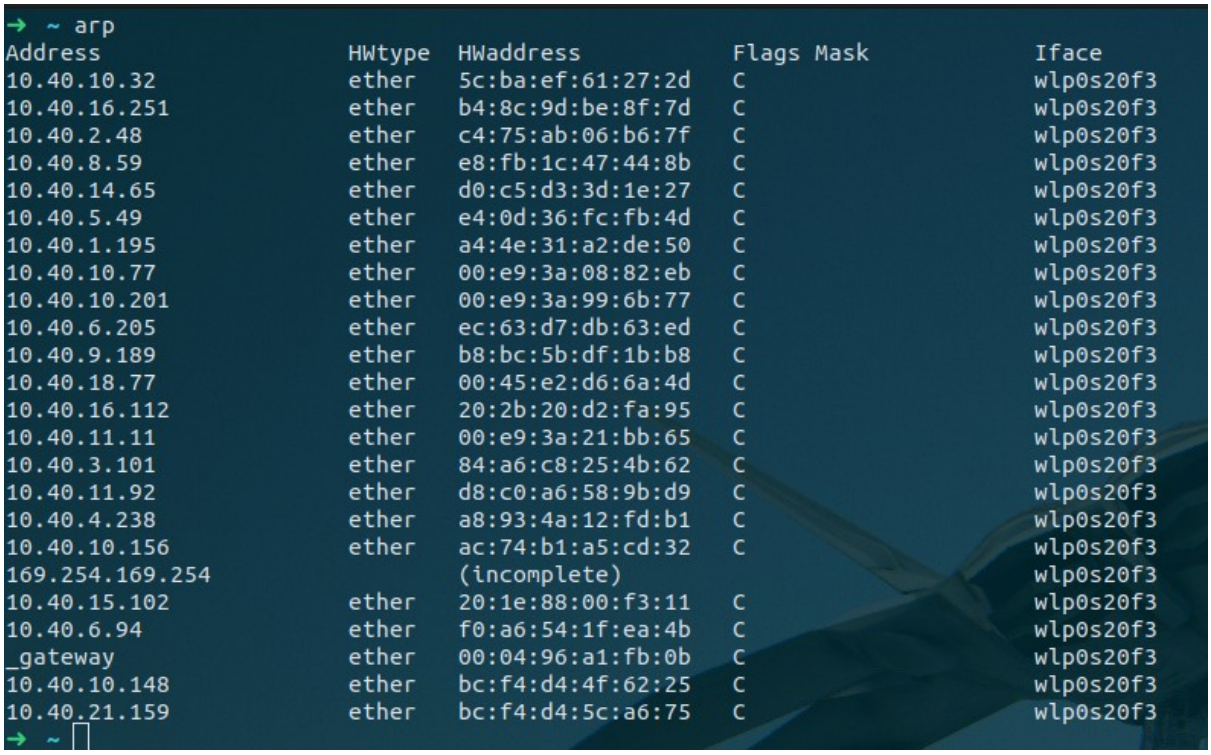
Assignment 6

Name – Harshavardhan Bamane

PRN – 22510112

S7



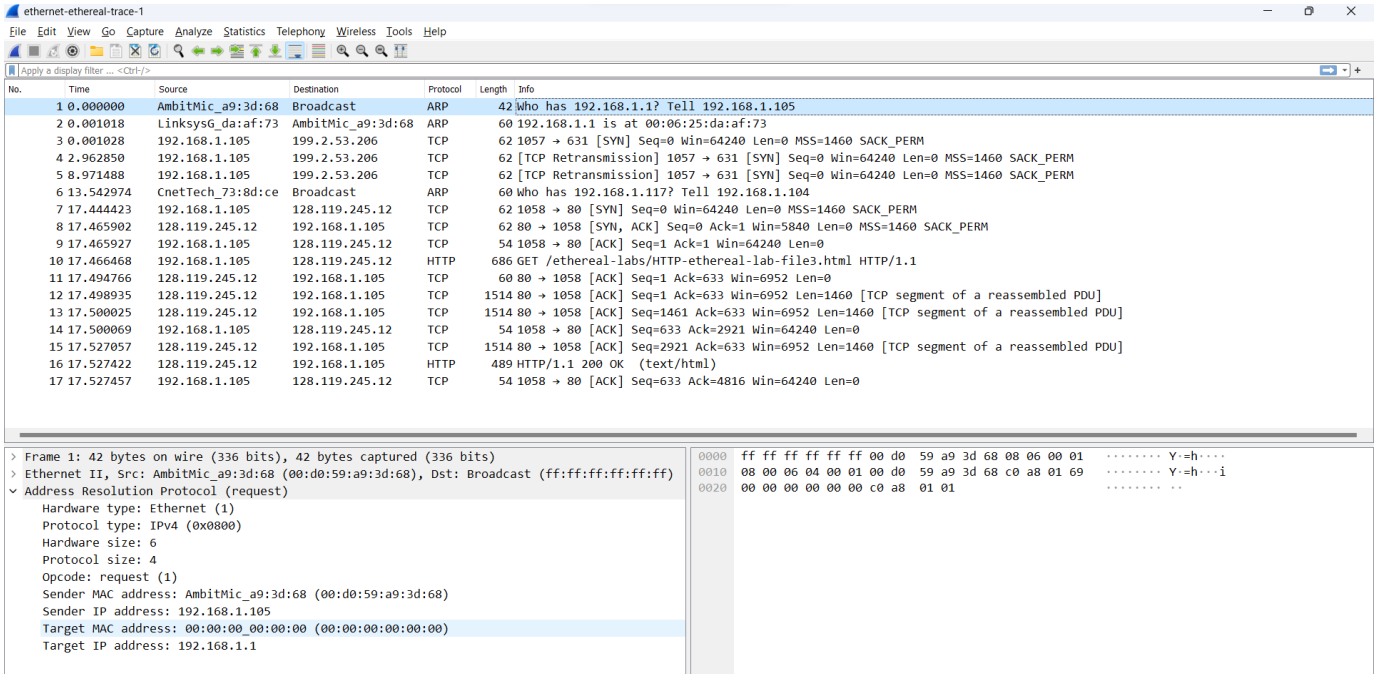
```
➜  ~ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.40.10.32              ether   5c:ba:ef:61:27:2d   C                     wlp0s20f3
10.40.16.251             ether   b4:8c:9d:be:8f:7d   C                     wlp0s20f3
10.40.2.48               ether   c4:75:ab:06:b6:7f   C                     wlp0s20f3
10.40.8.59               ether   e8:fb:1c:47:44:8b   C                     wlp0s20f3
10.40.14.65              ether   d0:c5:d3:3d:1e:27   C                     wlp0s20f3
10.40.5.49               ether   e4:0d:36:fc:fb:4d   C                     wlp0s20f3
10.40.1.195              ether   a4:4e:31:a2:de:50   C                     wlp0s20f3
10.40.10.77              ether   00:e9:3a:08:82:eb   C                     wlp0s20f3
10.40.10.201             ether   00:e9:3a:99:6b:77   C                     wlp0s20f3
10.40.6.205              ether   ec:63:d7:db:63:ed   C                     wlp0s20f3
10.40.9.189              ether   b8:bc:5b:df:1b:b8   C                     wlp0s20f3
10.40.18.77              ether   00:45:e2:d6:6a:4d   C                     wlp0s20f3
10.40.16.112             ether   20:2b:20:d2:fa:95   C                     wlp0s20f3
10.40.11.11              ether   00:e9:3a:21:bb:65   C                     wlp0s20f3
10.40.3.101              ether   84:a6:c8:25:4b:62   C                     wlp0s20f3
10.40.11.92              ether   d8:c0:a6:58:9b:d9   C                     wlp0s20f3
10.40.4.238              ether   a8:93:4a:12:fd:b1   C                     wlp0s20f3
10.40.10.156             ether   ac:74:b1:a5:cd:32   C                     wlp0s20f3
169.254.169.254                  (incomplete)                              wlp0s20f3
10.40.15.102             ether   20:1e:88:00:f3:11   C                     wlp0s20f3
10.40.6.94               ether   f0:a6:54:1f:ea:4b   C                     wlp0s20f3
_gateway                 ether   00:04:96:a1:fb:0b   C                     wlp0s20f3
10.40.10.148             ether   bc:f4:d4:4f:62:25   C                     wlp0s20f3
10.40.21.159             ether   bc:f4:d4:5c:a6:75   C                     wlp0s20f3
➜  ~
```

