ASSIGNMENT 5: PASSWORD CRACKING (PART A + B)

CYSE 301

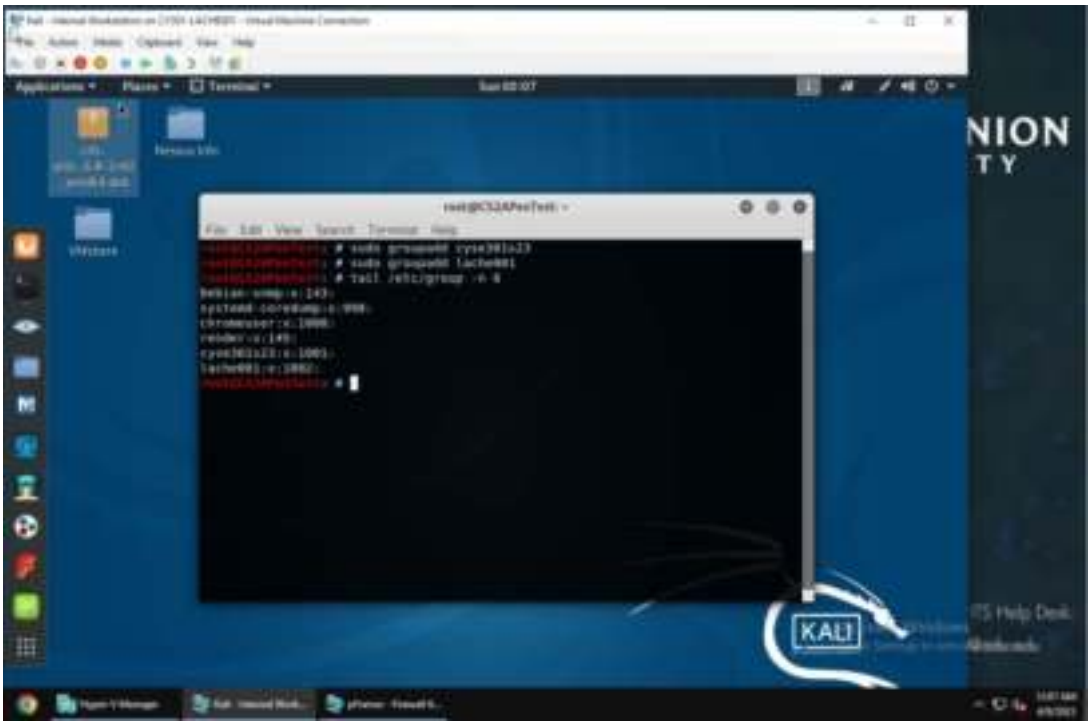
LEE ACHEAMPONG

LAB REPORT

Due: 4/11/23

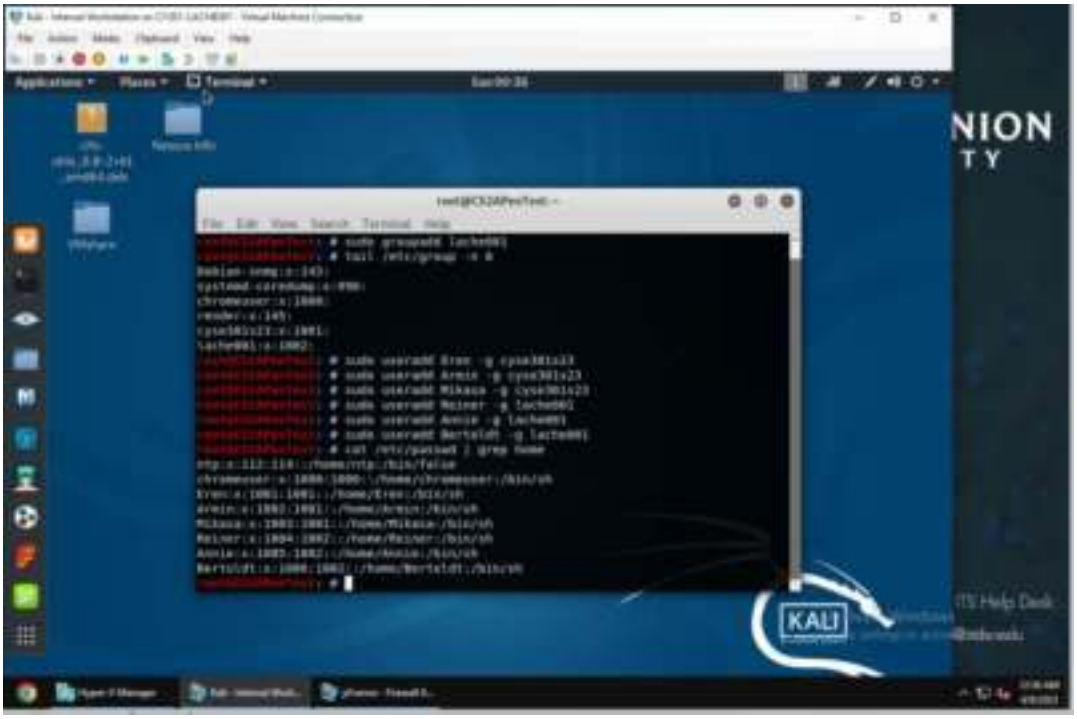
TASK A.

1.



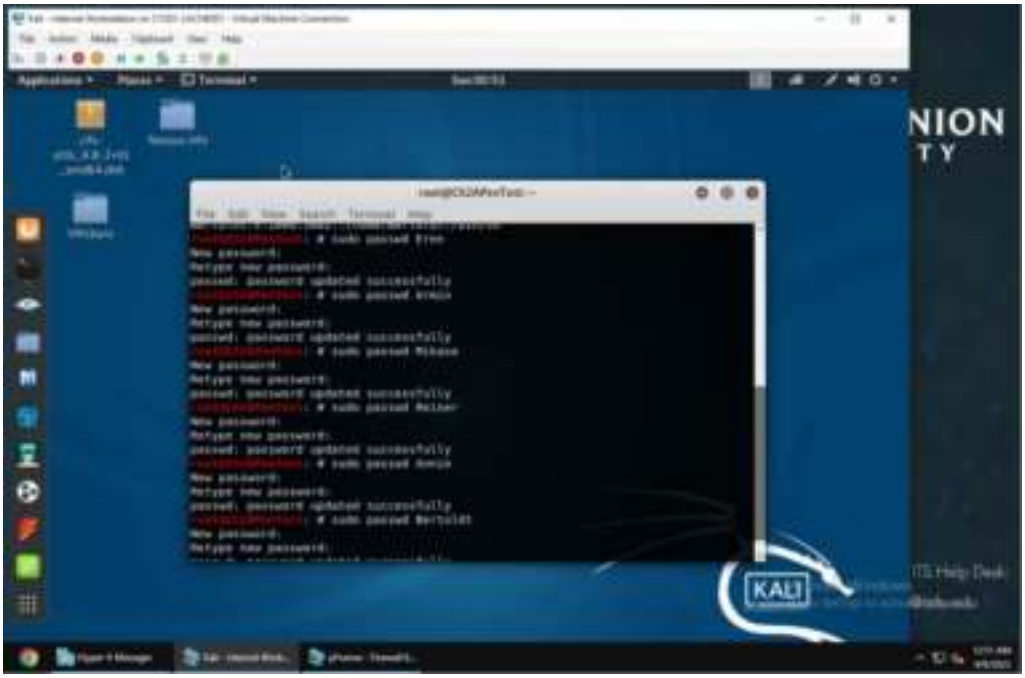
I created 2 groups with the “sudo groupadd” command. 1 group “cyse301s23” and the other “lache001”. Then I used the “tail /etc/group -n 6” command to show the corresponding groups IDs

2.



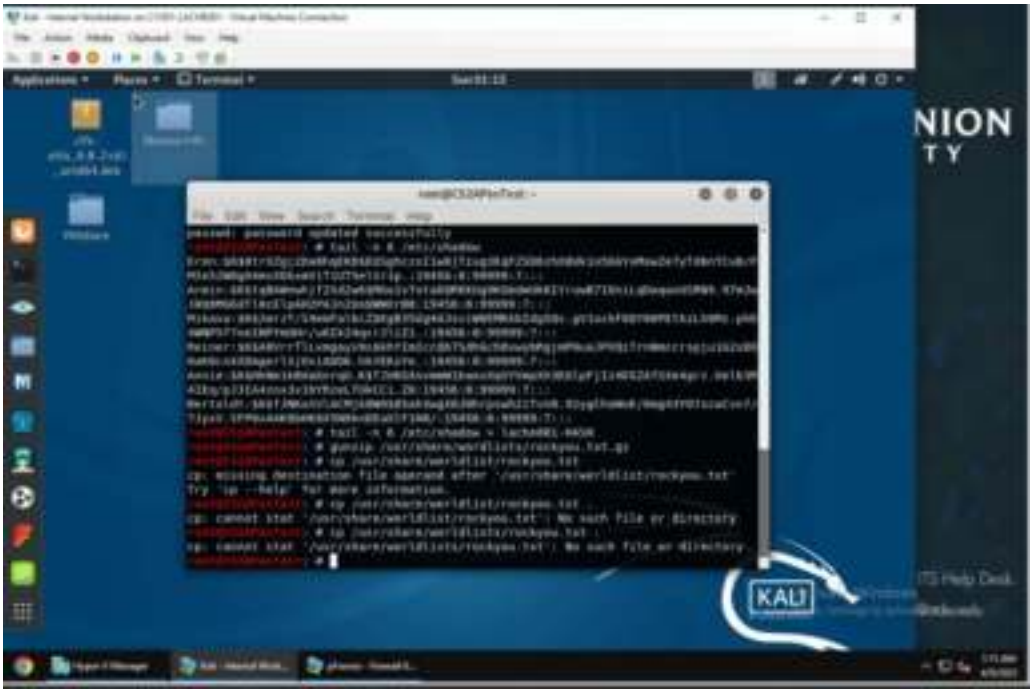
I then added 3 new users to the cyse301s23 group. I added Eren, Armin, and Mikasa. Then I added 3 more users to the lache001 group, which were Reiner, Annie, and Bertoldt. I added all of the using the “sudo useradd (user name) -g then (groupname). I also used the “cat /etc/passwd | grep home” command to display the UID and GID info for all users.

3.

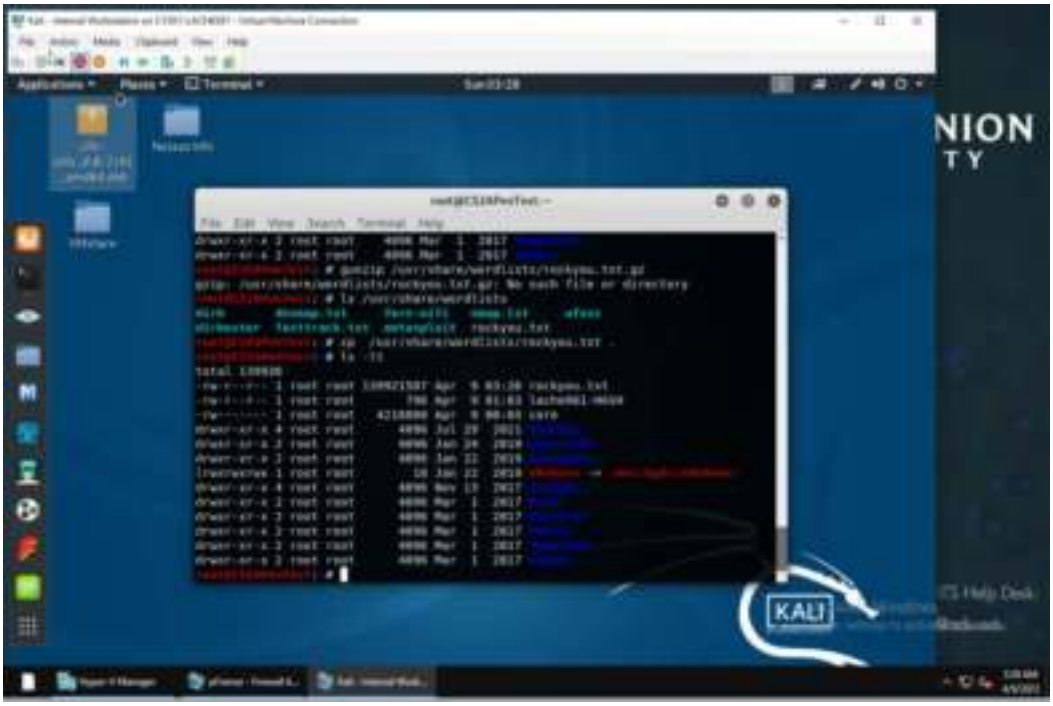


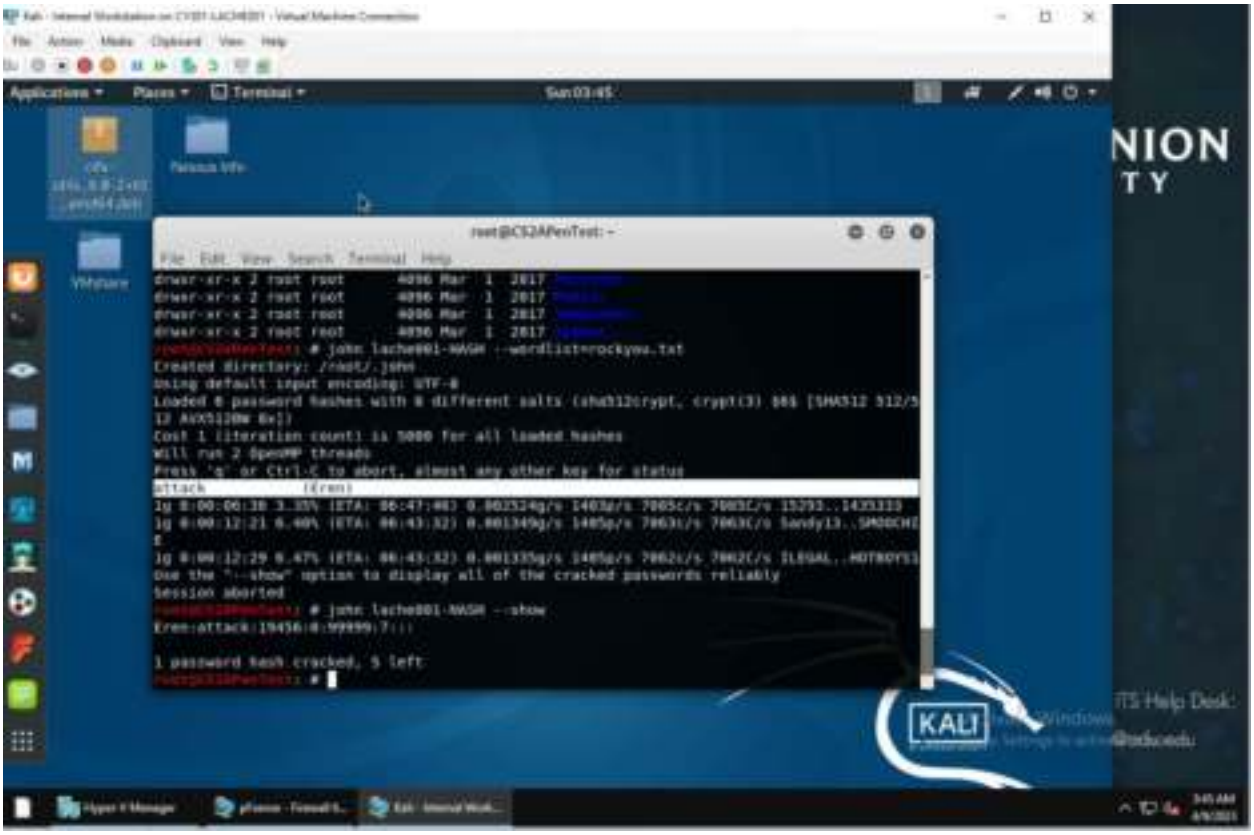
Then I went ahead added passwords for all the accounts. Using “sudo passwd (username)” command. The passwords I programmed are Eren = attack, Armin = collosal2, Mikasa = Scouts3, Reiner = Armor11, Annie = female42++, Bertoldt = Marley4ever!

