PRACTICAL: 10

AIM:

Approach to study Wireshark.

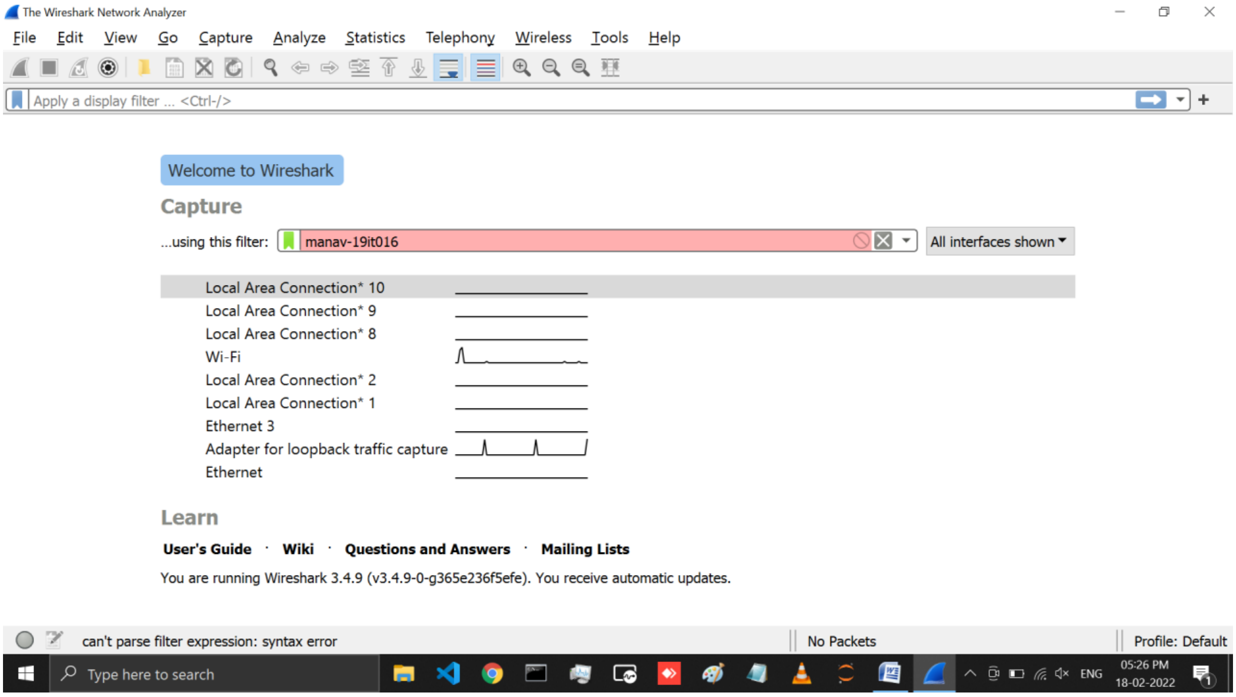
THEORY:

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often danger) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

OUTPUT:



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Type here to search
ENG

…using this filter: manav-19it016

All interfaces shown

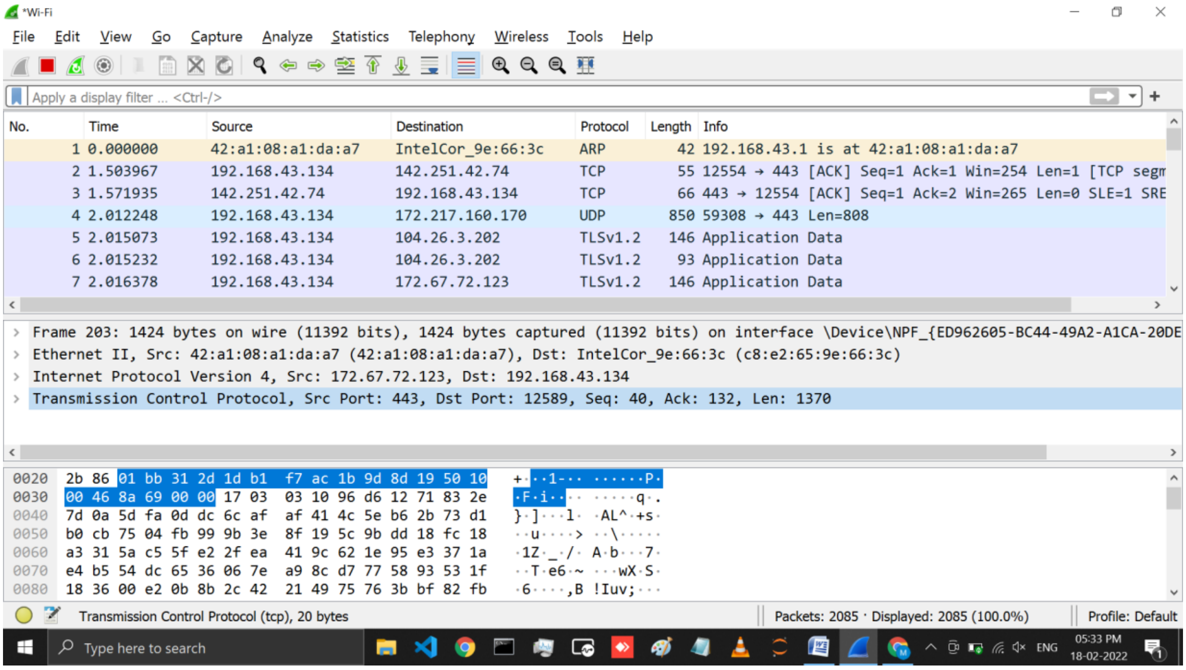
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Wi-Fi
Local Area Connection* 2
Local Area Connection* 1
Ethernet 3
Adapter for loopback traffic capture
Ethernet

