

CSE3501 - Information Security Analysis and Audit

Embedded Lab ELA

FALL SEMESTER – 2020-2021

Theory: G1+TG1 SLOT Lab: L33+L34

Digital assignment

Assessment: 4

Submitted By

ELIO J LOPES Reg. No.: 18BCE2040

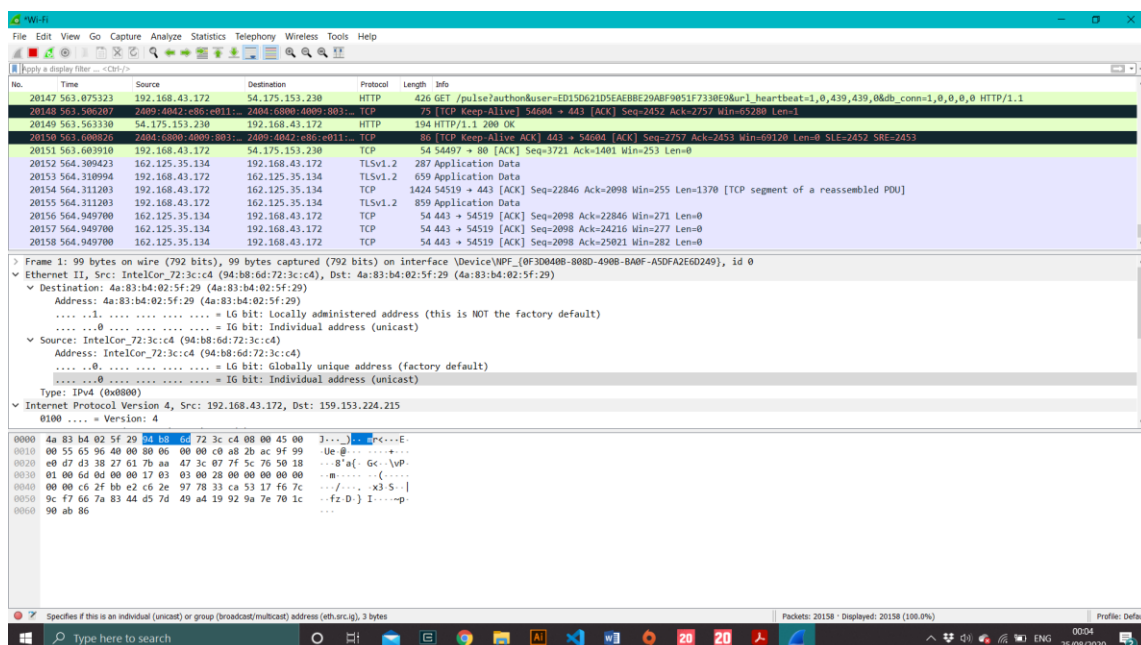
B.Tech. (C.S.E) – III Year



Wireshark - HTTP analysis

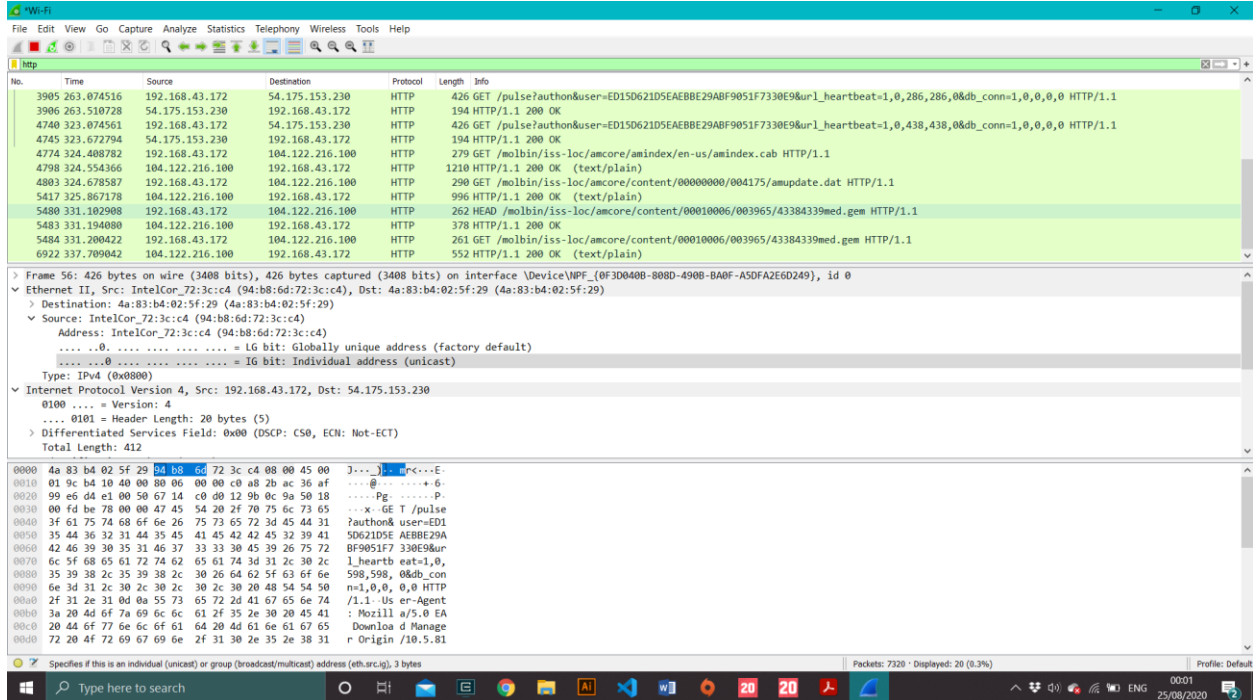
Procedure:

1. Open wireshark
2. Run it as an administrator.
3. Select the interface as WiFi
4. Start to capture the packets by clicking the “capture” option.
5. Open the browser and enter a url. Eg: www.vit.ac.in
6. Then, you will be able to see packet flow in the wireshark app.

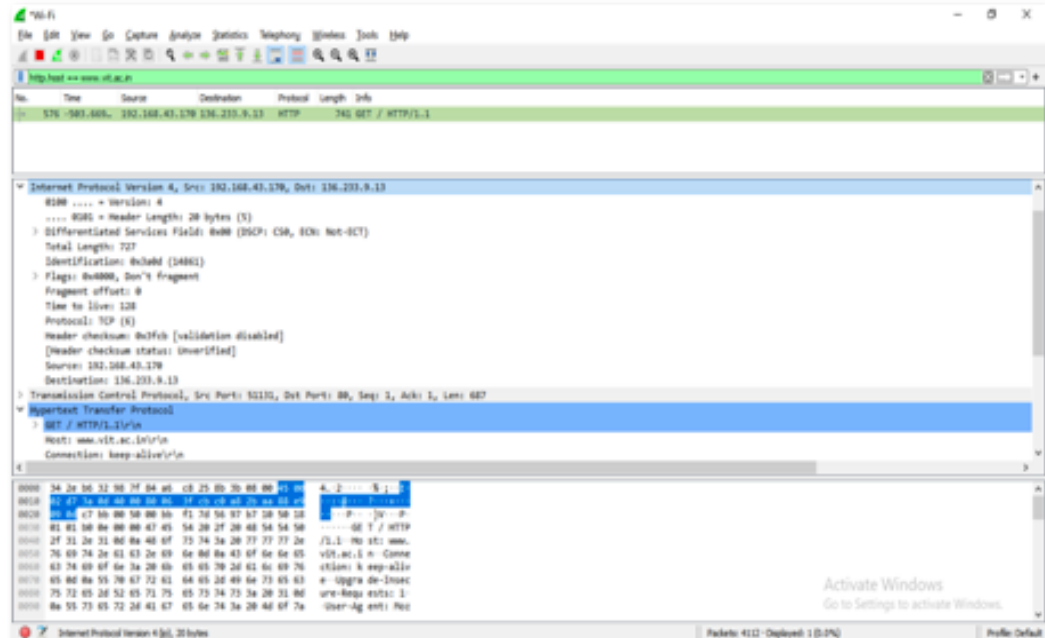


7. The packets can be filtered and analysed by entering some queries in the filter text box.
8. Some of the important queries to analyze the packets include:

