Lab 02: Network Troubleshooting

NET311 - Computer Network Management

Instructor: Dr. Mostafa Dahshan

Objectives

1. Use protocol analyzers, such as Wireshark, to inspect the packet contents.
2. Use basic network troubleshooting tools, such as ping and traceroute utilities.

References

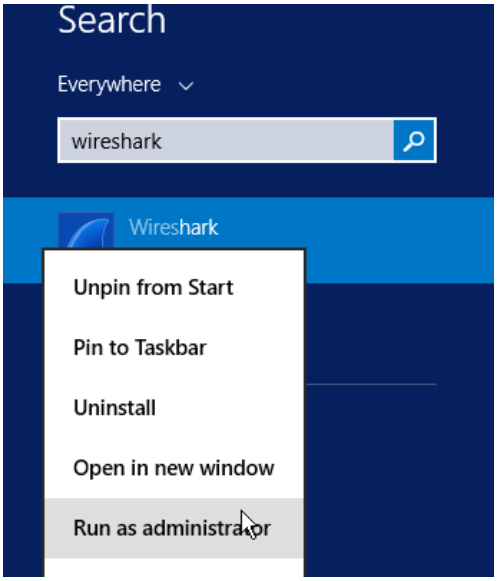
1. Computer Networks 5/E, Lab Exercise, Protocol Layers, David Wetherall.
2. Computer Networks 5/E, Lab Exercise, ICMP, David Wetherall.

Instructions

1. Read the lab instructions.
2. Provide question answers and screenshots in the supplied answer sheet.
3. After finishing the lab, upload your saved answer sheet to LMS.

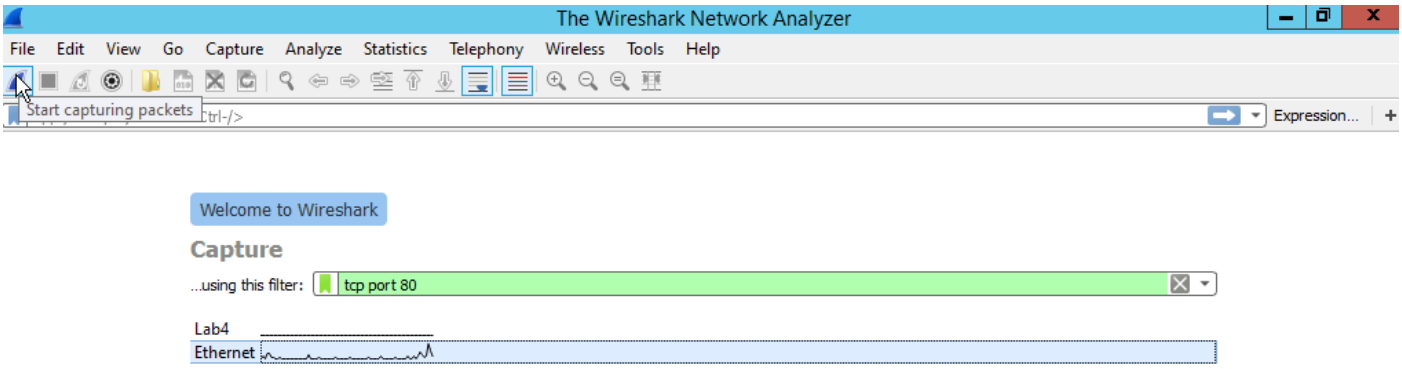
Part 1: Protocol Analyzers

1. Run the **Wireshark** application as an **Administrator**.



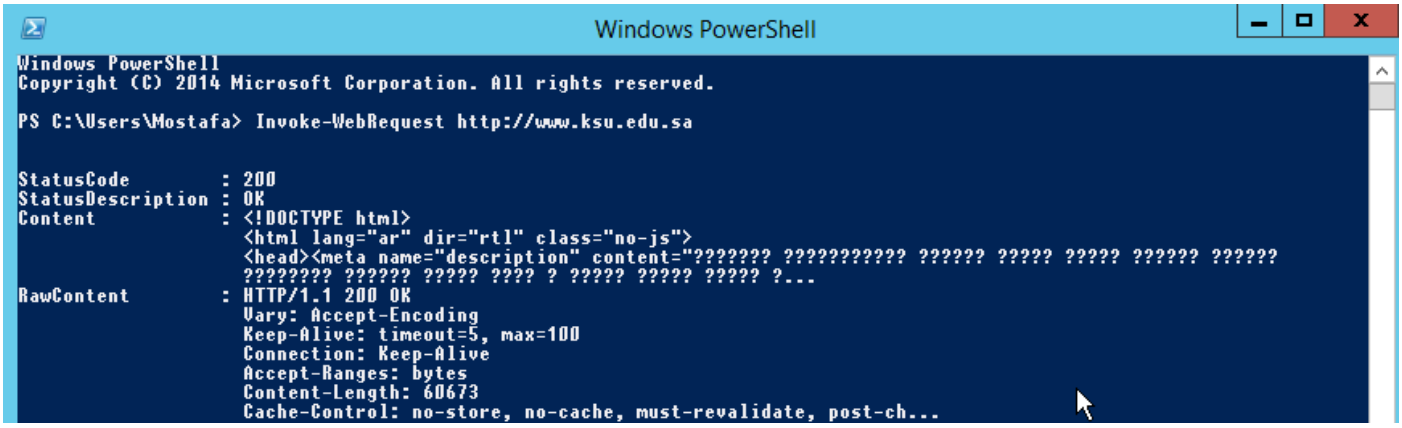
2. In Wireshark, select the **Ethernet** interface, and start a capture using the following **filter**:

```
tcp port 80
```

