|  |
| --- |
| Wireshark Lab - 2: ICMP  Version: March 2016  © Jinwei Cao. All Rights Reserved. Adapted from © 2005 J.F. Kurose, K.W. Ross. |

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

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

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.

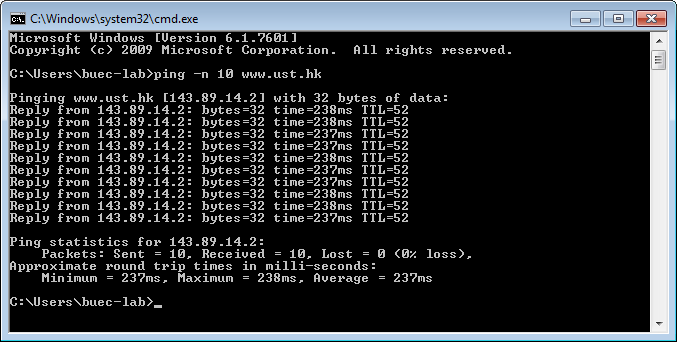
Part I. ICMP and Ping

Let’s begin our ICMP adventure by capturing the packets generated by the Ping program. You may recall that the Ping program is a 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[[1]](#footnote-1):

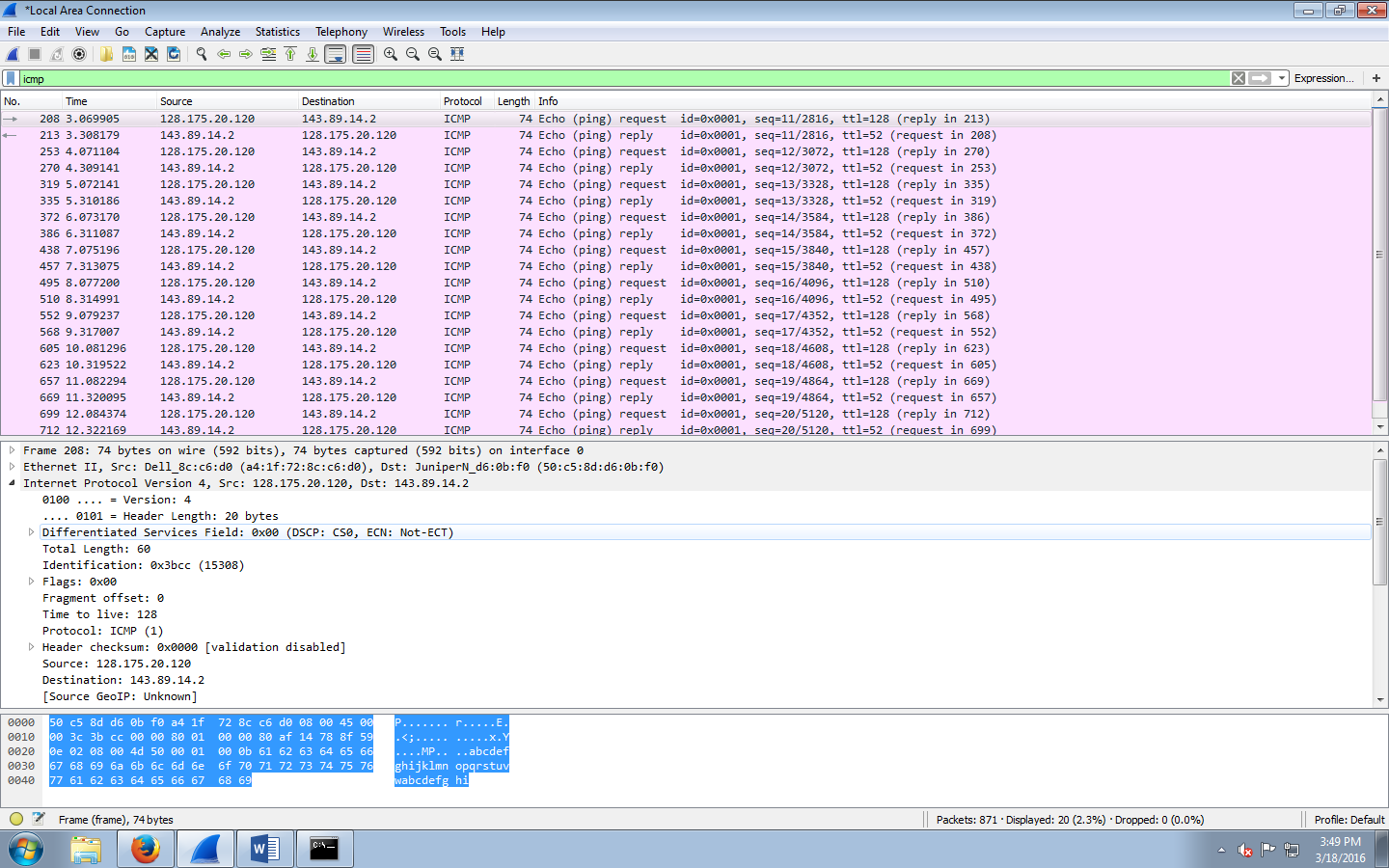
* Let’s begin this adventure by opening the Windows Command Prompt application (which can be found in your Accessories folder).
* Start up the Wireshark packet sniffer, and begin Wireshark packet capture.
* The *ping* command is in c:\windows\system32, so type either “*ping –n 10 hostname*” or “*c:\windows\system32\ping –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 237 msec.