4.



I used the “tail -n 6 /etc/shadow/” command to display the password hash. Then copied it into my own hash file using the “tail -n 6/etc/shadow/ > lache001-HASH. I then used the “gunzip /usr/share/wordlists/rockyou.txt.gz” command to the dictionary attack and used “cp /usr/share/wordlists/rockyou.txt” to copy the file and put in into the right directory.



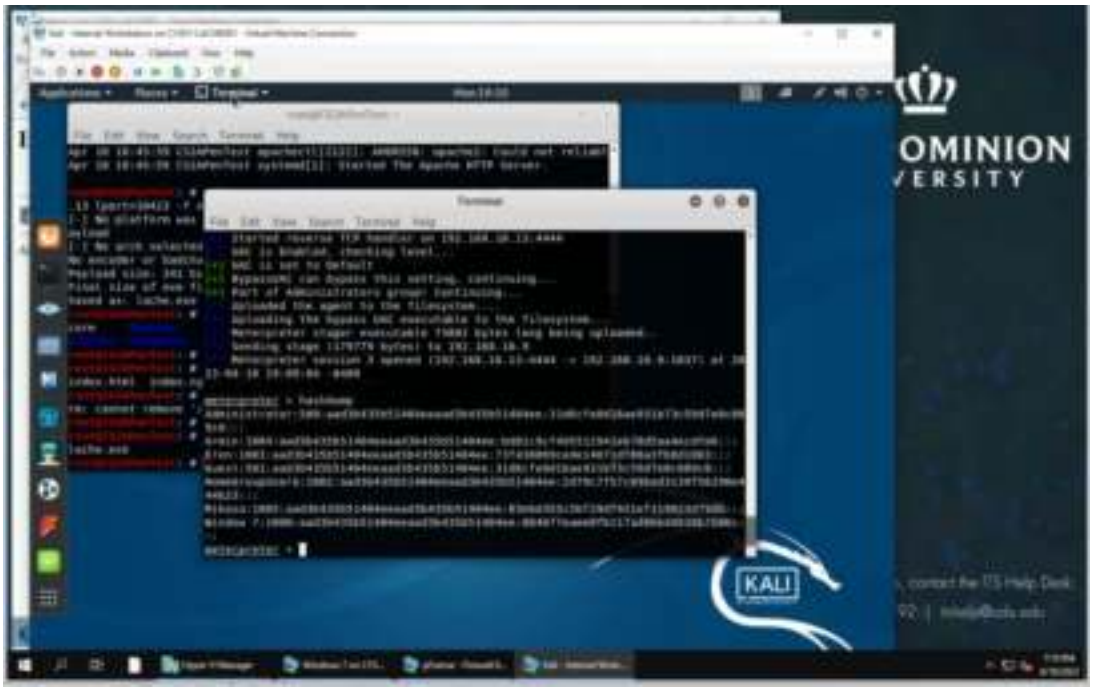


I launched the dictionary attack by using the “john lache001-HASH - - wordlist=rockyou.txt” command.

It was only able to only crack 1 password. Which was the easiest password of “attack.”

TASK B

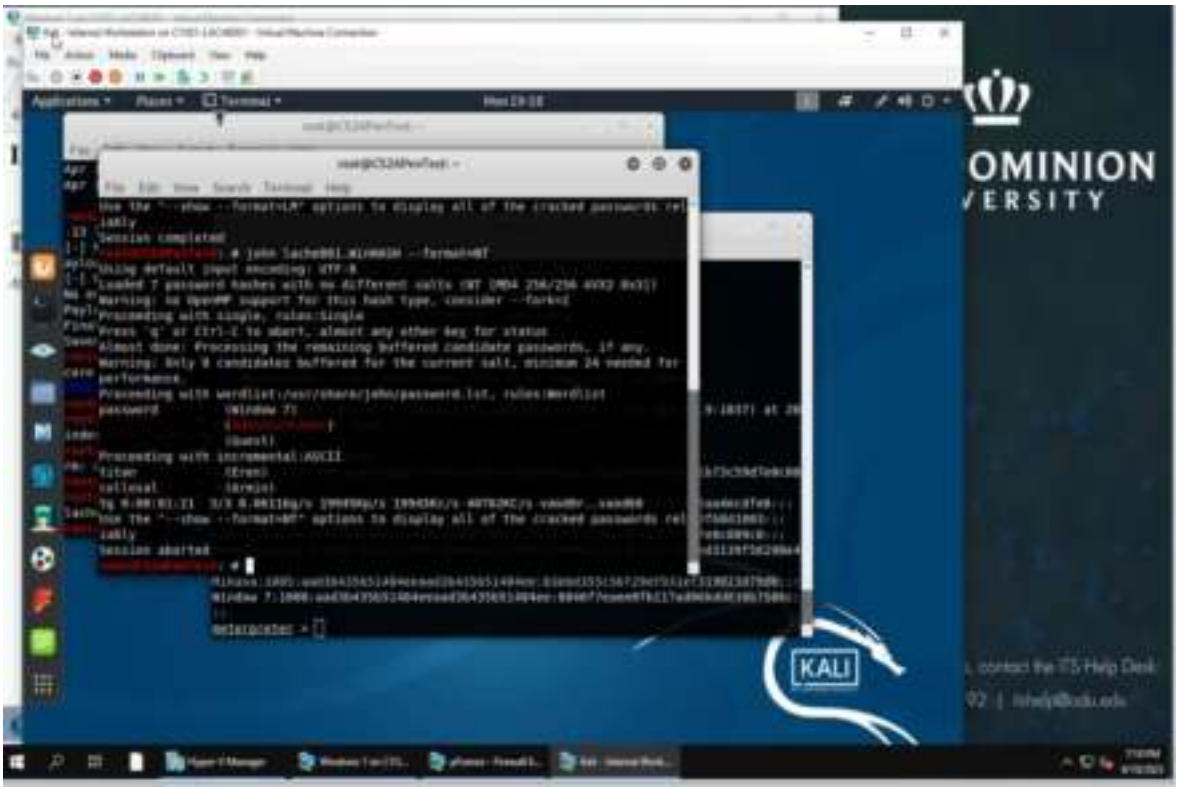
1.



I established a reverse tcp connection and used the “hashdump” command in meterpreter to show the hash of all the account passwords created.

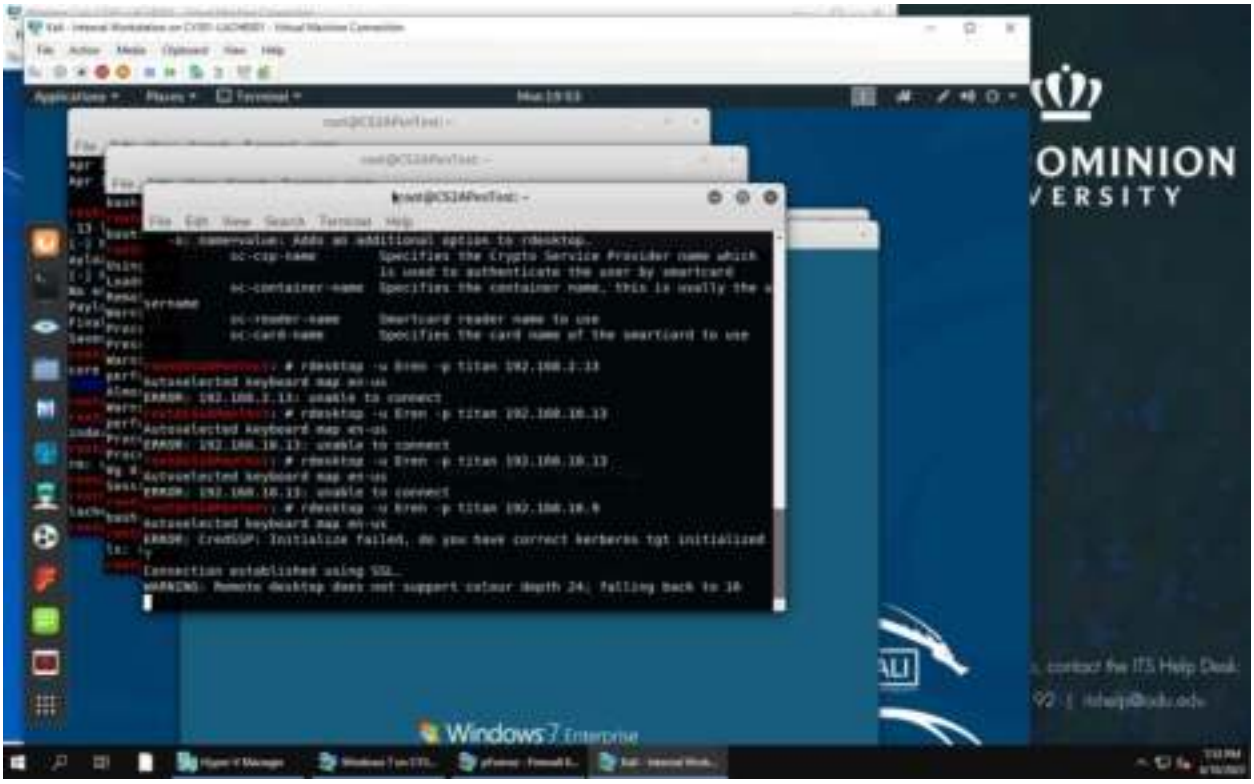
2.

I then used the “gedit lache00.WinHASH” to open a file and copy all the hash into that file.

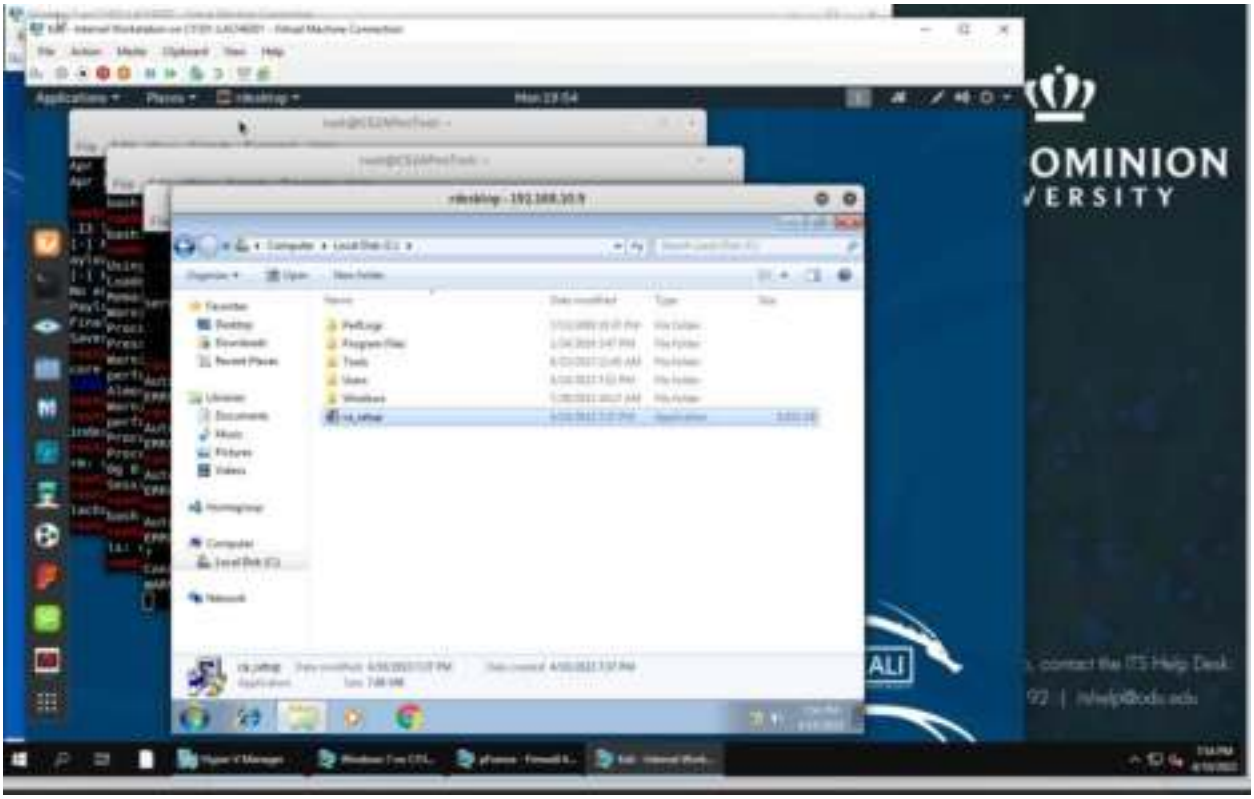


I then used the “john lache001.WinHASH --format=NT” to crack the password hashes. I was able to crack 2 of the 3 passwords.

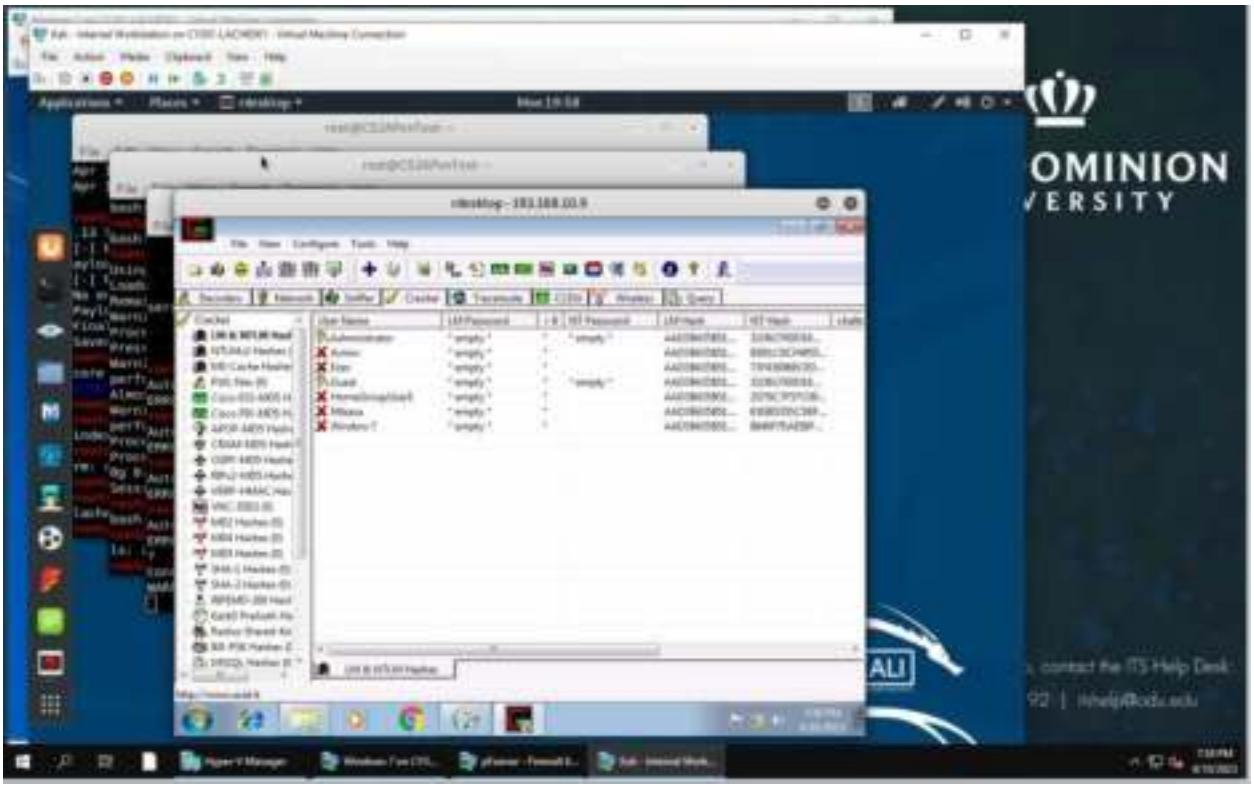
3.



