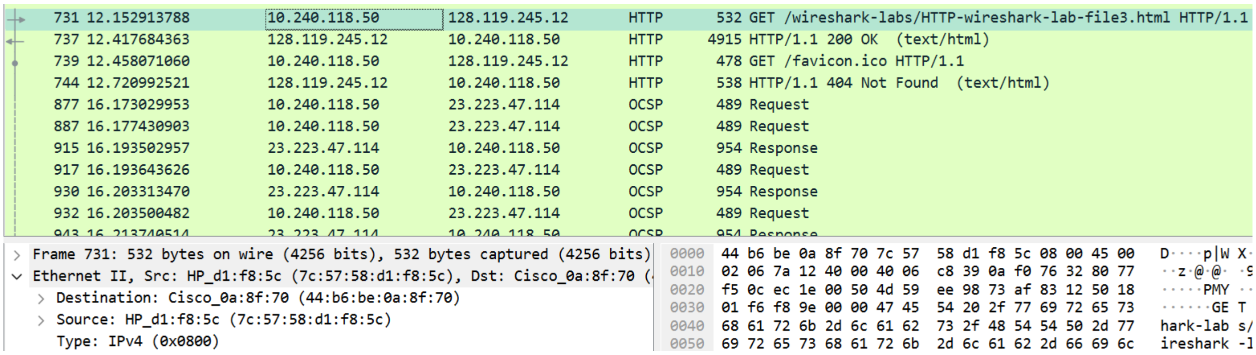
Assignment 11

Part-1



```
731 12.152913788   10.240.118.50    128.119.245.12   HTTP    532 GET /wireshark-labs/HTTP-wireshark-lab-file3.html HTTP/1.1
737 12.417684363   128.119.245.12   10.240.118.50    HTTP   4915 HTTP/1.1 200 OK  (text/html)
739 12.458071060   10.240.118.50    128.119.245.12   HTTP    478 GET /favicon.ico HTTP/1.1
744 12.720992521   128.119.245.12   10.240.118.50    HTTP    538 HTTP/1.1 404 Not Found  (text/html)
877 16.173029953   10.240.118.50    23.223.47.114    OCSP    489 Request
887 16.177430903   10.240.118.50    23.223.47.114    OCSP    489 Request
915 16.193502957   23.223.47.114    10.240.118.50    OCSP    954 Response
917 16.193643626   10.240.118.50    23.223.47.114    OCSP    489 Request
930 16.203313470   23.223.47.114    10.240.118.50    OCSP    954 Response
932 16.203500482   10.240.118.50    23.223.47.114    OCSP    489 Request
943 16.213740514   23.223.47.114    10.240.118.50    OCSP    954 Response
```

```
> Frame 731: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits)
v Ethernet II, Src: HP_d1:f8:5c (7c:57:58:d1:f8:5c), Dst: Cisco_0a:8f:70 (
  > Destination: Cisco_0a:8f:70 (44:b6:be:0a:8f:70)
  > Source: HP_d1:f8:5c (7c:57:58:d1:f8:5c)
    Type: IPv4 (0x0800)
```

```
0000  44 b6 be 0a 8f 70 7c 57  58 d1 f8 5c 08 00 45 00   D····p|W X·
0010  02 06 7a 12 40 00 40 06  c8 39 0a f0 76 32 80 77   ··z·@·@· ·9
0020  f5 0c ec 1e 00 50 4d 59  ee 98 73 af 83 12 50 18   ·····PMY ··
0030  01 f6 f8 9e 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/
0050  69 72 65 73 68 61 72 6b  2d 6c 61 62 2d 66 69 6c   ireshark -l
```

