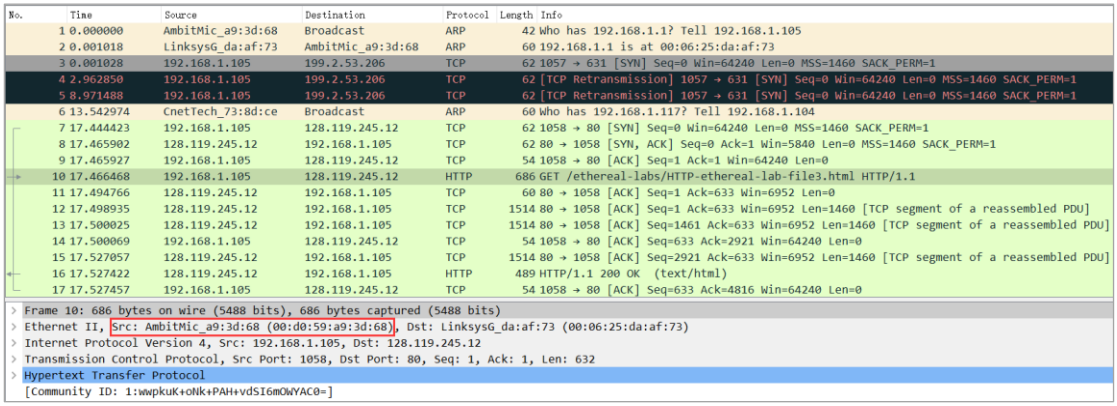
Wireshark Lab 5 - Ethernet and ARP
Xiaoying Li

NOTE: I used the downloaded trace ethernet--ethereal-trace-1 to answer all the questions.

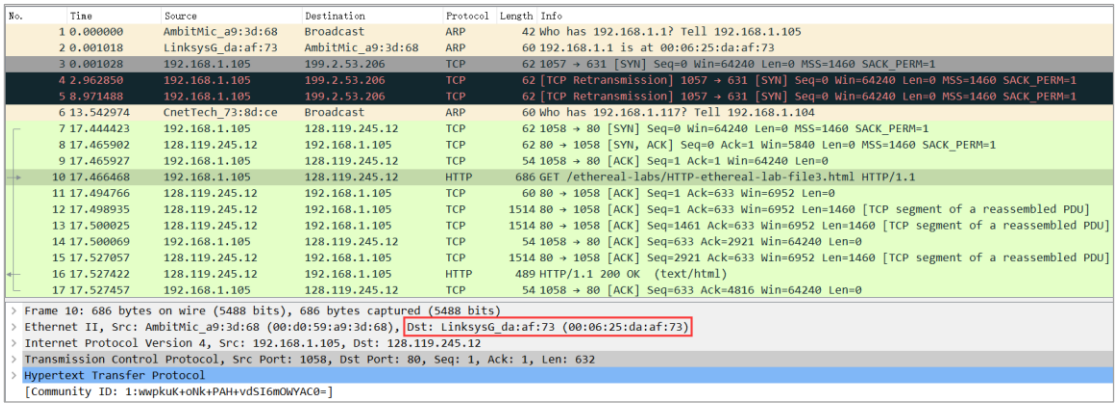
1. What is the 48-bit Ethernet address of your computer?

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



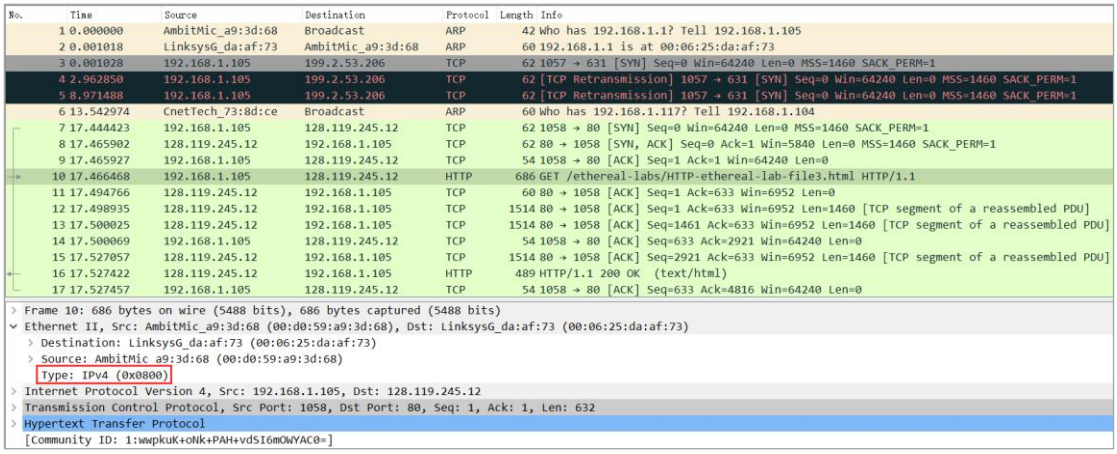
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address?

