Wireshark Lab:

ICMP

v

8

.0

Supplement to

*Computer Networking: A Top*

*-*

*Down*

*Approach,*

*8*

*th*

*ed.*

*,*

J.F. Kurose and K.W. Ross

*“Tell me and I forget. Show me and I remember. Involve me*

*and I understand.”*

Chinese proverb

©

2005

-

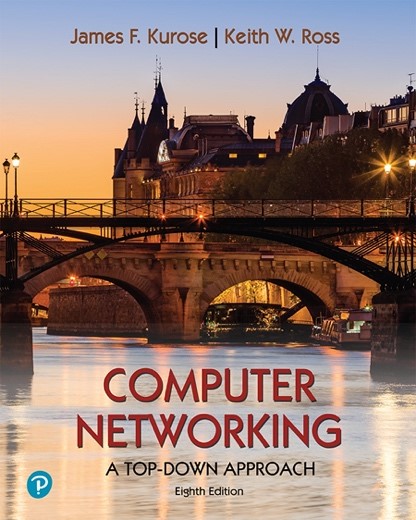
20

20

, J.F Kurose and K.W. Ross, Al

l

Rights Reserved



In this lab, we’ll explore several aspects of the ICMP protocol:

* ICMP messages generating by the Ping program; • ICMP messages generated by the Traceroute program;
* the format and contents of an ICMP message.

Before attacking this lab, you’re encouraged to review the ICMP material in section 5.6 of the text[[1]](#footnote-1). We present this lab in the context of the Microsoft Windows operating system. However, it is straightforward to translate the lab to a Unix or Linux environment.

