ECE361 – Computer Networks

Wireshark Lab 5: Ethernet and ARP

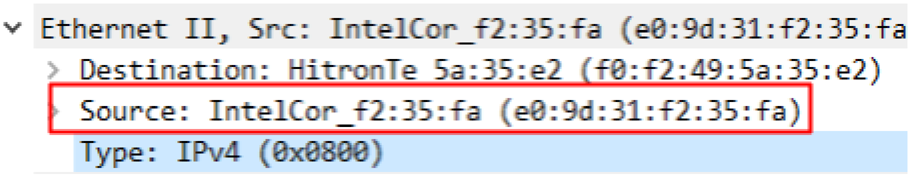
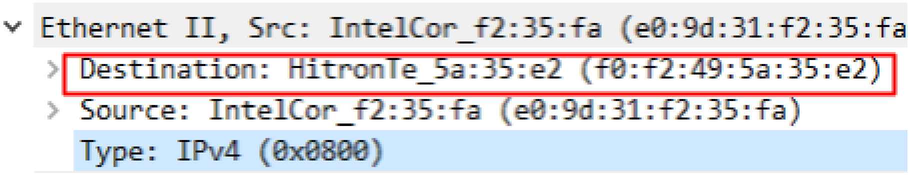
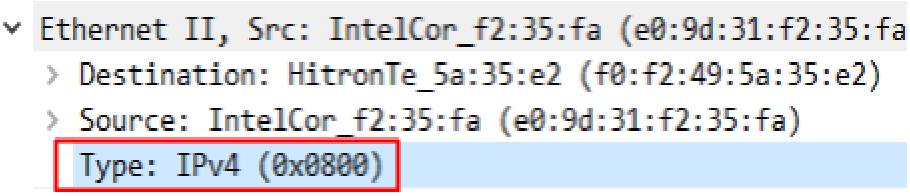
First Name: Tianyi (Nora)   Last Name: Xu

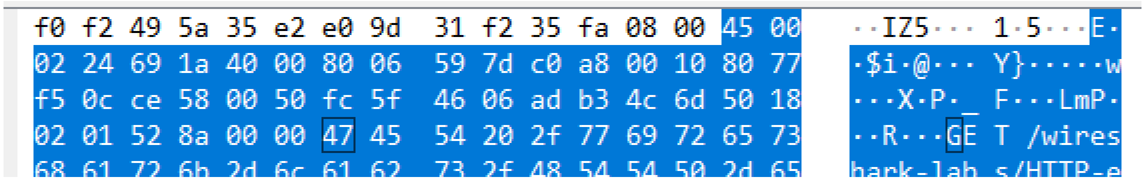
First Name: Yanyi (Will)   Last Name: Zhang

Group Details:

Student #: 1003130809 Student #: 1003327517

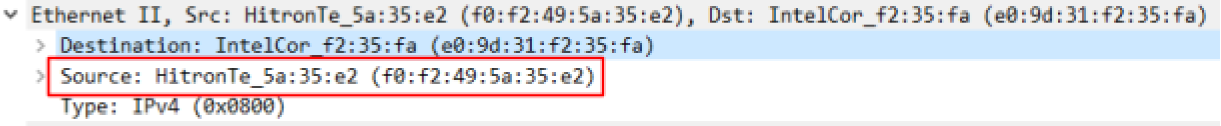
Mark:

	Question	Answer
1	What is the 48-bit Ethernet address of your computer?	e0:9d:31:f2:35:fa
 Ethernet II, Src: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa Destination: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2) Source: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa) Type: IPv4 (0x0800)		
2	What is the 48-bit destination address in the Ethernet frame? What device has this as its Ethernet address?	f0:f2:49:5a:35:e2 The device is the first hop router in the path to the destination address. (i.e. the default gateway in my local network)
 Ethernet II, Src: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa Destination: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2) Source: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa) Type: IPv4 (0x0800)		
3	Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?	0x800. IPv4
 Ethernet II, Src: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa Destination: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2) Source: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa) Type: IPv4 (0x0800)		
4	How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?	“G” appears as the 55th byte in the Ethernet frame. source addr: 6 bytes, dest addr: 6 bytes, type: 2 bytes, IP header: 20 bytes, TCP header: 20 bytes



