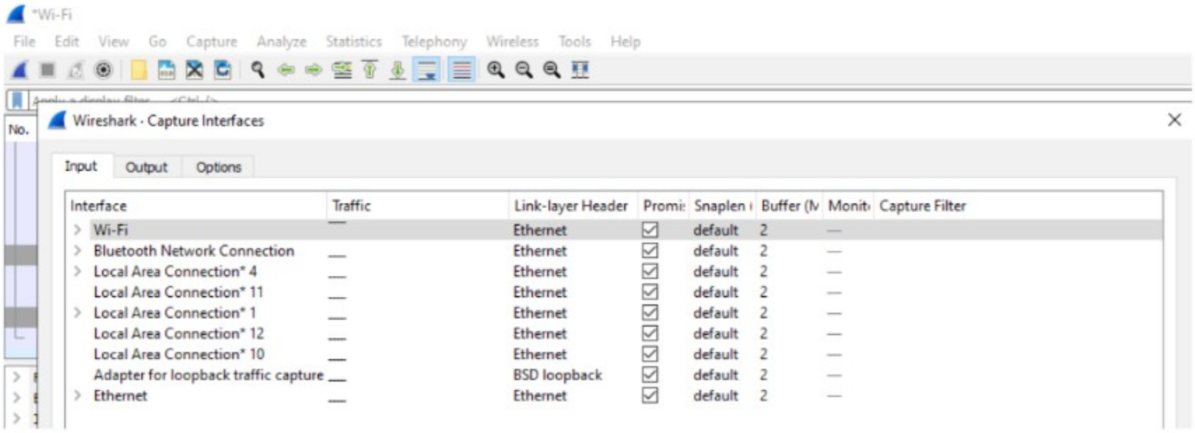
Name:- Alok Bhawankar

Roll no.:- PA06

WMS LAB 4

Title:- Install , configure and demonstrate any one traffic analyzer using sniffing tools such as Wireshark,Aircrack,Airsnort,etc.

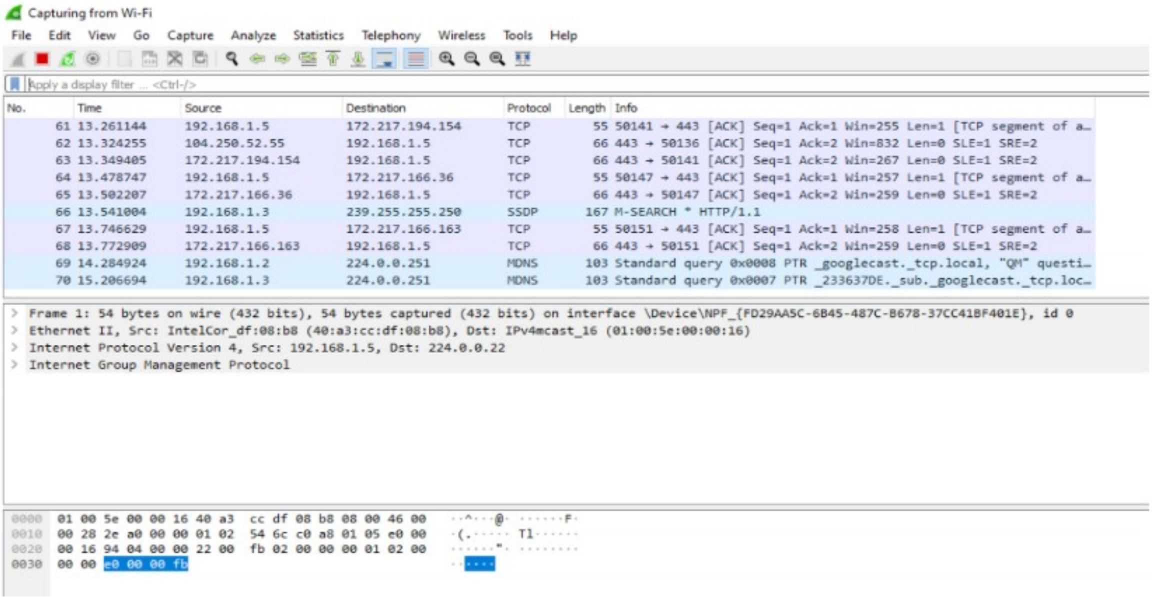
1] List of interfaces:-



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Capture Interfaces
Input Output Options

Interface	Traffic	Link-layer Header	Promi:	Snaplen	Buffer (M	Monit	Capture Filter
Wi-Fi		Ethernet	☑	default	2	—	
Bluetooth Network Connection		Ethernet	☑	default	2	—	
Local Area Connection* 4		Ethernet	☑	default	2	—	
Local Area Connection* 11		Ethernet	☑	default	2	—	
Local Area Connection* 1		Ethernet	☑	default	2	—	
Local Area Connection* 12		Ethernet	☑	default	2	—	
Local Area Connection* 10		Ethernet	☑	default	2	—	
Adapter for loopback traffic capture		BSD loopback	☑	default	2	—	
Ethernet		Ethernet	☑	default	2	—	