Internet address are ip addresses

Physical address are MAC / Ethernet addresses

Type column shows that ip address is static or dynamic.

1.



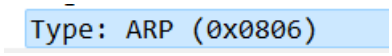
2.What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

ANS: Source MAC address: 00:d0:59:a9:3d:68

Destination MAC address: ff:ff:ff:ff:ff:ff

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

ANS: Type: ARP (0x0806)

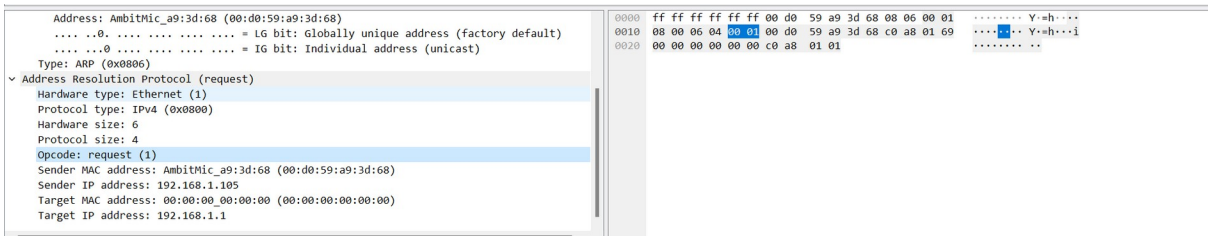


ARP protocol correspond to this upper layer protocol.

4.

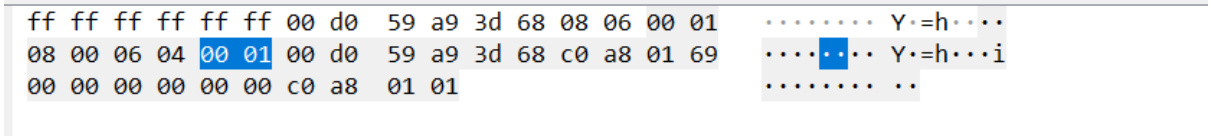
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

Ans: 20 bytes



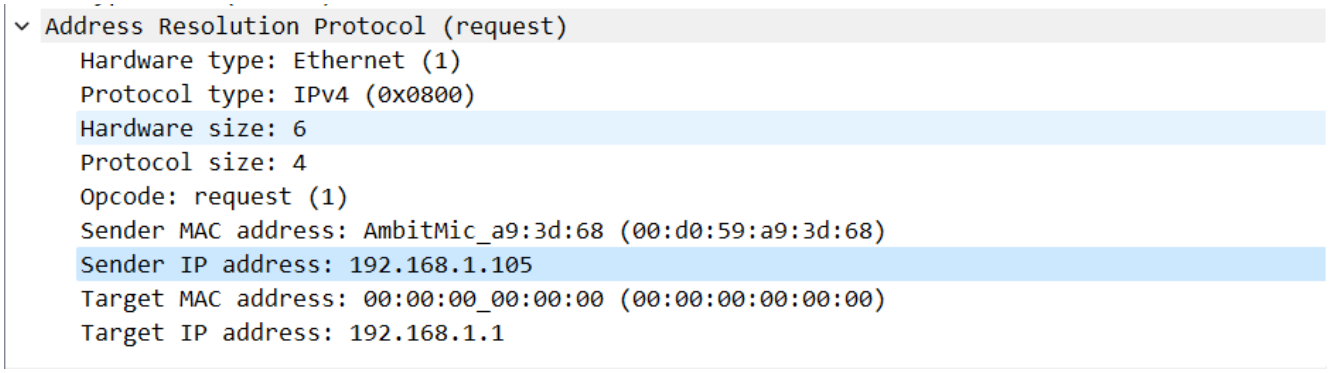
b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