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

can't parse filter expression: syntax error | No Packets | Profile: Default

05:26 PM 18-02-2022

Above image represent the home page of the wireshark application on which different network interface are listed and beside them shows the graph of the activity going on (it is not sniffing). We can click on any of the network interface and can capture the traffic and start sniffing.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
ENG
05:33 PM
18-02-2022

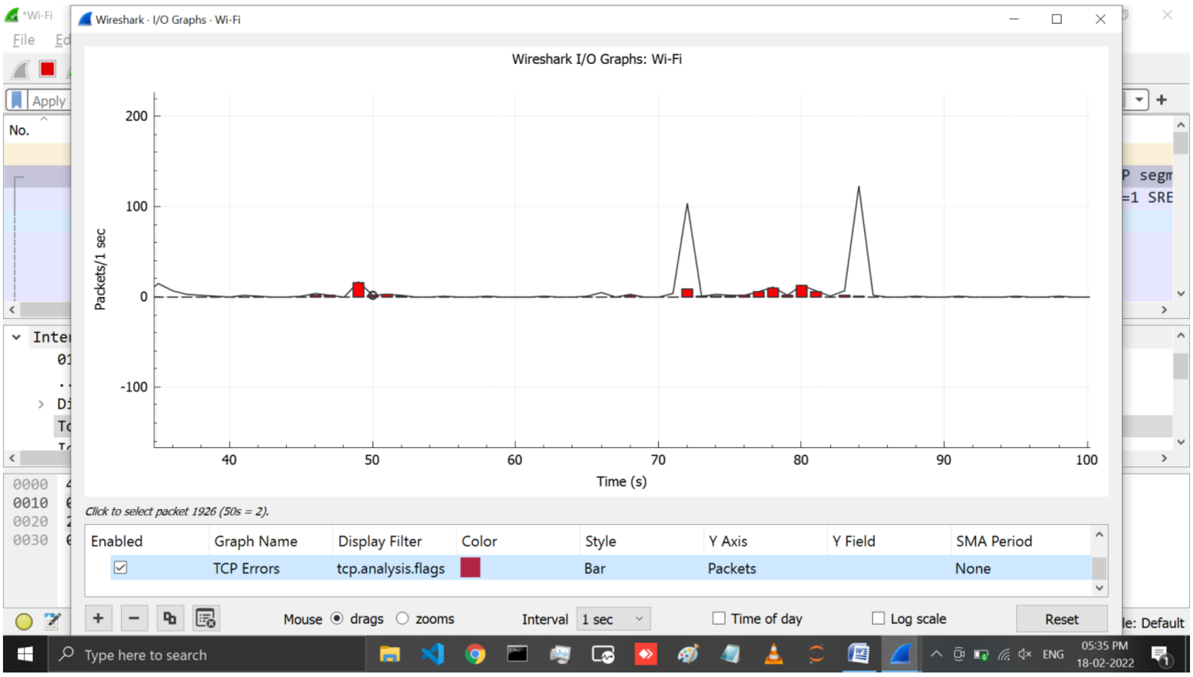
```
No.   Time       Source              Destination         Protocol  Length Info
    1 0.000000   42:a1:08:a1:da:a7   IntelCor_9e:66:3c   ARP         42 192.168.43.1 is at 42:a1:08:a1:da:a7
    2 1.503967   192.168.43.134      142.251.42.74       TCP         55 12554 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1 [TCP segm
    3 1.571935   142.251.42.74       192.168.43.134      TCP         66 443 → 12554 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE
    4 2.012248   192.168.43.134      172.217.160.170     UDP        850 59308 → 443 Len=808
    5 2.015073   192.168.43.134      104.26.3.202        TLSv1.2    146 Application Data
    6 2.015232   192.168.43.134      104.26.3.202        TLSv1.2     93 Application Data
    7 2.016378   192.168.43.134      172.67.72.123       TLSv1.2    146 Application Data
```

```
> Frame 203: 1424 bytes on wire (11392 bits), 1424 bytes captured (11392 bits) on interface \Device\NPF_{ED962605-BC44-49A2-A1CA-20DE
> Ethernet II, Src: 42:a1:08:a1:da:a7 (42:a1:08:a1:da:a7), Dst: IntelCor_9e:66:3c (c8:e2:65:9e:66:3c)
> Internet Protocol Version 4, Src: 172.67.72.123, Dst: 192.168.43.134
> Transmission Control Protocol, Src Port: 443, Dst Port: 12589, Seq: 40, Ack: 132, Len: 1370
```

```
0020  2b 86 01 bb 31 2d 1d b1  f7 ac 1b 9d 8d 19 50 10   +···1-·· ······P·
0030  00 46 8a 69 00 00 17 03  03 10 96 d6 12 71 83 2e   ·F·i···· ·····q·.
0040  7d 0a 5d fa 0d dc 6c af  af 41 4c 5e b6 2b 73 d1   }·]···l· ·AL^·+s·
0050  b0 cb 75 04 fb 99 9b 3e  8f 19 5c 9b dd 18 fc 18   ··u····> ··\·····
0060  a3 31 5a c5 5f e2 2f ea  41 9c 62 1e 95 e3 37 1a   ·1Z·_·/· A·b···7·
0070  e4 b5 54 dc 65 36 06 7e  a9 8c d7 77 58 93 53 1f   ··T·e6·~ ···wX·S·
0080  18 36 00 e2 0b 8b 2c 42  21 49 75 76 3b bf 82 fb   ·6····,B !Iuv;···
```

