

## Lab 5

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

The 48-bit Ethernet address of my computer is fc:3f:db:d5:91:dc

The screenshot shows a Wireshark packet capture on interface 0. The packet list shows 38 packets. Packet 28 is selected, showing details of an Ethernet II frame. The source is HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc) and the destination is D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68). The data field shows a hex dump and ASCII representation of the payload.

No.	Time	Source	Destination	Protocol	Length	Info
19	11:07:44.717478	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	80	IPv4
20	11:07:44.725557	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1392	IPv4
21	11:07:44.726292	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	83	IPv4
22	11:07:44.743261	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	489	IPv4
23	11:07:44.771996	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	77	IPv4
24	11:07:45.716217	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	66	IPv4
25	11:07:45.966606	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	66	IPv4
26	11:07:45.972739	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	66	IPv4
27	11:07:45.972882	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
28	11:07:45.975197	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	480	IPv4
29	11:07:46.217608	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	66	IPv4
30	11:07:46.217797	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
31	11:07:46.231967	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	60	IPv4
32	11:07:46.232781	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1514	IPv4
33	11:07:46.233324	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1514	IPv4
34	11:07:46.233325	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1514	IPv4
35	11:07:46.233327	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	537	IPv4
36	11:07:46.233406	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
37	11:07:46.277621	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	55	IPv4
38	11:07:46.281601	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	66	IPv4

> Frame 28: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0  
Ethernet II, Src: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc), Dst: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)  
> Destination: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)  
> Source: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
Type: IPv4 (0x0800)  
> Data (466 bytes)  
Data: 450001d23c95400080060000c0a8006b8077f50c33910050...  
[Length: 466]  
0000 10 be f5 20 a9 68 fc 3f db d5 91 dc 08 00 45 00 ... .h.? .....E.  
0010 01 d2 3c 95 40 00 00 06 00 00 c0 a8 00 6b 80 77 ... <.@... ..k.w  
0020 f5 0c 33 91 00 50 22 cd 68 bc 4b 75 ed 06 50 18 ... 3..P". h.Ku..P.  
0030 01 00 38 5c 00 00 45 54 20 2f 77 69 72 65 73 ... 8\..E T /wires  
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 65 ... hark-lab s/HTTP-e  
0050 74 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 ... thereal- lab-file

### 2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is *no*). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]

The 48-bit destination address in the Ethernet frame is 10:be:f5:20:a9:68

This is not the Ethernet address of gaia.cs.umass.edu. It is the Ethernet address of my D-Link router.



The ASCII “G” in “GET” appears 54 bytes from the very start of the Ethernet frame.

The image shows a Wireshark capture of an Ethernet frame. The packet list pane shows a list of packets, with packet 28 selected. The packet details pane shows the structure of the selected packet: Ethernet II, Src: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc), Dst: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68), Type: IPv4 (0x0800). The packet bytes pane shows the raw data of the packet, with the ASCII representation of the data visible. A red arrow points to the 'G' in 'GET' at offset 54.

No.	Time	Source	Destination	Protocol	Length	Info
19	11:07:44.717478	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	80	IPv4
20	11:07:44.725557	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1392	IPv4
21	11:07:44.726292	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	83	IPv4
22	11:07:44.743261	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	489	IPv4
23	11:07:44.771996	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	77	IPv4
24	11:07:45.716217	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	66	IPv4
25	11:07:45.966606	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	66	IPv4
26	11:07:45.972739	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	66	IPv4
27	11:07:45.972882	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
28	11:07:45.975197	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	480	IPv4
29	11:07:46.217608	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	66	IPv4
30	11:07:46.217797	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
31	11:07:46.231967	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	60	IPv4
32	11:07:46.232781	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1514	IPv4
33	11:07:46.233324	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1514	IPv4
34	11:07:46.233325	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1514	IPv4
35	11:07:46.233327	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	537	IPv4
36	11:07:46.233406	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
37	11:07:46.277621	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	55	IPv4
38	11:07:46.281601	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	66	IPv4

> Frame 28: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0  
> Ethernet II, Src: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc), Dst: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)  
> Destination: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)  
> Source: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
> Type: IPv4 (0x0800)  
> Data (466 bytes)  
Data: 450001d23c9540080000c0a8006b8077f50c33910050...  
[Length: 466]

0000 10 be f5 20 a9 68 fc 3f db d5 91 dc 08 00 45 00 ... .h.? .....E.  
0010 01 d2 3c 95 40 00 06 00 00 c0 a8 00 6b 80 77 ... <.@... ....k.w  
0020 f5 0c 33 91 00 50 22 cd 68 bc 4b 75 ed 06 50 18 ... 3..P.. h.Ku..P.  
0030 01 00 38 5c 00 00 45 54 20 2f 77 69 72 65 73 ... 8\..GE T /wires  
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 50 2d 65 ... ark-lab s/HTTP-e  
0050 74 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 ... thereal- lab-file

5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is *no*). What device has this as its Ethernet address?

The value of the Ethernet source address is 10:be:f5:20:a9:68

This is neither the address of my computer nor is it the address of gaia.cs.umass.edu. This is the Ethernet address of my D-Link router.