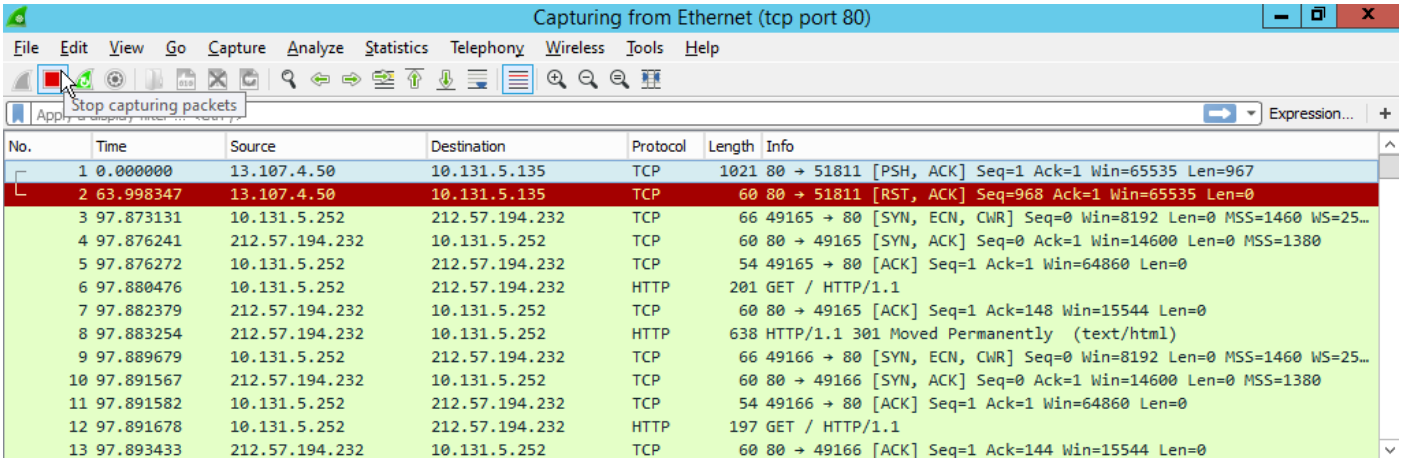


3. Open **Windows PowerShell** and type the following command:

```
Invoke-WebRequest http://www.ksu.edu.sa
```

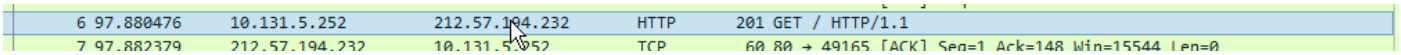


4. After the command is finished, return to Wireshark and **stop** the capture.

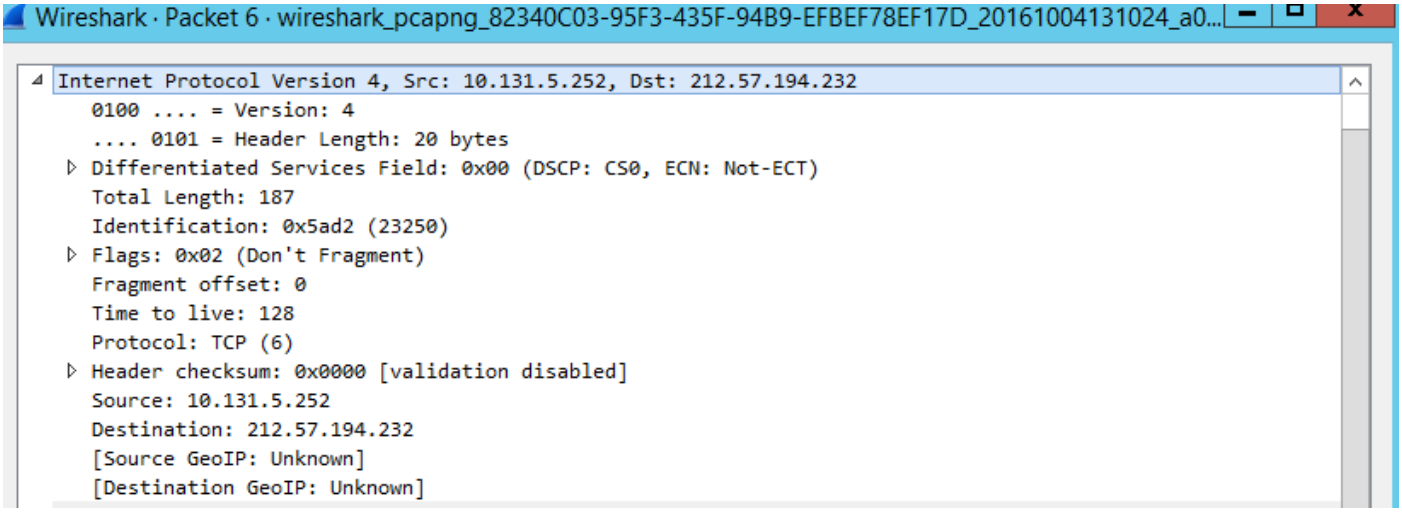


Lab sheet 1.1: provide a screenshot of Wireshark screen showing the captured packets.

