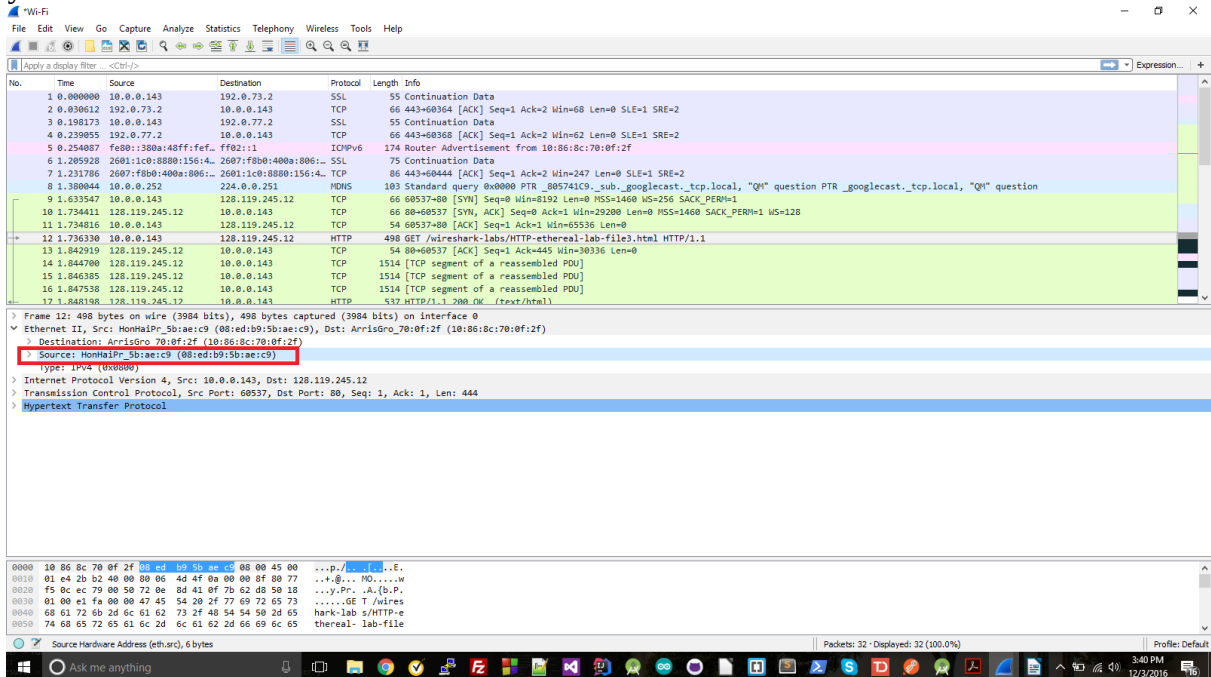
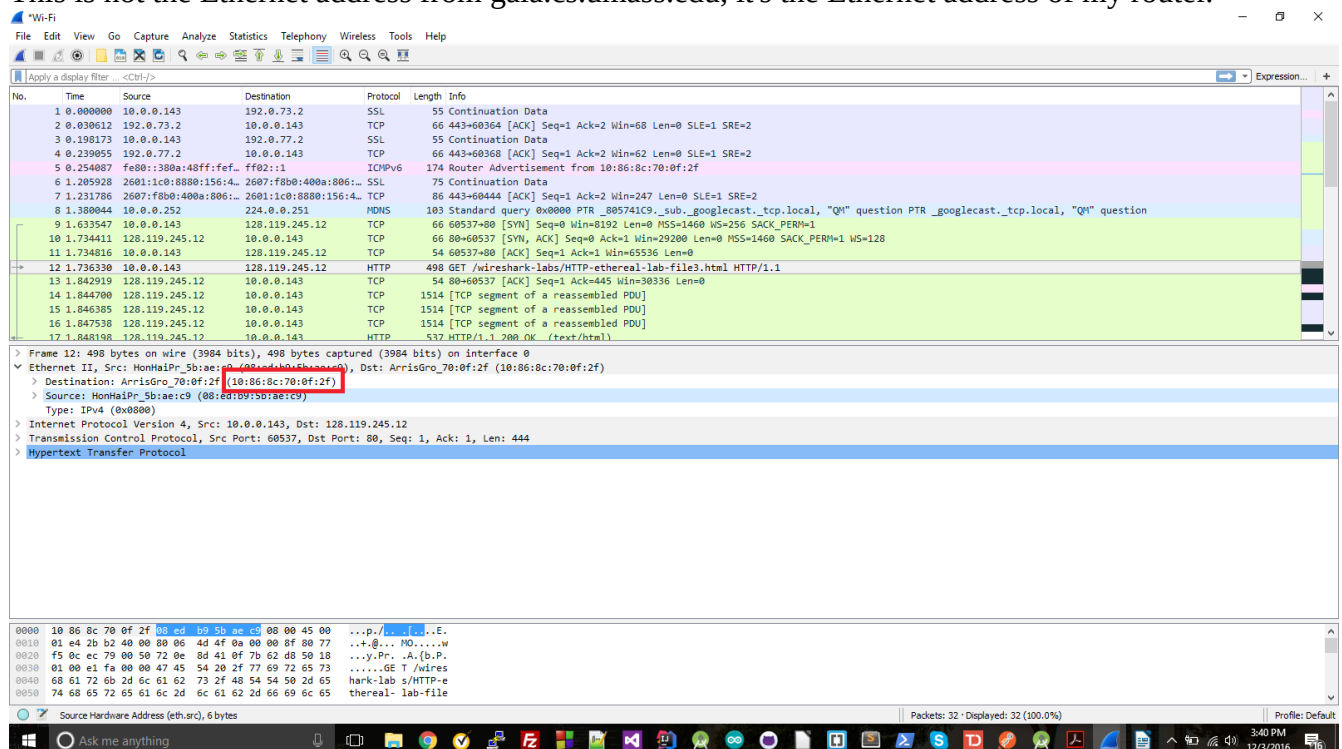


