



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

The screenshot displays the Wireshark Network Analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The 'Capture' window is open, showing a list of network interfaces. The 'Wi-Fi' interface is selected. Below the 'Capture' window, the 'Packets' list shows a series of DNS queries and responses. The packet details pane shows the structure of a DNS query packet, including Ethernet II, Internet Protocol Version 6, User Datagram Protocol, and Domain Name System (query). The packet bytes pane shows the raw hex and ASCII data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
34	7.325203	2402:3a80:1a31::	2402:3a80:1a31::	DNS	297	Standard query response 0x3214 AAAA login.live.com CNAME login.msa.msidentity.com CNAME www.tm.lg.prod.a
35	7.325898	2402:3a80:1a31::	2402:3a80:1a31::	DNS	116	Standard query 0xdb92 AAAA www.tm.a.prd.aadg.trafficmanager.net
36	7.420992	2402:3a80:1a31::	2402:3a80:1a31::	DNS	177	Standard query response 0xdb92 AAAA www.tm.a.prd.aadg.trafficmanager.net SOA tml.dns-tm.com
37	8.637808	2402:3a80:1a31::	2603:1040:a01::	TLSv...	132	Application Data
38	8.717762	2603:1040:a01::	2402:3a80:1a31::	TLSv...	121	Application Data
39	8.764746	2402:3a80:1a31::	2603:1040:a01::	TCP	74	62770 → 443 [ACK] Seq=59 Ack=48 Win=511 Len=0
40	9.923386	2402:3a80:1a31::	2402:3a80:1a31::	DNS	110	Standard query 0x429e A self.events.data.microsoft.com
41	9.923891	2402:3a80:1a31::	2402:3a80:1a31::	DNS	110	Standard query 0xdf0f AAAA self.events.data.microsoft.com
42	10.025892	2402:3a80:1a31::	2402:3a80:1a31::	DNS	233	Standard query response 0x429e A self.events.data.microsoft.com CNAME self-events-data.trafficmanager.net
43	10.034886	2402:3a80:1a31::	2402:3a80:1a31::	DNS	273	Standard query response 0xdf0f AAAA self.events.data.microsoft.com CNAME self-events-data.trafficmanager.net
44	10.035641	2402:3a80:1a31::	2402:3a80:1a31::	DNS	127	Standard query 0xe1bf A onedscolprneu03.northeurope.cloudapp.azure.com
45	10.035804	2402:3a80:1a31::	2402:3a80:1a31::	DNS	127	Standard query 0x6f9e AAAA onedscolprneu03.northeurope.cloudapp.azure.com
46	10.069655	2402:3a80:1a31::	2402:3a80:1a31::	DNS	143	Standard query response 0xe1bf A onedscolprneu03.northeurope.cloudapp.azure.com A 13.69.239.73
47	10.076758	2402:3a80:1a31::	2402:3a80:1a31::	DNS	198	Standard query response 0x6f9e AAAA onedscolprneu03.northeurope.cloudapp.azure.com SOA ns1-201.azure-dn

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{14E44EF3-135D-45FD-9815-570F885F17A8}, 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 6, Src: 2402:3a80:1a31:41f4:a177:a4f2:c898:3278, Dst: 2402:3a80:1a31:41f4:d2

User Datagram Protocol, Src Port: 50725, Dst Port: 53

Domain Name System (query)

0000 be af d6 6b a4 22 80 2b f9 ae f2 e9 86 dd 60 0c ...k...+.....
0010 fe 6f 00 30 11 3f 24 02 3a 80 1a 31 41 f4 a1 77 ...o 0? \$: : 1A w
0020 a4 f2 c8 98 32 78 24 02 3a 80 1a 31 41 f4 00 00 ...2x\$: : 1A w
0030 00 00 00 00 d2 c6 25 00 35 00 30 09 f0 d2 b0% 5 0 : :
0040 01 00 00 01 00 00 00 00 00 00 08 70 72 6f 74 65prote
0050 63 74 69 09 71 75 69 63 6b 68 65 61 6c 03 63 6f cti:quic kheal:co
0060 6d 00 00 1c 00 01 m...4

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

tcp

Wireshark 3.4.10 interface showing packet capture on Wi-Fi. The packet list displays several TCP and TLSv1.2 packets. The packet details pane shows the structure of a TCP packet (Frame 1). The packet bytes pane shows the raw hex and ASCII data.

