ISS Assignment 2

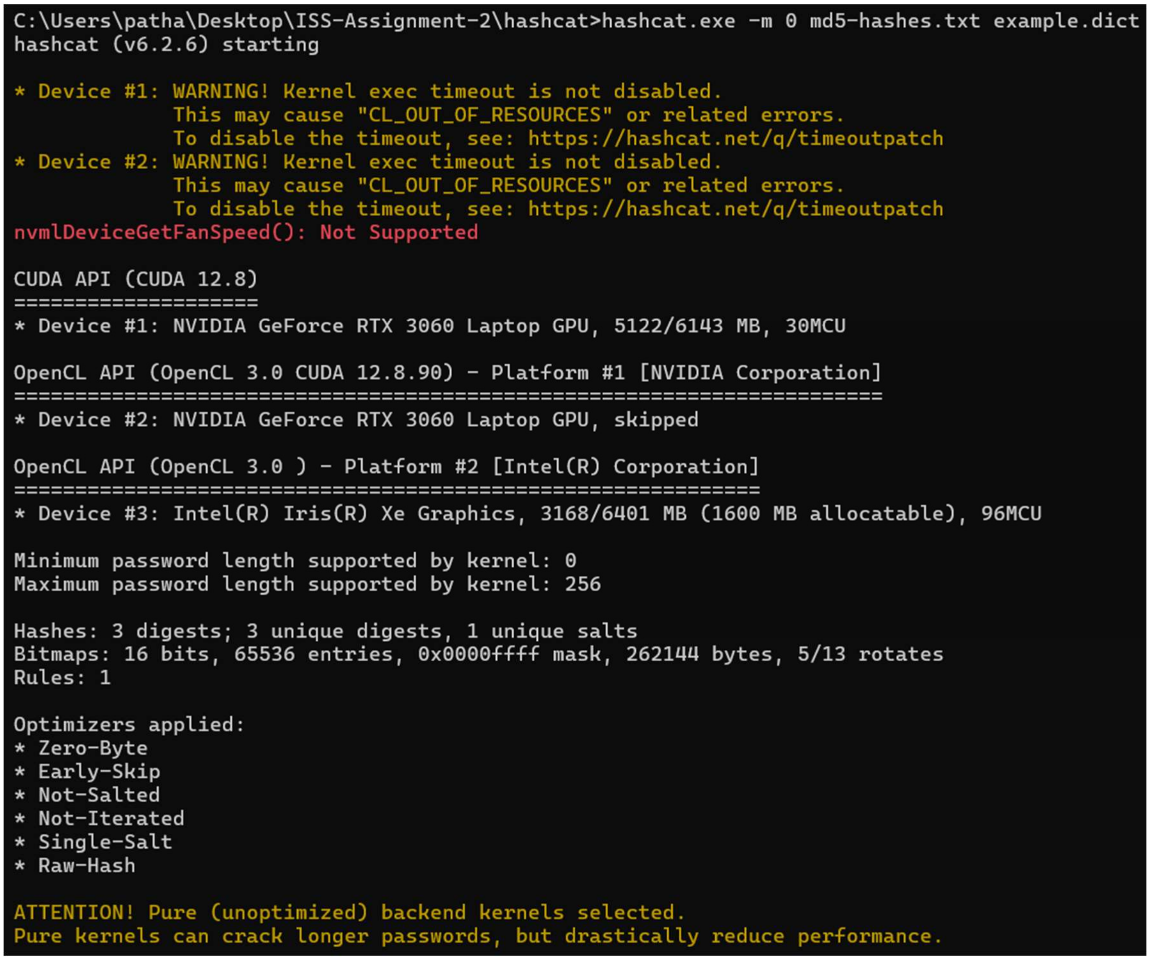
Name: Amrut Pathane

MIS: 112215132

1. **SubLab-1**: Cracking MD5 Password Hashes using Hashcat/John the Ripper
   MD5 examples shown for three users.
   student: 29e08fb7103c327d68327f23d8d9256c
   jsmith: f6a0cb102c62879d397b12b62c092c06
   jtripper: c8645ebb3300e01459f7554dcbee024f

   Crack the passwords of student, jsmith, and jtripper and include the screenshot in the report for each user.

