

NETWORK LAB

LAB ASSIGNMENT for Week # 3

Usirikayala Likhith

20223295, D2

IP

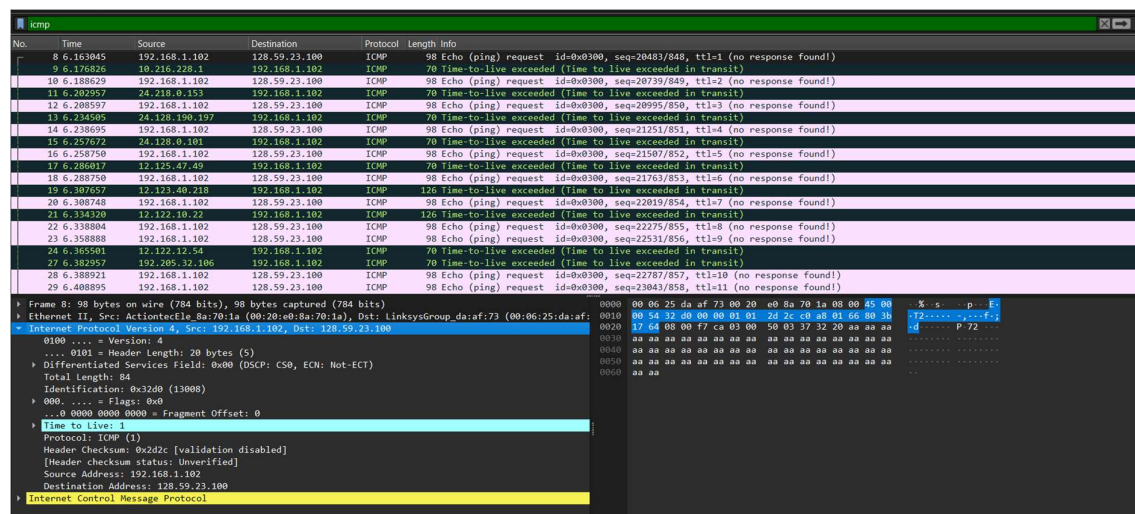
I. Simple IP Trace

Note: Answer the following questions using the ip-ethereal-trace-1 packet trace to answer the questions

below

1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

ANS:



The ip address of my computer is 192.168.1.102

2. Within the IP packet header, what is the value in the upper layer protocol field?

The Upper Layer protocol field is ICMP.

3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

There are 20 bytes in the IP header. The packet was sending 84 bytes of data. So remaining 64 bytes are payload bytes.

Payload bytes = Total bytes-IP header bytes.

Payload bytes = 84-20 = 64 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/849, ttl=1 (no response found!)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	6.205597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20993/854, ttl=3 (no response found!)
13	6.214505	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
15	6.257672	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
16	6.258750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
17	6.268017	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
18	6.288750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found!)
19	6.307657	12.123.40.210	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
20	6.308745	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22019/854, ttl=7 (no response found!)
21	6.334320	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
22	6.338804	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22275/855, ttl=8 (no response found!)
23	6.358888	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22531/856, ttl=9 (no response found!)
24	6.358501	12.122.12.54	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
27	6.382957	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
28	6.388921	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22787/857, ttl=10 (no response found!)
29	6.408895	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=23043/858, ttl=11 (no response found!)

Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0	0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00	% s...p...E
Ethernet II, Src: ActiontecLea_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)	0010 00 54 32 d0 00 00 01 20 2c c0 a0 01 66 80 3b	T2...p...f;
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100	0020 17 64 08 00 f7 ca 03 00 50 03 37 32 20 aa aa aa	d...P.72...
0100 = Version: 4	0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0101 = Header Length: 20 bytes (5)	0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
Total length: 84	0060 aa aa
Identification: 0x32d0 (13008)		
0000 = Flags: 0x0		
0000 0000 0000 = Fragment Offset: 0		
Time to Live: 1		
Protocol: ICMP (1)		
Header checksum: 0x2d2c [validation disabled]		
[Header checksum status: Unverified]		
Source Address: 192.168.1.102		
Destination Address: 128.59.23.100		
Internet Control Message Protocol		