Transmission Control Protocol (tcp), 20 bytes | Packets: 2085 · Displayed: 2085 (100.0%) | Profile: Default

After clicking on any network interface wireshark will start capturing the packets, there are three sections in the window 1st section will show the list of the packet, 2nd section contains details such as the type of protocol used for that packet sender and receivers IP address, of the specific packet selected. And in 3rd section that the actual message that was received is shown in binary which is interpreted and shown in the 2nd section.

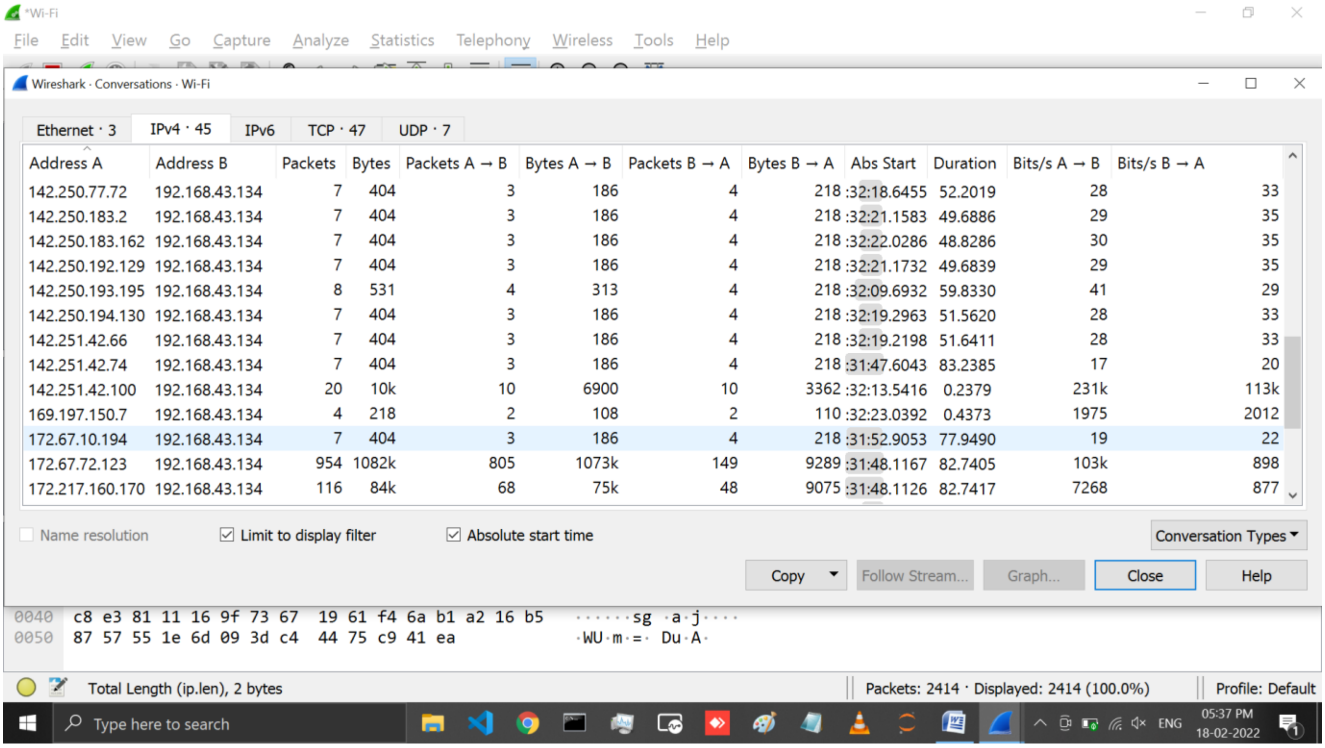


Click to select packet 1926 (50s = 2).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	TCP Errors	tcp.analysis.flags	🟥	Bar	Packets		None

Mouse ● drags ○ zooms Interval 1 sec □ Time of day □ Log scale Reset

This particular graph is showing typical traffic generated by a laptop. The spikes in the graph are bursts of traffic. Many times, cyber security pros use Wireshark as a quick and dirty way to identifytraffic bursts during attacks.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · Wi-Fi
Ethernet · 3
IPv4 · 45
IPv6
TCP · 47