5. Locate the packet **HTTP GET** packet and double click on it to inspect it.



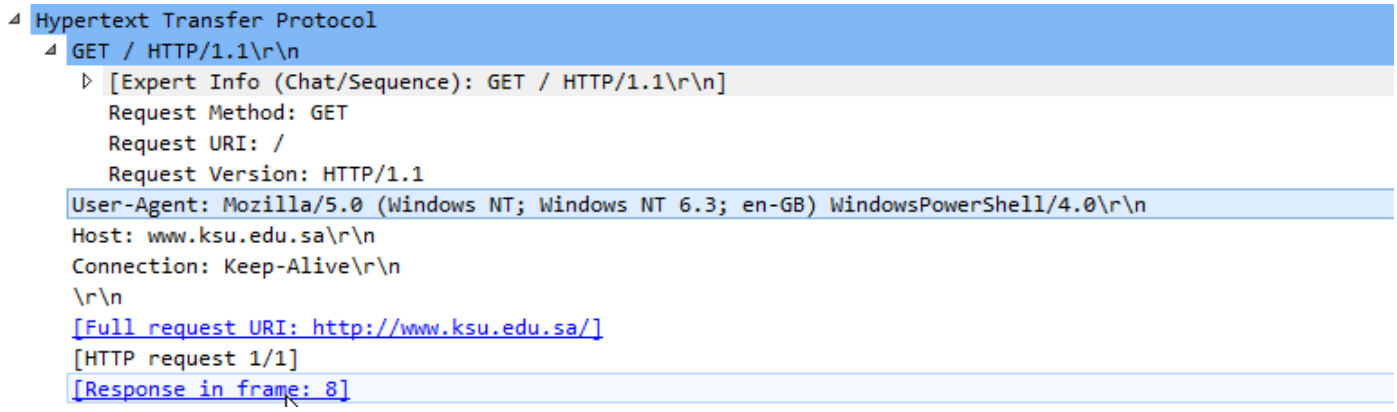
6. Expand the details of **Internet Protocol Version 4**.



Lab sheet 1.2: Fill the following details of the Internet Protocol Version 4 protocol.

Total Length	Time to Live	Protocol	Source	Destination

7. Expand the details of **Hypertext Transfer Protocol**.



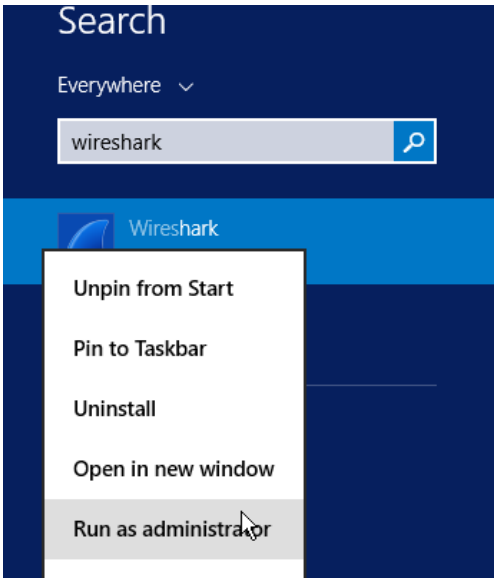
Lab sheet 1.3: Fill the following details of the Hypertext Transfer Protocol.

Hint: You can use Control-C to copy from the Wireshark window.

