# ITIS 6167/8167: Network Security

# Bonus Project

**Divyansh Jain**

**801364884**

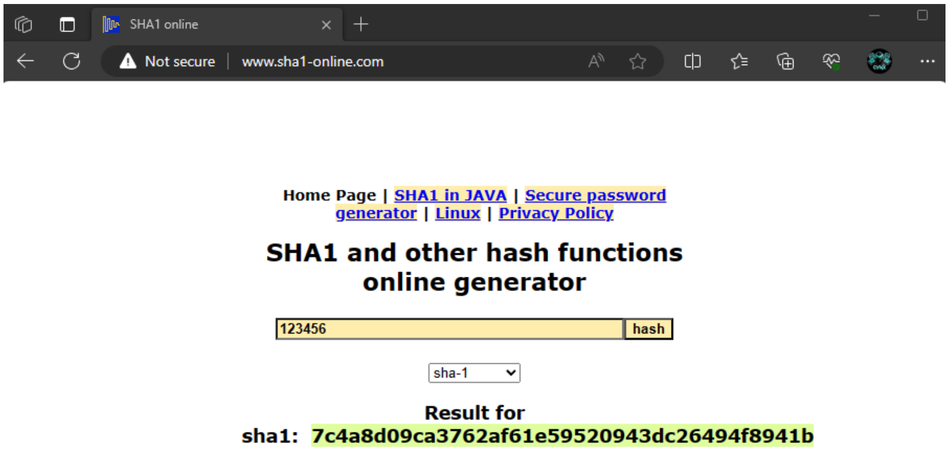
**03-Dec-2023**

## Introduction:

In the realm of cybersecurity, the importance of robust password security cannot be overstated. Unfortunately, users often compromise their security by employing weak password practices. In this project, we are presented with a challenge: a password file named "password_sha1_DJ.txt" containing SHA-1 hashed passwords in the format [User ID] [SPACE] [SHA-1 Hash of The User's Password]. Our mission is to crack as many passwords as possible, leveraging our knowledge of common bad practices in password creation.

To tackle this task, we will combine the power of Hashcat, a widely used password recovery tool, with the flexibility of Python scripting. Hashcat excels in efficiently cracking hashed passwords through a variety of attack modes, while Python allows us to implement customized strategies and leverage additional tools.

## Verification:


SHA1 online
Not secure
www.sha1-online.com
Home Page | SHA1 in JAVA | Secure password generator | Linux | Privacy Policy
hash

SHA1 and other hash functions online generator

123456

sha-1

Result for
sha1: 7c4a8d09ca3762af61e59520943dc26494f8941b

*Fig 1: Verification*

## Method Used:

### Hashcat Setup:

- Install and configure Hashcat, a powerful password recovery tool, on the chosen system.
- Utilize Hashcat's capabilities to support various attack modes, including dictionary attacks, brute force attacks, and Combinator Attack.

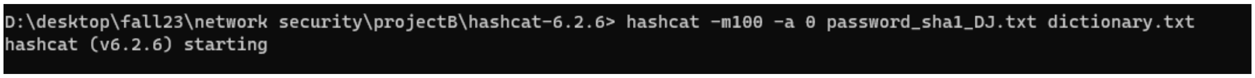
### Dictionary Attack:

- Employ Python to generate password candidates by combining words from "dictionary.txt" with known patterns (digits, symbols).
- Feed the generated passwords to Hashcat for hashing and comparison with the entries in "passwords.txt."

### Combinator Attack:

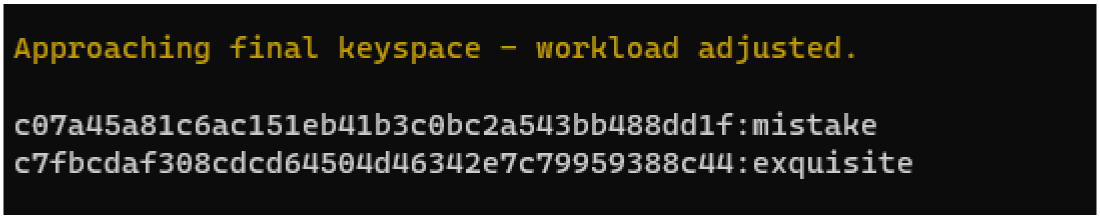
- Develop Python scripts to intelligently combine elements (words, digits, symbols) based on observed patterns.
- Integrate these scripts with Hashcat to efficiently explore likely password structures.

