

How to Use John the Ripper in Kali Linux

John the Ripper is a popular and free password-cracking tool that is included in Kali Linux. It allows you to perform dictionary attacks or brute force attacks on hashed passwords. Using John the Ripper can help you recover lost passwords or test the strength of account passwords.

➤ What is John the Ripper

John the Ripper is an open-source password-cracking tool first developed in 1996. It can crack passwords by performing dictionary attacks, brute force attacks, or through its own rule-based cracker.

Some key features of John the Ripper:

1. Cracks hashed passwords through dictionary attacks or brute force
2. Supports a wide range of hashing algorithms like MD5, SHA, etc
3. Can detect password lengths and character sets
4. Performs fast parallel cracking using multiple cores

➤ Why Use John the Ripper

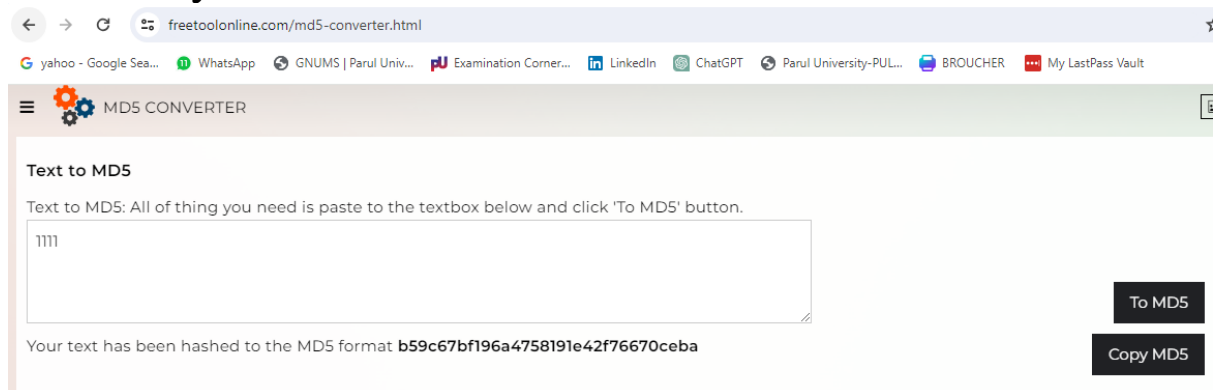
Here are some common reasons for using John the Ripper:

1. Recover lost or forgotten passwords
2. Test account password strength
3. Perform security audits by cracking hashed passwords
4. Educational purposes to understand password security

Practical -1 CRACKING THE HASHED PASSWORDS

STEPT-1 CREATE HASH FILE

1.1 OPEN any md5 to text converter online



The screenshot shows a web browser at the URL `freetoolonline.com/md5-converter.html`. The page has a header with various social media and utility links. The main content area is titled "MD5 CONVERTER" and contains a section "Text to MD5". It instructs the user to paste text into a box and click "To MD5". The text "1111" has been entered, and the resulting MD5 hash `b59c67bf196a4758191e42f76670ceba` is displayed below. There are buttons for "To MD5" and "Copy MD5".

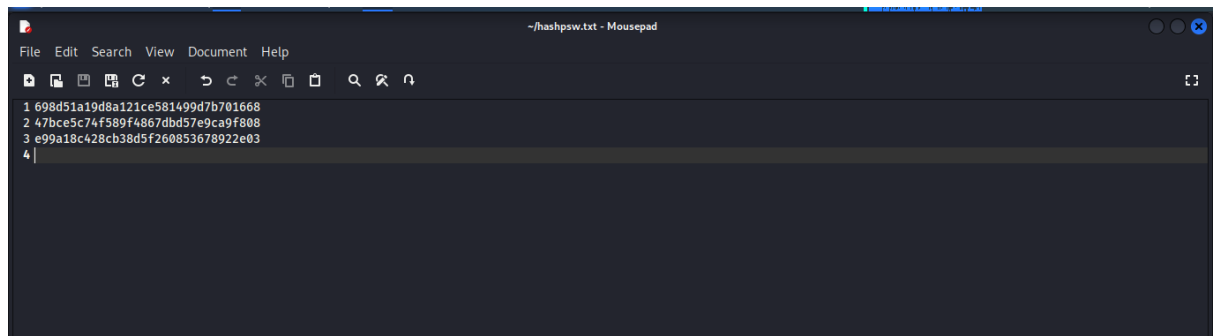
1.2 Copy hash value in text file

```
(kali㉿kali)-[~]  
$ echo 698d51a19d8a121ce581499d7b701668 > hashpsw.txt  
  
(kali㉿kali)-[~]  
$ cat hashpsw.txt  
698d51a19d8a121ce581499d7b701668
```

