

## Lab 1 -- Part 2 : Using Wireshark in Kali to look at ICMP packets

due 9/18 @ 3:00 PM ....And be ready for a quiz on 9/18

1. Access the ProxMox Kali VM (those several students that are still having authentication problems, use your own laptop running Kali in VMWare.)
2. Bring up a terminal command prompt (the second icon on the left side of the screen)
3. Type in the next command, but don't hit enter yet (If you do accidentally hit enter, then you will not get the DNS packets in the sniff)

ping www.guimp.com

4. Don't close the window .... But bring up Wireshark (Applications > 09 - Sniffing...> Wireshark) and start listening on the Ethernet interface
5. **Now** switch back to **terminal cmd prompt** and hit enter to ping the website
6. **Quickly** go back to Wireshark and **stop the sniff** and **save it** as

Lab1-section#-yourname-Linux\_icmp.pcap

7. Now, explore the sniff capture and apply a filter to only show the packets with the ICMP protocol : ip.proto == ICMP
8. Screenshot the filtered packet results and place the picture in here :

The screenshot shows the Wireshark interface with the filter `ip.proto == ICMP` applied. The packet list displays several ICMP Echo (ping) requests and replies. The packet details pane shows the structure of an ICMP Echo request.

No.	Time	Source	Destination	Protocol	Length	Info
5	0.000641081	192.168.1.7	77.92.69.132	ICMP	98	Echo (ping) request id=0x20
6	0.098260639	77.92.69.132	192.168.1.7	ICMP	98	Echo (ping) reply id=0x20
9	1.001695418	192.168.1.7	77.92.69.132	ICMP	98	Echo (ping) request id=0x20
10	1.099493617	77.92.69.132	192.168.1.7	ICMP	98	Echo (ping) reply id=0x20
11	2.002561508	192.168.1.7	77.92.69.132	ICMP	98	Echo (ping) request id=0x20
12	2.100254100	77.92.69.132	192.168.1.7	ICMP	98	Echo (ping) reply id=0x20
13	3.003475643	192.168.1.7	77.92.69.132	ICMP	98	Echo (ping) request id=0x20

Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
Ethernet II, Src: d6:e8:6e:32:ff:e9 (d6:e8:6e:32:ff:e9), Dst: da:fd:10:9d:0f:05 (da:fd:10:9d:0f:05)  
Internet Protocol Version 4, Src: 192.168.1.7, Dst: 77.92.69.132  
Internet Control Message Protocol

0000 da fd 10 9d 0f 05 d6 e8 6e 32 ff e9 08 00 45 00 ..... n2....E.  
0010 00 54 52 86 40 00 40 01 93 93 c0 a8 01 07 4d 5c .TR.@. ....M\  
0020 45 84 08 00 37 64 20 b6 00 01 3d 57 a0 5b 00 00 E...7d . . =W. [...  
0030 00 00 00 5f 03 00 00 00 00 00 10 11 12 13 14 15 .....  
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ..... !"#\$\$%  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()\*+,-./012345  
0060 36 37 67

Sequence number (big en...on) (icmp.seq), 2 bytes Packets: 26 · Displayed: 16 (61.5%) · Dropped: 0 (0.0%) · Load time: 0:0.1 Profile: Default

9. Now let's explore the first ICMP packet in depth. Still in Wireshark, highlight one of the ICMP packets where you are the source IP. Look in the detail section (in the middle), and answer the following:

What is the Frame size in bytes ? **98**

What is the **actual** source MAC? **d6: e8:6e:32:ff:e9**

What does shark identify as the "vendor" portion of the source MAC? **(d6: e8:6e:32: ff:e9)**

What is the **actual** destination MAC? **da: fd:10:9d:0f:05**

What does shark identify as the "vendor" portion of the destination MAC? **(da: fd: 10:9d:0f:05)**

Expand the Internet Control Message Protocol header.

What is the ICMP Type number ? **8** and associated meaning? **(Echo(ping)request)**

Expand the Internet Protocol header.

What is the value of **Time to live** ? **64**

Describe the payload data:

..\_... ..  
..!'"#\$%&'()\*+,-./01234567

10. Now let's explore the ICMP packet response in depth. Highlight the ICMP packet where you are the destination IP. Look in the detail section (in the middle), and answer the following:

Expand the Internet Control Message Protocol header.

What is the ICMP Type number ? **0** and associated meaning? **(Echo (ping) reply)**

Expand the Internet Protocol header.

What is the value of **Time to live** ? **51**

Did the payload data change? **No, the payload data haven't been changed**

11. Compare these results with Part 1 of the lab (Windows ping) – identify the components of the ping packets and their values that are different below:

12. Save this updated Word file with your responses as

Lab1-section#-yourname-Linux\_icmp.docx

13. Attach the the pcap file from Step 6, and your updated docx file to the Assignment