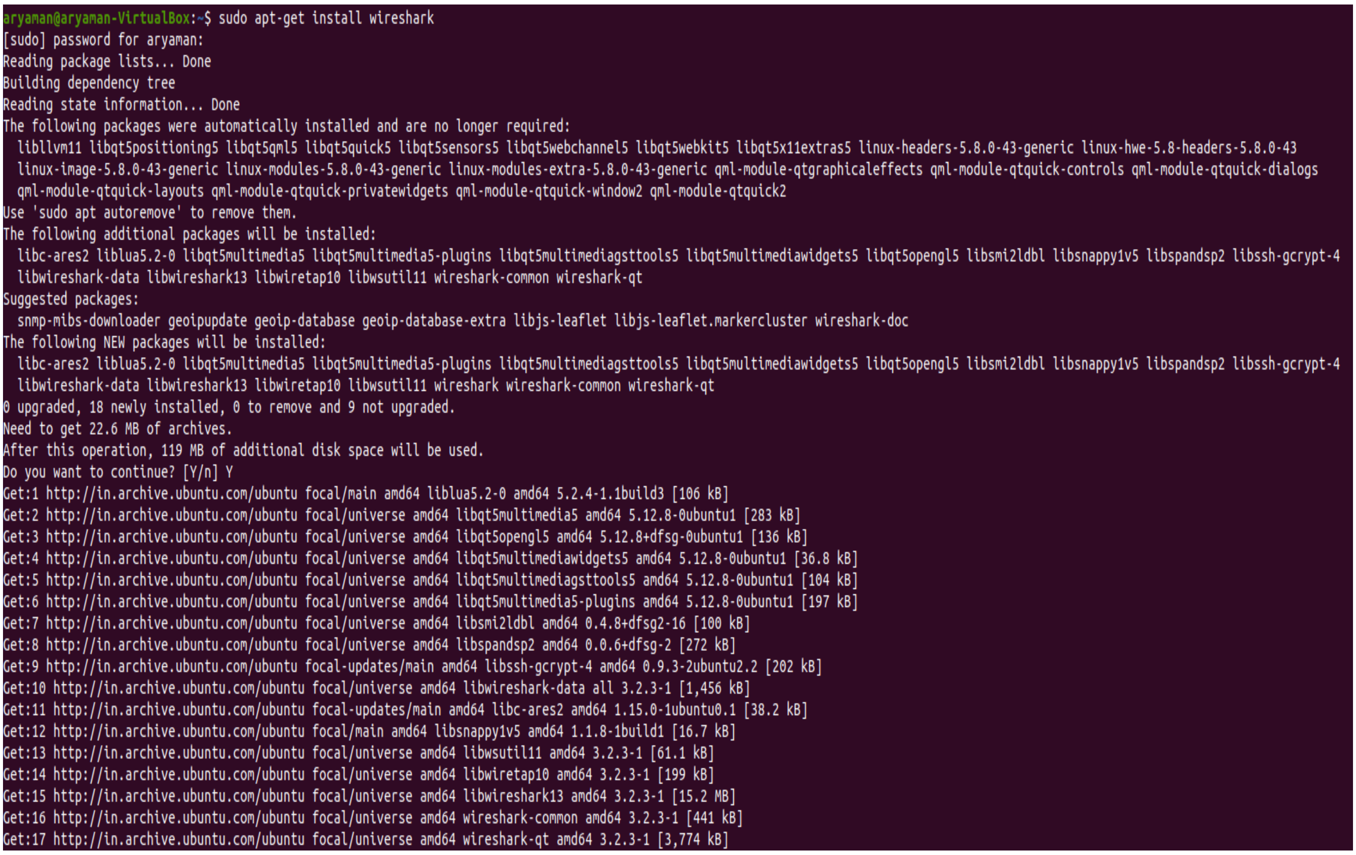
ARYAMAN MISHRA

19BCE1027

LAB 3

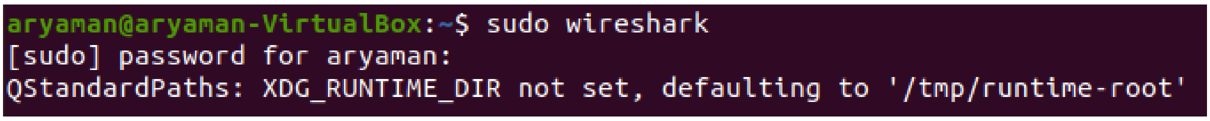
INSTALLATION GUIDE FOR LINUX OS

I'll be using Wireshark to monitor incoming traffic in networks and we will use sudo to download it via terminal.



```
aryaman@aryaman-VirtualBox:~$ sudo apt-get install wireshark
[sudo] password for aryaman:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libllvm11 libqt5positioning5 libqt5qml5 libqt5quick5 libqt5sensors5 libqt5webchannel5 libqt5webkit5 libqt5x11extras5 linux-headers-5.8.0-43-generic linux-hwe-5.8-headers-5.8.0-43
  linux-image-5.8.0-43-generic linux-modules-5.8.0-43-generic linux-modules-extra-5.8.0-43-generic qml-module-qtgraphicaleffects qml-module-qtquick-controls qml-module-qtquick-dialogs
  qml-module-qtquick-layouts qml-module-qtquick-privatewidgets qml-module-qtquick-window2 qml-module-qtquick2
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libc-ares2 liblua5.2-0 libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5opengl5 libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4
  libwireshark-data libwireshark13 libwiretap10 libwsutil11 wireshark-common wireshark-qt
Suggested packages:
  snmp-mibs-downloader geoipupdate geoip-database geoip-database-extra libjs-leaflet libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
  libc-ares2 liblua5.2-0 libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5opengl5 libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4
  libwireshark-data libwireshark13 libwiretap10 libwsutil11 wireshark wireshark-common wireshark-qt
0 upgraded, 18 newly installed, 0 to remove and 9 not upgraded.
Need to get 22.6 MB of archives.
After this operation, 119 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 liblua5.2-0 amd64 5.2.4-1.1build3 [106 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5multimedia5 amd64 5.12.8-0ubuntu1 [283 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5opengl5 amd64 5.12.8+dfsg-0ubuntu1 [136 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5multimediawidgets5 amd64 5.12.8-0ubuntu1 [36.8 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5multimediagsttools5 amd64 5.12.8-0ubuntu1 [104 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libqt5multimedia5-plugins amd64 5.12.8-0ubuntu1 [197 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libsmi2ldbl amd64 0.4.8+dfsg2-16 [100 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libspandsp2 amd64 0.0.6+dfsg-2 [272 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 libssh-gcrypt-4 amd64 0.9.3-2ubuntu2.2 [202 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libwireshark-data all 3.2.3-1 [1,456 kB]
Get:11 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 libc-ares2 amd64 1.15.0-1ubuntu0.1 [38.2 kB]
Get:12 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libsnappy1v5 amd64 1.1.8-1build1 [16.7 kB]
Get:13 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libwsutil11 amd64 3.2.3-1 [61.1 kB]
Get:14 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libwiretap10 amd64 3.2.3-1 [199 kB]
Get:15 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libwireshark13 amd64 3.2.3-1 [15.2 MB]
Get:16 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 wireshark-common amd64 3.2.3-1 [441 kB]
Get:17 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 wireshark-qt amd64 3.2.3-1 [3,774 kB]
```

