Name: SUSHANT BAGUL

ROLL-NO: 221070011

BATCH-A-CS

Experiment 8

Aim: To analyze the ICMP messages generated by the Ping program

The Ping program is a simple tool that allows anyone 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. Both of these Ping packets are ICMP packets.

Do the following

Let's begin by opening the Windows Command Prompt application. •

Start up the Wireshark packet sniffer, and begin Wireshark packet capture.

• Type —ping –n 10 hostname‖ in the MS-DOS command line (without quotation marks), where hostname is a host on another continent. The argument —-n 10‖ indicates that 10 ping messages should be sent. Then run the Ping program by typing return.

• When the Ping program terminates, stop the packet capture in Wireshark. At the end of the experiment, your Command Prompt Window should look something like Figure 1. In this example, the source ping program is in Massachusetts and the destination Ping program is in Hong Kong. From this window we see that the source ping program sent 10 query packets and received 10 responses. Note also that for each response, the source calculates

the round-trip time (RTT), which for the 10 packets is on average 375 msec.

```
sysadmin@sysadmin:~$ ping -c 10 www.hkust.edu.hk
PING www.ust.hk (143.89.12.134) 56(84) bytes of data.
64 bytes from www.ust.hk (143.89.12.134): icmp_seq=1 ttl=50 time=286 ms
64 bytes from www.ust.hk (143.89.12.134): icmp_seq=2 ttl=50 time=226 ms
64 bytes from www.ust.hk (143.89.12.134): icmp_seq=3 ttl=50 time=320 ms
64 bytes from www.ust.hk (143.89.12.134): icmp_seq=4 ttl=50 time=201 ms
64 bytes from www.ust.hk (143.89.12.134): icmp_seq=5 ttl=50 time=293 ms
64 bytes from www.ust.hk (143.89.12.134): icmp_seq=6 ttl=50 time=420 ms
64 bytes from www.ust.hk (143.89.12.134): icmp_seq=7 ttl=50 time=309 ms
64 bytes from www.ust.hk (143.89.12.134): icmp_seq=8 ttl=50 time=263 ms
64 bytes from www.ust.hk (143.89.12.134): icmp_seq=9 ttl=50 time=283 ms
64 bytes from www.ust.hk (143.89.12.134): icmp_seq=10 ttl=50 time=211 ms

--- www.ust.hk ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9011ms
rtt min/avg/max/mdev = 201.241/281.310/419.752/60.248 ms
```

Figure 1 Command Prompt window after entering Ping command. Figure 2 provides a screenshot of the Wireshark output, after —icmpll has been entered into the filter display window. Note that the packet listing shows 20 packets: the 10 Ping queries sent by the source and the 10 Ping responses received by the source. Also note that the source's IP address is a private address of the form 192.168/12; the destination's IP address is that of the Web server at HKUST. Now let's zoom in on the first packet (sent by the client); in the figure below, the packet contents area provides information about this packet. We see that the IP datagram within this packet has protocol number 01, which is the protocol number for ICMP. This means that the payload of the IP datagram is an ICMP packet.

