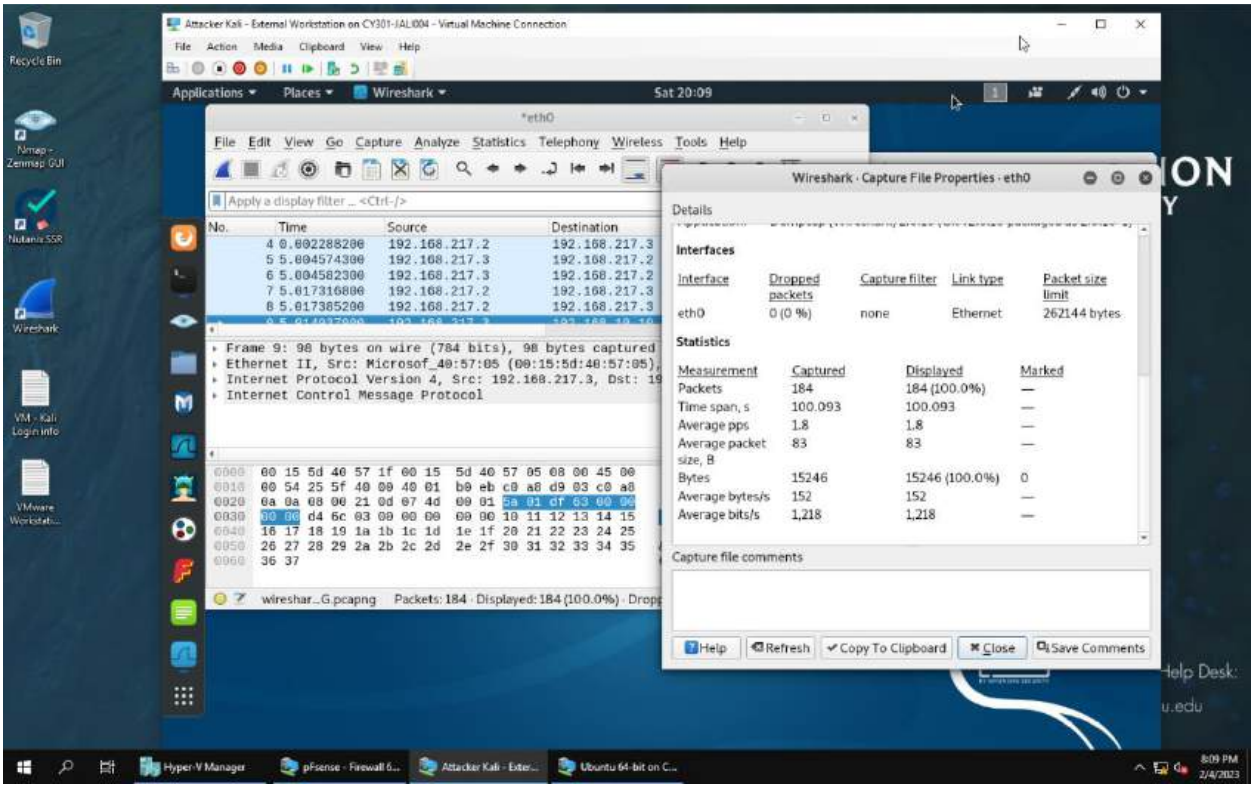
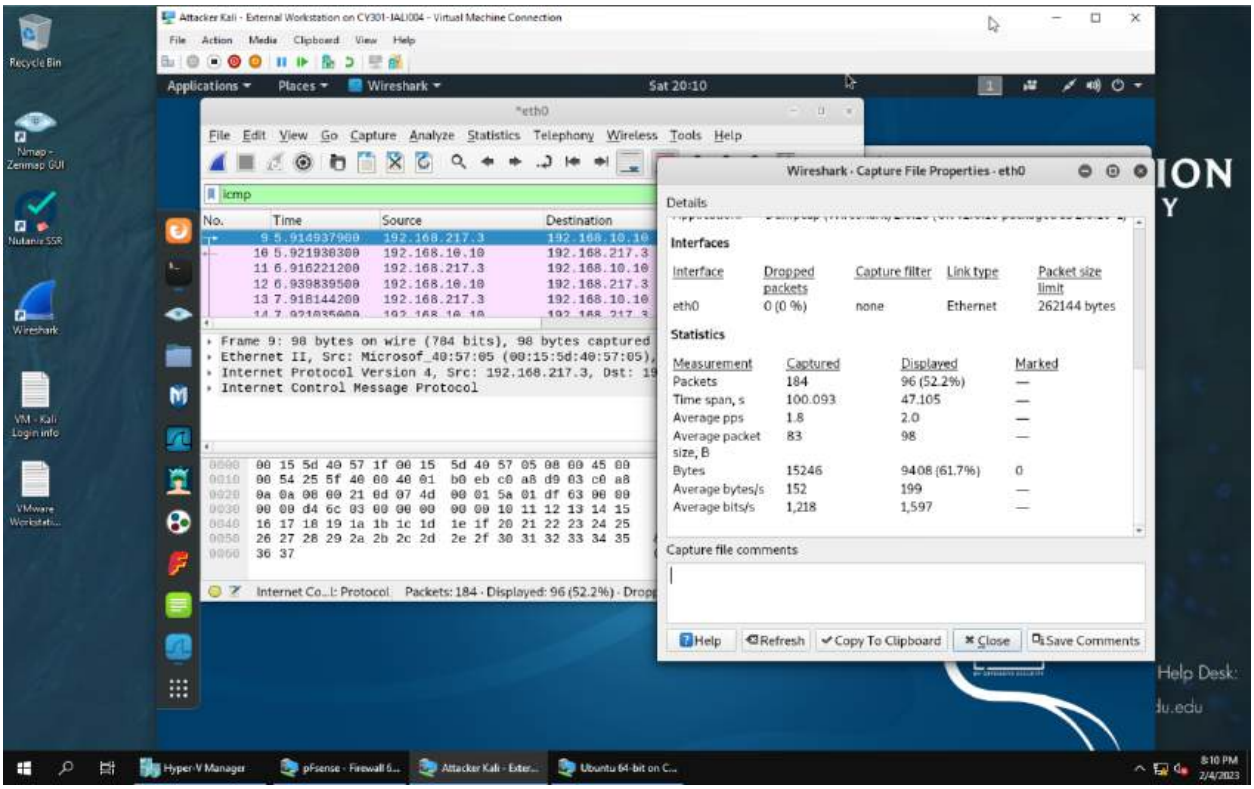
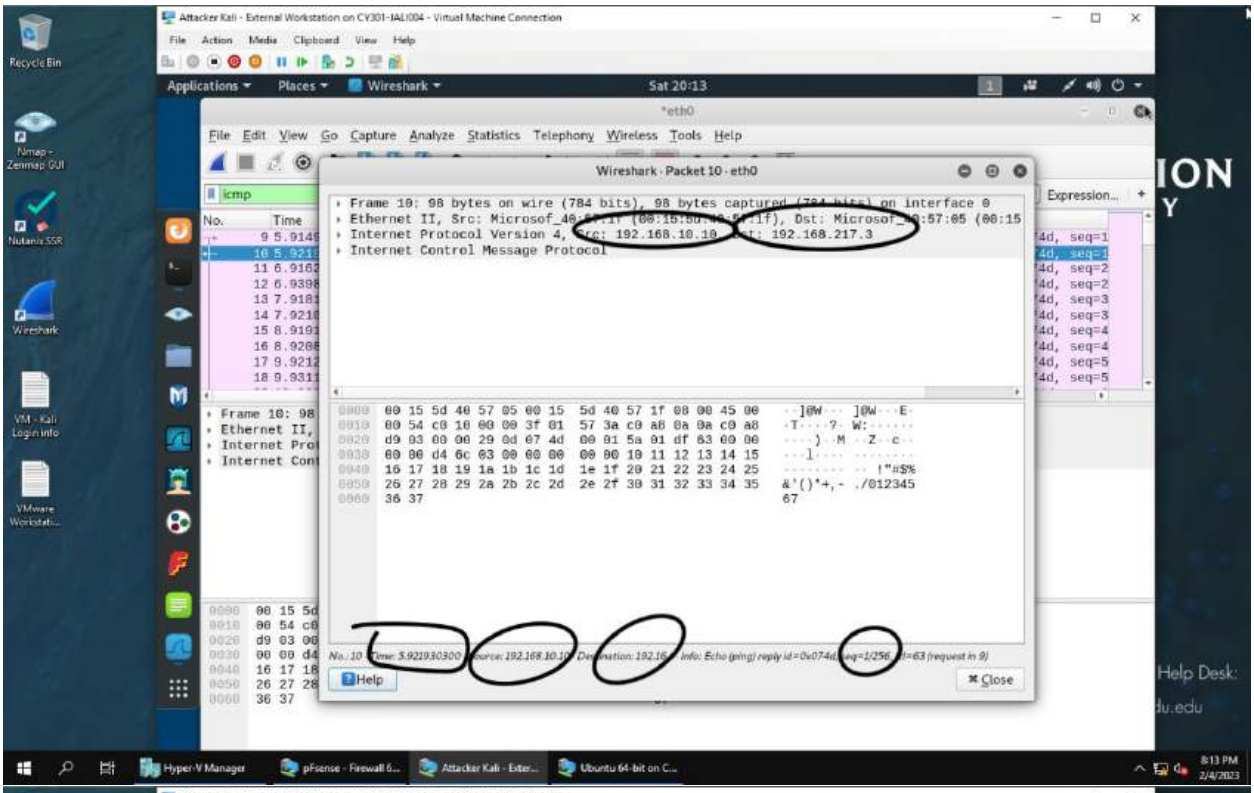
TASK A