Transmission Control Protocol: Protocol

Profile: Default

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
1984	33.428469	2402:3a80:1a31::...	2620:1ec:42::132	TCP	74	63191 → 443 [ACK] Seq=7184 Ack=47 Win=508 Len=0
1985	33.786840	2620:1ec:42::132	2402:3a80:1a31::...	TLSv1.2	309	Application Data
1986	33.786840	2620:1ec:42::132	2402:3a80:1a31::...	TLSv1.2	323	Application Data
1987	33.786840	2620:1ec:42::132	2402:3a80:1a31::...	TLSv1.2	112	Application Data
1988	33.786888	2402:3a80:1a31::...	2620:1ec:42::132	TCP	74	63191 → 443 [ACK] Seq=7184 Ack=569 Win=512 Len=0
2804	39.871295	2402:3a80:1a31::...	64:ff9b::1762:6::	TLSv1.2	143	Application Data
2921	40.024040	64:ff9b::1762:6::	2402:3a80:1a31::...	TCP	74	443 → 62826 [ACK] Seq=70 Ack=139 Win=2048 Len=0
3468	40.424557	64:ff9b::1762:6::	2402:3a80:1a31::...	TLSv1.2	410	Application Data
3469	40.430765	2402:3a80:1a31::...	64:ff9b::1762:6::	TLSv1.2	251	Application Data
3955	40.751449	64:ff9b::1762:6::	2402:3a80:1a31::...	TCP	74	443 → 63003 [ACK] Seq=672 Ack=355 Win=2044 Len=0
4304	43.373100	2402:3a80:1a31::...	2404:6800:4003::...	TCP	75	62786 → 5228 [ACK] Seq=1 Ack=1 Win=509 Len=1
4305	43.488877	2404:6800:4003::...	2402:3a80:1a31::...	TCP	86	5228 → 62786 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
5984	48.472248	2402:3a80:1a31::...	2603:1040:a01::...	TLSv1.2	132	Application Data
5985	48.525953	2603:1040:a01::...	2402:3a80:1a31::...	TLSv1.2	121	Application Data
5990	48.565885	2402:3a80:1a31::...	2603:1040:a01::...	TCP	74	62770 → 443 [ACK] Seq=117 Ack=95 Win=508 Len=0

> Frame 1: 409 bytes on wire (3272 bits), 409 bytes captured (3272 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: 64:ff9b::1762:8ef4, Dst: 2402:3a80:1a31:41f4:a177:a4f2:c898:3278

> Transmission Control Protocol, Src Port: 443, Dst Port: 63003, Seq: 1, Ack: 1, Len: 335

> Transport Layer Security

0000 80 2b f9 ae f2 e9 be af d6 6b a4 22 86 dd 60 00 +-+...K...
0010 00 00 01 63 06 6c 00 64 ff 9b 00 00 00 00 00 00 --cld...
0020 00 00 34 72 8e f4 24 02 3a 80 1a 31 41 f4 a1 77 --4m\$...1A:w
0030 a4 f2 c8 98 32 78 01 bb f6 1b c9 eb 19 c4 82 e5 --2x...
0040 f4 64 50 18 07 fe c4 37 00 00 17 03 03 01 4a 00 -dP...7...J...
0050 00 00 00 00 00 00 1e bd fa ee 8e a8 5f 57 7c 07 -...W...
0060 b2 8d 2b a3 df 7e 6e e4 8d 81 d0 01 e4 0b 26 f8 -+...n...&...
0070 bf 66 84 af 12 ac 57 1f 33 5d 64 69 8d 5e 05 00 -f...W...3di...
0080 36 05 dc b4 0a 41 06 77 74 35 26 c1 70 33 a0 56 6...Aw t5&p3.V
0090 37 62 ec 1f 5b 91 fd b0 44 3c 25 3b 3d a5 49 75 7b...[...D&=Iu
00a0 61 d5 9c 4b 20 9c fe 38 3a f3 9a fe 15 33 7c 32 a-K...8...3|2
00b0 bf 1e 41 2f 54 6d 19 18 41 f0 70 9f 0e 0e 6e 75 -A/Tm...A-p...nu

Wi-Fi: <live capture in progress>

Packets: 6290 · Displayed: 41 (0.7%)

Profile: Default

udp

Wireshark 3.4.10 interface showing packet capture on Wi-Fi. The packet list is empty. The packet details pane shows the structure of a User Datagram Protocol (UDP) packet.

