Alex Banning

Wireshark Lab 3 – December 1st, 2019

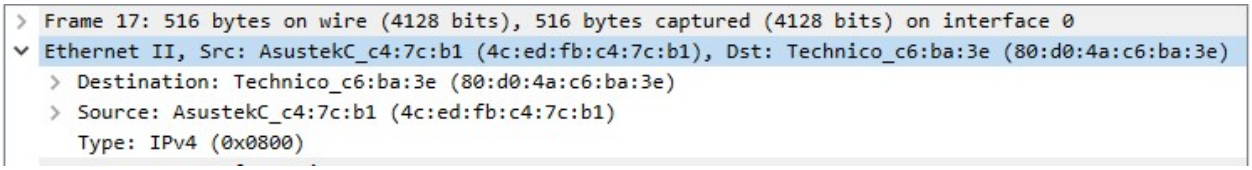
PART 1: Ethernet

Answer the following questions about the packet containing the HTTP GET message:

a) **What is the 48-bit Ethernet address of your computer?**

Source: AsustekC_c4:7c:b1 **(4c:ed:fb:c4:7c:b1)**

Destination: Technico_c6:ba:3e (80:d0:4a:c6:ba:3e)



b) **What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? What device has this as its Ethernet address?**

Destination: Technico_c6:ba:3e **(80:d0:4a:c6:ba:3e)**

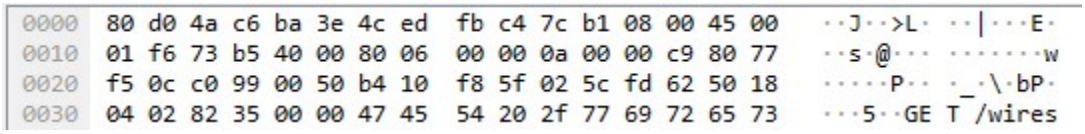
This is the address of the TP link router that my computer is connected to (Gateway to Internet)

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

Hexadecimal for Type: IPv4 is 0x0800

d) **After how many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? (Ignore the 8-byte preamble since by default Wireshark does not include it in the content of the Ethernet frame).**

The index in the figure below indicate that the ASCII G appears in the frame after 54 bytes.

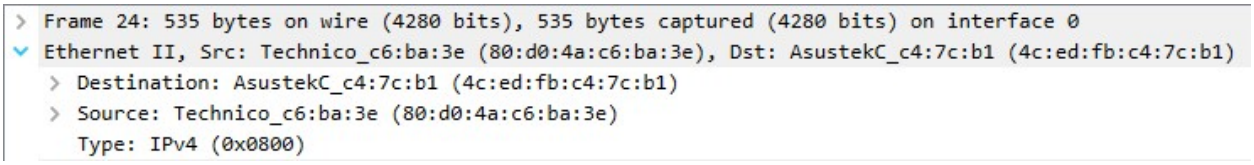


Answer the following questions about the HTTP packet containing the response (OK) message:

e) What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu? What device has this as its Ethernet address?

Source: Technico_c6:ba:3e **(80:d0:4a:c6:ba:3e)**

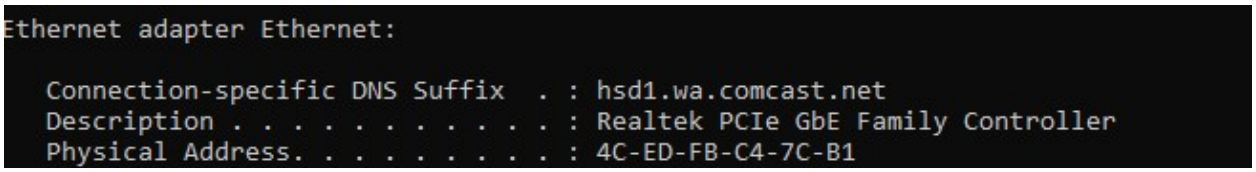
This is the address of my router.



f) What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

Destination: AsustekC_c4:7c:b1 **(4c:ed:fb:c4:7c:b1)**

Confirmation:



This is the address of my computer.

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

Type: IPv4 (0x0800)

PART 2: APR

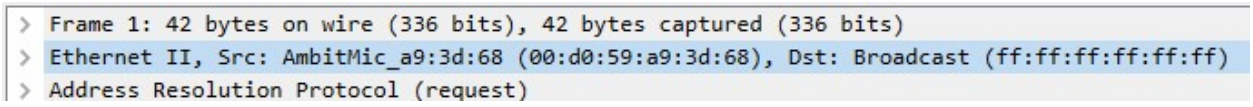
a) **Provide a screenshot of the contents of the ARP cache on your computer.**

```
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\abanning>arp -a

Interface: 10.0.0.201 --- 0x15
  Internet Address      Physical Address      Type
  10.0.0.1              80-d0-4a-c6-ba-3e     dynamic
  10.0.0.178            b4-ae-2b-54-8e-bb     dynamic
  10.0.0.200            b0-05-94-92-7a-21     dynamic
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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

Interface: 192.168.56.1 --- 0x16
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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

C:\Users\abanning>
```

b) **What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?**

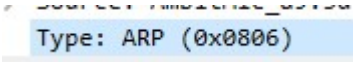
Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