The screenshot shows a Wireshark packet capture on interface 0. The packet list displays 38 packets. Packet 32 is selected, showing details for an Ethernet II frame. The destination address is highlighted as **fc:3f:db:d5:91:dc** (fc:3f:db:d5:91:dc). The source address is **D-LinkIn\_20:a9:68** (10:be:f5:20:a9:68). The frame type is IPv4 (0x0800). The data field shows 1500 bytes of data.

No.	Time	Source	Destination	Protocol	Length	Info
19	11:07:44.717478	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	80	IPv4
20	11:07:44.725557	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1392	IPv4
21	11:07:44.726292	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	83	IPv4
22	11:07:44.743261	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	489	IPv4
23	11:07:44.771996	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	77	IPv4
24	11:07:45.716217	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	66	IPv4
25	11:07:45.966606	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	66	IPv4
26	11:07:45.972739	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	66	IPv4
27	11:07:45.972882	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
28	11:07:45.975197	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	480	IPv4
29	11:07:46.217608	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	66	IPv4
30	11:07:46.217797	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
31	11:07:46.231967	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	60	IPv4
32	11:07:46.232781	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1514	IPv4
33	11:07:46.233324	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1514	IPv4
34	11:07:46.233325	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1514	IPv4
35	11:07:46.233327	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	537	IPv4
36	11:07:46.233406	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
37	11:07:46.277621	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	55	IPv4
38	11:07:46.281601	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	66	IPv4

Frame 32: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0  
 Ethernet II, Src: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
 Destination: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
 Source: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)  
 Type: IPv4 (0x0800)  
 Data (1500 bytes)

Bytes 14-1513: Data (data.data)

Packets: 38 · Displayed: 38 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

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

The destination address in the Ethernet frame is **fc:3f:db:d5:91:dc** and is the Ethernet address of my computer.

The screenshot shows a Wireshark packet capture on interface 0. The packet list displays 38 packets. Packet 32 is selected, showing details for an Ethernet II frame. The destination address is highlighted as **fc:3f:db:d5:91:dc** (fc:3f:db:d5:91:dc). The source address is **D-LinkIn\_20:a9:68** (10:be:f5:20:a9:68). The frame type is IPv4 (0x0800). The data field shows 1500 bytes of data.

No.	Time	Source	Destination	Protocol	Length	Info
19	11:07:44.717478	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	80	IPv4
20	11:07:44.725557	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1392	IPv4
21	11:07:44.726292	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	83	IPv4
22	11:07:44.743261	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	489	IPv4
23	11:07:44.771996	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	77	IPv4
24	11:07:45.716217	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	66	IPv4
25	11:07:45.966606	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	66	IPv4
26	11:07:45.972739	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	66	IPv4
27	11:07:45.972882	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
28	11:07:45.975197	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	480	IPv4
29	11:07:46.217608	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	66	IPv4
30	11:07:46.217797	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
31	11:07:46.231967	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	60	IPv4
32	11:07:46.232781	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1514	IPv4
33	11:07:46.233324	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1514	IPv4
34	11:07:46.233325	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	1514	IPv4
35	11:07:46.233327	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	537	IPv4
36	11:07:46.233406	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
37	11:07:46.277621	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	55	IPv4
38	11:07:46.281601	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	66	IPv4

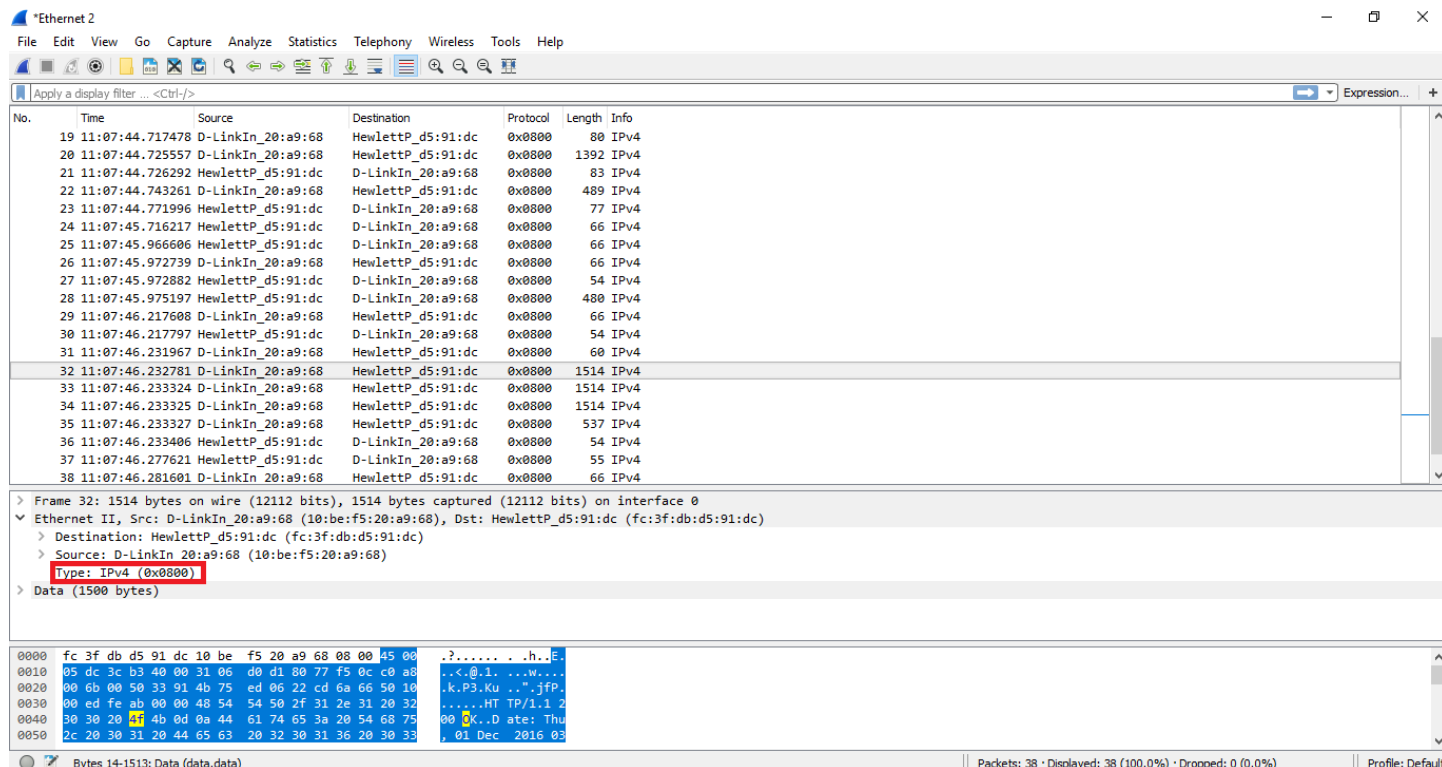
Frame 32: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0  
 Ethernet II, Src: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
 Destination: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
 Source: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)  
 Type: IPv4 (0x0800)  
 Data (1500 bytes)

