Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Computer Science & Engineering

CSE3501 – Information Security Analysis and Audit

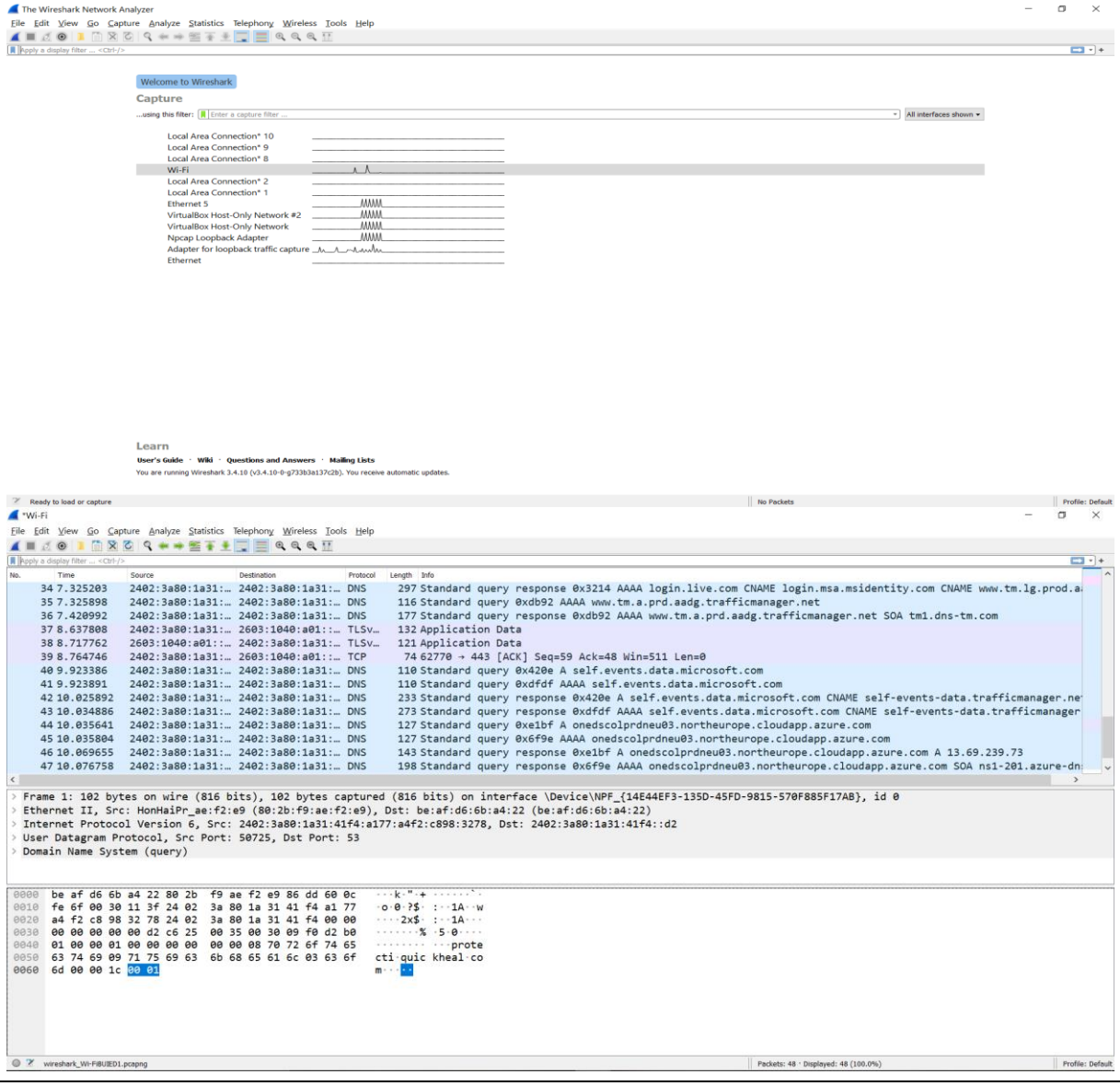
LAB ASSIGNMENT 4

Submitted to **Prof. RAJA SP**

NAME: PUNIT MIDDHA
REG.NO: 19BCE2060
SLOT: L39+L40
DATE: 20/11/2021

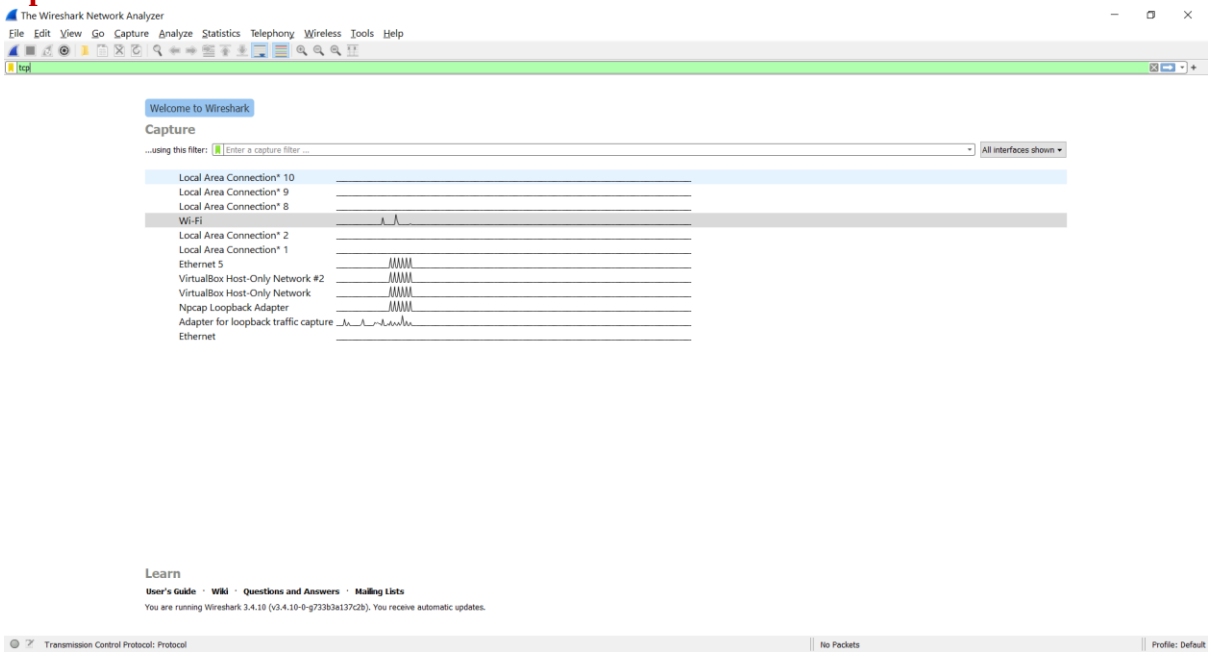
Network Packets Sniffing using Wireshark