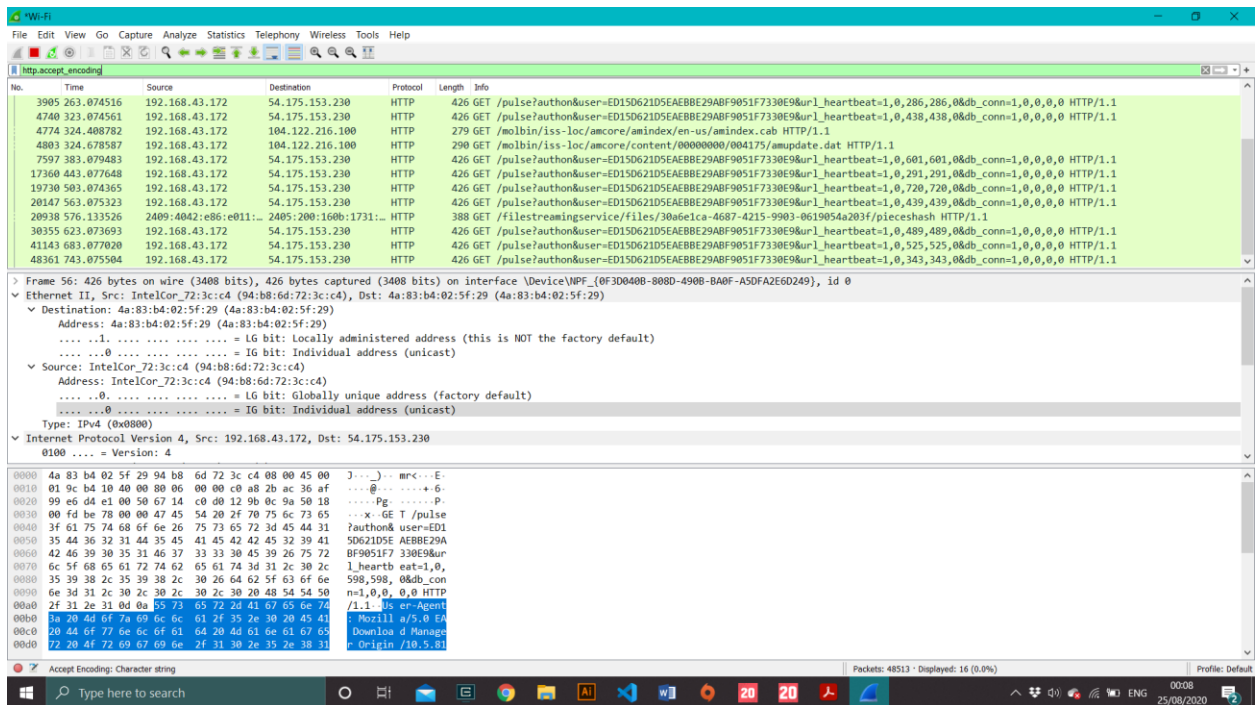
(a) **http** - This will return all the http packets.

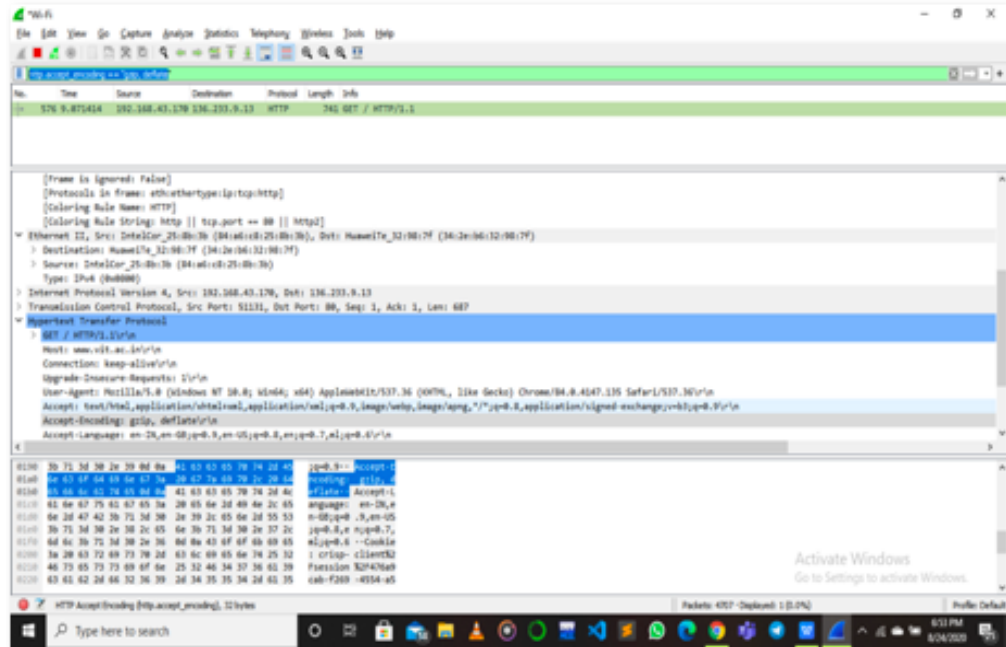


(b) **http.host == www.vit.ac.in** - This will return the http packets directed to www.vit.ac.in