Ans: value of a opcode field : 00 01



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

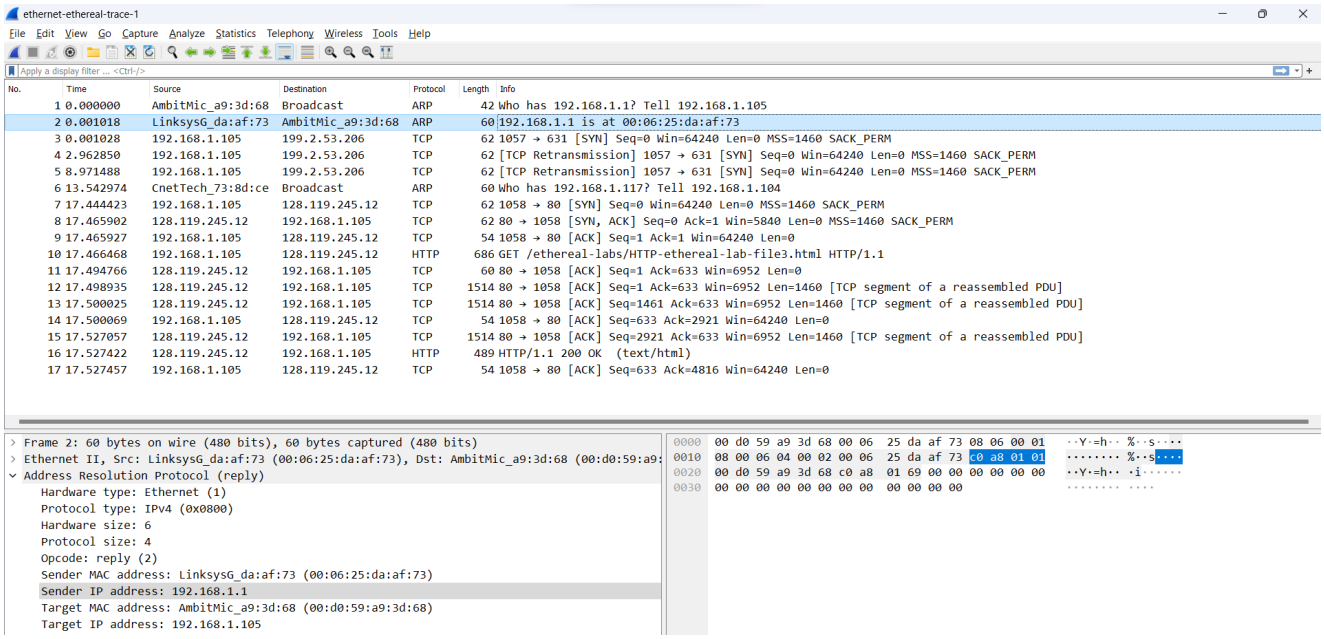
Ans: Yes, ARP message contain the IP address of the sender.



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

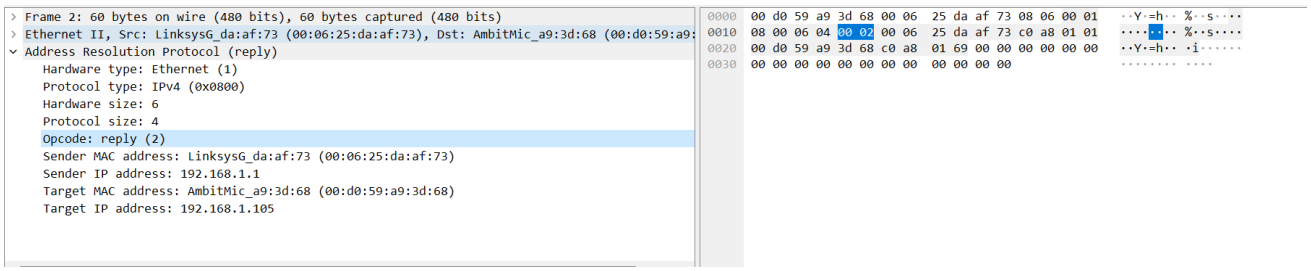
Ans: The field “Target MAC address” is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.1.1) is being queried.

