

Mawlana Bhashani Science and Technology University



Lab-Report

Report No: 04

Course code: ICT-4202

Course title: Wireless and Mobile Communication Lab

Date of Performance: 11.09.2020

Date of Submission: 18.09.2020

Submitted by

Name: Md Amanullah Rafi

ID:IT-16020

4th year 2nd semester

Session: 2015-2016

Dept. of ICT

MBSTU.

Submitted To

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

Experiment No: 04

Experiment Name: Protocol Analysis with Wireshark

Objectives:

In this Lab, We can learn to capture live packet data from a network interface, Display packets with very detailed protocol information, Filter packets on many criteria, Search for packets on many criteria, Colorize packet display based on filters, Create various statistics.

Capturing Packets:

By clicking Capture menu the process of capturing will be started. It will show the available interfaces list. Then, we need to start Capturing on interface that has IP address

The packet capture will display the details of each packet as they were transmitted over the wireless LAN.

Capturing can be stopped by clicking on Stop the running capture button on the main toolbar.

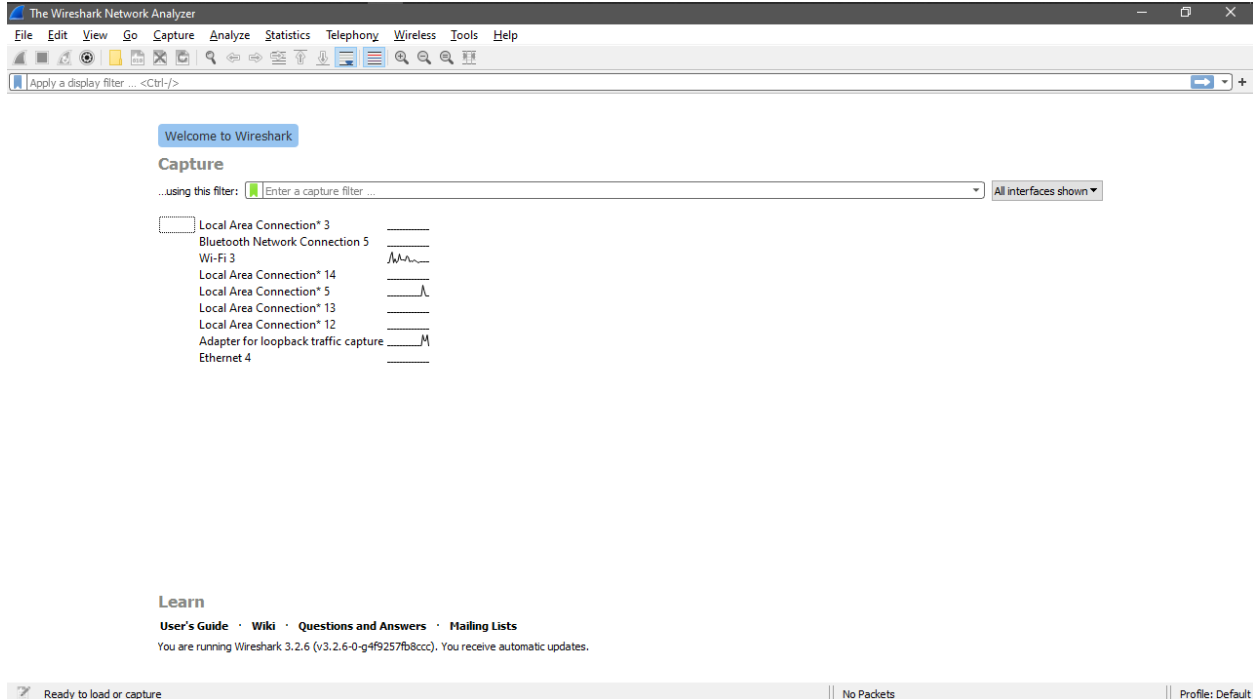


Figure 01: Wireshark Interface List

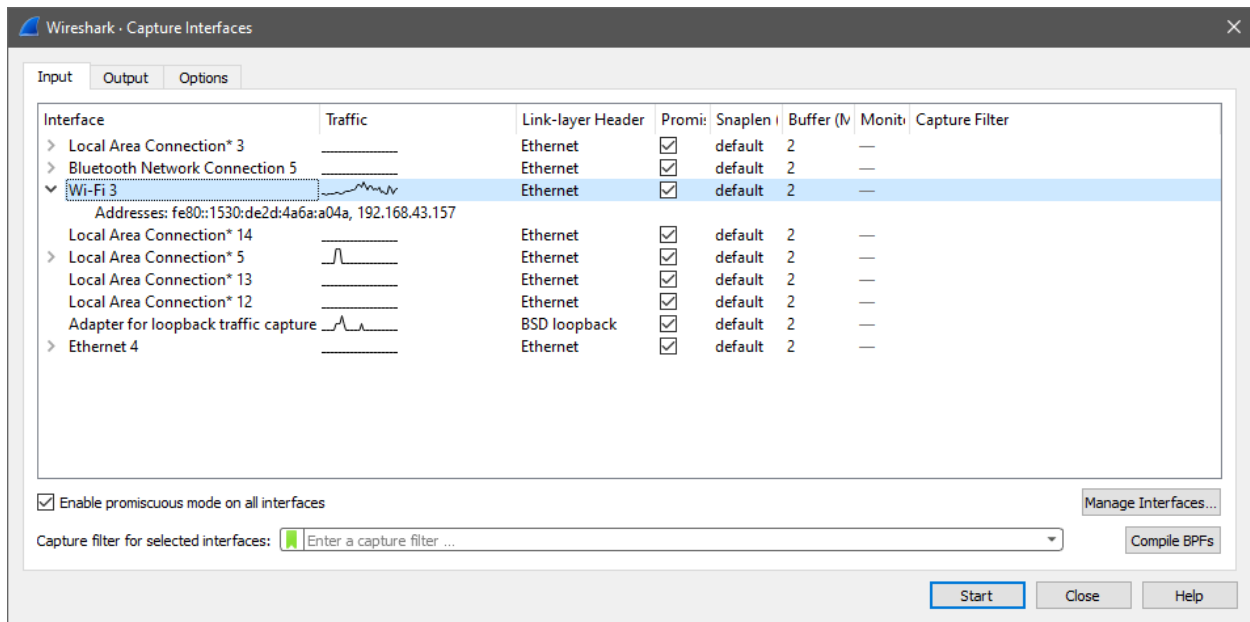


Figure 02: Start Capturing Interface that has IP address

Packet list pane

Packet details pane

Packet bytes pane

Capturing from Wi-Fi 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
213	16.793558	192.168.43.157	184.26.84.23	TCP	66	[TCP Dup ACK 205#4] 49787 → 443 [ACK] Seq=1 Ack=142801 Win=514 Len=0 SLE=144201 SRE=149801
214	16.886837	184.26.84.23	192.168.43.157	TCP	1454	[TCP Retransmission] 443 → 49787 [ACK] Seq=142801 Ack=1 Win=245 Len=1400
215	16.886882	192.168.43.157	184.26.84.23	TCP	54	49787 → 443 [ACK] Seq=1 Ack=149801 Win=514 Len=0
216	17.605692	184.26.84.23	192.168.43.157	SSL	1454	[TCP Previous segment not captured] , Continuation Data