1) My Ethernet address is: 08:ed:b9:5b:ae:c9

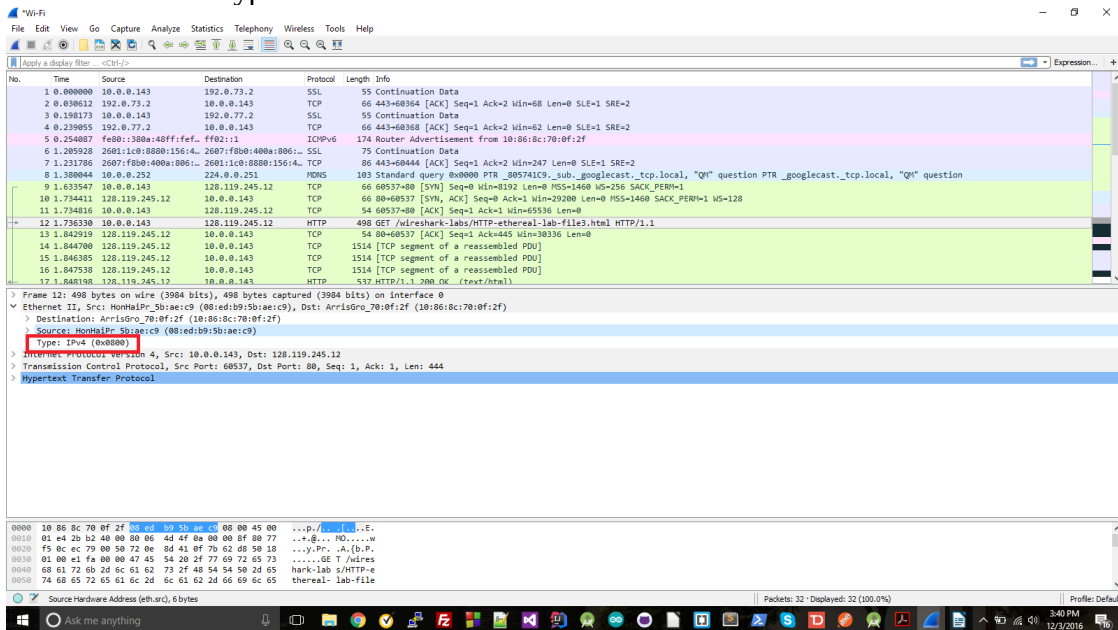


2) The destination Ethernet address is: 10:86:8c:70:0f:2f

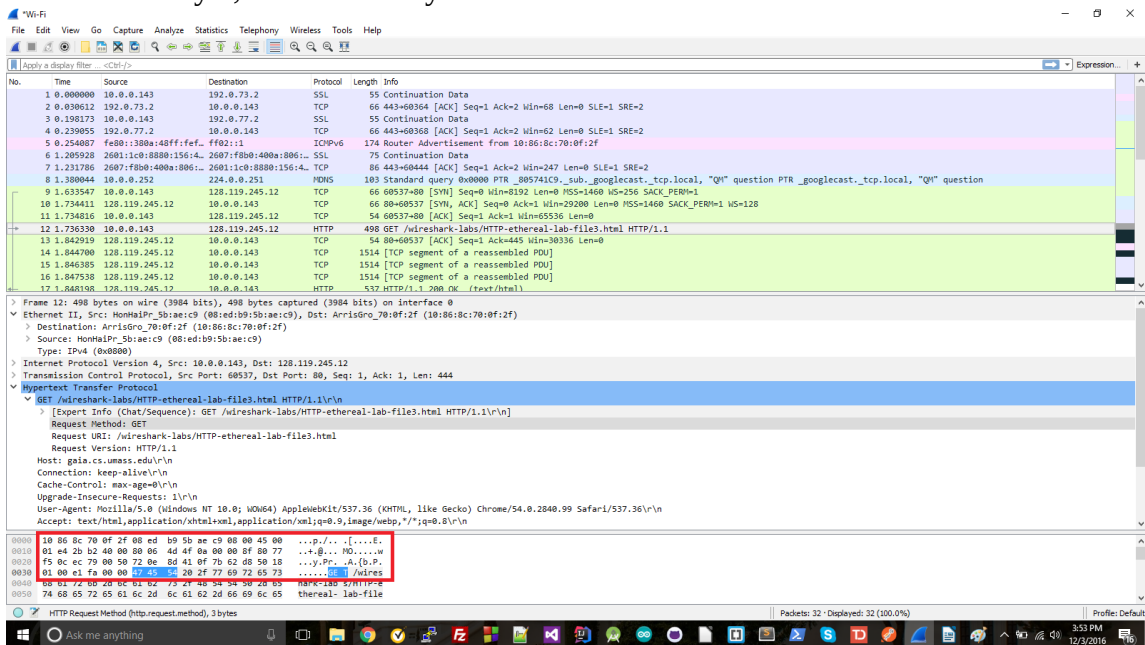
This is not the Ethernet address from gaia.cs.umass.edu, it's the Ethernet address of my router.



3) The hex value for the Type field is 0x0800. This is IPv4



4) The 'G' is the 55th byte; there are 44 bytes before it



5) The source is 10:86:8c:70:0f:2f. It is not the ethernet address of gaia.umass, but of my router.

The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main display area shows a list of captured packets. Packet 14 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The source MAC address is 10:86:8c:70:0f:2f and the destination MAC address is 08:ed:b9:5b:ae:c9. The packet is an HTTP GET request for /wireshark-labs/HTTP-ethereal-lab-file3.html. The packet length is 1514 bytes.

