UNIVERSITY OF BAHRAIN

COLLEGE OF INFORMATION TECHNOLOGY

DEPARTMENT OF COMPUTER ENGINEERING

ITC416 Computer Networks II

Experiment No 2

**Wireshark Lap: ICMP**

Name: Fadhel Abdullah Salman AbedAli

ID:20082923

Sec : 02

Objective:

* *Explore ICMP messages which are generated by Ping command.*
* *Explore ICMP messages which are generated by Traceroute command.*
* *Understanding the format and content of ICMP messages.*

Introduction:

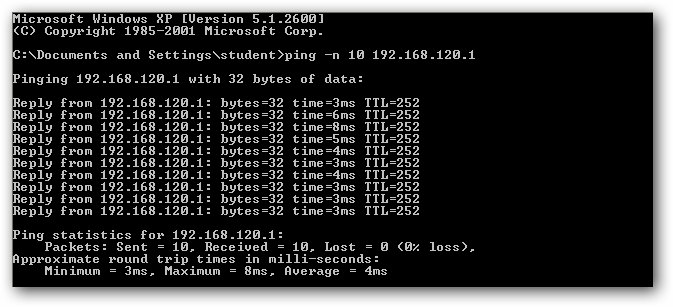
*In this lab we will experiment the ICMP protocol, and focus on its fields. We will generate ICMP messages using the ping and Tracert commands and capture the packets which are generated using the WireShark program and then we will explore these packets in order to understand ICMP messages.*

**Procedure:**

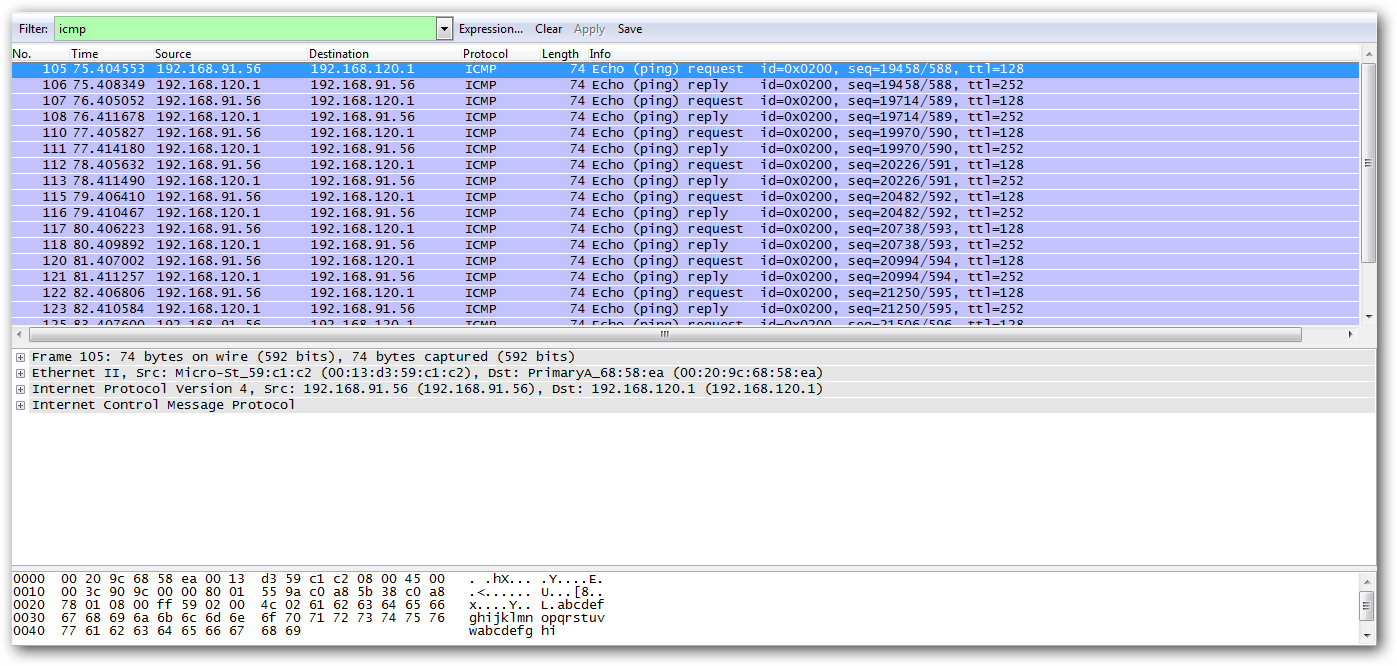
**Part I:**

1. *First, we open Wireshark program and start capturing.*
2. *Open command prompt and issue the following command*