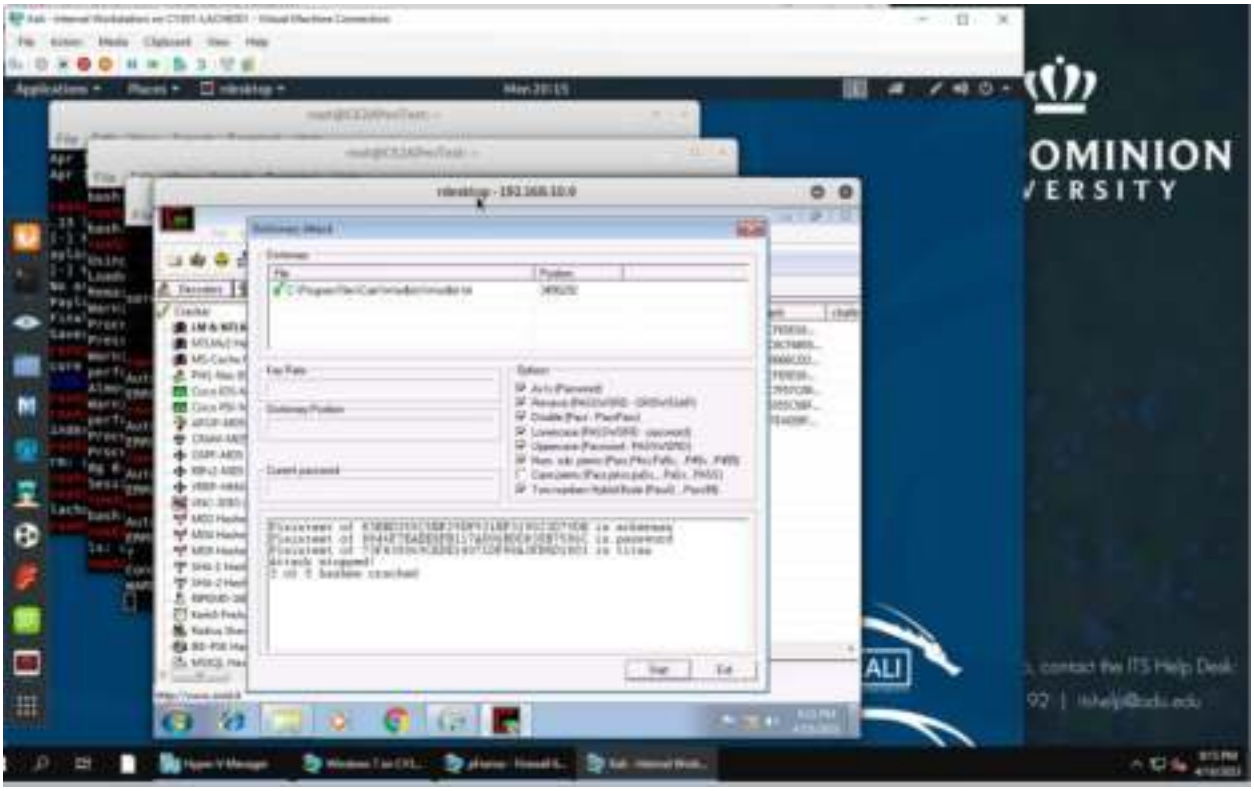
I used the “rdesktop -u Eren -p titan 192.168.10.9” command to upload the Cain and Abel cracking tool on the windows 7VM.



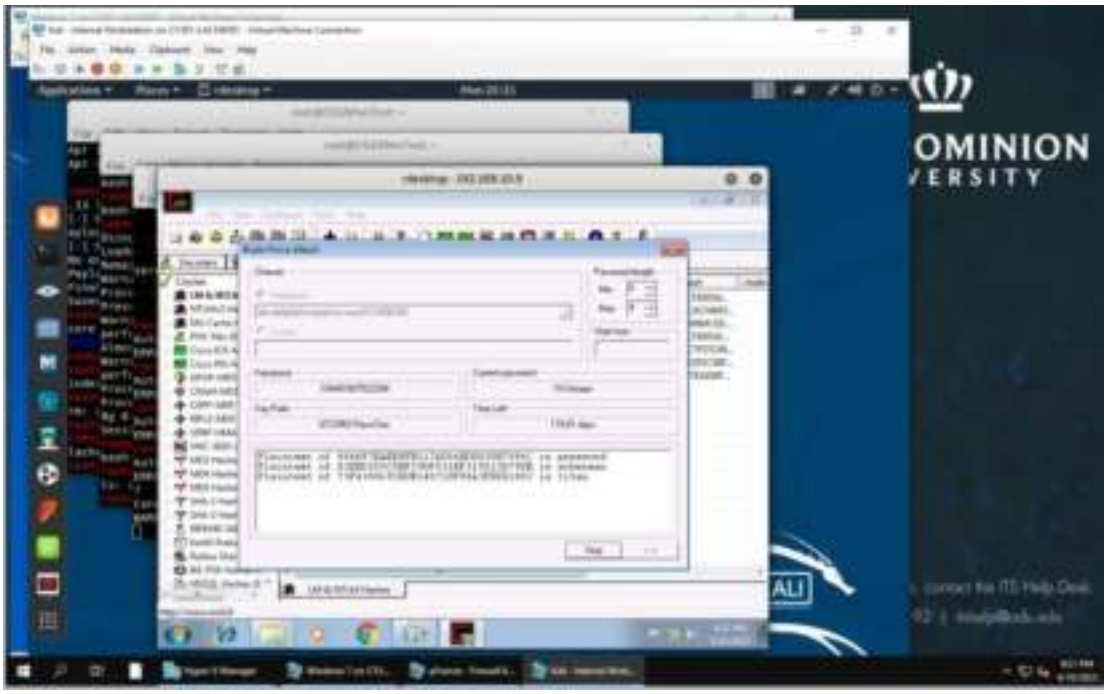
This screenshot shows that the file was successfully uploaded to the windows 7 VM.



This screenshot shows all the user accounts on the Windows 7 VM.

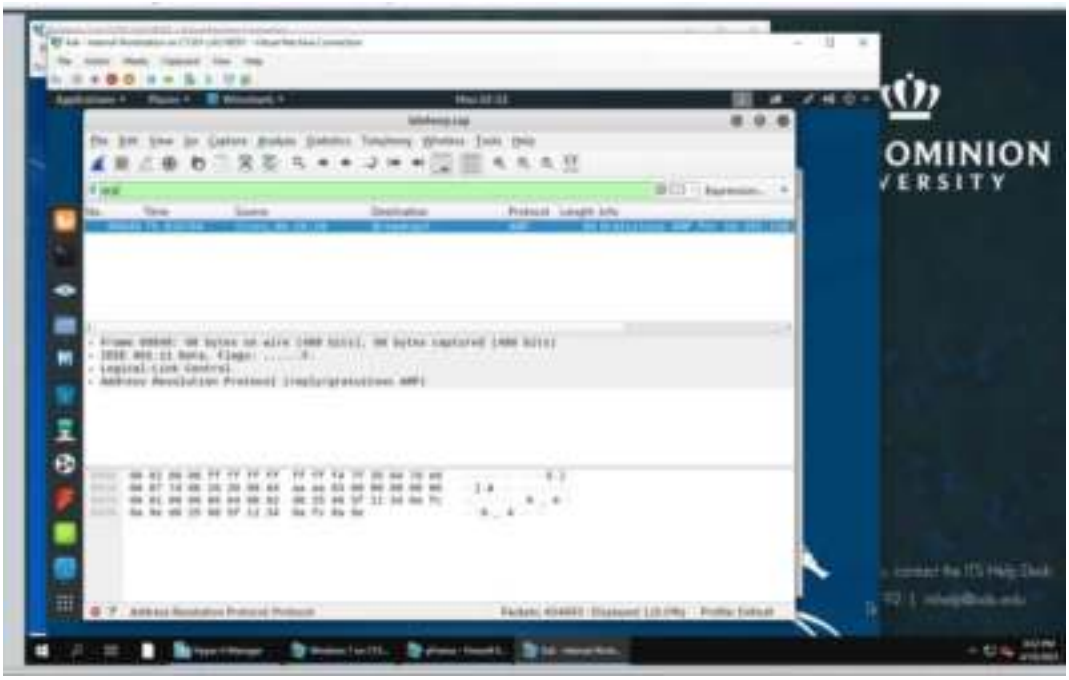


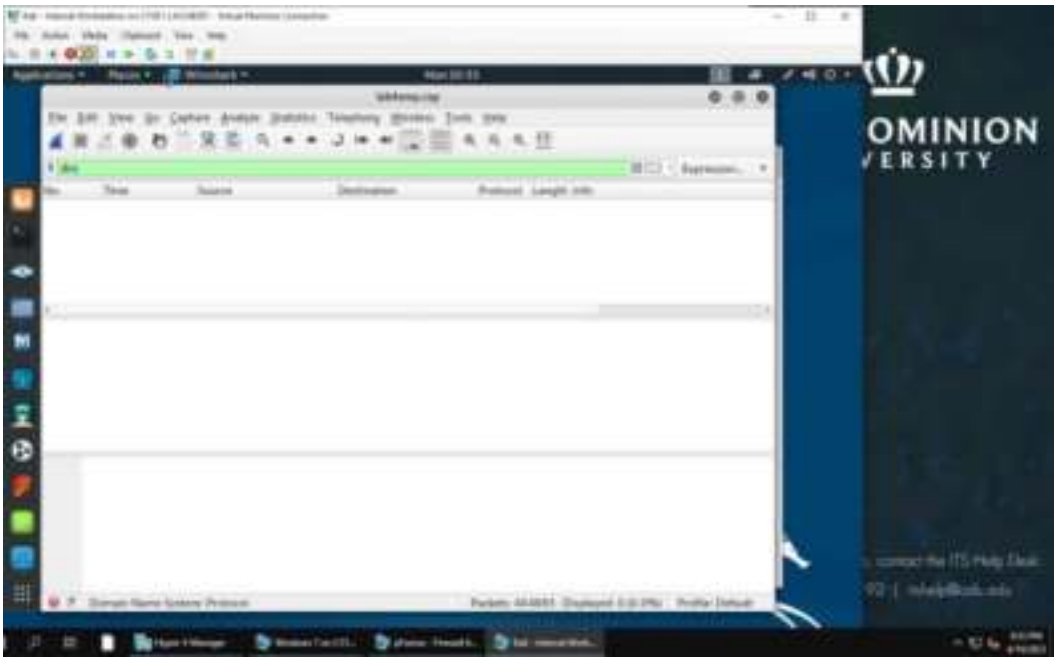
Dictionary Attack. This screenshot is when I implemented the dictionary attack and was able to get 3 of the 5 hashes cracked.

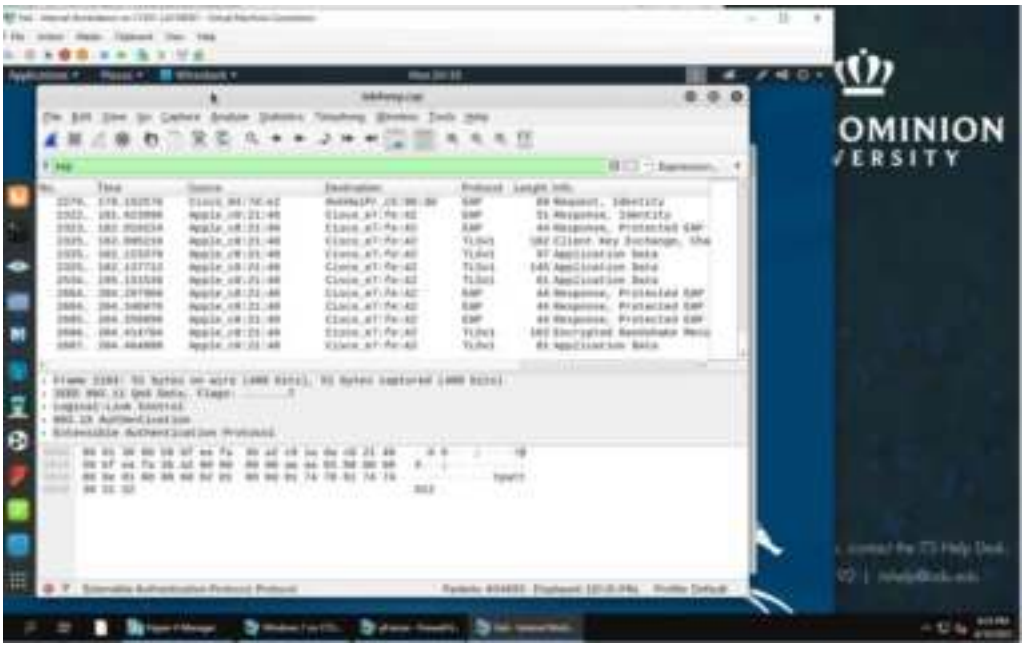


Brute Force Attack. This screenshot is the result of implementing the brute force attack where it also got 3 of the 5 hashes cracked.

