PRACTICAL 6

Name: Isha Raut

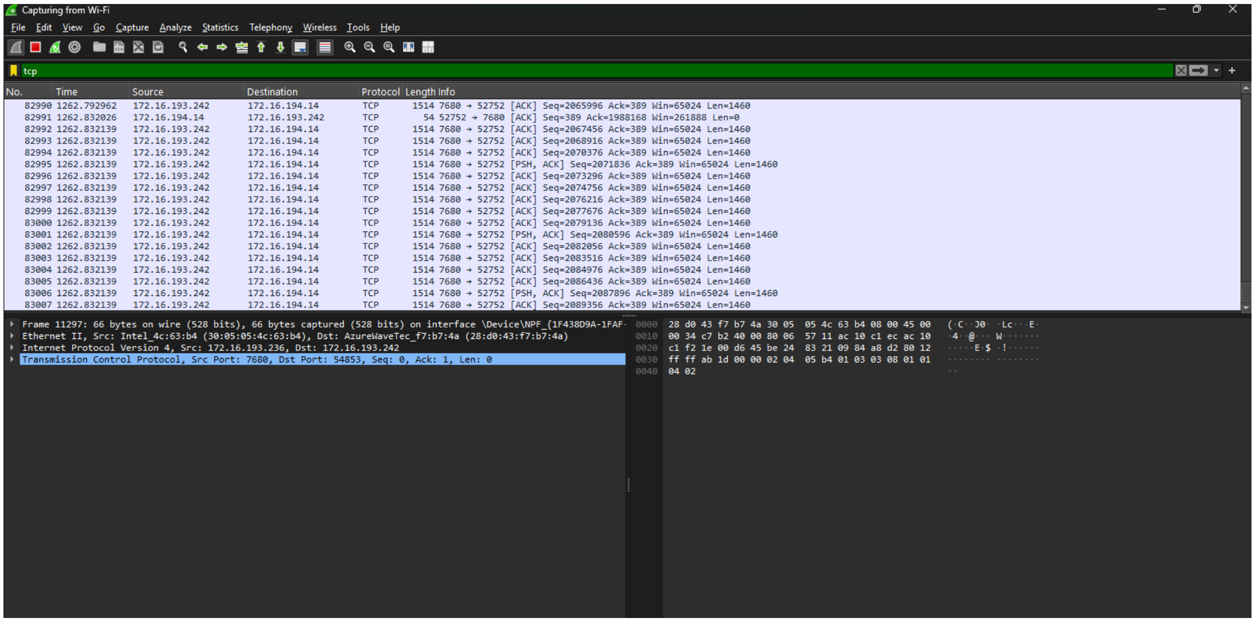
Section: A4

Batch: B2

Roll No: 23

AIM: Wire shark traffic analyser.

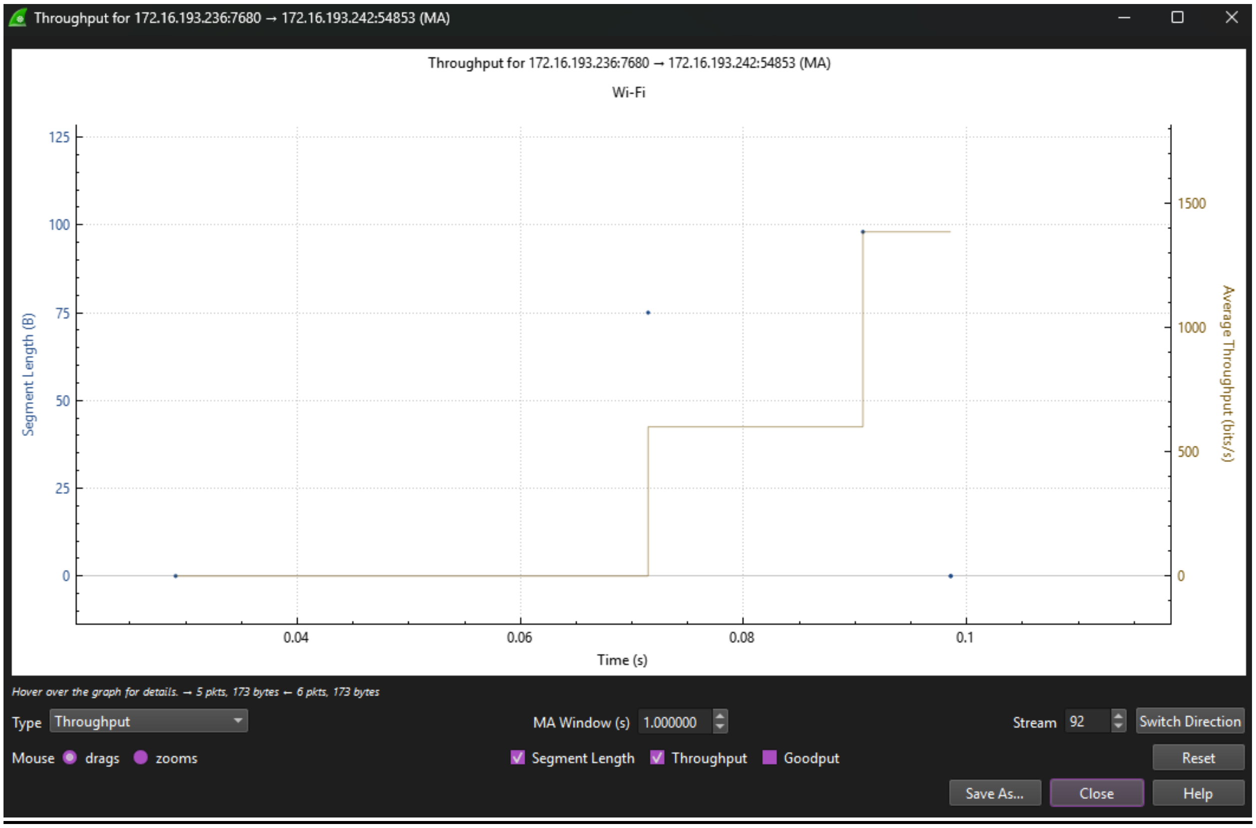
1.TCP


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.   Time        Source          Destination     Protocol Length Info
82990 1262.792962 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [ACK] Seq=2065996 Ack=389 Win=65024 Len=1460
82991 1262.832026 172.16.194.14   172.16.193.242  TCP        54 52752 → 7680 [ACK] Seq=389 Ack=1988168 Win=261888 Len=0
82992 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [ACK] Seq=2067456 Ack=389 Win=65024 Len=1460
82993 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [ACK] Seq=2068916 Ack=389 Win=65024 Len=1460
82994 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [ACK] Seq=2070376 Ack=389 Win=65024 Len=1460
82995 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [PSH, ACK] Seq=2071836 Ack=389 Win=65024 Len=1460
82996 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [ACK] Seq=2073296 Ack=389 Win=65024 Len=1460
82997 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [ACK] Seq=2074756 Ack=389 Win=65024 Len=1460
82998 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [ACK] Seq=2076216 Ack=389 Win=65024 Len=1460
82999 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [ACK] Seq=2077676 Ack=389 Win=65024 Len=1460
83000 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [ACK] Seq=2079136 Ack=389 Win=65024 Len=1460
83001 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [PSH, ACK] Seq=2080596 Ack=389 Win=65024 Len=1460
83002 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [ACK] Seq=2082056 Ack=389 Win=65024 Len=1460
83003 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [ACK] Seq=2083516 Ack=389 Win=65024 Len=1460
83004 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [ACK] Seq=2084976 Ack=389 Win=65024 Len=1460
83005 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [ACK] Seq=2086436 Ack=389 Win=65024 Len=1460
83006 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [PSH, ACK] Seq=2087896 Ack=389 Win=65024 Len=1460
83007 1262.832139 172.16.193.242  172.16.194.14   TCP      1514 7680 → 52752 [ACK] Seq=2089356 Ack=389 Win=65024 Len=1460
```