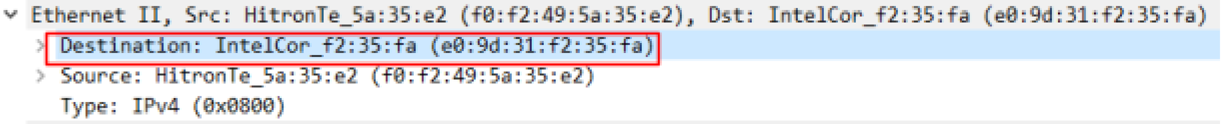
```
f0 f2 49 5a 35 e2 e0 9d  31 f2 35 fa 08 00 45 00   ··IZ5··· 1·5···E·
02 24 69 1a 40 00 80 06  59 7d c0 a8 00 10 80 77   ·$i·@··· Y}·····w
f5 0c ce 58 00 50 fc 5f  46 06 ad b3 4c 6d 50 18   ···X·P·_ F···LmP·
02 01 52 8a 00 00 47 45  54 20 2f 77 69 72 65 73   ··R···GE T /wires
68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 65   hark-lab s/HTTP-e
```

5	What is the value of the Ethernet source address? What device has this as its Ethernet address?	f0:f2:49:5a:35:e2 The device is the first hop router to the client (i.e. default gateway in my local network)



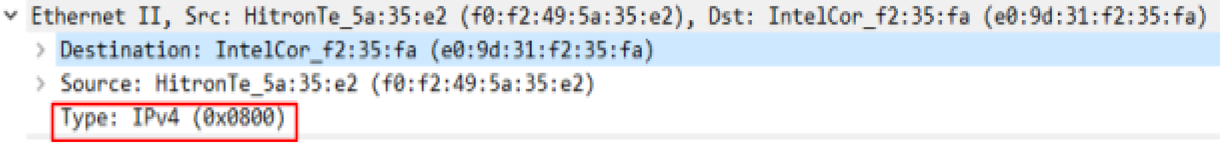
```
Ethernet II, Src: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2), Dst: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa)
  Destination: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa)
  Source: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2)
  Type: IPv4 (0x0800)
```

6	What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?	e0:9d:31:f2:35:fa Yes, it is the Ethernet address of my computer.



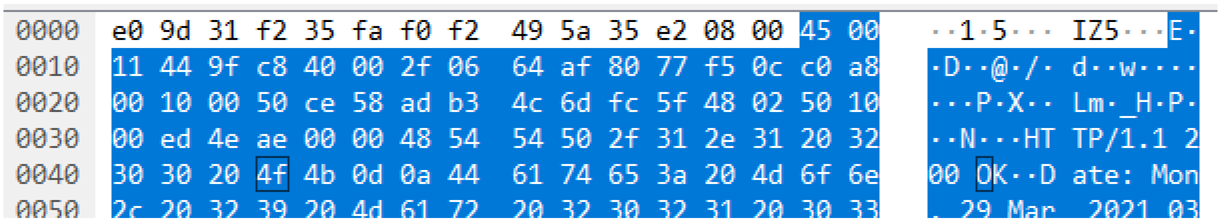
```
Ethernet II, Src: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2), Dst: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa)
  Destination: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa)
  Source: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2)
  Type: IPv4 (0x0800)
```