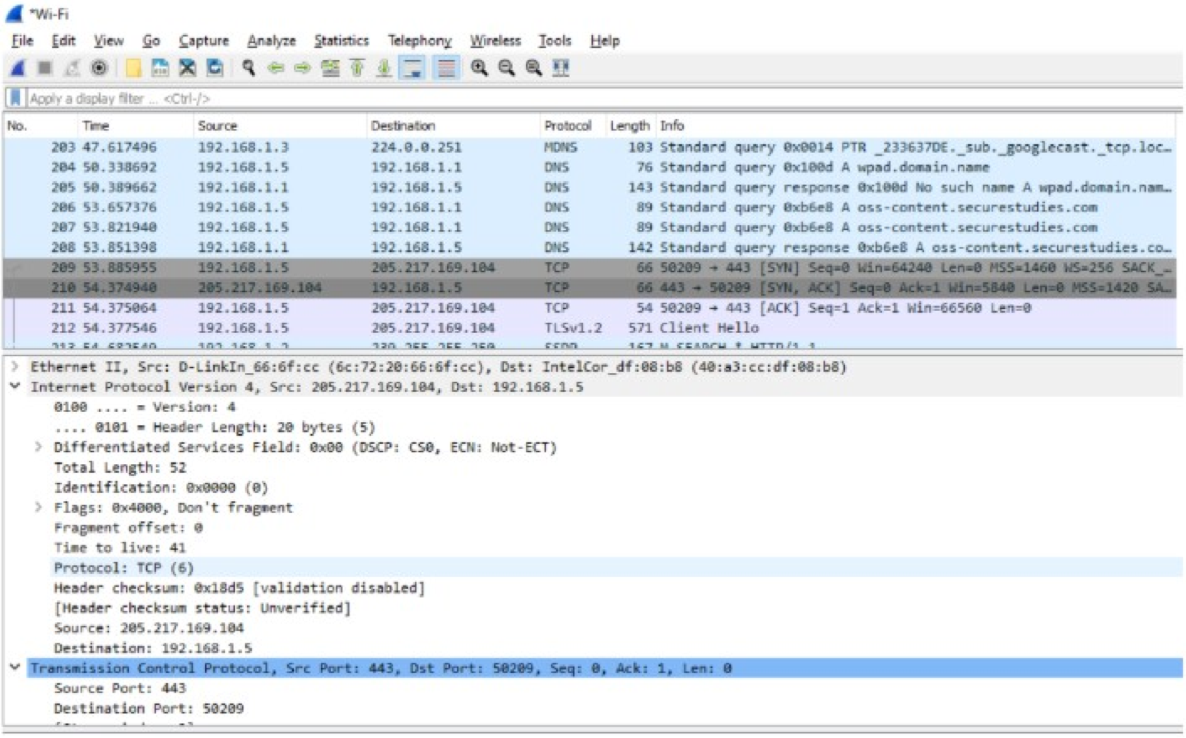
2] Capturing Packets from WIFI:-



Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source           Destination      Protocol Length Info
   61 13.261144  192.168.1.5      172.217.194.154  TCP       55 50141 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a…
   62 13.324255  104.250.52.55    192.168.1.5      TCP       66 443 → 50136 [ACK] Seq=1 Ack=2 Win=832 Len=0 SLE=1 SRE=2
   63 13.349405  172.217.194.154  192.168.1.5      TCP       66 443 → 50141 [ACK] Seq=1 Ack=2 Win=267 Len=0 SLE=1 SRE=2
   64 13.478747  192.168.1.5      172.217.166.36   TCP       55 50147 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [TCP segment of a…
   65 13.502207  172.217.166.36   192.168.1.5      TCP       66 443 → 50147 [ACK] Seq=1 Ack=2 Win=259 Len=0 SLE=1 SRE=2
   66 13.541004  192.168.1.3      239.255.255.250  SSDP     167 M-SEARCH * HTTP/1.1
   67 13.746629  192.168.1.5      172.217.166.163  TCP       55 50151 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a…
   68 13.772909  172.217.166.163  192.168.1.5      TCP       66 443 → 50151 [ACK] Seq=1 Ack=2 Win=259 Len=0 SLE=1 SRE=2
   69 14.284924  192.168.1.2      224.0.0.251      MDNS     103 Standard query 0x0008 PTR _googlecast._tcp.local, "QM" questi…
   70 15.206694  192.168.1.3      224.0.0.251      MDNS     103 Standard query 0x0007 PTR _233637DE._sub._googlecast._tcp.loc…

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{FD29AA5C-6B45-487C-B678-37CC41BF401E}, id 0
> Ethernet II, Src: IntelCor_df:08:b8 (40:a3:cc:df:08:b8), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 224.0.0.22
> Internet Group Management Protocol

0000  01 00 5e 00 00 16 40 a3  cc df 08 b8 08 00 46 00   ··^···@· ······F·
0010  00 28 2e a0 00 00 01 02  54 6c c0 a8 01 05 e0 00   ·(.····· Tl······
0020  00 16 94 04 00 00 22 00  fb 02 00 00 00 01 02 00   ······"· ········
0030  00 00 e0 00 00 fb                                  ······
```

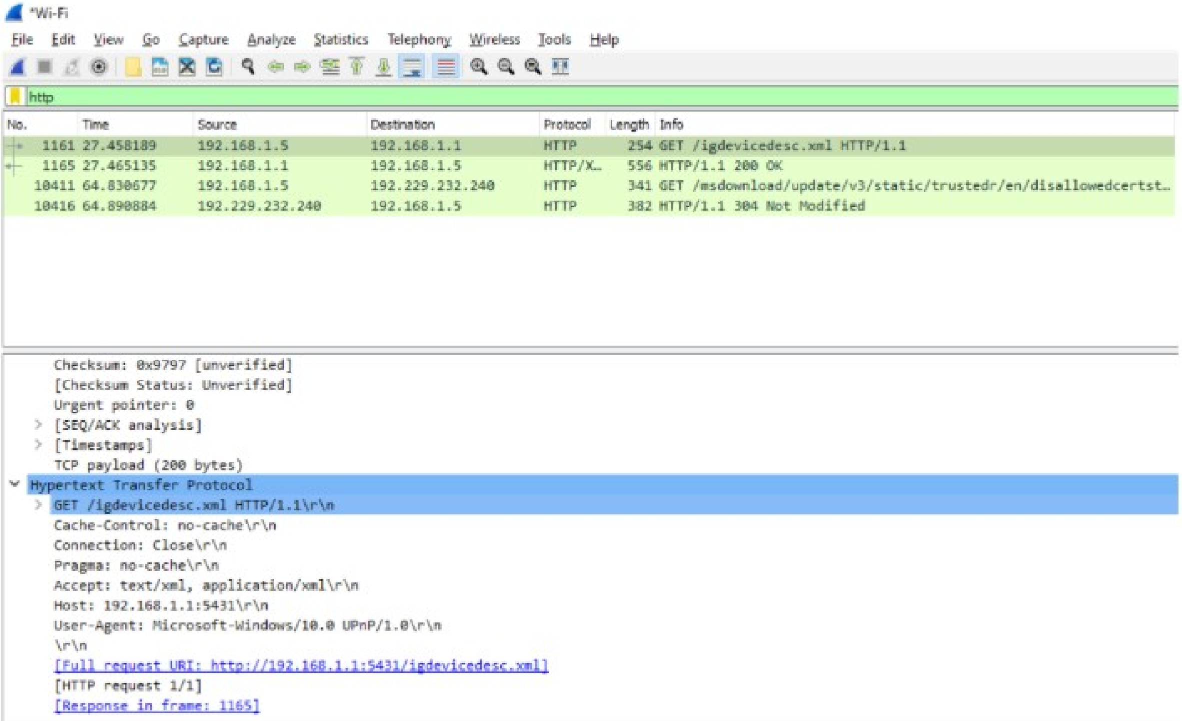
3] Exploring the packet number 210 in detail(TCP):-


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

No.	Time	Source	Destination	Protocol	Length	Info
203	47.617496	192.168.1.3	224.0.0.251	MDNS	103	Standard query 0x0014 PTR _233637DE._sub._googlecast._tcp.loc…
204	50.338692	192.168.1.5	192.168.1.1	DNS	76	Standard query 0x100d A wpad.domain.name
205	50.389662	192.168.1.1	192.168.1.5	DNS	143	Standard query response 0x100d No such name A wpad.domain.nam…
206	53.657376	192.168.1.5	192.168.1.1	DNS	89	Standard query 0xb6e8 A oss-content.securestudies.com
207	53.821940	192.168.1.5	192.168.1.1	DNS	89	Standard query 0xb6e8 A oss-content.securestudies.com
208	53.851398	192.168.1.1	192.168.1.5	DNS	142	Standard query response 0xb6e8 A oss-content.securestudies.co…
209	53.885955	192.168.1.5	205.217.169.104	TCP	66	50209 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_…
210	54.374940	205.217.169.104	192.168.1.5	TCP	66	443 → 50209 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1420 SA…
211	54.375064	192.168.1.5	205.217.169.104	TCP	54	50209 → 443 [ACK] Seq=1 Ack=1 Win=66560 Len=0
212	54.377546	192.168.1.5	205.217.169.104	TLSv1.2	571	Client Hello

