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

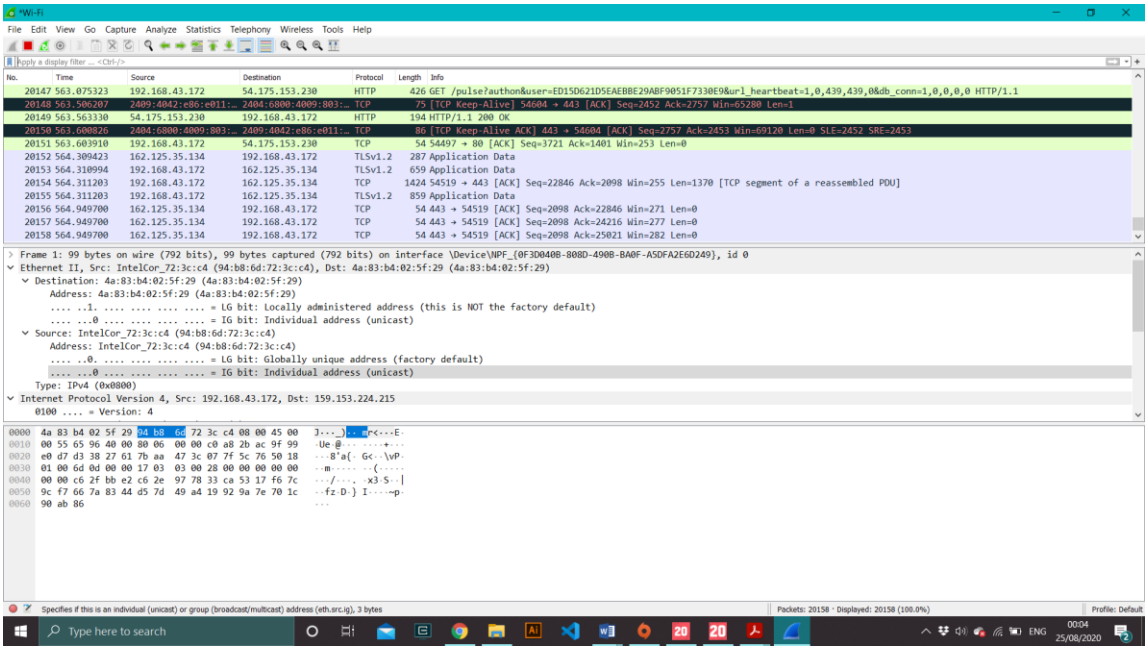
VELLORE INSTITUTE OF TECHNOLOGY VELLORE – 632 014

TAMIL NADU, INDIA

Wireshark - HTTP analysis

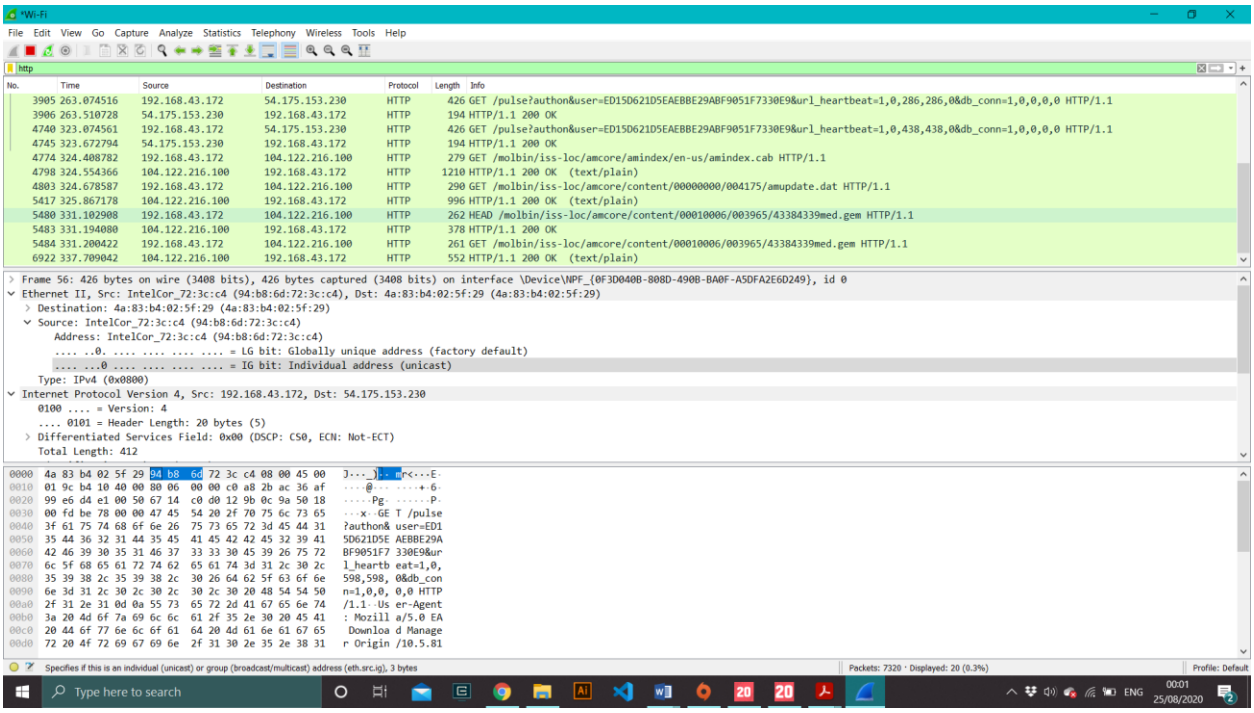
Procedure:

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.i n
6. Then, you will be able to see packet flow in the wireshark app.

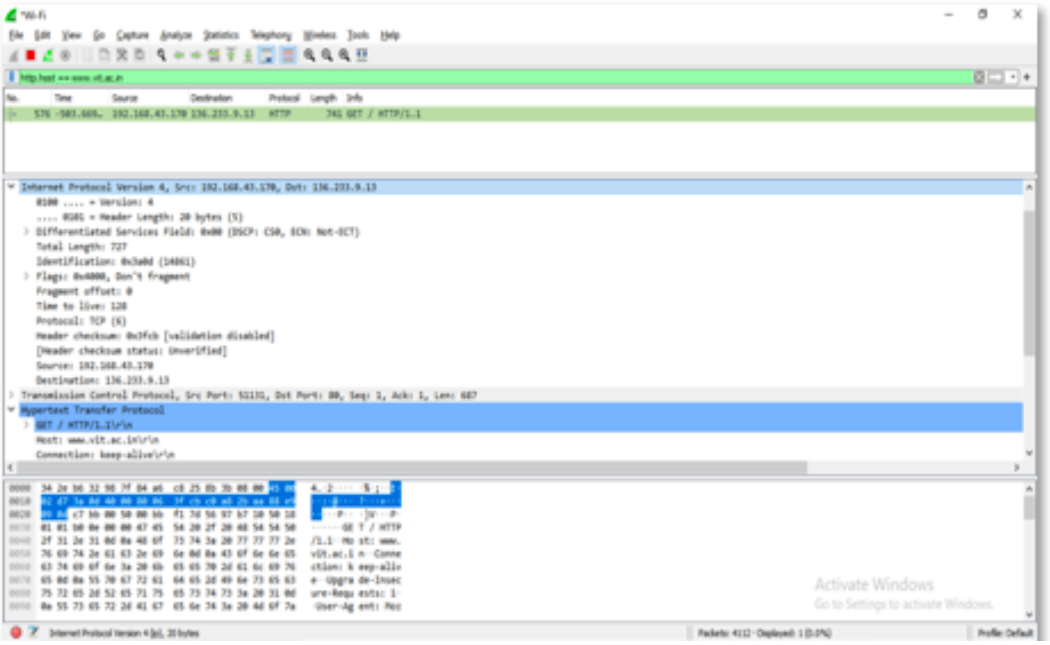


7. The packets can be filtered and analysed by entering some queries in the filter text box.
8. Some of the important queries to analyze the packets include:

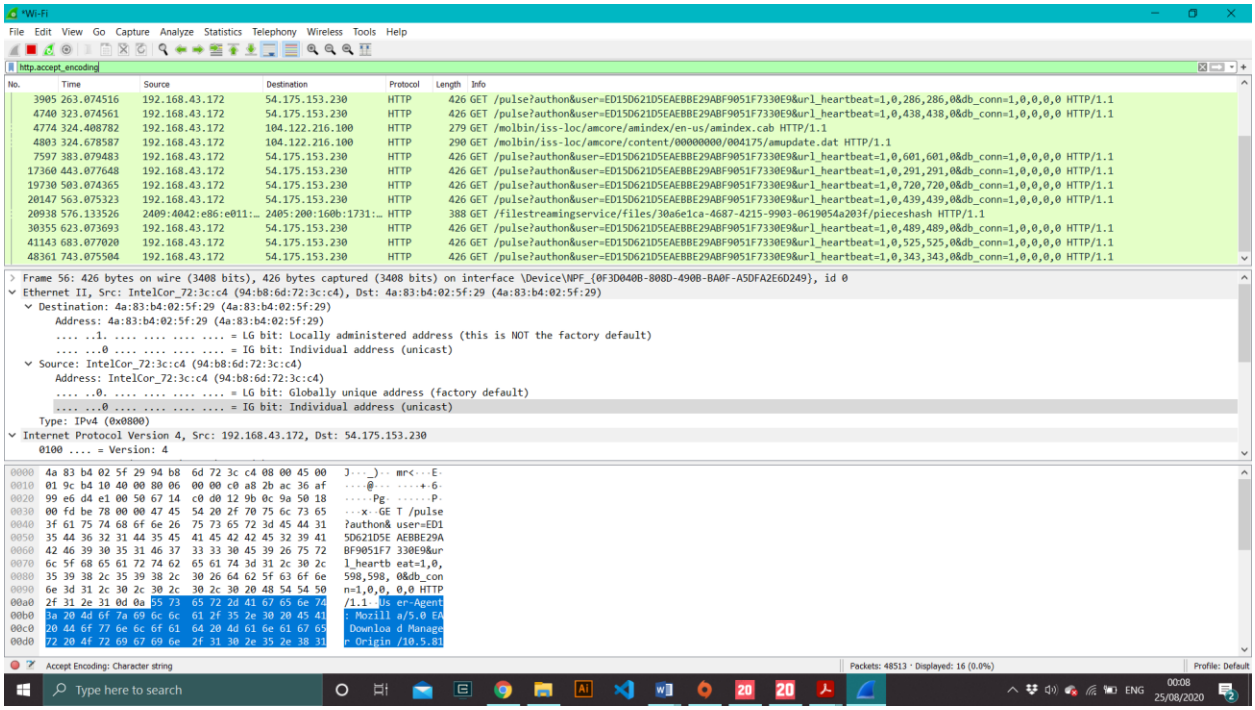
(a) **http** - This will return all the http packets.

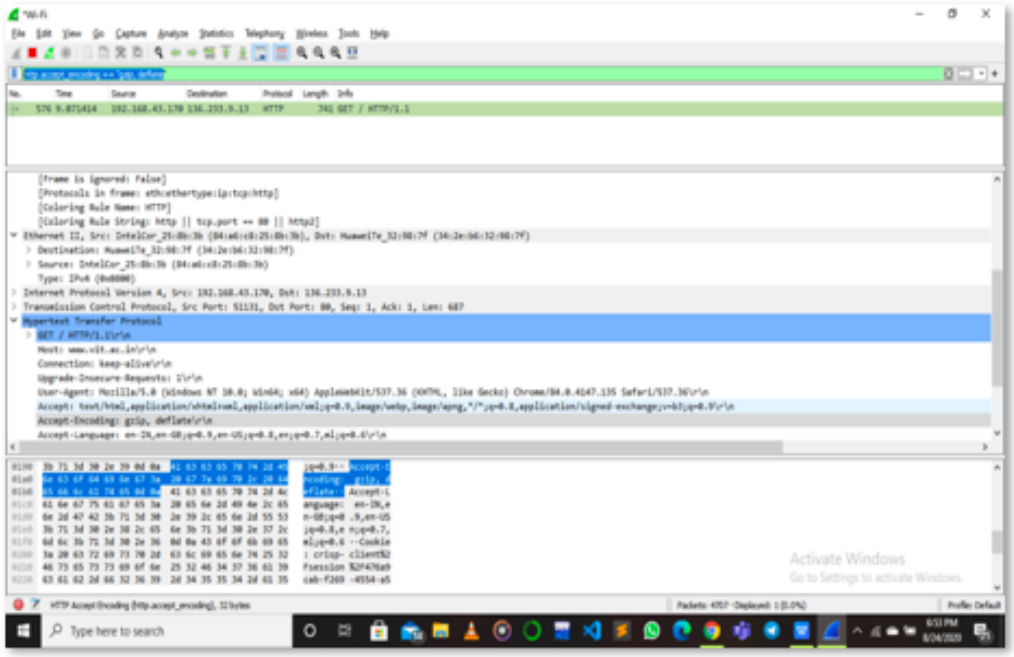


(b) **http.host == w ww.vit.ac.in** - This will return the http packets directed to www.vit.ac.in