217	17.605747	192.168.43.157	184.26.84.23	TCP	66	[TCP Dup ACK 215#1] 49787 → 443 [ACK] Seq=1 Ack=149801 Win=514 Len=0 SLE=152601 SRE=154001
218	17.605807	184.26.84.23	192.168.43.157	SSL	1454	Continuation Data
219	17.605927	192.168.43.157	184.26.84.23	TCP	66	[TCP Dup ACK 215#2] 49787 → 443 [ACK] Seq=1 Ack=149801 Win=514 Len=0 SLE=152601 SRE=155401
220	17.605861	184.26.84.23	192.168.43.157	SSL	1454	Continuation Data
221	17.605884	192.168.43.157	184.26.84.23	TCP	66	[TCP Dup ACK 215#3] 49787 → 443 [ACK] Seq=1 Ack=149801 Win=514 Len=0 SLE=152601 SRE=156801
222	18.007790	184.26.84.23	192.168.43.157	SSL	1454	[TCP Previous segment not captured] , Continuation Data

> Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface \Device\NPF_{CC0F8893-E998-4143-82B1-D5A131FB6E03}, id 0

> Ethernet II, Src: XiaomiCo_aa:a2:d4 (48:2c:a0:aa:a2:d4), Dst: 7a:b8:b7:7d:52:24 (7a:b8:b7:7d:52:24)

> Internet Protocol Version 4, Src: 184.26.84.23, Dst: 192.168.43.157

> Transmission Control Protocol, Src Port: 443, Dst Port: 49787, Seq: 1, Ack: 1, Len: 1400

Transport Layer Security

0000 7a b8 b7 7d 52 24 48 2c a0 aa a2 d4 08 00 45 00 z...}RSH,E-
0010 05 a0 8f 9e 40 00 34 06 b9 42 b8 1a 54 17 c0 a8 ...@.4. .B...T...
0020 2b 9d 01 bb c2 7b 11 08 e7 0d 04 3a 5f 44 50 10 +...{..._DP...
0030 00 f5 54 c3 08 00 f1 c2 c9 1e 37 2b a0 c8 0d ac -T...-7+...
0040 44 0a 13 91 92 48 35 92 cd 24 24 24 d5 45 3f 39 D...H5...\$\$.E?9
0050 52 bb 22 27 6b b2 3d 5a 08 fb f1 6a 30 b4 e4 47 R...k=-Z...j0...G
0060 8f c8 80 9f a9 89 64 66 28 5b 4b 76 91 cc 53 90df ([Kv...S
0070 e6 18 16 59 01 c3 20 b1 d9 de 99 a9 2c 42 9a 3eY... ..B...>
0080 f2 d3 e4 77 72 8e 76 09 6e 23 0b e5 58 64 37 d9 ...w-v...n#...Xd7
0090 96 1f 33 c2 d7 fc f4 e8 46 c7 ff 05 e3 b2 47 b8 -3... ..F... ..G
00a0 9b 0a 2d 94 86 1d 0d 01 2e 07 14 5f f4 c6 95 ae
00b0 ba fd 0b b2 94 3c 95 a5 29 9b b2 11 45 94 fa 51<... ..E...Q
00c0 8f fc 46 99 c5 9d fb 69 b3 71 37 df 25 a4 fe 09i...q7...%