Request Method	Request URI	User-Agent	Host

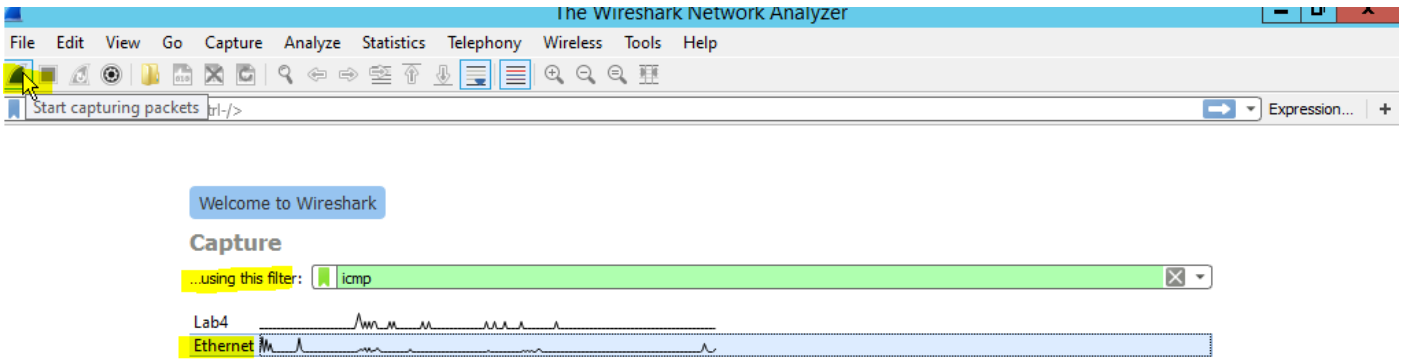
Part 2: Network Troubleshooting Tools

1. Run the **Wireshark** application as an **Administrator**.



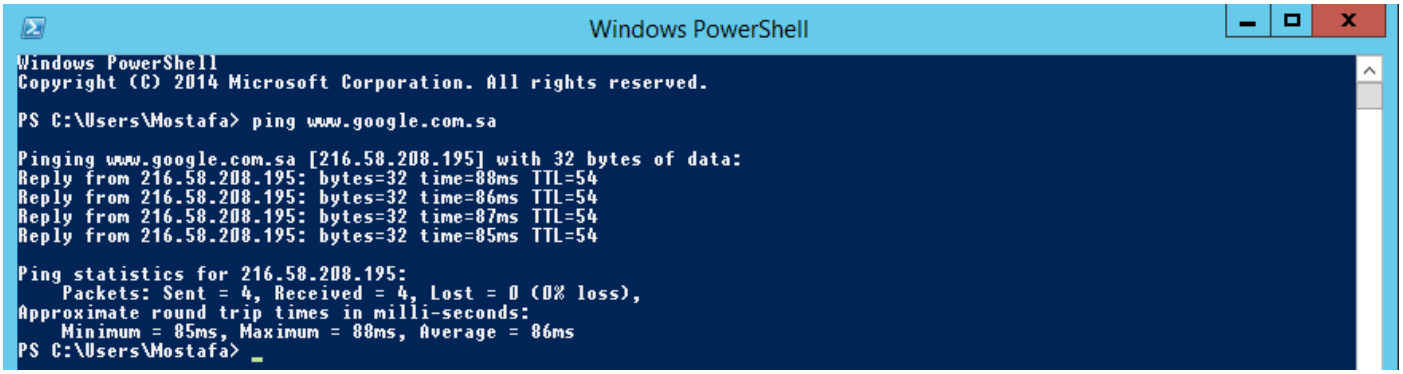
2. In Wireshark, select the **Ethernet** interface, and start a capture using the following **filter**:

```
icmp
```

