

## Experiment 4 - Usage of Wireshark

### Directory

<b>Part 1-Ethernet frame analyzing.....</b>	<b>2</b>
1. Open file ethernet--ethereal-trace-1 in wireshark.....	2
2. Analyze ARP frames.....	2
3. Question 10 of Wireshark_Ethernet_ARP_v8.0.pdf.....	3
4. Question 11 of Wireshark_Ethernet_ARP_v8.0.pdf.....	4
5. Question 13 of Wireshark_Ethernet_ARP_v8.0.pdf.....	4
6. Question 14 of Wireshark_Ethernet_ARP_v8.0.pdf.....	6
<b>Part 2-Address Resolution Protocol.....</b>	<b>7</b>

# Part 1-Ethernet frame analyzing

## 1. Open file ethernet--ethereal-trace-1 in wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMicrosy_a9:3d:...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	LinksysGroup_da:af:...	AmbitMicrosy_a9:3d:...	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
6	13.542974	CnetTechnolo_73:8d:...	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.498935	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
13	17.500025	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
14	17.500069	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0
15	17.527057	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
16	17.527422	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1 200 OK (text/html)
17	17.527457	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=4816 Win=64240 Len=0

## 2. Analyze ARP frames

Establishing a TCP connection involves a **three-way handshake**, facilitated by ARP. As a result, there are three ARP data frames, which are detailed as follows.

- (1) Device A needs to establish a connection with Device B.
- (2) Device A knows Device B's IP address but lacks its MAC address.
- (3) Device A broadcasts an ARP request into the network, where:
  - Sender Hardware Address is Device A's MAC address.
  - Sender Protocol Address is Device A's IP address.
  - Target Hardware Address is the broadcast address (typically represented by an all-ones MAC address, i.e., FF:FF:FF:FF:FF:FF).
  - Target Protocol Address is Device B's IP address.

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
Ethernet II, Src: AmbitMicrosy\_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Destination: Broadcast (ff:ff:ff:ff:ff:ff)  
Address: Broadcast (ff:ff:ff:ff:ff:ff)  
... .. LG bit: Locally administered address (this is NOT the default)  
... .. IG bit: Group address (multicast/broadcast)  
Source: AmbitMicrosy\_a9:3d:68 (00:d0:59:a9:3d:68)  
Address: AmbitMicrosy\_a9:3d:68 (00:d0:59:a9:3d:68)  
... .. LG bit: Globally unique address (factory default)  
... .. IG bit: Individual address (unicast)  
Type: ARP (0x0806)  
Address Resolution Protocol (request)  
Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: request (1)  
Sender MAC address: AmbitMicrosy\_a9:3d:68 (00:d0:59:a9:3d:68)  
Sender IP address: 192.168.1.105  
Target MAC address: Xerox\_00:00:00 (00:00:00:00:00:00)  
Target IP address: 192.168.1.1

0000 ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01  
0010 08 00 06 00 00 01 00 d0 59 a9 3d 68 c0 a8 01 69  
0020 00 00 00 00 00 00 c0 a8 01 01

① 广播地址    ② 设备A地址    ③ 协议类型 ARP    ④ 硬件类型  
⑤ 协议类型 IPv4    ⑥ 硬件地址长度    ⑦ 协议地址长度    ⑧ 操作码 (Opcode)  
⑨ 发送硬件地址    ⑩ 发送接收地址    ⑪ 目标硬件地址    ⑫ 目标IP地址

- (4) All devices within the broadcast domain receive this ARP request.
- (5) Upon receiving the ARP request, Device B responds with an ARP reply, in which:
  - Source MAC Address is Device B's MAC address.
  - Source IP Address is Device B's IP address.
  - Target MAC Address is Device A's MAC address.
  - Target IP Address is Device A's IP address.