Wi-Fi 3: <live capture in progress>

Packets: 222 · Displayed: 222 (100.0%)

Profile: Default

Figure 03: A sample packet capture window

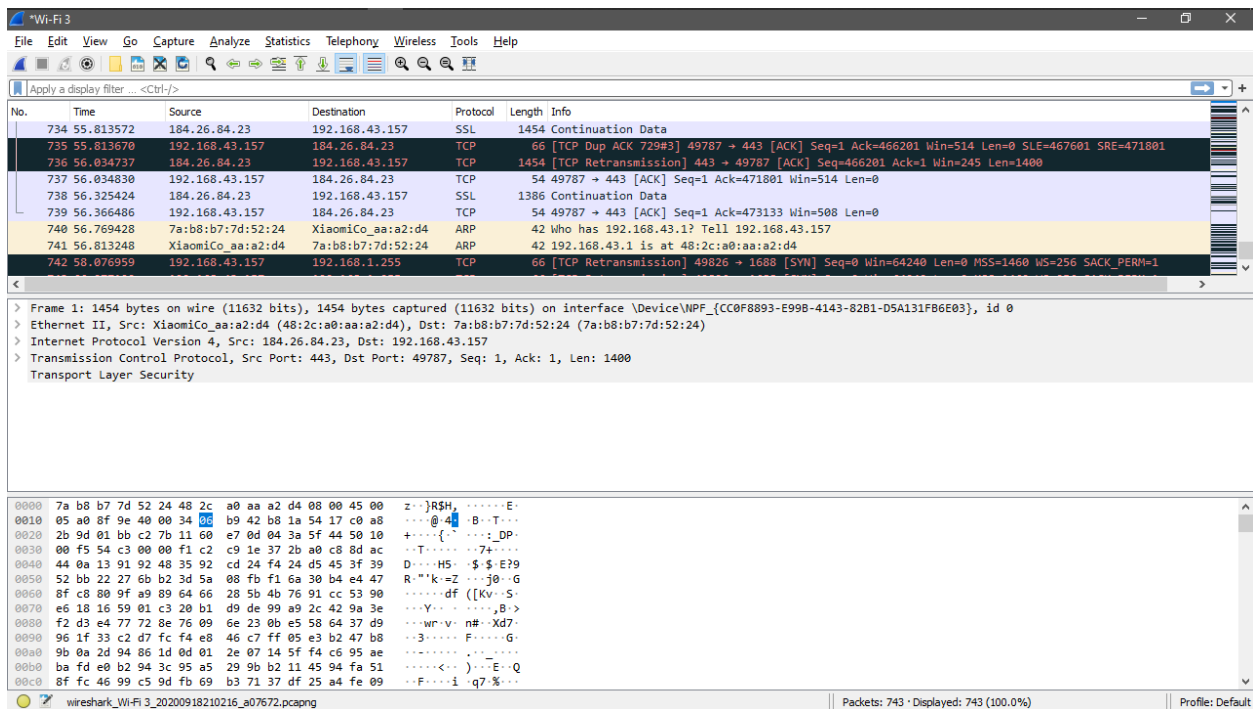


Figure 04: Stopping Capture

Filtering:

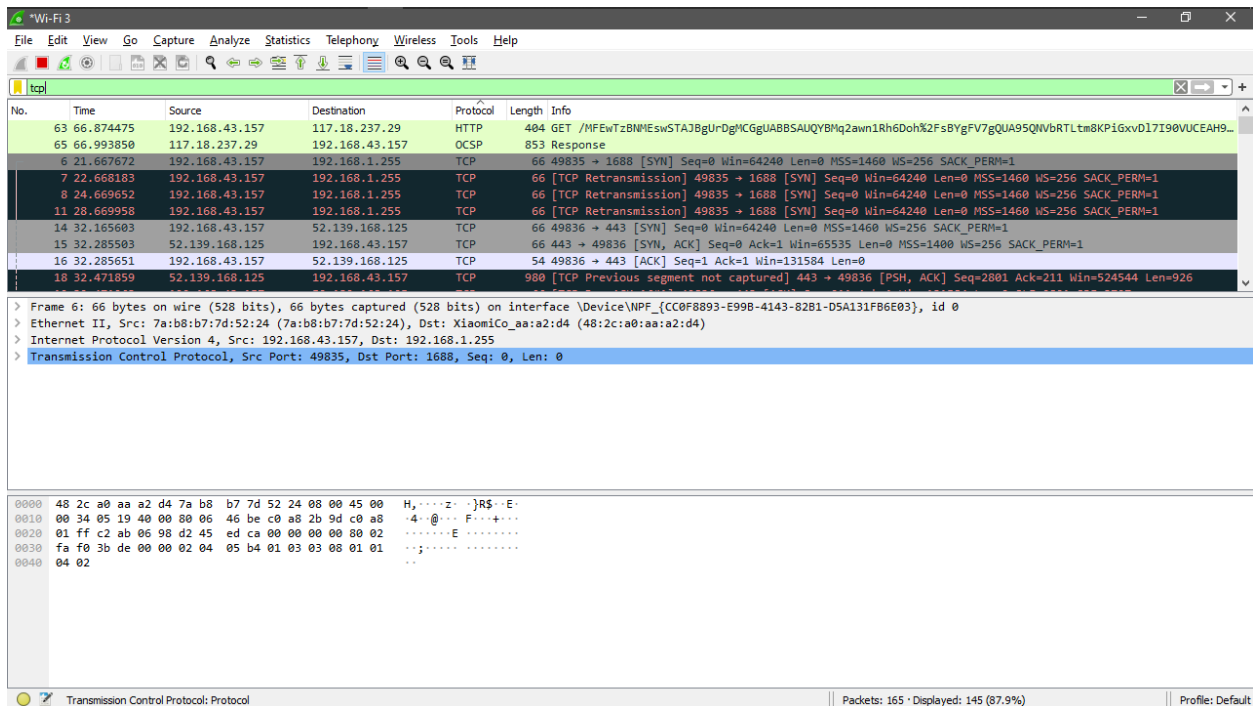


Figure 05: Filter by Protocol

A source filter can be applied to restrict the packet view in wireshark to only those packets that

have source IP as mentioned in the filter.

