Name : Vishvesh Shatalwar
Mis : 112115146

ISS Assignment #2 - Password Cracking Tools

1. SubLab-1: Cracking MD5 Password Hashes using Hashcat/John the Ripper:

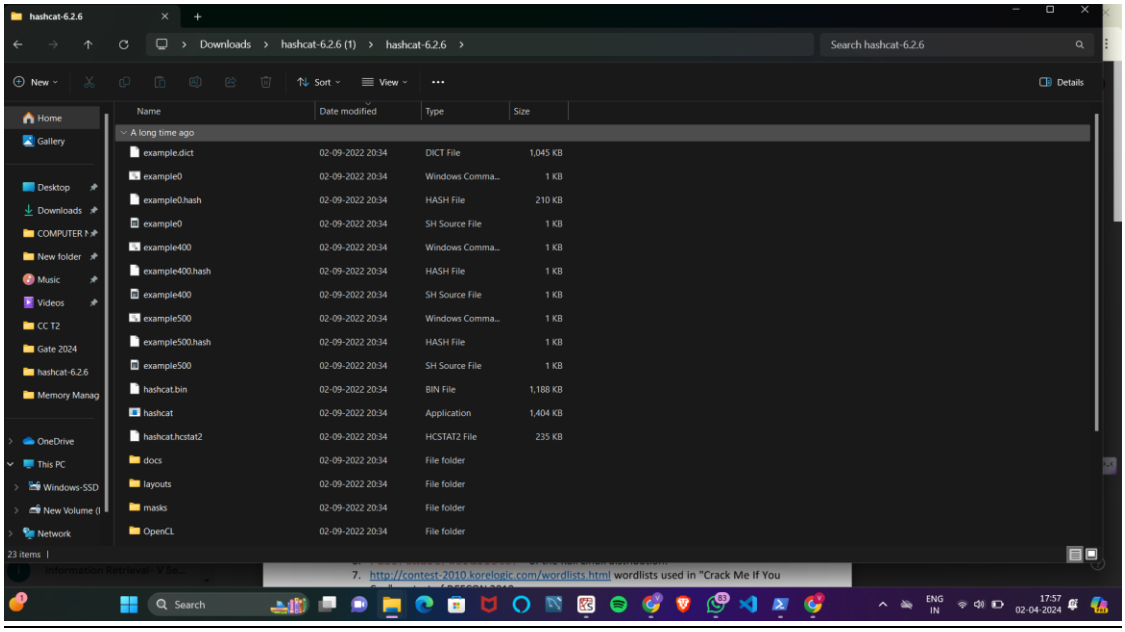
Step 1 – Installing Hashcat for Windows:

hashcat
advanced
password
recovery

Download

Name	Version	Date	Download	Signature
hashcat binaries	v6.2.6	2022.09.02	Download	PGP
hashcat sources	v6.2.6	2022.09.02	Download	PGP

Extracted hashcat folder:



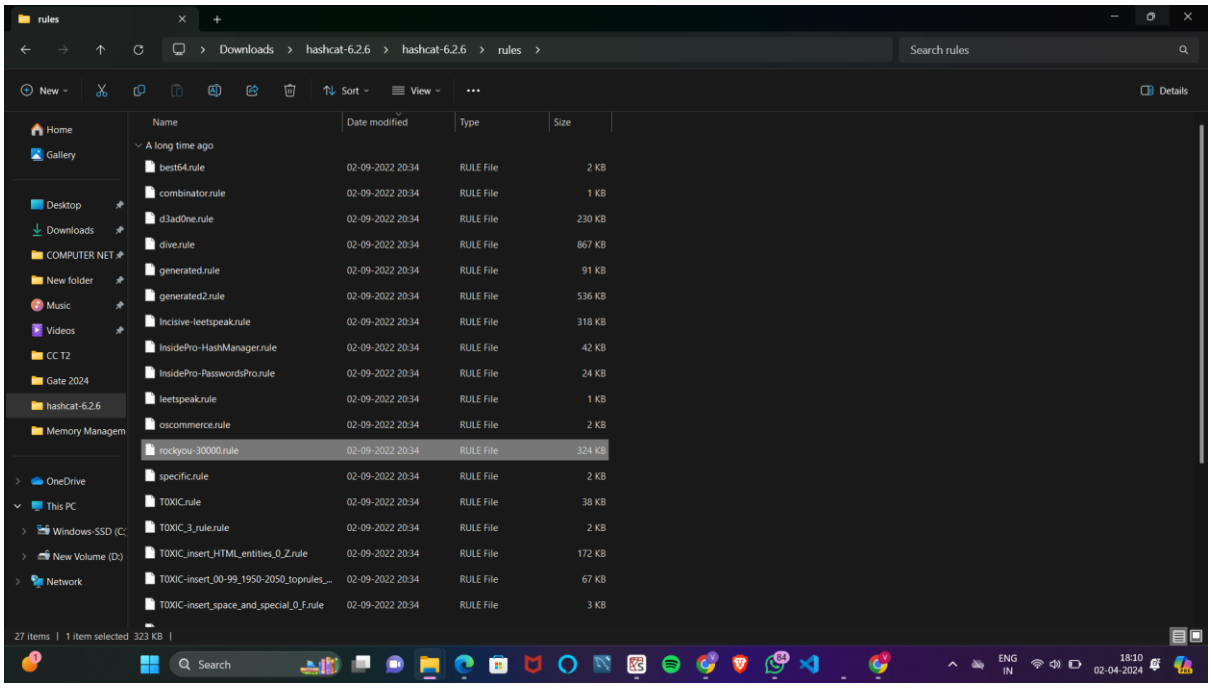
a) student: 29e08fb7103c327d68327f23d8d9256c

(Given MD5 hash here we are using the 10 million Leaked passwords Wordlist and the rockyou-30000 rules list to crack the hash as it was getting exhausted if applied without any rule.)

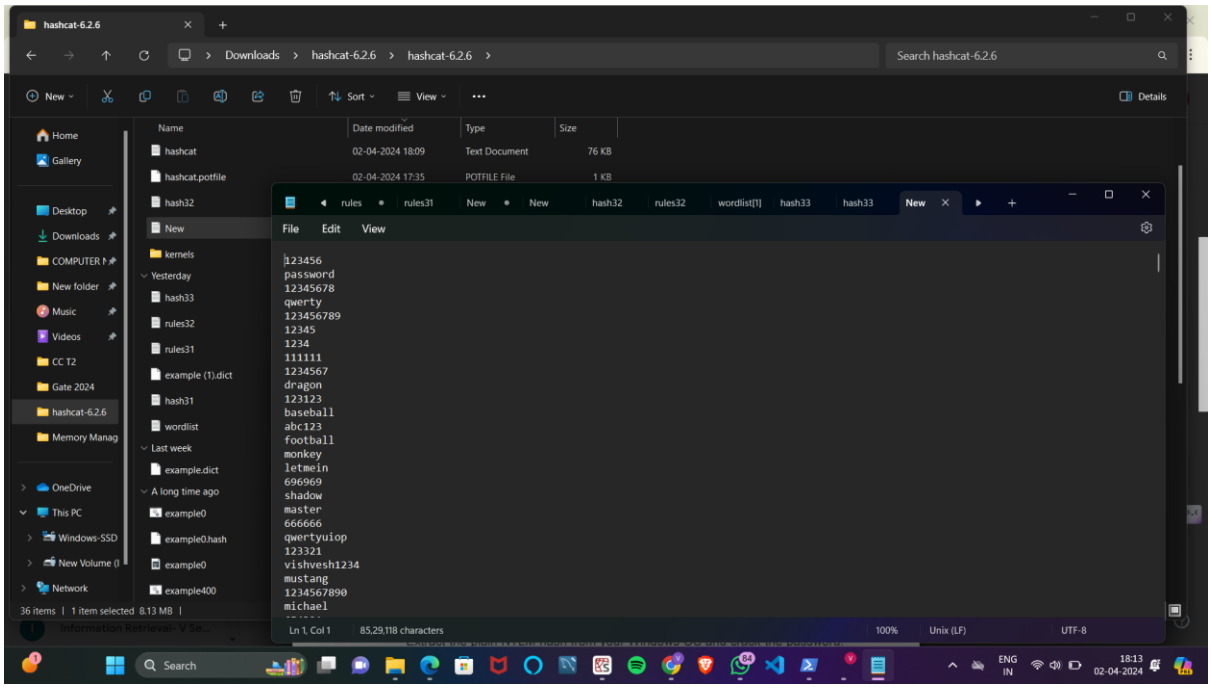
Name : Vishvesh Shatalwar
Mis : 112115146

HASH - 29e08fb7103c327d68327f23d8d9256c

Special Rule that is to applied and its path:
Path : "C:\Users\vishv\Downloads\hashcat-6.2.6\hashcat-6.2.6\rules\rockyou-30000.rule"