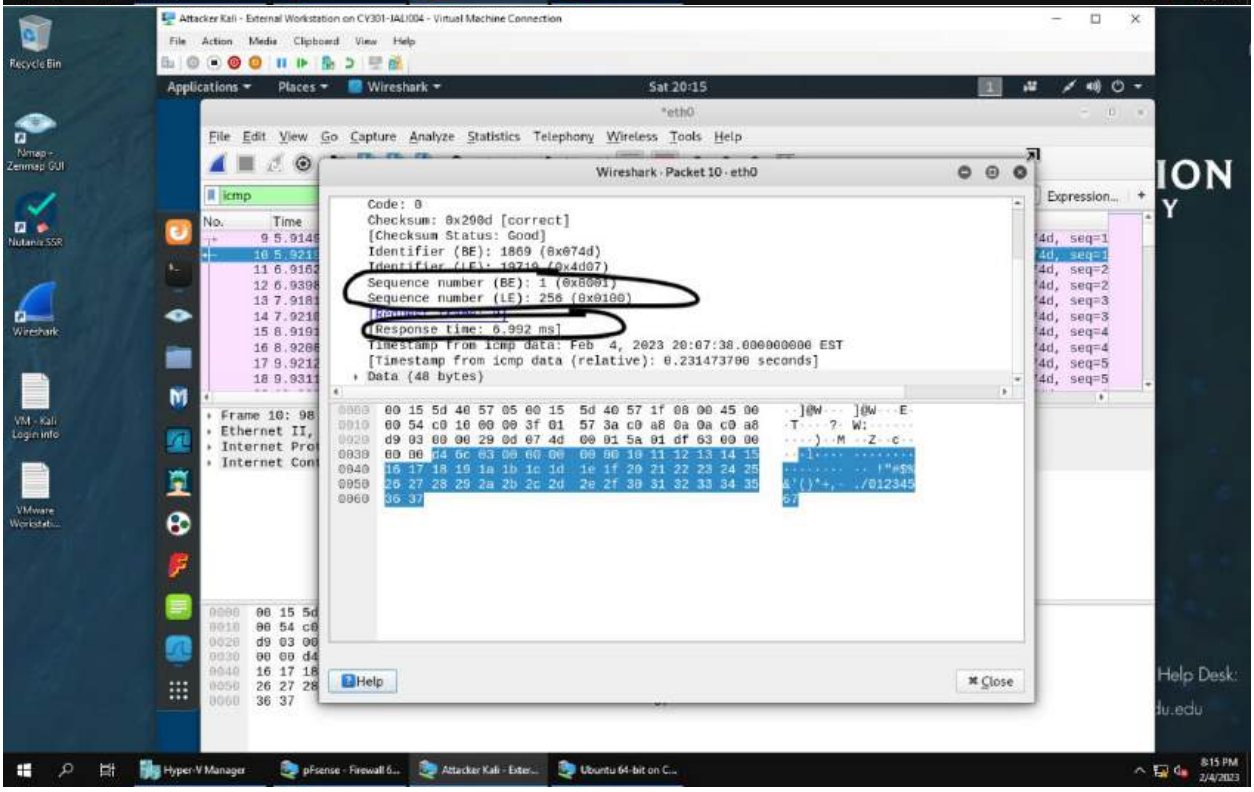


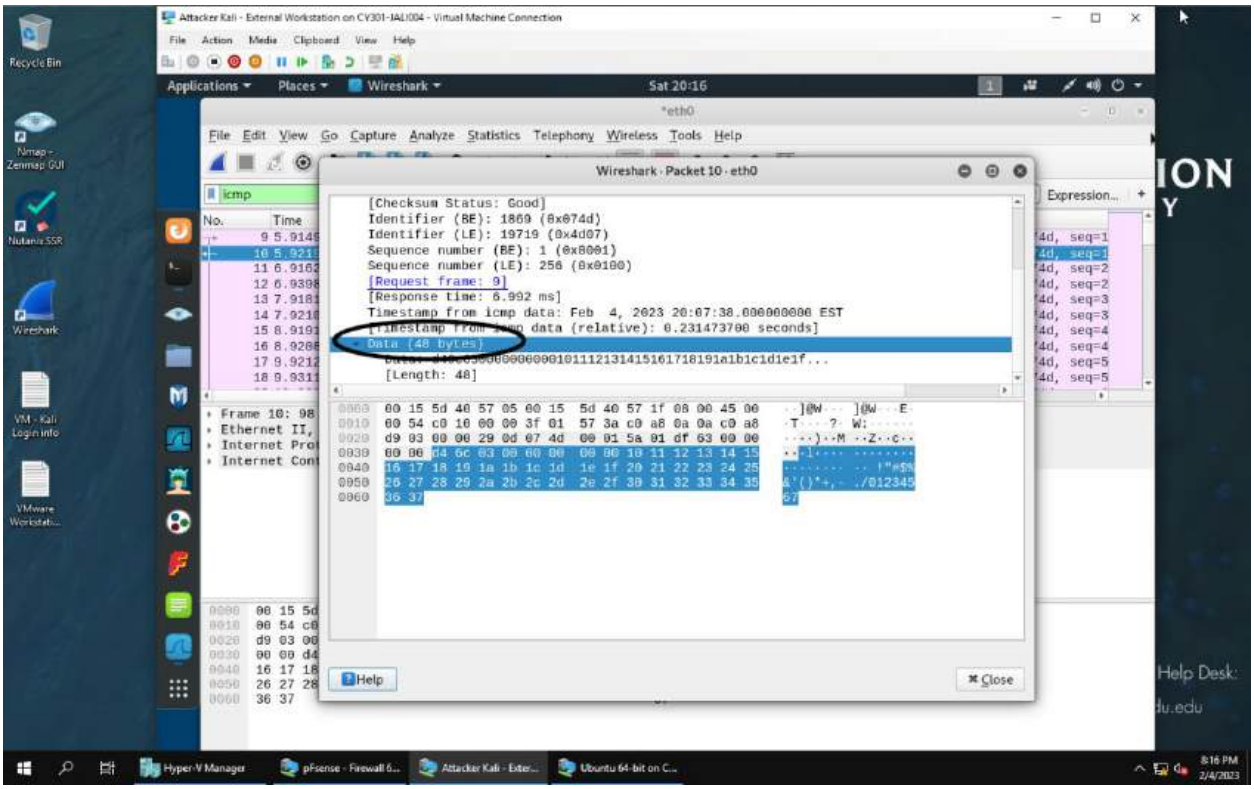
1. Opened up Statistics, capture file properties to see 184 total and displaying all. Also located on bottom of first Wireshark pane. 184 packets in total and all 184 are being displayed because I did not apply a filter.



