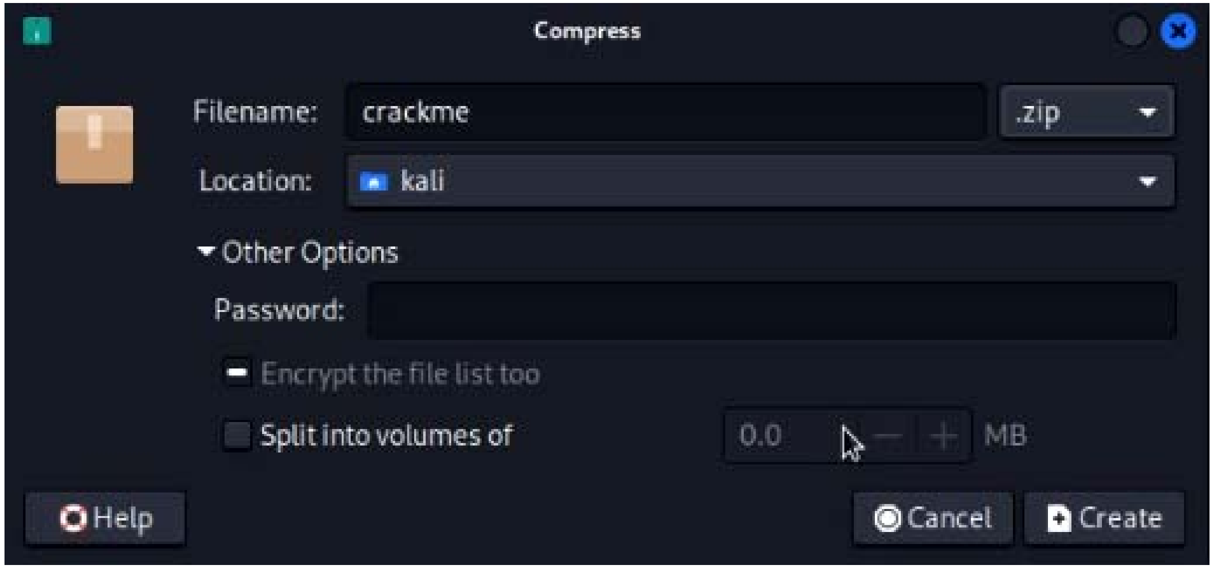
Cracking Zip and Rar Passwords

Cracking ZIP Files

Step- 1

- Prepare a password protected ZIP archive (KALI)

Right Click the file and click “create Archive” and set a password



Filename: crackme .zip

Location: kali

Password:

☐ Encrypt the file list too

☐ Split into volumes of 0.0 MB

Step- 2

- Open the terminal
- Get the hash of the document with the following command

```
zip2john crackme.zip > hash.txt
```

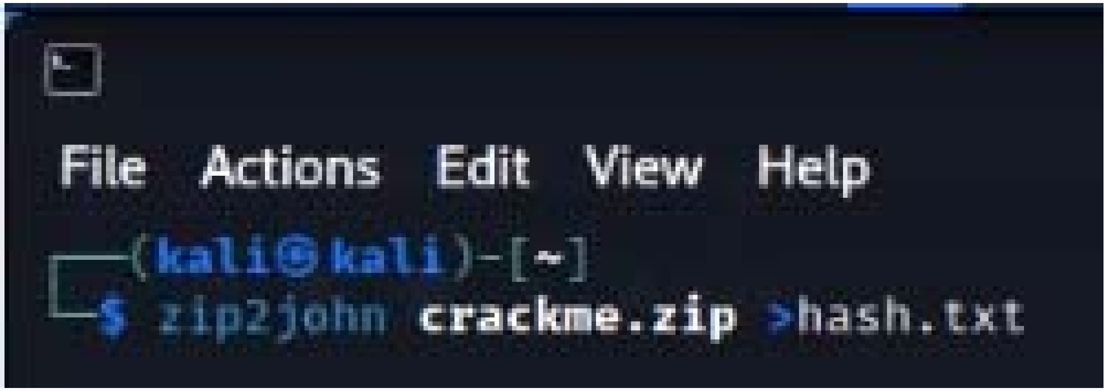
Here :

- Crackme.zip is the password-protected file
- Hash.txt is the txt file that will contain our hash that is required to be cracked