2 0.001018	LinksysGroup_da:af:73... AmbitMicrosy_a9:3d:68 ARP	60 192.168.1.1 is at 00:06:25:da:af:73	
>	Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)		0000 00 d0 59 a9 3d 68 00 06 25 da af 73 08 06 00 01 ..V..h..%..s...
✓	Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)		0010 08 00 06 04 00 02 00 06 25 da af 73 c0 a8 01 01 .....%..s...-..
	Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)		0020 00 d0 59 a9 3d 68 c0 a8 01 69 00 00 00 00 00 ..Y..h...i.....
	Address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)		0030 00 00 00 00 00 00 00 00 00 00 00 00 ..... ..
	.....0..... = LG bit: Globally unique address (factory default)		
	.....0..... = IG bit: Individual address (unicast)		
	Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)		
	Address: LinksysGroup_da:af:73 (00:06:25:da:af:73)		
	.....0..... = LG bit: Globally unique address (factory default)		
	.....0..... = IG bit: Individual address (unicast)		
	Type: ARP (0x0806)		
	Padding: 00000000000000000000000000000000		
	Address Resolution Protocol (reply)		
	Hardware type: Ethernet (1)		
	Protocol type: IPv4 (0x0800)		
	Hardware size: 6		
	Protocol size: 4		
	Opcode: reply (2)		
	Sender MAC address: LinksysGroup_da:af:73 (00:06:25:da:af:73)		
	Sender IP address: 192.168.1.1		
	Target MAC address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)		
	Target IP address: 192.168.1.105		

- (6) Upon receiving the ARP reply, Device A learns Device B's MAC address.
- (7) Now, Device A can use Device B's MAC address to establish a TCP connection.

6 13.542974	CnetTechnolo_73:8d:ce Broadcast ARP	60 Who has 192.168.1.117? Tell 192.168.1.104	
>	Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)		0000 ff ff ff ff ff 00 80 ad 73 8d ce 08 06 00 01 .....-S...-..
✓	Ethernet II, Src: CnetTechnolo_73:8d:ce (00:80:ad:73:8d:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff)		0010 08 00 06 04 00 01 00 80 ad 73 8d ce c0 a8 01 68 .....%..s...-..
	Destination: Broadcast (ff:ff:ff:ff:ff:ff)		0020 00 00 00 00 00 00 c0 a8 01 75 00 00 00 00 .....-B.....
	Address: Broadcast (ff:ff:ff:ff:ff:ff)		0030 00 00 00 00 00 00 00 00 00 00 00 00 ..... ..
	.....1..... = LG bit: Locally administered address (this is NOT the factory default)		
	.....1..... = IG bit: Group address (multicast/broadcast)		
	Source: CnetTechnolo_73:8d:ce (00:80:ad:73:8d:ce)		
	Address: CnetTechnolo_73:8d:ce (00:80:ad:73:8d:ce)		
	.....0..... = LG bit: Globally unique address (factory default)		
	.....0..... = IG bit: Individual address (unicast)		
	Type: ARP (0x0806)		
	Padding: 00000000000000000000000000000000		
	Address Resolution Protocol (request)		
	Hardware type: Ethernet (1)		
	Protocol type: IPv4 (0x0800)		
	Hardware size: 6		
	Protocol size: 4		
	Opcode: request (1)		
	Sender MAC address: CnetTechnolo_73:8d:ce (00:80:ad:73:8d:ce)		
	Sender IP address: 192.168.1.104		
	Target MAC address: Xerox_00:00:00 (00:00:00:00:00)		
	Target IP address: 192.168.1.117		

Throughout this process, ARP's role is to resolve the mapping between the target device's IP address and MAC address, ensuring that before establishing a TCP connection, Device A is aware of Device B's MAC address for proper data transmission.

