



In the name of God

University of Tehran

ECE faculty



Computer Networks

Wireshark Lab

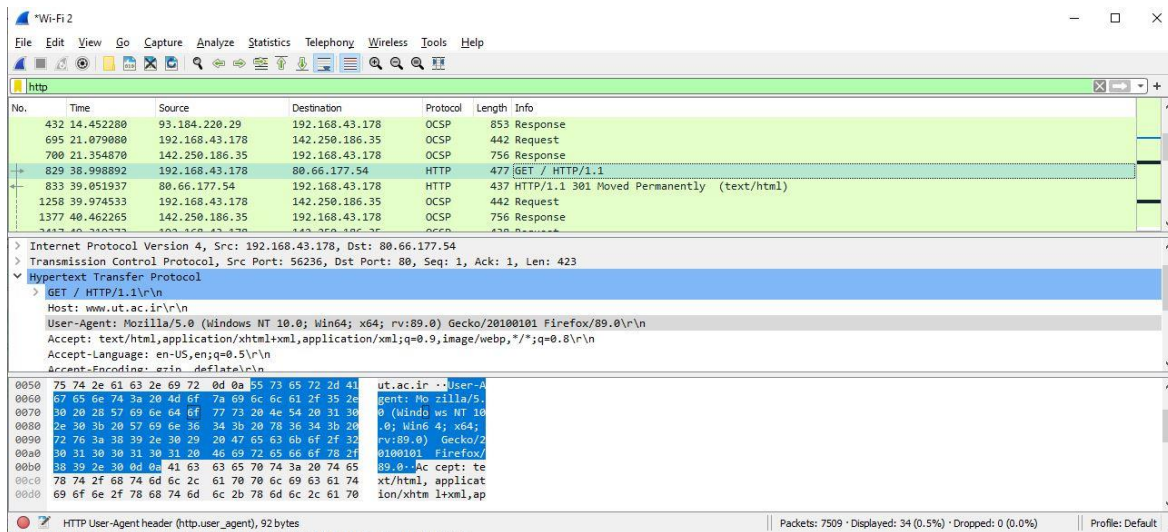
Ashkan Jafari Fesharaki

810197483

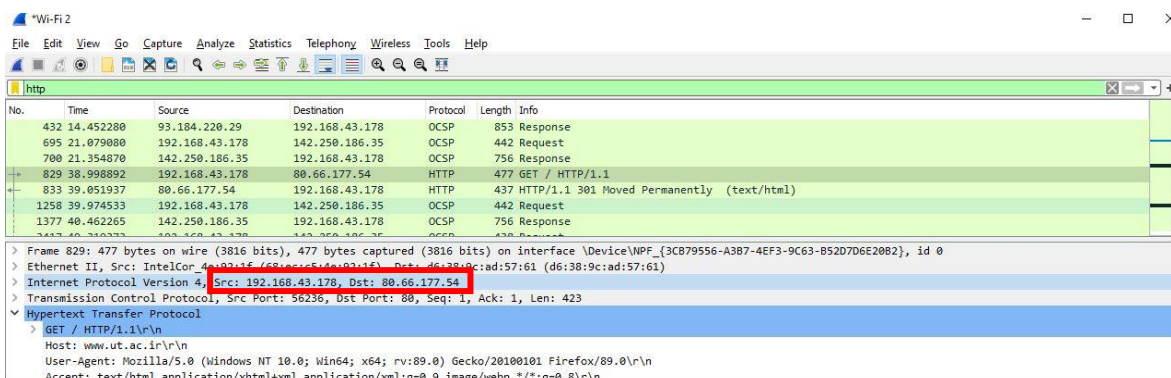
Khordad

1400

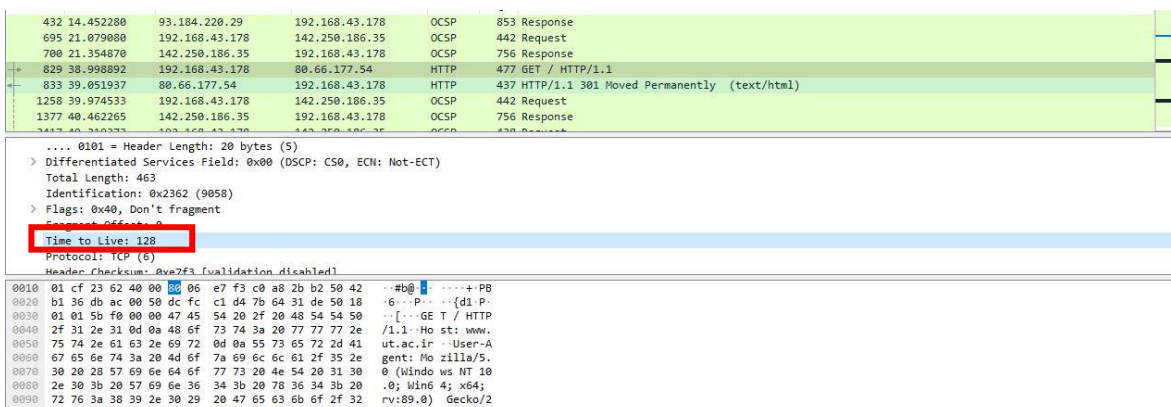
Part1: Capturing and analyzing Ethernet and IP headers



- 1) It is mentioned in the below picture, Source is 192.168.43.178 and Destination is 80.66.177.54.



- 2)



3)

432	14.452280	93.184.220.29	192.168.43.178	OCSP	853	Response
695	21.079080	192.168.43.178	142.250.186.35	OCSP	442	Request
700	21.354870	142.250.186.35	192.168.43.178	OCSP	756	Response
829	38.998892	192.168.43.178	80.66.177.54	HTTP	477	GET / HTTP/1.1
833	39.051937	80.66.177.54	192.168.43.178	HTTP	437	HTTP/1.1 301 Moved Permanently (text/html)
1258	39.974533	192.168.43.178	142.250.186.35	OCSP	442	Request
1377	40.462265	142.250.186.35	192.168.43.178	OCSP	756	Response

> Frame 829: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface \Device\NPF_{3CB79556-A3B7-4EF3-9C63-B52D7D6E20B2}, id 0

> Ethernet II, Src: IntelCor_4e:92:1f (68:ec:c5:4e:92:1f), Dst: d6:38:9c:ad:57:61 (d6:38:9c:ad:57:61)

> Destination: d6:38:9c:ad:57:61 (d6:38:9c:ad:57:61)

> Source: IntelCor_4e:92:1f (68:ec:c5:4e:92:1f)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.43.178, Dst: 80.66.177.54

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

4) I use Ethernet through Hotspot so this is my mobile address:

432	14.452280	93.184.220.29	192.168.43.178	OCSP	853	Response
