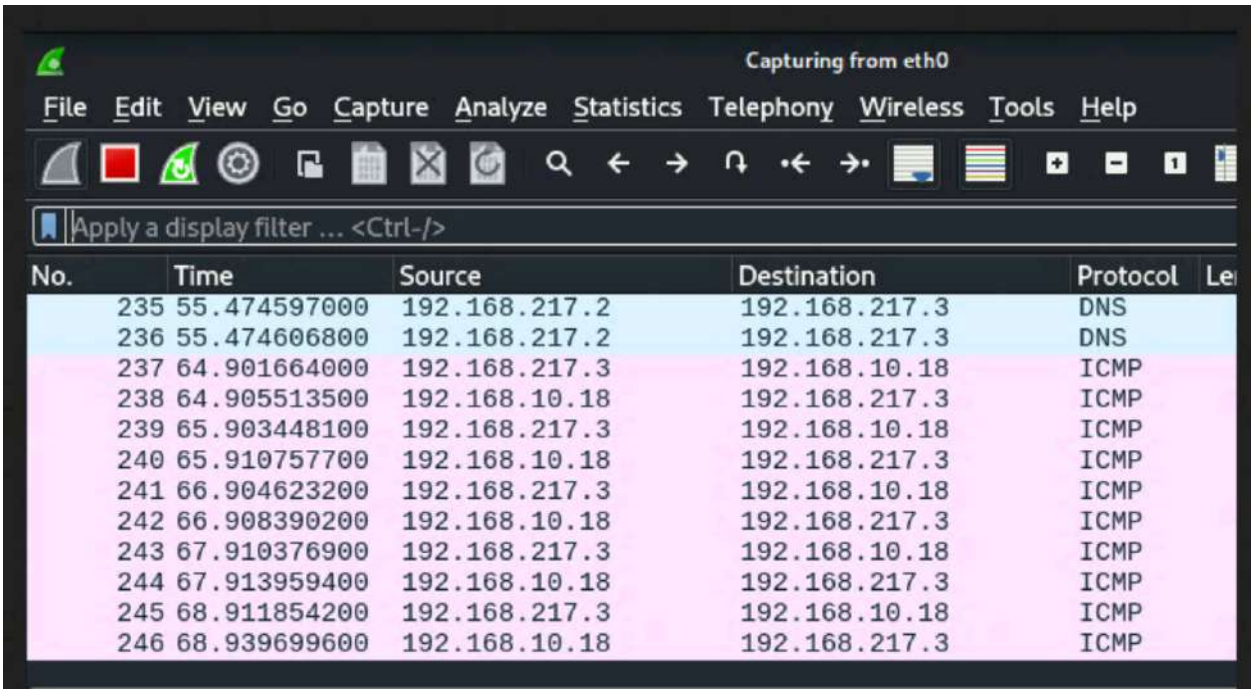
CYSE 301 Assignment 2

Derek D. Hillman
UIN:00861068

Task A

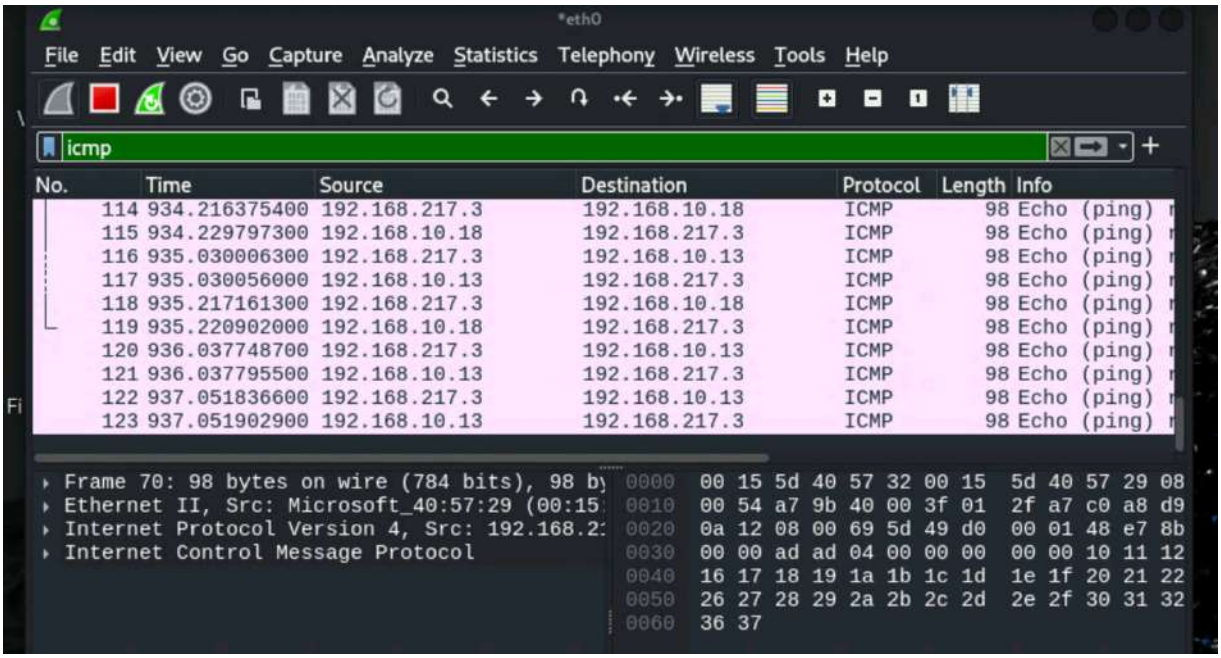
Question 1

246 Packets were captured



Question 2.

I used the ICMP filter below.