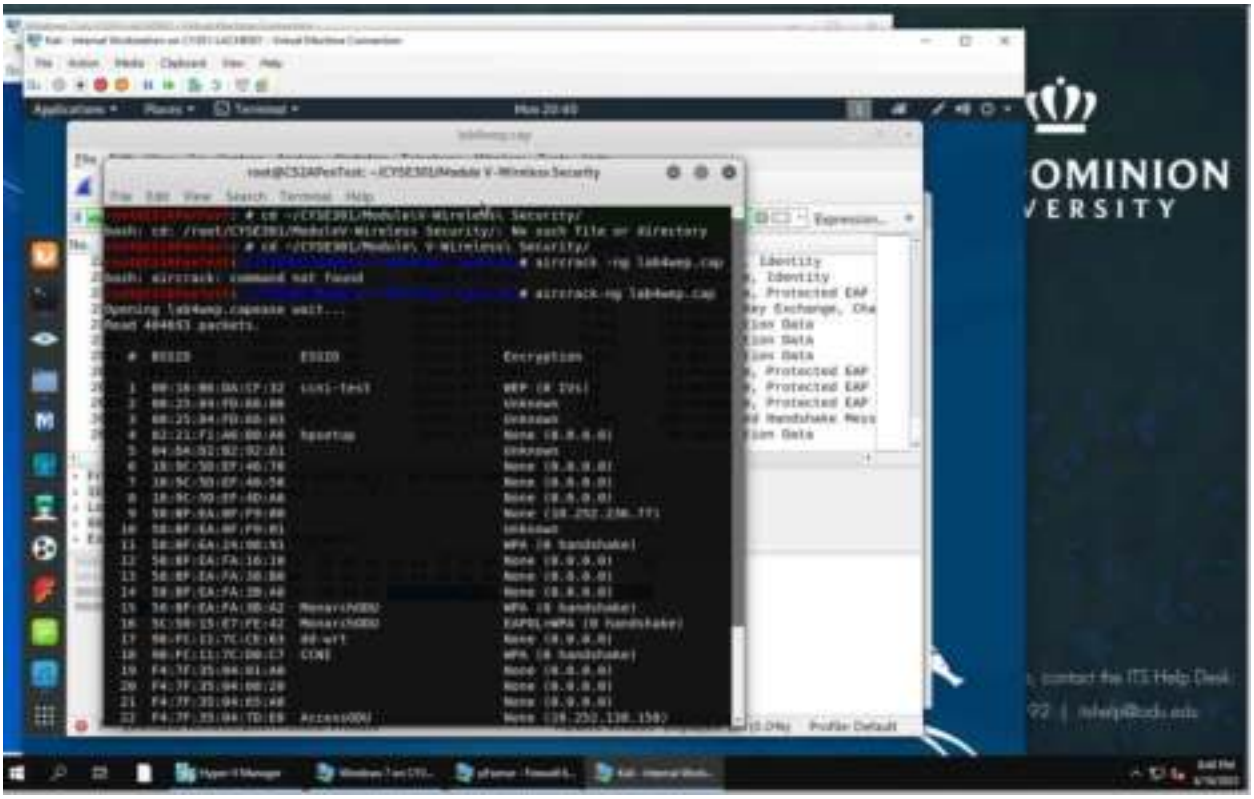
PART B

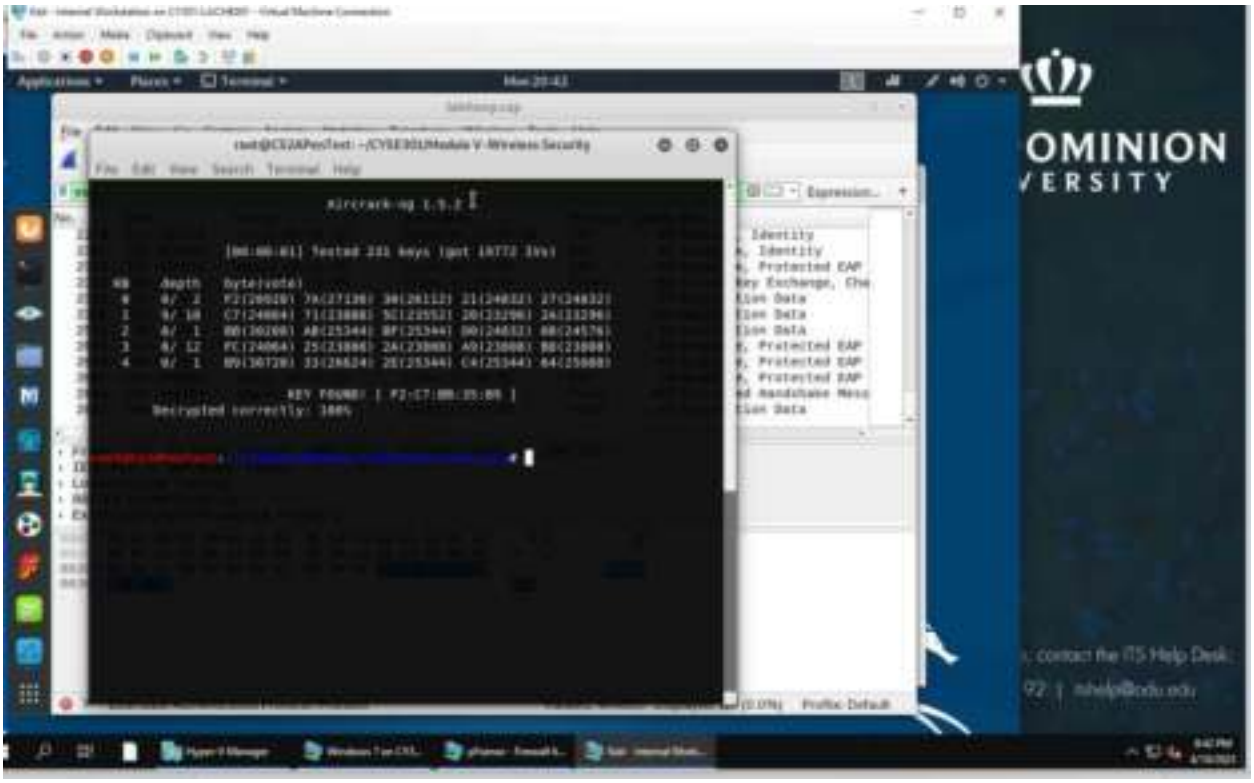




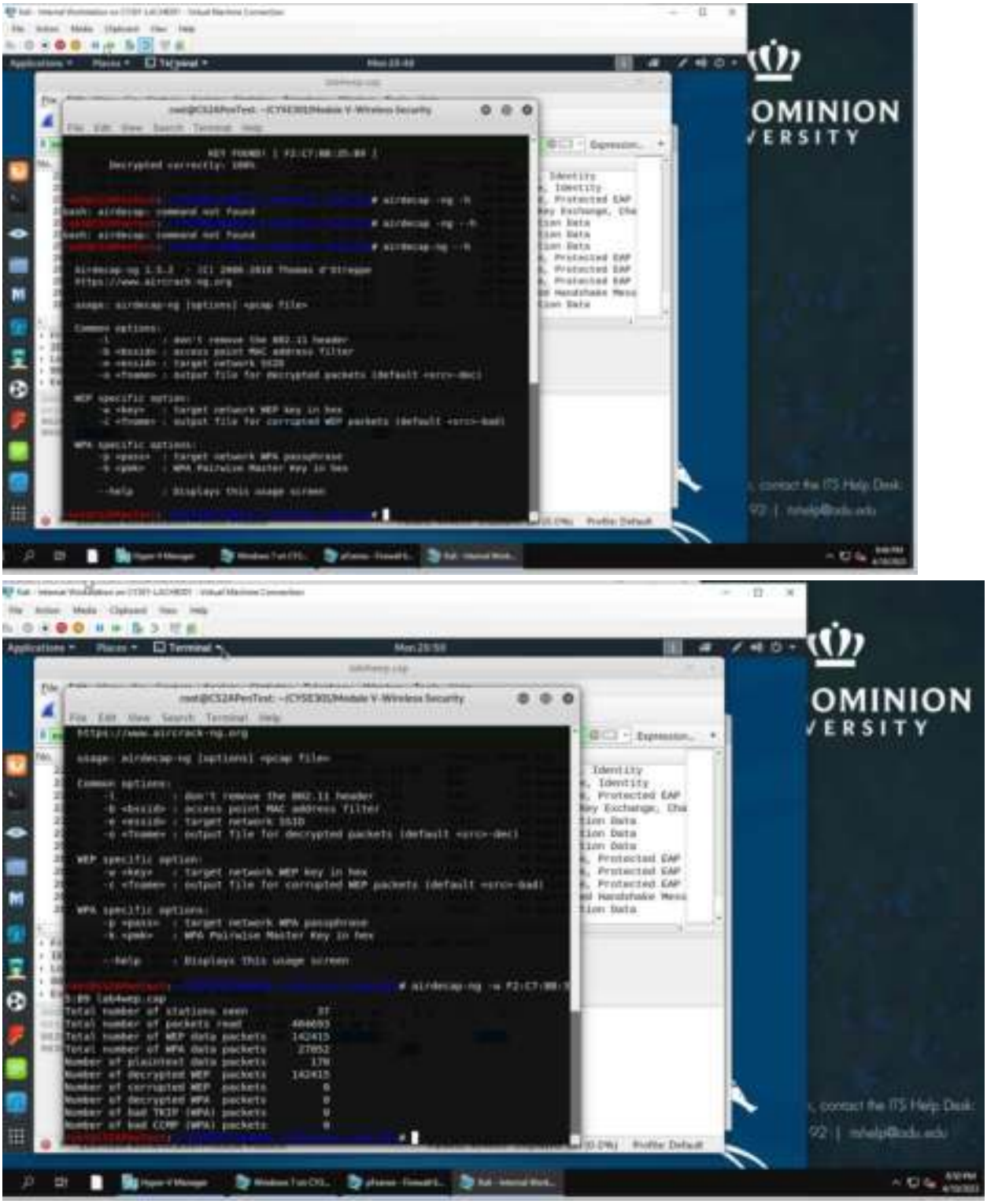


Theses 3 screenshots show me applying filters on the traffic. I applied “dns”, “eap” and “arp”.



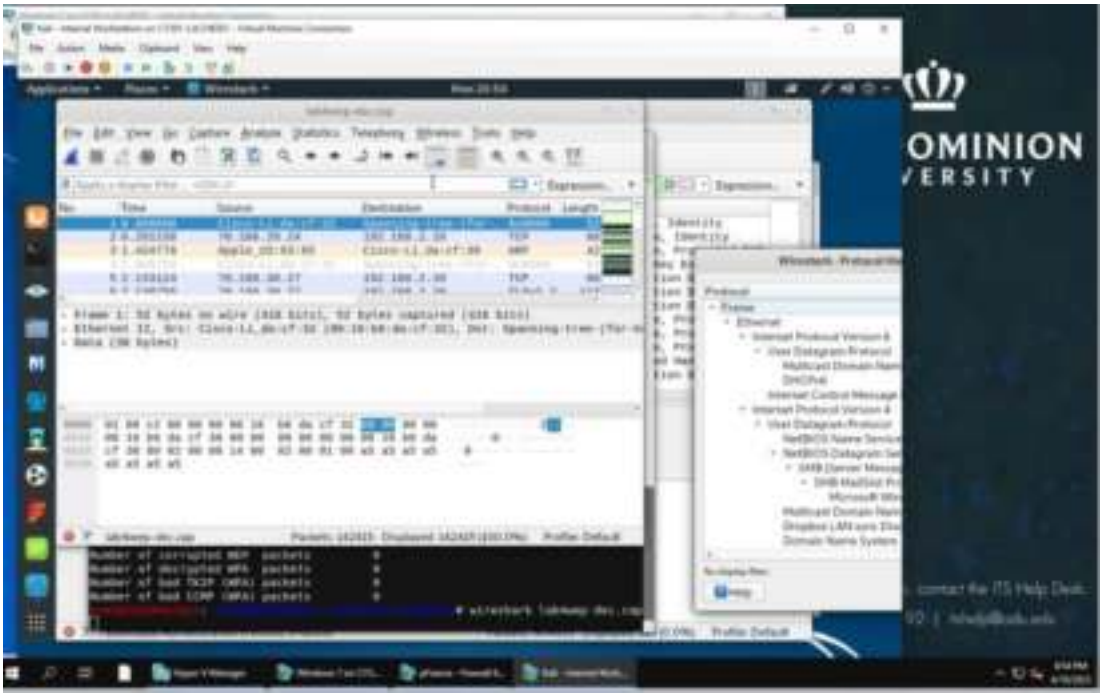


I place “1” for the index number of the target system and got the key [F2: C7 :BB :35 :B9]

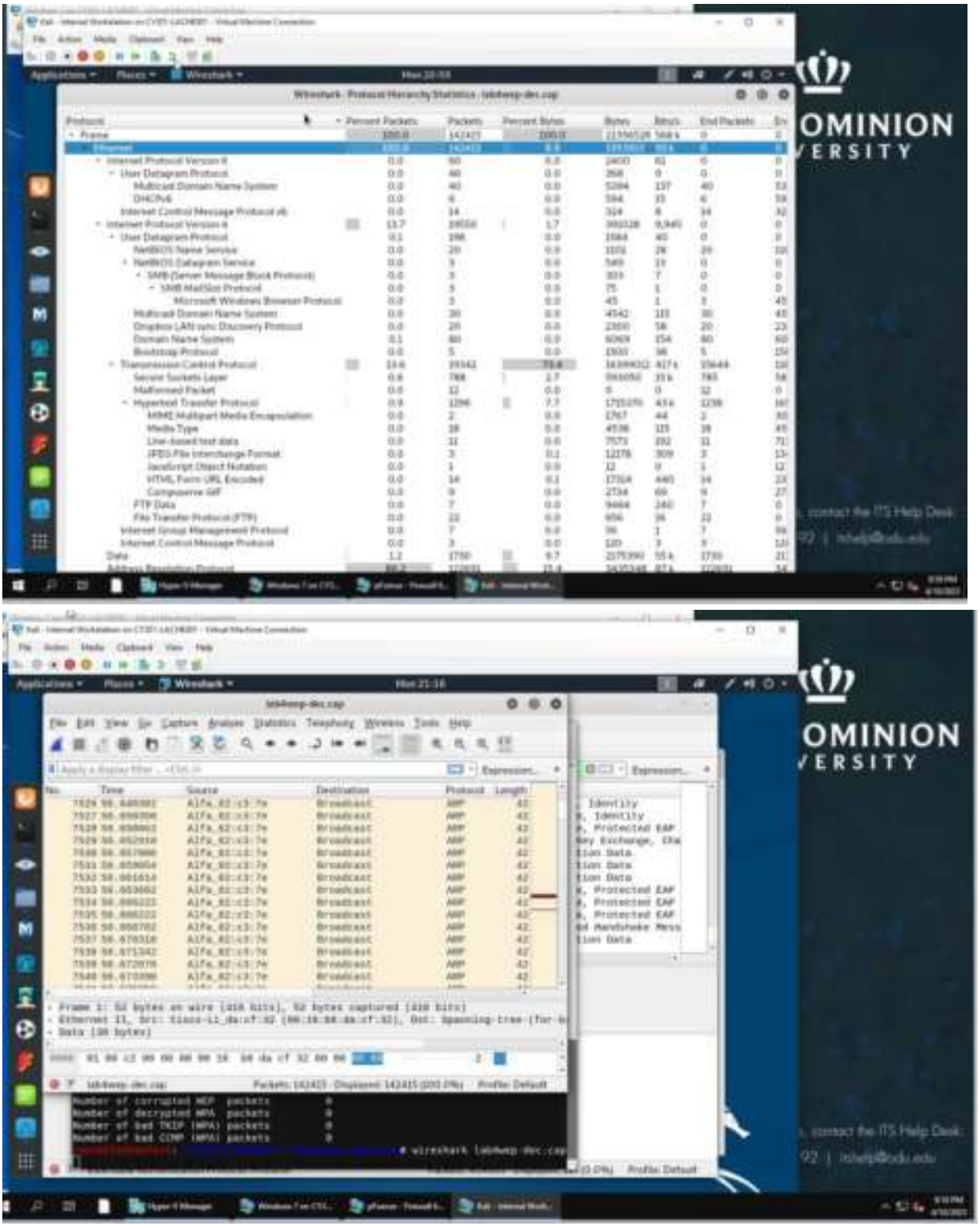


I input the “airdecap -ng - - h” to show options related to airedecap command. Then I used the “ airdecap-ng -w F2:

C7:BB:35:B9 lab4wep.cap” to find all the Wep packets that were decrypted with the key.



