Week 3
ICMP

ip-ethereal-trace-1

Ans.1: The IP address of computer is: 192.168.1.102 .
Ans.2: The value in the upper layer protocol field is ICMP(1).
Ans.3: The IP header contains 20 bytes. The total size of data is 84 bytes so size of payload is (84-20)= 64 bytes.
Ans.4: No, this IP datagram has not been fragmented. This can be determined as the more fragment flag is 0 and the fragment offset is also 0, so there can be only one fragment of the actual size of the packet.
Ans.5: The fields of IP datagram which always change from one datagram to the next within the series of ICMP are : Time-to-live, Header checksum and Identification.
Ans.6: Following fields stay constant: IP Version(since we are using IPv4 for all packets), Header Length(since these are ICMP packets), Source IP(since we are sending from the same source), Destination IP(since we are sending to the same destination) and Upper Layer Protocol(since these are ICMP packets).
Following fields must stay constant: IP Version(since we are using IPv4 for all packets), Header Length(since these are ICMP packets), Source IP(since we are sending from the same source), Destination IP(since we are sending to the same destination) and Upper Layer Protocol(since these are ICMP packets).
The following fields must change: Identification(each IP packet must have different identifier), Header checksum(since identification is different so its checksum must also be different) and Time-to-live(traceroute increments each subsequent packet).
Ans.7: The values in the Identification field of the IP datagram increment by 1.
Ans.8: Identification is 0x9d7c (40316) and Time to live is 255.
Ans.9: No, the message has not been fragmented across more than one IP datagram.
Ans.10: The More Fragments flag is set, which indicates that the datagram has been fragmented.
Fragment offset is 0, which indicates that this is the first fragment. This first datagram has a total length of 1500, including the header.
Ans.11: Fragment offset is not zero, which indicates that this is the not the first fragment. Yes there are more fragments since the More Fragments flag is set.
Ans.12: The fields which change in the IP header between the first and second fragment are: Fragment offset and header checksum.

ARP

I. Capturing and analyzing Ethernet frames

Ans.1: The Ethernet address of computer is: 00:d0:59:a9:3d:68.
Ans.2: The Ethernet address of computer Destination:00:06:25:da:af:73. No, this is not the Ethernet address of gaia.cs.umass.edu rather it is the destination address of the router LinkSys to which the computer is connected.
Ans.3: The hexadecimal value for the two-byte Frame type field is 0x0806. This corresponds to ARP
Ans.4: 'G' in GET appears after 54 bytes from the starting.
Ans.5: The Ethernet address of source:00:06:25:da:af:73. No, this is neither the Ethernet address of gaia.cs.umass.edu nor computer rather it is the address of the router LinkSys to which the computer is connected.
Ans.6: The destination address in the Ethernet frame is 00:d0:59:a9:3d:68. Yes, this is the address of computer.
Ans.7: The hexadecimal value for the two-byte Frame type field is 0x0800 for IPv4.
Ans.8: 'O' in OK appears after 13 bytes from the starting.

II. The Address Resolution Protocol

Ans.9: The ARP cache is as below:

```
Interface: 172.31.86.146 --- 0x3
  Internet Address      Physical Address      Type
  172.31.86.129         00-1b-d4-74-6e-7f     dynamic
  172.31.86.191         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

Interface: 192.168.170.1 --- 0x1a
  Internet Address      Physical Address      Type
  192.168.170.101       7c-46-85-13-45-51     dynamic
  192.168.170.103       ac-29-3a-e7-87-5c     dynamic
  192.168.170.255       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
```

The internet address represents IP address, the physical address represents the MAC address and type represents the type of protocol.

Ans.10: The hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message are 00:d0:59:a9:3d:68 and ff:ff:ff:ff:ff:ff respectively.

Ans.11: The hexadecimal value for the two-byte Frame type field is 0x0806. This corresponds to ARP.

Ans.12:(a) ARP opcode field begins 20 bytes from the starting.

(b) The value of the opcode field is 0x0001.

(c) Yes, the ARP message do contain the IP address of the sender that's 192.168.1.105.

(d) The field "Target MAC address" is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.1.1) is being queried.

Ans.13:(a) ARP opcode field begins 20 bytes from the starting.

(b) The value of the opcode field is 0x0002.

(c) The answer appears in the Sender MAC Address that's 00:06:25:da:af:73.

Ans.14: The hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message are 00:06:25:da:af:73 and 00:d0:59:a9:3d:68 respectively.

Ans.15: There is no reply in this trace, because we are not at the machine that sent the request. The ARP request is broadcast, but the ARP reply is sent back directly to the sender's Ethernet address