Old Dominion University

CYSE 301 Cybersecurity Techniques and Operations

Assignment #5 Password Cracking

Bradley Hamilton

01240068

TASK A

1. Linux Password Cracking:

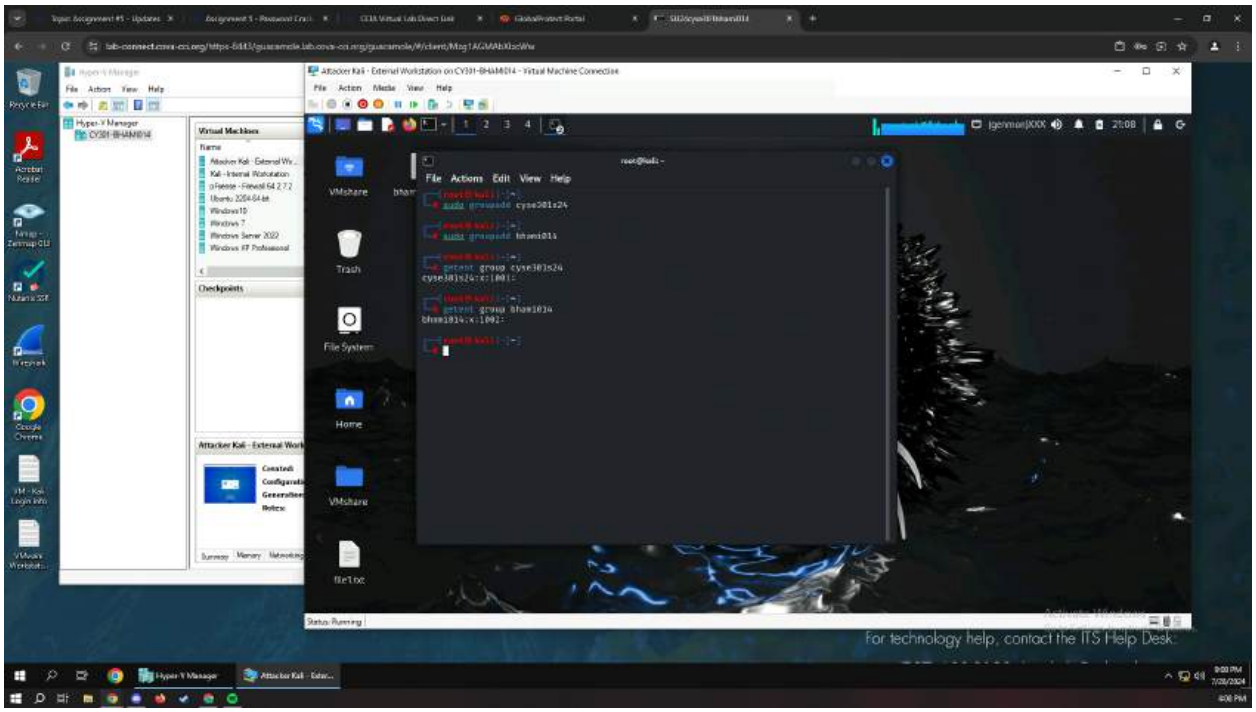

Figure 1 Groups being made with CYSE301s24 and MIDAS ID

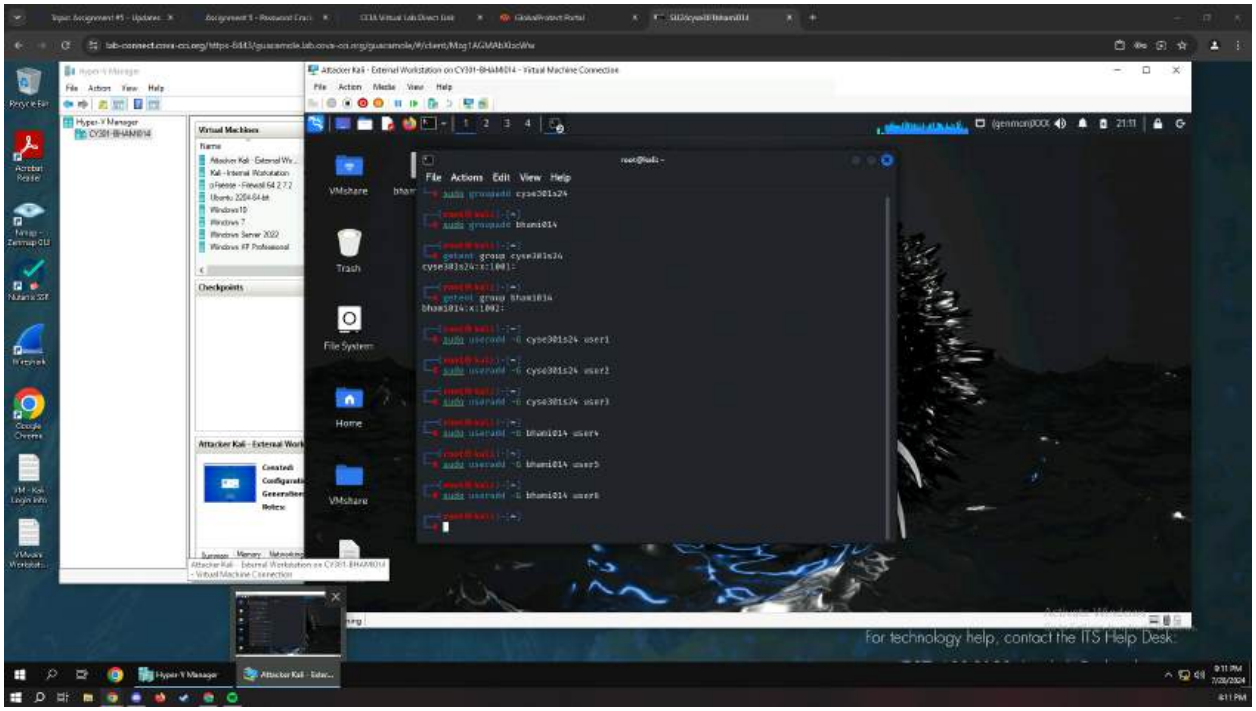

Figure 2 Screenshot of Users being added to groups

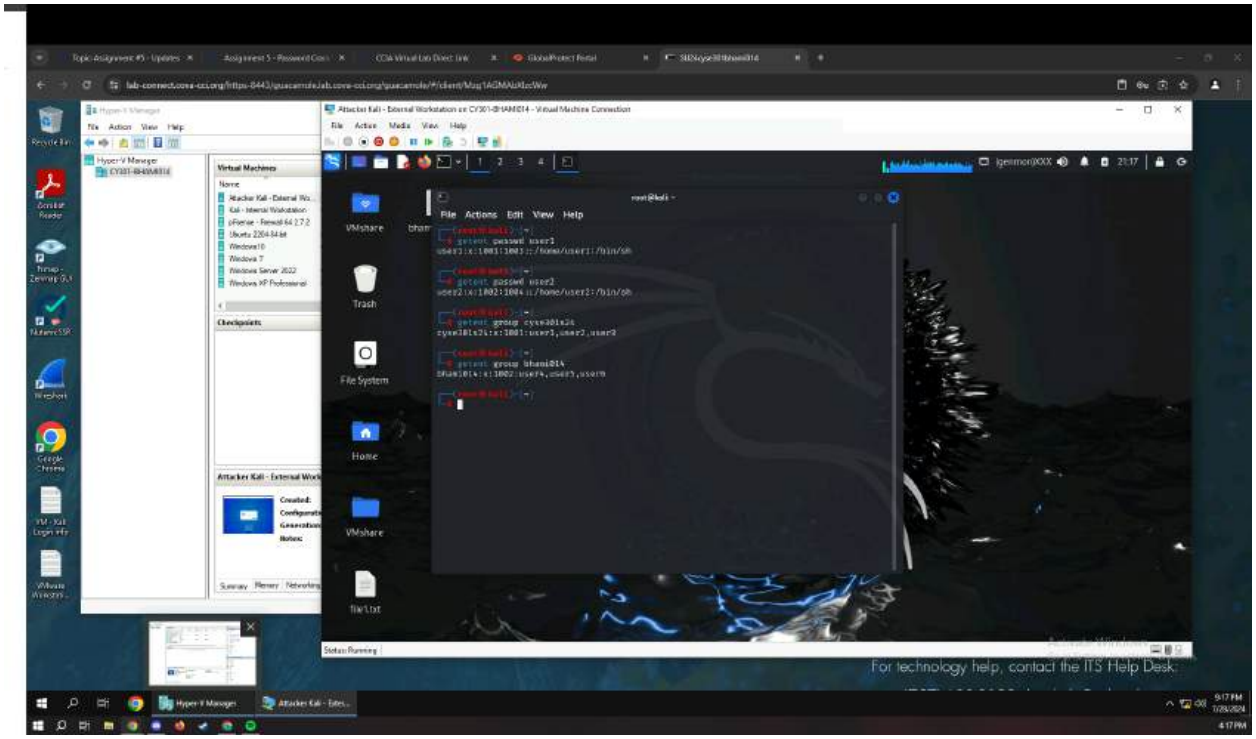

Figure 3 Screenshot of groups listing users

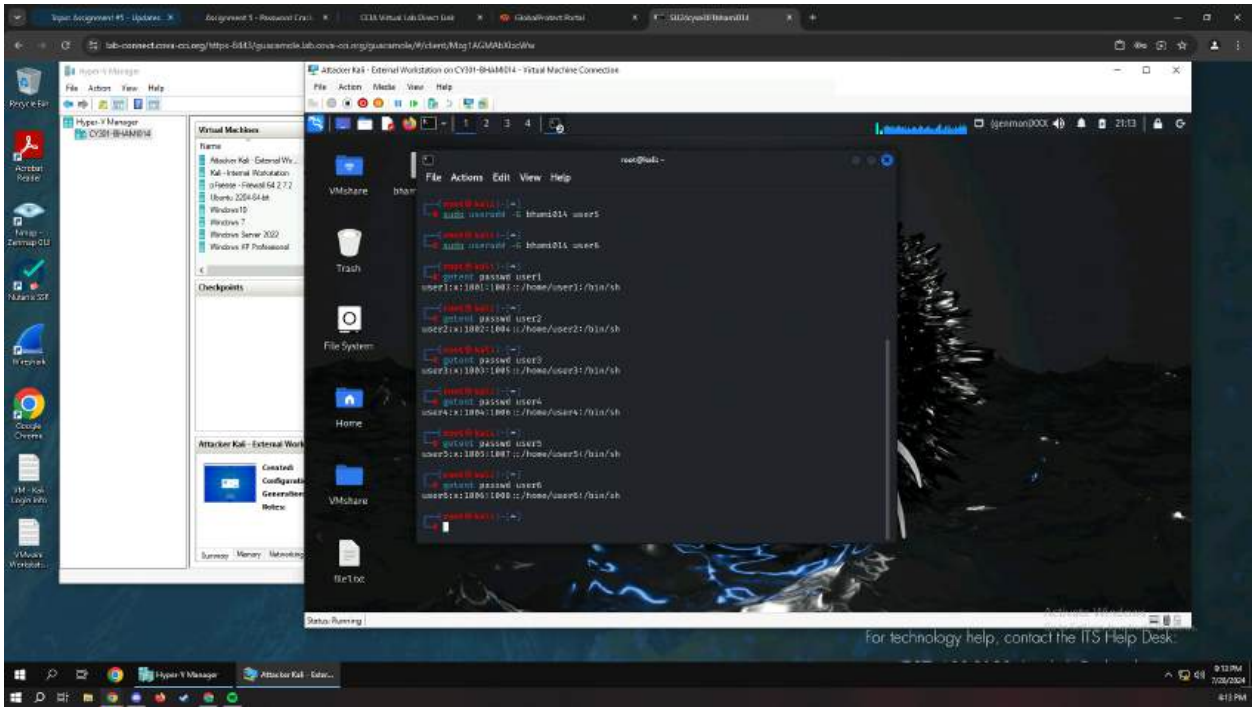

Figure 4 Screenshot of individual password hashes

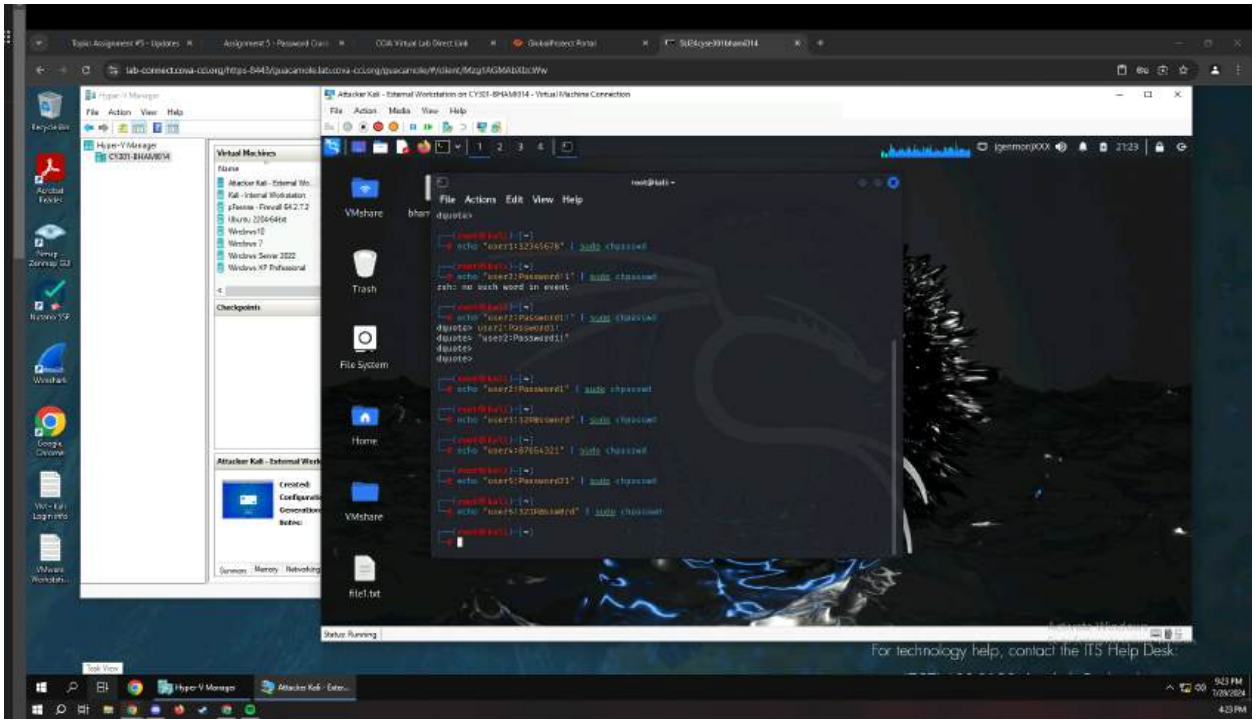

Figure 5 Screenshot of changing user passwords to easy, medium, and hard passwords