```
> Ethernet II, Src: D-LinkIn_66:6f:cc (6c:72:20:66:6f:cc), Dst: IntelCor_df:08:b8 (40:a3:cc:df:08:b8)
v Internet Protocol Version 4, Src: 205.217.169.104, Dst: 192.168.1.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x0000 (0)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 41
    Protocol: TCP (6)
    Header checksum: 0x18d5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 205.217.169.104
    Destination: 192.168.1.5
v Transmission Control Protocol, Src Port: 443, Dst Port: 50209, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 50209
```

4] Filtering Packets using HTTP filter:-

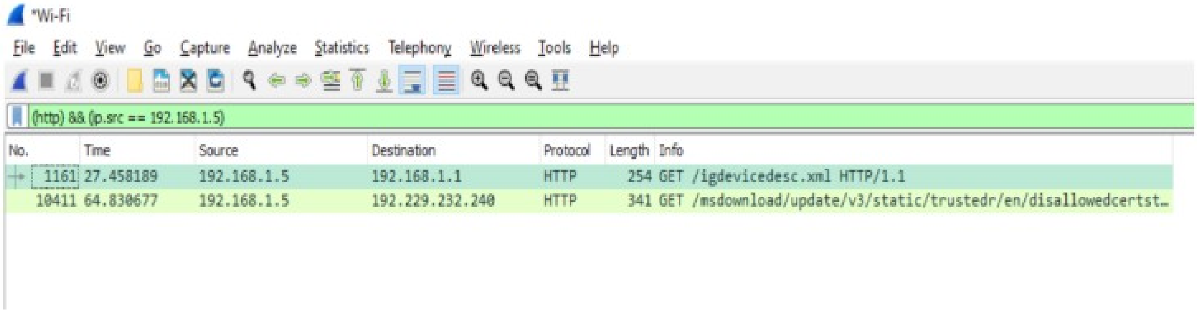

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
1161	27.458189	192.168.1.5	192.168.1.1	HTTP	254	GET /igdevicedesc.xml HTTP/1.1
1165	27.465135	192.168.1.1	192.168.1.5	HTTP/X…	556	HTTP/1.1 200 OK
10411	64.830677	192.168.1.5	192.229.232.240	HTTP	341	GET /msdownload/update/v3/static/trustedr/en/disallowedcertst…
10416	64.890884	192.229.232.240	192.168.1.5	HTTP	382	HTTP/1.1 304 Not Modified