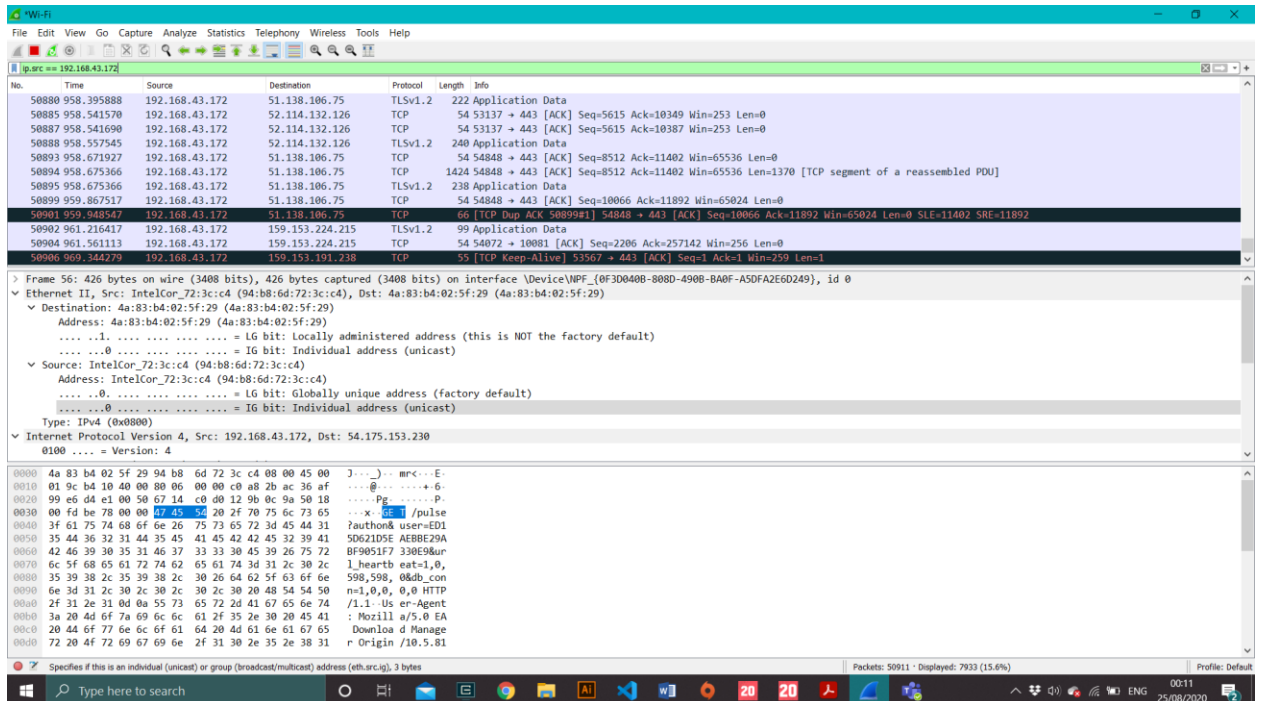


(c) `http.accept_encoding == "gzip, deflate"` - This will return all the packets which have the encoding as gzip, deflate.