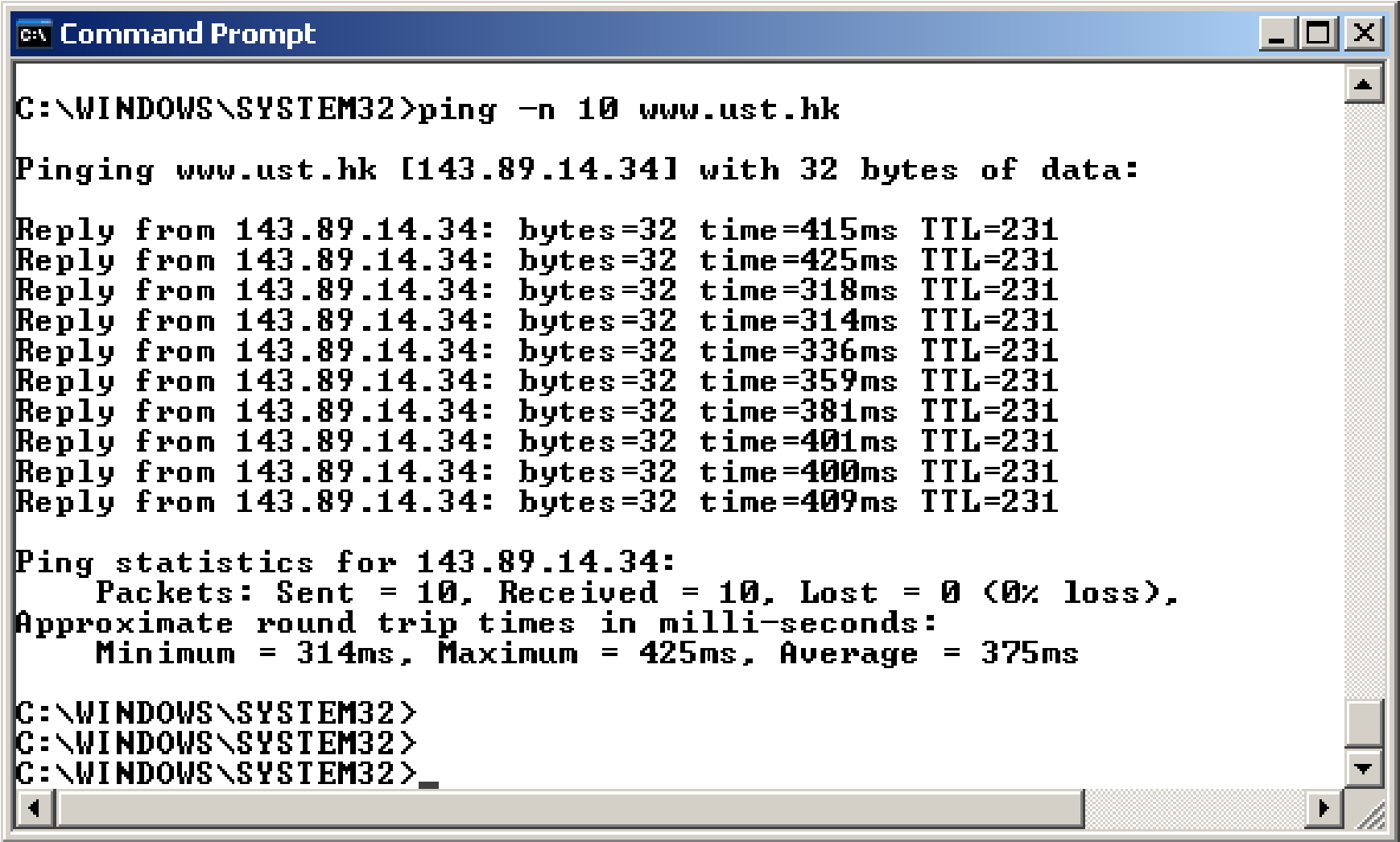
# ICMP and Ping

Let’s begin our ICMP adventure by capturing the packets generated by the Ping program. You may recall that the Ping program is simple tool that allows anyone (for example, a network administrator) 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. As you might have guessed (given that this lab is about ICMP), both of these Ping packets are ICMP packets.

Do the following[[2]](#footnote-2):

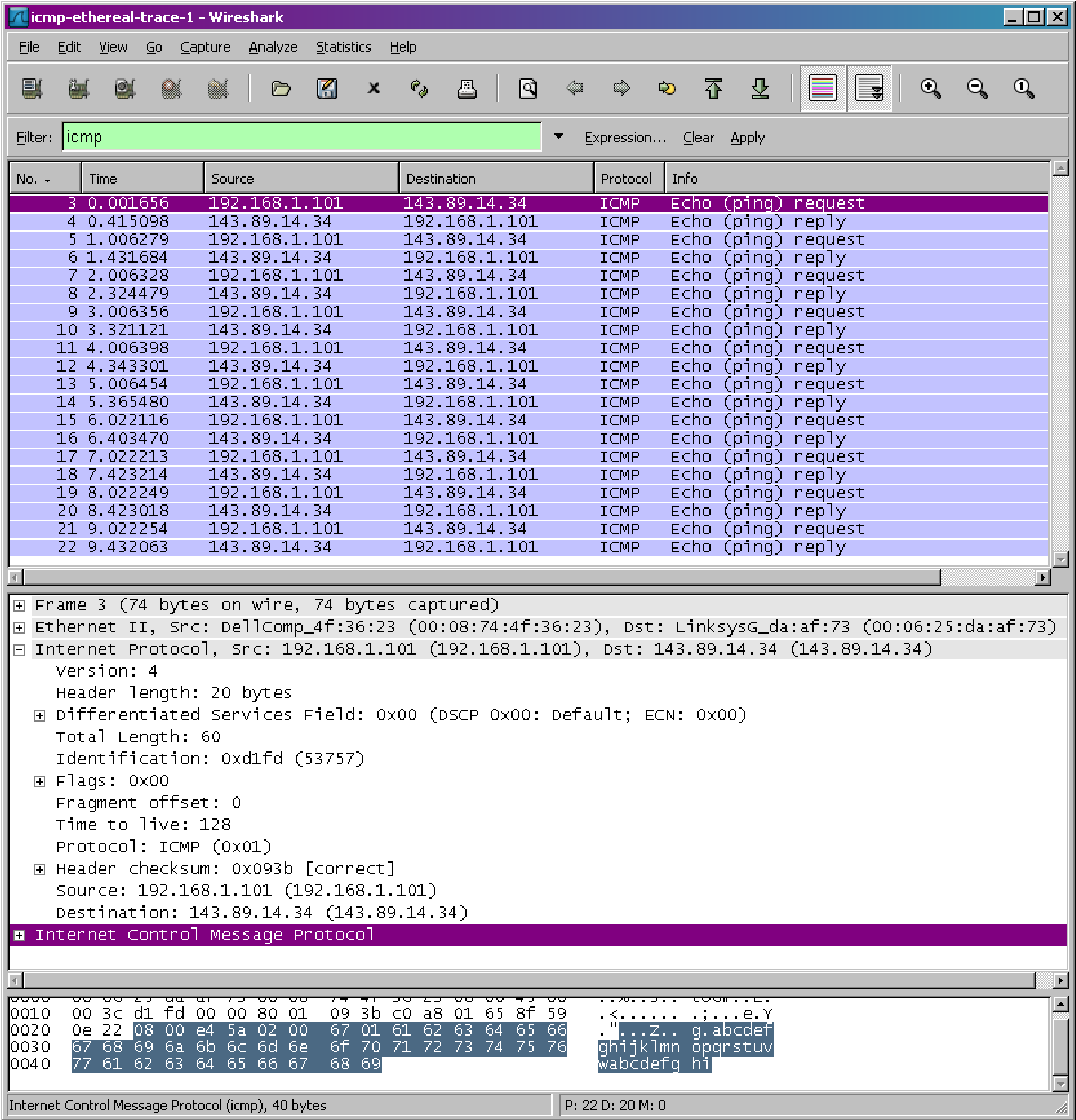
* Let’s begin this adventure by opening the Windows Command Prompt application (which can be found in your Accessories folder).
* Start up the Wireshark packet sniffer, and begin Wireshark packet capture.
* The *ping* command is in c:\windows\system32, so type either “*ping –n 10 hostname*” or “*c:\windows\system32\ping –n 10 hostname*” in the MS-DOS command line (without quotation marks), where hostname is a host on another continent. If you’re outside of Asia, you may want to enter www.ust.hk for the Web server at Hong Kong University of Science and Technology. 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.