```
    Checksum: 0x9797 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (200 bytes)
v Hypertext Transfer Protocol
  > GET /igdevicedesc.xml HTTP/1.1\r\n
    Cache-Control: no-cache\r\n
    Connection: Close\r\n
    Pragma: no-cache\r\n
    Accept: text/xml, application/xml\r\n
    Host: 192.168.1.1:5431\r\n
    User-Agent: Microsoft-Windows/10.0 UPnP/1.0\r\n
    \r\n
    [Full request URI: http://192.168.1.1:5431/igdevicedesc.xml]
    [HTTP request 1/1]
    [Response in frame: 1165]
```

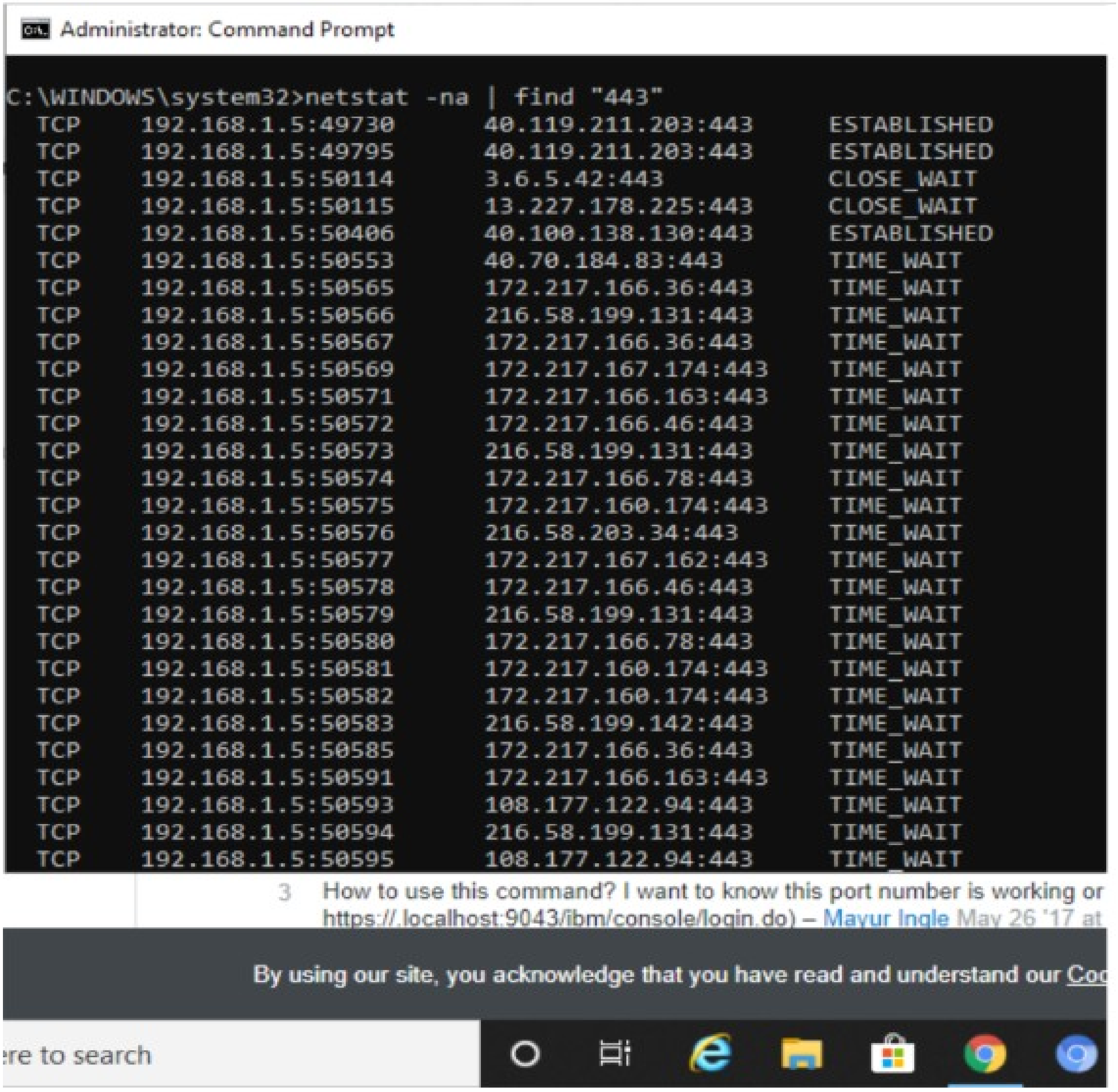
5] Filtering HTTP with source IP:-


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

(http) && (ip.src == 192.168.1.5)

No.	Time	Source	Destination	Protocol	Length	Info
1161	27.458189	192.168.1.5	192.168.1.1	HTTP	254	GET /igdevicedesc.xml HTTP/1.1
10411	64.830677	192.168.1.5	192.229.232.240	HTTP	341	GET /msdownload/update/v3/static/trustedr/en/disallowedcertst…

6] Listning to particular ports:-



