

Joel Benjamin Castillo (jc5383)
CS6843 - Computer Networking
Prof. Rafail Portnoy

Wireshark Lab - Ethernet

Ethernet Frames

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

f0:6e:0b:d5:b4:de

Wireshark packet capture analysis of an Ethernet frame. The packet list shows packet 23 selected, which is an IPv4 packet. The packet details pane shows the Ethernet II header with source MAC f0:6e:0b:d5:b4:de and destination MAC 0c:8d:db:84:47:c7. The data field contains a GET request for /wires/hark-lab/s/HTTP-e/thereal-lab-file/3.html. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
14	2018-12-01 18:11:40.173887	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
15	2018-12-01 18:11:40.206764	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	117	IPv4
16	2018-12-01 18:11:40.247755	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
17	2018-12-01 18:11:40.495841	CiscoMer_84:47:c7	Microsof_d5:b4:de	ARP	60	Who ha
18	2018-12-01 18:11:40.495883	Microsof_d5:b4:de	CiscoMer_84:47:c7	ARP	42	10.0.1
19	2018-12-01 18:11:40.692653	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	66	IPv4
20	2018-12-01 18:11:40.700362	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	986	IPv4
21	2018-12-01 18:11:40.703749	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	66	IPv4
22	2018-12-01 18:11:40.703807	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
23	2018-12-01 18:11:40.719538	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	424	IPv4
24	2018-12-01 18:11:40.730971	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	60	IPv4
25	2018-12-01 18:11:40.731773	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
26	2018-12-01 18:11:40.731775	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
27	2018-12-01 18:11:40.731783	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
28	2018-12-01 18:11:40.731785	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	535	IPv4
29	2018-12-01 18:11:40.731924	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
30	2018-12-01 18:11:40.757546	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	66	IPv4

Frame 23: 424 bytes on wire (3392 bits), 424 bytes captured (3392 bits) on interface 0

Ethernet II, Src: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de), Dst: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)

- Destination: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
Address: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
....0. = LG bit: Globally unique address (factory default)
....0 = IG bit: Individual address (unicast)
- Source: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
Address: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
....0. = LG bit: Globally unique address (factory default)
....0 = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
- Data (410 bytes)
Data: 4500019a5c8c400080065e920a00bebb8077f50c5add0050...
[Length: 410]

0000 0c 8d db 84 47 c7 f0 6e 0b d5 b4 de 08 00 45 00G..n....E.
0010 01 9a 5c 8c 40 00 80 06 5e 92 0a 00 be bb 80 77 ..\..@...^.....w
0020 f5 0c 5a dd 00 50 cc 71 36 ad 3a af 1c 9e 50 18 ..Z..P.q 6:..P.
0030 01 00 d8 91 00 00 47 45 54 20 2f 77 69 72 65 73GE 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
0060 33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 3.html H TTP/1.1
0070 0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 .Host: g aia.cs.u
0080 6d 61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 mass.edu ..User-A
0090 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e gent: Mo zilla/5.
00a0 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 0 (Windo ws NT 10

Ethernet (eth), 14 bytes | Packets: 65 · Displayed: 65 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

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.]

0c:8d:db:84:47:c7

This is the Ethernet address of the router I am connected to.

The image shows a Wireshark packet capture window. 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. A filter bar at the top of the packet list says "Apply a display filter ... <Ctrl-/>".

The packet list shows 30 packets. Packet 23 is selected, showing a timestamp of 2018-12-01 18:11:40.719538, source Microsof_d5:b4:de, destination CiscoMer_84:47:c7, protocol 0x0800, length 424, and info IPv4.