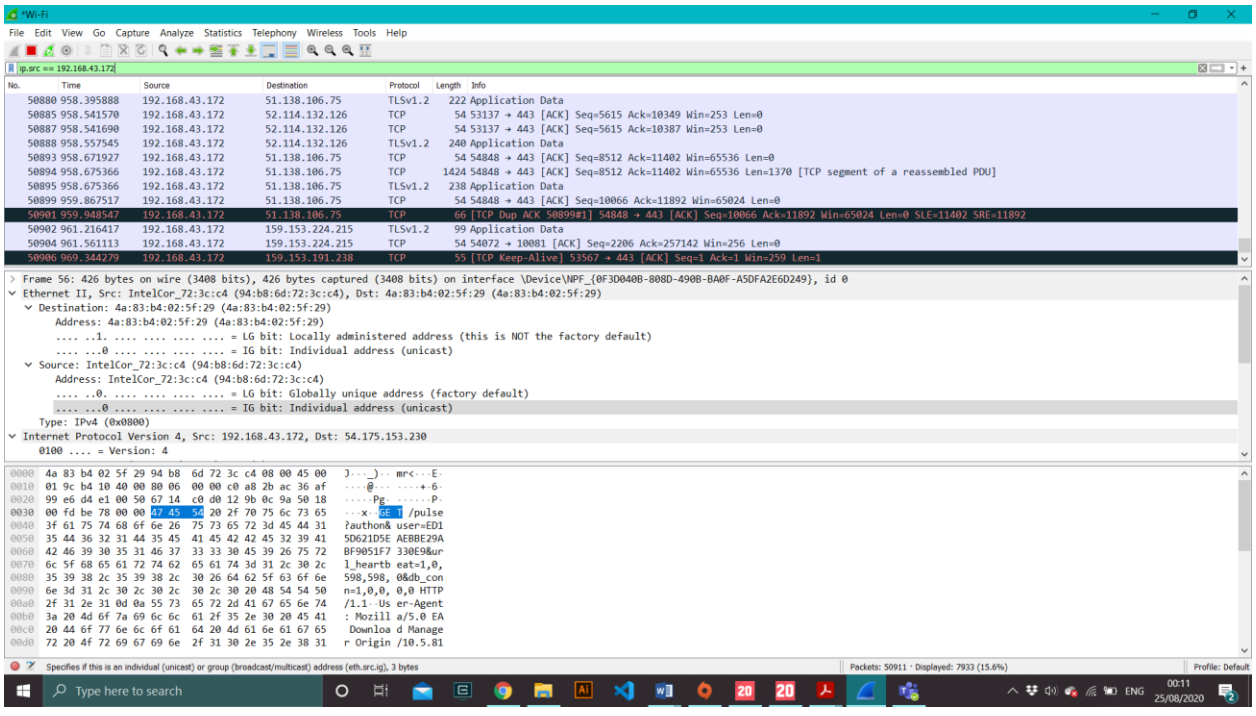


(c) **http.accept_encoding == “gzip, deflate”** - This will return all the packets which have the encoding as gzip, deflate.