STEP-2 Crack the password file

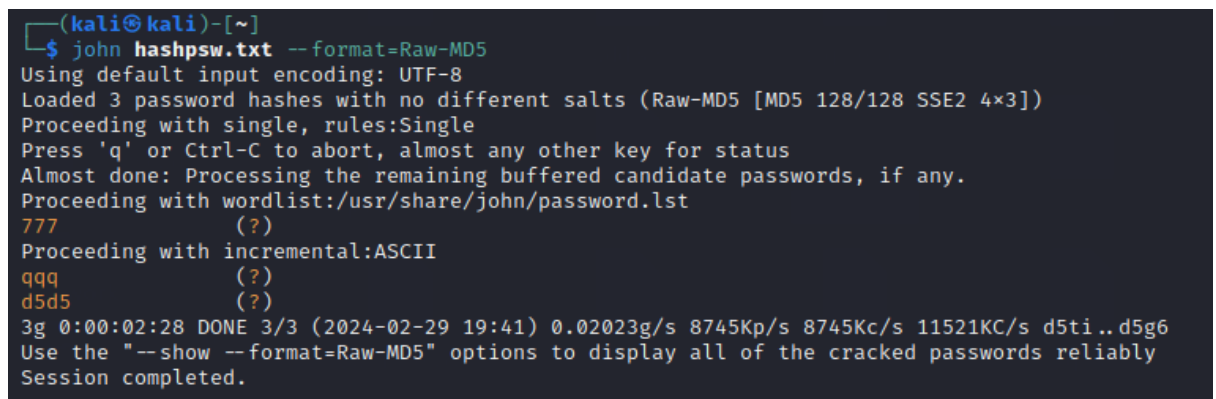
```
(kali㉿kali)-[~]  
$ john hashpsw.txt --format=Raw-MD5  
Using default input encoding: UTF-8  
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst  
Proceeding with incremental:ASCII  
111 (?)  
1g 0:00:00:01 DONE 3/3 (2024-02-29 19:27) 0.9900g/s 180956p/s 180956c/s 180956C/s abilo1..10093  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably  
Session completed.
```

STEP-3 Add more hash password in same text file



```
File Edit Search View Document Help
1 698d51a19d8a121ce581499d7b701668
2 47bce5c74f589f4867dbd57e9ca9f808
3 e99a18c428cb38d5f260853678922e03
4
```

STEP-4 Cracks multiple passwords USING john the ripper command

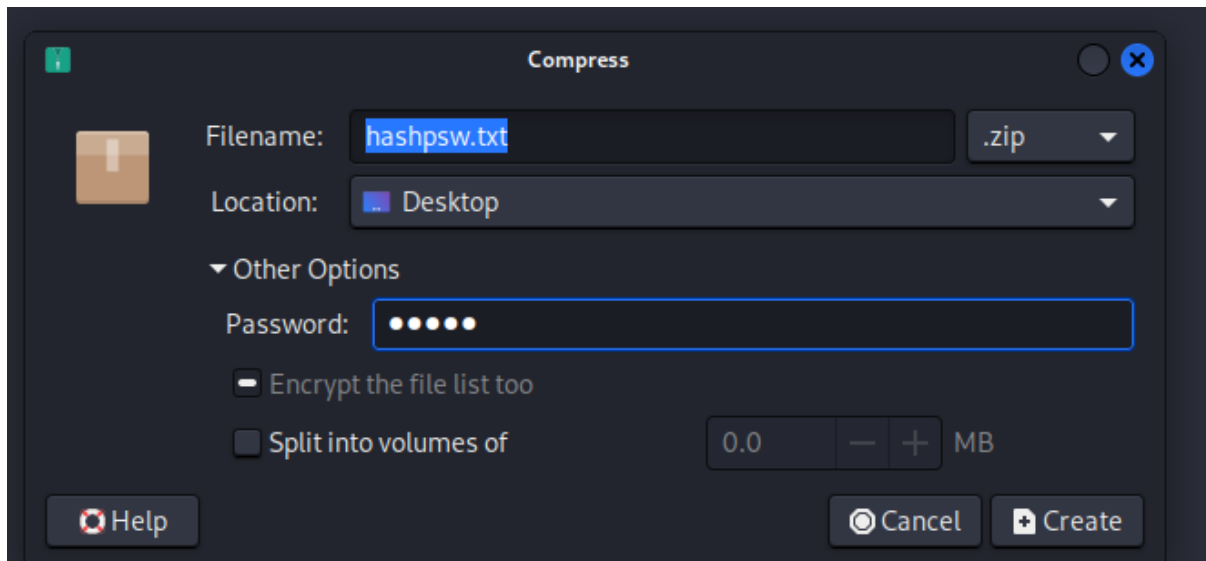


```
(kali㉿kali)-[~]
$ john hashpsw.txt --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
777 (?)
Proceeding with incremental:ASCII
qqq (?)
d5d5 (?)
3g 0:00:02:28 DONE 3/3 (2024-02-29 19:41) 0.02023g/s 8745Kp/s 8745Kc/s 11521KC/s d5ti..d5g6
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Practical -2 RECOVER/CRACK ZIP FILE PASSWORDS

STEP-1 Create archive password protected file.

STEP-1.1 write click on file and choose create archive and enter your password.



STEP-2 remove normal text file and now to open zip text file but it is password protected

STEP-3 Identify the file path

```
(kali㉿kali)-[~]
$ cd Desktop
Text to MD5
(kali㉿kali)-[~/Desktop]
$ ls
hide.zip.zip parul
```

STEP-4 create hash file using ZIP2JOHN command for storing zip file password.

```
(kali㉿kali)-[~]
$ zip2john Desktop/hide.zip.zip > hash.txt
```

STEP-5 see the hash file

```
(kali㉿kali)-[~]
└─$ cat hash.txt
hide.zip.zip/hashpsw.txt:$zip2$*0*1*0*f71bb73433fd7e43*f1b1*21*47b19257dfefb03a93608aef322237a2e87649f373d333ae3a304bdd6827e0e72*7ede39be3d5686950031*$/zip2$:hashpsw
.txt:hide.zip.zip:Desktop/hide.zip.zip
```

STEP-6 apply John command for crack the password.

```
(kali㉿kali)-[~]
└─$ john hash.txt --hashes=MD5 --wordlist=/usr/share/john/password.lst --show
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
Cost 1 (HMAC size) is 33 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1234567890..maggie (hide.zip.zip/hashpsw.txt)
1g 0:00:00:17 DONE 2/3 (2024-02-29 20:04) 0.05797g/s 3399p/s 3399c/s 3399C/s 123456..maggie
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```