2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question (Q1).
   After applying the filter icmp (internet control message protocol), WireShark will display 96 of the original 194 packets.

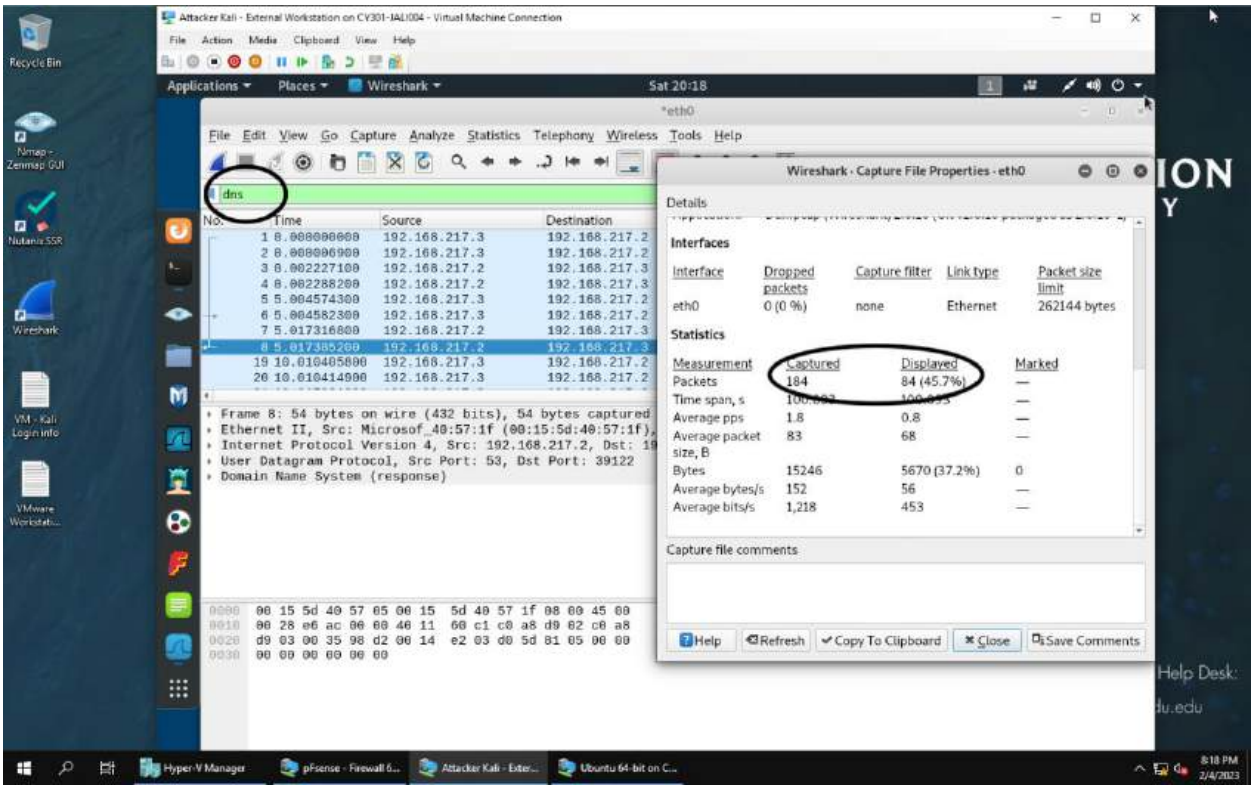

Attacker Kali - External Workstation on CY301-IALI004 - Virtual Machine Connection
Wireshark · Packet 10 · eth0
Frame 10: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Microsof_40:57:1f (00:15:5d:40:57:1f), Dst: Microsof_40:57:05 (00:15
Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.217.3
Internet Control Message Protocol
Help
Close


Attacker Kali - External Workstation on CY301-IALI004 - Virtual Machine Connection
Wireshark · Packet 10 · eth0
Code: 0
Checksum: 0x298d [correct]
[Checksum Status: Good]
Identifier (BE): 1869 (0x074d)
Identifier (LE): 19719 (0x4d07)
Sequence number (BE): 1 (0x0001)
Sequence number (LE): 256 (0x0100)
[Response time: 6.992 ms]
Timestamp from icmp data: Feb 4, 2023 20:07:38.000000000 EST
[Timestamp from icmp data (relative): 0.231473700 seconds]
Data (48 bytes)
Help
Close

