

Wireshark Experiments-Mobile WIFI

1) TCP-Mobile WIFI

The screenshot shows a Wireshark capture of TCP traffic on a mobile Wi-Fi interface. The packet list pane displays several TCP packets, including an ACK and a FIN. The packet details pane shows the structure of a TCP segment, including the Ethernet II header, Internet Protocol Version 6 header, and Transmission Control Protocol header. The packet bytes pane shows the raw data in hexadecimal and ASCII.

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:d81a: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

2) UDP-Mobile WIFI

The screenshot shows a Wireshark capture of UDP traffic on a mobile Wi-Fi interface. The packet list pane displays several UDP packets, including an ARP request and a DNS query. The packet details pane shows the structure of a UDP segment, including the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol header. The packet bytes pane shows the raw data in hexadecimal and ASCII.

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)

3) HTTP-Mobile WIFI

The screenshot shows a Wireshark capture of HTTP traffic on a mobile Wi-Fi interface. The packet list shows several packets, with the selected packet being a Domain Name System (query) packet. The packet details pane shows the structure of the packet, including the Ethernet II header, Internet Protocol Version 4 header, User Datagram Protocol header, and Domain Name System (query) header. The packet bytes pane shows the raw data of the packet.

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 00 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.

0030 00 00 00 00 00 00 08 70 72 6f 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 ..

4) ARP-Mobile WIFI

The screenshot shows a Wireshark capture of ARP traffic on a mobile Wi-Fi interface. The packet list shows several packets, with the selected packet being an ARP request. The packet details pane shows the structure of the packet, including the Ethernet II header, Internet Protocol Version 6 header, Transmission Control Protocol header, and Transport Layer Security header. The packet bytes pane shows the raw data of the packet.

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:ea2:3ef7:878
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:b6
14	1.142584	fe80::c0e6:29ff:fed...	fe80::db49:ea2:3ef7...	ICMPv6	78	Neighbor Advertisement fe80::c0e6:29ff:fedd:b6b

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 0d 00 00 ...u.&. .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 03 ea 15 81 .yI\..e..L.....

0070 9c dd 9e 08 b6 c7 b1 b0 bc c4 a5 5f ba f2 3a 40:@

5) SMTP-Mobile WIFI

The screenshot shows a Wireshark capture of an ICMPv6 Neighbor Solicitation packet. The packet list table is as follows:

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, "QM" question

The packet details pane shows the following structure:

- Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{0416AB78-8E2A-4A3C-9387-E03ECB00484}.
- 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)

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

```

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 00 01  .....$ .....
0030  00 00 00 00 00 00 04 77 70 61 64 05 6c 6f 63 61  .....w pad.loca
0040  6c 00 00 1c 00 01                                1.....
  
```

6) ICMP-Mobile WIFI

The screenshot shows a Wireshark capture of an ICMPv6 Echo Request packet. The packet list table is as follows:

No.	icmp	Source	Destination	Protocol	Length	Info
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...

The packet details pane shows the following structure:

- Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{0416AB78-8E2A-4A3C-9387-E03ECB00484}.
- 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

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

```

0000  c2 e6 29 dd b6 6b 34 f5 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.....
  
```