6) The destination is 08:ed:b9:5b:ae:c9. This is the address of my computer

The image shows a Wireshark packet capture interface, similar to the one above. The main display area shows the details of packet 14, which is an HTTP GET request. The source MAC address is 10:86:8c:70:0f:2f and the destination MAC address is 08:ed:b9:5b:ae:c9. The packet is an HTTP GET request for /wireshark-labs/HTTP-ethereal-lab-file3.html. The packet length is 1514 bytes.

7) The type field hex value is 0x0800, which is IPv4.

The image shows a Wireshark packet capture window titled "Wi-Fi". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar, and a display filter bar set to "eth[0]".

The packet list pane shows several packets. Packet 14 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.

Packet 14 Details:

- Ethernet II:** Src: ArrisGro_70:0f:2f (10:86:8c:70:0f:2f), Dst: HonHaiPr_5b:ae:c9 (08:ed:b9:5b:ae:c9). Type: IPv4 (0x0800).
- Internet Protocol Version 4:** Src: 128.119.245.12, Dst: 10.0.0.143.
- Transmission Control Protocol:** Src Port: 80, Dst Port: 60537, Seq: 1, Ack: 445, Len: 1460.

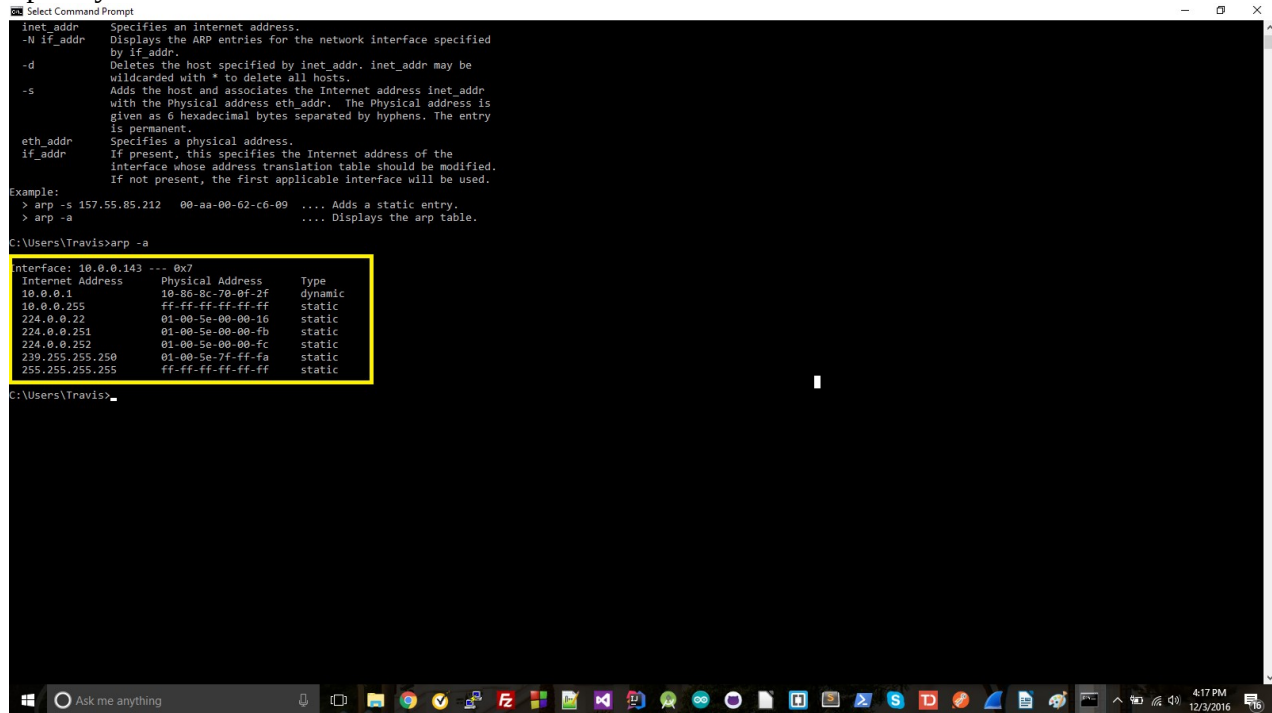
The packet bytes pane shows the raw data of the selected packet, starting with the Ethernet II header (00 ed 2c e1 00 00 48 54 54 50 2f 31 2e 31 20 32) and the IPv4 header (00 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74).

8) The 'O' in OK appears after 74 bytes.

Wireshark packet capture showing an HTTP 200 OK response. The packet list shows packet 14 as the first segment of a reassembled PDU. The packet details pane shows the HTTP status line as '200 OK (text/html)'. The packet bytes pane shows the raw data, with a red box highlighting the sequence of bytes starting at offset 0000:0000, which includes the '200 OK' status code.

Wireshark packet capture showing an HTTP 200 OK response. The packet list shows packet 14 as the first segment of a reassembled PDU. The packet details pane shows the HTTP status line as '200 OK (text/html)'. The packet bytes pane shows the raw data, with a red box highlighting the sequence of bytes starting at offset 0000:0000, which includes the '200 OK' status code.