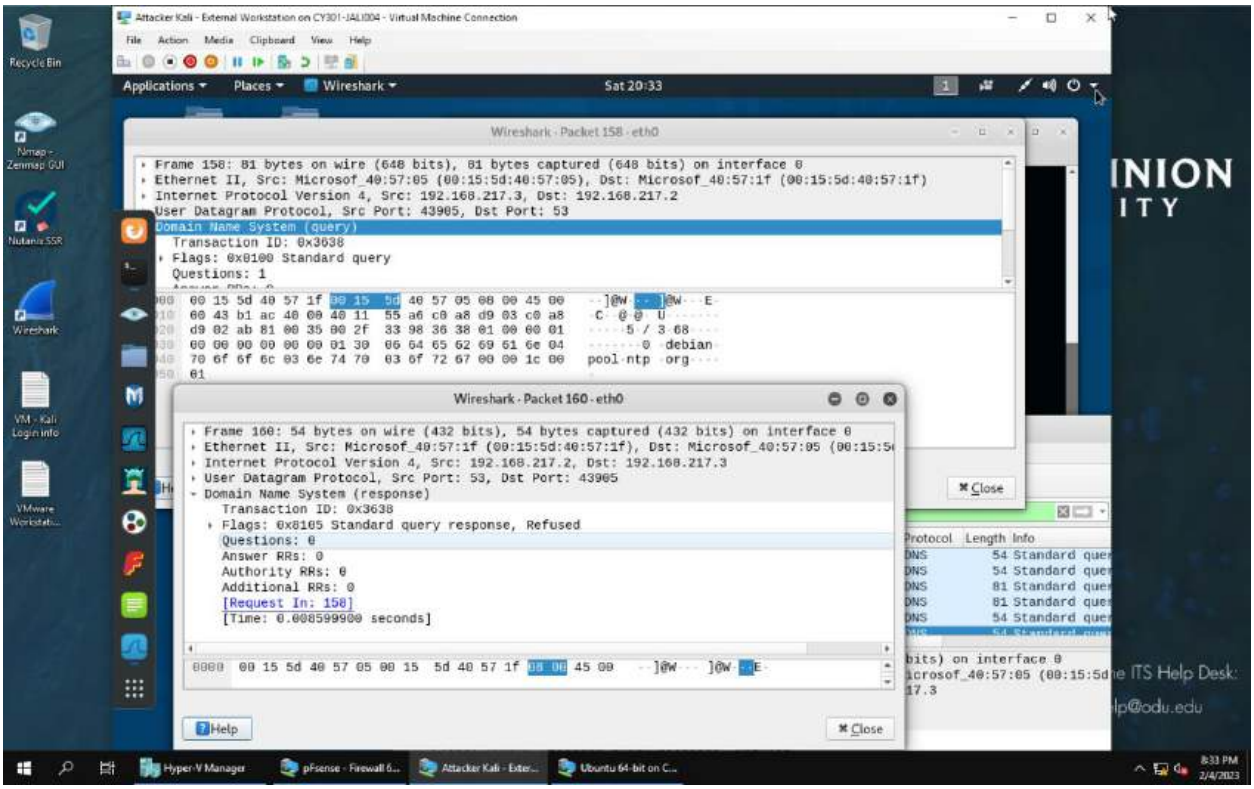


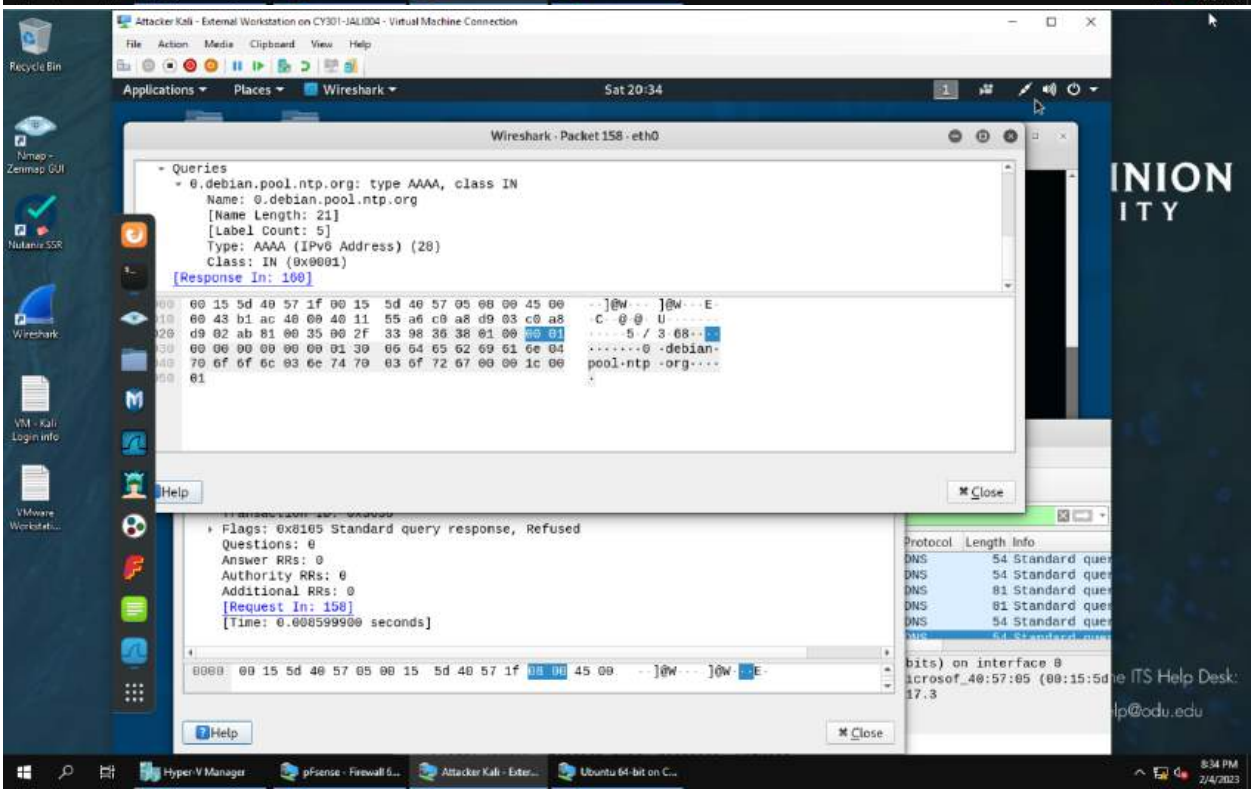
3. Selected echo message from link using the icmp (internet control message protocol) filter, double clicked, information can be found in bottom of pane but also in Internet Protocol dropdown. Information is as follows:

   Source IP is 192.168.10.10, Dst IP is 192.168.217.3; sequence number is 1 ; size of data is 48 bytes; response time is located at bottom of first pane 5.92… ms.



4. Applied DNS (domain name system) display filter in Wireshark, 84 of the original 184 are displayed.





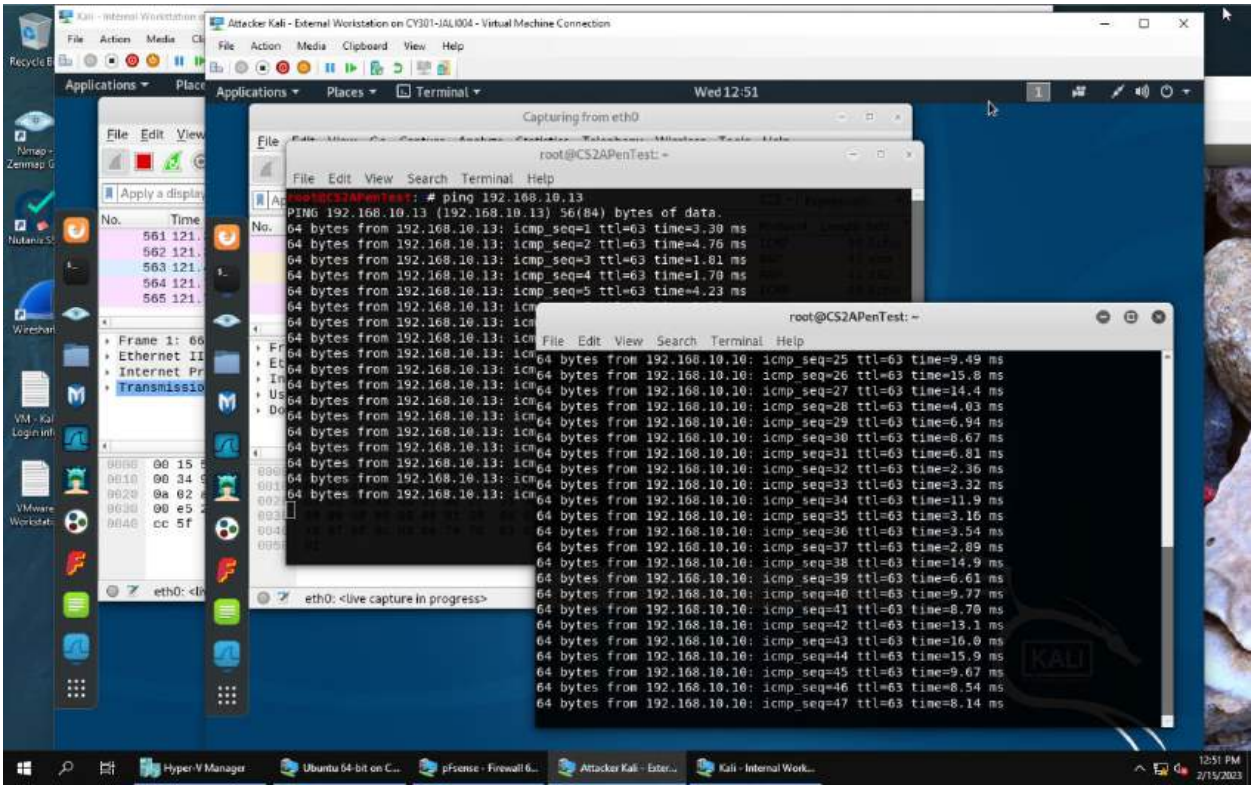
5. Found a DNS query packet by looking at the description “query” to located the correct packet. The domain name the host is trying to resolve is debian.pool.ntp.org and can be found within the