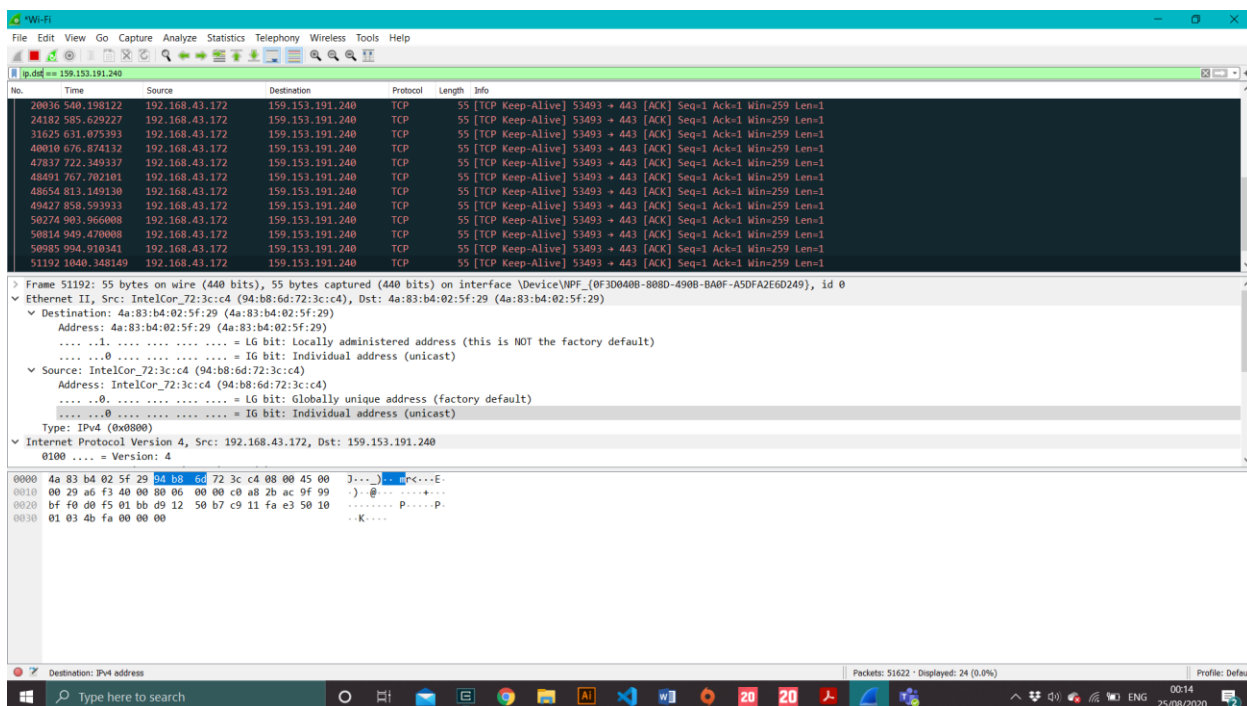




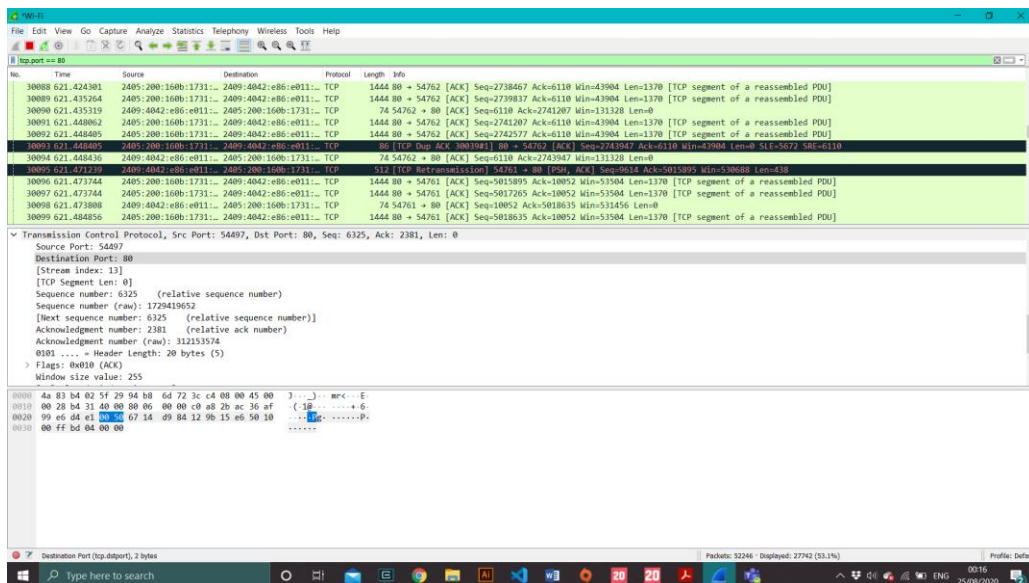
(d) **ip.src == 192.168.43.172** - Returns all the packets having source ip address as 192.168.43.172