### 3. Question 10 of Wireshark\_Ethernet\_ARP\_v8.0.pdf

10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

First handshake:

Source MAC Address: 00:d0:59:a9:3d:68  
 Source IP Address: c0 a8 01 69  
 Destination MAC Address: 00:00:00:00:00:00 (Unknown)  
 Destination IP Address: c0 a8 01 01

Second handshake:

Source MAC Address: 00:06:25:da:af:73  
 Source IP Address: c0 a8 01 01  
 Destination MAC Address: 00:d0:59:a9:3d:68  
 Destination IP Address: c0 a8 01 69

#### 4. Question 11 of Wireshark\_Ethernet\_ARP\_v8.0.pdf

11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

Hexadecimal value for the Ethernet Frame type field: 0x0800

Corresponding upper layer protocol: **IPv4**

```
2 0.001018 LinksysGroup_da:af:73 -> AmbitMicrosy_a9:3d:68 ARP 60 192.168.1.1 is at 00:06:25:da:af:73
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on 0
  Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:68 (00:00:59:a9:3d:68)
    Destination: AmbitMicrosy_a9:3d:68 (00:00:59:a9:3d:68)
      Address: AmbitMicrosy_a9:3d:68 (00:00:59:a9:3d:68)
        ..0. .... = LG bit: Globally unique address (factory default)
        ....0. .... = IG bit: Individual address (unicast)
      Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
        Address: LinksysGroup_da:af:73 (00:06:25:da:af:73)
          ..0. .... = LG bit: Globally unique address (factory default)
          ....0. .... = IG bit: Individual address (unicast)
      Type: ARP (0x0806)
      Padding: 00000000000000000000000000000000
    Address Resolution Protocol (reply)
      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
      Hardware size: 6
      Protocol size: 4
      Opcode: reply (2)
      Sender MAC address: LinksysGroup_da:af:73 (00:06:25:da:af:73)
      Sender IP address: 192.168.1.1
      Target MAC address: AmbitMicrosy_a9:3d:68 (00:00:59:a9:3d:68)
      Target IP address: 192.168.1.105
```

#### 5. Question 13 of Wireshark\_Ethernet\_ARP\_v8.0.pdf

13. Now find the ARP reply that was sent in response to the ARP request.

a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

As indicated in the display, it begins **20 bytes** from the very beginning of the Ethernet frame.

```
> Frame 1: 42 bytes on wire (336 bits)
  Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:00:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
        ....1. ....
        ....1. ....
    Source: AmbitMicrosy_a9:3d:68 (00:00:59:a9:3d:68)
      Address: AmbitMicrosy_a9:3d:68 (00:00:59:a9:3d:68)
        ....0. ....
        ....0. ....
      Type: ARP (0x0806)
    Address Resolution Protocol (request)
      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
      Hardware size: 6
      Protocol size: 4
      Opcode: request (1)
      Sender MAC address: AmbitMicrosy_a9:3d:68 (00:00:59:a9:3d:68)
```

b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

In the first handshake, the opcode field value is 1.

In the second handshake, the opcode field value is 2.

The first handshake:

1	0.000000	AmbitMicrosy_a9:3d:...	Broadcast	ARP	42	Who has 192.168.1.1 is at
2	0.001018	LinksysGroup_da:af:...	AmbitMicrosy_a9:3d:...	ARP	60	192.168.1.1 is at
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN]
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission]
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission]
6	13.542974	CnetTechnolo_73:8d:...	Broadcast	ARP	60	Who has 192.168.1.1 is at

  

> Frame 1: 42 bytes on wire (336 bits)	0000	ff ff ff ff ff ff 00 d0	59 a9 3d 68 08 06 00 01
✓ Ethernet II, Src: AmbitMicrosy_a9:3d:68 00 00 00 00 00 00 00	0010	08 00 06 04 00 01 00 d0	59 a9 3d 68 c0 a8 01 69
Destination: Broadcast (ff:ff:ff:ff:ff:ff)	0020	00 00 00 00 00 00 c0 a8	01 01
Address: Broadcast (ff:ff:ff:ff:ff:ff)			
... ..1. ....			
... ..1. ....			
Source: AmbitMicrosy_a9:3d:68 (08:00:06:04:00:01)			
Address: AmbitMicrosy_a9:3d:68 (08:00:06:04:00:01)			
... ..0. ....			
... ..0. ....			
Type: ARP (0x0806)			
Address Resolution Protocol (request)			
Hardware type: Ethernet (1)			
Protocol type: IPv4 (0x0800)			
Hardware size: 6			
Protocol size: 4			
Opcode: request (1)			
Sender MAC address: AmbitMicrosy_a9:3d:68 00 00 00 00 00 00 00			