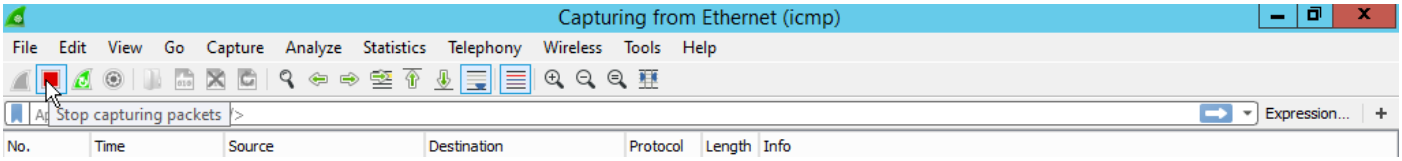


3. Open **Windows PowerShell** and type the following command:

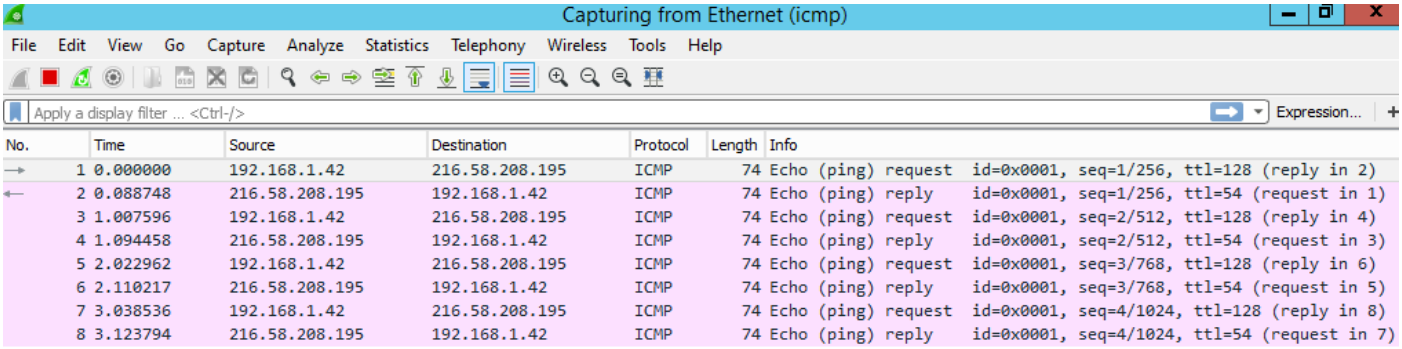
```
ping www.google.com.sa
```

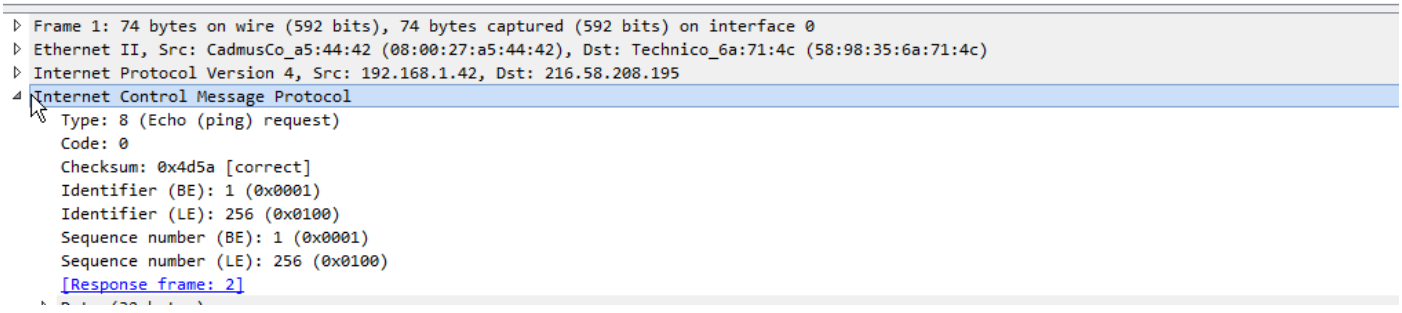


4. After the command is finished, return to Wireshark and **stop** the capture.



5. Inspect the ICMP packets by expanding the **Internet Control Message Protocol** fields, then answer the following questions.

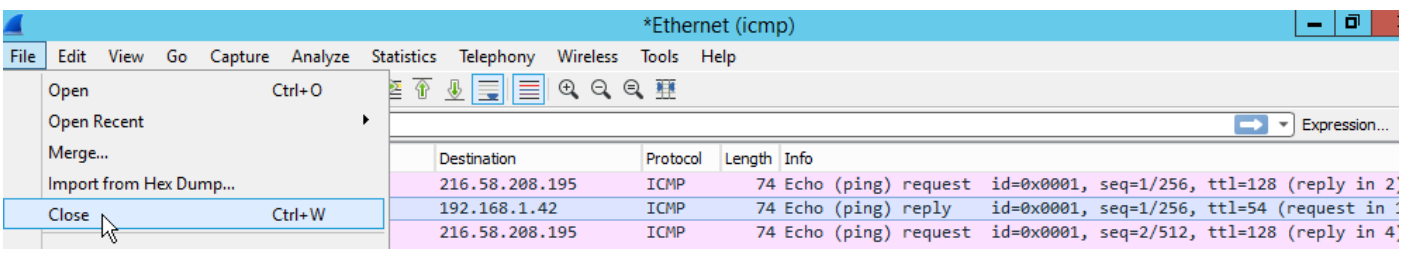




Lab sheet 2.1: Answer the following questions.

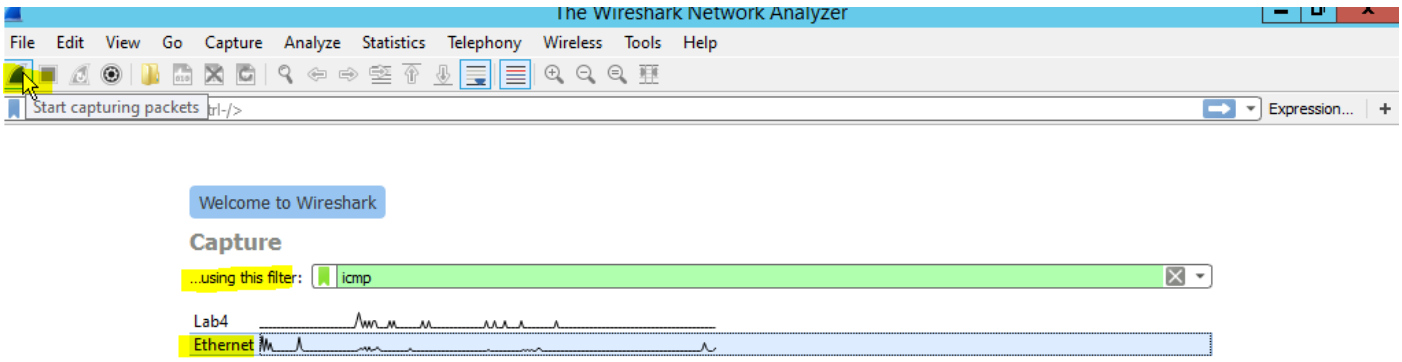
What is the Type/Code value of the first ICMP request?	
What is Type/Code value of the first ICMP reply?	
What is Sequence number of the second ICMP request?	
What is Sequence number of the second ICMP reply?	
What is Data of the third ICMP request?	
What is Data of the third ICMP reply?	
What is Time of the fourth ICMP request?	
What is Time of the fourth ICMP reply?	

