

IP Lab Assignment -6

Name: Ramya Ajay

Roll No: CB.EN.P2CYS22004

Date: 3-11-2022

AIM: Analysing ARP request and response using Wireshark.

Tools: Wireshark

Use the provided pcap file (Arp) to answer the following questions.

1. Answer the following questions based on the contents of the Ethernet frame containing the HTTP GET message.

a. What is the 48-bit Ethernet address of your computer?

17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4
17.494766	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
17.498935	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
17.500025	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
17.500069	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
17.527057	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
17.527422	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	489	IPv4

> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits) on interface 0
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)

The source 48 bit ethernet address is 00:d0:59:a9:3d:68

b. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? What device has this as its Ethernet address?

Time	Source	Destination	Protocol	Length	Info
0.001028	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
13.542974	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has
17.444423	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4
17.494766	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
17.498935	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
17.500025	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
17.500069	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
17.527057	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
17.527422	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	489	IPv4

▼ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
 ▼ Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
 Address: LinksysG_da:af:73 (00:06:25:da:af:73)

The 48 bit destination address in the Ethernet frame is 00:06:25:da:af:73 which is the address of the router/gateway

▼ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73) ▼ Destination: LinksysG_da:af:73 (00:06:25:da:af:73) Address: LinksysG_da:af:73 (00:06:25:da:af:73)0. = LG bit: Globally unique address

No this is the address of the router/gateway to which the source computer is sending the request. From there it gets transferred to the destination computer.

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

17.498935	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
17.500025	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
17.500069	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
17.527057	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
17.527422	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	489	IPv4
17.527457	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4

Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)		0000	00 d0 59 a9 3d 68 00 06	25 da af 73 08 00	45 60	..Y.=h..%..s..E`
Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)		0010	05 dc 8f 2f 40 00 37 06	76 f7 80 77 f5 0c c0 a8		.../@ 7- v..w....
Type: IPv4 (0x0800)		0020	01 69 00 50 04 22 ac a5	3f b4 65 14 9c 1f 50 10		..i.p."...?e...P..
Data (1500 bytes)		0030	1b 28 5e d0 00 00 48 54	54 50 2f 31 2e 31 20 32		..(^...HT TP/1.1 2
		0040	30 30 20 4f 4b 0d 0a 44	61 74 65 3a 20 53 61 74		00 OK..D ate: Sat
		0050	2c 20 32 38 20 41 75 67	20 32 30 30 34 20 31 37		, 28 Aug 2004 17
		0060	3a 31 39 3a 33 37 20 47	4d 54 0d 0a 53 65 72 76		:19:37 G MT..Serv
		0070	65 72 3a 20 41 70 61 63	68 65 2f 32 2e 30 2e 34		er: Apac he/2.0.4
		0080	30 20 28 52 65 64 20 48	61 74 20 4c 69 6e 75 78		0 (Red H at Linux
		0090	29 0d 0a 4c 61 73 74 2d	4d 6f 64 69 66 69 65 64)...Last- Modified
		00a0	3a 20 53 61 74 2c 20 32	38 20 41 75 67 20 32 30		: Sat, 2 8 Aug 20

The hex value of the 2 byte frame field is 0x0800 . It corresponds to IPV4 protocol.

2. Answer the following questions based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

a. What is the value of the Ethernet source address?

17.498935	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
17.500025	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
17.500069	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
17.527057	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
17.527422	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	489	IPv4
17.527457	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4

Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)		0000	00 d0 59 a9 3d 68 00 06	25 da af 73 08 00	45 60	..Y.=h..%..s..E`
Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)		0010	05 dc 8f 2f 40 00 37 06	76 f7 80 77 f5 0c c0 a8		.../@ 7- v..w....
Type: IPv4 (0x0800)		0020	01 69 00 50 04 22 ac a5	3f b4 65 14 9c 1f 50 10		..i.p."...?e...P..
Data (1500 bytes)		0030	1b 28 5e d0 00 00 48 54	54 50 2f 31 2e 31 20 32		..(^...HT TP/1.1 2
		0040	30 30 20 4f 4b 0d 0a 44	61 74 65 3a 20 53 61 74		00 OK..D ate: Sat
		0050	2c 20 32 38 20 41 75 67	20 32 30 30 34 20 31 37		, 28 Aug 2004 17
		0060	3a 31 39 3a 33 37 20 47	4d 54 0d 0a 53 65 72 76		:19:37 G MT..Serv

The value of ethernet source address in reply packet is 00:06:25:da:af:73

b. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

[Protocols in frame: eth:ethertype:data]	
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)	
Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)	

The Ethernet address of destination in reply packet is 00:d0:59;a9:ed:68

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

The hex value of the two byte frame field is 0x0800. It corresponds to IPV4 layer.