695	21.079080	192.168.43.178	142.250.186.35	OCSP	442	Request
700	21.354870	142.250.186.35	192.168.43.178	OCSP	756	Response
829	38.998892	192.168.43.178	80.66.177.54	HTTP	477	GET / HTTP/1.1
833	39.051937	80.66.177.54	192.168.43.178	HTTP	437	HTTP/1.1 301 Moved Permanently (text/html)
1258	39.974533	192.168.43.178	142.250.186.35	OCSP	442	Request
1377	40.462265	142.250.186.35	192.168.43.178	OCSP	756	Response

> Frame 829: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface \Device\NPF_{3CB79556-A3B7-4EF3-9C63-B52D7D6E20B2}, id 0

> Ethernet II, Src: IntelCor_4e:92:1f (68:ec:c5:4e:92:1f), Dst: d6:38:9c:ad:57:61 (d6:38:9c:ad:57:61)

> Destination: d6:38:9c:ad:57:61 (d6:38:9c:ad:57:61)

> Source: IntelCor_4e:92:1f (68:ec:c5:4e:92:1f)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.43.178, Dst: 80.66.177.54

> Transmission Control Protocol, Src Port: 56236, Dst Port: 80, Seq: 1, Ack: 1, Len: 423

Source Port: 56236

Destination Port: 80

0000 00 30 06 00 57 61 68 ec c5 4e 92 1f 08 00 45 00 8: Wah: N: ...

0010 01 cf 23 62 40 00 00 06 e7 f3 c0 a8 2b b2 50 42 ..#b@...+PB

0020 b1 36 db ac 00 50 dc fc c1 d4 7b 64 31 de 50 18 ..6..P...[d1.P

0030 01 01 5b f0 00 00 47 45 54 20 2f 20 48 54 54 50 ..[...GE T / HTTP

0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1..Ho st: www.

0050 75 74 2e 61 63 2e 69 72 0d 0a 55 73 65 72 2d 41 ut.ac.ir ..User-A

0060 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e gent: Mo zilla/5.