Dst: Broadcast (ff:ff:ff:ff:ff:ff)



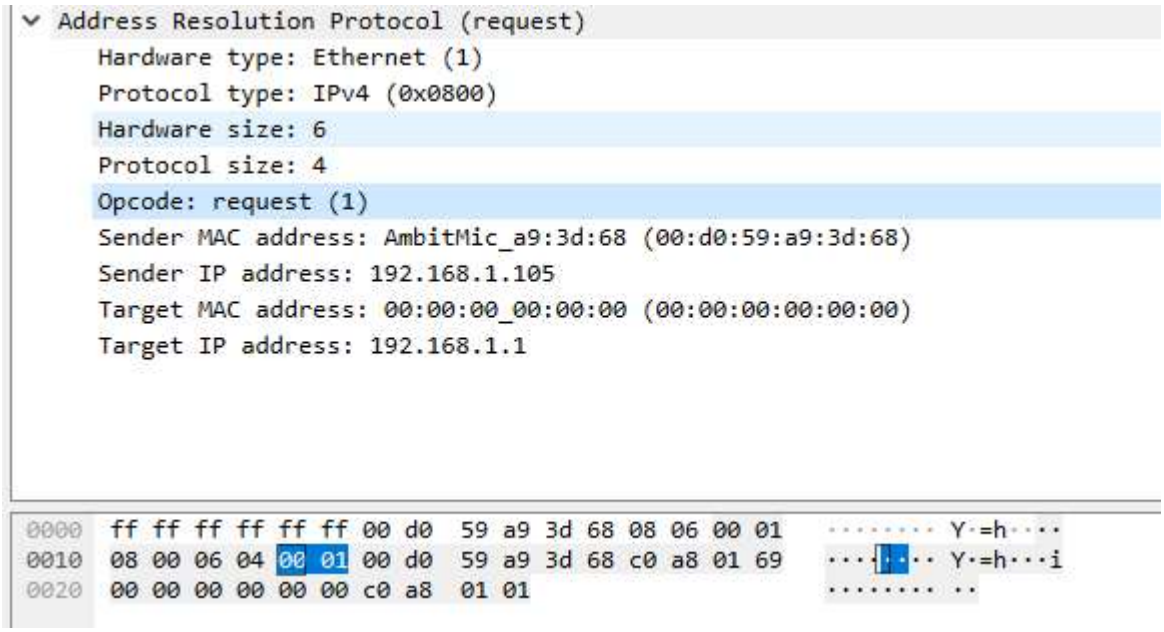
c) **Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?**

Type: ARP (0x0806)



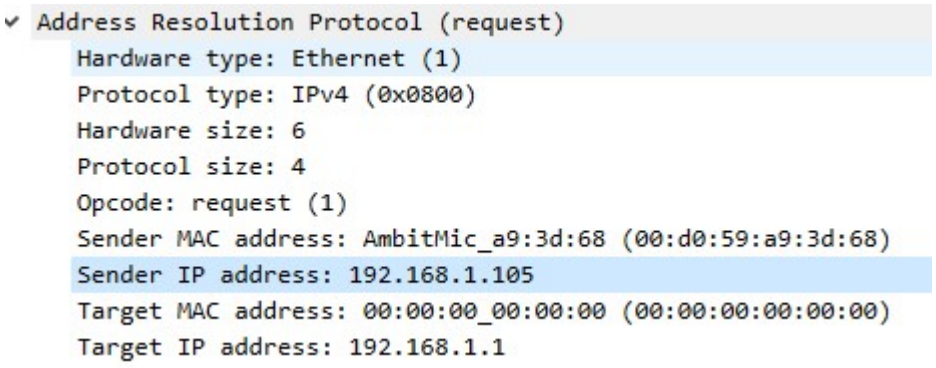
d) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

Opcode begins on the 21st byte



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

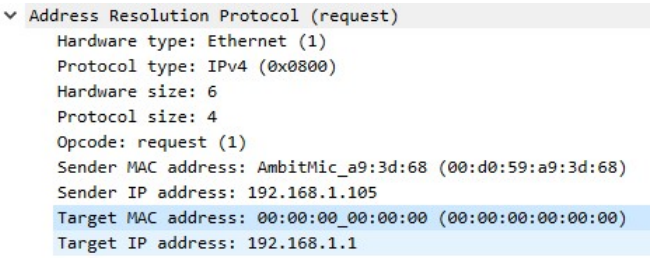
Yes: 192.168.1.105



f) What is the opcode field value for the ARP request message?

Opcode field is 0x0001 as seen highlighted above.

g) How in the ARP request message does the target MAC address "in question" appear?



All 0s

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

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

Opcode = 0x0002

```
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
```

```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01   ··Y·=h·· %··s····
0010  08 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               ········ ····
```

i) Where in the ARP message does the "answer" to the earlier ARP request appear?

Sender IP Address and Sender MAC Address answer the request

They appear at byte 23

```
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
```

```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01   ··Y·=h·· %··s····
0010  08 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               ········ ····
```

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

Src: LinksysG_da:af:73 (00:06:25:da:af:73)

Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

```
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
```

k) There is yet another computer on the network of the Wireshark trace, 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?

There is no reply in the Wireshark trace because replies are not broadcast, so only the sender of the request will receive a reply.