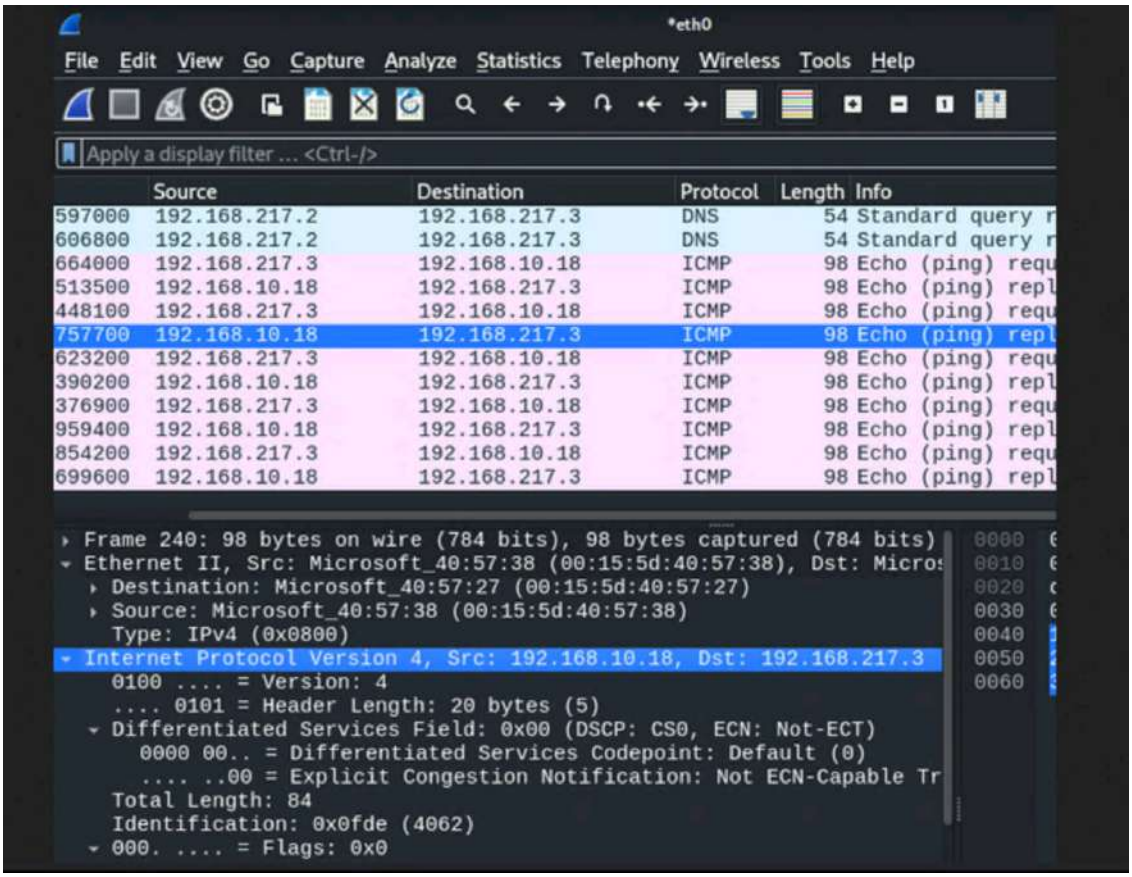


CYSE 301 Assignment 2

Derek D. Hillman
UIN:00861068

Question 3

The source IP is **192.168.10.18** and the destination IP is **192.168.217.3** as highlighted below.