1. The 48-bit Ethernet address of my computer is **7c:57:58:d1:f8:5c**

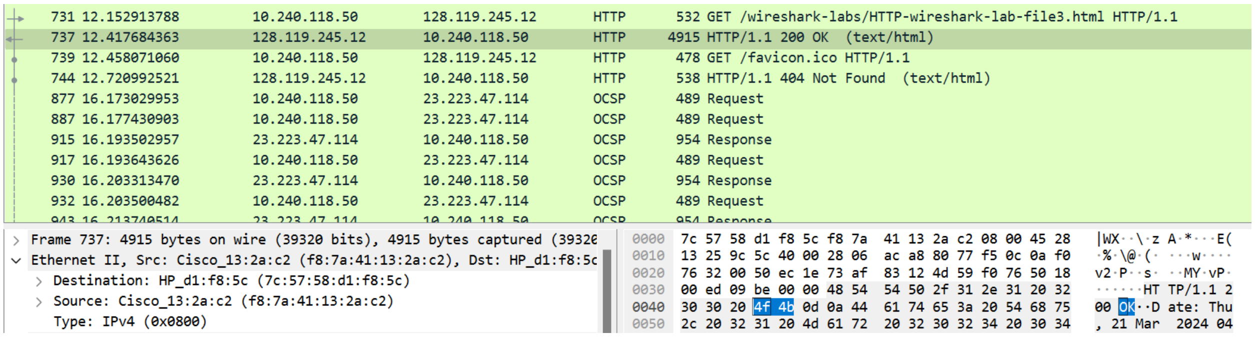
2. The 48-bit destination address is **44:b6:be:0a:8f:70**

No,This address is not the ethernet address of gaia.cs.umass.edu, but it is the address of my TP link router (Gateway to Internet).

3. The hexadecimal value for the two-byte Frame type field in the Ethernet frame is **0x0800**

It corresponds to the **IPv4** layer protocol.

4. The ASCII “G” in GET appears after **54 bytes** in to the Ethernet frame



```
731 12.152913788   10.240.118.50    128.119.245.12   HTTP    532 GET /wireshark-labs/HTTP-wireshark-lab-file3.html HTTP/1.1
737 12.417684363   128.119.245.12   10.240.118.50    HTTP   4915 HTTP/1.1 200 OK  (text/html)
739 12.458071060   10.240.118.50    128.119.245.12   HTTP    478 GET /favicon.ico HTTP/1.1
744 12.720992521   128.119.245.12   10.240.118.50    HTTP    538 HTTP/1.1 404 Not Found  (text/html)
877 16.173029953   10.240.118.50    23.223.47.114    OCSP    489 Request
887 16.177430903   10.240.118.50    23.223.47.114    OCSP    489 Request
915 16.193502957   23.223.47.114    10.240.118.50    OCSP    954 Response
917 16.193643626   10.240.118.50    23.223.47.114    OCSP    489 Request
930 16.203313470   23.223.47.114    10.240.118.50    OCSP    954 Response
932 16.203500482   10.240.118.50    23.223.47.114    OCSP    489 Request
943 16.213740514   23.223.47.114    10.240.118.50    OCSP    954 Response
```

```
> Frame 737: 4915 bytes on wire (39320 bits), 4915 bytes captured (39320
v Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: HP_d1:f8:5c
  > Destination: HP_d1:f8:5c (7c:57:58:d1:f8:5c)
  > Source: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2)
    Type: IPv4 (0x0800)
```

```
0000  7c 57 58 d1 f8 5c f8 7a  41 13 2a c2 08 00 45 28   |WX··\·z A·*···E(
0010  13 25 9c 5c 40 00 28 06  ac a8 80 77 f5 0c 0a f0   ·%·\@·(· ···w····
0020  76 32 00 50 ec 1e 73 af  83 12 4d 59 f0 76 50 18   v2·P··s· ··MY·vP·
0030  00 ed 09 be 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54 68 75   00 OK··D ate: Thu
0050  2c 20 32 31 20 4d 61 72  20 32 30 32 34 20 30 34   , 21 Mar  2024 04
```

5. The Ethernet source address is **44:b6:be:0a:8f:70**

No, This address is not the address of my computer or gaia.cs.umass.edu. This is the address of my router.

6. The destination address in the Ethernet Frame is: **7c:57:58:d1:f8:5c**

Yes, This is the Ethernet address of the computer.