## Cracking hashes:



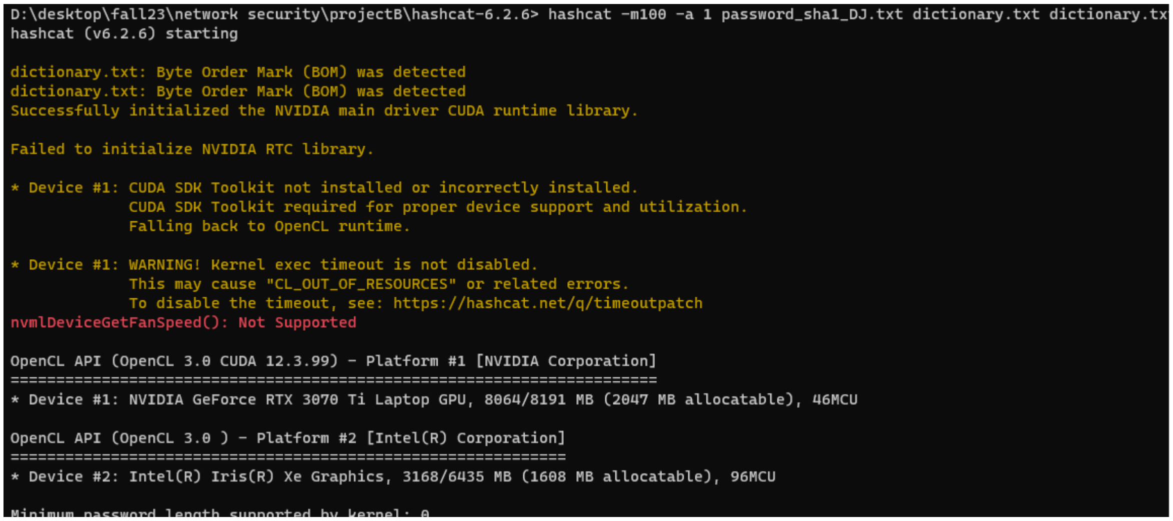
```
D:\desktop\fall23\network security\projectB\hashcat-6.2.6> hashcat -m100 -a 0 password_sha1_DJ.txt dictionary.txt
hashcat (v6.2.6) starting
```

*Fig 1: Cracking single word password hashcat command*



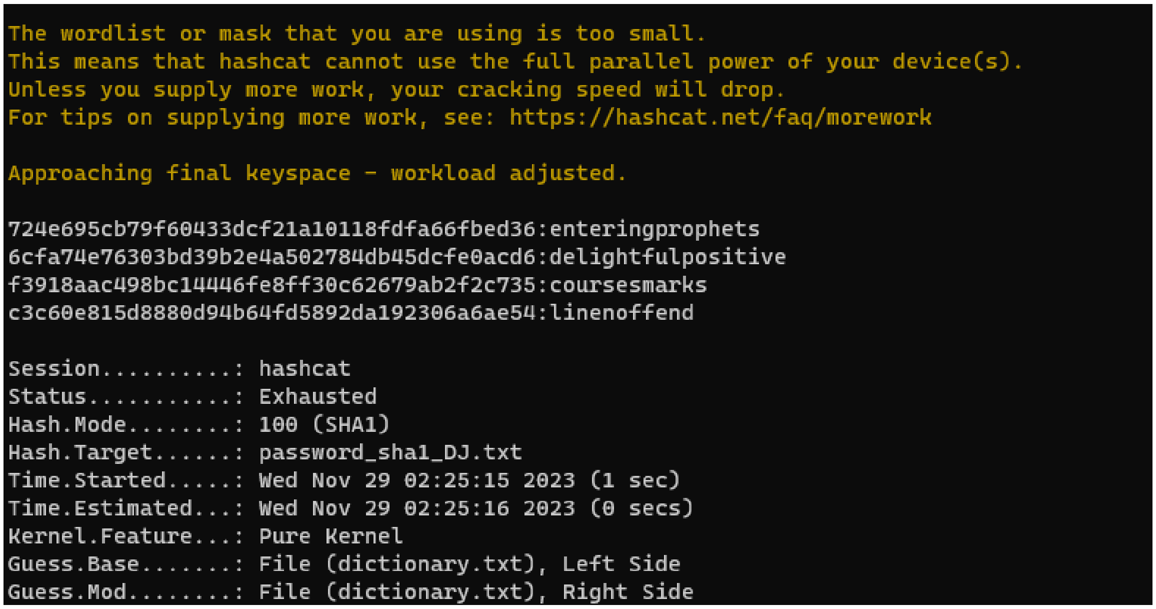
```
Approaching final keyspace - workload adjusted.

c07a45a81c6ac151eb41b3c0bc2a543bb488dd1f:mistake
c7fbcdaf308cdcd64504d46342e7c79959388c44:exquisite
```