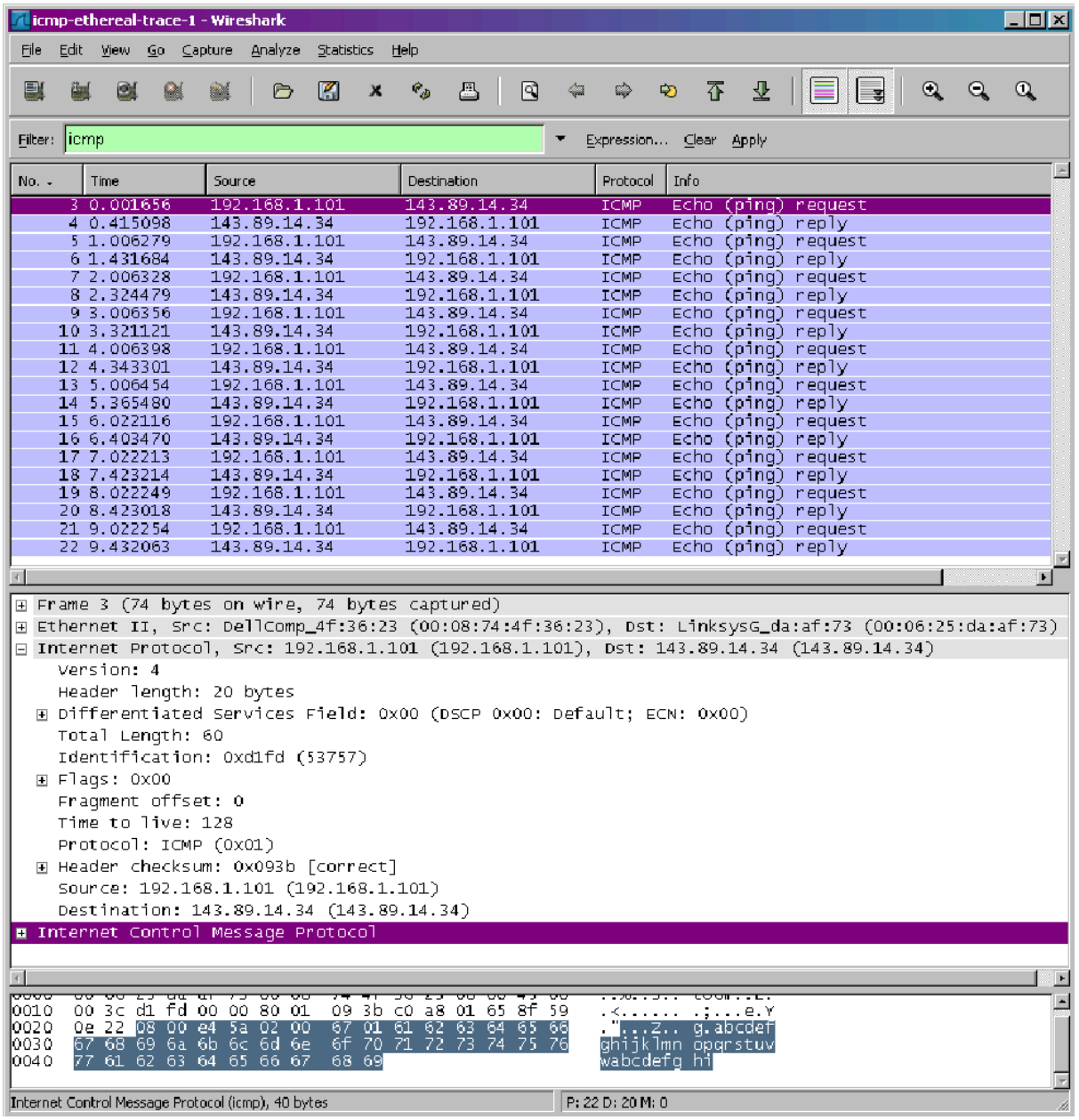
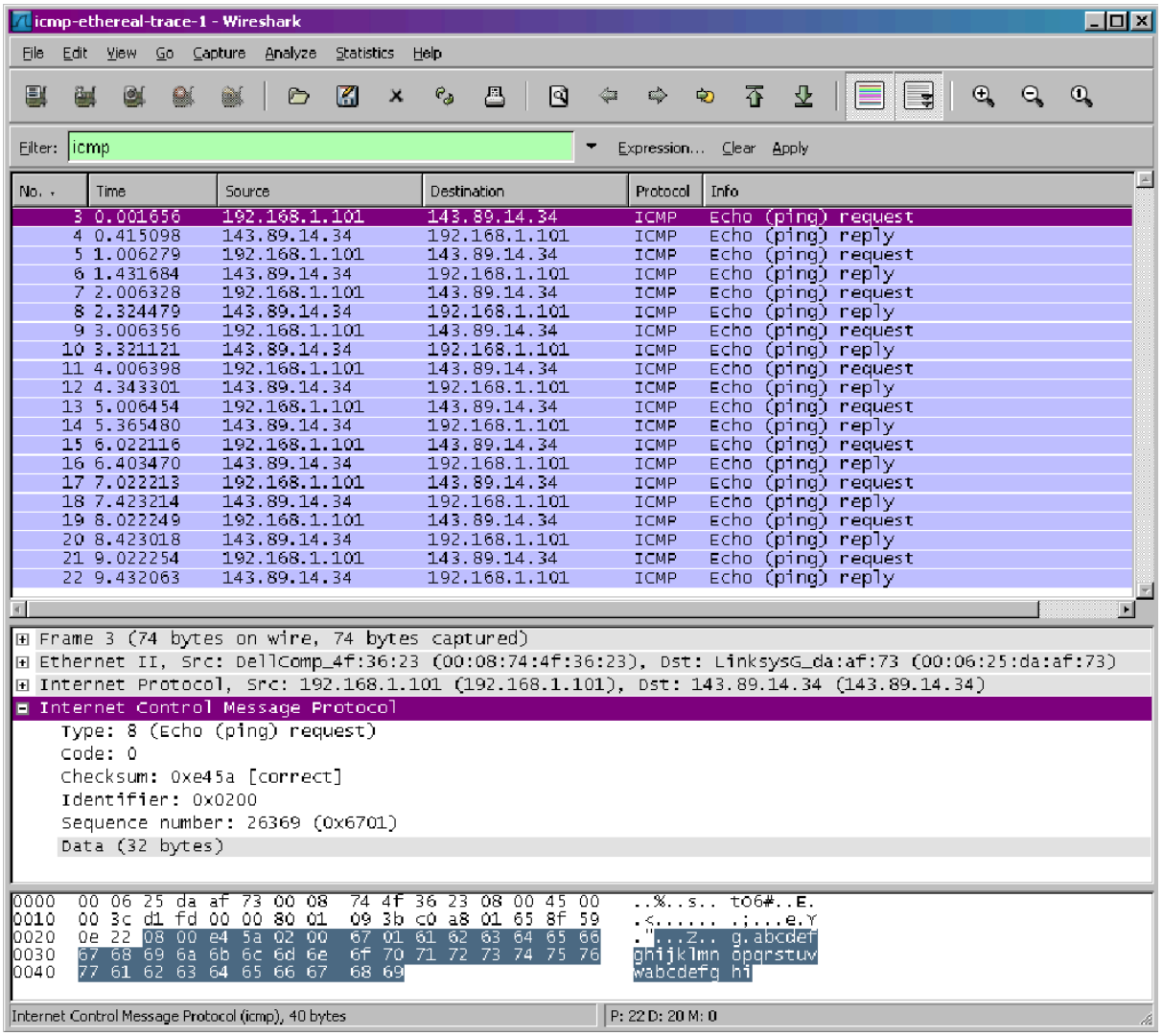


Figure 2 Wireshark output for Ping program with Internet Protocol expanded. Figure 3 focuses on the same ICMP but has expanded the ICMP protocol information in the packet contents window. Observe that this ICMP packet is of Type 8 and Code 0 - a so-called ICMP —echo requestll packet. Also note that this ICMP packet contains a checksum, an identifier, and a sequence number



What to do:

You should hand in a screen shot of the Command Prompt window similar to Figure 1 above. You should answer the following questions:

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?

Conclusion: Thus we have generated ICMP packets using ping and analyzed their contents