The 48-bit destination address in the Ethernet frame: 00:06:25:da:af:73
This is not the Ethernet address of gaia.cs.umass.edu.
This is the Ethernet address of the Linksys router.



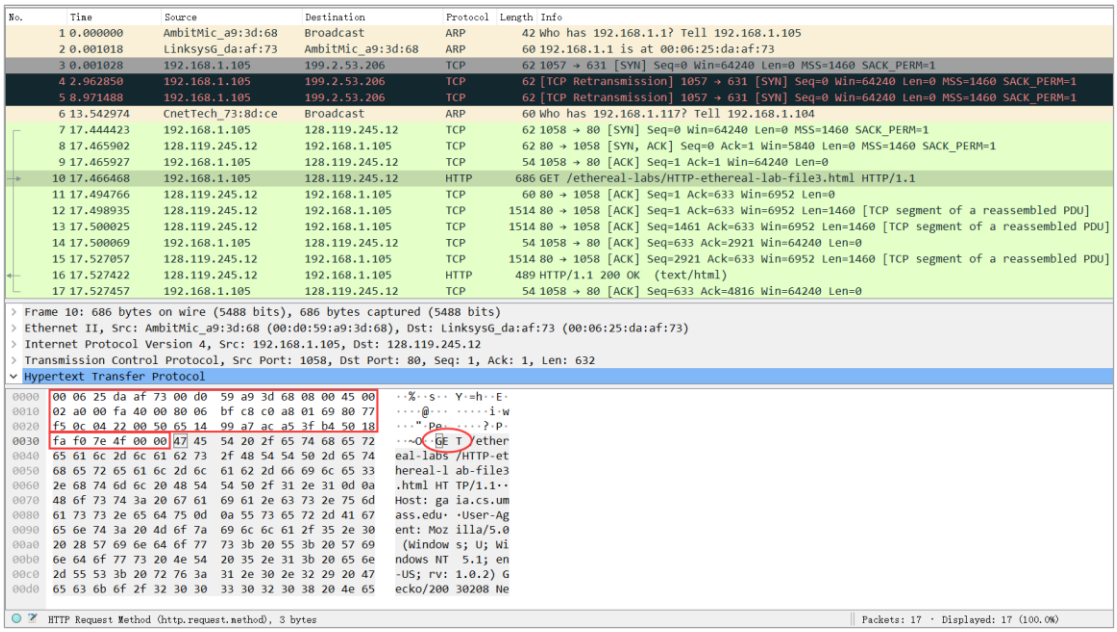
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

The hexadecimal value for the two-byte Frame type field: 0×0800
Upper layer protocol corresponding to: IPv4



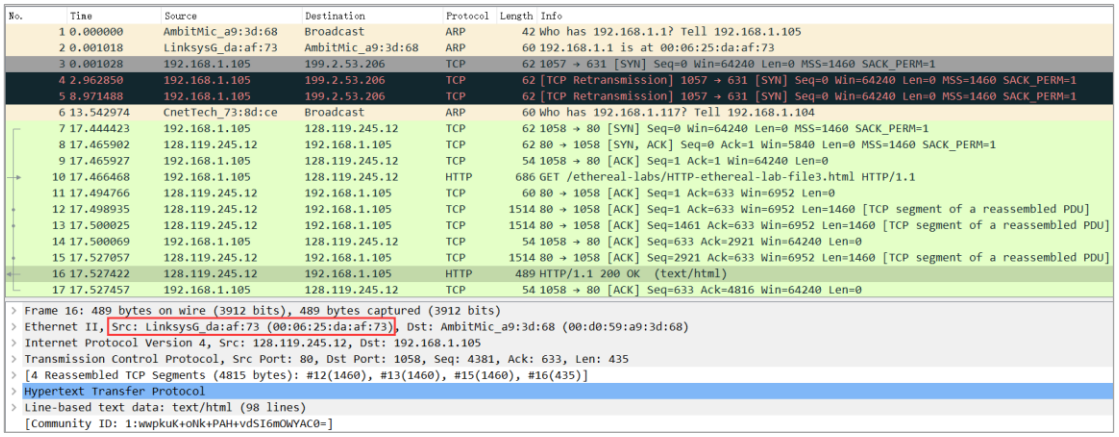
4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

The ASCII “G” in “GET” appear in the Ethernet frame after 54 bytes from the very start of the Ethernet frame.
(Bytes from the very start of the Ethernet frame to the ASCII “G” in “GET” appears in the Ethernet frame are highlighted in the screenshot below.)