```
▸ Frame 11297: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{1F438D9A-1FAF-
▸ Ethernet II, Src: Intel_4c:63:b4 (30:05:05:4c:63:b4), Dst: AzureWaveTec_f7:b7:4a (28:d0:43:f7:b7:4a)
▸ Internet Protocol Version 4, Src: 172.16.193.236, Dst: 172.16.193.242
▸ Transmission Control Protocol, Src Port: 7680, Dst Port: 54853, Seq: 0, Ack: 1, Len: 0
```

```
0000  28 d0 43 f7 b7 4a 30 05  05 4c 63 b4 08 00 45 00   (·C··J0· ·Lc···E·
0010  00 34 c7 b2 40 00 80 06  57 11 ac 10 c1 ec ac 10   ·4··@··· W·······
0020  c1 f2 1e 00 d6 45 be 24  83 21 09 84 a8 d2 80 12   ·····E·$ ·!······
0030  ff ff ab 1d 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```



Hover over the graph for details. → 5 pkts, 173 bytes ← 6 pkts, 173 bytes

Type Throughput

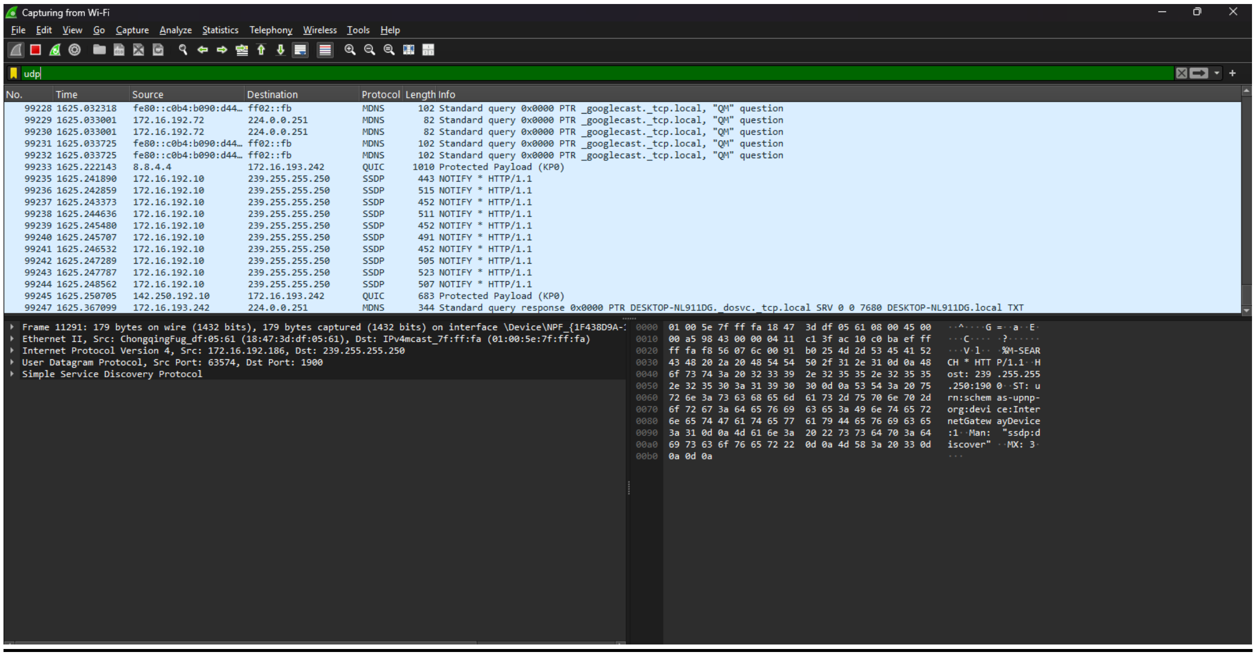
MA Window (s) 1.000000

Stream 92

Mouse ● drags ○ zooms

☑ Segment Length ☑ Throughput □ Goodput

2.UDP

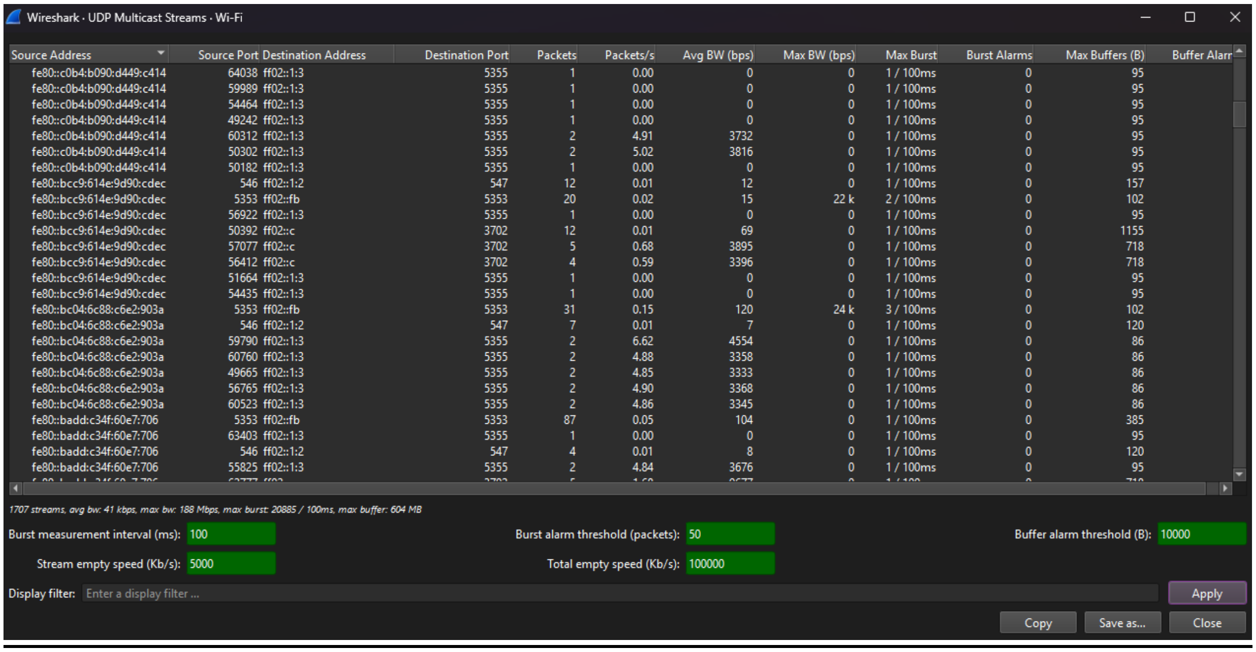

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

```
No.    Time        Source                Destination      Protocol Length Info
 99228 1625.032318 fe80::c0b4:b090:d44… ff02::fb         MDNS      102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
 99229 1625.033001 172.16.192.72        224.0.0.251      MDNS       82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
 99230 1625.033001 172.16.192.72        224.0.0.251      MDNS       82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
 99231 1625.033725 fe80::c0b4:b090:d44… ff02::fb         MDNS      102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
 99232 1625.033725 fe80::c0b4:b090:d44… ff02::fb         MDNS      102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
 99233 1625.222143 8.8.4.4              172.16.193.242   QUIC     1010 Protected Payload (KP0)
 99235 1625.241890 172.16.192.10        239.255.255.250  SSDP      443 NOTIFY * HTTP/1.1
 99236 1625.242859 172.16.192.10        239.255.255.250  SSDP      515 NOTIFY * HTTP/1.1
 99237 1625.243373 172.16.192.10        239.255.255.250  SSDP      452 NOTIFY * HTTP/1.1
 99238 1625.244636 172.16.192.10        239.255.255.250  SSDP      511 NOTIFY * HTTP/1.1
 99239 1625.245480 172.16.192.10        239.255.255.250  SSDP      452 NOTIFY * HTTP/1.1
 99240 1625.245707 172.16.192.10        239.255.255.250  SSDP      491 NOTIFY * HTTP/1.1
 99241 1625.246532 172.16.192.10        239.255.255.250  SSDP      452 NOTIFY * HTTP/1.1
 99242 1625.247289 172.16.192.10        239.255.255.250  SSDP      505 NOTIFY * HTTP/1.1
 99243 1625.247787 172.16.192.10        239.255.255.250  SSDP      523 NOTIFY * HTTP/1.1
 99244 1625.248562 172.16.192.10        239.255.255.250  SSDP      507 NOTIFY * HTTP/1.1
 99245 1625.250705 142.250.192.10       172.16.193.242   QUIC      683 Protected Payload (KP0)
 99247 1625.367099 172.16.193.242       224.0.0.251      MDNS      344 Standard query response 0x0000 PTR DESKTOP-NL911DG._dosvc._tcp.local SRV 0 0 7680 DESKTOP-NL911DG.local TXT
```

```
Frame 11291: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface \Device\NPF_{1F438D9A-
Ethernet II, Src: ChongqingFug_df:05:61 (18:47:3d:df:05:61), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 172.16.192.186, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 63574, Dst Port: 1900
Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa 18 47  3d df 05 61 08 00 45 00   ··^····G =··a··E·
0010  00 a5 98 43 00 00 04 11  c1 3f ac 10 c0 ba ef ff   ···C···· ·?······
0020  ff fa f8 56 07 6c 00 91  b0 25 4d 2d 53 45 41 52   ···V·l·· ·%M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  6f 73 74 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   ost: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 53 54 3a 20 75   .250:190 0··ST: u
0060  72 6e 3a 73 63 68 65 6d  61 73 2d 75 70 6e 70 2d   rn:schem as-upnp-
0070  6f 72 67 3a 64 65 76 69  63 65 3a 49 6e 74 65 72   org:devi ce:Inter
0080  6e 65 74 47 61 74 65 77  61 79 44 65 76 69 63 65   netGatew ayDevice
0090  3a 31 0d 0a 4d 61 6e 3a  20 22 73 73 64 70 3a 64   :1··Man:  "ssdp:d
00a0  69 73 63 6f 76 65 72 22  0d 0a 4d 58 3a 20 33 0d   iscover" ··MX: 3·
00b0  0a 0d 0a                                           ···
```



Wireshark · UDP Multicast Streams · Wi-Fi

Source Address	Source Port	Destination Address	Destination Port	Packets	Packets/s	Avg BW (bps)	Max BW (bps)	Max Burst	Burst Alarms	Max Buffers (B)	Buffer Alarr
fe80::c0b4:b090:d449:c414	64038	ff02::1:3	5355	1	0.00	0	0	1 / 100ms	0	95	
fe80::c0b4:b090:d449:c414	59989	ff02::1:3	5355	1	0.00	0	0	1 / 100ms	0	95	
fe80::c0b4:b090:d449:c414	54464	ff02::1:3	5355	1	0.00	0	0	1 / 100ms	0	95	
fe80::c0b4:b090:d449:c414	49242	ff02::1:3	5355	1	0.00	0	0	1 / 100ms	0	95	
fe80::c0b4:b090:d449:c414	60312	ff02::1:3	5355	2	4.91	3732	0	1 / 100ms	0	95	
fe80::c0b4:b090:d449:c414	50302	ff02::1:3	5355	2	5.02	3816	0	1 / 100ms	0	95	
fe80::c0b4:b090:d449:c414	50182	ff02::1:3	5355	1	0.00	0	0	1 / 100ms	0	95	
fe80::bcc9:614e:9d90:cdec	546	ff02::1:2	547	12	0.01	12	0	1 / 100ms	0	157	
fe80::bcc9:614e:9d90:cdec	5353	ff02::fb	5353	20	0.02	15	22 k	2 / 100ms	0	102	
fe80::bcc9:614e:9d90:cdec	56922	ff02::1:3	5355	1	0.00	0	0	1 / 100ms	0	95	
fe80::bcc9:614e:9d90:cdec	50392	ff02::c	3702	12	0.01	69	0	1 / 100ms	0	1155	
fe80::bcc9:614e:9d90:cdec	57077	ff02::c	3702	5	0.68	3895	0	1 / 100ms	0	718	
fe80::bcc9:614e:9d90:cdec	56412	ff02::c	3702	4	0.59	3396	0	1 / 100ms	0	718	
fe80::bcc9:614e:9d90:cdec	51664	ff02::1:3	5355	1	0.00	0	0	1 / 100ms	0	95	
fe80::bcc9:614e:9d90:cdec	54435	ff02::1:3	5355	1	0.00	0	0	1 / 100ms	0	95	
fe80::bc04:6c88:c6e2:903a	5353	ff02::fb	5353	31	0.15	120	24 k	3 / 100ms	0	102	
fe80::bc04:6c88:c6e2:903a	546	ff02::1:2	547	7	0.01	7	0	1 / 100ms	0	120	
fe80::bc04:6c88:c6e2:903a	59790	ff02::1:3	5355	2	6.62	4554	0	1 / 100ms	0	86	
fe80::bc04:6c88:c6e2:903a	60760	ff02::1:3	5355	2	4.88	3358	0	1 / 100ms	0	86	
fe80::bc04:6c88:c6e2:903a	49665	ff02::1:3	5355	2	4.85	3333	0	1 / 100ms	0	86	
fe80::bc04:6c88:c6e2:903a	56765	ff02::1:3	5355	2	4.90	3368	0	1 / 100ms	0	86	
fe80::bc04:6c88:c6e2:903a	60523	ff02::1:3	5355	2	4.86	3345	0	1 / 100ms	0	86	
fe80::badd:c34f:60e7:706	5353	ff02::fb	5353	87	0.05	104	0	1 / 100ms	0	385	
fe80::badd:c34f:60e7:706	63403	ff02::1:3	5355	1	0.00	0	0	1 / 100ms	0	95	
fe80::badd:c34f:60e7:706	546	ff02::1:2	547	4	0.01	8	0	1 / 100ms	0	120	
fe80::badd:c34f:60e7:706	55825	ff02::1:3	5355	2	4.84	3676	0	1 / 100ms	0	95	

1707 streams, avg bw: 41 kbps, max bw: 188 Mbps, max burst: 20885 / 100ms, max buffer: 604 MB

