HW4 IP

HW rules:

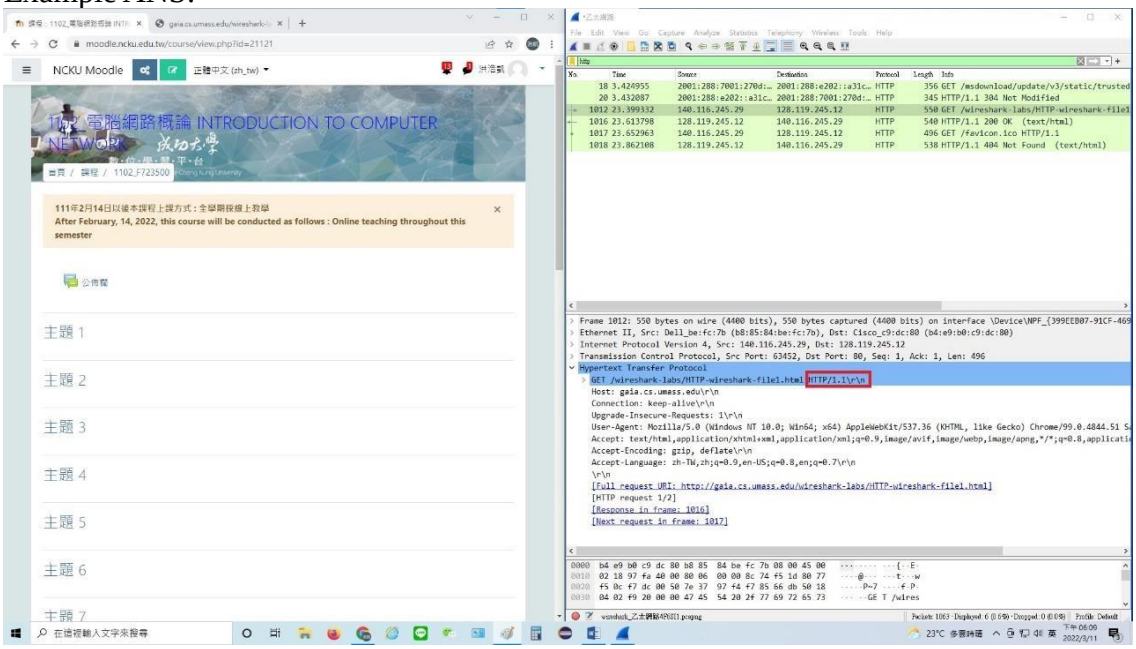
(Please take a screenshot to show your moodle and wireshark then highlight the answer or you will get no score.)

Note: Handing late will lead to a perceptibly lower score.

***Discussion is encouraged, but DO NOT share your homework to your classmate. If plagiarism is found, both students will get 0 score in this assignment.**

Example Question: Is your browser running HTTP version 1.0, 1.1, or 2? What versionof HTTP is the server running?

Example ANS:



Descriptions:

In this lab, we'll investigate the celebrated IP protocol, focusing on the IPv4. In the section, we'll analyze packets in a trace of IPv4 datagrams sent and received by the traceroute program (the traceroute program itself is explored in more detail in the Wireshark ICMP lab).

