John The Ripper Full Tutorial

john the ripper is an advanced **password cracking** tool used by many which are free and open source. **John the Ripper** initially developed for UNIX operating system but now it works on Fifteen different platforms.

John The Ripper widely used to reduce the risk of network security causes by weak passwords as well as to measure other security flaws regarding encryptions. John The Ripper uses a wide variety of password cracking techniques against user accounts of many operating systems, password encryptions, and hashes.

such as crypt password hash types(MD5, DES or Blowfish).
Windows NT/XP/2000/2003/LM hash.
Also, passwords stored in MySQL, LDAP, and others.

John The Ripper is a combination of the number of password crackers in one package makes it one of the best password testing and breaking program which autodetects password hashes and customizable password cracker.

John the Ripper has an official free version, a community enhanced version, and also a pro version.

In this **tutorial**, we will see the most common password cracking like **Linux password, Zip file protected with a password, Windows password, and Wifi Handshake file cracking**.

Table Of Contents

Installing and Downloading John the Ripper in Kali Linux.

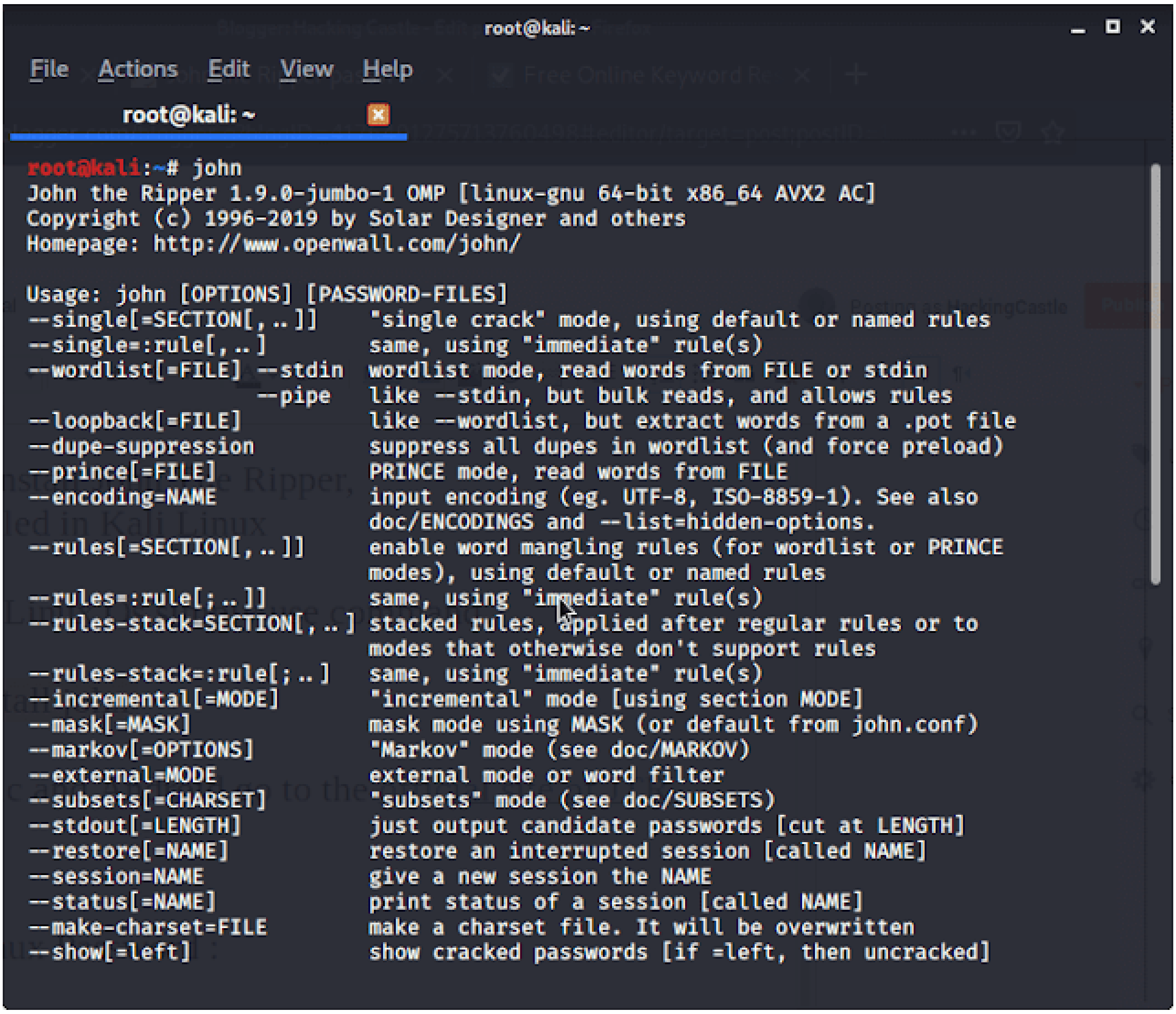
first, we need to install **John The Ripper,**
it comes preinstalled in Kali Linux

to **install in other Linux Os simply use command**.

```
# sudo apt-get install john
```