3. Answer the following questions based on the contents of the ARP Request packets.

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

▼ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: B	0000	ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01 Y=h....
▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)	0010	08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8 01 69 Y=h...i
Address: Broadcast (ff:ff:ff:ff:ff:ff)	0020	00 00 00 00 00 00 c0 a8 01 01
....1. = LG bit: Locally administer			
....1. = IG bit: Group address (mul			
▼ Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)			
Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)			
....0. = LG bit: Globally unique ad			
....0. = IG bit: Individual address			
Type: ARP (0x0806)			

The address of

Source -> 00:d0:59:a9:3d:6d

Destination -> ff:ff:ff:ff:ff:ff

b. Give the hexadecimal value for the two-byte Ethernet Frame type field.

▼ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: B	0000	ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01 Y=h....
▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)	0010	08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8 01 69 Y=h...i
Address: Broadcast (ff:ff:ff:ff:ff:ff)	0020	00 00 00 00 00 00 c0 a8 01 01
....1. = LG bit: Locally administer			
....1. = IG bit: Group address (mul			
▼ Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)			
Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)			
....0. = LG bit: Globally unique ad			
....0. = IG bit: Individual address			
Type: ARP (0x0806)			

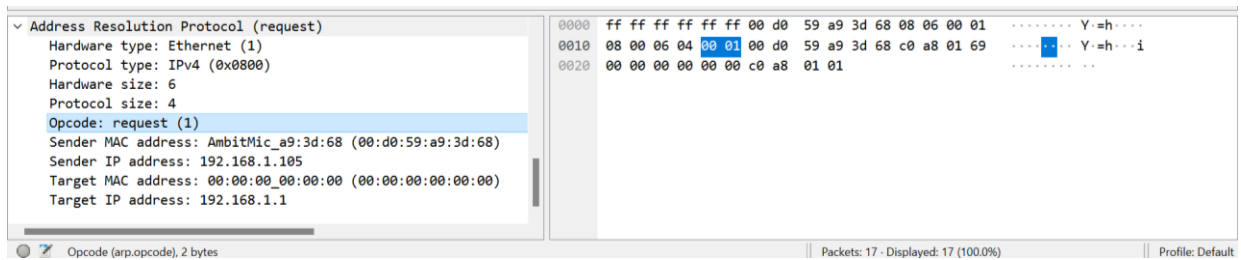
The hex value of the two byte field is 0x0806

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

▼ Address Resolution Protocol (request)	0000	ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01 Y=h....
Hardware type: Ethernet (1)	0010	08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8 01 69	... Y=h...i
Protocol type: IPv4 (0x0800)	0020	00 00 00 00 00 00 c0 a8 01 01
Hardware size: 6			
Protocol size: 4			
Opcode: request (1)			
Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)			
Sender IP address: 192.168.1.105			
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)			
Target IP address: 192.168.1.1			

On clicking the OPCODE field we get to see the hex values 20-21. On clicking the hex values we see that the OPCODE field begins at 20 th field

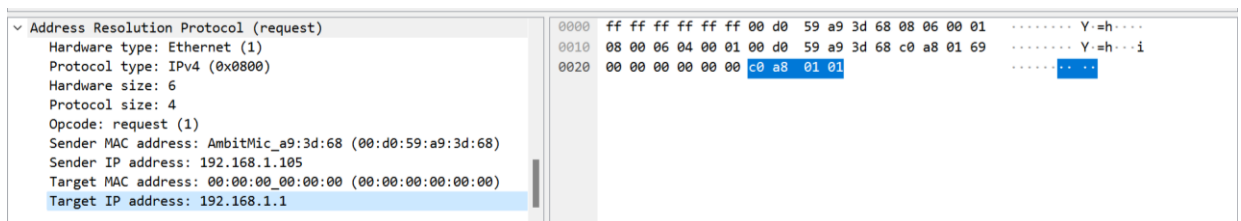
d. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?



e. Does the ARP message contain the IP address of the sender?

Yes it contains the sender IP address .