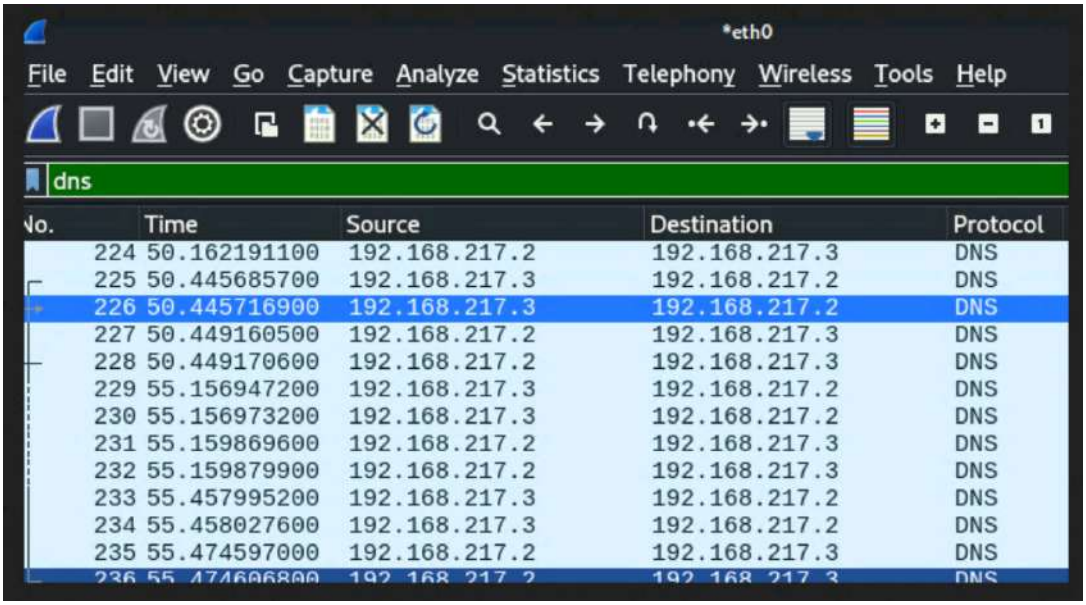


Question 4

I used the DNS filter to view all of the DNS packets below. There were a total of 236 DNS packets.