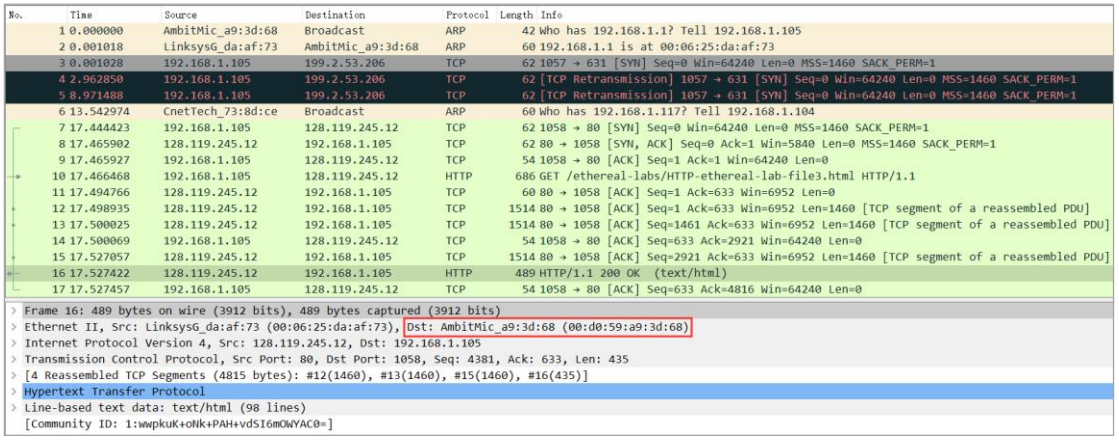
5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address?

The value of the Ethernet source address: 00:06:25:da:af:73
This is not the address of the computer, or of gaia.cs.umass.edu.
This is the Ethernet address of the Linksys router.



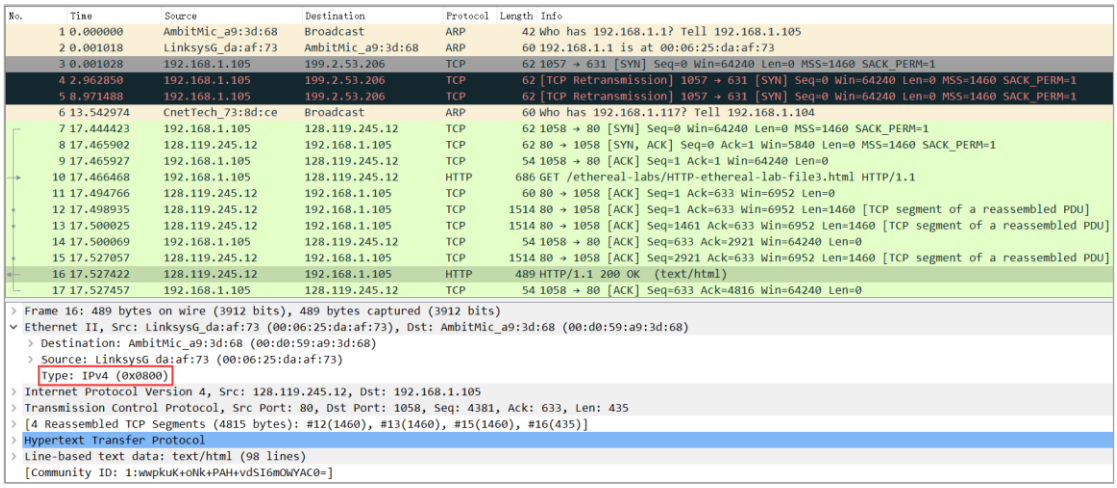
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

The destination address in the Ethernet frame: 00:d0:59:a9:3d:68
This is the Ethernet address of the computer.



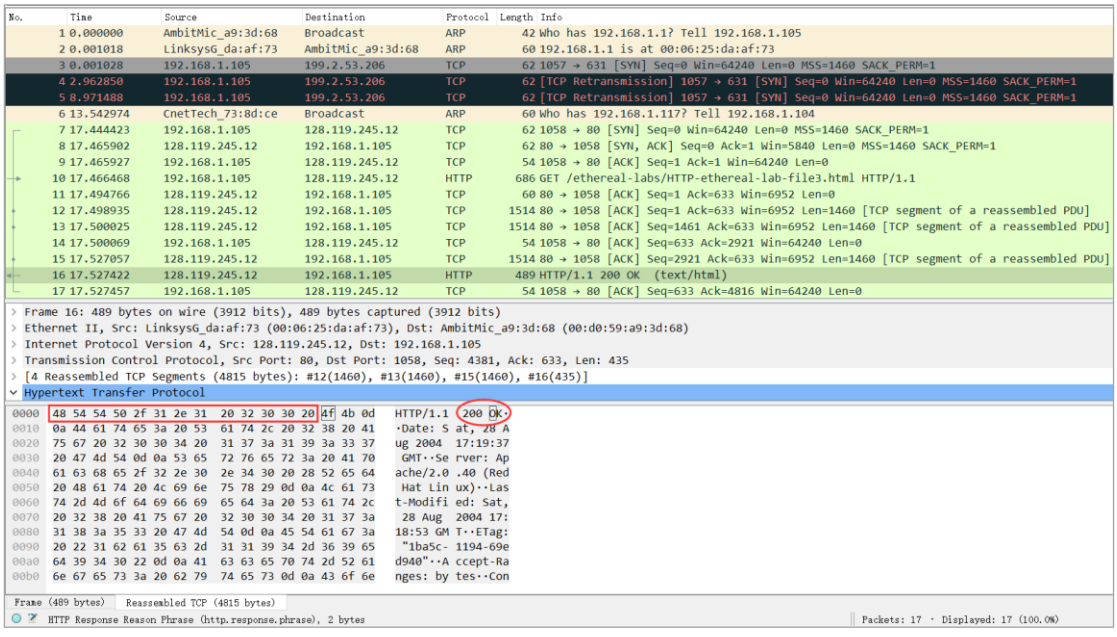
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