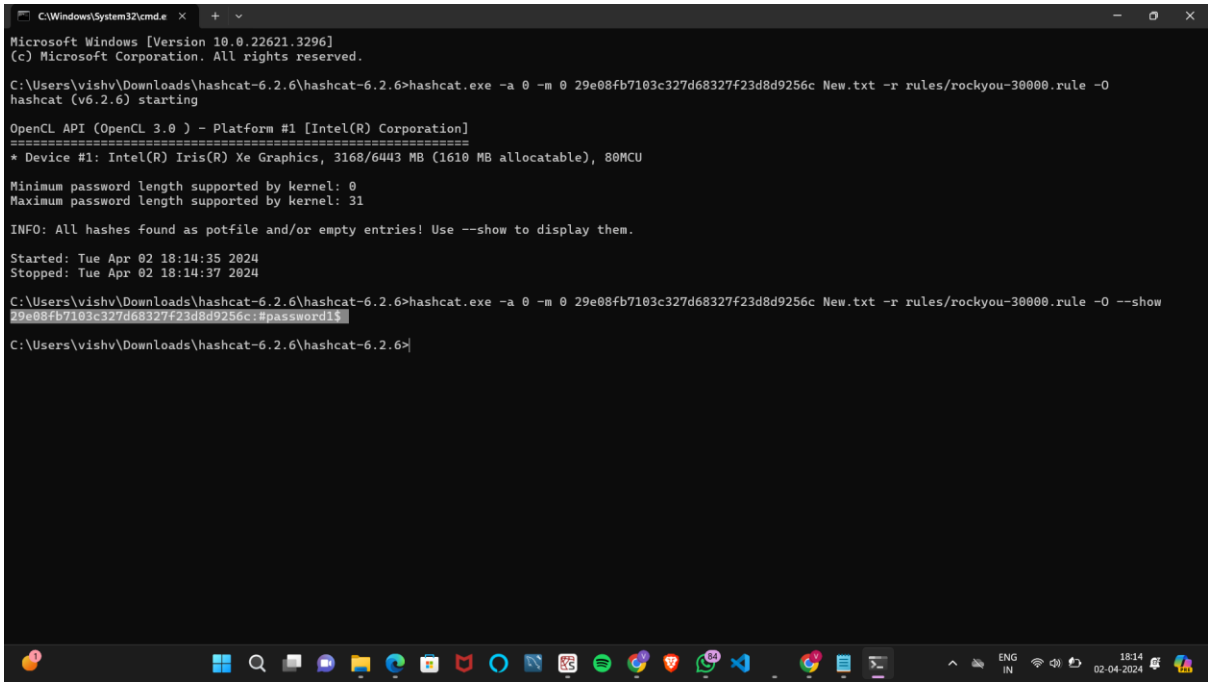
Shared 10million dictionary saved as **New.txt** which is to be used as dictionary for the attack :



Name : Vishvesh Shatalwar
Mis : 112115146

Running the command with its respective :
-a : attack mode : Dictionary based (0)
-m : Hash type : MD5 (0)
-O : Optimization in execution
--show : for displaying the password

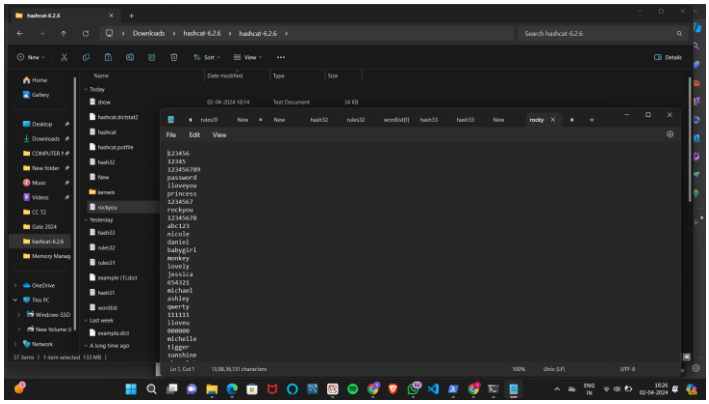
Password : **#password1$**



b) jsmith: f6a0cb102c62879d397b12b62c092c06

HASH - f6a0cb102c62879d397b12b62c092c06

Rockyou Dictionary that is to be used :
Path : "C:\Users\vishv\Downloads\hashcat-6.2.6\rockyou.txt"



Name : Vishvesh Shatalwar
Mis : 112115146

rockyou.txt : Dictionary
Password – **bluered**

```
C:\Windows\System32\cmd.e

Microsoft Windows [Version 10.0.22621.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\vishv\Downloads\hashcat-6.2.6\hashcat-6.2.6>hashcat.exe -a 0 -m 0 f6a0cb102c62879d397b12b62c092c06 rockyou.txt hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 ) - Platform #1 [Intel(R) Corporation]
============================================================
* Device #1: Intel(R) Iris(R) Xe Graphics, 3168/6443 MB (1610 MB allocatable), 80MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Meet-In-The-Middle
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 1448 MB

Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

f6a0cb102c62879d397b12b62c092c06:bluered
```

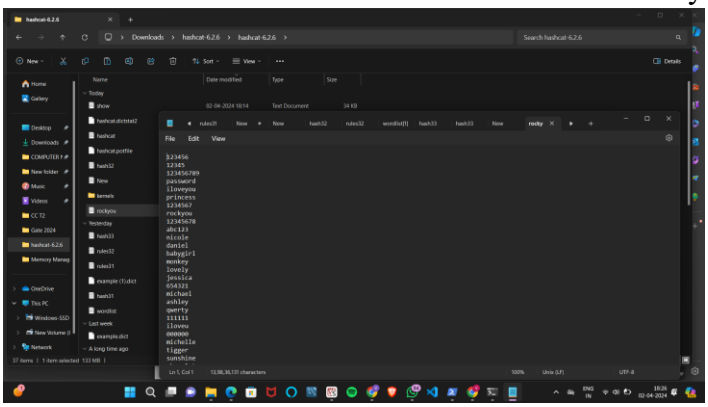
```
C:\Windows\System32\cmd.e

Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

f6a0cb102c62879d397b12b62c092c06:bluered

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: f6a0cb102c62879d397b12b62c092c06
Time.Started.....: Tue Apr 02 18:32:36 2024 (0 secs)
Time.Estimated...: Tue Apr 02 18:32:36 2024 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 23590.9 kH/s (10.09ms) @ Accel:256 Loops:1 Thr:128 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2622142/14344384 (18.28%)
Rejected.........: 702/2622142 (0.03%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> yayauran120196

Started: Tue Apr 02 18:32:30 2024
Stopped: Tue Apr 02 18:32:38 2024

C:\Users\vishv\Downloads\hashcat-6.2.6\hashcat-6.2.6>hashcat.exe -a 0 -m 0 f6a0cb102c62879d397b12b62c092c06 rockyou.txt  -O --show
f6a0cb102c62879d397b12b62c092c06:bluered

C:\Users\vishv\Downloads\hashcat-6.2.6\hashcat-6.2.6>
```

Name : Vishvesh Shatalwar
Mis : 112115146

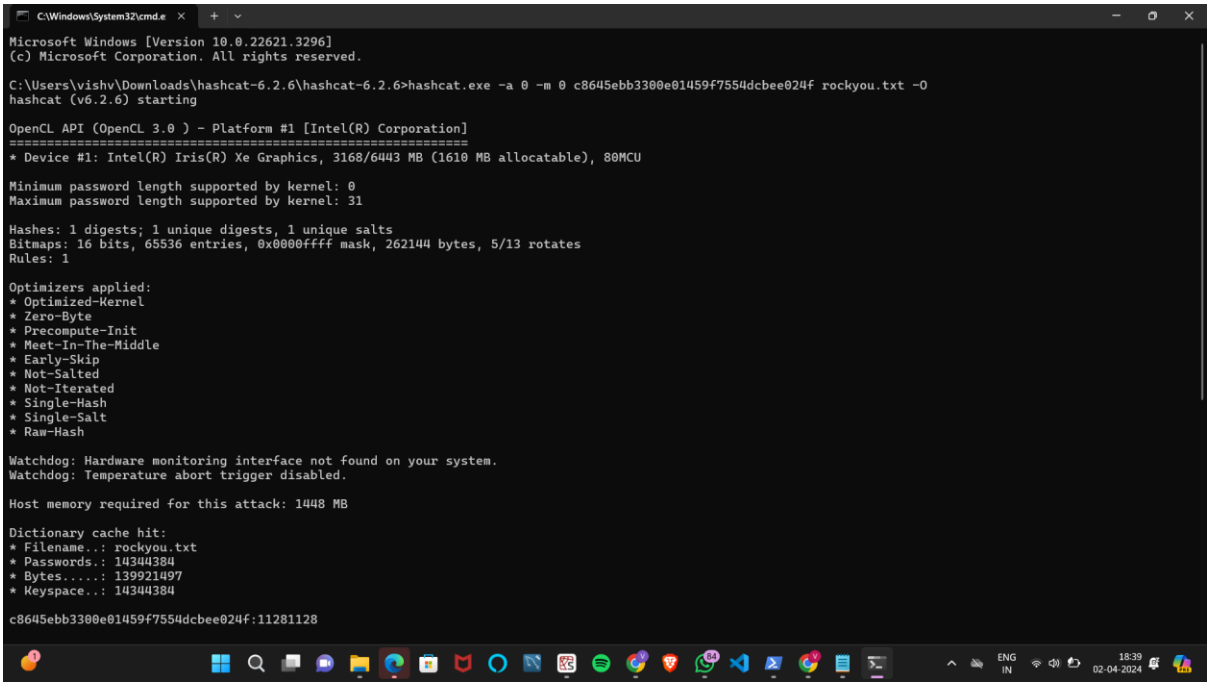
c) jtripper: c8645ebb3300e01459f7554dcbee024f