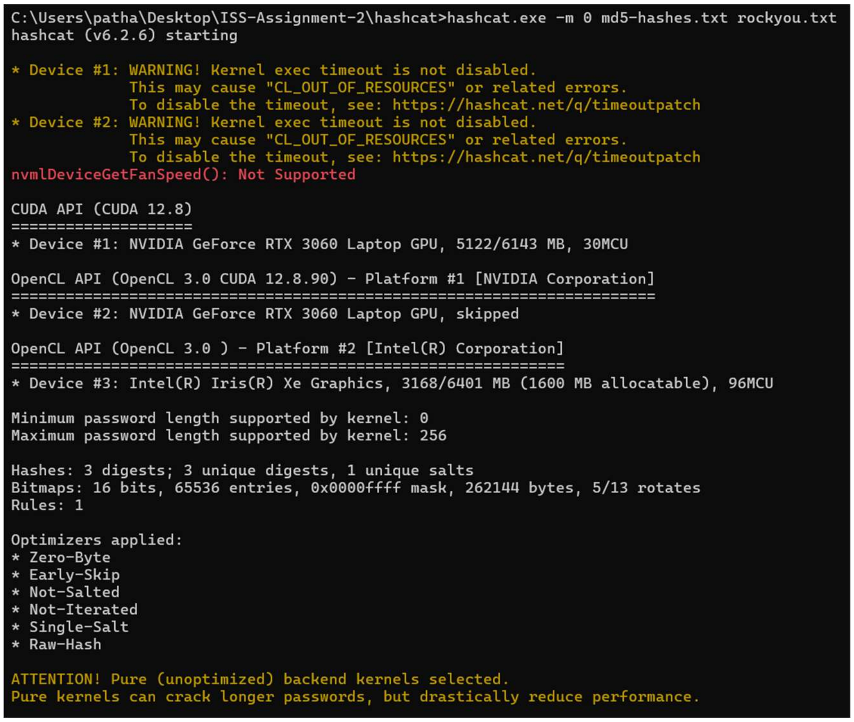
   a) Trying : hashcat.exe -m 0 md5-hashes.txt example.dict



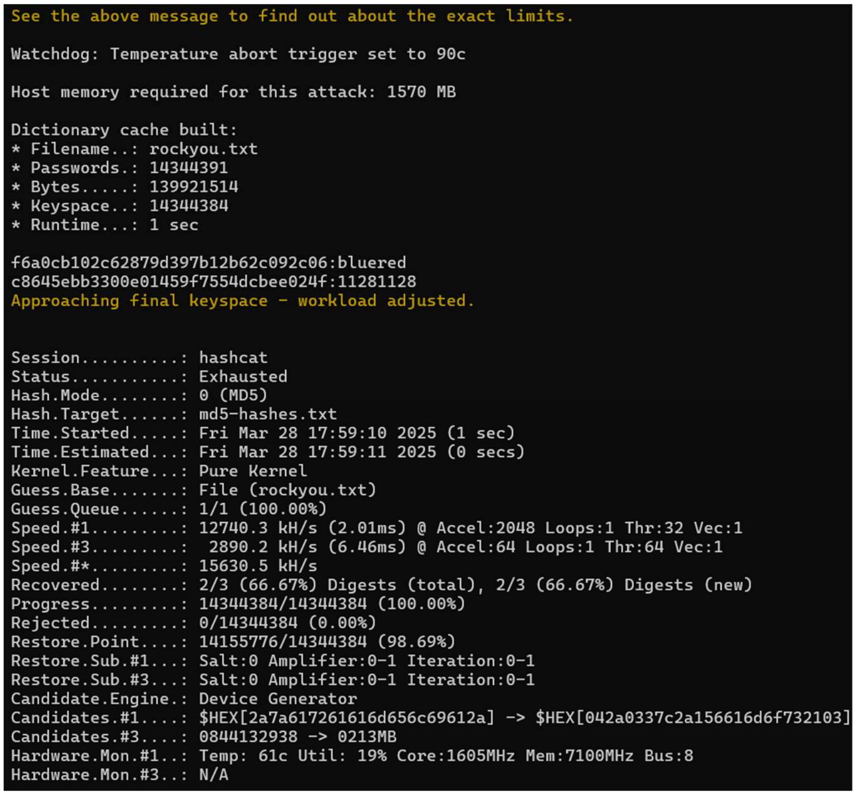
```
C:\Users\patha\Desktop\ISS-Assignment-2\hashcat>hashcat.exe -m 0 md5-hashes.txt example.dict
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported

CUDA API (CUDA 12.8)
====================
* Device #1: NVIDIA GeForce RTX 3060 Laptop GPU, 5122/6143 MB, 30MCU

OpenCL API (OpenCL 3.0 CUDA 12.8.90) - Platform #1 [NVIDIA Corporation]
=======================================================================
* Device #2: NVIDIA GeForce RTX 3060 Laptop GPU, skipped

OpenCL API (OpenCL 3.0 ) - Platform #2 [Intel(R) Corporation]
=============================================================
* Device #3: Intel(R) Iris(R) Xe Graphics, 3168/6401 MB (1600 MB allocatable), 96MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 3 digests; 3 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
```