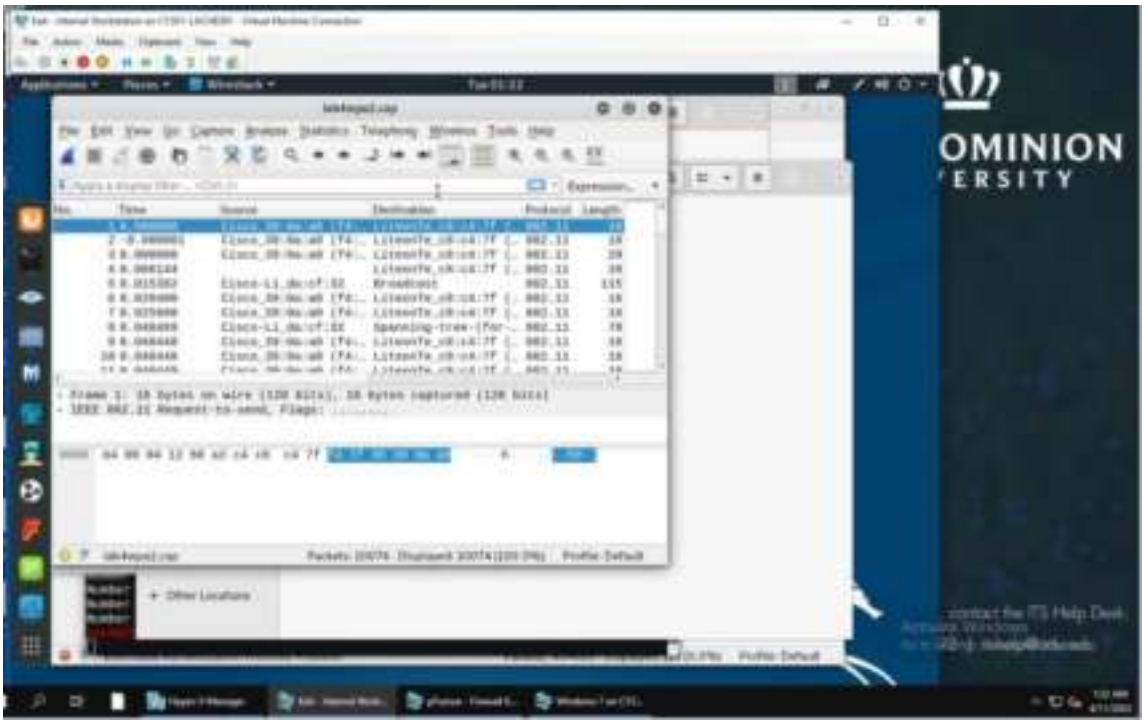
After inputting the command “wireshark lab4wep-dec.cap”, the Wireshark screen appeared and showed all the decrypted traffic.

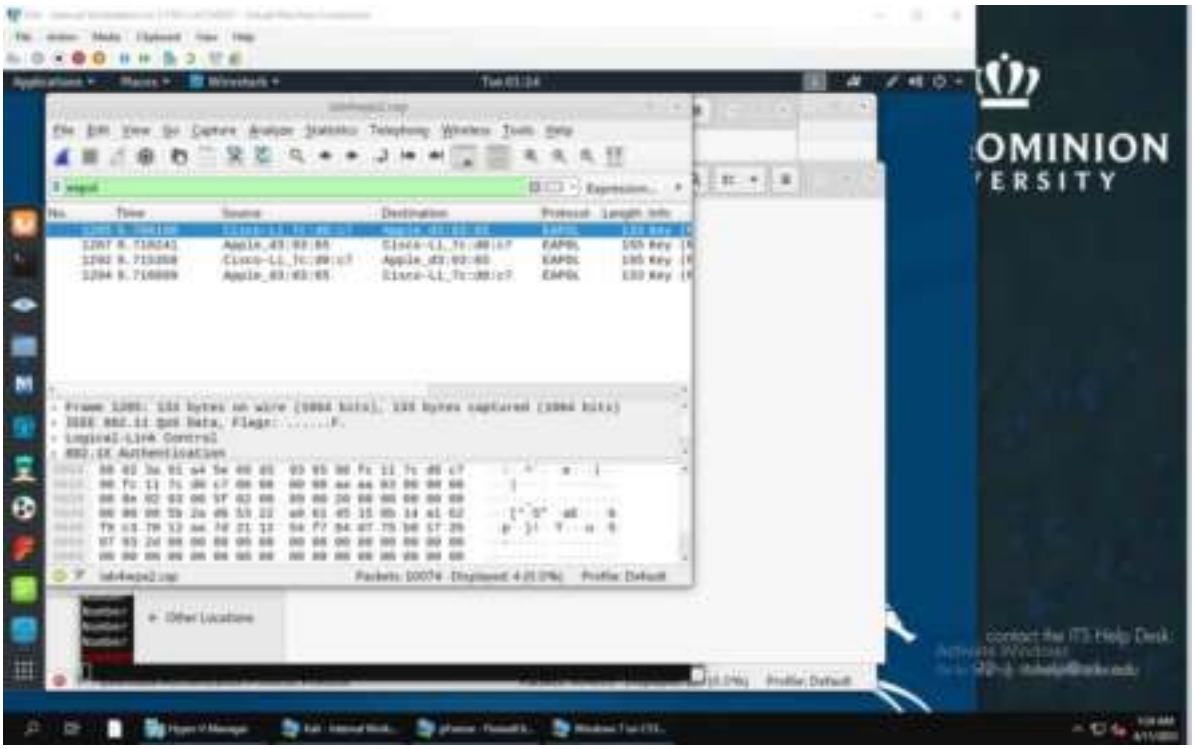


This is a screenshot of the protocol hierarchy and it shows a lot of decrypted packets, mostly ARP data packets. There

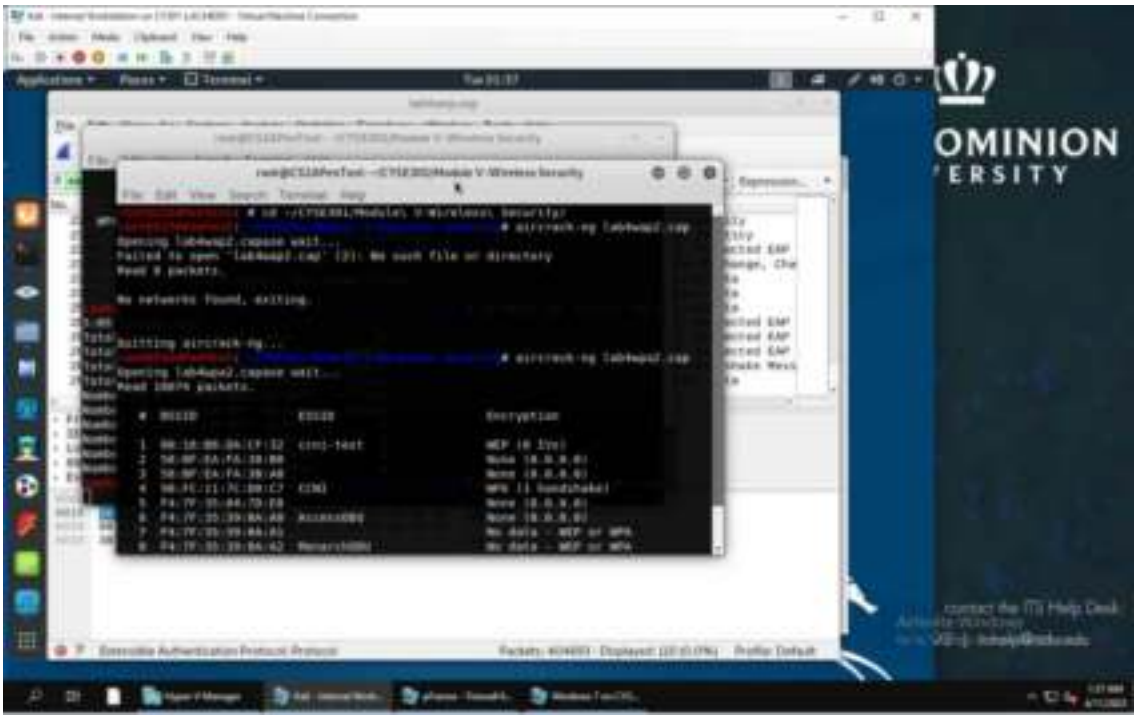
were also a lot of broadcast protocols, which show that the host was communicating with other hosts. There were also several TCP packets in the traffic observed.

2.

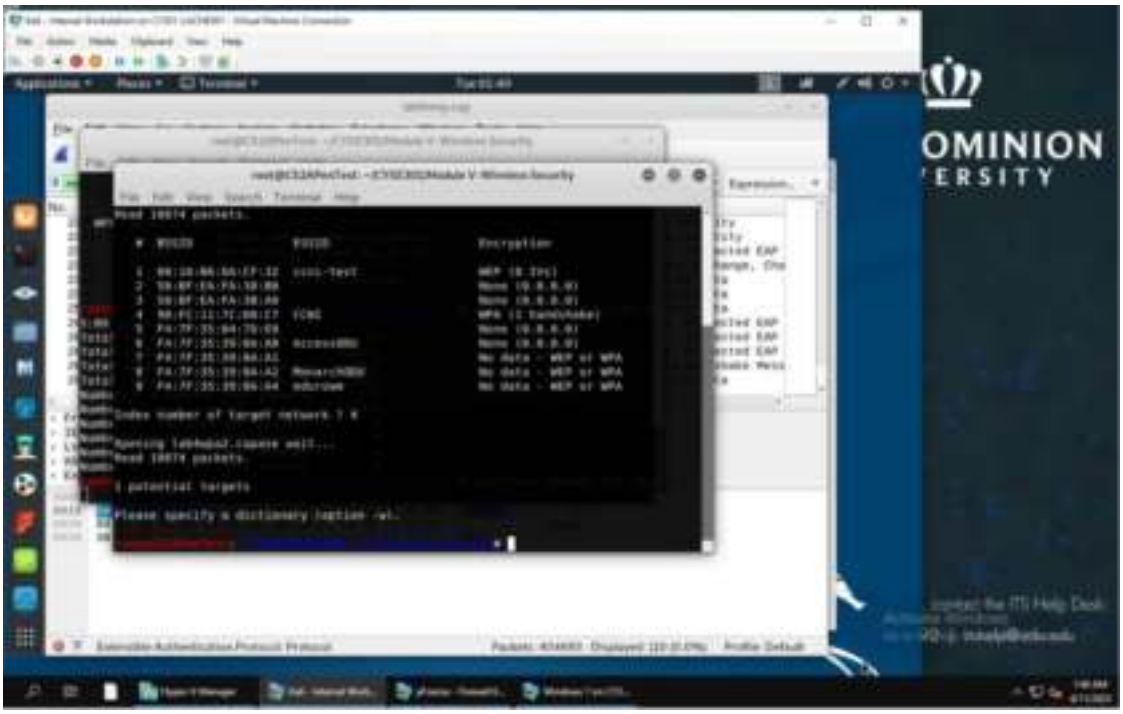




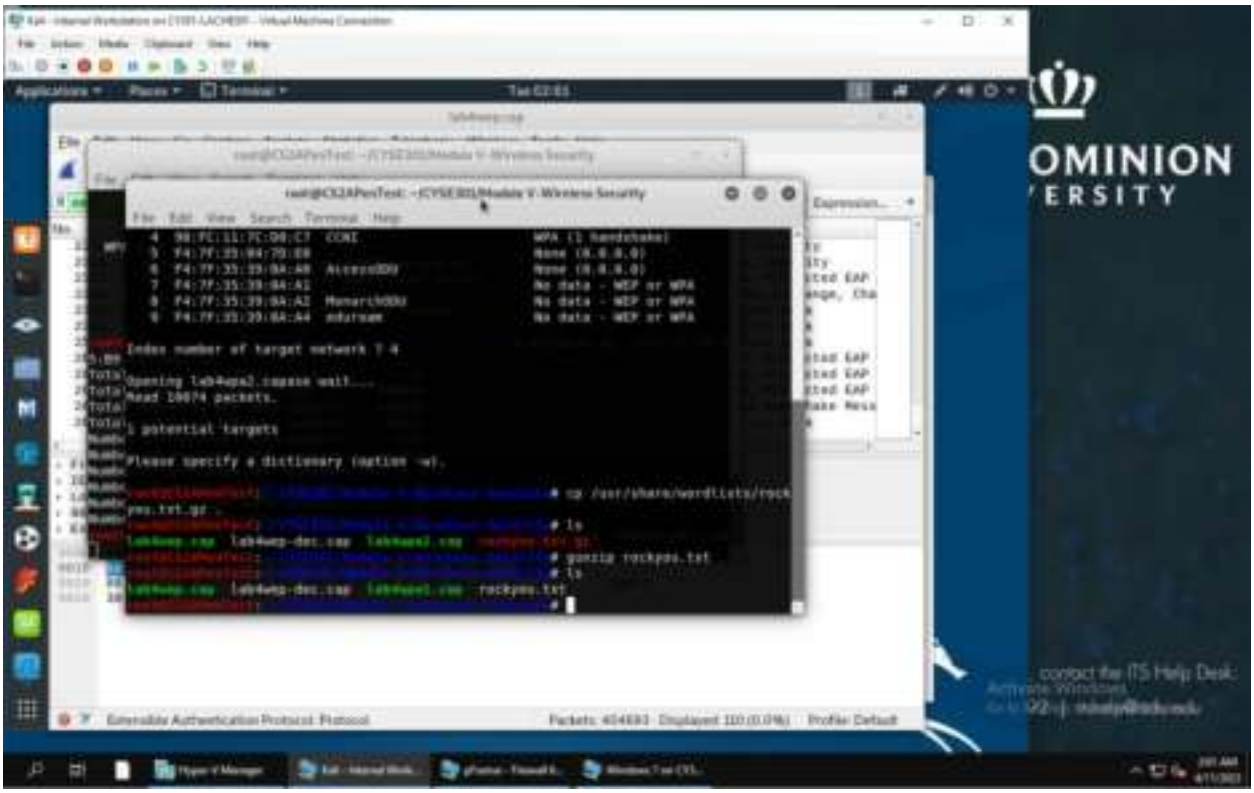
The first 2 screenshots show the encrypted traffic files before I performed the operation to decrypt them.



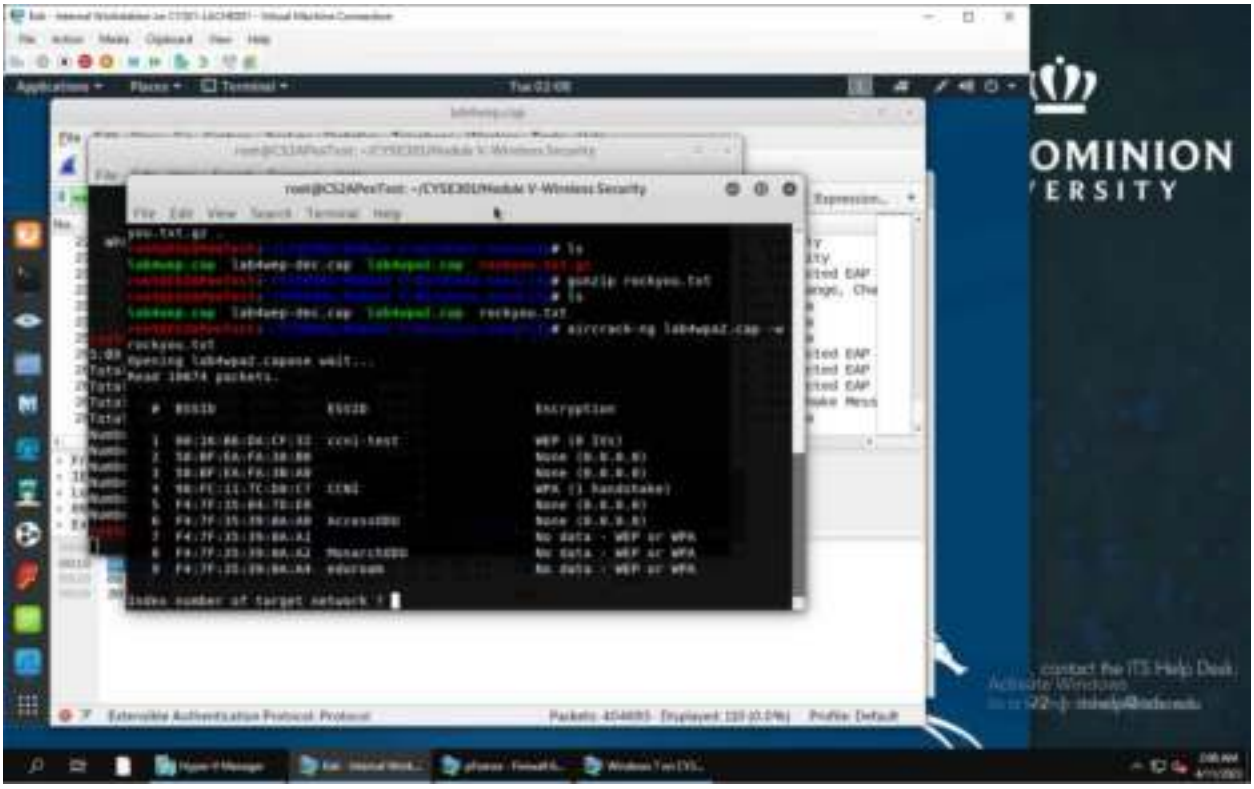
I used the “cd ~/CYSE301/Module\ V-Wireless\ Security/” command to bring me into the proper directory. Then used “aircrack lab4wpa2.cap” to find the index number. Which was “4”.