Step- 2

- Open the terminal
- Get the hash of the document with the following command

```
zip2john crackme.zip > hash.txt
```



```
┌──(kali㉿kali)-[~]
└─$ zip2john crackme.zip >hash.txt
```

Step- 4

- Now crack the password with following command

```
john --w hash.txt
```

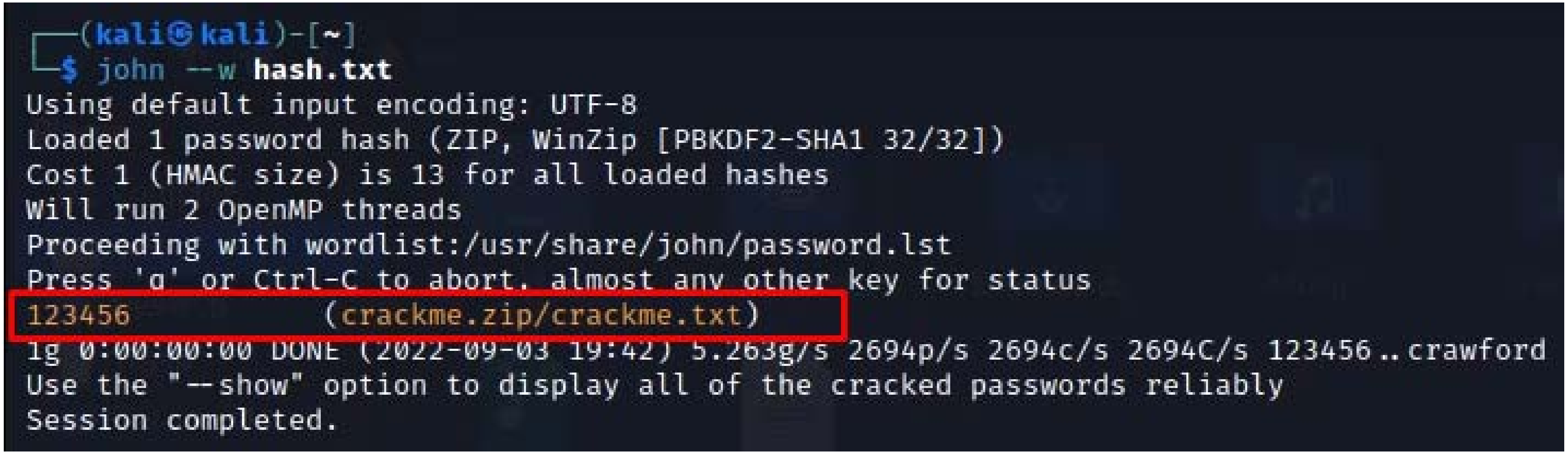
Here :

- Hash.txt file is the file that contains our hash for the document file
- --w tells john to use the default dictionary