Hash : c8645ebb3300e01459f7554dcbee024f

Rockyou Dictionary that is to be used :
Path : "C:\Users\vishv\Downloads\hashcat-6.2.6\rockyou.txt"

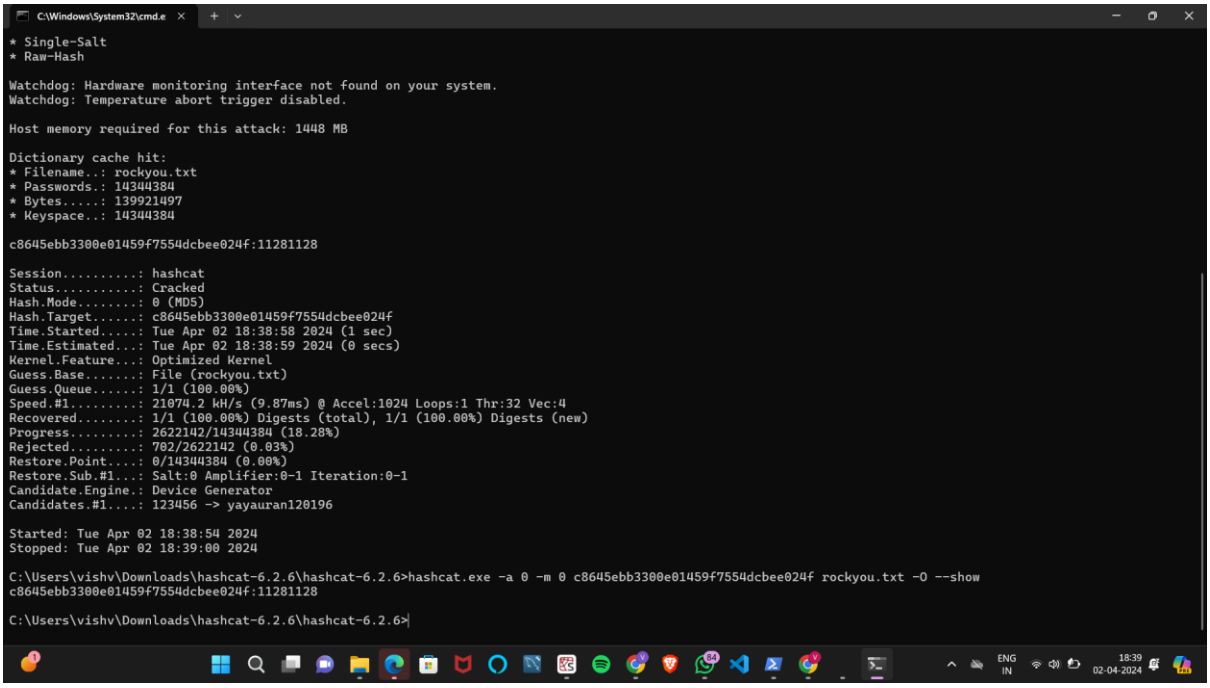


rockyou.txt : Dictionary
Password – **11281128**



```
C:\Windows\System32\cmd.e

Microsoft Windows [Version 10.0.22621.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\vishv\Downloads\hashcat-6.2.6\hashcat-6.2.6>hashcat.exe -a 0 -m 0 c8645ebb3300e01459f7554dcbee024f rockyou.txt -O
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 ) - Platform #1 [Intel(R) Corporation]
====================================================================
* Device #1: Intel(R) Iris(R) Xe Graphics, 3168/6443 MB (1610 MB allocatable), 80MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Meet-In-The-Middle
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 1448 MB

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

c8645ebb3300e01459f7554dcbee024f:11281128
```

Name : Vishvesh Shatalwar
Mis : 112115146

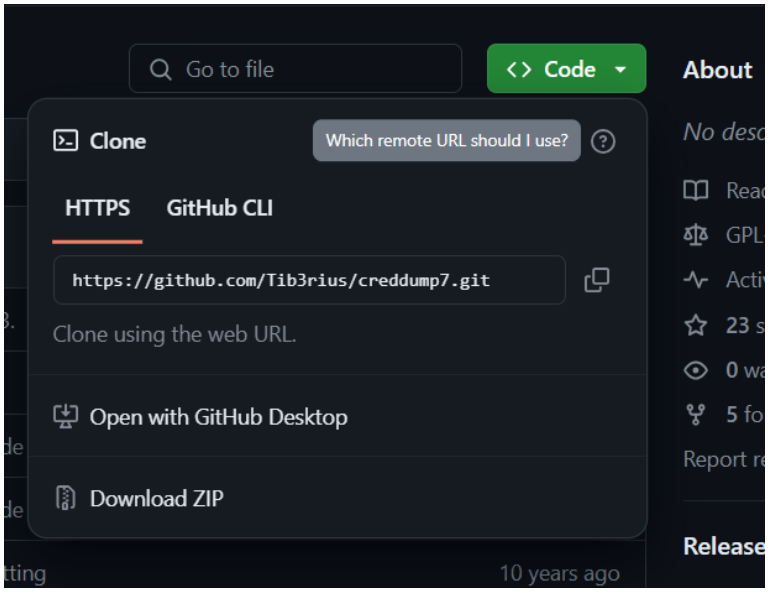


```
* Single-Salt
* Raw-Hash

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 1448 MB

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

c8645ebb3300e01459f7554dcbee024f:11281128

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: c8645ebb3300e01459f7554dcbee024f
Time.Started.....: Tue Apr 02 18:38:58 2024 (1 sec)
Time.Estimated...: Tue Apr 02 18:38:59 2024 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 21074.2 kH/s (9.87ms) @ Accel:1024 Loops:1 Thr:32 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2622142/14344384 (18.28%)
Rejected.........: 702/2622142 (0.03%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> yayauran120196

Started: Tue Apr 02 18:38:54 2024
Stopped: Tue Apr 02 18:39:00 2024

C:\Users\vishv\Downloads\hashcat-6.2.6\hashcat-6.2.6>hashcat.exe -a 0 -m 0 c8645ebb3300e01459f7554dcbee024f rockyou.txt -O --show
c8645ebb3300e01459f7554dcbee024f:11281128

C:\Users\vishv\Downloads\hashcat-6.2.6\hashcat-6.2.6>
```

2) SubLab-2: Cracking Windows NTLM Password Hashes using Hashcat

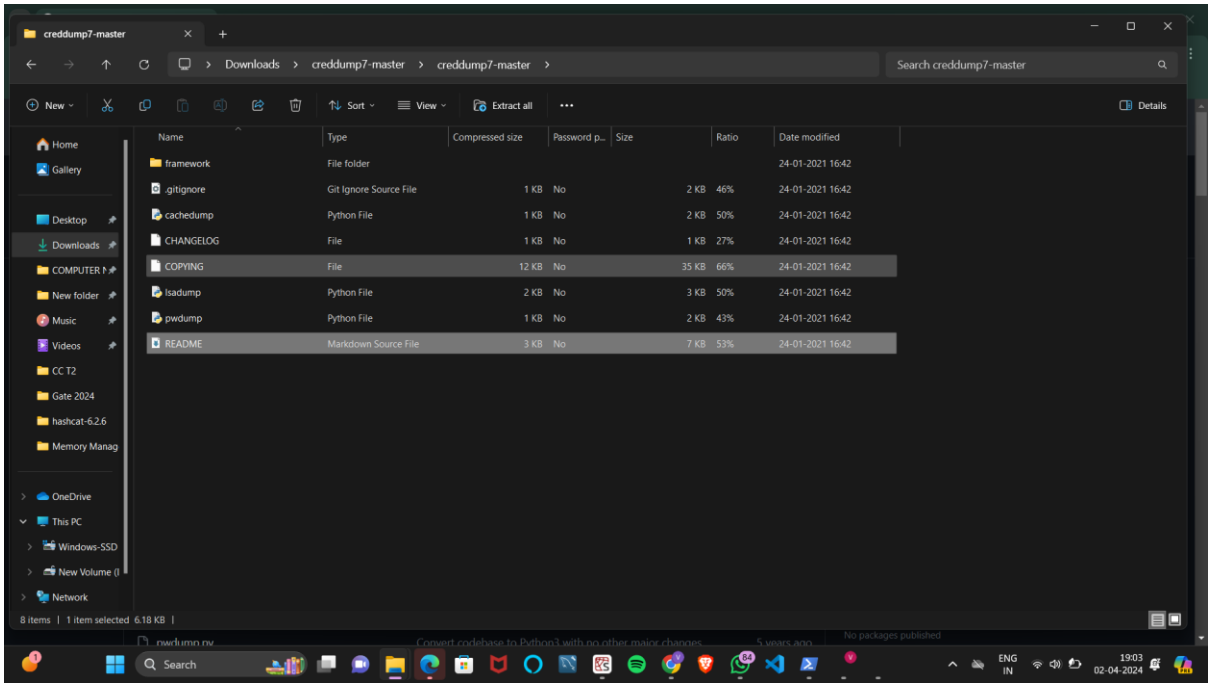
(Extract the plain NTLM hash from your Windows OS and crack the password. Include the screenshots with username and cracked password. You can use existing dictionaries with rules, if password is not recovered then prepare a new dictionary with partial password and use best64.rule to crack it.)