The packet details pane for packet 23 shows:

- Frame 23: 424 bytes on wire (3392 bits), 424 bytes captured (3392 bits) on interface 0
- Ethernet II, Src: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de), Dst: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 - Destination: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 - Address: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 - 0. = LG bit: Globally unique address (factory default)
 - 0 = IG bit: Individual address (unicast)
 - Source: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
 - Address: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
 - 0. = LG bit: Globally unique address (factory default)
 - 0 = IG bit: Individual address (unicast)
 - Type: IPv4 (0x0800)
- Data (410 bytes)
 - Data: 4500019a5c8c400080065e920a00bebb8077f50c5add0050...
 - [Length: 410]

The packet bytes pane shows the raw data in hexadecimal and ASCII. The first few bytes are 0000 0c 8d db 84 47 c7 f0 6e 0b d5 b4 de 08 00 45 00, which correspond to the Ethernet II header fields: destination MAC, source MAC, and frame type.

The status bar at the bottom shows "Ethernet (eth), 14 bytes" and "Packets: 65 · Displayed: 65 (100.0%) · Dropped: 0 (0.0%)".

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

0x0800 - IP

The image shows a Wireshark packet capture window titled "Wi-Fi". 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. A display filter bar shows "Apply a display filter ... <Ctrl-/>".

The packet list pane shows 30 packets. Packet 23 is selected, showing a timestamp of 2018-12-01 18:11:40.719538, source IP 18.11.40.719538, destination IP 18.11.40.730971, protocol 0x0800 (IPv4), and length 424. The info pane shows the packet details: Ethernet II, Src: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de), Dst: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7). The destination and source MAC addresses are expanded, showing their bit fields (LG bit, IG bit). The type is IPv4 (0x0800). The data field is expanded, showing the first 410 bytes of the data.

The packet bytes pane shows the raw data of the selected packet. The first 14 bytes are highlighted in blue, corresponding to the Ethernet II header. The ASCII column shows the corresponding ASCII values for the data.

No.	Time	Source	Destination	Protocol	Length	Info
14	2018-12-01 18:11:40.173887	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
15	2018-12-01 18:11:40.206764	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	117	IPv4
16	2018-12-01 18:11:40.247755	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
17	2018-12-01 18:11:40.495841	CiscoMer_84:47:c7	Microsof_d5:b4:de	ARP	60	Who ha
18	2018-12-01 18:11:40.495883	Microsof_d5:b4:de	CiscoMer_84:47:c7	ARP	42	10.0.1
19	2018-12-01 18:11:40.692653	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	66	IPv4
20	2018-12-01 18:11:40.700362	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	986	IPv4
21	2018-12-01 18:11:40.703749	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	66	IPv4
22	2018-12-01 18:11:40.703807	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
23	2018-12-01 18:11:40.719538	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	424	IPv4
24	2018-12-01 18:11:40.730971	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	60	IPv4
25	2018-12-01 18:11:40.731773	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
26	2018-12-01 18:11:40.731775	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
27	2018-12-01 18:11:40.731783	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
28	2018-12-01 18:11:40.731785	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	535	IPv4
29	2018-12-01 18:11:40.731924	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
30	2018-12-01 18:11:40.757546	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	66	IPv4

Frame 23: 424 bytes on wire (3392 bits), 424 bytes captured (3392 bits) on interface 0

Ethernet II, Src: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de), Dst: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)

- Destination: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 - Address: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
- Source: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
 - Address: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
- Type: IPv4 (0x0800)
- Data (410 bytes)
 - Data: 4500019a5c8c400080065e920a00bebb8077f50c5add0050...
 - [Length: 410]

0000 0c 8d db 84 47 c7 f0 6e 0b d5 b4 de 08 00 45 00G..n....E.
 0010 01 9a 5c 8c 40 00 80 06 5e 92 0a 00 be bb 80 77 ..\.@...^.....w
 0020 f5 0c 5a dd 00 50 cc 71 36 ad 3a af 1c 9e 50 18 ..Z..P.q 6:..P.
 0030 01 00 d8 91 00 00 47 45 54 20 2f 77 69 72 65 73GE 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
 0060 33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 3.html H TTP/1.1
 0070 0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 .Host: g aia.cs.u
 0080 6d 61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 mass.edu ..User-A
 0090 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e gent: Mo zilla/5.
 00a0 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 0 (Windo ws NT 10

Ethernet (eth), 14 bytes | Packets: 65 · Displayed: 65 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?