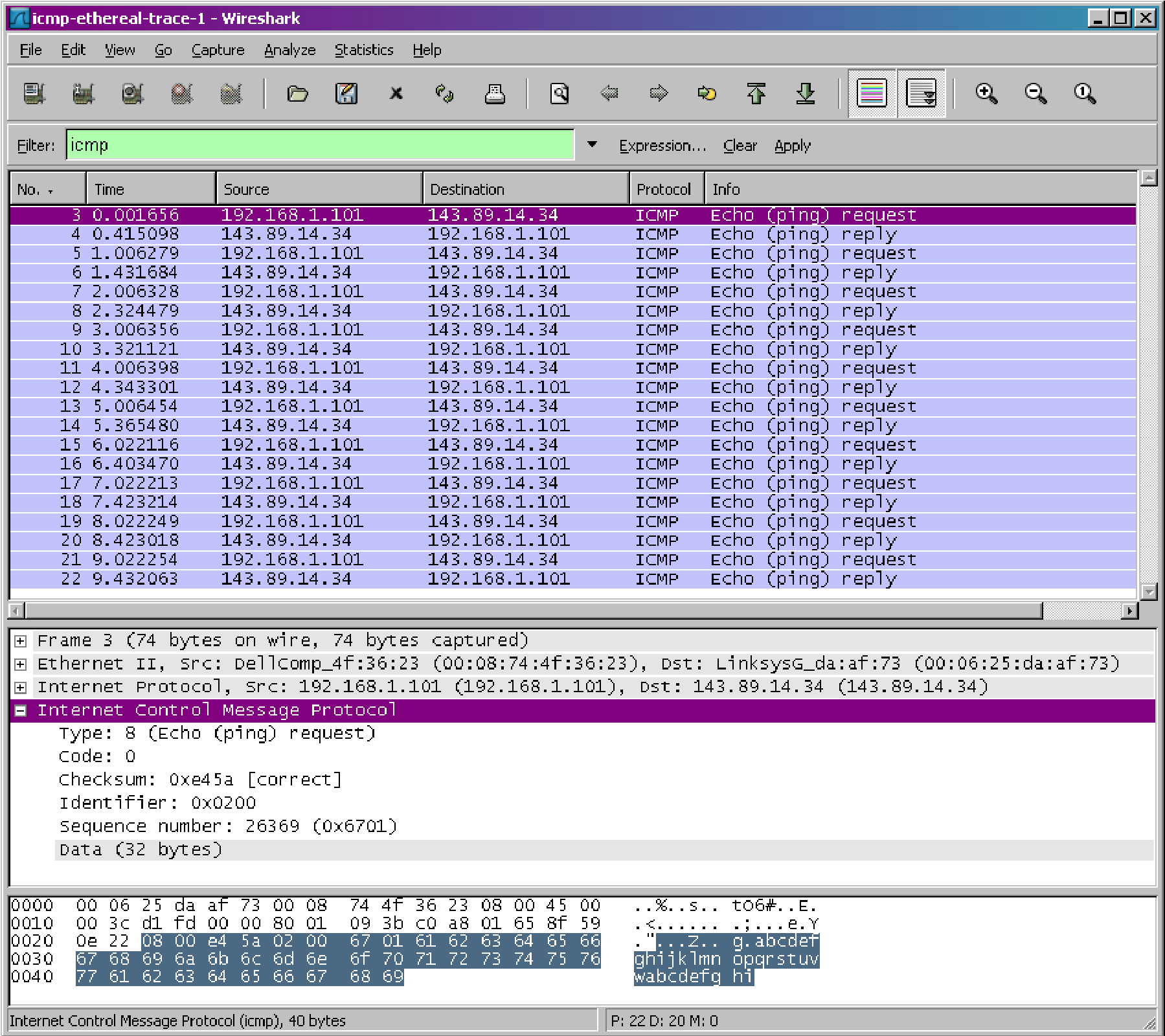
**Figure 1** Command Prompt window after entering Ping command.