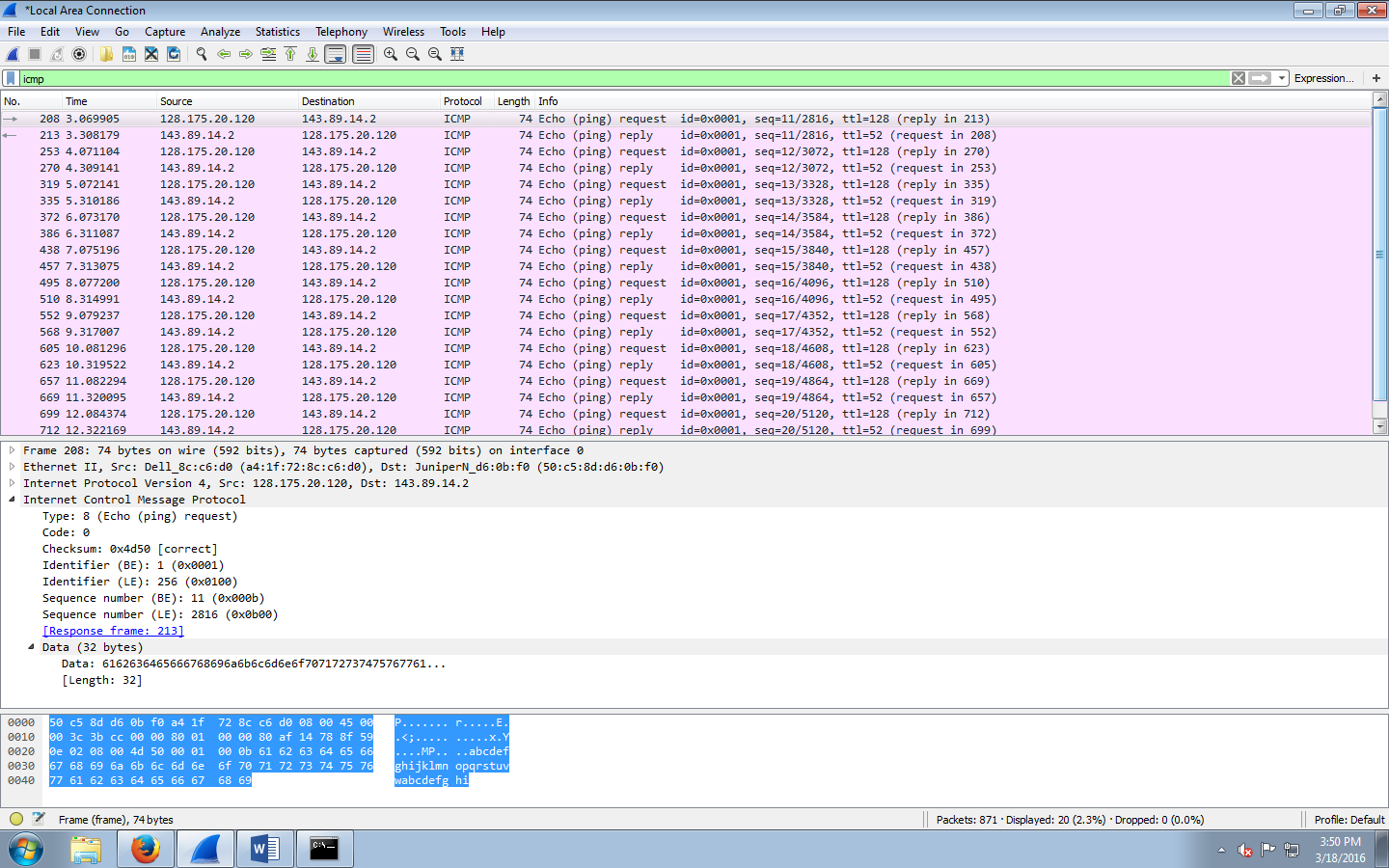
**Figure 1** Command Prompt window after entering Ping command.