The hexadecimal value for the two-byte Frame type field: 0×0800
Upper layer protocol corresponding to: IPv4



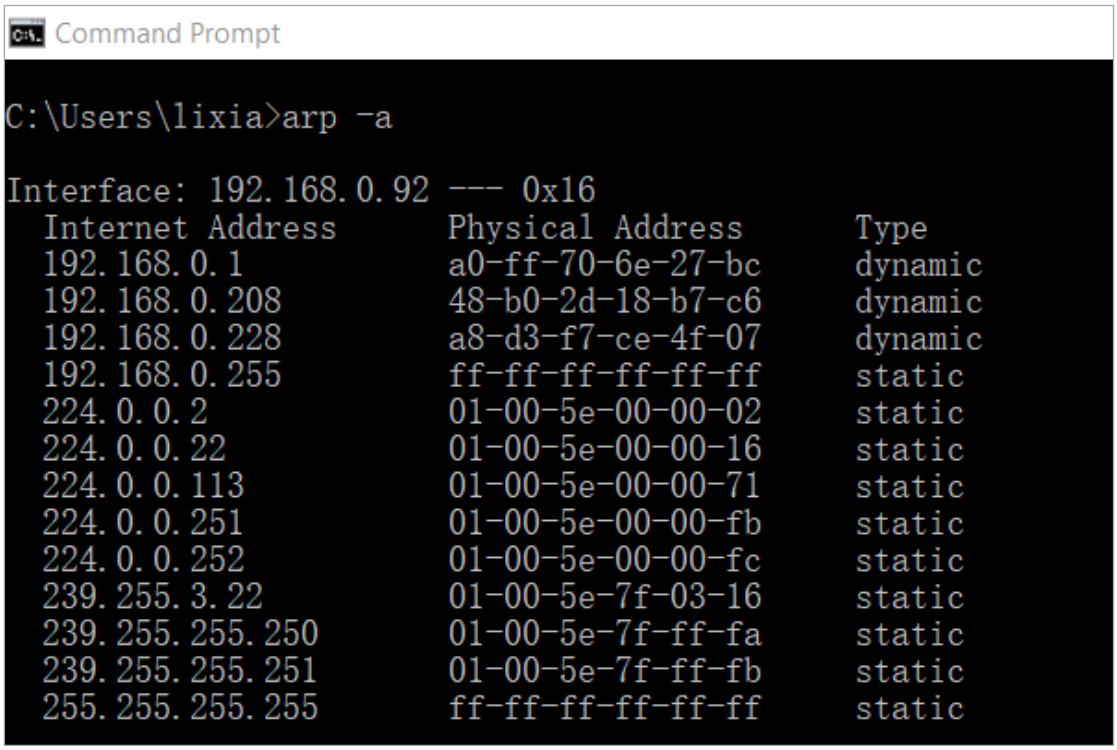
8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?

The ASCII “O” in “OK” appear in the Ethernet frame after 13 bytes from the very start of the Ethernet frame.
(Bytes from the very start of the Ethernet frame to the ASCII “O” in “OK” appears in the Ethernet frame are highlighted in the screenshot below.)



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

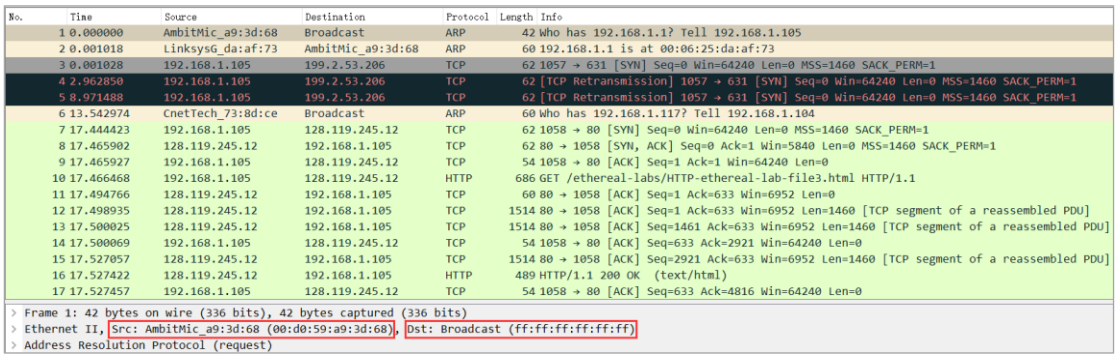
Internet Address: IP address
Physical Address: MAC address
Type: Protocol type



NOTE: The above screenshot shows the contents of the ARP cache on my own computer.

