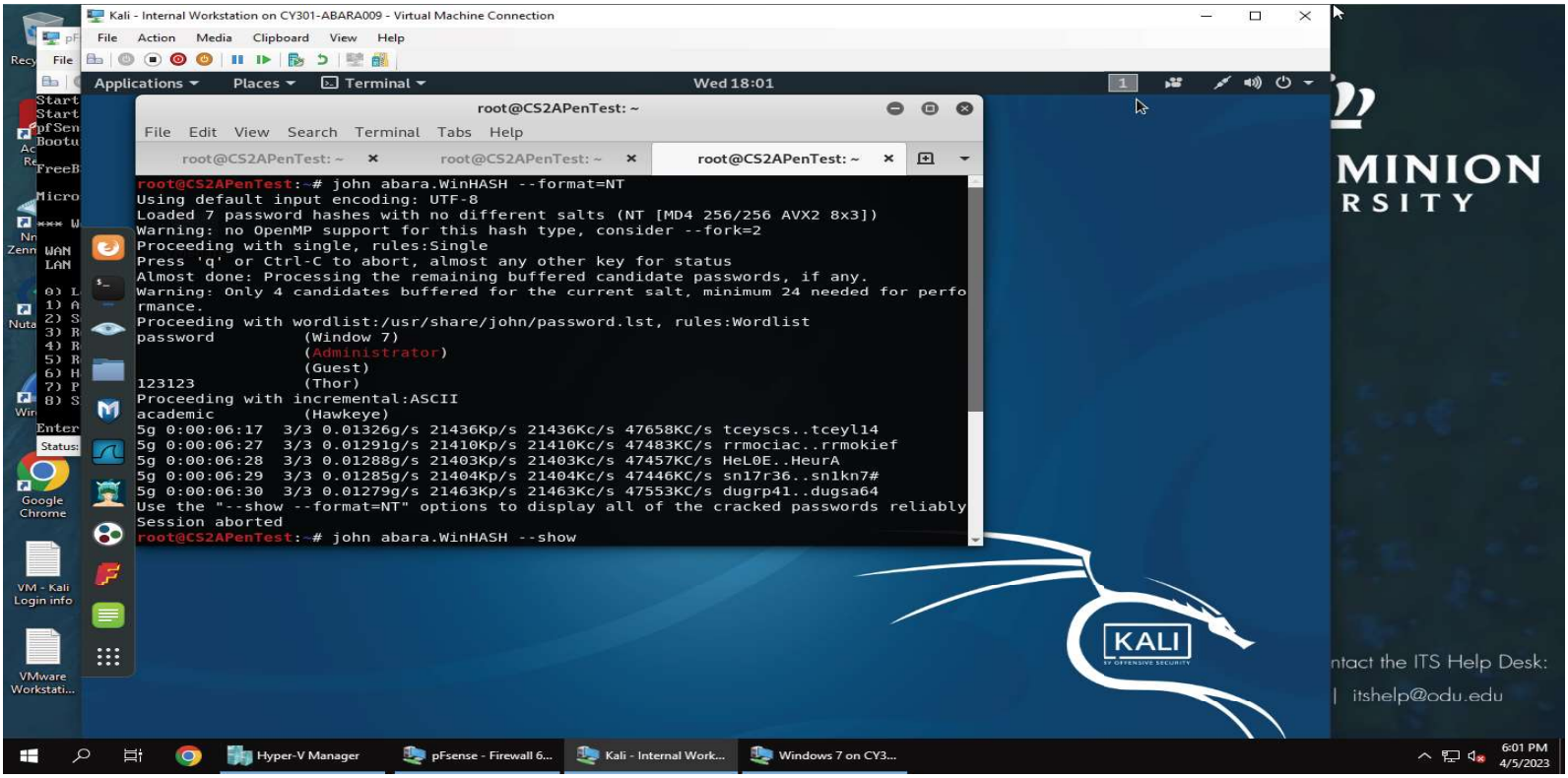
TASK B: WINDOWS PASSWORD CRACKING

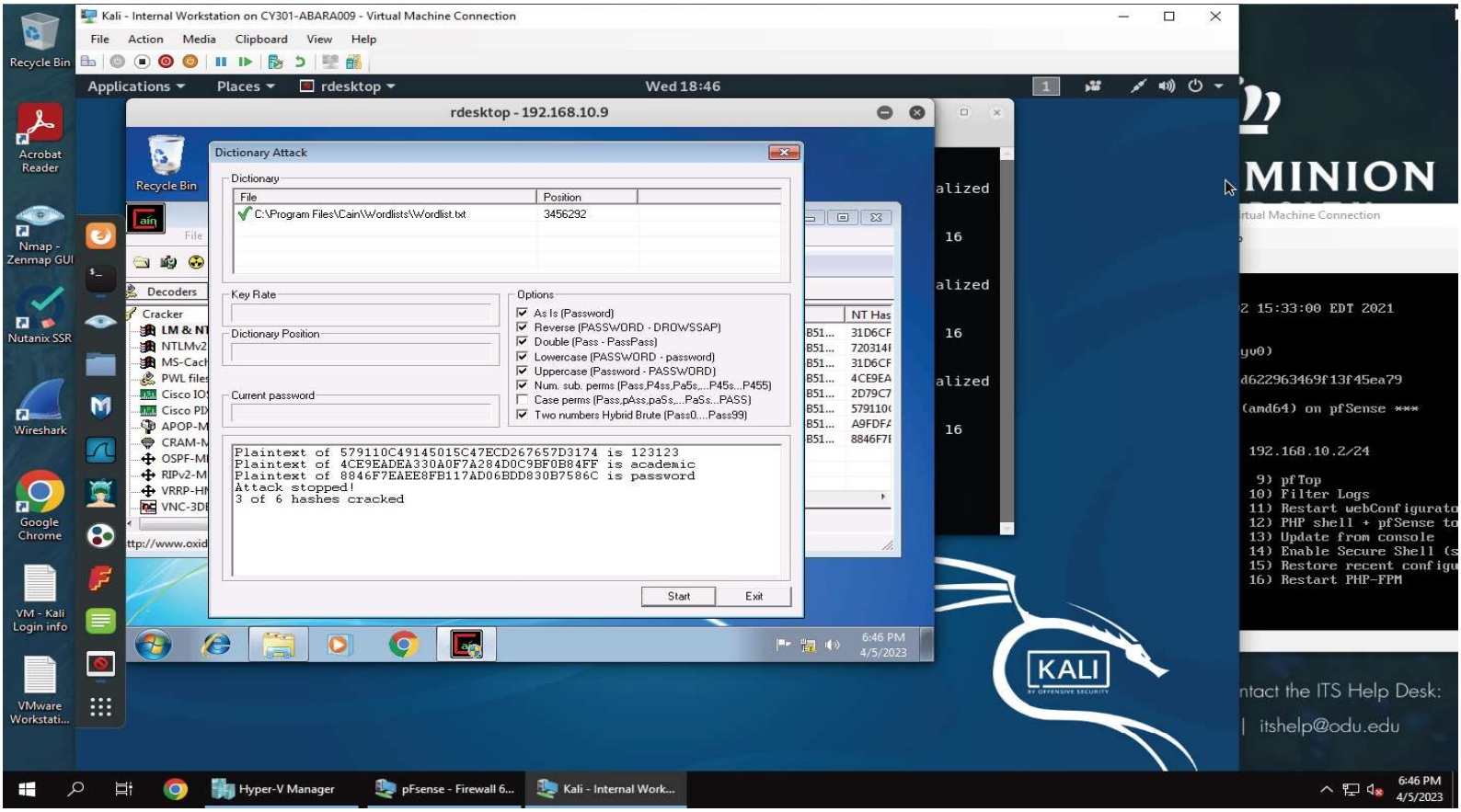
2. 10 points. Save the password hashes into a file named “your_midas.WinHASH” in Kali Linux
(you need to replace the “your_midas” with your university MIDAS ID). Then run John the ripper
for 10 minutes to crack the passwords (You MUST crack at least one password in order to
complete this assignment.)



For this command, I copied and pasted the users’ hashes into a file named abara.winHASH using “gedit abara.winHASH.” To use John the Ripper, I used john abara-winHASH –format=NT to crack the password hashes in this file. The terminal shows that John the Ripper cracked Thor’s password of 123123 and Hawkeye’s password of academic.