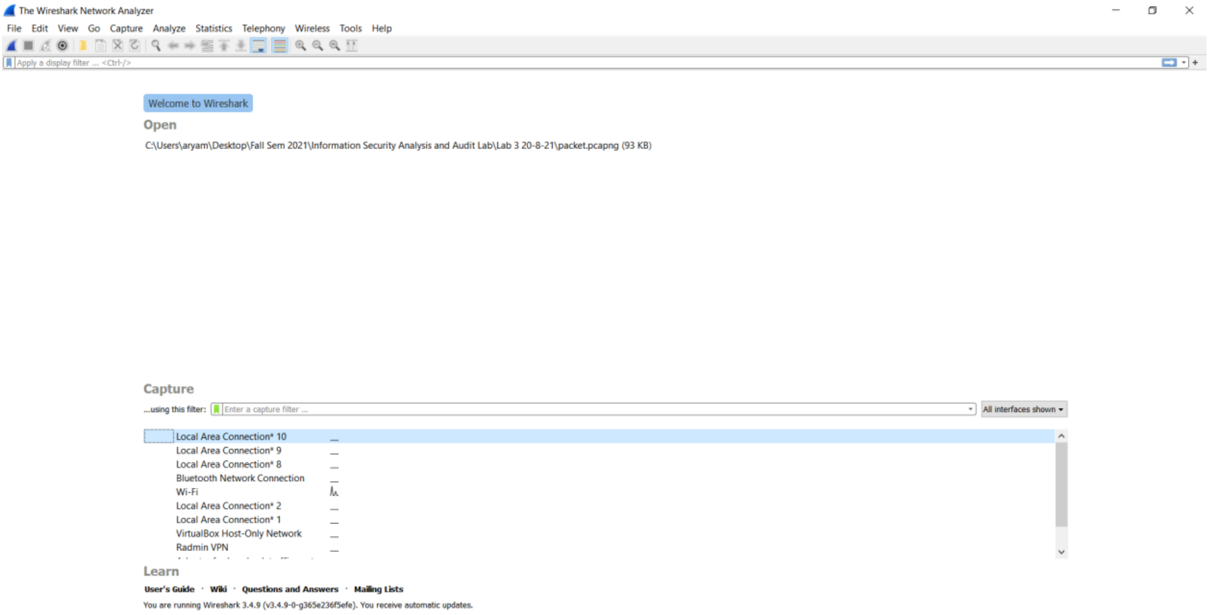
We will then launch Wireshark:



```
aryaman@aryaman-VirtualBox:~$ sudo wireshark
[sudo] password for aryaman:
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

FUNCTIONALITIES:

1)Launch Wireshark


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark

Open

C:\Users\aryam\Desktop\Fall Sem 2021\Information Security Analysis and Audit Lab\Lab 3 20-8-21\packet.pcapng (93 KB)

Capture

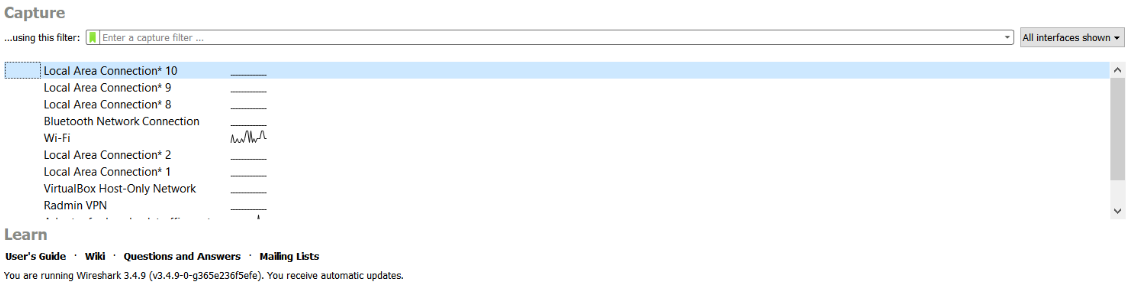
...using this filter: Enter a capture filter ... All interfaces shown

Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Wi-Fi
Local Area Connection* 2
Local Area Connection* 1
VirtualBox Host-Only Network
Radmin VPN

Learn

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

You are running Wireshark 3.4.9 (v3.4.9-0-g365e236f5efe). You receive automatic updates.


Capture

...using this filter: Enter a capture filter ... All interfaces shown

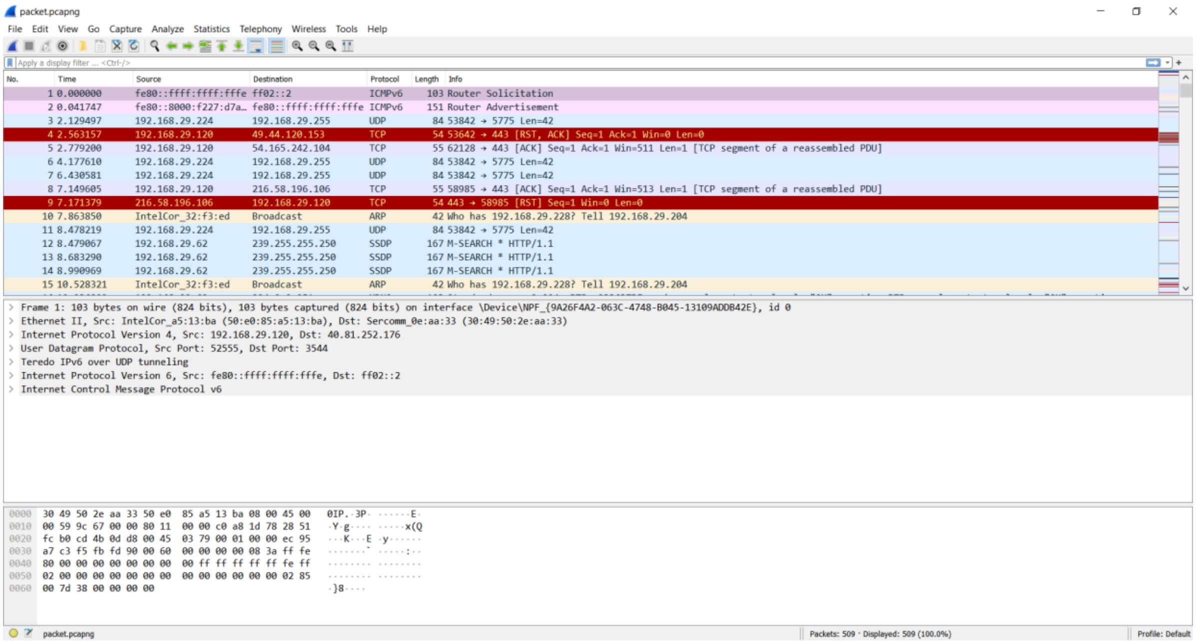
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Wi-Fi
Local Area Connection* 2
Local Area Connection* 1
VirtualBox Host-Only Network
Radmin VPN

Learn

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

You are running Wireshark 3.4.9 (v3.4.9-0-g365e236f5efe). You receive automatic updates.

2)START CAPTURING PACKETS.


packet.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

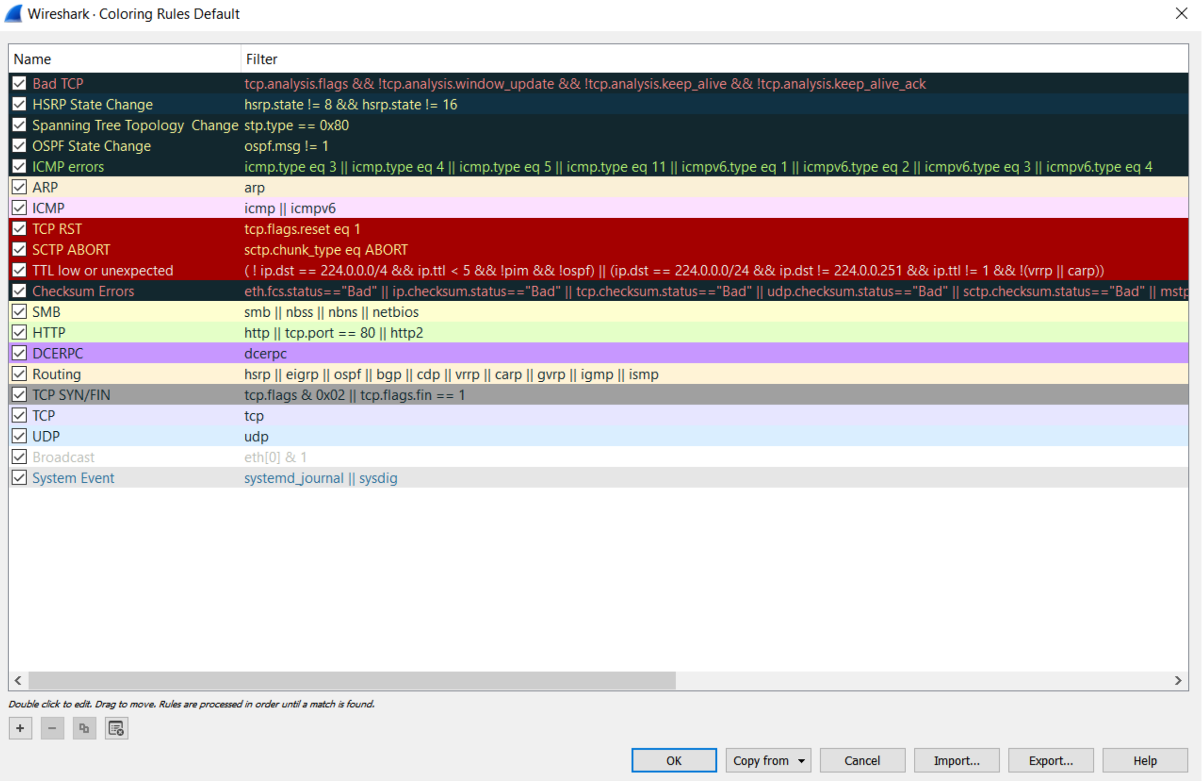
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::ffff:ffff:fffe	ff02::2	ICMPv6	103	Router Solicitation
2	0.041747	fe80::8000:f227:d7a…	fe80::ffff:ffff:fffe	ICMPv6	151	Router Advertisement
3	2.129497	192.168.29.224	192.168.29.255	UDP	84	53842 → 5775 Len=42
4	2.563157	192.168.29.120	49.44.120.153	TCP	54	53642 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	2.779200	192.168.29.120	54.165.242.104	TCP	55	62128 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PDU]
6	4.177610	192.168.29.224	192.168.29.255	UDP	84	53842 → 5775 Len=42
7	6.430581	192.168.29.224	192.168.29.255	UDP	84	53842 → 5775 Len=42
8	7.149605	192.168.29.120	216.58.196.106	TCP	55	58985 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
9	7.171379	216.58.196.106	192.168.29.120	TCP	54	443 → 58985 [RST] Seq=1 Win=0 Len=0
10	7.863850	IntelCor_32:f3:ed	Broadcast	ARP	42	Who has 192.168.29.228? Tell 192.168.29.204
11	8.478219	192.168.29.224	192.168.29.255	UDP	84	53842 → 5775 Len=42
12	8.479067	192.168.29.62	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
13	8.683290	192.168.29.62	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
14	8.990969	192.168.29.62	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
15	10.528321	IntelCor_32:f3:ed	Broadcast	ARP	42	Who has 192.168.29.228? Tell 192.168.29.204

```
> Frame 1: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface \Device\NPF_{9A26F4A2-063C-4748-B045-13109ADDB42E}, id 0
> Ethernet II, Src: IntelCor_a5:13:ba (50:e0:85:a5:13:ba), Dst: Sercomm_0e:aa:33 (30:49:50:2e:aa:33)
> Internet Protocol Version 4, Src: 192.168.29.120, Dst: 40.81.252.176
> User Datagram Protocol, Src Port: 52555, Dst Port: 3544
> Teredo IPv6 over UDP tunneling
> Internet Protocol Version 6, Src: fe80::ffff:ffff:fffe, Dst: ff02::2
> Internet Control Message Protocol v6
```