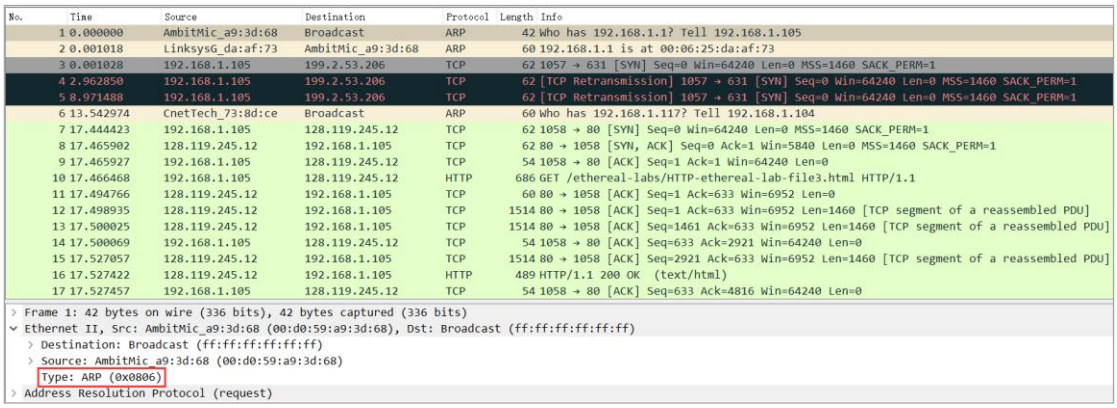
10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

The hexadecimal values for the source address: 00:d0:59:a9:3d:68
The hexadecimal values for the destination addresses: ff:ff:ff:ff:ff:ff



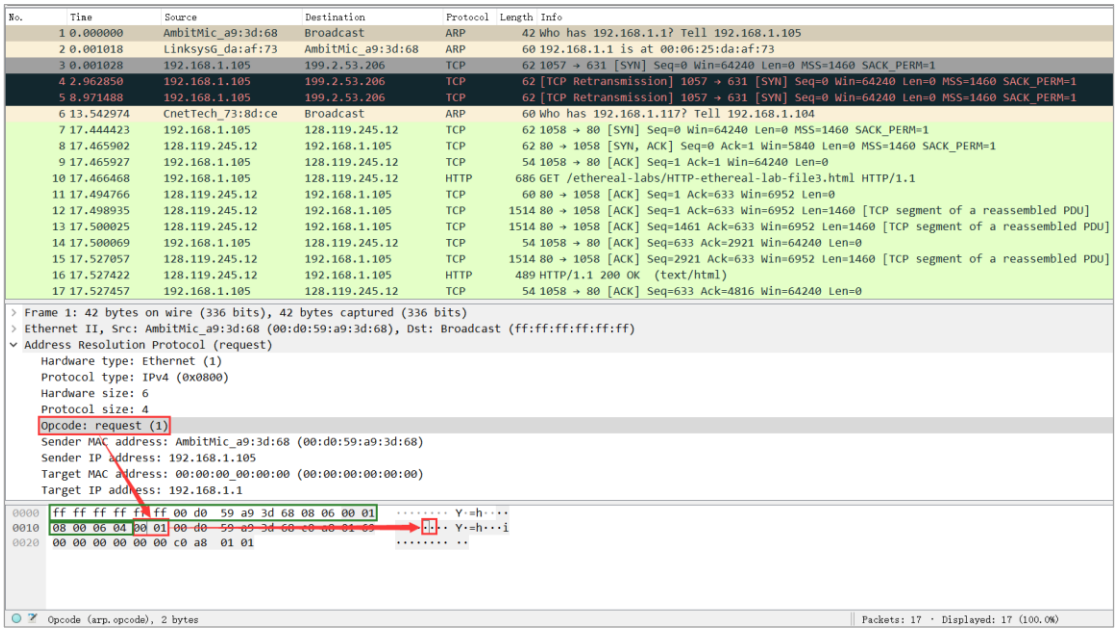
11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

The hexadecimal value for the two-byte Ethernet Frame type field: 0×0806
Upper layer protocol corresponding to: ARP