0070 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 0 (Windo ws NT 10

0080 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 3b 20 .0; Win6 4; x64;

5)

No.	Time	Source	Destination	Protocol	Length	Info
432	14.452280	93.184.220.29	192.168.43.178	OCSP	853	Response
695	21.079080	192.168.43.178	142.250.186.35	OCSP	442	Request
700	21.354870	142.250.186.35	192.168.43.178	OCSP	756	Response
829	38.998892	192.168.43.178	80.66.177.54	HTTP	477	GET / HTTP/1.1
833	39.051937	80.66.177.54	192.168.43.178	HTTP	437	HTTP/1.1 301 Moved Permanently (text/html)
1258	39.974533	192.168.43.178	142.250.186.35	OCSP	442	Request
1377	40.462265	142.250.186.35	192.168.43.178	OCSP	756	Response

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.43.178, Dst: 80.66.177.54

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 463

Identification: 0x2362 (9050)

Flags: 0x40, Don't fragment

Fragment Offset: 0

0000 d6 38 9c ad 57 61 68 ec c5 4e 92 1f 08 00 45 00 8: Wah: N: ...

0010 01 cf 23 62 40 00 00 06 e7 f3 c0 a8 2b b2 50 42 ..#b@...+PB

0020 b1 36 db ac 00 50 dc fc c1 d4 7b 64 31 de 50 18 ..6..P...[d1.P

0030 01 01 5b f0 00 00 47 45 54 20 2f 20 48 54 54 50 ..[...GE T / HTTP

0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1..Ho st: www.

0050 75 74 2e 61 63 2e 69 72 0d 0a 55 73 65 72 2d 41 ut.ac.ir ..User-A

0060 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e gent: Mo zilla/5.

0070 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 0 (Windo ws NT 10

0080 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 3b 20 .0; Win6 4; x64;

- 6) As it is shown below there is 52 bytes in the Ethernet frame which 14 bytes are for Ethernet frame, 20 bytes for IP header and at the end 20 bytes for TCP header.

http						
No.	Time	Source	Destination	Protocol	Length	Info
432	14.452280	93.184.220.29	192.168.43.178	OCSP	853	Response
695	21.079080	192.168.43.178	142.250.186.35	OCSP	442	Request
700	21.354870	142.250.186.35	192.168.43.178	OCSP	756	Response
829	38.998892	192.168.43.178	80.66.177.54	HTTP	477	GET / HTTP/1.1
833	39.051937	80.66.177.54	192.168.43.178	HTTP	437	HTTP/1.1 301 Moved Permanently (text/html)
1258	39.974533	192.168.43.178	142.250.186.35	OCSP	442	Request
1377	40.462265	142.250.186.35	192.168.43.178	OCSP	756	Response
3417	49.319373	192.168.43.178	142.250.186.35	OCSP	438	Request
3538	50.151924	142.250.186.35	192.168.43.178	OCSP	756	Response
3539	50.152824	192.168.43.178	142.250.186.35	OCSP	438	Request

Window: 257
[Calculated window size: 65792]
[Window size scaling factor: 256]
Checksum: 0x5bf0 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]
TCP payload (423 bytes)
Hypertext Transfer Protocol

0030	01 01 5b f0 00 00 47 45	54 20 2f 20 48 54 54 50	...GET / HTTP
0040	2f 31 2e 31 0d 0a 48 6f	73 74 3a 20 77 77 77 2e	/1.1..Host: www.
0050	75 74 2e 61 63 2e 69 72	0d 0a 55 73 65 72 2d 41	ut.ac.ir --User-A
0060	67 65 6e 74 3a 20 4d 6f	7a 69 6c 6c 61 2f 35 2e	gent: Mozilla/5.
0070	30 20 28 57 69 6e 64 6f	77 73 20 4e 54 20 31 30	0 (Windows NT 10
0080	2e 30 3b 20 57 69 6e 36	34 3b 20 78 36 34 3b 20	.0; Win64; x64;
0090	72 76 3a 38 39 2e 30 29	20 47 65 63 6b 6f 2f 32	rv:89.0) Gecko/2
00a0	30 31 30 30 31 30 31 20	46 69 72 65 66 6f 78 2f	0100101 Firefox/
00b0	38 39 2e 30 0d 0a 41 63	63 65 70 74 3a 20 74 65	89.0..Accept: te
00c0	78 74 2f 68 74 6d 6c 2c	61 70 70 6c 69 63 61 74	xt/html, applicat
00d0	69 6f 6e 2f 78 68 74 6d	6c 2b 78 6d 6c 2c 61 70	ion/xhtml+xml,ap