```
0000  30 49 50 2e aa 33 50 e0  85 a5 13 ba 08 00 45 00   0IP.·3P· ······E·
0010  00 59 9c 67 00 00 80 11  00 00 c0 a8 1d 78 28 51   ·Y·g···· ·····x(Q
0020  fc b0 cd 4b 0d d8 00 45  03 79 00 01 00 00 ec 95   ···K···E ·y······
0030  a7 c3 f5 fb fd 90 00 60  00 00 00 00 08 3a ff fe   ·······` ·····:··
0040  80 00 00 00 00 00 00 00  00 ff ff ff ff ff fe ff   ········ ········
0050  02 00 00 00 00 00 00 00  00 00 00 00 00 00 02 85   ········ ········
0060  00 7d 38 00 00 00 00                               ·}8····
```

packet.pcapng   Packets: 509 · Displayed: 509 (100.0%)   Profile: Default

3)You can apply/change color schemes for packets of different protocols from the View->Change Color Menu.

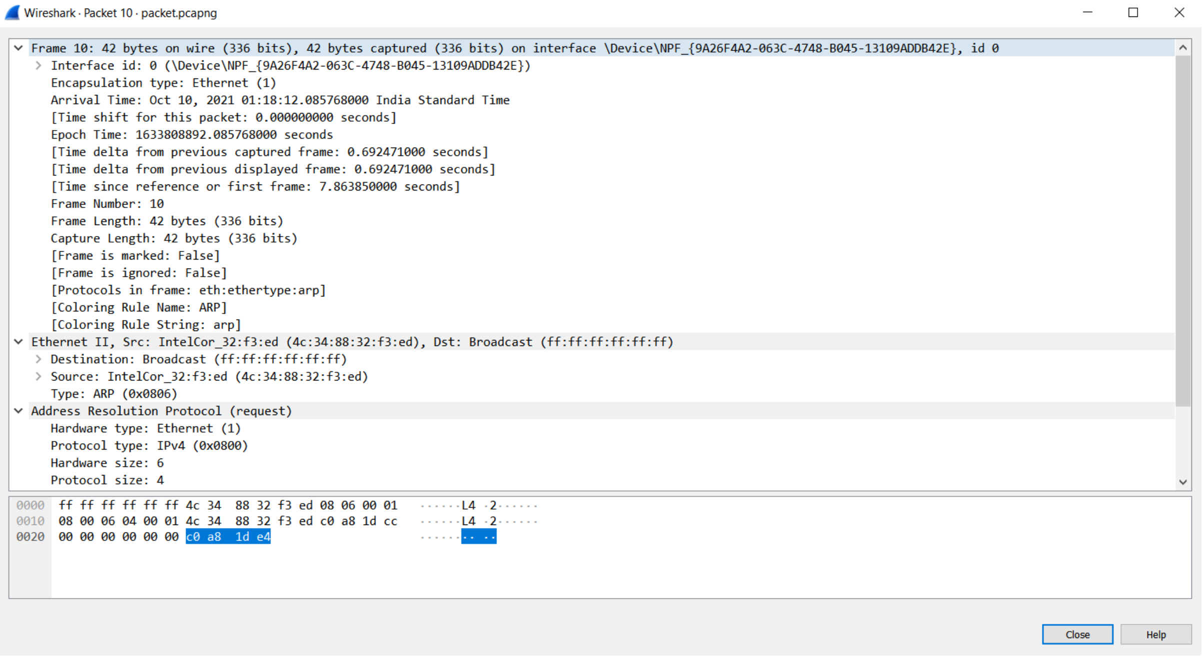


Wireshark · Coloring Rules Default

Name	Filter
☑ Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
☑ HSRP State Change	hsrp.state != 8 && hsrp.state != 16
☑ Spanning Tree Topology Change	stp.type == 0x80
☑ OSPF State Change	ospf.msg != 1
☑ ICMP errors	icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type eq 3 || icmpv6.type eq 4
☑ ARP	arp
☑ ICMP	icmp || icmpv6
☑ TCP RST	tcp.flags.reset eq 1
☑ SCTP ABORT	sctp.chunk_type eq ABORT
☑ TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || carp))
☑ Checksum Errors	eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checksum.status=="Bad" || mstp
☑ SMB	smb || nbss || nbns || netbios
☑ HTTP	http || tcp.port == 80 || http2
☑ DCERPC	dcerpc
☑ Routing	hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
☑ TCP SYN/FIN	tcp.flags & 0x02 || tcp.flags.fin == 1
☑ TCP	tcp
☑ UDP	udp
☑ Broadcast	eth[0] & 1
☑ System Event	systemd_journal || sysdig

Double click to edit. Drag to move. Rules are processed in order until a match is found.

4)You can select any particular packet to study about it in another window by double clicking on it.

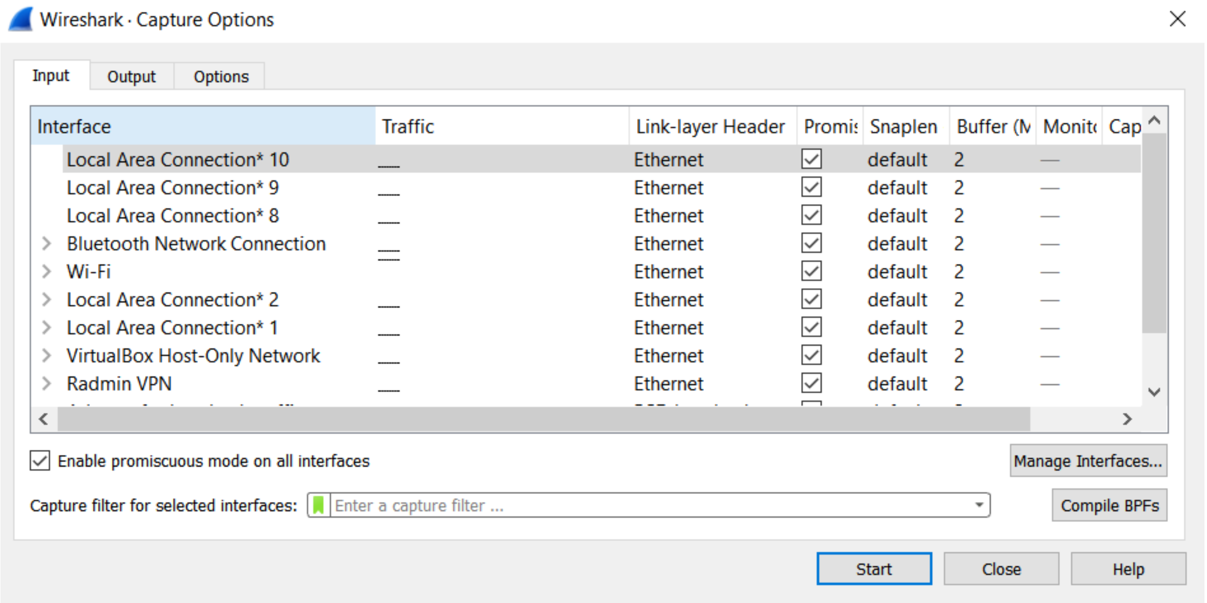


Wireshark · Packet 10 · packet.pcapng

```
∨ Frame 10: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{9A26F4A2-063C-4748-B045-13109ADDB42E}, id 0
  > Interface id: 0 (\Device\NPF_{9A26F4A2-063C-4748-B045-13109ADDB42E})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 10, 2021 01:18:12.085768000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1633808892.085768000 seconds
    [Time delta from previous captured frame: 0.692471000 seconds]
    [Time delta from previous displayed frame: 0.692471000 seconds]
    [Time since reference or first frame: 7.863850000 seconds]
    Frame Number: 10
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
∨ Ethernet II, Src: IntelCor_32:f3:ed (4c:34:88:32:f3:ed), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_32:f3:ed (4c:34:88:32:f3:ed)
    Type: ARP (0x0806)
∨ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
```