Bytes 14-1513: Data (data.data)

Packets: 38 · Displayed: 38 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

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

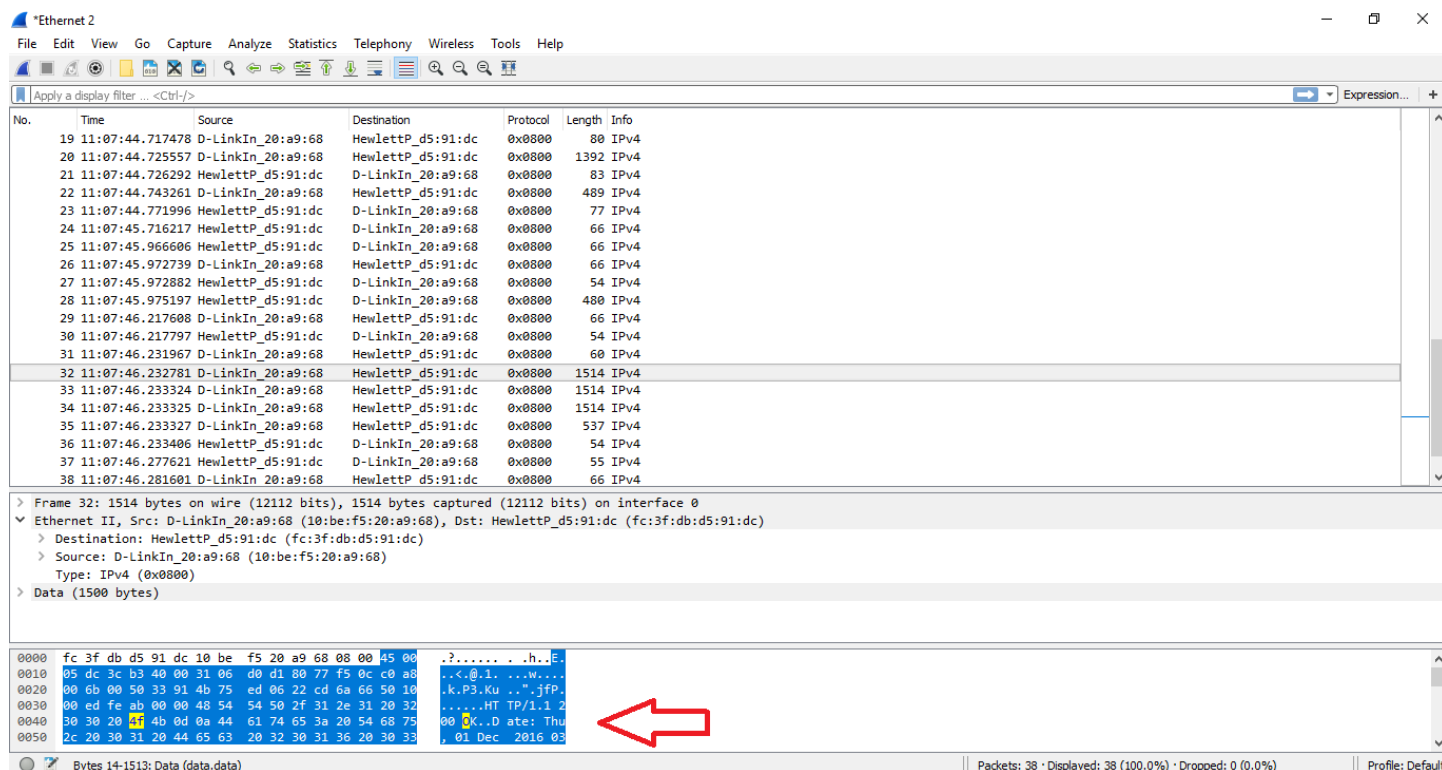
The hexadecimal value for the two-byte Frame type field is 0x0800. This corresponds to the IPv4 upper layer protocol.