Part 2. The Address Resolution Protocol

1) s

Internet Address: IP Address

Physical Address: the MAC Address

Type: The protocol type

```
C:\Users\Asus>arp -a

Interface: 192.168.43.178 --- 0xb
Internet Address      Physical Address      Type
192.168.43.1          d6-38-9c-ad-57-61    dynamic
192.168.43.255        ff-ff-ff-ff-ff-ff    static
224.0.0.2              01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```


2)

a.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61
20	3.276705	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61
23	6.553477	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61
36	9.830145	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61
49	12.567787	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	Who has 192.168.43.178? Tell 192.168.43.1
50	12.567829	IntelCor_4e:92:1f	d6:38:9c:ad:57:61	ARP	42	192.168.43.178 is at 68:ec:c5:4e:92:1f
51	13.106996	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61
72	16.383762	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61
97	19.660633	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61
98	23.025883	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61

Frame 49: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{3CB79556-A3B7-4EF3-9C63-B52D7D6E20B2}, id 0
 Ethernet II, Src: d6:38:9c:ad:57:61 (d6:38:9c:ad:57:61), Dst: IntelCor_4e:92:1f (68:ec:c5:4e:92:1f)
 Destination: IntelCor_4e:92:1f (68:ec:c5:4e:92:1f)
 Address: IntelCor_4e:92:1f (68:ec:c5:4e:92:1f)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)
 Source: d6:38:9c:ad:57:61 (d6:38:9c:ad:57:61)
 Address: d6:38:9c:ad:57:61 (d6:38:9c:ad:57:61)
1. = LG bit: Locally administered address (this is NOT the factory default)
0. = IG bit: Individual address (unicast)
 Type: ARP (0x0806)

0000 68 ec c5 4e 92 1f d6 38 9c ad 57 61 08 06 00 01 h-N-8-Wah-
 0010 08 00 06 04 00 02 68 ec c5 4e 92 1f c0 a8 2b b2h-N-+
 0020 d6 38 9c ad 57 61 c0 a8 2b b28-Wa-+

- The hex value of ARP is 0x0806. The corresponding upper layer protocol is ARP.
- According to the above figure: 0x001(1 in decimal).
- Yes, it contains IP address of the sender and it's (192.168.43.178)
- The field "Target MAC address" is set to "00:00:00:00:00:00" to question the machine whose corresponding IP address (192.168.43.1) is being queried.

3)

a. 0x002

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61