*Fig 2: Cracked single word passwords*



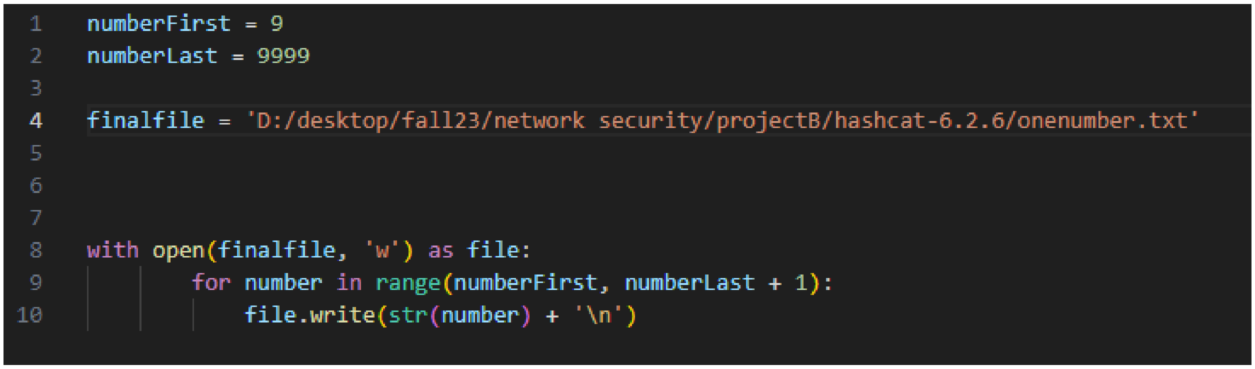
```
D:\desktop\fall23\network security\projectB\hashcat-6.2.6> hashcat -m100 -a 1 password_sha1_DJ.txt dictionary.txt dictionary.tx
hashcat (v6.2.6) starting

dictionary.txt: Byte Order Mark (BOM) was detected
dictionary.txt: Byte Order Mark (BOM) was detected
Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
             CUDA SDK Toolkit required for proper device support and utilization.
             Falling back to OpenCL runtime.

* 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
nvmlDeviceGetFanSpeed(): Not Supported

OpenCL API (OpenCL 3.0 CUDA 12.3.99) - Platform #1 [NVIDIA Corporation]
=======================================================================
* Device #1: NVIDIA GeForce RTX 3070 Ti Laptop GPU, 8064/8191 MB (2047 MB allocatable), 46MCU

OpenCL API (OpenCL 3.0 ) - Platform #2 [Intel(R) Corporation]
=============================================================
* Device #2: Intel(R) Iris(R) Xe Graphics, 3168/6435 MB (1608 MB allocatable), 96MCU

Minimum password length supported by kernel: 0
```

*Fig 3: Cracking double word password with hashcat command*



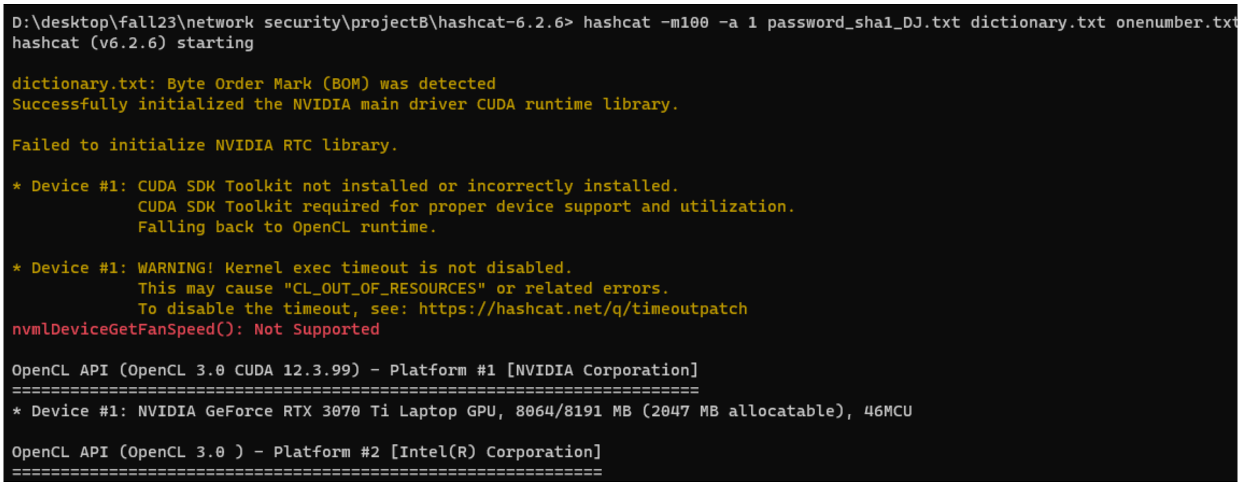
```
The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

724e695cb79f60433dcf21a10118fdfa66fbed36:enteringprophets
6cfa74e76303bd39b2e4a502784db45dcfe0acd6:delightfulpositive
f3918aac498bc14446fe8ff30c62679ab2f2c735:coursesmarks
c3c60e815d8880d94b64fd5892da192306a6ae54:linenoffend

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 100 (SHA1)
Hash.Target......: password_sha1_DJ.txt
Time.Started.....: Wed Nov 29 02:25:15 2023 (1 sec)
Time.Estimated...: Wed Nov 29 02:25:16 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (dictionary.txt), Left Side
Guess.Mod........: File (dictionary.txt), Right Side
```