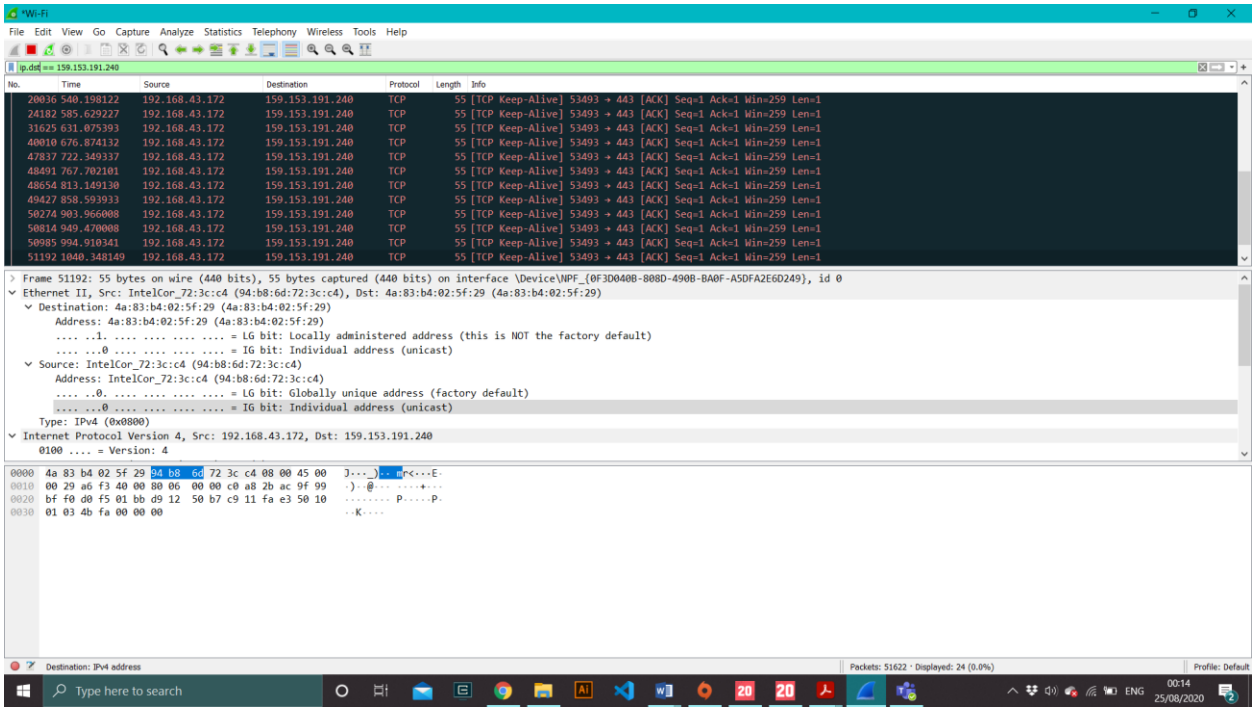




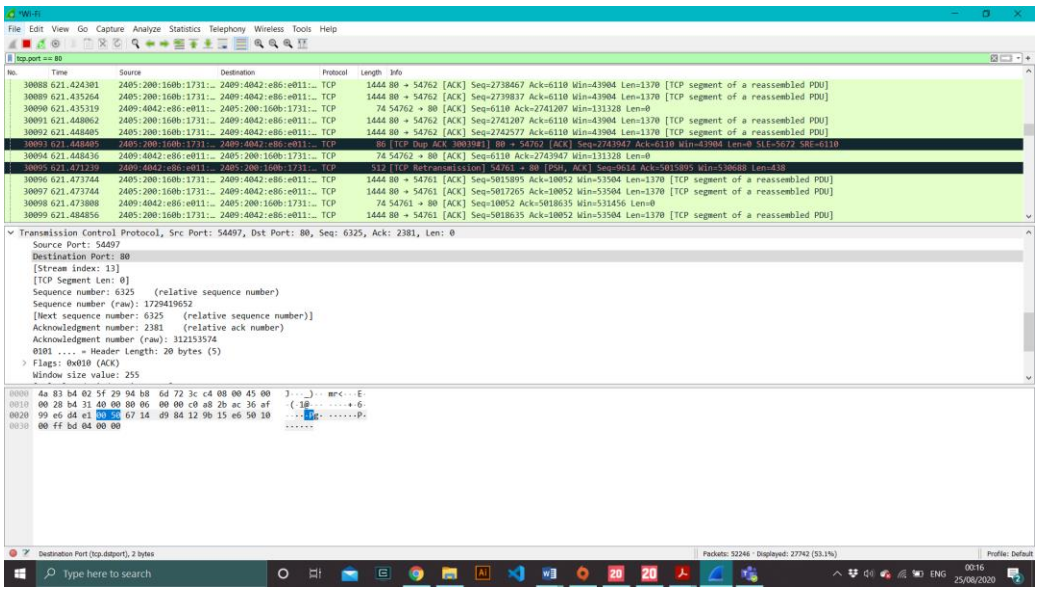
(d) **ip.src == 192.168.43.172** - Returns all the packets having source ip address as 192.168.43.172