6. Close the Wireshark capture.



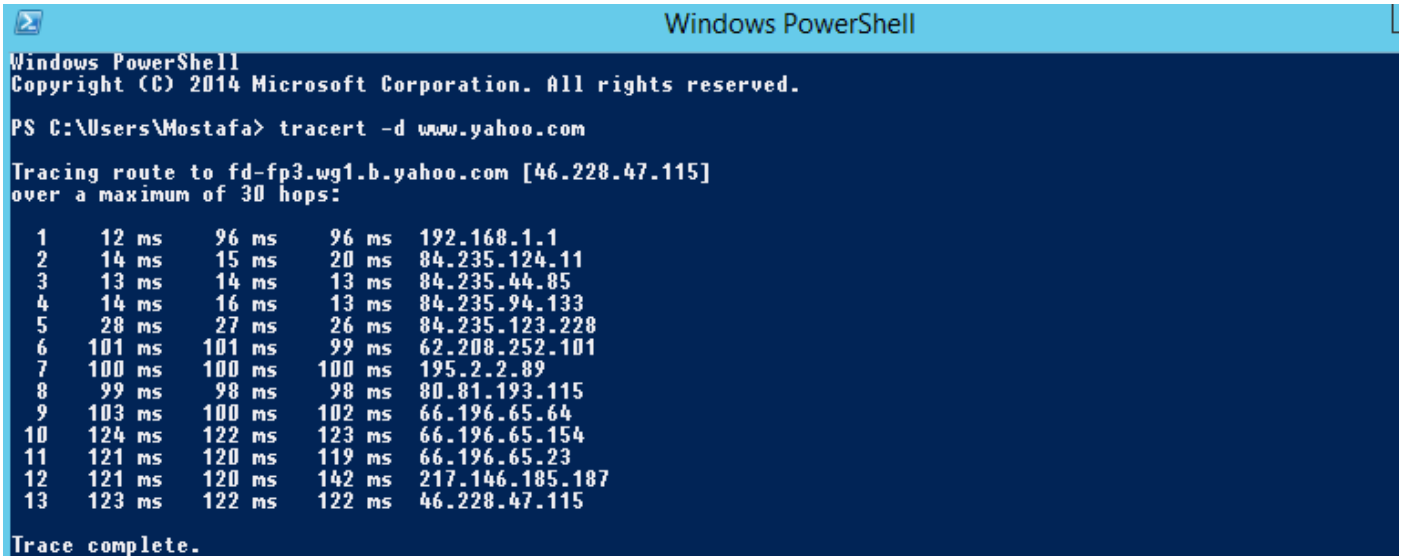
7. In Wireshark, select the **Ethernet** interface, and start a capture using the following **filter**:

```
icmp
```



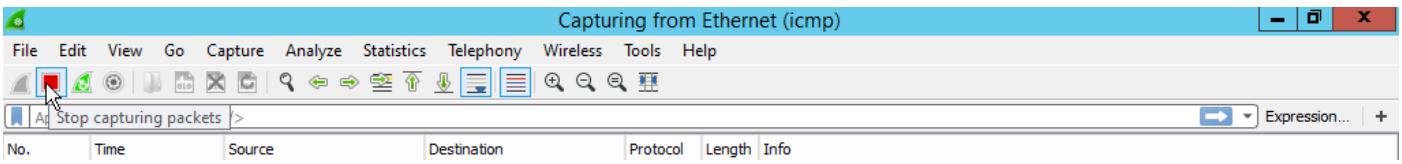
8. Open **Windows PowerShell** and type the following command:

```
tracert -d www.yahoo.com
```