7. The hexadecimal value for the two-byte Frame type field is: **0x0800**

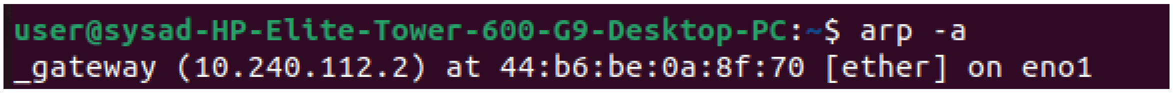
The upper layer protocol is **IPv4**

8. The ASCII “O” in “OK” appears after **67 bytes** from the very start of the Ethernet frame.

9. 4 Ethernet frames carry the data that is part of the complete HTTP “OK 200…” reply message.

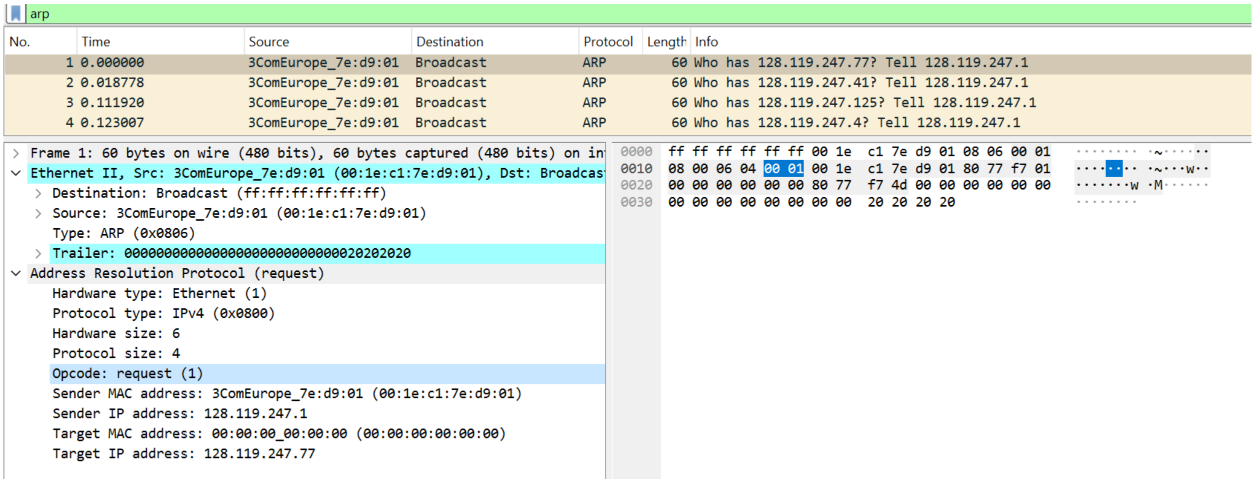
Part-2

1. No. of entries in ARP cache = **1**



```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ arp -a
_gateway (10.240.112.2) at 44:b6:be:0a:8f:70 [ether] on eno1
```

2. The ARP cache contains entries that map **IP addresses to MAC addresses**. A static ARP table contains entries that are user-configured.



```
arp

No.  Time      Source               Destination  Protocol Length Info
   1 0.000000  3ComEurope_7e:d9:01  Broadcast    ARP        60 Who has 128.119.247.77? Tell 128.119.247.1
   2 0.018778  3ComEurope_7e:d9:01  Broadcast    ARP        60 Who has 128.119.247.41? Tell 128.119.247.1
   3 0.111920  3ComEurope_7e:d9:01  Broadcast    ARP        60 Who has 128.119.247.125? Tell 128.119.247.1
   4 0.123007  3ComEurope_7e:d9:01  Broadcast    ARP        60 Who has 128.119.247.4? Tell 128.119.247.1

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on in
v Ethernet II, Src: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01), Dst: Broadcas
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
    Type: ARP (0x0806)
  > Trailer: 000000000000000000000000000020202020
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
    Sender IP address: 128.119.247.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 128.119.247.77

0000  ff ff ff ff ff ff 00 1e  c1 7e d9 01 08 06 00 01   ········ ·~······
0010  08 00 06 04 00 01 00 1e  c1 7e d9 01 80 77 f7 01   ········ ·~···w··
0020  00 00 00 00 00 00 80 77  f7 4d 00 00 00 00 00 00   ·······w ·M······
0030  00 00 00 00 00 00 00 00  20 20 20 20               ········
```