9) The Internet Address column is a list of IP addresses that have been added to the ARP table. The Physical Address column is the Physical addresses that have been logged for each IP (aka the physical address that is the actual address of that IP). The third column is type, which says if a particular IP/Physical pairing is static or dynamic, static being pairs that are manually added to the cache and are permanent, and dynamic being pairs that are added by past ARP requests/resolutions, which are temporary.



```
Select Command Prompt

inet_addr Specifies an Internet address.
-N if_addr Displays the ARP entries for the network interface specified by if_addr.
-d Deletes the host specified by inet_addr. inet_addr may be wildcarded with * to delete all hosts.
-s Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.
eth_addr Specifies a physical address.
if_addr If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

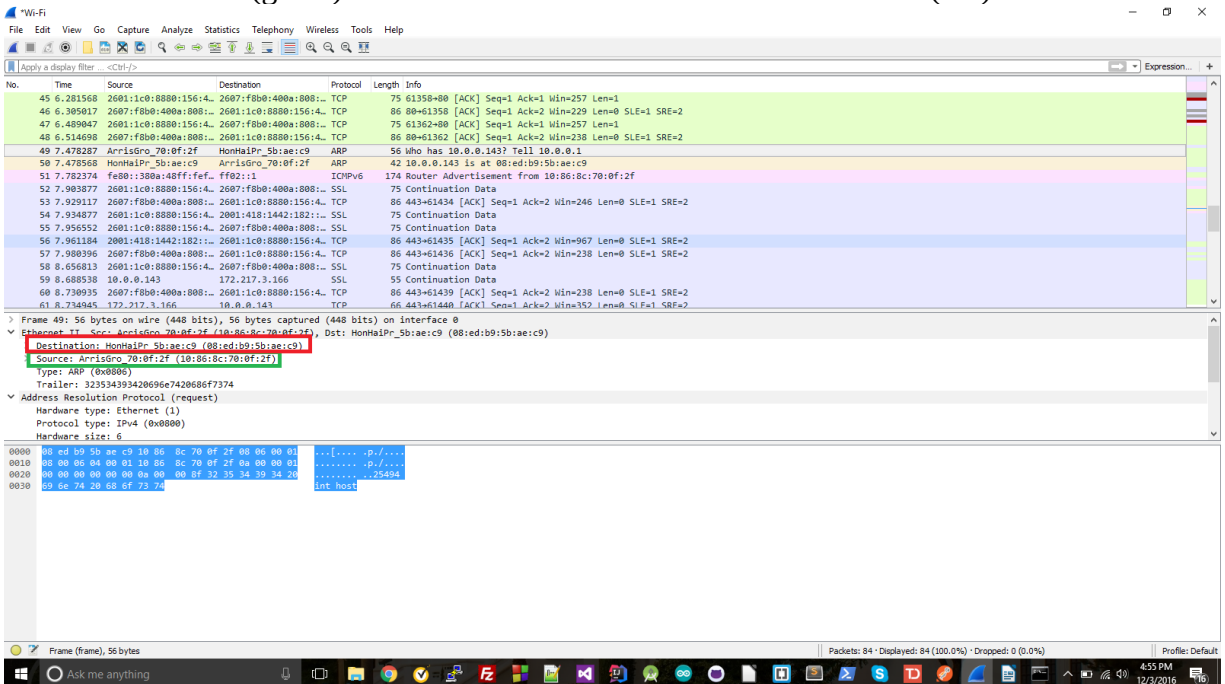
Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a .... Displays the arp table.

C:\Users\Travis>arp -a

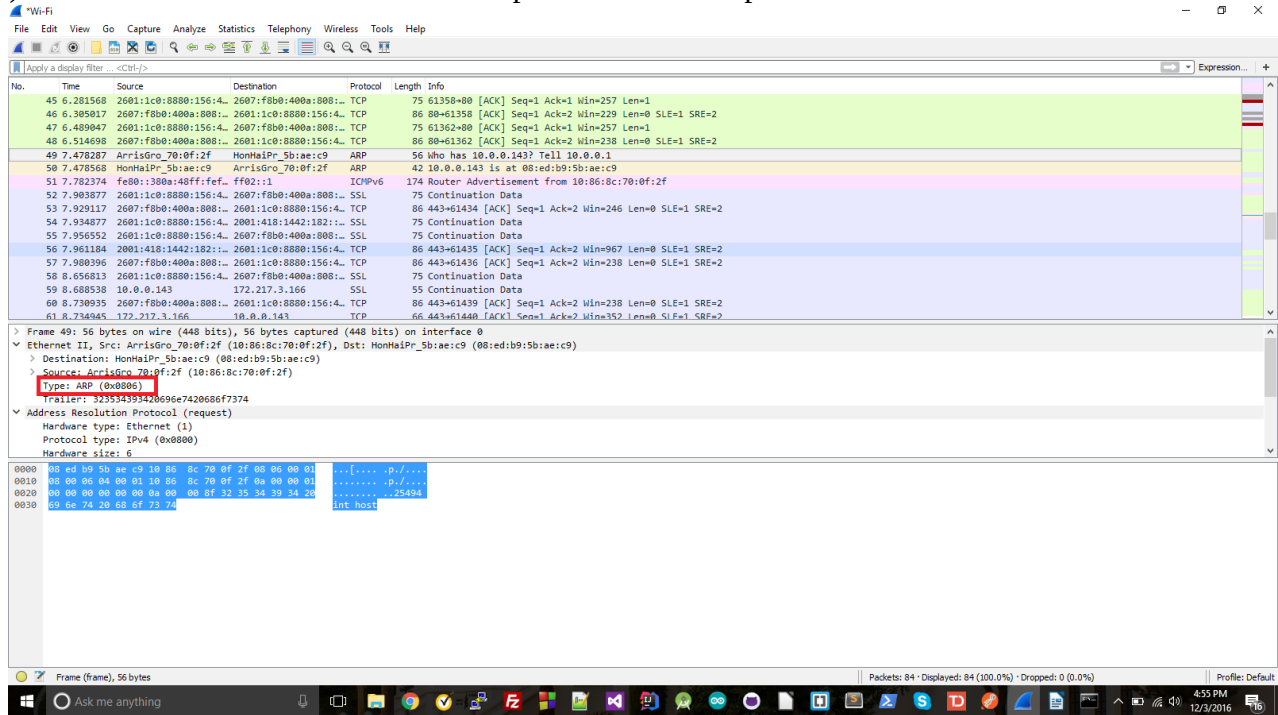
Interface: 10.0.0.143 --- 0x7
Internet Address Physical Address Type
10.0.0.1 10-86-8c-70-0f-2f dynamic
10.0.0.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static

C:\Users\Travis>
```

