Sample Lab Report

Lab Exercise 3: Wireshark Installation and Introduction

Answers to questions:

1. The frame length of an ICMP Echo Request/ping should be 74 bytes overall for Windows (not including the preamble). For a Linux or macOS device, it will be 98 bytes.

2. Verify the source and destination Ethernet addresses are in 6-byte hex format, similar to:

Source: 00:04:5a:83:b6:4c

Destination: 00:06:25:04:ce:e1

3. In most cases, Wireshark will be able to determine the adapter manufacturer, as in…

Source: Hewlett-_1f:0c:4d (18:a9:05:1f:0c:4d)

…which indicates a Hewlett Packard adapter.

If not, they'll have to look up the 3-byte vendor code at *standards.ieee.org/regauth/oui/oui.txt*.

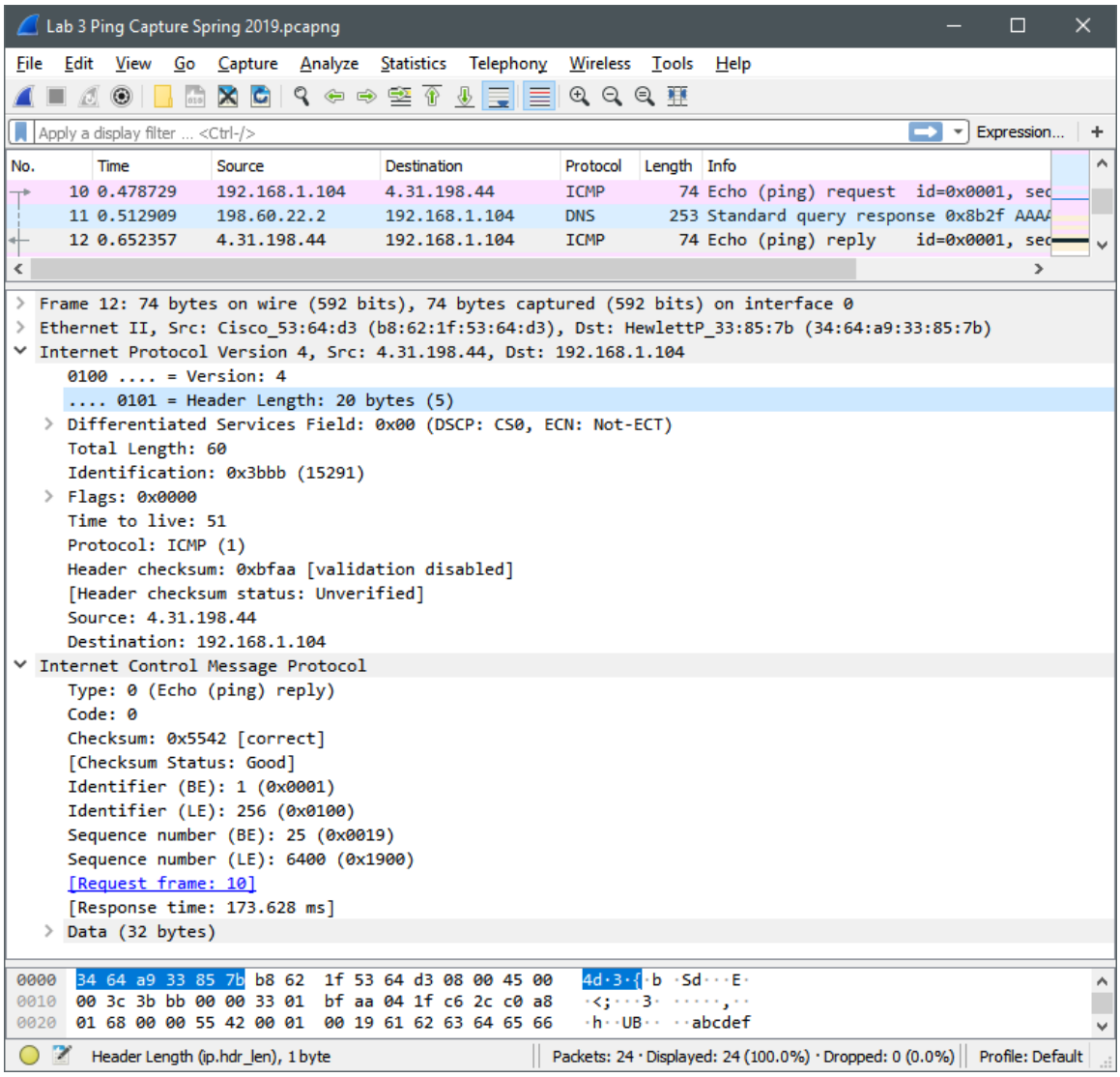
4. Type will be 0x0800 (IPv4).

5. IP Version = 4. Header length will normally be 20 bytes.

6. IP source and destination addresses could be anything. They should be shown in dotted decimal form, like this: 192.168.1.15 and 74.125.224.101.

7. ICMP Echo Request Type = 8. Echo Reply Type = 0.

8. Must include a screenshot of the ICMP Echo Reply frame, similar to the one shown below.



Lab Test Log

3/3/17 Used Wireshark v2.2.5 on macOS Sierra.

10/20/18 Used Wireshark v2.6 on Windows 10 with WinPcap v4.1.3.

3/1/19 Used Wireshark 3.0.0 on Windows 10 with Npcap 0.99