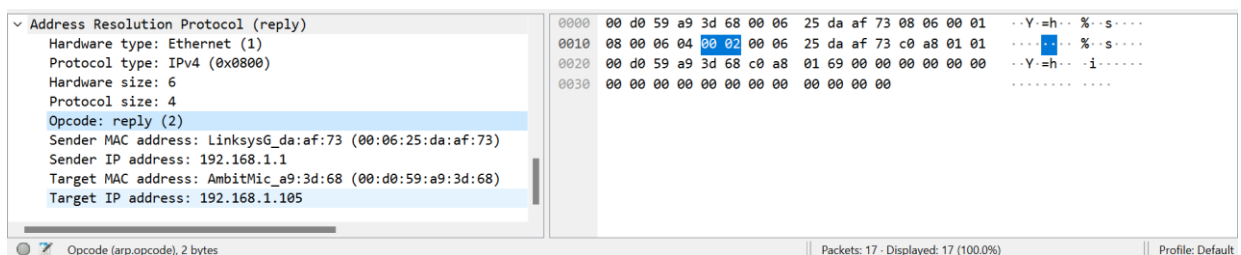
f. Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?



From the above we can see that the request where the sender asks which system has the IP address 192.168.1.1

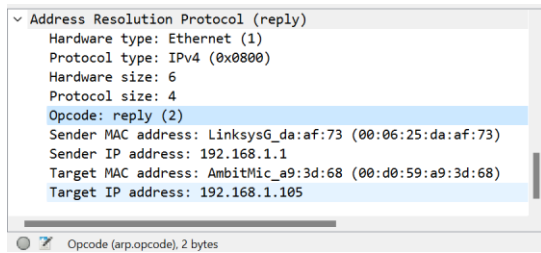
4. Answer the following questions based on the contents of the ARP Reply packets.

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



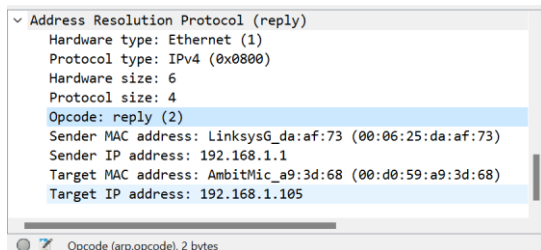
It begins at 20-21 st field

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?



The value of the OPCODE field within the arp payload in response packet is 2.

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?



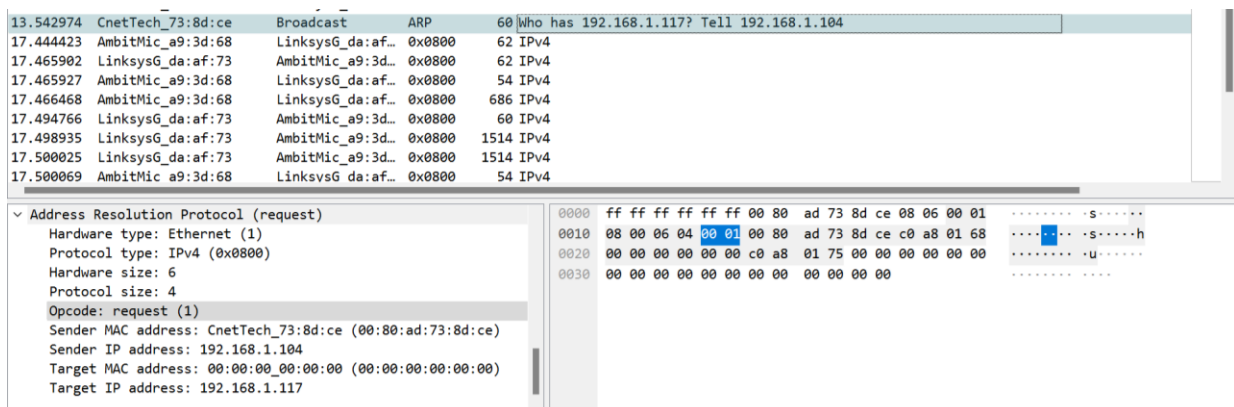
We can confirm that this packet contains the answer since it contains both the sender and receiver's MAC address along with their IP address.

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

The hex value of the source address is 00 06 25 da af 73

The value of the destination address is 00 d0 59 a9 3d 68

e. There is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace



There is no response for the second ARP request packet because ARP request packet is a

broadcast message and the arp response is unicast . So the computer which has the IP that is queried by the server will send a unicast response packet back to the router. So since the traffic is captured from this computer which has the ip .105 we are not able to see the reply arp packet which is sent back.

Result:

The experiment to understand ARP requests and responses have been done successfully.