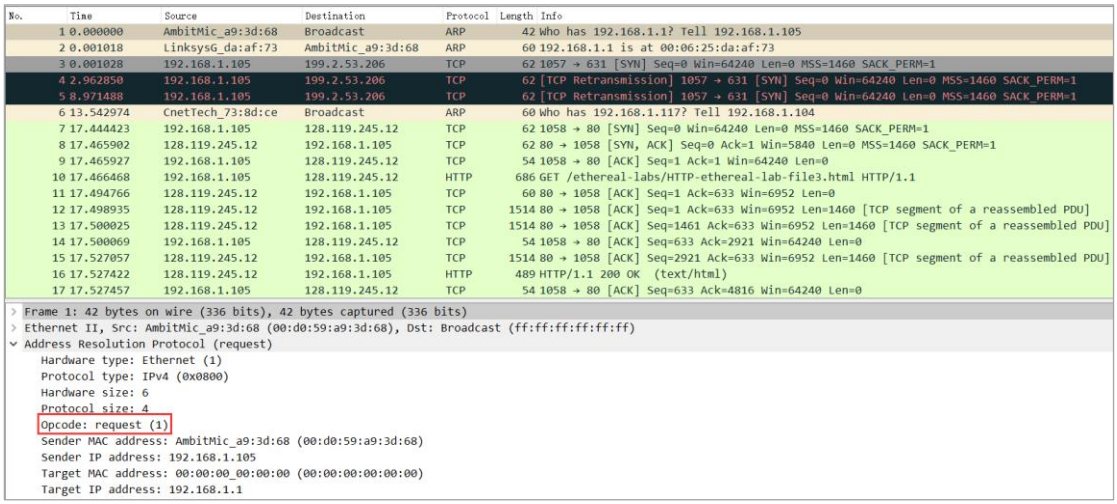
12. a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame. (The ARP opcode field are highlighted in red, and bytes from the very beginning of the Ethernet frame and before the ARP opcode field are highlighted in green in the screenshot below.)



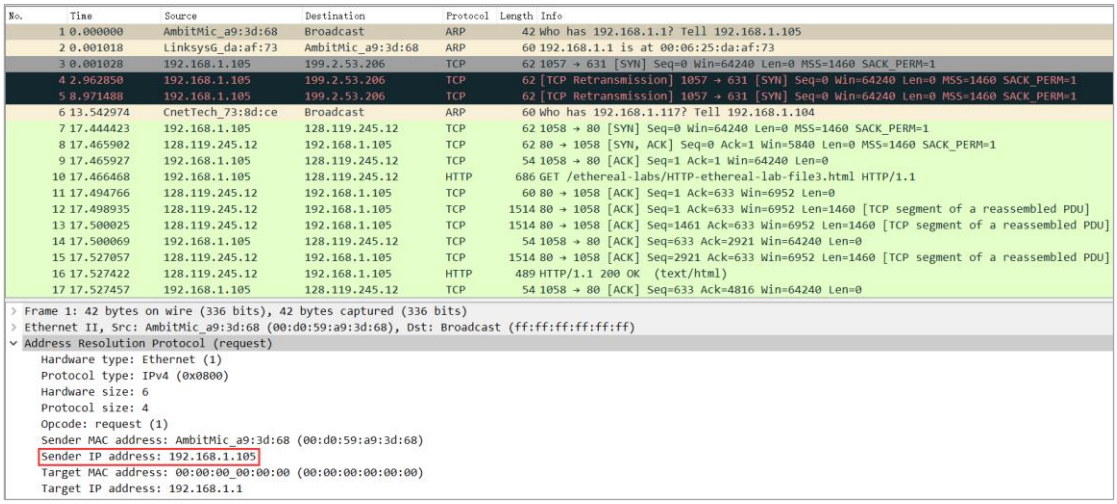
12. b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

The value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made: 1



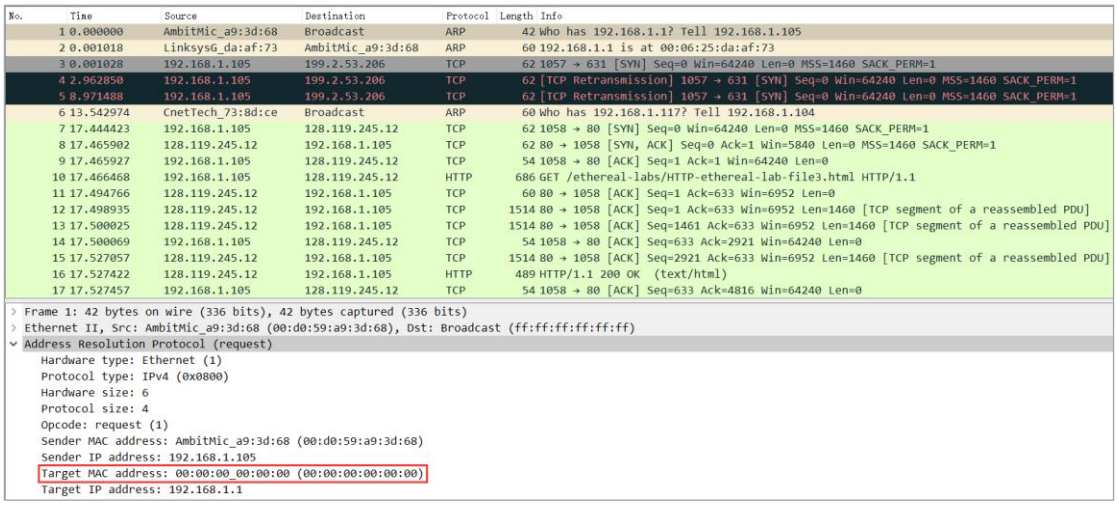
12. c) Does the ARP message contain the IP address of the sender?