User Datagram Protocol: Protocol

Profile: Default

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

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

Npcap Loopback Adapter

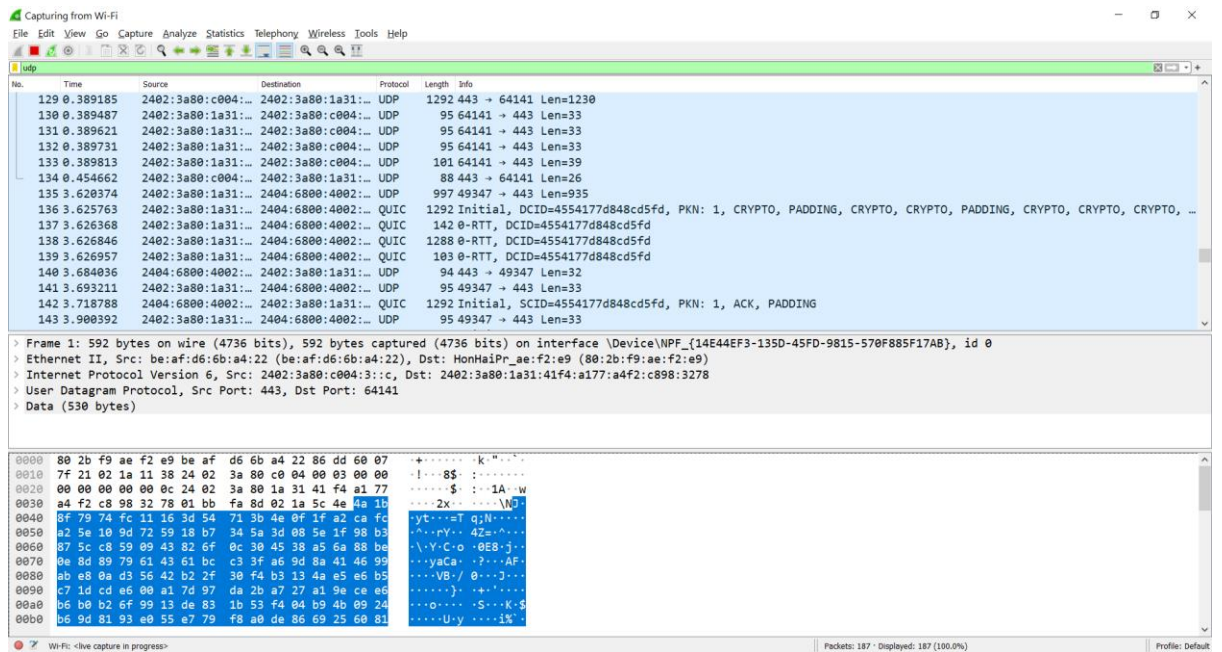
Adapter for loopback traffic capture

Ethernet

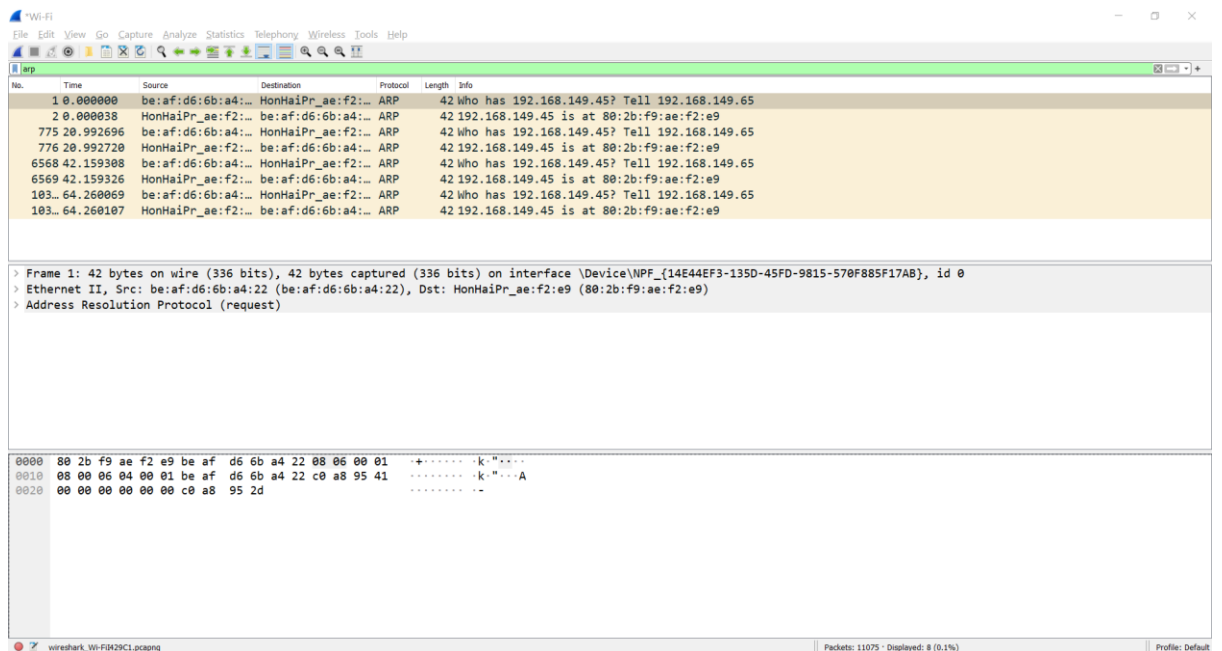
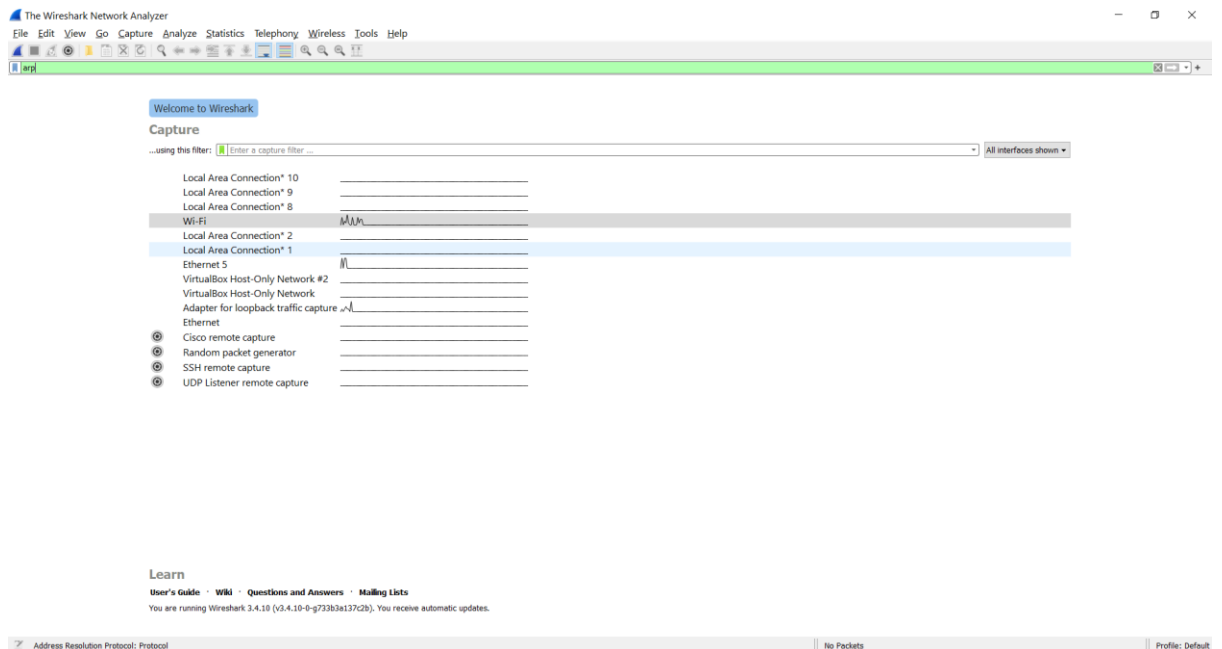
Learn

