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

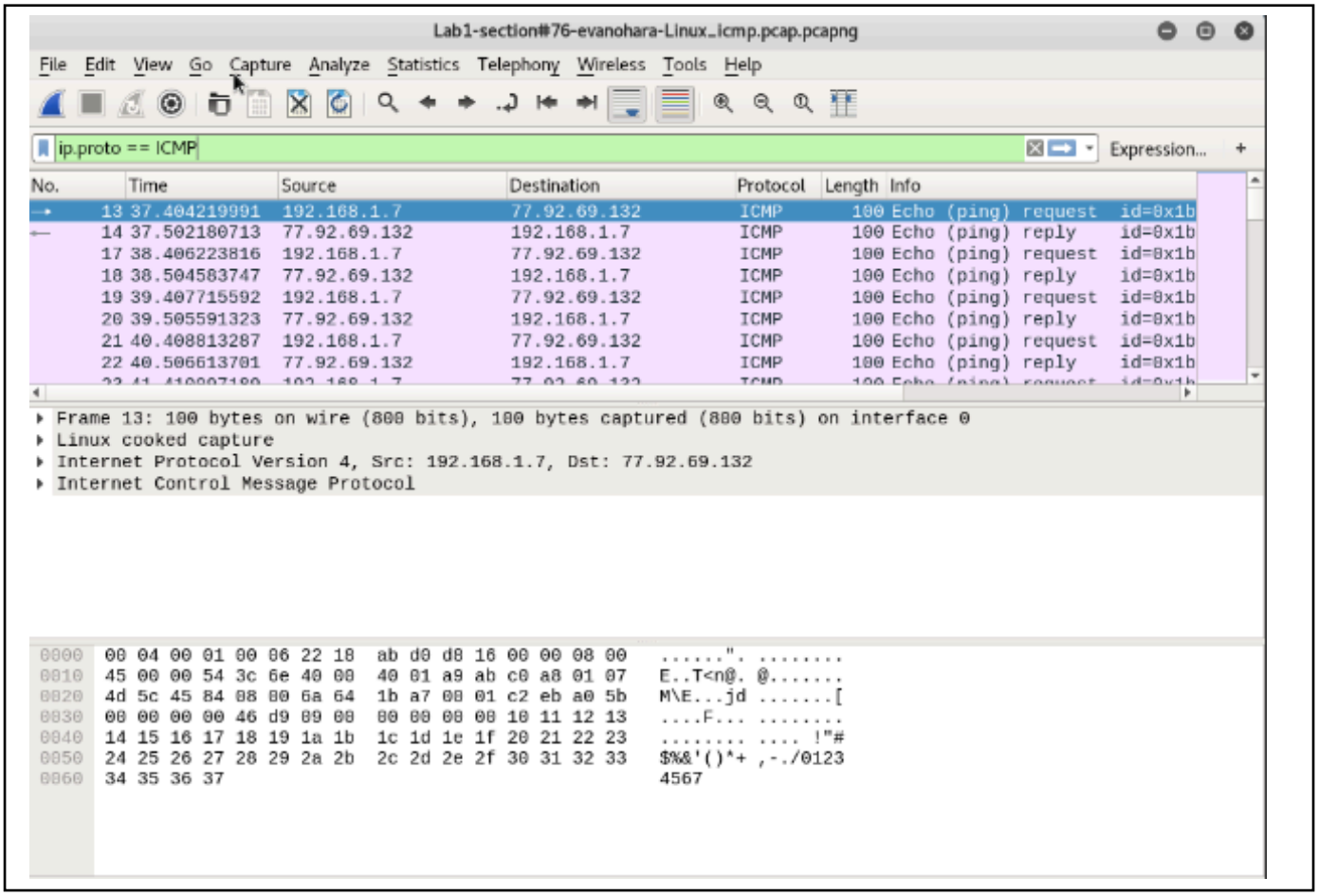
1. Access the ProxMox Kali VM (those several students that are still having authentication problems, use your own laptop running Kali in VMWare.)
2. Bring up a terminal command prompt (the second icon on the left side of the screen)
3. Type in the next command, **<u>but don't hit enter</u>** yet (If you do accidently 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 :



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 ? 100 bytes

   What is the **actual** source MAC? 22:18:ab:d0:d8:16
   What does shark identify as the "vendor" portion of the source MAC? d0:d8:16

   What is the **actual** destination MAC? 56:dc:9b:6a:8b:aa
   What does shark identify as the "vendor" portion of the destination MAC? 6a:8b:aa

   Expand the Internet Control Message Protocol header.
   What is the ICMP Type number ? 8 and associated meaning ? Echo

   Expand the Internet Protocol header.
   What is the value of **Time to live** ? 64

   Describe the payload data : Starts with the letter "F" followed by a series of "." Then a series of symbols (!"#$ etc.), and finally numbers counting up to 7 starting at 0

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 reply

    Expand the Internet Protocol header.
    What is the value of **Time to live** ? 51

    Did the payload data change? No change

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:
    - Source IP was different but Destination IP was the same
    - Data payloads were different as well
    - Time to live values different
    -

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