```
C:\WINDOWS\system32>netstat -na | find "443"
  TCP    192.168.1.5:49730      40.119.211.203:443     ESTABLISHED
  TCP    192.168.1.5:49795      40.119.211.203:443     ESTABLISHED
  TCP    192.168.1.5:50114      3.6.5.42:443           CLOSE_WAIT
  TCP    192.168.1.5:50115      13.227.178.225:443     CLOSE_WAIT
  TCP    192.168.1.5:50406      40.100.138.130:443     ESTABLISHED
  TCP    192.168.1.5:50553      40.70.184.83:443       TIME_WAIT
  TCP    192.168.1.5:50565      172.217.166.36:443     TIME_WAIT
  TCP    192.168.1.5:50566      216.58.199.131:443     TIME_WAIT
  TCP    192.168.1.5:50567      172.217.166.36:443     TIME_WAIT
  TCP    192.168.1.5:50569      172.217.167.174:443    TIME_WAIT
  TCP    192.168.1.5:50571      172.217.166.163:443    TIME_WAIT
  TCP    192.168.1.5:50572      172.217.166.46:443     TIME_WAIT
  TCP    192.168.1.5:50573      216.58.199.131:443     TIME_WAIT
  TCP    192.168.1.5:50574      172.217.166.78:443     TIME_WAIT
  TCP    192.168.1.5:50575      172.217.160.174:443    TIME_WAIT
  TCP    192.168.1.5:50576      216.58.203.34:443      TIME_WAIT
  TCP    192.168.1.5:50577      172.217.167.162:443    TIME_WAIT
  TCP    192.168.1.5:50578      172.217.166.46:443     TIME_WAIT
  TCP    192.168.1.5:50579      216.58.199.131:443     TIME_WAIT
  TCP    192.168.1.5:50580      172.217.166.78:443     TIME_WAIT
  TCP    192.168.1.5:50581      172.217.160.174:443    TIME_WAIT
  TCP    192.168.1.5:50582      172.217.160.174:443    TIME_WAIT
  TCP    192.168.1.5:50583      216.58.199.142:443     TIME_WAIT
  TCP    192.168.1.5:50585      172.217.166.36:443     TIME_WAIT
  TCP    192.168.1.5:50591      172.217.166.163:443    TIME_WAIT
  TCP    192.168.1.5:50593      108.177.122.94:443     TIME_WAIT
  TCP    192.168.1.5:50594      216.58.199.131:443     TIME_WAIT
  TCP    192.168.1.5:50595      108.177.122.94:443     TIME_WAIT
```

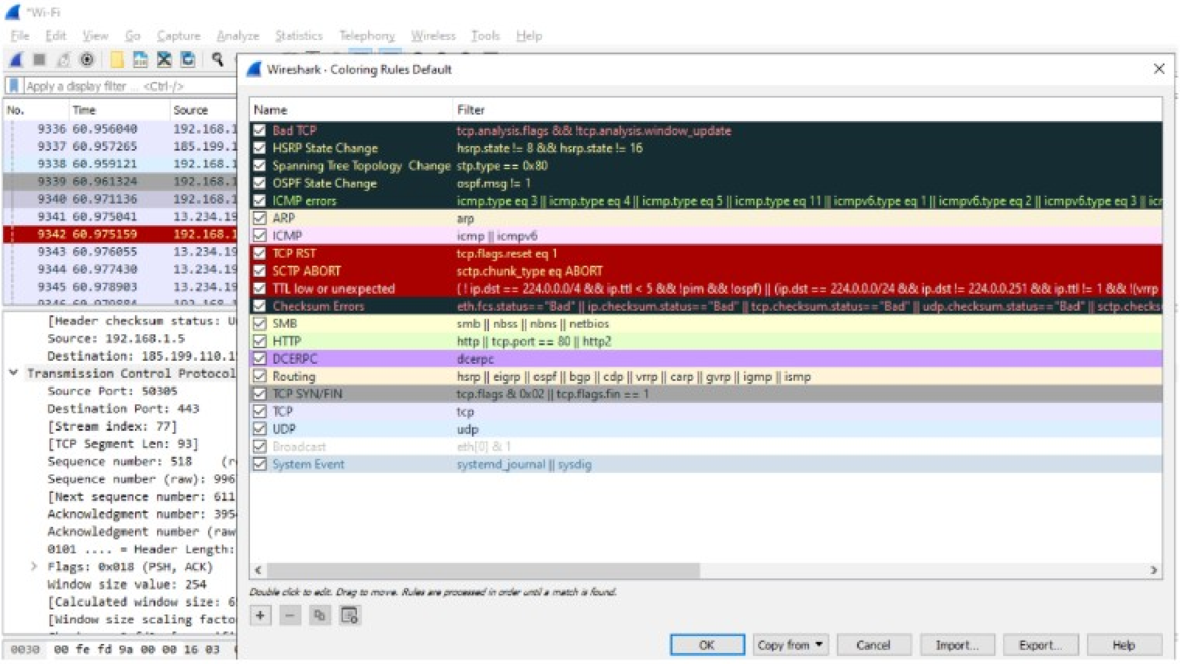
3 How to use this command? I want to know this port number is working or https://.localhost:9043/ibm/console/login.do) – Mayur Ingle May 26 '17 at

By using our site, you acknowledge that you have read and understand our Coo

7]

Colouring Rules:-

1

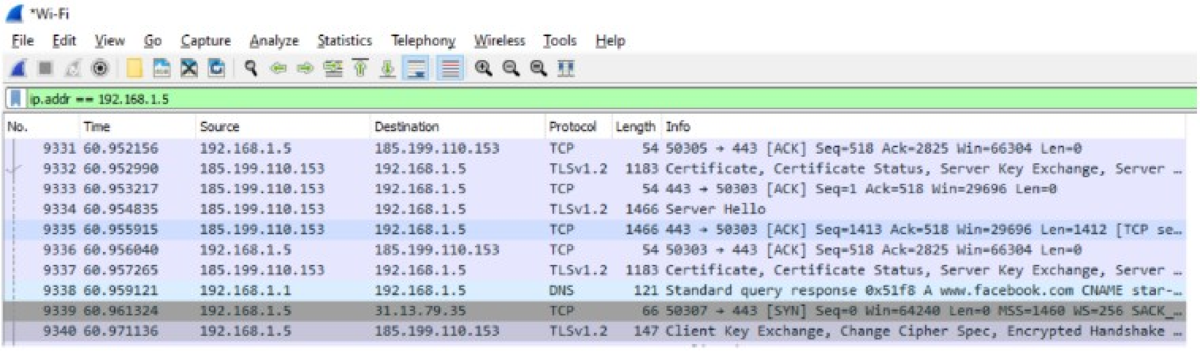

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Coloring Rules Default

```
No.     Time        Source
   9336 60.956040   192.168.1
   9337 60.957265   185.199.1
   9338 60.959121   192.168.1
   9339 60.961324   192.168.1
   9340 60.971136   192.168.1
   9341 60.975041   13.234.19
   9342 60.975159   192.168.1
   9343 60.976055   13.234.19
   9344 60.977430   13.234.19
   9345 60.978903   13.234.19

      [Header checksum status: U
      Source: 192.168.1.5
      Destination: 185.199.110.1
  ˅ Transmission Control Protocol
      Source Port: 50305
      Destination Port: 443
      [Stream index: 77]
      [TCP Segment Len: 93]
      Sequence number: 518    (r
      Sequence number (raw): 996
      [Next sequence number: 611
      Acknowledgment number: 395
      Acknowledgment number (raw
      0101 .... = Header Length:
    > Flags: 0x018 (PSH, ACK)
      Window size value: 254
      [Calculated window size: 6
      [Window size scaling facto

0030  00 fe fd 9a 00 00 16 03
```

Name	Filter
☑ Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update
☑ 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 || icr
☑ 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
☑ Checksum Errors	eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checks
☑ 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.

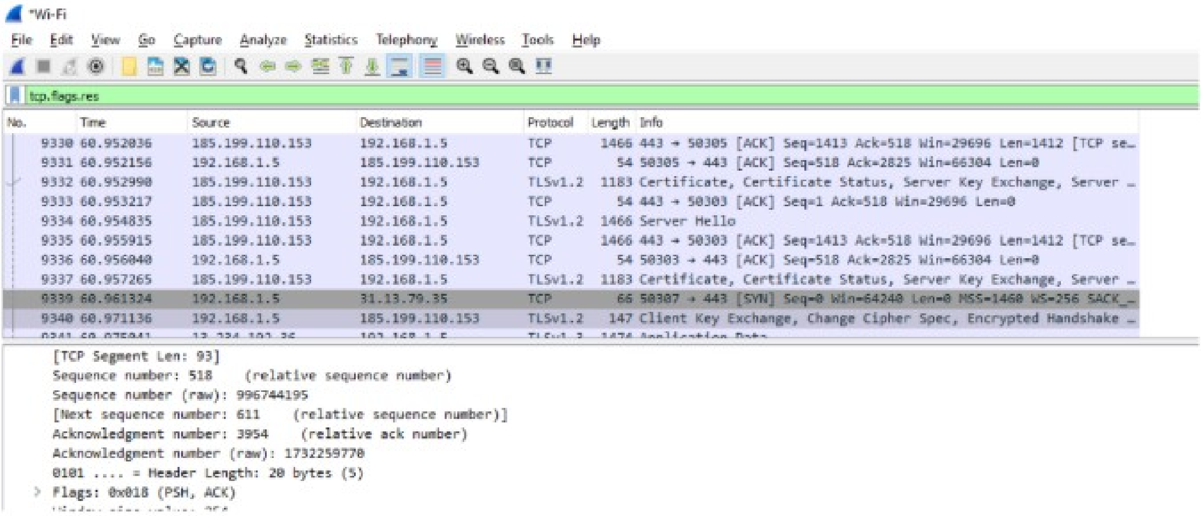
8] Applying IP filter to IP address 192.168.1.5:-


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

ip.addr == 192.168.1.5