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

No.	Time	Source	Destination	Protocol	Length	Info
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/849, ttl=1 (no response found!)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	6.205597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20993/854, ttl=3 (no response found!)
13	6.214505	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
15	6.257672	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
16	6.258750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
17	6.268017	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
18	6.288750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found!)
19	6.307657	12.123.40.210	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
20	6.308745	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22019/854, ttl=7 (no response found!)
21	6.334320	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
22	6.338804	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22275/855, ttl=8 (no response found!)
23	6.358888	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22531/856, ttl=9 (no response found!)
24	6.358501	12.122.12.54	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
27	6.382957	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
28	6.388921	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22787/857, ttl=10 (no response found!)
29	6.408895	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=23043/858, ttl=11 (no response found!)

Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0	0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00	% s...p...E
Ethernet II, Src: ActiontecLea_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)	0010 00 54 32 d0 00 00 01 20 2c c0 a0 01 66 80 3b	T2...p...f;
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100	0020 17 64 08 00 f7 ca 03 00 50 03 37 32 20 aa aa aa	d...P.72...
0100 = Version: 4	0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0101 = Header Length: 20 bytes (5)	0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
Total length: 84	0060 aa aa
Identification: 0x32d0 (13008)		
0000 = Flags: 0x0		
0000 0000 0000 = Fragment Offset: 0		
Time to Live: 1		
Protocol: ICMP (1)		
Header checksum: 0x2d2c [validation disabled]		
[Header checksum status: Unverified]		
Source Address: 192.168.1.102		
Destination Address: 128.59.23.100		
Internet Control Message Protocol		

As of now this ip datagram hasn't been fragmented as the more fragments bit in the flag is not set.

Next, sort the traced packets according to IP source address by clicking on the Source column header; a small downward pointing arrow should appear next to the word Source. If the arrow points up, click on the Source column header again. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the details of selected packet header window. In the listing of captured packets window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent by other protocols running on your computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by your computer.

5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

The Identification Number and the header Check sum are always changing from one datagram to the next within the series of ICMP messages.

6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Fields that stay constant:

Version

Length of header

Source IP

Destination IP

Upper layer protocol

Fields that must change:

The header checksum

Identification

7. Describe the pattern you see in the values in the Identification field of the IP datagram

The pattern in the identification field is that the field increases by one in each packet.

Next (with the packets still sorted by source address) find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router.

8. What is the value in the Identification field and the TTL field?

No.	Time	Source	Destination	Protocol	Length	Info
47	11.256578	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
15	6.257672	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
375	54.553282	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
319	49.538344	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
264	44.543862	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
210	39.098928	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
168	34.082998	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
127	29.078887	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
84	16.410867	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
59	11.489686	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
30	6.415141	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
374	54.431198	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
318	49.427542	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
263	44.414483	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
209	39.036379	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
167	34.014412	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
126	29.004477	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
81	16.386561	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
57	11.388011	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
27	6.382957	192.205.32.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 374: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

Ethernet II, Src: LinksysGroup_dar:af:73 (00:06:25:da:af:73), Dst: ActiontecEle_8a:70:1a (00:20:e0:8a:70:1a)

Internet Protocol Version 4, Src: 192.205.32.106, Dst: 192.168.1.102

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 56

Identification: 0x0000 (0)

0000 = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 246

Protocol: ICMP (1)

Header Checksum: 0x217f [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.205.32.106

Destination Address: 192.168.1.102

Internet Control Message Protocol

The TTL field value is 246 and the Identification field value is 0X0000(0).

II. Fragmentation

Sort the packet listing according to time again by clicking on the Time column.

9. Find the first ICMP Echo Request message that was sent by your computer. Has that message been fragmented across more than one IP datagram?