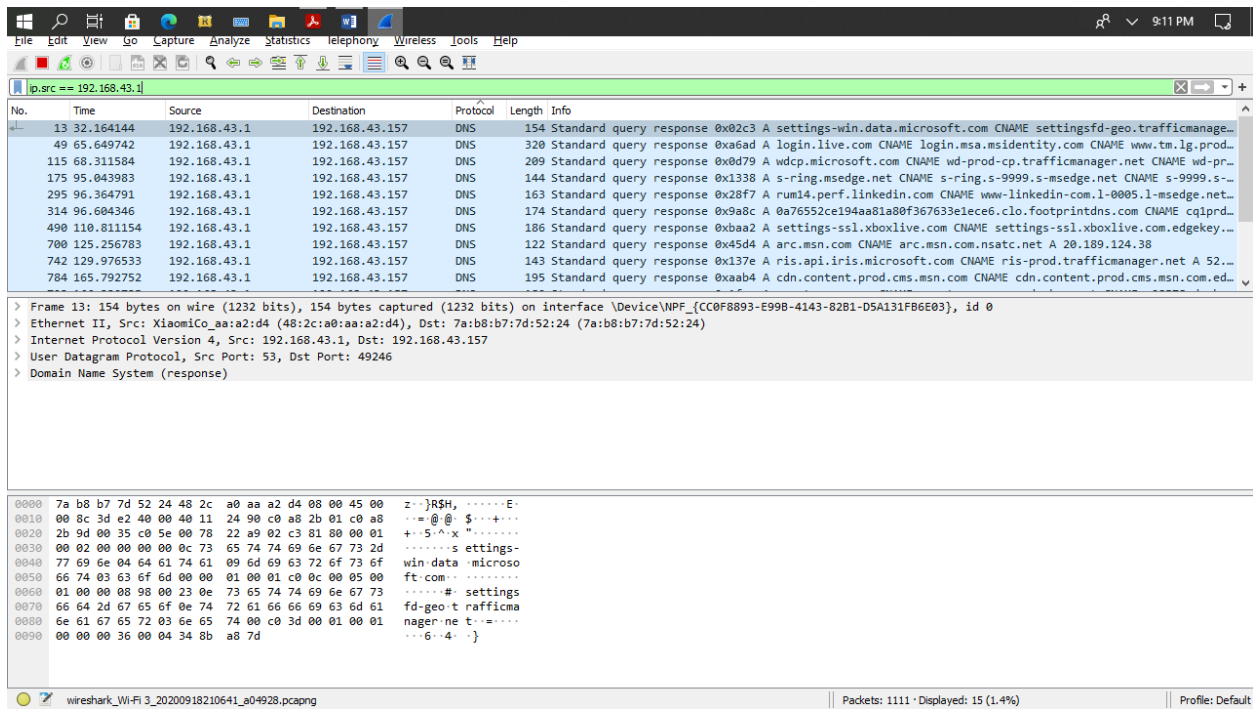


Figure 06: Source IP filter

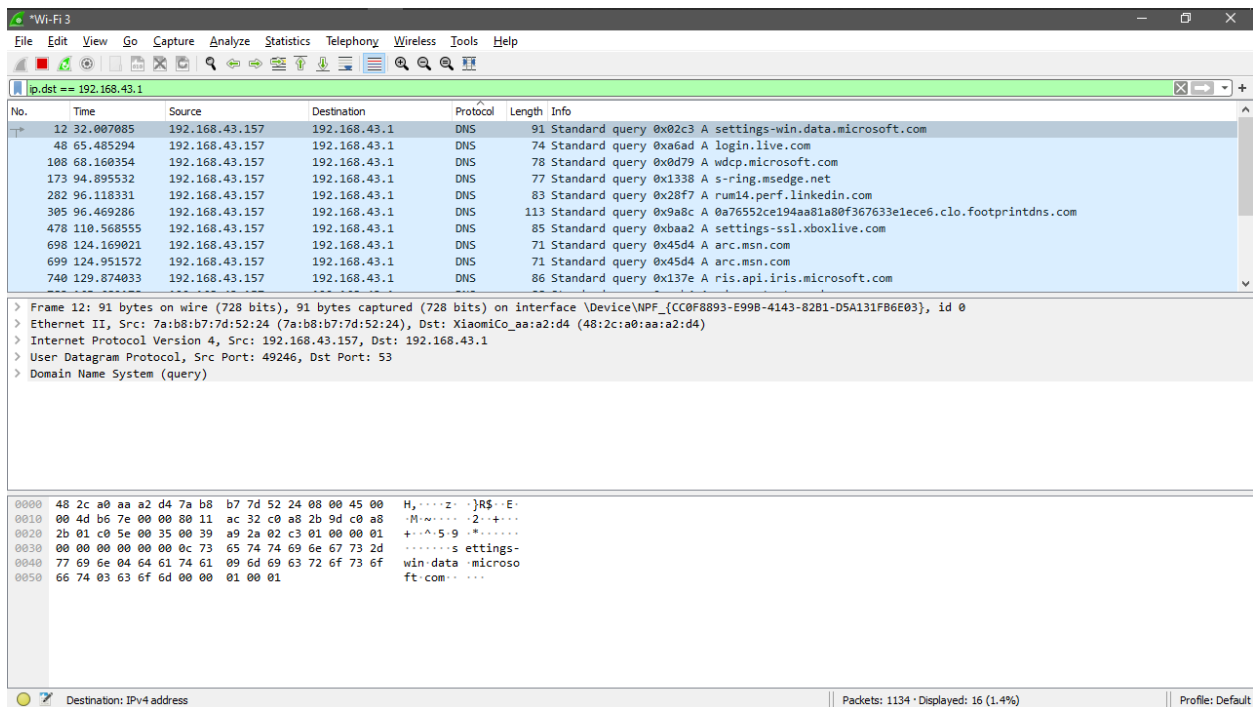


Figure 07: Destination IP filter

- Packets and protocols can be analyzed after capture

-
- Wireshark capture of an ICMP Echo (ping) request. The packet list shows a single packet of 91 bytes. The packet details pane shows Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane shows the raw data in hexadecimal and ASCII.
- | No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|--------------|----------|--------|---|
| 1 | 0.000000 | 192.168.43.157 | 192.168.43.1 | ICMP | 91 | Standard query 0x521a settings.win.data.microsoft.com |
- Frame 12: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF{CC0F8893-E998-4143-82B1-D5A131F86E03}, id 0
- Ethernet II, Src: 7a:b8:b7:7d:52:24 (7a:b8:b7:7d:52:24), Dst: XiaomiCo_aa:a2:d4 (48:2c:a0:aa:a2:d4)
- Internet Protocol Version 4, Src: 192.168.43.157, Dst: 192.168.43.1
- User Datagram Protocol, Src Port: 49246, Dst Port: 53
- Domain Name System (query)
- ```

0000 48 2c a0 aa a2 d4 7a b8 b7 7d 52 24 08 00 45 00 H,....z...}R$...E-
0010 00 4d b6 7e 00 00 80 11 ac 32 c0 a8 2b 9d c0 a8 M.....2....+...
0020 2b 01 c0 5e 00 35 00 39 a9 2a 02 c3 01 00 00 01 +...^5.9.....
0030 00 00 00 00 00 00 0c 73 65 74 74 69 6e 67 73 2d ettings...
0040 77 69 6e 04 64 61 74 61 09 6d 69 63 72 6f 73 6f win.data.microsoft
0050 66 74 03 63 6f 6d 00 00 01 00 01 ft.com...