TASK B: WINDOWS PASSWORD CRACKING

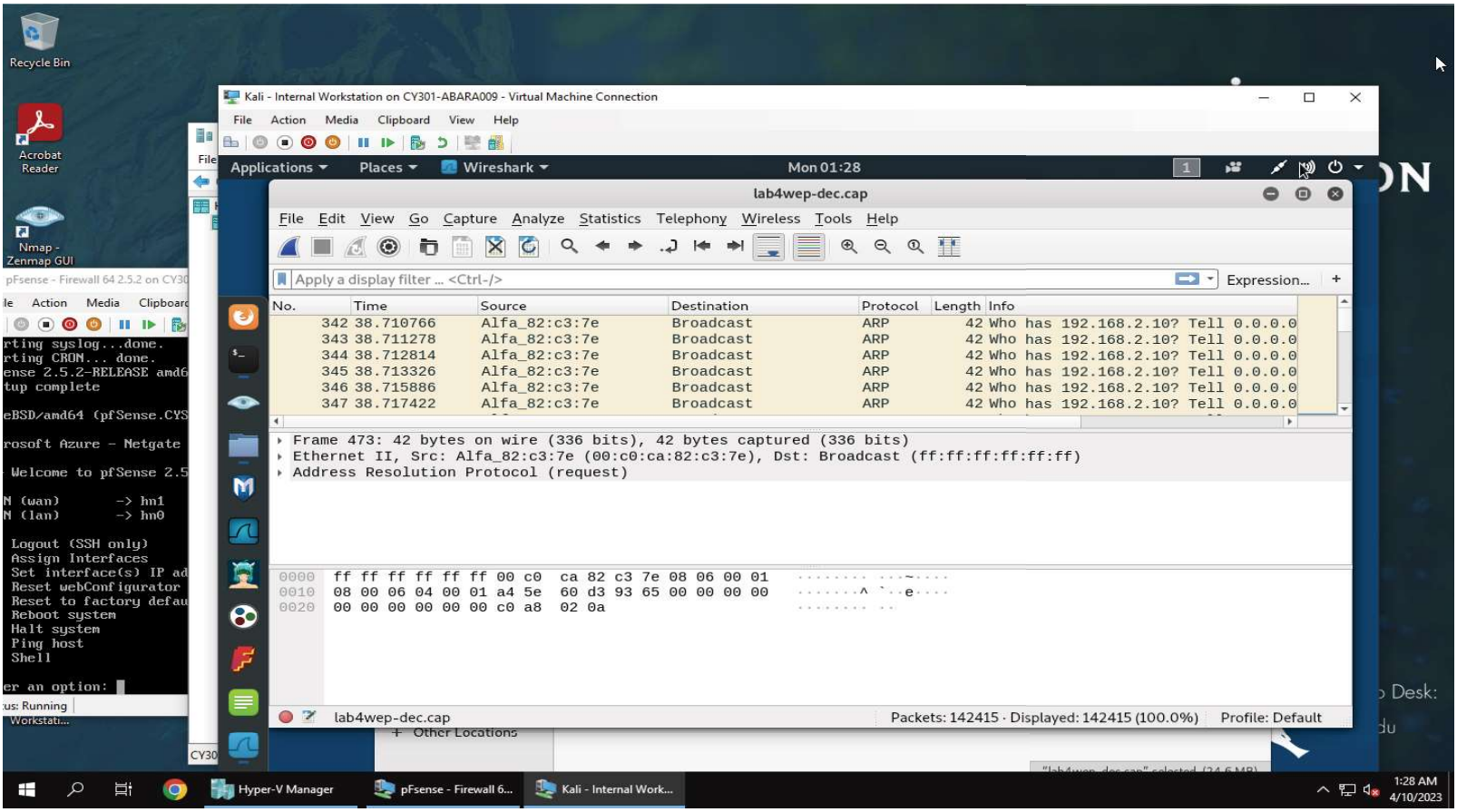
10 points. Upload the password cracking tool, Cain and Abel, to the remote Windows 7 VM, and
install it via a remote desktop window. Then, implement BOTH brute force and dictionary
attacks to crack the passwords. (You MUST crack at least one password in order to complete this
assignment.)



