IP, ICMP, and Fragmentation

In this lab, you will analyze IP datagrams and fragmentation using Wireshark. You will load a pre-captured trace file and explore the various fields in the IP datagram. Include screenshots of Wireshark where necessary.

Opening the Wireshark Trace File

To analyze the IP datagrams in this lab, you need to open the provided trace file `ip-ethereal-trace-1` in Wireshark.

1. Download the `wireshark-traces.zip` file from the course materials.
2. Unzip the file, which should include the trace file `ip-ethereal-trace-1`.
3. In Wireshark, go to `File -> Open` and navigate to the directory where the unzipped trace files are located. Select the file `ip-ethereal-trace-1` and click `Open`.

Lab Questions

Q1: **First ICMP Echo Request Message**

(a) What is the IP address of the computer that sent the ICMP Echo Request message? `192.168.1.102`

(b) Within the IP packet header, what is the value in the upper-layer protocol field?

(c) How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

(d) Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

Q2: **Sorting by Source IP Address**

(a) Sort the trace by the source IP address by clicking on the "Source" column header. Examine the ICMP Echo Request messages.

(b) Which fields in the IP datagram typically change from one datagram to the next?

(c) Which fields typically stay constant? Which fields must stay constant, and why?

(d) Describe the pattern you see in the values in the Identification field of the IP datagram.

Q3: **Fragmentation Analysis**

(a) Find the first ICMP Echo Request message that was sent after the packet size was set to 2000 bytes. Has this message been fragmented across more than one IP datagram?

(b) What information in the IP header of the first datagram indicates that the datagram has been fragmented?

(c) What information in the IP header of the second datagram indicates that this is not the first fragment? Are there more fragments? How can you tell?

(d) What fields change in the IP header between the first and second fragments?

Q4: **Fragmentation with Larger Packet Size**

(a) Find the ICMP Echo Request message that was sent after the packet size was set to 3500 bytes.

(b) How many fragments were created from the original datagram?

(c) What fields change in the IP header among the fragments?

Submission Guidelines

Please submit answers to all the questions on Canvas as a PDF.