**Lab Manual for Computer Communication and Networking**

**Lab No. 11**

**Capturing IP Header Using Wireshark**

**BAHRIA UNIVERSITY KARACHI CAMPUS**

**Department of Software Engineering**

**COMPUTER COMMUNICATION & NETWORKING**

**LAB EXPERIMENT # 11**

Capturing IP Header in Wireshark

**OBJECTIVE: -**

* Capturing IP Computergram to study its various fields, and study IP fragmentation in detail.

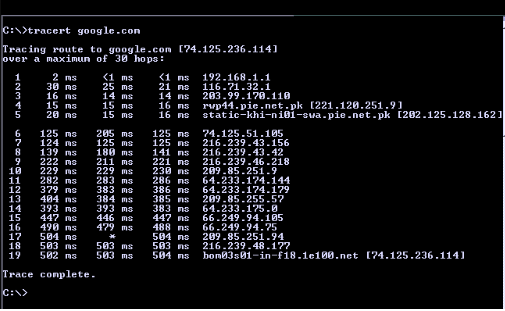
**THEORY: -**

In this lab, we’ll investigate the IP protocol, focusing on the IP Computergram. We’ll do so by analyzing a trace of IP Computergrams sent and received by an execution of the traceroute program.

**Capturing IP Packets from an execution of traceroute:**

To generate a trace of IP Computergrams for this lab, we’ll use the traceroute program to send Computergrams of different sizes towards some destination, *X*.

Run traceroute program to trace the route e.g. [www.google.com](http://www.google.com) etc.

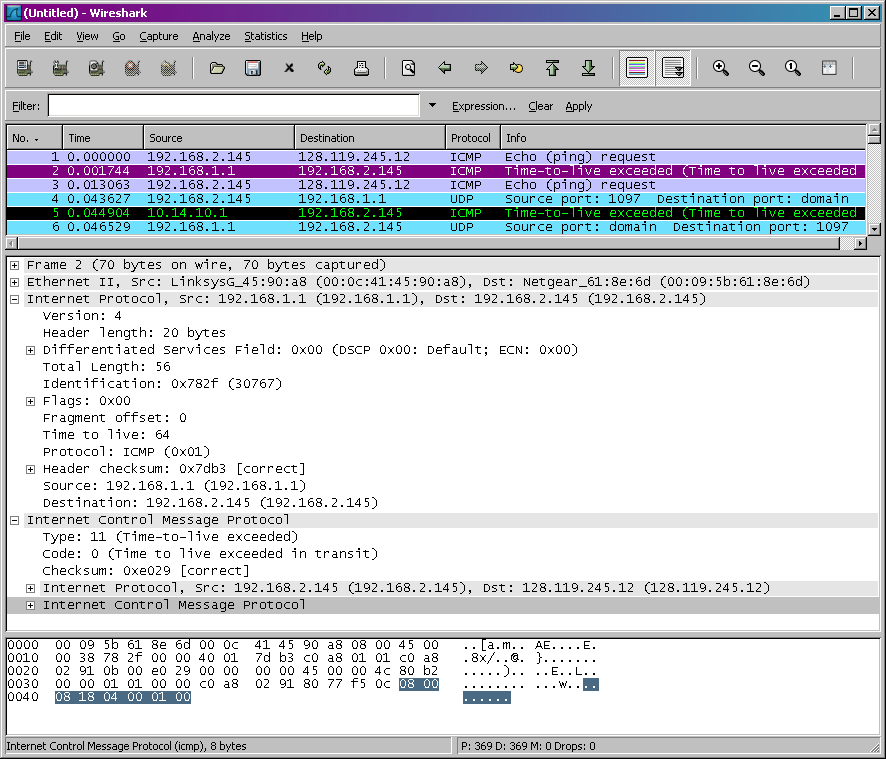


Do the following:

* Start Wireshark and begin packet capture *(Capture->Option)* and then press *OK* on the Wireshark Packet Capture Options screen (we’ll not need to select any options here).
* When tracing is completed stop Wireshark tracing.

In your trace, you should be able to see the series of ICMP Echo Request

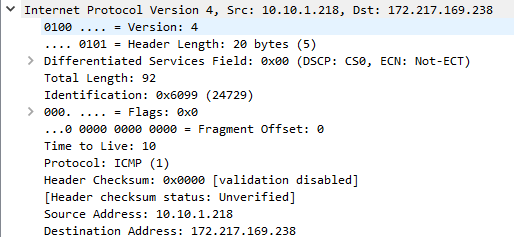
Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window.



**Fig: ICMP Packet Selection**

**QUESTIONS: -**

1. Name the fields in IP header



1. What is the IP address of your computer?



1. Within the IP packet header, what is the value in the upper layer protocol field?



1. How many bytes are in the IP header? How many bytes are in the payload *of the* *IP Computergram*?
   * 1. Payload length: total length-header length

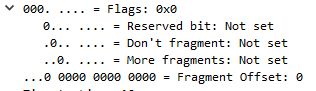
92-20=72

1. Explain how you determined the number of payload bytes.

Payload length: total length-header length

1. Has this IP Computergram been fragmented? Explain how you determined whether the Computergram has been fragmented.

No



1. What is the value in the Identification field and the TTL field?



1. What information in the IP header indicates that the Computergram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment?

* If more fragement field is zero then there is no fragementation occur.
* If offset field set up with zero, it shows first fragementation

**TIME BOXING:**

|  |  |  |
| --- | --- | --- |
| **Activity Name** | **Activity Time** | **Total Time** |
| **Instruments Allocation + Setting up Lab** | 10 mints | 10 mints |
| **Walk through Theory & Tasks (Lecture)** | 60 mints | 60 mints |
| **Implementation & Practice time** | 90 mints | 80 mints |
| **Evaluation Time** | 20 mints | 20 mints |
|  | Total Duration | 180 mints |

**Teacher Signature**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Student Registration No**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_