Before this step, I used “upload ca_setup.exe c;// to the c drive of windows for easier setup. Then, for this command, I used rdesktop -u TryHackMe 192.168.10.9 to access the Window’s remote desktop from Internal Kali. In the remote desktop, I went to files, C drive and double clicked on ca_setup.exe and ran the file to install Cain and Abel. Once I was in the program, I clicked on cracker and next that automatically dumped all the password hashes of the users in the window’s system. Then, I highlighted all the user hashes and right clicked on the dictionary attack option and selected NTLM hash. Then, I specified the dictionary by adding the wordlist file to the attack to start the dictionary attack. Here, it shows that 3 of the 6 password hashes were cracked. Cain and Abel were able to crack the hash text passwords, revealing the plaintext of 123123, academic, and password.

TASK C:

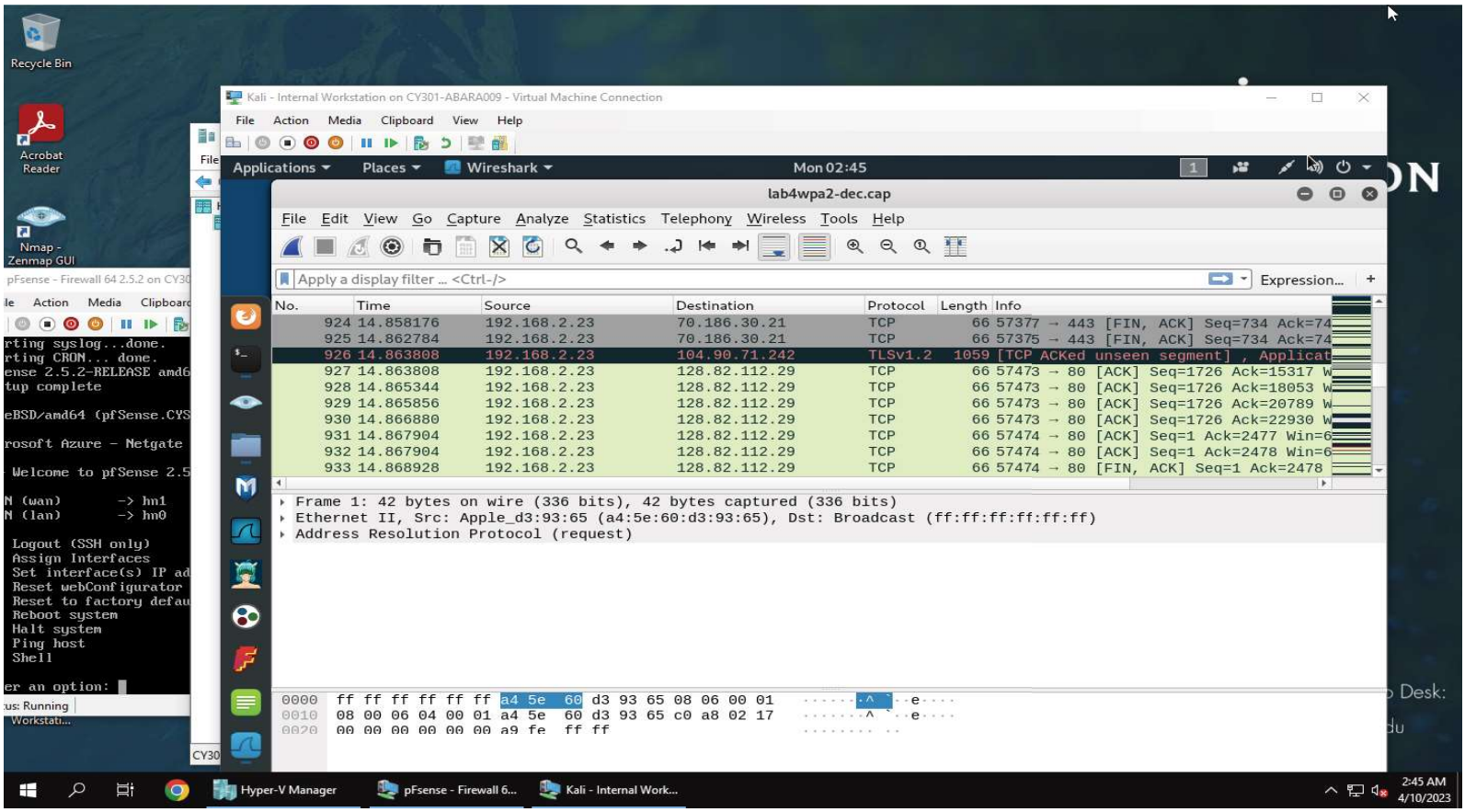
1. Decrypt the lab4wep. cap file (5 points) and perform a detailed traffic analysis (5 points)