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 128.175.20.120; 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 packet 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 (ping) request” packet. 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 screenshot of the Command Prompt window similar to Figure 1 above. Save the displayed packet(s) and answer the following questions.

Answer the following questions:

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

128.175.20.82

143.89.14.2

1. Does an ICMP packet have source and destination **port** numbers? Why?

No. port number is used in transport layer, but ICMP is in internet layer

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?

Type:8 code:0

Checksum fields, identifier,

1. Examine the corresponding ping **reply** packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have?

Type:0

Code:0

1. For the first ping request/reply cycle, calculate the Round Trip Time (RTT) based on the time field in the Wireshark packet trace. Compare it with the RTT listed in the Command Prompt window. Are they the same?

First RTT:0.247851 Yes they are the same

Part II. ICMP and Traceroute

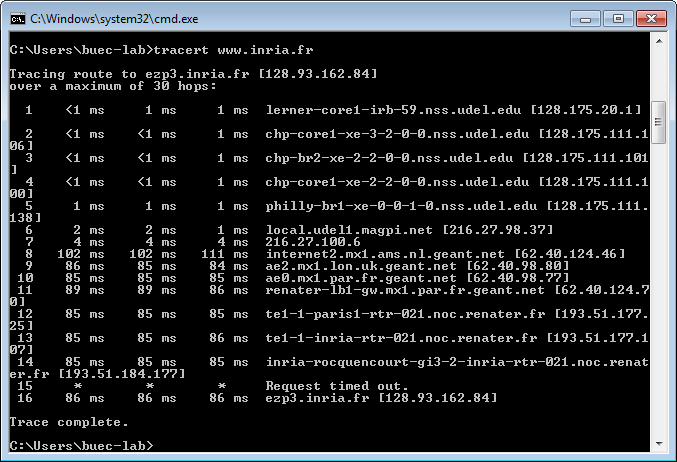
Let’s now continue our ICMP adventure by capturing the packets generated by the Traceroute program. You may recall that the Traceroute program can be used to figure out the path a packet takes from source to destination.

Traceroute is implemented in different ways in Unix/Linux 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 decrement this TTL value to 0, and then sends an ICMP error packet back to the source. In the following, we’ll use the native Windows *tracert* program to illustrate this process.