UDP · 7

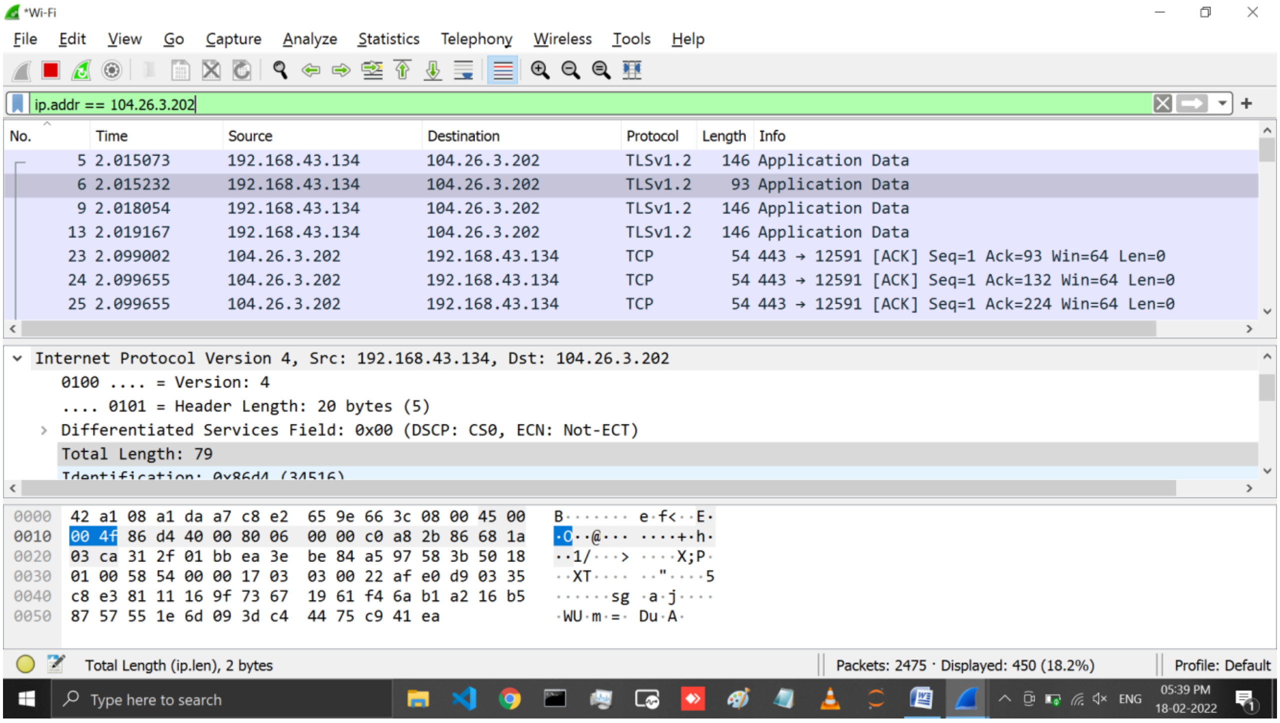
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Abs Start	Duration	Bits/s A → B	Bits/s B → A
142.250.77.72	192.168.43.134	7	404	3	186	4	218	:32:18.6455	52.2019	28	33
142.250.183.2	192.168.43.134	7	404	3	186	4	218	:32:21.1583	49.6886	29	35
142.250.183.162	192.168.43.134	7	404	3	186	4	218	:32:22.0286	48.8286	30	35
142.250.192.129	192.168.43.134	7	404	3	186	4	218	:32:21.1732	49.6839	29	35
142.250.193.195	192.168.43.134	8	531	4	313	4	218	:32:09.6932	59.8330	41	29
142.250.194.130	192.168.43.134	7	404	3	186	4	218	:32:19.2963	51.5620	28	33
142.251.42.66	192.168.43.134	7	404	3	186	4	218	:32:19.2198	51.6411	28	33
142.251.42.74	192.168.43.134	7	404	3	186	4	218	:31:47.6043	83.2385	17	20
142.251.42.100	192.168.43.134	20	10k	10	6900	10	3362	:32:13.5416	0.2379	231k	113k
169.197.150.7	192.168.43.134	4	218	2	108	2	110	:32:23.0392	0.4373	1975	2012
172.67.10.194	192.168.43.134	7	404	3	186	4	218	:31:52.9053	77.9490	19	22
172.67.72.123	192.168.43.134	954	1082k	805	1073k	149	9289	:31:48.1167	82.7405	103k	898
172.217.160.170	192.168.43.134	116	84k	68	75k	48	9075	:31:48.1126	82.7417	7268	877