The screenshot shows a Wireshark capture of an Ethernet frame. The packet list pane shows a list of packets, with packet 32 selected. The packet details pane shows the frame structure: Ethernet II, Src: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc), Type: IPv4 (0x0800). The packet bytes pane shows the raw data of the frame, with the frame type field (0x0800) highlighted in red.

## 8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?

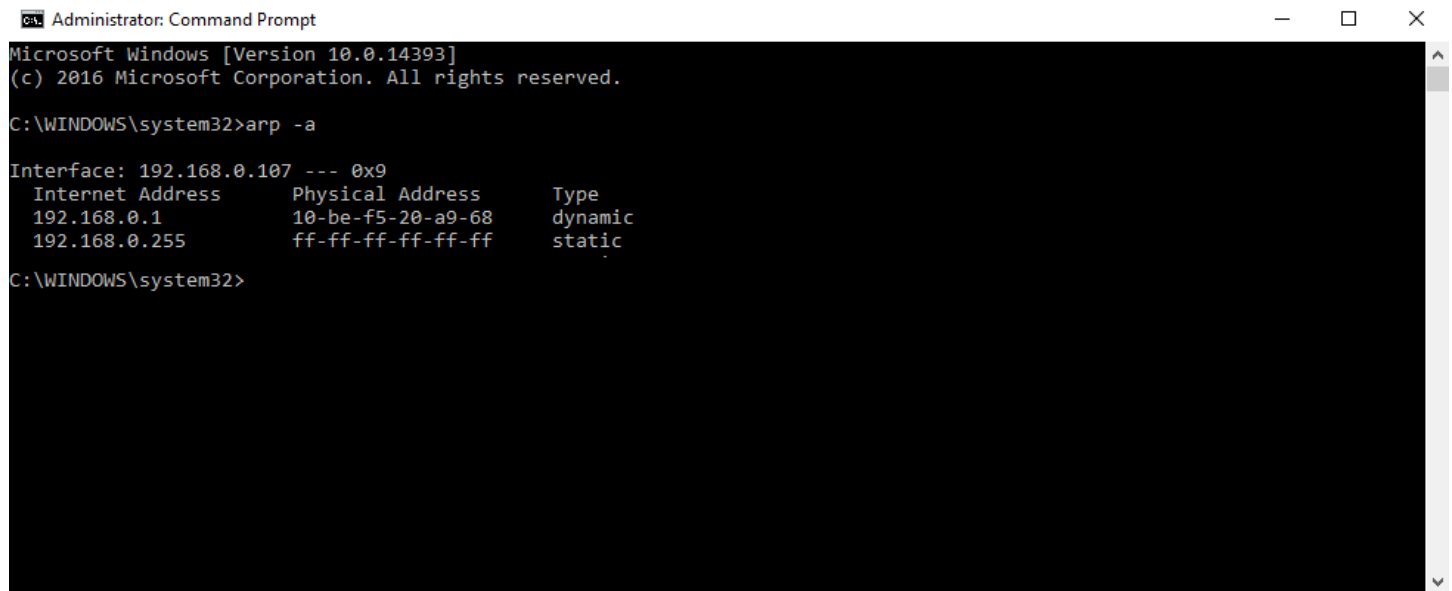
The ASCII “O” in “OK” appears 67 bytes from the very start of the Ethernet frame.



The screenshot shows a Wireshark capture of an Ethernet frame, similar to the one above. The packet list pane shows a list of packets, with packet 32 selected. The packet details pane shows the frame structure: Ethernet II, Src: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc), Type: IPv4 (0x0800). The packet bytes pane shows the raw data of the frame, with the ASCII string "OK" highlighted in red. A red arrow points to the 'O' in "OK", which is located at byte 67 (0x43) from the start of the frame.

**9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?**

The columns show Internet Address (IPv4), Physical Address (Ethernet), and Type (whether the IPv4 address is dynamic or static).



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>arp -a

Interface: 192.168.0.107 --- 0x9
Internet Address      Physical Address      Type
192.168.0.1           10-be-f5-20-a9-68     dynamic
192.168.0.255         ff-ff-ff-ff-ff-ff     static