Capturing packets from an execution of traceroute

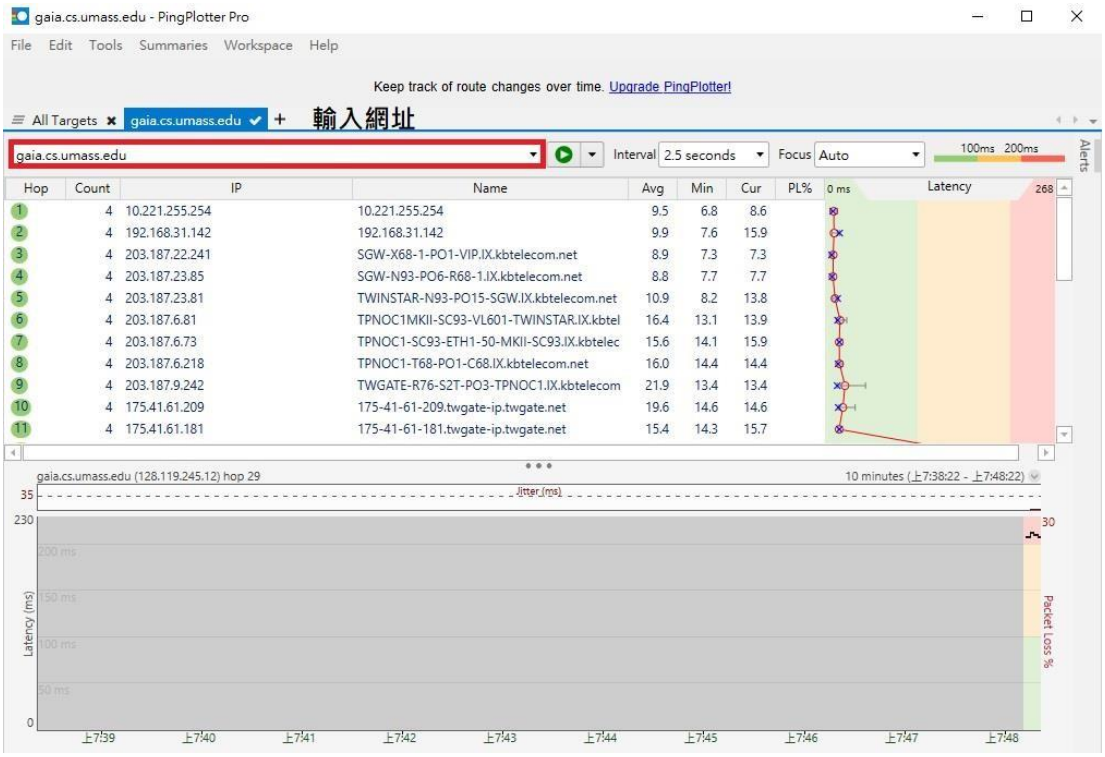
In order to generate a trace of IPv4 datagrams for the first two parts of this lab, we'll use the traceroute program to send datagrams of two different sizes to gaia.cs.umass.edu. Recall that traceroute operates by first sending one or more datagrams with the time- to-live (TTL) field in the IP header set to 1; it then sends a series of one or more datagrams towards the same destination with a TTL value of 2; it then sends a series of datagrams towards the same destination with a TTL value of 3; and so on. Recall that a router must decrement the TTL in each received datagram by 1 (actually, RFC 791 says that the router must decrement the TTL by at least one). If the TTL reaches 0, the router returns an ICMP message (type 11 – TTL-exceeded) to the sending host. As a result of this behavior, a datagram with a TTL of 1 (sent by the host executing traceroute) will cause the router one hop away from the sender to send an ICMP TTL-exceeded message back to the sender; the datagram sent with a TTL of 2 will cause the router two hops away to send an ICMP message back to the sender; the datagram sent with a TTL of 3 will cause the router three hops away to send an ICMP message back to the sender; and so on. In this manner, the host executing traceroute can learn the IP addresses of the routers between itself and the destination by looking at the source IP addresses in the datagrams containing the ICMP TTL-exceeded messages.

Let's run traceroute and have it send datagrams of two different sizes. The larger of the two datagram lengths will require traceroute messages to be fragmented across multiple IPv4 datagrams.