   No Hashes Were Cracked using example.dict

b) Trying : hashcat.exe -m 0 md5-hashes.txt rockyou.txt



```
C:\Users\patha\Desktop\ISS-Assignment-2\hashcat>hashcat.exe -m 0 md5-hashes.txt rockyou.txt
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported

CUDA API (CUDA 12.8)
====================
* Device #1: NVIDIA GeForce RTX 3060 Laptop GPU, 5122/6143 MB, 30MCU

OpenCL API (OpenCL 3.0 CUDA 12.8.90) - Platform #1 [NVIDIA Corporation]
=======================================================================
* Device #2: NVIDIA GeForce RTX 3060 Laptop GPU, skipped

OpenCL API (OpenCL 3.0 ) - Platform #2 [Intel(R) Corporation]
=============================================================
* Device #3: Intel(R) Iris(R) Xe Graphics, 3168/6401 MB (1600 MB allocatable), 96MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 3 digests; 3 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
```



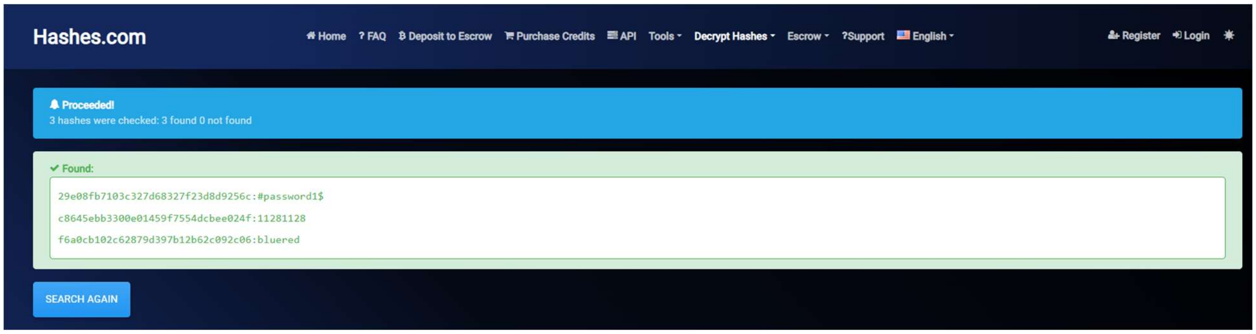
```
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1570 MB

Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921514
* Keyspace..: 14344384
* Runtime...: 1 sec

f6a0cb102c62879d397b12b62c092c06:bluered
c8645ebb3300e01459f7554dcbee024f:11281128
Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: md5-hashes.txt
Time.Started.....: Fri Mar 28 17:59:10 2025 (1 sec)
Time.Estimated...: Fri Mar 28 17:59:11 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 12740.3 kH/s (2.01ms) @ Accel:2048 Loops:1 Thr:32 Vec:1
Speed.#3.........:  2890.2 kH/s (6.46ms) @ Accel:64 Loops:1 Thr:64 Vec:1
Speed.#*.........: 15630.5 kH/s
Recovered........: 2/3 (66.67%) Digests (total), 2/3 (66.67%) Digests (new)
Progress.........: 14344384/14344384 (100.00%)
Rejected.........: 0/14344384 (0.00%)
Restore.Point....: 14155776/14344384 (98.69%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Restore.Sub.#3...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[2a7a617261616d656c69612a] -> $HEX[042a0337c2a156616d6f732103]
Candidates.#3....: 0844132938 -> 0213MB
Hardware.Mon.#1..: Temp: 61c Util: 19% Core:1605MHz Mem:7100MHz Bus:8
Hardware.Mon.#3..: N/A
```

Cracked 2 out of 3 MD5 hashes using rockyou.txt

f6a0cb102c62879d397b12b62c092c06:**bluered**

c8645ebb3300e01459f7554dcbee024f:**11281128**

c) Trying cracking the MD5 hashes from hashes.com :



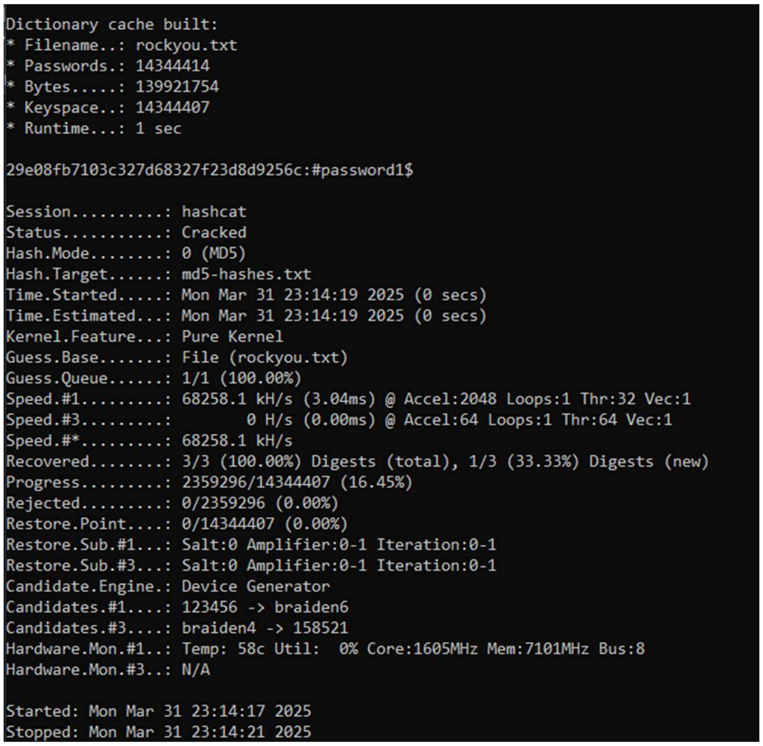
Proceeded!
3 hashes were checked: 3 found 0 not found