```
No.    Time        Source           Destination      Protocol  Length Info
  9331 60.952156   192.168.1.5      185.199.110.153  TCP          54 50305 → 443 [ACK] Seq=518 Ack=2825 Win=66304 Len=0
  9332 60.952990   185.199.110.153  192.168.1.5      TLSv1.2    1183 Certificate, Certificate Status, Server Key Exchange, Server …
  9333 60.953217   185.199.110.153  192.168.1.5      TCP          54 443 → 50303 [ACK] Seq=1 Ack=518 Win=29696 Len=0
  9334 60.954835   185.199.110.153  192.168.1.5      TLSv1.2    1466 Server Hello
  9335 60.955915   185.199.110.153  192.168.1.5      TCP        1466 443 → 50303 [ACK] Seq=1413 Ack=518 Win=29696 Len=1412 [TCP se…
  9336 60.956040   192.168.1.5      185.199.110.153  TCP          54 50303 → 443 [ACK] Seq=518 Ack=2825 Win=66304 Len=0
  9337 60.957265   185.199.110.153  192.168.1.5      TLSv1.2    1183 Certificate, Certificate Status, Server Key Exchange, Server …
  9338 60.959121   192.168.1.1      192.168.1.5      DNS         121 Standard query response 0x51f8 A www.facebook.com CNAME star-…
  9339 60.961324   192.168.1.5      31.13.79.35      TCP          66 50307 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_…
  9340 60.971136   192.168.1.5      185.199.110.153  TLSv1.2     147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake …
```

9] Filter for displaying TCP falgs:-

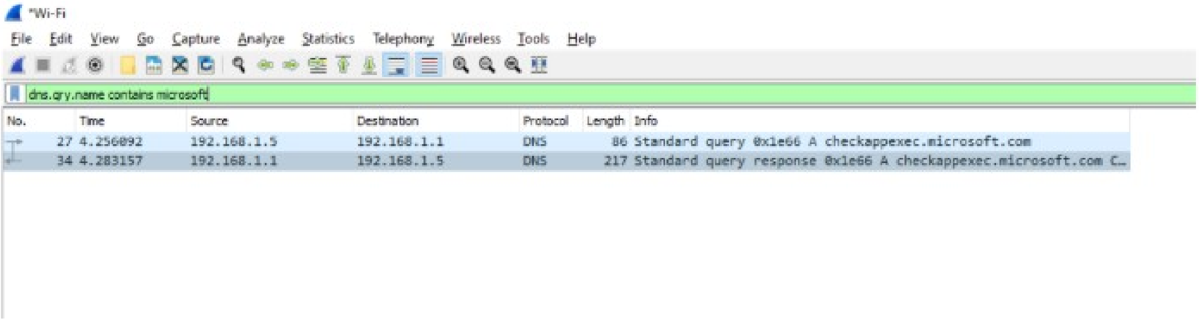

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags.res
```

```
No.   Time       Source           Destination      Protocol Length Info
 9330 60.952036  185.199.110.153  192.168.1.5      TCP      1466 443 → 50305 [ACK] Seq=1413 Ack=518 Win=29696 Len=1412 [TCP se…
 9331 60.952156  192.168.1.5      185.199.110.153  TCP        54 50305 → 443 [ACK] Seq=518 Ack=2825 Win=66304 Len=0
 9332 60.952990  185.199.110.153  192.168.1.5      TLSv1.2  1183 Certificate, Certificate Status, Server Key Exchange, Server …
 9333 60.953217  185.199.110.153  192.168.1.5      TCP        54 443 → 50303 [ACK] Seq=1 Ack=518 Win=29696 Len=0
 9334 60.954835  185.199.110.153  192.168.1.5      TLSv1.2  1466 Server Hello
 9335 60.955915  185.199.110.153  192.168.1.5      TCP      1466 443 → 50303 [ACK] Seq=1413 Ack=518 Win=29696 Len=1412 [TCP se…
 9336 60.956040  192.168.1.5      185.199.110.153  TCP        54 50303 → 443 [ACK] Seq=518 Ack=2825 Win=66304 Len=0
 9337 60.957265  185.199.110.153  192.168.1.5      TLSv1.2  1183 Certificate, Certificate Status, Server Key Exchange, Server …
 9339 60.961324  192.168.1.5      31.13.79.35      TCP        66 50307 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_…
 9340 60.971136  192.168.1.5      185.199.110.153  TLSv1.2   147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake …
```

```
    [TCP Segment Len: 93]
    Sequence number: 518    (relative sequence number)
    Sequence number (raw): 996744195
    [Next sequence number: 611    (relative sequence number)]
    Acknowledgment number: 3954    (relative ack number)
    Acknowledgment number (raw): 1732259770
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
```