20	3.276705	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61
23	6.553477	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61
36	9.830145	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61
49	12.567787	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	Who has 192.168.43.178? Tell 192.168.43.1
50	12.567829	IntelCor_4e:92:1f	d6:38:9c:ad:57:61	ARP	42	192.168.43.178 is at 68:ec:c5:4e:92:1f
51	13.106996	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61
72	16.383762	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61
97	19.660633	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61
98	23.025883	d6:38:9c:ad:57:61	IntelCor_4e:92:1f	ARP	42	192.168.43.1 is at d6:38:9c:ad:57:61

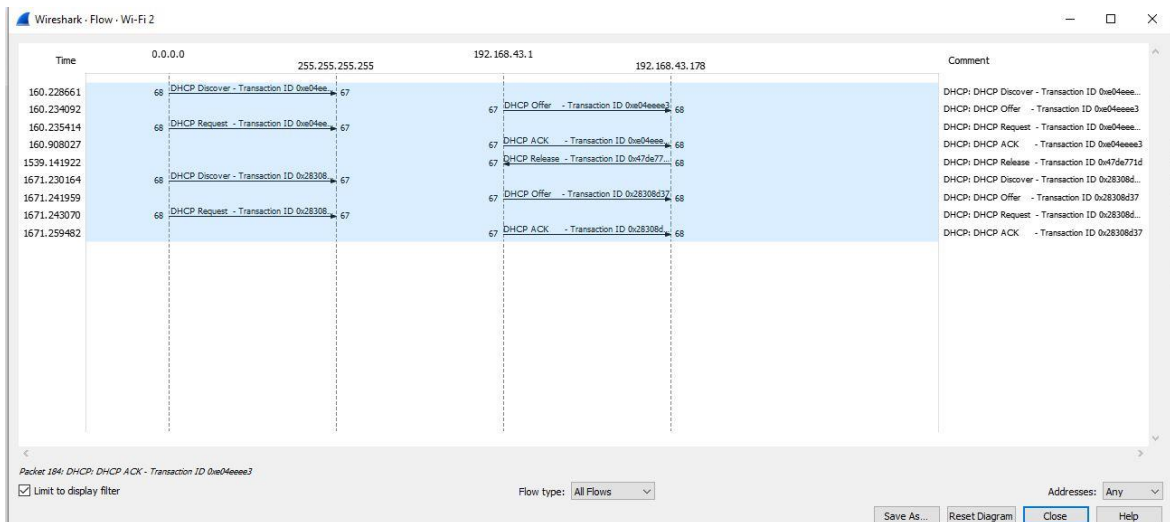
Address Resolution Protocol (reply)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: reply (2)
 Sender MAC address: IntelCor_4e:92:1f (68:ec:c5:4e:92:1f)
 Sender IP address: 192.168.43.178
 Target MAC address: d6:38:9c:ad:57:61 (d6:38:9c:ad:57:61)
 Target IP address: 192.168.43.1

0000 d6 38 9c ad 57 61 68 ec c5 4e 92 1f 08 06 00 01 -8-Wah-N-
 0010 08 00 06 04 00 02 68 ec c5 4e 92 1f c0 a8 2b b2h-N-+
 0020 d6 38 9c ad 57 61 c0 a8 2b b28-Wa-+

- b. The answer to the earlier ARP request appears in the "Sender MAC address" field, which contains the Ethernet address 68:ec:c5:4e:92:1f for the sender with IP address 192.168.43.178
- c. According to the above figure, Source: 68:ec:c5:4e:92:1f and Destination: d6:38:9c:ad:57:61.

Part 3. DHCP

1)



- 2) The values which differentiate the Discover message from the Request message are in "Option(53): DHCP Message Type".

The screenshot shows the Wireshark interface with a packet capture of a DHCP Discover message. The packet list shows the following details:

No.	Time	Source	Destination	Protocol	Length	Info
180	160.228661	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe04eee3
181	160.234092	192.168.43.1	192.168.43.178	DHCP	351	DHCP Offer - Transaction ID 0xe04eee3
182	160.235414	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0xe04eee3
184	160.908027	192.168.43.1	192.168.43.178	DHCP	362	DHCP ACK - Transaction ID 0xe04eee3
7824	1539.141922	192.168.43.178	192.168.43.1	DHCP	342	DHCP Release - Transaction ID 0x47de771d
8467	1671.230164	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x28308d37