For Windows, Mac and Android go to the official site of JTR

Type John in terminal to see options.



```
root@kali:~# john
John the Ripper 1.9.0-jumbo-1 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2019 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,..]]    "single crack" mode, using default or named rules
--single=:rule[,..]        same, using "immediate" rule(s)
--wordlist[=FILE] --stdin  wordlist mode, read words from FILE or stdin
                  --pipe   like --stdin, but bulk reads, and allows rules
--loopback[=FILE]          like --wordlist, but extract words from a .pot file
--dupe-suppression         suppress all dupes in wordlist (and force preload)
--prince[=FILE]            PRINCE mode, read words from FILE
--encoding=NAME            input encoding (eg. UTF-8, ISO-8859-1). See also
                           doc/ENCODINGS and --list=hidden-options.
--rules[=SECTION[,..]]     enable word mangling rules (for wordlist or PRINCE
                           modes), using default or named rules
--rules=:rule[;..]]        same, using "immediate" rule(s)
--rules-stack=SECTION[,..] stacked rules, applied after regular rules or to
                           modes that otherwise don't support rules
--rules-stack=:rule[;..]   same, using "immediate" rule(s)
--incremental[=MODE]       "incremental" mode [using section MODE]
--mask[=MASK]              mask mode using MASK (or default from john.conf)
--markov[=OPTIONS]         "Markov" mode (see doc/MARKOV)
--external=MODE            external mode or word filter
--subsets[=CHARSET]        "subsets" mode (see doc/SUBSETS)
--stdout[=LENGTH]          just output candidate passwords [cut at LENGTH]
--restore[=NAME]           restore an interrupted session [called NAME]
--session=NAME             give a new session the NAME
--status[=NAME]            print status of a session [called NAME]
--make-charset=FILE        make a charset file. It will be overwritten
--show[=left]              show cracked passwords [if =left, then uncracked]
```

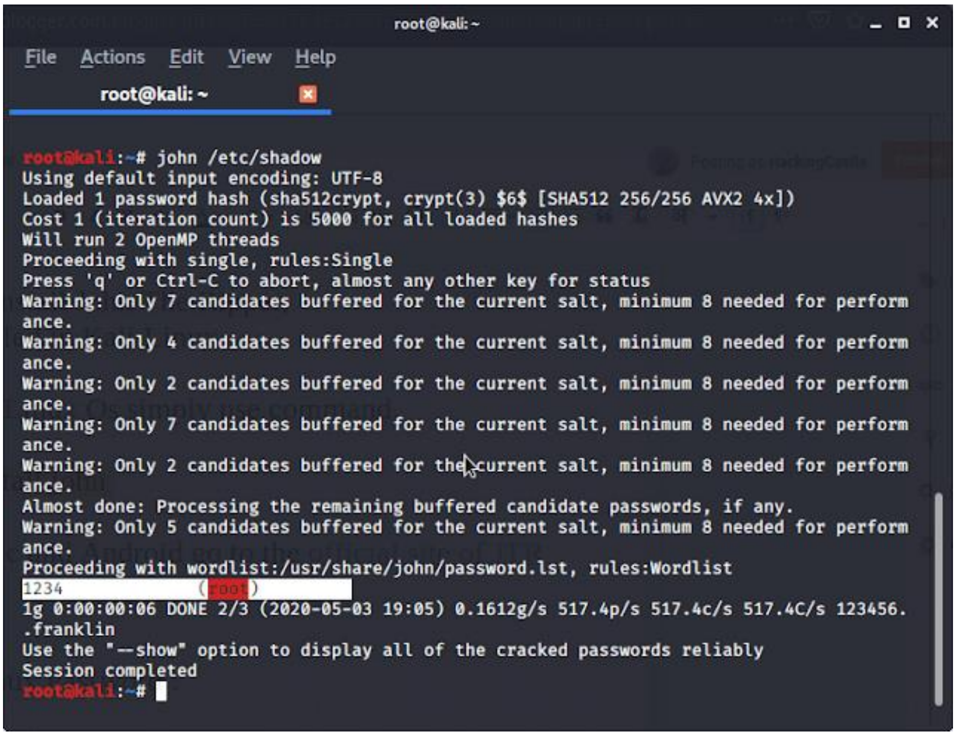
Cracking Linux user Passwords:

Cracking Linux password in John The Ripper also called unshadowing because Linux passwords are saved in Shadow files which located in

/etc/shadow

so cracking Linux password or unshadow password simply use this command in John The Ripper.