Step- 4

- Now crack the password with following command

```
john --w hash.txt
```



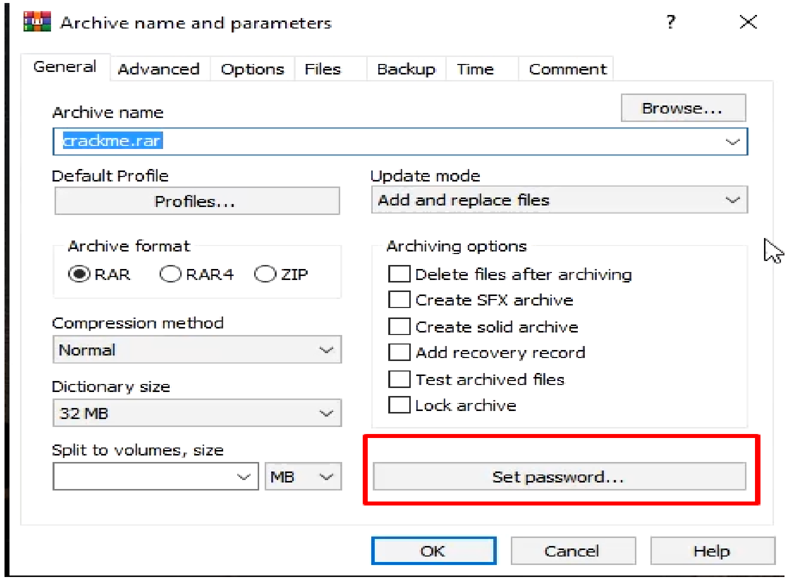
```
┌──(kali㉿kali)-[~]
└─$ john --w hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 32/32])
Cost 1 (HMAC size) is 13 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
123456           (crackme.zip/crackme.txt)
1g 0:00:00:00 DONE (2022-09-03 19:42) 5.263g/s 2694p/s 2694c/s 2694C/s 123456..crawford
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Cracking RAR Files

Step- 1

- Prepare a password protected rar archive (Windows)

Right Click the file and click “add to create Archive” and set a password in windows



Archive name and parameters

General | Advanced | Options | Files | Backup | Time | Comment

Archive name: crackme.rar

Default Profile: Profiles...

Update mode: Add and replace files

Archive format: ● RAR ○ RAR4 ○ ZIP

Compression method: Normal

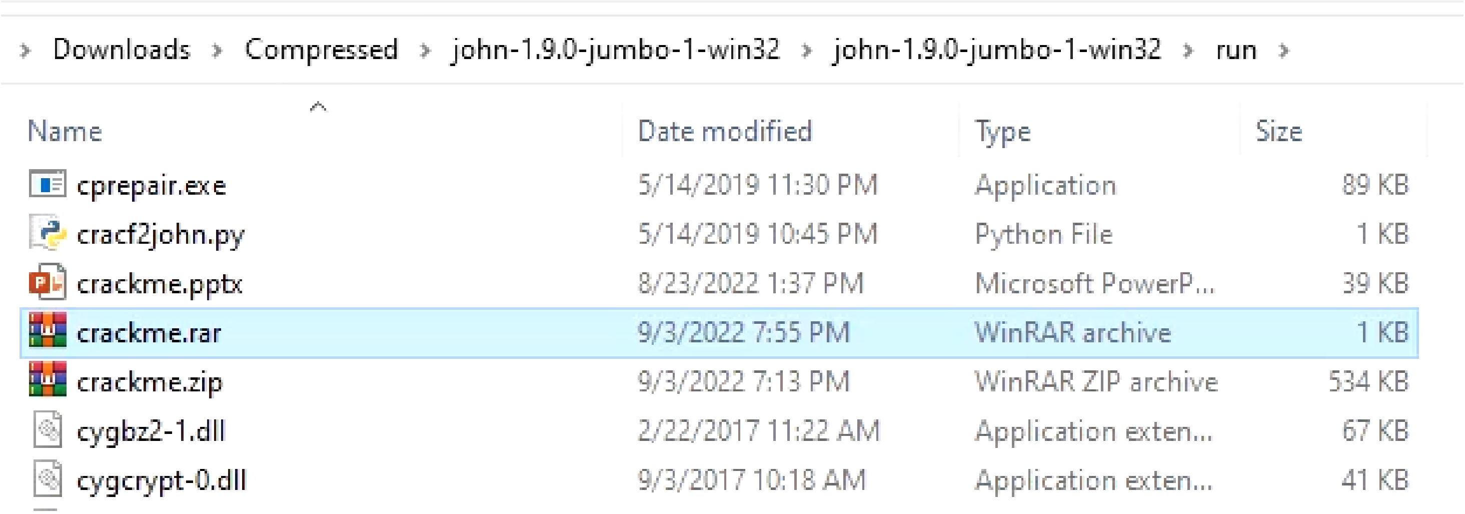
Dictionary size: 32 MB

Split to volumes, size: MB

Archiving options:
- □ Delete files after archiving
- □ Create SFX archive
- □ Create solid archive
- □ Add recovery record
- □ Test archived files
- □ Lock archive

Step- 2

- Copy the file to John/run folder in Windows



› Downloads › Compressed › john-1.9.0-jumbo-1-win32 › john-1.9.0-jumbo-1-win32 › run ›

Name	Date modified	Type	Size
cprepair.exe	5/14/2019 11:30 PM	Application	89 KB
cracf2john.py	5/14/2019 10:45 PM	Python File	1 KB
crackme.pptx	8/23/2022 1:37 PM	Microsoft PowerP...	39 KB
crackme.rar	9/3/2022 7:55 PM	WinRAR archive	1 KB
crackme.zip	9/3/2022 7:13 PM	WinRAR ZIP archive	534 KB
cygbz2-1.dll	2/22/2017 11:22 AM	Application exten...	67 KB
cygcrypt-0.dll	9/3/2017 10:18 AM	Application exten...	41 KB

Step- 3

- Open the command terminal in the same folder.
- Get the hash of the document with following command