Step 1: Installing creddump zip file :



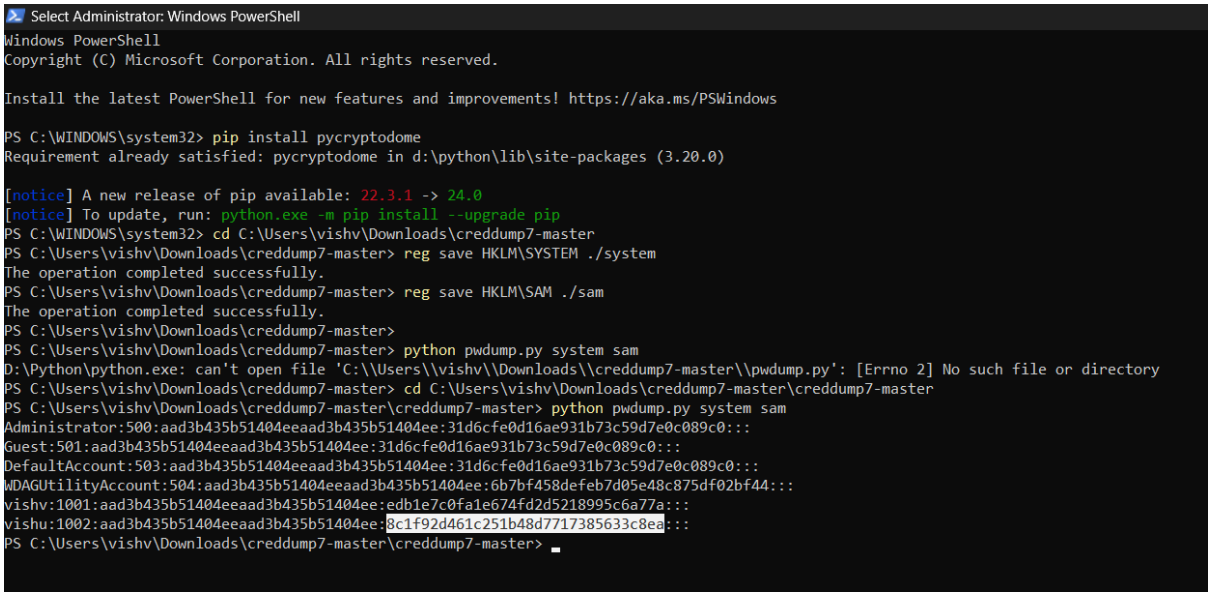
Name : Vishvesh Shatalwar
Mis : 112115146

creddump7-master folder :



Step 2 : Extracting Plain NTLM Hash for my Windows Account :

a) reg save HKLM\SYSTEM ./system for saving system file from registry
b) reg save HKLM\SAM ./sam for saving sam file from registry.
c) Python pwdump.py system sam for extracting Usernames and their respective plain NTLM Hashes.
(vishu – alternate account)



Hash : 8c1f92d461c251b48d7717385633c8ea

Name : Vishvesh Shatalwar
Mis : 112115146

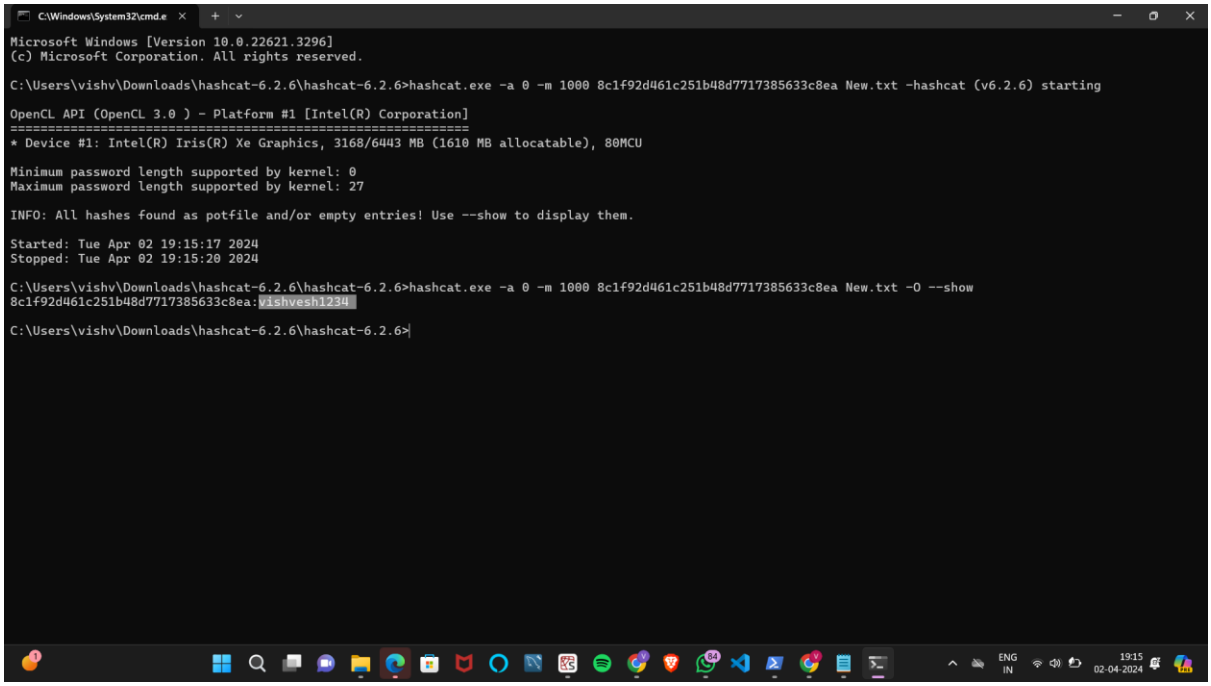
Step 3 : Extracting the password from the received hash from above step by using Hashcat tool

-a : attack mode (0)

-m : Hash type : NTLM (1000)

Dictionary : 10millionpasswd (saved as New.txt)