CYSE 301 Assignment 2

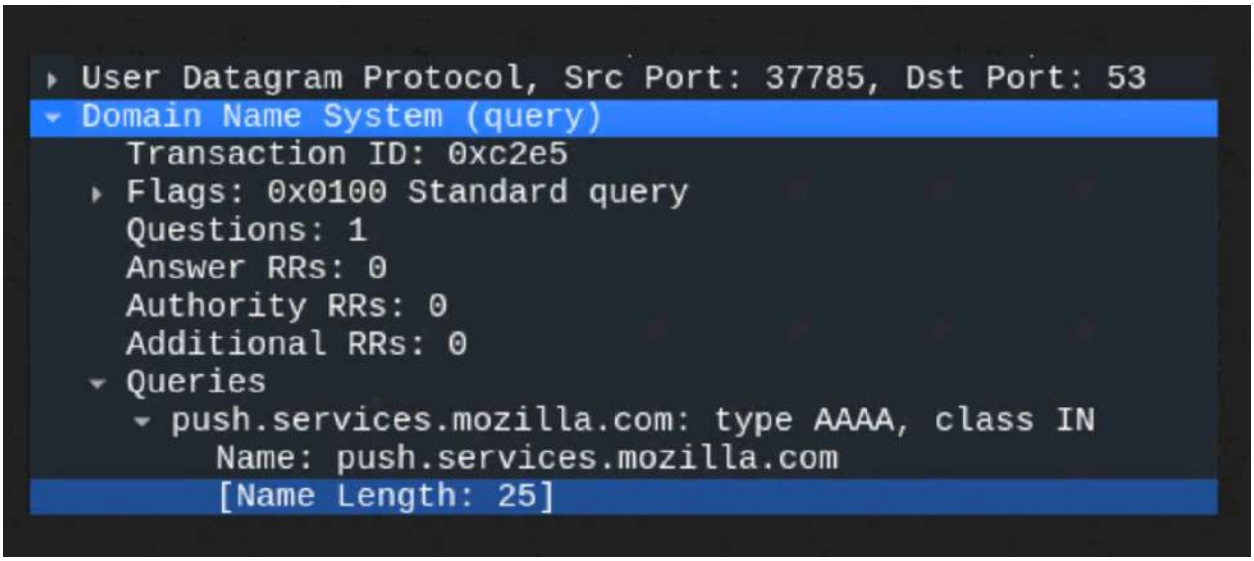
Derek D. Hillman
UIN:00861068



Question 5.

The domain name the host is trying to resolve is mozilla.com.

The source IP is the IP of the VM at **192.168.217.3** and the source port is **37785**. The destination IP is **192.168.217.2** and the destination port is **53**. Since we are using a lab that doesn't have internet access the default network gateway is the destination IP.