```
rar2john crackme.rar > hash.txt
```

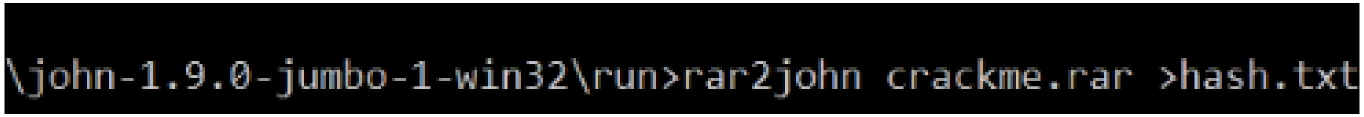
Here :

- Crackme.rar is the password-protected file
- Hash.txt is the txt file that will contain our hash that is required to be cracked

Step- 3

- Get the hash of the document with following command

```
rar2john crackme.rar > hash.txt
```



```
\john-1.9.0-jumbo-1-win32\run>rar2john crackme.rar >hash.txt
```

Step- 4

- Now crack the password with following command

```
john --w=“rockyou.txt” hash.txt
```

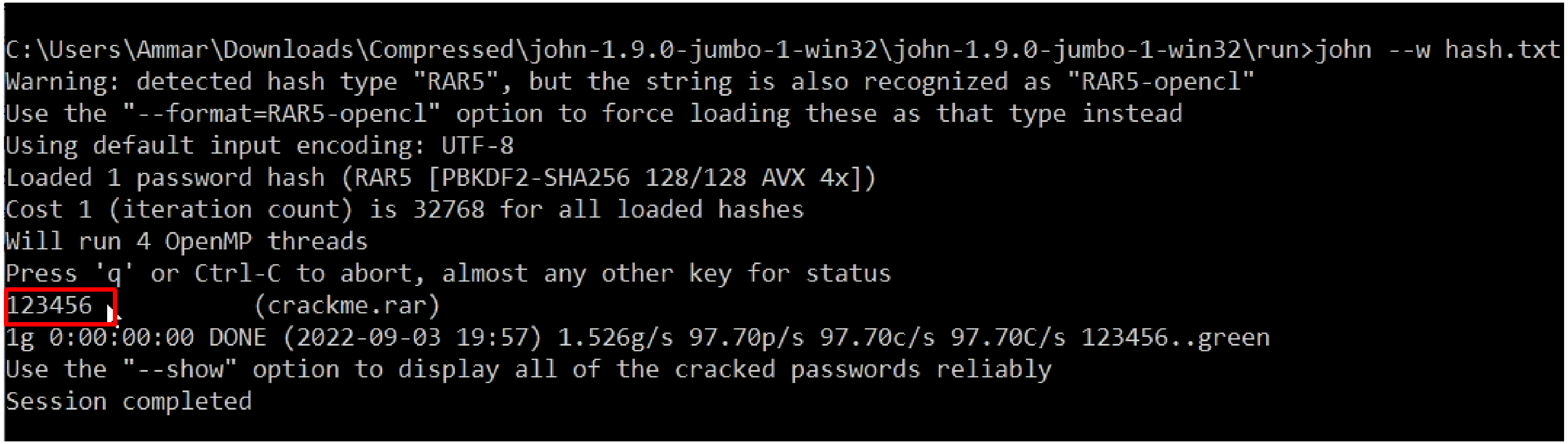
Here :

- Hash.txt file is the file that contains our hash for the document file
- Rockyou.txt is our dictionary file

Step- 4

- Now crack the password with following command

john --w=“rockyou.txt” hash.txt

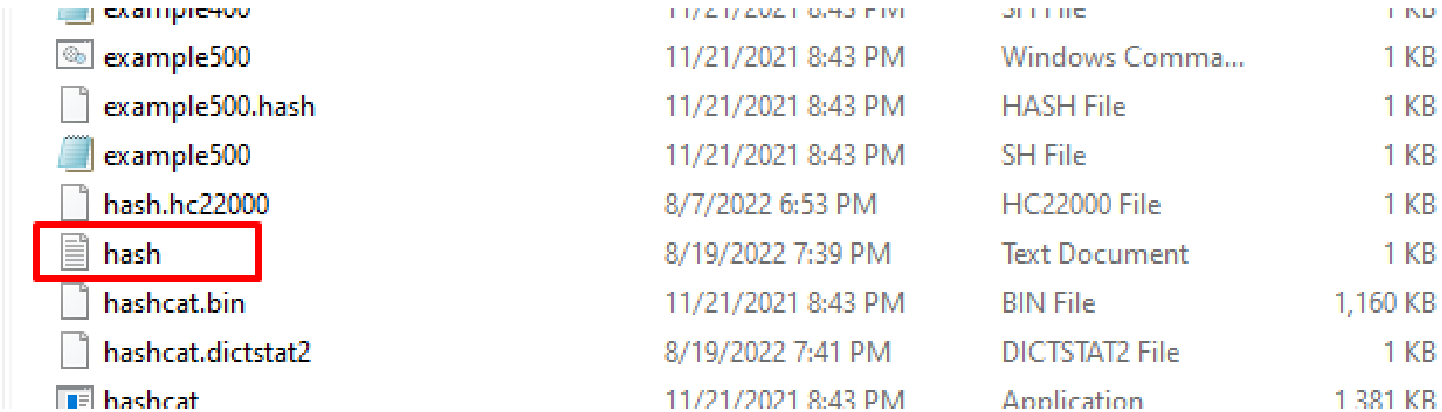