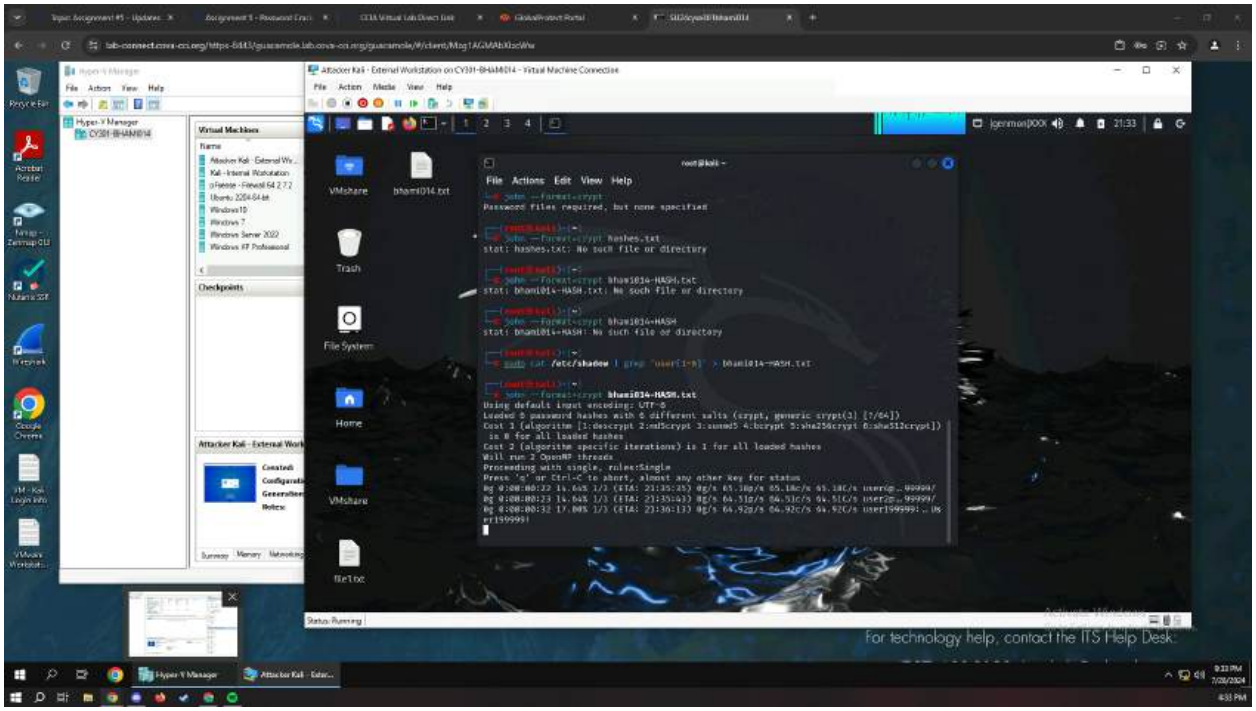

Figure 6 Screenshot cracking passwords using –format=crypt command

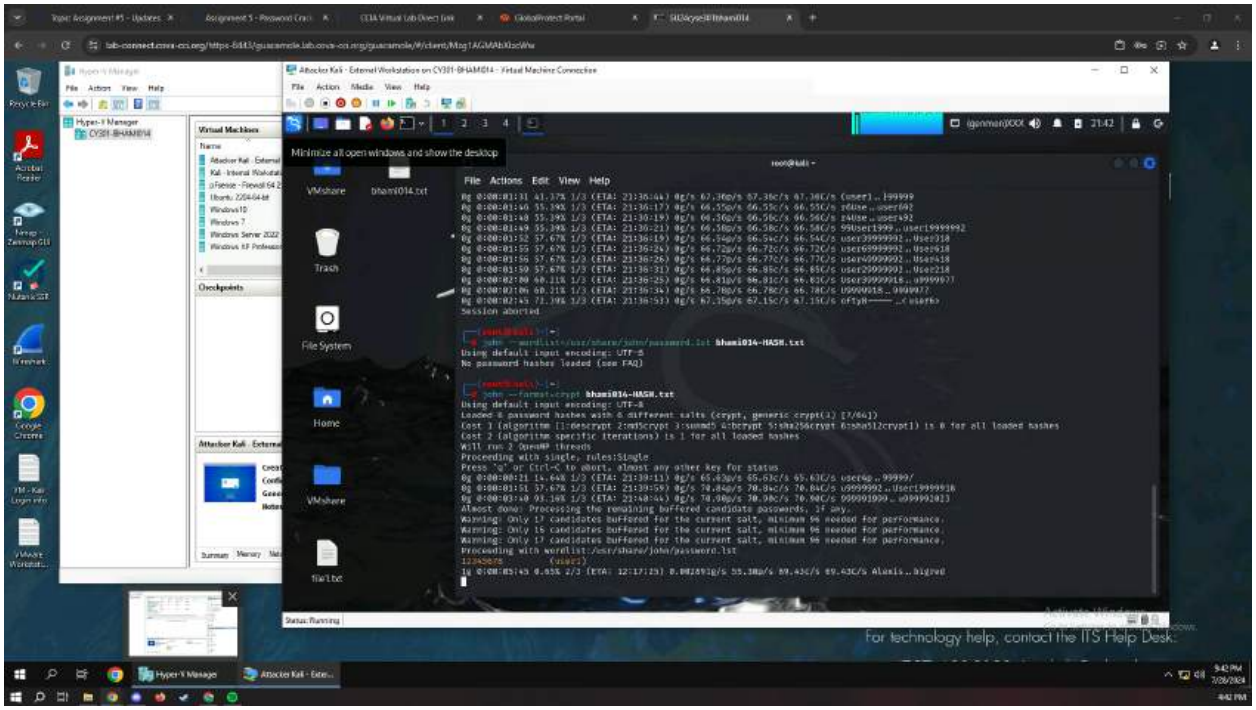

Figure 7 shows password being cracked for one of the users

Password cracking is very time consuming and the screenshot above shows one being cracked, the following screenshots show two others being revealed

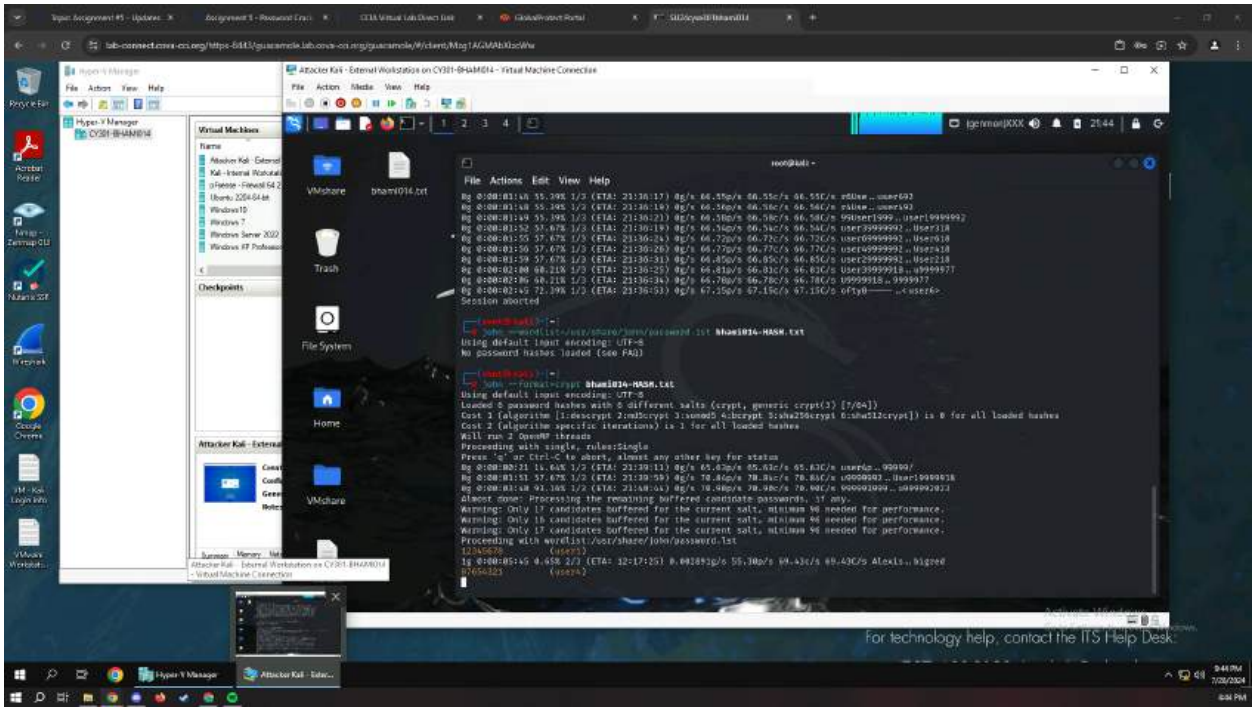

Figure 8 second password revealed

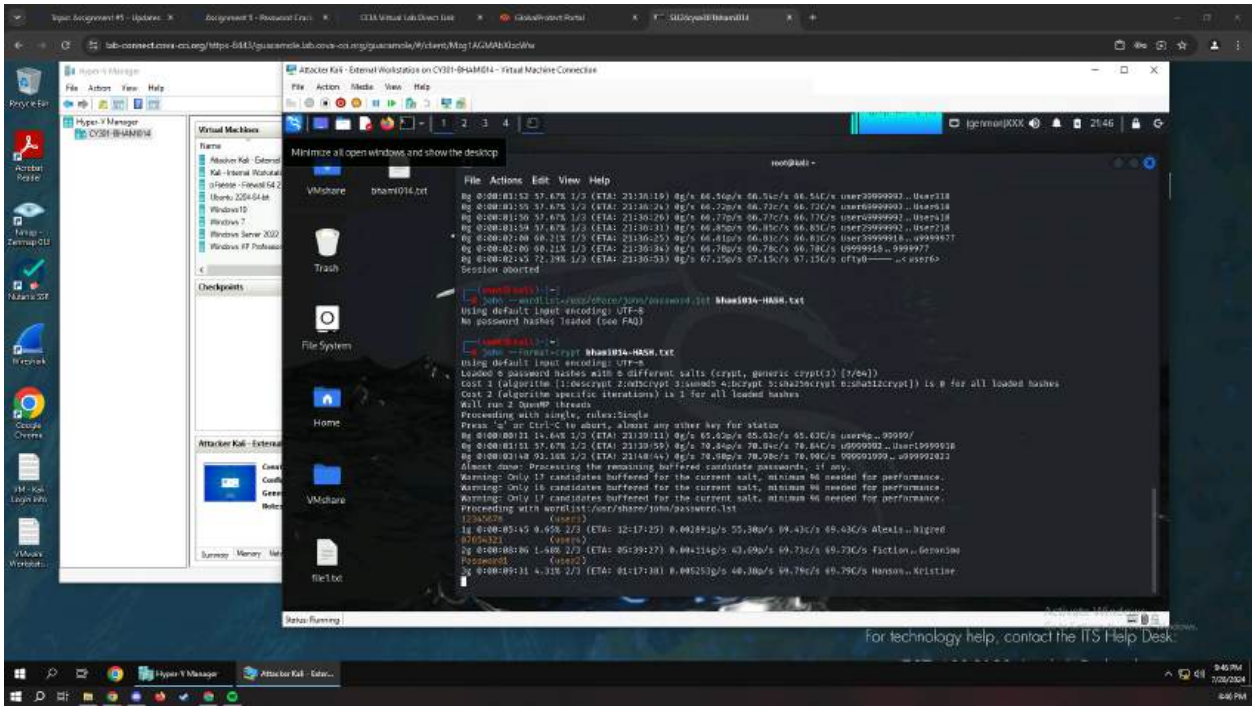

Figure 9 Screenshot of third password cracked.

TASK B

1. Windows Password Cracking:

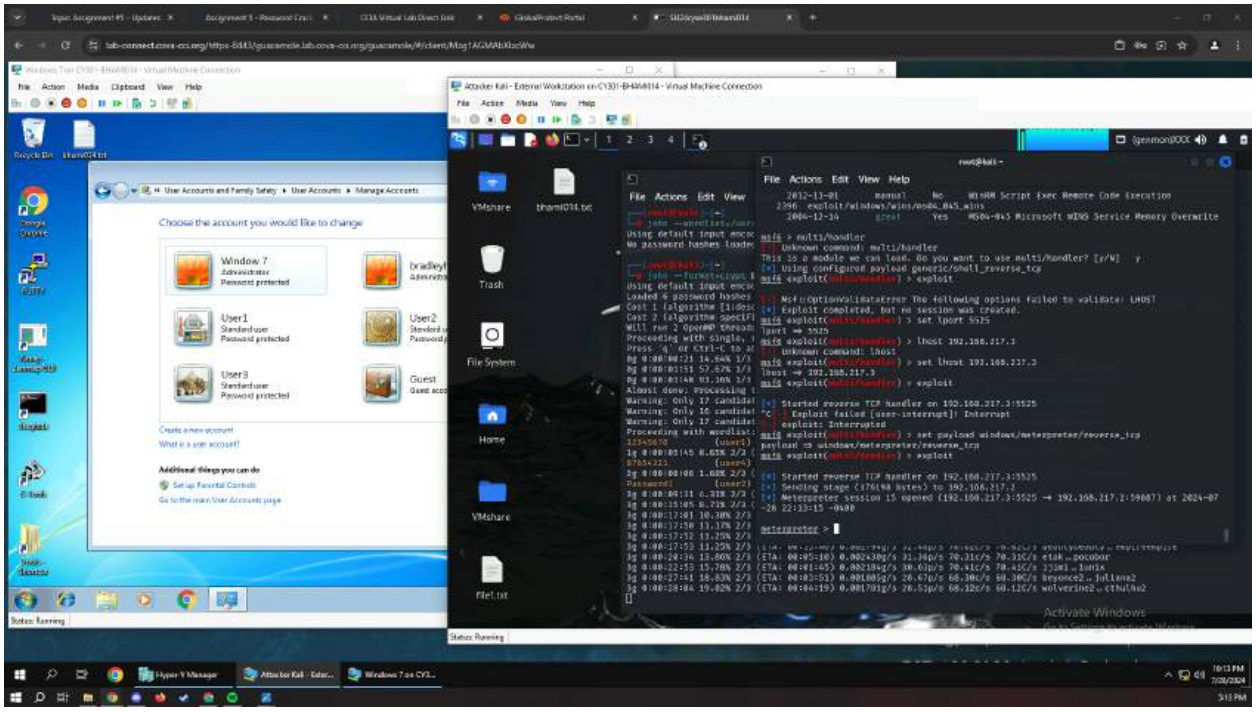

Figure 10 Screenshot of new users created on Win 8 and reverse shell connection to Win 7 VM