The second handshake:

1	0.000000	AmbitMicrosy_a9:3d:...	Broadcast	ARP	42	Who has 192.168.1.1 is at
2	0.001018	LinksysGroup_da:af:...	AmbitMicrosy_a9:3d:...	ARP	60	192.168.1.1 is at
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN]
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission]
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission]
6	13.542974	CnetTechnolo_73:8d:...	Broadcast	ARP	60	Who has 192.168.1.1 is at

  

> Frame 2: 60 bytes on wire (480 bits)	0000	00 d0 59 a9 3d 68 00 06	25 da af 73 08 06 00 01
✓ Ethernet II, Src: LinksysGroup_da:af:73 08 06 00 00 00 00 00	0010	08 00 06 04 00 02 00 06	25 da af 73 c0 a8 01 01
Destination: AmbitMicrosy_a9:3d:68 00 00 00 00 00 00 00	0020	00 d0 59 a9 3d 68 c0 a8	01 69 00 00 00 00 00 00
Address: AmbitMicrosy_a9:3d:68 00 00 00 00 00 00 00	0030	00 00 00 00 00 00 00 00	00 00 00 00
... ..0. ....			
... ..0. ....			
Source: LinksysGroup_da:af:73 (08:00:06:04:00:02)			
Address: LinksysGroup_da:af:73 (08:00:06:04:00:02)			
... ..0. ....			
... ..0. ....			
Type: ARP (0x0806)			
Padding: 00000000000000000000000000000000			
Address Resolution Protocol (reply)			
Hardware type: Ethernet (1)			
Protocol type: IPv4 (0x0800)			
Hardware size: 6			
Protocol size: 4			
Opcode: reply (2)			
Sender MAC address: LinksysGroup_da:af:73 08 06 00 00 00 00 00			

c) Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

The "answer" to the earlier ARP request appears in the Sender IP address field of the ARP reply message, indicating the IP address of the machine querying the Ethernet address corresponding to its respective IP address.

Sender MAC address: LinksysGroup\_da:af:73 (00:06:25:da:af:73)

Sender IP address: 192.168.1.1



## 6. Question 14 of Wireshark\_Ethernet\_ARP\_v8.0.pdf

14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

```

▼ Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
  ▼ Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    Address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  ▼ Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
    Address: LinksysGroup_da:af:73 (00:06:25:da:af:73)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  Padding: 00000000000000000000000000000000

```

## Part 2-Address Resolution Protocol

Analyzing the TCP packets captured on my own. Here is an example of me accessing Baidu. The local client establishes a TCP connection with Baidu, involving a three-way handshake facilitated by ARP. The specific protocols are outlined in the following diagram.