*Fig 4: Double word password cracked*



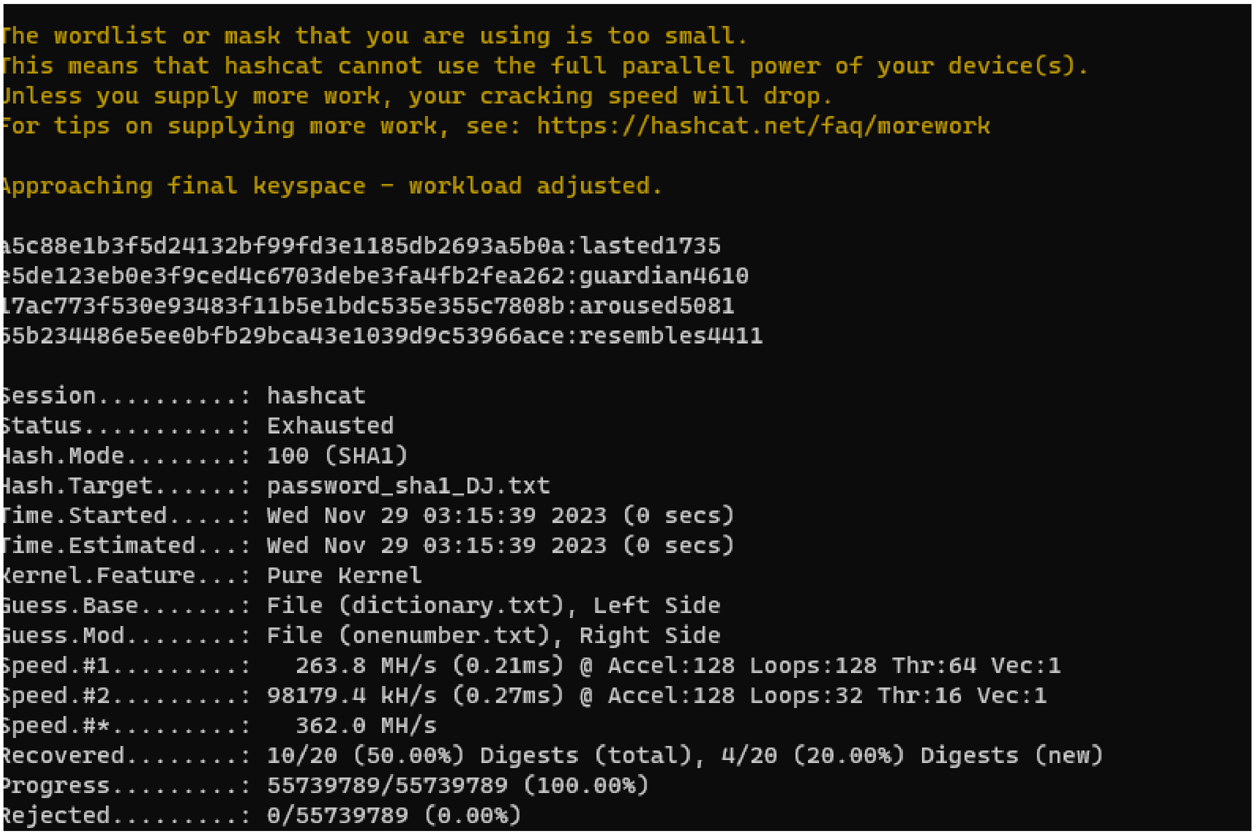
```python
numberFirst = 9
numberLast = 9999

finalfile = 'D:/desktop/fall23/network security/projectB/hashcat-6.2.6/onenumber.txt'



with open(finalfile, 'w') as file:
    for number in range(numberFirst, numberLast + 1):
        file.write(str(number) + '\n')
```