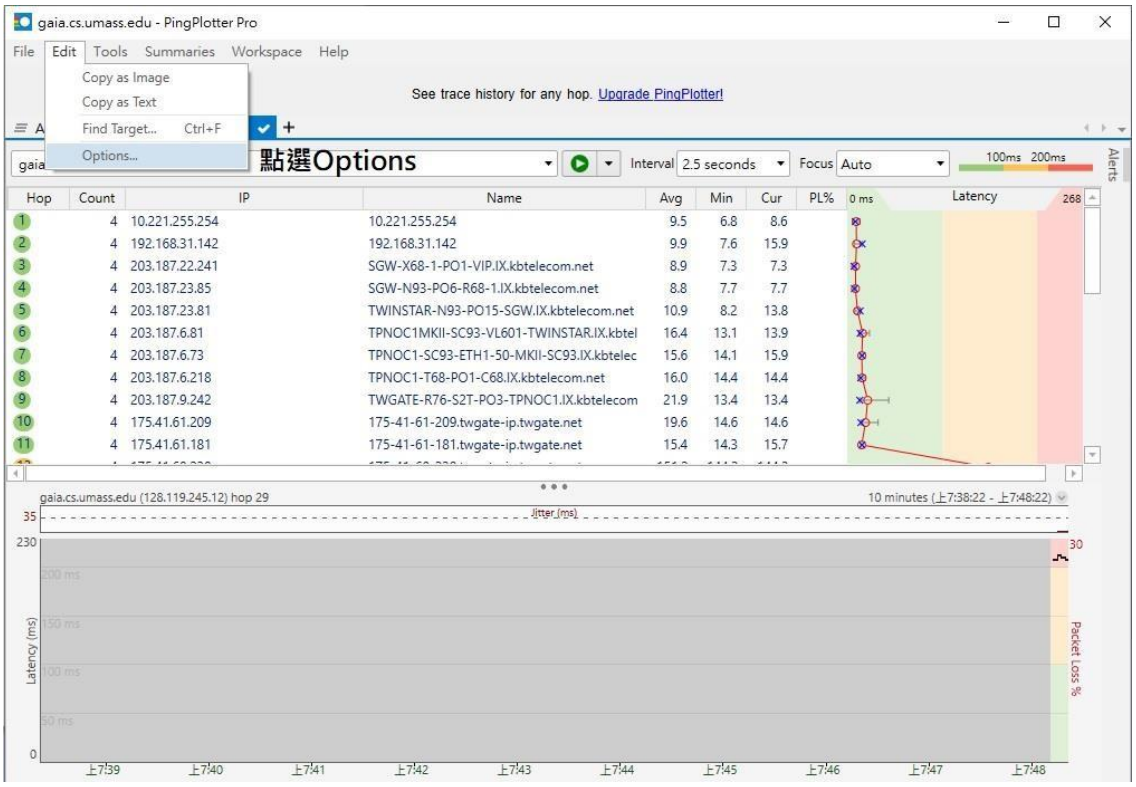
You have to download PingPlotter to do traceroute, the download address: https://www.pingplotter.com/download .

Example:

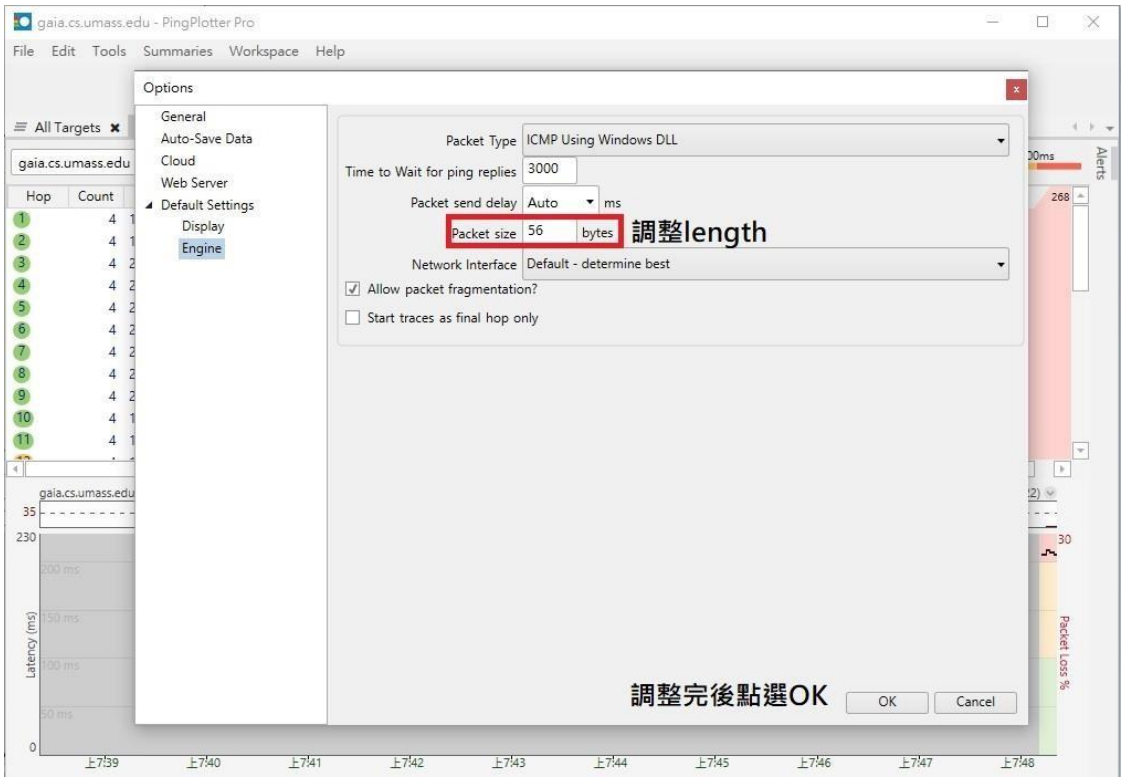
1.