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.



arp



icmp
The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Welcome to Wireshark

Capture

...using this 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-g723b3a1372b). You receive automatic updates.

Internet Control Message Protocol: Protocol

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
460	62.232240	192.168.149.45	192.168.149.65	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 461)
461	62.235636	192.168.149.65	192.168.149.45	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=64 (request in 460)
462	63.237975	192.168.149.45	192.168.149.65	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 463)
463	63.240901	192.168.149.65	192.168.149.45	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=64 (request in 462)
468	64.253105	192.168.149.45	192.168.149.65	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 469)
469	64.257999	192.168.149.65	192.168.149.45	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 468)
472	65.268069	192.168.149.45	192.168.149.65	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 473)
473	65.271992	192.168.149.65	192.168.149.45	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 472)

> Frame 460: 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 ...k-+-----E:
0010 00 3c 4b e6 00 00 80 01 43 1b c0 a8 95 2d c0 a8 -<K-----C-----
0020 95 41 08 00 4d 4e 00 01 00 0d 61 62 63 64 65 66 -A-MN-- -abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Wi-Fi: <live capture in progress> Packets: 497 · Displayed: 8 (1.6%) Profile: Default

3. Receive the packets which belongs to HTTP

http
The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Welcome to Wireshark

Capture

...using this 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
Npcap Loopback Adapter
Adapter for loopback traffic capture
Ethernet

Learn

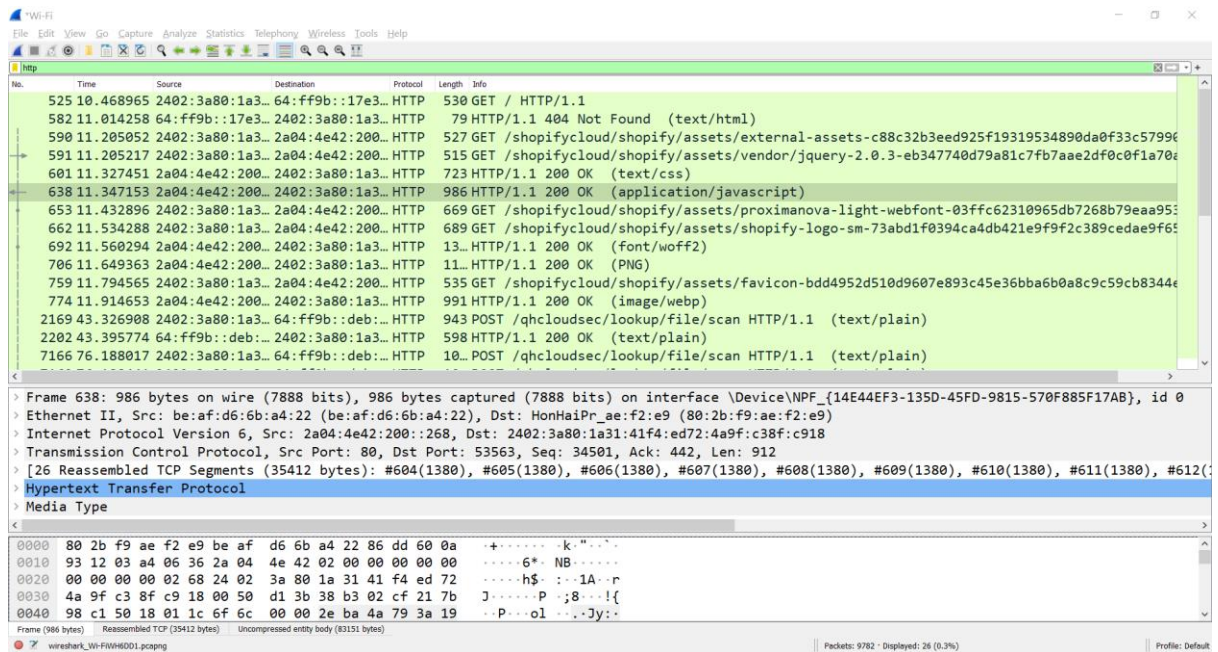
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.4.10 (v3.4.10-0-g723b3a1372b). You receive automatic updates.

