NTNU
The Norwegian University of
Science and Technology
Department of Information Security
and Communications Technology

TTM4100
Communication – Services and Networks

Wireshark Lab: IP

This lab is one of the 8 programming labs in this course. You must deliver and pass at least 6 of these labs to be qualified for the exam. Any questions about the exercises can be posted on the forum or you can come to the tuition.

Deadline of submission: **25.02.2018**

In this lab, we'll investigate the IP protocol, focusing on the IP datagram. We'll do so by analyzing a trace of IP datagrams sent and received by an execution of the traceroute program. We'll investigate the various fields in the IP datagram, and study IP fragmentation in detail.

Before beginning this lab, you'll probably want to review sections 1.4.3 in the text book to update yourself on the operation of the traceroute program. You'll also want to read Section 4.4 in the text book, for a discussion of the IP protocol.

2. A look at the captured trace

Using the trace from blackboard, you should be able to see the series of ICMP Echo Request sent by the client and the ICMP TTL-exceeded messages returned by the intermediate routers. Before answering the questions below, filter the messages in Wireshark by applying the "icmp" filter.

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. What is the IP address of the client?

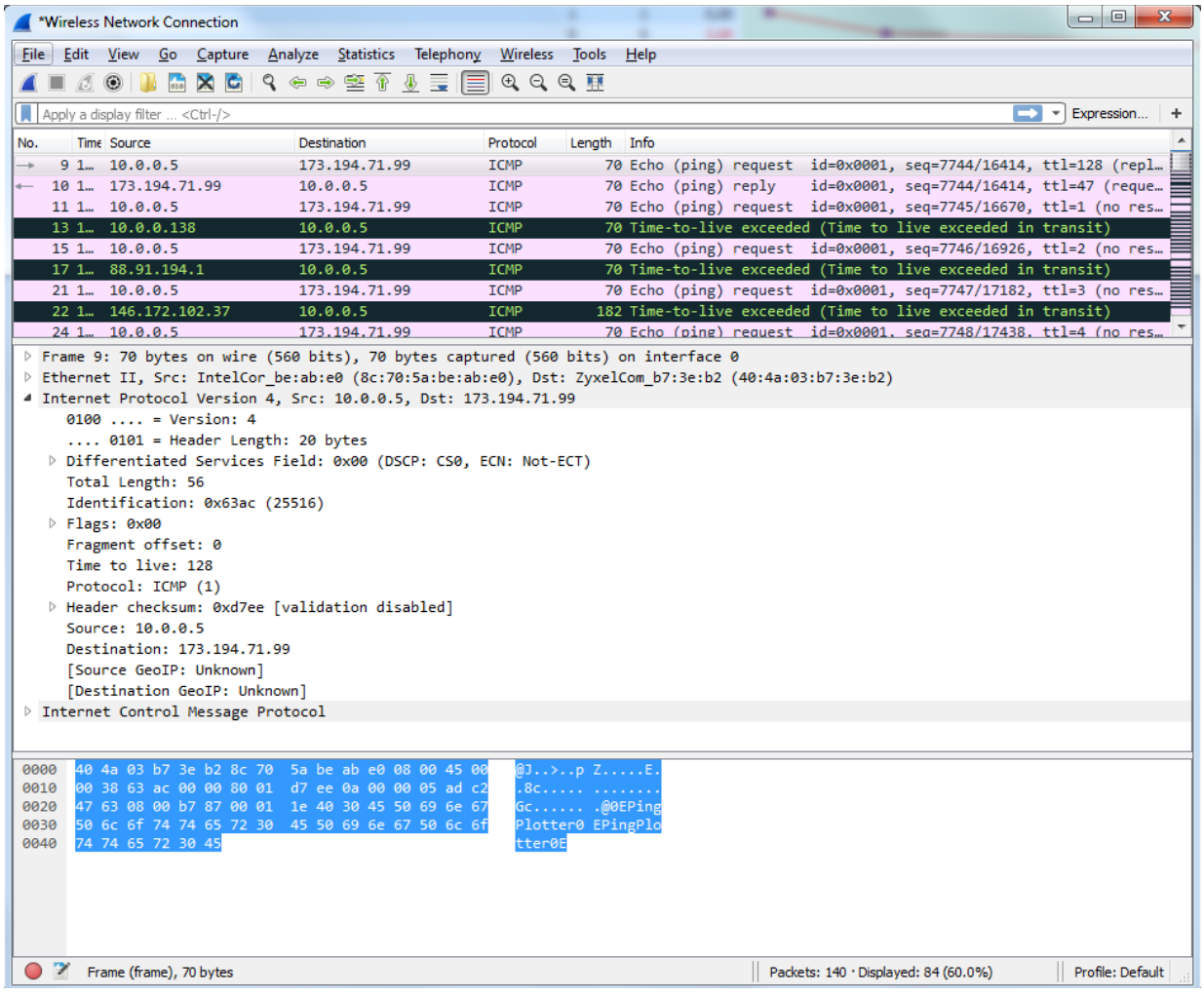

Figure 1: ICMP messages example trace.

2. How many bytes are in the IP header?

3. How many bytes are in the payload *of the IP datagram*?
4. Has this IP datagram been fragmented?

Next, sort the traced packets according to IP source address by clicking on the *Source* column header; a small downward pointing arrow should appear next to the word *Source*. If the arrow points up, click on the *Source* column header again. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the "details of selected packet header" window. In the "listing of captured packets" window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent by other protocols running on your computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by your computer.

5. Which fields in the IP datagram *always* change from one datagram to the next within this series of ICMP messages sent by the client?
6. Which fields stay constant?

Next (with the packets still sorted by source address) find the series of ICMP TTL-exceeded replies sent to the client by the nearest (**first hop**) router. You can look in the ICMP part of the message to find the response to the first message sent by the client.

7. What is the value in the Identification field?
8. What is the value in the TTL field?

Fragmentation

Sort the packet listing according to time again by clicking on the *Time* column. To see fragmentation, you will have to remove the "icmp" filter.

9. Find the first ICMP Echo Request message that was sent the client after the *Packet Size* was changed to a larger number. Has that message been fragmented across more than one IP datagram?