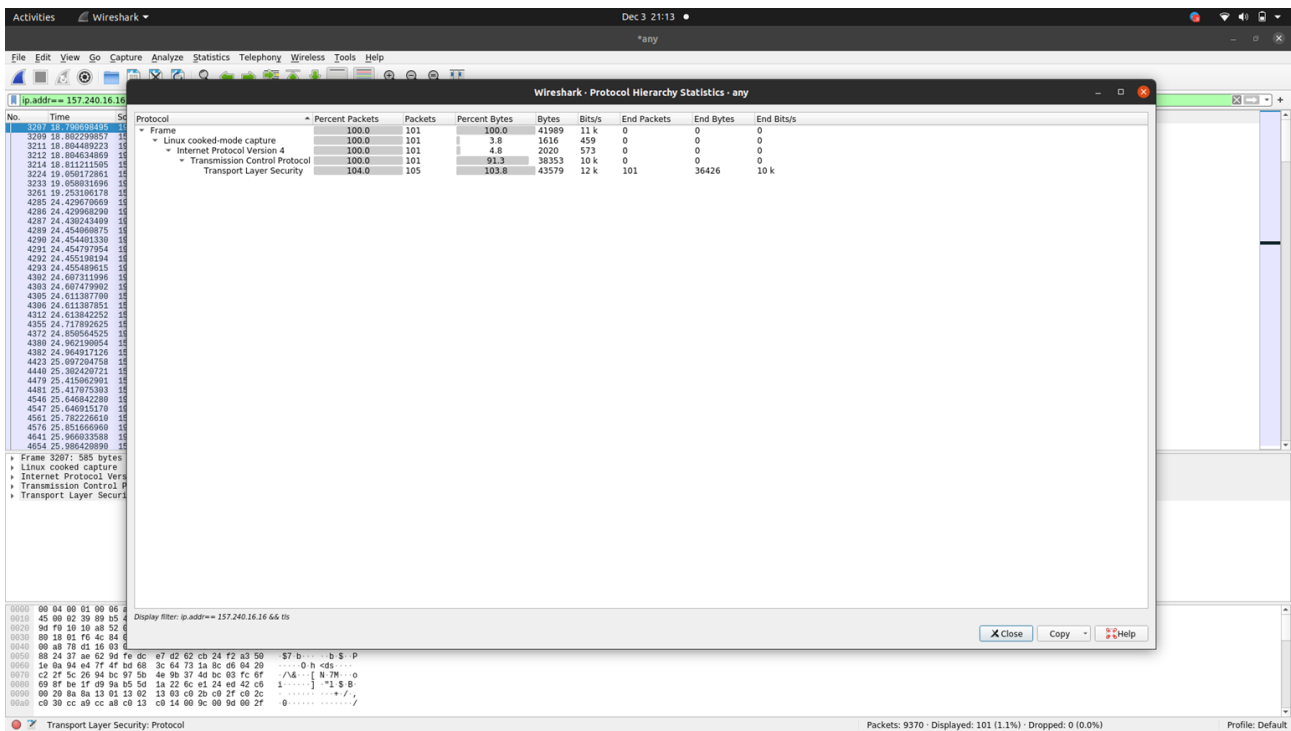
The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like opening files, saving, and analyzing. The main window is divided into three panes:

- Packet List:** Displays a list of captured packets. The filter bar at the top shows the active filter: `ip.addr == 157.240.16.16 && tls`. The list shows packets 3200 through 4654, all of which are TLS application data packets between 157.240.16.16 and 192.168.219.175.
- Packet Details:** Shows the hierarchical structure of the selected packet (No. 3207). It includes the Ethernet II header, Internet Protocol Version 4 header, and the Transport Layer Security (TLS) record. The TLS record is expanded to show the TLS header and application data.
- Packet Bytes:** Displays the raw hex and ASCII data of the selected packet, showing the TLS record structure in detail.

The status bar at the bottom indicates that 9370 packets were captured, 101 (1.1%) were displayed, and 0 (0.0%) were dropped. The profile is set to Default.