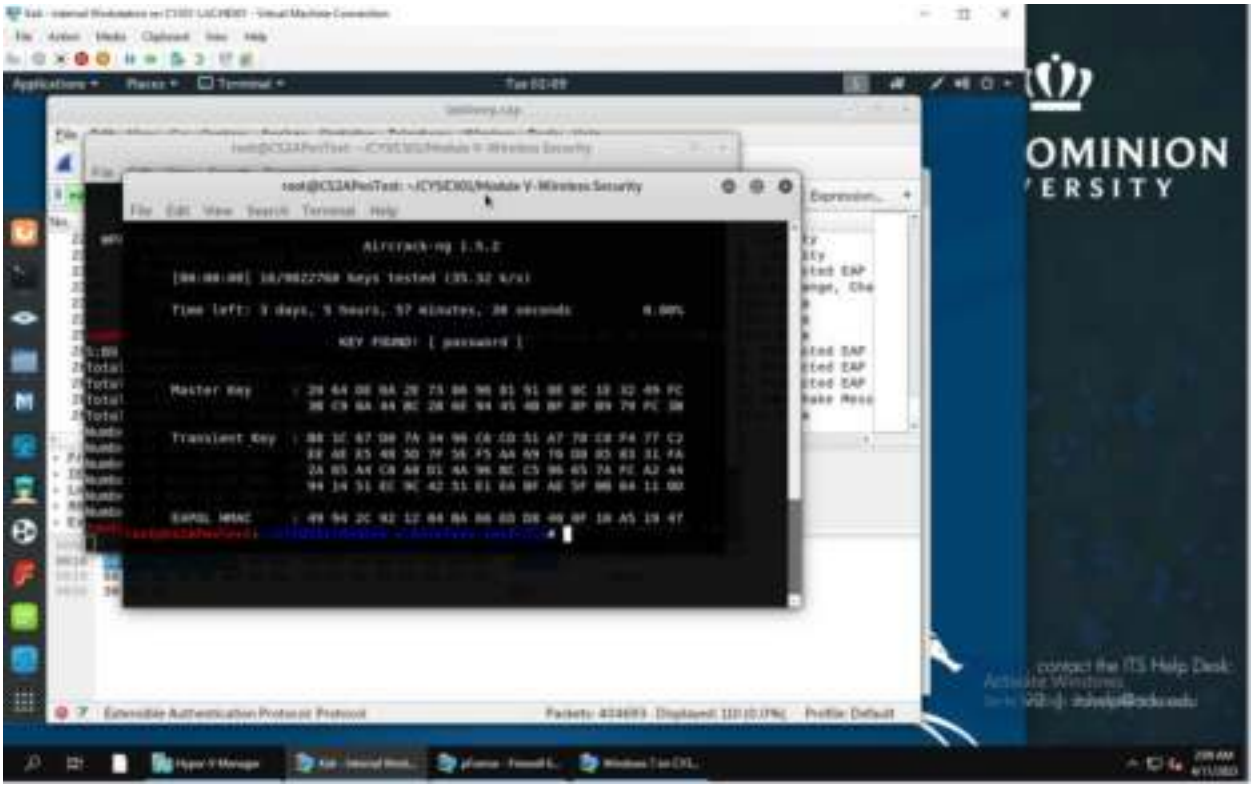
The index number I needed to choose was “4”, which I did.



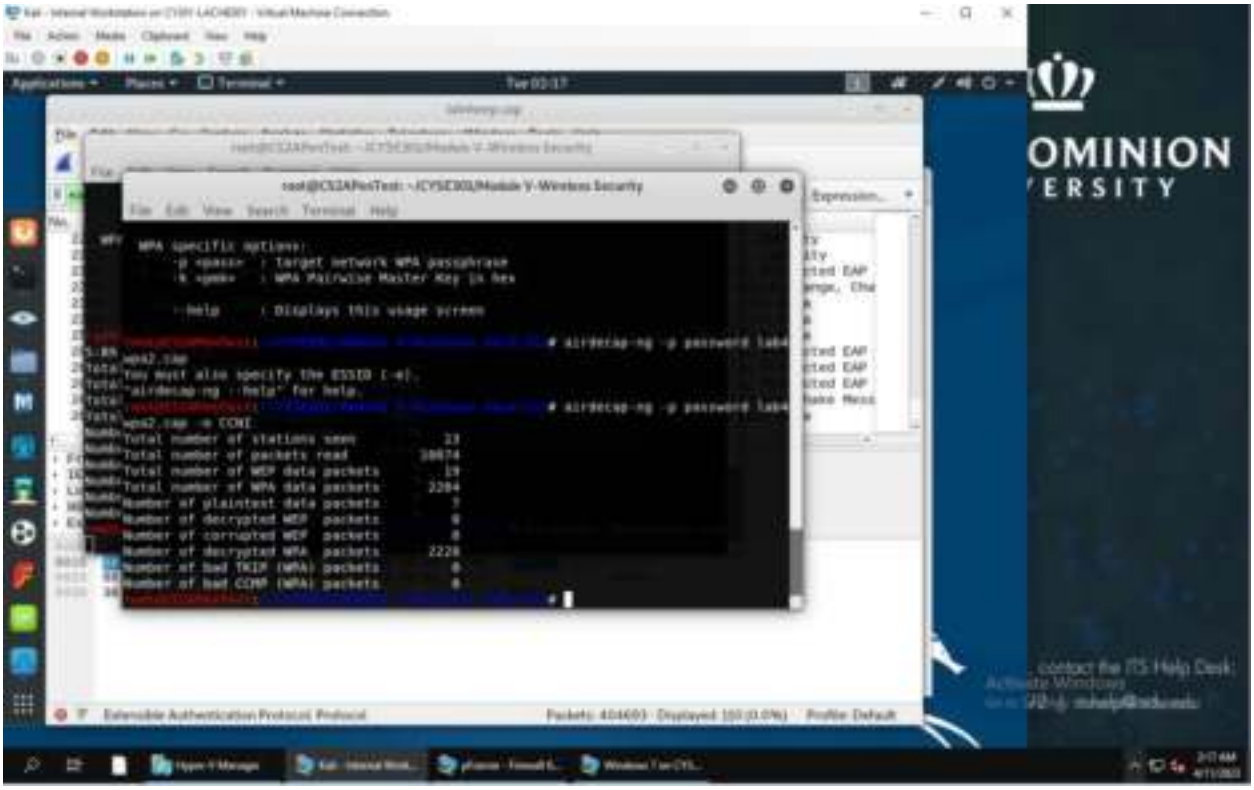
I then used the “cp /usr/share/wordlists/rockyou.txt.gz” command to copy the john the ripper dictionary attack into the current directory.



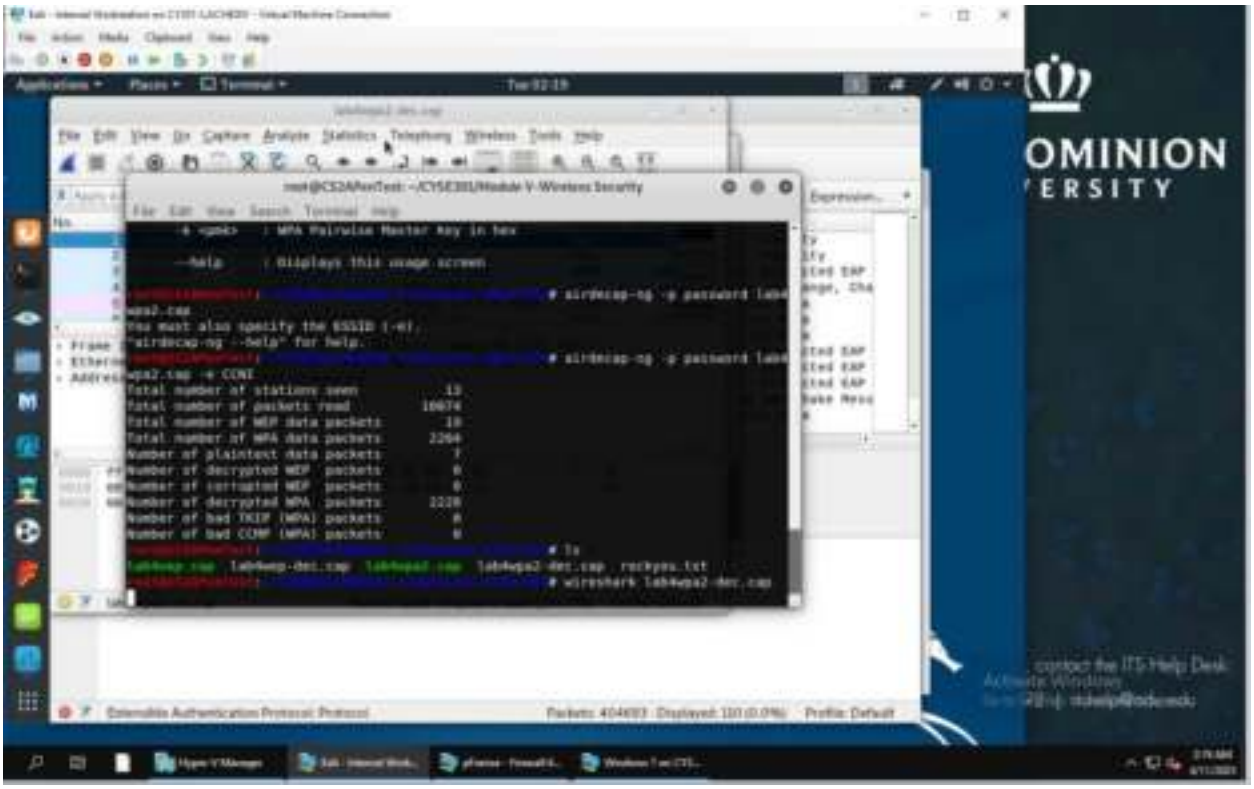
I used “ls” command to make sure that it was indeed in the current directory. I used the “aircrack-ng labwpa2.cap -w rockyou.txt” to bring up all the packets. Then chose the index number “4” again.



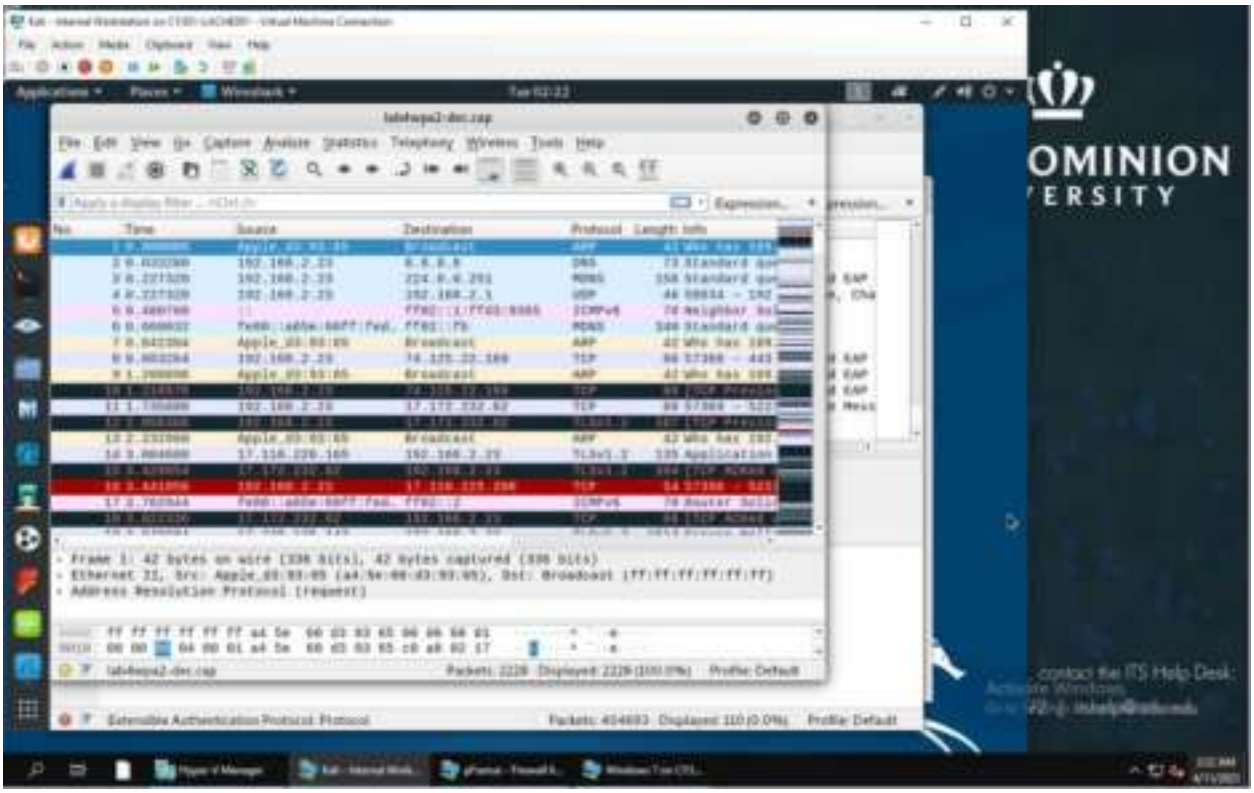
After choosing the index number, it decrypted the file and showed me that the key was “password”.



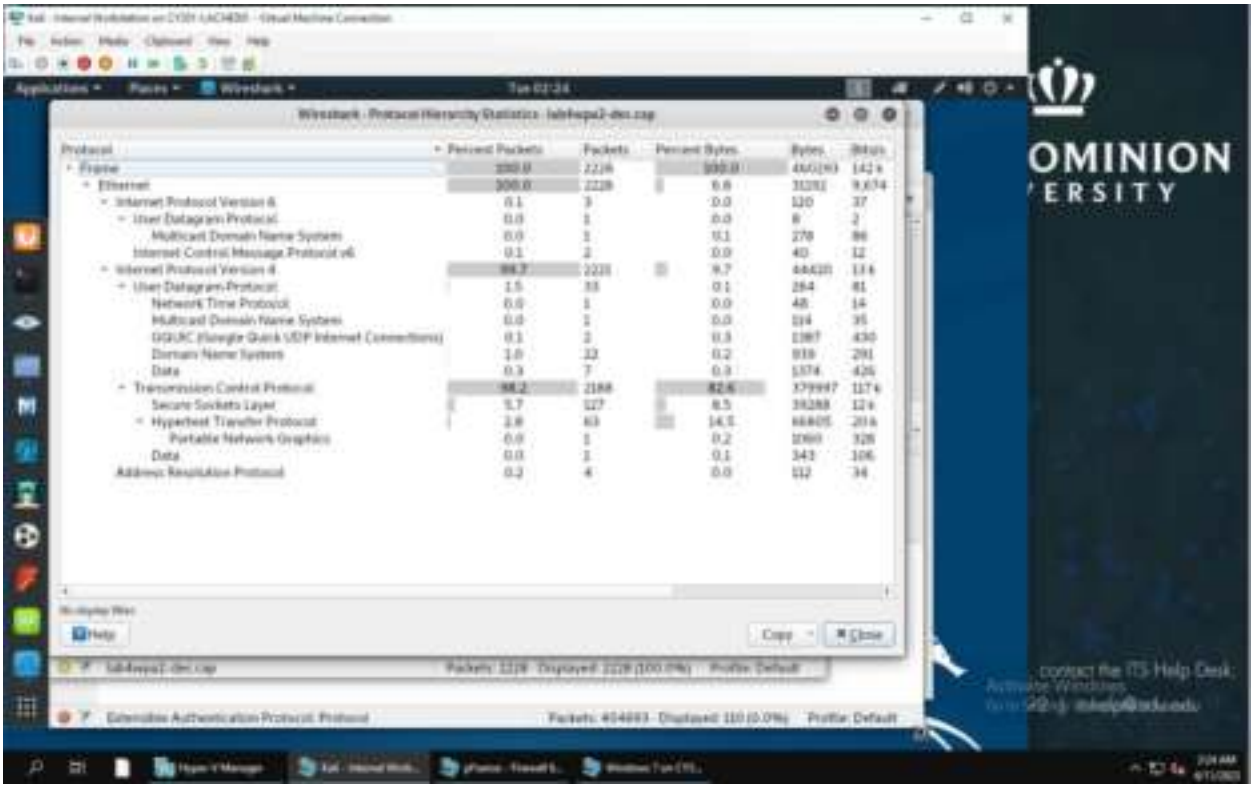
I then used the command “airdecap-ng -p password lab4wpa2.cap -e CCNI” to show all the decrypted packets.