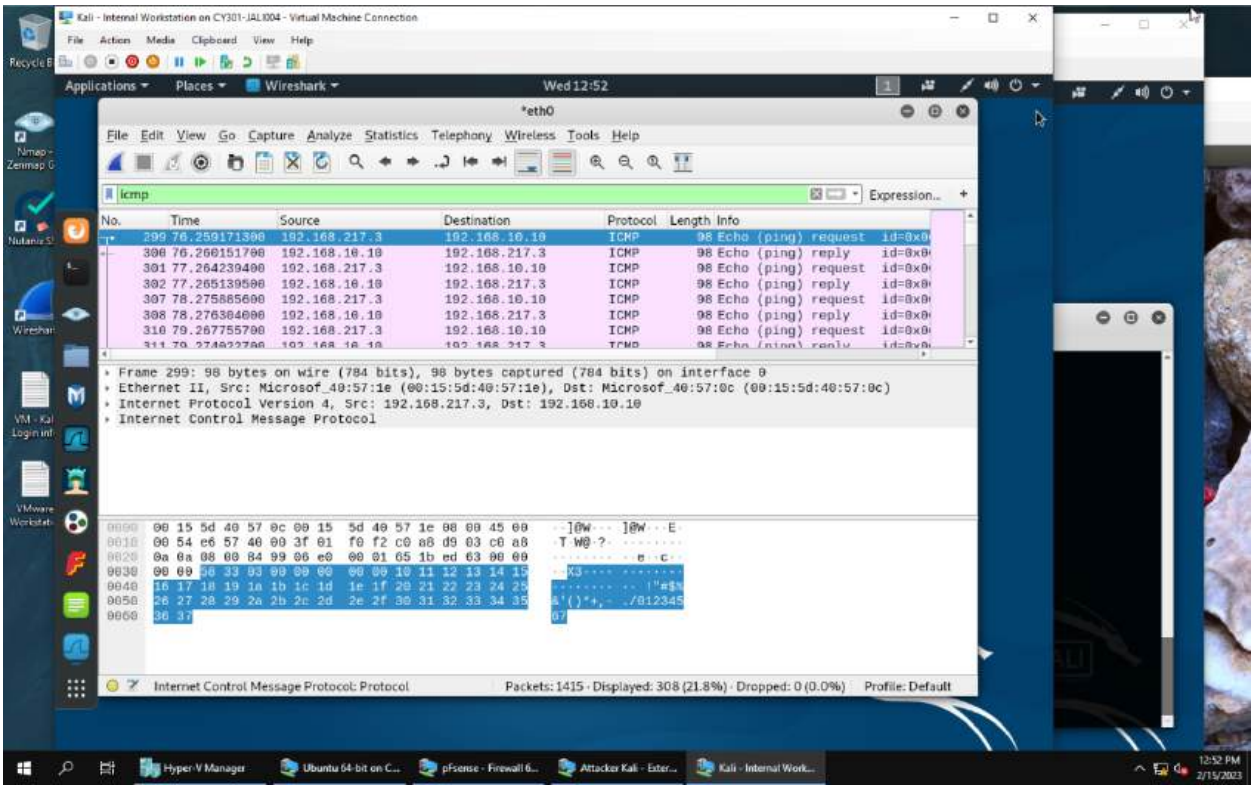
message as shown above. The source IP and port number is **192.168.217.3: 43905** and destination IP and port number is **192.168.217.2: 53**.

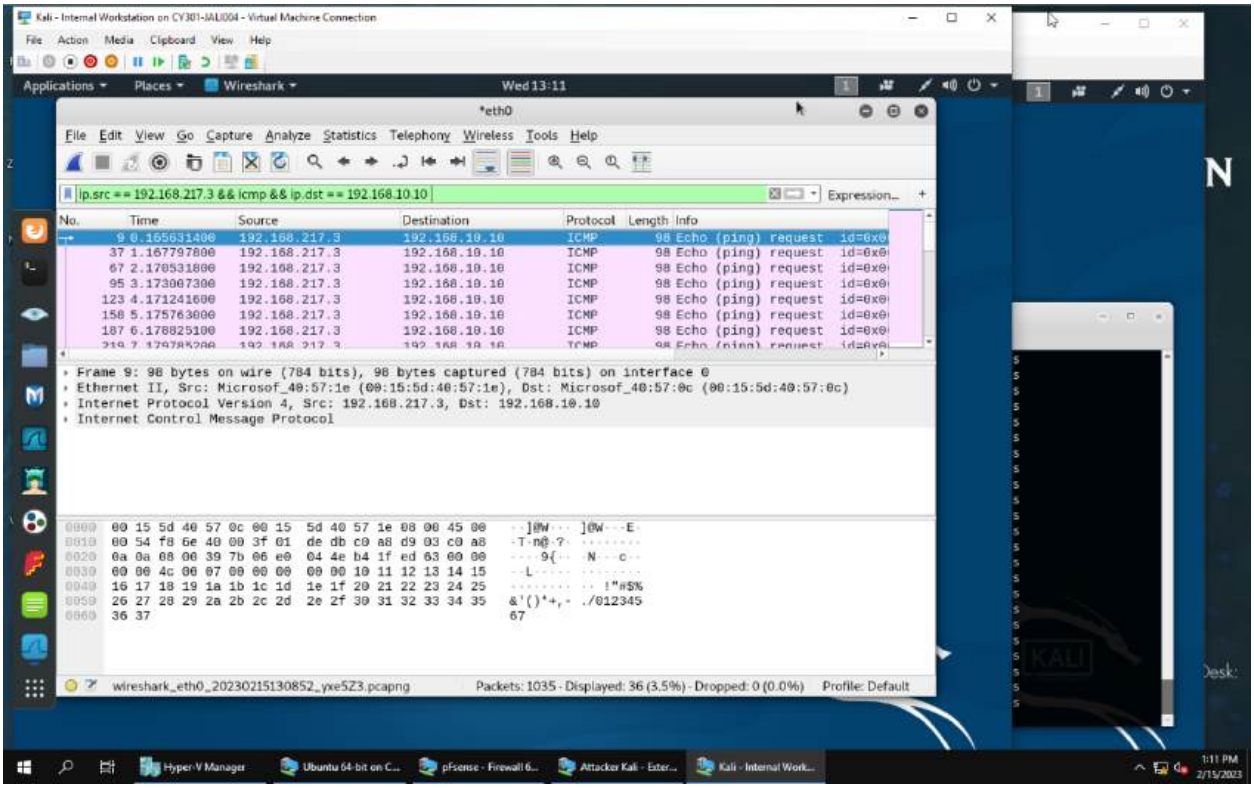
6. Found the **corresponding** DNS response by looking at the listing description as I am following the flipped IP address. Source is now destination and vice versa. Also, Wireshark also has information of response and request, which can be found by expanding DNS row within listing. The source IP and port number is **192.168.217.2: 53** and the destination source IP and port number is **192.168.217.3: 43905.** The response is "refused" meaning DNS refuses to preform operations. This is because the VM is not connected to the internet.