5. Now find the ARP reply that was sent in response to the ARP request.



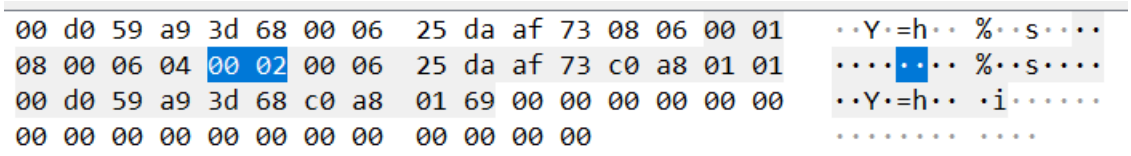
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

Ans: 20 bytes.



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?

Ans: opcode field = 00 02



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?

Ans: The answer to the earlier ARP request appears in the Sender MAC address field, which contains the Ethernet address 00:06:25:da:af:73 for the sender with IP address 192.168.1.1.

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105
```

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

Ans: The hex value for the source address is 00:06:25:da:af:73 and for the destination is 00:d0:59:a9:3d:68 .

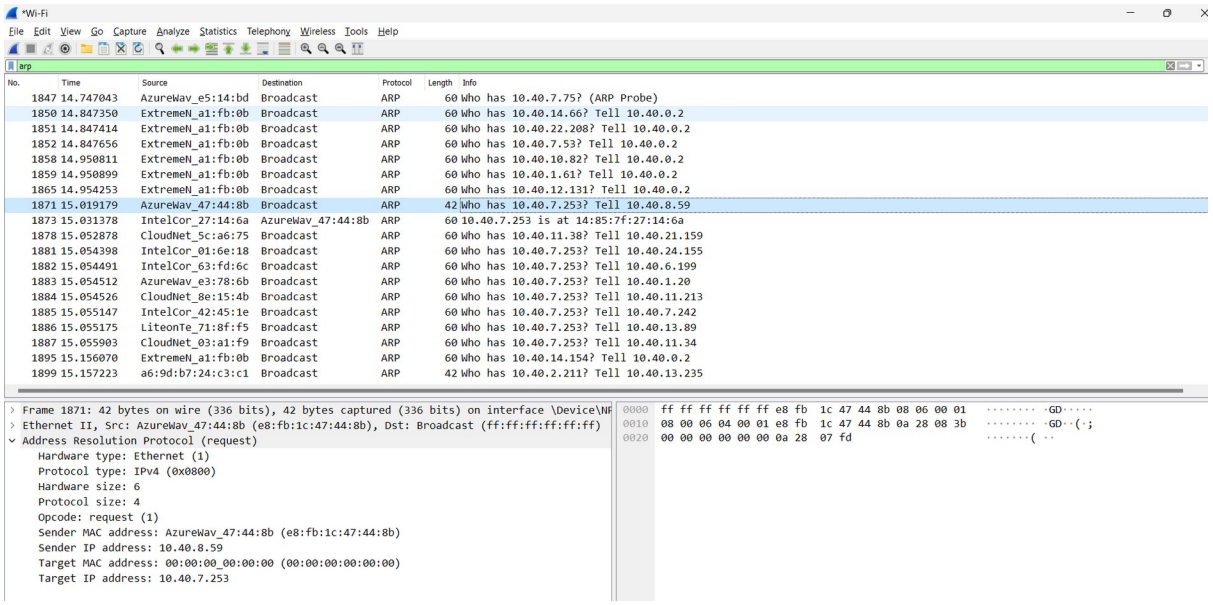
```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105
```

7. 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?

Ans: The ARP request is broadcast, but the ARP reply is sent back directly to the sender’s Ethernet address.

Captured packet.



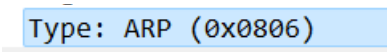
2.What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

ANS: Source MAC address: e8:fb:1c:47:44:8b

Destination MAC address: 00:00:00:00:00:00

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

ANS: Type: ARP (0x0806)

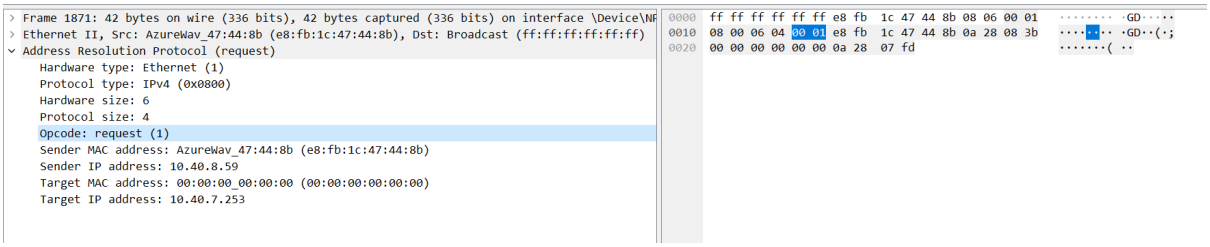


ARP protocol correspond to this upper layer protocol.

4.

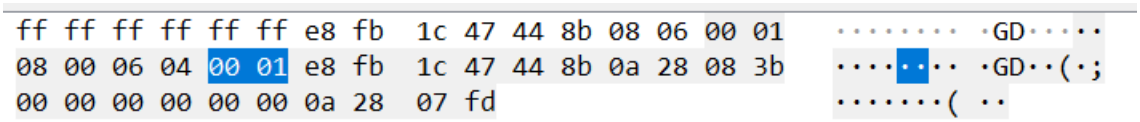
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