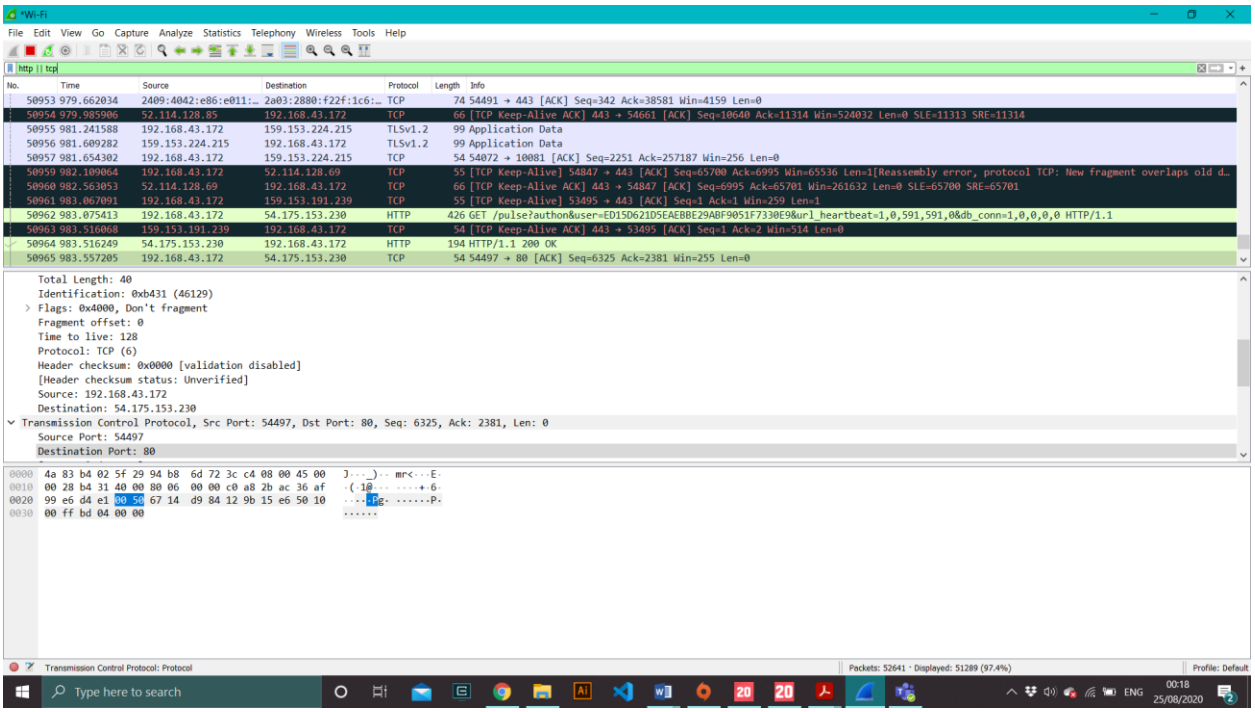
(e) **ip.dst == 159.153.191.240** - Returns all the packets that have their destination ip address as 159.159.191.240



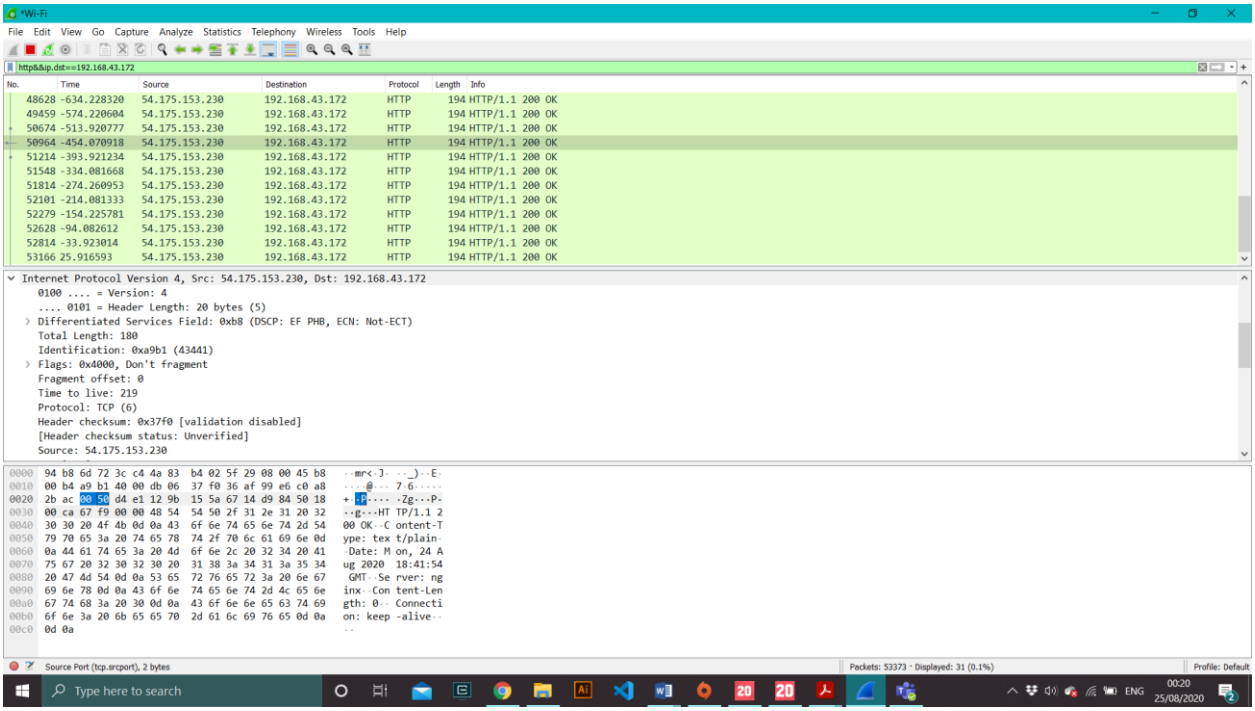
(f) **tcp.port == 80** - Returns all tcp packets which have port as 80.

