OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignments #4 & #5 Password Cracking

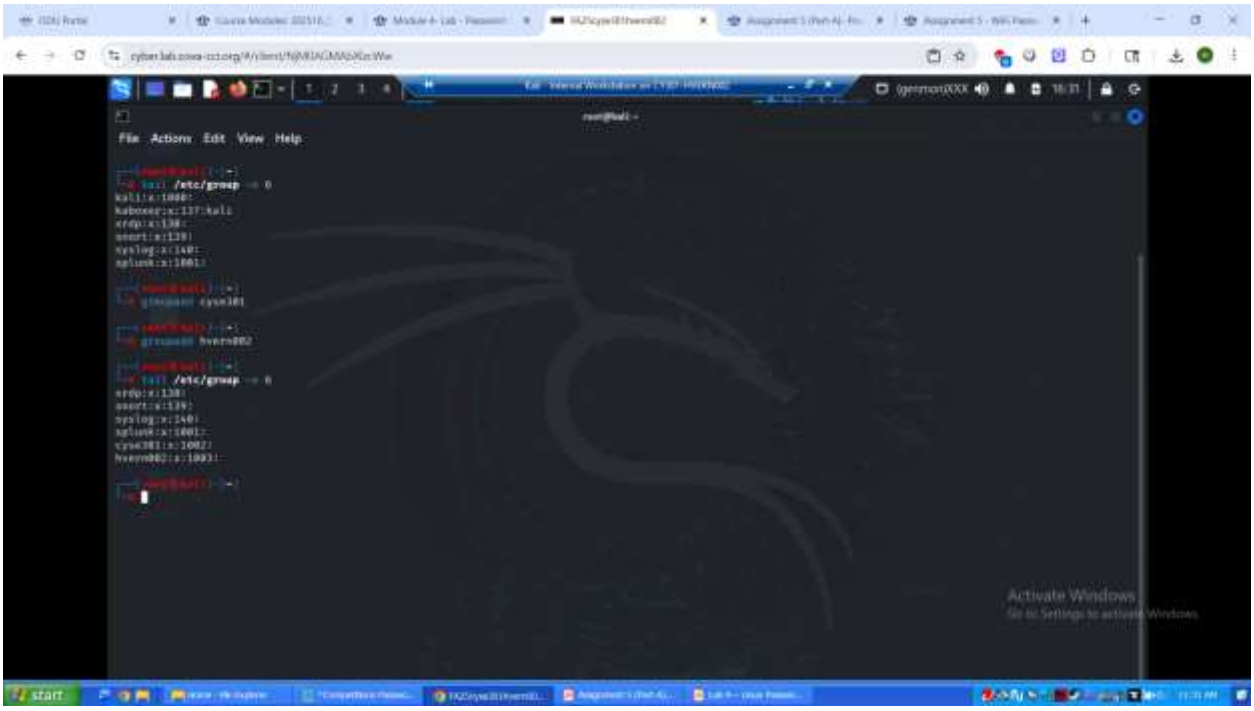
Harold Vernon

01265958

Below is the snippet of a sample lab report.