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

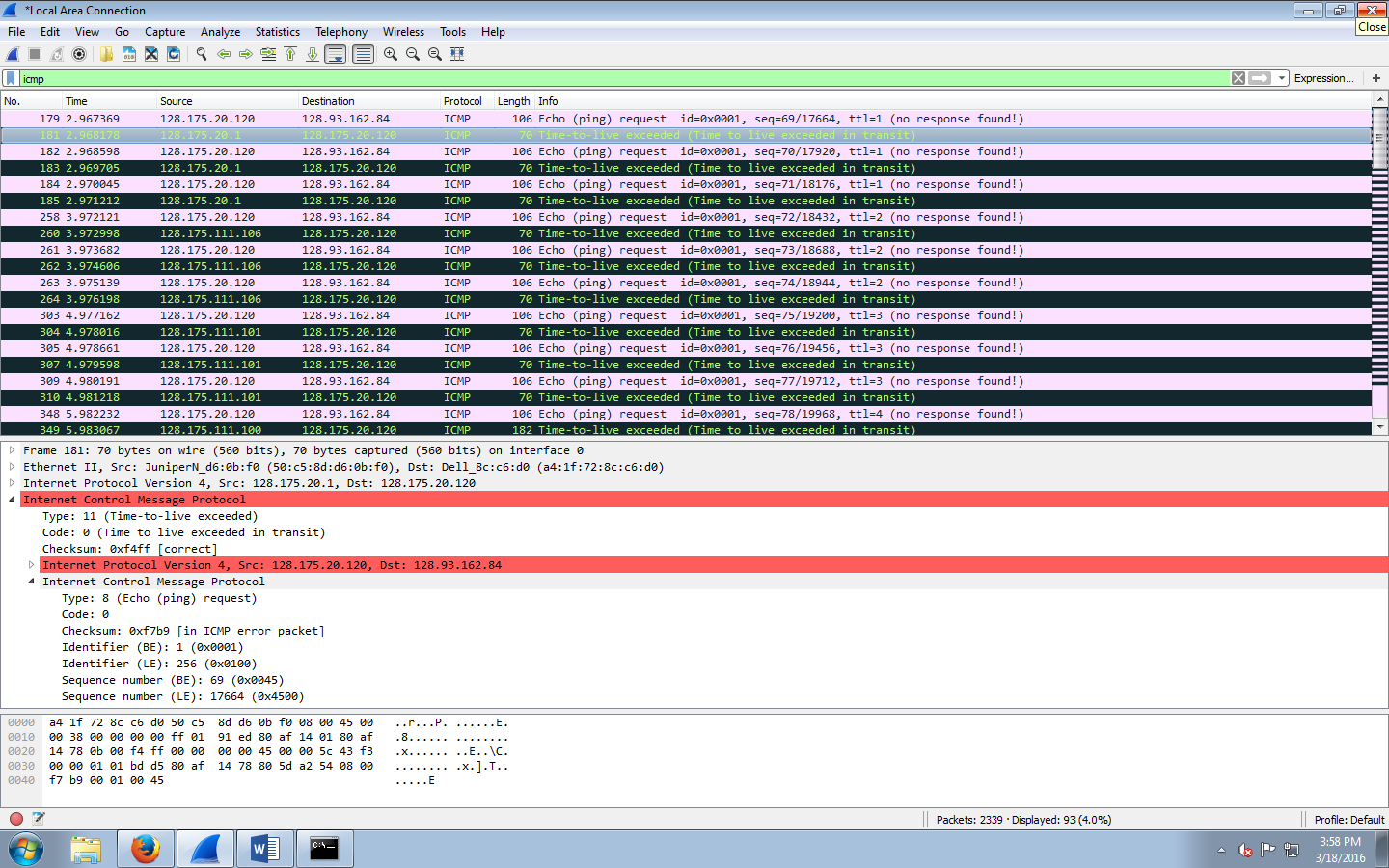
* Let’s begin by opening the Windows Command Prompt application (which can be found in your Accessories folder).
* Start up the Wireshark packet sniffer, and begin Wireshark packet capture.
* The *tracert* command is in c:\windows\system32, so type either “*tracert hostname*” or “*c:\windows\system32\tracert 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 if ICMP fields expanded for one ICMP error packet.