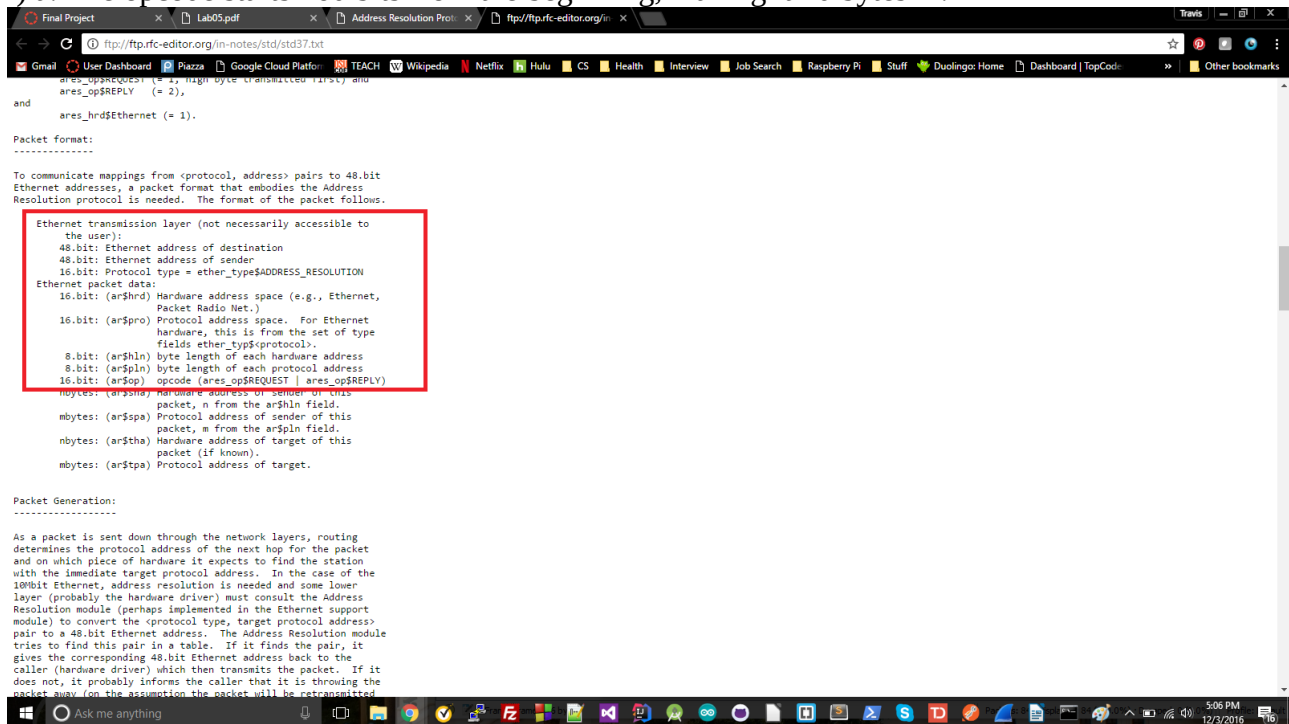
10) The source address (green) is 10:86:8c:70:0f:2f. The destination address (red) is 08:ed:b9:5b:ae:c9.



11) The value field is 0x0806. This corresponds to the ARP protocol



12) a) The opcode starts 160 bits from the beginning, making it 20 bytes in.



b: The opcode value is request (1)

Wireshark packet capture showing an ARP request. The packet list shows an ARP request from 10.0.0.1 to 10.0.0.1. The packet details pane shows the 'Opcode: request (1)' field highlighted in red. The packet bytes pane shows the raw data of the ARP request.

No.	Time	Source	Destination	Protocol	Length	Info
45	6.281568	2601:1c0:8800:156:4	2607:f8b0:400a:808::	TCP	75	61358→80 [ACK] Seq=1 Ack=1 Win=257 Len=1
46	6.305017	2607:f8b0:400a:808::	2601:1c0:8800:156:4	TCP	86	80→61358 [ACK] Seq=1 Ack=2 Win=229 Len=0 SLE=1 SRE=2
47	6.489047	2601:1c0:8800:156:4	2607:f8b0:400a:808::	TCP	75	61362→80 [ACK] Seq=1 Ack=1 Win=257 Len=1
48	6.514698	2607:f8b0:400a:808::	2601:1c0:8800:156:4	TCP	86	80→61362 [ACK] Seq=1 Ack=2 Win=238 Len=0 SLE=1 SRE=2
49	7.478287	ArriGro_70:0f:2f	HonHaiPr_5b:aec:c9	ARP	56	Who has 10.0.0.143? Tell 10.0.0.1
50	7.478568	HonHaiPr_5b:aec:c9	ArriGro_70:0f:2f	ARP	42	10.0.0.143 is at 00:ed:b9:5b:aec:c9
51	7.782374	fe80::3b0a:48ff:fe01::ff02:1	ff02::1	ICMPv6	174	Router Advertisement from 10:86:8c:70:0f:2f
52	7.903877	2601:1c0:8800:156:4	2607:f8b0:400a:808::	SSL	75	Continuation Data
53	7.929117	2607:f8b0:400a:808::	2601:1c0:8800:156:4	TCP	86	443→61434 [ACK] Seq=1 Ack=2 Win=246 Len=0 SLE=1 SRE=2
54	7.934877	2601:1c0:8800:156:4	2601:418:1442:182::	SSL	75	Continuation Data
55	7.956552	2601:1c0:8800:156:4	2607:f8b0:400a:808::	SSL	75	Continuation Data
56	7.961184	2601:418:1442:182::	2601:1c0:8800:156:4	TCP	86	443→61435 [ACK] Seq=1 Ack=2 Win=967 Len=0 SLE=1 SRE=2
57	7.980996	2607:f8b0:400a:808::	2601:1c0:8800:156:4	TCP	86	443→61436 [ACK] Seq=1 Ack=2 Win=238 Len=0 SLE=1 SRE=2
58	8.656813	2601:1c0:8800:156:4	2607:f8b0:400a:808::	SSL	75	Continuation Data
59	8.688538	10.0.0.143	172.217.3.166	SSL	55	Continuation Data
60	8.730935	2607:f8b0:400a:808::	2601:1c0:8800:156:4	TCP	86	443→61439 [ACK] Seq=1 Ack=2 Win=238 Len=0 SLE=1 SRE=2
61	8.734945	172.217.3.166	10.0.0.143	TCP	66	443→61440 [ACK] Seq=1 Ack=2 Win=352 Len=0 SLE=1 SRE=2