54 bytes

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 packet capture and analysis. The main display area is divided into three panes:

- Packet List Pane:** Displays a list of captured packets. Packet 23 is selected, showing it is an IPv4 packet of 424 bytes, captured on interface 0.
- Packet Details Pane:** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II header, source and destination MAC addresses, and the IP data payload.
- Packet Bytes Pane:** Shows the raw hexadecimal and ASCII data of the selected packet. The first few bytes of the IP header are highlighted in red.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
14	2018-12-01 18:11:40.173887	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
15	2018-12-01 18:11:40.206764	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	117	IPv4
16	2018-12-01 18:11:40.247755	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
17	2018-12-01 18:11:40.495841	CiscoMer_84:47:c7	Microsof_d5:b4:de	ARP	60	Who ha
18	2018-12-01 18:11:40.495883	Microsof_d5:b4:de	CiscoMer_84:47:c7	ARP	42	10.0.1
19	2018-12-01 18:11:40.692653	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	66	IPv4
20	2018-12-01 18:11:40.700362	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	986	IPv4
21	2018-12-01 18:11:40.703749	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	66	IPv4
22	2018-12-01 18:11:40.703807	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
23	2018-12-01 18:11:40.719538	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	424	IPv4
24	2018-12-01 18:11:40.730971	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	60	IPv4
25	2018-12-01 18:11:40.731773	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
26	2018-12-01 18:11:40.731775	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
27	2018-12-01 18:11:40.731783	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
28	2018-12-01 18:11:40.731785	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	535	IPv4
29	2018-12-01 18:11:40.731924	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
30	2018-12-01 18:11:40.757546	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	66	IPv4

Packet Details:

- Frame 23: 424 bytes on wire (3392 bits), 424 bytes captured (3392 bits) on interface 0
- Ethernet II, Src: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de), Dst: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 - Destination: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 - Address: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 - 0. = LG bit: Globally unique address (factory default)
 - 0. = IG bit: Individual address (unicast)
 - Source: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
 - Address: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
 - 0. = LG bit: Globally unique address (factory default)
 - 0. = IG bit: Individual address (unicast)
 - Type: IPv4 (0x0800)
- Data (410 bytes)
 - Data: 4500019a5c8c400080065e920a00bebb8077f50c5add0050...
 - [Length: 410]

Packet Bytes:

Offset	Hex	ASCII
0000	0c 8d db 84 47 c7 f0 6e 0b d5 b4 de 08 00 45 00	...G..n...E..
0010	01 9a 5c 8c 40 00 80 06 5e 92 0a 00 be bb 80 77	..\.@...^.....w
0020	f5 0c 5a dd 00 50 cc 71 36 ad 3a af 1c 9e 50 18	..Z..P.q 6:..P.
0030	01 00 d8 91 00 00 47 45 54 20 2f 77 69 72 65 73GE 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
0060	33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d	3.html H TTP/1.1.
0070	0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75	Host: g aia.cs.u
0080	6d 61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41	mass.edu ..User-A
0090	67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e	gent: Mo zilla/5.
00a0	30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30	0 (Windo ws NT 10

Status Bar: Ethernet (eth), 14 bytes | Packets: 65 · Displayed: 65 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

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?

0c:8d:db:84:47:c7

This is the Ethernet address of the router that I am connected to.

The image shows a Wireshark packet capture window titled '*Wi-Fi'. The packet list on the left shows 30 packets. Packet 25 is selected, showing details for an Ethernet II frame. The destination MAC address is f0:6e:0b:d5:b4:de, and the source MAC address is 0c:8d:db:84:47:c7. The data field contains a large block of hexadecimal data.