*Fig 5: Number generator python file*



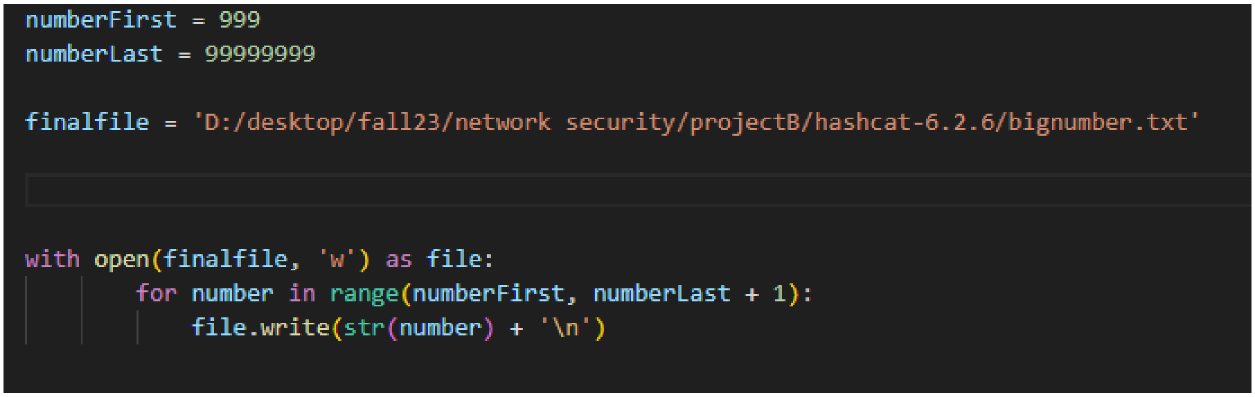
```
D:\desktop\fall23\network security\projectB\hashcat-6.2.6> hashcat -m100 -a 1 password_sha1_DJ.txt dictionary.txt onenumber.txt
hashcat (v6.2.6) starting

dictionary.txt: Byte Order Mark (BOM) was detected
Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
             CUDA SDK Toolkit required for proper device support and utilization.
             Falling back to OpenCL runtime.

* 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
nvmlDeviceGetFanSpeed(): Not Supported

OpenCL API (OpenCL 3.0 CUDA 12.3.99) - Platform #1 [NVIDIA Corporation]
=======================================================================
* Device #1: NVIDIA GeForce RTX 3070 Ti Laptop GPU, 8064/8191 MB (2047 MB allocatable), 46MCU

OpenCL API (OpenCL 3.0 ) - Platform #2 [Intel(R) Corporation]
=============================================================
```

*Fig 6: Cracking single word and number password with hashcat command*



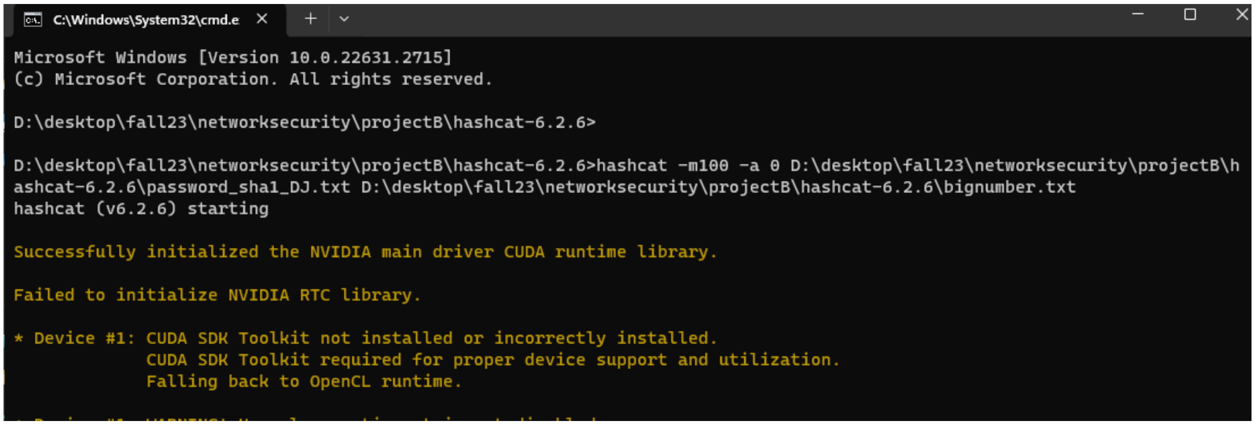
```
The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

a5c88e1b3f5d24132bf99fd3e1185db2693a5b0a:lasted1735
e5de123eb0e3f9ced4c6703debe3fa4fb2fea262:guardian4610
17ac773f530e93483f11b5e1bdc535e355c7808b:aroused5081
55b234486e5ee0bfb29bca43e1039d9c53966ace:resembles4411

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 100 (SHA1)
Hash.Target......: password_sha1_DJ.txt
Time.Started.....: Wed Nov 29 03:15:39 2023 (0 secs)
Time.Estimated...: Wed Nov 29 03:15:39 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (dictionary.txt), Left Side
Guess.Mod........: File (onenumber.txt), Right Side
Speed.#1.........:   263.8 MH/s (0.21ms) @ Accel:128 Loops:128 Thr:64 Vec:1
Speed.#2.........: 98179.4 kH/s (0.27ms) @ Accel:128 Loops:32 Thr:16 Vec:1
Speed.#*.........:   362.0 MH/s
Recovered........: 10/20 (50.00%) Digests (total), 4/20 (20.00%) Digests (new)
Progress.........: 55739789/55739789 (100.00%)
Rejected.........: 0/55739789 (0.00%)
```