□ Name resolution ☑ Limit to display filter ☑ Absolute start time

```
0040  c8 e3 81 11 16 9f 73 67  19 61 f4 6a b1 a2 16 b5   ······sg ·a·j····
0050  87 57 55 1e 6d 09 3d c4  44 75 c9 41 ea            ·WU·m·=· Du·A·
```

Total Length (ip.len), 2 bytes | Packets: 2414 · Displayed: 2414 (100.0%) | Profile: Default

It’s also possible to capture the amount of traffic generated between one system and another. If you go to Statistics and then select Conversations, you will see a summary of conversations between end points.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 104.26.3.202

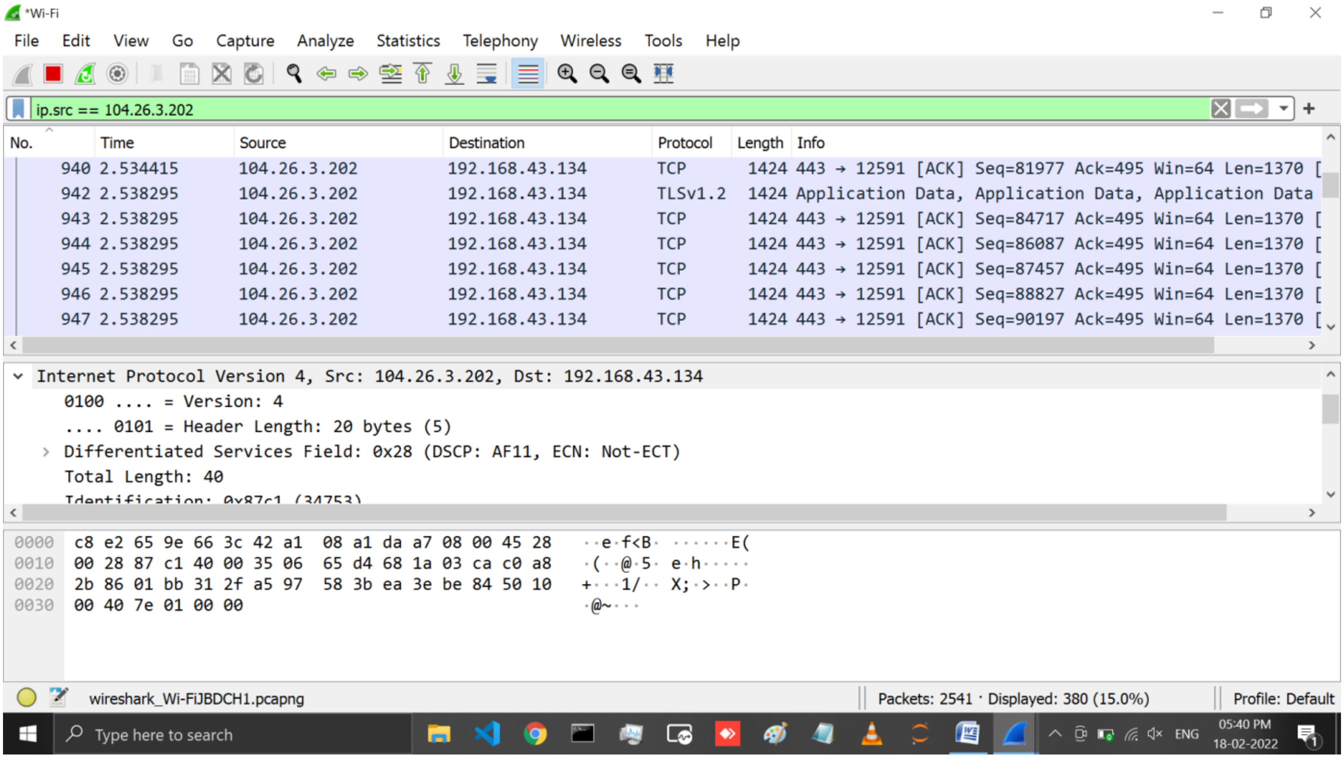
No.	Time	Source	Destination	Protocol	Length	Info
5	2.015073	192.168.43.134	104.26.3.202	TLSv1.2	146	Application Data
6	2.015232	192.168.43.134	104.26.3.202	TLSv1.2	93	Application Data
9	2.018054	192.168.43.134	104.26.3.202	TLSv1.2	146	Application Data
13	2.019167	192.168.43.134	104.26.3.202	TLSv1.2	146	Application Data
23	2.099002	104.26.3.202	192.168.43.134	TCP	54	443 → 12591 [ACK] Seq=1 Ack=93 Win=64 Len=0
24	2.099655	104.26.3.202	192.168.43.134	TCP	54	443 → 12591 [ACK] Seq=1 Ack=132 Win=64 Len=0
