

WIRE SHARK-WIFI

1.TCP-SIMATS WIFI

The screenshot shows the Wireshark interface with a capture of traffic on the 'Wi-Fi' interface. The packet list pane shows several packets, with packet 5597 selected. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Simple Service Discovery Protocol (SSDP). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
5592	34.006177	172.18.53.75	172.18.73.98	TCP	1514	7680 → 51829 [ACK] Seq=2461513 Ack=533 Win=4099 L
5593	34.006177	172.18.53.75	172.18.73.98	TCP	1514	7680 → 51829 [ACK] Seq=2462973 Ack=533 Win=4099 L
5594	34.006177	172.18.53.75	172.18.73.98	TCP	1340	7680 → 51829 [PSH, ACK] Seq=2464433 Ack=533 Win=4
5595	34.007394	62:3f:72:80:b1:68	AzureWav_c8:f5:d9	ARP	60	Who has 172.18.56.72? Tell 172.18.49.84
5596	34.041317	LiteON_f1:67:c8	AzureWav_c8:f5:d9	ARP	60	Who has 172.18.55.251? Tell 172.18.49.90
5597	34.049726	172.18.51.16	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{0416AB78-8E2A-4A3C-9387-E03ECB800...}

Ethernet II, Src: AzureWav_c8:f5:d9 (34:6f:24:c8:f5:d9), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol Version 4, Src: 172.18.53.75, Dst: 239.255.255.250

User Datagram Protocol, Src Port: 56082, Dst Port: 1900

Simple Service Discovery Protocol

0000 01 00 5e 7f ff fa 34 6f 24 c8 f5 d9 08 00 45 00 ..^...4o \$.....E..

0010 ff fa db 12 07 6c 00 b7 e4 2a 4d 2d 53 45 41 521... *M-SEAR

0020 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H

0030 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255

0040 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0..MAN:

0050 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:di scover"

0060 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a .MX: 1.. ST: urn:

2. HTTP-SIMATS WIFI

The screenshot shows the Wireshark interface with a capture of traffic on the 'Wi-Fi' interface. The packet list pane shows several packets, with packet 1111 selected. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Router Solicitation. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1106	6.216312	172.18.53.75	41.63.107.128	TCP	54	54726 → 80 [ACK] Seq=1 Ack=538741 Win=513 Len=0
1107	6.219570	41.63.107.128	172.18.53.75	TCP	1514	80 → 54726 [ACK] Seq=538741 Ack=1 Win=237 Len=146
1108	6.221155	41.63.107.128	172.18.53.75	TCP	1514	80 → 54726 [ACK] Seq=540201 Ack=1 Win=237 Len=146
1109	6.221283	172.18.53.75	41.63.107.128	TCP	54	54726 → 80 [ACK] Seq=1 Ack=541661 Win=513 Len=0
1110	6.247290	41.63.107.128	172.18.53.75	TCP	1514	80 → 54726 [ACK] Seq=541661 Ack=1 Win=237 Len=146
1111	6.249256	fe80::ec64:73ff:fe1... ff02::2	ff02::2	ICMPv6	70	Router Solicitation from ee:64:73:16:04:97

Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{0416AB78-8E2A-4A3C-9387-E03ECB800...}

Ethernet II, Src: Cisco_c8:4d:57 (38:90:a5:c8:4d:57), Dst: AzureWav_c8:f5:d9 (34:6f:24:c8:f5:d9)

Internet Protocol Version 4, Src: 41.63.107.128, Dst: 172.18.53.75

Transmission Control Protocol, Src Port: 80, Dst Port: 54726, Seq: 1, Ack: 1, Len: 1460

0000 34 6f 24 c8 f5 d9 38 90 a5 c8 4d 57 08 00 45 00 4o\$...8... MW...E..

0010 05 dc 4d 7f 40 00 3e 06 73 80 29 3f 6b 80 ac 12 .M.@>.s.)?k...

0020 35 4b 00 50 d5 c6 af 01 a2 8c c6 16 eb 9f 50 10 5K.P....P..

0030 00 ed df 32 00 00 0c 89 bc 92 d4 db c5 18 78 7c ...2....X|

0040 a2 e2 ec 3c 7d d0 0e 7e d3 64 50 49 b2 b4 e3 09<}...dPI....

0050 db e5 f3 fb 9e 7d 93 db c5 11 2a 92 54 c9 53 68}...*.T.Sh

0060 13 dd 23 88 7a 26 b0 d5 09 ad 81 83 da 21 65 07 .#.z&....!e..