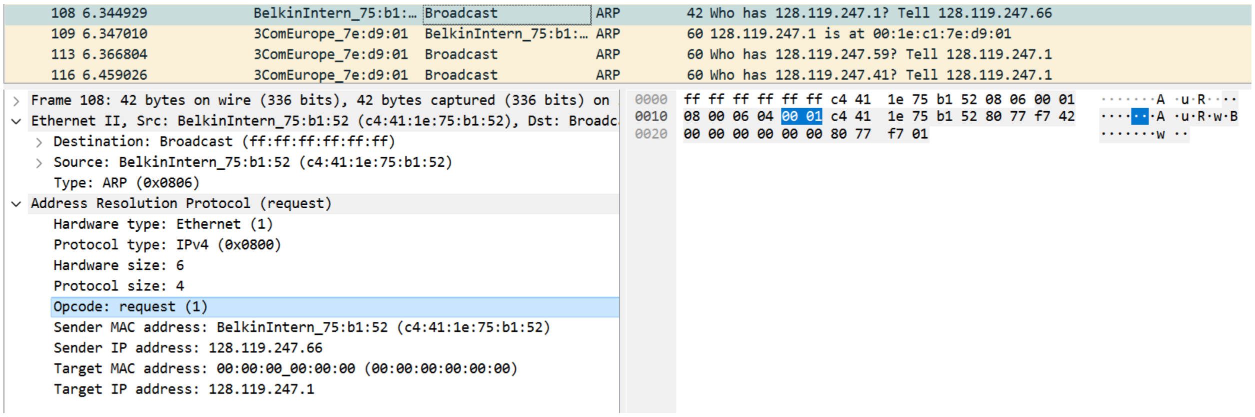
3. The hexadecimal value of the source address in the Ethernet frame is: **00:1e:c1:7e:d9:01**

4. The hexadecimal value of the destination addresses in the Ethernet frame containing the ARP request message sent out by the computer is: **ff:ff:ff:ff:ff:ff**

This is the Ethernet address of the **router** (Gateway to the Internet).

5. The hexadecimal value for the two-byte Ethernet frame type field is: **0x0806**.

The upper layer protocol is: **ARP**.



