

# Password cracking

## Cracking password of zip file

Used tool : John the ripper

### Step 1 :-

Find the hash of the zip file and save it as .txt file

**Command used : zip2john "file name" > hash.txt**

```
(kali㉿kali)-[~/Desktop]
$ zip2john crack.zip > hash.txt
ver 81.9 crack.zip/sms_dump_20210630122912.txt is not encrypted, or stored with non-handled compression type
```

### Step 2 :-

Resolve the hash to get password

**Command used :- john --format=zip hash.txt**

```
(kali㉿kali)-[~/Desktop]
$ john --format=zip hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 7 candidates buffered for the current salt, minimum 16 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
1234 (crack.zip/sms_dump_20210630122912.txt)
1g 0:00:00:02 DONE 2/3 (2021-07-04 09:00) 0.4016g/s 22896p/s 22896c/s 22896C/s 123456..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

**Password of the file is 1234.**