Figure 2 provides a screenshot of the Wireshark output, after “icmp” 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 (behind a NAT) 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.



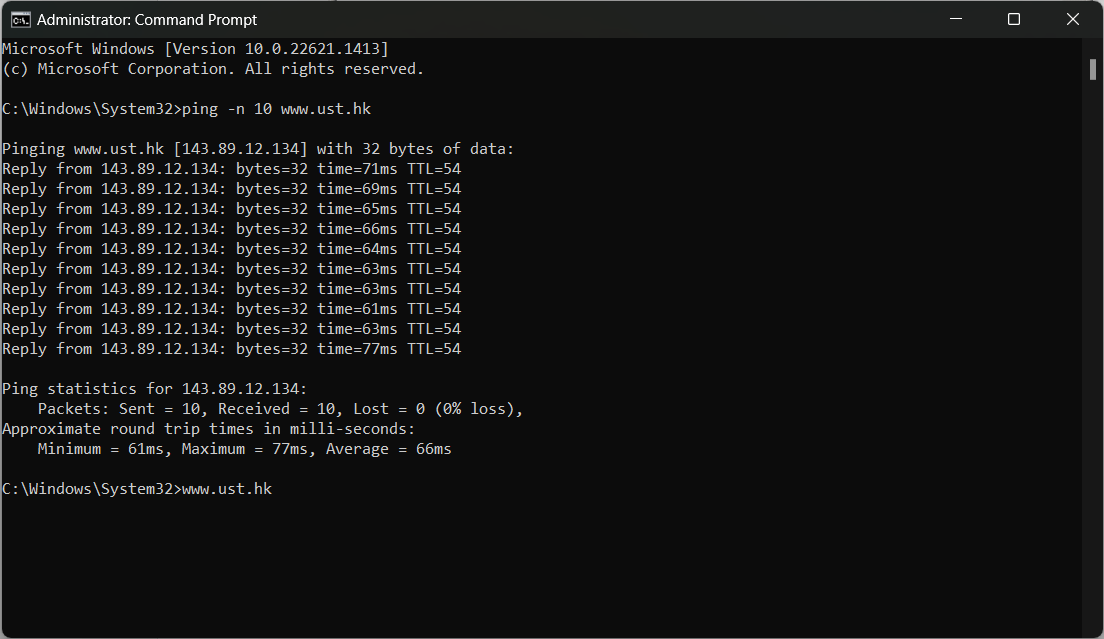
**Figure 2** Wireshark output for Ping program with Internet Protocol expanded.

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 request” packet. (See Figure 5.19 of text.) Also note that this ICMP packet contains a checksum, an identifier, and a sequence number.



**Figure 3** Wireshark capture of ping packet with ICMP packet expanded.

**What to Hand In:**



You should hand in a screen shot of the Command Prompt window similar to Figure 1 above. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout[[3]](#footnote-3) to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line,* and select the minimum amount of packet detail that you need to answer the question.

You should answer the following questions:

1. What is the IP address of your host? What is the IP address of the destination host?

The IP address of my host is 172.17.37.93

The IP address of the destination host is 143.89.12.134

1. Why is it that an ICMP packet does not have source and destination port numbers?

The ICMP packet does not have source and destination port numbers because it was designed to commuicate network-layer information between application layer processes. Each ICMP packet has a “Type” and a “Code”. The Type/Code combination indentifies the specific message being received. Since the network software itself interprets all ICMP messages, no port numbers are needed to direct the ICMP message to an application layer process.