7	Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?	0x0800 IPv4



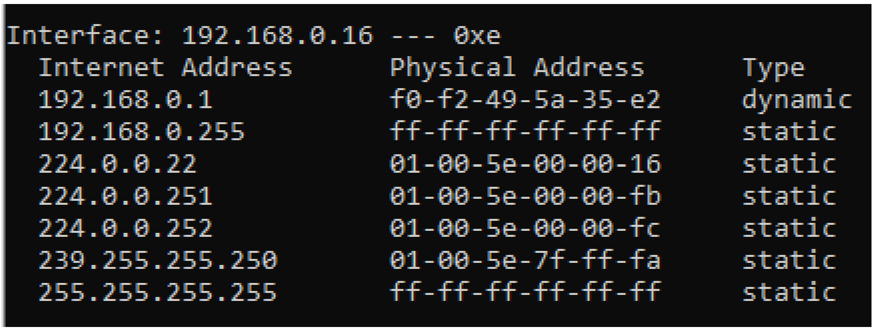
```
Ethernet II, Src: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2), Dst: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa)
  Destination: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa)
  Source: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2)
  Type: IPv4 (0x0800)
```

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 “O” appears as the 68th byte in the Ethernet frame.



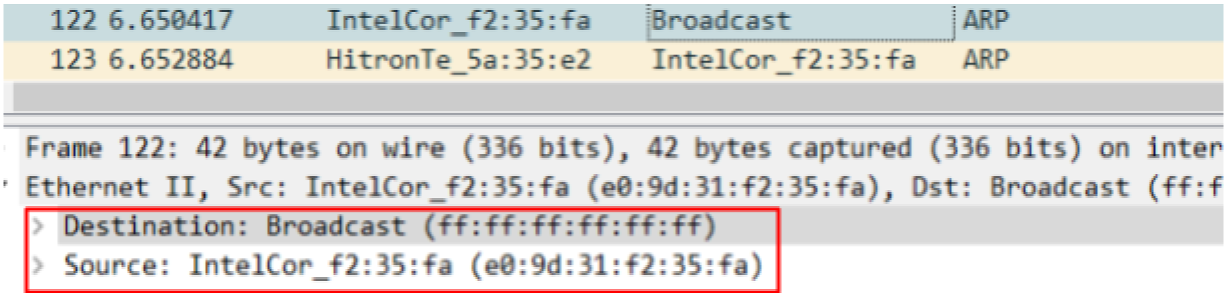
```
0000  e0 9d 31 f2 35 fa f0 f2  49 5a 35 e2 08 00 45 00   ··1·5··· IZ5···E·
0010  11 44 9f c8 40 00 2f 06  64 af 80 77 f5 0c c0 a8   ·D··@·/· d··w····
0020  00 10 00 50 ce 58 ad b3  4c 6d fc 5f 48 02 50 10   ···P·X·· Lm·_H·P·
0030  00 ed 4e ae 00 00 48 54  54 50 2f 31 2e 31 20 32   ··N···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK··D ate: Mon
0050  2c 20 32 39 20 4d 61 72  20 32 30 32 31 20 30 33   , 29 Mar  2021 03
```

9	Write down the contents of your computer's ARP cache. What is the meaning of each column value?	The first column is IP addresses. The second column is MAC addresses. The third column is protocol type. (**Static MAC addresses in the MAC address table** were manually configured. The **dynamic entries in the MAC address table** will time out after a while.)



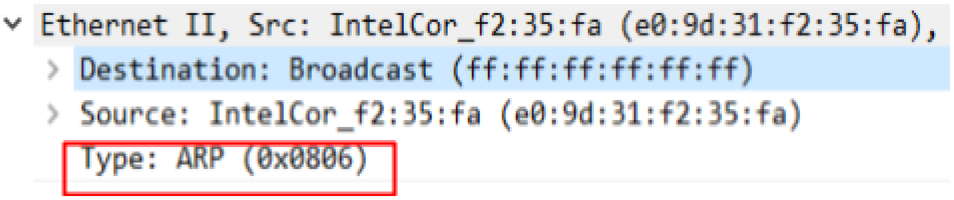
```
Interface: 192.168.0.16 --- 0xe
  Internet Address      Physical Address      Type
  192.168.0.1           f0-f2-49-5a-35-e2     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  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
```

10	What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?	source MAC address: e0:9d:31:f2:35:fa (my computer) destination MAC address: ff:ff:ff:ff:ff:ff:ff (broadcast address)