No.	Time	Source	Destination	Protocol	Length	Info
8	6.163845	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found)
11	6.202257	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=2 (no response found)
13	6.234585	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found)
15	6.257672	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
16	6.257520	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found)
17	6.266017	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
18	6.288750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found)
19	6.307657	12.123.40.218	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
20	6.307745	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22019/854, ttl=7 (no response found)
21	6.314370	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
22	6.338804	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22275/855, ttl=8 (no response found)
23	6.358888	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22531/856, ttl=9 (no response found)
24	6.365591	12.122.12.54	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
25	6.382957	192.208.31.106	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
26	6.389321	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=22787/857, ttl=10 (no response found)
29	6.408895	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=23043/858, ttl=11 (no response found)

Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
 Ethernet II, Src: ActiontecE1c:8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysGroup da:af:73 (00:06:25:da:af:73)
 Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
 ICMP 98 bytes
 0101 = Header Length: 20 bytes (5)
 0101 = Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 98
 Identification: 0x3240 (13008)
 0000 = Flags: 0x0
 0000 = Reserved bit: Not set
 0000 = Don't fragment: Not set
 0000 = More fragments: Not set
 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 1
 Protocol: ICMP (1)
 Header Checksum: 0x2dc (validation disabled)
 [Header checksum status: Unverified]
 Source Address: 192.168.1.102
 Destination Address: 128.59.23.100
 Internet Control Message Protocol

No The packet hasn't been fragmented because the more fragments bit is not set and fragment number is 0.

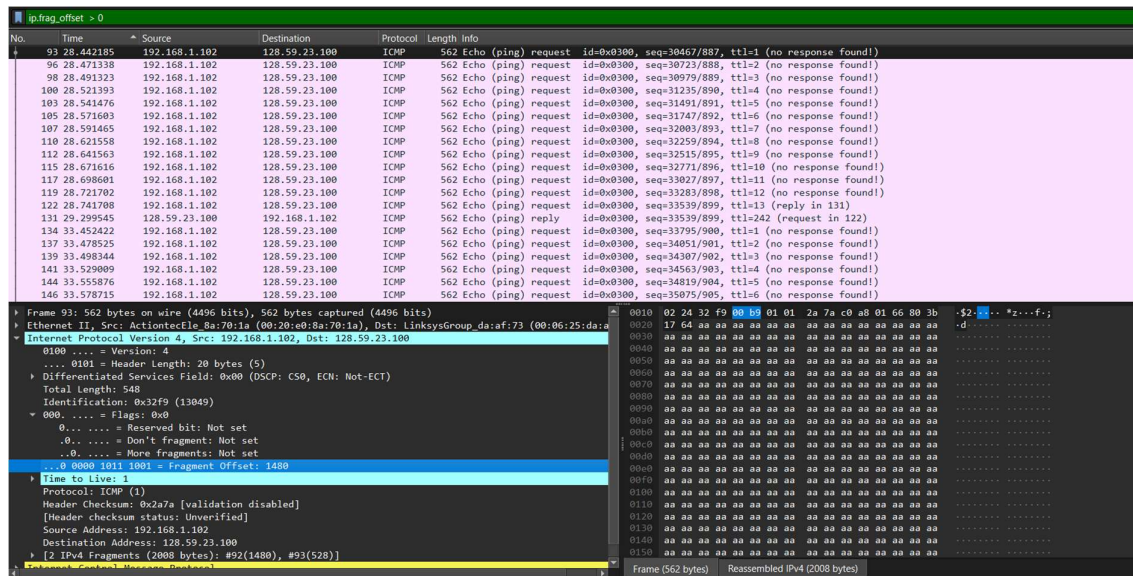
10. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