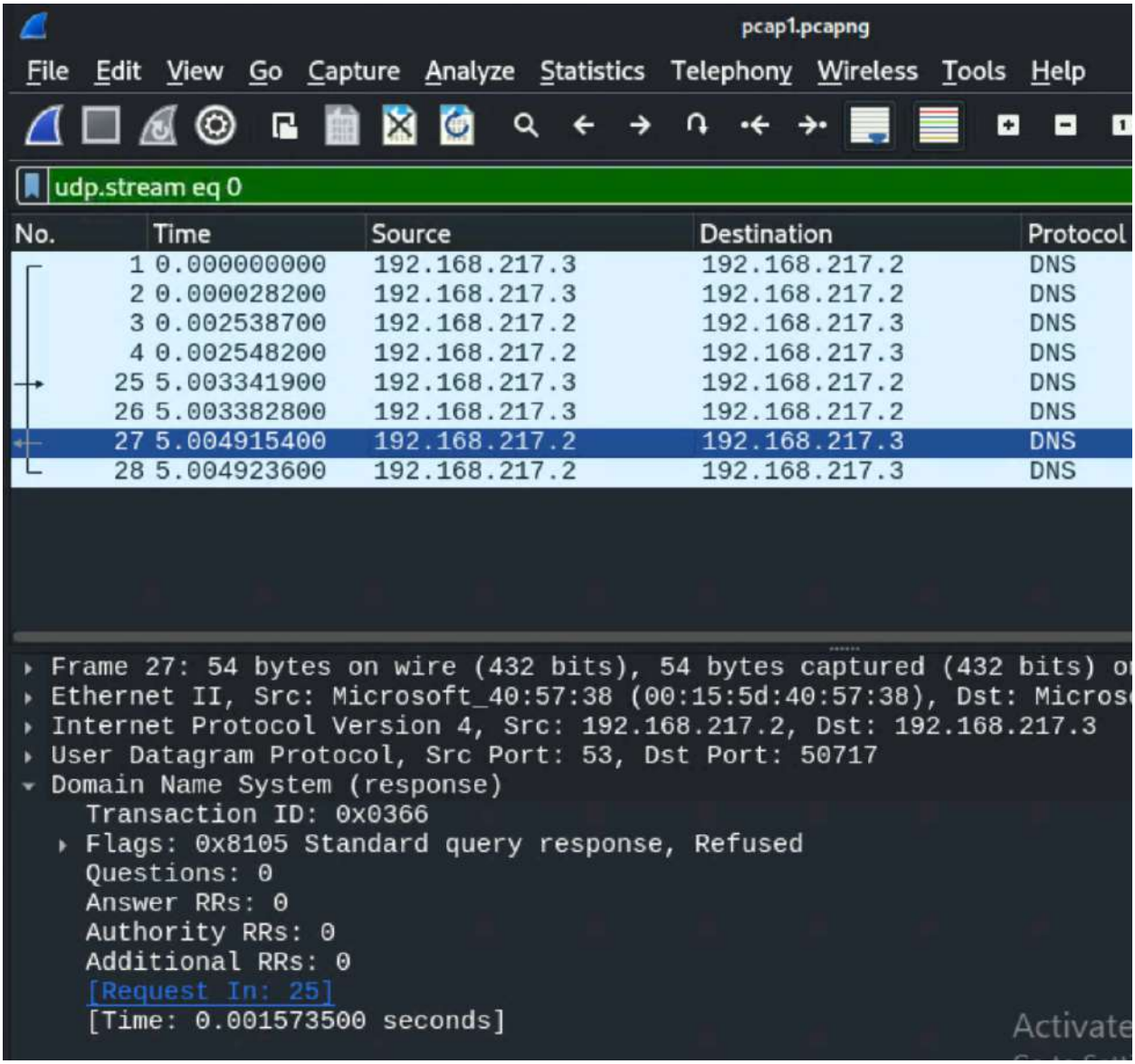


Question 6

The DNS response was refused due to the inability to touch the internet. The Source IP is **192.168.217.2** and the source port is **53.** The Destination IP is **192.168.217.3** and the destination port is **50717**