Burst measurement interval (ms): 100

Burst alarm threshold (packets): 50

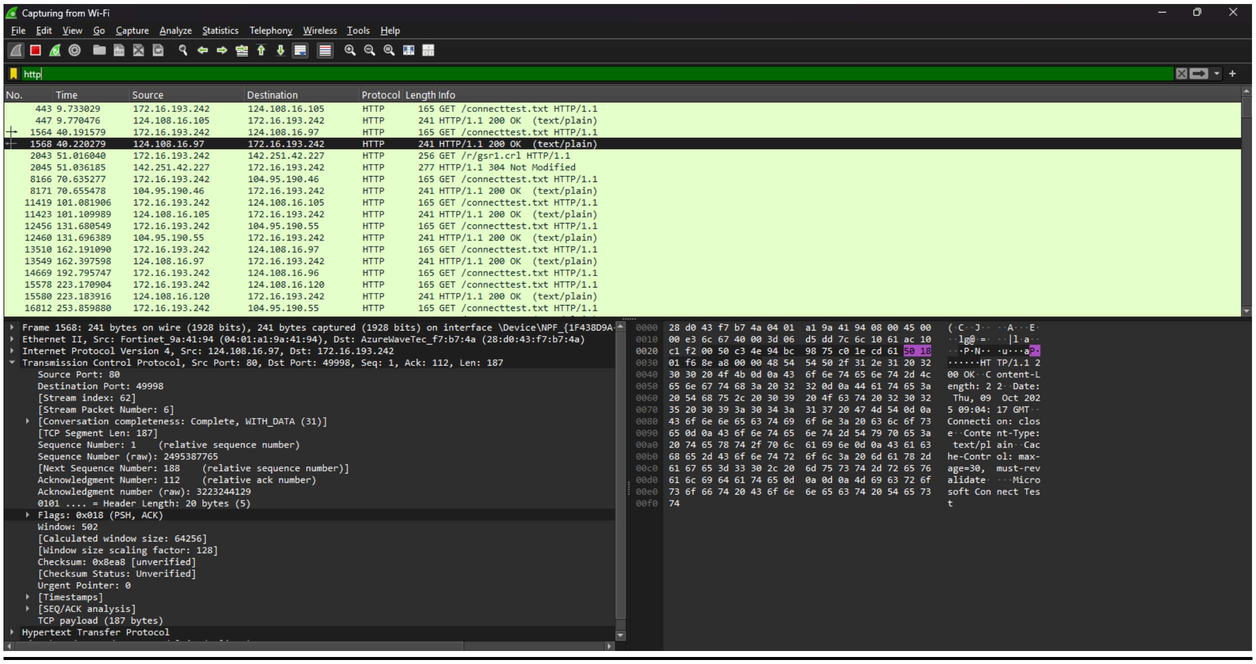
Buffer alarm threshold (B): 10000

Stream empty speed (Kb/s): 5000

Total empty speed (Kb/s): 100000

Display filter: Enter a display filter ...

3.HTTP



Capturing from Wi-Fi

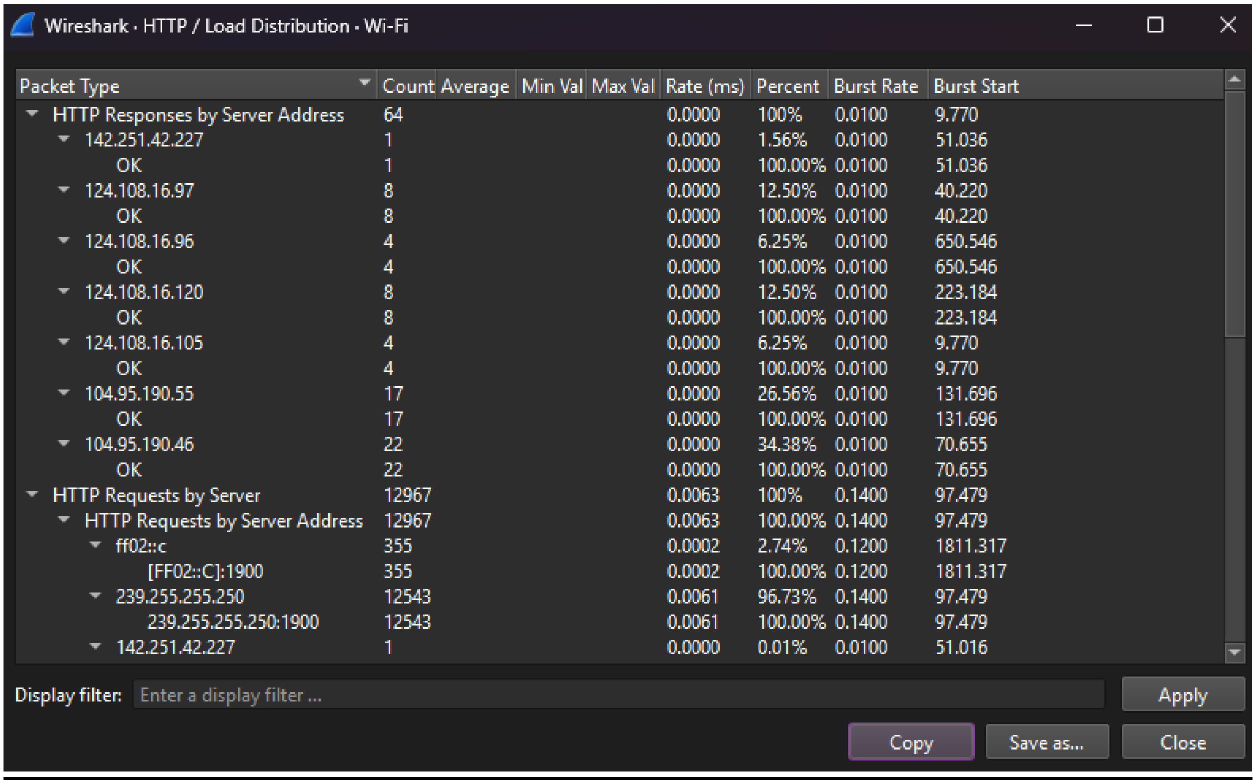
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.    Time        Source          Destination     Protocol Length Info
  443 9.733029     172.16.193.242  124.108.16.105  HTTP      165 GET /connecttest.txt HTTP/1.1
  447 9.770476     124.108.16.105  172.16.193.242  HTTP      241 HTTP/1.1 200 OK  (text/plain)
 1564 40.191579    172.16.193.242  124.108.16.97   HTTP      165 GET /connecttest.txt HTTP/1.1
 1568 40.220279    124.108.16.97   172.16.193.242  HTTP      241 HTTP/1.1 200 OK  (text/plain)
 2043 51.016040    172.16.193.242  142.251.42.227  HTTP      256 GET /r/gsr1.crl HTTP/1.1
 2045 51.036185    142.251.42.227  172.16.193.242  HTTP      277 HTTP/1.1 304 Not Modified
 8166 70.635277    172.16.193.242  104.95.190.46   HTTP      165 GET /connecttest.txt HTTP/1.1
 8171 70.655478    104.95.190.46   172.16.193.242  HTTP      241 HTTP/1.1 200 OK  (text/plain)
11419 101.081906   172.16.193.242  124.108.16.105  HTTP      165 GET /connecttest.txt HTTP/1.1
11423 101.109989   124.108.16.105  172.16.193.242  HTTP      241 HTTP/1.1 200 OK  (text/plain)
12456 131.680549   172.16.193.242  104.95.190.55   HTTP      165 GET /connecttest.txt HTTP/1.1
12460 131.696389   104.95.190.55   172.16.193.242  HTTP      241 HTTP/1.1 200 OK  (text/plain)
13510 162.191090   172.16.193.242  124.108.16.97   HTTP      165 GET /connecttest.txt HTTP/1.1
13549 162.397598   124.108.16.97   172.16.193.242  HTTP      241 HTTP/1.1 200 OK  (text/plain)
14669 192.795747   172.16.193.242  124.108.16.96   HTTP      165 GET /connecttest.txt HTTP/1.1
15578 223.170904   172.16.193.242  124.108.16.120  HTTP      165 GET /connecttest.txt HTTP/1.1
15580 223.183916   124.108.16.120  172.16.193.242  HTTP      241 HTTP/1.1 200 OK  (text/plain)
16812 253.859880   172.16.193.242  104.95.190.55   HTTP      165 GET /connecttest.txt HTTP/1.1
```

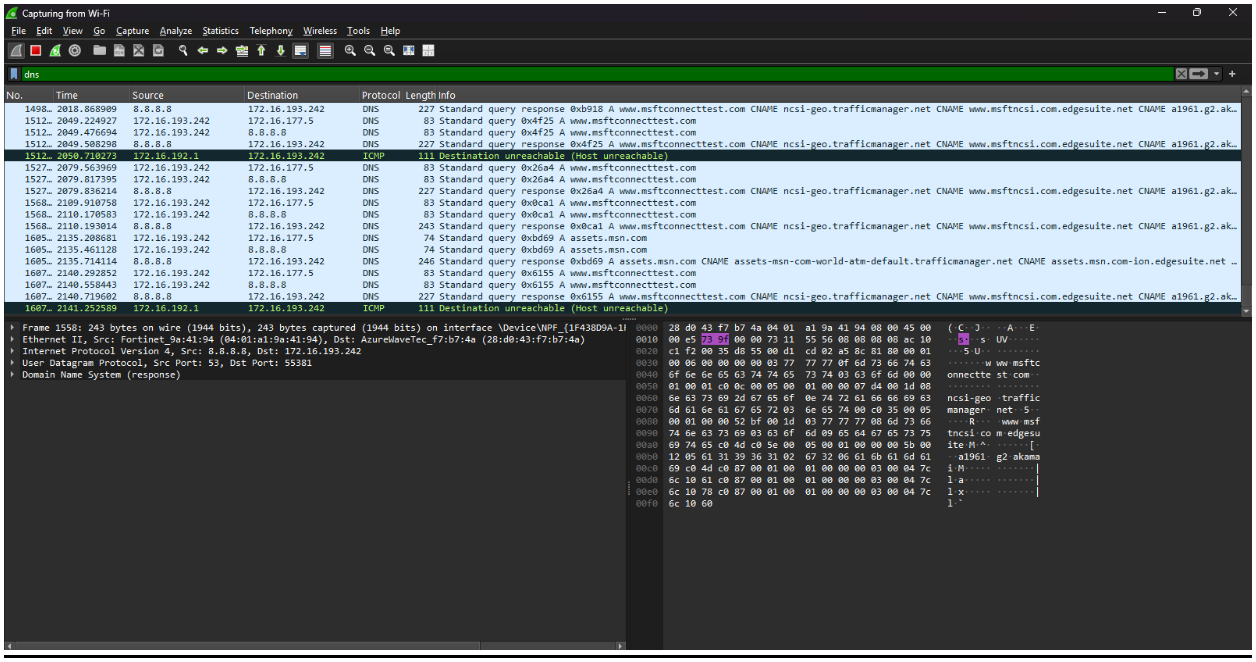
```
Frame 1568: 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface \Device\NPF_{1F438D9A-
Ethernet II, Src: Fortinet_9a:41:94 (04:01:a1:9a:41:94), Dst: AzureWaveTec_f7:b7:4a (28:d0:43:f7:b7:4a)
Internet Protocol Version 4, Src: 124.108.16.97, Dst: 172.16.193.242
Transmission Control Protocol, Src Port: 80, Dst Port: 49998, Seq: 1, Ack: 112, Len: 187
    Source Port: 80
    Destination Port: 49998
    [Stream index: 62]
    [Stream Packet Number: 6]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 187]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2495387765
    [Next Sequence Number: 188    (relative sequence number)]
    Acknowledgment Number: 112    (relative ack number)
    Acknowledgment number (raw): 3223244129
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
    Checksum: 0x8ea8 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (187 bytes)
Hypertext Transfer Protocol
```