Ans: 20 bytes



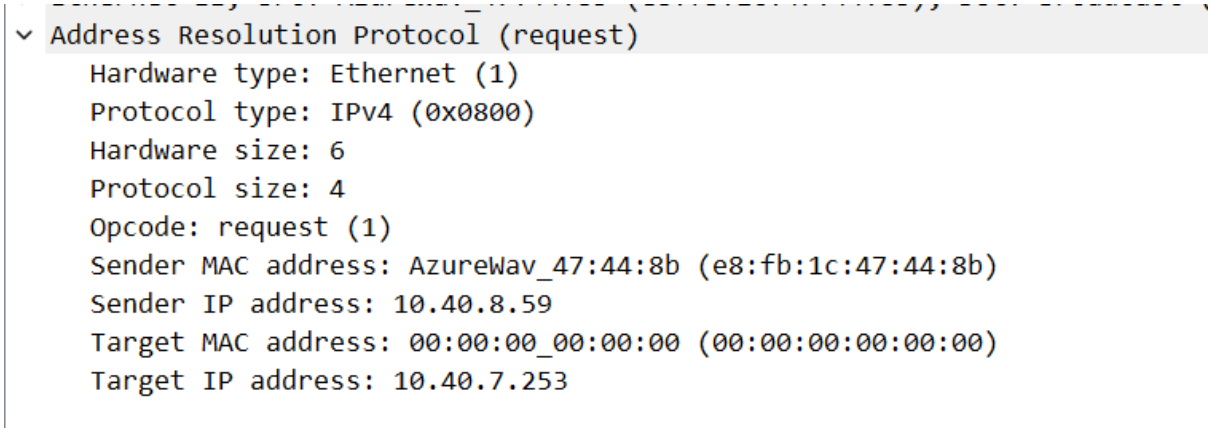
b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

Ans: value of a opcode field : 00 01



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

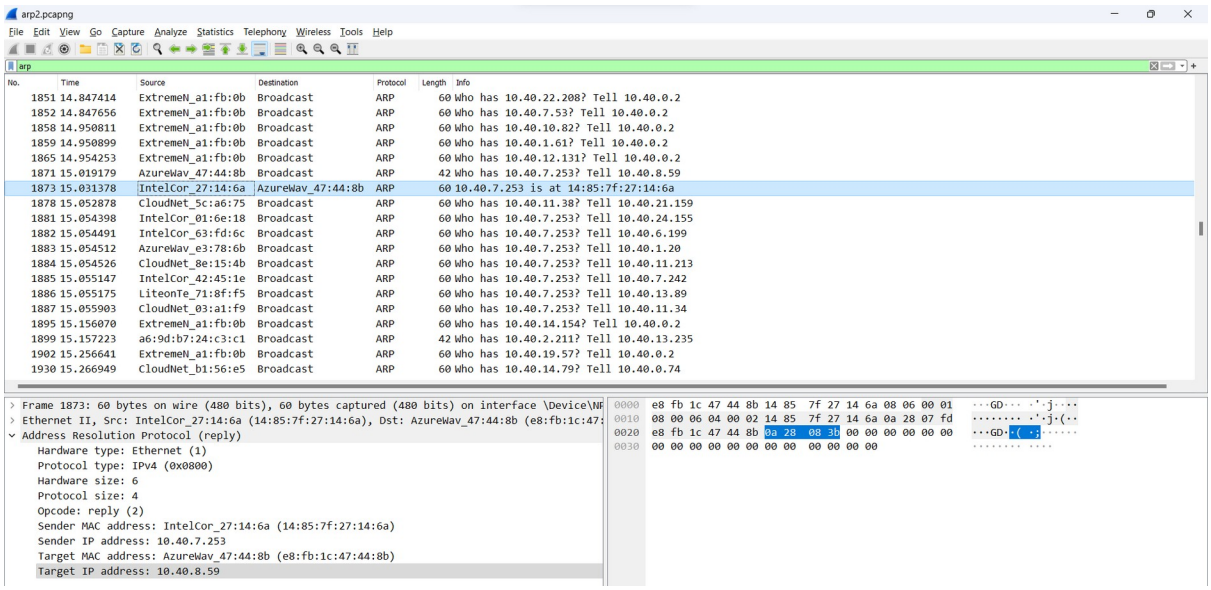
Ans: Yes, ARP message contain the IP address of the sender.



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

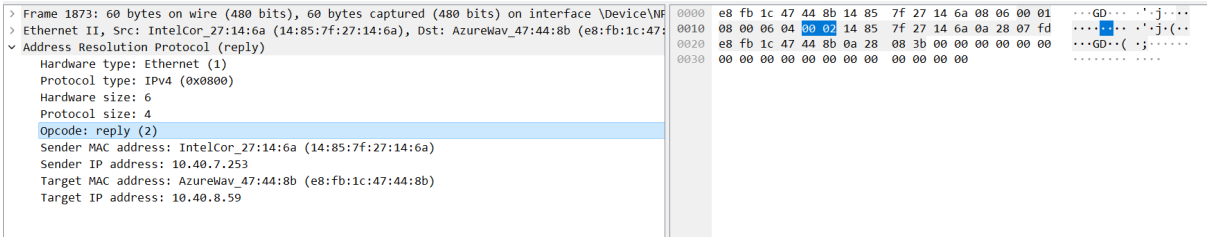
Ans: The field “Target MAC address” is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address 10.40.7.253 is being queried.

5. Now find the ARP reply that was sent in response to the ARP request.



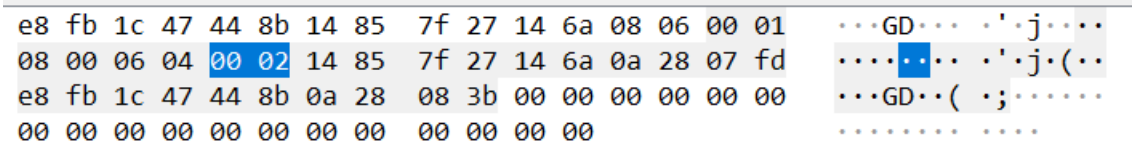
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

Ans: 20 bytes.