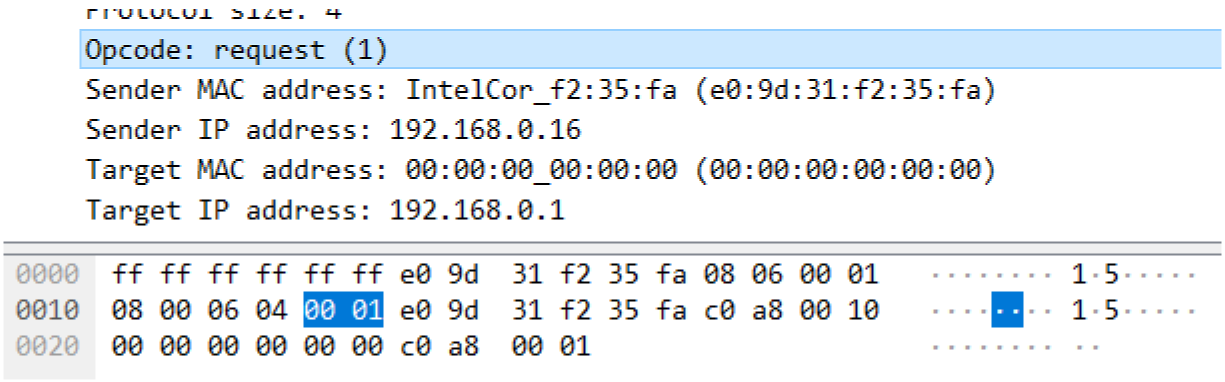
```
122 6.650417    IntelCor_f2:35:fa    Broadcast            ARP
123 6.652884    HitronTe_5a:35:e2    IntelCor_f2:35:fa    ARP

Frame 122: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on inter
Ethernet II, Src: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa), Dst: Broadcast (ff:f
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa)
```

11	Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?	0x0806. ARP



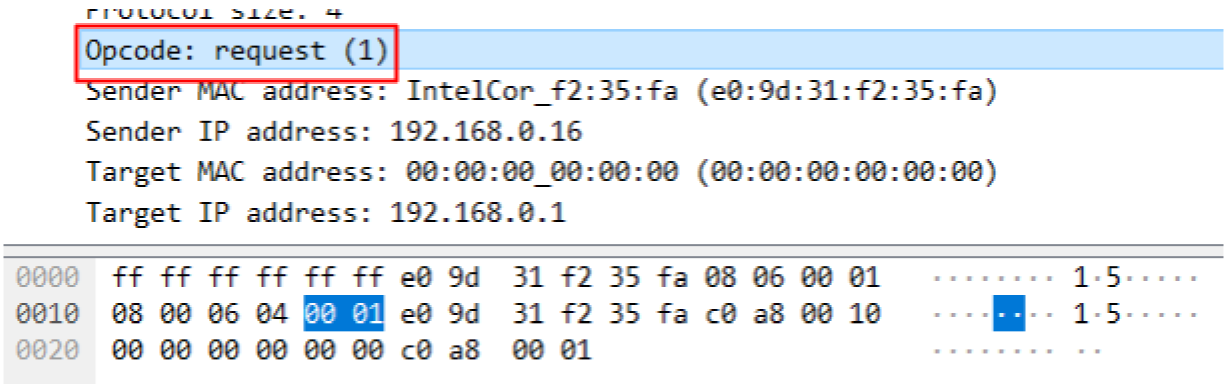
```
∨ Ethernet II, Src: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa),
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa)
    Type: ARP (0x0806)
```

12.a	How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?	20 bytes. Explanation: source addr: 6 bytes dest addr: 6 bytes type: 2 bytes HW type: 2 bytes Protocol type: 2 bytes HLEN: 1 byte PLEN: 1 byte



