## Lab 1 -- Using Wireshark to look at ICMP packets

due 9/12 ….And be ready for a quiz in lab on 9/13

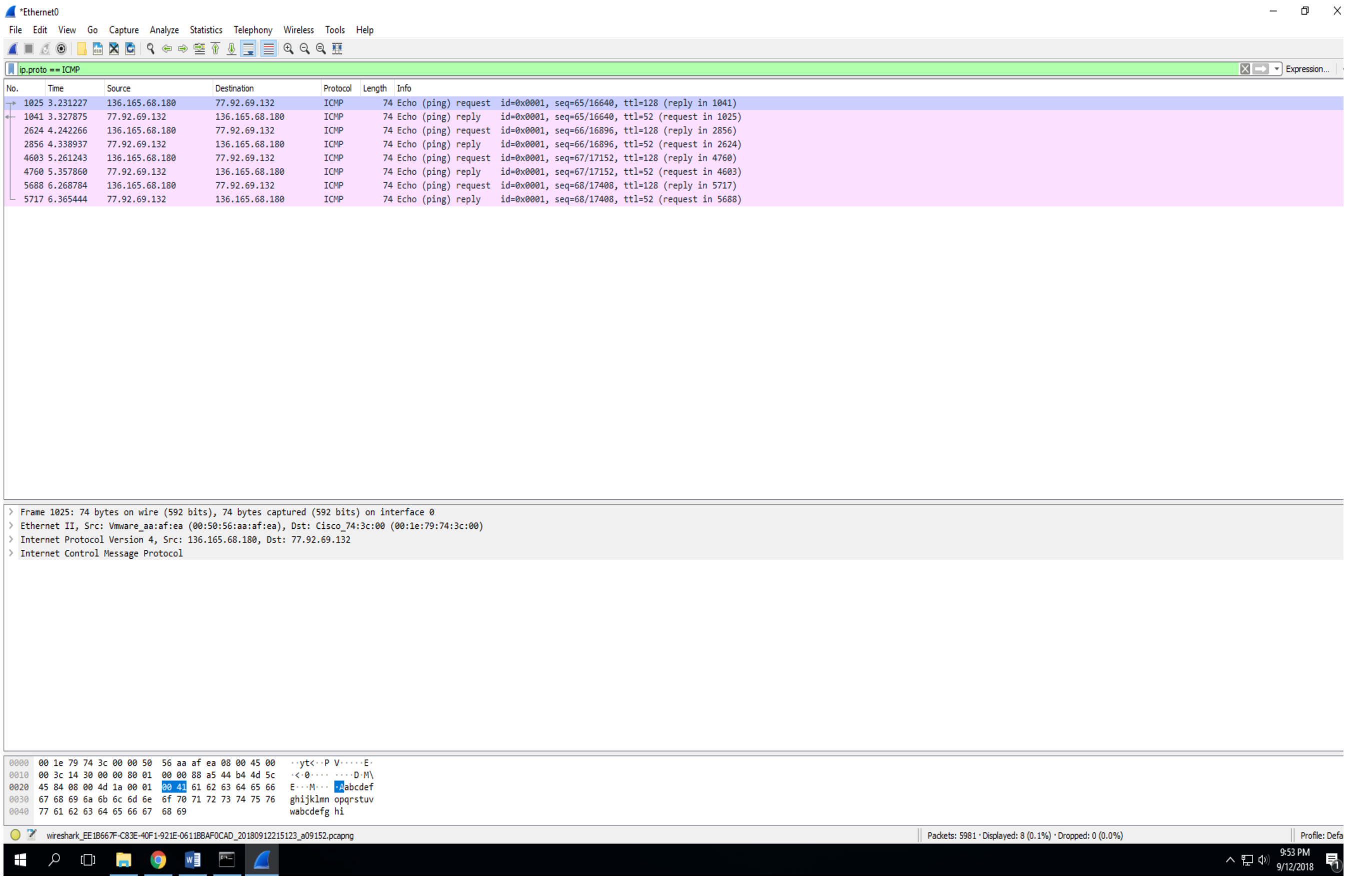
1. Access the Virtual Lab through Horizon Client
2. Bring up a command prompt
3. Type in the next command, **<u>but don’t hit enter</u>** yet (If you do accidently hit enter, then you will not get the DNS packets in the sniff)

   ping www.guimp.com

4. Don’t close the window …. But bring up Wireshark and start listening on the Ethernet interface
5. **Now** switch back to **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*-Windows_icmp.pcap on your desktop

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 :



ip.proto == ICMP

```
No.  Time     Source          Destination     Protocol Length Info
1025 3.231227 136.165.68.180  77.92.69.132    ICMP        74 Echo (ping) request  id=0x0001, seq=65/16640, ttl=128 (reply in 1041)
1041 3.327875 77.92.69.132    136.165.68.180  ICMP        74 Echo (ping) reply    id=0x0001, seq=65/16640, ttl=52 (request in 1025)
2624 4.242266 136.165.68.180  77.92.69.132    ICMP        74 Echo (ping) request  id=0x0001, seq=66/16896, ttl=128 (reply in 2856)
2856 4.338937 77.92.69.132    136.165.68.180  ICMP        74 Echo (ping) reply    id=0x0001, seq=66/16896, ttl=52 (request in 2624)
4603 5.261243 136.165.68.180  77.92.69.132    ICMP        74 Echo (ping) request  id=0x0001, seq=67/17152, ttl=128 (reply in 4760)
4760 5.357860 77.92.69.132    136.165.68.180  ICMP        74 Echo (ping) reply    id=0x0001, seq=67/17152, ttl=52 (request in 4603)
5688 6.268784 136.165.68.180  77.92.69.132    ICMP        74 Echo (ping) request  id=0x0001, seq=68/17408, ttl=128 (reply in 5717)
5717 6.365444 77.92.69.132    136.165.68.180  ICMP        74 Echo (ping) reply    id=0x0001, seq=68/17408, ttl=52 (request in 5688)
```

```
> Frame 1025: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Vmware_aa:af:ea (00:50:56:aa:af:ea), Dst: Cisco_74:3c:00 (00:1e:79:74:3c:00)
> Internet Protocol Version 4, Src: 136.165.68.180, Dst: 77.92.69.132
> Internet Control Message Protocol
```

```
0000  00 1e 79 74 3c 00 00 50  56 aa af ea 08 00 45 00   ··yt<··P V·····E·
0010  00 3c 14 30 00 00 80 01  00 00 88 a5 44 b4 4d 5c   ·<·0···· ····D·M\
0020  45 84 08 00 4d 1a 00 01  00 41 61 62 63 64 65 66   E···M··· ·Aabcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

wireshark_EE1B667F-C83E-40F1-921E-0611BBAF0CAD_20180912215123_a09152.pcapng

Packets: 5981 · Displayed: 8 (0.1%) · Dropped: 0 (0.0%)

Profile: Defa

9:53 PM
9/12/2018

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 ? **74**

   What is the **actual** source MAC? **00:50:56:aa:af:ea**
   What does shark identify as the “vendor” portion of the source MAC? **Vmware_aa:af:ea**

   What is the **actual** destination MAC? **00:1e:79:74:3c:00**
   What does shark identify as the “vendor” portion of the destination MAC? **Cisco_74:3c:00**

   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** ? **128**
   Describe the payload data **: it’s a 32 bytes and the alphabets abcdefghijklmn opqrstuvwabcdefg hi**

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** ? **52**

    Did the payload data change? **no**

11. Save this updated Word file with your responses as

    Lab1-*section#-yourname*-Windows_icmp.docx on your desktop

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