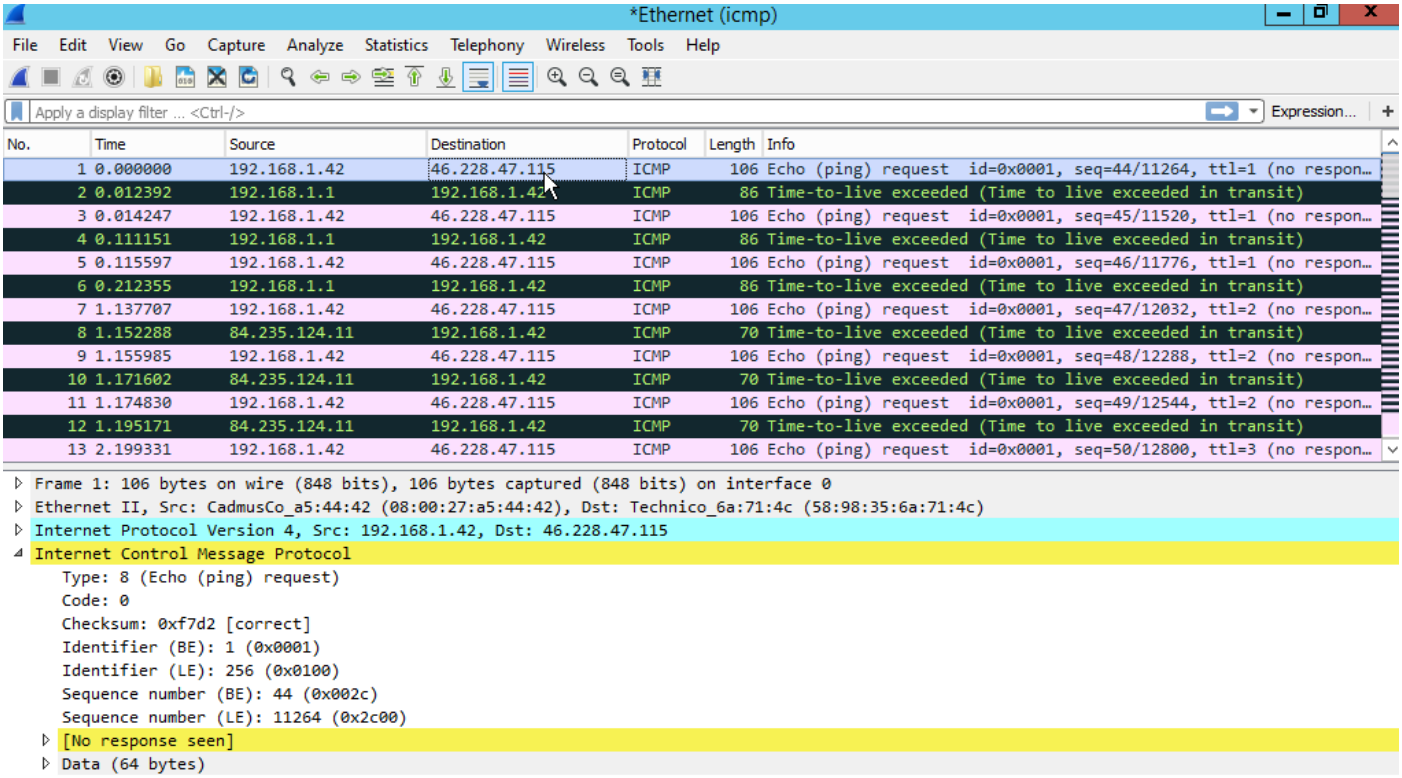


Lab sheet 2.2: Provide a screenshot showing the output of the tracert command.

9. After the command is finished, return to Wireshark and **stop** the capture.



10. Inspect the ICMP packets by expanding the **Internet Control Message Protocol** fields, then answer the following questions.

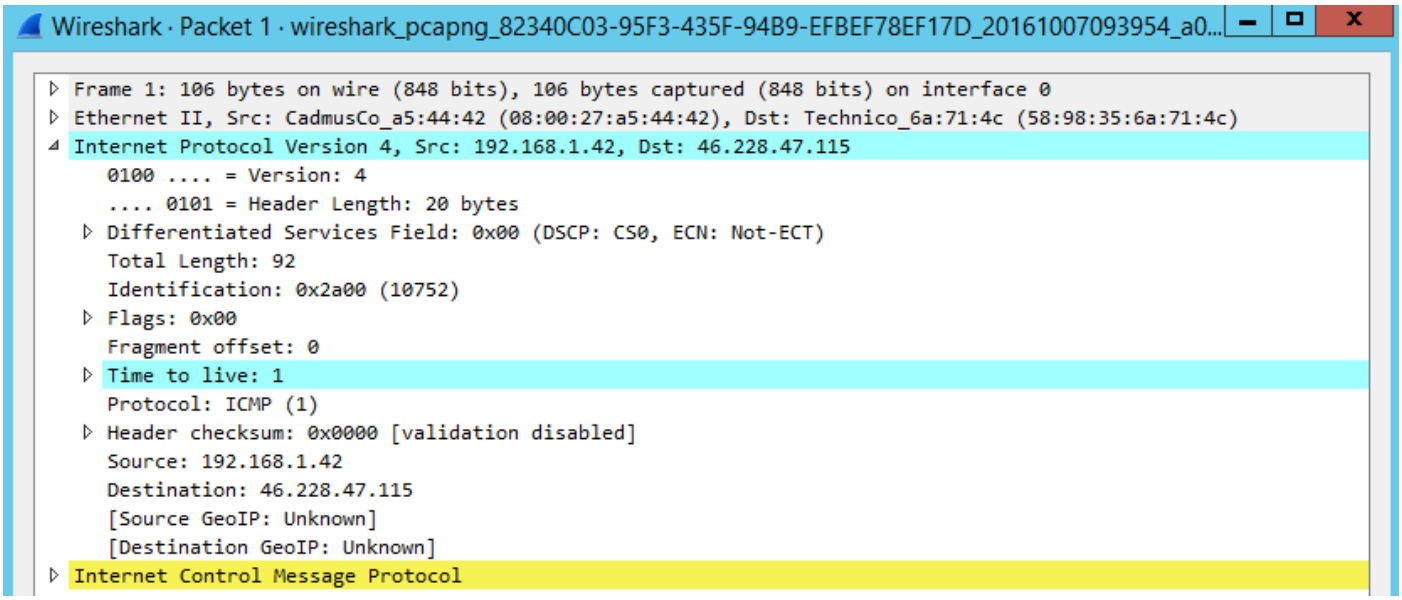


Lab sheet 2.3: Answer the following questions.

