



**VILNIUS UNIVERSITY
SIAULIAI ACADEMY**

PROGRAMŲ SISTEMOS BACHELOR STUDY PROGRAMME

Software engineering

ANNA KUTOVA

**Computer Networks
Laboratory work No.7
ARP**

Šiauliai, 2025

Laboratory Work Report

Table of contents

<i>Capturing and analyzing Ethernet frames</i>	2
<i>The Address Resolution Protocol</i>	6
ARP Caching	6
Observing ARP in action	6

Capturing and analyzing Ethernet frames

Since I used the file *ethernet--ethereal-trace-1* for this lab, for convenience I will refer to the sender's machine and MAC address in the trace as my machine and my MAC address - even though the trace was originally captured on the authors' computer.

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

No.	Time	Source	Destination	Protocol	Length	Ethernet	Info
1	0.000000	00:d0:59:a9:3d:68	ff:ff:ff:ff:ff:ff	ARP	42	✓	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	00:06:25:da:af:73	00:d0:59:a9:3d:68	ARP	60	✓	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	✓	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	✓	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	✓	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0
6	13.542974	00:80:ad:73:8d:ce	ff:ff:ff:ff:ff:ff	ARP	60	✓	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1.105	128.119.245.12	TCP	62	✓	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	✓	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 S
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	✓	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	✓	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	✓	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.498935	128.119.245.12	192.168.1.105	TCP	1514	✓	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [TCP PDU r
13	17.500025	128.119.245.12	192.168.1.105	TCP	1514	✓	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460 [TCP PD
14	17.500069	192.168.1.105	128.119.245.12	TCP	54	✓	1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0
15	17.527057	128.119.245.12	192.168.1.105	TCP	1514	✓	80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460 [TCP PD
16	17.527422	128.119.245.12	192.168.1.105	HTTP	489	✓	HTTP/1.1 200 OK (text/html)
17	17.527457	192.168.1.105	128.119.245.12	TCP	54	✓	1058 → 80 [ACK] Seq=633 Ack=4816 Win=64240 Len=0

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: 00:d0:59:a9:3d:68, Dst: ff:ff:ff:ff:ff:ff
Destination: ff:ff:ff:ff:ff:ff

Answer: the 48-bit Ethernet address of my computer is
00:d0:59:a9:3d:68

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?

No.	Time	Source	Destination	Protocol	Length	Ethernet	Info
1	0.000000	00:d0:59:a9:3d:68	ff:ff:ff:ff:ff:ff	ARP	42	✓	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	00:06:25:da:af:73	00:d0:59:a9:3d:68	ARP	60	✓	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	✓	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	✓	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	✓	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0
6	13.542974	00:80:ad:73:8d:ce	ff:ff:ff:ff:ff:ff	ARP	60	✓	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1.105	128.119.245.12	TCP	62	✓	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	✓	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 S
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	✓	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	✓	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	✓	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.498935	128.119.245.12	192.168.1.105	TCP	1514	✓	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [TCP PDU r
13	17.500025	128.119.245.12	192.168.1.105	TCP	1514	✓	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460 [TCP PDI
14	17.500069	192.168.1.105	128.119.245.12	TCP	54	✓	1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0
15	17.527057	128.119.245.12	192.168.1.105	TCP	1514	✓	80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460 [TCP PDI
16	17.527422	128.119.245.12	192.168.1.105	HTTP	489	✓	HTTP/1.1 200 OK (text/html)
17	17.527457	192.168.1.105	128.119.245.12	TCP	54	✓	1058 → 80 [ACK] Seq=633 Ack=4816 Win=64240 Len=0

> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)	0000	00 d0 59 a9 3d 68 00 06 25 da af 73 08 06 00 01	Y=h	%:s
✓ Ethernet II, Src: 00:06:25:da:af:73, Dst: 00:d0:59:a9:3d:68	0010	08 00 06 04 00 02 00 06 25 da af 73 c0 a8 01 01	Y=h	%:s
Destination: 00:d0:59:a9:3d:68	0020	00 d0 59 a9 3d 68 c0 a8 01 69 00 00 00 00 00 00	Y=h	%:s
... .. = LG bit: Globally unique address	0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
... .. = IG bit: Individual address (unicast)				
Source: 00:06:25:da:af:73				
... .. = LG bit: Globally unique address				
... .. = IG bit: Individual address (unicast)				

Answer:

- The 48-bit destination address in the Ethernet frame is **00:06:25:da:af:73**
- This address is not the Ethernet address of gaia.cs.umass.edu - it belongs to my TP-Link router, which serves as the gateway to the Internet.