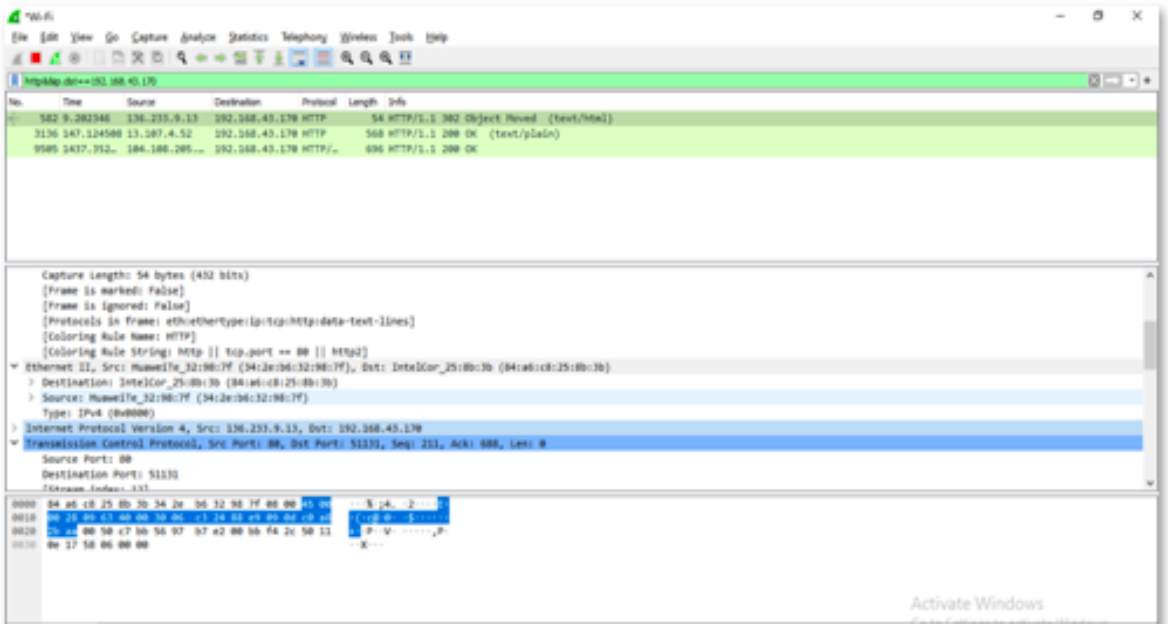


(g) **http || tcp** - Returns all tcp or http packets.