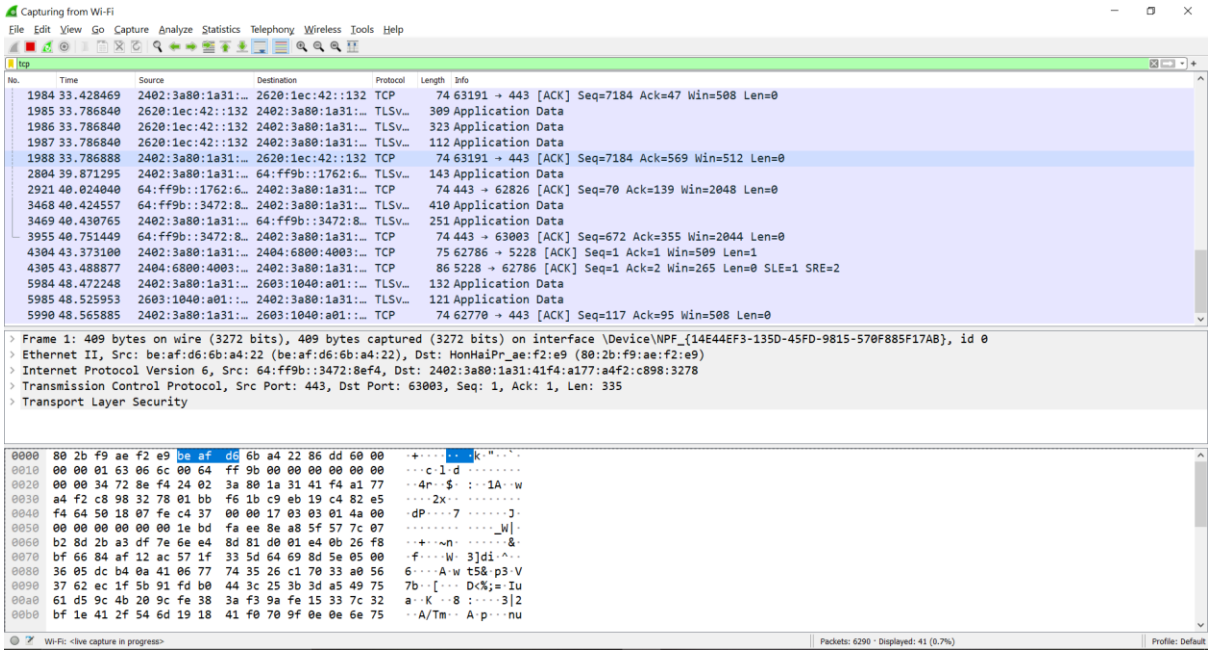
1. Interfaces



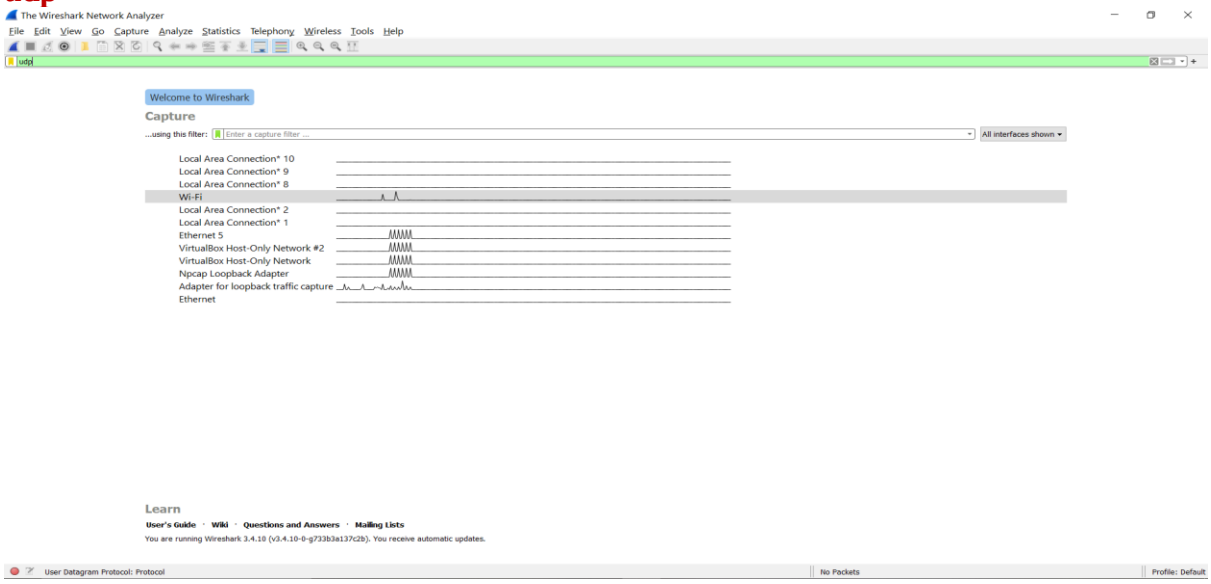
2. Apply a filter which shows the packets which belongs to any one of the categories (ICMP, ARP, UDP, TCP)