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

What upper layer protocol does this correspond to?

1	0.000000	00:d0:59:a9:3d:68	ff:ff:ff:ff:ff:ff	ARP	42	✓	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	00:06:25:da:af:73	00:d0:59:a9:3d:68	ARP	60	✓	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	✓	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	✓	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	✓	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240
6	13.542974	00:80:ad:73:8d:ce	ff:ff:ff:ff:ff:ff	ARP	60	✓	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1.105	128.119.245.12	TCP	62	✓	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	✓	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)	0000	ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01	Y=h	%:s
✓ Ethernet II, Src: 00:06:25:da:af:73, Dst: 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	%:s
Destination: ff:ff:ff:ff:ff:ff	0020	00 00 00 00 00 00 c0 a8 01 01		
Source: 00:d0:59:a9:3d:68				
Type: ARP (0x0806)				

Answer:

- The hexadecimal value for the two-byte Frame type field is **0x0806**
- This corresponds to the **ARP** (Address Resolution Protocol), which is used to map IP addresses to MAC (Ethernet) addresses on a local network.

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

Is this the Ethernet address of your computer?

12	17.498935	128.119.245.12	192.168.1.105	TCP	1514	✓	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460	TC
13	17.500025	128.119.245.12	192.168.1.105	TCP	1514	✓	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460	
> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0 Ethernet II, Src: 00:06:25:da:af:73, Dst: 00:d0:59:a9:3d:68 Destination: 00:d0:59:a9:3d:68								

Answer:

- The destination address in the Ethernet frame is **00:d0:59:a9:3d:68**
- Yes, this is the Ethernet address of my computer

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

> Ethernet II, Src: 00:06:25:da:af:73, Dst: 00:d0:59:a9:3d:68 > Destination: 00:d0:59:a9:3d:680. = LG bit: Globally unique address0. = IG bit: Individual address (unicast) > Source: 00:06:25:da:af:730. = LG bit: Globally unique address0. = IG bit: Individual address (unicast) Type: IPv4 (0x0800) [Stream index: 1]	> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.105
--	--

Answer:

- The hexadecimal value for the two-byte Frame type field is **0x0800**
- This correspond to **Internet Protocol Version 4 (IPv4)**

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?

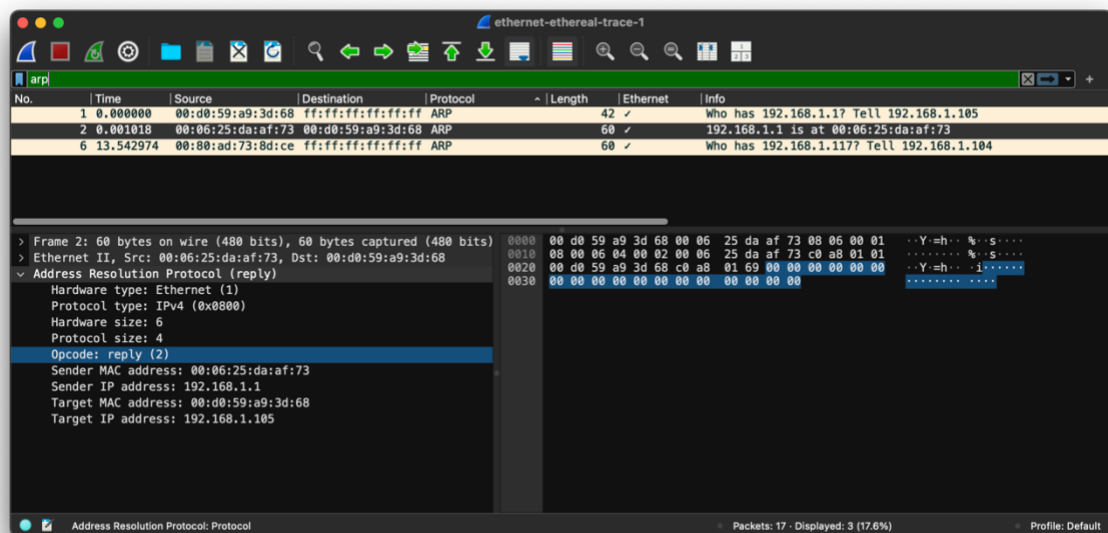
16	17.527422	128.119.245.12	192.168.1.105	HTTP	489	✓	HTTP/1.1 200 OK (text/html)	
17	17.527457	192.168.1.105	128.119.245.12	TCP	54	✓	1058 → 80 [ACK] Seq=633 Ack=4816 Win=64240 Len=0	
> Source: 00:06:25:da:af:730. = LG bit: Globally unique address (factory default)0. = IG bit: Individual address (unicast) Type: IPv4 (0x0800) [Stream index: 1]								
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.105 > Transmission Control Protocol, Src Port: 80, Dst Port: 1058, Seq: 4381, Ack: 633, Len: 0 > [4 Reassembled TCP Segments (4815 bytes): #12(1460), #13(1460), #15(1460), #16(1460)] > Hypertext Transfer Protocol > HTTP/1.1 200 OK\r\n Response Version: HTTP/1.1 Status Code: 200 [Status Code Description: OK] Response Phrase: OK								