I used “aircrack-ng lab4wep.cap” to gain the key of F2:C7: BB: 35:B9 to decrypt the file. Then, I copy and pasted this key into the command, “airdecap-ng -w F2:C7: BB: 35:B9 lab4wep.cap to crack this WEP file. Then, I went into my filesystem and double clicked on lab4wep-dec.cap to view the decrypted Wireshark traffic. The Wireshark traffic shows that there were many Broadcast messages when there was an interruption during the attack. During this aircrack attack, this source “Alfa_82:c3:7e” sent any broadcast messages using the protocol ARP that consisted of many unnecessary messages inquiring about the IP address. If a network viewed their traffic and saw this disruption, the network should block Alfa_82:c3:7e from accessing their network and causing this immense network traffic. An organization can use this information to block sources like these that can create security concerns. In addition, it is evident that the frame was 473, with 42 bytes on wire (336 bits) and 42 bytes captured (336 bits.)

TASK C:

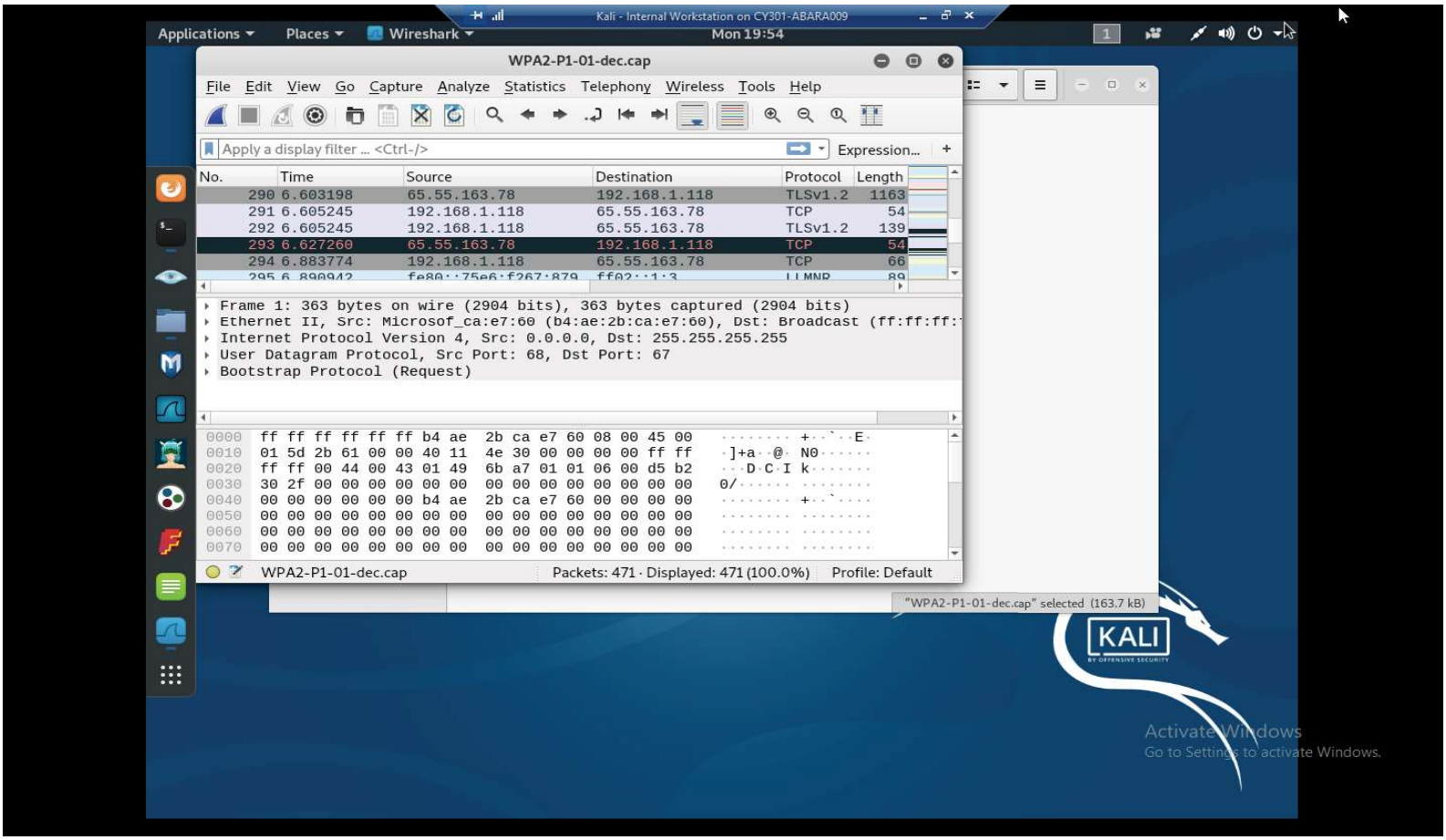
2. Decrypt the lab4wpa2. cap file (5 points) and perform a detailed traffic analysis (5 points)