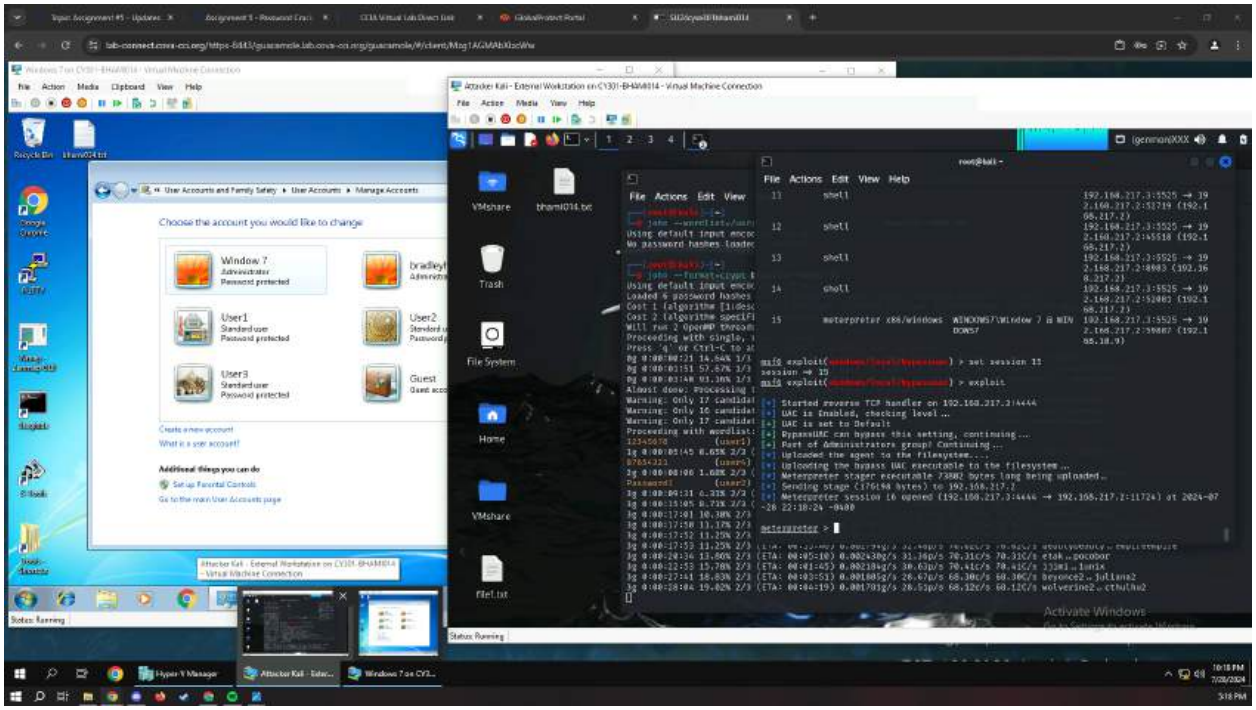

Figure 11 Screenshot of admin privileges from meterpreter

Admin access is needed to perform hashdump command on meterpreter.

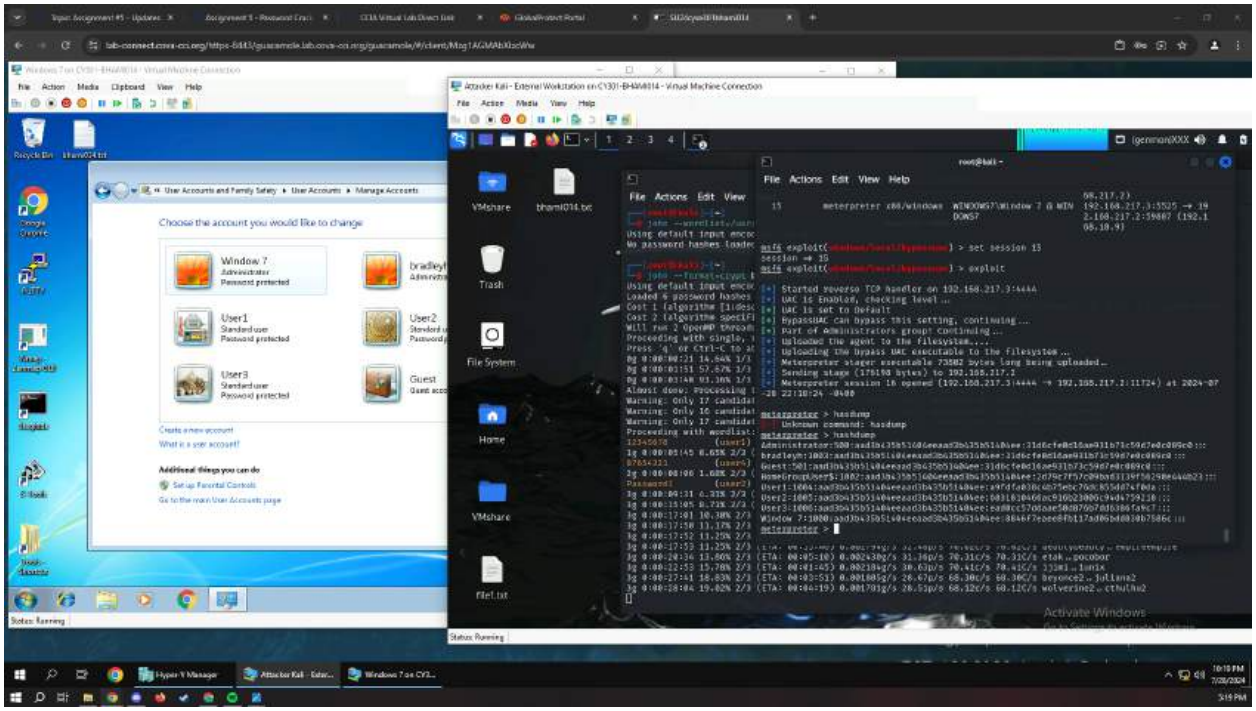

Figure 12 Screenshot of hash dump being executed and grabbing all users from Win 7

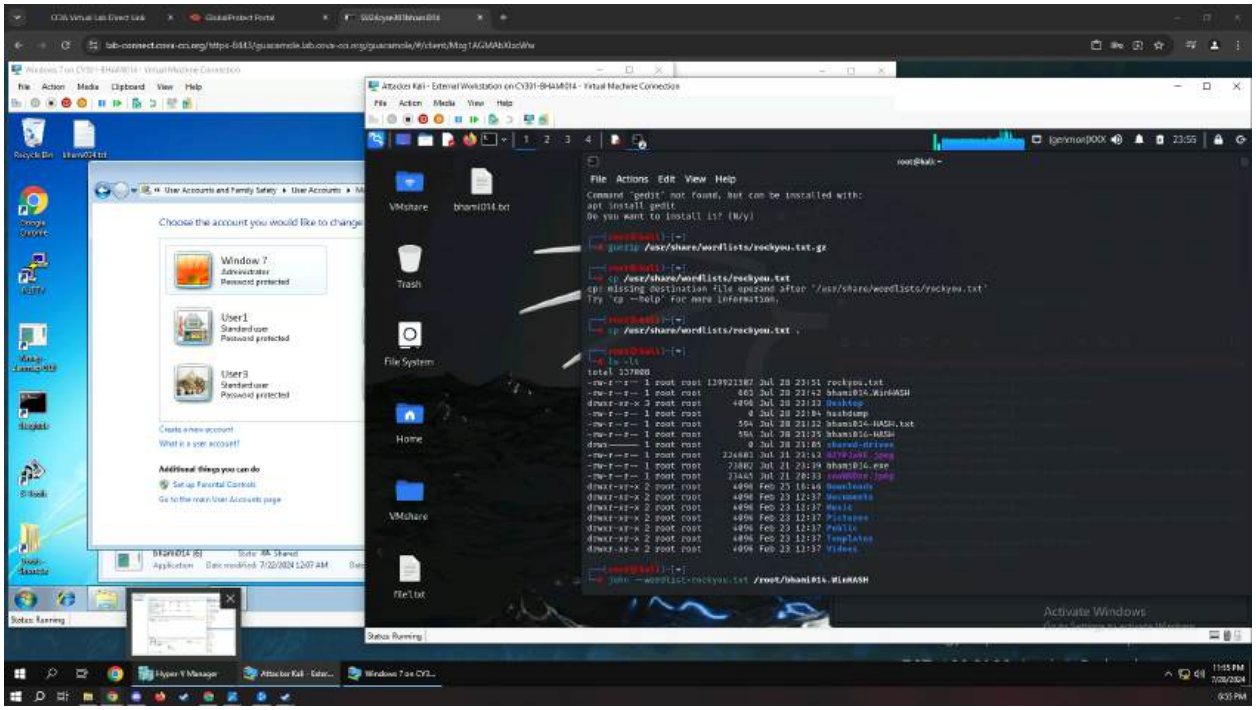

Figure 13 Screenshot of retrieving rockyou.txt for password definitions

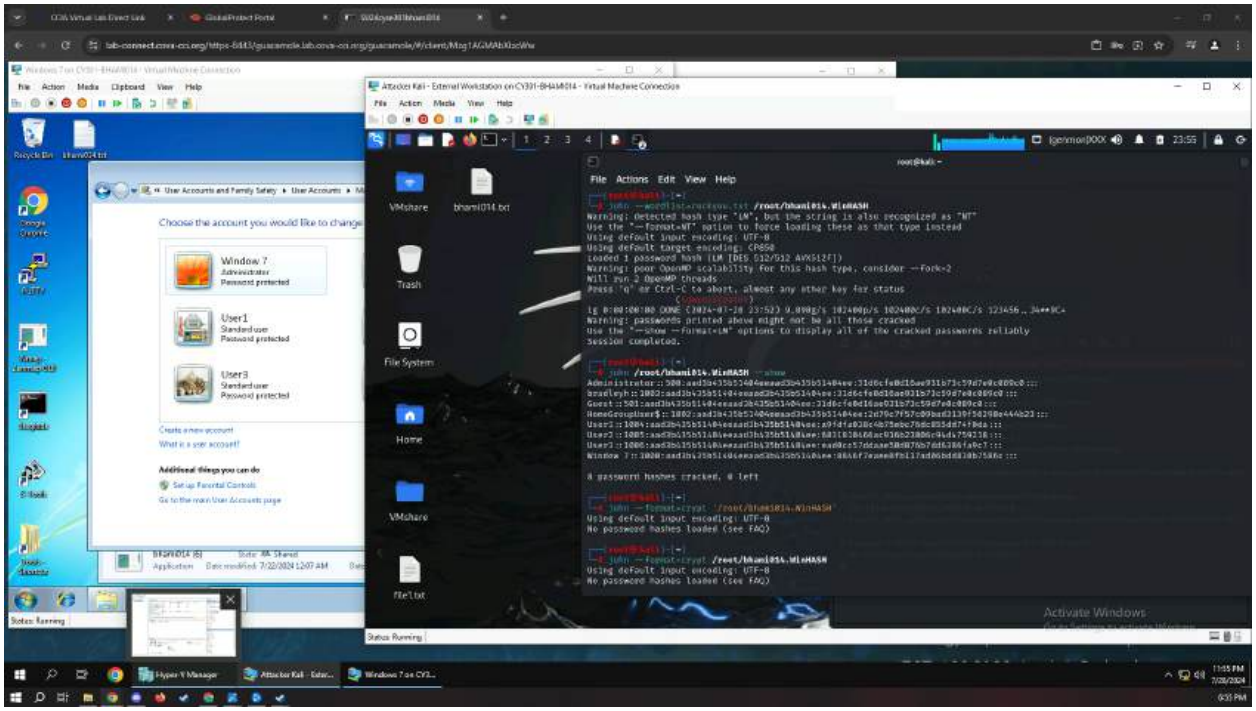

Figure 14 Screenshot of executing password cracking with rockyou.txt extracted.

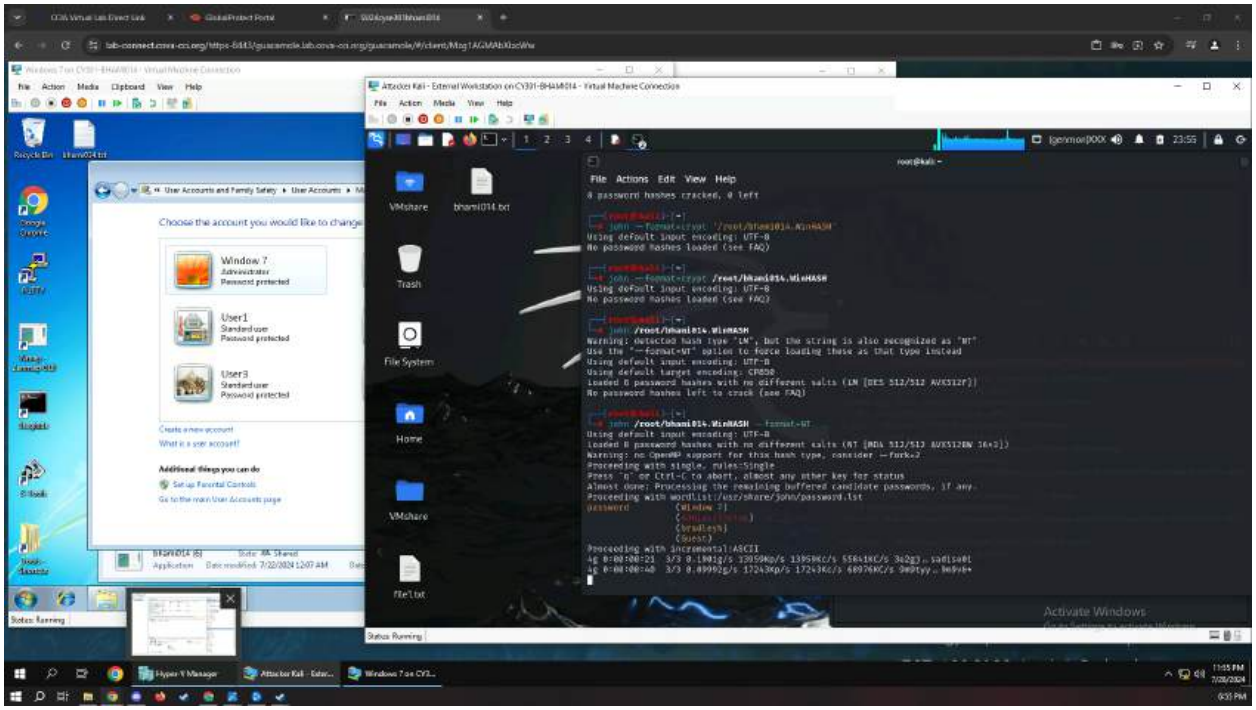

Figure 15 Screenshot of password cracks of 4 users.

