

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

```
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
Ethernet II, Src: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01),  
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)
```

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?

Destination:

```
7e:d9:01 (00:1e:c1:7e:d9:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
.. .... = 16 bit: Locally administered address (this is NO  
.. .... = 16 bit: Group address (multicast/broadcast)  
01 (00:1e:c1:7e:d9:01)
```

It's the address of the zip file capture, since I used the zip file (I was unwell in class for Tuesday)

3. What is the hexadecimal value for the two-byte Frame type field in the Ethernet frame carrying the HTTP GET request? What upper layer protocol does this correspond to?

```
> Frame 126: 677 bytes on wire (5416 bits), 677 bytes captured (5416 bits) on :  
Ethernet II, Src: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52), Dst: 3ComEurope_7e:d9:01  
> Destination: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)  
> Source: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)  
Type: IPv4 (0x0800)
```

Two-byte frame type is 08 00, it's the IP protocol

4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.

```
> Transmission Control Protocol, Src Port: 54042, Dst Port: 80, Seq: 1, Ack: 1
  ▾ Hypertext Transfer Protocol
    ▾ GET /wireshark-labs/HTTP-wireshark-lab-file3.html HTTP/1.1\r\n
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-lab-file3.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:93.0) Gecko/
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.5
    GET /wireshark-labs/HTTP-wireshark-lab-file3.html HTTP/1.1\r\n
    0040 96 a8 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b GET /w ireshark
    0040 96 a8 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b GET /w ireshark
```

G is equal to 47

Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

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?

```
> Frame 126: 677 bytes on wire (5416 bits), 677 bytes captured (5416 bits) on
  ▾ Ethernet II, Src: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52), Dst: 3ComEurope
    > Destination: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
    > Source: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
    Type: IPv4 (0x0800)
```

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

```
Ethernet II, Src: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52), Dst: 3ComEurope
  ▾ Destination: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0. .... = IG bit: Individual address (unicast)
  > Source: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
  Type: IPv4 (0x0800)
  [Stream index: 7]
```

Yes it's the zip file's capture address

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

Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.72.238
Transmission Control Protocol, Src Port: 80, Dst Port: 53204, Seq: 423
08 00 45 68 ... ? _ a G ?

The upper layer is IP layer

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? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.

4f 4b 0d HTTP/1.1 200 OK

O = 4f

9. How many Ethernet frames (each containing an IP datagram, each containing a TCP segment) carry data that is part of the complete HTTP “OK 200 ...” reply message?

[4 Reassembled TCP Segments (4861 bytes): #131(1448), #132(1448), #133(1448), #134(517)]
[Frame: 131, payload: 0-1447 (1448 bytes)]
[Frame: 132, payload: 1448-2895 (1448 bytes)]
[Frame: 133, payload: 2896-4343 (1448 bytes)]
[Frame: 134, payload: 4344-4860 (517 bytes)]
[Segment count: 4]
[Reassembled TCP length: 4861]