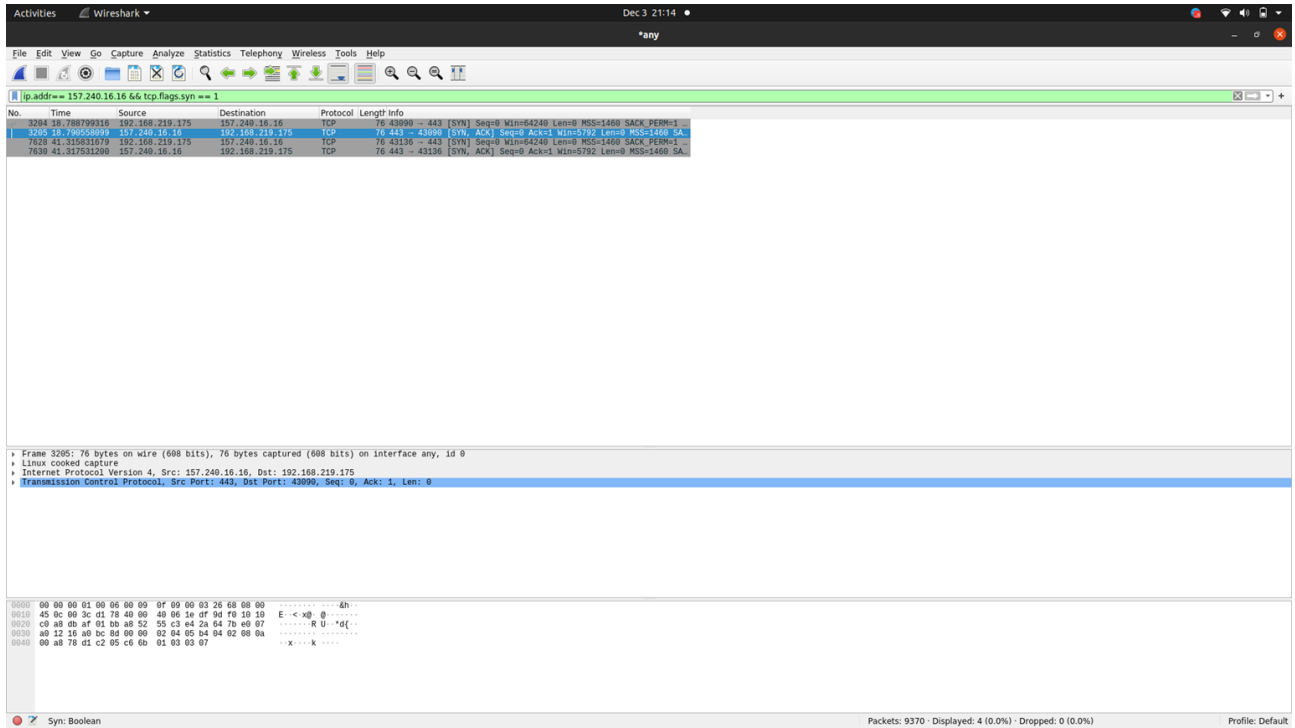
## PROTOCOL HIERARCHY STATS for Transport Layer Security Over Facebook Packets