0070 f4 c6 59 55 8d a2 40 8e e5 80 f7 ba 61 b1 48 3d ..YU...@...a.H=

3.UDP-SIMATS WIFI

The screenshot shows a Wireshark capture of network traffic on a Wi-Fi interface. The filter bar at the top is set to 'udp'. The packet list pane shows several packets, with packet 2477 selected. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 6, and Internet Control Message Protocol v6. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2477	8.972005	41.63.107.128	172.18.53.75	TCP	1514	80 → 54726 [ACK] Seq=886221 Ack=1 Win=237 Len=146
2478	8.972115	172.18.53.75	41.63.107.128	TCP	54	54726 → 80 [ACK] Seq=1 Ack=887681 Win=513 Len=0
2479	8.974749	AzureWav_a0:bc:9f	AzureWav_c8:f5:d9	ARP	60	Who has 172.18.55.75? Tell 172.18.49.92
2480	8.978266	41.63.107.128	172.18.53.75	TCP	1514	80 → 54726 [ACK] Seq=887681 Ack=1 Win=237 Len=146
2481	8.979437	41.63.107.128	172.18.53.75	TCP	1514	80 → 54726 [ACK] Seq=889141 Ack=1 Win=237 Len=146
2482	8.979875	172.18.53.75	41.63.107.128	TCP	54	54726 → 80 [ACK] Seq=1 Ack=890601 Win=513 Len=0

Frame 1: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface \Device\NPF_{0416AB78-8E2A-4A3C-9387-E03ECBB00...}

Ethernet II, Src: 66:8f:30:5e:4f:6e (66:8f:30:5e:4f:6e), Dst: AzureWav_c8:f5:d9 (34:6f:24:c8:f5:d9)

Internet Protocol Version 6, Src: fe80::648f:30ff:fe5e:4f6e, Dst: ff02::16

Internet Control Message Protocol v6

4.ICMP-SIMATS WIFI

The screenshot shows a Wireshark capture of network traffic on a Wi-Fi interface. The filter bar at the top is set to 'icmp'. The packet list pane shows several packets, with packet 664 selected. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Transport Layer Security. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
664	7.080370	172.18.53.159	224.0.0.251	MDNS	292	Standard query response 0x0000 PTR, cache flush A
665	7.086002	fe80::d847:bd64:ca3...	ff02::fb	MDNS	312	Standard query response 0x0000 PTR, cache flush A
666	7.126102	172.18.59.4	224.0.0.251	MDNS	814	Standard query response 0x0000 TXT, cache flush P
667	7.127256	fe80::781e:d0ff:78a...	ff02::fb	MDNS	834	Standard query response 0x0000 TXT, cache flush P
668	7.169166	HewlettP_19:3f:83	AzureWav_c8:f5:d9	0x3600	68	Ethernet II
669	7.172724	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x47dcffb0

Frame 1: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{0416AB78-8E2A-4A3C-9387-E03ECBB00...}