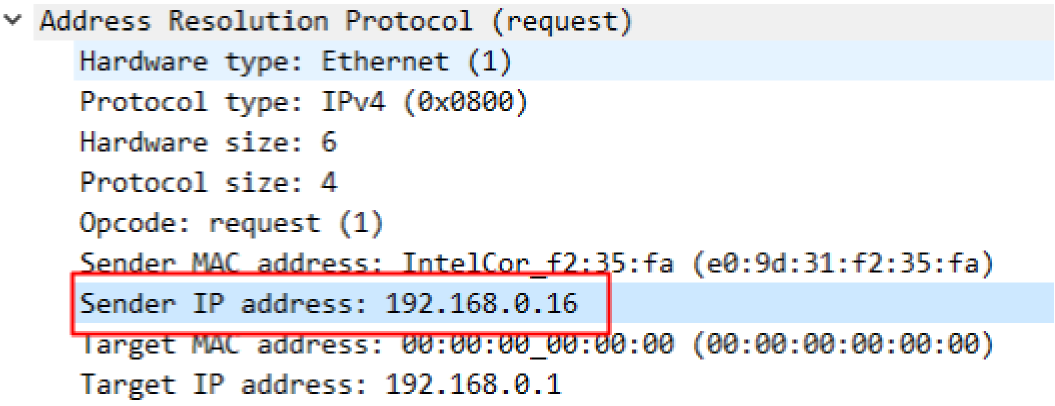
```
Protocol size: 4
Opcode: request (1)
Sender MAC address: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa)
Sender IP address: 192.168.0.16
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.0.1

0000  ff ff ff ff ff ff e0 9d  31 f2 35 fa 08 06 00 01   ........ 1.5.....
0010  08 00 06 04 00 01 e0 9d  31 f2 35 fa c0 a8 00 10   ........ 1.5.....
0020  00 00 00 00 00 00 c0 a8  00 01                     ........ ..
```

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?	1 (opcode is request)



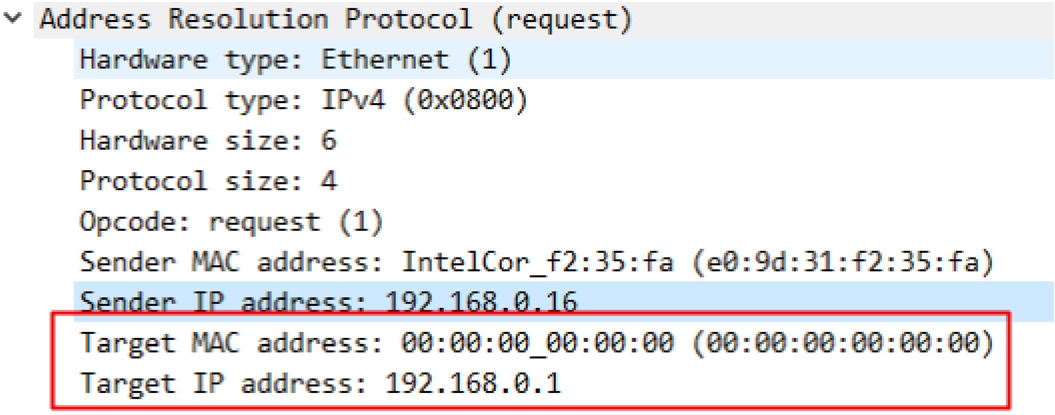
```
Protocol size: 4
Opcode: request (1)
Sender MAC address: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa)
Sender IP address: 192.168.0.16
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.0.1

0000  ff ff ff ff ff ff e0 9d  31 f2 35 fa 08 06 00 01   ........ 1.5.....
0010  08 00 06 04 00 01 e0 9d  31 f2 35 fa c0 a8 00 10   ........ 1.5.....
0020  00 00 00 00 00 00 c0 a8  00 01                     ........ ..
```

12.c	Does the ARP message contain the IP address of the sender?	Yes. IP address is 192.168.0.16.