Win 7 has ‘password’ and 3 others are passwordless. The other 3 users were still not cracked after 1 hour of time elapsing.

TASK C

2. Decrypting WEP and WPA/WPA2:

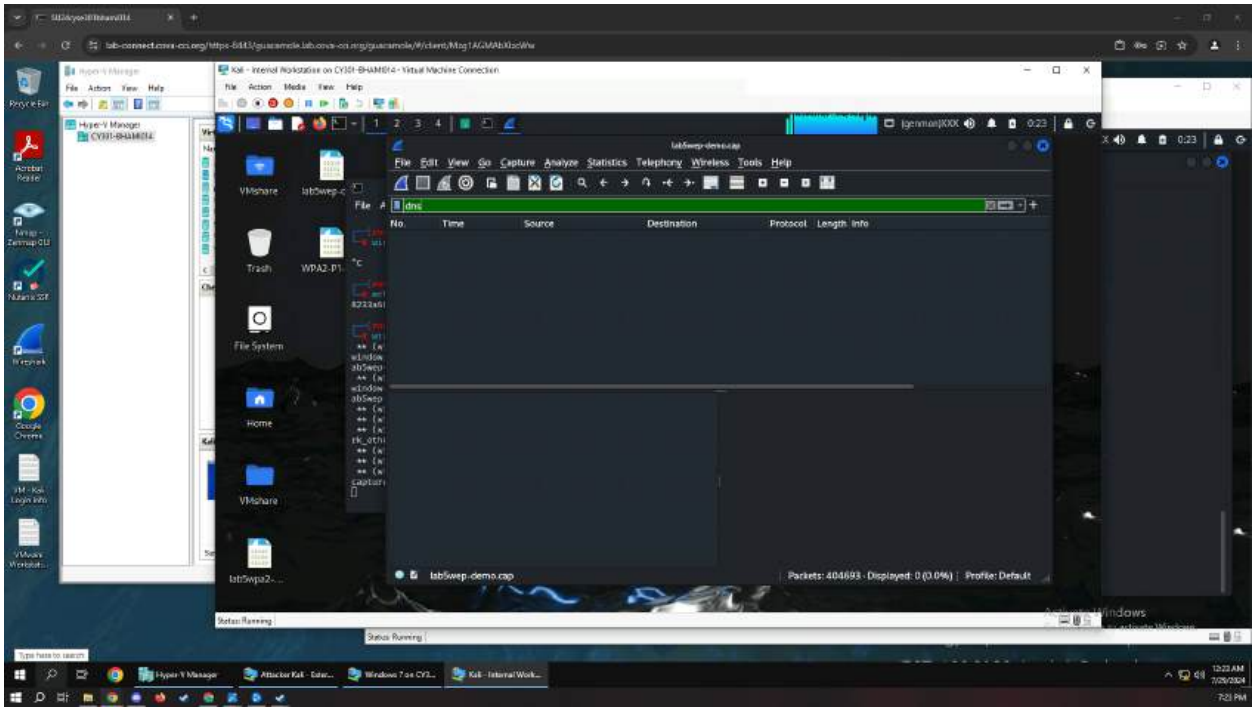

Figure 16 Screenshot of opened demo file and filtering DNS packets

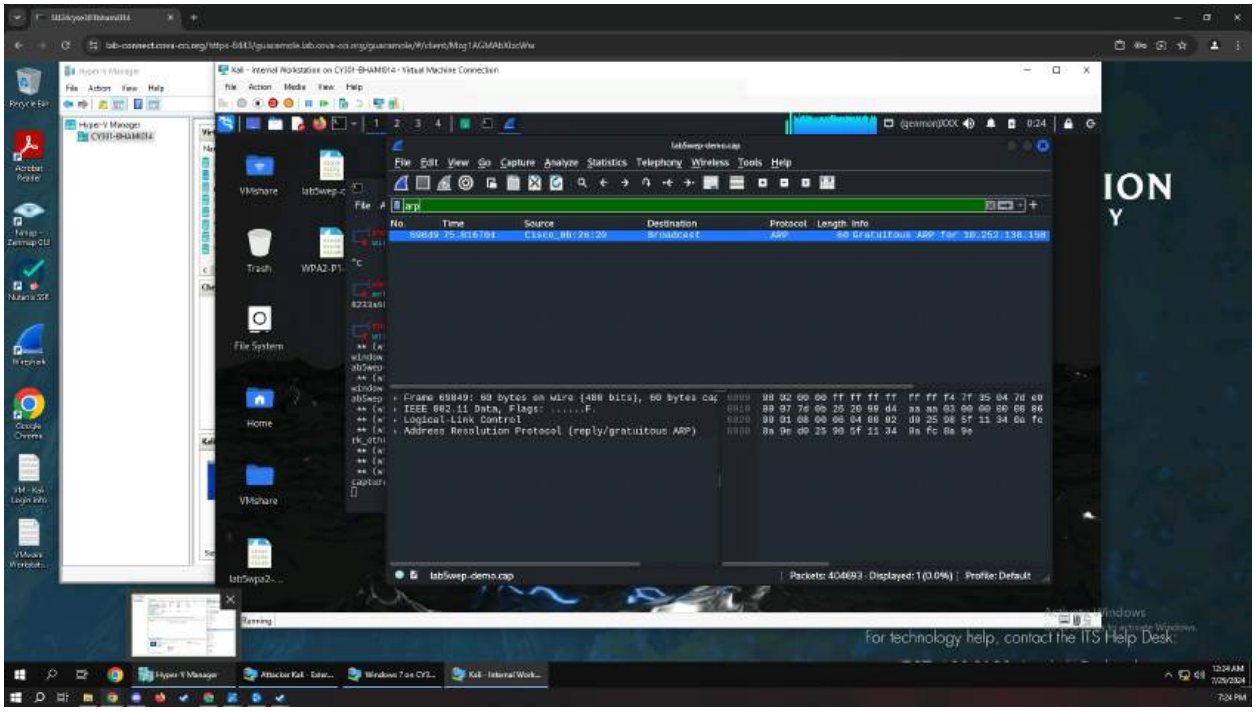

Figure 17 Screenshot of filtering arp packets

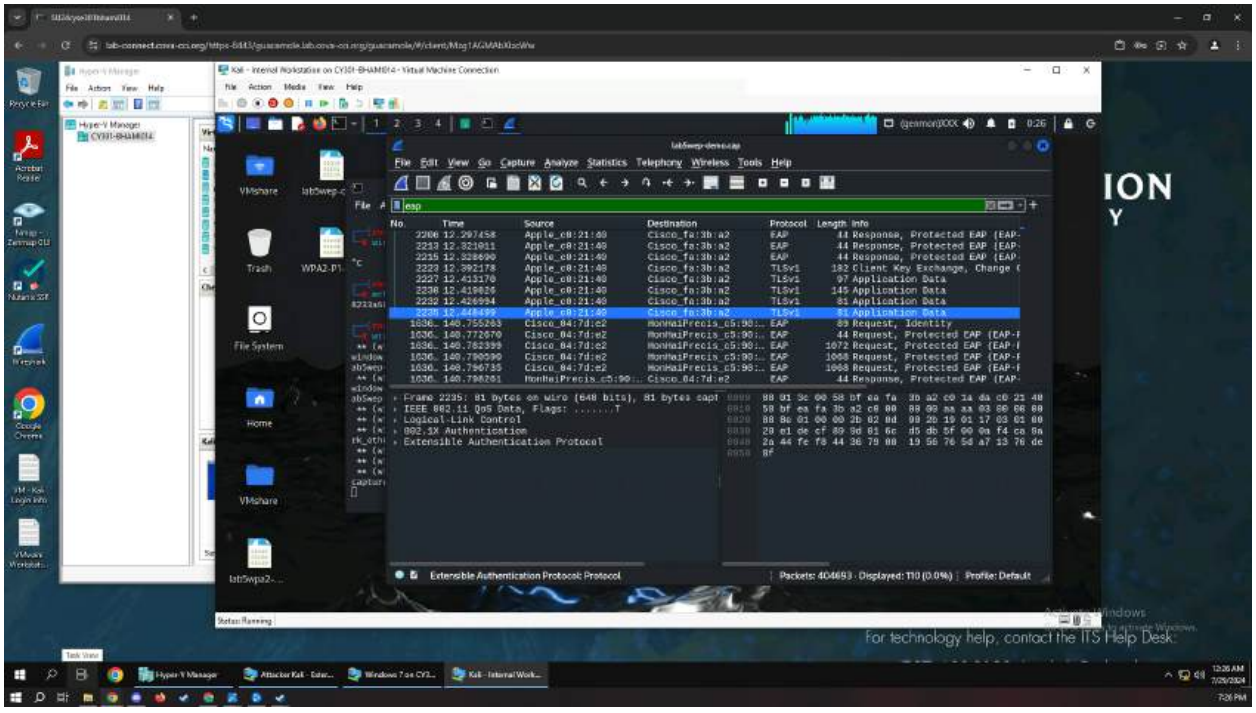

Figure 18 Screenshot of filtering eap packets

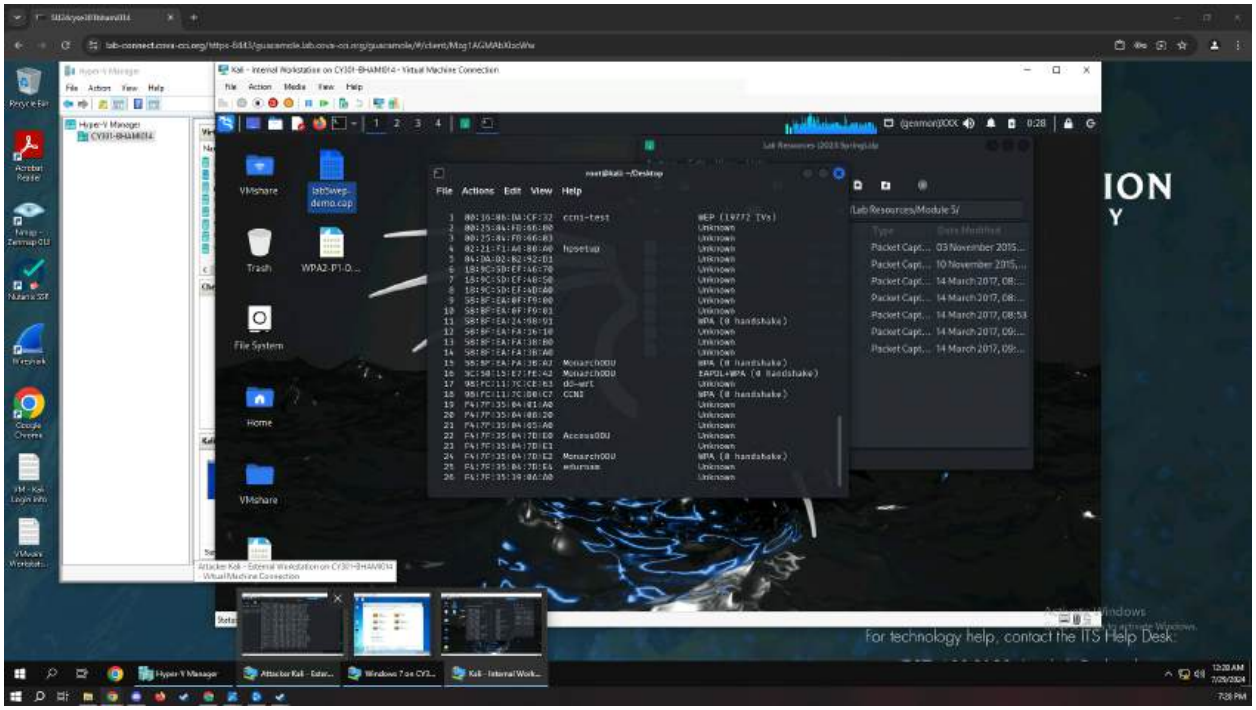

Figure 19 Screenshot of aircrack-ng command on WEP demo file

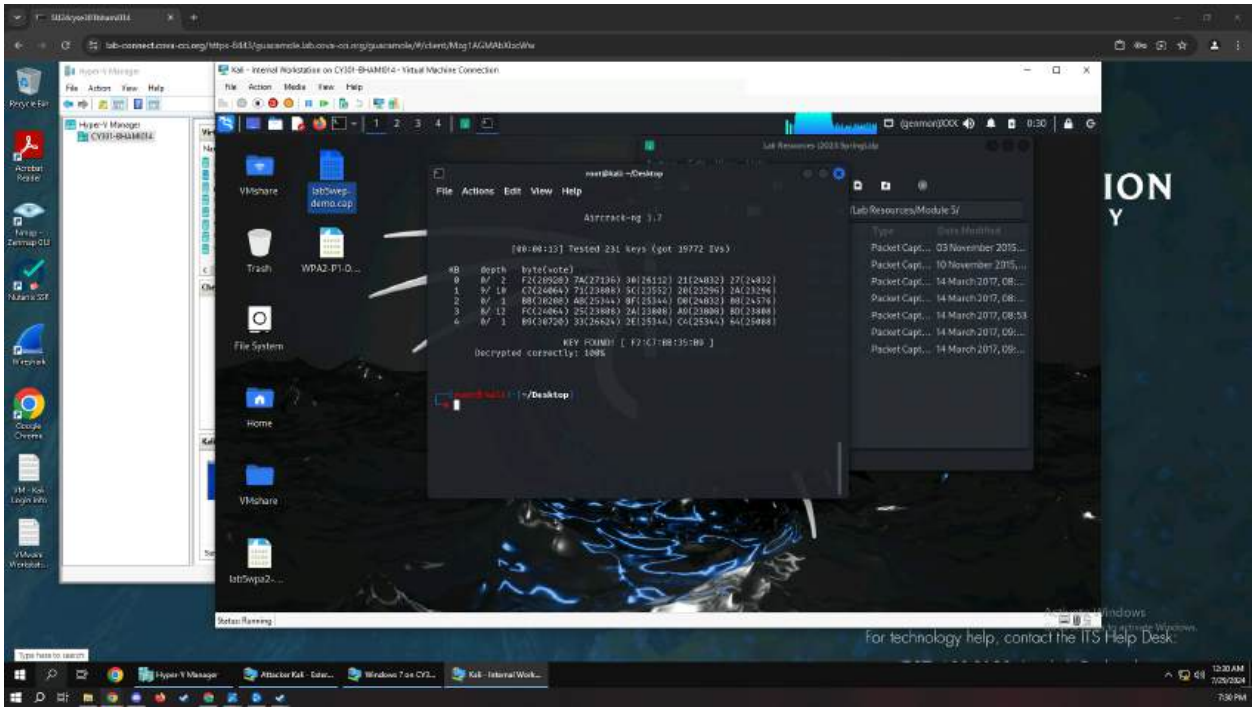

