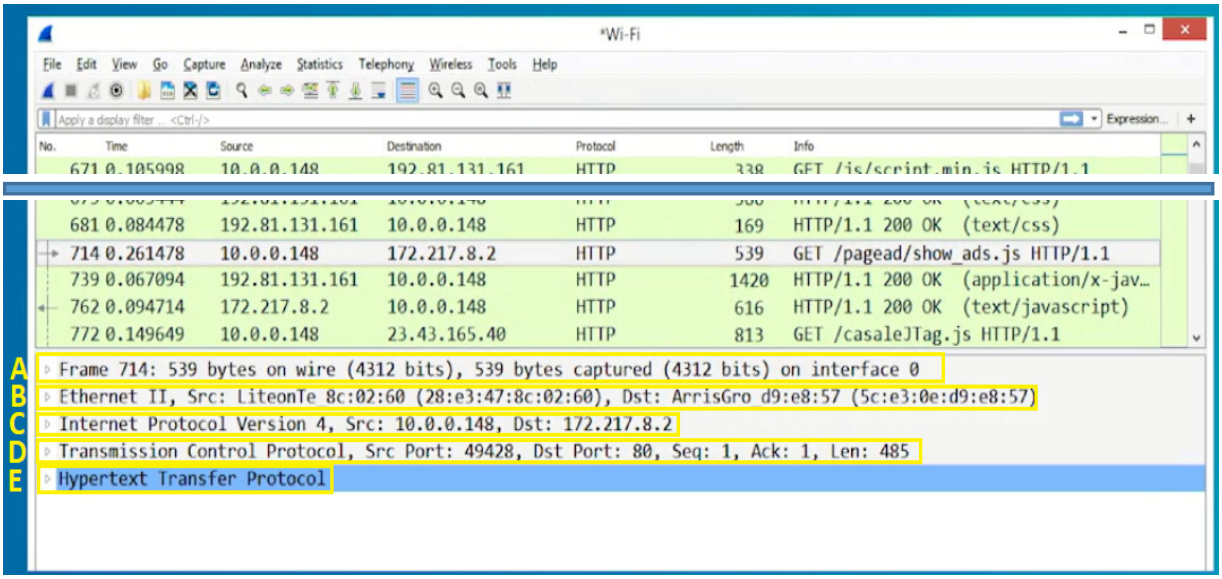
Network Management Course

Dr. Z.Movahedi

Assignment_1

Subject: ARP, IP and ICMP protocols by Wireshark software

1- The following picture depicts the HTTP packets:



- In frame 714, which section in packet details represents the frame header? Why? (Choose between A, B, C, D and E) (Multiple choice could be correct)

2- Go to http://packetlife.net/captures/protocol/icmp/ and download and open the packet capture “ICMP_across_dot1q.cap”.

A-In packet list, find packet from “Cisco_ea:b8:c1”. What is the source and destination MAC address of this request and the corresponding reply?

B-In packet list, how many ICMP request packets do you see?

3- According to the previous question, find ICMP request/reply packets.

According to this packet list, obtain the following parameters:

According to this log, obtain the following parameters:

A-What is minimum round-trip time in milliseconds?

B- What is maximum round-trip time in milliseconds?

C- What is average round trip time in milliseconds?

4- According to the following captured packets, fill requested fields:

Note: for each packet, the first 14 Bytes are the Ethernet header.

01 00 5e 00 00 fc 60 eb 69 4d 97 3f 08 00 46 00 00 20 07 32 00 00 01 02 33 d7 ac 11 5c c1 e0 00 00 fc 94 04 00 00 16 00 09 03 e0 00 00 fc 00 00 00 00 00 00 00 00 00 00 00 00 00 00
IP source address:
IP Destination address:
Which application has generated this packet? Why?

01 00 5e 00 00 01 64 31 50 0e 0a 2f 08 00 45 00 00 3c 2c a3 00 00 80 01 25 77 ac 11 5c 94 e0 00 00 01 08 00 2d de 00 01 0a 90 42 69 74 44 65 66 65 6e 64 65 72 20 46 69 72 65 77 61 6c 6c 20 42 72 6f 61 64 63 61 73 74 00 00
IP source address:
IP Destination address:
Which application has generated this packet? Why?

5- Open your Wireshark program and select ICMP as filter. Start capturing packets on your interface (en0, wlan0, etc.). Now open up your terminal (Linux) or command prompt (windows) and use one of the following commands:

Windows: ping –n 10 8.8.8.8

Linux: ping –c 10 8.8.8.8

A- Why is it that an ICMP packet does not have source and destination port numbers?

B- Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

C- Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

Good luck
TA Team
Fall 2022