

# Wireshark Experiments – WIFI

## 1) TCP-WIFI

The screenshot shows a Wireshark capture of network traffic on a Wi-Fi interface. The filter is set to 'tcp'. The packet list shows several TCP packets, with packet 5597 selected. The packet details pane shows the following structure:

- Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF\_{0416AB78-8E2A-4A3C-9387-E03ECB8000}
- 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

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 01 00 5e 7f ff fa 34 6f 24 c8 f5 d9 08 00 45 00  ..^...4o $.....E-
0010 00 cb af 34 00 00 01 11 38 96 ac 12 35 4b ef ff  ....4....8...5K..
0020 ff fa db 12 07 6c 00 b7 e4 2a 4d 2d 53 45 41 52  ....1... *M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48  CH * HTTP/1.1..H
0040 4f 53 54 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 4d 41 4e 3a 20  .250:1900..MAN:
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d  "ssdp:discover"
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a  .MX: 1..ST: urn:
```

## 2) UDP-WIFI

The screenshot shows a Wireshark capture of network traffic on a Wi-Fi interface. The filter is set to 'udp'. The packet list shows several UDP packets, with packet 2477 selected. The packet details pane shows the following structure:

- Frame 1: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface \Device\NPF\_{0416AB78-8E2A-4A3C-9387-E03ECB8000}
- 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

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 34 6f 24 c8 f5 d9 66 8f 30 5e 4f 6e 86 dd 60 00  4o$...f. 0^On...
0010 00 00 00 00 00 01 fe 80 00 00 00 00 00 64 8f  ....d.
0020 30 ff fe 5e 4f 6e ff 02 00 00 00 00 00 00 00  0...^On.....
0030 00 00 00 00 00 16 3a 00 05 02 00 00 01 00 8f 00  ....:.....
0040 35 90 00 00 00 04 04 00 00 00 ff 02 00 00 00 00  5.....
0050 00 00 00 00 00 01 ff 00 00 00 04 00 00 00 ff 02  ....
0060 00 00 00 00 00 00 00 00 00 01 ff 5e 4f 6e 04 00  ....^On...
0070 00 00 ff 05 00 00 00 00 00 00 00 00 00 00 00  ....
```

### 3) HTTP-WIFI

Wireshark capture of HTTP traffic over Wi-Fi. The packet list shows several TCP ACKs and an ICMPv6 Router Solicitation. The packet details pane shows the structure of an Ethernet II frame, an IPv4 packet, and a TCP segment. The packet bytes pane shows the raw hex and ASCII data.

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		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-E03ECB00...}

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

### 4) ARP-WIFI

Wireshark capture of ARP traffic over Wi-Fi. The packet list shows several SSDP and MDNS packets, and an ARP request. The packet details pane shows the structure of an Ethernet II frame, an IPv4 packet, and an ARP request. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
724	8.095629	172.18.50.162	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
725	8.095629	172.18.61.142	224.0.0.251	MDNS	103	Standard query 0x0001 PTR _233637DE._sub._googlec
726	8.157108	172.18.49.12	224.0.0.251	MDNS	433	Standard query response 0x0000 TXT, cache flush P
727	8.157108	fe80::1d77:bbb0:3ed... ff02::fb		MDNS	453	Standard query response 0x0000 TXT, cache flush P
728	8.200928	HonHaiPr_4a:fd:bb	AzureWav_c8:f5:d9	ARP	60	Who has 172.18.49.84? Tell 172.18.52.252
729	8.206696	172.18.54.35	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

Frame 1: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits) on interface \Device\NPF\_{0416AB78-8E2A-4A3C-9387-E03ECB00...}

Ethernet II, Src: 44:64:3c:1e:48:85 (44:64:3c:1e:48:85), Dst: AzureWav\_c8:f5:d9 (34:6f:24:c8:f5:d9)