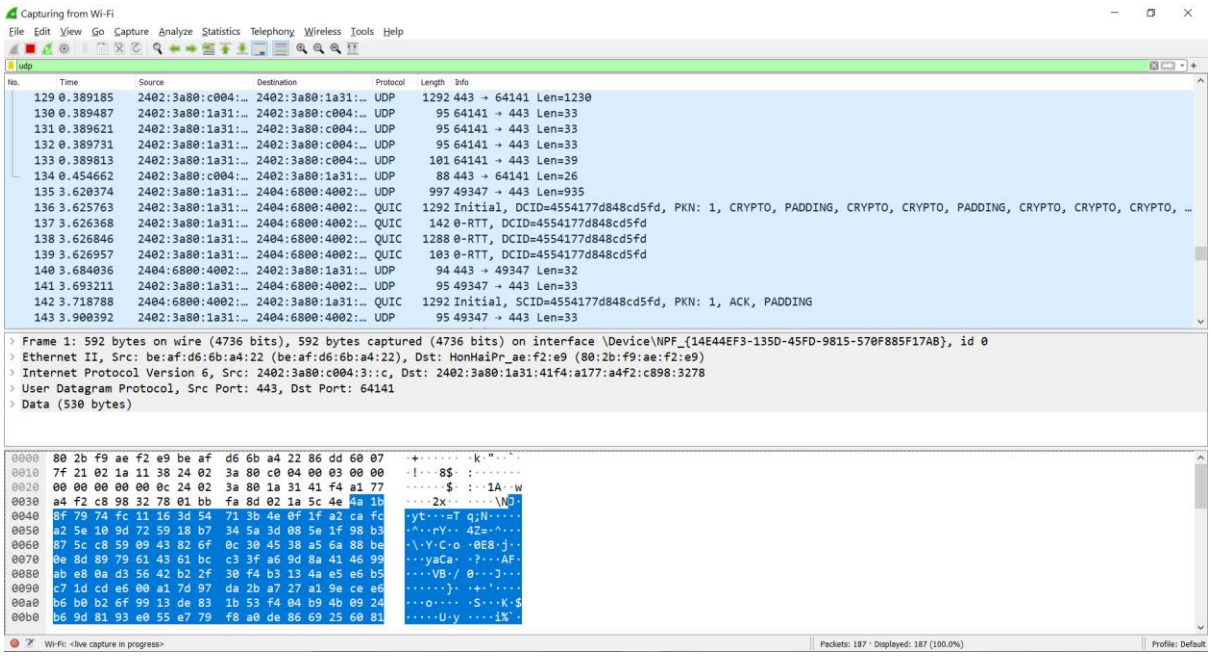
tcp



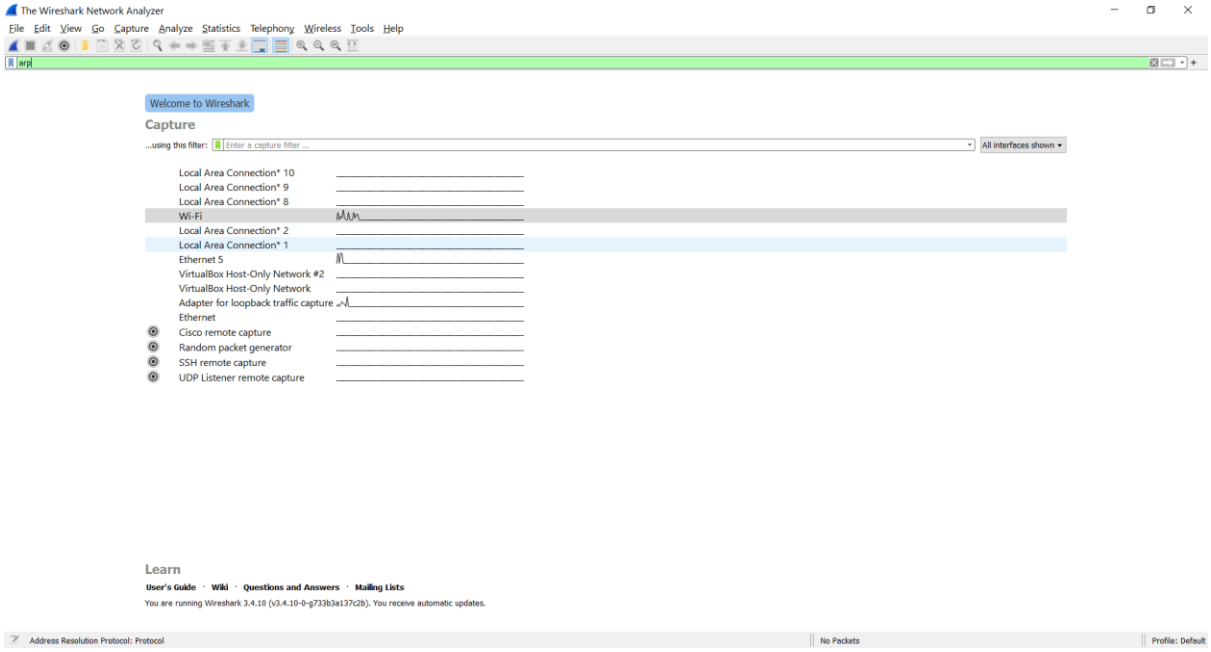


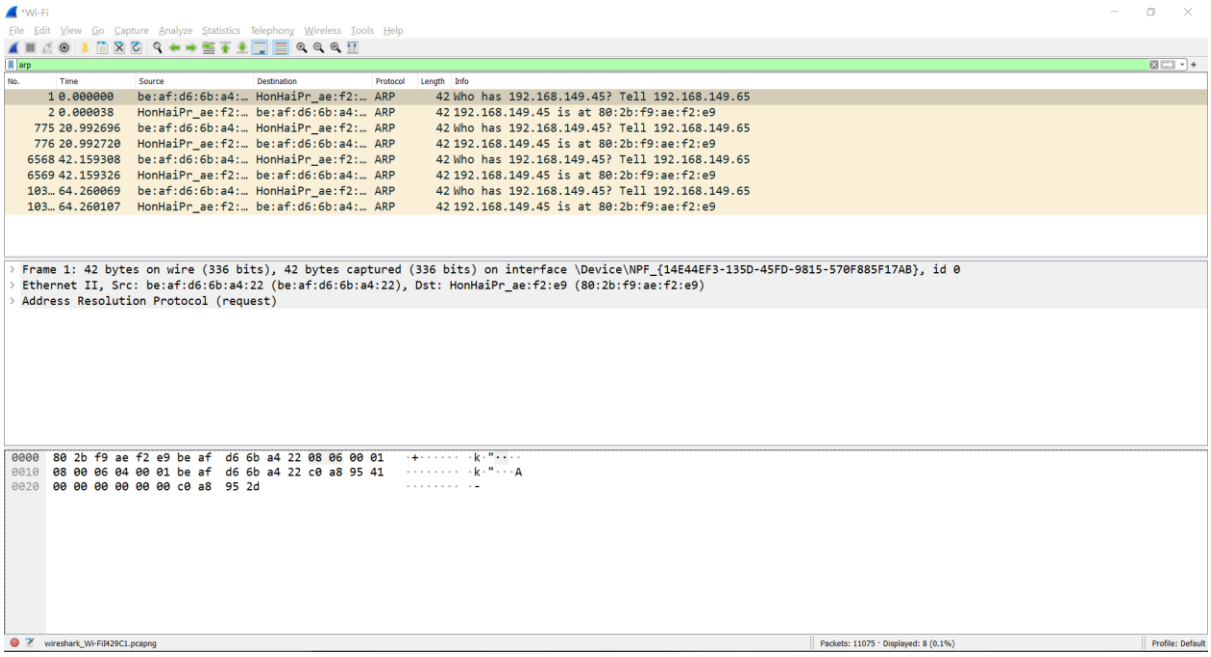
udp



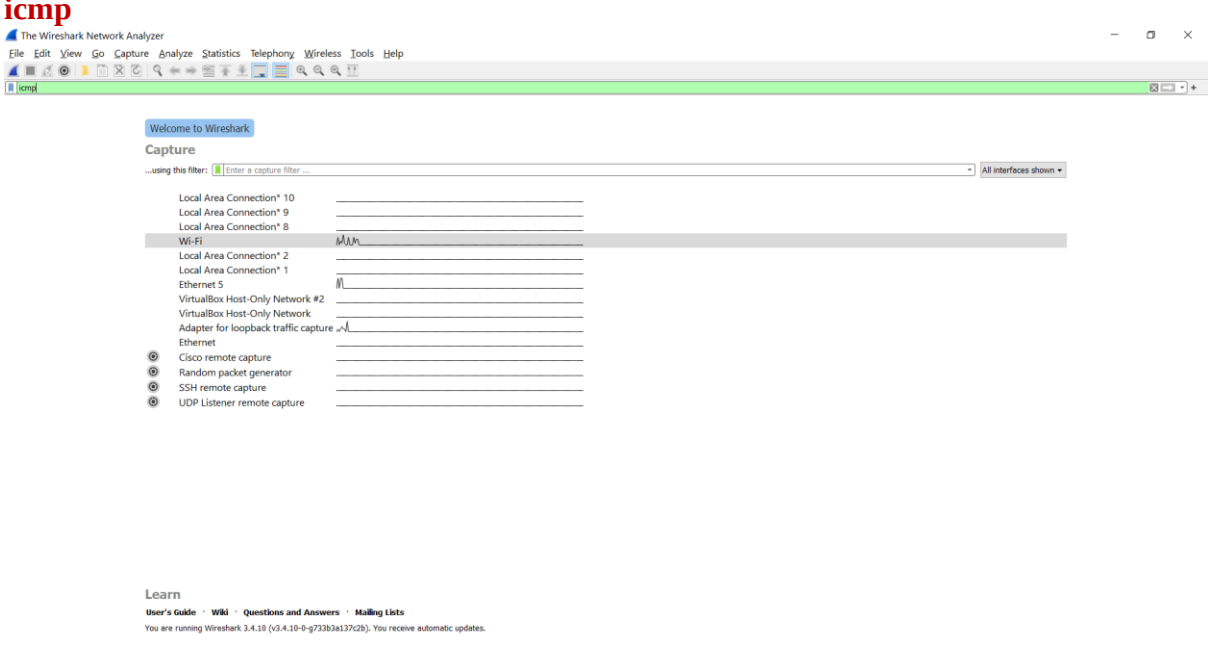

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
No. Time Source Destination Protocol Length Info
129 0.389185 2402:3a80:c004:… 2402:3a80:1a31:… UDP 1292 443 → 64141 Len=1230
130 0.389487 2402:3a80:1a31:… 2402:3a80:c004:… UDP 95 64141 → 443 Len=33
131 0.389621 2402:3a80:1a31:… 2402:3a80:c004:… UDP 95 64141 → 443 Len=33
132 0.389731 2402:3a80:1a31:… 2402:3a80:c004:… UDP 95 64141 → 443 Len=33
133 0.389813 2402:3a80:1a31:… 2402:3a80:c004:… UDP 101 64141 → 443 Len=39
134 0.454662 2402:3a80:c004:… 2402:3a80:1a31:… UDP 88 443 → 64141 Len=26
135 3.620374 2402:3a80:1a31:… 2404:6800:4002:… UDP 997 49347 → 443 Len=935
136 3.625763 2402:3a80:1a31:… 2404:6800:4002:… QUIC 1292 Initial, DCID=4554177d848cd5fd, PKN: 1, CRYPTO, PADDING, CRYPTO, CRYPTO, PADDING, CRYPTO, CRYPTO, CRYPTO, …
137 3.626368 2402:3a80:1a31:… 2404:6800:4002:… QUIC 142 0-RTT, DCID=4554177d848cd5fd
138 3.626846 2402:3a80:1a31:… 2404:6800:4002:… QUIC 1288 0-RTT, DCID=4554177d848cd5fd
139 3.626957 2402:3a80:1a31:… 2404:6800:4002:… QUIC 103 0-RTT, DCID=4554177d848cd5fd
140 3.684036 2404:6800:4002:… 2402:3a80:1a31:… UDP 94 443 → 49347 Len=32
141 3.693211 2402:3a80:1a31:… 2404:6800:4002:… UDP 95 49347 → 443 Len=33
142 3.718788 2404:6800:4002:… 2402:3a80:1a31:… QUIC 1292 Initial, SCID=4554177d848cd5fd, PKN: 1, ACK, PADDING
143 3.900392 2402:3a80:1a31:… 2404:6800:4002:… UDP 95 49347 → 443 Len=33
Frame 1: 592 bytes on wire (4736 bits), 592 bytes captured (4736 bits) on interface \Device\NPF_{14E44EF3-135D-45FD-9815-570F885F17AB}, id 0