Password : **vishvesh1234**

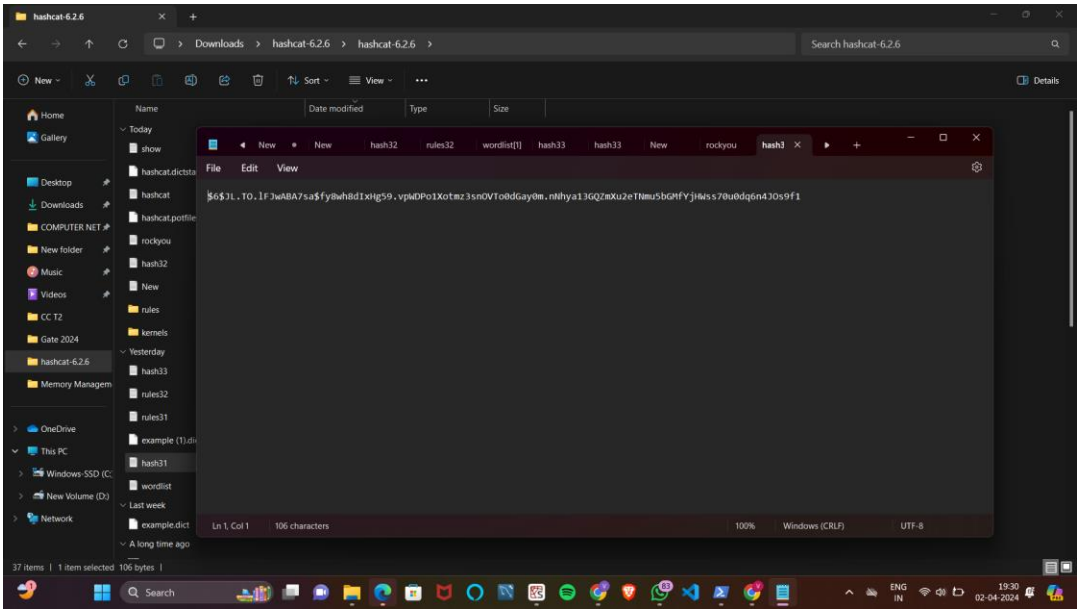


3. SubLab-3: Cracking SHA512 Password Hashes using Hashcat/JohntheRipper

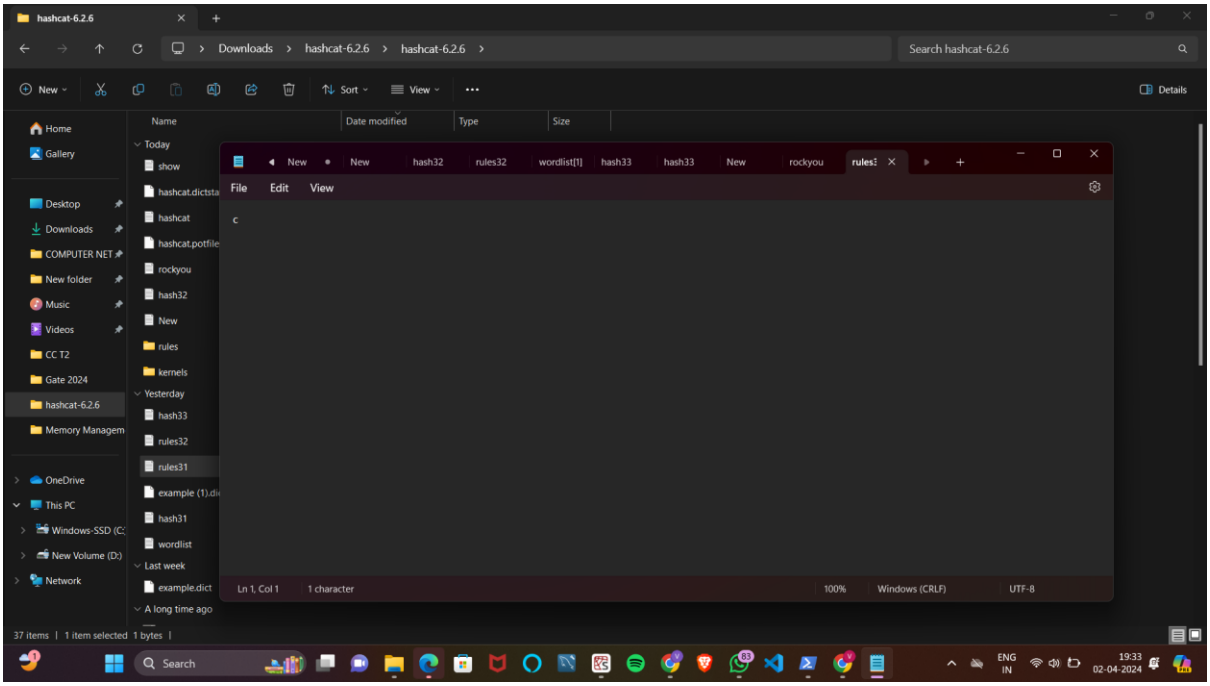
1) root:6JL.TO.lFJwABA7sa$fy8wh8dIxHg59.vpWDPo1Xotmz3snOVTo0dGay0m.nNhya13GQZmXu2eTNmu5bGMfYjHWss70u0dq6n4JOs9f1

   Step 1 : Storing the given Hash in a txt file in Hashcat folder named as hash31.txt (while storing removing root: from given hash)

Name : Vishvesh Shatalwar
Mis : 112115146

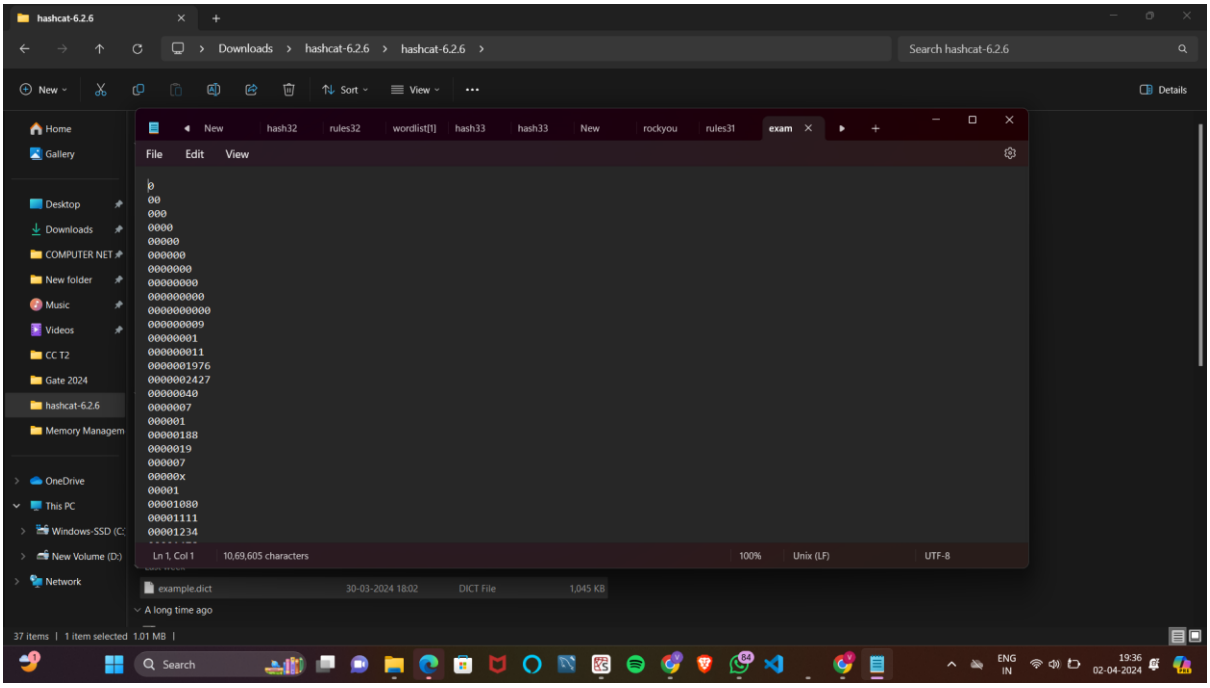


Step 2 : Defining the rules in a text document named rules31.txt , as mentioned in the assignment that first letter of the password is in Uppercase so rule states : c (depicting first letter as uppercase)



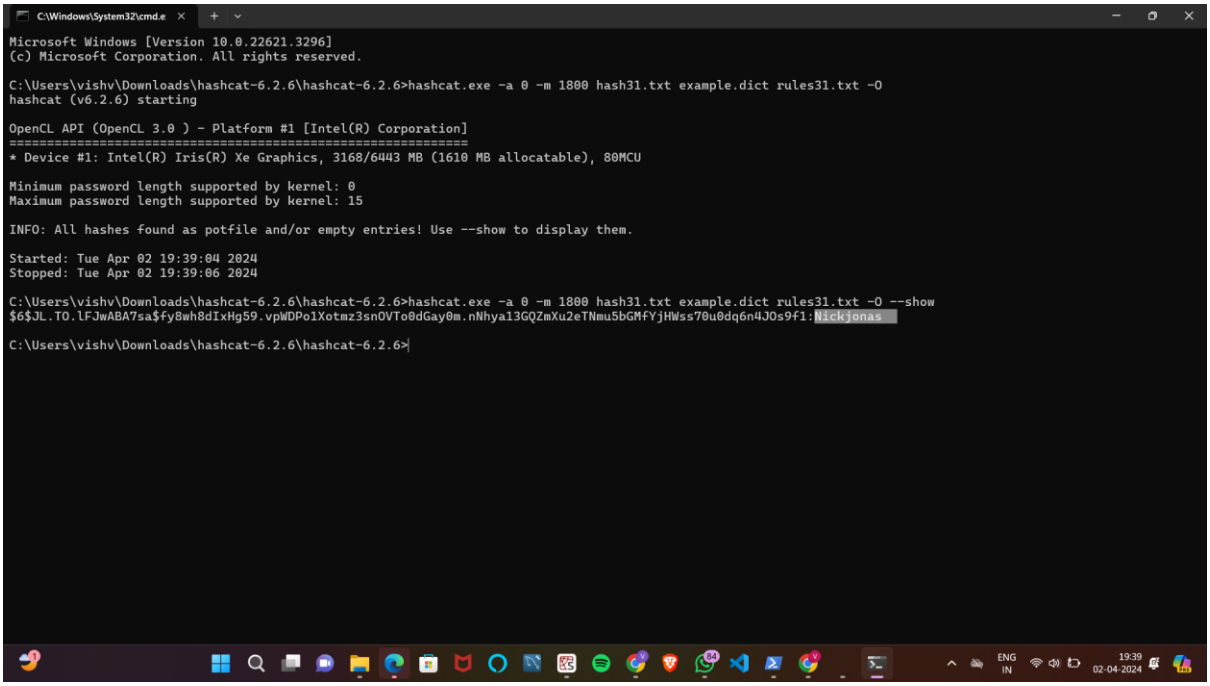
Step 3 : Downloading and saving the example.dict dictionary mentioned in the assignment in Hashcat folder.