```
0000  28 d0 43 f7 b7 4a 04 01  a1 9a 41 94 08 00 45 00   (·C··J·· ··A···E·
0010  00 e3 6c 67 40 00 3d 06  d5 dd 7c 6c 10 61 ac 10   ··lg@·=· ··|l·a··
0020  c1 f2 00 50 c3 4e 94 bc  98 75 c0 1e cd 61 50 18   ···P·N·· ·u···aP·
0030  01 f6 8e a8 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   00 OK··C ontent-L
0050  65 6e 67 74 68 3a 20 32  32 0d 0a 44 61 74 65 3a   ength: 2 2··Date:
0060  20 54 68 75 2c 20 30 39  20 4f 63 74 20 32 30 32    Thu, 09  Oct 202
0070  35 20 30 39 3a 30 34 3a  31 37 20 47 4d 54 0d 0a   5 09:04: 17 GMT··
0080  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 63 6c 6f 73   Connecti on: clos
0090  65 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   e··Conte nt-Type:
00a0  20 74 65 78 74 2f 70 6c  61 69 6e 0d 0a 43 61 63    text/pl ain··Cac
00b0  68 65 2d 43 6f 6e 74 72  6f 6c 3a 20 6d 61 78 2d   he-Contr ol: max-
00c0  61 67 65 3d 33 30 2c 20  6d 75 73 74 2d 72 65 76   age=30,  must-rev
00d0  61 6c 69 64 61 74 65 0d  0a 0d 0a 4d 69 63 72 6f   alidate· ···Micro
00e0  73 6f 66 74 20 43 6f 6e  6e 65 63 74 20 54 65 73   soft Con nect Tes
00f0  74                                                 t
```



Packet Type	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
HTTP Responses by Server Address	64				0.0000	100%	0.0100	9.770
142.251.42.227	1				0.0000	1.56%	0.0100	51.036
OK	1				0.0000	100.00%	0.0100	51.036
124.108.16.97	8				0.0000	12.50%	0.0100	40.220
OK	8				0.0000	100.00%	0.0100	40.220
124.108.16.96	4				0.0000	6.25%	0.0100	650.546
OK	4				0.0000	100.00%	0.0100	650.546
124.108.16.120	8				0.0000	12.50%	0.0100	223.184
OK	8				0.0000	100.00%	0.0100	223.184
124.108.16.105	4				0.0000	6.25%	0.0100	9.770
OK	4				0.0000	100.00%	0.0100	9.770
104.95.190.55	17				0.0000	26.56%	0.0100	131.696
OK	17				0.0000	100.00%	0.0100	131.696
104.95.190.46	22				0.0000	34.38%	0.0100	70.655
OK	22				0.0000	100.00%	0.0100	70.655
HTTP Requests by Server	12967				0.0063	100%	0.1400	97.479
HTTP Requests by Server Address	12967				0.0063	100.00%	0.1400	97.479
ff02::c	355				0.0002	2.74%	0.1200	1811.317
[FF02::C]:1900	355				0.0002	100.00%	0.1200	1811.317
239.255.255.250	12543				0.0061	96.73%	0.1400	97.479
239.255.255.250:1900	12543				0.0061	100.00%	0.1400	97.479
142.251.42.227	1				0.0000	0.01%	0.0100	51.016

4.DNS

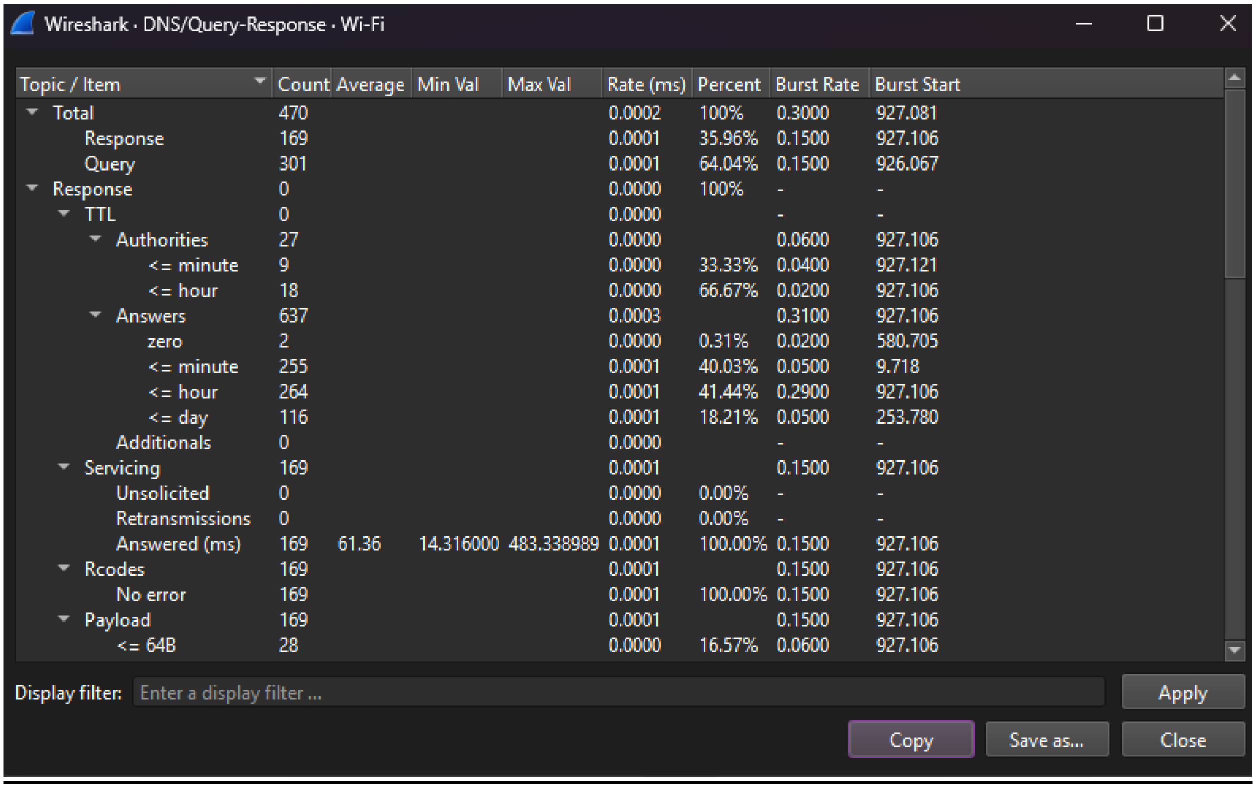


dns