Ethernet II, Src: be:af:d6:6b:a4:22 (be:af:d6:6b:a4:22), Dst: HonHaiPr_ae:f2:e9 (80:2b:f9:ae:f2:e9)
Internet Protocol Version 6, Src: 2402:3a80:c004:3::c, Dst: 2402:3a80:1a31:41f4:a177:a4f2:c898:3278
User Datagram Protocol, Src Port: 443, Dst Port: 64141
Data (530 bytes)
0000 80 2b f9 ae f2 e9 be af d6 6b a4 22 86 dd 60 07
0010 7f 21 02 1a 11 38 24 02 3a 80 c0 04 00 03 00 00
0020 00 00 00 00 00 0c 24 02 3a 80 1a 31 41 f4 a1 77
0030 a4 f2 c8 98 32 78 01 bb fa 8d 02 1a 5c 4e 4a 1b
0040 8f 79 74 fc 11 16 3d 54 71 3b 4e 0f 1f a2 ca fc
0050 a2 5e 10 9d 72 59 18 b7 34 5a 3d 08 5e 1f 98 b3
0060 87 5c c8 59 09 43 82 6f 0c 30 45 38 a5 6a 88 be
0070 0e 8d 89 79 61 43 61 bc c3 3f a6 9d 8a 41 46 99
0080 ab e8 0a d3 56 42 b2 2f 30 f4 b3 13 4a e5 e6 b5
0090 c7 1d cd e6 00 a1 7d 97 da 2b a7 27 a1 9e ce e6
00a0 b6 b0 b2 6f 99 13 de 83 1b 53 f4 04 b9 4b 09 24
00b0 b6 9d 81 93 e0 55 e7 79 f8 a0 de 86 69 25 60 81
Wi-Fi: <live capture in progress>
Packets: 187 · Displayed: 187 (100.0%)
Profile: Default

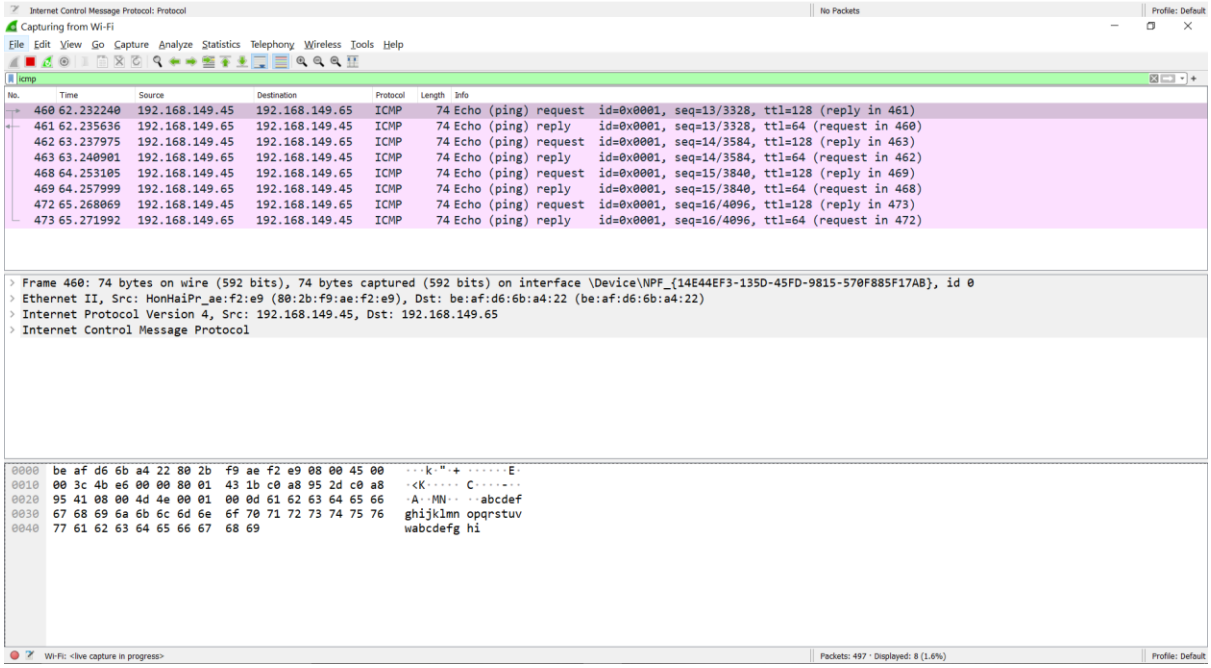
arp


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
Welcome to Wireshark
Capture
…using this filter: Enter a capture filter …
All interfaces shown
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Wi-Fi
Local Area Connection* 2
Local Area Connection* 1
Ethernet 5
VirtualBox Host-Only Network #2
VirtualBox Host-Only Network
Adapter for loopback traffic capture
Ethernet
Cisco remote capture
Random packet generator
SSH remote capture
UDP Listener remote capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.4.10 (v3.4.10-0-g733b3a137c2b). You receive automatic updates.
Address Resolution Protocol: Protocol
No Packets
Profile: Default