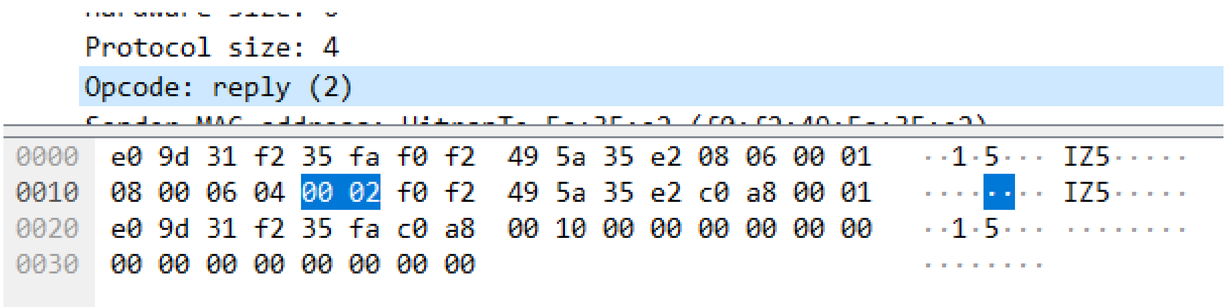
```
⌄ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa)
    Sender IP address: 192.168.0.16
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.1
```

12.d	Where in the ARP request does the "question" appear -- the Ethernet address of the machine whose corresponding IP address is being queried?	In the last 2 fields of the ARP request. The target MAC address is the address the ARP request is trying to query and the target IP address is the IP address of the target machine.



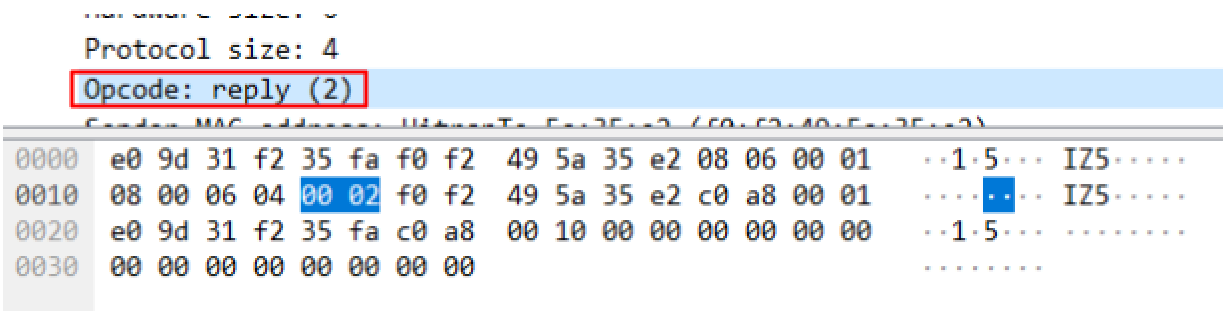
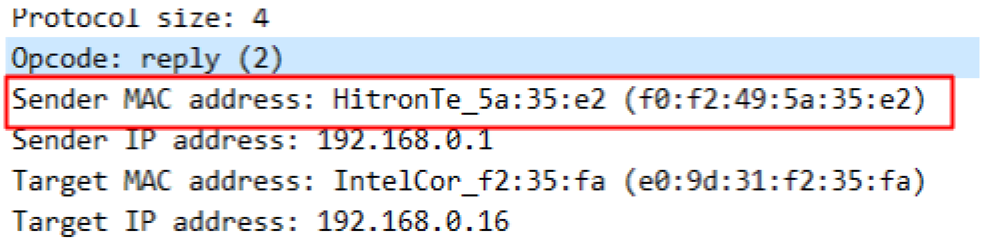
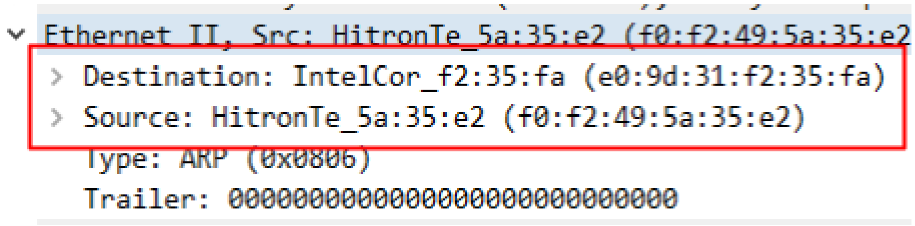
```
⌄ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa)
    Sender IP address: 192.168.0.16
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.1
```