HyperText Transfer Protocol: Protocol

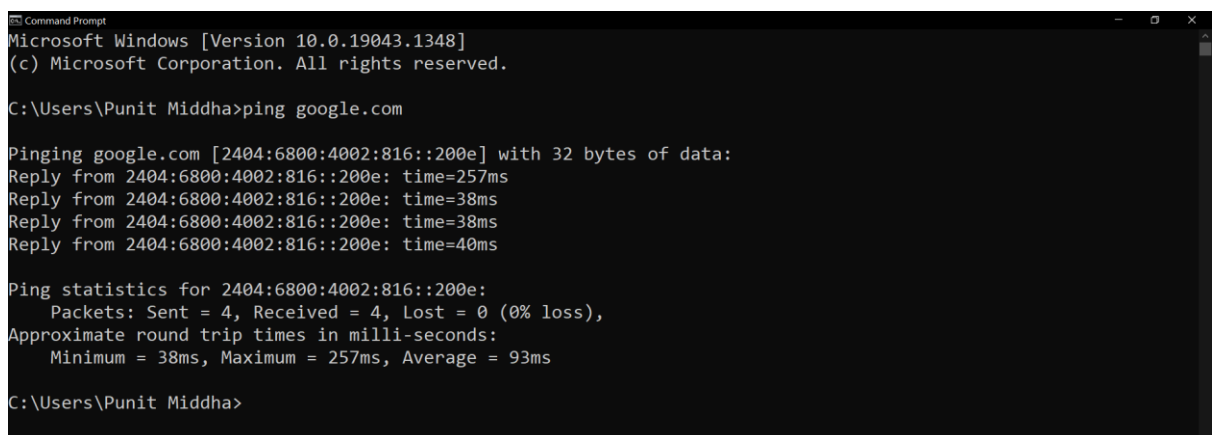
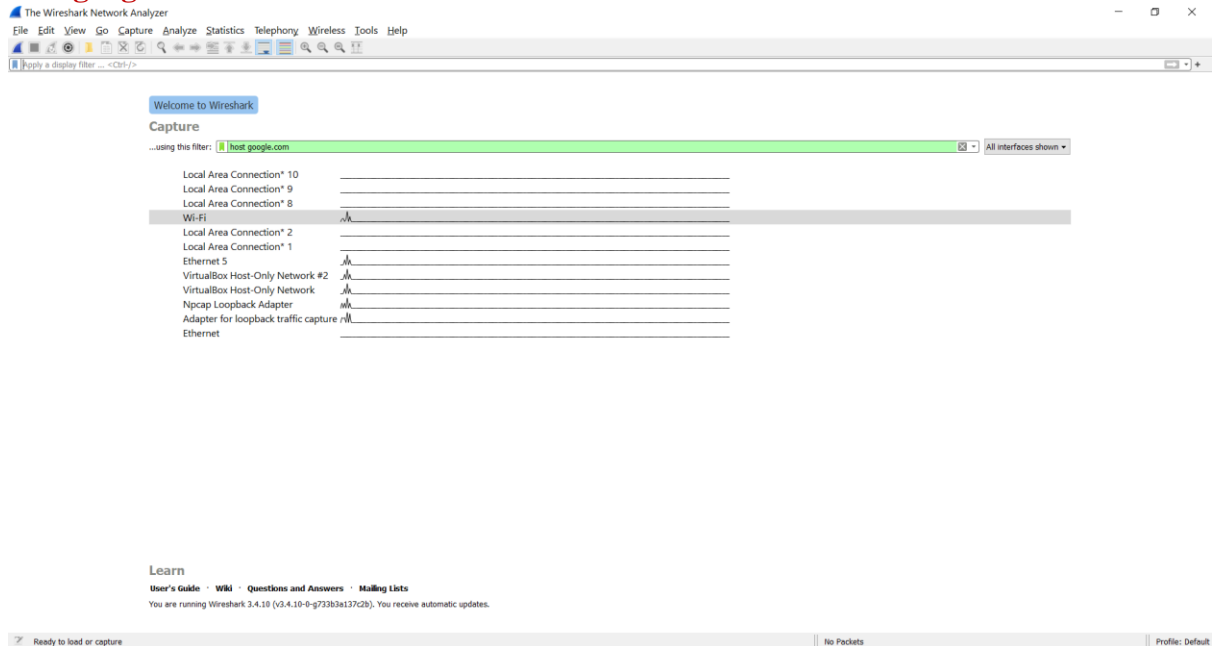
No Packets