Answer: The ASCII "O" in "OK" appears 54 bytes from the very start of the Ethernet frame.

The Address Resolution Protocol

ARP Caching

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



Answer: Based on the captured file, the ARP cache on the Mac would include entries from ARP reply packets.

For example:

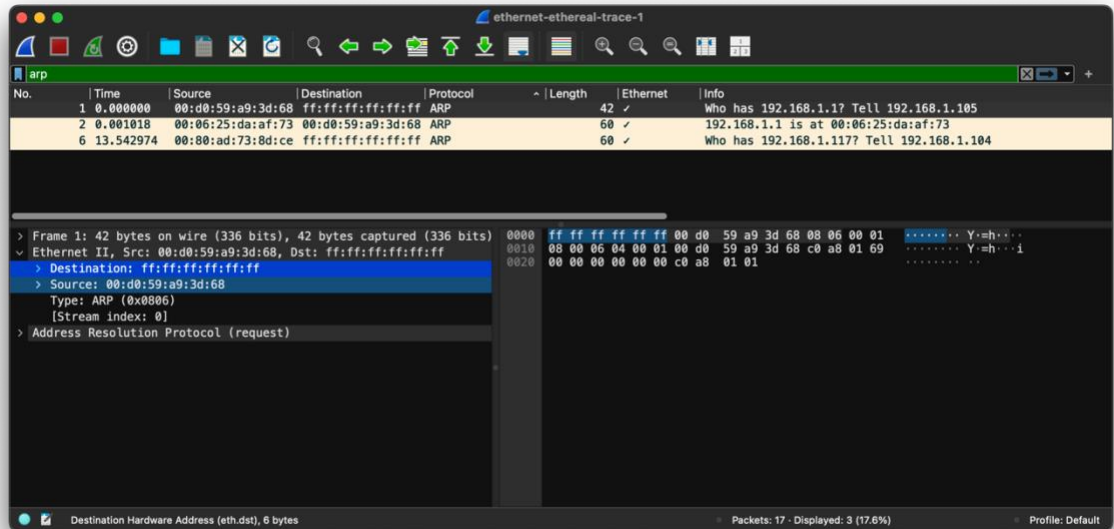
IP Address: **192.168.1.1**

MAC Address: **00:06:25:da:af:73**

This information is taken from an ARP reply, where the sender informs the target of its MAC address. The target device can then store this mapping in its ARP cache.

Observing ARP in action

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



Answer:

Source MAC: **00:d0:59:a9:3d:68**

Destination MAC: **ff:ff:ff:ff:ff:ff**

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

Answer:

- The hexadecimal value for the two-byte Ethernet Frame type field is **(0x0806)**
- This corresponds to **ARP (Address Resolution Protocol)**

12. 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>.

- How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
- What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

- c) *Does the ARP message contain the IP address of the sender?*
- d) *Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?*

Answer:

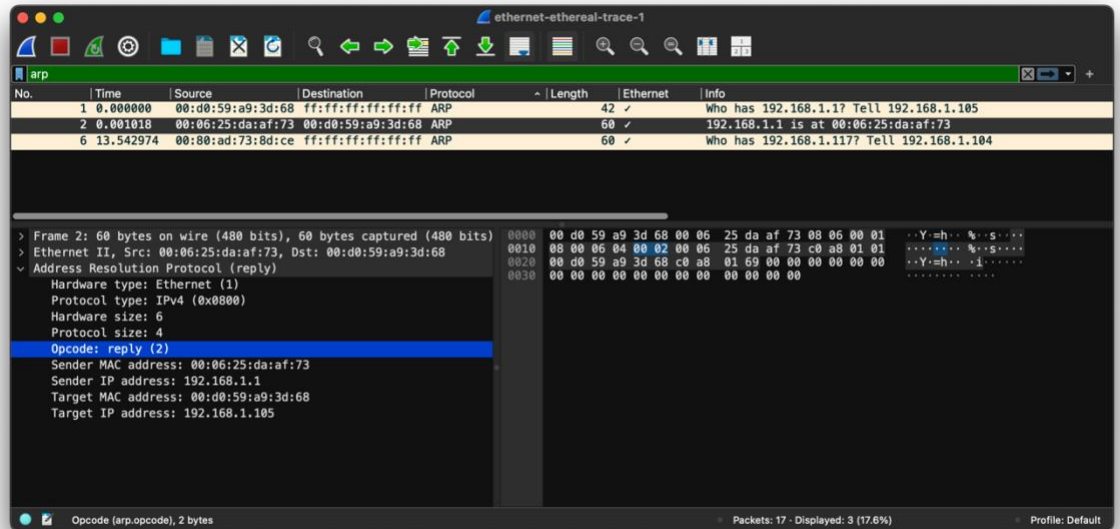
- a. The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.
- b. The value of the opcode field in an ARP request is 1.
- c. Yes, the ARP message contains the IP address of the sender.

```
> Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: 00:80:ad:73:8d:ce, Dst: ff:ff:ff:ff:ff:ff
v Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: 00:80:ad:73:8d:ce
  Sender IP address: 192.168.1.104
  Target MAC address: 00:00:00:00:00:00
  Target IP address: 192.168.1.117
```

- d. The "question" - the Ethernet address being queried - appears in the target hardware address field of the ARP request, which is typically empty (all zeros) because the sender is requesting that address.

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?*
- 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?*
- 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?*



Answer:

- The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.
- The value of the opcode field in an ARP reply is 2.
- The “answer” appears in the sender protocol address field of the ARP reply message. This field contains the IP address corresponding to the Ethernet (MAC) address being provided:

Sender IP address: 192.168.1.1

Sender MAC address: 00:06:25:da:af:73

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

```
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: 00:06:25:da:af:73, Dst: 00:d0:59:a9:3d:68
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 00:06:25:da:af:73
    Sender IP address: 192.168.1.1
    Target MAC address: 00:d0:59:a9:3d:68
    Target IP address: 192.168.1.105
```

Answer: The hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message are:

Sender MAC address: 00:06:25:da:af:73 (source)

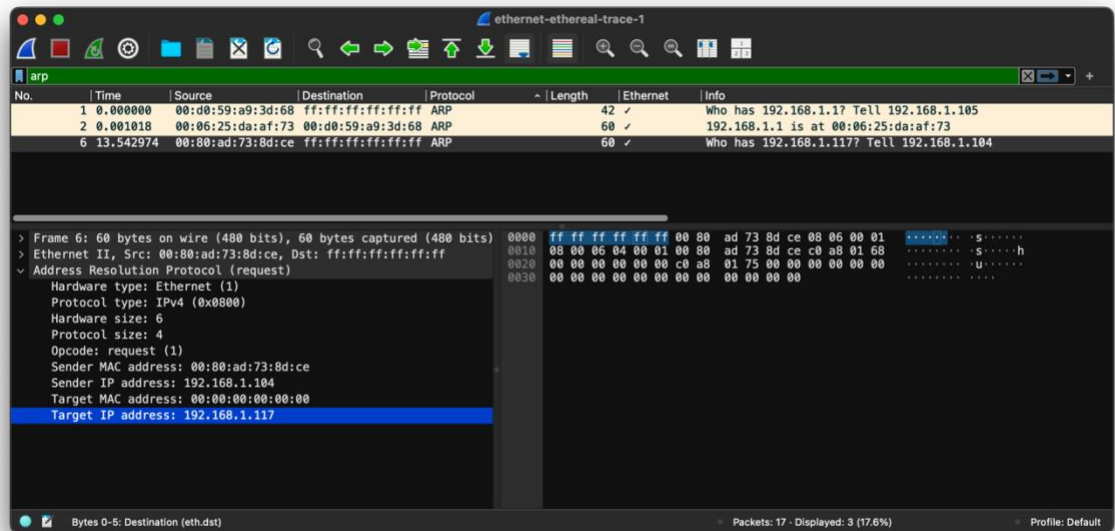
Target MAC address: 00:d0:59:a9:3d:68 (destination)

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?



Answer: There is no ARP reply in the trace for packet 6 because the ARP request is broadcast to all devices, but the ARP reply is sent only directly to the requester.

If the device with IP 192.168.1.117 did not respond (for example: it is offline or unreachable), no reply packet will appear in the trace.