No.	Time	Source	Destination	Protocol	Length	Info
92	28.441511	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto:ICMP 1, offset: 0, ID=32fa) [Reassembled in #93]
94	28.462164	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	28.478668	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto:ICMP 1, offset: 0, ID=32fa) [Reassembled in #96]
97	28.498663	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto:ICMP 1, offset: 0, ID=32fb) [Reassembled in #98]
99	28.528729	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto:ICMP 1, offset: 0, ID=32fc) [Reassembled in #100]
101	28.538219	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
102	28.548742	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto:ICMP 1, offset: 0, ID=32fd) [Reassembled in #103]
104	28.578848	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto:ICMP 1, offset: 0, ID=32fe) [Reassembled in #105]
106	28.598801	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto:ICMP 1, offset: 0, ID=32ff) [Reassembled in #107]
108	28.597502	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
109	28.628895	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto:ICMP 1, offset: 0, ID=3300) [Reassembled in #110]
111	28.648895	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto:ICMP 1, offset: 0, ID=3301) [Reassembled in #112]
113	28.667160	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
114	28.678921	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto:ICMP 1, offset: 0, ID=3302) [Reassembled in #115]
116	28.697934	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto:ICMP 1, offset: 0, ID=3303) [Reassembled in #117]
118	28.721037	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto:ICMP 1, offset: 0, ID=3304) [Reassembled in #119]
120	28.734675	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
121	28.741043	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto:ICMP 1, offset: 0, ID=3305) [Reassembled in #122]
123	28.804963	12.123.40.218	192.168.1.102	IPv4	554	Fragmented IP protocol (proto:ICMP 1, offset: 0, ID=0000)
124	28.871954	12.122.10.22	192.168.1.102	IPv4	554	Fragmented IP protocol (proto:ICMP 1, offset: 0, ID=0000)

Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
 Ethernet II, Src: ActiontecE1c:8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysGroup da:af:73 (00:06:25:da:af:73)
 Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 0101 = Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 1500
 Identification: 0x32f9 (13049)
 001 = Flags: 0x1, More Fragments
 0000 = Reserved bit: Not set
 0000 = Don't fragment: Not set
 0000 = More fragments: Set
 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 1
 Protocol: ICMP (1)
 Header Checksum: 0x077b (validation disabled)
 [Header checksum status: Unverified]
 Source Address: 192.168.1.102
 Destination Address: 128.59.23.100
 Reassembled IPv4 in frame: 93
 More fragments (ip.flags.mf == 1) 1 byte
 Packets: 380 - Displayed: 200 (52.6%)

The more fragments bit is set so this packet is fragmented. The fragment offset is 0 so this is the first packet of this fragment. The length of this IP datagram is 1514.

11. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?



The fragment offset is not 0. It indicates that this packet is not first fragment. There are no more fragments for this packet because the more fragment bit is not set.

12. What fields change in the IP header between the first and second fragment?

Length

Flags Set

Fragment offset

header checksum

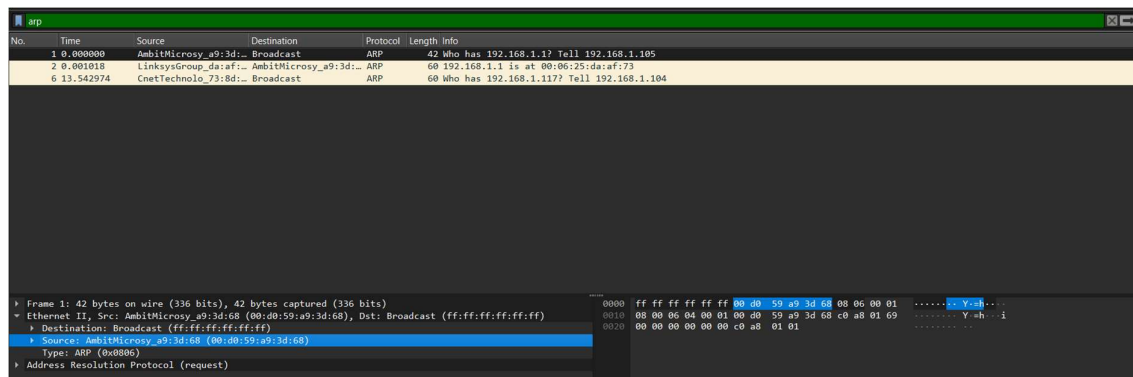
ARP

I. Capturing and analysing Ethernet frames

Note: Answer the following questions using the ethernet-ethereal-trace-1 packet trace to answer the

questions below

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



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? [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 destination address in the Ethernet frame is ff:ff:ff:ff:ff:ff. No this is not the gaii.cs.umass.edu ethernet address. Broadcast MAC address.