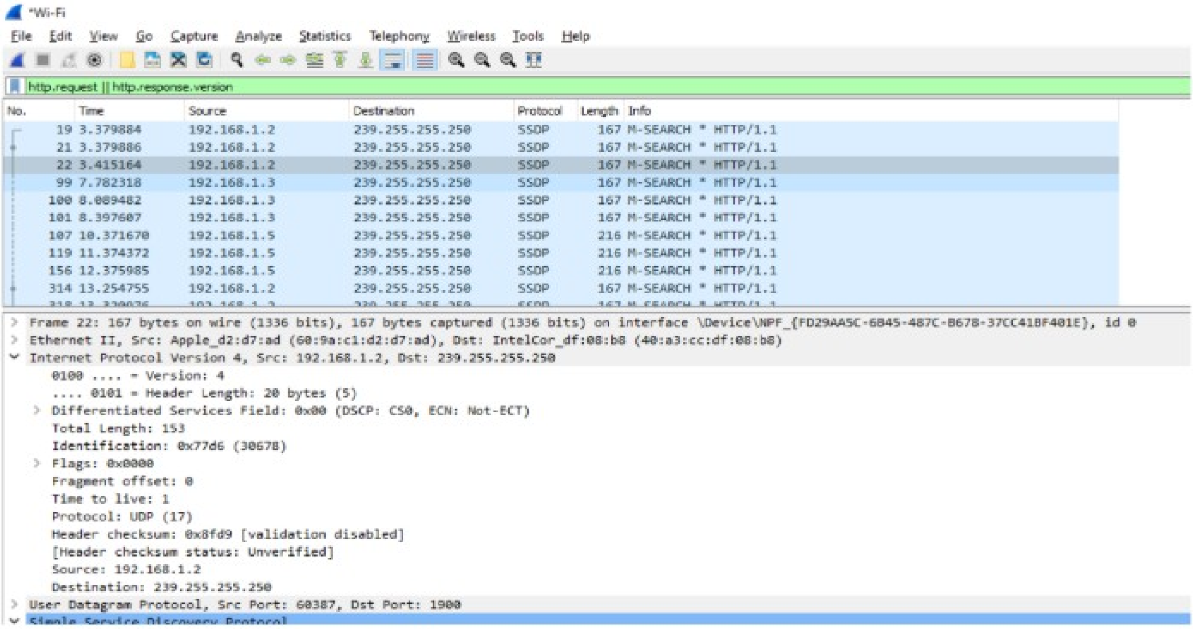
10] DNS query contains window:-


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

```
dns.qry.name contains microsoft
```

```
No.   Time      Source       Destination  Protocol Length Info
   27 4.256092  192.168.1.5  192.168.1.1  DNS        86 Standard query 0x1e66 A checkappexec.microsoft.com
   34 4.283157  192.168.1.1  192.168.1.5  DNS       217 Standard query response 0x1e66 A checkappexec.microsoft.com C…
```

11] HTTP Request and Response Filter:-

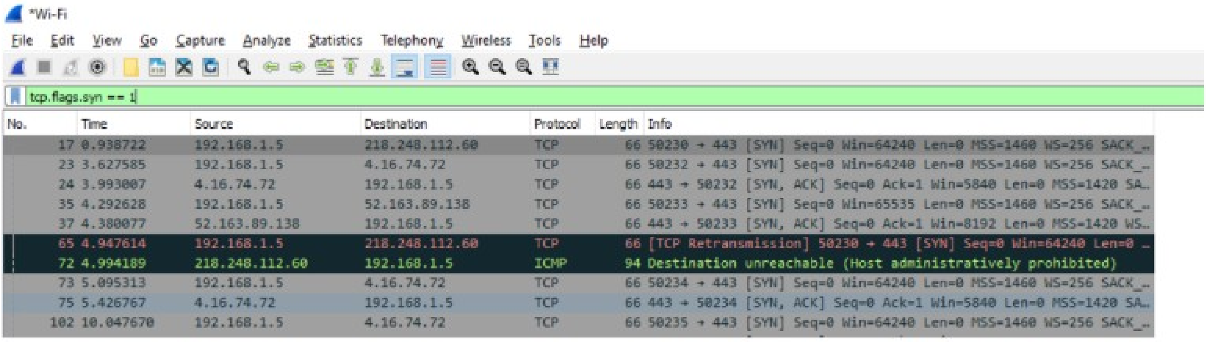

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request || http.response.version
```

```
No.   Time       Source       Destination      Protocol Length Info
   19 3.379884   192.168.1.2  239.255.255.250  SSDP      167 M-SEARCH * HTTP/1.1
   21 3.379886   192.168.1.2  239.255.255.250  SSDP      167 M-SEARCH * HTTP/1.1
   22 3.415164   192.168.1.2  239.255.255.250  SSDP      167 M-SEARCH * HTTP/1.1
   99 7.782318   192.168.1.3  239.255.255.250  SSDP      167 M-SEARCH * HTTP/1.1
  100 8.089482   192.168.1.3  239.255.255.250  SSDP      167 M-SEARCH * HTTP/1.1
  101 8.397607   192.168.1.3  239.255.255.250  SSDP      167 M-SEARCH * HTTP/1.1
  107 10.371670  192.168.1.5  239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
  119 11.374372  192.168.1.5  239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
  156 12.375985  192.168.1.5  239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
  314 13.254755  192.168.1.2  239.255.255.250  SSDP      167 M-SEARCH * HTTP/1.1
```

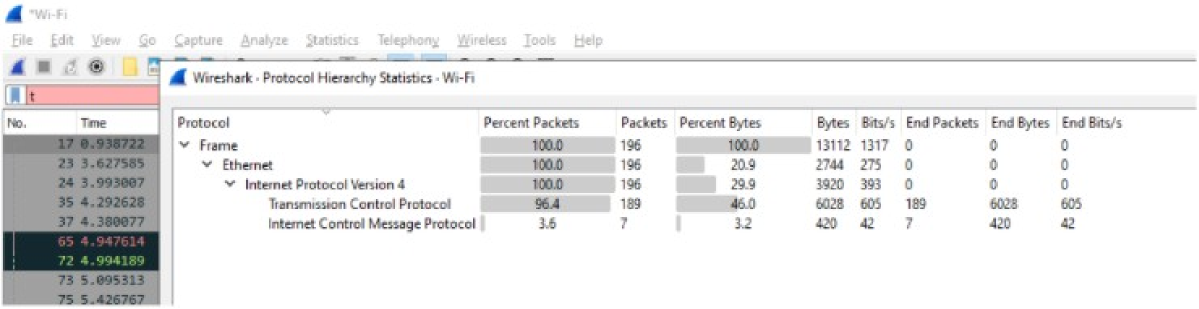
```
> Frame 22: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface \Device\NPF_{FD29AA5C-6845-487C-B678-37CC418F401E}, id 0
> Ethernet II, Src: Apple_d2:d7:ad (60:9a:c1:d2:d7:ad), Dst: IntelCor_df:08:b8 (40:a3:cc:df:08:b8)
v Internet Protocol Version 4, Src: 192.168.1.2, Dst: 239.255.255.250
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 153
    Identification: 0x77d6 (30678)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0x8fd9 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.2
    Destination: 239.255.255.250
> User Datagram Protocol, Src Port: 60387, Dst Port: 1900
v Simple Service Discovery Protocol
```

12] TCP Flag SYN Filter:-


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