Graphical user interface, text, application

Description automatically generated

1. 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?

Graphical user interface, application, Word

Description automatically generated

The ICMP type is 8, and the code number is 0.

The ICMP packet also has checksum, indetifier, sequence number and data field. The checksum, sequence number and identifier fields are two bytes each.

1. 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?

Graphical user interface, application, Word

Description automatically generated

The ICMP type is 0, and the code number is 0.

The ICMP packet also has checksum, indetifier, sequence number and data field. The checksum, sequence number and identifier fields are two bytes each.

# ICMP and Traceroute

Let’s now continue our ICMP adventure by capturing the packets generated by the Traceroute program. You may recall that the Traceroute program can be used to figure out the path a packet takes from source to destination. Traceroute is discussed in Section 1.4 and in Section 5.6 of the text.

Traceroute is implemented in different ways in Unix/Linux/MacOS and in Windows. In Unix/Linux, the source sends a series of UDP packets to the target destination using an unlikely destination port number; in Windows, the source sends a series of ICMP packets to the target destination. For both operating systems, the program sends the first packet with TTL=1, the second packet with TTL=2, and so on. Recall that a router will decrement a packet’s TTL value as the packet passes through the router. When a packet arrives at a router with TTL=1, the router sends an ICMP error packet back to the source. In the following, we’ll use the native Windows *tracert* program. A shareware version of a much nice Windows Traceroute program is *pingplotter* (www.pingplotter.com). We’ll use *pingplotter* in our Wireshark IP lab since it provides additional functionality that we’ll need there.

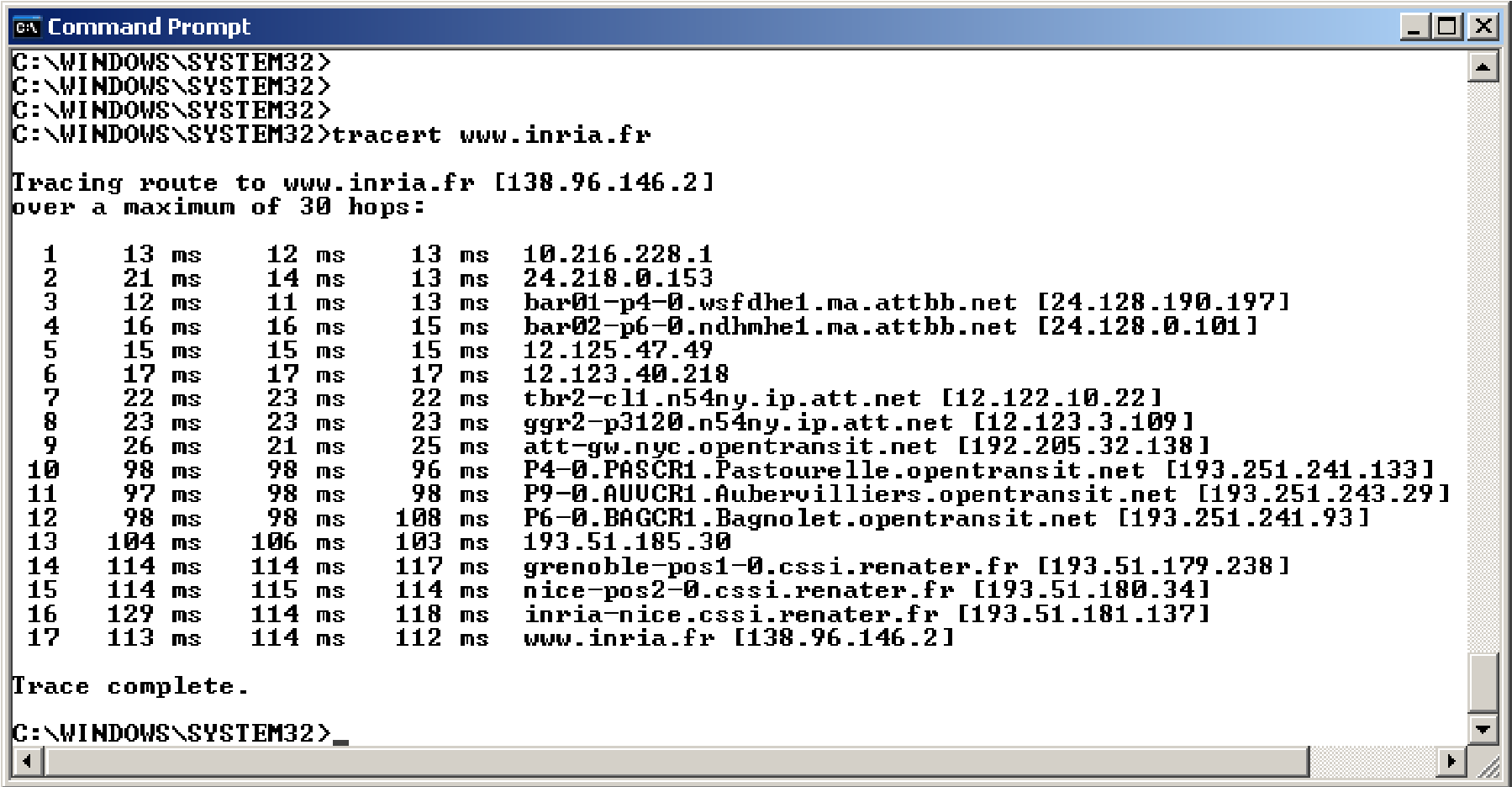
Do the following[[4]](#footnote-4):