TASK B

1. Sniff ICMP Traffic



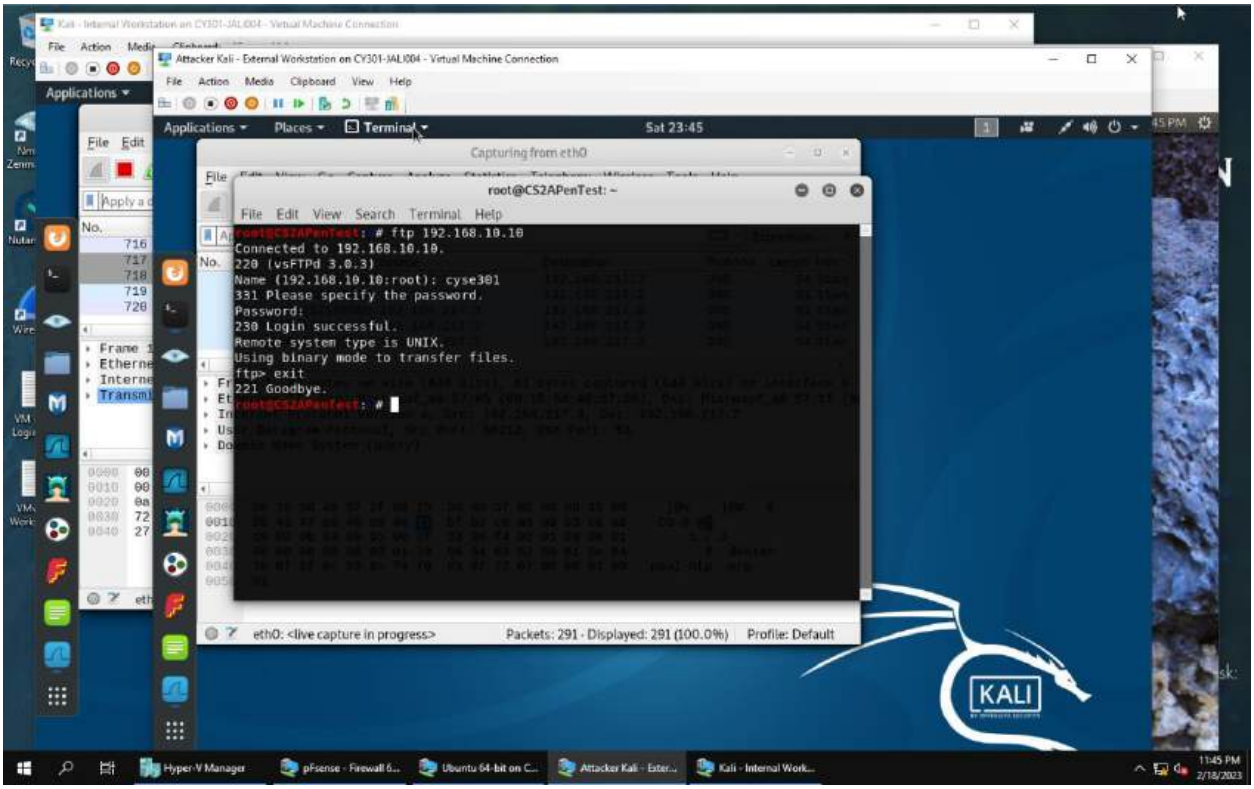


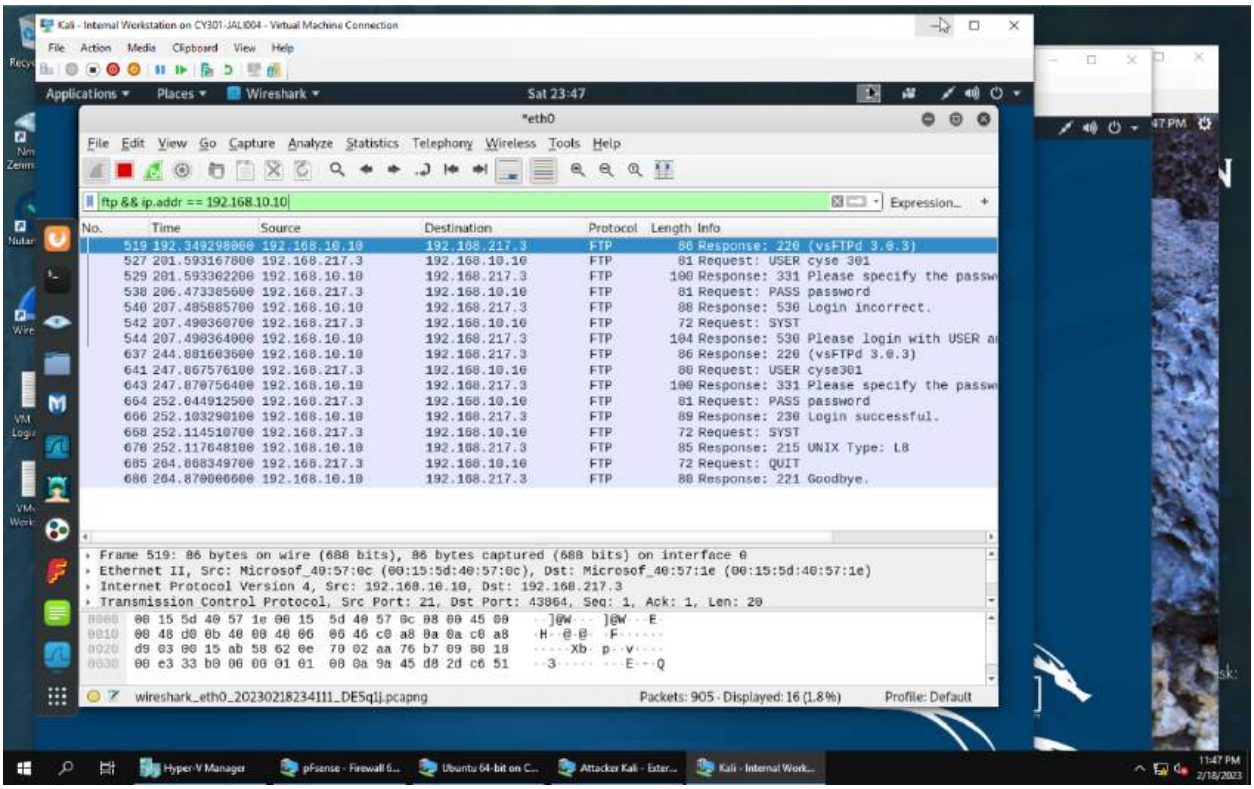


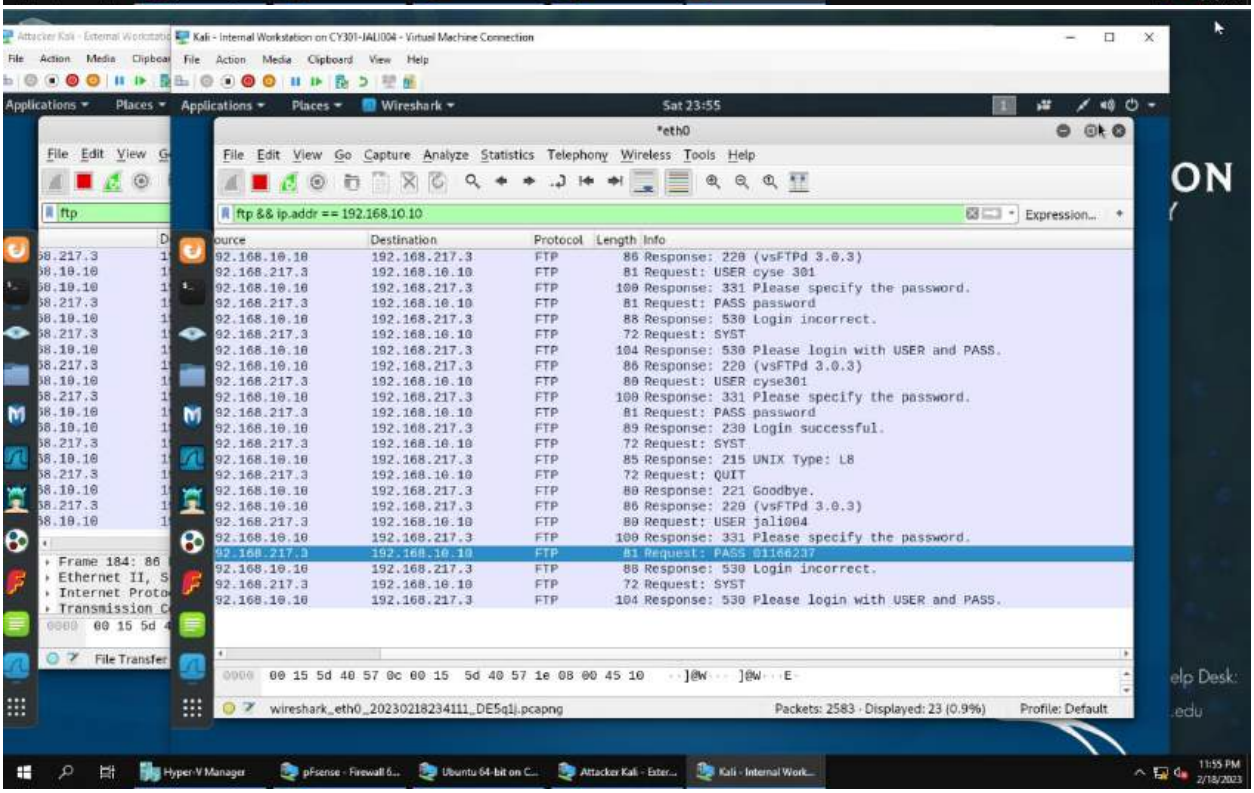
Explanation: Opened two terminals on Ext. Kali VM and used “ping” command to create traffic for Ubuntu (192.168.10.10) and Int. Kali (192.168.19.13). Then applied “icmp” display filter on Int. Kali VM

to view ICMP traffic. Lastly, I applied proper display filter “ip.src ==192.168.217.3 && icmp && ip.dst. ==192.168.10.10”on Internal Kali VM that ONLY displays ICMP request originating from External Kali VM and going to Ubuntu 64-bit VM. The first part of the display filter specifies where the traffic came from while the second part defines the type of traffic, and the last or third part defines the destination. The operators && mean that all conditions must be met to display packet.