✓ Found:

```
29e08fb7103c327d68327f23d8d9256c:#password1$
c8645ebb3300e01459f7554dcbee024f:11281128
f6a0cb102c62879d397b12b62c092c06:bluered
```

Added password for student in rockyou.txt

d) Trying : hashcat.exe -m 0 md5-hashes.txt rockyou.txt



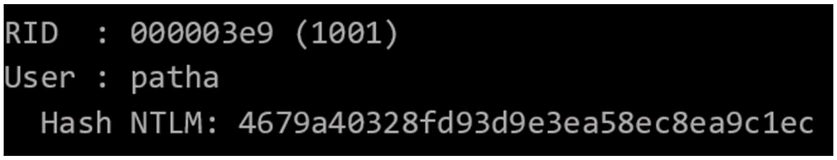
```
Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344414
* Bytes.....: 139921754
* Keyspace..: 14344407
* Runtime...: 1 sec

29e08fb7103c327d68327f23d8d9256c:#password1$

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: md5-hashes.txt
Time.Started.....: Mon Mar 31 23:14:19 2025 (0 secs)
Time.Estimated...: Mon Mar 31 23:14:19 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 68258.1 kH/s (3.04ms) @ Accel:2048 Loops:1 Thr:32 Vec:1
Speed.#3.........:        0 H/s (0.00ms) @ Accel:64 Loops:1 Thr:64 Vec:1
Speed.#*.........: 68258.1 kH/s
Recovered........: 3/3 (100.00%) Digests (total), 1/3 (33.33%) Digests (new)
Progress.........: 2359296/14344407 (16.45%)
Rejected.........: 0/2359296 (0.00%)
Restore.Point....: 0/14344407 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Restore.Sub.#3...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> braiden6
Candidates.#3....: braiden4 -> 158521
Hardware.Mon.#1..: Temp: 58c Util:  0% Core:1605MHz Mem:7101MHz Bus:8
Hardware.Mon.#3..: N/A

Started: Mon Mar 31 23:14:17 2025
Stopped: Mon Mar 31 23:14:21 2025
```

Cracked 29e08fb7103c327d68327f23d8d9256c:**#password1$**

Cracked passwords:

1. student: 29e08fb7103c327d68327f23d8d9256c => **#password1$**
2. jsmith: f6a0cb102c62879d397b12b62c092c06 => **11281128**
3. jtripper: c8645ebb3300e01459f7554dcbee024f => **bluered**

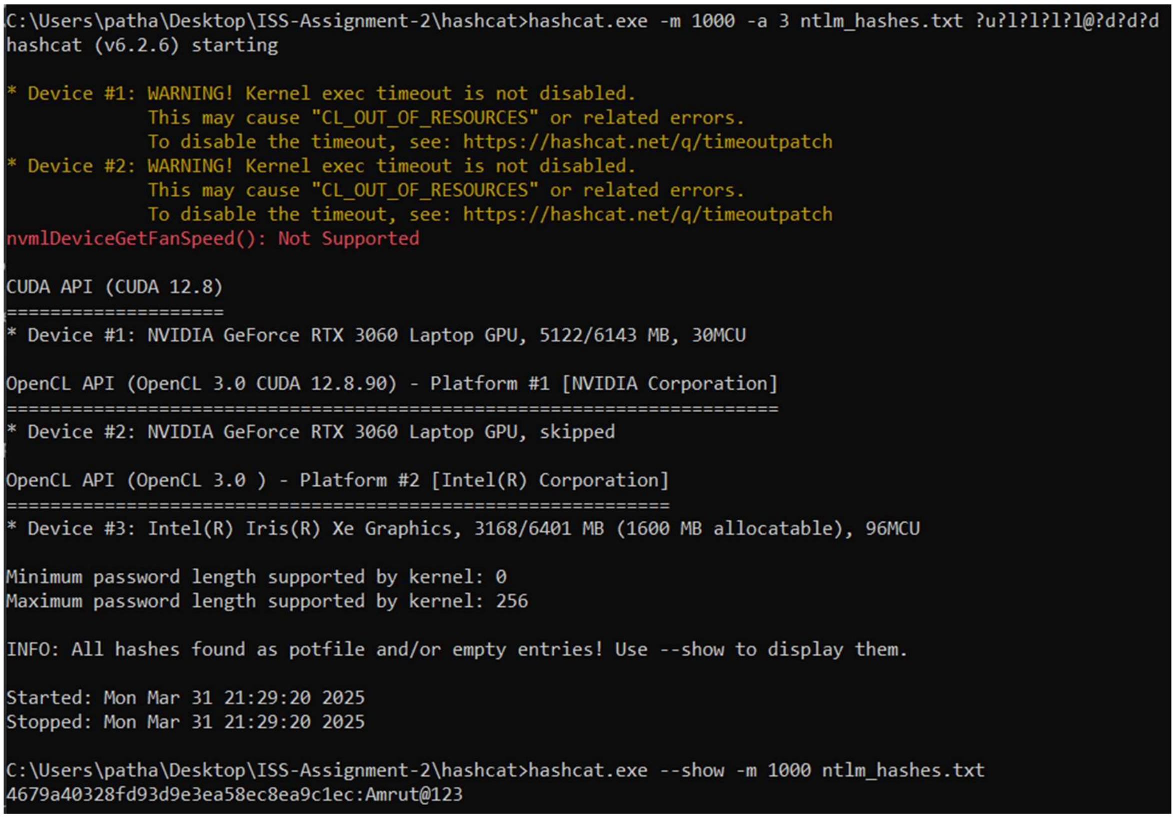
2. **SubLab-2:** Cracking Windows NTLM Password Hashes using Hashcat Extract the plain NTLM hash from your Windows OS and crack the password. Include the screenshots with username and cracked password. You can use existing dictionaries with rules, if password is not recovered then prepare a new dictionary with partial password and use best64.rule to crack it.



```
RID  : 000003e9 (1001)
User : patha
  Hash NTLM: 4679a40328fd93d9e3ea58ec8ea9c1ec
```