Name : Vishvesh Shatalwar
Mis : 112115146



Step 4 : Cracking the Password using Hashcat :
-a attack mode (0) : Dictionary Attack
-m Hash type (1800) : SHA512 Hash
hash31.txt : containing hash given in assignment
example.dict : Dicitionary provided
rules31.txt : Rules defined (first letter is uppercase)

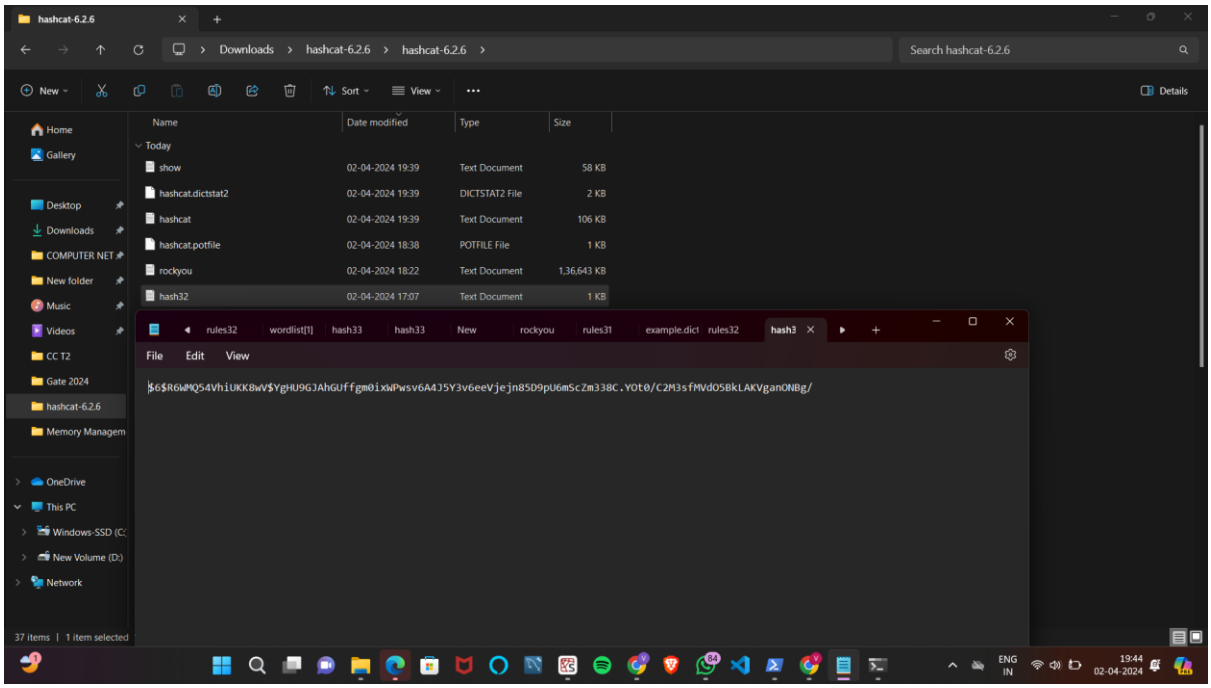
Password : **Nickjonas**



Name : Vishvesh Shatalwar
Mis : 112115146

2) iiit:6R6WMQ54VhiUKK8wV$YgHU9GJAhGUffgm0ixWPwsv6A4J5Y3v6eeVjejn85D9pU6mScZm338C.YOt0/C2M3sfMVdO5BkLAKVganONBg/

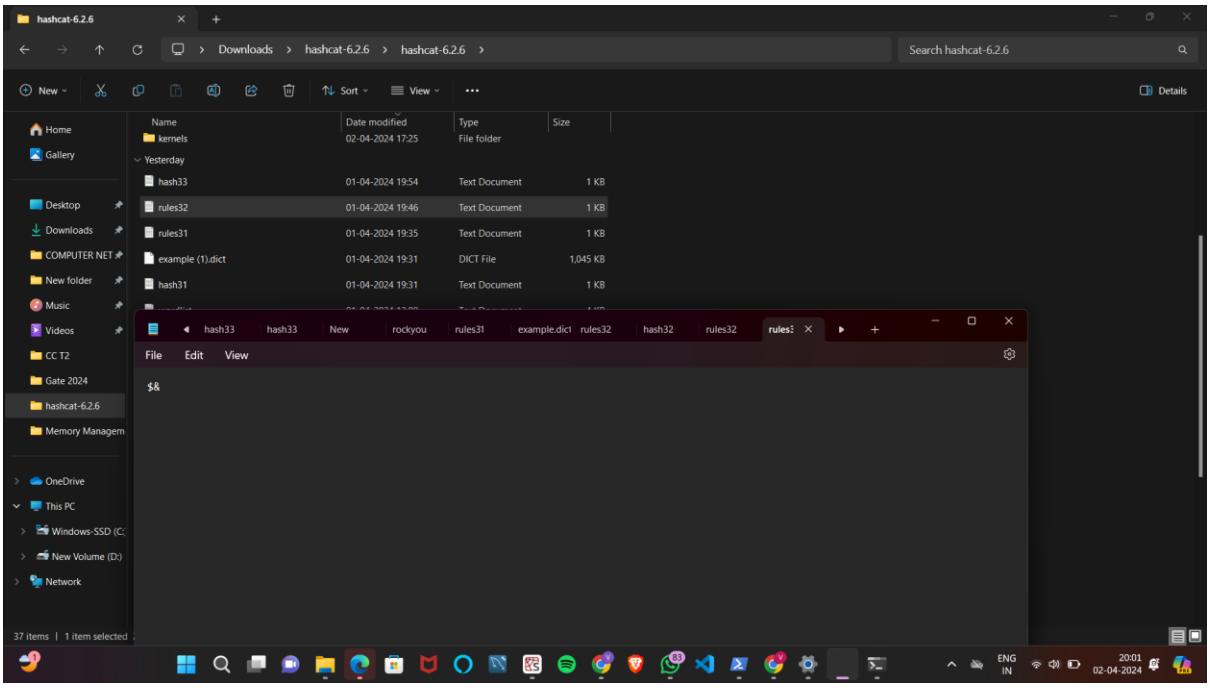
Step 1 : Storing the given Hash in a txt file in Hashcat folder named as hash32.txt (while storing removing iiit: from given hash)



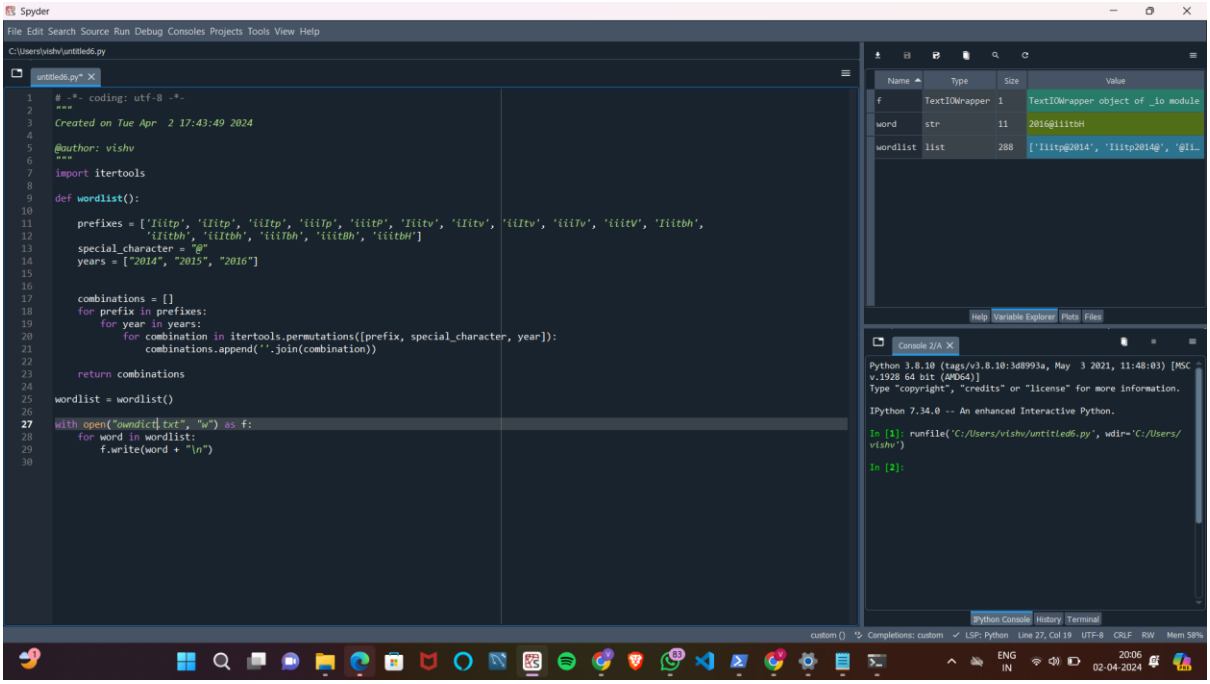
Step 2) Defining the rules in a text document named rules32.txt , as mentioned in the assignment that password end with & so rule states : $& (depicting that password ends with &)

Name : Vishvesh Shatalwar
Mis : 112115146

rules32.txt :

