

Lab Manual for Computer Communication and Networking

Lab No. 10

Capturing IP Header Using Wireshark



BAHRIA UNIVERSITY KARACHI CAMPUS

Department of Software Engineering

COMPUTER COMMUNICATION & NETWORKING

LAB EXPERIMENT # 10

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 etc.

```
C:\>tracert google.com
Tracing route to google.com [74.125.236.114]
over a maximum of 30 hops:
  0  2 ms  <1 ms  <1 ms  192.168.1.1
  1  30 ms  25 ms  21 ms  116.71.32.1
  2  16 ms  14 ms  14 ms  203.99.170.110
  3  15 ms  15 ms  16 ms  rwp44.pie.net.pk [221.120.251.9]
  4  20 ms  15 ms  16 ms  static-khi-n101-sva.pie.net.pk [202.125.128.162]

  5  125 ms  205 ms  125 ms  74.125.51.105
  6  124 ms  125 ms  125 ms  216.239.43.156
  7  139 ms  180 ms  141 ms  216.239.43.42
  8  222 ms  211 ms  221 ms  216.239.46.218
  9  229 ms  229 ms  230 ms  209.85.251.9
 10  282 ms  283 ms  286 ms  64.233.174.144
 11  379 ms  383 ms  386 ms  64.233.174.179
 12  404 ms  384 ms  385 ms  209.85.255.57
 13  393 ms  393 ms  383 ms  64.233.175.8
 14  447 ms  446 ms  447 ms  66.249.94.105
 15  490 ms  479 ms  488 ms  66.249.94.75
 16  504 ms  *  504 ms  209.85.251.94
 17  503 ms  503 ms  503 ms  216.239.48.177
 18  502 ms  503 ms  504 ms  bon03s01-in-f18.1e100.net [74.125.236.114]

Trace complete.
C:\>
```

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.

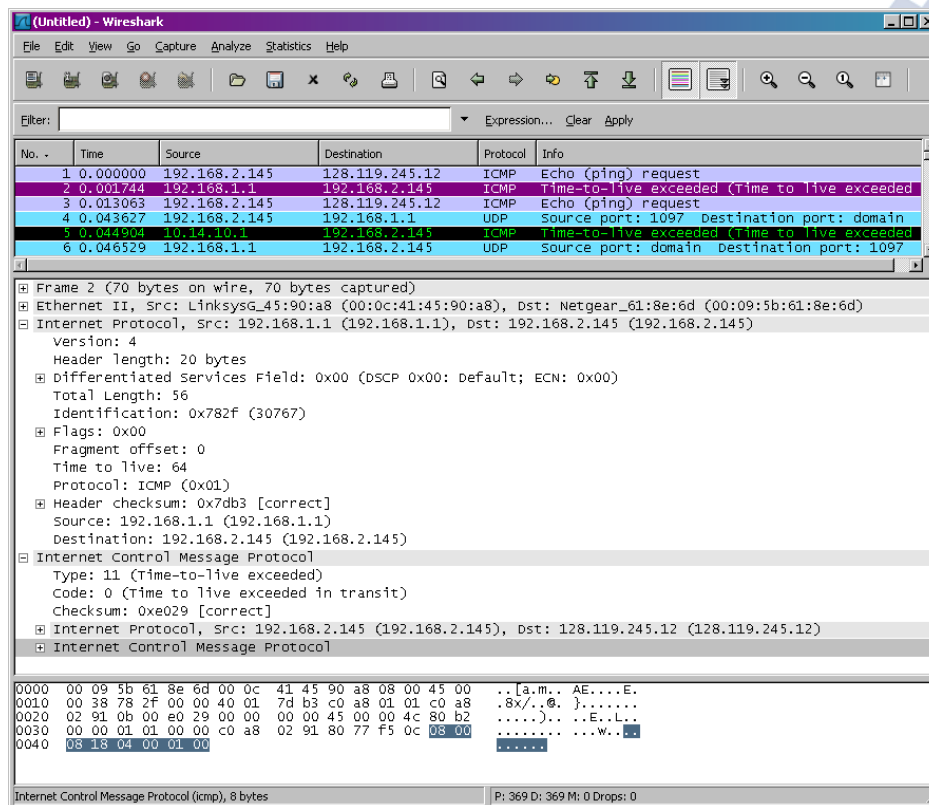


Fig: ICMP Packet Selection

QUESTIONS: -

1. Name the fields in IP header.
2. What is the IP address of your computer?
3. Within the IP packet header, what is the value in the upper layer protocol field?
4. How many bytes are in the IP header? How many bytes are in the payload of the IP Computergram?
5. Explain how you determined the number of payload bytes.
6. Has this IP Computergram been fragmented? Explain how you determined whether the Computergram has been fragmented.
7. What is the value in the Identification field and the TTL field?
8. 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?

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: _____