13.a	How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?	20 bytes. same as question 12.a

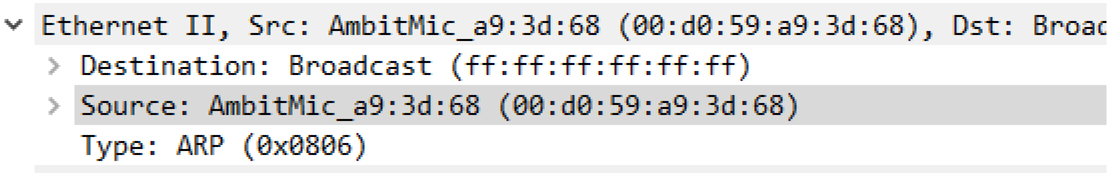


```
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2)

0000  e0 9d 31 f2 35 fa f0 f2  49 5a 35 e2 08 06 00 01   ··1·5··· IZ5·····
0010  08 00 06 04 00 02 f0 f2  49 5a 35 e2 c0 a8 00 01   ········ IZ5·····
0020  e0 9d 31 f2 35 fa c0 a8  00 10 00 00 00 00 00 00   ··1·5··· ········
0030  00 00 00 00 00 00 00 00                            ········
```

13.b	What is the value of the opcode field within the ARP-payload part of the	2 (the opcode is reply)

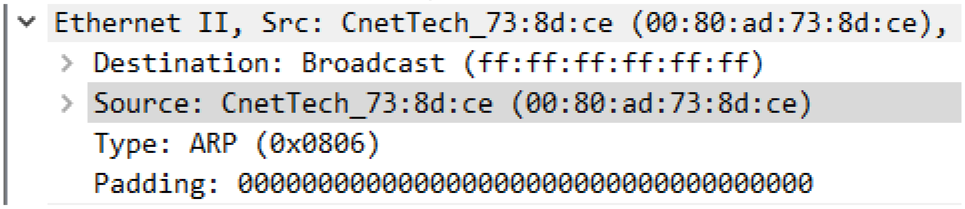
<table>
<tr><td></td><td>Ethernet frame in which an ARP response is made?</td><td></td></tr>
<tr><td colspan="3">
Protocol size: 4
Opcode: reply (2)
0000 e0 9d 31 f2 35 fa f0 f2 49 5a 35 e2 08 06 00 01   ··1·5··· IZ5·····
0010 08 00 06 04 00 02 f0 f2 49 5a 35 e2 c0 a8 00 01   ········ IZ5·····
0020 e0 9d 31 f2 35 fa c0 a8 00 10 00 00 00 00 00 00   ··1·5··· ········
0030 00 00 00 00 00 00 00 00   ········</td></tr>
<tr><td>13.c</td><td>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?</td><td>The sender MAC address is the answer. (f0:f2:49:5a:35:e2)</td></tr>
<tr><td colspan="3">
Protocol size: 4
Opcode: reply (2)
Sender MAC address: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2)
Sender IP address: 192.168.0.1
Target MAC address: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa)
Target IP address: 192.168.0.16</td></tr>
<tr><td>14</td><td>What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?</td><td>source address: f0:f2:49:5a:35:e2 (next-hop router)
destination address: e0:9d:31:f2:35:fa (my computer)</td></tr>
<tr><td colspan="3">
Ethernet II, Src: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2
Destination: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa)
Source: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2)
Type: ARP (0x0806)
Trailer: 0000000000000000000000000000</td></tr>
<tr><td>15</td><td>Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?</td><td>There is no reply in this trace, because we are not the sender or the receiver of the request.

We received the message because it is a broadcast message.</td></tr>
</table>



```
⌄ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broac
  › Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  › Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Type: ARP (0x0806)
```

packet 1



```
⌄ Ethernet II, Src: CnetTech_73:8d:ce (00:80:ad:73:8d:ce),
  › Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  › Source: CnetTech_73:8d:ce (00:80:ad:73:8d:ce)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
```

packet 6