# john /etc/shadow



```
root@kali:~# john /etc/shadow
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
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 8 needed for perform
ance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for perform
ance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for perform
ance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for perform
ance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for perform
ance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for perform
ance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
1234             (root)
1g 0:00:00:06 DONE 2/3 (2020-05-03 19:05) 0.1612g/s 517.4p/s 517.4c/s 517.4C/s 123456.
.franklin
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```

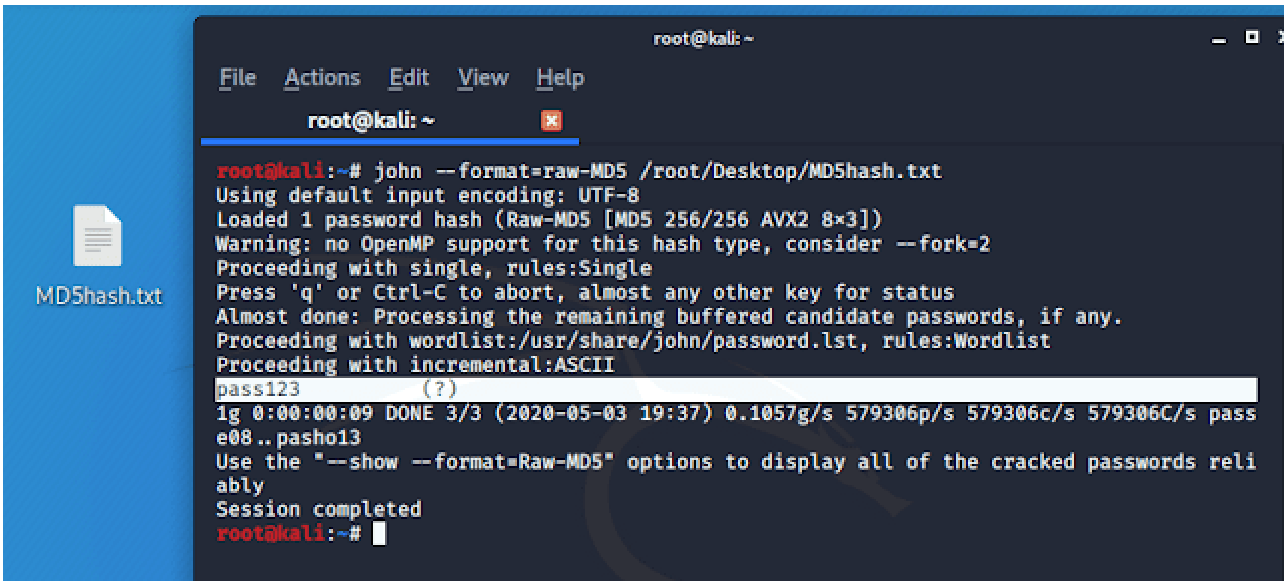
As you can see John cracked the password in the shadow file.
This process sometimes takes time depending upon password complexity and the number of users.

Decrypting MD5 hash:

There are lots of hash types present over the internet but we are going to use MD5 in this article MD5 hash is a new type of encryption now widely used so let's crack the hash.
 first, we need to store the hash in .txt file which can then accessible for john the ripper using the command.

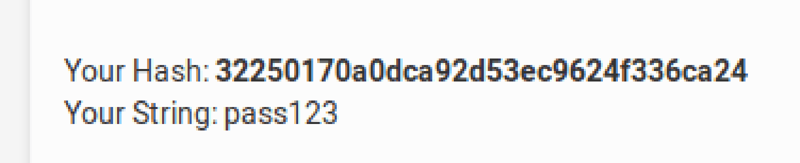
 I stored MD5 hash in MD5hash.txt and used this command.

john --format=raw-MD5 /root/Desktop/MD5hash.txt