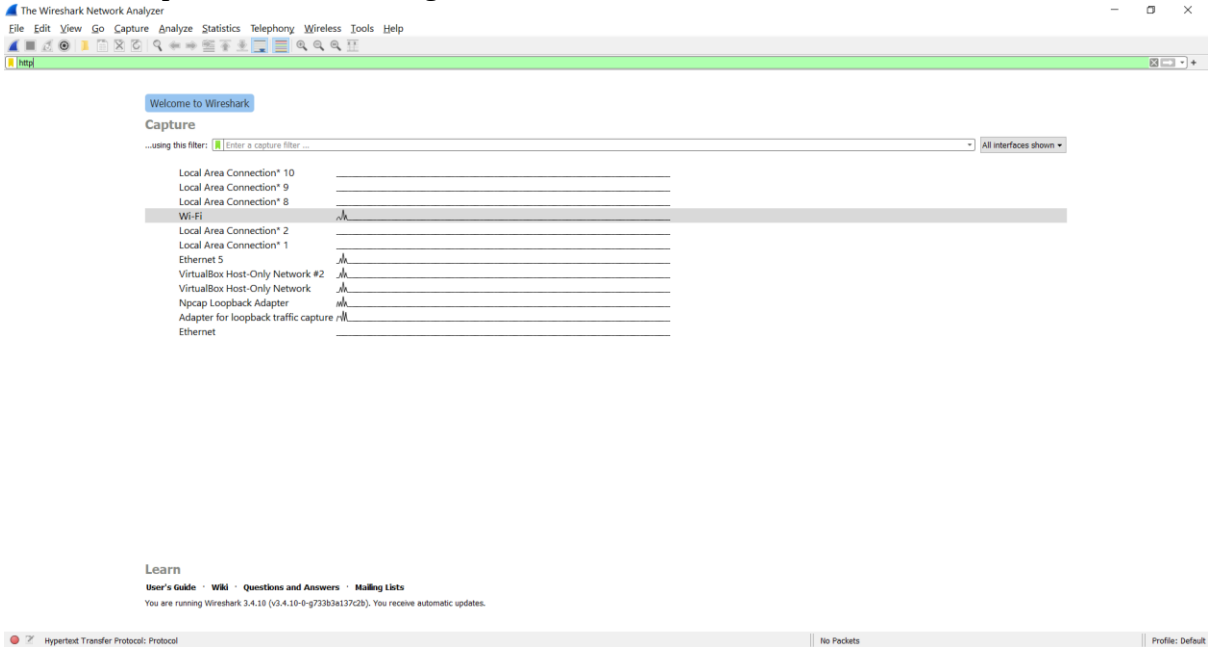

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Source Destination Protocol Length Info
1 0.000000 be:af:d6:6b:a4:… HonHaiPr_ae:f2:… ARP 42 Who has 192.168.149.45? Tell 192.168.149.65
2 0.000038 HonHaiPr_ae:f2:… be:af:d6:6b:a4:… ARP 42 192.168.149.45 is at 80:2b:f9:ae:f2:e9
775 20.992696 be:af:d6:6b:a4:… HonHaiPr_ae:f2:… ARP 42 Who has 192.168.149.45? Tell 192.168.149.65
776 20.992720 HonHaiPr_ae:f2:… be:af:d6:6b:a4:… ARP 42 192.168.149.45 is at 80:2b:f9:ae:f2:e9
6568 42.159308 be:af:d6:6b:a4:… HonHaiPr_ae:f2:… ARP 42 Who has 192.168.149.45? Tell 192.168.149.65
6569 42.159326 HonHaiPr_ae:f2:… be:af:d6:6b:a4:… ARP 42 192.168.149.45 is at 80:2b:f9:ae:f2:e9
103… 64.260069 be:af:d6:6b:a4:… HonHaiPr_ae:f2:… ARP 42 Who has 192.168.149.45? Tell 192.168.149.65
103… 64.260107 HonHaiPr_ae:f2:… be:af:d6:6b:a4:… ARP 42 192.168.149.45 is at 80:2b:f9:ae:f2:e9
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{14E44EF3-135D-45FD-9815-570F885F17AB}, id 0
Ethernet II, Src: be:af:d6:6b:a4:22 (be:af:d6:6b:a4:22), Dst: HonHaiPr_ae:f2:e9 (80:2b:f9:ae:f2:e9)
Address Resolution Protocol (request)
0000 80 2b f9 ae f2 e9 be af d6 6b a4 22 08 06 00 01
0010 08 00 06 04 00 01 be af d6 6b a4 22 c0 a8 95 41
0020 00 00 00 00 00 00 c0 a8 95 2d
wireshark_Wi-Fi429C1.pcapng
Packets: 11075 · Displayed: 8 (0.1%)
Profile: Default