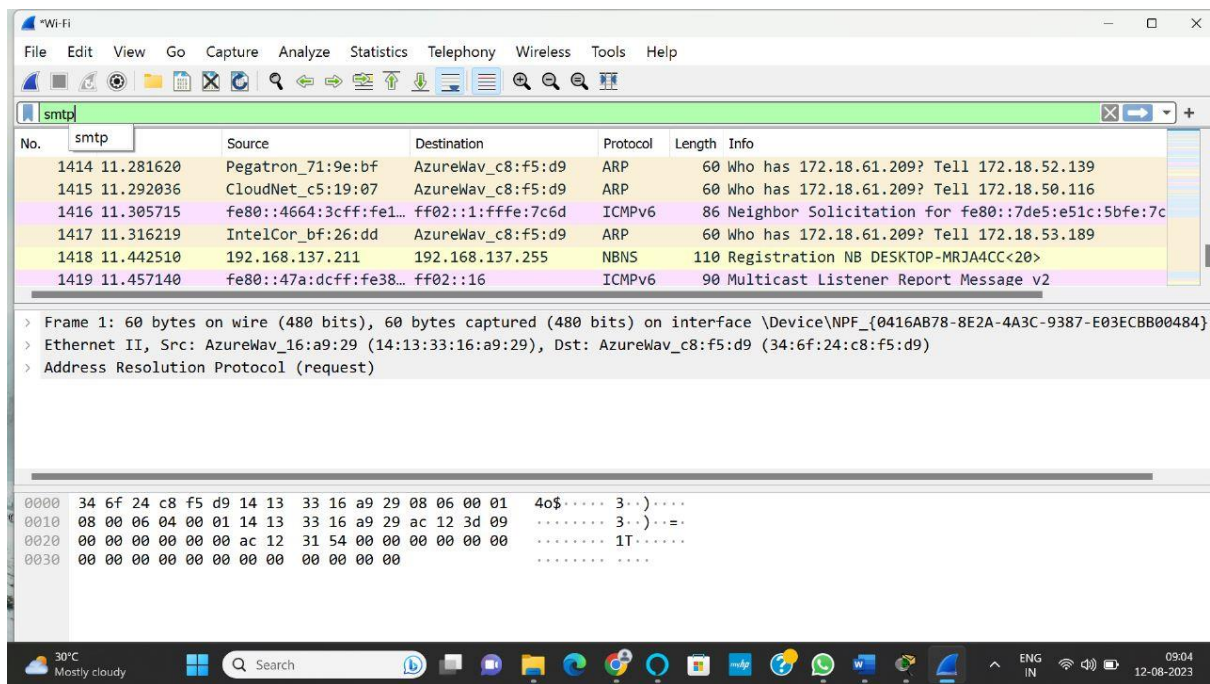
Ethernet II, Src: Cisco_c8:4d:57 (38:90:a5:c8:4d:57), Dst: AzureWav_c8:f5:d9 (34:6f:24:c8:f5:d9)

Internet Protocol Version 4, Src: 204.79.197.254, Dst: 172.18.53.75

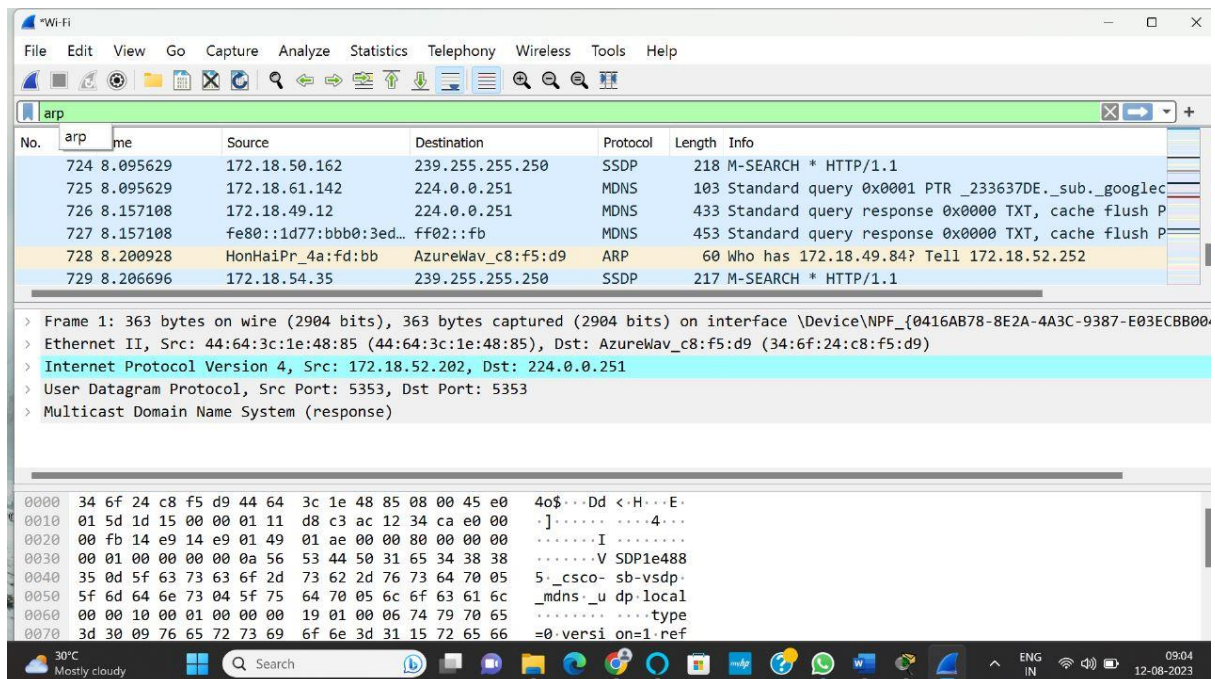
Transmission Control Protocol, Src Port: 443, Dst Port: 54797, Seq: 1, Ack: 1, Len: 239