No.	Time	Source	Destination	Protocol	Length	Info
14	2018-12-01 18:11:40.173887	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
15	2018-12-01 18:11:40.206764	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	117	IPv4
16	2018-12-01 18:11:40.247755	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
17	2018-12-01 18:11:40.495841	CiscoMer_84:47:c7	Microsof_d5:b4:de	ARP	60	Who ha
18	2018-12-01 18:11:40.495883	Microsof_d5:b4:de	CiscoMer_84:47:c7	ARP	42	10.0.1
19	2018-12-01 18:11:40.692653	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	66	IPv4
20	2018-12-01 18:11:40.700362	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	986	IPv4
21	2018-12-01 18:11:40.703749	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	66	IPv4
22	2018-12-01 18:11:40.703807	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
23	2018-12-01 18:11:40.719538	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	424	IPv4
24	2018-12-01 18:11:40.730971	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	60	IPv4
25	2018-12-01 18:11:40.731773	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
26	2018-12-01 18:11:40.731775	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
27	2018-12-01 18:11:40.731783	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
28	2018-12-01 18:11:40.731785	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	535	IPv4
29	2018-12-01 18:11:40.731924	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
30	2018-12-01 18:11:40.757546	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	66	IPv4

Frame 25: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

Ethernet II, Src: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7), Dst: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)

- Destination: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
 - Address: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
- Source: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 - Address: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
 - Type: IPv4 (0x0800)
- Data (1500 bytes)
 - Data: 450005dcb735400033064ca78077f50c0a00bebb00505add...
 - [Length: 1500]

0000 f0 6e 0b d5 b4 de 0c 8d db 84 47 c7 08 00 45 00 .n..... ..G...E.
 0010 05 dc b7 35 40 00 33 06 4c a7 80 77 f5 0c 0a 00 ...5@.3. L..w...
 0020 be bb 00 50 5a dd 3a af 1c 9e cc 71 38 1f 50 10 ...PZ.:. ...q8.P.
 0030 00 ed 8f 1d 00 00 48 54 54 50 2f 31 2e 31 20 32HT 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 30 31 20 44 65 63 20 32 30 31 38 20 32 33 , 01 Dec 2018 23
 0060 3a 31 31 3a 34 31 20 47 4d 54 0d 0a 53 65 72 76 :11:41 G MT..Serv
 0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
 0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS) OpenSS
 0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH
 00a0 50 2f 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72 P/5.4.16 mod_per

Ethernet (eth), 14 bytes | Packets: 65 · Displayed: 65 (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?

f0:6e:0b:d5:b4:de

Yes, this is the Ethernet address of my network adapter.

Wireshark packet capture showing an ARP request. The packet list shows frame 25 selected. The packet details pane shows the Ethernet II header with Source: CiscoMer_84:47:c7 and Destination: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de). The data field shows the ARP request payload.

No.	Time	Source	Destination	Protocol	Length	Info
14	2018-12-01 18:11:40.173887	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
15	2018-12-01 18:11:40.206764	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	117	IPv4
16	2018-12-01 18:11:40.247755	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
17	2018-12-01 18:11:40.495841	CiscoMer_84:47:c7	Microsof_d5:b4:de	ARP	60	Who ha
18	2018-12-01 18:11:40.495883	Microsof_d5:b4:de	CiscoMer_84:47:c7	ARP	42	10.0.1
19	2018-12-01 18:11:40.692653	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	66	IPv4
20	2018-12-01 18:11:40.700362	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	986	IPv4
21	2018-12-01 18:11:40.703749	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	66	IPv4
22	2018-12-01 18:11:40.703807	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
23	2018-12-01 18:11:40.719538	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	424	IPv4
24	2018-12-01 18:11:40.730971	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	60	IPv4
25	2018-12-01 18:11:40.731773	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
26	2018-12-01 18:11:40.731775	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
27	2018-12-01 18:11:40.731783	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
28	2018-12-01 18:11:40.731785	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	535	IPv4
29	2018-12-01 18:11:40.731924	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
30	2018-12-01 18:11:40.757546	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	66	IPv4

Frame 25: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

Ethernet II, Src: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7), Dst: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)

- Destination: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
 - Address: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
- Source: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 - Address: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
- Type: IPv4 (0x0800)
- Data (1500 bytes)
 - Data: 450005dcb735400033064ca78077f50c0a00bebb00505add... [Length: 1500]