***Ping –n 10 192.168.120.1***

******

1. *Stop Wireshark capturing.*
2. *Filter Wireshark capturing result by writing ICMP in filter filed.*

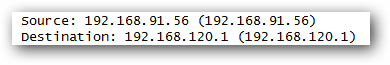
**

***Questions:***

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

*The IP address of my host is 192.168.91.56. The IP address of the destination*

*host is 192.168.120.1*

******

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

*The ICMP packet does not have source and destination port numbers because*

*it was designed to communicate network-layer information between hosts and*

*routers, not between application layer processes. Each ICMP packet has a*

*"Type" and a "Code". The Type/Code combination identifies the specific*

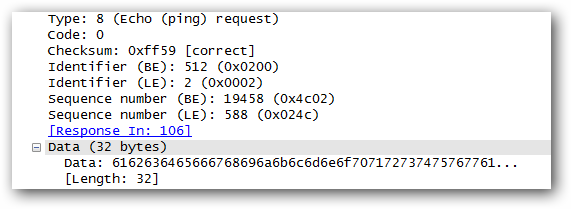
*message being received. Since the network software itself interprets all ICMP*

*messages, no port numbers are needed to direct the ICMP message to an*

*application layer process.*

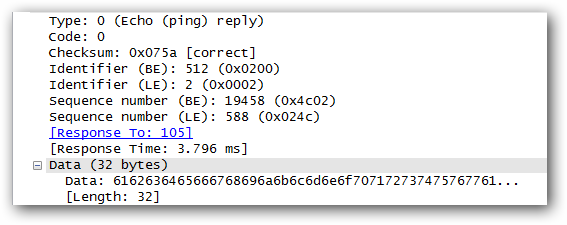
1. ***Examine one of the ping request packets sent by your host. What are the ICMP***
   1. ***type and code numbers? What other fields does this ICMP packet have? How***
   2. ***many bytes are the checksum, sequence number and identifier fields?***

*ICMP is of type 8 and the code number is 0 and there also Checksum identifier, sequence number, and data fields. 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***
   1. ***numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?***

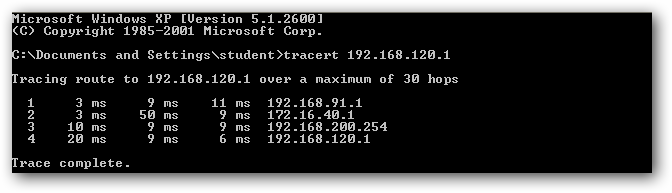
*ICMP is of type 0 and the code number is 0 and there also Checksum identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.*