Transport Layer Security

5.STMP-SIMATS WIFI



6.ARP-SIMATS WIFI



WIRE SHARK MOBILE HOTSPOT

1.ARP

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Info
9	0.616623	c2:e6:29:dd:b6:6b	AzureWav_c8:f5:d9	ARP	42	192.168.85.22 is at c2:e6:29:dd:b6:6b
10	0.676461	2401:4900:628c:de34...	2603:1046:c06:d::2	TLSv1.2	228	Application Data, Application Data
11	0.735523	fe80::c0e6:29ff:fed...	fe80::db49:ea2:3ef7...	ICMPv6	86	Neighbor Solicitation for fe80::db49:ea2:3ef7:8783
12	0.735601	fe80::db49:ea2:3ef7...	fe80::c0e6:29ff:fed...	ICMPv6	86	Neighbor Advertisement fe80::db49:ea2:3ef7:8783
13	1.119779	fe80::db49:ea2:3ef7...	fe80::c0e6:29ff:fed...	ICMPv6	86	Neighbor Solicitation for fe80::c0e6:29ff:fedd:b66b
14	1.142584	fe80::c0e6:29ff:fed...	fe80::db49:ea2:3ef7...	ICMPv6	78	Neighbor Advertisement fe80::c0e6:29ff:fedd:b66b

> Frame 1: 1112 bytes on wire (8896 bits), 1112 bytes captured (8896 bits) on interface \Device\NPF_{0416AB78-8E2A-4A3C-9387-E03ECBB00484}

> Ethernet II, Src: AzureWav_c8:f5:d9 (34:6f:24:c8:f5:d9), Dst: c2:e6:29:dd:b6:6b (c2:e6:29:dd:b6:6b)

> Internet Protocol Version 6, Src: 2401:4900:628c:de34:cc9b:efa3:9311:7508, Dst: 2603:1046:c06:d::2

> Transmission Control Protocol, Src Port: 54933, Dst Port: 443, Seq: 1, Ack: 1, Len: 1038

> Transport Layer Security

0000 c2 e6 29 dd b6 6b 34 6f 24 c8 f5 d9 86 dd 60 09 ..)k4o \$.....
0010 ad aa 04 22 06 3f 24 01 49 00 62 8c de 34 cc 9b ..."?\$-I.b.4..
0020 ef a3 93 11 75 08 26 03 10 46 0c 06 00 00 00 00u&-F.....
0030 00 00 00 00 00 02 d6 95 01 bb 47 a9 10 86 9d d5G.....
0040 84 4f 50 18 03 fe 83 4a 00 00 17 03 03 00 1a 58 .OP....J.....X
0050 af b4 2f cf fb c2 a0 14 5d e5 66 9a a9 16 24 a6 ./.....].f...\$..
0060 15 79 49 5c a8 65 fb dd 4c 17 03 03 ea 15 81 .yI\..e..L.....
0070 9c dd 9e 08 b6 c7 b1 b0 bc c4 a5 5f ba f2 3a 40:;@

30°C Mostly cloudy

Search

ENG IN 09:09 12-08-2023

2.HTTP

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
93	6.731264	23.215.215.248	192.168.85.93	TCP	54	443 → 54929 [ACK] Seq=9126 Ack=26601 Win=501 Len=
94	6.731264	23.215.215.248	192.168.85.93	TCP	54	443 → 54929 [ACK] Seq=9126 Ack=29401 Win=501 Len=
95	6.731264	23.215.215.248	192.168.85.93	TCP	54	443 → 54929 [ACK] Seq=9126 Ack=30801 Win=501 Len=
96	6.731264	23.215.215.248	192.168.85.93	TLSv1.2	1454	Ignored Unknown Record
97	6.731368	192.168.85.93	23.215.215.248	TCP	66	54929 → 443 [ACK] Seq=30801 Ack=7726 Win=1024 Len=
98	6.731626	192.168.85.93	23.215.215.248	TLSv1.2	1454	Ignored Unknown Record

> Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{0416AB78-8E2A-4A3C-9387-E03ECBB00484}

> Ethernet II, Src: AzureWav_c8:f5:d9 (34:6f:24:c8:f5:d9), Dst: c2:e6:29:dd:b6:6b (c2:e6:29:dd:b6:6b)

> Internet Protocol Version 4, Src: 192.168.85.93, Dst: 192.168.85.22

> User Datagram Protocol, Src Port: 59825, Dst Port: 53

> Domain Name System (query)