8468	1671.241959	192.168.43.1	192.168.43.178	DHCP	351	DHCP Offer - Transaction ID 0x28308d37
8469	1671.243070	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x28308d37
8470	1671.259482	192.168.43.1	192.168.43.178	DHCP	362	DHCP ACK - Transaction ID 0x28308d37

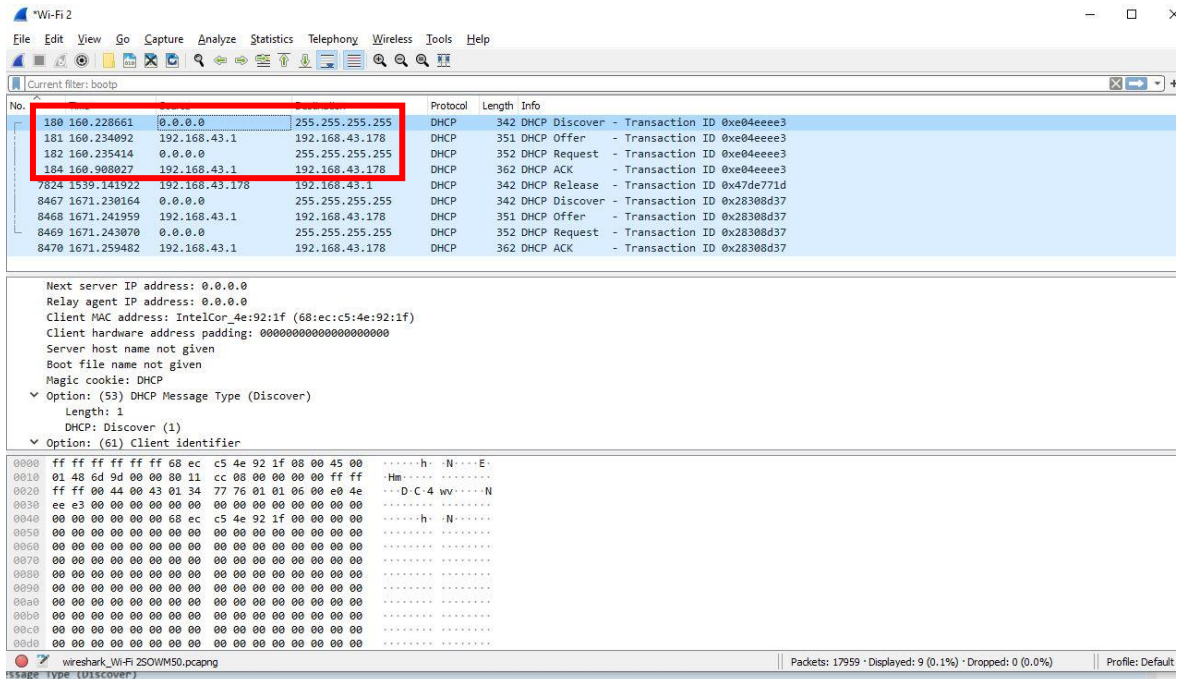
The packet details pane shows the following information:

- Next server IP address: 0.0.0.0
- Relay agent IP address: 0.0.0.0
- Client MAC address: IntelCor_4e:92:1f (68:ec:c5:4e:92:1f)
- Client hardware address padding: 00000000000000000000
- Server host name not given
- Boot file name not given
- Option(53) DHCP Message Type (Discover)
 - Length: 1
 - DHCP: Discover (1)
- Option(61) Client Identifier

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and DHCP message.

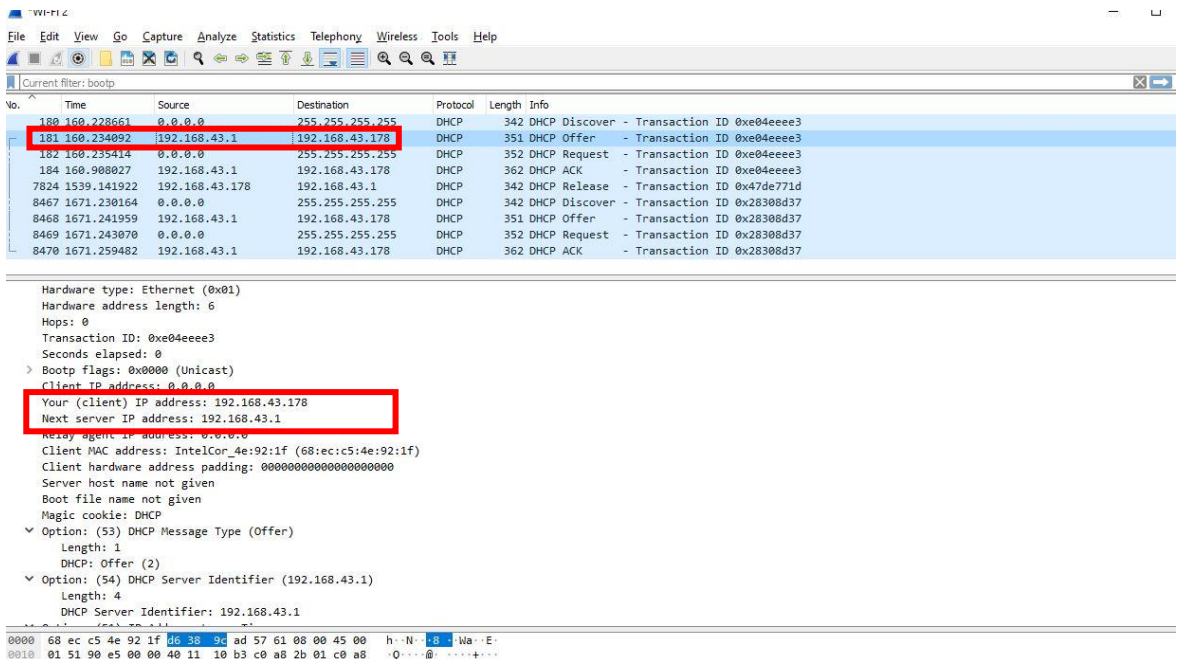
3) According to the above picture, Transaction ID in each of first four is 0xe04eeee93. Transaction-ID in the second set is 0x28308d37. The purpose of **transaction ID** is that the host can differentiate between different requests made by the user.

4)



5) The IP address of my DHCP server is 192.168.43.1

6) The DHCP server offered the IP address 192.168.43.178 to my client.



7) Yes, in option(50) we observe request IP address is 192.168.43.178.

*Wi-Fi 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: bootp

No.	Time	Source	Destination	Protocol	Length	Info
180	160.228661	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe04eeee3
181	160.234092	192.168.43.1	192.168.43.178	DHCP	351	DHCP Offer - Transaction ID 0xe04eeee3
182	160.235414	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0xe04eeee3
184	160.908027	192.168.43.1	192.168.43.178	DHCP	362	DHCP ACK - Transaction ID 0xe04eeee3
7824	1539.141922	192.168.43.178	192.168.43.1	DHCP	342	DHCP Release - Transaction ID 0x47de771d
8467	1671.230164	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x28308d37
8468	1671.241959	192.168.43.1	192.168.43.178	DHCP	351	DHCP Offer - Transaction ID 0x28308d37
8469	1671.243070	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x28308d37
8470	1671.259482	192.168.43.1	192.168.43.178	DHCP	362	DHCP ACK - Transaction ID 0x28308d37

Relay agent IP address: 0.0.0.0
Client MAC address: IntelCor_4e:92:1f (68:ec:c5:4e:92:1f)
Client hardware address padding: 000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

- Option: (53) DHCP Message Type (Request)