```
No.      Time         Source           Destination      Protocol Length Info
   1498… 2018.868909  8.8.8.8          172.16.193.242   DNS      227 Standard query response 0xb918 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961.g2.ak…
   1512… 2049.224927  172.16.193.242   172.16.177.5     DNS       83 Standard query 0x4f25 A www.msftconnecttest.com
   1512… 2049.476694  172.16.193.242   8.8.8.8          DNS       83 Standard query 0x4f25 A www.msftconnecttest.com
   1512… 2049.508298  8.8.8.8          172.16.193.242   DNS      227 Standard query response 0x4f25 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961.g2.ak…
   1512… 2050.710273  172.16.192.1     172.16.193.242   ICMP     111 Destination unreachable (Host unreachable)
   1527… 2079.563969  172.16.193.242   172.16.177.5     DNS       83 Standard query 0x26a4 A www.msftconnecttest.com
   1527… 2079.817395  172.16.193.242   8.8.8.8          DNS       83 Standard query 0x26a4 A www.msftconnecttest.com
   1527… 2079.836214  8.8.8.8          172.16.193.242   DNS      227 Standard query response 0x26a4 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961.g2.ak…
   1568… 2109.910758  172.16.193.242   172.16.177.5     DNS       83 Standard query 0x0ca1 A www.msftconnecttest.com
   1568… 2110.170583  172.16.193.242   8.8.8.8          DNS       83 Standard query 0x0ca1 A www.msftconnecttest.com
   1568… 2110.193014  8.8.8.8          172.16.193.242   DNS      243 Standard query response 0x0ca1 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961.g2.ak…
   1605… 2135.208681  172.16.193.242   172.16.177.5     DNS       74 Standard query 0xbd69 A assets.msn.com
   1605… 2135.461128  172.16.193.242   8.8.8.8          DNS       74 Standard query 0xbd69 A assets.msn.com
   1605… 2135.714114  8.8.8.8          172.16.193.242   DNS      246 Standard query response 0xbd69 A assets.msn.com CNAME assets-msn-com-world-atm-default.trafficmanager.net CNAME assets.msn.com-ion.edgesuite.net …
   1607… 2140.292852  172.16.193.242   172.16.177.5     DNS       83 Standard query 0x6155 A www.msftconnecttest.com
   1607… 2140.558443  172.16.193.242   8.8.8.8          DNS       83 Standard query 0x6155 A www.msftconnecttest.com
   1607… 2140.719602  8.8.8.8          172.16.193.242   DNS      227 Standard query response 0x6155 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a1961.g2.ak…
   1607… 2141.252589  172.16.192.1     172.16.193.242   ICMP     111 Destination unreachable (Host unreachable)
```

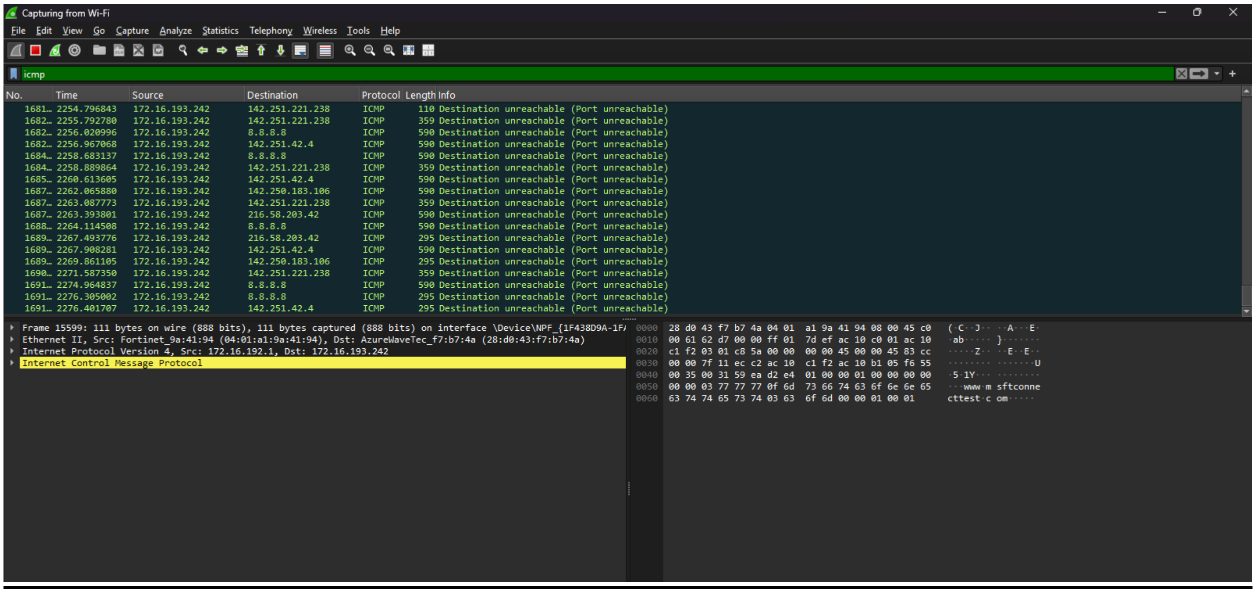
```
▸ Frame 1558: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface \Device\NPF_{1F438D9A-1I
▸ Ethernet II, Src: Fortinet_9a:41:94 (04:01:a1:9a:41:94), Dst: AzureWaveTec_f7:b7:4a (28:d0:43:f7:b7:4a)
▸ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.16.193.242
▸ User Datagram Protocol, Src Port: 53, Dst Port: 55381
▸ Domain Name System (response)
```