C:\WINDOWS\system32>
```

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

The hexadecimal value for the source addresses in the Ethernet frame containing the ARP request message is 10:be:f5:20:a9:68

The hexadecimal value for the destination addresses in the Ethernet frame containing the ARP request message is fc:3f:db:d5:91:dc



Wireshark interface showing a packet capture on Ethernet 2. The packet list shows a packet from D-LinkIn\_20:a9:68 to HewlettP\_d5:91:dc. The packet details pane shows the Ethernet II frame structure, including the destination and source MAC addresses, and the ARP request details. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
80	12:10:52.998712	Apple_bf:ce:8d	IPv6mcast_fb	0x86dd	132	IPv6
81	12:10:53.078758	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	60	IPv4
82	12:10:53.337487	D-LinkIn_20:a9:68	IPv4mcast_7f:ff:fa	0x0800	388	IPv4
83	12:10:53.353069	D-LinkIn_20:a9:68	IPv4mcast_7f:ff:fa	0x0800	436	IPv4
84	12:10:53.353070	D-LinkIn_20:a9:68	IPv4mcast_7f:ff:fa	0x0800	440	IPv4
85	12:10:53.460860	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	779	IPv4
86	12:10:53.571143	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
87	12:10:55.793690	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
88	12:10:55.793729	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	ARP	42	192.168.0.107 is at fc:3f:db:d5:91:dc

Frame 87: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
 Ethernet II, Src: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
 Destination: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
 Address: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
 ....0. .... = LG bit: Globally unique address (factory default)  
 ....0. .... = IG bit: Individual address (unicast)  
 Source: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)  
 Type: ARP (0x0806)  
 Padding: 00000000000000000000000000000000b861f2c1  
 Address Resolution Protocol (request)  
 Hardware type: Ethernet (1)  
 Protocol type: IPv4 (0x0800)  
 Hardware size: 6  
 Protocol size: 4  
 Opcode: request (1)  
 Sender MAC address: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)  
 Sender IP address: 192.168.0.1  
 Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)  
 Target IP address: 192.168.0.107

0000 fc 3f db d5 91 dc 10 be f5 20 a9 68 08 06 00 01 .?..... .h....  
 0010 08 00 06 04 00 01 10 be f5 20 a9 68 c0 a8 00 01 .... .h....  
 0020 00 00 00 00 00 00 c0 a8 00 6b 00 00 00 00 00 .....k.....  
 0030 00 00 00 00 00 00 00 b8 61 f2 c1 .....a..

Opcode (arp.opcode), 2 bytes

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

The hexadecimal value for the two-byte Ethernet Frame type field is 0x0806 which corresponds to the ARP upper level protocol.

Wireshark interface showing a packet capture on Ethernet 2. The packet list shows a packet from D-LinkIn\_20:a9:68 to HewlettP\_d5:91:dc. The packet details pane shows the Ethernet II frame structure, including the destination and source MAC addresses, and the ARP request details. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
80	12:10:52.998712	Apple_bf:ce:8d	IPv6mcast_fb	0x86dd	132	IPv6
81	12:10:53.078758	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	60	IPv4
82	12:10:53.337487	D-LinkIn_20:a9:68	IPv4mcast_7f:ff:fa	0x0800	388	IPv4
83	12:10:53.353069	D-LinkIn_20:a9:68	IPv4mcast_7f:ff:fa	0x0800	436	IPv4
84	12:10:53.353070	D-LinkIn_20:a9:68	IPv4mcast_7f:ff:fa	0x0800	440	IPv4
85	12:10:53.460860	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	779	IPv4
86	12:10:53.571143	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
87	12:10:55.793690	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
88	12:10:55.793729	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	ARP	42	192.168.0.107 is at fc:3f:db:d5:91:dc

Frame 87: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
 Ethernet II, Src: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
 Destination: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
 Address: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
 ....0. .... = LG bit: Globally unique address (factory default)  
 ....0. .... = IG bit: Individual address (unicast)  
 Source: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)  
 Type: ARP (0x0806)  
 Padding: 00000000000000000000000000000000b861f2c1  
 Address Resolution Protocol (request)  