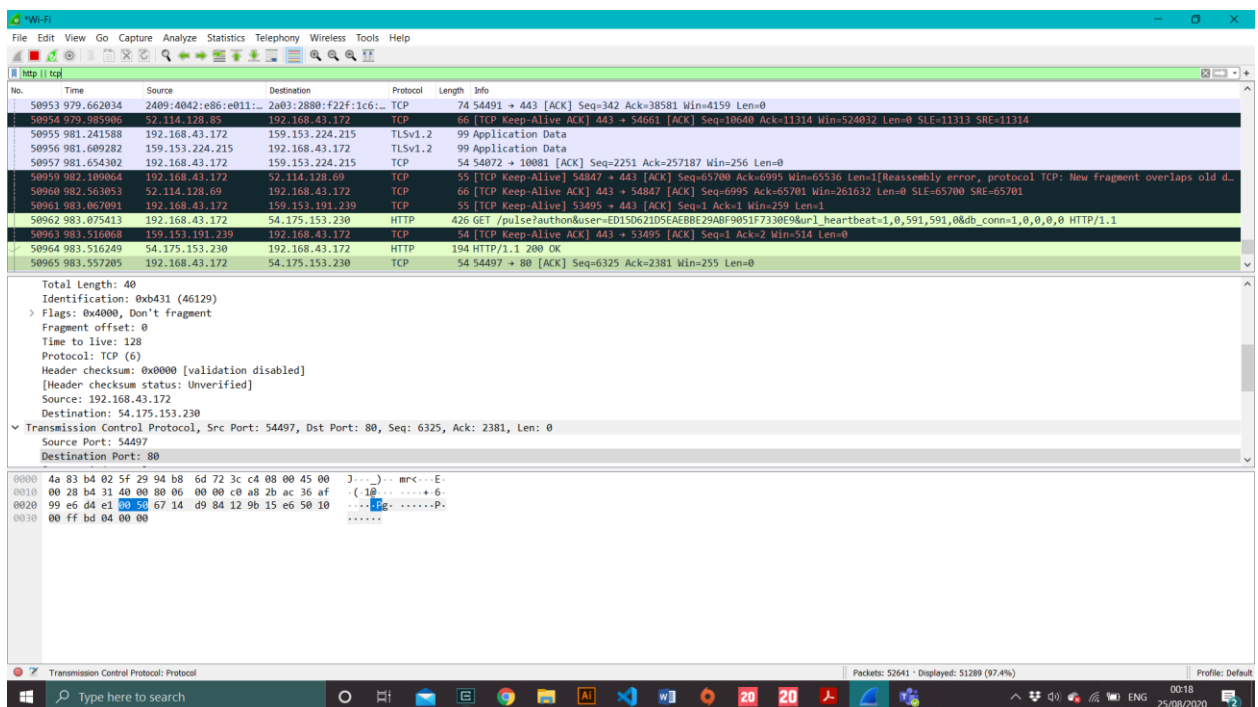
(e) **ip.dst == 159.153.191.240** - Returns all the packets that have their destination ip address as 159.159.191.240



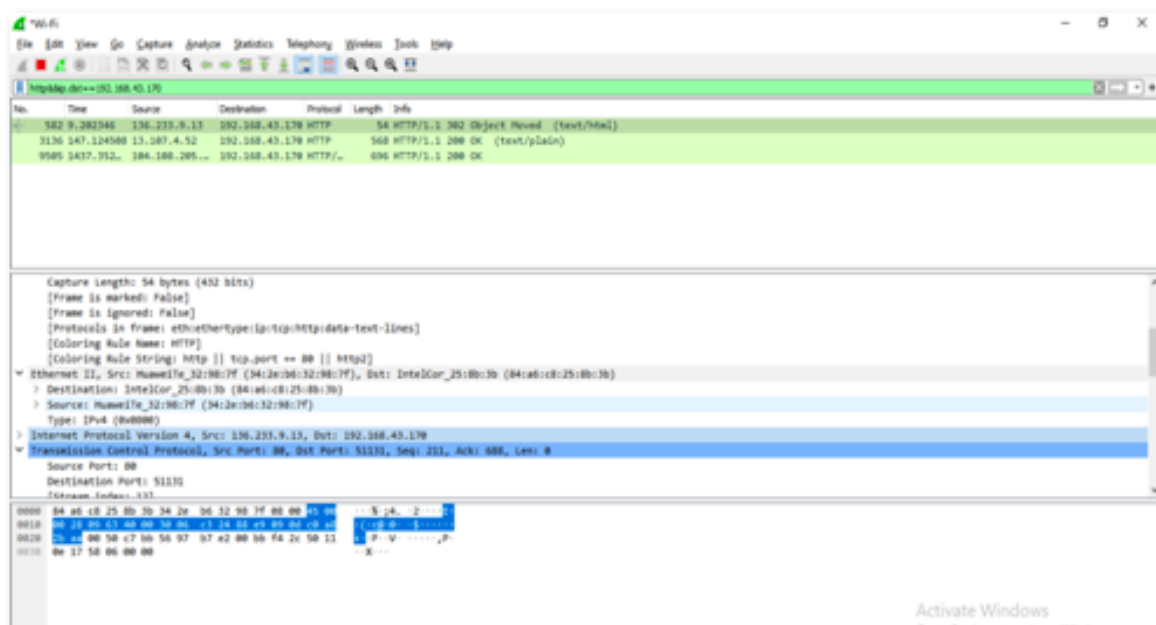
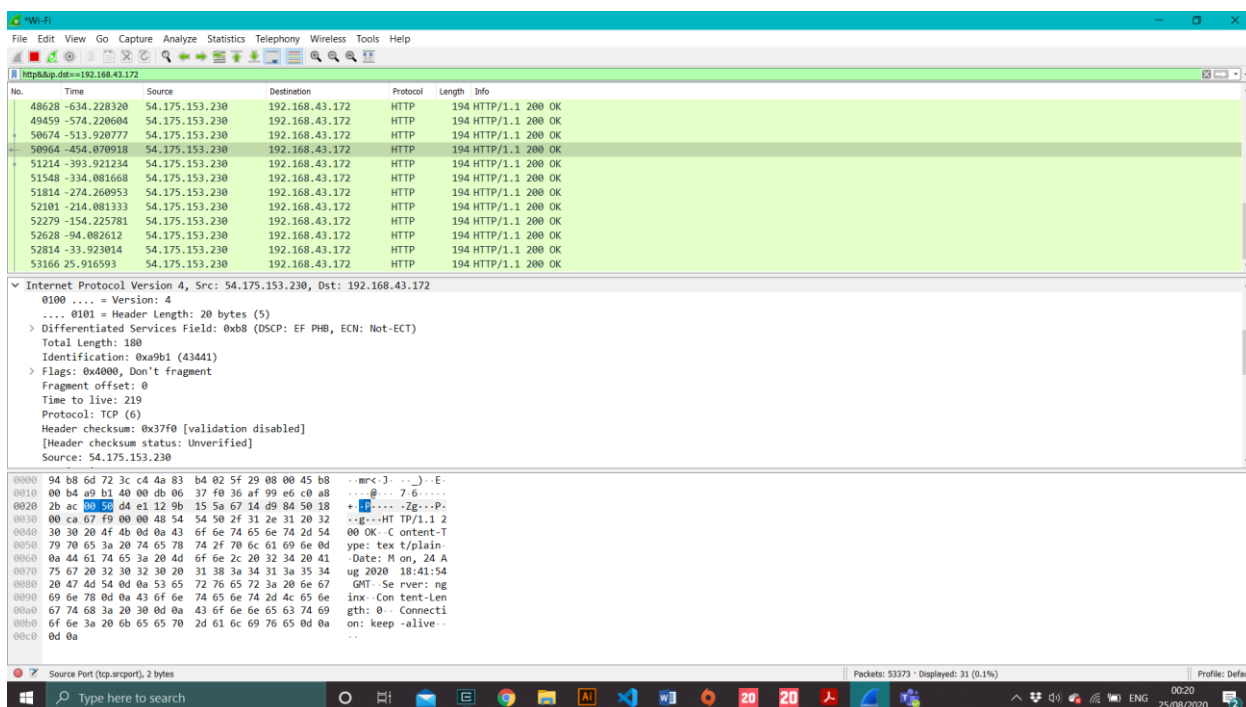
(f) **tcp.port == 80** - Returns all tcp packets which have port as 80.