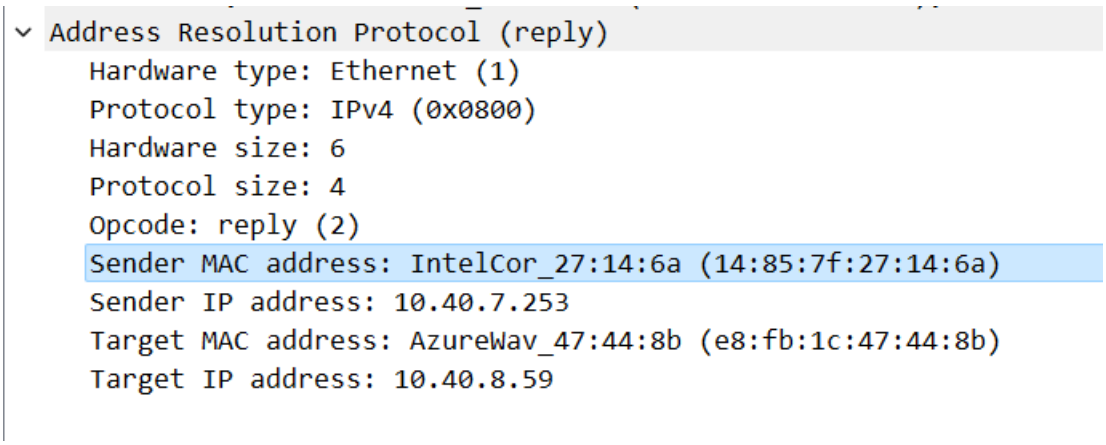
b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

Ans: opcode field = 00 02



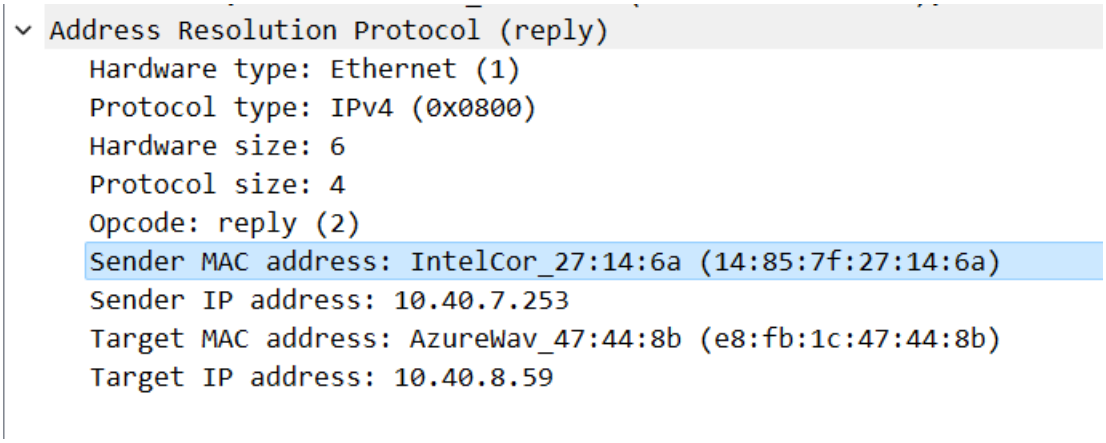
c) Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

Ans: The answer to the earlier ARP request appears in the Sender MAC address field, which contains the Ethernet address 14:85:7f:27:14:6a for the sender with IP address 10.40.7.253.



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

Ans: The hex value for the source address is 14:85:7f:27:14:6a and for the destination is e8:fb:1c:47:44:8b.



7. 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?

Ans: The ARP request is broadcast, but the ARP reply is sent back directly to the sender’s Ethernet address.