*Fig 7: Cracked single word and number password*



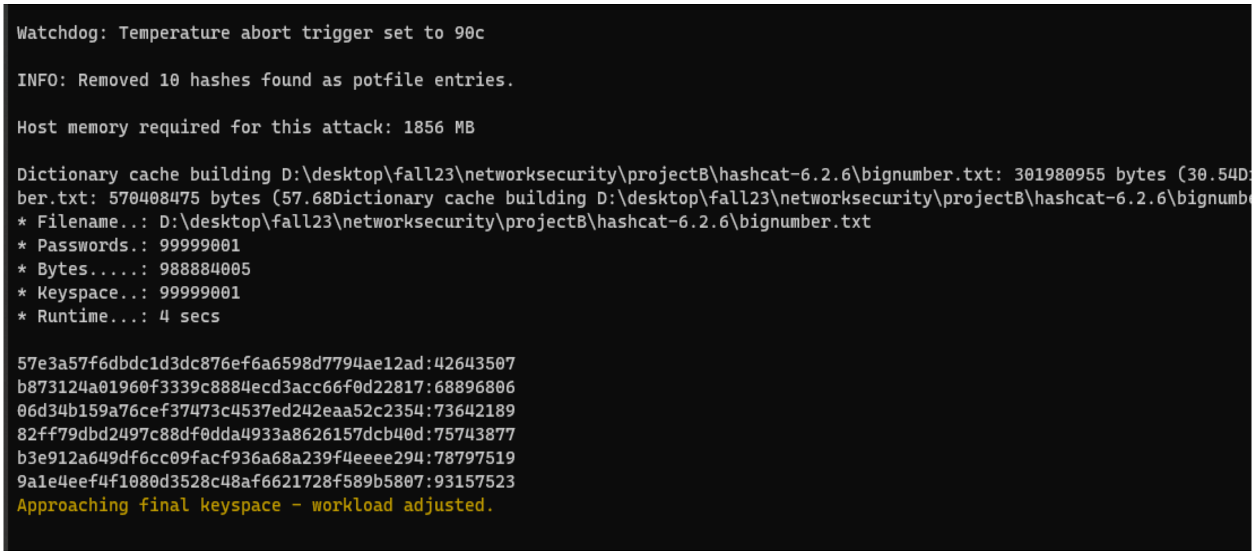
```python
numberFirst = 999
numberLast = 99999999

finalfile = 'D:/desktop/fall23/network security/projectB/hashcat-6.2.6/bignumber.txt'


with open(finalfile, 'w') as file:
        for number in range(numberFirst, numberLast + 1):
            file.write(str(number) + '\n')
```

*Fig 8: Number generator python file*



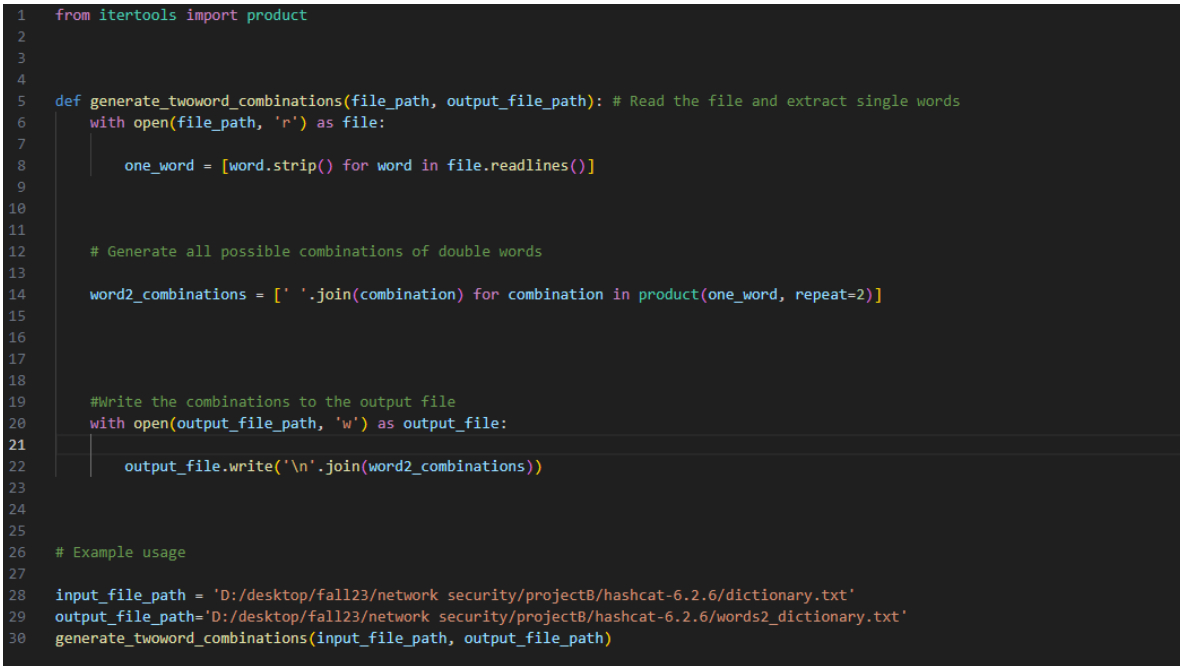
```
Microsoft Windows [Version 10.0.22631.2715]
(c) Microsoft Corporation. All rights reserved.

D:\desktop\fall23\networksecurity\projectB\hashcat-6.2.6>

D:\desktop\fall23\networksecurity\projectB\hashcat-6.2.6>hashcat -m100 -a 0 D:\desktop\fall23\networksecurity\projectB\h
ashcat-6.2.6\password_sha1_DJ.txt D:\desktop\fall23\networksecurity\projectB\hashcat-6.2.6\bignumber.txt
hashcat (v6.2.6) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
             CUDA SDK Toolkit required for proper device support and utilization.
             Falling back to OpenCL runtime.
```

