Vellore Institute of Technology
(Deemed to be University under section 3 of the UGC Act, 1956)

WINTER SEMESTER 2019-20
DIGITAL FORENSICS (CSE4004)
LAB ASSIGNMENT - 8

Dishi Jain
17BCB0055

HASHCAT – Software Forensics Tool

- Hashcat is a well-known password cracker. It is designed to break even the most complex passwords. To do this, it enables the cracking of a specific password in multiple ways, combined with versatility and speed.
- Password representations are primarily associated with hash keys, such as MD5, SHA, WHIRLPOOL, RipeMD, etc. They are also defined as a one-way function — this is a mathematical operation that is easy to perform, but very difficult to reverse engineer.
- Hashcat turns readable data into a garbled state (this is a random string of fixed length size). Hashes do not allow someone to decrypt data with a specific key, as standard encryption protocols allow.
- It uses precomputed dictionaries, rainbow tables, and even a brute-force approach to find an effective and efficient way crack passwords.
- It is possible to resume or limit sessions automatically. They recognize recovered hashes from the outfile at startup.
- It can load the salt list from the external file. This can be used as a brute-force attack variant.
- The number of threads can be configured and executed based on the lowest priority.

C:\Windows\System32\cmd.exe

```
C:\Users\Shivi.DESKTOP-0E1GBNI\Downloads\hashcat-5.1.0\hashcat-5.1.0>hashcat64.exe -m 0 -a 3 md5.txt
hashcat (v5.1.0) starting...

* Device #1: Intel's OpenCL runtime (GPU only) is currently broken.
             We are waiting for updated OpenCL drivers from Intel.
             You can use --force to override, but do not report related errors.
* Device #3: This hardware has outdated CUDA compute capability (3.5).
             For modern OpenCL performance, upgrade to hardware that supports
             CUDA compute capability version 5.0 (Maxwell) or higher.
* Device #3: 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
nvmlDeviceGetCurrPcieLinkWidth(): Not Supported

nvmlDeviceGetClockInfo(): Not Supported

nvmlDeviceGetFanSpeed(): Not Supported

nvmlDeviceGetClockInfo(): Not Supported

nvmlDeviceGetTemperatureThreshold(): Not Supported

nvmlDeviceGetTemperatureThreshold(): Not Supported

nvmlDeviceGetUtilizationRates(): Not Supported

OpenCL Platform #1: Intel(R) Corporation
======================================
* Device #1: Intel(R) HD Graphics 5500, skipped.
* Device #2: Intel(R) Core(TM) i3-5005U CPU @ 2.00GHz, skipped.
```

C:\Windows\System32\cmd.exe

```
* Device #2: Intel(R) Core(TM) i3-5005U CPU @ 2.00GHz, skipped.

OpenCL Platform #2: NVIDIA Corporation
======================================
* Device #3: GeForce 920M, 512/2048 MB allocatable, 2MCU

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

Applicable optimizers:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Brute-Force
* Raw-Hash

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

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Temperature abort trigger set to 90c

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
```

Encrypt: jain

```
bf76b73579ee889af8815b497e5c6bbe:jain

Session..........: hashcat
Status...........: Exhausted
Hash.Type........: MD5
Hash.Target......: md5.txt
Time.Started.....: Tue Jun 02 15:42:04 2020 (0 secs)
Time.Estimated...: Tue Jun 02 15:42:04 2020 (0 secs)
Guess.Mask.......: ?1?2?2?2 [4]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue......: 4/15 (26.67%)
Speed.#3.........: 57775.6 kH/s (5.66ms) @ Accel:32 Loops:31 Thr:1024 Vec:1
Recovered........: 1/3 (33.33%) Digests, 0/1 (0.00%) Salts
Progress.........: 2892672/2892672 (100.00%)
Rejected.........: 0/2892672 (0.00%)
Restore.Point....: 46656/46656 (100.00%)
Restore.Sub.#3...: Salt:0 Amplifier:31-62 Iteration:0-31
Candidates.#3....: 6ari -> Xqxv
Hardware.Mon.#3..: Temp: 53c
```

Encrypt: dishi

```
759d201176db276addf8bd6c664ef9cb:dishi
Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Exhausted
Hash.Type........: MD5
Hash.Target......: md5.txt
Time.Started.....: Tue Jun 02 15:42:05 2020 (1 sec)
Time.Estimated...: Tue Jun 02 15:42:06 2020 (0 secs)
Guess.Mask.......: ?1?2?2?2?2 [5]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue......: 5/15 (33.33%)
Speed.#3.........:   115.7 MH/s (7.93ms) @ Accel:32 Loops:31 Thr:1024 Vec:1
Recovered........: 2/3 (66.67%) Digests, 0/1 (0.00%) Salts
Progress.........: 104136192/104136192 (100.00%)
Rejected.........: 0/104136192 (0.00%)
Restore.Point....: 1679616/1679616 (100.00%)
Restore.Sub.#3...: Salt:0 Amplifier:31-62 Iteration:0-31
Candidates.#3....: 6uphq -> Xqxvq
Hardware.Mon.#3..: Temp: 54c
```

OUTCOME:

```
C:\Users\Shivi.DESKTOP-0E1GBNI\Downloads\hashcat-5.1.0\hashcat-5.1.0>hashcat64
.exe -m 0 -a 3 -O md5.txt --show
759d201176db276addf8bd6c664ef9cb:dishi
bf76b73579ee889af8815b497e5c6bbe:jain
```