 Hardware type: Ethernet (1)  
 Protocol type: IPv4 (0x0800)  
 Hardware size: 6  
 Protocol size: 4  
 Opcode: request (1)  
 Sender MAC address: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)  
 Sender IP address: 192.168.0.1  
 Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)  
 Target IP address: 192.168.0.107

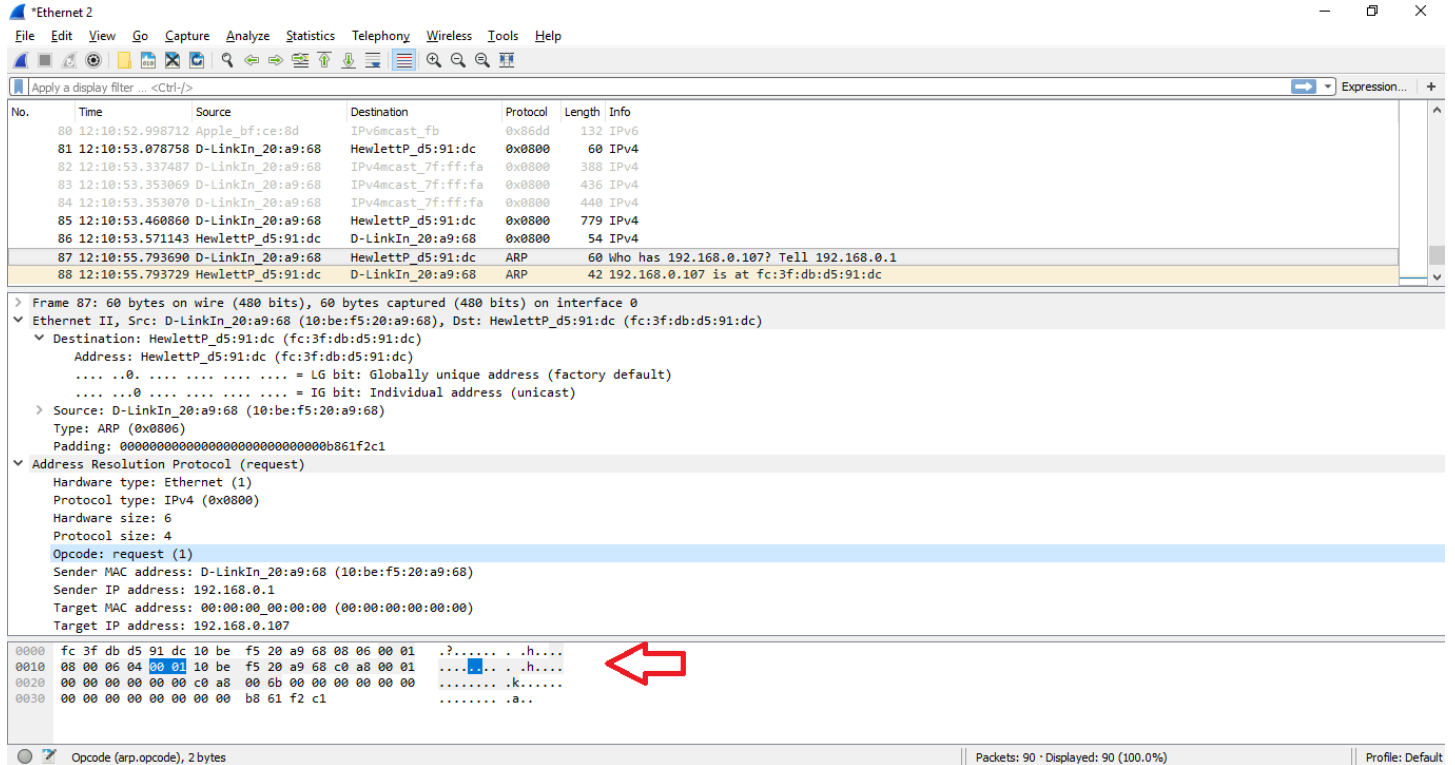
0000 fc 3f db d5 91 dc 10 be f5 20 a9 68 08 06 00 01 .?..... .h....  
 0010 08 00 06 04 00 01 10 be f5 20 a9 68 c0 a8 00 01 .... .h....  
 0020 00 00 00 00 00 00 c0 a8 00 6b 00 00 00 00 00 .....k.....  
 0030 00 00 00 00 00 00 00 b8 61 f2 c1 .....a..

Opcode (arp.opcode), 2 bytes

12. Download the ARP specification from <http://ftp.rfc-editor.org/in-notes/std/std37.txt>. A readable, detailed discussion of ARP is also at <http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>.

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

The ARP *opcode* field begins 20 bytes from the very beginning of the Ethernet frame.



Wireshark packet capture showing an ARP request. The packet list shows packet 87 as an ARP request from D-LinkIn\_20:a9:68 to HewlettP\_d5:91:dc. The packet details show the ARP request structure with the opcode field set to 1. The packet bytes pane shows the raw data with a red arrow pointing to the opcode field at offset 20.

No.	Time	Source	Destination	Protocol	Length	Info
80	12:10:52.998712	Apple_bf:ce:8d	IPv6mcast_fb	0x86dd	132	IPv6
81	12:10:53.078758	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	60	IPv4
82	12:10:53.337487	D-LinkIn_20:a9:68	IPv4mcast_7f:ff:fa	0x0800	388	IPv4
83	12:10:53.353069	D-LinkIn_20:a9:68	IPv4mcast_7f:ff:fa	0x0800	436	IPv4
84	12:10:53.353070	D-LinkIn_20:a9:68	IPv4mcast_7f:ff:fa	0x0800	440	IPv4
85	12:10:53.460860	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	779	IPv4
86	12:10:53.571143	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
87	12:10:55.793690	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
88	12:10:55.793729	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	ARP	42	192.168.0.107 is at fc:3f:db:d5:91:dc

Frame 87: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
Ethernet II, Src: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
Destination: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
Address: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
...0. .... = LG bit: Globally unique address (factory default)  
...0. .... = IG bit: Individual address (unicast)  
Source: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)  
Type: ARP (0x0806)  
Padding: 00000000000000000000000000000000b861f2c1  
Address Resolution Protocol (request)  
Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: request (1)  
Sender MAC address: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)  
Sender IP address: 192.168.0.1  
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)  
Target IP address: 192.168.0.107

0000 fc 3f db d5 91 dc 10 be f5 20 a9 68 08 06 00 01 ..?.....h....  
0010 08 00 06 04 00 01 10 be f5 20 a9 68 c0 a8 00 01 ...h....  
0020 00 00 00 00 00 00 c0 a8 00 6b 00 00 00 00 00 .....k.....  
0030 00 00 00 00 00 00 00 b8 61 f2 c1 .....a....

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

The value of the *opcode* field within the ARP-payload part of the Ethernet frame is 0x0001 (request).



Wireshark packet capture showing an ARP request. The packet details pane highlights the 'Sender IP address' field, which is 192.168.0.1. A red arrow points to this field.

c) Does the ARP message contain the IP address of the sender?

Yes, the ARP message contains the IP address of the sender.

Wireshark packet capture showing an ARP request. The packet details pane highlights the 'Sender IP address' field, which is 192.168.0.1.

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

[illegible]

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

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into three panes:

- Packet List:** Displays a list of captured packets. Packet 88 is selected, showing it as an ARP request from 192.168.0.107 to 192.168.0.1.
- Packet Details:** Shows the hierarchical structure of the selected packet. It includes Ethernet II, Internet Protocol Version 4, and ARP request details.
- Packet Bytes:** Displays the raw data of the packet in hexadecimal and ASCII. A red arrow points to the 'op' field (0002) in the ARP section, which represents the operation code for a request.

