

# Assignment 11

## 210010033

### Part1:

1. The 48 bit-ethernet address of the machine is c4:41:1e:75:b1:52 .
2. The 48 bit-ethernet address of the destination is 00:1e:c1:7e:d9:01. No, it is not the ethernet address of gaia.cs.umass.edu. It is the address of the next hop router.
3. The frame type is 0x0800. This corresponds to the IPV4 protocol.
4. 'G' appears after 65 bytes in the Ethernet frame.
5. Ethernet source address is 00:1e:c1:7e:d9:01. Next hop router (3ComEurope\_7e:d9:01) has this as its ethernet address.
6. Destination address is c4:41:1e:75:b1:52. Yes, this is the ethernet address of the device used for capturing the trace.
7. The type is 0x0800. It corresponds to IPV4 protocol.
8. 14<sup>th</sup> byte is the position of O in OK in HTTP. 80<sup>th</sup> byte is the position of O in OK from start of ethernet frame.
9. 4 different Ethernet frames contain carry data that is part of the complete HTTP "OK 200 ..." reply message.

The image shows a Wireshark packet capture analysis. The left pane displays the packet list with the following details:

- Frame 134: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface en9, id 0
- Ethernet II, Src: 3ComEurope\_7e:d9:01 (00:1e:c1:7e:d9:01), Dst: BelkinIntern\_75:b1:52 (c4:41:1e:75:b1:52)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 128.119.247.66
- Transmission Control Protocol, Src Port: 80, Dst Port: 54842, Seq: 4345, Ack: 612, Len: 517
- 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
- Reassembled TCP Data [truncated]: 485454502f312e3120323030204f4b0d0a446174653a2054756552c203032
- Hypertext Transfer Protocol
- HTTP/1.1 200 OK\r\n
- [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
- Response Version: HTTP/1.1
- Status Code: 200
- [Status Code Description: OK]
- Response Phrase: OK
- Date: Tue, 02 Nov 2021 17:37:43 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod\_perl/2.0.11 Perl/v5.16.3\r\n
- Last-Modified: Tue, 02 Nov 2021 05:59:02 GMT\r\n

The right pane shows the packet bytes and the reassembled TCP data. The packet bytes are displayed in hexadecimal and ASCII. The reassembled TCP data is displayed in hexadecimal and ASCII. The ASCII data shows the HTTP response body, which is a truncated version of the complete HTTP "OK 200 ..." reply message.

## Part2:

```
> Frame 108: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en9, i
< Ethernet II, Src: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
  Type: ARP (0x0806)
  < 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
```

1.

```
(base) → ~ arp -a
? (10.200.92.2) at b0:8b:d0:60:ff:ff on en0 ifscope [ethernet]
? (10.200.95.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
mdns.mcast.net (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
(base) → ~ |
```

There are 4 entries in my arp cache.

2. Each entry is of the form *(IP address) at MAC address on interface*
3. Source address is c4:41:1e:75:b1:52.
4. Destination address is ff:ff:ff:ff:ff:ff. This does not correspond to any device.
5. Type is 0x0806. The upper layer protocol here is ARP.
6. The opcode starts from the 21<sup>st</sup> byte.
7. Opcode field values is request (1)
8. Yes. Sender IP address is 128.119.247.66
9. Target IP address: 128.119.247.1

```
> Frame 109: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en9, i
✓ Ethernet II, Src: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01), Dst: BelkinIntern_75:b1:52 (c
  > 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: 00000000000000000000000000000000
  ✓ 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
```

10. Opcode field value is reply (2)

11. Target MAC address is c4:41:1e:75:b1:52 .

12. The reply comes only to the one sending the queries.