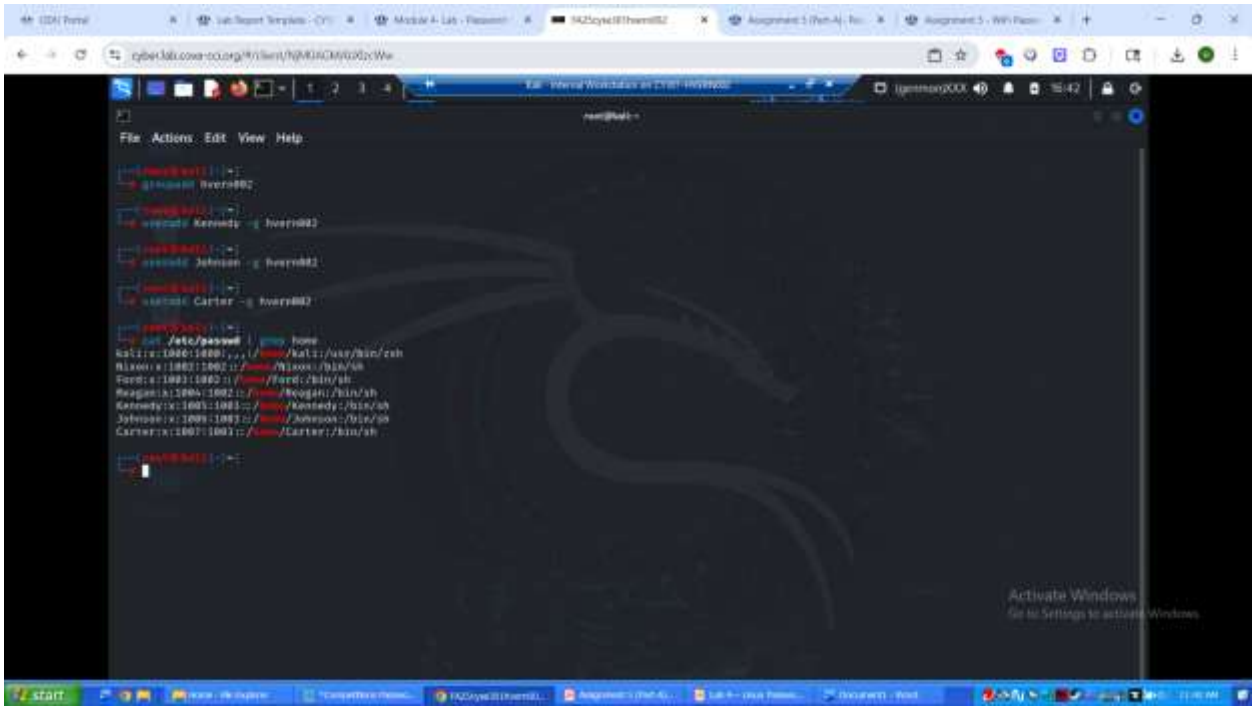
TASK A

1. Create two groups, one is **cyse301**, and the other is your ODU Midas ID (for example, svatsa). Then display the corresponding group IDs.



Explanation:
Above are the groups for the Internal Kali VM. “cyse301” and “hvern002” are visible as requested.

2. Create and assign three users to each group. Display related UID and GID information of each user.



Explanation:

Above, the added users can be seen. “cyse301” contains the users Nixon, Ford, and Reagan while “hvern002” contains the users Kennedy, Johnson, and Carter.

3. Choose Three new passwords, **from easy to hard**, and assign them to the users you created. You need to show me the password you selected in your report, and **DO NOT** use your real-world passwords.

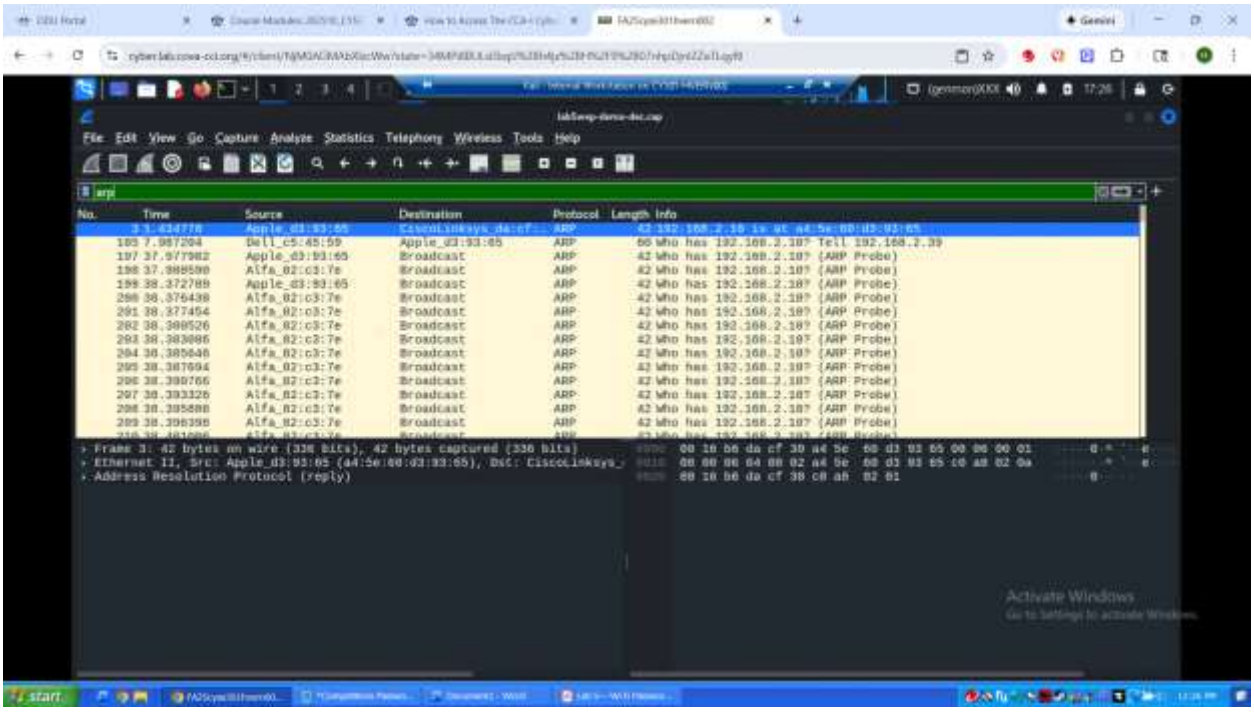
Explanation:

Above, the tail command has been run on the shadow file. The shadows of the six users' passwords can be seen. Their actual passwords are red (Nixon), Red38 (Ford), ?81R3D3L3PH4N7589RR! (Reagan), blue (Kennedy), Blue36 (Johnson), and ?71BLU3D0NK3Y575JC! (Carter.)

4. Export all Three users' password hashes into a file named "**YourMIDAS-HASH**" (for example, svatsa-HASH). Then launch a dictionary attack to crack the passwords. You MUST crack at least one password in order to complete this assignment.

Explanation:
Above are the results of the dictionary attack. In a realistic attack, the passwords red, blue, Red38, and Blue36 would not be secure. If an attacker is using John with the wrong hash, they could just as easily guess red or blue to access Nixon or Kennedy's account respectively.

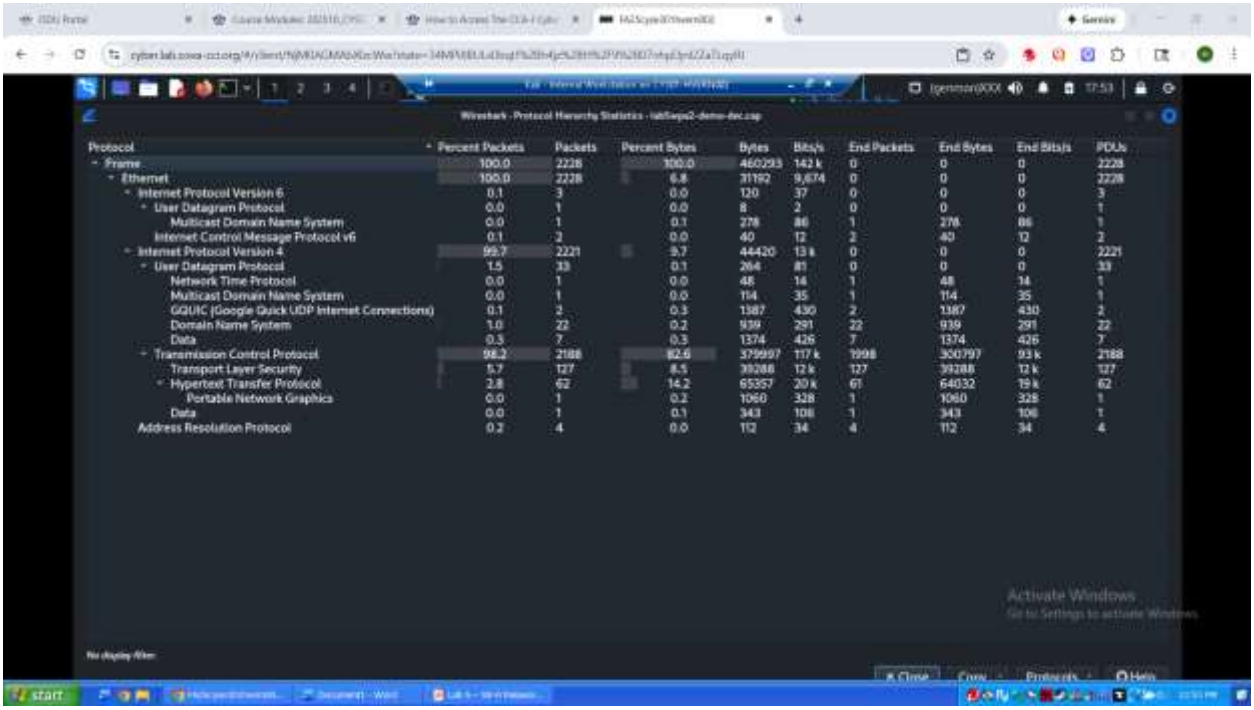
5. Decrypt the lab5wep-demo. cap file and perform a detailed traffic analysis.