The status bar at the bottom indicates the current capture status: 'Oncode (arp.opcode), 2 bytes' and 'Packets: 90 · Displayed: 90 (100.0%)'.

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 part of the Ethernet frame is 0x0002 (reply).

Wireshark packet capture showing an ARP response. The packet list shows frame 88 as an ARP response from HewlettP\_d5:91:dc to D-LinkIn\_20:a9:68. The packet details show the ARP opcode as 'reply (2)'. The packet bytes show the opcode field at offset 0004 as 0002, highlighted with a red arrow.

No.	Time	Source	Destination	Protocol	Length	Info
80	12:10:52.998712	Apple_bf:ce:8d	IPv6mcast_fb	0x86dd	132	IPv6
81	12:10:53.078758	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	60	IPv4
82	12:10:53.337487	D-LinkIn_20:a9:68	IPv4mcast_7f:ff:fa	0x0800	388	IPv4
83	12:10:53.353069	D-LinkIn_20:a9:68	IPv4mcast_7f:ff:fa	0x0800	436	IPv4
84	12:10:53.353070	D-LinkIn_20:a9:68	IPv4mcast_7f:ff:fa	0x0800	440	IPv4
85	12:10:53.460860	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	779	IPv4
86	12:10:53.571143	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
87	12:10:55.793690	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
88	12:10:55.793729	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	ARP	42	192.168.0.107 is at fc:3f:db:d5:91:dc

Frame 88: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
Ethernet II, Src: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc), Dst: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)  
Destination: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)  
Address: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)  
... .. = LG bit: Globally unique address (factory default)  
... .. = IG bit: Individual address (unicast)  
Source: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
Address: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
... .. = LG bit: Globally unique address (factory default)  
... .. = IG bit: Individual address (unicast)  
Type: ARP (0x0806)  
Address Resolution Protocol (reply)  
Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: reply (2)  
Sender MAC address: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)  
Sender IP address: 192.168.0.107

0000 10 be f5 20 a9 68 fc 3f db d5 91 dc 08 06 00 01 ... .h.? .....  
0010 08 00 06 04 00 02 fc 3f db d5 91 dc c0 a8 00 6b ... ..k  
0020 10 be f5 20 a9 68 c0 a8 00 01 ... .h. ..

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 MAC address* field which contains the corresponding IP address that is being queried.

Wireshark 2.10.0 (64-bit) - Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
80	12:10:52.998712	Apple_bf:ce:8d	IPv6mcast_fb	0x86dd	132	IPv6
81	12:10:53.078758	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	60	IPv4
82	12:10:53.337487	D-LinkIn_20:a9:68	IPv4mcast_7f:ff:fa	0x0800	388	IPv4
83	12:10:53.353069	D-LinkIn_20:a9:68	IPv4mcast_7f:ff:fa	0x0800	436	IPv4
84	12:10:53.353070	D-LinkIn_20:a9:68	IPv4mcast_7f:ff:fa	0x0800	440	IPv4
85	12:10:53.460860	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	0x0800	779	IPv4
86	12:10:53.571143	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	0x0800	54	IPv4
87	12:10:55.793690	D-LinkIn_20:a9:68	HewlettP_d5:91:dc	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
88	12:10:55.793729	HewlettP_d5:91:dc	D-LinkIn_20:a9:68	ARP	42	192.168.0.107 is at fc:3f:db:d5:91:dc

> Frame 88: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc), Dst: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)

- Destination: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)
  - Address: D-LinkIn\_20:a9:68 (10:be:f5:20:a9:68)
    - ... ..0. .... = LG bit: Globally unique address (factory default)
    - ... ..0. .... = IG bit: Individual address (unicast)
- Source: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)
  - Address: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)
    - ... ..0. .... = LG bit: Globally unique address (factory default)
    - ... ..0. .... = IG bit: Individual address (unicast)
- Type: ARP (0x0806)
- Address Resolution Protocol (reply)
  - Hardware type: Ethernet (1)
  - Protocol type: IPv4 (0x0800)
  - Hardware size: 6
  - Protocol size: 4
  - Opcode: reply (2)
  - Sender MAC address: HewlettP\_d5:91:dc (fc:3f:db:d5:91:dc)
  - Sender IP address: 192.168.0.107