Figure 20 Screenshot of successfully finding key from aircrack

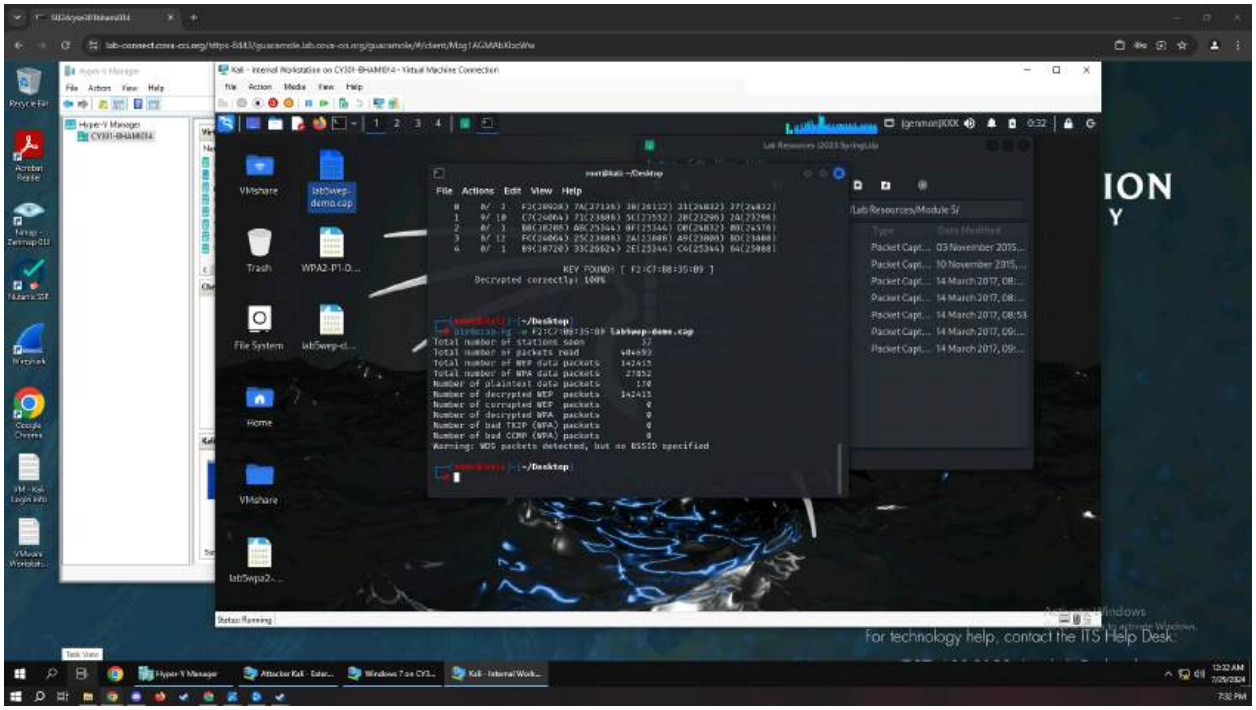

Figure 21 Screenshot of using the key to decrypt packets, all packets shown to be decrypted for WEP

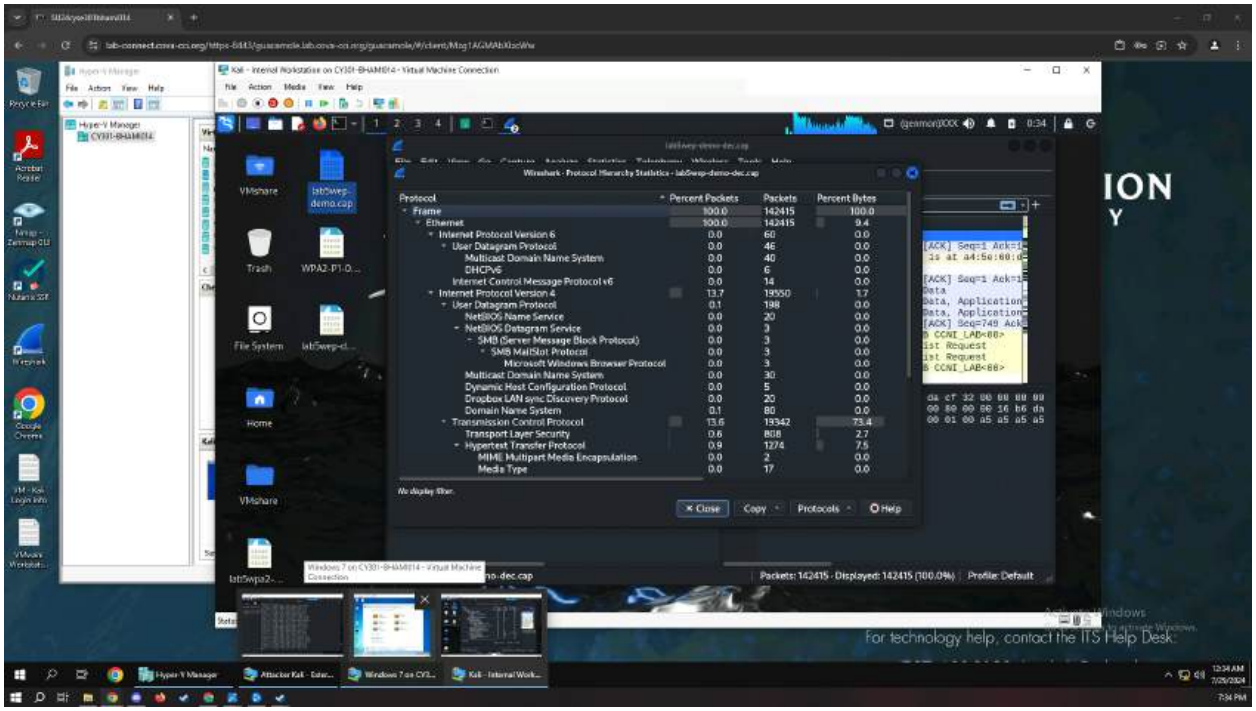

Figure 22 Screenshot of Protocol Hierarchy for after decrypting packets for WEP

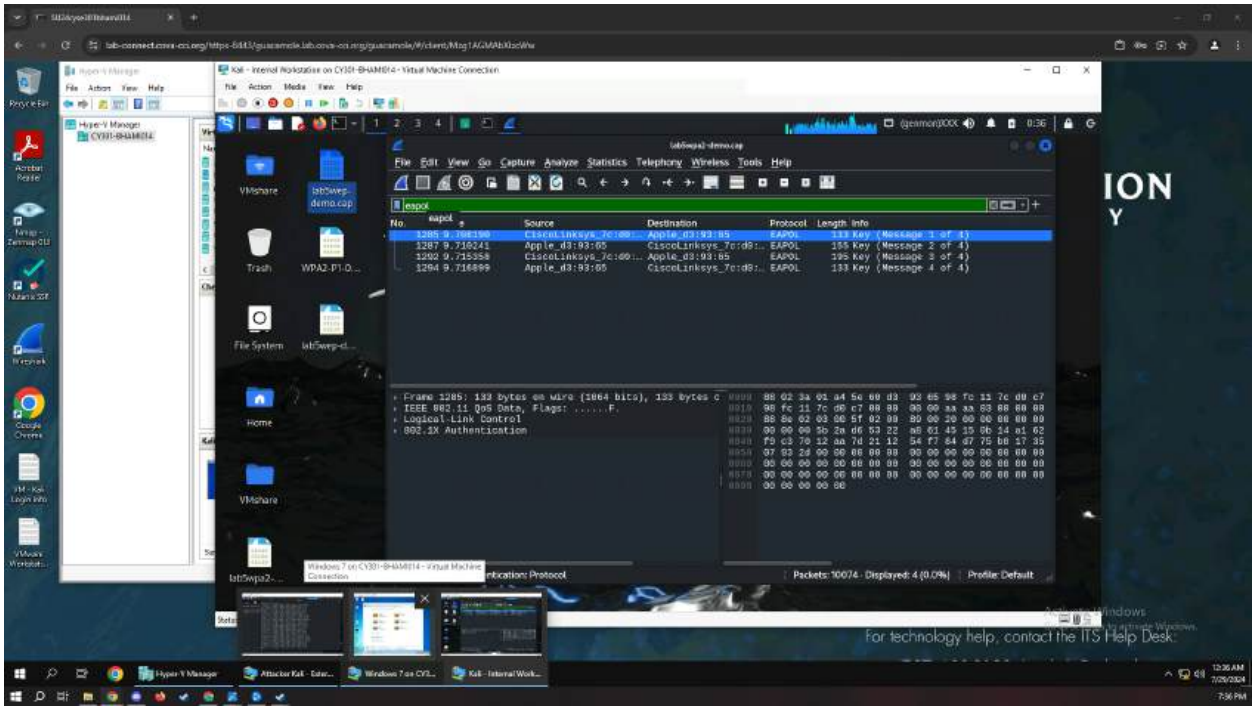

Figure 23 Screenshot of filtering eapol packets for WPA lab demo

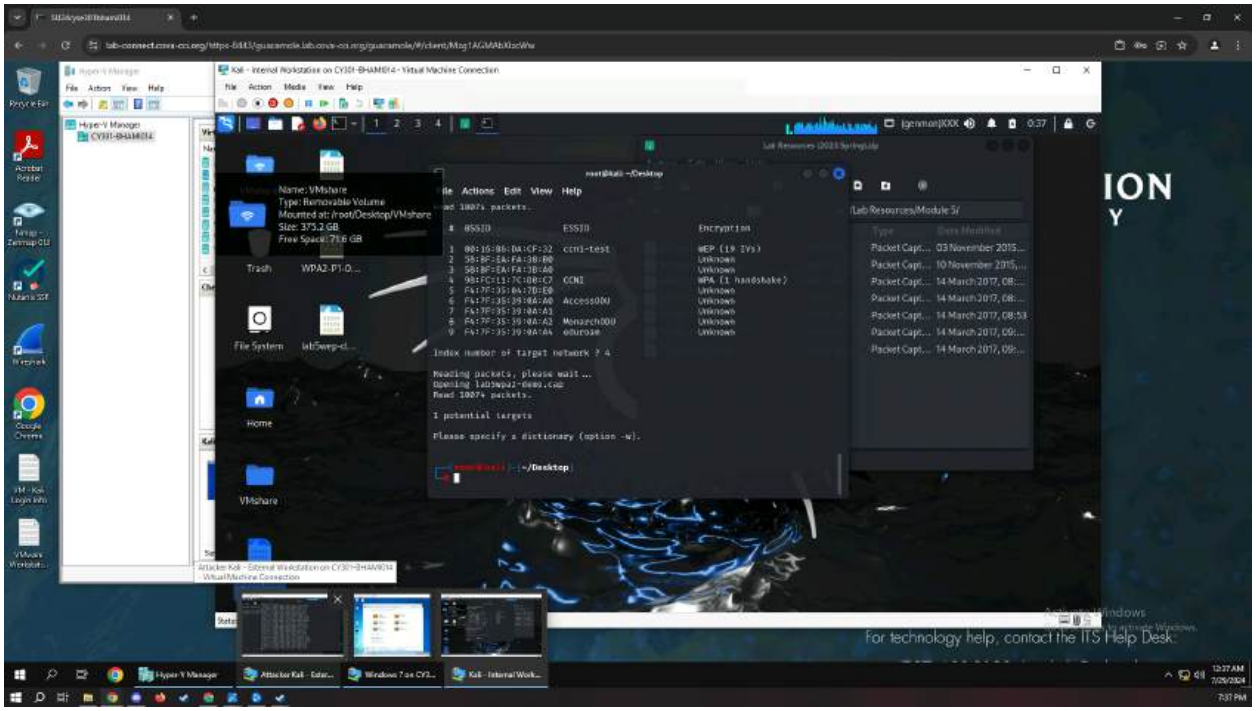

Figure 24 Screenshot of aircrack used on WPA lab demo

WPA aircrack-ng requests a dictionary to be used, which rockyou.txt was the main one used.

