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 etc.

```
C:\>tracert google.con

Tracing route to google.com [74.125.236.114]
over a maximun of 30 hops:

  1     2 ms    <1 ms    <1 ms  192.168.1.1
  2    30 ms    25 ms    21 ms  116.71.32.1
  3    16 ms    14 ms    14 ms  203.99.170.110
  4    15 ms    15 ms    16 ms  rwp44.pie.net.pk [221.120.251.9]
  5    20 ms    15 ms    16 ms  static-khi-ni01-swa.pie.net.pk [202.125.128.162]

  6   125 ms   205 ms   125 ms  74.125.51.105
  7   124 ms   125 ms   125 ms  216.239.43.156
  8   139 ms   180 ms   141 ms  216.239.43.42
  9   222 ms   211 ms   221 ms  216.239.46.218
 10   229 ms   229 ms   230 ms  209.85.251.9
 11   282 ms   283 ms   286 ms  64.233.174.144
 12   379 ms   383 ms   386 ms  64.233.174.179
 13   404 ms   384 ms   385 ms  209.85.255.57
 14   393 ms   393 ms   383 ms  64.233.175.0
 15   447 ms   446 ms   447 ms  66.249.94.105
 16   490 ms   479 ms   488 ms  66.249.94.25
 17   504 ms     *      504 ms  209.85.251.94
 18   503 ms   503 ms   503 ms  216.239.48.177
 19   502 ms   503 ms   504 ms  bom03s01-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.

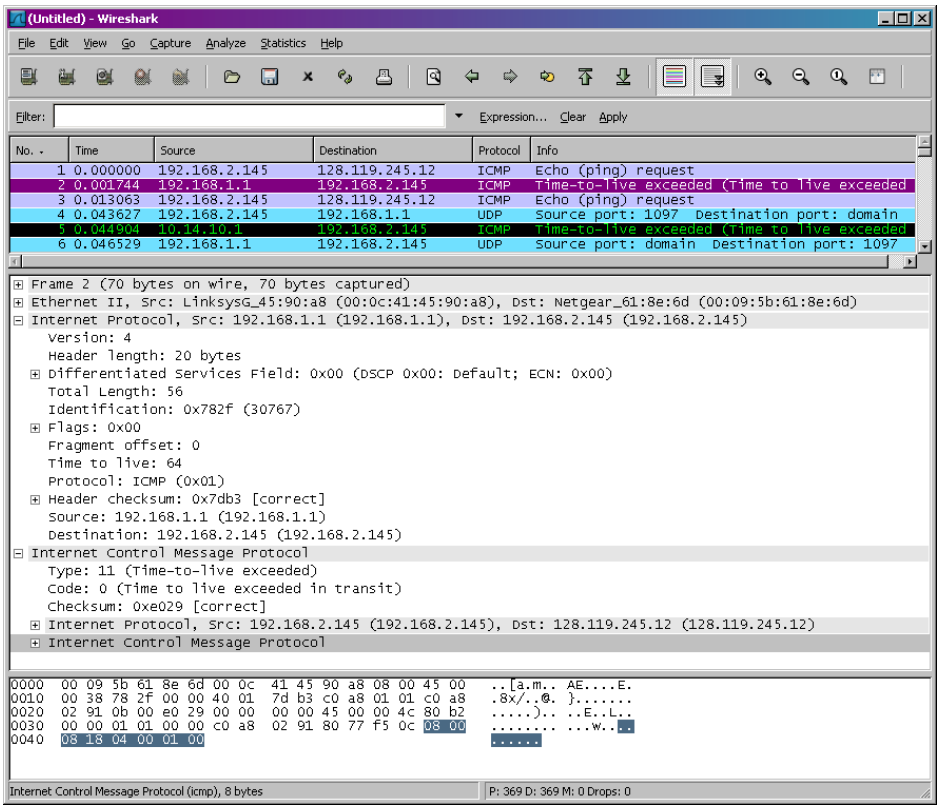

Fig: ICMP Packet Selection

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?

Solution: -

1. Fields in the ip header are as follows: -

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   0000 00.. = Differentiated Services Codepoint: Default (0)
   .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 60
Identification: 0x5d92 (23954)
000. .... = Flags: 0x0
   0... .... = Reserved bit: Not set
   .0.. .... = Don't fragment: Not set
   ..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x9bc0 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.105
Destination Address: 172.217.18.132
```

2. Source address field in the ip header gives the ip addressof our computer.

```
Source Address: 192.168.1.105
```

3. The Protocol field in the ip header gives the protocol used by the packet.

```
Protocol: ICMP (1)
```

4. Header length field of ip header specifies the total bytes in ip header.

```
.... 0101 = Header Length: 20 bytes (5)
```

   By subtracting no of bytes in total length field and header length field, It gives payload length

```
Total Length: 60
```

   Payload Length => 60 - 20 => 40

5. By subtracting no of bytes in total length field and header length field, It gives payload length
6. We can check if the computergram is fragmented or not by checking the donot fragment field.

```
.0.. .... = Don't fragment: Not set
```

7. Identification field: -

```
Identification: 0x5d92 (23954)
```

   Time to live field: -

```
Time to Live: 64
```

8. We can check if the computergram is fragmented or not by checking the donot fragment

field. If it is not set, The fragmentation is not done.

```
.0.. .... = Don't fragment: Not set
```

We check if the current fragment is the very first or not by checking the fragment offset field. If it is 0,It means that it is the very first fragment. Else, The fragment is not the very first.

```
...0 0000 0000 0000 = Fragment Offset: 0
```

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: 69966_____