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

arp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMicrosy_a9:3d:...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	LinksysGroup_da:af:...	AmbitMicrosy_a9:3d:...	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
6	13.542974	CnetTechnolo_73:8d:...	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)

Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)

Type: ARP (0x0806)

Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01 Y-eh

0010 08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8 01 69 Y-h-i

0020 00 00 00 00 00 c0 a8 01 01

0X0806 is the hexadecimal value and this correspond to ARP.

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

http

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMicrosy_a9:3d:...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	LinksysGroup_da:af:...	AmbitMicrosy_a9:3d:...	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=0 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 MSS=1460 SACK_PERM
5	8.971488	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
6	13.542974	CnetTechnolo_73:8d:...	Broadcast	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 SACK_PERM
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 /etherreal-lab/HTTP-etherreal-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 segment of a reassembled PDU]
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 segment of a reassembled PDU]
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 segment of a reassembled PDU]
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

[Stream index: 1]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 632]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 1695848871

[Next Sequence Number: 633 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 2896510900

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window: 64240

[Calculated window size: 64240]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x7e4f (unverified)

[Checksum Status: Unverified]

Urgent Pointer: 0

[Timestamps]

[SEQ/ACK analysis]

TCP payload (632 bytes)

Hypertext Transfer Protocol

0030 fa 70 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72 ...G GET /ether

0040 65 61 6c 2d 6c 61 62 73 2f 48 54 54 50 2d 65 74 eal-lab/HTTP-et

0050 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33 hereal-lab-file3

0060 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HTTP/1.1

0070 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d Host: gaia.cs.um

0080 61 73 73 2e 65 64 75 0d 0e 55 73 65 72 2d 41 67 ass.edu~User-Ag

0090 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 ent: Mozilla/5.0

00a0 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69 (Window s; U; Wi

00b0 6e 64 6f 77 73 20 4e 54 20 25 2e 31 3b 20 65 6e ndows NT 5.1; en

00c0 2d 55 53 3b 20 72 76 3a 31 2e 30 2e 32 29 20 47 -US; rv:1.0.2) G

00d0 65 63 6b 6f 2f 32 30 30 33 30 32 30 38 20 4e 65 ecko/200.30208

00e0 74 73 63 61 70 65 2f 37 2e 30 32 8d 0a 41 63 63 tscape/7.02~Acc

00f0 65 70 74 3a 20 74 65 78 74 7a 2f 78 6d 6c 2c 61 70 npt: text/xml; ap

0100 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2c 61 70 plication/xml; ap

0110 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2c 61 70 plication/xml

0120 78 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b 71 3d xml;text/html;q=

0130 20 2e 29 2c 74 65 78 74 2f 70 6c 61 69 6e 3b 71 0.5;text/plain;q

0140 3d 30 2e 38 2c 76 69 64 65 6f 2f 78 2d 6d 6e 67 =0.8;vid eo/x-mng

0150 2c 69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 67 65 ,image/png,image

0160 2f 6a 70 65 67 2c 69 6d 61 67 65 2f 67 69 66 3b /jpeg,image/gif;

0170 71 3d 30 2e 32 2c 74 65 78 74 2f 63 73 73 2c 2a =0.2;text/css;+

0180 2f 2a 3b 71 3d 30 2e 31 0d 0a 41 63 63 65 70 74 /*jq=0.1--Accepts

686 – 632 = 54 bytes.

Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

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 Ethernet Source address is 00:d0:59:a9:3d:68.

No.