0000 c2 e6 29 dd b6 6b 34 6f 24 c8 f5 d9 08 00 45 00 ..)k4o \$.....E-
0010 00 44 8b 1c 00 00 80 11 83 c8 c0 a8 55 5d c0 a8 .D.....[U]..
0020 55 16 e9 b1 00 35 00 30 ba dd 8a 29 01 00 00 01 U.....5.0...).
0030 00 00 00 00 00 00 08 70 72 f6 74 65 63 74 69 09p rotecti..
0040 71 75 69 63 6b 68 65 61 6c 03 63 6f 6d 00 00 01 quickhea l.com...
0050 00 01 ..

30°C Mostly cloudy

Search

ENG IN 09:08 12-08-2023

3.TCP

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
1972	23.138835	192.168.85.93	41.63.107.128	TCP	66	54847 → 80 [ACK] Seq=1 Ack=187649 Win=13 Len=0 TS
1973	23.266833	41.63.107.128	192.168.85.93	TCP	1155	80 → 54847 [PSH, ACK] Seq=187649 Ack=1 Win=32362
1974	23.267317	192.168.85.93	41.63.107.128	TCP	66	54847 → 80 [FIN, ACK] Seq=1 Ack=188738 Win=16 Len
1975	23.337185	41.63.107.128	192.168.85.93	TCP	66	80 → 54847 [FIN, ACK] Seq=188738 Ack=2 Win=32362
1976	23.337272	192.168.85.93	41.63.107.128	TCP	66	54847 → 80 [ACK] Seq=2 Ack=188739 Win=16 Len=0 TS

> Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{0416AB78-8E2A-4A3C-9387-E03ECBB00484}

> Ethernet II, Src: c2:e6:29:dd:b6:6b (c2:e6:29:dd:b6:6b), Dst: AzureWav_c8:f5:d9 (34:6f:24:c8:f5:d9)

> Internet Protocol Version 6, Src: 2406:dala:52f:6201:649e:91f2:19c1:7048, Dst: 2401:4900:628c:de34:cc9b:efa3:9311:7508

> Transmission Control Protocol, Src Port: 443, Dst Port: 54882, Seq: 0, Ack: 1, Len: 0

```

0000 34 6f 24 c8 f5 d9 c2 e6 29 dd b6 6b 86 dd b6 8d 40 $.....)..k..k.
0010 6f 1f 00 20 06 f0 24 06 da 1a 05 2f 62 01 64 9e o... ..$.../b.d.
0020 91 f2 19 c1 70 48 24 01 49 00 62 8c de 34 cc 9b ....pH$. I..b..4..
0030 ef a3 93 11 75 08 01 bb d6 62 ac 3a 04 61 fa 82 ....u....b...a...
0040 50 5a 80 12 68 c7 da d6 00 00 02 04 05 78 01 01 PZ..h....x....
0050 04 02 01 03 03 08

```

30°C Mostly cloudy 09:07 12-08-2023

4.UDP

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
28	2.893183	104.208.16.90	192.168.85.93	TLSv1.2	108	Application Data
29	2.893298	192.168.85.93	104.208.16.90	TCP	54	54926 → 443 [ACK] Seq=2617 Ack=6401 Win=261888 Le
30	2.893341	104.208.16.90	192.168.85.93	TCP	54	443 → 54926 [ACK] Seq=6401 Ack=2617 Win=524800 Le
31	2.893680	104.208.16.90	192.168.85.93	TLSv1.2	507	Application Data
32	2.893765	192.168.85.93	104.208.16.90	TCP	54	54926 → 443 [ACK] Seq=2617 Ack=6854 Win=261376 Le
33	3.681124	c2:e6:29:dd:b6:6b	AzureWav c8:f5:d9	ARP	42	Who has 192.168.85.93? Tell 192.168.85.22

> Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{0416AB78-8E2A-4A3C-9387-E03ECBB00484}

> Ethernet II, Src: AzureWav_c8:f5:d9 (34:6f:24:c8:f5:d9), Dst: c2:e6:29:dd:b6:6b (c2:e6:29:dd:b6:6b)