Similarly to WEP, I first started to decrypt this WPA2.cap file by using “aircrack-ng lab4wpa2.cap” This command then showed me a list of networks with BSSID and ESSIDs. I looked at the fourth network which I was using for the lab. The terminal showed that the WPA encryption had an ESSID of CCNI. Then, I copied rockyou.txt to my working directory using “cp /usr/share/wordlists/rockyou.txt.gz .” Then I gunziped that file. Then to gain the password of the network , I used aircrack-ng lab4wpa2.cap -w rockyou.txt. I found the key was “password.” To decrypt the packets, I used airdecap-ng -p password lap4wpa.cap -e CCNI. After analyzing the decrypted packets in Wireshark, it is evident that there is a lot of traffic originating from the source 192.168.2.23 and heading to the destination IP of several addressing composing of 70.186.30.21, 104.90.71.242, 120.02.112.29. It is evident that there were a lot of packets that used the TCP protocol. In addition, there were {FIN, ACK} messages. There were seq= 1720 and Ack=5317. This capture shows that the was address resolution protocol (request).

TASK D:

1. Implement a dictionary attack and decrypt the traffic. - 20 points
2. 2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored
from this encrypted traffic file. -10 points



For this task, I used “echo -n abara | md5sum" that echoed my password hash of 6469be1b2b738cc578425f14a92bf671. Because my hash ends in 1, I used the WPA2-P1-01-decap file. I double-clicked on the VMshare folder on the desktop and right clicked “Lab resources” then clicked on “extract here”to unzip the file. Then I copied the file to the c drive in “VMshare” to access this file in internal kali. Then, I went to the kali terminal and repeated the previous steps to crack the password. I used aircrack=ng WPA2-P1-01.cap. Then I used aircrack-ng lab4wpa2.cap -w rockyou.txt to find the key of PASSWORD. Then I used airdecap-ng -p PASSWORD WPA2-P1-01.cap with the network ESSID to gather the decrypted Wireshark file. From analyzing this capture, it is evident that there are a variety of protocols used. One major protocol apparent is the TCP protocol There are many packets originating from sources of 65.55.163.76 and 192.168.1.118, Many packets additionally reach the destination of 192.168.1.110 and 65.55.163.78. Out of this Wireshark capture, there were471 packets displayed. In Frame 1, there were 363 bytes on wire and captured (2904 bits.) This capture shows that the network was using Internet Protocol Version 4, . The capture also shows that the network used user datagram protocol with a source port of 68 and a dst port of 67. The capture shows that there was Bootstrap Protocol request. In addition, it was present that there was TLSv1.2 protocol used in the traffic and network communications.