```
tcp.flags.syn == 1

No.   Time        Source          Destination     Protocol Length Info
   17 0.938722    192.168.1.5     218.248.112.60  TCP      66 50230 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_…
   23 3.627585    192.168.1.5     4.16.74.72      TCP      66 50232 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_…
   24 3.993007    4.16.74.72      192.168.1.5     TCP      66 443 → 50232 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1420 SA…
   35 4.292628    192.168.1.5     52.163.89.138   TCP      66 50233 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_…
   37 4.380077    52.163.89.138   192.168.1.5     TCP      66 443 → 50233 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1420 WS…
   65 4.947614    192.168.1.5     218.248.112.60  TCP      66 [TCP Retransmission] 50230 → 443 [SYN] Seq=0 Win=64240 Len=0 …
   72 4.994189    218.248.112.60  192.168.1.5     ICMP     94 Destination unreachable (Host administratively prohibited)
   73 5.095313    192.168.1.5     4.16.74.72      TCP      66 50234 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_…
   75 5.426767    4.16.74.72      192.168.1.5     TCP      66 443 → 50234 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1420 SA…
  102 10.047670   192.168.1.5     4.16.74.72      TCP      66 50235 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_…
```

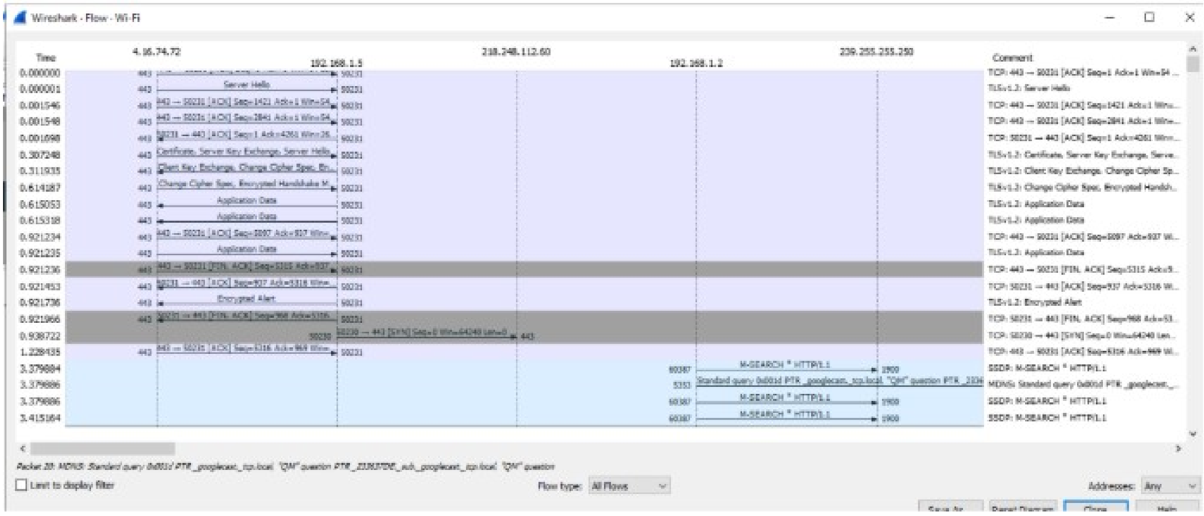
13] Protocol Hirearchy Statistics:-



Wireshark · Protocol Hierarchy Statistics · Wi-Fi

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	196	100.0	13112	1317	0	0	0
Ethernet	100.0	196	20.9	2744	275	0	0	0
Internet Protocol Version 4	100.0	196	29.9	3920	393	0	0	0
Transmission Control Protocol	96.4	189	46.0	6028	605	189	6028	605
Internet Control Message Protocol	3.6	7	3.2	420	42	7	420	42

14] Flow Graph:-



```
Time      Comment
0.000000  TCP: 443 → 50231 [ACK] Seq=1 Ack=1 Win=54 ...
0.000001  TLSv1.2: Server Hello
0.001546  TCP: 443 → 50231 [ACK] Seq=1421 Ack=1 Win=...
0.001548  TCP: 443 → 50231 [ACK] Seq=2841 Ack=1 Win=...
0.001698  TCP: 50231 → 443 [ACK] Seq=1 Ack=4261 Win=...
0.307248  TLSv1.2: Certificate, Server Key Exchange, Serve...
0.311935  TLSv1.2: Client Key Exchange, Change Cipher Sp...
0.614187  TLSv1.2: Change Cipher Spec, Encrypted Handsh...
0.615053  TLSv1.2: Application Data
0.615318  TLSv1.2: Application Data
0.921234  TCP: 443 → 50231 [ACK] Seq=5097 Ack=937 Wi...
0.921235  TLSv1.2: Application Data
0.921236  TCP: 443 → 50231 [FIN, ACK] Seq=5315 Ack=9...
0.921453  TCP: 50231 → 443 [ACK] Seq=937 Ack=5316 Wi...
0.921736  TLSv1.2: Encrypted Alert
0.921966  TCP: 50231 → 443 [FIN, ACK] Seq=968 Ack=53...
0.938722  TCP: 50230 → 443 [SYN] Seq=0 Win=64240 Len...
1.228435  TCP: 443 → 50231 [ACK] Seq=5316 Ack=969 Wi...
3.379884  SSDP: M-SEARCH * HTTP/1.1
3.379886  MDNS: Standard query 0x001d PTR _googlecast._...
3.379886  SSDP: M-SEARCH * HTTP/1.1
3.415164  SSDP: M-SEARCH * HTTP/1.1

Packet 20: MDNS: Standard query 0x001d PTR _googlecast._tcp.local, "QM" question PTR _233B7DE._sub._googlecast._tcp.local, "QM" question
```