* Let’s begin by opening the Windows Command Prompt application (which can be found in your Accessories folder).
* Start up the Wireshark packet sniffer, and begin Wireshark packet capture.
* The *tracert* command is in c:\windows\system32, so type either “*tracert hostname*” or “*c:\windows\system32\tracert hostname*” in the MS-DOS command line (without quotation marks), where hostname is a host on another continent.

(Note that on a Windows machine, the command is “*tracert*” and not “*traceroute*”.) If you’re outside of Europe, you may want to enter www.inria.fr for the Web server at INRIA, a computer science research institute in France. Then run the Traceroute program by typing return.

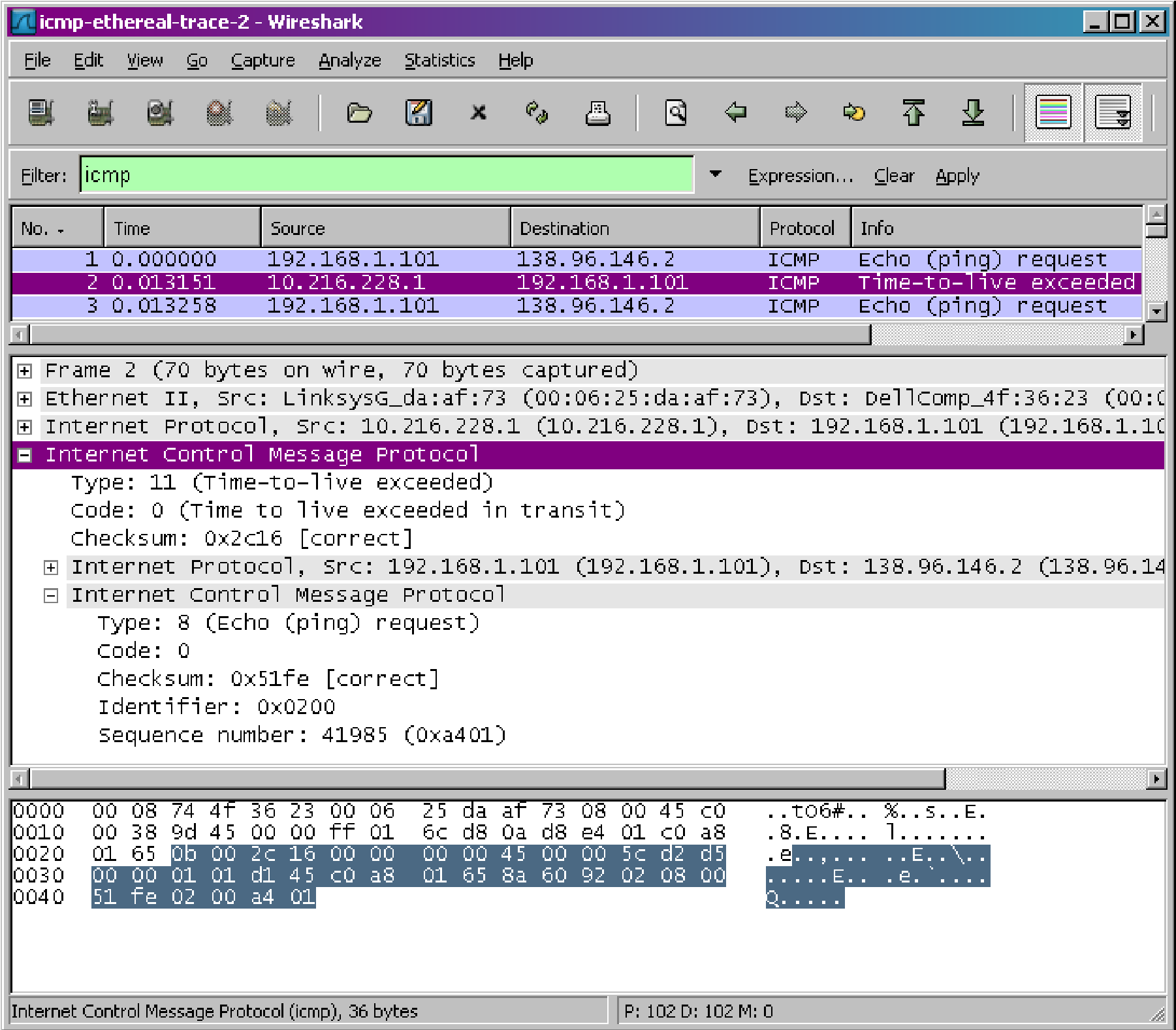
* When the Traceroute program terminates, stop packet capture in Wireshark.