Explanation:

Above is the ARP traffic from the packet. It was previously hidden when the packet was encrypted. But now that it has been decrypted with the aircrack tool, the ARP traffic is visible for analysis.

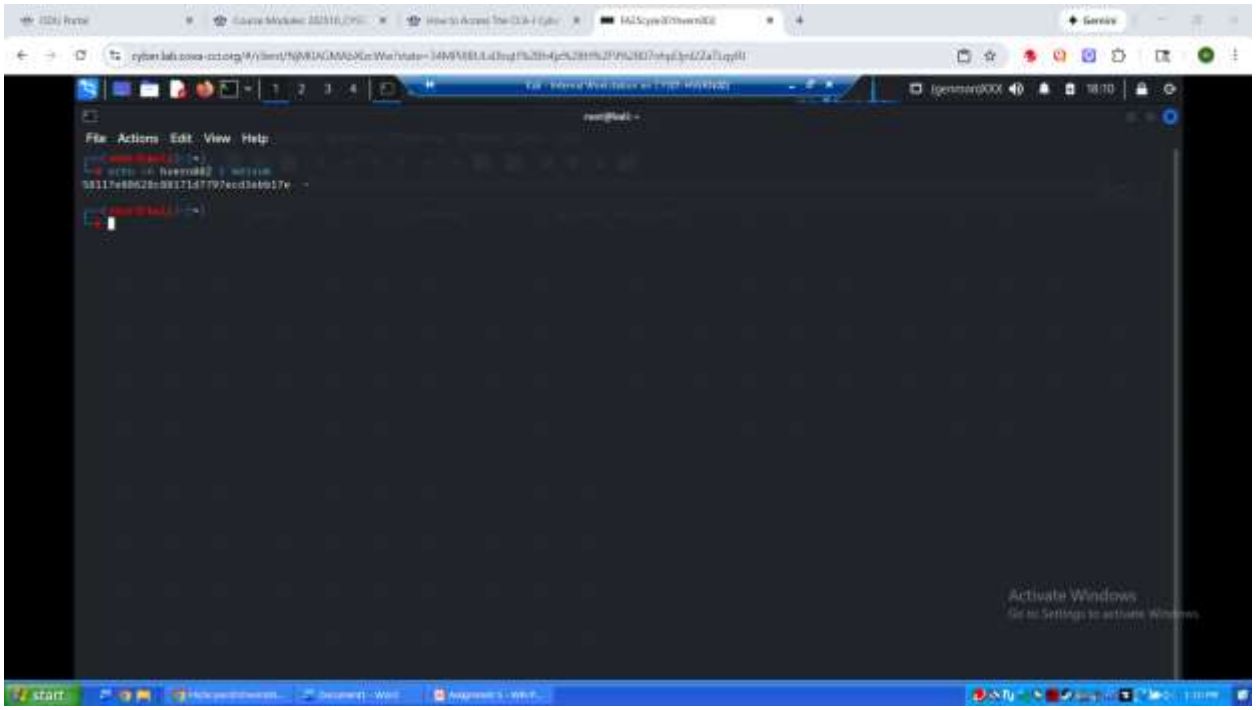
6. Decrypt the lab5wpa2-demo. cap file and perform a detailed traffic analysis.



Explanation:

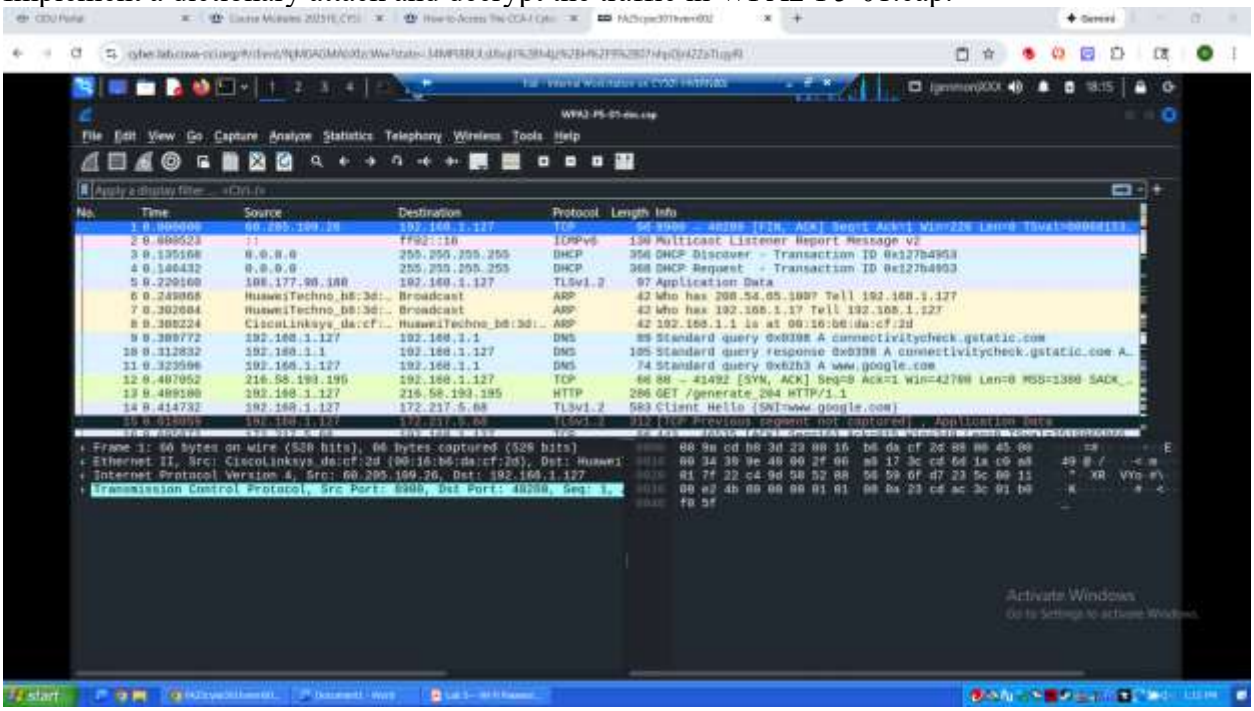
Above is the protocol hierarchy of the given packet. Due to the decryption carried out using the aircrack tool and rockyou wordlist for a dictionary attack, nearly all packets and their protocols are visible.

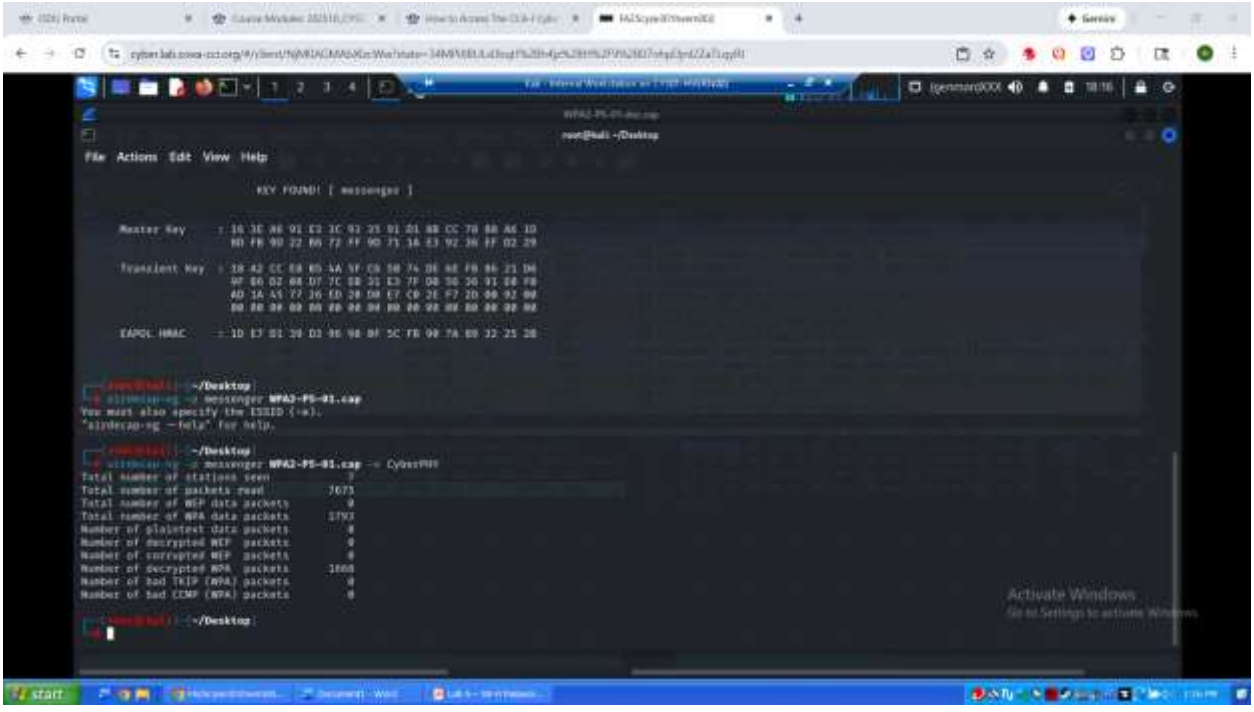
7. Each student will be assigned a new WPA2 traffic file for analysis. You need to refer to the table below and find the file assigned to you based on the LAST digit of the MD5 of your MIDAS ID.