```
0000  ff ff ff ff ff ff 4c 34  88 32 f3 ed 08 06 00 01   ······L4 ·2······
0010  08 00 06 04 00 01 4c 34  88 32 f3 ed c0 a8 1d cc   ······L4 ·2······
0020  00 00 00 00 00 00 c0 a8  1d e4                     ········ ··
```

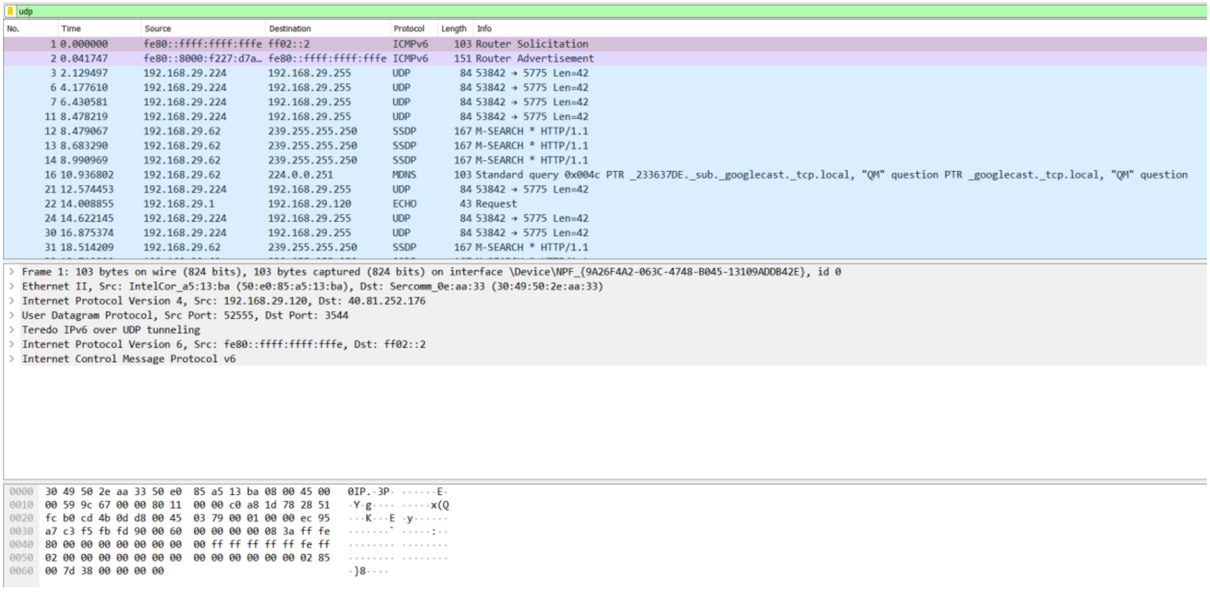
5)We can monitor the network devices and any devices connected to our network.We can enable/disable any device we want to connect to.



Interface	Traffic	Link-layer Header	Promis	Snaplen	Buffer (M	Monit	Cap
Local Area Connection* 10		Ethernet	☑	default	2	—	
Local Area Connection* 9		Ethernet	☑	default	2	—	
Local Area Connection* 8		Ethernet	☑	default	2	—	
Bluetooth Network Connection		Ethernet	☑	default	2	—	
Wi-Fi		Ethernet	☑	default	2	—	
Local Area Connection* 2		Ethernet	☑	default	2	—	
Local Area Connection* 1		Ethernet	☑	default	2	—	
VirtualBox Host-Only Network		Ethernet	☑	default	2	—	
Radmin VPN		Ethernet	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

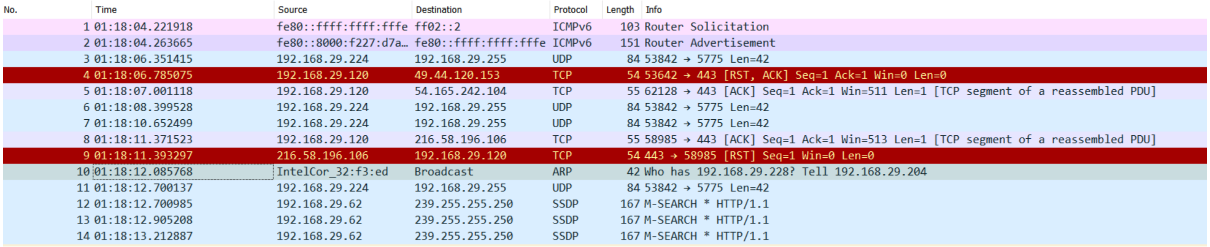


```
udp
No.  Time        Source                 Destination            Protocol Length Info
   1 0.000000    fe80::ffff:ffff:fffe   ff02::2                ICMPv6   103 Router Solicitation
   2 0.041747    fe80::8000:f227:d7a…   fe80::ffff:ffff:fffe   ICMPv6   151 Router Advertisement
   3 2.129497    192.168.29.224         192.168.29.255         UDP       84 53842 → 5775 Len=42
   6 4.177610    192.168.29.224         192.168.29.255         UDP       84 53842 → 5775 Len=42
   7 6.430581    192.168.29.224         192.168.29.255         UDP       84 53842 → 5775 Len=42
  11 8.478219    192.168.29.224         192.168.29.255         UDP       84 53842 → 5775 Len=42
  12 8.479067    192.168.29.62          239.255.255.250        SSDP     167 M-SEARCH * HTTP/1.1
  13 8.683290    192.168.29.62          239.255.255.250        SSDP     167 M-SEARCH * HTTP/1.1
  14 8.990969    192.168.29.62          239.255.255.250        SSDP     167 M-SEARCH * HTTP/1.1
  16 10.936802   192.168.29.62          224.0.0.251            MDNS     103 Standard query 0x004c PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
  21 12.574453   192.168.29.224         192.168.29.255         UDP       84 53842 → 5775 Len=42
  22 14.008855   192.168.29.1           192.168.29.120         ECHO      43 Request
  24 14.622145   192.168.29.224         192.168.29.255         UDP       84 53842 → 5775 Len=42
  30 16.875374   192.168.29.224         192.168.29.255         UDP       84 53842 → 5775 Len=42
  31 18.514209   192.168.29.62          239.255.255.250        SSDP     167 M-SEARCH * HTTP/1.1
```