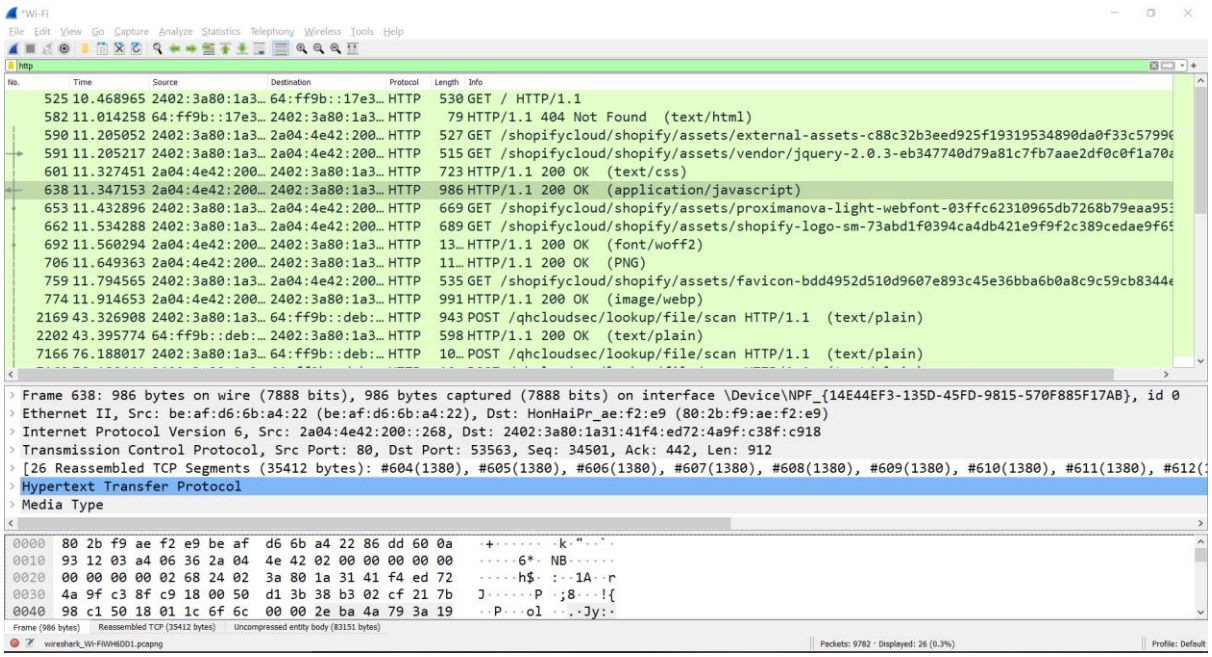
icmp





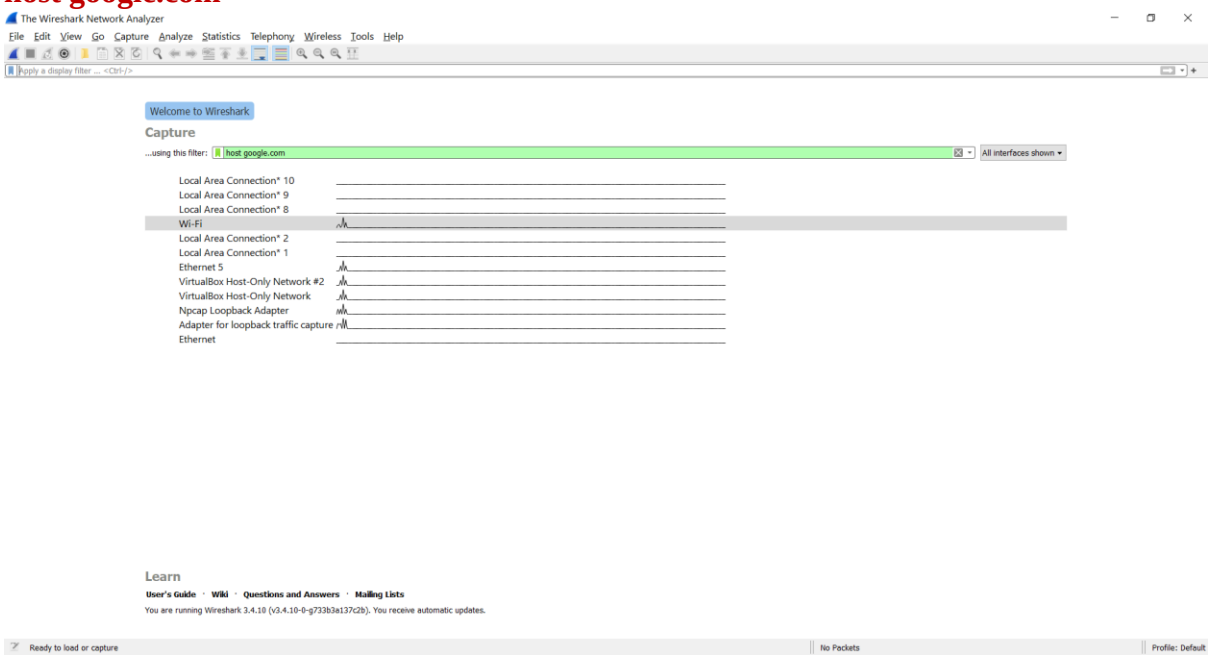
3. Receive the packets which belongs to HTTP