0000 f0 6e 0b d5 b4 de 0c 8d db 84 47 c7 08 00 45 00 .n..... ..G...E.
 0010 05 dc b7 35 40 00 33 06 4c a7 80 77 f5 0c 0a 00 ...5@.3. L..w...
 0020 be bb 00 50 5a dd 3a af 1c 9e cc 71 38 1f 50 10 ...PZ.:. ...q8.P.
 0030 00 ed 8f 1d 00 00 48 54 54 50 2f 31 2e 31 20 32HT 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 30 31 20 44 65 63 20 32 30 31 38 20 32 33 , 01 Dec 2018 23
 0060 3a 31 31 3a 34 31 20 47 4d 54 0d 0a 53 65 72 76 :11:41 G MT..Serv
 0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
 0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS) OpenSS
 0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH
 00a0 50 2f 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72 P/5.4.16 mod_per

Ethernet (eth), 14 bytes | Packets: 65 · Displayed: 65 (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?

0x0800 - IP

The screenshot shows the Wireshark interface with a packet capture on the 'Wi-Fi' interface. The packet list shows 30 packets. Packet 25 is selected, showing details for an Ethernet II frame from CiscoMer_84:47:c7 to Microsof_d5:b4:de. The destination MAC address is f0:6e:0b:d5:b4:de. The source MAC address is 0c:8d:db:84:47:c7. The type is IPv4 (0x0800). The data field shows the start of an HTTP response: 'Data: 450005dcb735400033064ca78077f50c0a00bebb00505add...'. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
14	2018-12-01 18:11:40.173887	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
15	2018-12-01 18:11:40.206764	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	117	IPv4
16	2018-12-01 18:11:40.247755	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
17	2018-12-01 18:11:40.495841	CiscoMer_84:47:c7	Microsof_d5:b4:de	ARP	60	Who ha
18	2018-12-01 18:11:40.495883	Microsof_d5:b4:de	CiscoMer_84:47:c7	ARP	42	10.0.1
19	2018-12-01 18:11:40.692653	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	66	IPv4
20	2018-12-01 18:11:40.700362	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	986	IPv4
21	2018-12-01 18:11:40.703749	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	66	IPv4
22	2018-12-01 18:11:40.703807	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
23	2018-12-01 18:11:40.719538	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	424	IPv4
24	2018-12-01 18:11:40.730971	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	60	IPv4
25	2018-12-01 18:11:40.731773	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
26	2018-12-01 18:11:40.731775	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
27	2018-12-01 18:11:40.731783	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	1514	IPv4
28	2018-12-01 18:11:40.731785	CiscoMer_84:47:c7	Microsof_d5:b4:de	0x0800	535	IPv4
29	2018-12-01 18:11:40.731924	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	54	IPv4
30	2018-12-01 18:11:40.757546	Microsof_d5:b4:de	CiscoMer_84:47:c7	0x0800	66	IPv4

Frame 25: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

Ethernet II, Src: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7), Dst: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)

- Destination: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
 - Address: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
- Source: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 - Address: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
- Type: IPv4 (0x0800)
- Data (1500 bytes)
 - Data: 450005dcb735400033064ca78077f50c0a00bebb00505add...
 - [Length: 1500]

0000 f0 6e 0b d5 b4 de 0c 8d db 84 47 c7 08 00 45 00 .n..... ..G...E.
 0010 05 dc b7 35 40 00 33 06 4c a7 80 77 f5 0c 0a 00 ...5@.3. L..w...
 0020 be bb 00 50 5a dd 3a af 1c 9e cc 71 38 1f 50 10 ...PZ.:. ...q8.P.
 0030 00 ed 8f 1d 00 00 48 54 54 50 2f 31 2e 31 20 32HT 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 30 31 20 44 65 63 20 32 30 31 38 20 32 33 , 01 Dec 2018 23
 0060 3a 31 31 3a 34 31 20 47 4d 54 0d 0a 53 65 72 76 :11:41 G MT..Serv
 0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
 0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS) OpenSS
 0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH
 00a0 50 2f 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72 P/5.4.16 mod_per

Ethernet (eth), 14 bytes | Packets: 65 · Displayed: 65 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

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?