```
> Frame 1: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface \Device\NPF_{9A26F4A2-063C-4748-B045-13109ADDB42E}, id 0
> Ethernet II, Src: IntelCor_a5:13:ba (50:e0:85:a5:13:ba), Dst: Sercomm_0e:aa:33 (30:49:50:2e:aa:33)
> Internet Protocol Version 4, Src: 192.168.29.120, Dst: 40.81.252.176
> User Datagram Protocol, Src Port: 52555, Dst Port: 3544
> Teredo IPv6 over UDP tunneling
> Internet Protocol Version 6, Src: fe80::ffff:ffff:fffe, Dst: ff02::2
> Internet Control Message Protocol v6
```

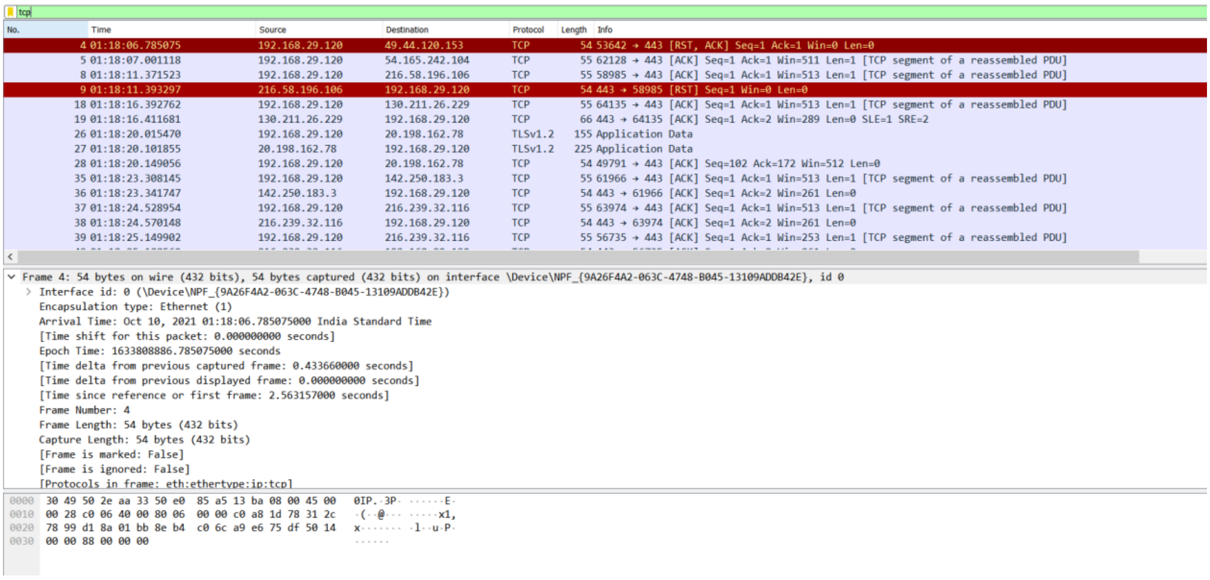
```
0000  30 49 50 2e aa 33 50 e0  85 a5 13 ba 08 00 45 00   0IP.·3P· ······E·
0010  00 59 9c 67 00 00 80 11  00 00 c0 a8 1d 78 28 51   ·Y·g···· ·····x(Q
0020  fc b0 cd 4b 0d d8 00 45  03 79 00 01 00 00 ec 95   ···K···E ·y······
0030  a7 c3 f5 fb fd 90 00 60  00 00 00 00 08 3a ff fe   ·······` ·····:··
0040  80 00 00 00 00 00 00 00  00 ff ff ff ff ff fe ff   ········ ········
0050  02 00 00 00 00 00 00 00  00 00 00 00 00 00 02 85   ········ ········
0060  00 7d 38 00 00 00 00                               ·}8····
```

6) We can search for any particular packet using Capture Filter.



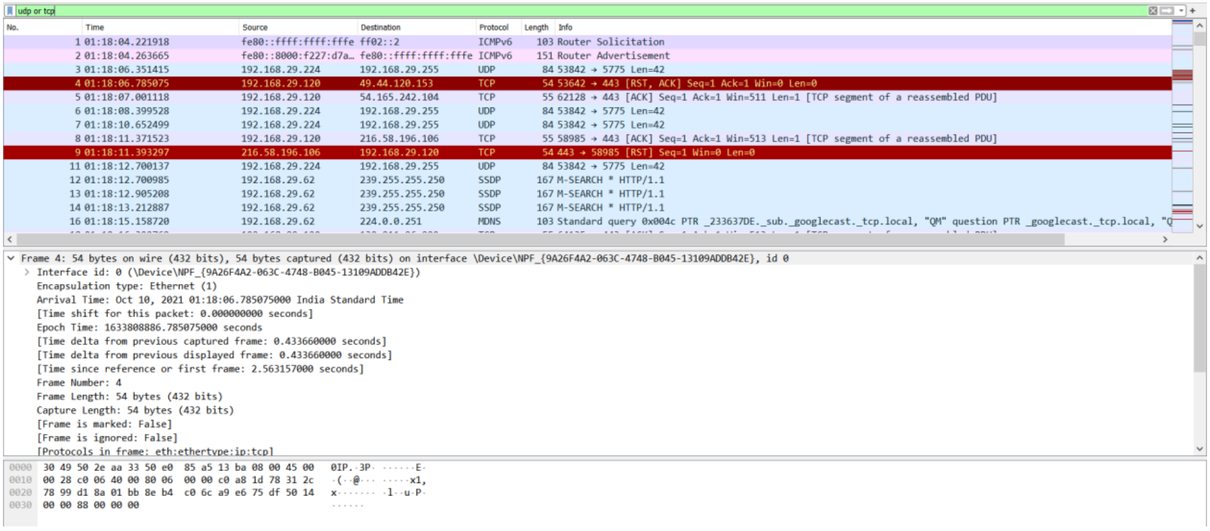
```
No.  Time             Source                 Destination            Protocol Length Info
   1 01:18:04.221918  fe80::ffff:ffff:fffe   ff02::2                ICMPv6   103 Router Solicitation
   2 01:18:04.263665  fe80::8000:f227:d7a…   fe80::ffff:ffff:fffe   ICMPv6   151 Router Advertisement
   3 01:18:06.351415  192.168.29.224         192.168.29.255         UDP       84 53842 → 5775 Len=42
   4 01:18:06.785075  192.168.29.120         49.44.120.153          TCP       54 53642 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   5 01:18:07.001118  192.168.29.120         54.165.242.104         TCP       55 62128 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PDU]
   6 01:18:08.399528  192.168.29.224         192.168.29.255         UDP       84 53842 → 5775 Len=42
   7 01:18:10.652499  192.168.29.224         192.168.29.255         UDP       84 53842 → 5775 Len=42
   8 01:18:11.371523  192.168.29.120         216.58.196.106         TCP       55 58985 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
   9 01:18:11.393297  216.58.196.106         192.168.29.120         TCP       54 443 → 58985 [RST] Seq=1 Win=0 Len=0
  10 01:18:12.085768  IntelCor_32:f3:ed      Broadcast              ARP       42 Who has 192.168.29.228? Tell 192.168.29.204
  11 01:18:12.700137  192.168.29.224         192.168.29.255         UDP       84 53842 → 5775 Len=42
  12 01:18:12.700985  192.168.29.62          239.255.255.250        SSDP     167 M-SEARCH * HTTP/1.1
  13 01:18:12.905208  192.168.29.62          239.255.255.250        SSDP     167 M-SEARCH * HTTP/1.1
  14 01:18:13.212887  192.168.29.62          239.255.255.250        SSDP     167 M-SEARCH * HTTP/1.1
```

7)Capture only TCP Packets.



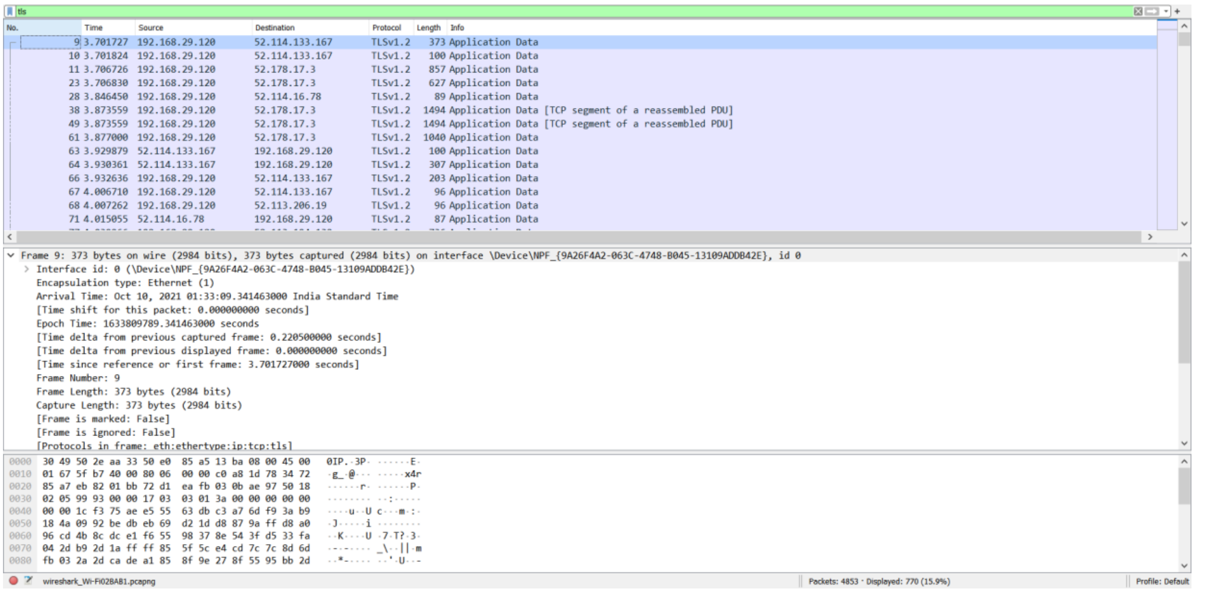
```
tcp
No.   Time              Source            Destination       Protocol  Length  Info
    4 01:18:06.785075   192.168.29.120    49.44.120.153     TCP         54 53642 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    5 01:18:07.001118   192.168.29.120    54.165.242.104    TCP         55 62128 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PDU]
    8 01:18:11.371523   192.168.29.120    216.58.196.106    TCP         55 58985 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
    9 01:18:11.393297   216.58.196.106    192.168.29.120    TCP         54 443 → 58985 [RST] Seq=1 Win=0 Len=0
   18 01:18:16.392762   192.168.29.120    130.211.26.229    TCP         55 64135 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
   19 01:18:16.411681   130.211.26.229    192.168.29.120    TCP         66 443 → 64135 [ACK] Seq=1 Ack=2 Win=289 Len=0 SLE=1 SRE=2
   26 01:18:20.015470   192.168.29.120    20.198.162.78     TLSv1.2    155 Application Data
   27 01:18:20.101855   20.198.162.78     192.168.29.120    TLSv1.2    225 Application Data
   28 01:18:20.149056   192.168.29.120    20.198.162.78     TCP         54 49791 → 443 [ACK] Seq=102 Ack=172 Win=512 Len=0
   35 01:18:23.308145   192.168.29.120    142.250.183.3     TCP         55 61966 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
   36 01:18:23.341747   142.250.183.3     192.168.29.120    TCP         54 443 → 61966 [ACK] Seq=1 Ack=2 Win=261 Len=0
   37 01:18:24.528954   192.168.29.120    216.239.32.116    TCP         55 63974 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
   38 01:18:24.570148   216.239.32.116    192.168.29.120    TCP         54 443 → 63974 [ACK] Seq=1 Ack=2 Win=261 Len=0
   39 01:18:25.149902   192.168.29.120    216.239.32.116    TCP         55 56735 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1 [TCP segment of a reassembled PDU]

v Frame 4: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{9A26F4A2-063C-4748-B045-13109ADDB42E}, id 0
  > Interface id: 0 (\Device\NPF_{9A26F4A2-063C-4748-B045-13109ADDB42E})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 10, 2021 01:18:06.785075000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1633808886.785075000 seconds
    [Time delta from previous captured frame: 0.433660000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 2.563157000 seconds]
    Frame Number: 4
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]

0000  30 49 50 2e aa 33 50 e0  85 a5 13 ba 08 00 45 00   0IP.·3P· ······E·
0010  00 28 c0 06 40 00 80 06  00 00 c0 a8 1d 78 31 2c   ·(··@··· ·····x1,
0020  78 99 d1 8a 01 bb 8e b4  c0 6c a9 e6 75 df 50 14   x······· ·l··u·P·
0030  00 00 88 00 00 00                                  ······
```

8)Capture only TCP or UDP packets using capture filter.



```
udp or tcp
No.   Time              Source                Destination             Protocol  Length  Info
    1 01:18:04.221918   fe80::ffff:ffff:fffe  ff02::2                 ICMPv6     103 Router Solicitation
    2 01:18:04.263665   fe80::8000:f227:d7a…  fe80::ffff:ffff:fffe    ICMPv6     151 Router Advertisement
    3 01:18:06.351415   192.168.29.224        192.168.29.255          UDP         84 53842 → 5775 Len=42
    4 01:18:06.785075   192.168.29.120        49.44.120.153           TCP         54 53642 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    5 01:18:07.001118   192.168.29.120        54.165.242.104          TCP         55 62128 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PDU]
    6 01:18:08.399528   192.168.29.224        192.168.29.255          UDP         84 53842 → 5775 Len=42
    7 01:18:10.652499   192.168.29.224        192.168.29.255          UDP         84 53842 → 5775 Len=42
    8 01:18:11.371523   192.168.29.120        216.58.196.106          TCP         55 58985 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
    9 01:18:11.393297   216.58.196.106        192.168.29.120          TCP         54 443 → 58985 [RST] Seq=1 Win=0 Len=0
   11 01:18:12.700137   192.168.29.224        192.168.29.255          UDP         84 53842 → 5775 Len=42
   12 01:18:12.700985   192.168.29.62         239.255.255.250         SSDP       167 M-SEARCH * HTTP/1.1
   13 01:18:12.905208   192.168.29.62         239.255.255.250         SSDP       167 M-SEARCH * HTTP/1.1
   14 01:18:13.212887   192.168.29.62         239.255.255.250         SSDP       167 M-SEARCH * HTTP/1.1
   16 01:18:15.158720   192.168.29.62         224.0.0.251             MDNS       103 Standard query 0x004c PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "Q

v Frame 4: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{9A26F4A2-063C-4748-B045-13109ADDB42E}, id 0
  > Interface id: 0 (\Device\NPF_{9A26F4A2-063C-4748-B045-13109ADDB42E})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 10, 2021 01:18:06.785075000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1633808886.785075000 seconds
    [Time delta from previous captured frame: 0.433660000 seconds]
    [Time delta from previous displayed frame: 0.433660000 seconds]
    [Time since reference or first frame: 2.563157000 seconds]
    Frame Number: 4
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]