gaia.cs.umass.edu - PingPlotter Pro
File Edit Tools Summaries Workspace Help
Keep track of route changes over time. Upgrade PingPlotter!
All Targets
gaia.cs.umass.edu
輸入網址
gaia.cs.umass.edu
Interval 2.5 seconds
Focus Auto
100ms 200ms
Alerts
Hop Count IP Name Avg Min Cur PL% 0 ms Latency 268
1 4 10.221.255.254 10.221.255.254 9.5 6.8 8.6
2 4 192.168.31.142 192.168.31.142 9.9 7.6 15.9
3 4 203.187.22.241 SGW-X68-1-PO1-VIP.IX.kbtelecom.net 8.9 7.3 7.3
4 4 203.187.23.85 SGW-N93-PO6-R68-1.IX.kbtelecom.net 8.8 7.7 7.7
5 4 203.187.23.81 TWINSTAR-N93-PO15-SGW.IX.kbtelecom.net 10.9 8.2 13.8
6 4 203.187.6.81 TPNOC1MKII-SC93-VL601-TWINSTAR.IX.kbtel 16.4 13.1 13.9
7 4 203.187.6.73 TPNOC1-SC93-ETH1-50-MKII-SC93.IX.kbtelec 15.6 14.1 15.9
8 4 203.187.6.218 TPNOC1-T68-PO1-C68.IX.kbtelecom.net 16.0 14.4 14.4
9 4 203.187.9.242 TWGATE-R76-S2T-PO3-TPNOC1.IX.kbtelecom 21.9 13.4 13.4
10 4 175.41.61.209 175-41-61-209.twgate-ip.twgate.net 19.6 14.6 14.6
11 4 175.41.61.181 175-41-61-181.twgate-ip.twgate.net 15.4 14.3 15.7
gaia.cs.umass.edu (128.119.245.12) hop 29
10 minutes (上7:38:22 - 上7:48:22)
Jitter (ms)
35
230
30
Latency (ms)
Packet Loss %
0
上7:39
上7:40
上7:41
上7:42
上7:43
上7:44
上7:45
上7:46
上7:47
上7:48

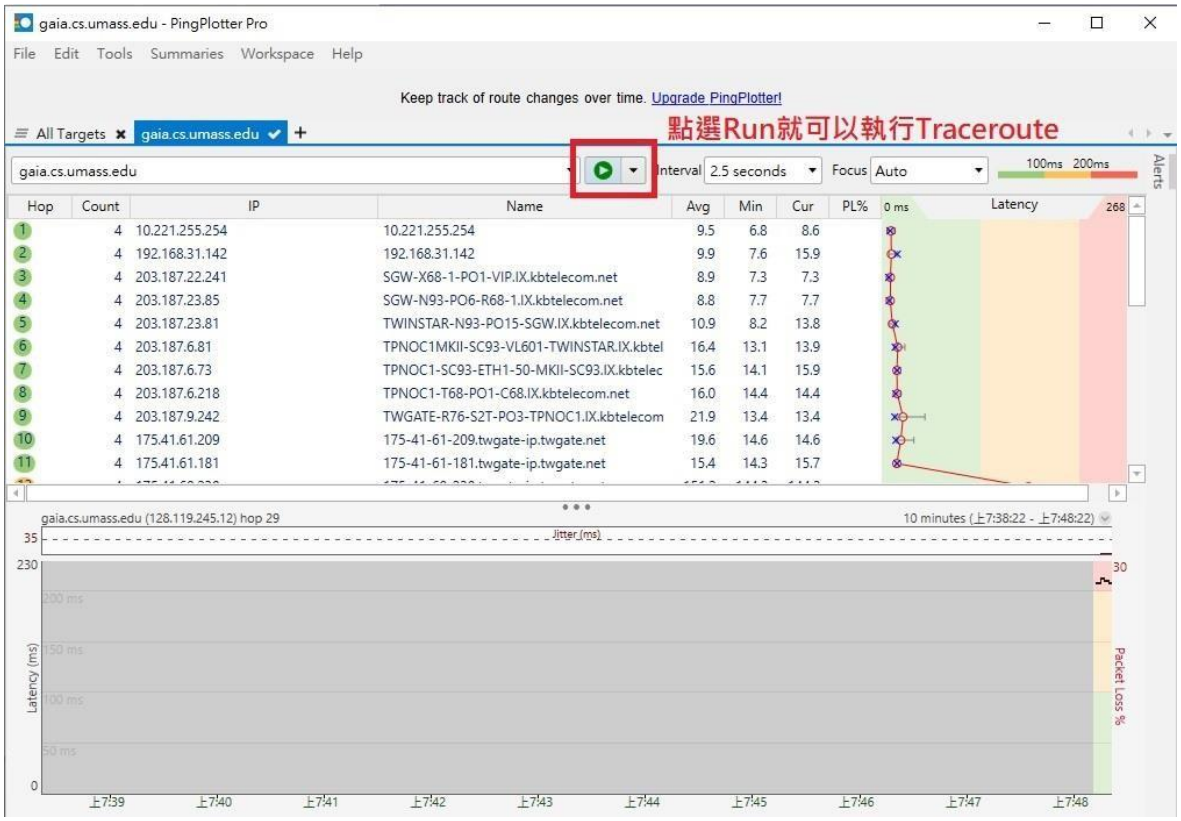
2.