```

The image shows a Wireshark packet capture analysis of a DNS query. The top pane displays the packet list, showing a single packet (Frame 12) of 91 bytes on the wire, captured on interface \Device\NPF\_{CC0F8893-E99B-4143-82B1-D5A131FB6E03}. The packet is an Ethernet II frame from 7a:b8:b7:d5:24 to 7a:b8:b7:d5:24, encapsulating an Internet Protocol Version 4 packet from 192.168.43.157 to 192.168.43.1, which is a User Datagram Protocol (UDP) packet from port 49246 to port 53, and finally a Domain Name System (query) packet.

The middle pane shows the packet details, highlighting the Ethernet II, Internet Protocol Version 4, and User Datagram Protocol layers. The bottom pane displays the raw packet data in hexadecimal and ASCII. The ASCII column shows the query for 'settings-win-data.microsoft.com'.

| No. | Time     | Source         | Destination  | Protocol | Length | Info                                                      |
|-----|----------|----------------|--------------|----------|--------|-----------------------------------------------------------|
| 12  | 0.000000 | 192.168.43.157 | 192.168.43.1 | HTTP     | 91     | Standard query 0x00000000 settings-win-data.microsoft.com |

Frame 12: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF\_{CC0F8893-E99B-4143-82B1-D5A131FB6E03}, id 0

Ethernet II, Src: 7a:b8:b7:d5:24 (7a:b8:b7:d5:24), Dst: XiaomiCo\_aa:a2:d4 (48:2c:a0:aa:a2:d4)

Internet Protocol Version 4, Src: 192.168.43.157, Dst: 192.168.43.1

User Datagram Protocol, Src Port: 49246, Dst Port: 53

Domain Name System (query)

```

0000 48 2c a0 aa a2 d4 7a b8 b7 d5 24 00 00 45 00 H,....E..S..E..
0010 00 4d b5 7e 00 00 11 8c 32 c0 a6 2b 9d c0 a6 R.....2+....
0020 2b 01 c0 5e 00 35 00 39 a9 2a 02 c3 01 00 00 01 +...5.9*.....
0030 00 00 00 00 00 00 0c 73 65 74 7a 69 6e 67 73 2d ettings-
0040 77 69 6e 04 64 61 74 61 09 6d 69 63 72 6f 73 6f win_data_microso
0050 66 74 03 63 6f 6d 00 00 01 00 01 ft.com...

```

Wireshark - Wi-Fi 3\_20200918210641\_a04928.pcapng

Packets: 1157 · Displayed: 1157 (100.0%)

Profile: Default

### Figure 09: Packet Details Pane (Ethernet Segment)

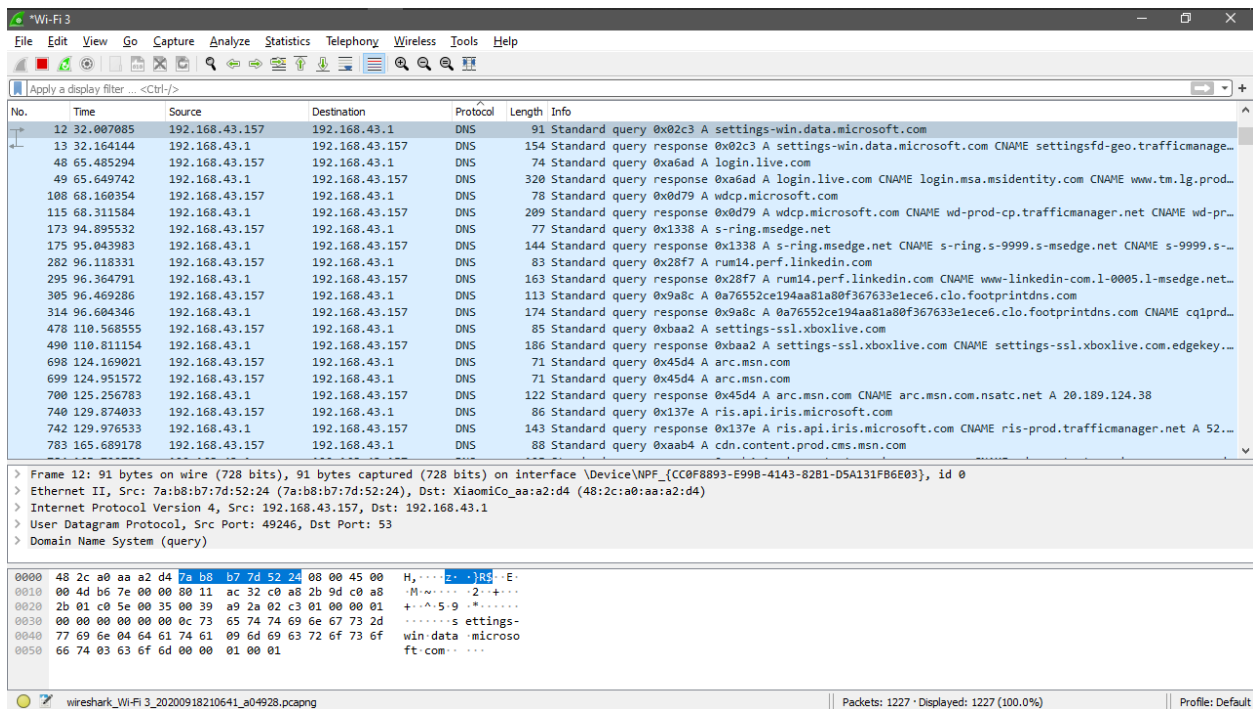


Figure 10: Packet Details Pane(IP segment)