 - Length: 1
 - DHCP: Request (3)
- Option: (61) Client identifier
 - Length: 7
 - Hardware type: Ethernet (0x01)
 - Client MAC address: IntelCor_4e:92:1f (68:ec:c5:4e:92:1f)
- Option: (50) Requested IP Address (192.168.43.178)
 - Length: 4
 - Requested IP Address: 192.168.43.178
- Option: (54) DHCP Server Identifier (192.168.43.1)
 - Length: 4
 - DHCP Server Identifier: 192.168.43.1
- Option: (12) Host Name
 - Length: 6

0120 68 ec c5 4e 92 1f 32 04 c0 a8 2b b2 36 04 c0 a8 h...N...2...+...6...
0130 2b 01 0c 06 41 53 48 4b 41 4e 51 09 00 00 00 41 +...ASHK ANQ...+...A

DHCP/BOOTP option type (dhcp.option.type), 6 bytes

8) The purpose of a lease is to limit the length of time that a client can use an IP address.

*Wi-Fi 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: bootp

No.	Time	Source	Destination	Protocol	Length	Info
180	160.228661	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe04eeee3
181	160.234092	192.168.43.1	192.168.43.178	DHCP	351	DHCP Offer - Transaction ID 0xe04eeee3
182	160.235414	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0xe04eeee3
184	160.908027	192.168.43.1	192.168.43.178	DHCP	362	DHCP ACK - Transaction ID 0xe04eeee3
7824	1539.141922	192.168.43.178	192.168.43.1	DHCP	342	DHCP Release - Transaction ID 0x47de771d
8467	1671.230164	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x28308d37
8468	1671.241959	192.168.43.1	192.168.43.178	DHCP	351	DHCP Offer - Transaction ID 0x28308d37
8469	1671.243070	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x28308d37
8470	1671.259482	192.168.43.1	192.168.43.178	DHCP	362	DHCP ACK - Transaction ID 0x28308d37

Hops: 0
Transaction ID: 0xe04eeee3
Seconds elapsed: 0

- Bootp flags: 0x0000 (Unicast)
- Client IP address: 0.0.0.0
- Your (client) IP address: 192.168.43.178
- Next server IP address: 192.168.43.1
- Relay agent IP address: 0.0.0.0
- Client MAC address: IntelCor_4e:92:1f (68:ec:c5:4e:92:1f)
- Client hardware address padding: 000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (Offer)
 - Length: 1
 - DHCP: Offer (2)
- Option: (51) IP Address Lease Time
 - Length: 4
 - IP Address Lease Time: (3600s) 1 hour
- Option: (58) Renewal Time Value
- Option: (59) Rebinding Time Value
- Option: (1) Subnet Mask (255.255.255.0)

0120 a8 2b 01 33 04 00 00 0e 18 3a 04 00 00 07 08 3b +...+...:.....
0130 04 00 00 0c 4e 01 04 ff ff ff 00 1c 04 c0 a8 2bN...+...+