gaia.cs.umass.edu - PingPlotter Pro
File Edit Tools Summaries Workspace Help
Copy as Image
Copy as Text
Find Target... Ctrl+F
Options...
點選Options
See trace history for any hop. Upgrade PingPlotter!
Interval 2.5 seconds
Focus Auto
Hop Count IP Name Avg Min Cur PL% Latency
1 4 10.221.255.254 10.221.255.254 9.5 6.8 8.6
2 4 192.168.31.142 192.168.31.142 9.9 7.6 15.9
3 4 203.187.22.241 SGW-X68-1-PO1-VIP.IX.kbtelecom.net 8.9 7.3 7.3
4 4 203.187.23.85 SGW-N93-PO6-R68-1.IX.kbtelecom.net 8.8 7.7 7.7
5 4 203.187.23.81 TWINSTAR-N93-PO15-SGW.IX.kbtelecom.net 10.9 8.2 13.8
6 4 203.187.6.81 TPNOC1MKII-SC93-VL601-TWINSTAR.IX.kbtel 16.4 13.1 13.9
7 4 203.187.6.73 TPNOC1-SC93-ETH1-50-MKII-SC93.IX.kbtelec 15.6 14.1 15.9
8 4 203.187.6.218 TPNOC1-T68-PO1-C68.IX.kbtelecom.net 16.0 14.4 14.4
9 4 203.187.9.242 TWGATE-R76-S2T-PO3-TPNOC1.IX.kbtelecom 21.9 13.4 13.4
10 4 175.41.61.209 175-41-61-209.twgate-ip.twgate.net 19.6 14.6 14.6
11 4 175.41.61.181 175-41-61-181.twgate-ip.twgate.net 15.4 14.3 15.7
gaia.cs.umass.edu (128.119.245.12) hop 29
10 minutes (上7:38:22 - 上7:48:22)
Jitter (ms)
Latency (ms)
Packet Loss %
上7:39 上7:40 上7:41 上7:42 上7:43 上7:44 上7:45 上7:46 上7:47 上7:48

3.


gaia.cs.umass.edu - PingPlotter Pro
File Edit Tools Summaries Workspace Help
Options
General
Auto-Save Data
Cloud
Web Server
Default Settings
Display
Engine
Packet Type ICMP Using Windows DLL
Time to Wait for ping replies 3000
Packet send delay Auto ms
Packet size 56 bytes
調整length
Network Interface Default - determine best
Allow packet fragmentation?
Start traces as final hop only
調整完後點選OK
OK
Cancel

4.



Do the following:

- Start up Wireshark and begin packet capture. (Capture->Start or click on the blue shark fin button in the top left of the Wireshark window).
- Enter a traceroute commands, using gaia.cs.umass.edu as the destination with a length of 56 bytes.
- Stop Wireshark tracing.

Part 1: Basic IPv4

In your trace, you should be able to see the series of UDP segments (in the case of MacOS/Linux) or ICMP Echo Request messages (Windows) sent by traceroute on your computer, and the ICMP TTL-exceeded messages returned to your computer by the intermediate routers. In the questions below, we'll assume you're using a MacOS/Linux computer; the corresponding questions for the case of a Windows machine should be clear. Your screen should look similar to the screenshot in Figure 2, where we have used the display filter "udp||icmp" (see the light-green-filled display-filter field in Figure 2) so that only UDP and/or ICMP protocol packets are displayed.