1. Go to statistics
2. Go to protocol hierarchy stats
3. Take screenshot



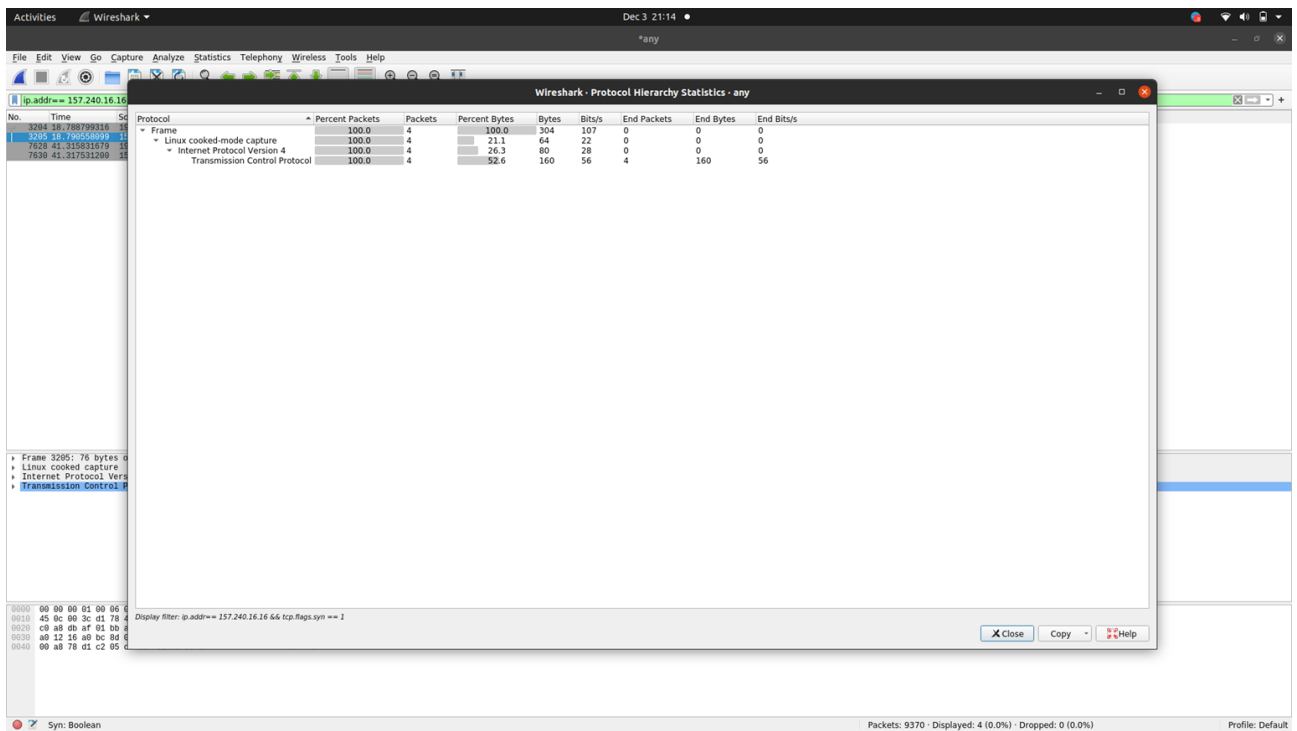
## DISPLAYING filter expression to count all TCP packets that have the flag SYN

1. Select search box
2. Add filter ip.addr == 157.240.16.16 && tcp.flags.syn == 1
3. Take screenshot



## PROTOCOL HIERARCHY STATS for the SAME.

1. Go to statistics
2. Go to protocol hierarchy stats
3. Take screenshot



# DISPLAYING filter expression to count all TCP packets that have the flag PUSH

1. Select search box
2. Add filter ip.addr == 157.240.16.16 && tcp.flags.push == 1
3. Take screenshot

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like opening files, saving, and analyzing. The filter bar at the top displays the active filter: `ip.addr == 157.240.16.16 && tcp.flags.push == 1`. Below the filter bar, a list of captured packets is shown, including details, packet bytes, and packet hex. The details pane for the selected packet (No. 3207) shows the following structure:

- Linux cooked capture
- Internet Protocol Version 4, Src: 192.168.219.175, Dst: 157.240.16.16
- Transmission Control Protocol, Src Port: 43990, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
- Transport Layer Security

The packet hex pane shows the raw data in hexadecimal and ASCII format.

## PROTOCOL HIERARCHY STATS to count all TCP packets that have the flag PUSH

1. Go to statistics
2. Go to protocol hierarchy stats
3. Take screenshot

The screenshot shows the Wireshark interface with the Protocol Hierarchy Statistics window open. The window displays a tree view of the protocol hierarchy and a table of statistics. The filter applied is `ip.addr == 157.240.16.16`.