25	2.099655	104.26.3.202	192.168.43.134	TCP	54	443 → 12591 [ACK] Seq=1 Ack=224 Win=64 Len=0

```
˅ Internet Protocol Version 4, Src: 192.168.43.134, Dst: 104.26.3.202
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 79
    Identification: 0x86d4 (34516)
```

```
0000  42 a1 08 a1 da a7 c8 e2  65 9e 66 3c 08 00 45 00   B······· e·f<··E·
0010  00 4f 86 d4 40 00 80 06  00 00 c0 a8 2b 86 68 1a   ·O··@··· ····+·h·
0020  03 ca 31 2f 01 bb ea 3e  be 84 a5 97 58 3b 50 18   ··1/···> ····X;P·
0030  01 00 58 54 00 00 17 03  03 00 22 af e0 d9 03 35   ··XT···· ··"····5
0040  c8 e3 81 11 16 9f 73 67  19 61 f4 6a b1 a2 16 b5   ······sg ·a·j····
0050  87 57 55 1e 6d 09 3d c4  44 75 c9 41 ea            ·WU·m·=· Du·A·
```

Total Length (ip.len), 2 bytes | Packets: 2475 · Displayed: 450 (18.2%) | Profile: Default

We can even filter the packets based on the IP address using the command ***“ip.addr == 104.26.3.202”*** this command will filter the packets which includes 104.26.3.202 as source or destination.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search
ENG
05:40 PM
18-02-2022

