

JOHN THE RIPPER AND THE HASHCAT

ENCRYPT

STEP 1 RIGHT CLICK THE FOLDER CLICK THE ADD TO ARCHIVE

STEP 2 CHOOSE RAR

STEP 3 SET A PASSWORD AND ENCRYPT NAME AND PRESS OK

DECRYPT

STEP 1

· **Install the Latest Version of Hashcat**

Download and install the latest version of Hashcat.

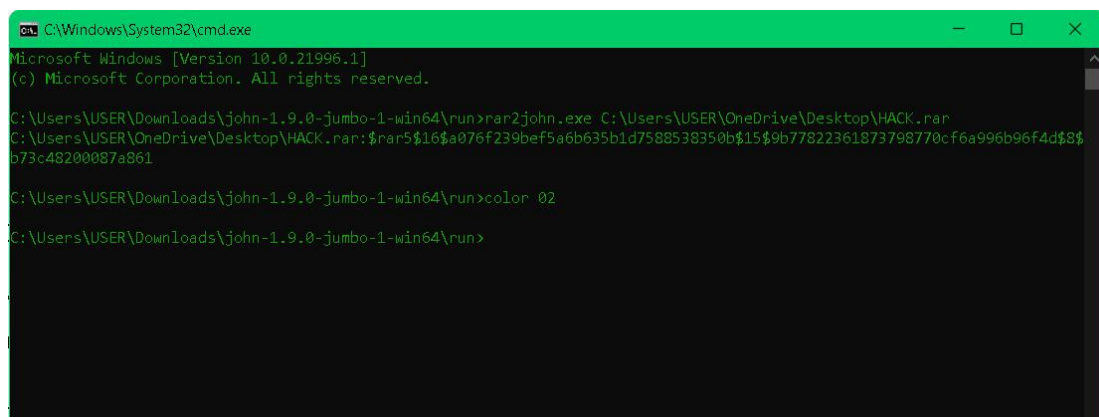
Install John the Ripper 1.9.0

Download and install John the Ripper 1.9.0.

STEP 2

Using John the Ripper

- Extract the John the Ripper files and open the folder.
- Go to the "run" folder and find rar5john.application.
- Open Command Prompt (CMD) and copy the path of rar5john.application.
- In CMD, type:
rar2john.exe <path to the rar file you want to decrypt>
Example: c:/user/desktop/decrypt.rar.



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.21996.1]
(c) Microsoft Corporation. All rights reserved.

C:\Users\USER\Downloads\john-1.9.0-jumbo-1-win64\run>rar2john.exe C:\Users\USER\OneDrive\Desktop\HACK.rar
C:\Users\USER\OneDrive\Desktop\HACK.rar:$rar5$16$a076f239bef5a6b635b1d7588538350b$15$9b77822361873798770cf6a996b96f4d$8$b73c48200087a861

C:\Users\USER\Downloads\john-1.9.0-jumbo-1-win64\run>color 02
C:\Users\USER\Downloads\john-1.9.0-jumbo-1-win64\run>
```

copy the hash start from \$dakdasjdkasjdkj--

STEP 3

Using Hashcat

- Extract Hashcat and open CMD.
- Copy the path of Hashcat and paste it in CMD, then type hashcat.exe.
- Identify the hash mode. For RAR5, use mode 13000.
If it's a different hash type (e.g., MD5 for passwords), use mode 0.
- To see the available hash modes, use the command:
hashcat.exe -h.

```
? | Charset
===+=====
l | abcdefghijklmnopqrstuvwxyz [a-z]
u | ABCDEFGHIJKLMNOPQRSTUVWXYZ [A-Z]
d | 0123456789 [0-9]
h | 0123456789abcdef [0-9a-f]
H | 0123456789ABCDEF [0-9A-F]
s | !"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~
a | ?l?u?d?s
b | 0x00 - 0xff
```

Running Hashcat

In CMD, type:

```
hashcat.exe -m 13000 -a3 <PASTE THE HASH FROM JOHN THE RIPPER>
<charset>
```

Example charset for a 3-letter password: ?l?l?l.

- -a3 is the attack mode.
- Press Enter to start the attack.

```
\Users\USER\Downloads\hashcat-6.2.6>hashcat.exe -m 0 -a3 f632fa6f8c3d5f551c5df867588381ab ?l?l?l
charset
```

```
# | Mode
===+=====
0 | Straight
1 | Combination
3 | Brute-force
6 | Hybrid Wordlist + Mask
7 | Hybrid Mask + Wordlist
9 | Association
```

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

C:\Users\USER\Downloads\hashcat-6.2.6>hashcat.exe -m 13000 -a3 $rar5$16$a076f239bef5a6b635b1d7588538350b$15$9b77822361873798770cf6a9
96b96f4d$8$b73c48200087a861 ?l?l?l
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 ) - Platform #1 [Intel(R) Corporation]
=====
* Device #1: Intel(R) UHD Graphics, 1536/3183 MB (795 MB allocatable), 32MCU

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

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

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force
* Slow-Hash-SIMD-LOOP

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

Host memory required for this attack: 298 MB

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).
```

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

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

Session.....: hashcat
Status.....: Running
Hash.Mode.....: 13000 (RAR5)
Hash.Target.....: $rar5$16$a076f239bef5a6b635b1d7588538350b$15$9b7782...87a861
Time.Started.....: Tue Feb 18 01:37:57 2025 (3 secs)
Time.Estimated....: Tue Feb 18 01:39:15 2025 (1 min, 15 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: ?l?l?l [3]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 225 H/s (0.16ms) @ Accel:64 Loops:8 Thr:16 Vec:1
Recovered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.....: 512/17576 (2.91%)
Rejected.....: 0/512 (0.00%)
Restore.Point....: 0/676 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:1-2 Iteration:15864-15872
Candidate.Engine.: Device Generator
Candidates.#1....: mar -> mbf

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

Session.....: hashcat
Status.....: Running
Hash.Mode.....: 13000 (RAR5)
Hash.Target.....: $rar5$16$a076f239bef5a6b635b1d7588538350b$15$9b7782...87a861
Time.Started.....: Tue Feb 18 01:37:57 2025 (16 secs)
Time.Estimated....: Tue Feb 18 01:39:13 2025 (1 min, 0 secs)
Kernel.Feature...: Pure Kernel
```

STEP 4

• Wait for Decryption

- Press s to continue.
- Wait for the estimated time for Hashcat to crack the password.

STEP 5

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

$rar5$16$a076f239bef5a6b635b1d7588538350b$15$9b77822361873798770cf6a996b96f4d$8$b73c48200087a861:ily

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 13000 (RAR5)
Hash.Target.....: $rar5$16$a076f239bef5a6b635b1d7588538350b$15$9b7782...87a861
Time.Started.....: Tue Feb 18 01:37:57 2025 (36 secs)
Time.Estimated....: Tue Feb 18 01:38:33 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: ?l?l?l [3]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 239 H/s (0.16ms) @ Accel:64 Loops:8 Thr:16 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 8704/17576 (49.52%)
Rejected.....: 0/8704 (0.00%)
Restore.Point....: 0/676 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:16-17 Iteration:32792-32799
Candidate.Engine.: Device Generator
Candidates.#1....: iar -> ibf

Started: Tue Feb 18 01:37:52 2025
Stopped: Tue Feb 18 01:38:34 2025
```

· View the Cracked Password

Once done, the cracked password will be displayed.