Ambit Micro Systems.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMicrosy_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	LinksysGroup_da:af:73	AmbitMicrosy_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	192.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
4	2.542530	192.168.1.105	192.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
5	8.521488	192.168.1.105	192.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
6	13.542974	CnetTechnolo_73:8d:12	Broadcast	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 SACK_PERM
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	1059 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /etherreal-labs/HTTP-etherreal-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 segment of a reassembled PDU]
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 segment of a reassembled PDU]
14	17.500069	192.168.1.105	128.119.245.12	TCP	54	1059 → 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 segment of a reassembled PDU]
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	1059 → 80 [ACK] Seq=633 Ack=4816 Win=64240 Len=0

Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)	
Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)	0000 00 06 25 da af 73 00 40 59 a9 3d 68 00 00 45 00
Internet Protocol Version 4, Src: 192.168.1.105, Dst: 128.119.245.12	0010 02 a0 00 fa 40 00 80 06 bf c8 c0 a8 01 69 80 77
Transmission Control Protocol, Src Port: 1058, Dst Port: 80, Seq: 1, Ack: 1, Len: 632	0020 f5 0c 04 22 00 50 65 14 99 a7 ac a5 3f b4 50 18
Hypertext Transfer Protocol	0030 fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72
	0040 65 61 6c 2d 6c 61 62 73 2f 48 54 54 50 2d 65 7a
	0050 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33
	0060 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a
	0070 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d
	0080 61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67
	0090 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2a 30
	00a0 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69
	00b0 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 65 6e
	00c0 2d 55 53 3b 20 72 76 3a 31 2e 30 2e 32 29 20 47
	00d0 65 63 6b 6f 2f 32 30 30 33 30 32 30 38 20 4e 65
	00e0 74 73 63 61 70 65 2f 37 2e 30 32 0d 0a 41 63 63
	00f0 65 70 74 3a 20 74 65 78 74 2f 78 6d 6c 2e 61 70
	0100 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2e 61 70
	0110 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2e 61 70
	0120 78 6d 6c 2e 74 65 78 74 2f 68 74 6d 6c 3b 71 3d
	0130 3b 2e 39 2c 74 65 78 74 2f 70 6c 61 69 6e 3b 71
	0140 3d 3b 2e 30 2c 76 69 64 65 6f 2f 78 2d 6d 6e 67
	0150 2c 69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 67 65

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

00:06:25:da:af:73.

NO

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

0X0800

IPV4.

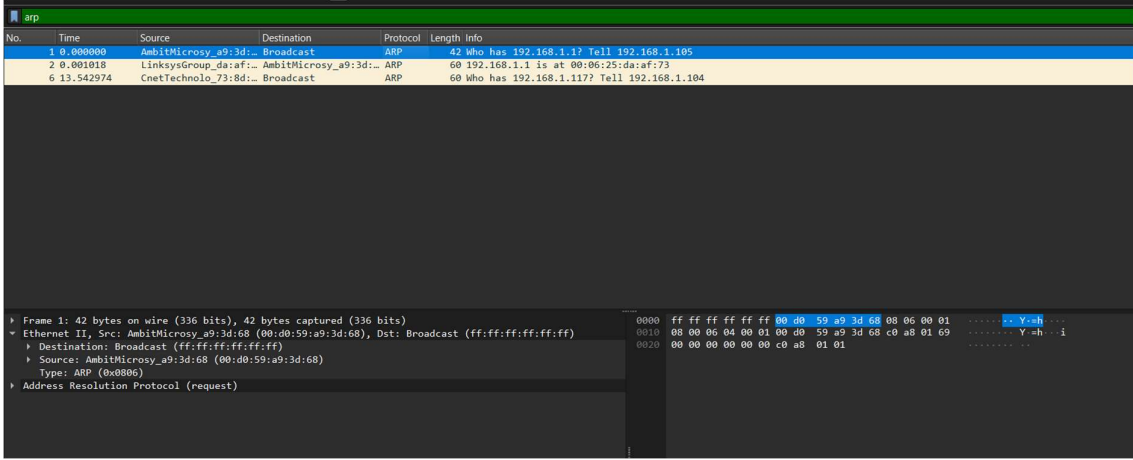
Type: The type of ARP entry. dynamic means the entry was learned dynamically through ARP requests. static means it was manually configured and will not change

```
C:\Users\91934>arp -a

Interface: 192.168.56.1 --- 0xf
Internet Address      Physical Address      Type
192.168.56.255        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

Interface: 172.29.45.68 --- 0x14
Internet Address      Physical Address      Type
172.29.32.1           00-1b-90-95-b0-00    dynamic
172.29.63.255         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
```