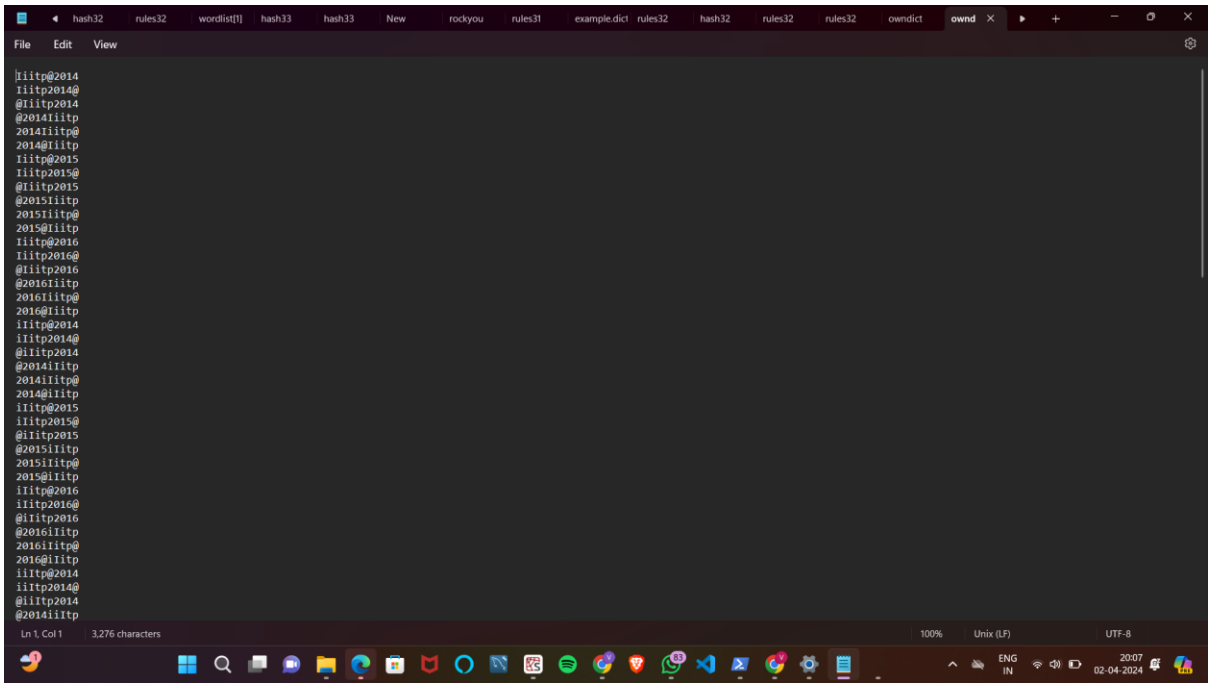


Step 3) Creating own dictionary that the password consists of iiitv or iiitp or iiitbh, special character i.e @ and 2014 or 2015 or 2016 in any order by writing the python code for the same satisfying above conditions and writing it in a txt document named wordlist.



Name : Vishvesh Shatalwar
Mis : 112115146

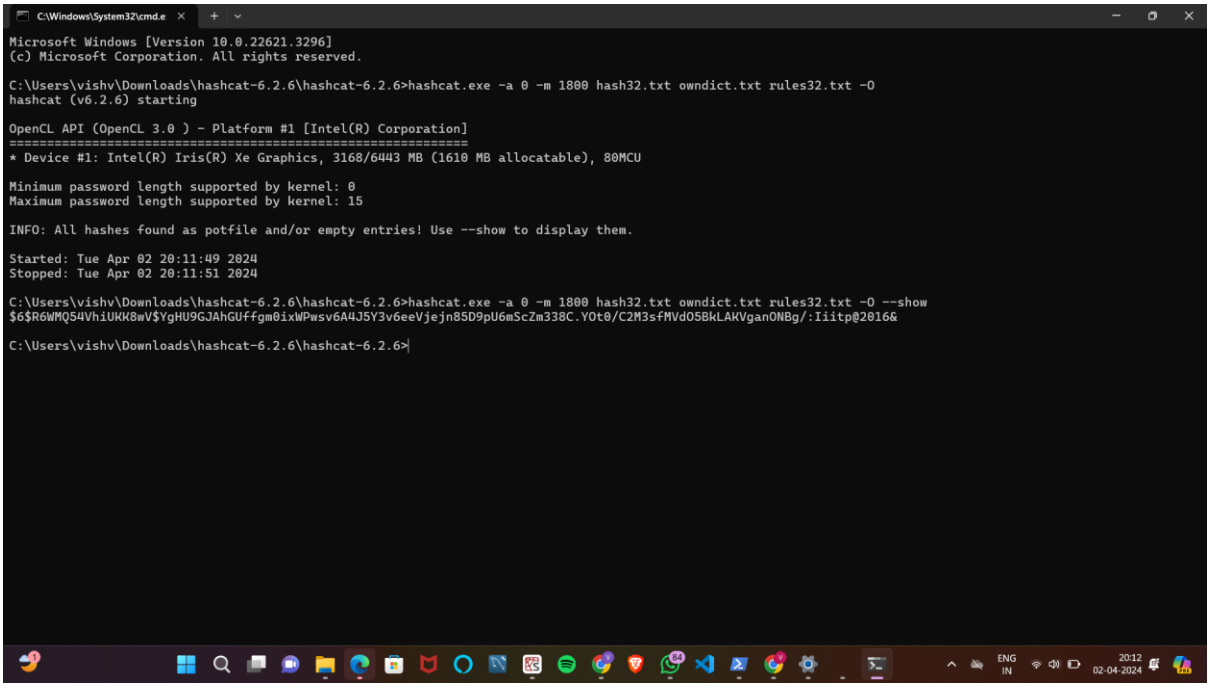
owndict.txt:



Step 4 : Cracking the Password using Hashcat :
-a attack mode (0) : Dictionary Attack
-m Hash type (1800) : SHA512 Hash
hash32.txt : containing hash given in assignment
owndict.txt : Dicitionary that we created
rules32.txt : Rules defined (one letter is uppercase)

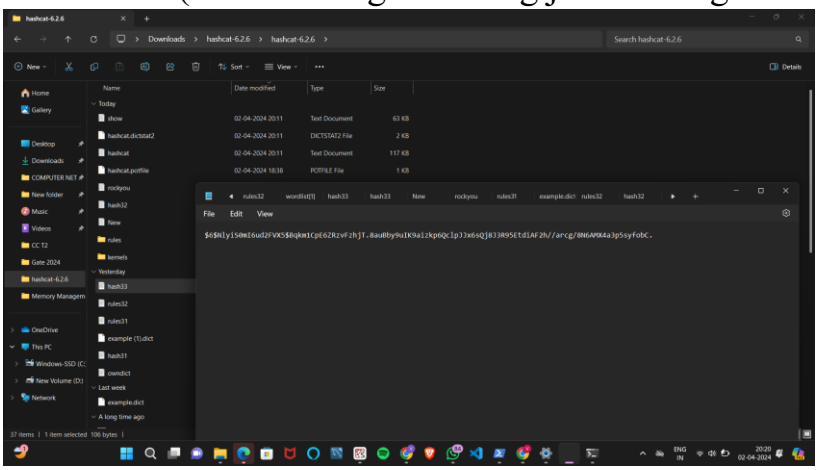
Password : **Iiitp@2016&**

Name : Vishvesh Shatalwar
Mis : 112115146



3) jazz:6NlyiS0mI6ud2FVX5$Bqkm1CpE6ZRzvFzhjT.8auBby9uIK9aizkp6QclpJJx6sQj8J3R95EtdiAF2h//arcg/8N6AMX4a3p5syfobC.

Step 1 : Storing the given Hash in a txt file in Hashcat folder named as **hash33.txt** (while storing removing jazz: from given hash)



Step 2) Defining the Mask given that password is having exactly 8 characters, first character as #, second character is in uppercase, rest characters are in lowercase and ends with digit 1.

Mask : #?u?l?l?l?l?l1

(?u – Uppercase letter , ?l – lowercase letter)

Name : Vishvesh Shatalwar
Mis : 112115146

Step 3) Cracking the Password using Hashcat :

-a attack mode (3) : Masking Attack

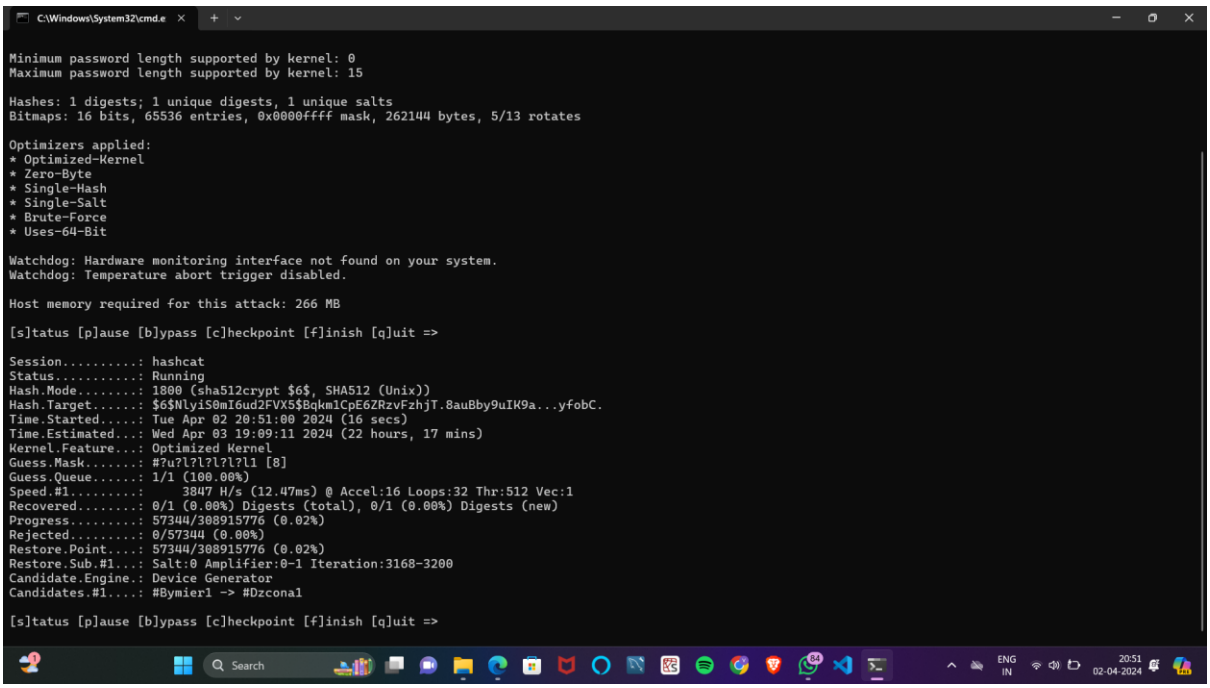
-m Hash type (1800) : SHA512 Hash

hash33.txt : containing hash given in assignment

Mask : #?u?l?l?l?l?l1

(The below cracking was taking more than 22 hours in first try Since there are 26^6 which is equivalent to around 30 million combinations possible it will take a lot of time to check all possible combinations of hashes , so below included all various mask variations for reducing time for cracking)

