Operating Systems

Professor Ward

Spring 2021

**Packet Inspection Assignment**

Download and install Wireshark. Run it, select an interface with traffic, and start capturing packets. Do a ping, plus a whois or anything else to generate network traffic. Stop the capture.

1. Show a screenshot of Wireshark at the end.
2. How many packets did it capture? What was the packets-per-second rate?

🡪 7766 packetsText

Description automatically generated

1. What protocol is used by ping?

🡪 uses ICMP protocol

Table

Description automatically generated with low confidence

1. List the protocols used by the captured packets.  
   🡪 TLS (TLSv1.3, TLSv1.2), TCP, SSDP, NTP, MDNS, IGMP (IGMPv3), ICMP (ICMPv6, ICMP), HTTP, DNS, ARP, 0x7373

Text

Description automatically generated

1. Pick one of these protocols which was unfamiliar to you, learn what it does, and give a one-sentence summary in your own words.Graphical user interface

   Description automatically generated  
   🡪 IGMP: Internet Group Message Protocol --- This protocol is used to allow a host to advertise its multicast group with neighboring switches and routers, which means it lets to communicate from one source to a selected group of destination.
2. Find the longest packet and double click on it. Show a screenshot of the payload, and give your guess as to what this packet is for.  
   🡪

Graphical user interface, application

Description automatically generated

Since the source port is 433, I know that it is an HTTPS (website) packet.

1. Look at any 3 UDP packets. The header should include the protocol number for UDP, namely 17 (1116). Where does this occur (at what byte number)? Is this the same for each UDP packet? Explain why it occurs here, based the information Wireshark displays and your knowledge of the length and layout of packet headers.

Text

Description automatically generated

1. A picture containing text

   Description automatically generated
2. 

Text

Description automatically generated

🡪 All of them are 17 indicating that it is an UDP protocol. In addition, all of them occurred on byte 23 and had the number ‘11’.   
Convert 11x to a decimal is: 1\*16^1 + 1\*16^0 = 16 + 1 = 17 (UDP protcol number).  
The position when protocol occurs is at byte 23.   
‘Enternet II’ contains 14 bytes which is irrelevant to IPv4 Header, and ‘Internet Protocol Version 4, Src: 192:168:1:254, Dst: 192.168.1.210’ contains 20 bytes which matches with IPv4 header from Version to Destination Address. Within the IPv4 Header, the protocol is located on the 10th. Thus, 14 bytes, “Internet Protocol Version 4’ which comes before IP header information, plus 10 since the order of IPv4 Header format.   
10 + 14 = 24. Counting starts from 0, therefore 24 – 1 = 23.  
With this information, it make sense why it have 11, 17, and location of 23rd byte.

Table

Description automatically generated with medium confidence  
Picture of a wireshark screen for Question 1.