Type: ARP (0x0806)
Trailer: 3235343934206967420686f7374
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: ArriGro_70:0f:2f (10:86:8c:70:0f:2f)
Sender IP address: 10.0.0.1

0000 08 ed b9 5b ae c9 10 86 8c 70 0f 2f 08 06 00 01 ...[.....].p./....
0010 08 00 06 04 00 01 10 86 8c 70 0f 2f 0a 00 00 01 ...[.....].p./....
0020 00 00 00 00 00 0a 00 00 8f 32 35 34 39 34 2025494
0030 69 6e 74 20 68 6f 73 74int host

c: It does

Wireshark packet capture showing an ARP request. The packet list shows an ARP request from 10.0.0.1 to 10.0.0.1. The packet details pane shows the 'Opcode: request (1)' field highlighted in red. The packet bytes pane shows the raw data of the ARP request.

No.	Time	Source	Destination	Protocol	Length	Info
45	6.281568	2601:1c0:8800:156:4	2607:f8b0:400a:808::	TCP	75	61358→80 [ACK] Seq=1 Ack=1 Win=257 Len=1
46	6.305017	2607:f8b0:400a:808::	2601:1c0:8800:156:4	TCP	86	80→61358 [ACK] Seq=1 Ack=2 Win=229 Len=0 SLE=1 SRE=2
47	6.489047	2601:1c0:8800:156:4	2607:f8b0:400a:808::	TCP	75	61362→80 [ACK] Seq=1 Ack=1 Win=257 Len=1
48	6.514698	2607:f8b0:400a:808::	2601:1c0:8800:156:4	TCP	86	80→61362 [ACK] Seq=1 Ack=2 Win=238 Len=0 SLE=1 SRE=2
49	7.478287	ArriGro_70:0f:2f	HonHaiPr_5b:aec:c9	ARP	56	Who has 10.0.0.143? Tell 10.0.0.1
50	7.478568	HonHaiPr_5b:aec:c9	ArriGro_70:0f:2f	ARP	42	10.0.0.143 is at 00:ed:b9:5b:aec:c9
51	7.782374	fe80::3b0a:48ff:fe01::ff02:1	ff02::1	ICMPv6	174	Router Advertisement from 10:86:8c:70:0f:2f
52	7.903877	2601:1c0:8800:156:4	2607:f8b0:400a:808::	SSL	75	Continuation Data
53	7.929117	2607:f8b0:400a:808::	2601:1c0:8800:156:4	TCP	86	443→61434 [ACK] Seq=1 Ack=2 Win=246 Len=0 SLE=1 SRE=2
54	7.934877	2601:1c0:8800:156:4	2601:418:1442:182::	SSL	75	Continuation Data
55	7.956552	2601:1c0:8800:156:4	2607:f8b0:400a:808::	SSL	75	Continuation Data
56	7.961184	2601:418:1442:182::	2601:1c0:8800:156:4	TCP	86	443→61435 [ACK] Seq=1 Ack=2 Win=967 Len=0 SLE=1 SRE=2
57	7.980996	2607:f8b0:400a:808::	2601:1c0:8800:156:4	TCP	86	443→61436 [ACK] Seq=1 Ack=2 Win=238 Len=0 SLE=1 SRE=2
58	8.656813	2601:1c0:8800:156:4	2607:f8b0:400a:808::	SSL	75	Continuation Data
59	8.688538	10.0.0.143	172.217.3.166	SSL	55	Continuation Data
60	8.730935	2607:f8b0:400a:808::	2601:1c0:8800:156:4	TCP	86	443→61439 [ACK] Seq=1 Ack=2 Win=238 Len=0 SLE=1 SRE=2
61	8.734945	172.217.3.166	10.0.0.143	TCP	66	443→61440 [ACK] Seq=1 Ack=2 Win=352 Len=0 SLE=1 SRE=2

Type: ARP (0x0806)
Trailer: 3235343934206967420686f7374
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: ArriGro_70:0f:2f (10:86:8c:70:0f:2f)
Sender IP address: 10.0.0.1

0000 08 ed b9 5b ae c9 10 86 8c 70 0f 2f 08 06 00 01 ...[.....].p./....
0010 08 00 06 04 00 01 10 86 8c 70 0f 2f 0a 00 00 01 ...[.....].p./....
0020 00 00 00 00 00 0a 00 00 8f 32 35 34 39 34 2025494
0030 69 6e 74 20 68 6f 73 74int host

d: The question is the MAC address set to all 0's

Wireshark packet capture showing an ARP request. The packet list pane shows a packet from 10.0.0.1 to 10.0.0.143. The packet details pane shows the hardware type as Ethernet (I), protocol type as IPv4 (0x0800), and the target MAC address as 00:00:00:00:00:00. The packet bytes pane shows the raw data of the ARP request.

