Assignment 2

Individual Assignment

In this assignment, you will explore ICMP packets by capturing the packets generated by the Ping and traceroute programs. You may recall that the Ping program is a simple tool that allows anyone (for example, a network administrator) to verify if a host is live or not. The Ping program in the source host sends a packet to the target IP address; if the target is live, the Ping program in the target host responds by sending a packet back to the source host. Also, you may recall that the Traceroute program can be used to figure out the path a packet takes from source to destination.

Part I: ICMP using ping

Capture the packets using Wireshark tool in the duration of the following command and answer the following questions. Save the captured file with the name: <*RollNo-ping.pcapng*> to save the capture file.

i. ping -c 10 www.google.com

1. What is the IP address of your host? What is the IP address of the destination host?
2. Why is it that an ICMP packet does not have source and destination port numbers?
3. 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?
4. 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?

Part II: ICMP using traceroute

Capture the packets using Wireshark tool in the duration of the following commands and answer the following questions. Save the captured file with the name: <*RollNo-traceroute.pcapng*> to save the capture file.

i. traceroute -I www.youtube.com 64
ii. traceroute -I www.youtube.com 3000

1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window.

2. Which of the IP datagrams are fragmented?

3. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

4. Which fields stay constant? Why?

Deliverables in Eduserver as a tarball with the following:

- Captured wireshark packet traces with the names: <*RollNo-ping.pcapng*> and <*RollNo-traceroute.pcapng*>
- A readable PDF Report (with name “WiresharkICMP-<RollNo>.PDF”) with the answers for the aforementioned questions in Part I and II on the captured packet traces.