0000  30 49 50 2e aa 33 50 e0  85 a5 13 ba 08 00 45 00   0IP.·3P· ······E·
0010  00 28 c0 06 40 00 80 06  00 00 c0 a8 1d 78 31 2c   ·(··@··· ·····x1,
0020  78 99 d1 8a 01 bb 8e b4  c0 6c a9 e6 75 df 50 14   x······· ·l··u·P·
0030  00 00 88 00 00 00                                  ······
```

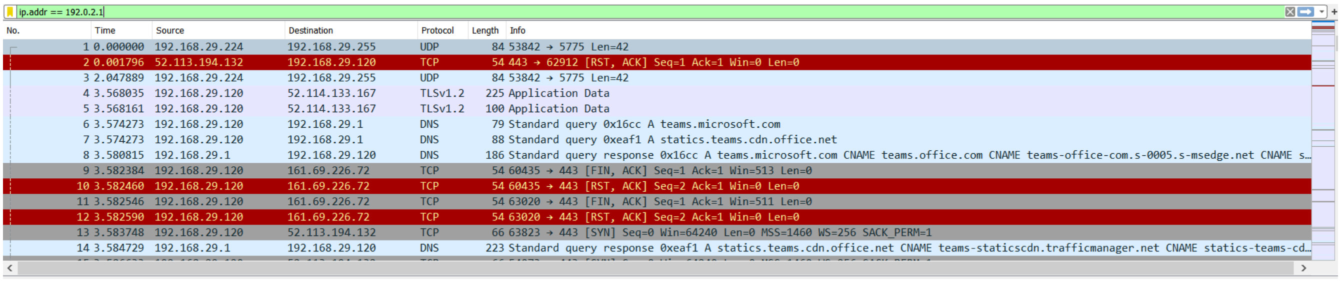
If we want to search for **https**,we have to put **tls** in the capture filter.



```
tls
No.   Time      Source            Destination       Protocol  Length  Info
    9 3.701727  192.168.29.120    52.114.133.167    TLSv1.2    373 Application Data
   10 3.701824  192.168.29.120    52.114.133.167    TLSv1.2    100 Application Data
   11 3.706726  192.168.29.120    52.178.17.3       TLSv1.2    857 Application Data
   23 3.706830  192.168.29.120    52.178.17.3       TLSv1.2    627 Application Data
   28 3.846450  192.168.29.120    52.114.16.78      TLSv1.2     89 Application Data
   38 3.873559  192.168.29.120    52.178.17.3       TLSv1.2   1494 Application Data [TCP segment of a reassembled PDU]
   49 3.873559  192.168.29.120    52.178.17.3       TLSv1.2   1494 Application Data [TCP segment of a reassembled PDU]
   61 3.877000  192.168.29.120    52.178.17.3       TLSv1.2   1040 Application Data
   63 3.929879  52.114.133.167    192.168.29.120    TLSv1.2    100 Application Data
   64 3.930361  52.114.133.167    192.168.29.120    TLSv1.2    307 Application Data
   66 3.932636  192.168.29.120    52.114.133.167    TLSv1.2    203 Application Data
   67 4.006710  192.168.29.120    52.114.133.167    TLSv1.2     96 Application Data
   68 4.007262  192.168.29.120    52.113.206.19     TLSv1.2     96 Application Data
   71 4.015055  52.114.16.78      192.168.29.120    TLSv1.2     87 Application Data

v Frame 9: 373 bytes on wire (2984 bits), 373 bytes captured (2984 bits) on interface \Device\NPF_{9A26F4A2-063C-4748-B045-13109ADDB42E}, id 0
  > Interface id: 0 (\Device\NPF_{9A26F4A2-063C-4748-B045-13109ADDB42E})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 10, 2021 01:33:09.341463000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1633809789.341463000 seconds
    [Time delta from previous captured frame: 0.220500000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 3.701727000 seconds]
    Frame Number: 9
    Frame Length: 373 bytes (2984 bits)
    Capture Length: 373 bytes (2984 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]

0000  30 49 50 2e aa 33 50 e0  85 a5 13 ba 08 00 45 00   0IP.·3P· ······E·
0010  01 67 5f b7 40 00 80 06  00 00 c0 a8 1d 78 34 72   ·g_·@··· ·····x4r
0020  85 a7 eb 82 01 bb 72 d1  ea fb 03 0b ae 97 50 18   ······r· ······P·
0030  02 05 99 93 00 00 17 03  03 01 3a 00 00 00 00 00   ········ ··:·····
0040  00 00 1c f3 75 ae e5 55  63 db c3 a7 6d f9 3a b9   ····u··U c···m·:·
0050  18 4a 09 92 be db eb 69  d2 1d d8 87 9a ff d8 a0   ·J·····i ········
0060  96 cd 4b 8c dc e1 f6 55  98 37 8e 54 3f d5 33 fa   ··K····U ·7·T?·3·
0070  04 2d b9 2d 1a ff ff 85  5f 5c e4 cd 7c 7c 8d 6d   ·-·-···· _\··||·m
0080  fb 03 2a 2d ca de a1 85  8f 9e 27 8f 55 95 bb 2d   ··*-···· ··'·U··-