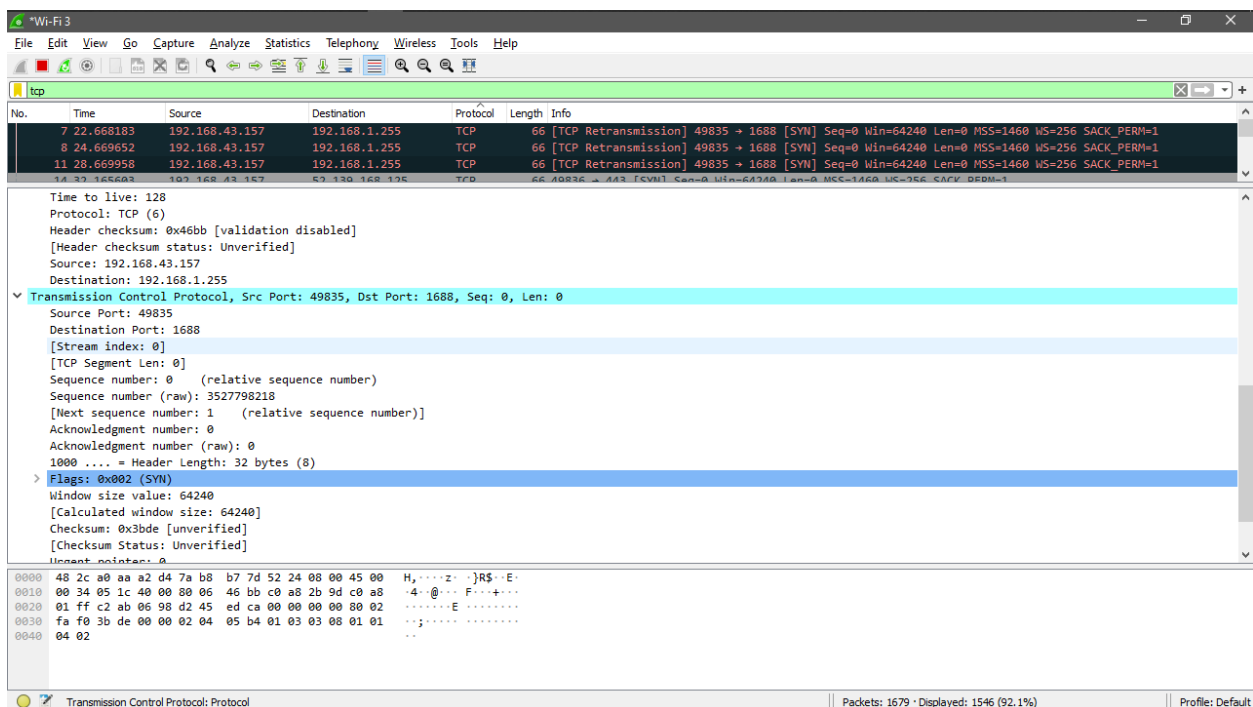


Figure 11: Packet Details Pane (TCP Segment)