(g) **http || tcp** - Returns all tcp or http packets.



(h) **http&&ip.dst==192.168.43.170** - Returns all http packets having destination ip address as 192.168.43.170



(i) tcp contains 3b:08:00 - Returns all tcp packets containing 3b:08:00 in the header

Wireshark packet capture showing a TCP segment of a reassembled PDU. The packet list shows two segments: 12764 (430.810937) and 22482 (580.090672). The selected packet 22482 is a TCP segment from 2405:200:160b:1731::2409:4042:e86:e011:: to 192.168.43.172, Seq=122702, Ack=861, Win=1370, Len=1370. The packet details show Ethernet II, Internet Protocol Version 6, and Transmission Control Protocol. The packet bytes are displayed in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|------------|--|----------------|----------|--------|--|
| 12764 | 430.810937 | 3.7.81.32 | 192.168.43.172 | TCP | 1424 | 443 → 54689 [ACK] Seq=155323 Ack=18463 Win=56576 Len=1370 [TCP segment of a reassembled PDU] |
| 22482 | 580.090672 | 2405:200:160b:1731::2409:4042:e86:e011:: | 192.168.43.172 | TCP | 1444 | 80 → 54762 [ACK] Seq=122702 Ack=861 Win=1370 Len=1370 [TCP segment of a reassembled PDU] |

Ethernet II, Src: 4a:83:b4:02:5f:29 (4a:83:b4:02:5f:29), Dst: IntelCor_72:3c:c4 (94:b8:6d:72:3c:c4)
Destination: IntelCor_72:3c:c4 (94:b8:6d:72:3c:c4)
Address: IntelCor_72:3c:c4 (94:b8:6d:72:3c:c4)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
Source: 4a:83:b4:02:5f:29 (4a:83:b4:02:5f:29)
Address: 4a:83:b4:02:5f:29 (4a:83:b4:02:5f:29)
.....1..... = LG bit: Locally administered address (this is NOT the factory default)
.....0..... = IG bit: Individual address (unicast)
Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: 2405:200:160b:1731::312c:7311, Dst: 2409:4042:e86:e011:bd53:d3c6:e28a:a21f
Transmission Control Protocol, Src Port: 80, Dst Port: 54762, Seq: 122702, Ack: 861, Len: 1370
Source Port: 80