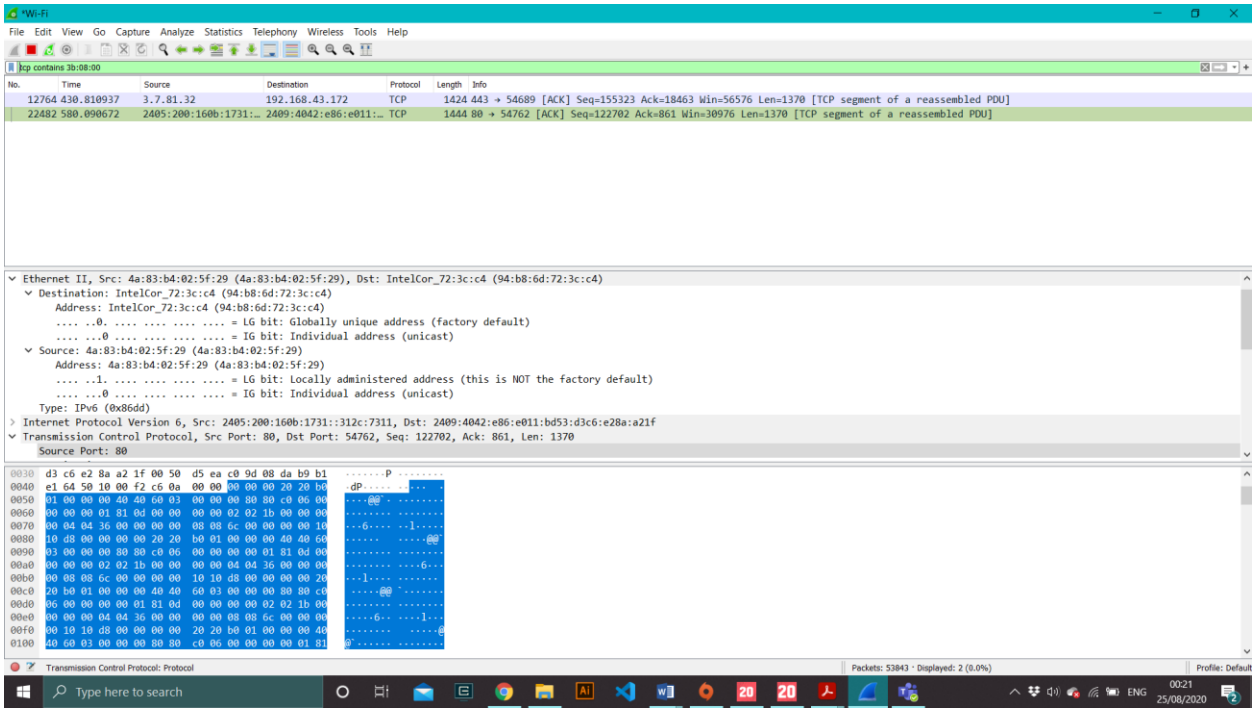


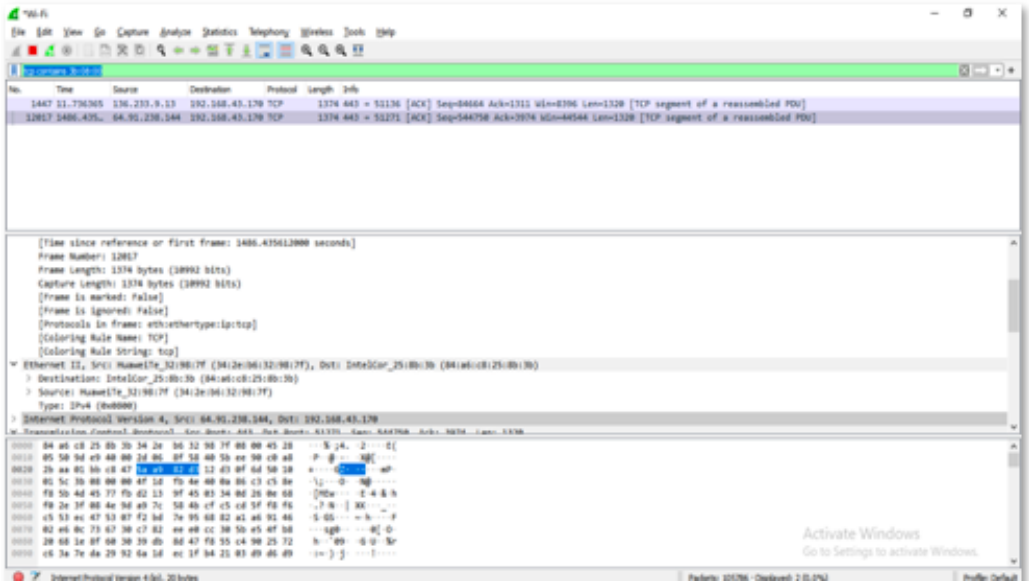
(h) http&&ip.dst==192.168.43.170 - Returns all http packets having destination ip address as 192.168.43.170





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


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp contains 3b:08:00
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:… TCP 1444 80 → 54762 [ACK] Seq=122702 Ack=861 Win=30976 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
Transmission Control Protocol: Protocol
Packets: 53843 · Displayed: 2 (0.0%)
Profile: Default
Type here to search
ENG
00:21
25/08/2020


*Wi-Fi
[Time since reference or first frame: 1486.435612000 seconds]
Frame Number: 12017
Frame Length: 1374 bytes (10992 bits)
Capture Length: 1374 bytes (10992 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: HuaweiTe_32:98:7f (34:2e:b6:32:98:7f), Dst: IntelCor_25:8b:3b (84:a6:c8:25:8b:3b)
Destination: IntelCor_25:8b:3b (84:a6:c8:25:8b:3b)
Source: HuaweiTe_32:98:7f (34:2e:b6:32:98:7f)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 64.91.238.144, Dst: 192.168.43.170
Activate Windows
Go to Settings to activate Windows.

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