RID : 000003e9 (1001)
User : patha
Hash NTLM: 4679a40328fd93d9e3ea58ec8ea9c1ec

- NTLM hash cracked by brute force
  hashcat.exe -m 1000 -a 3 ntlm_hashes.txt ?u?l?l?l?l@?d?d?d



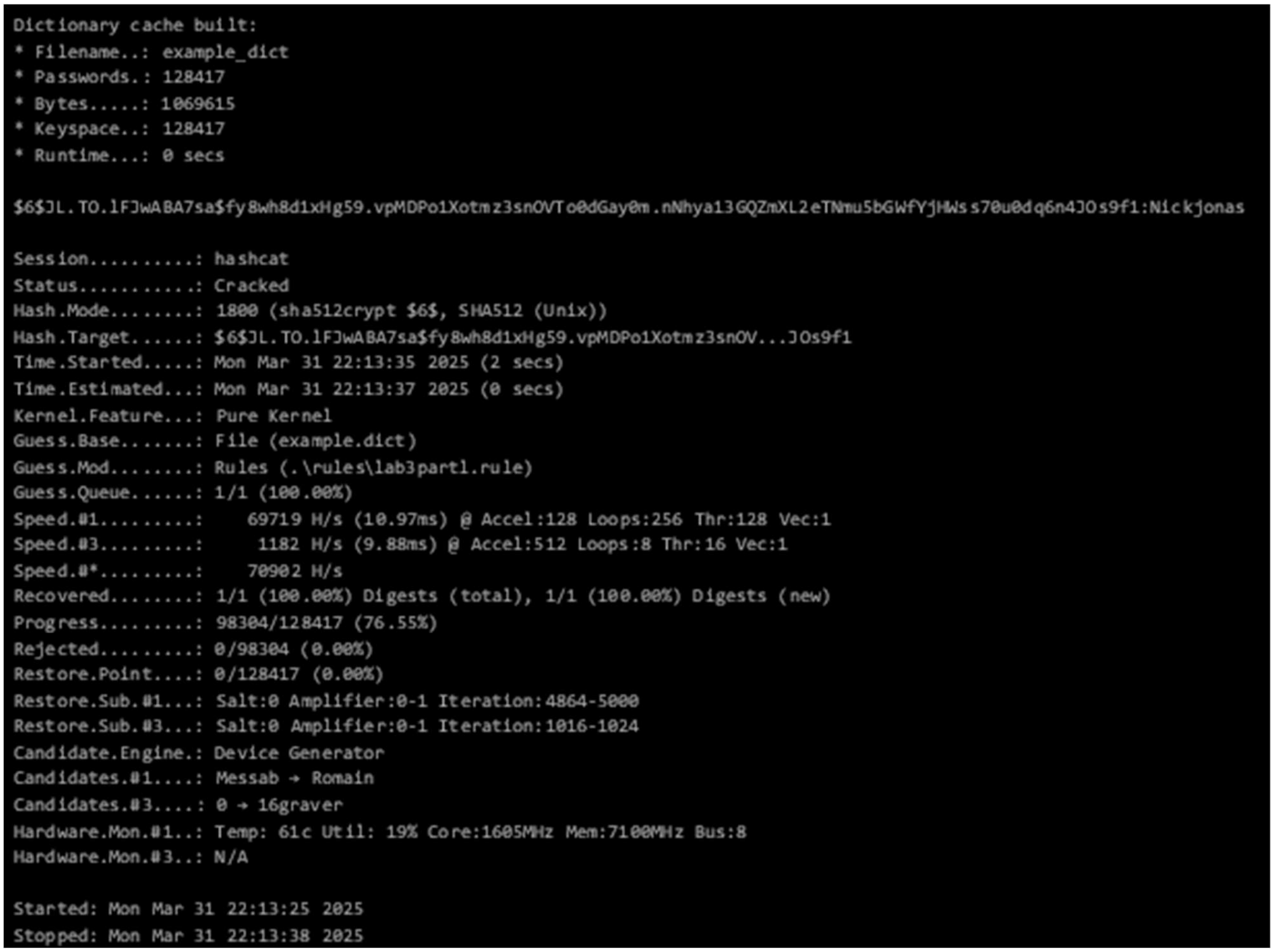
```
C:\Users\patha\Desktop\ISS-Assignment-2\hashcat>hashcat.exe -m 1000 -a 3 ntlm_hashes.txt ?u?l?l?l?l@?d?d?d
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported

CUDA API (CUDA 12.8)
====================
* Device #1: NVIDIA GeForce RTX 3060 Laptop GPU, 5122/6143 MB, 30MCU

OpenCL API (OpenCL 3.0 CUDA 12.8.90) - Platform #1 [NVIDIA Corporation]
=======================================================================
* Device #2: NVIDIA GeForce RTX 3060 Laptop GPU, skipped

OpenCL API (OpenCL 3.0 ) - Platform #2 [Intel(R) Corporation]
=============================================================
* Device #3: Intel(R) Iris(R) Xe Graphics, 3168/6401 MB (1600 MB allocatable), 96MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

INFO: All hashes found as potfile and/or empty entries! Use --show to display them.

Started: Mon Mar 31 21:29:20 2025
Stopped: Mon Mar 31 21:29:20 2025

C:\Users\patha\Desktop\ISS-Assignment-2\hashcat>hashcat.exe --show -m 1000 ntlm_hashes.txt
4679a40328fd93d9e3ea58ec8ea9c1ec:Amrut@123
```