*Fig 9: Cracking numbers only password with hashcat command*



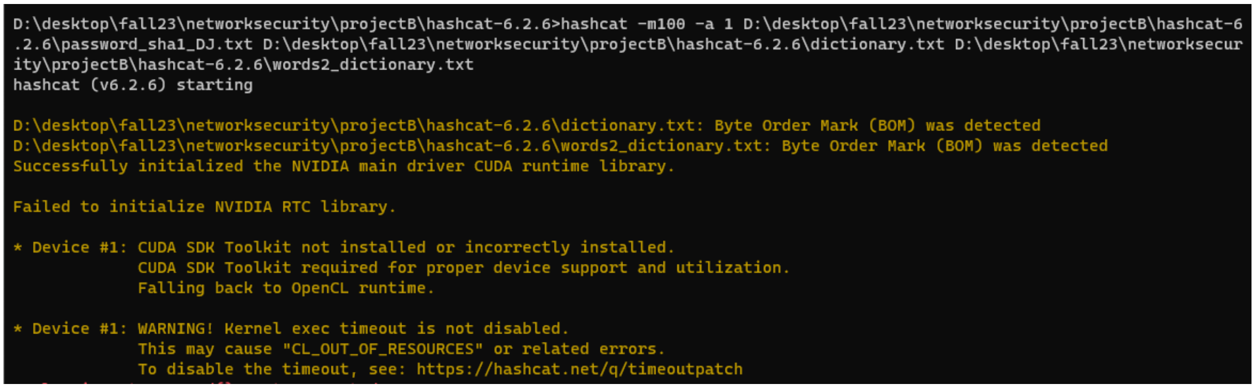
```
Watchdog: Temperature abort trigger set to 90c

INFO: Removed 10 hashes found as potfile entries.

Host memory required for this attack: 1856 MB

Dictionary cache building D:\desktop\fall23\networksecurity\projectB\hashcat-6.2.6\bignumber.txt: 301980955 bytes (30.54D:
ber.txt: 570408475 bytes (57.68Dictionary cache building D:\desktop\fall23\networksecurity\projectB\hashcat-6.2.6\bignumbe
* Filename..: D:\desktop\fall23\networksecurity\projectB\hashcat-6.2.6\bignumber.txt
* Passwords.: 99999001
* Bytes.....: 988884005
* Keyspace..: 99999001
* Runtime...: 4 secs

57e3a57f6dbdc1d3dc876ef6a6598d7794ae12ad:42643507
b873124a01960f3339c8884ecd3acc66f0d22817:68896806
06d34b159a76cef37473c4537ed242eaa52c2354:73642189
82ff79dbd2497c88df0dda4933a8626157dcb40d:75743877
b3e912a649df6cc09facf936a68a239f4eeee294:78797519
9a1e4eef4f1080d3528c48af6621728f589b5807:93157523
Approaching final keyspace - workload adjusted.
```

