CSC358 Wireshark Assignment 5 Solution

1. In the packet that contains the http GET message, what is the source mac address? Is this your computer’s mac address?

Solution:
The source mac address is: 78:ca:39:b2:bc:fd.
It is my computer’s mac address.

Frame: 517 bytes on wire (4136 bits), 517 bytes captured (4136 bits) on interface 0
- IP, Src: 100.64.167.139 (100.64.167.139), Dst: 128.119.245.12 (128.119.245.12)
- Transmission Control Protocol, Src Port: 40513 (40513), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 451
- Hypertext Transfer Protocol
  - GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
    - Host: gaza.cs.umass.edu
    - Connection: keep-alive
    - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
    - Upgrade-Insecure-Requests: 1
    - User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.116 Safari/537.36
    - Accept-Encoding: gzip, deflate, sdch
    - Accept-Language: en-US,en;q=0.8,zh-CN;q=0.6,zh;q=0.4

[Full request URL: http://gaza.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html]
[HTTP request 3/1]
[Response in Frame: 35]
2. What is the destination mac address of the above packet, is this the mac address of gaia.cs.umass.edu? If not, then which device has this mac address?

Solution:
The mac address of the destination is 00:90:0b:27:12:11. This is not the Ethernet address of gaia.cs.umass.edu. It is the mac address for my router or internet gateway address.
3. What is the hexadecimal frame type field in the ethernet header of this packet? What is the correspond upper layer protocol?

Solution:
The hexadecimal frame type field in the ethernet header of this packet is 0x0800. It indicates that the upper layer protocol is Internet Protocol version 4 (IPv4).
4. Do you notice that WireShark can display the manufacturer of the sender (source) and receiver (destination) of this packet? How this can be done? What is the manufacture of the mac address cc:20:e8:11:22:33?

Solution:
The mac address contains an OUI (Organizationally Unique Identifier) field. It is a 24-bit number that uniquely identifies a vendor or manufacturer. They are purchased and assigned by the IEEE. The OUI is basically the first three octets of a MAC address.
Wireshark tries to convert the first 3 bytes of an ethernet address to an abbreviated manufacturer name by looking up OUI database.
The manufacturer of cc:20:e8:11:22:33 is Apple.
5. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame? Explain how do you obtain this result.

Solution:
After 528 bits or 66 bytes the G in get appears.
Or before “G”, we have 14 ethernet header + 20 IP header + 32 tcp header = 66 bytes
6. Focus on the first packet in the trace file. What is the frame type in ethernet header? What is the destination mac address?

**Solution:**
The frame type is ARP (0x0806).
The destination mac address is ff:ff:ff:ff:ff:ff.

```plaintext
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: AmbitMic a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: AmbitMic a9:3d:68 (00:d0:59:a9:3d:68)
  Type: ARP (0x0806)
Address Resolution Protocol (request)
```
7. Is the destination of the above packet a real computer? If not, who will receive the above packet?

Solution:
No. The mac address ff:ff:ff:ff:ff:ff is used for broadcast. All machines on the local area network (LAN) will receive it.
8. Which type of ARP packet is the above one? What operation does this packet try accomplishing? Find the corresponding packet of the above ARP packet. Which type of ARP packet is this one? What information it provides?

Solution:
It is a address resolution request. It tries to find the mac address of the 192.168.1.1.
The corresponding packet:

```
Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
  Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  Type: ARP (0x0806)
  Padding: 00000000000000000000000000000000
Protocol: Address Resolution Protocol [reply]
  Hardware type: Ethernet (1)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender IP address: 192.168.1.1 (192.168.1.1)
  Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  Target IP address: 192.168.1.105 (192.168.1.105)
```

It is a reply for the above request.
It provides the mac address of 192.168.1.1.
9. In the first packet, what is the target mac address in the arp header? Is it the same as the destination mac address in the ethernet header? If not, will this be a problem?

Solution:
The target mac address is 00:00:00:00:00:00.
It is different with the destination mac address in the ethernet header.
It is not a problem. The target mac address in the arp header of the request is a non-useful field.
It can be ignored, whatever the value in it does not matter. The destination mac address in the ethernet header is ff:ff:ff:ff:ff:ff, which is used to broadcast the arp request within the local area network (LAN).

```
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
  Ethernet II, Src: AmbitMic_a9:3d:68 (00:00:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: AmbitMic_a9:3d:68 (00:00:59:a9:3d:68)
    Type: ARP (0x0806)
  Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AmbitMic_a9:3d:68 (00:00:59:a9:3d:68)
    Sender IP address: 192.168.1.105 (192.168.1.105)
    Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1 (192.168.1.1)
```
10. Notice that the 6th packet in the trace file is also an arp packet, explain why we didn’t see a corresponding arp packet to this one.

**Solution:**
There is no reply in this trace, because we are not at the machine that sent the request. The ARP request is broadcast, but arp reply is an unicast packet, only the targeted machine will receive it.