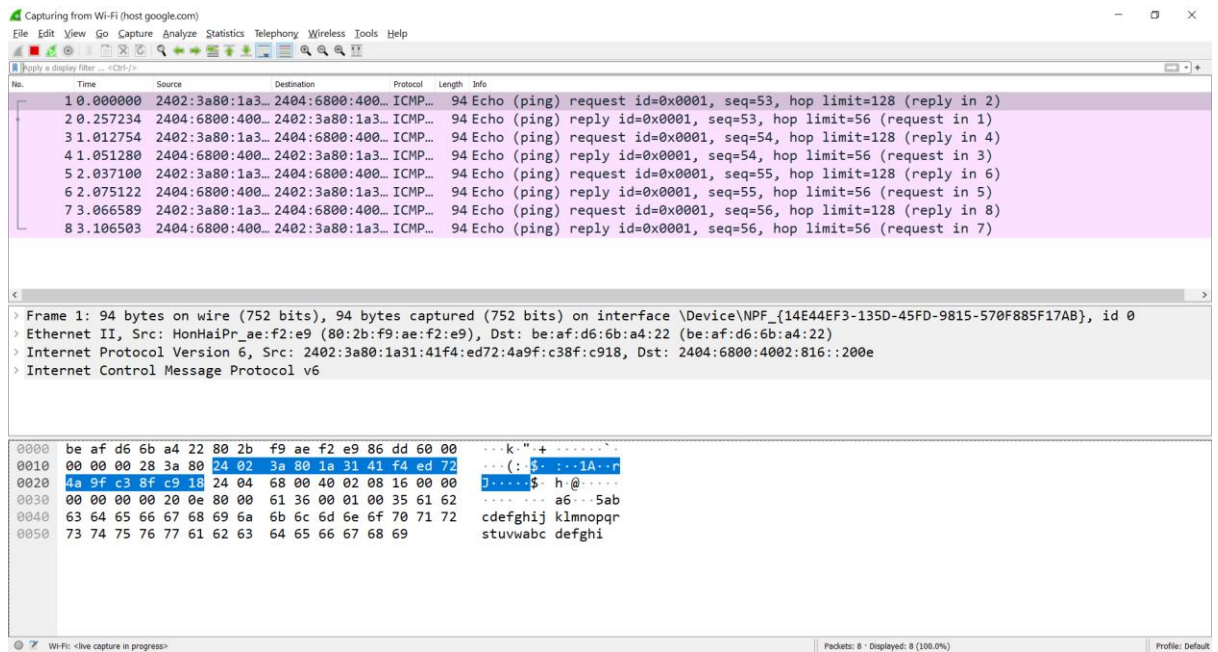
Profile: Default



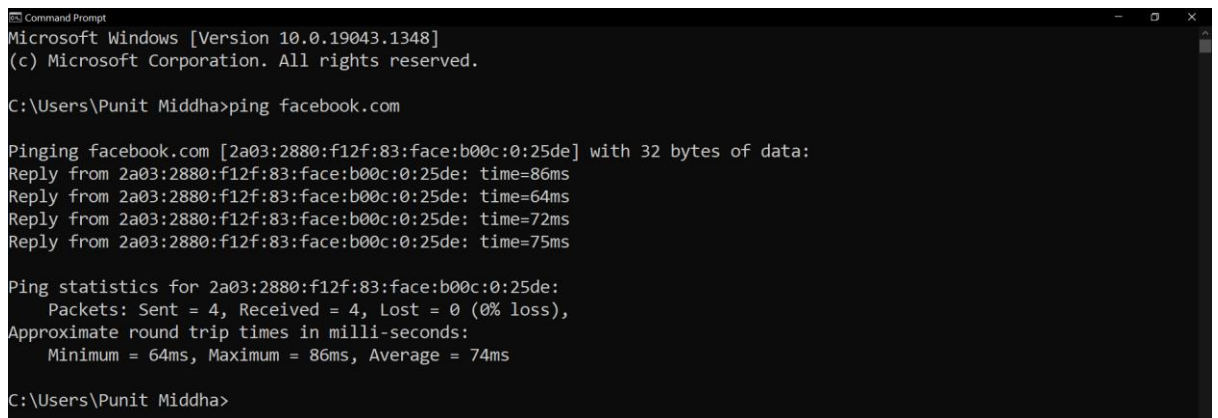
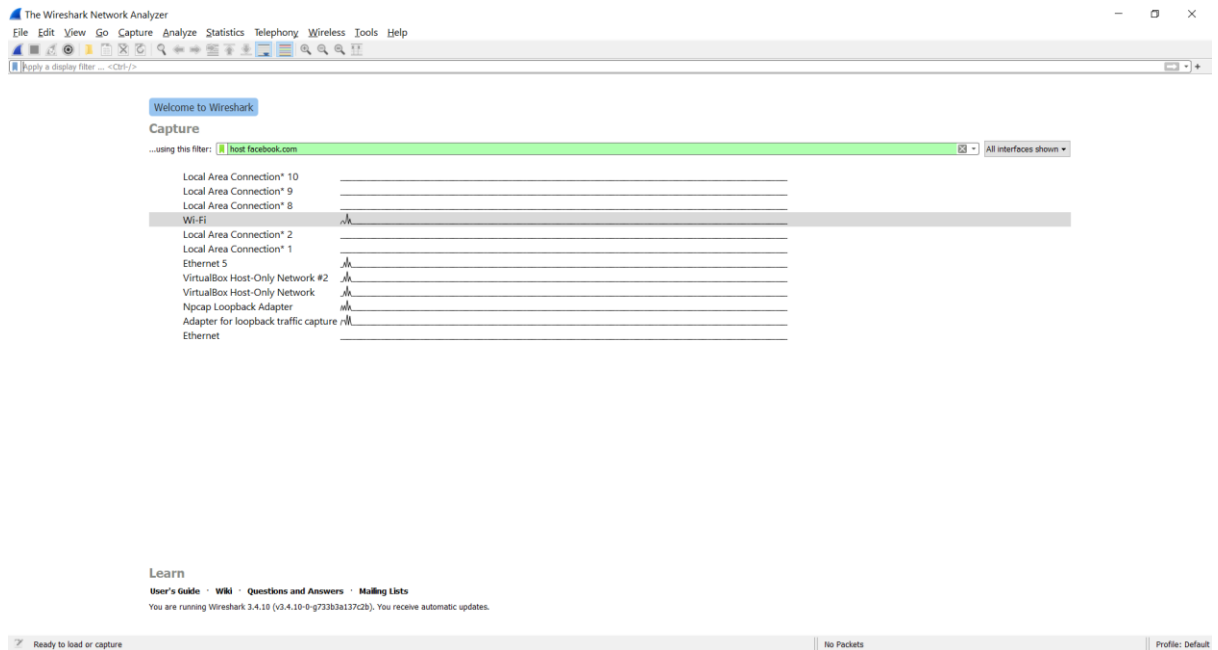
4. Apply a filter which is able to capture the packets from a particular website