67 bytes

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 packet capture and analysis. The main display area is divided into three panes:

- Packet List Pane:** Displays a list of captured packets. The selected packet is 25, which is an IPv4 packet from CiscoMer_84:47:c7 to Microsof_d5:b4:de. The packet length is 1514 bytes.
- Packet Details Pane:** Shows the hierarchical structure of the selected packet. It includes Ethernet II, Internet Protocol Version 4 (IPv4), and Data (1500 bytes). The data field is highlighted, showing a hexadecimal dump and its corresponding ASCII representation.
- Packet Bytes Pane:** Displays the raw data of the selected packet in hexadecimal and ASCII. The data is a 1500-byte payload, likely a file transfer, as indicated by the ASCII text "n... ..G...E...5@...3...L...w...PZ...:...q8...P...HT TP/1.1 2...OK...D ate: Sat...01 Dec 2018 23:11:41 G MT...Serv...er: Apac he/2.4.6 (CentOS) OpenSS L/1.0.2k -fips PH P/5.4.16 mod_per".

The status bar at the bottom indicates that the capture is on the Ethernet (eth) interface, showing 14 bytes of data. It also displays statistics: Packets: 65, Displayed: 65 (100.0%), Dropped: 0 (0.0%), and Profile: Default.

ARP

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

```

Windows PowerShell

~ $ arp -a

Interface: 10.0.190.187 --- 0x4
  Internet Address      Physical Address      Type
  10.128.128.128        0c-8d-db-84-47-c7    dynamic
  10.255.255.255        ff-ff-ff-ff-ff-ff    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
  239.255.255.253       01-00-5e-7f-ff-fd    static
  255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 10.0.0.1 --- 0x5
  Internet Address      Physical Address      Type
  10.0.0.255            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
  239.255.255.253       01-00-5e-7f-ff-fd    static

Interface: 169.254.250.98 --- 0x8
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff    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
  239.255.255.253       01-00-5e-7f-ff-fd    static
  255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.56.1 --- 0x1c
  Internet Address      Physical Address      Type
  192.168.56.255        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
  239.255.255.253       01-00-5e-7f-ff-fd    static
  255.255.255.255       ff-ff-ff-ff-ff-ff    static

~ $