***What to hand in***

You should hand in a screenshot of the Command Prompt window similar to Figure 4 above. Save the displayed packet(s) and answer the following questions.

Answer the following questions:

1. What is the IP address of your host? What is the IP address of the target destination host?
2. Examine the ICMP **echo** packet in your captured packets. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?

Yes. Because in the first part, the TTL is the destination one while in this part the TTL is adding up

1. Examine the ICMP **error** packet in your captured packets. It has more fields than the ICMP echo packet. What are included in those fields?

Ping request in error message (a copy of the original request, because it causes the error). It tells where the error comes from

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?

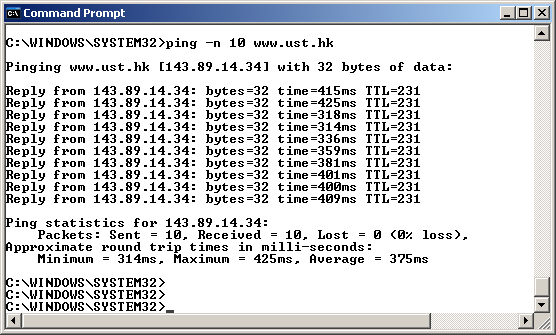
The color is different, and they reach the destination so they don’t return error messages

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?

Yes.

The Next Step

You can use Ping and Traceroute for some simple network troubleshooting. For example, if you are trying to ping a hostname but it fails, try to ping the IP address of this host. (You can get it from the ping result even though it fails.)



If ping fails when you try the name of the site, but works when you try the IP address, it's NOT a network problem, but DNS problem.

If both the name and the IP address fail, the following problems may exist.

1. **Your computer is not connected to the Internet.**   
   – How to find out? Check your wire or your wireless signal!
2. **Your computer’s TCP/IP protocol stack is damaged.**   
   – How to find out? Type “ping localhost” or “ping 127.0.0.1” (recall that 127.0.0.1 is the loopback IP address) in your Command Prompt window. If this ping command fails, you need to verify that your computer was restarted after TCP/IP was installed and configured. Or you might want to reinstall the TCP/IP protocol stack.
3. **Your computer’s IP address is not added to the network correctly.**– How to find out? Type “ping *IP\_address\_of\_local\_host*” (you can find your computer’s IP address by using the “ipconfig” utility) in your Command Prompt window. If this ping command fails, again you need to verify that your computer was restarted after TCP/IP was installed and configured.
4. **Your default gateway (router) is not working appropriately.**   
   – How to find out? Type “ping IP\_address\_of\_default\_gateway” (you can find the default gateway by using the “ipconfig” utility). If this ping command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.
5. **There is a routing problem and the destination network is unreachable.**– How to find out? If you know the IP address of another server that is in the same destination network, try to ping and traceroute to that server. If it is successful, you can rule out this problem.
6. Finally, the destination host may be **blocking ICMP packets**. Or, the destination host may **not exist on the network**. It could be disconnected, or turned off.  
   – How to find out? Contact the person who is taking charge of that destination host!

Now, try to ping “**be21-79.be.udel.edu**”, and identify possible problems with this host.

***What to hand in***

For this part of the lab, you should hand in the screenshot(s) of the Command Prompt window that display the steps you performed in this troubleshooting process.

Answer the following questions:

1. What is the IP address of this destination host? Is there a DNS problem? Why?
2. Are there any problems with your local computer? Why?
3. Are there any problems with your local network? Why?
4. You know that the server “**be21-72.be.udel.edu**” is in the same network as the destination host. Based on this information, can you find out the possible problems with this destination host? Specify these possible problems.

1. 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-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-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-2)