```
C:\Users\Ammar\Downloads\Compressed\john-1.9.0-jumbo-1-win32\john-1.9.0-jumbo-1-win32\run>john --w hash.txt
Warning: detected hash type "RAR5", but the string is also recognized as "RAR5-opencl"
Use the "--format=RAR5-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 128/128 AVX 4x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456           (crackme.rar)
1g 0:00:00:00 DONE (2022-09-03 19:57) 1.526g/s 97.70p/s 97.70c/s 97.70C/s 123456..green
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Crack RAR Password with Hashcat

Step- 4

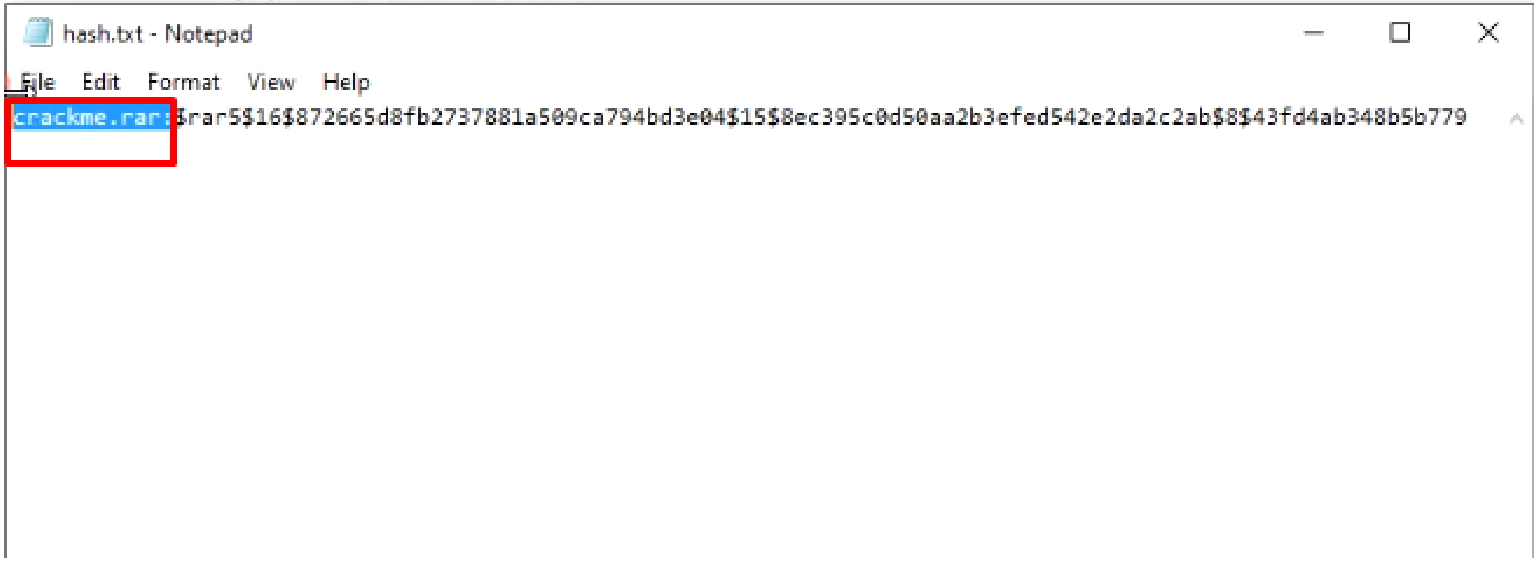
- Copy the hash file back to the Hashcat Directory