> Internet Protocol Version 4, Src: 192.168.85.93, Dst: 192.168.85.22

> User Datagram Protocol, Src Port: 63537, Dst Port: 53

> Domain Name System (query)

```

0000 c2 e6 29 dd b6 6b 34 6f 24 c8 f5 d9 08 00 45 00 ..)..k4o $.....E-
0010 00 4c 8b 0f 00 00 80 11 83 cd c0 a8 55 5d c0 a8 .L.....[U]..
0020 55 16 f8 31 00 35 00 38 c5 19 4a ed 01 00 00 01 U..1.5.8..J.....
0030 00 00 00 00 00 00 04 73 65 6c 66 06 65 76 65 6e .....s elf..even
0040 74 73 04 64 61 74 61 09 6d 69 63 72 6f 73 6f 66 ts..data..microsof
0050 74 03 63 6f 6d 00 00 01 00 01

```

30°C Mostly cloudy 09:08 12-08-2023

5.SMTP

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

smtp

No.	smtp	Source	Destination	Protocol	Length	Info
217	5.653953	192.168.85.93	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
218	5.669907	192.168.85.93	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
219	5.706371	192.168.85.213	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
220	5.923766	fe80::285a:2a0b:d20...	ff02::1:ffdd:b66b	ICMPv6	86	Neighbor Solicitation for fe80::c0e6:29ff:fedd:b6...
221	6.259931	192.168.85.213	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
222	6.260107	fe80::285a:2a0b:d20...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "OM" question

> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{0416AB78-8E2A-4A3C-9387-E03ECBB00484}

> Ethernet II, Src: AzureWav_15:5e:85 (b4:8c:9d:15:5e:85), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)

> Internet Protocol Version 4, Src: 192.168.85.213, Dst: 224.0.0.251

> User Datagram Protocol, Src Port: 5353, Dst Port: 5353

> Multicast Domain Name System (query)

```

0000  01 00 5e 00 00 fb b4 8c 9d 15 5e 85 08 00 45 00  ..^.....E-
0010  00 38 86 c8 00 00 01 11 3b 74 c0 a8 55 d5 e0 00  -8.....;t..U...
0020  00 fb 14 e9 14 e9 00 24 c9 8d 00 00 00 00 01     .....$.....
0030  00 00 00 00 00 00 04 77 70 61 64 05 6c 6f 63 61  .....wpad-loc
0040  6c 00 00 1c 00 01                                1.....
  
```

30°C Mostly cloudy 09:09 12-08-2023

6.ICMP

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	icmp	Source	Destination	Protocol	Length	Info
137	icmpv6	2401:4900:628c:de34...	2406:da1a:e20:7902:...	TCP	74	54999 → 443 [ACK] Seq=2730 Ack=4389 Win=65536 Len...
81	10.063697	c2:e6:29:dd:b6:6b	Broadcast	ARP	42	Who has 192.168.85.213? Tell 192.168.85.22
82	10.880916	c2:e6:29:dd:b6:6b	Broadcast	ARP	42	Who has 192.168.85.213? Tell 192.168.85.22
83	11.706287	c2:e6:29:dd:b6:6b	Broadcast	ARP	42	Who has 192.168.85.213? Tell 192.168.85.22
84	13.541416	c2:e6:29:dd:b6:6b	Broadcast	ARP	42	Who has 192.168.85.213? Tell 192.168.85.22
85	14.156052	2a03:2880:f237:c7:f...	2401:4900:628c:de34...	TCP	267	5222 → 54900 [PSH, ACK] Seq=2544 Ack=58 Win=269 L...

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{0416AB78-8E2A-4A3C-9387-E03ECBB00484}

> Ethernet II, Src: AzureWav_c8:f5:d9 (34:6f:24:c8:f5:d9), Dst: c2:e6:29:dd:b6:6b (c2:e6:29:dd:b6:6b)

> Internet Protocol Version 6, Src: 2401:4900:628c:de34:cc9b:efa3:9311:7508, Dst: 2600:140f:2400:1a6::1011

> Transmission Control Protocol, Src Port: 54995, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

```

0000  c2 e6 29 dd b6 6b 34 6f 24 c8 f5 d9 86 dd 60 0a  ..)..k4o $.....
0010  f3 e6 00 14 06 3f 24 01 49 00 62 8c de 34 cc 9b  ....?$. I..b..4..
0020  ef a3 93 11 75 08 26 00 14 0f 24 00 01 a6 00 00  ....u-&...$. ....
0030  00 00 00 00 10 11 d6 d3 01 bb bc ff 75 04 40 b5  .....u@..
0040  b6 ee 50 11 00 fe ca bc 00 00                    ..P.....
  
```

31°C Mostly cloudy 09:10 12-08-2023