I then used “ls” command to show that it was indeed decrypted, which it was because the “labwpa2-dec.cap” showed up. Then i used the “wireshark lab4wpa2-dec.cap” to show the traffic in wireshark.

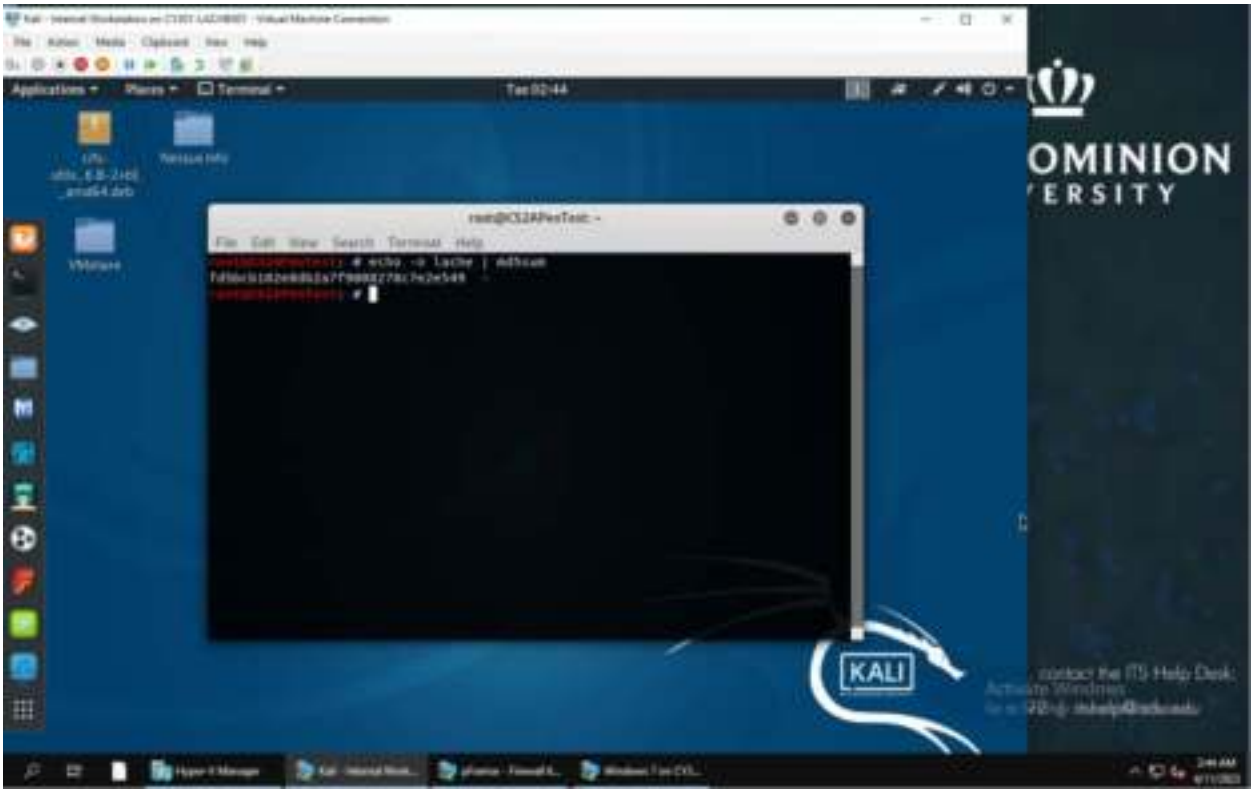


After I typed the wireshark command, it showed all the traffic on wireshark.



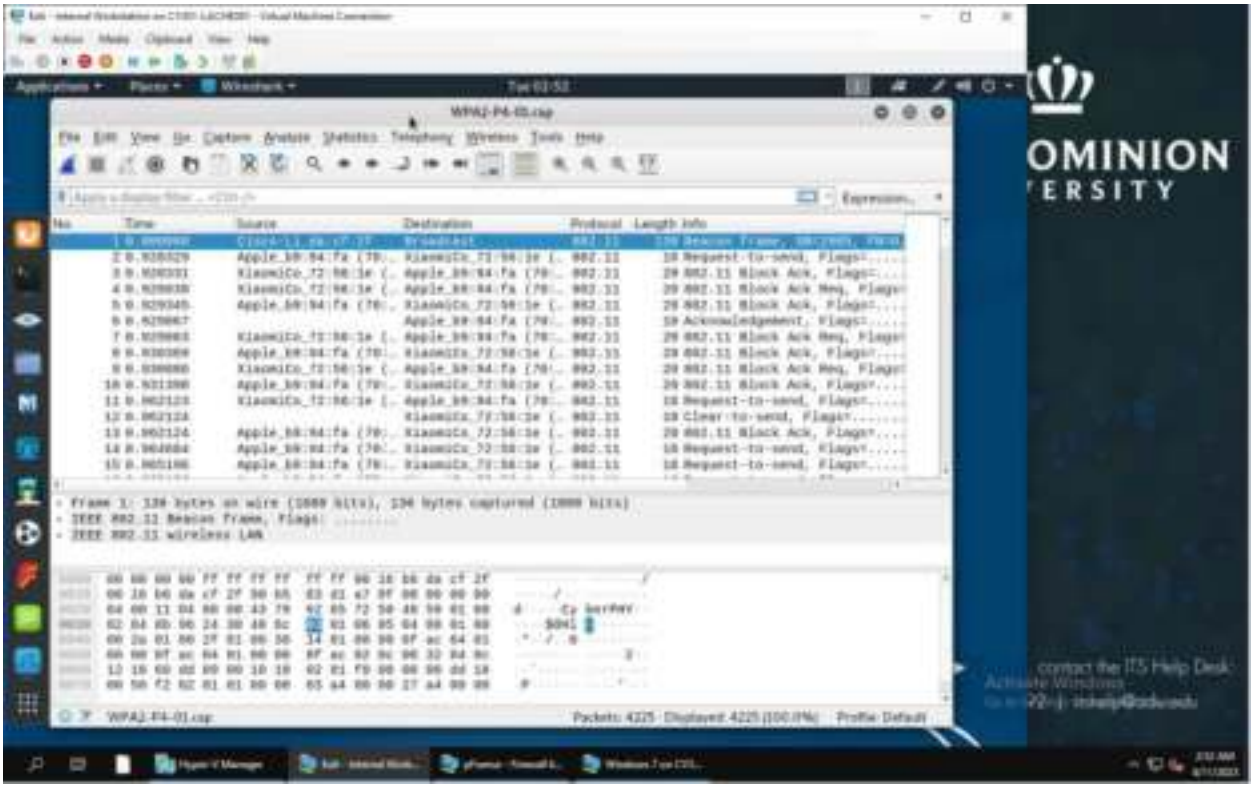
The main different between this traffic and the one found on the WEP is that there seems to be way more TCP traffic compared to the WEP, which had a lot more ARP traffic. Also there seems to be alot more IPV4 traffic as well. It showed that a lot of connections had been established between hosts.

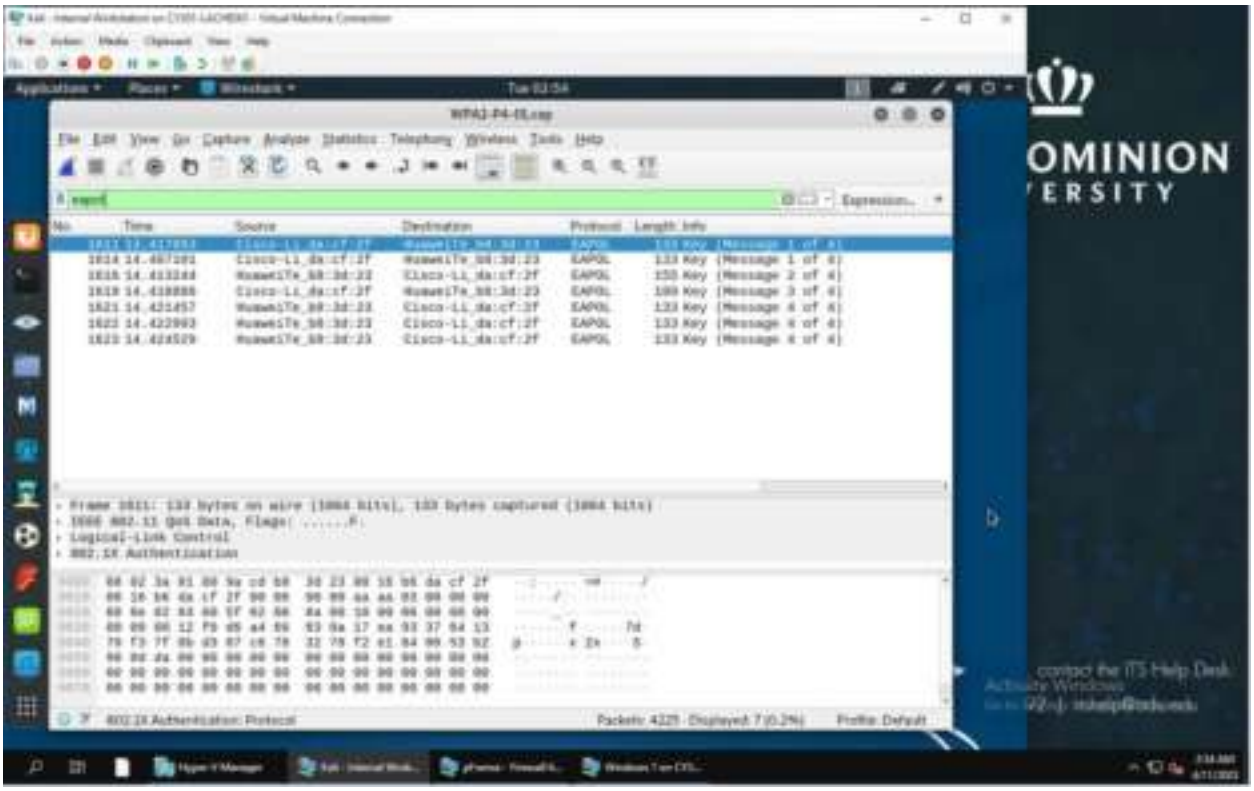
TASK D



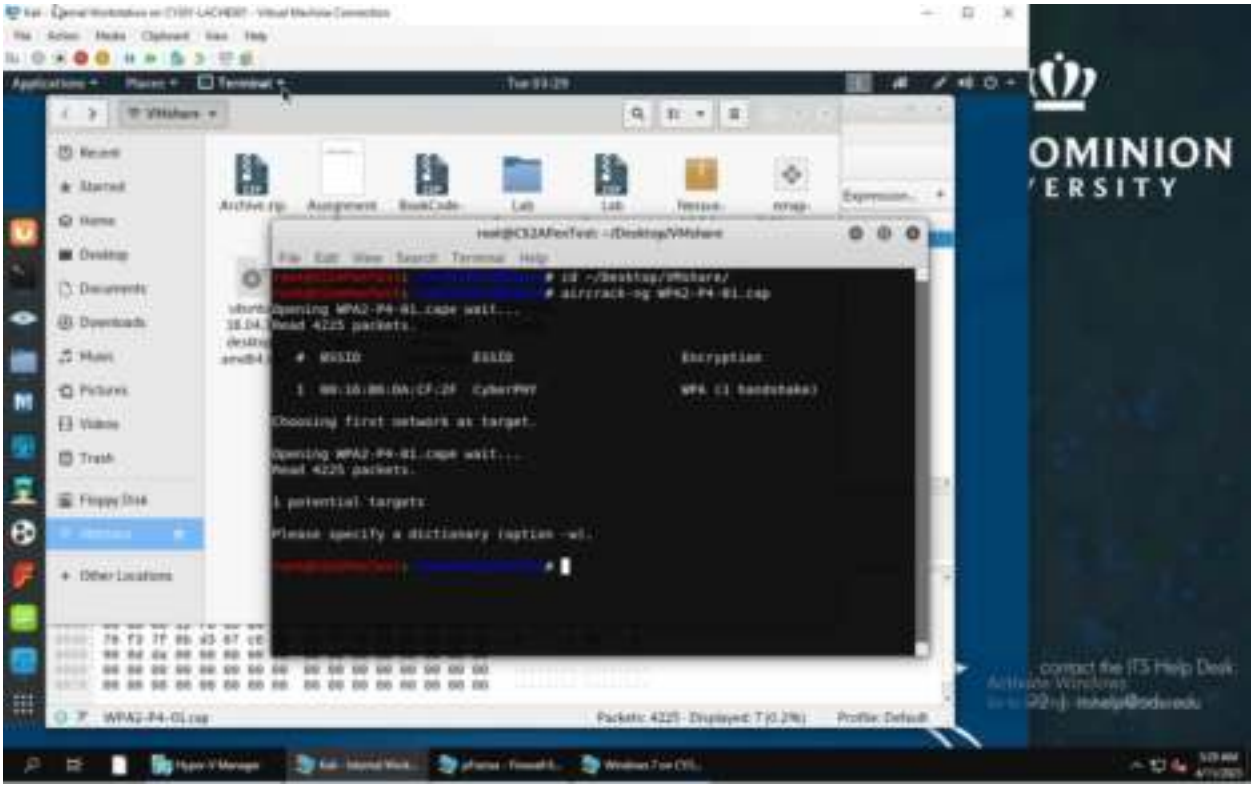
I used the “echo -n lache | md5sum” command to find the hash for my MIDAS.
I had to choose the 4th option out of the list given for us. Which was “WPA2-P4-01.cap”

I unzipped the file by right clicking on the folder and clicked on “extract here”.