0030 d3 c6 e2 8a a2 1f 00 50 d5 ea c0 9d 08 da b9 b1P.....
0040 e1 64 50 10 00 f2 c6 0a 00 00 00 00 20 20 b0dP.....
0050 01 00 00 40 40 60 03 00 00 80 80 c0 06 00@.....
0060 00 00 01 81 04 00 00 00 02 02 1b 00 00:.....
0070 00 04 36 00 00 00 00 00 0c 00 00 00 10-6---1---
0080 10 d9 00 00 00 20 20 b0 01 00 00 40 40 60@.....
0090 03 00 00 80 80 c0 06 00 00 00 01 81 0d 00:.....
00a0 00 00 02 02 1b 00 00 00 04 04 36 00 00-6---1---
00b0 00 08 0c 6c 00 00 00 10 10 d8 00 00 00 20:.....
00c0 10 b0 01 00 00 40 40 60 03 00 00 00 00 c0:.....
00d0 00 00 00 01 81 0d 00 00 00 02 02 1b 00:.....
00e0 00 00 04 36 00 00 00 00 08 0c 6c 00 00-6---1---
00f0 00 10 10 d8 00 00 20 20 b0 01 00 00 40 40:.....
0100 00 03 00 00 00 80 80 c0 06 00 00 00 01 81:.....

Wireshark packet capture showing a TCP segment of a reassembled PDU. The packet list shows two segments: 1447 (11.736305) and 12817 (1406.435). The selected packet 12817 is a TCP segment from 64.91.238.144 to 192.168.43.170, Seq=544758, Ack=3874, Win=40544, Len=1320. The packet details show Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes are displayed in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|-----------|---------------|----------------|----------|--------|---|
| 1447 | 11.736305 | 136.233.9.13 | 192.168.43.170 | TCP | 1374 | 643 → 51136 [ACK] Seq=88668 Ack=1315 Win=8396 Len=1320 [TCP segment of a reassembled PDU] |
| 12817 | 1406.435 | 64.91.238.144 | 192.168.43.170 | TCP | 1374 | 643 → 51171 [ACK] Seq=544758 Ack=3874 Win=40544 Len=1320 [TCP segment of a reassembled PDU] |

[Time since reference or first frame: 1406.43512000 seconds]
Frame Number: 12817
Frame Length: 1374 bytes (10992 bits)
Capture Length: 1374 bytes (10992 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: ethertype:ip:tcp]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: Huawei_Et_32:90:7f (34:2e:06:32:90:7f), Dst: IntelCor_25:80:3b (84:ad:c0:25:80:3b)
Destination: IntelCor_25:80:3b (84:ad:c0:25:80:3b)
Source: Huawei_Et_32:90:7f (34:2e:06:32:90:7f)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 64.91.238.144, Dst: 192.168.43.170
Transmission Control Protocol, Seq=544758, Ack=3874, Win=40544, Len=1320

0000 64 ad c0 25 80 3b 34 2e 06 32 90 7f 84 ad c0 25 80 3bE.....
0010 05 50 5d e5 48 00 2f 06 0f 50 40 50 ee 90 c0 a0P.....
0020 26 aa 8c b6 c8 47 5a 90 52 02 12 43 8f 6d 50 38@.....
0030 02 5c 39 08 00 00 4f 1d 7b 4e 00 00 c3 c3 8a:.....
0040 f8 5b 4d 45 77 f0 42 13 9f 45 83 54 0d 26 8e 68@.....
0050 70 2e 3f 06 4e 5d a9 7c 50 4b c7 e5 c0 5f f0 f6-7-@-[]@.....
0060 c5 53 ec 47 53 87 f2 bd 7e 95 68 82 a1 a6 91 4e\$-@---b---P
0070 82 e6 8c 73 67 30 c7 82 ee a0 cc 38 50 e5 e7 58@---@-@-@-
0080 28 68 1a 8f 68 50 39 6d 9d 47 f8 55 c4 98 25 72b---@---@-@-
0090 c5 3a 7e da 29 92 6a 5d ec 3f 94 25 83 49 46 49-+---}---[.....

(j) http || tcp contains e2:8a:a2 - Returns http packets or tcp packets containing e2:8a:a2 in the header.