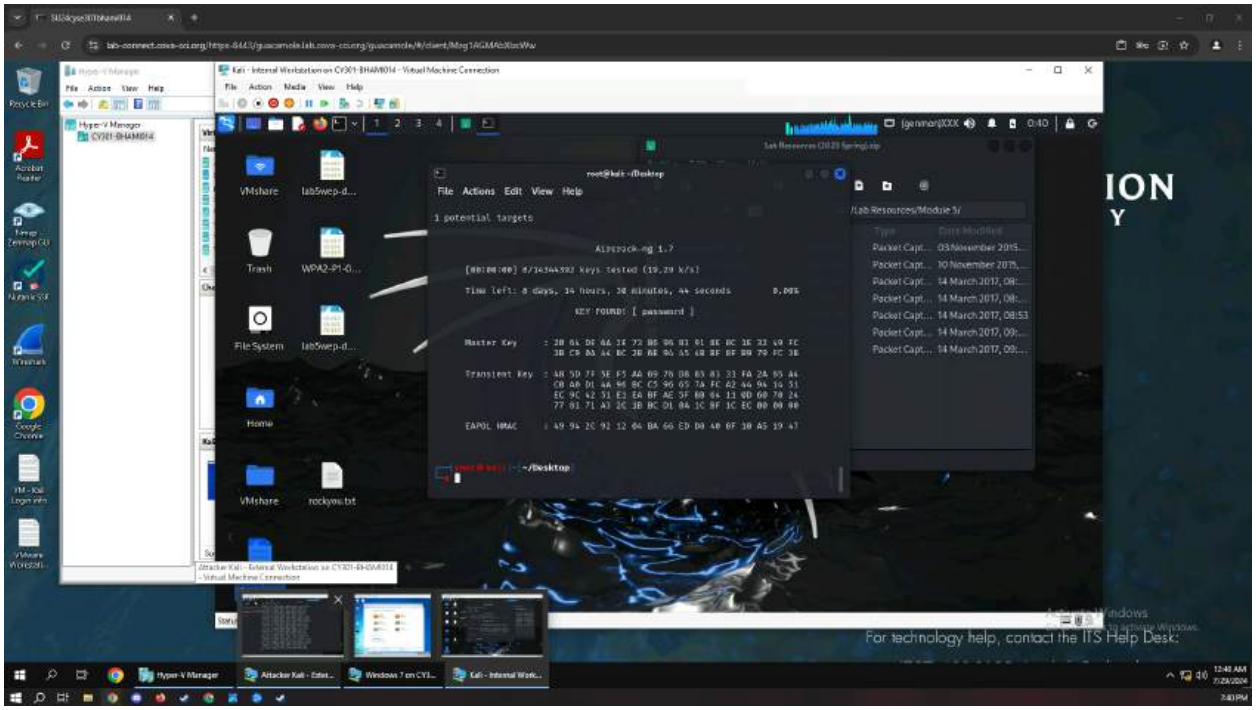

Figure 25 Screenshot of password being shown after cracking with dictionary attack

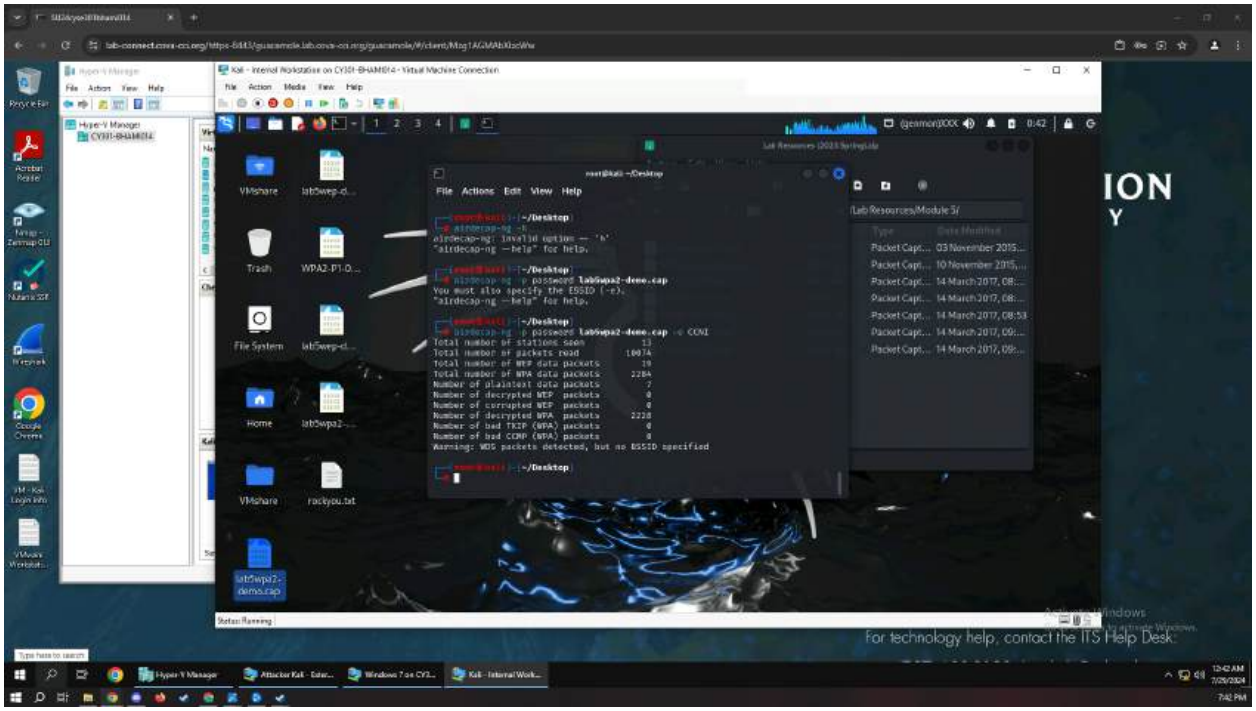

Figure 26 Screenshot of inputting password and ESSID in order to decrypt packets

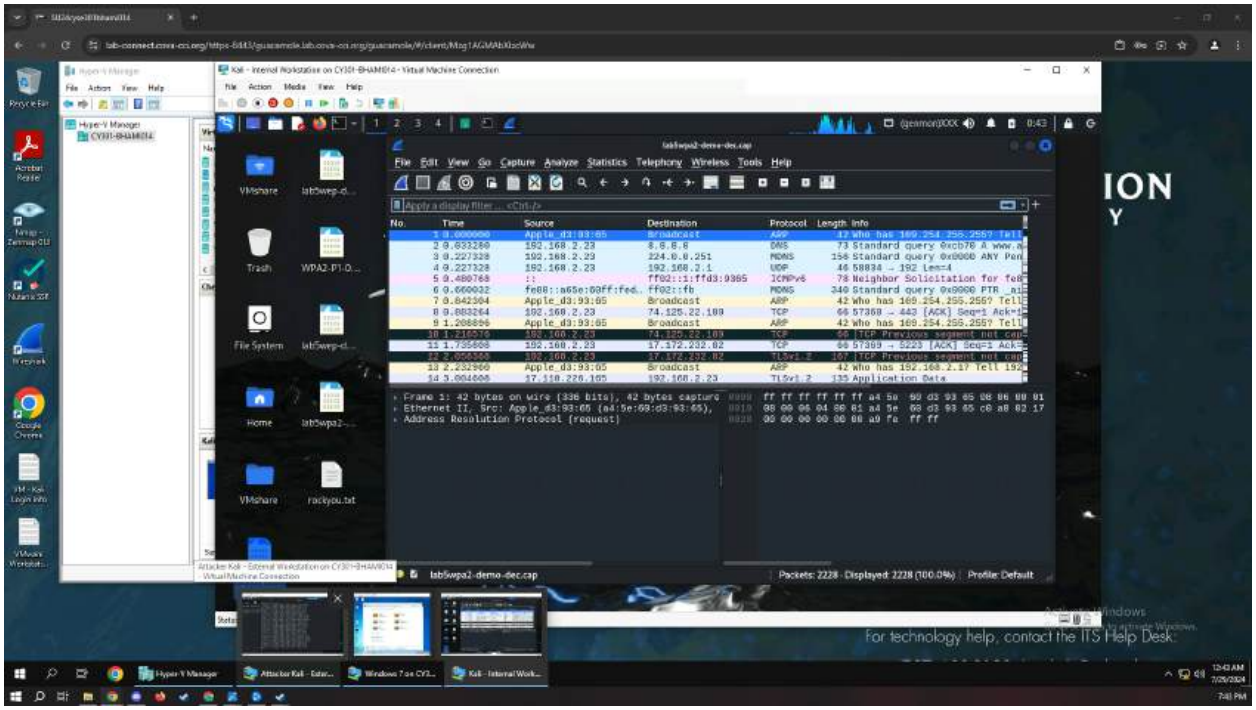

Figure 27 Screenshot of packets after decrypting

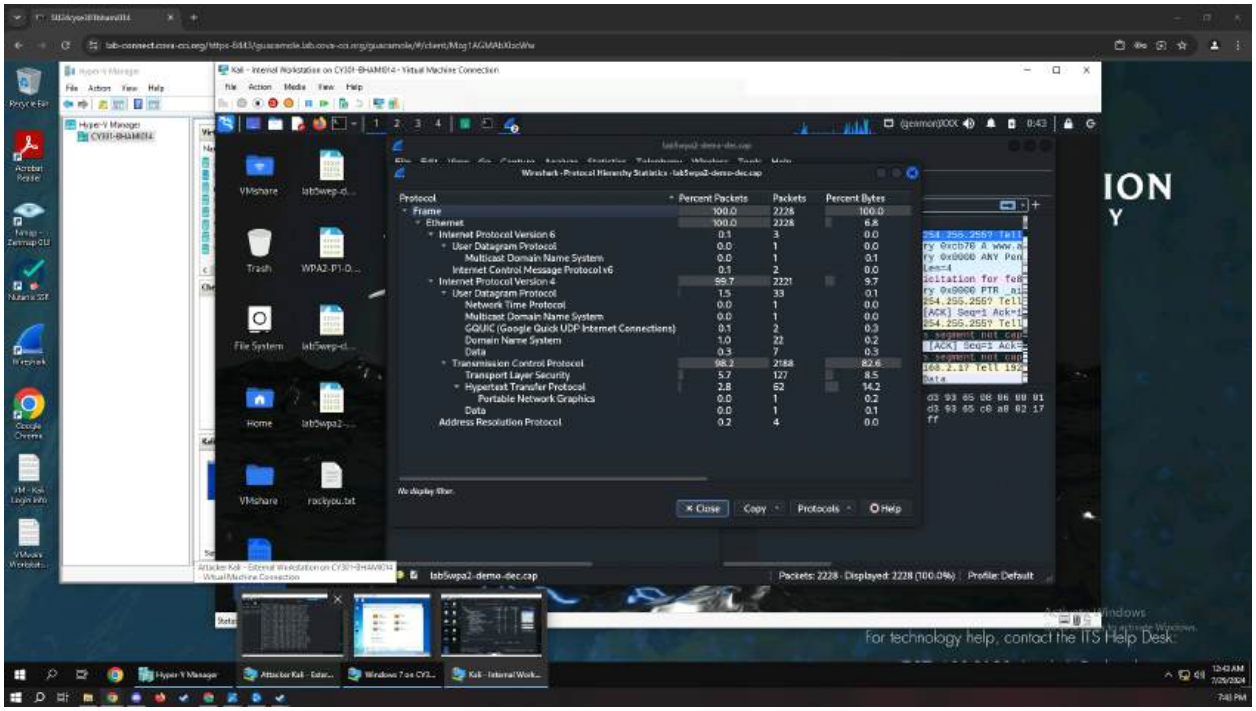

Figure 28 Screenshot of Protocol Hierarchy after decrypting packets

TASK C

3. Decrypting WPA2-P1-01.cap

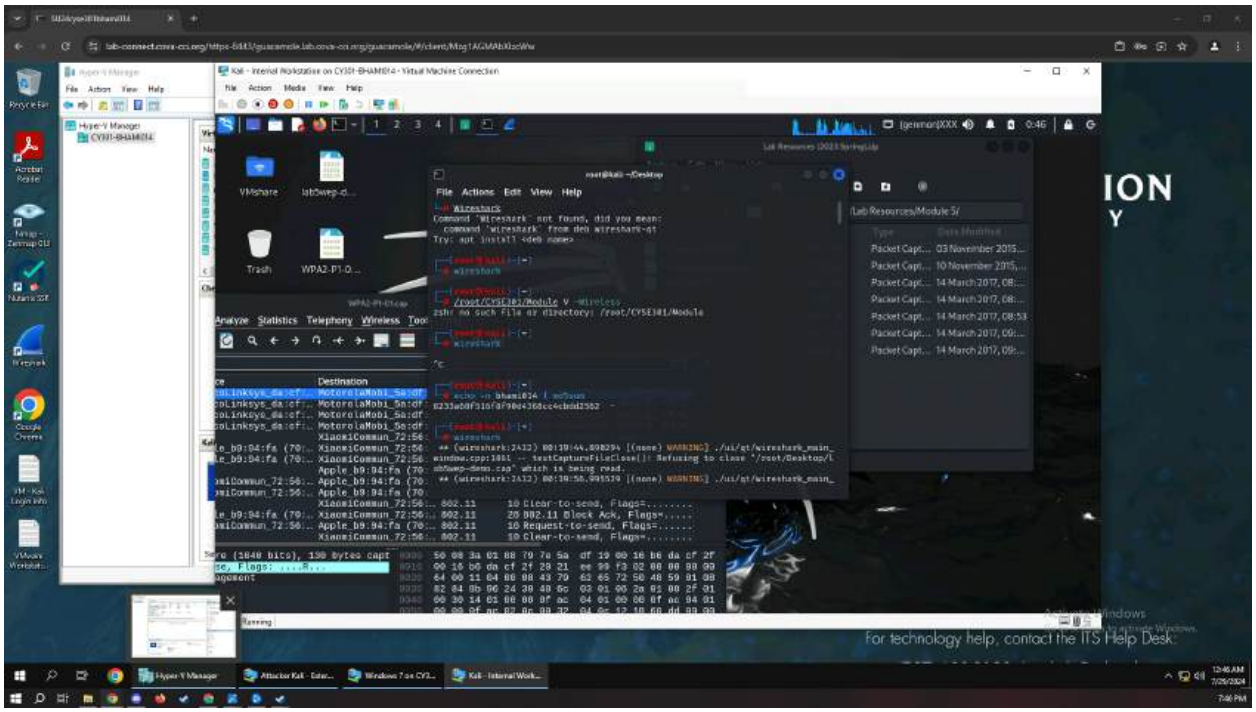

Figure 29 Screenshot with MD5SUM ending in 2 -> referencing WPA2-P1-01.cap file to decrypt