ip.src == 104.26.3.202

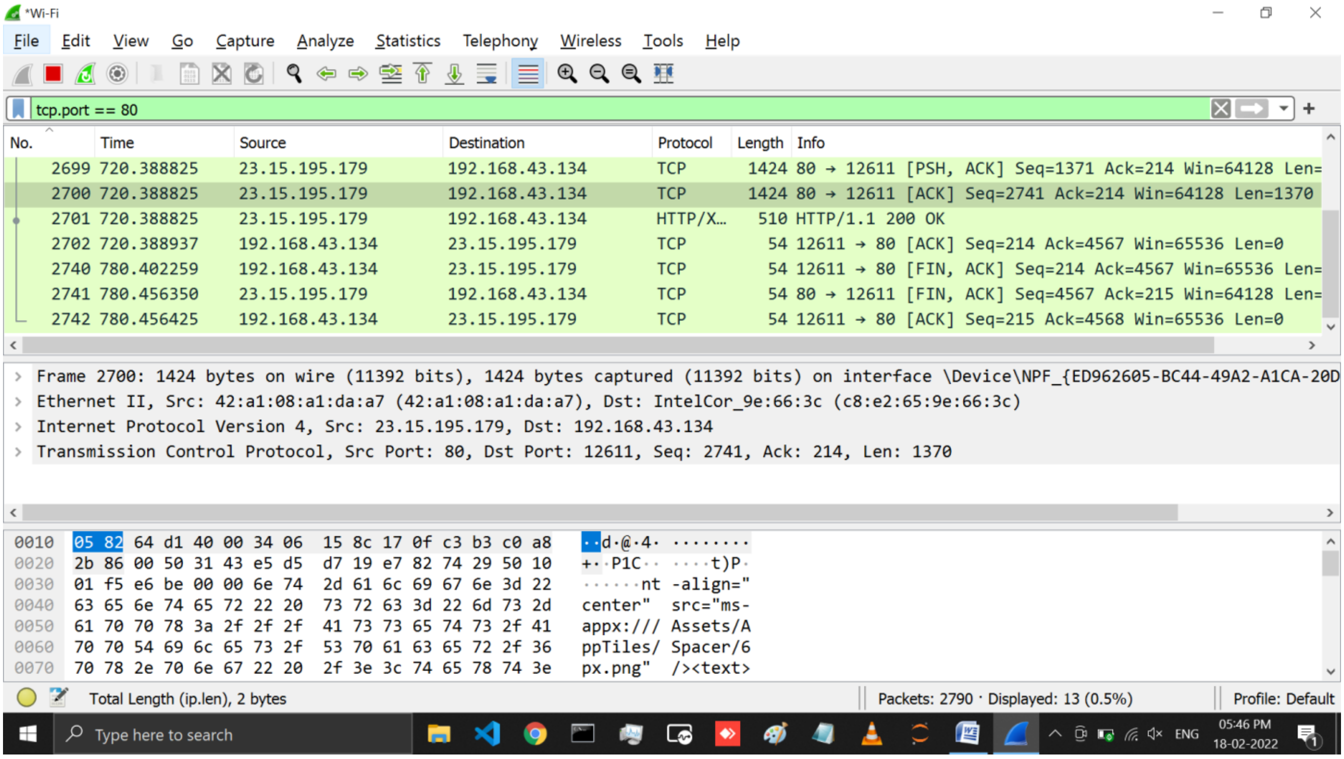
```
No.   Time      Source        Destination     Protocol Length Info
  940 2.534415  104.26.3.202  192.168.43.134  TCP      1424 443 → 12591 [ACK] Seq=81977 Ack=495 Win=64 Len=1370 [
  942 2.538295  104.26.3.202  192.168.43.134  TLSv1.2  1424 Application Data, Application Data, Application Data
  943 2.538295  104.26.3.202  192.168.43.134  TCP      1424 443 → 12591 [ACK] Seq=84717 Ack=495 Win=64 Len=1370 [
  944 2.538295  104.26.3.202  192.168.43.134  TCP      1424 443 → 12591 [ACK] Seq=86087 Ack=495 Win=64 Len=1370 [
  945 2.538295  104.26.3.202  192.168.43.134  TCP      1424 443 → 12591 [ACK] Seq=87457 Ack=495 Win=64 Len=1370 [
  946 2.538295  104.26.3.202  192.168.43.134  TCP      1424 443 → 12591 [ACK] Seq=88827 Ack=495 Win=64 Len=1370 [
  947 2.538295  104.26.3.202  192.168.43.134  TCP      1424 443 → 12591 [ACK] Seq=90197 Ack=495 Win=64 Len=1370 [
```

```
Internet Protocol Version 4, Src: 104.26.3.202, Dst: 192.168.43.134
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x28 (DSCP: AF11, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x87c1 (34753)
```

```
0000  c8 e2 65 9e 66 3c 42 a1  08 a1 da a7 08 00 45 28   ··e·f<B· ······E(
0010  00 28 87 c1 40 00 35 06  65 d4 68 1a 03 ca c0 a8   ·(··@·5· e·h·····
0020  2b 86 01 bb 31 2f a5 97  58 3b ea 3e be 84 50 10   +···1/·· X;·>··P·
0030  00 40 7e 01 00 00                                  ·@~···
```

wireshark_Wi-FiJBDCH1.pcapng | Packets: 2541 · Displayed: 380 (15.0%) | Profile: Default