```
0000  28 d0 43 f7 b7 4a 04 01  a1 9a 41 94 08 00 45 00   (·C··J····A···E·
0010  00 e5 73 9f 00 00 73 11  55 56 08 08 08 08 ac 10   ··s···s·UV······
0020  c1 f2 00 35 d8 55 00 d1  cd 02 a5 8c 81 80 00 01   ···5·U··········
0030  00 06 00 00 00 00 03 77  77 77 0f 6d 73 66 74 63   ·······www·msftc
0040  6f 6e 6e 65 63 74 74 65  73 74 03 63 6f 6d 00 00   onnecttest·com··
0050  01 00 01 c0 0c 00 05 00  01 00 00 07 d4 00 1d 08   ················
0060  6e 63 73 69 2d 67 65 6f  0e 74 72 61 66 66 69 63   ncsi-geo·traffic
0070  6d 61 6e 61 67 65 72 03  6e 65 74 00 c0 35 00 05   manager·net··5··
0080  00 01 00 00 52 bf 00 1d  03 77 77 77 08 6d 73 66   ····R····www·msf
0090  74 6e 63 73 69 03 63 6f  6d 09 65 64 67 65 73 75   tncsi·com·edgesu
00a0  69 74 65 c0 4d c0 5e 00  05 00 01 00 00 00 5b 00   ite·M·^·······[·
00b0  12 05 61 31 39 36 31 02  67 32 06 61 6b 61 6d 61   ··a1961·g2·akama
00c0  69 c0 4d c0 87 00 01 00  01 00 00 00 03 00 04 7c   i·M············|
00d0  6c 10 61 c0 87 00 01 00  01 00 00 00 03 00 04 7c   l·a············|
00e0  6c 10 78 c0 87 00 01 00  01 00 00 00 03 00 04 7c   l·x············|
00f0  6c 10 60                                           l·`
```


Wireshark · DNS/Query-Response · Wi-Fi
Display filter:
Enter a display filter ...
Apply
Copy
Save as...
Close

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total	470				0.0002	100%	0.3000	927.081
Response	169				0.0001	35.96%	0.1500	927.106
Query	301				0.0001	64.04%	0.1500	926.067
Response	0				0.0000	100%	-	-
TTL	0				0.0000		-	-
Authorities	27				0.0000		0.0600	927.106
<= minute	9				0.0000	33.33%	0.0400	927.121
<= hour	18				0.0000	66.67%	0.0200	927.106
Answers	637				0.0003		0.3100	927.106
zero	2				0.0000	0.31%	0.0200	580.705
<= minute	255				0.0001	40.03%	0.0500	9.718
<= hour	264				0.0001	41.44%	0.2900	927.106
<= day	116				0.0001	18.21%	0.0500	253.780
Additionals	0				0.0000		-	-
Servicing	169				0.0001		0.1500	927.106
Unsolicited	0				0.0000	0.00%	-	-
Retransmissions	0				0.0000	0.00%	-	-
Answered (ms)	169	61.36	14.316000	483.338989	0.0001	100.00%	0.1500	927.106
Rcodes	169				0.0001		0.1500	927.106
No error	169				0.0001	100.00%	0.1500	927.106
Payload	169				0.0001		0.1500	927.106
<= 64B	28				0.0000	16.57%	0.0600	927.106

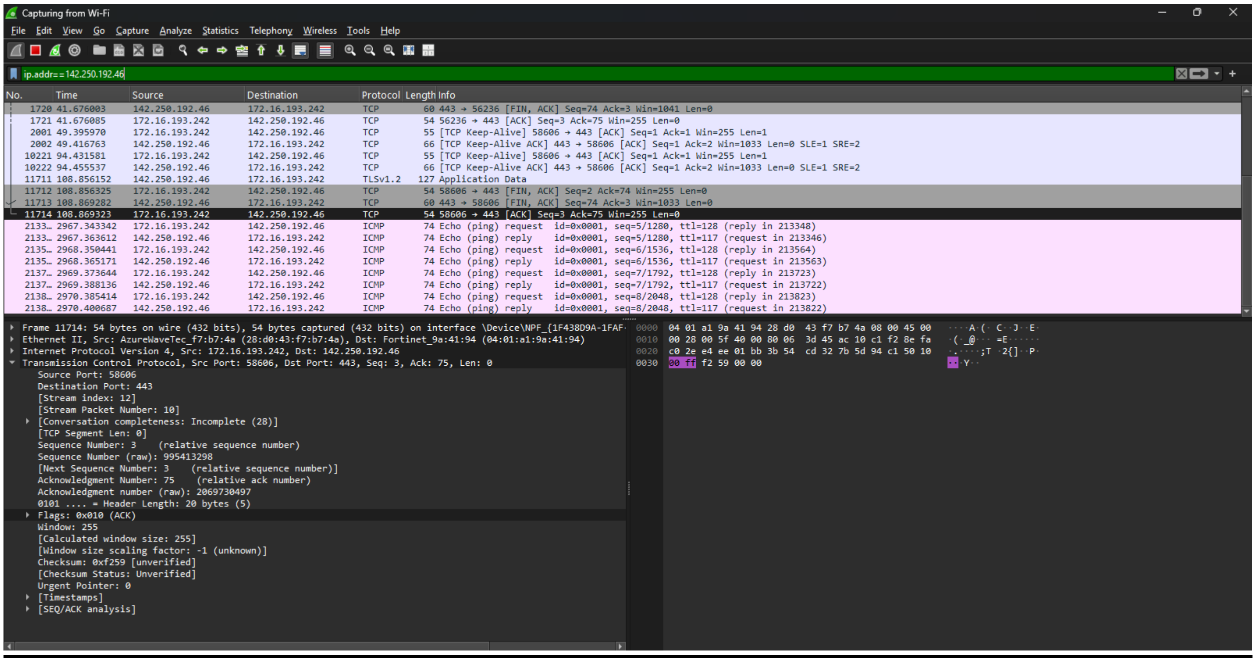
5.ICMP


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
No.   Time         Source          Destination       Protocol Length Info
1681… 2254.796843  172.16.193.242  142.251.221.238   ICMP     110 Destination unreachable (Port unreachable)
1682… 2255.792780  172.16.193.242  142.251.221.238   ICMP     359 Destination unreachable (Port unreachable)
1682… 2256.020996  172.16.193.242  8.8.8.8           ICMP     590 Destination unreachable (Port unreachable)
1682… 2256.967068  172.16.193.242  142.251.42.4      ICMP     590 Destination unreachable (Port unreachable)
1684… 2258.683137  172.16.193.242  8.8.8.8           ICMP     590 Destination unreachable (Port unreachable)
1684… 2258.889864  172.16.193.242  142.251.221.238   ICMP     359 Destination unreachable (Port unreachable)
1685… 2260.613605  172.16.193.242  142.251.42.4      ICMP     590 Destination unreachable (Port unreachable)
1687… 2262.065880  172.16.193.242  142.250.183.106   ICMP     590 Destination unreachable (Port unreachable)
1687… 2263.087773  172.16.193.242  142.251.221.238   ICMP     359 Destination unreachable (Port unreachable)
1687… 2263.393801  172.16.193.242  216.58.203.42     ICMP     590 Destination unreachable (Port unreachable)
1688… 2264.114508  172.16.193.242  8.8.8.8           ICMP     590 Destination unreachable (Port unreachable)
1689… 2267.493776  172.16.193.242  216.58.203.42     ICMP     295 Destination unreachable (Port unreachable)
1689… 2267.908281  172.16.193.242  142.251.42.4      ICMP     590 Destination unreachable (Port unreachable)
1689… 2269.861105  172.16.193.242  142.250.183.106   ICMP     295 Destination unreachable (Port unreachable)
1690… 2271.587350  172.16.193.242  142.251.221.238   ICMP     359 Destination unreachable (Port unreachable)
1691… 2274.964837  172.16.193.242  8.8.8.8           ICMP     590 Destination unreachable (Port unreachable)
1691… 2276.305002  172.16.193.242  8.8.8.8           ICMP     295 Destination unreachable (Port unreachable)
1691… 2276.401707  172.16.193.242  142.251.42.4      ICMP     295 Destination unreachable (Port unreachable)
```

```
> Frame 15599: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface \Device\NPF_{1F438D9A-1F/