At the end of the experiment, your Command Prompt Window should look something like Figure 4. In this figure, the client Traceroute program is in Massachusetts and the target destination is in France. From this figure we see that for each TTL value, the source program sends three probe packets. Traceroute displays the RTTs for each of the probe packets, as well as the IP address (and possibly the name) of the router that returned the ICMP TTL-exceeded message.



**Figure 4** Command Prompt window displays the results of the Traceroute program.

Figure 5 displays the Wireshark window for an ICMP packet returned by a router. Note that this ICMP error packet contains many more fields than the Ping ICMP messages.



**Figure 5** Wireshark window of ICMP fields expanded for one ICMP error packet.

**What to Hand In:**

For this part of the lab, you should hand in a screen shot of the Command Prompt window. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line,* and select the minimum amount of packet detail that you need to answer the question.

Answer the following questions:

Note: I use the file *icmp-ethereal-trace-2* for question, 5, 6, 7, 8, 9.

1. What is the IP address of your host? What is the IP address of the target destination host?

The IP address of my host is 192.168.1.101. The IP address of the destination host is 138.96.146.2

Application

Description automatically generated with low confidence

1. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

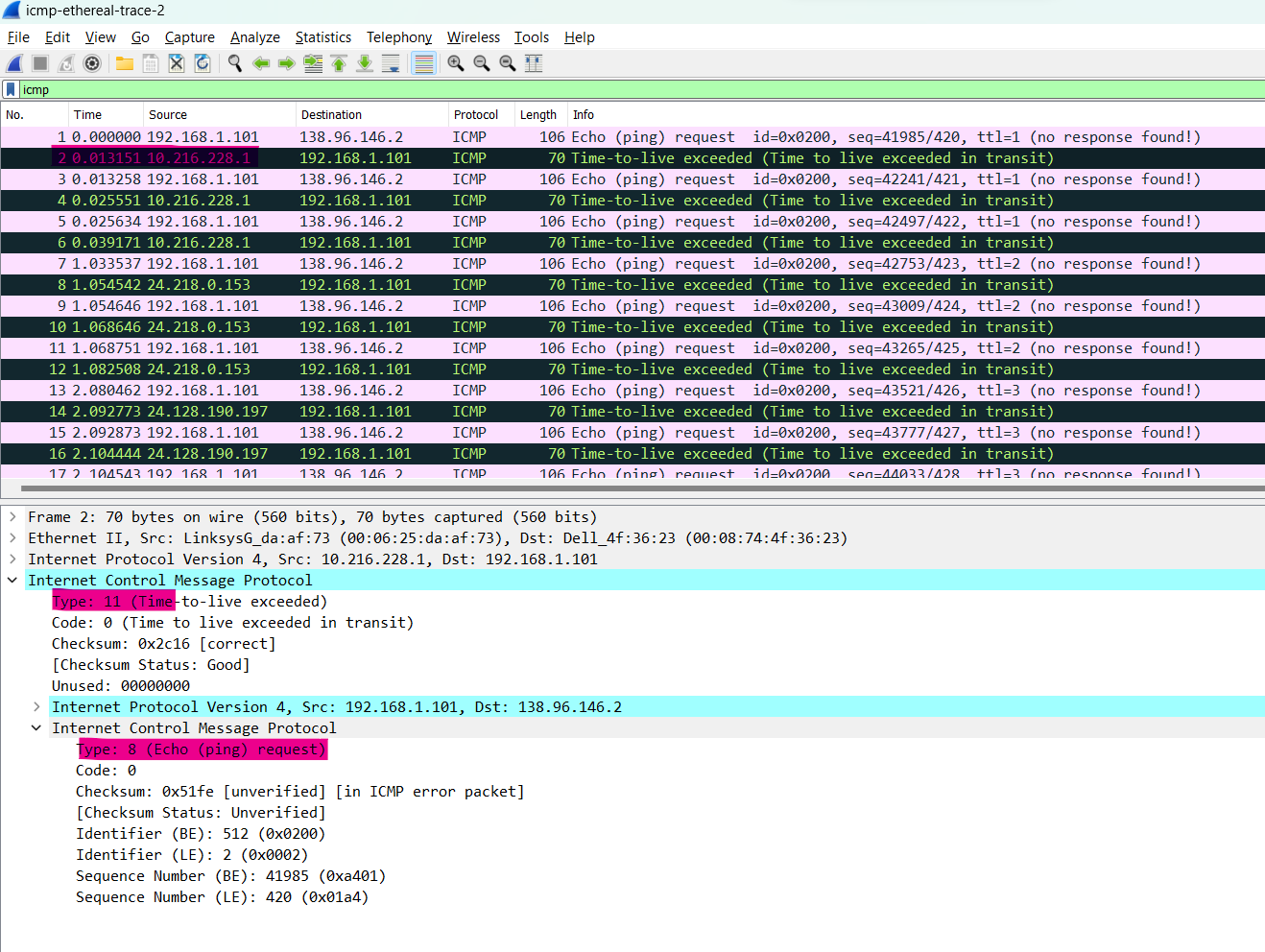
No. If ICMP sent UDP packets instead, the IP protocol number should be 0x11

1. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?

The ICMP echo packet has the same fields as the ping query packets.

1. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

The ICMP error packet is not the same as the ping query packets. It contains both the IP header and the first 8 bytes of the original ICMP packet that the error is for.



1. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

The last three ICMP packets are message type 0 (echo reply) rather than 11 (TTL expired). They are different because the datagrams have made it all the way to the destination host before the TTL expired.

Text

Description automatically generated

1. Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?

In figure 4 from the lab, the link is from New York to Pastourelle, France.

# Extra Credit

For one of the programming assignments you created a UDP client ping program. This ping program, unlike the standard ping program, sends UDP probe packets rather than ICMP probe packets. Use the client program to send a UDP packet with an unusual destination port number to some live host. At the same time, use Wireshark to capture any response from the target host. Provide a Wireshark screenshot for the response as well as an analysis of the response.

1. References to figures and sections are for the 8h edition of our text, *Computer Networks, A Top-down Approach, 8th ed.,* J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2020. [↑](#footnote-ref-1)
2. If you are unable to run Wireshark live on a computer, you can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file *ICMP-ethereal-trace-1*. The traces in this zip file were collected by Wireshark running on one of the author’s computers, while performing the steps indicated in the Wireshark lab. Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the *ICMP-ethereal-trace-1* trace file. You can then use this trace file to answer the questions below. [↑](#footnote-ref-2)
3. What do we mean by “annotate”? If you hand in a paper copy, please highlight where in the printout you’ve found the answer and add some text (preferably with a colored pen) noting what you found in what you ‘ve highlight. If you hand in an electronic copy, it would be great if you could also highlight and annotate. [↑](#footnote-ref-3)
4. If you are unable to run Wireshark live on a computer, you can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file *ICMP-ethereal-trace-2*. The traces in this zip file were collected by Wireshark running on one of the author’s computers, while performing the steps indicated in the Wireshark lab. Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the *ICMP-ethereal-trace-2* trace file. You can then use this trace file to answer the questions below. [↑](#footnote-ref-4)