CYSE 301 Assignment 2

Derek D. Hillman
UIN:00861068



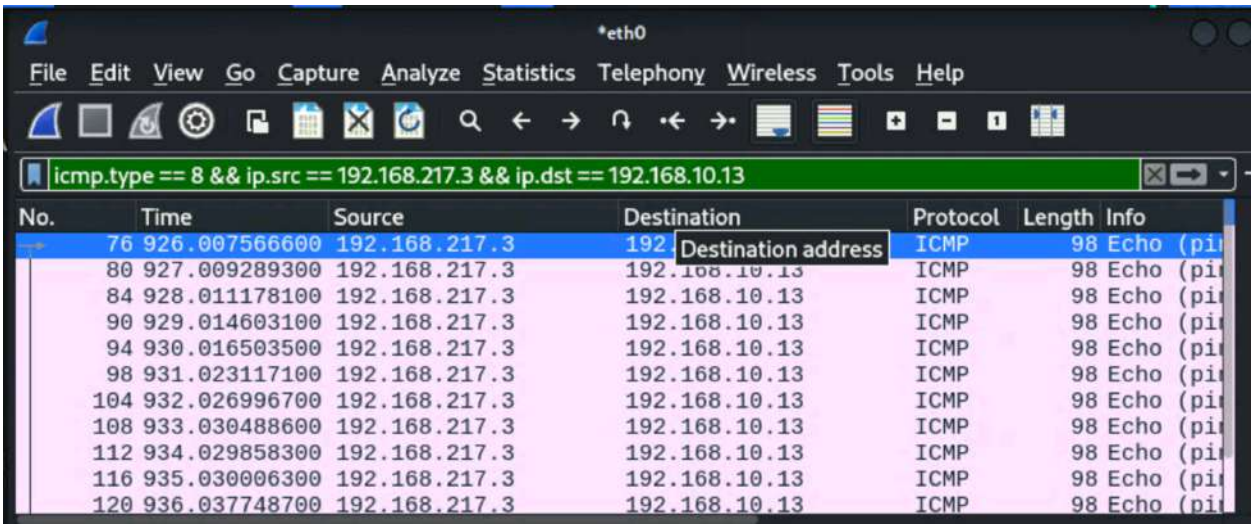
CYSE 301 Assignment 2

Derek D. Hillman
UIN:00861068

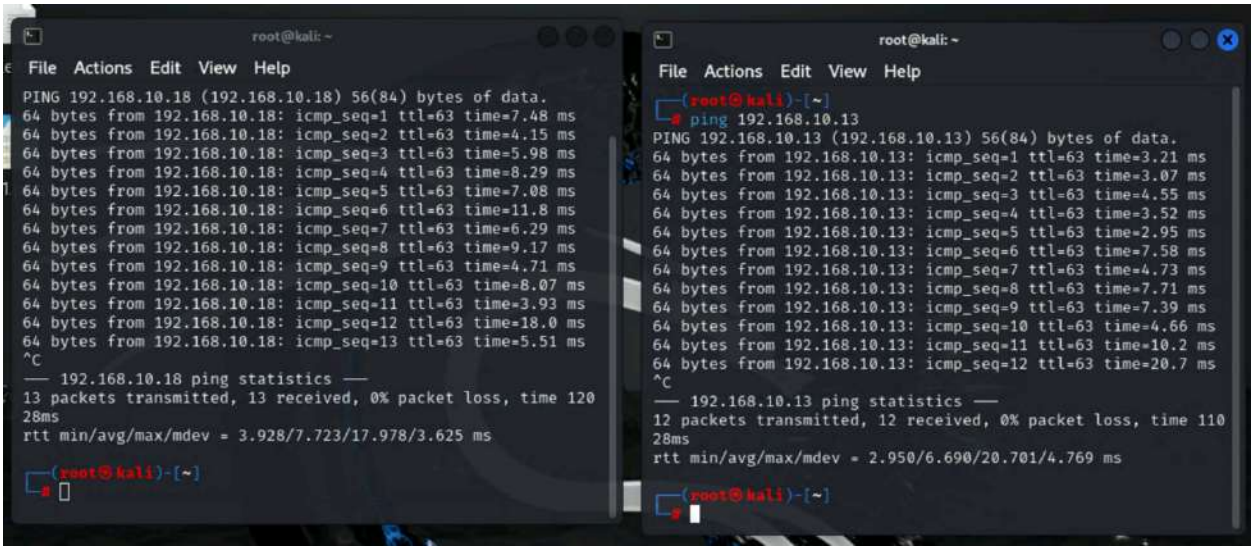
Task B

Question 1

A. I launched wireshark as instructed from the Internal Kali VM



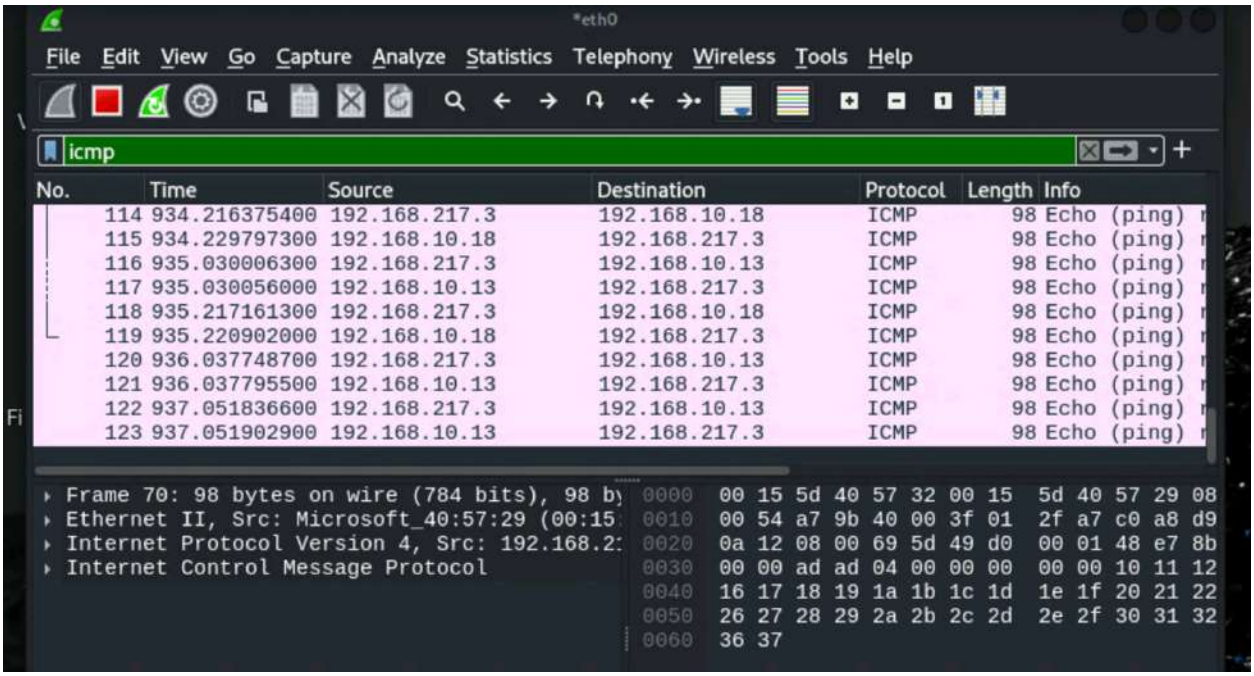
B. I opened two CLI terminals and pinged both vm's for a few seconds.