> Ethernet II, Src: Fortinet_9a:41:94 (04:01:a1:9a:41:94), Dst: AzureWaveTec_f7:b7:4a (28:d0:43:f7:b7:4a)
> Internet Protocol Version 4, Src: 172.16.192.1, Dst: 172.16.193.242
> Internet Control Message Protocol
```

```
0000  28 d0 43 f7 b7 4a 04 01  a1 9a 41 94 08 00 45 c0   (·C··J·· ··A···E·
0010  00 61 62 d7 00 00 ff 01  7d ef ac 10 c0 01 ac 10   ·ab····· }·······
0020  c1 f2 03 01 c8 5a 00 00  00 00 45 00 00 45 83 cc   ·····Z·· ··E··E··
0030  00 00 7f 11 ec c2 ac 10  c1 f2 ac 10 b1 05 f6 55   ········ ·······U
0040  00 35 00 31 59 ea d2 e4  01 00 00 01 00 00 00 00   ·5·1Y··· ········
0050  00 00 03 77 77 77 0f 6d  73 66 74 63 6f 6e 6e 65   ···www·m sftconne
0060  63 74 74 65 73 74 03 63  6f 6d 00 00 01 00 01      cttest·c om·····
```



```
ip.addr==142.250.192.46
```

```
No.    Time          Source            Destination       Protocol Length Info
  1720 41.676003     142.250.192.46    172.16.193.242    TCP        60 443 → 56236 [FIN, ACK] Seq=74 Ack=3 Win=1041 Len=0
  1721 41.676085     172.16.193.242    142.250.192.46    TCP        54 56236 → 443 [ACK] Seq=3 Ack=75 Win=255 Len=0
  2001 49.395970     172.16.193.242    142.250.192.46    TCP        55 [TCP Keep-Alive] 58606 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
  2002 49.416763     142.250.192.46    172.16.193.242    TCP        66 [TCP Keep-Alive ACK] 443 → 58606 [ACK] Seq=1 Ack=2 Win=1033 Len=0 SLE=1 SRE=2
 10221 94.431581     172.16.193.242    142.250.192.46    TCP        55 [TCP Keep-Alive] 58606 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
 10222 94.455537     142.250.192.46    172.16.193.242    TCP        66 [TCP Keep-Alive ACK] 443 → 58606 [ACK] Seq=1 Ack=2 Win=1033 Len=0 SLE=1 SRE=2
 11711 108.856152    142.250.192.46    172.16.193.242    TLSv1.2   127 Application Data
 11712 108.856325    172.16.193.242    142.250.192.46    TCP        54 58606 → 443 [FIN, ACK] Seq=2 Ack=74 Win=255 Len=0
 11713 108.869282    142.250.192.46    172.16.193.242    TCP        60 443 → 58606 [FIN, ACK] Seq=74 Ack=3 Win=1033 Len=0
 11714 108.869323    172.16.193.242    142.250.192.46    TCP        54 58606 → 443 [ACK] Seq=3 Ack=75 Win=255 Len=0
 2133… 2967.343342   172.16.193.242    142.250.192.46    ICMP       74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (reply in 213348)
 2133… 2967.363612   142.250.192.46    172.16.193.242    ICMP       74 Echo (ping) reply    id=0x0001, seq=5/1280, ttl=117 (request in 213346)
 2135… 2968.350441   172.16.193.242    142.250.192.46    ICMP       74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (reply in 213564)
 2135… 2968.365171   142.250.192.46    172.16.193.242    ICMP       74 Echo (ping) reply    id=0x0001, seq=6/1536, ttl=117 (request in 213563)
 2137… 2969.373644   172.16.193.242    142.250.192.46    ICMP       74 Echo (ping) request  id=0x0001, seq=7/1792, ttl=128 (reply in 213723)
 2137… 2969.388136   142.250.192.46    172.16.193.242    ICMP       74 Echo (ping) reply    id=0x0001, seq=7/1792, ttl=117 (request in 213722)
 2138… 2970.385414   172.16.193.242    142.250.192.46    ICMP       74 Echo (ping) request  id=0x0001, seq=8/2048, ttl=128 (reply in 213823)
 2138… 2970.400687   142.250.192.46    172.16.193.242    ICMP       74 Echo (ping) reply    id=0x0001, seq=8/2048, ttl=117 (request in 213822)
```

```
Frame 11714: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{1F438D9A-1FAF-
Ethernet II, Src: AzureWaveTec_f7:b7:4a (28:d0:43:f7:b7:4a), Dst: Fortinet_9a:41:94 (04:01:a1:9a:41:94)
Internet Protocol Version 4, Src: 172.16.193.242, Dst: 142.250.192.46
Transmission Control Protocol, Src Port: 58606, Dst Port: 443, Seq: 3, Ack: 75, Len: 0
    Source Port: 58606
    Destination Port: 443
    [Stream index: 12]
    [Stream Packet Number: 10]
    [Conversation completeness: Incomplete (28)]
    [TCP Segment Len: 0]
    Sequence Number: 3    (relative sequence number)
    Sequence Number (raw): 995413298
    [Next Sequence Number: 3    (relative sequence number)]
    Acknowledgment Number: 75    (relative ack number)
    Acknowledgment number (raw): 2069730497
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
    Window: 255
    [Calculated window size: 255]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xf259 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
```

```
0000  04 01 a1 9a 41 94 28 d0  43 f7 b7 4a 08 00 45 00   ····A·(· C··J··E·
0010  00 28 00 5f 40 00 80 06  3d 45 ac 10 c1 f2 8e fa   ·(·_@··· =E······
0020  c0 2e e4 ee 01 bb 3b 54  cd 32 7b 5d 94 c1 50 10   ·.····;T ·2{]··P·
0030  00 ff f2 59 00 00                                  ···Y··
```