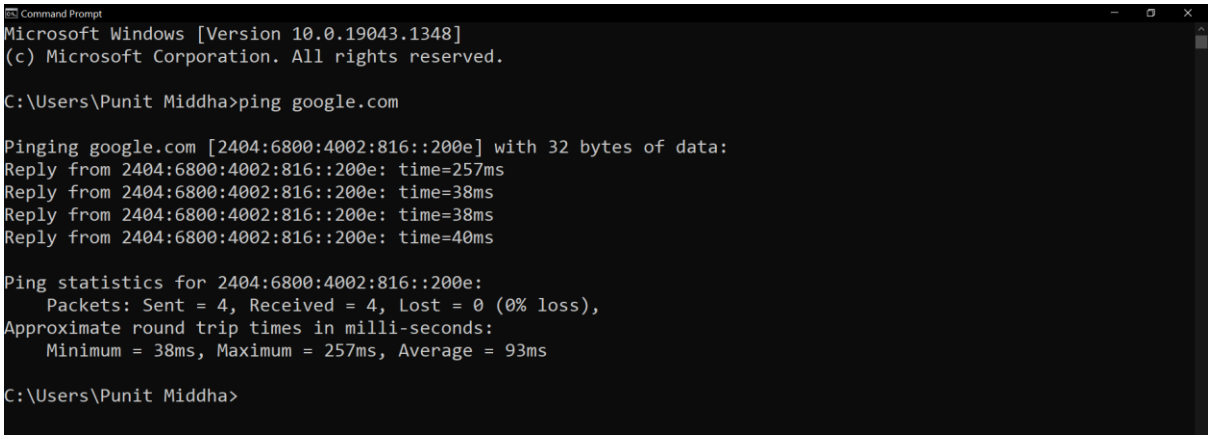


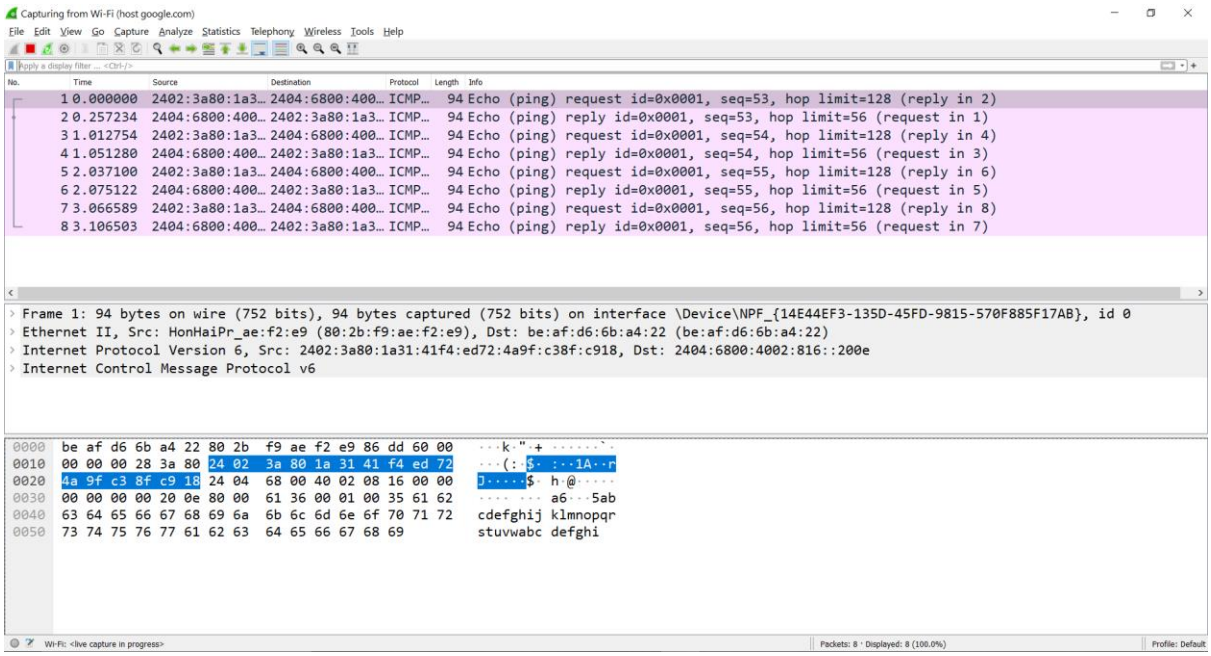


4. Apply a filter which is able to capture the packets from a particular website

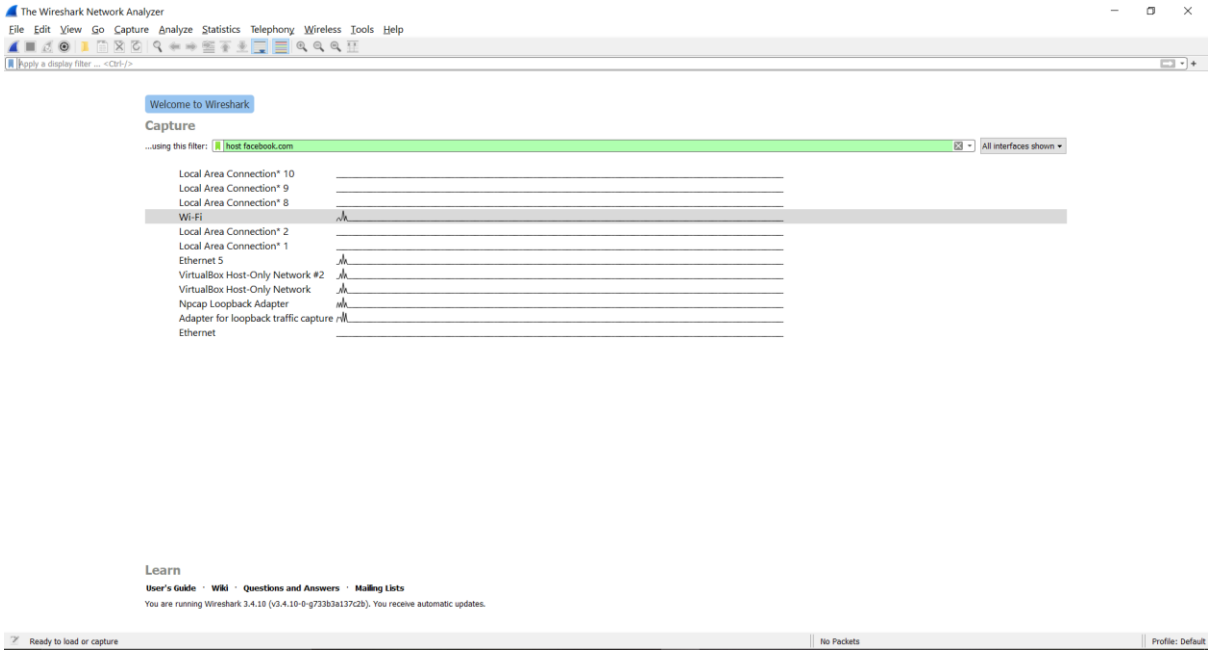
host google.com

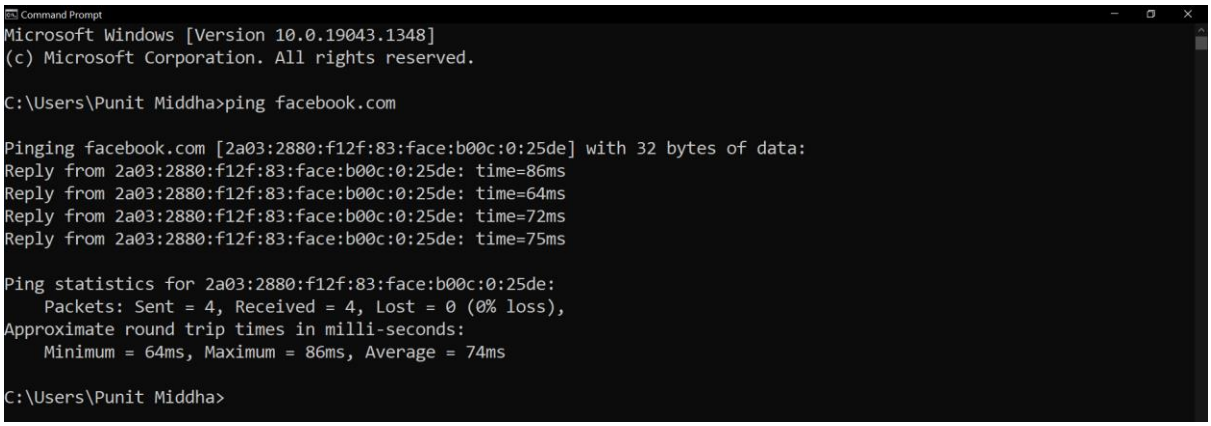


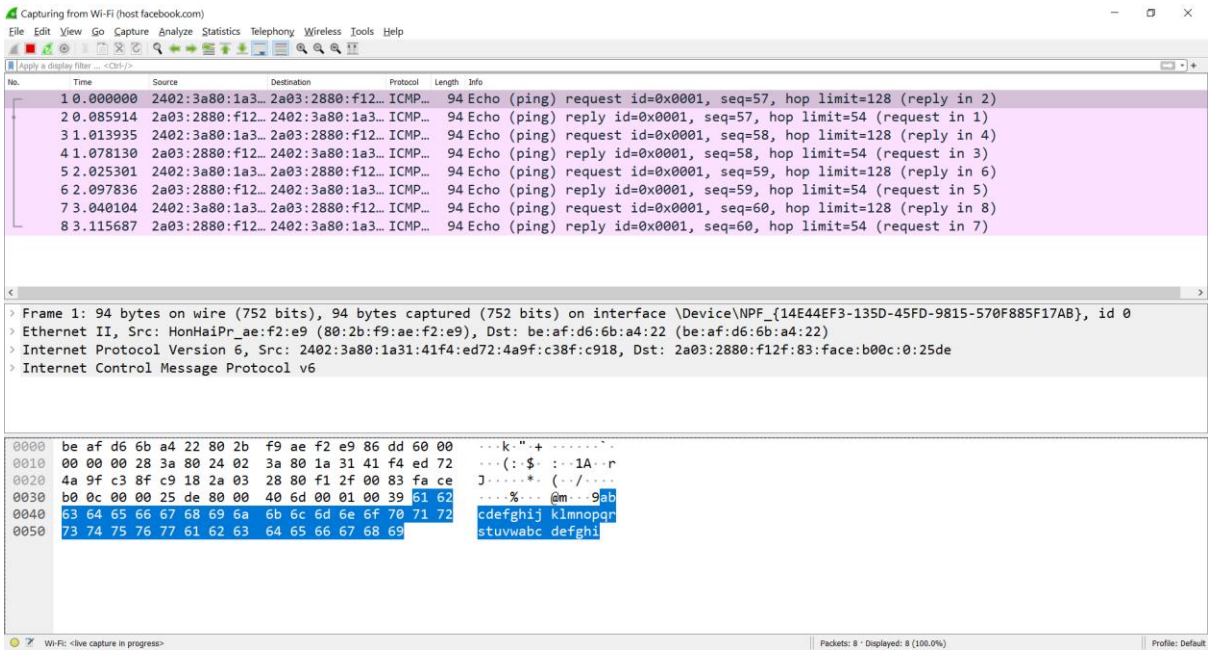




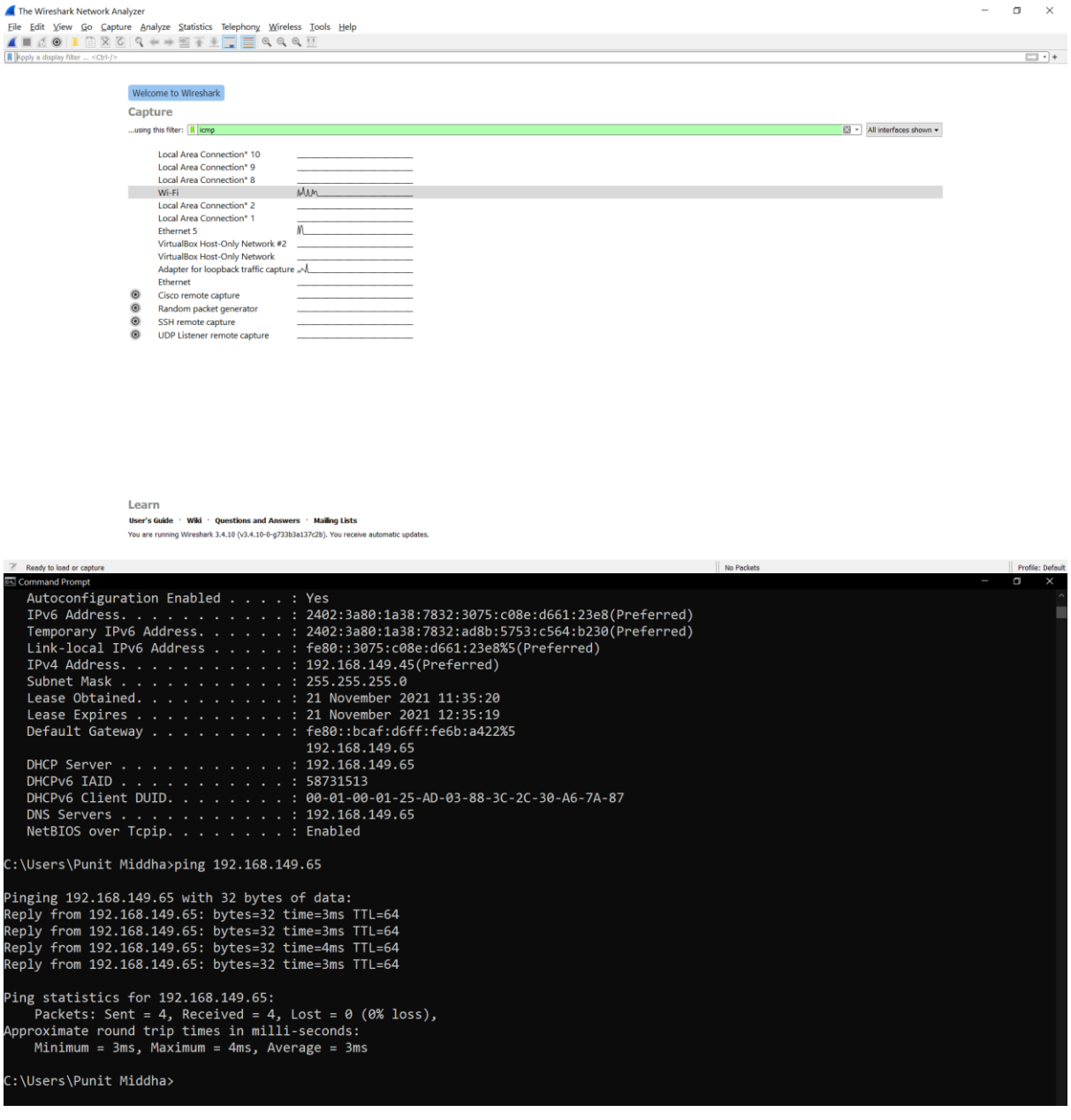
host facebook.com

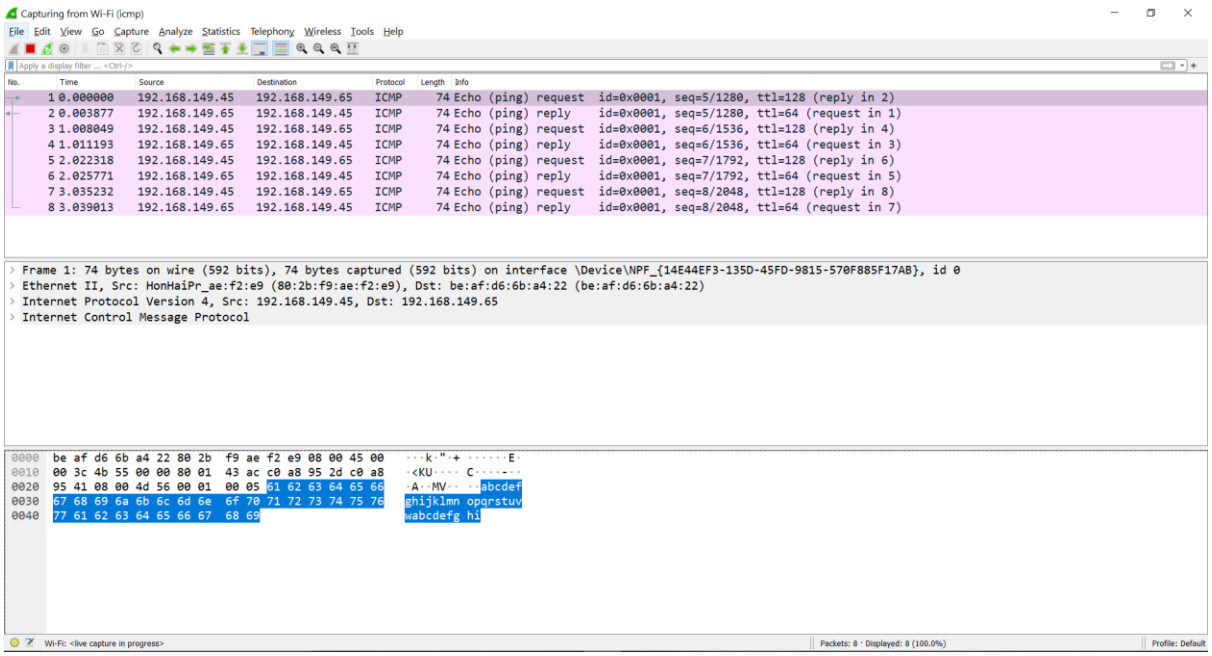






5. Receive the packets which belongs to icmp




Capturing from Wi-Fi (icmp)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.149.45 192.168.149.65 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 2)
2 0.003877 192.168.149.65 192.168.149.45 ICMP 74 Echo (ping) reply id=0x0001, seq=5/1280, ttl=64 (request in 1)
3 1.008049 192.168.149.45 192.168.149.65 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 4)
4 1.011193 192.168.149.65 192.168.149.45 ICMP 74 Echo (ping) reply id=0x0001, seq=6/1536, ttl=64 (request in 3)
5 2.022318 192.168.149.45 192.168.149.65 ICMP 74 Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 6)