What is the TTL (Time to live) value in the first ICMP request?	
What is the Type/Code value of the first ICMP request?	
What is the Type/Code value of the first ICMP TTCL Exceeded response?	
How many ICMP packets with TTL = 1?	
What is the source IP address of the second ICMP TTL Exceeded response?	
What is the source IP address of the third ICMP TTL Exceeded response?	
What is the largest TTL value in ICMP requests after the last TTL Exceeded response?	

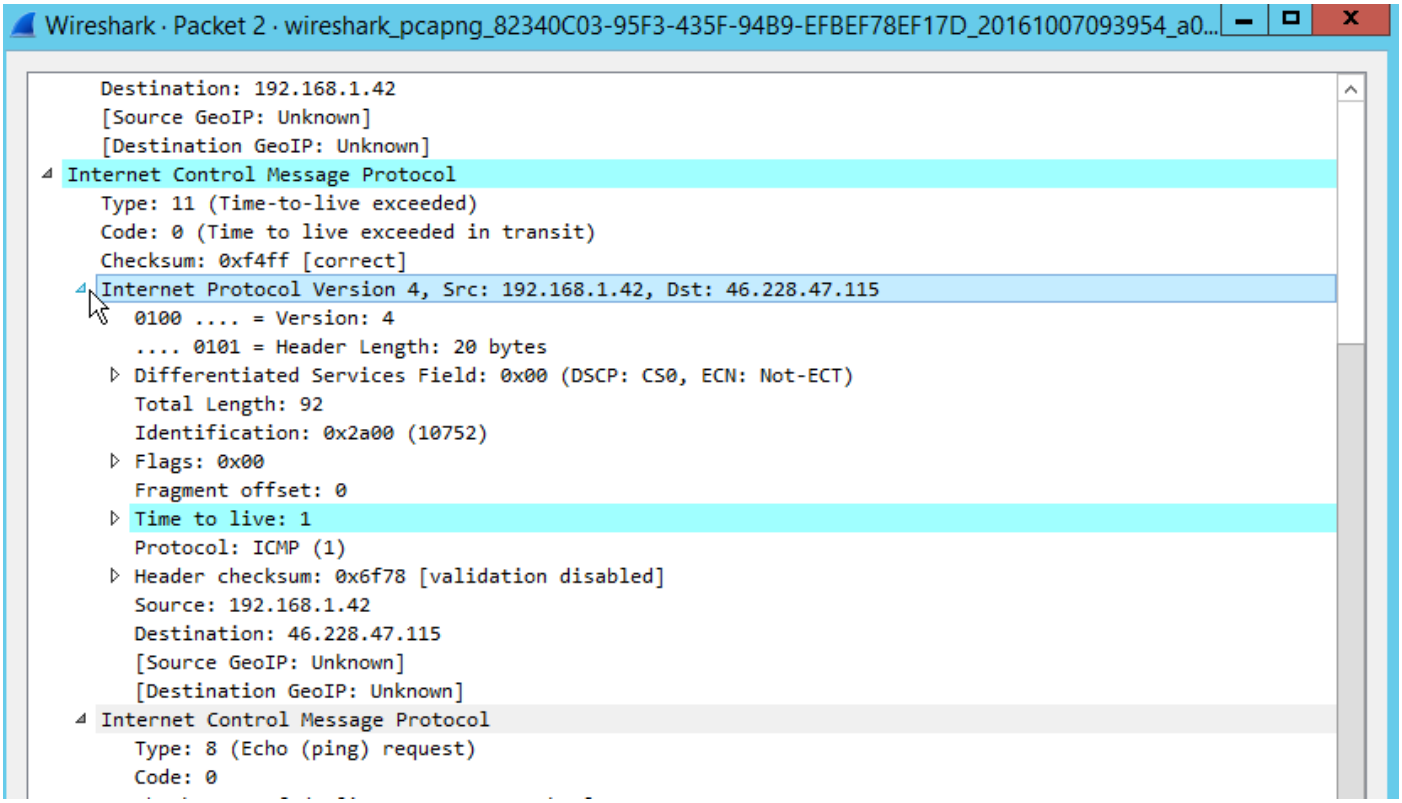
11. Expand the **Internet Protocol Version 4** section of the first ICMP request.

Lab sheet 2.4: Provide a screenshot showing the details of the Internet Protocol Version 4 section of the first ICMP request.



12. Expand the **Internet Control Message Protocol** -> **Internet Protocol Version 4** subsection of the first ICMP Time Exceeded response.

Lab sheet 2.5: Provide a screenshot showing the details of the first ICMP Time Exceeded response.



13. Compare the payload of the ICMP response with the ICMP request.