wireshark_Wi-Fi02BAB1.pcapng          Packets: 4853 · Displayed: 770 (15.9%)          Profile: Default
```

Black colored packets either mean as mad TCP or it indicates checksum error.
To view only HTTP traffic, type http (lower case) in the Filter box and press Enter. Select the first HTTP packet labeled GET /. Observe the destination IP address.
UDP is much faster. TCP is slow as it requires 3-way handshake. The load on DNS servers is also an important factor. DNS servers (since they use UDP) don't have to keep connections. DNS requests are generally very small and fit well within UDP segments. UDP is not reliable, but reliability can added on application layer. An application can use UDP and can be reliable by using a timeout and resend at the application layer. Differentiate http and https traffic. HTTPS is HTTP with encryption. The only difference between the two protocols is that HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses. As a result, HTTPS is far more secure than HTTP.

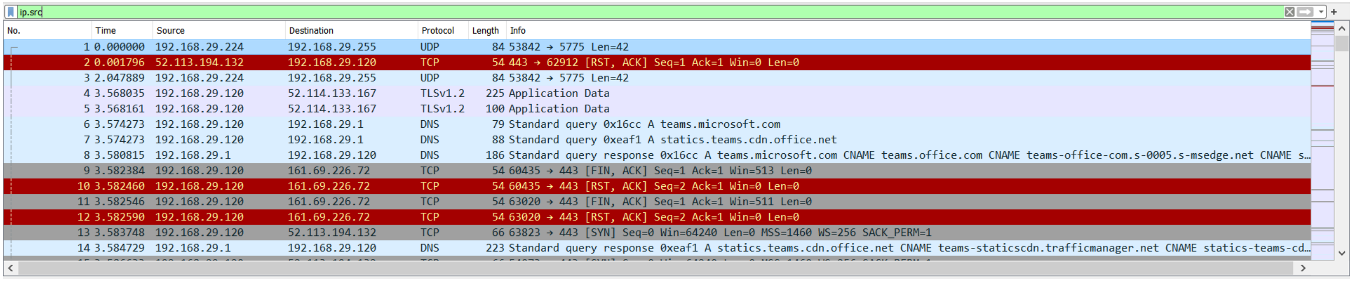
9)Capture packets for any IP Address.



ip.addr == 192.0.2.1

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.29.224	192.168.29.255	UDP	84	53842 → 5775 Len=42
2	0.001796	52.113.194.132	192.168.29.120	TCP	54	443 → 62912 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	2.047889	192.168.29.224	192.168.29.255	UDP	84	53842 → 5775 Len=42
4	3.568035	192.168.29.120	52.114.133.167	TLSv1.2	225	Application Data
5	3.568161	192.168.29.120	52.114.133.167	TLSv1.2	100	Application Data
6	3.574273	192.168.29.120	192.168.29.1	DNS	79	Standard query 0x16cc A teams.microsoft.com
7	3.574273	192.168.29.120	192.168.29.1	DNS	88	Standard query 0xeaf1 A statics.teams.cdn.office.net
8	3.580815	192.168.29.1	192.168.29.120	DNS	186	Standard query response 0x16cc A teams.microsoft.com CNAME teams.office.com CNAME teams-office-com.s-0005.s-msedge.net CNAME s…
9	3.582384	192.168.29.120	161.69.226.72	TCP	54	60435 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
10	3.582460	192.168.29.120	161.69.226.72	TCP	54	60435 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
11	3.582546	192.168.29.120	161.69.226.72	TCP	54	63020 → 443 [FIN, ACK] Seq=1 Ack=1 Win=511 Len=0
12	3.582590	192.168.29.120	161.69.226.72	TCP	54	63020 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
13	3.583748	192.168.29.120	52.113.194.132	TCP	66	63823 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
14	3.584729	192.168.29.1	192.168.29.120	DNS	223	Standard query response 0xeaf1 A statics.teams.cdn.office.net CNAME teams-staticscdn.trafficmanager.net CNAME statics-teams-cd…

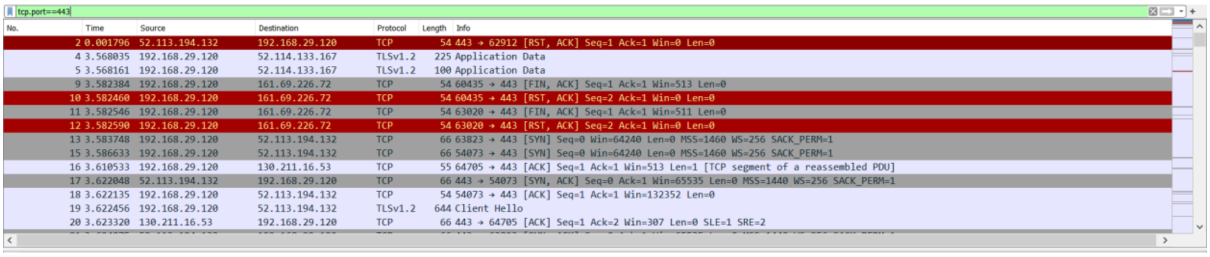
10)Capture packets from source IP.



ip.src

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.29.224	192.168.29.255	UDP	84	53842 → 5775 Len=42
2	0.001796	52.113.194.132	192.168.29.120	TCP	54	443 → 62912 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	2.047889	192.168.29.224	192.168.29.255	UDP	84	53842 → 5775 Len=42
4	3.568035	192.168.29.120	52.114.133.167	TLSv1.2	225	Application Data
5	3.568161	192.168.29.120	52.114.133.167	TLSv1.2	100	Application Data
6	3.574273	192.168.29.120	192.168.29.1	DNS	79	Standard query 0x16cc A teams.microsoft.com
7	3.574273	192.168.29.120	192.168.29.1	DNS	88	Standard query 0xeaf1 A statics.teams.cdn.office.net
8	3.580815	192.168.29.1	192.168.29.120	DNS	186	Standard query response 0x16cc A teams.microsoft.com CNAME teams.office.com CNAME teams-office-com.s-0005.s-msedge.net CNAME s…
9	3.582384	192.168.29.120	161.69.226.72	TCP	54	60435 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
10	3.582460	192.168.29.120	161.69.226.72	TCP	54	60435 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
11	3.582546	192.168.29.120	161.69.226.72	TCP	54	63020 → 443 [FIN, ACK] Seq=1 Ack=1 Win=511 Len=0
12	3.582590	192.168.29.120	161.69.226.72	TCP	54	63020 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
13	3.583748	192.168.29.120	52.113.194.132	TCP	66	63823 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
14	3.584729	192.168.29.1	192.168.29.120	DNS	223	Standard query response 0xeaf1 A statics.teams.cdn.office.net CNAME teams-staticscdn.trafficmanager.net CNAME statics-teams-cd…

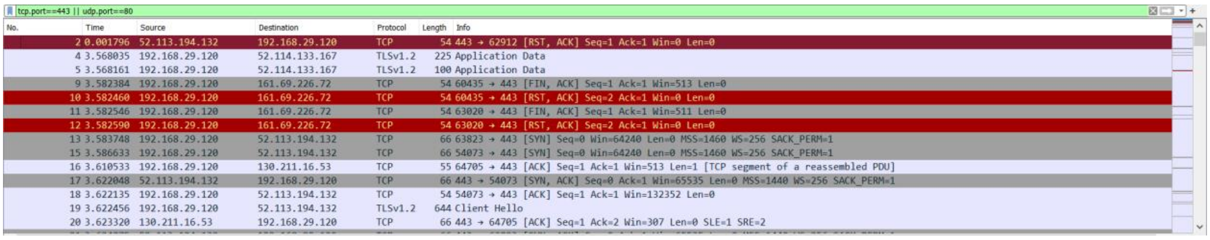
11)Capture packets for any specified TCP port.



tcp.port==443

No.	Time	Source	Destination	Protocol	Length	Info
2	0.001796	52.113.194.132	192.168.29.120	TCP	54	443 → 62912 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4	3.568035	192.168.29.120	52.114.133.167	TLSv1.2	225	Application Data
5	3.568161	192.168.29.120	52.114.133.167	TLSv1.2	100	Application Data
9	3.582384	192.168.29.120	161.69.226.72	TCP	54	60435 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
10	3.582460	192.168.29.120	161.69.226.72	TCP	54	60435 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
11	3.582546	192.168.29.120	161.69.226.72	TCP	54	63020 → 443 [FIN, ACK] Seq=1 Ack=1 Win=511 Len=0
12	3.582590	192.168.29.120	161.69.226.72	TCP	54	63020 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
13	3.583748	192.168.29.120	52.113.194.132	TCP	66	63823 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
15	3.586633	192.168.29.120	52.113.194.132	TCP	66	54073 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
16	3.610533	192.168.29.120	130.211.16.53	TCP	55	64705 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
17	3.622048	52.113.194.132	192.168.29.120	TCP	66	443 → 54073 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
18	3.622135	192.168.29.120	52.113.194.132	TCP	54	54073 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
19	3.622456	192.168.29.120	52.113.194.132	TLSv1.2	644	Client Hello
20	3.623320	130.211.16.53	192.168.29.120	TCP	66	443 → 64705 [ACK] Seq=1 Ack=2 Win=307 Len=0 SLE=1 SRE=2

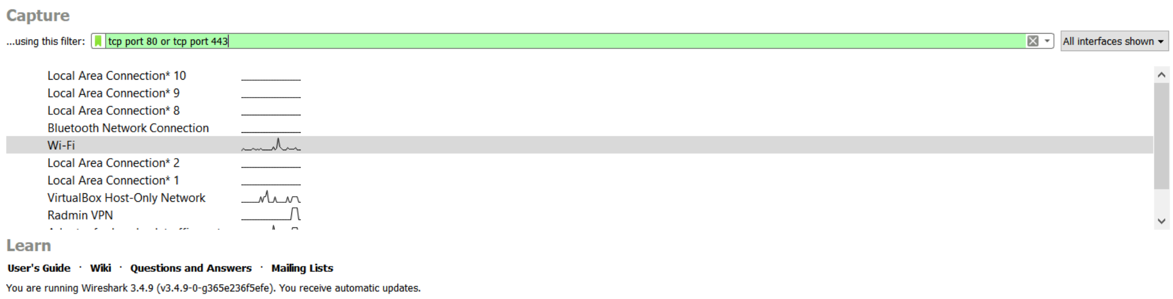
12) Capture packets for any specified TCP or UDP port.



tcp.port==443 || udp.port==80

No.	Time	Source	Destination	Protocol	Length	Info
2	0.001796	52.113.194.132	192.168.29.120	TCP	54	443 → 62912 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4	3.568035	192.168.29.120	52.114.133.167	TLSv1.2	225	Application Data
5	3.568161	192.168.29.120	52.114.133.167	TLSv1.2	100	Application Data
9	3.582384	192.168.29.120	161.69.226.72	TCP	54	60435 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
10	3.582460	192.168.29.120	161.69.226.72	TCP	54	60435 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
11	3.582546	192.168.29.120	161.69.226.72	TCP	54	63020 → 443 [FIN, ACK] Seq=1 Ack=1 Win=511 Len=0
12	3.582590	192.168.29.120	161.69.226.72	TCP	54	63020 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
13	3.583748	192.168.29.120	52.113.194.132	TCP	66	63823 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
15	3.586633	192.168.29.120	52.113.194.132	TCP	66	54073 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
16	3.610533	192.168.29.120	130.211.16.53	TCP	55	64705 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
17	3.622048	52.113.194.132	192.168.29.120	TCP	66	443 → 54073 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
18	3.622135	192.168.29.120	52.113.194.132	TCP	54	54073 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
19	3.622456	192.168.29.120	52.113.194.132	TLSv1.2	644	Client Hello
20	3.623320	130.211.16.53	192.168.29.120	TCP	66	443 → 64705 [ACK] Seq=1 Ack=2 Win=307 Len=0 SLE=1 SRE=2

13)You can also use the Capture Filter from the main menu and select your desired interface you want to capture packets on.



Capture

...using this filter: tcp port 80 or tcp port 443

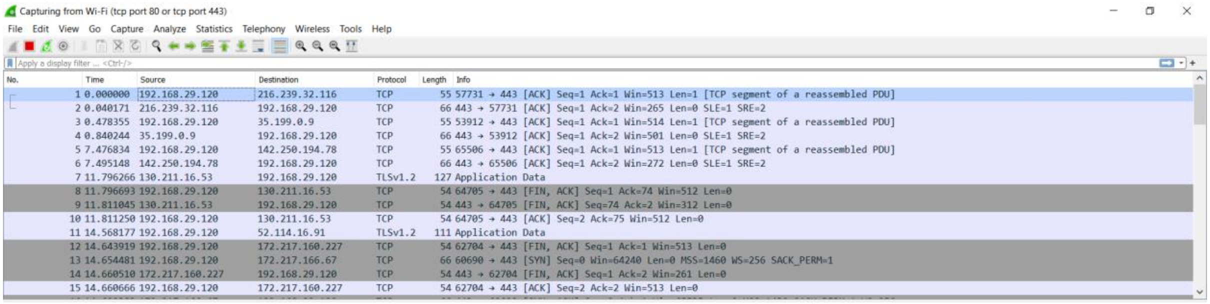
All interfaces shown

Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Wi-Fi
Local Area Connection* 2
Local Area Connection* 1
VirtualBox Host-Only Network
Radmin VPN

Learn

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

You are running Wireshark 3.4.9 (v3.4.9-0-g365e236f5efe). You receive automatic updates.



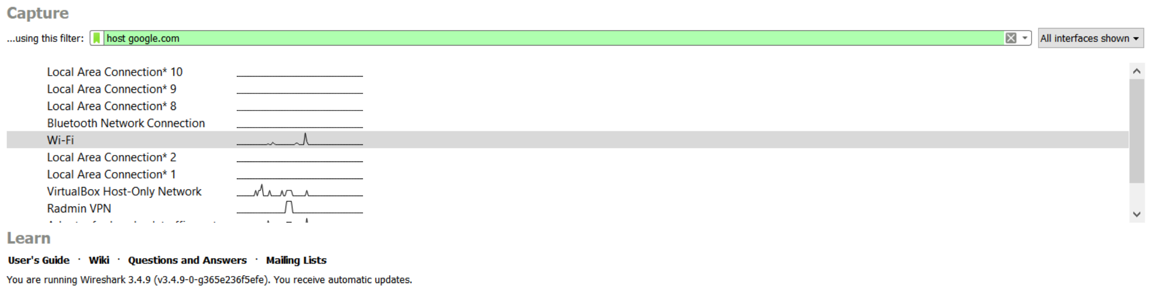
Capturing from Wi-Fi (tcp port 80 or tcp port 443)

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	192.168.29.120	216.239.32.116	TCP	55	57731 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
2	0.040171	216.239.32.116	192.168.29.120	TCP	66	443 → 57731 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
3	0.478355	192.168.29.120	35.199.0.9	TCP	55	53912 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of a reassembled PDU]
4	0.840244	35.199.0.9	192.168.29.120	TCP	66	443 → 53912 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
5	7.476834	192.168.29.120	142.250.194.78	TCP	55	65506 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
6	7.495148	142.250.194.78	192.168.29.120	TCP	66	443 → 65506 [ACK] Seq=1 Ack=2 Win=272 Len=0 SLE=1 SRE=2
7	11.796266	130.211.16.53	192.168.29.120	TLSv1.2	127	Application Data
8	11.796693	192.168.29.120	130.211.16.53	TCP	54	64705 → 443 [FIN, ACK] Seq=1 Ack=74 Win=512 Len=0
9	11.811045	130.211.16.53	192.168.29.120	TCP	54	443 → 64705 [FIN, ACK] Seq=74 Ack=2 Win=312 Len=0
10	11.811250	192.168.29.120	130.211.16.53	TCP	54	64705 → 443 [ACK] Seq=2 Ack=75 Win=512 Len=0
11	14.568177	192.168.29.120	52.114.16.91	TLSv1.2	111	Application Data
12	14.643919	192.168.29.120	172.217.160.227	TCP	54	62704 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
13	14.654481	192.168.29.120	172.217.166.67	TCP	66	60690 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
14	14.660510	172.217.160.227	192.168.29.120	TCP	54	443 → 62704 [FIN, ACK] Seq=1 Ack=2 Win=261 Len=0
15	14.660666	192.168.29.120	172.217.160.227	TCP	54	62704 → 443 [ACK] Seq=2 Ack=2 Win=513 Len=0

14)Ping from cmd and capture packets on Wireshark.

Write host google.com on the filter bar.



Capture

...using this filter: host google.com

All interfaces shown

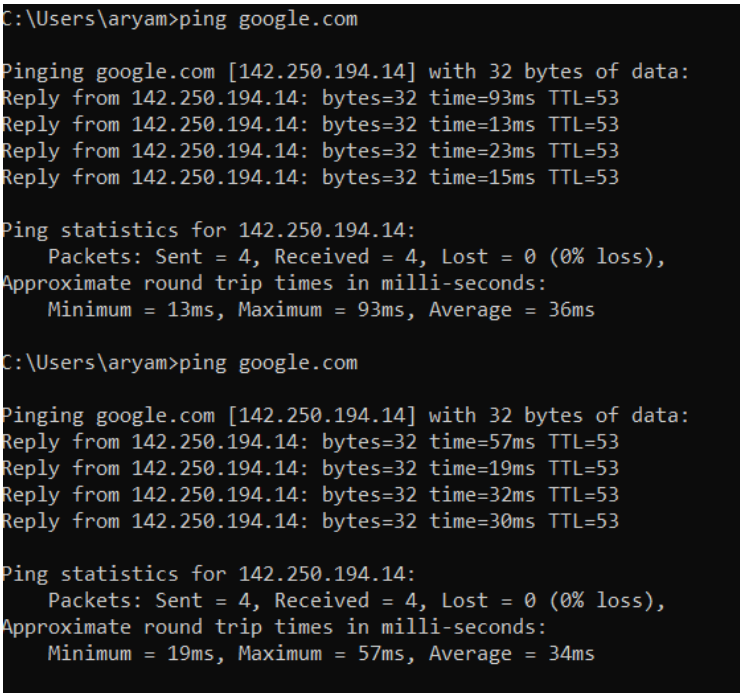
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Wi-Fi
Local Area Connection* 2
Local Area Connection* 1
VirtualBox Host-Only Network
Radmin VPN

Learn

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

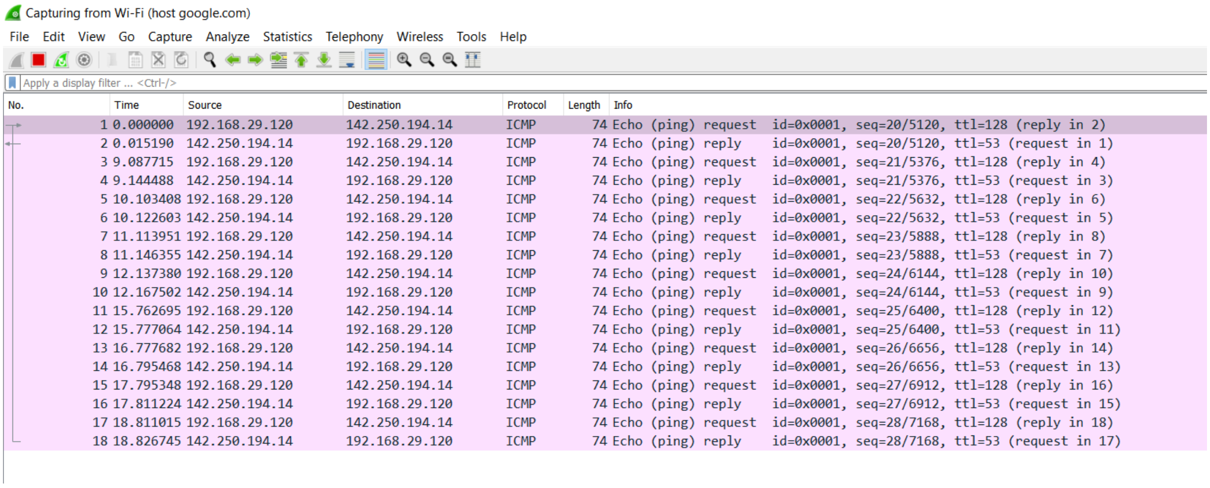
You are running Wireshark 3.4.9 (v3.4.9-0-g365e236f5efe). You receive automatic updates.

Open Command Prompt on your device and ping google.com.When pinging starts,start the capture process on Wireshark.