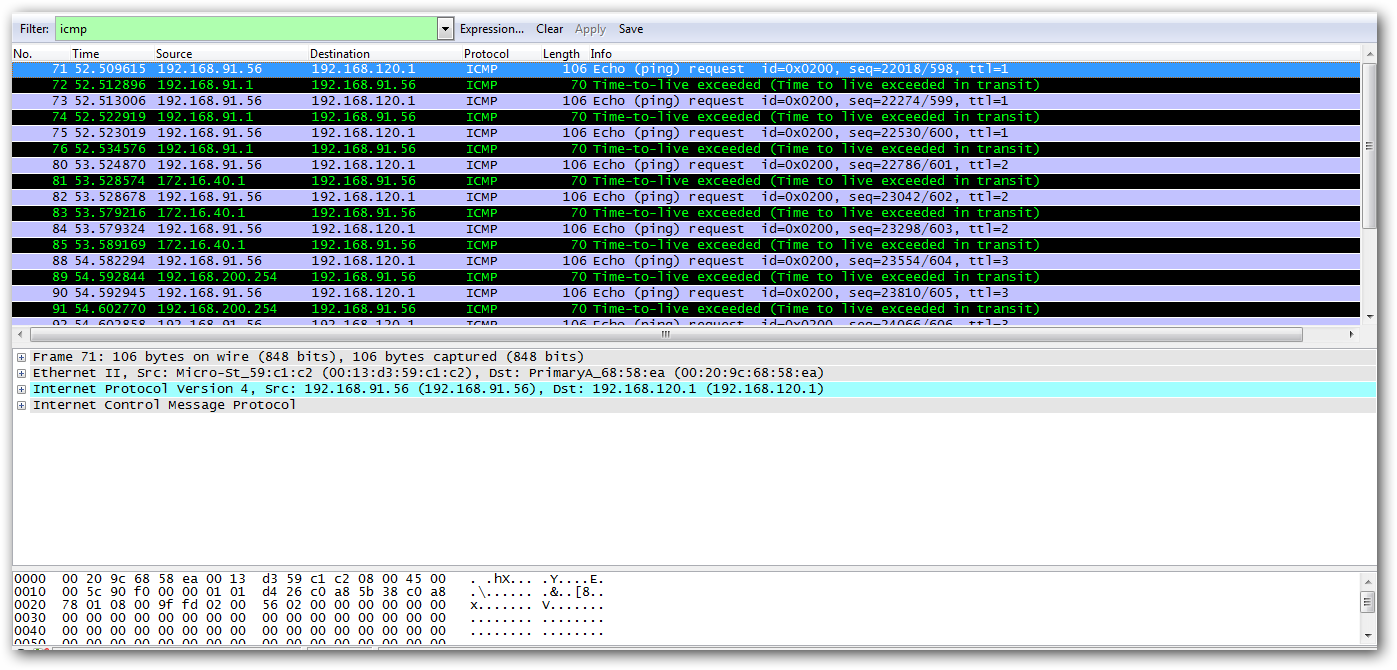
**Part II:**

1. *First, we open Wireshark program and start capturing.*
2. *Open command prompt and issue the following command*

***tracert 192.168.120.1***

******

1. *Stop Wireshark capturing.*
2. *Filter Wireshark capturing result by writing ICMP in filter filed.*

**

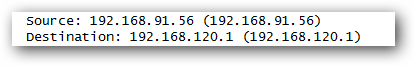
***Questions:***

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 192.168.91.56. The IP address of the destination*

*host is 192.168.120.1*

**

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 (17).*

1. ***Examine the ICMP echo packet in your screenshot. Is this different from the***

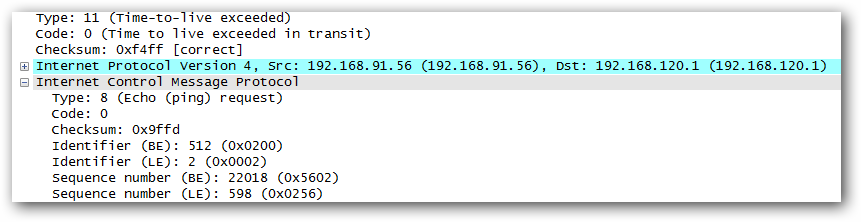
***ICMP ping query packets in the first half of this lab? If yes, how so?***

*No, it’s the same felids as ping query packet.*

1. ***Examine the ICMP error packet in your screenshot. It has more fields than the***

***ICMP echo packet. What is included in those fields?***

*It includes both the IP header which contains all ipv4 fields and the first 8 bytes of the original ICMP packet that the error is for and these bytes contains information’s about the packet like the type, code and checksum.*

******

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.*

**Conclusion:**

*After doing this lab I have being more familiar with the ping, tracert commands and wireshark program. I have understood how dose ICMP protocol works not only that but also, what are the fields and their contents in ICMP messages.*