```

0000  10 be f5 20 a9 68 fc 3f db d5 91 dc 08 06 00 01  ... .h.? .....
0010  08 00 06 04 00 02 fc 3f db d5 91 dc c0 a8 00 6b  ....? .....k
0020  10 be f5 20 a9 68 c0 a8 00 01  ... .h.. ..

```

Opcode (arp.opcode), 2 bytes

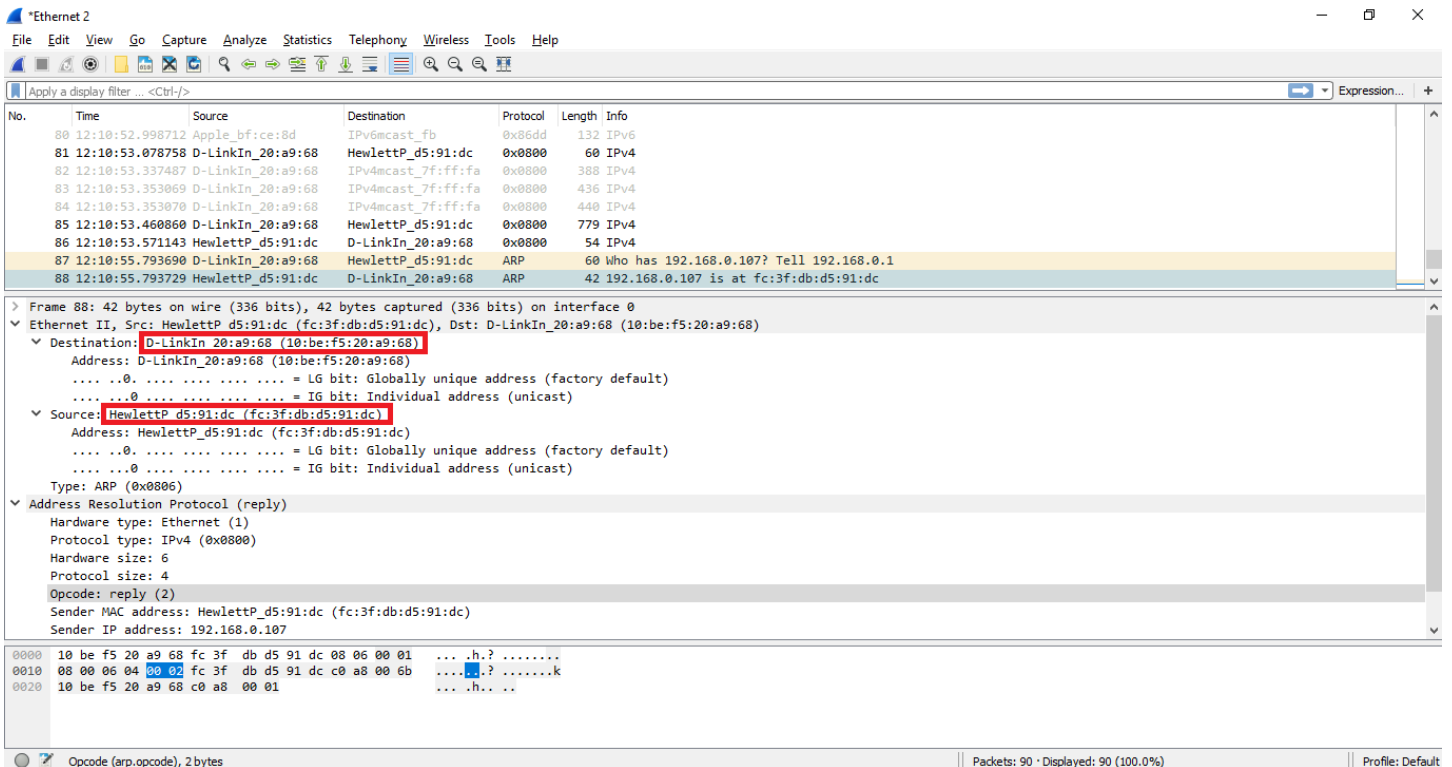
Packets: 90 · Displayed: 90 (100.0%)

Profile: Default

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

The hexadecimal value for the source addresses in the Ethernet frame containing the ARP reply message is fc:3f:db:d5:91:dc

The hexadecimal value for the destination addresses in the Ethernet frame containing the ARP reply message is 10:be:f5:20:a9:68



15. Open the *ethernet-ethereal-trace-1* trace file in <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But 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 ARP reply sent in response to the ARP request in packet 6 in the packet trace because we are not the ones sending the request, and thus will not receive a reply. In the request sent in packet 1, ‘our computer’ is AmbitMic\_a9:3d:68 and the request specifies that the response should be sent back to us – so we receive it. However, in packet 6, the sender is Telebit\_73:8d:ce (not us) and they will receive the response directly.

## Extra Credit

EX-1. The *arp* command:

```
arp -s InetAddr EtherAddr
```

allows you to manually add an entry to the ARP cache that resolves the IP address *InetAddr* to the physical address *EtherAddr*. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

EX-2. What is the default amount of time that an entry remains in your ARP cache before being removed. You can determine this empirically (by monitoring the cache contents) or by looking this up in your operation system documentation. Indicate how/where you determined this value.