Try 1 : **(Mask used : #?u?l?l?l?l?l1 , Time estimated – 22hrs17mins)**



```
C:\Windows\System32\cmd.e

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 15

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force
* Uses-64-Bit

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 266 MB

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>

Session..........: hashcat
Status...........: Running
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$NlyiS0mI6ud2FVX5$Bqkm1CpE6ZRzvFzhjT.8auBby9uIK9a...yfobC.
Time.Started.....: Tue Apr 02 20:51:00 2024 (16 secs)
Time.Estimated...: Wed Apr 03 19:09:11 2024 (22 hours, 17 mins)
Kernel.Feature...: Optimized Kernel
Guess.Mask.......: #?u?l?l?l?l?l1 [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     3847 H/s (12.47ms) @ Accel:16 Loops:32 Thr:512 Vec:1
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 57344/308915776 (0.02%)
Rejected.........: 0/57344 (0.00%)
Restore.Point....: 57344/308915776 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:3168-3200
Candidate.Engine.: Device Generator
Candidates.#1....: #Bymier1 -> #Dzcona1

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>
```

Name : Vishvesh Shatalwar
Mis : 112115146

Try 2 : (**Mask Used : #J?l?l?l?l?l1 , Time Estimated : 59mins 2sec**)

```
C:\Users\vishv\Downloads\hashcat-6.2.6\hashcat-6.2.6>hashcat.exe -a 3 -m 1800 hash33.txt #J?l?l?l?l?l1 -O
```

```
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 15

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force
* Uses-64-Bit

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 266 MB

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>

Session..........: hashcat
Status...........: Running
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$NlyiS0mI6ud2FVX5$Bqkm1CpE6ZRzvFzhjT.8auBby9uIK9a...yfobC.
Time.Started.....: Tue Apr 02 20:53:56 2024 (8 secs)
Time.Estimated...: Tue Apr 02 21:53:06 2024 (59 mins, 2 secs)
Kernel.Feature...: Optimized Kernel
Guess.Mask.......: #J?l?l?l?l?l1 [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     3347 H/s (6.89ms) @ Accel:32 Loops:16 Thr:256 Vec:1
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 24576/11881376 (0.21%)
Rejected.........: 0/24576 (0.00%)
Restore.Point....: 24576/11881376 (0.21%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:736-752
Candidate.Engine.: Device Generator
Candidates.#1....: #Jcucan1 -> #Jivfin1

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>
```

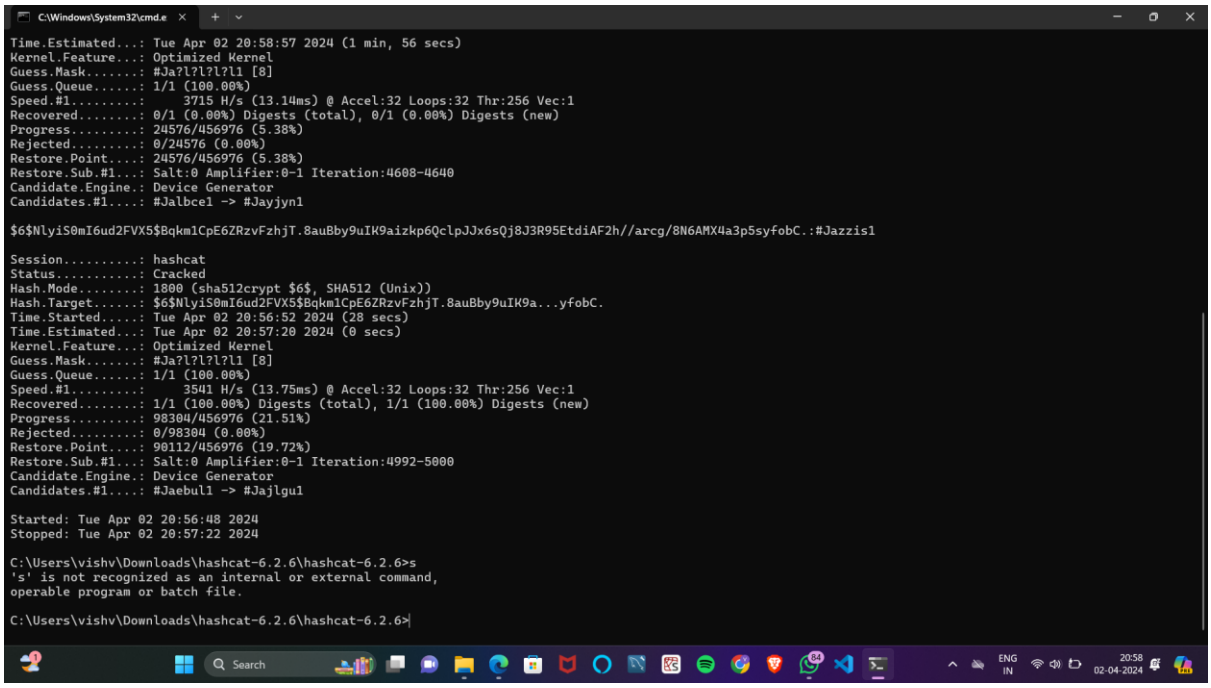
Try 3 : (**Mask Used : #Ja?l?l?l?l1 , Time estimated : 1min56sec**)

```
C:\Users\vishv\Downloads\hashcat-6.2.6\hashcat-6.2.6>hashcat.exe -a 3 -m 1800 hash33.txt #Ja?l?l?l?l1 -O
hashcat (v6.2.6) starting
```

```
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 15

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force
* Uses-64-Bit

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 266 MB

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>

Session..........: hashcat
Status...........: Running
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$NlyiS0mI6ud2FVX5$Bqkm1CpE6ZRzvFzhjT.8auBby9uIK9a...yfobC.
Time.Started.....: Tue Apr 02 20:56:52 2024 (9 secs)
Time.Estimated...: Tue Apr 02 20:58:57 2024 (1 min, 56 secs)
Kernel.Feature...: Optimized Kernel
Guess.Mask.......: #Ja?l?l?l?l1 [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     3715 H/s (13.14ms) @ Accel:32 Loops:32 Thr:256 Vec:1
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 24576/456976 (5.38%)
Rejected.........: 0/24576 (0.00%)
Restore.Point....: 24576/456976 (5.38%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4608-4640
Candidate.Engine.: Device Generator
Candidates.#1....: #Jalbce1 -> #Jayjyn1

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>
```

Name : Vishvesh Shatalwar
Mis : 112115146

Password : **#Jazzis1**



```
C:\Windows\System32\cmd.e

Time.Estimated...: Tue Apr 02 20:58:57 2024 (1 min, 56 secs)
Kernel.Feature...: Optimized Kernel
Guess.Mask.......: #Ja?l?l?l?l1 [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     3715 H/s (13.14ms) @ Accel:32 Loops:32 Thr:256 Vec:1
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 24576/456976 (5.38%)
Rejected.........: 0/24576 (0.00%)
Restore.Point....: 24576/456976 (5.38%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4608-4640
Candidate.Engine.: Device Generator
Candidates.#1....: #Jalbce1 -> #Jayjyn1

$6$NlyiS0mI6ud2FVX5$Bqkm1CpE6ZRzvFzhjT.8auBby9uIK9aizkp6QclpJJx6sQj8J3R95EtdiAF2h//arcg/8N6AMX4a3p5syfobC.:#Jazzis1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$NlyiS0mI6ud2FVX5$Bqkm1CpE6ZRzvFzhjT.8auBby9uIK9a...yfobC.
Time.Started.....: Tue Apr 02 20:56:52 2024 (28 secs)
Time.Estimated...: Tue Apr 02 20:57:20 2024 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Mask.......: #Ja?l?l?l?l1 [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     3541 H/s (13.75ms) @ Accel:32 Loops:32 Thr:256 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 98304/456976 (21.51%)
Rejected.........: 0/98304 (0.00%)
Restore.Point....: 90112/456976 (19.72%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4992-5000
Candidate.Engine.: Device Generator
Candidates.#1....: #Jaebul1 -> #Jajlgu1

Started: Tue Apr 02 20:56:48 2024
Stopped: Tue Apr 02 20:57:22 2024

C:\Users\vishv\Downloads\hashcat-6.2.6\hashcat-6.2.6>s
's' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\vishv\Downloads\hashcat-6.2.6\hashcat-6.2.6>
```