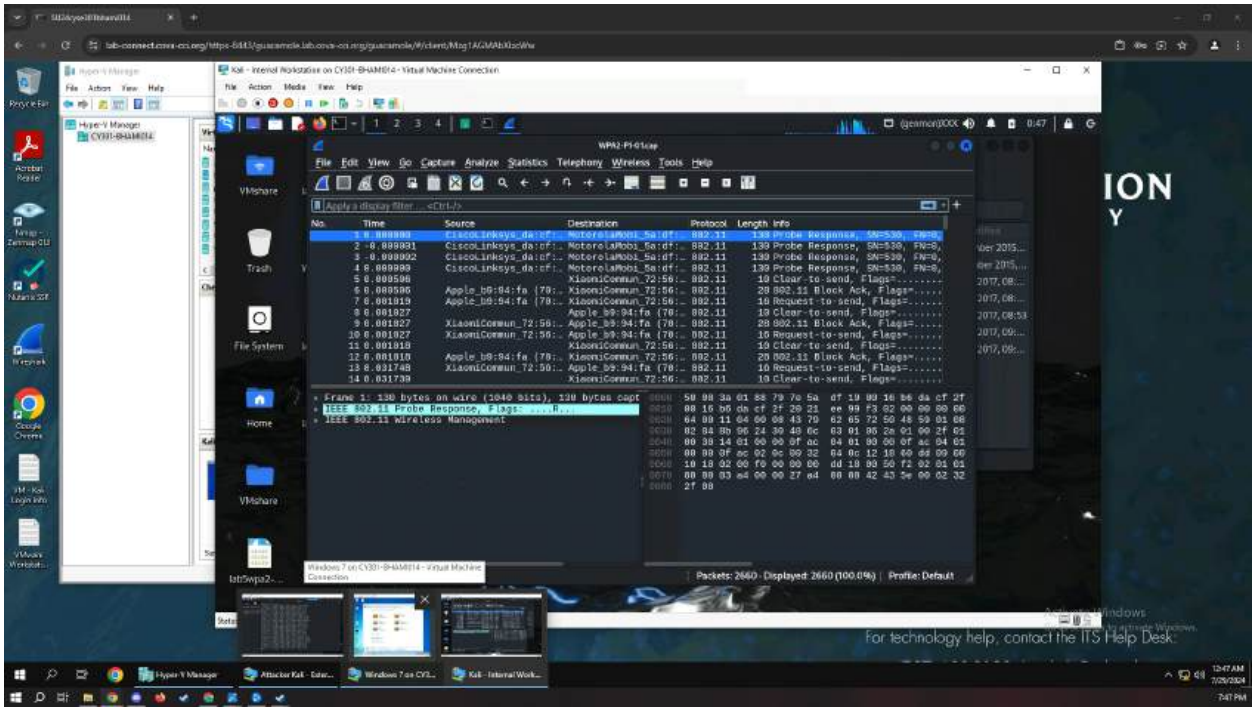

Figure 30 Screenshot with Wireshark referencing WPA2-P1-01.cap file to decrypt

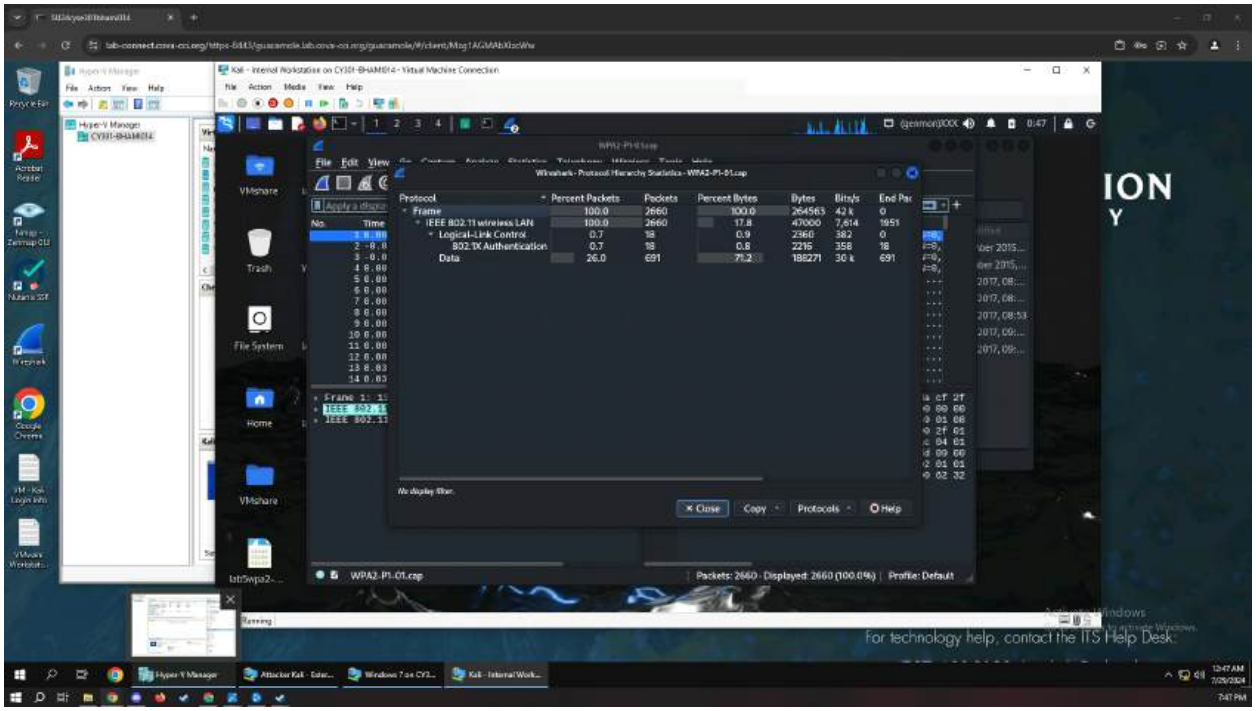

Figure 32 Screenshot with WPA2-P1-01.cap Protocol Hierarchy

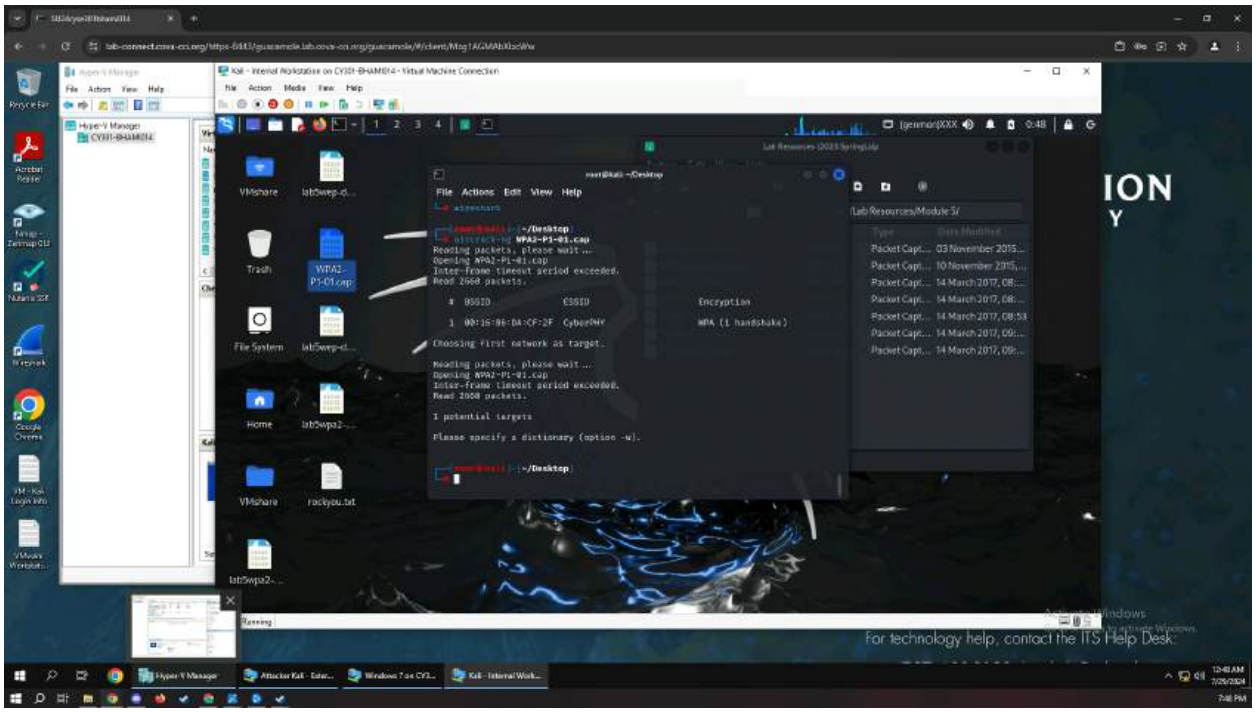

Figure 33 Screenshot with aircrack-ng on WPA2-P1-01.cap which needs a dictionary attack

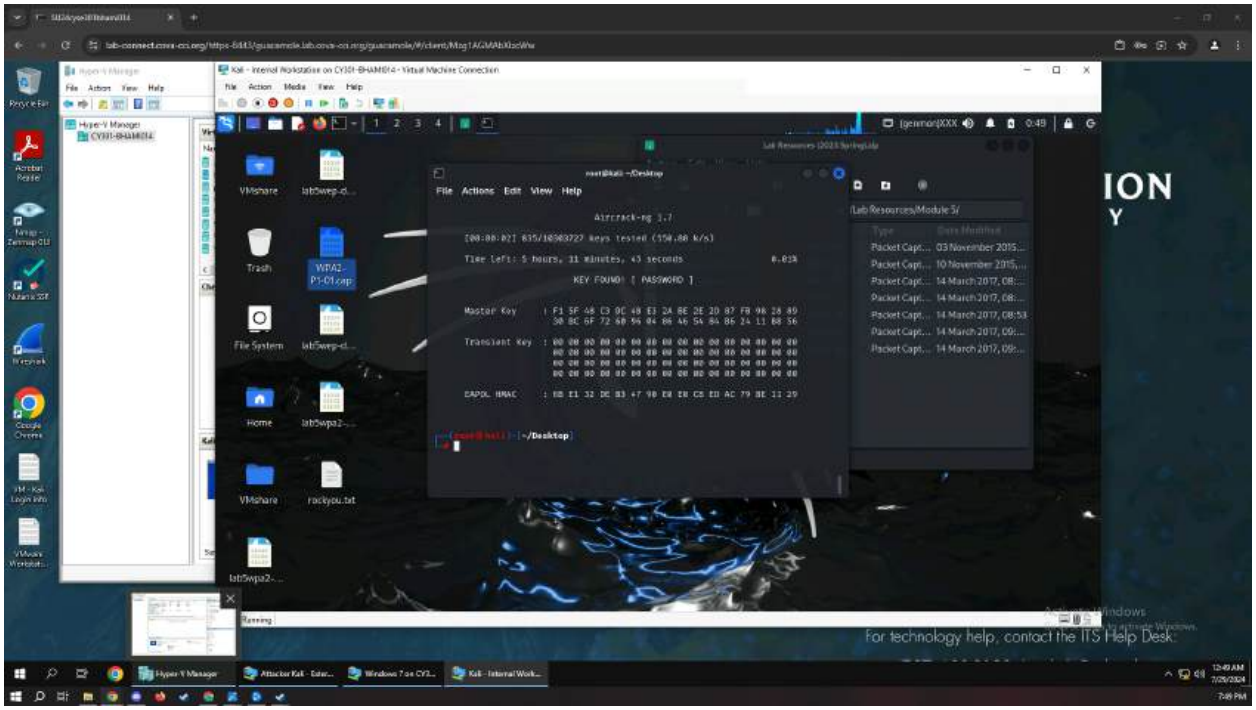

Figure 34 Screenshot shows dictionary attack with PASSWORD being the password

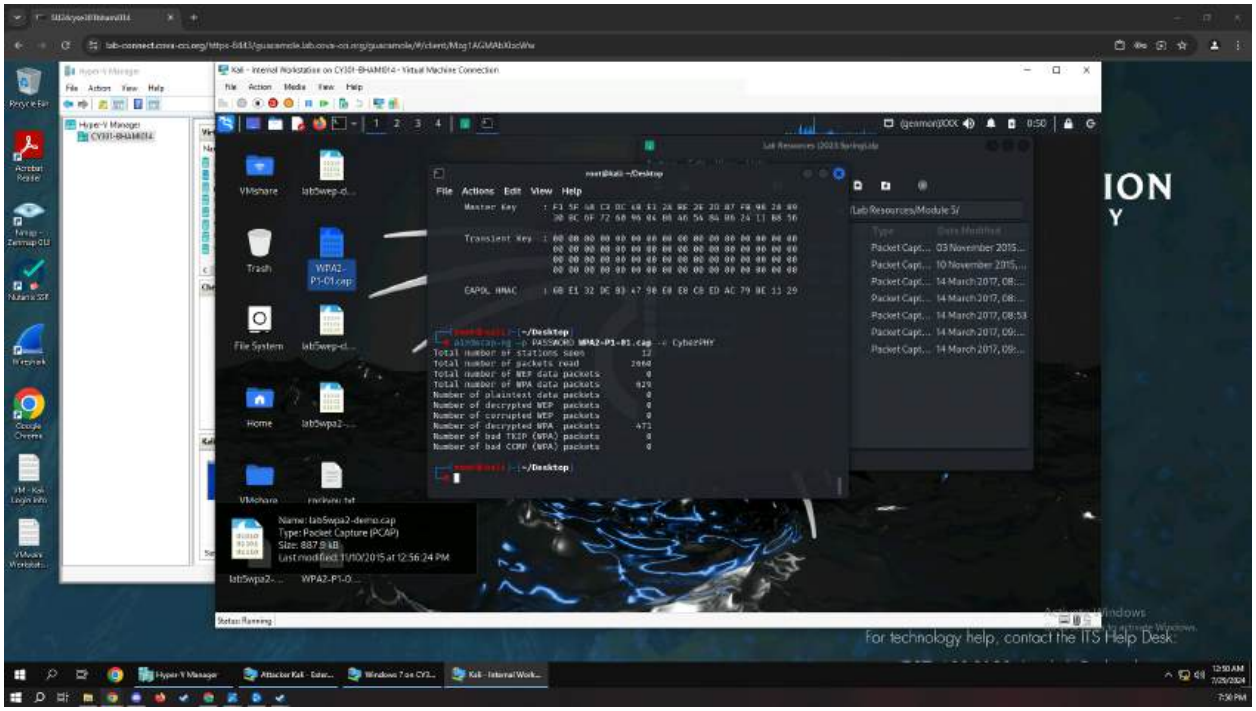

Figure 35 Screenshot shows implementation of the password and CyberPHY to decrypt packets