Yes. The IP address of the sender is 192.168.1.105.



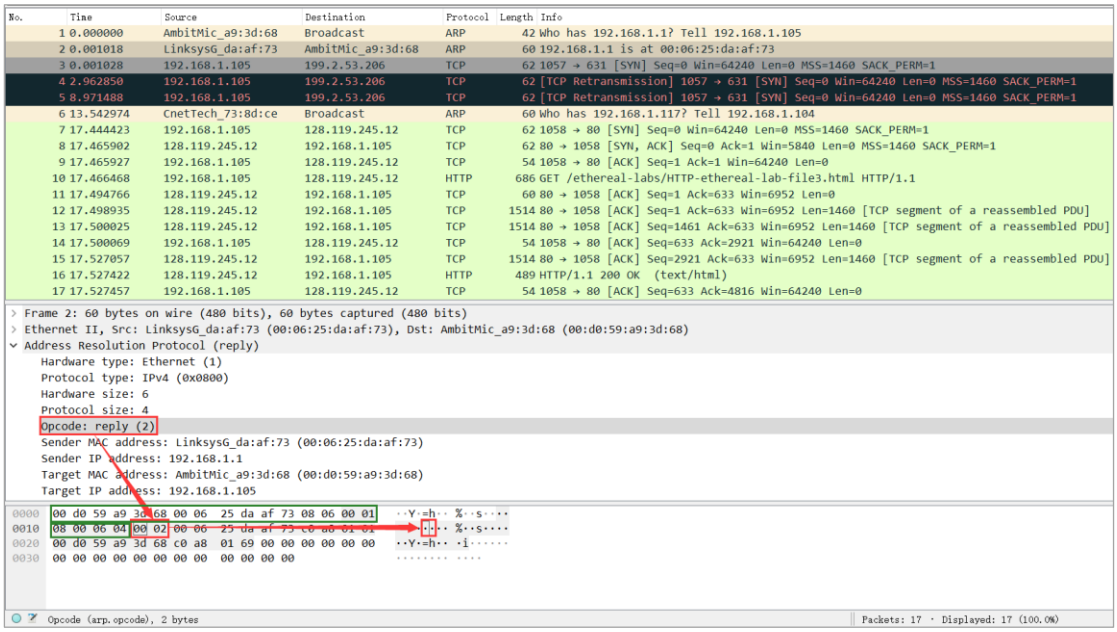
12. d) Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?

The field "Target MAC address" in the ARP request shows the "question".



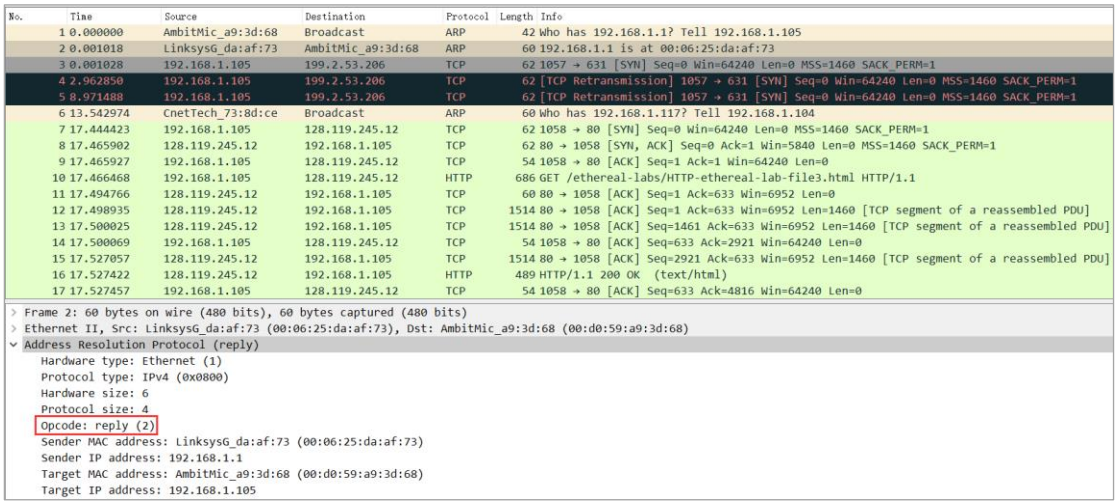
13. a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame. (The ARP opcode field are highlighted in red, and bytes from the very beginning of the Ethernet frame and before the ARP opcode field are highlighted in green in the screenshot below.)