We can filter the packets based on the source destination as ***"ip.src == 104.26.3.202"*** and this willshow the packets for which the source is ***104.26.3.202***


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search
ENG
05:46 PM
18-02-2022

tcp.port == 80

```
No.   Time        Source          Destination     Protocol Length Info
 2699 720.388825  23.15.195.179   192.168.43.134  TCP      1424 80 → 12611 [PSH, ACK] Seq=1371 Ack=214 Win=64128 Len=
 2700 720.388825  23.15.195.179   192.168.43.134  TCP      1424 80 → 12611 [ACK] Seq=2741 Ack=214 Win=64128 Len=1370
 2701 720.388825  23.15.195.179   192.168.43.134  HTTP/X…   510 HTTP/1.1 200 OK
 2702 720.388937  192.168.43.134  23.15.195.179   TCP        54 12611 → 80 [ACK] Seq=214 Ack=4567 Win=65536 Len=0
 2740 780.402259  192.168.43.134  23.15.195.179   TCP        54 12611 → 80 [FIN, ACK] Seq=214 Ack=4567 Win=65536 Len=
 2741 780.456350  23.15.195.179   192.168.43.134  TCP        54 80 → 12611 [FIN, ACK] Seq=4567 Ack=215 Win=64128 Len=
 2742 780.456425  192.168.43.134  23.15.195.179   TCP        54 12611 → 80 [ACK] Seq=215 Ack=4568 Win=65536 Len=0
```

```
> Frame 2700: 1424 bytes on wire (11392 bits), 1424 bytes captured (11392 bits) on interface \Device\NPF_{ED962605-BC44-49A2-A1CA-20D
> Ethernet II, Src: 42:a1:08:a1:da:a7 (42:a1:08:a1:da:a7), Dst: IntelCor_9e:66:3c (c8:e2:65:9e:66:3c)
> Internet Protocol Version 4, Src: 23.15.195.179, Dst: 192.168.43.134
> Transmission Control Protocol, Src Port: 80, Dst Port: 12611, Seq: 2741, Ack: 214, Len: 1370
```

```
0010  05 82 64 d1 40 00 34 06  15 8c 17 0f c3 b3 c0 a8   ··d·@·4· ········
0020  2b 86 00 50 31 43 e5 d5  d7 19 e7 82 74 29 50 10   +··P1C·· ····t)P·
0030  01 f5 e6 be 00 00 6e 74  2d 61 6c 69 67 6e 3d 22   ······nt -align="
0040  63 65 6e 74 65 72 22 20  73 72 63 3d 22 6d 73 2d   center"  src="ms-
0050  61 70 70 78 3a 2f 2f 2f  41 73 73 65 74 73 2f 41   appx:/// Assets/A
0060  70 70 54 69 6c 65 73 2f  53 70 61 63 65 72 2f 36   ppTiles/ Spacer/6
0070  70 78 2e 70 6e 67 22 20  2f 3e 3c 74 65 78 74 3e   px.png"  /><text>
```

Total Length (ip.len), 2 bytes | Packets: 2790 · Displayed: 13 (0.5%) | Profile: Default

We can also filter the packets based on the TCP port number with the following command as ***"tcp.port == 80"*** which will filter the TCP port 80.

LATEST APPLICATIONS

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- To learn network protocol internals
- Cybersecurity professionals often use Wireshark to trace connections, view the contents of suspect network transactions and identify bursts of network traffic.

LEARNING OUTCOME:

with this practical learned about wireshark which is an open source tool for network traffic analyzer it is a tool which sniffs the network and gives the result as the list of packets. We can then analyze this packets and can identify if the network is behaving properly or not. This tools is also used by professionals to identify the attack in a network.

REFERENCES:

1. **https://www.wireshark.org/**
2. **https://www.wireshark.org/docs/**
3. **https://www.wireshark.org/index.html#download**
4. **https://www.youtube.com/watch?v=yC0e0bSSleo**
5. **https://www.comparitech.com/net-admin/wireshark-cheat-sheet/**
6. **https://www.stationx.net/wireshark-cheat-sheet/**