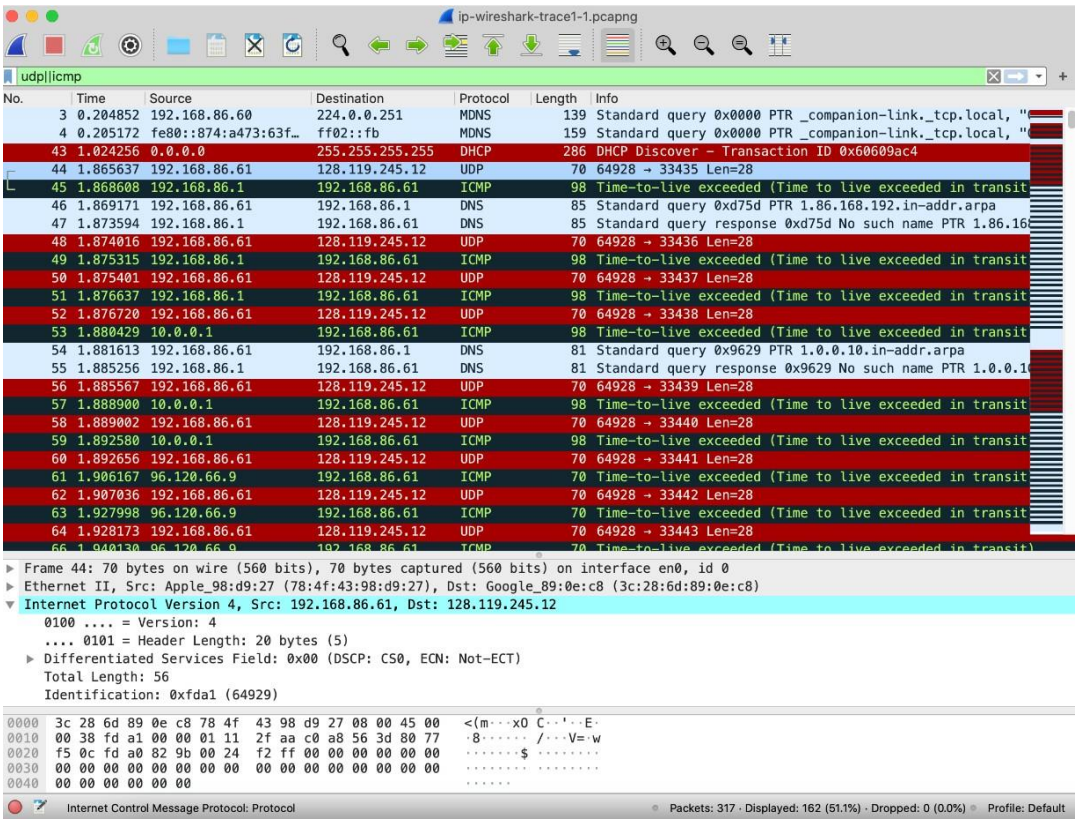


Figure 2: Wireshark screenshot, showing UDP and ICMP packets in the tracefile *ip-wireshark-trace1-1.pcapng*

Question 1: Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer? (You may find the answer in Internet Protocol Version 4)**(15%)**

Question 2: Within the IP packet header, what is the value in the upper layer protocol field? **(15%)**

Question 3: How many bytes are in the IP header? (You may find the answer in Internet Protocol Version 4) **(10%)**

Question 4: How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes. (You may find the answer in Internet Protocol Version 4) **(10%)**

Question 5: Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented. (You may find the answer in Internet Protocol Version 4) **(20%)**

Next, sort the traced packets according to IP source address by clicking on the Source column header; a small downward pointing arrow should appear next to the word Source. If the arrow points up, click on the Source column header again. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the "details of selected packet header" window. In the "listing of captured packets" window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent by other protocols running on your computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by your computer.

Question 6: Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer? (You may find the answer in Internet Protocol Version 4) **(20%)**

Note: Use at least two images to show your answer. (Hand in two images named 6-1.jpg and 6-2.jpg or combine them into one image.)

Next (with the packets still sorted by source address) find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router.

Question 7: What is the value in the Identification field and the TTL field? **(10%)**