**Protocol Hierarchy Statistics - any**

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	107	100.0	47954	13 k	0	0	0
Linux cooked mode capture	100.0	107	3.6	1712	466	0	0	0
Internet Protocol Version 4	100.0	107	4.5	2140	607	0	0	0
Transmission Control Protocol	100.0	107	92.0	44102	12 k	7	7229	2.053
Transport Layer Security	97.2	104	82.4	39493	11 k	100	32340	9.186

Display filter: `ip.addr == 157.240.16.16 && tcp.flags.push == 1`

Push: Boolean

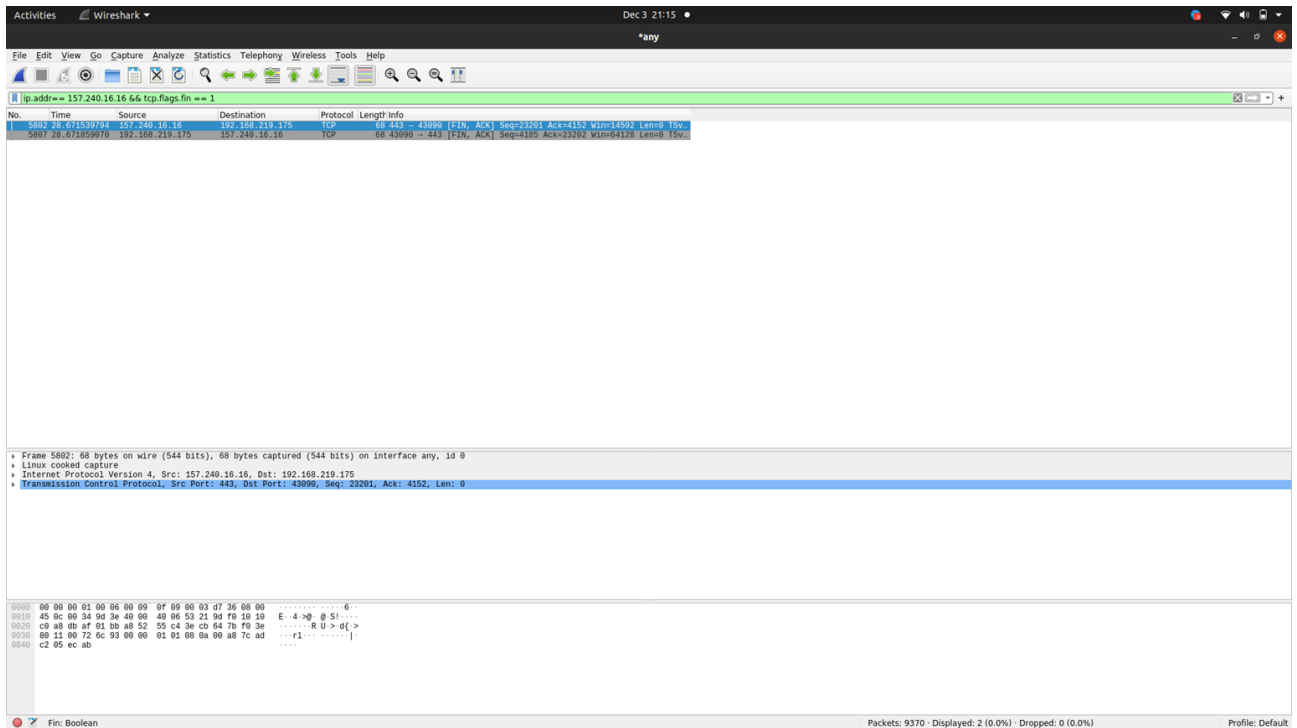
Packets: 9370 · Displayed: 107 (1.1%) · Dropped: 0 (0.0%)

Profile: Default



## DISPLAYING filter expression to count all TCP packets that have the flag FIN

1. Select search box
2. Add filter `ip.addr == 157.240.16.16 && tcp.flags.fin == 1`
3. Take screenshot



## PROTOCOL HIERARCHY STATS to count all TCP packets that have the flags FIN

1. Go to statistics
2. Go to protocol hierarchy stats
3. Take screenshot