Cracked password :
4679a40328fd93d9e3ea58ec8ea9c1ec:Amrut@123

3. **SubLab-3:** Cracking SHA512 Password Hashes using Hashcat/John the Ripper
   Since MD5 is considered "broken", Linux distributions have moved to using salted SHA512 password hashes (crypt id 6, i.e., $6$), which are several orders of magnitude more difficult to brute-force. Example lines from machine M2:

   a) root:$6$JL.TO.lFJwABA7sa$fy8wh8dIxHg59.vpWDPo1Xotmz3snOVTo0dG a y0m.nNhya13GQZmXu2eTNmu5bGMfYjHWss70u0dq6n4JOs9f1

      Hint: i. First letter of the password is in uppercase.
      ii. Use example.dict wordlist given in Google Classroom.



```
Dictionary cache built:
* Filename..: example_dict
* Passwords.: 128417
* Bytes.....: 1069615
* Keyspace..: 128417
* Runtime...: 0 secs

$6$JL.TO.lFJwABA7sa$fy8wh8d1xHg59.vpMDPo1Xotmz3snOVTo0dGay0m.nNhya13GQZmXL2eTNmu5bGWfYjHWss70u0dq6n4JOs9f1:Nickjonas

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$JL.TO.lFJwABA7sa$fy8wh8d1xHg59.vpMDPo1Xotmz3snOV...JOs9f1
Time.Started.....: Mon Mar 31 22:13:35 2025 (2 secs)
Time.Estimated...: Mon Mar 31 22:13:37 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (example.dict)
Guess.Mod........: Rules (.\rules\lab3part1.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    69719 H/s (10.97ms) @ Accel:128 Loops:256 Thr:128 Vec:1
Speed.#3.........:     1182 H/s (9.88ms) @ Accel:512 Loops:8 Thr:16 Vec:1
Speed.#*.........:    70902 H/s
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 98304/128417 (76.55%)
Rejected.........: 0/98304 (0.00%)
Restore.Point....: 0/128417 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4864-5000
Restore.Sub.#3...: Salt:0 Amplifier:0-1 Iteration:1016-1024
Candidate.Engine.: Device Generator
Candidates.#1....: Messab → Romain
Candidates.#3....: 0 → 16graver
Hardware.Mon.#1..: Temp: 61c Util: 19% Core:1605MHz Mem:7100MHz Bus:8
Hardware.Mon.#3..: N/A

Started: Mon Mar 31 22:13:25 2025
Stopped: Mon Mar 31 22:13:38 2025
```