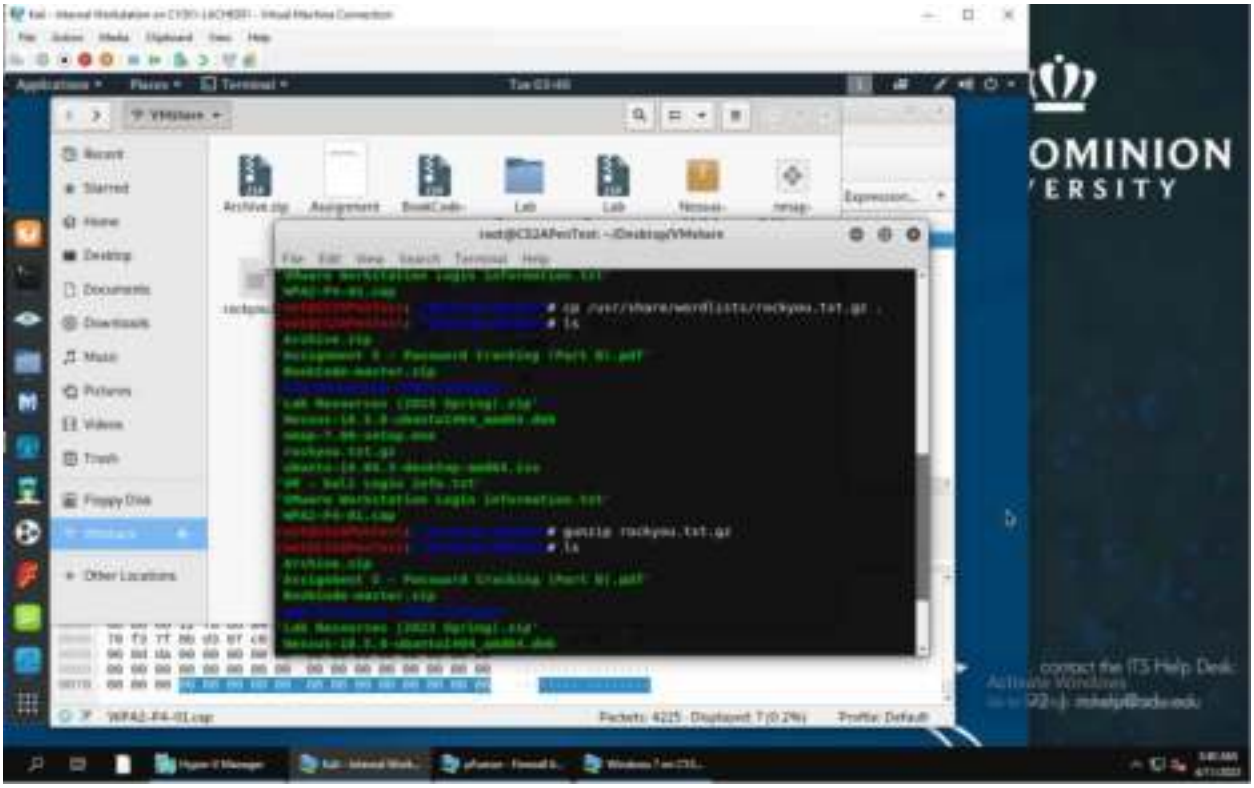




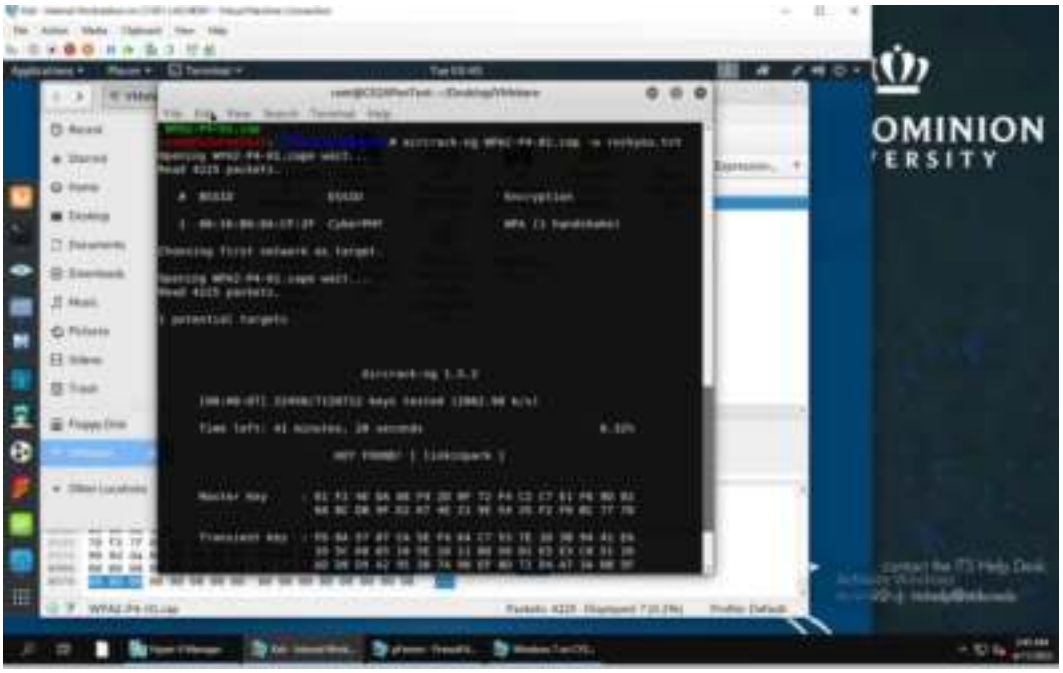
I opened the file I was assigned and this was what I saw.



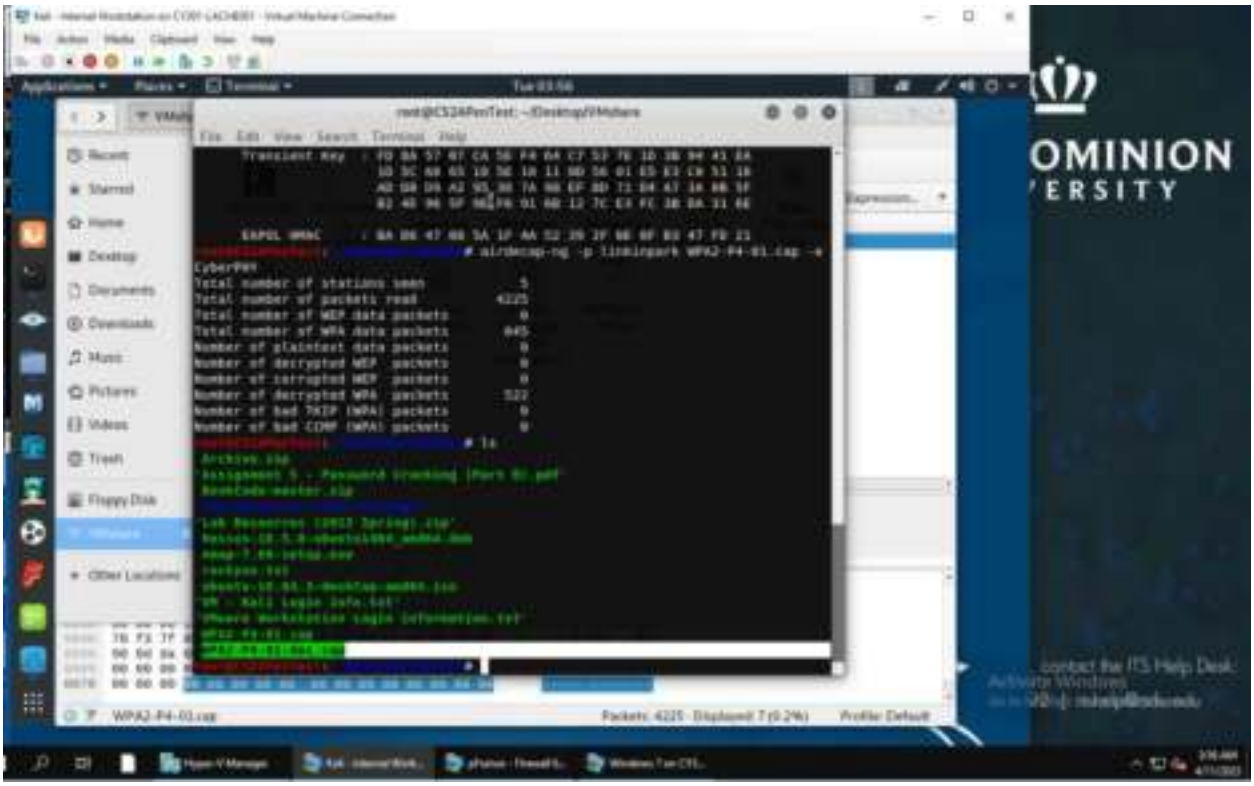
I used the “cd ~/Desktop/VMshare/” command to get into the VMshare directory. From there I used the “aircrack-ng WPA-P4-01.cap” command to try to crack the encrypted file.



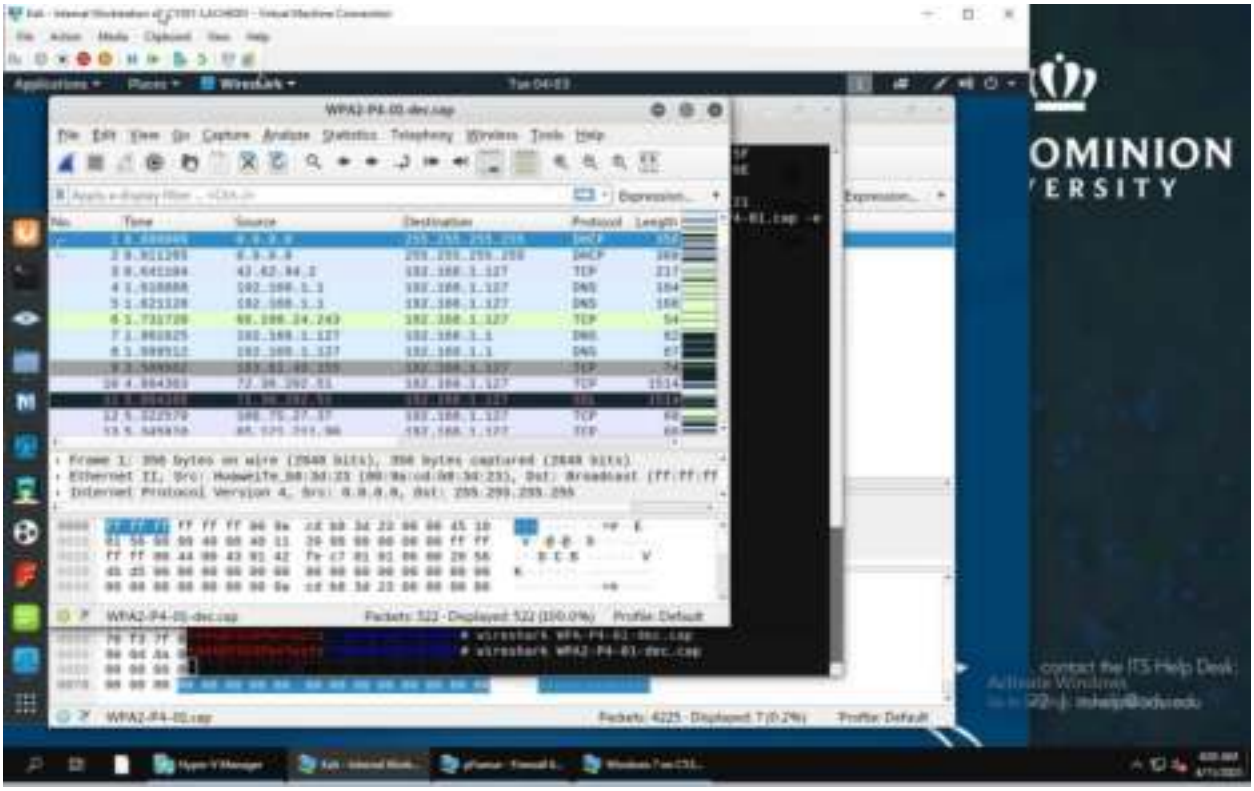
I used the “cp /usr/sharewordlists/rockyou.txt.gz .” command to copy the rockyou.txt file onto my current working directory. I then unzipped the file using the command “gunzip rockyou.txt.gz”. Then used the “ls” command to list the files in the directory.



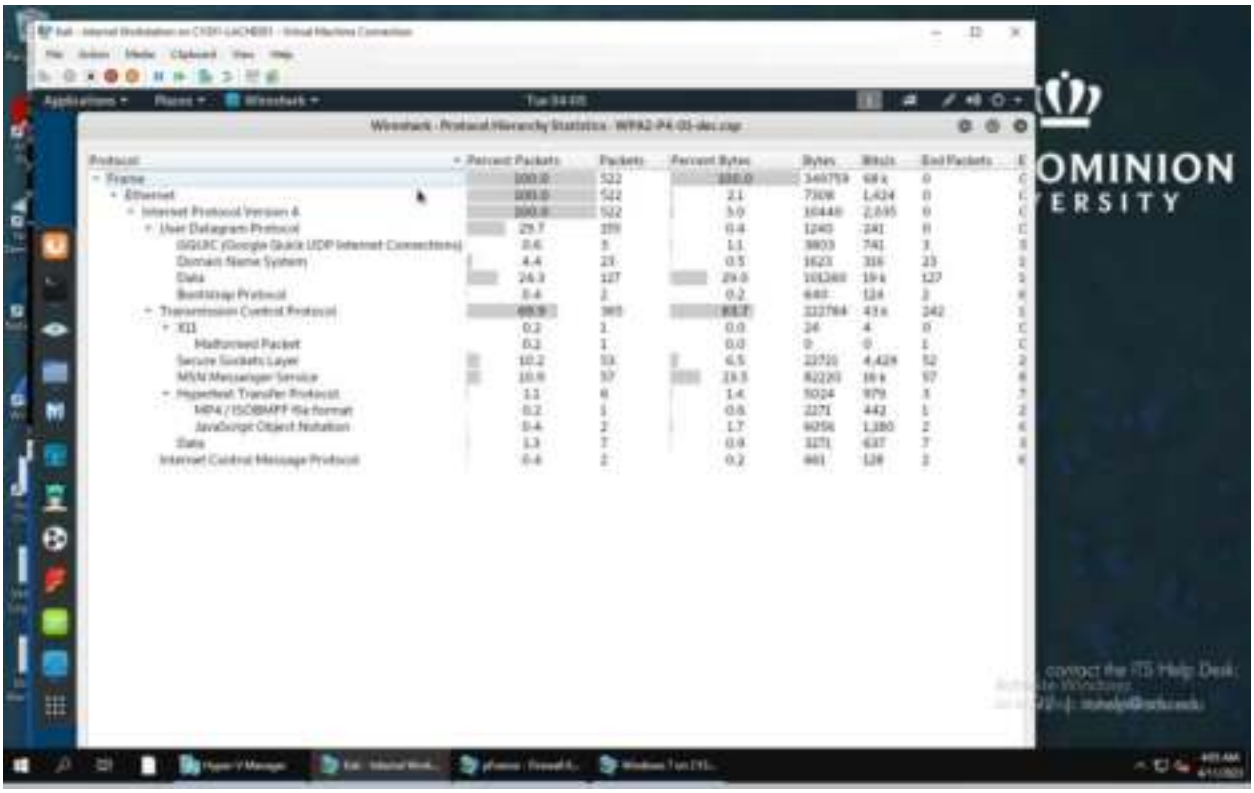
I used the “aircrack-ng WPA2-P4-01.cap -w rockyou.txt” command to decrypt the encrypted file and it showed the Key Found was “linkinpark”.



I used the “airdecap-ng -p linkinpark WPA2-P4-01.cap -e CyberPHY” command to fully decrypt the file. Then used “ls” command to display, to see if if was actually decrypted, and it was.



I used the “wireshark WPA2-P4-01-dec.cap” to display the decrypted traffic for the file.



The protocol hierarchy showed that there were indeed a lot of IPV4 packets. Along witha lot Frame and Ethernet packets as well. Which means that the frame packets shows that there was informational tranfer between two nodes on the same network.While the ethernet packets suggest that there were alot of packets transferred between 2 different networks.