13) a: 20 bytes

Wireshark packet capture showing an ARP reply. The packet list pane shows a packet from 10.0.0.143 to 10.0.0.1. The packet details pane shows the hardware type as Ethernet (I), protocol type as IPv4 (0x0800), and the target MAC address as 00:00:00:00:00:00. The packet bytes pane shows the raw data of the ARP reply.

b: reply(2)

The screenshot shows a Wireshark packet capture of an ARP request and reply. The packet list shows a sequence of TCP and SSL packets, followed by an ARP request (No. 49) and an ARP reply (No. 50). The details pane for the ARP reply packet is expanded, showing the 'Opcode: reply (2)' field. The packet bytes pane shows the raw data of the ARP reply packet.

No.	Time	Source	Destination	Protocol	Length	Info
45	6.281568	2601:1c0:8880:156:4...	2607:f8b0:400a:808::...	TCP	75	61358-80 [ACK] Seq=1 Ack=1 Win=257 Len=1
46	6.305017	2607:f8b0:400a:808::...	2601:1c0:8880:156:4...	TCP	86	80+61358 [ACK] Seq=1 Ack=2 Win=229 Len=0 SLE=1 SRE=2
47	6.489047	2601:1c0:8880:156:4...	2607:f8b0:400a:808::...	TCP	75	61362-80 [ACK] Seq=1 Ack=1 Win=257 Len=1
48	6.514698	2607:f8b0:400a:808::...	2601:1c0:8880:156:4...	TCP	86	80+61362 [ACK] Seq=1 Ack=2 Win=238 Len=0 SLE=1 SRE=2
49	7.478287	Arri5Gro_70:0f:2f	HonhaiPr_5b:ae:c9	ARP	56	Who has 10.0.0.143? Tell 10.0.0.1
50	7.478568	HonhaiPr_5b:ae:c9	Arri5Gro_70:0f:2f	ARP	42	10.0.0.143 is at 08:ed:b9:5b:ae:c9
51	7.782374	fe80::300a:48ff:fe02::1	ICMPv6	174	Router Advertisement from 10:86:8c:70:0f:2f	
52	7.903877	2601:1c0:8880:156:4...	2607:f8b0:400a:808::...	SSL	75	Continuation Data
53	7.929117	2607:f8b0:400a:808::...	2601:1c0:8880:156:4...	TCP	86	443+61434 [ACK] Seq=1 Ack=2 Win=246 Len=0 SLE=1 SRE=2
54	7.934877	2601:1c0:8880:156:4...	2001:418:1442:182::...	SSL	75	Continuation Data
55	7.956552	2601:1c0:8880:156:4...	2607:f8b0:400a:808::...	SSL	75	Continuation Data
56	7.961184	2001:418:1442:182::...	2601:1c0:8880:156:4...	TCP	86	443+61435 [ACK] Seq=1 Ack=2 Win=967 Len=0 SLE=1 SRE=2
57	7.980396	2607:f8b0:400a:808::...	2601:1c0:8880:156:4...	TCP	86	443+61436 [ACK] Seq=1 Ack=2 Win=238 Len=0 SLE=1 SRE=2
58	8.656813	2601:1c0:8880:156:4...	2607:f8b0:400a:808::...	SSL	75	Continuation Data
59	8.688538	10.0.0.143	172.217.3.166	SSL	55	Continuation Data
60	8.730935	2607:f8b0:400a:808::...	2601:1c0:8880:156:4...	TCP	86	443+61439 [ACK] Seq=1 Ack=2 Win=238 Len=0 SLE=1 SRE=2
61	8.734945	172.217.3.166	10.0.0.143	TCP	66	443+61440 [ACK] Seq=1 Ack=2 Win=352 Len=0 SLE=1 SRE=2

Hardware type: Ethernet (I)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: HonhaiPr_5b:ae:c9 (08:ed:b9:5b:ae:c9)
Sender IP address: 10.0.0.143
Target MAC address: Arri5Gro_70:0f:2f (10:86:8c:70:0f:2f)
Target IP address: 10.0.0.1

0000 10 86 8c 70 0f 2f 08 ed b9 5b ae c9 08 06 00 01 ...p./... [.....]
0010 08 00 06 04 00 02 08 ed b9 5b ae c9 0a 00 00 8f [.....]
0020 10 86 8c 70 0f 2f 0a 00 00 01 ...p./... [.....]

c: In the target MAC address field

The screenshot shows a Wireshark packet capture of an ARP request and reply. The packet list shows a sequence of TCP and SSL packets, followed by an ARP request (No. 49) and an ARP reply (No. 50). The details pane for the ARP request packet is expanded, showing the 'Target MAC address: Arri5Gro_70:0f:2f' field. The packet bytes pane shows the raw data of the ARP request packet.