Internet Protocol Version 4, Src: 172.18.52.202, Dst: 224.0.0.251

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

Multicast Domain Name System (response)

## 5) SMTP-WIFI

Wireshark capture of SMTP traffic over Wi-Fi. The packet list shows several ARP requests and ICMPv6 messages. The selected packet (No. 1414) is an ARP request from Pegatron\_71:9e:bf to AzureWav\_c8:f5:d9. The packet details show Ethernet II, Src: AzureWav\_16:a9:29, Dst: AzureWav\_c8:f5:d9, and Address Resolution Protocol (request). The packet bytes are displayed in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1414	11.281620	Pegatron_71:9e:bf	AzureWav_c8:f5:d9	ARP	60	Who has 172.18.61.209? Tell 172.18.52.139
1415	11.292036	CloudNet_c5:19:07	AzureWav_c8:f5:d9	ARP	60	Who has 172.18.61.209? Tell 172.18.50.116
1416	11.305715	fe80::4664:3cff:fe1...	ff02::1:fffe:7c6d	ICMPv6	86	Neighbor Solicitation for fe80::7de5:e51c:5bfe:7c...
1417	11.316219	IntelCor_bf:26:dd	AzureWav_c8:f5:d9	ARP	60	Who has 172.18.61.209? Tell 172.18.53.189
1418	11.442510	192.168.137.211	192.168.137.255	NBNS	110	Registration NB DESKTOP-MRJA4CC<20>
1419	11.457140	fe80::47a:dcff:fe38...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF\_{0416AB78-8E2A-4A3C-9387-E03ECB00484}.  
 Ethernet II, Src: AzureWav\_16:a9:29 (14:13:33:16:a9:29), Dst: AzureWav\_c8:f5:d9 (34:6f:24:c8:f5:d9)  
 Address Resolution Protocol (request)

```

0000  34 6f 24 c8 f5 d9 14 13 33 16 a9 29 08 06 00 01  4o$. . . . . 3.. ) . . . .
0010  08 00 06 04 00 01 14 13 33 16 a9 29 ac 12 3d 09  . . . . . 3.. ) . . = .
0020  00 00 00 00 00 00 ac 12 31 54 00 00 00 00 00 00  . . . . . 1T . . . . .
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . .
  
```

## 6) ICMP-WIFI

Wireshark capture of ICMP traffic over Wi-Fi. The packet list shows several MDNS and DHCP messages. The selected packet (No. 664) is a Standard query response from 172.18.53.159 to 224.0.0.251. The packet details show Ethernet II, Src: Cisco\_c8:4d:57, Dst: AzureWav\_c8:f5:d9, Internet Protocol Version 4, and Transport Layer Security.

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-E03ECB00484}.  
 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

```

0000  34 6f 24 c8 f5 d9 38 90 a5 c8 4d 57 08 00 45 00  4o$. . . . . 8.. . MW . . E .
0010  01 17 d7 b5 40 00 3e 06 f0 7f cc 4f c5 fe ac 12  . . . @ . > . . . 0 . . . .
0020  35 4b 01 bb d6 d0 ed 32 e0 e4 31 9c af 23 50 18  5K . . . . . 2 . . 1 . . # P .
0030  00 f5 c4 d6 00 00 17 03 03 00 c4 00 00 00 00 00  . . . . .
0040  00 00 05 a8 58 89 8b ad 5a 7e 03 bf 69 e8 23 69  . . . X . . . Z ~ . . i . # i
0050  2f 22 a4 31 30 84 6b 09 09 4b 3f 0b d8 cb fb ce  / " . 10 . k . . K ? . . . . .
0060  3a d4 9b f0 f9 5b 32 58 8c fc 80 f7 f8 d1 ee 0c  : . . . [ 2X . . . . .
0070  d8 29 de 96 53 ca a6 58 dc b1 21 f8 cf 60 d0 e8  . ) . . S . . X . . ! . . . .
  
```