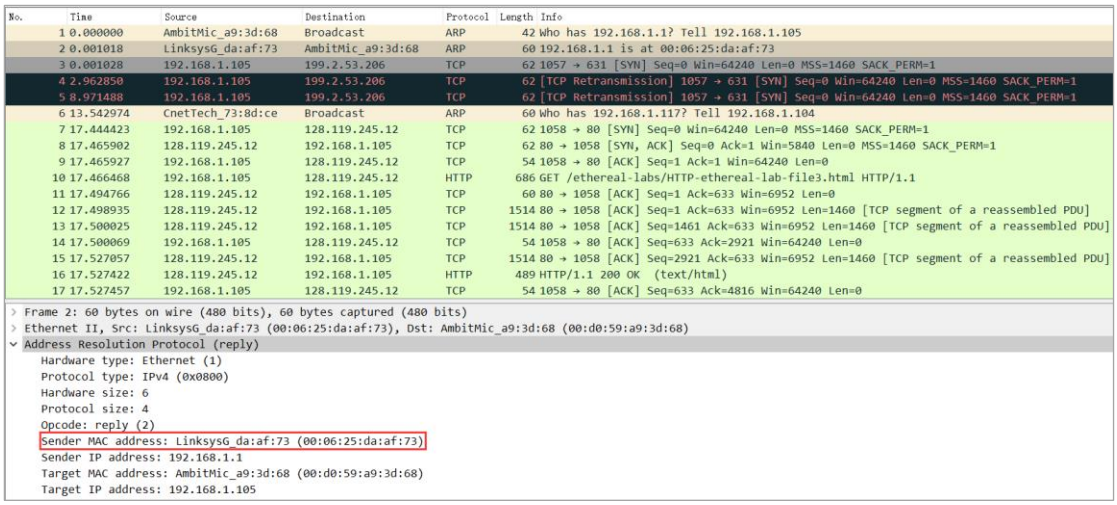
13. b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

The value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made: 2



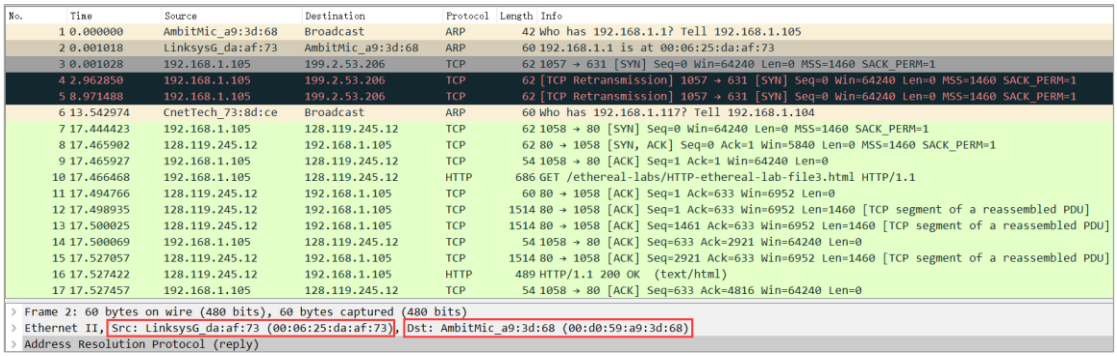
13. c) Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

The field "Sender MAC address" in the ARP message shows the "answer" to the earlier ARP request.



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

The hexadecimal values for the source address: 00:06:25:da:af:73
The hexadecimal values for the destination addresses: 00:d0:59:a9:3d:68

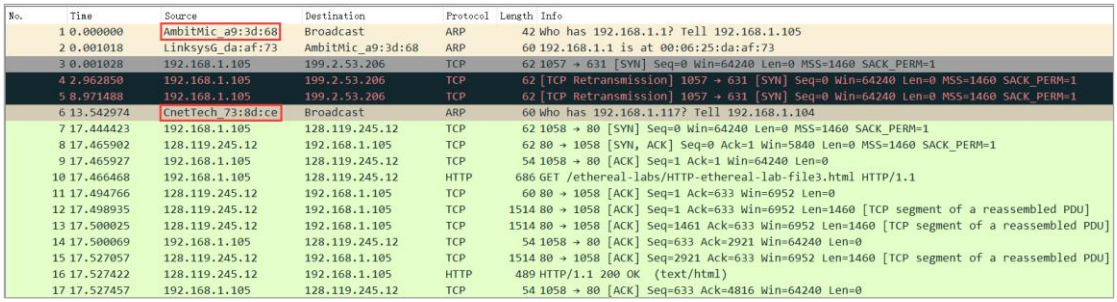


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=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	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=1
6	13.542974	CnetTech_73:8d:ce	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=1
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=1
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 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

> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
> Address Resolution Protocol (reply)

15. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

Because the ARP request in packet 6 is not sent from the computer we are on. The ARP reply only sends back to the computer sends that request.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	LinksysG_da:af:73	AmbitMic_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=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	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=1
6	13.542974	CnetTech_73:8d:ce	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=1
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=1
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 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