```

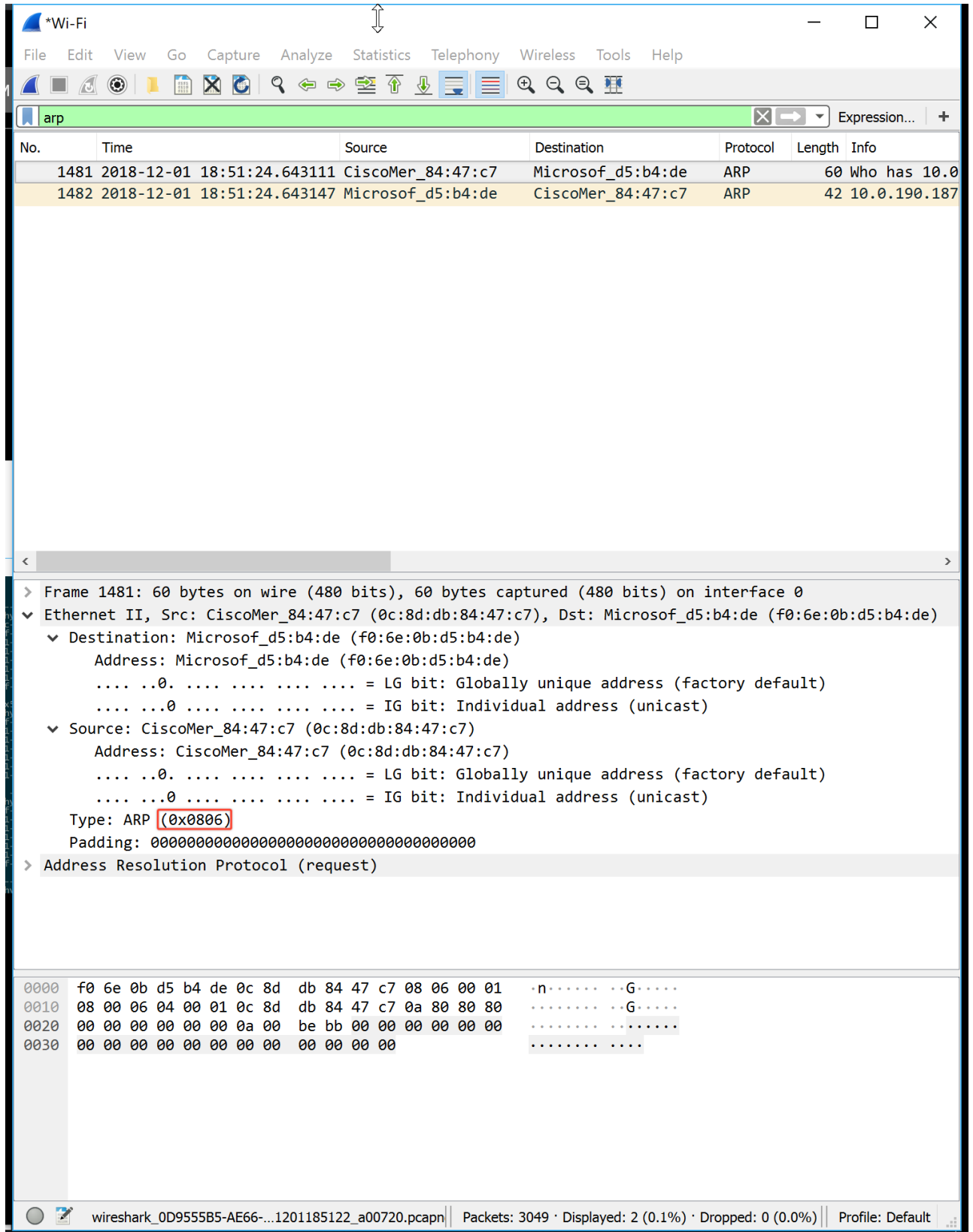
IP Address, MAC (Ethernet Address), ARP Entry Type - Static is manually configured and is permanent, Dynamic means the entry is created using the ARP protocol.

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

Destination: **f0:6e:0b:d5:b4:de**

[illegible]

- 11 / 15



- Download the ARP specification from <ftp://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?
20 bytes from the beginning of the frame
- 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 hex value in the ARP-payload of the request is 0x0001
- c) Does the ARP message contain the IP address of the sender?
Yes

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

The field **Target MAC Address** is set to **00:00:00:00:00:00** to query the machine whose IP address is being queried.

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?

20 bytes from the beginning of the frame

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?

0x0002 - 2

The image shows a Wireshark packet capture window titled '*Wi-Fi'. The filter bar at the top is set to 'arp'. The packet list shows two packets: packet 1481 (ARP request) and packet 1482 (ARP reply). Packet 1482 is selected, and its details pane shows the following structure:

- Frame 1482: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
- Ethernet II, Src: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de), Dst: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 - Destination: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 - Address: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
 - Source: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
 - Address: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
 -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: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
 - Sender IP address: 10.0.190.187
 - Target MAC address: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
 - Target IP address: 10.128.128.128

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. The first three lines are:

```

0000  0c 8d db 84 47 c7 f0 6e 0b d5 b4 de 08 06 00 01  ....G..n .....
0010  08 00 06 04 00 02 f0 6e 0b d5 b4 de 0a 00 be bb  ....n .....
0020  0c 8d db 84 47 c7 0a 80 80 80  ....G... ..

```

The status bar at the bottom indicates: Opcode (arp.opcode), 2 bytes | Packets: 3049 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

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 appears in the **Sender MAC Address** field. Value contains **f0:6e:0b:d5:b4:de**

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

Destination: **0c:8d:db:84:47:c7**

Source: **f0:6e:0b:d5:b4:de**

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 reply because this request came from a different host. It is a broadcast, but the reply will be sent to the sender's MAC address.