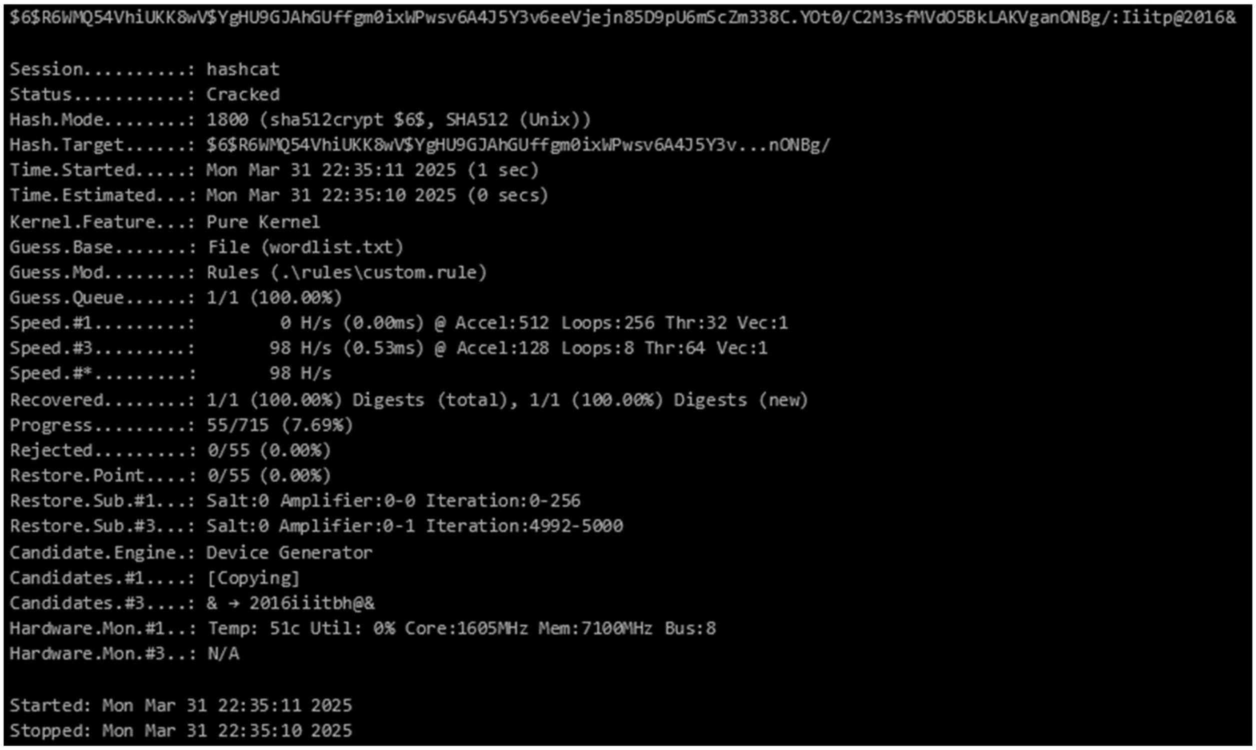
Cracked password : Nickjonas

b) iiit:$6$R6WMQ54VhiUKK8wV$YgHU9GJAhGUffgm0ixWPwsv6A4J5Y3v6eeVje jn85D9pU6mScZm338C.YOt0/C2M3sfMVdO5BkLAKVganONBg/

Hint:

i. The password consists of iiitv or iiitp or iiitbh, special character i.e @ and 2014 or 2015 or 2016 in any order. One letter is in uppercase. Create your own directory.

ii. The password ends with &. Use existing or create your rule.



