

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 3 Ping Capture Spring 2019.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
10	0.478729	192.168.1.104	4.31.198.44	ICMP	74	Echo (ping) request id=0x0001, seq=0x0000
11	0.512909	198.60.22.2	192.168.1.104	DNS	253	Standard query response 0x8b2f AAAA
12	0.652357	4.31.198.44	192.168.1.104	ICMP	74	Echo (ping) reply id=0x0001, seq=0x0000

> Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

> Ethernet II, Src: Cisco_53:64:d3 (b8:62:1f:53:64:d3), Dst: HewlettP_33:85:7b (34:64:a9:33:85:7b)

▼ Internet Protocol Version 4, Src: 4.31.198.44, Dst: 192.168.1.104

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 60
 - Identification: 0x3bbb (15291)
- > Flags: 0x0000
 - Time to live: 51
 - Protocol: ICMP (1)
 - Header checksum: 0xbfaa [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 4.31.198.44
 - Destination: 192.168.1.104
- ▼ Internet Control Message Protocol
 - Type: 0 (Echo (ping) reply)
 - Code: 0
 - Checksum: 0x5542 [correct]
 - [Checksum Status: Good]
 - Identifier (BE): 1 (0x0001)
 - Identifier (LE): 256 (0x0100)
 - Sequence number (BE): 25 (0x0019)
 - Sequence number (LE): 6400 (0x1900)
 - [\[Request frame: 10\]](#)
 - [Response time: 173.628 ms]
 - > Data (32 bytes)

```

0000 34 64 a9 33 85 7b b8 62 1f 53 64 d3 08 00 45 00 4d 33 85 7b 34 64 a9 33 85 7b
0010 00 3c 3b bb 00 00 33 01 bf aa 04 1f c6 2c c0 a8 <<...3... ..,..
0020 01 68 00 00 55 42 00 01 00 19 61 62 63 64 65 66 .h..UB... ..abcdef

```

Header Length (ip.hdr_len), 1 byte | Packets: 24 · Displayed: 24 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

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