```
C:\Users\aryam>ping google.com

Pinging google.com [142.250.194.14] with 32 bytes of data:
Reply from 142.250.194.14: bytes=32 time=93ms TTL=53
Reply from 142.250.194.14: bytes=32 time=13ms TTL=53
Reply from 142.250.194.14: bytes=32 time=23ms TTL=53
Reply from 142.250.194.14: bytes=32 time=15ms TTL=53

Ping statistics for 142.250.194.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 93ms, Average = 36ms

C:\Users\aryam>ping google.com

Pinging google.com [142.250.194.14] with 32 bytes of data:
Reply from 142.250.194.14: bytes=32 time=57ms TTL=53
Reply from 142.250.194.14: bytes=32 time=19ms TTL=53
Reply from 142.250.194.14: bytes=32 time=32ms TTL=53
Reply from 142.250.194.14: bytes=32 time=30ms TTL=53

Ping statistics for 142.250.194.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 57ms, Average = 34ms
```

You can view the ICMP packets captured during the ping on Wireshark.


Capturing from Wi-Fi (host google.com)
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	192.168.29.120	142.250.194.14	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=128 (reply in 2)
2	0.015190	142.250.194.14	192.168.29.120	ICMP	74	Echo (ping) reply id=0x0001, seq=20/5120, ttl=53 (request in 1)
3	9.087715	192.168.29.120	142.250.194.14	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 4)
4	9.144488	142.250.194.14	192.168.29.120	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=53 (request in 3)
5	10.103408	192.168.29.120	142.250.194.14	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 6)
6	10.122603	142.250.194.14	192.168.29.120	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=53 (request in 5)
7	11.113951	192.168.29.120	142.250.194.14	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 8)
8	11.146355	142.250.194.14	192.168.29.120	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=53 (request in 7)
9	12.137380	192.168.29.120	142.250.194.14	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 10)
10	12.167502	142.250.194.14	192.168.29.120	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=53 (request in 9)
11	15.762695	192.168.29.120	142.250.194.14	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 12)
12	15.777064	142.250.194.14	192.168.29.120	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=53 (request in 11)
13	16.777682	192.168.29.120	142.250.194.14	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 14)
14	16.795468	142.250.194.14	192.168.29.120	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=53 (request in 13)
15	17.795348	192.168.29.120	142.250.194.14	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (reply in 16)
16	17.811224	142.250.194.14	192.168.29.120	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=53 (request in 15)
17	18.811015	192.168.29.120	142.250.194.14	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (reply in 18)
18	18.826745	142.250.194.14	192.168.29.120	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=53 (request in 17)

Conclusion:The Installation and functionalities of Wireshark were noted successfully.