No.	Time	Source	Destination	Protocol	Length	Info
45	6.281568	2601:1c0:8880:156:4...	2607:f8b0:400a:808::...	TCP	75	61358-80 [ACK] Seq=1 Ack=1 Win=257 Len=1
46	6.305017	2607:f8b0:400a:808::...	2601:1c0:8880:156:4...	TCP	86	80+61358 [ACK] Seq=1 Ack=2 Win=229 Len=0 SLE=1 SRE=2
47	6.489047	2601:1c0:8880:156:4...	2607:f8b0:400a:808::...	TCP	75	61362-80 [ACK] Seq=1 Ack=1 Win=257 Len=1
48	6.514698	2607:f8b0:400a:808::...	2601:1c0:8880:156:4...	TCP	86	80+61362 [ACK] Seq=1 Ack=2 Win=238 Len=0 SLE=1 SRE=2
49	7.478287	Arri5Gro_70:0f:2f	HonhaiPr_5b:ae:c9	ARP	56	Who has 10.0.0.143? Tell 10.0.0.1
50	7.478568	HonhaiPr_5b:ae:c9	Arri5Gro_70:0f:2f	ARP	42	10.0.0.143 is at 08:ed:b9:5b:ae:c9
51	7.782374	fe80::300a:48ff:fe02::1	ICMPv6	174	Router Advertisement from 10:86:8c:70:0f:2f	
52	7.903877	2601:1c0:8880:156:4...	2607:f8b0:400a:808::...	SSL	75	Continuation Data
53	7.929117	2607:f8b0:400a:808::...	2601:1c0:8880:156:4...	TCP	86	443+61434 [ACK] Seq=1 Ack=2 Win=246 Len=0 SLE=1 SRE=2
54	7.934877	2601:1c0:8880:156:4...	2001:418:1442:182::...	SSL	75	Continuation Data
55	7.956552	2601:1c0:8880:156:4...	2607:f8b0:400a:808::...	SSL	75	Continuation Data
56	7.961184	2001:418:1442:182::...	2601:1c0:8880:156:4...	TCP	86	443+61435 [ACK] Seq=1 Ack=2 Win=967 Len=0 SLE=1 SRE=2
57	7.980396	2607:f8b0:400a:808::...	2601:1c0:8880:156:4...	TCP	86	443+61436 [ACK] Seq=1 Ack=2 Win=238 Len=0 SLE=1 SRE=2
58	8.656813	2601:1c0:8880:156:4...	2607:f8b0:400a:808::...	SSL	75	Continuation Data
59	8.688538	10.0.0.143	172.217.3.166	SSL	55	Continuation Data
60	8.730935	2607:f8b0:400a:808::...	2601:1c0:8880:156:4...	TCP	86	443+61439 [ACK] Seq=1 Ack=2 Win=238 Len=0 SLE=1 SRE=2
61	8.734945	172.217.3.166	10.0.0.143	TCP	66	443+61440 [ACK] Seq=1 Ack=2 Win=352 Len=0 SLE=1 SRE=2

Hardware type: Ethernet (I)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: HonhaiPr_5b:ae:c9 (08:ed:b9:5b:ae:c9)
Sender IP address: 10.0.0.143
Target MAC address: Arri5Gro_70:0f:2f (10:86:8c:70:0f:2f)
Target IP address: 10.0.0.1

0000 10 86 8c 70 0f 2f 08 ed b9 5b ae c9 08 06 00 01 ...p./... [.....]
0010 08 00 06 04 00 02 08 ed b9 5b ae c9 0a 00 00 8f [.....]
0020 10 86 8c 70 0f 2f 0a 00 00 01 ...p./... [.....]

14) The source IP address: 08:ed:b9L5bLaeLc9
The destination IP address: 10:86:8c:70:0f:2f

The screenshot shows a Wireshark packet capture on a Wi-Fi interface. The packet list displays several TCP and SSL packets, followed by an ARP request (No. 50) from 2601:1c0:8880:156:4:: to 2607:f80:400a:808::. The packet details pane shows the Ethernet II frame with source 08:ed:b9:5b:ae:c9 and destination 10:86:8c:70:0f:2f. The ARP request is for the IP 10:86:8c:70:0f:2f. The packet bytes pane shows the raw data of the ARP request.

No.	Time	Source	Destination	Protocol	Length	Info
45	6.281568	2601:1c0:8880:156:4::	2607:f80:400a:808::	TCP	75	61358→80 [ACK] Seq=1 Ack=1 Win=257 Len=1
46	6.305017	2607:f80:400a:808::	2601:1c0:8880:156:4::	TCP	86	80→61358 [ACK] Seq=1 Ack=2 Win=229 Len=0 SLE=1 SRE=2
47	6.489047	2601:1c0:8880:156:4::	2607:f80:400a:808::	TCP	75	61362→80 [ACK] Seq=1 Ack=1 Win=257 Len=1
48	6.514698	2607:f80:400a:808::	2601:1c0:8880:156:4::	TCP	86	80→61362 [ACK] Seq=1 Ack=2 Win=238 Len=0 SLE=1 SRE=2
49	7.478287	ArriGro_70:0f:2f	HonHaiPr_5b:ae:c9	ARP	56	Who has 10.0.0.143? Tell 10.0.0.1
50	7.478568	HonHaiPr_5b:ae:c9	ArriGro_70:0f:2f	ARP	42	10.0.0.143 is at 08:ed:b9:5b:ae:c9

Destination: ArriGro_70:0f:2f (10:86:8c:70:0f:2f)
Source: HonHaiPr_5b:ae:c9 (08:ed:b9:5b:ae:c9)
Type: ARP (0x0806)
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4

15) Because the wrong sender IP was used. The one that received the reply was 192.168.1.105 (green), while the one that did not was 192.168.1.104 (red), so the ARP reply was sent to the wrong IP for the one that did not get a reply.

The screenshot shows a Wireshark packet capture on an ethernet-ethereal-trace-1 interface. The packet list displays several TCP and HTTP packets, followed by an ARP request (No. 6) from 192.168.1.105 to 192.168.1.104. The packet details pane shows the Ethernet II frame with source 08:00:00:00:00:00 and destination ff:ff:ff:ff:ff:ff. The ARP request is for the IP 192.168.1.104. The packet bytes pane shows the raw data of the ARP request.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMlc_9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001016	Linksys_08:01:77:5	AmbitMlc_9:3d:68	ARP	60	192.168.1.1 is at 00:00:02:19:0a:01:77:5
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=1
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=1
5	6.901188	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=1
6	13.542974	Telebit_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104

Ethernet II, Src: Telebit_73:8d:ce (00:00:ad:73:8d:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

EX-1

You would send your messages to the wrong MAC address. This could cause your messages to be delayed or lost (depending on where your messages final destination were, the place you sent them could potentially still forward them towards the final destination)

EX-2

An ARP entry stays in the table for 2 minutes. If an entry is re-referenced it is given additional time in the table, up to 10 minutes.

Source: <https://technet.microsoft.com/en-us/library/cc940021.aspx>