1409 23.987655	ce:67:9f:a1:cb:7e	AzureWaveTec_c7:10:...	ARP	42 Who has 192.168.149.55? Tell 192.168.149.118	
1410 23.987667	AzureWaveTec_c7:10:...	ce:67:9f:a1:cb:7e	ARP	42 192.168.149.55 is at 34:6f:24:c7:10:99	
<div>&gt; Frame 1409: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF...</div> <div>&gt; Ethernet II, Src: ce:67:9f:a1:cb:7e (ce:67:9f:a1:cb:7e), Dst: AzureWaveTec_c7:10:99 (34:6f:24:c7:10:99)</div> <div>&gt; Destination: AzureWaveTec_c7:10:99 (34:6f:24:c7:10:99)</div> <div>&gt; Address: AzureWaveTec_c7:10:99 (34:6f:24:c7:10:99)</div> <div>&gt; ..0. .... = LG bit: Globally unique address (factory default)</div> <div>&gt; ..0. .... = IG bit: Individual address (unicast)</div> <div>&gt; Source: ce:67:9f:a1:cb:7e (ce:67:9f:a1:cb:7e)</div> <div>&gt; Address: ce:67:9f:a1:cb:7e (ce:67:9f:a1:cb:7e)</div> <div>&gt; ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</div> <div>&gt; ..0. .... = IG bit: Individual address (unicast)</div> <div>&gt; Type: ARP (0x0806)</div> <div>&gt; Address Resolution Protocol (request)</div> <div>&gt; Hardware type: Ethernet (1)</div> <div>&gt; Protocol type: IPv4 (0x0800)</div> <div>&gt; Hardware size: 6</div> <div>&gt; Protocol size: 4</div> <div>&gt; Opcode: request (1)</div> <div>&gt; Sender MAC address: ce:67:9f:a1:cb:7e (ce:67:9f:a1:cb:7e)</div> <div>&gt; Sender IP address: 192.168.149.118</div> <div>&gt; Target MAC address: Xerox_00:00:00 (00:00:00:00:00:00)</div> <div>&gt; Target IP address: 192.168.149.55</div>					
1409 23.987655	ce:67:9f:a1:cb:7e	AzureWaveTec_c7:10:...	ARP	42 Who has 192.168.149.55? Tell 192.168.149.118	
1410 23.987667	AzureWaveTec_c7:10:...	ce:67:9f:a1:cb:7e	ARP	42 192.168.149.55 is at 34:6f:24:c7:10:99	
1411 23.990708	183.240.98.14	192.168.149.55	TCP	54 443->63230 [ACK] Seq=150 Ack=689 Win=30592 Len=0	
<div>&gt; Frame 1410: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF...</div> <div>&gt; Ethernet II, Src: AzureWaveTec_c7:10:99 (34:6f:24:c7:10:99), Dst: ce:67:9f:a1:cb:7e (ce:67:9f:a1:cb:7e)</div> <div>&gt; Destination: ce:67:9f:a1:cb:7e (ce:67:9f:a1:cb:7e)</div> <div>&gt; Address: ce:67:9f:a1:cb:7e (ce:67:9f:a1:cb:7e)</div> <div>&gt; ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</div> <div>&gt; ..0. .... = IG bit: Individual address (unicast)</div> <div>&gt; Source: AzureWaveTec_c7:10:99 (34:6f:24:c7:10:99)</div> <div>&gt; Address: AzureWaveTec_c7:10:99 (34:6f:24:c7:10:99)</div> <div>&gt; ..0. .... = LG bit: Globally unique address (factory default)</div> <div>&gt; ..0. .... = IG bit: Individual address (unicast)</div> <div>&gt; Type: ARP (0x0806)</div> <div>&gt; Address Resolution Protocol (reply)</div> <div>&gt; Hardware type: Ethernet (1)</div> <div>&gt; Protocol type: IPv4 (0x0800)</div> <div>&gt; Hardware size: 6</div> <div>&gt; Protocol size: 4</div> <div>&gt; Opcode: reply (2)</div> <div>&gt; Sender MAC address: AzureWaveTec_c7:10:99 (34:6f:24:c7:10:99)</div> <div>&gt; Sender IP address: 192.168.149.55</div> <div>&gt; Target MAC address: ce:67:9f:a1:cb:7e (ce:67:9f:a1:cb:7e)</div> <div>&gt; Target IP address: 192.168.149.118</div>					

First handshake:

Source MAC Address: ce:67:9f:a1:cb:7e

Source IP Address: c0 a8 95 76

Destination MAC Address: 00:00:00:00:00:00 (Unknown)

Destination IP Address: c0 a8 95 37

Second handshake:

Source MAC Address: 34:6f:24:c7:10:99

Source IP Address: c0 a8 95 37

Destination MAC Address: ce:67:9f:a1:cb:7e

Destination IP Address: c0 a8 95 76

Hexadecimal value for the Ethernet Frame type field: 0x0800

Corresponding upper layer protocol: **IPv4**

It begins **20 bytes** from the very beginning of the Ethernet frame.

In the first handshake, the opcode field value is 1.

In the second handshake, the opcode field value is 2.