example400	11/21/2021 8:43 PM	SH File	1 KB
example500	11/21/2021 8:43 PM	Windows Comma...	1 KB
example500.hash	11/21/2021 8:43 PM	HASH File	1 KB
example500	11/21/2021 8:43 PM	SH File	1 KB
hash.hc22000	8/7/2022 6:53 PM	HC22000 File	1 KB
hash	8/19/2022 7:39 PM	Text Document	1 KB
hashcat.bin	11/21/2021 8:43 PM	BIN File	1,160 KB
hashcat.dictstat2	8/19/2022 7:41 PM	DICTSTAT2 File	1 KB
hashcat	11/21/2021 8:43 PM	Application	1,381 KB

Step- 5

- Now Open the hash.txt file and remove the file name from contents



```
crackme.rar:$rar5$16$872665d8fb2737881a509ca794bd3e04$15$8ec395c0d50aa2b3efed542e2da2c2ab$8$43fd4ab348b5b779
```

Step- 4

- Open the Power shell and then use the command to crack the handshake

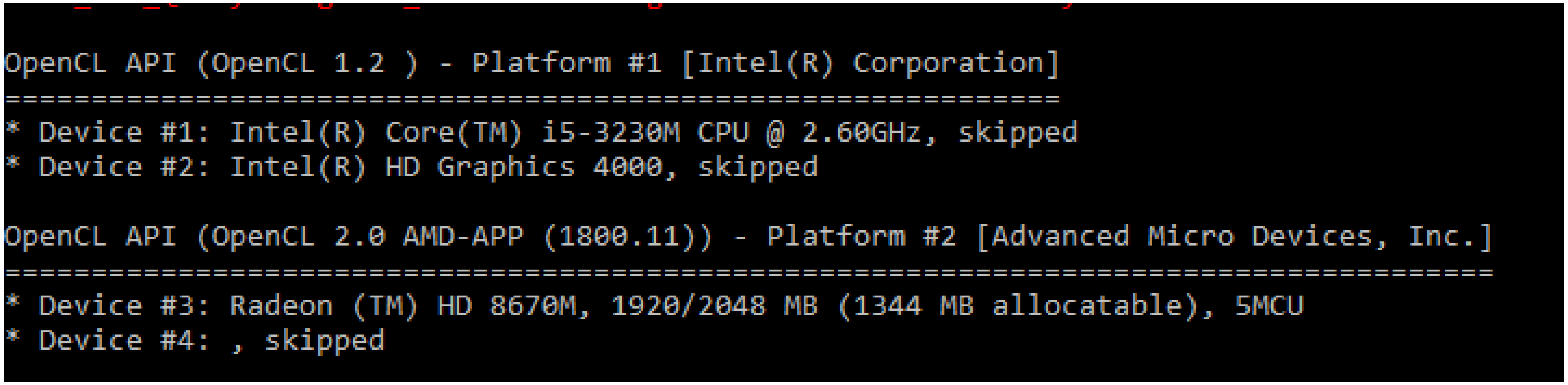
```
./hashcat -a 0 -m 13000 --status -o cracked.txt hash.txt rockyou.txt
```

Here :

- 13000 tells the hashcat that its rar5 password to be cracked
- Cracked.txt will store cracked passwords
- Hash.txt is the source file
- Rockyou.txt is the dictionary file

Step- 4 (Optional)

To select a particular device. Just select the device with category flag.



```
OpenCL API (OpenCL 1.2 ) - Platform #1 [Intel(R) Corporation]
=============================================================
* Device #1: Intel(R) Core(TM) i5-3230M CPU @ 2.60GHz, skipped
* Device #2: Intel(R) HD Graphics 4000, skipped

OpenCL API (OpenCL 2.0 AMD-APP (1800.11)) - Platform #2 [Advanced Micro Devices, Inc.]
======================================================================================
* Device #3: Radeon (TM) HD 8670M, 1920/2048 MB (1344 MB allocatable), 5MCU
* Device #4: , skipped
```

To select Device 3 only, use –D 2 –d 3

DEMO

THANKS