2. Sniff FTP Traffic




Kali - Internal Workstation on CY301-JALI004 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark Sat 23:47
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp && ip.addr == 192.168.10.10
No. Time Source Destination Protocol Length Info
519 192.349298000 192.168.10.10 192.168.217.3 FTP 86 Response: 220 (vsFTPd 3.0.3)
527 201.593167800 192.168.217.3 192.168.10.10 FTP 81 Request: USER cyse 301
529 201.593362200 192.168.10.10 192.168.217.3 FTP 100 Response: 331 Please specify the passw
538 206.473385600 192.168.217.3 192.168.10.10 FTP 81 Request: PASS password
540 207.485885700 192.168.10.10 192.168.217.3 FTP 88 Response: 530 Login incorrect.
542 207.490360700 192.168.217.3 192.168.10.10 FTP 72 Request: SYST
544 207.490364000 192.168.10.10 192.168.217.3 FTP 104 Response: 530 Please login with USER a
637 244.881603600 192.168.10.10 192.168.217.3 FTP 86 Response: 220 (vsFTPd 3.0.3)
641 247.867576100 192.168.217.3 192.168.10.10 FTP 80 Request: USER cyse301
643 247.870756400 192.168.10.10 192.168.217.3 FTP 100 Response: 331 Please specify the passw
664 252.044912500 192.168.217.3 192.168.10.10 FTP 81 Request: PASS password
666 252.103290100 192.168.10.10 192.168.217.3 FTP 89 Response: 230 Login successful.
668 252.114510700 192.168.217.3 192.168.10.10 FTP 72 Request: SYST
670 252.117648100 192.168.10.10 192.168.217.3 FTP 85 Response: 215 UNIX Type: L8
685 264.868349700 192.168.217.3 192.168.10.10 FTP 72 Request: QUIT
686 264.870006600 192.168.10.10 192.168.217.3 FTP 80 Response: 221 Goodbye.
Frame 519: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: Microsof_40:57:0c (00:15:5d:40:57:0c), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e)
Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.217.3
Transmission Control Protocol, Src Port: 21, Dst Port: 43864, Seq: 1, Ack: 1, Len: 20
wireshark_eth0_20230218234111_DE5q1j.pcapng
Packets: 905 · Displayed: 16 (1.8%)
Profile: Default
Hyper-V Manager
pFsense - Firewall 6...
Ubuntu 64-bit on C...
Attacker Kali - Exter...
Kali - Internal Work...
11:47 PM
2/18/2023


Kali - Internal Workstation on CY301-JALI004 - Virtual Machine Connection
Applications Places Wireshark Sat 23:55
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp && ip.addr == 192.168.10.10
Destination Protocol Length Info
192.168.217.3 FTP 86 Response: 220 (vsFTPd 3.0.3)
192.168.10.10 FTP 81 Request: USER cyse 301
192.168.217.3 FTP 100 Response: 331 Please specify the password.
192.168.10.10 FTP 81 Request: PASS password
192.168.217.3 FTP 88 Response: 530 Login incorrect.
192.168.10.10 FTP 72 Request: SYST
192.168.217.3 FTP 104 Response: 530 Please login with USER and PASS.
192.168.10.10 FTP 86 Response: 220 (vsFTPd 3.0.3)
192.168.217.3 FTP 80 Request: USER cyse301
192.168.10.10 FTP 100 Response: 331 Please specify the password.
192.168.217.3 FTP 81 Request: PASS password
192.168.10.10 FTP 89 Response: 230 Login successful.
192.168.217.3 FTP 72 Request: SYST
192.168.10.10 FTP 85 Response: 215 UNIX Type: L8
192.168.217.3 FTP 72 Request: QUIT
192.168.10.10 FTP 80 Response: 221 Goodbye.
192.168.10.10 FTP 86 Response: 220 (vsFTPd 3.0.3)
192.168.217.3 FTP 80 Request: USER jali004
192.168.10.10 FTP 100 Response: 331 Please specify the password.
192.168.217.3 FTP 81 Request: PASS 01166237
192.168.10.10 FTP 88 Response: 530 Login incorrect.
192.168.217.3 FTP 72 Request: SYST
192.168.10.10 FTP 104 Response: 530 Please login with USER and PASS.
wireshark_eth0_20230218234111_DE5q1j.pcapng
Packets: 2583 · Displayed: 23 (0.9%)
Profile: Default
Hyper-V Manager
pFsense - Firewall 6...
Ubuntu 64-bit on C...
Attacker Kali - Exter...
Kali - Internal Work...
11:55 PM
2/18/2023

Explanation:

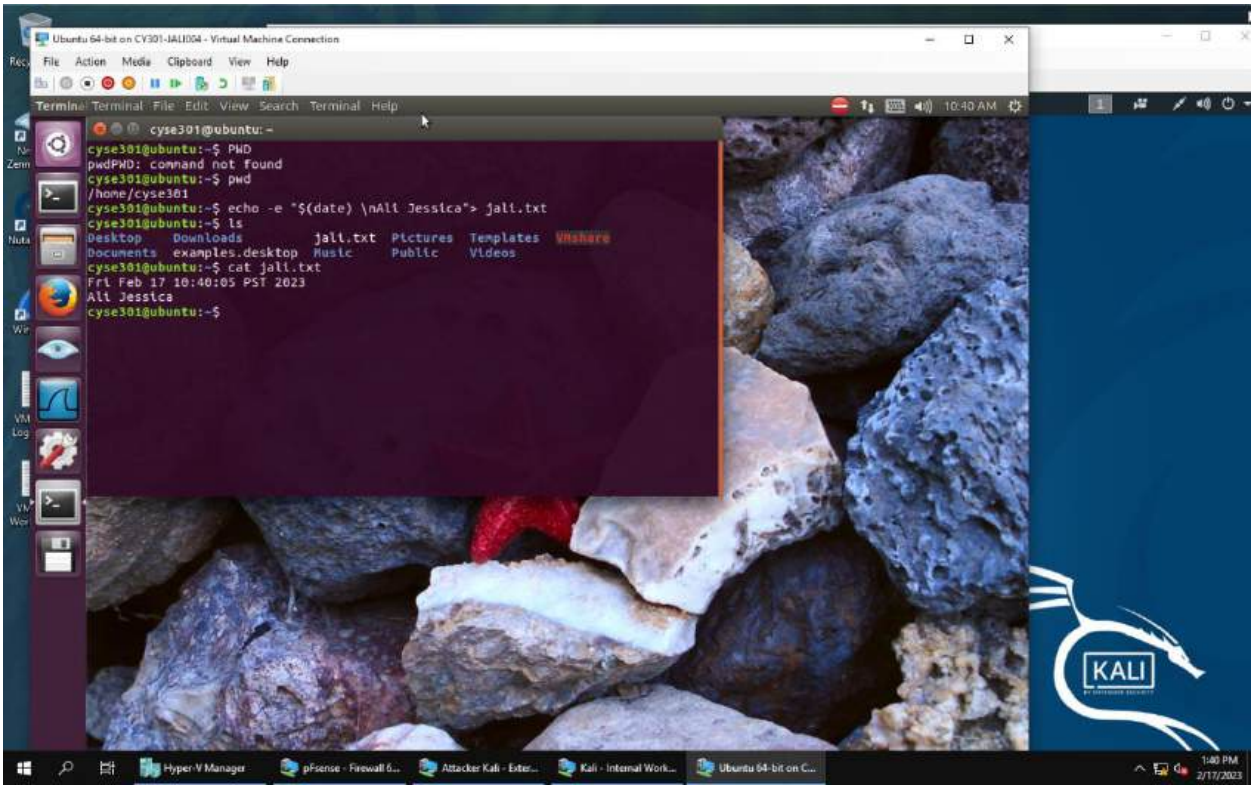
a) Ubuntu VM is also serving as an FTP server inside the LAN network. I use External Kali to access this FTP server by using the command: ftp 192.168.10.10 . The username for the FTP server is cyse301, and the password is password. I followed the steps in the photo to access the FTP server and also exited. I have created FTP traffic. While the password I typed did not show up in the terminal, it will in the traffic packets.