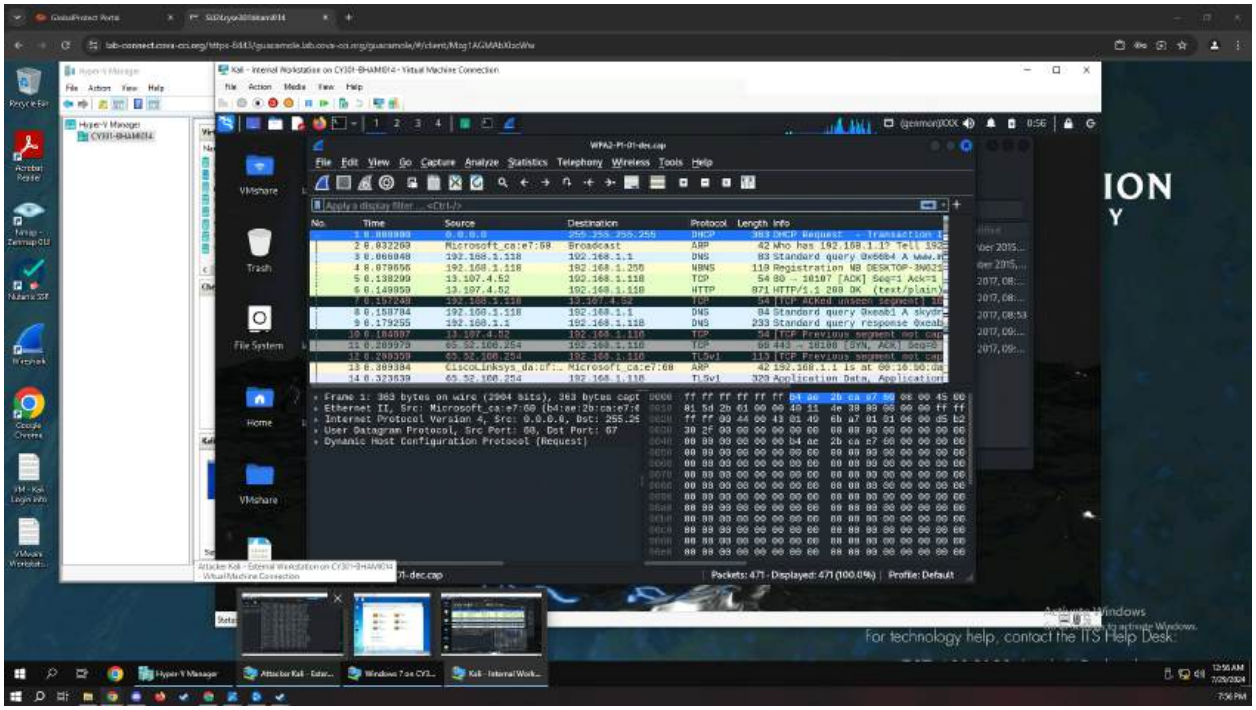

Figure 36 Screenshot shows Wireshark packets after decryption

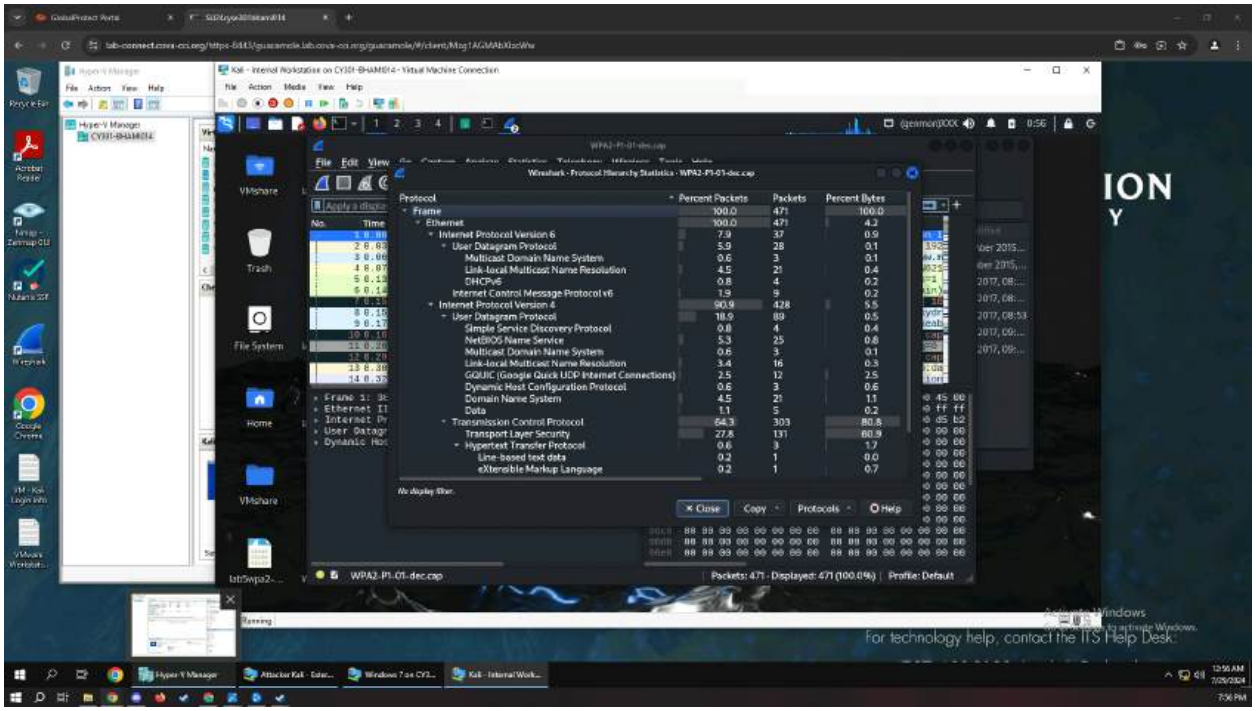

Figure 37 Screenshot shows Wireshark Protocol Hierarchy after decryption

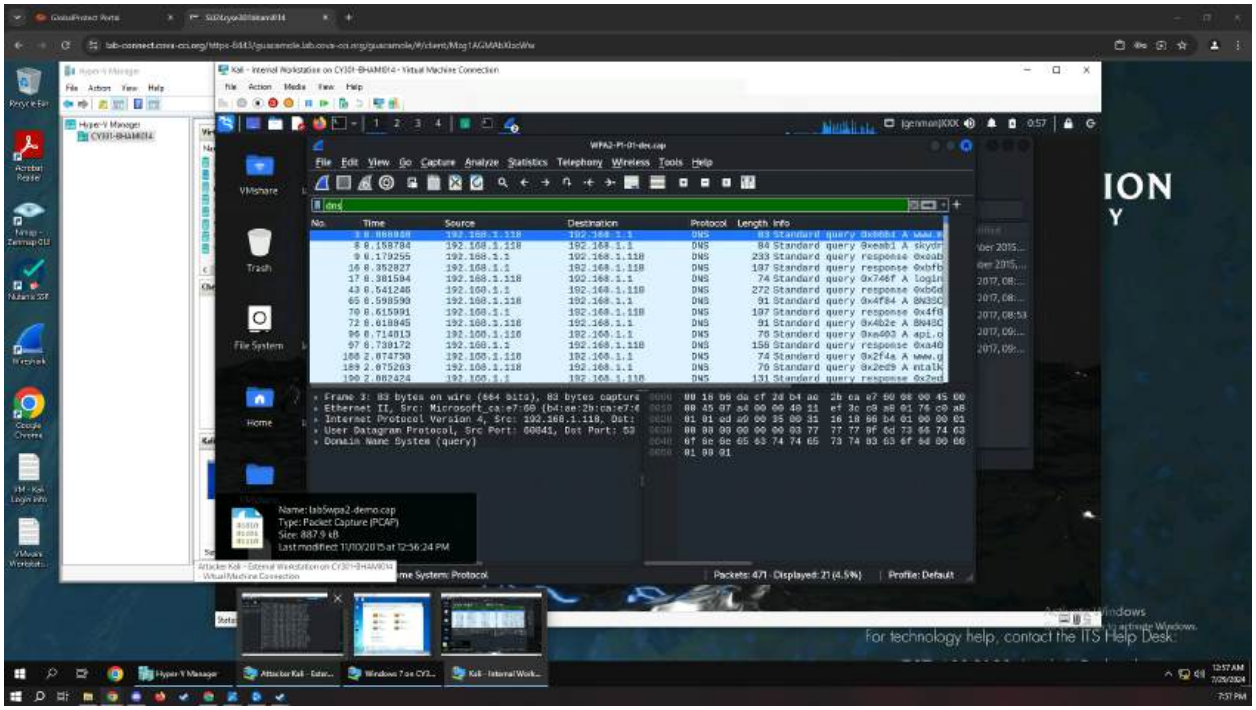

Figure 38 Screenshot shows Wireshark DNS filter after decryption

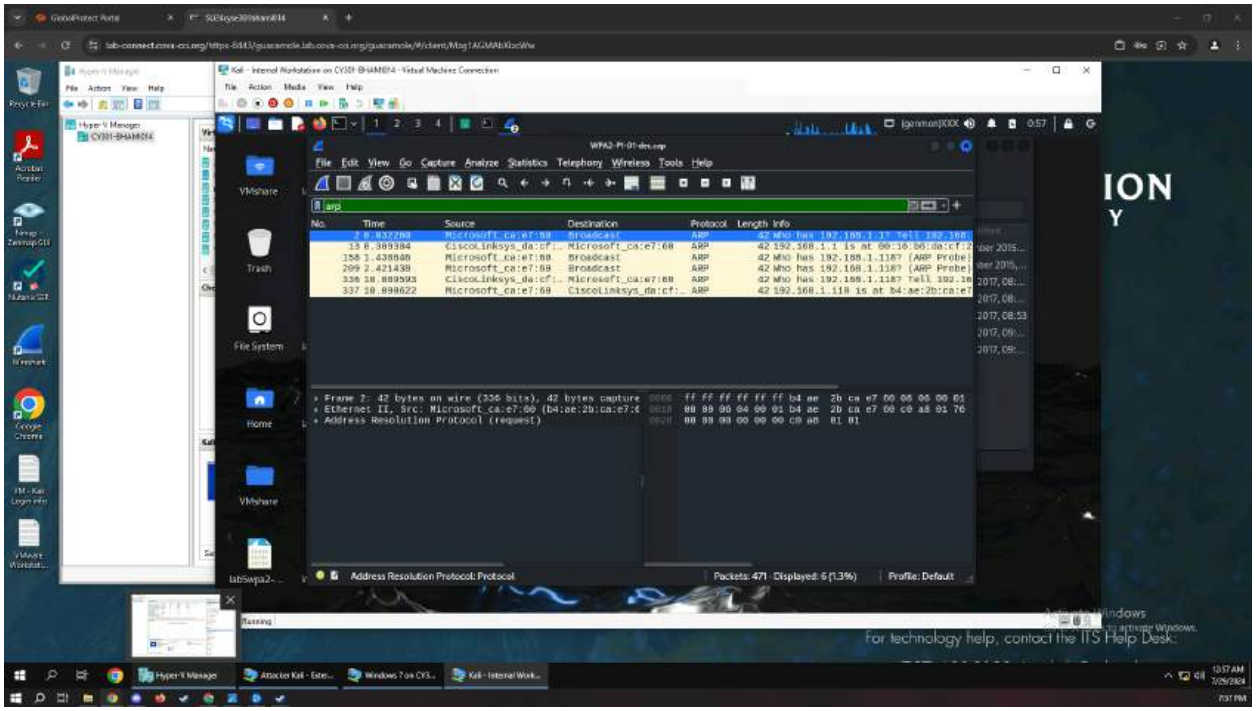

Figure 39 Screenshot shows Wireshark ARP filter after decryption

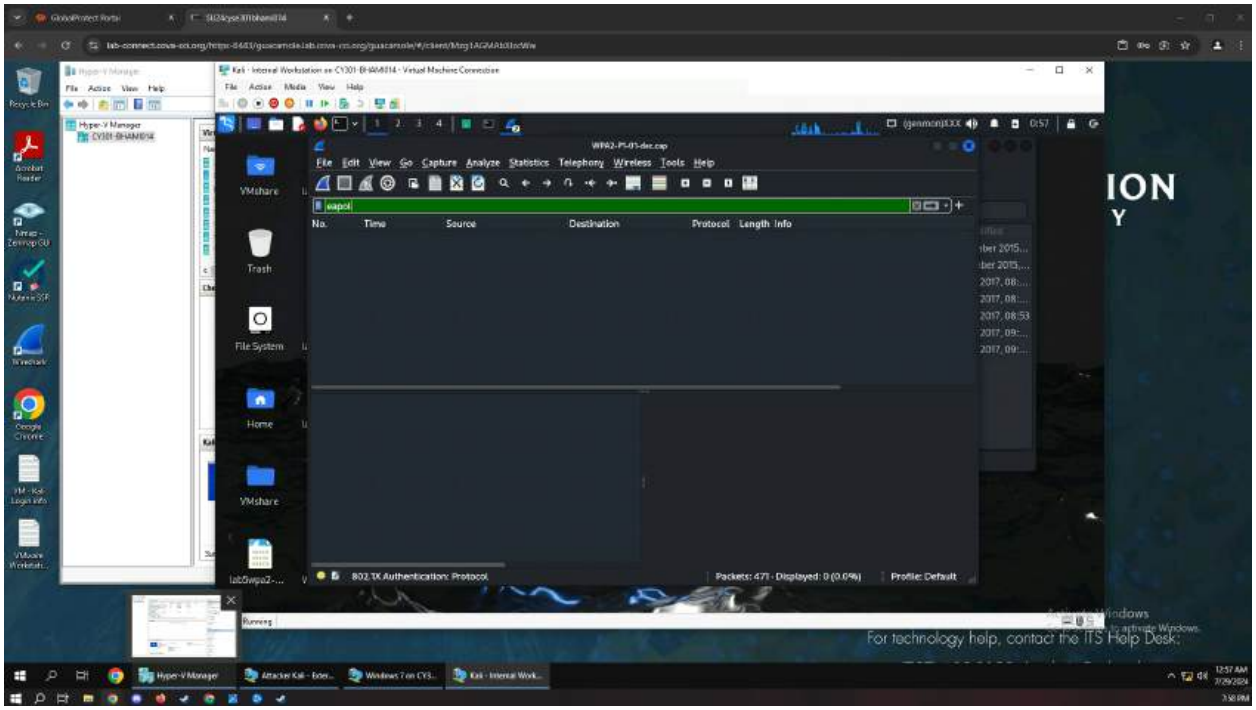

Figure 40 Screenshot shows Wireshark EAPOL filter after decryption

Decrypting the traffic was quite tedious, but after getting a grasp of the commands and utilizing it correctly, decrypting the traffic proved simple. When breaking the WPA/WPA2 down it seems as though they will require dictionary attacks in order to decrypt the packets in order to view what is within them. The screenshots provided shows the process step-by-step and provides a brief view into what the packets look like when encrypted and how they change after encryption. The best possible breakdown is looking at the protocol hierarchy and how more subcategories open, detailing what specifically is being sent across the network.

WPA/WPA2 shows that it has a stronger security and encryption of the packets and requires a little bit more work in order to figure out how to decrypt the packets in order to obtain information that is wanted. Furthermore, not all packets decrypt as only roughly 400 packets were during this process, so it would be safe to say that more protocols would need to be taken in order to access all of the data that is within the file.

This lab has been a great source of information regarding packet transmissions and how they are securely sent over the internet, but it also shows how they can be dissected in order to find information that is wanted. With the appropriate tools, much of the information can be found when cracking passwords or even figuring out wifi passwords that could be exploited by criminals and hackers.