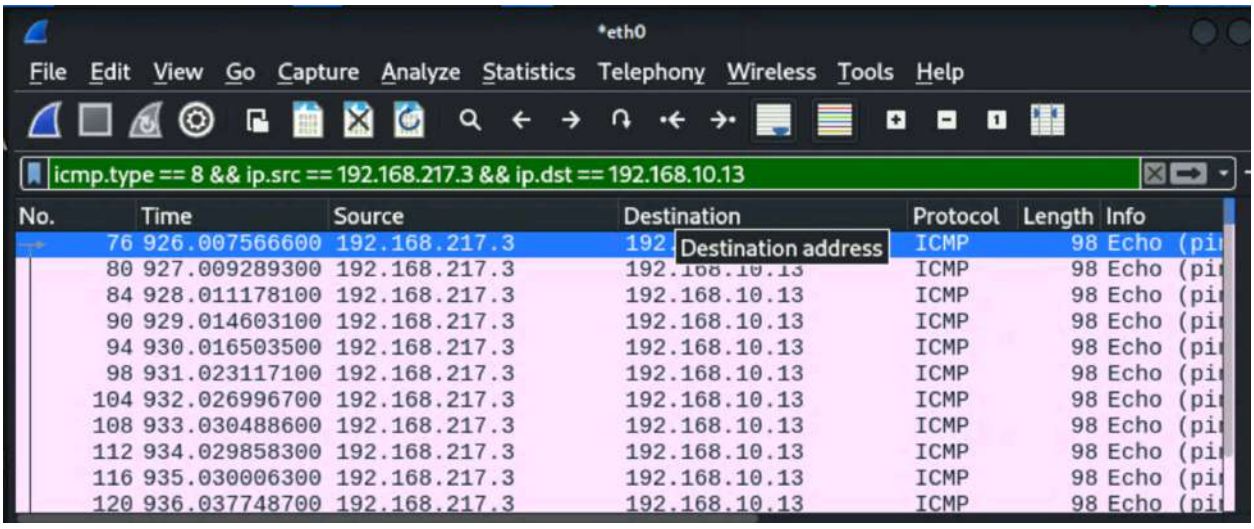
CYSE 301 Assignment 2

Derek D. Hillman
UIN:00861068

C. I applied the ICMP packet filter.



D. I applied a filter that listed ICMP packets with the specifications of the exact source and IP destination with the ip.dst syntax.

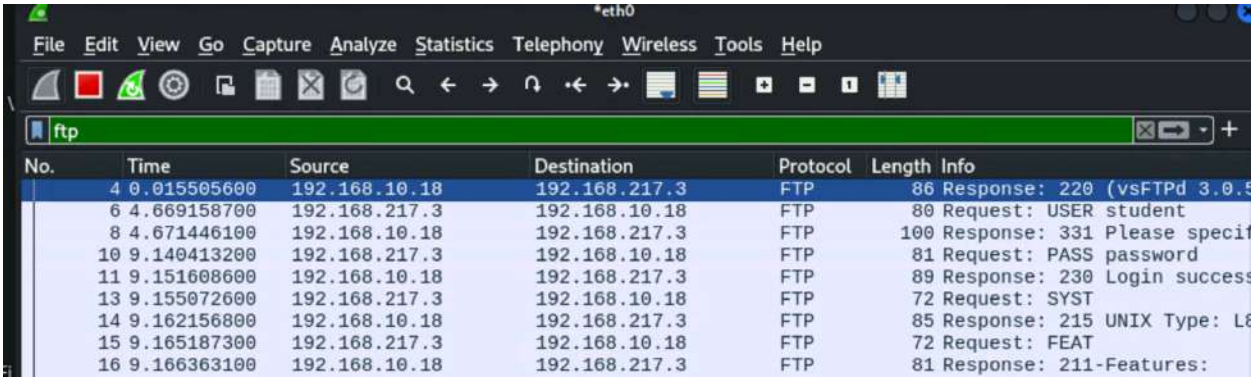


Question 2

CYSE 301 Assignment 2

Derek D. Hillman
UIN:00861068

A. From the CLI I executed ftp 192.168.10.13 to login to the FTP server. I captured packets while I logged in. I utilized the FTP filter to see the plain text in Wireshark



B After utilizing the FTP filter as you can see to the right the input from the VM has been captured and it can be read because it is in plain text. FTP is a non-encrypted protocol so anything passed between two systems on this port the traffic can be sniffed.

C. I repeated the steps again but with my MIDAS ID and through Wireshark you can see that there is a login error. In the image below you can see the request for the user and the source and where I typed in my username. You can also see the failed password attempt but since that password is my live MIDAS ID I intentionallyleft it out of the image.