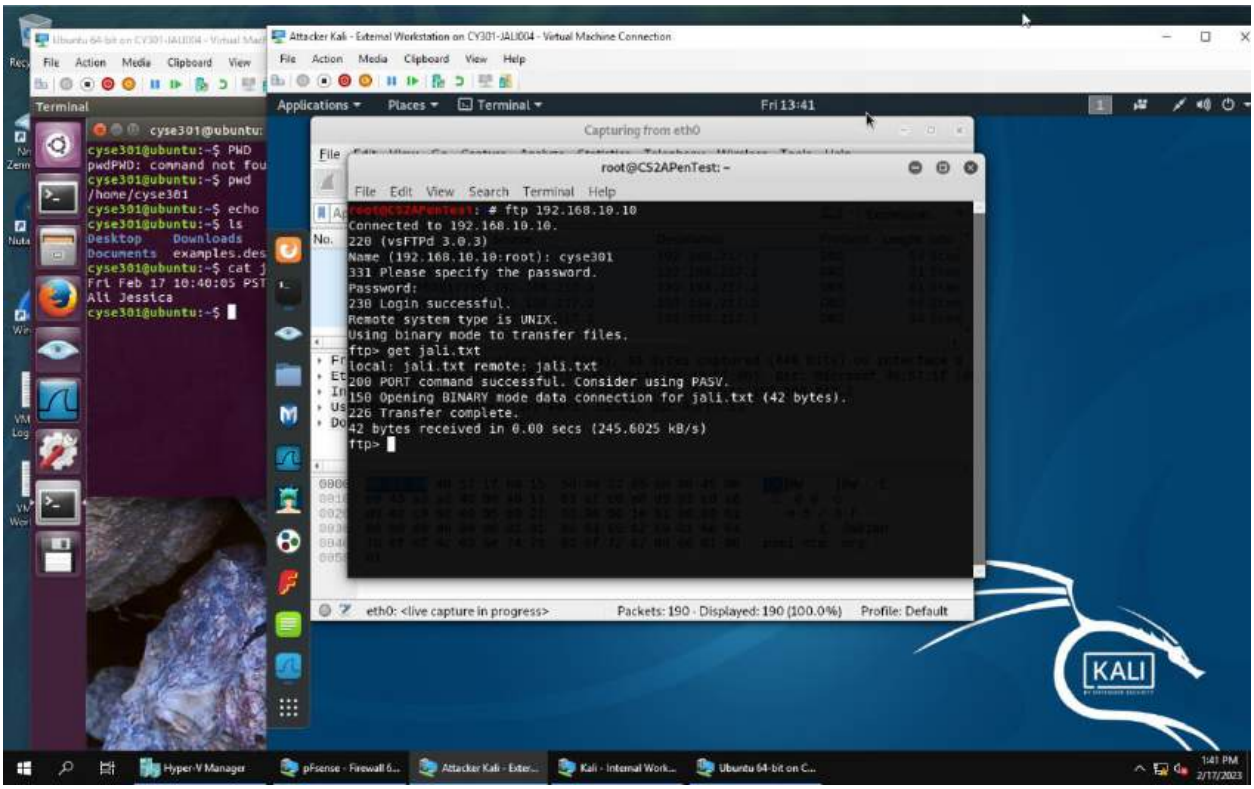
b)Unfortunately, Internal Kali, the attacker, is also sniffing to the communication. Therefore, all of my communication is exposed to the attacker. Now, I found out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali by using Wireshark on Int. Kali and applying the filter “ftp && ip.addr. 192.168.10.10”. Which means I am looking for ftp traffic originating from Ubuntu. The information I need is found the Info column.

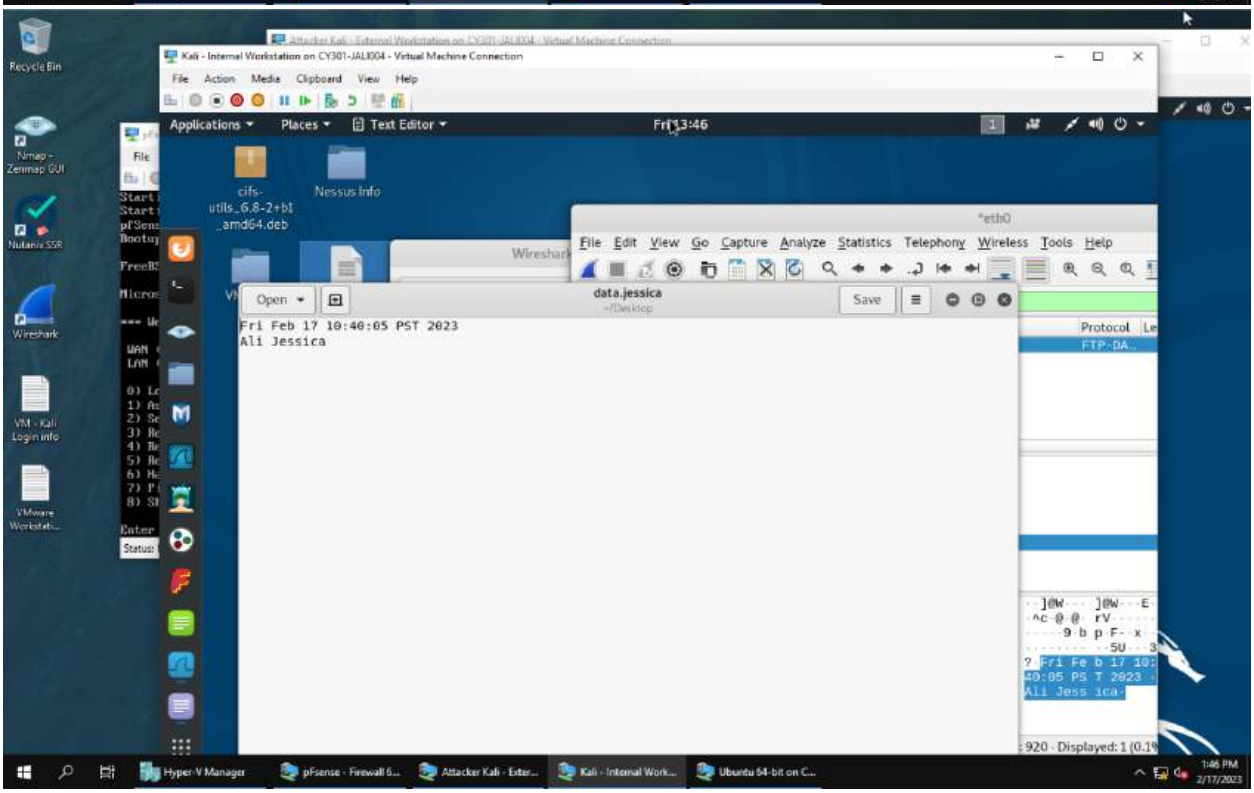
c)I repeat this process from part b in the terminal on Ext. Kali. but the only thing that changes is my username (jali004) and password (01166237), and I also establish a connection again because I logged out. In the last screenshot we can see what the password is in the column labeled info.

TASK C

1. Extra Credit: Steal files with Wireshark







Explanation: Logged into to Ubuntu VM, and created a file in my home directory with the command “echo -e “$(date) \nAli Jessica>jali.txt” and put the current timestamp and my name in the file. The first part is creating the contents while the second part of the command is naming/creating the actual file. I

also double checked that I had created it correctly with the “ls” command and called on the filled to check the contents with the “cat” command. I then switched back to Ext. Kali to see the file I just created with FTP protocol remotely. I did this connecting again with the command ftp 192.168.10.10 and logged into cyse301 with the password, password. Once the connection was established, I then used the “get jali.txt” command to successfully access the file, and waited for the code 226 transfer complete. Therefore creating ftp traffic. Lastly, using Wireshark on Int.Kali VM I applied the display filter (ftp-data) to display the FTP-DATA packets between External Kali and Ubuntu VM and followed the tcp steam of the FTP-DATA packet, viewed the content of the jali.txt and then exported the it as a text file in Int.Kali. Ultimately to view the content of my jali.txt file. I saved the file on Int. Kali’s desktop so I could access it easier as illustrated in my last screenshot above.