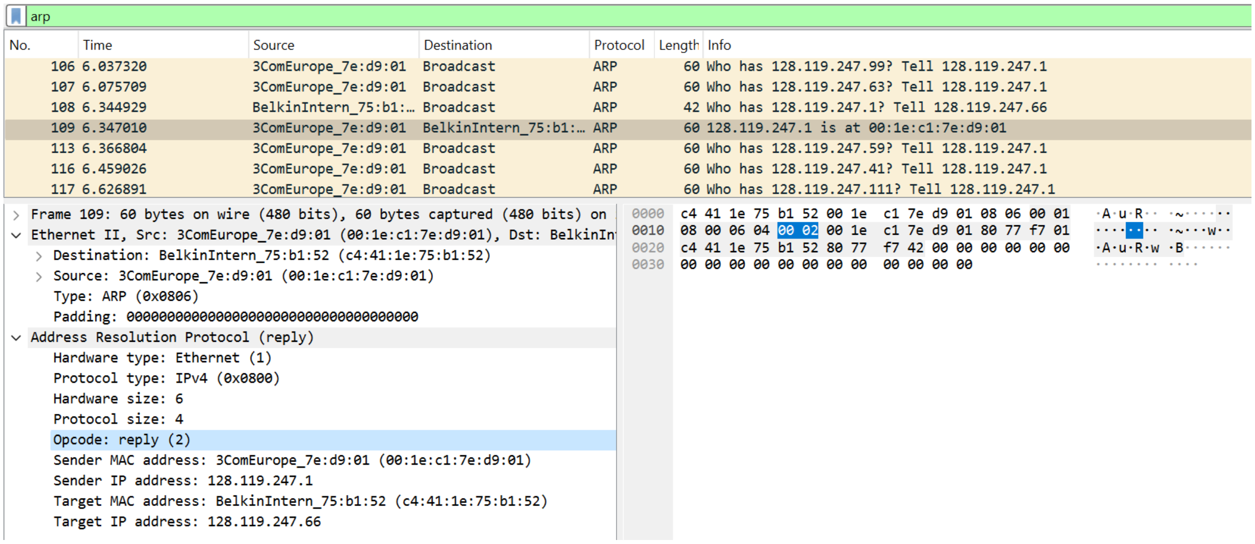
```
 108 6.344929  BelkinIntern_75:b1:…  Broadcast             ARP   42 Who has 128.119.247.1? Tell 128.119.247.66
 109 6.347010  3ComEurope_7e:d9:01   BelkinIntern_75:b1:…  ARP   60 128.119.247.1 is at 00:1e:c1:7e:d9:01
 113 6.366804  3ComEurope_7e:d9:01   Broadcast             ARP   60 Who has 128.119.247.59? Tell 128.119.247.1
 116 6.459026  3ComEurope_7e:d9:01   Broadcast             ARP   60 Who has 128.119.247.41? Tell 128.119.247.1

> Frame 108: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on
v Ethernet II, Src: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52), Dst: Broadc
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
    Type: ARP (0x0806)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
    Sender IP address: 128.119.247.66
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 128.119.247.1

0000  ff ff ff ff ff ff c4 41  1e 75 b1 52 08 06 00 01   ·······A ·u·R····
0010  08 00 06 04 00 01 c4 41  1e 75 b1 52 80 77 f7 42   ·······A ·u·R·w·B
0020  00 00 00 00 00 00 80 77  f7 01                     ·······w ··
```

6. The ARP opcode begins after **20 bytes** from the beginning of the Ethernet frame.

7. The value of the opcode filed within the ARP request message sent by the computer is: **request (1)**

8. Yes, the ARP request message contains the IP address of the sender, which is: **128.119.247.66**

9. The IP address of the device whose corresponding Ethernet address is being requested in the ARP request message is: **128.119.247.1**



No.	Time	Source	Destination	Protocol	Length	Info
106	6.037320	3ComEurope_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.99? Tell 128.119.247.1
107	6.075709	3ComEurope_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.63? Tell 128.119.247.1
108	6.344929	BelkinIntern_75:b1:…	Broadcast	ARP	42	Who has 128.119.247.1? Tell 128.119.247.66
109	6.347010	3ComEurope_7e:d9:01	BelkinIntern_75:b1:…	ARP	60	128.119.247.1 is at 00:1e:c1:7e:d9:01
113	6.366804	3ComEurope_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.59? Tell 128.119.247.1
116	6.459026	3ComEurope_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.41? Tell 128.119.247.1
117	6.626891	3ComEurope_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.111? Tell 128.119.247.1

```
> Frame 109: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on
v Ethernet II, Src: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01), Dst: BelkinIn
  > Destination: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
  > Source: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
    Sender IP address: 128.119.247.1
    Target MAC address: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
    Target IP address: 128.119.247.66
```

```
0000  c4 41 1e 75 b1 52 00 1e  c1 7e d9 01 08 06 00 01   ·A·u·R·· ·~······
0010  08 00 06 04 00 02 00 1e  c1 7e d9 01 80 77 f7 01   ········ ·~···w··
0020  c4 41 1e 75 b1 52 80 77  f7 42 00 00 00 00 00 00   ·A·u·R·w ·B······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

10. The value of the opcode filed with the ARP reply message is: **reply (2)**

11. The Ethernet address corresponding to the IP address that was specified in the ARP request message sent earlier by the computer is **00:1e:c1:7e:d9:01**

12. We are not able to see the responses that are being sent to other ARP requests Because the ARP request is broadcast, but the ARP reply is not broadcast. The reply will be sent to the computer(Ethernet Address) who made the request directly. Hence, we will be only seeing the response for our request and not the responses for other requests.