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



The screenshot shows a Wireshark packet capture of an ARP request. The packet list at the top shows three packets: a broadcast (packet 1), a request (packet 2), and a reply (packet 3). The packet details for the request (packet 2) are expanded, showing the Ethernet II header with source address 00:d0:59:a9:3d:68 and destination address ff:ff:ff:ff:ff:ff. The ARP section shows it is a request for 192.168.1.1.

Source : 00:d0:59:a9:3d:68.

Destination : 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?

0X0806. This Corresponds to ARP.

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>.

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

20 bytes.

6 for each source address and destination address and 2 for protocol type and 6 for arp header.

A total of 20 bytes.

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 opcode request is 1.

arp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMicrosy_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	LinksysGroup_da:af:1	AmbitMicrosy_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
6	13.542974	CnetTechnolo_73:8d:1	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)

Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
- Type: ARP (0x0806)

Address Resolution Protocol (request)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
- Sender IP address: 192.168.1.105
- Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Target IP address: 192.168.1.1

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

Yes it contains 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?

arp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMicrosy_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	LinksysGroup_da:af:1	AmbitMicrosy_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
6	13.542974	CnetTechnolo_73:8d:1	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)

Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
- Type: ARP (0x0806)

Address Resolution Protocol (request)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
- Sender IP address: 192.168.1.105
- Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Target IP address: 192.168.1.1

In the ARP section you can see the details about the query that has been asked.

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

6 for each source address and destination address and 2 for protocol type and 6 for arp header.

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 image shows a Wireshark packet capture of an ARP request. The packet list on the left shows three packets: a broadcast ARP request from AmbitMicrosy_a9:3d:.., a broadcast ARP request from CnetTechnolo_73:8d:.., and the selected packet, an ARP request from LinksysGroup_da:af:73 to AmbitMicrosy_a9:3d:...

The packet details pane for the selected packet (Frame 2) shows the following structure:

- Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
 - Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
 - Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
 - Type: ARP (0x0800)
 - Padding: 00
- Address Resolution Protocol (reply)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: reply (2)
 - Sender MAC address: LinksysGroup_da:af:73 (00:06:25:da:af:73)
 - Sender IP address: 192.168.1.1
 - Target MAC address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
 - Target IP address: 192.168.1.105

The packet bytes pane shows the raw data of the packet, with a hex dump and ASCII representation. The ARP request structure is visible in the hex dump, including the Ethernet II header, ARP header, and padding.

The answer appears on Sender MAC address field.

Destination address: 00:30:59:a9:3d:68

arp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMicrosy_a9:3d:...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
6	13.542974	CnetTechnolo_73:8d:...	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
2	0.001018	LinksysGroup_da:af:...	AmbitMicrosy_a9:3d:...	ARP	60	192.168.1.1 is at 00:06:25:da:af:73

Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)

Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)

Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)

Type: ARP (0x0806)

Padding: 00000000000000000000000000000000

Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

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

Sender IP address: 192.168.1.1

Target MAC address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)

Target IP address: 192.168.1.105

```

0000  00 d0 59 a9 3d 68 00 06 25 da af 73 08 06 00 01  --Y=h...s...
0010  00 00 06 04 00 02 00 06 25 da af 73 c0 a8 01 01  ...[...s...
0020  00 d0 59 a9 3d 68 c0 a8 01 69 00 00 00 00 00 00  --Y=h...i....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....

```

15. 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 ARPRequested 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?

The ARP request might be targeting an IP address that does not exist on the local network. If no device is using the IP address in question, no ARP reply will be generated