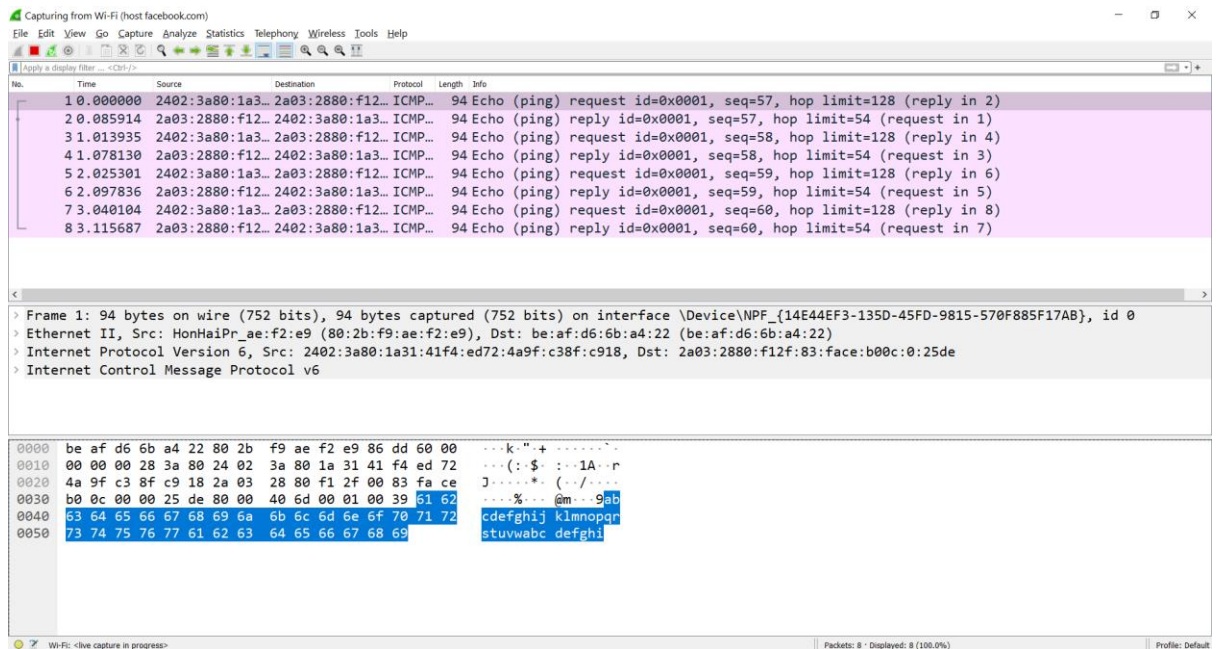
host google.com



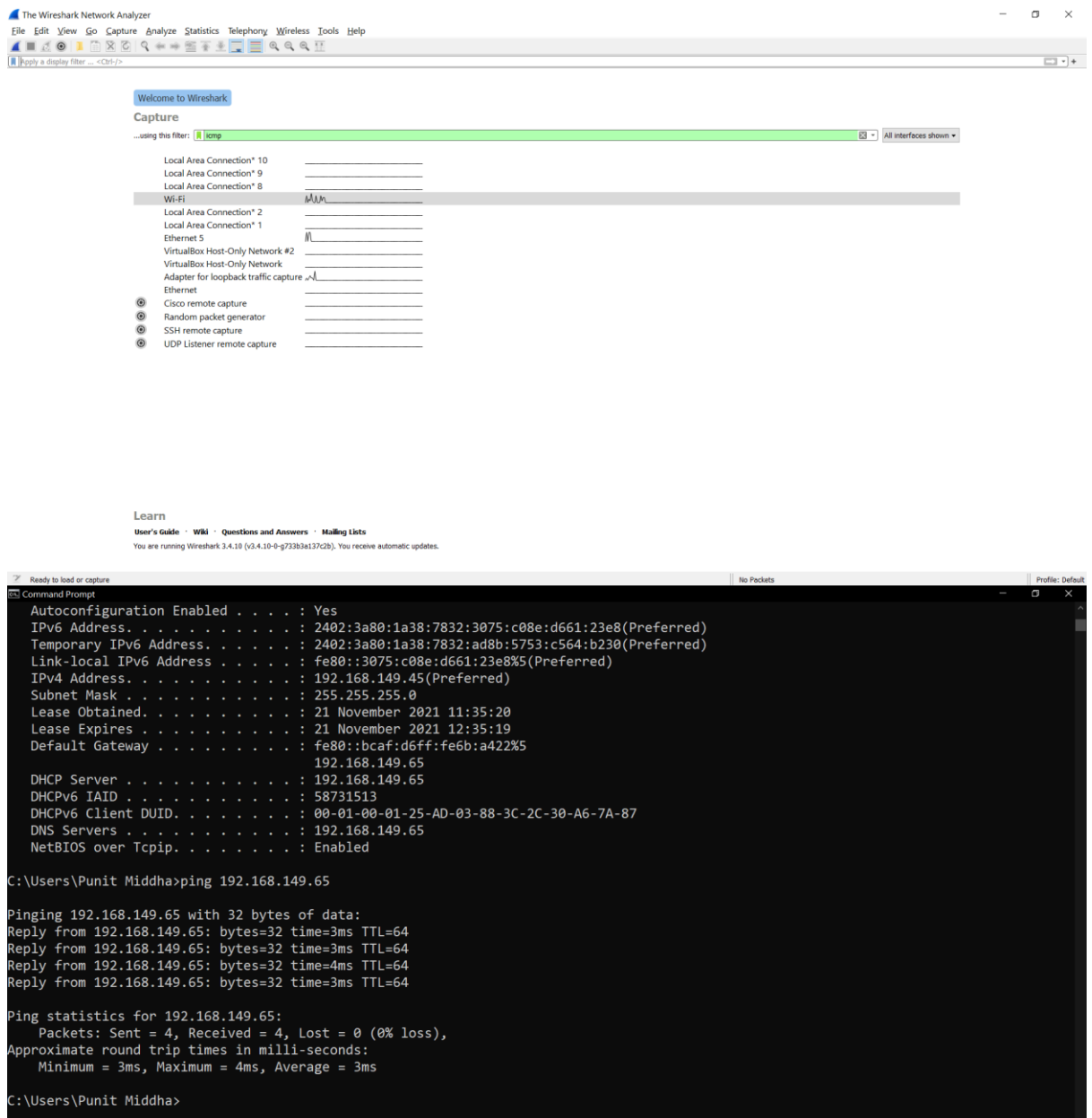


host facebook.com





5. Receive the packets which belongs to icmp



Capturing from Wi-Fi (icmp)

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

Apply a display filter ... <Ctrl-F>

No.

Time

Source

Destination

Protocol

Length

Info

10.000000

192.168.149.45

192.168.149.65

ICMP

74

Echo (ping) request

id=0x0001, seq=5/1280, ttl=128 (reply in 2)

20.003877

192.168.149.65

192.168.149.45

ICMP

74

Echo (ping) reply

id=0x0001, seq=5/1280, ttl=64 (request in 1)

31.008049

192.168.149.45

192.168.149.65

ICMP

74

Echo (ping) request

id=0x0001, seq=6/1536, ttl=128 (reply in 4)

41.011193

192.168.149.65

192.168.149.45

ICMP

74

Echo (ping) reply

id=0x0001, seq=6/1536, ttl=64 (request in 3)

52.022318

192.168.149.45

192.168.149.65

ICMP

74

Echo (ping) request

id=0x0001, seq=7/1792, ttl=128 (reply in 6)

62.025771

192.168.149.65

192.168.149.45

ICMP

74

Echo (ping) reply

id=0x0001, seq=7/1792, ttl=64 (request in 5)

73.035232

192.168.149.45

192.168.149.65

ICMP

74

Echo (ping) request

id=0x0001, seq=8/2048, ttl=128 (reply in 8)

83.039813

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

0000be af d6 6b a4 22 80 2b f9 ae f2 e9 08 00 45 00...k...+.....E:

001000 3c 4b 55 00 00 80 01 43 ac c0 a8 95 2d c0 a8...<KU....C.....

002095 41 08 00 4d 56 00 01 00 05 61 62 63 64 65 66...A..MV...abcdef

003067 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76...ghijklmn opqrstuv

004077 61 62 63 64 65 66 67 68 69...wabcdefg hij

Wi-Fi -<live capture in progress>

Packets: 8 · Displayed: 8 (100.0%)

Profile: Default