Explanation:
Since the last character of my MD5 is the letter E, I will be working with WPA2-P5-01.cap.

8. Implement a dictionary attack and decrypt the traffic in WPA2-P5-01.cap.

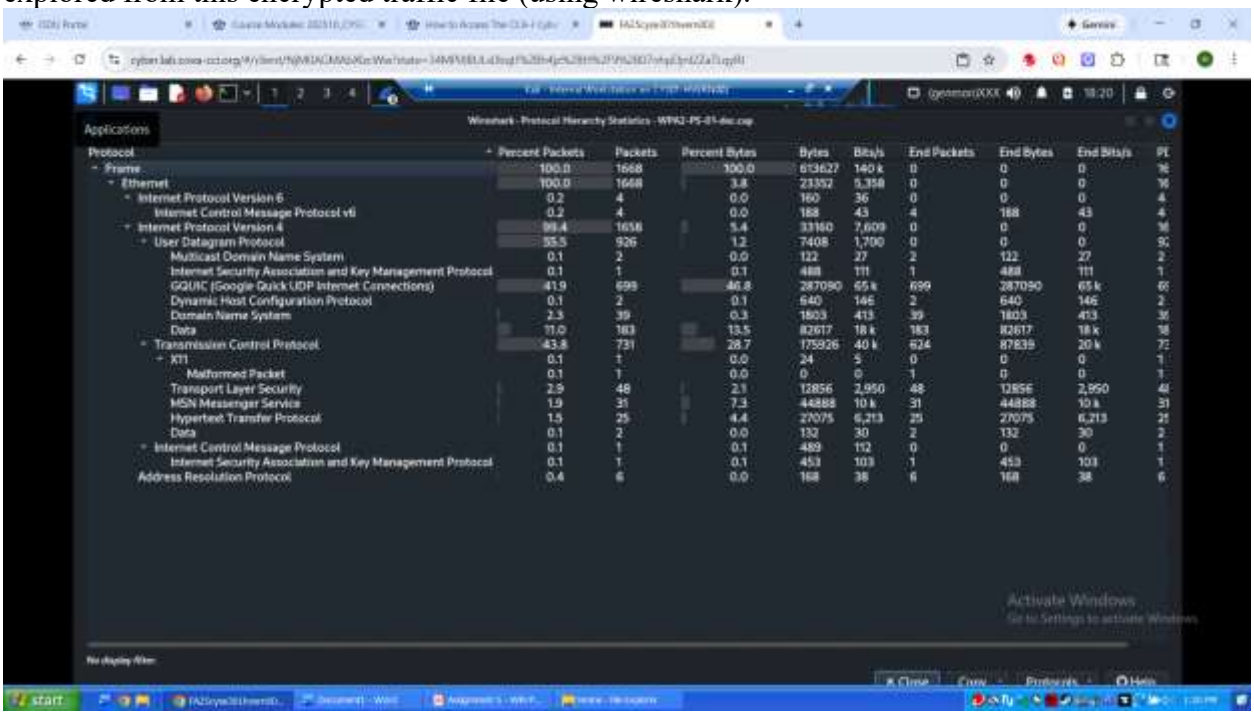




Explanation:

Above is the decrypted traffic of the given file and the command used to decrypt them after the successful dictionary attack.

9. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file (using wireshark).



Explanation: Above is the traffic file's protocol hierarchy. A simple dictionary attack removed all security that existed around the packets on the file. This could be dangerous as it means that threat actors can easily access the information being sent over a network. It is best to use an encrypted key to prevent dictionary attacks. When encrypting the key, however, it is important to avoid using insecure algorithms such as WEP because those too can be cracked with aircrack and similar tools.