6 2.025771 192.168.149.65 192.168.149.45 ICMP 74 Echo (ping) reply id=0x0001, seq=7/1792, ttl=64 (request in 5)
7 3.035232 192.168.149.45 192.168.149.65 ICMP 74 Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 8)
8 3.039013 192.168.149.65 192.168.149.45 ICMP 74 Echo (ping) reply id=0x0001, seq=8/2048, ttl=64 (request in 7)
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{14E44EF3-135D-45FD-9815-570F885F17AB}, id 0
Ethernet II, Src: HonHaiPr_ae:f2:e9 (80:2b:f9:ae:f2:e9), Dst: be:af:d6:6b:a4:22 (be:af:d6:6b:a4:22)
Internet Protocol Version 4, Src: 192.168.149.45, Dst: 192.168.149.65
Internet Control Message Protocol
0000 be af d6 6b a4 22 80 2b f9 ae f2 e9 08 00 45 00
0010 00 3c 4b 55 00 00 80 01 43 ac c0 a8 95 2d c0 a8
0020 95 41 08 00 4d 56 00 01 00 05 61 62 63 64 65 66
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040 77 61 62 63 64 65 66 67 68 69
Wi-Fi: <live capture in progress>
Packets: 8 · Displayed: 8 (100.0%)
Profile: Default