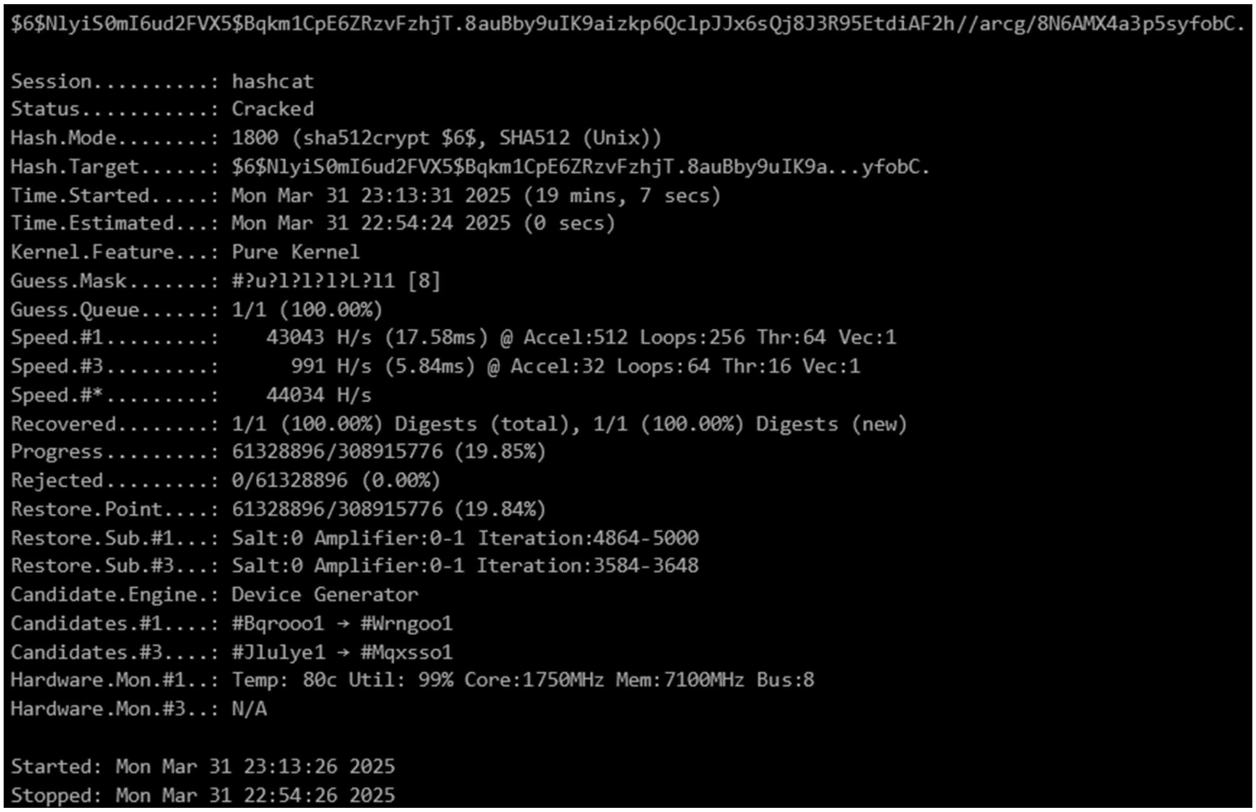
```
$6$R6WMQ54VhiUKK8wV$YgHU9GJAhGUffgm0ixWPwsv6A4J5Y3v6eeVjejn85D9pU6mScZm338C.YOt0/C2M3sfMVdO5BkLAKVganONBg/:Iiitp@2016&

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$R6WMQ54VhiUKK8wV$YgHU9GJAhGUffgm0ixWPwsv6A4J5Y3v...nONBg/
Time.Started.....: Mon Mar 31 22:35:11 2025 (1 sec)
Time.Estimated...: Mon Mar 31 22:35:10 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (wordlist.txt)
Guess.Mod........: Rules (.\rules\custom.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:        0 H/s (0.00ms) @ Accel:512 Loops:256 Thr:32 Vec:1
Speed.#3.........:       98 H/s (0.53ms) @ Accel:128 Loops:8 Thr:64 Vec:1
Speed.#*.........:       98 H/s
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 55/715 (7.69%)
Rejected.........: 0/55 (0.00%)
Restore.Point....: 0/55 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-0 Iteration:0-256
Restore.Sub.#3...: Salt:0 Amplifier:0-1 Iteration:4992-5000
Candidate.Engine.: Device Generator
Candidates.#1....: [Copying]
Candidates.#3....: & → 2016iiitbh@&
Hardware.Mon.#1..: Temp: 51c Util: 0% Core:1605MHz Mem:7100MHz Bus:8
Hardware.Mon.#3..: N/A

Started: Mon Mar 31 22:35:11 2025
Stopped: Mon Mar 31 22:35:10 2025
```

Cracked password : Iiitp@2016&

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

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.

Hint: Use mask instead of dictionary/wordlist.



```
$6$NlyiS0mI6ud2FVX5$Bqkm1CpE6ZRzvFzhjT.8auBby9uIK9aizkp6QclpJJx6sQj8J3R95EtdiAF2h//arcg/8N6AMX4a3p5syfobC.

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$NlyiS0mI6ud2FVX5$Bqkm1CpE6ZRzvFzhjT.8auBby9uIK9a...yfobC.
Time.Started.....: Mon Mar 31 23:13:31 2025 (19 mins, 7 secs)
Time.Estimated...: Mon Mar 31 22:54:24 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: #?u?l?l?l?L?l1 [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    43043 H/s (17.58ms) @ Accel:512 Loops:256 Thr:64 Vec:1
Speed.#3.........:      991 H/s (5.84ms) @ Accel:32 Loops:64 Thr:16 Vec:1
Speed.#*.........:    44034 H/s
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 61328896/308915776 (19.85%)
Rejected.........: 0/61328896 (0.00%)
Restore.Point....: 61328896/308915776 (19.84%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4864-5000
Restore.Sub.#3...: Salt:0 Amplifier:0-1 Iteration:3584-3648
Candidate.Engine.: Device Generator
Candidates.#1....: #Bqrooo1 → #Wrngoo1
Candidates.#3....: #Jlulye1 → #Mqxsso1
Hardware.Mon.#1..: Temp: 80c Util: 99% Core:1750MHz Mem:7100MHz Bus:8
Hardware.Mon.#3..: N/A

Started: Mon Mar 31 23:13:26 2025
Stopped: Mon Mar 31 22:54:26 2025
```

Cracked password : #Jazzis1