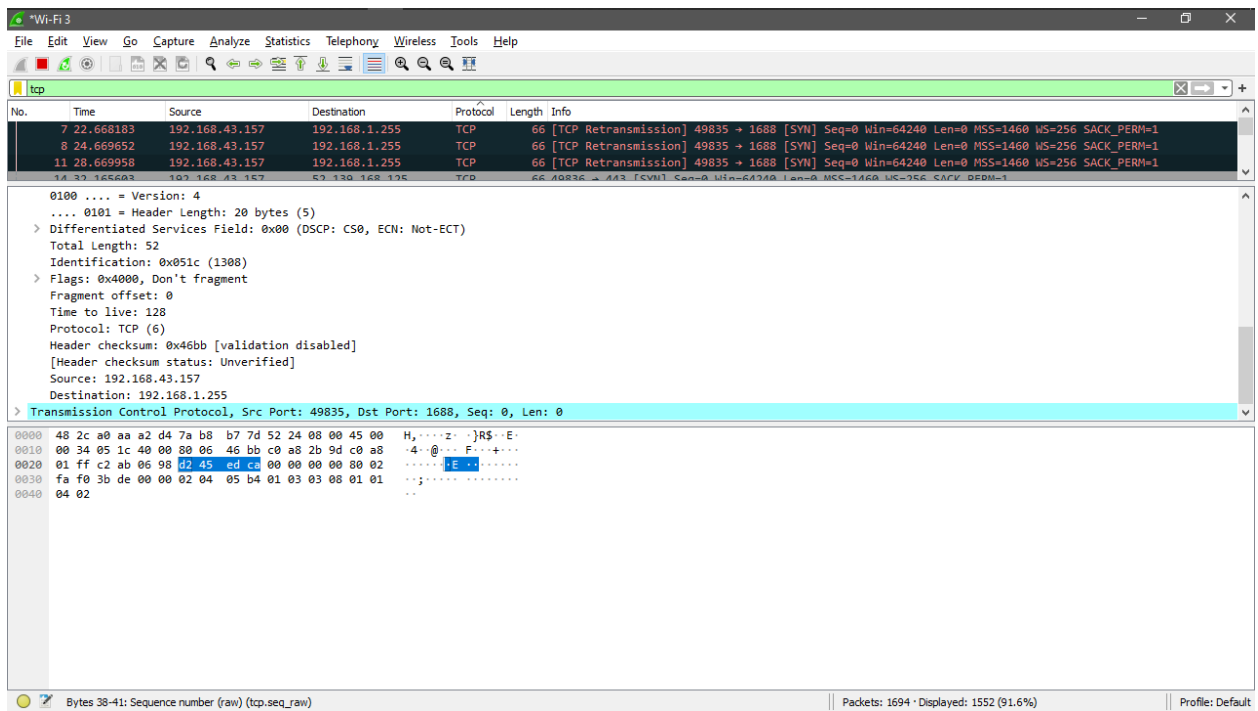


Figure 12: Packet Byte Pane

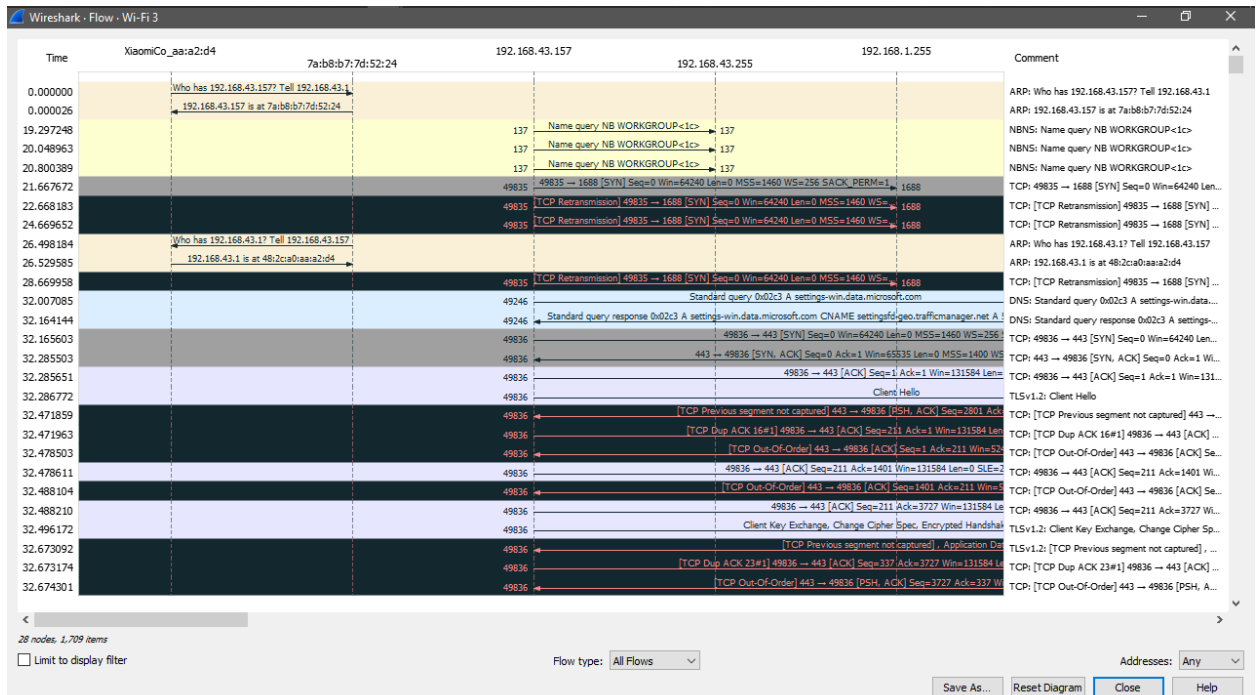


Figure 13: Statistics- Flow Graph (All Flows)





**Figure 13: Statistics- Flow Graph (TCP Flows)**

## **Conclusion:**

Using Wireshark , It makes ease to Capture live packet data from a network interface. Here, We have applied filter to monitor particular traffic like source IP and destination IP. The TCP Flow Throughput graph gives the throughput from one TCP stream, in one direction, based on our selected packet.