*Fig 10: Numbers only password cracked*



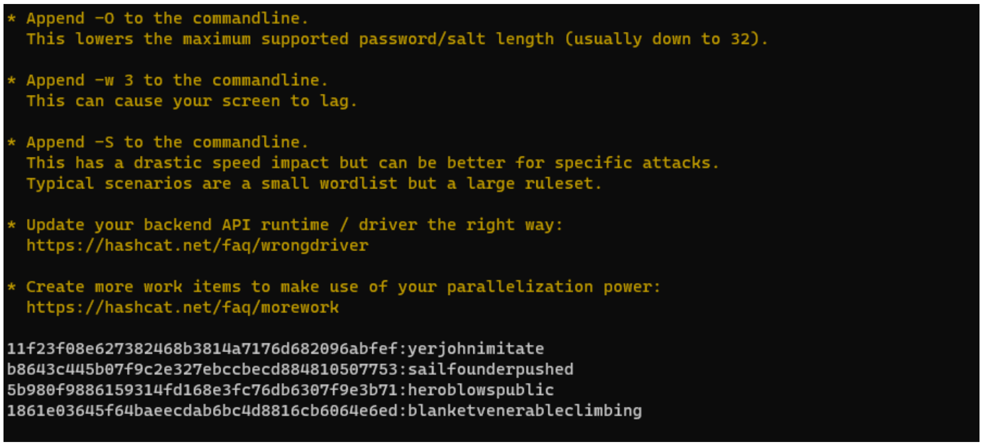
```python
from itertools import product



def generate_twoword_combinations(file_path, output_file_path): # Read the file and extract single words
    with open(file_path, 'r') as file:

        one_word = [word.strip() for word in file.readlines()]



    # Generate all possible combinations of double words

    word2_combinations = [' '.join(combination) for combination in product(one_word, repeat=2)]




    #Write the combinations to the output file
    with open(output_file_path, 'w') as output_file:

        output_file.write('\n'.join(word2_combinations))




# Example usage

input_file_path = 'D:/desktop/fall23/network security/projectB/hashcat-6.2.6/dictionary.txt'
output_file_path='D:/desktop/fall23/network security/projectB/hashcat-6.2.6/words2_dictionary.txt'
generate_twoword_combinations(input_file_path, output_file_path)
```

*Fig 11: Double words generator python file*



```
D:\desktop\fall23\networksecurity\projectB\hashcat-6.2.6>hashcat -m100 -a 1 D:\desktop\fall23\networksecurity\projectB\hashcat-6
.2.6\password_sha1_DJ.txt D:\desktop\fall23\networksecurity\projectB\hashcat-6.2.6\dictionary.txt D:\desktop\fall23\networksecur
ity\projectB\hashcat-6.2.6\words2_dictionary.txt
hashcat (v6.2.6) starting

D:\desktop\fall23\networksecurity\projectB\hashcat-6.2.6\dictionary.txt: Byte Order Mark (BOM) was detected
D:\desktop\fall23\networksecurity\projectB\hashcat-6.2.6\words2_dictionary.txt: Byte Order Mark (BOM) was detected
Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
             CUDA SDK Toolkit required for proper device support and utilization.
             Falling back to OpenCL runtime.

* 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
```

*Fig 12: Triple word password cracking with hashcat command*



```
* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

11f23f08e627382468b3814a7176d682096abfef:yerjohnimitate
b8643c445b07f9c2e327ebccbecd884810507753:sailfounderpushed
5b980f9886159314fd168e3fc76db6307f9e3b71:heroblowspublic
1861e03645f64baeecdab6bc4d8816cb6064e6ed:blanketvenerableclimbing
```

*Fig 13: Triple word password cracked*

## Final Results:

c07a45a81c6ac151eb41b3c0bc2a543bb488dd1f: mistake

c7fbcdaf308cdcd64504d46342e7c79959388c44: exquisite

724e695cb79f60433dcf21a10118fdfa66fbed36: enteringprophets

6cfa74e76303bd39b2e4a502784db45dcfe0acd6: delightfulpositive

f3918aac498bc14446fe8ff30c62679ab2f2c735: coursesmarks

c3c60e815d8880d94b64fd5892da192306a6ae54: linenoffend

a5c88e1b3f5d24132bf99fd3e1185db2693a5b0a: lasted1735

e5de123eb0e3f9ced4c6703debe3fa4fb2fea262: guardian4610

17ac773f530e93483f11b5e1bdc535e355c7808b: aroused5081

55b234486e5ee0bfb29bca43e1039d9c53966ace: resembles4411

57e3a57f6dbdc1d3dc876ef6a6598d7794ae12ad: 42643507

b873124a01960f3339c8884ecd3acc66f0d22817: 68896806

06d34b159a76cef37473c4537ed242eaa52c2354: 73642189

82ff79dbd2497c88df0dda4933a8626157dcb40d: 75743877

b3e912a649df6cc09facf936a68a239f4eeee294: 78797519

9a1e4eef4f1080d3528c48af6621728f589b5807: 93157523

11f23f08e627382468b3814a7176d682096abfef: yerjohnimitate

b8643c445b07f9c2e327ebccbecd884810507753: sailfounderpushed

5b980f9886159314fd168e3fc76db6307f9e3b71: heroblowspublic

1861e03645f64baeecdab6bc4d8816cb6064e6ed: blanketvenerableclimbing