```
root@kali:~# john --format=raw-MD5 /root/Desktop/MD5hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
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, rules:Wordlist
Proceeding with incremental:ASCII
pass123          (?)
1g 0:00:00:09 DONE 3/3 (2020-05-03 19:37) 0.1057g/s 579306p/s 579306c/s 579306C/s pass
e08..pasho13
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reli
ably
Session completed
root@kali:~#
```

So John cracked the hash successfully and also correctly.



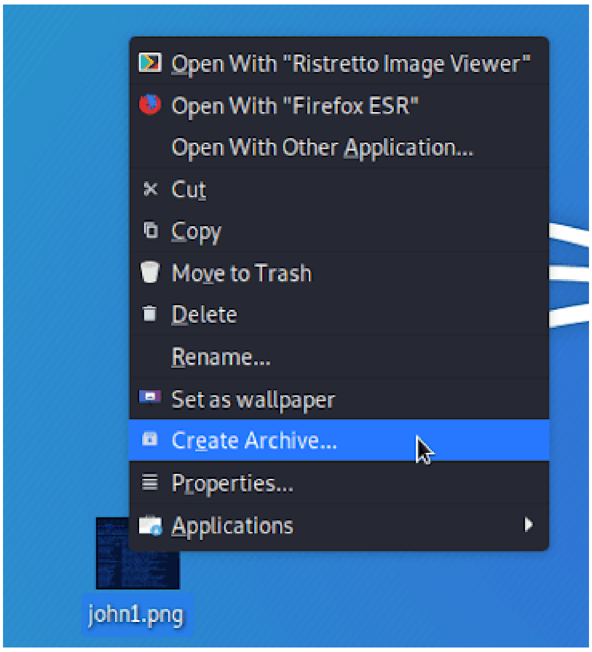
Your Hash: **32250170a0dca92d53ec9624f336ca24**
Your String: pass123

You can also decrypt other hashes like MD5 just by changing the command of hash format.

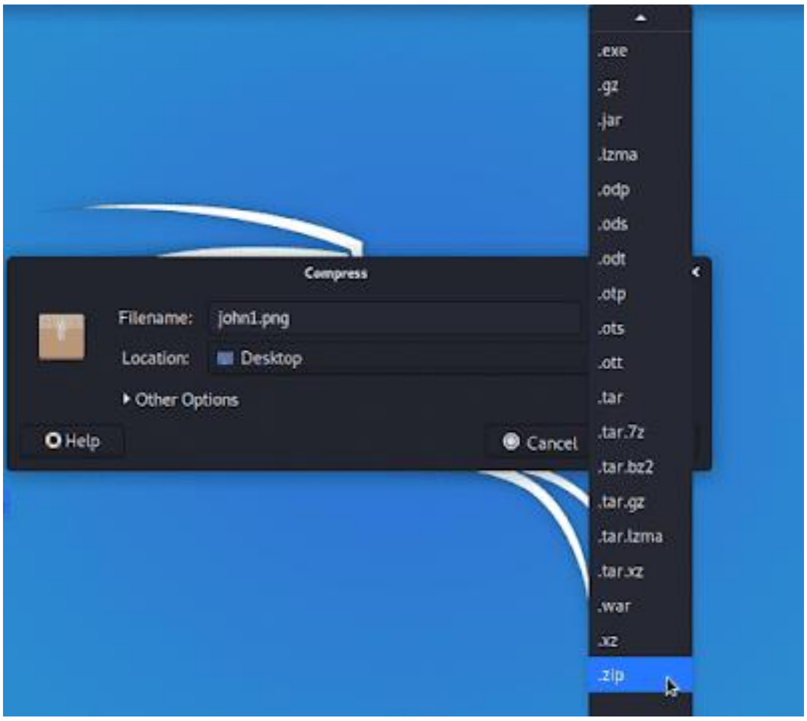
---------XXX--------

Cracking password protected Zip/RAR file:

Zip/RAR file is the most commonly used password protection to files and is widely used. we many times stumbled upon a password-protected ZIP file that has lots of valuable data in it. So here we will **crack the Zip file password in John the Ripper**. And Also **John the Ripper RAR password Cracking**
Lots of Folks Asking about how to **create password protected files in Linux**, So let's cover them up also. First, select the file which you want to password encrypted and right-click on it and select Create Archive.



After that select which compression you want to choose we will ZIP which is way bottom in there.

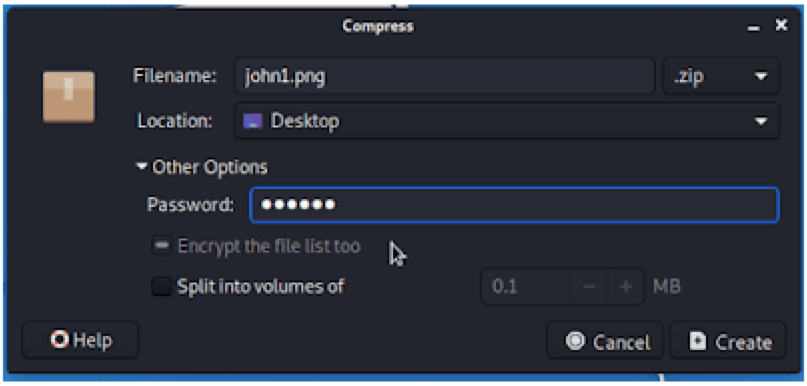


Compress

Filename: john1.png

Location: Desktop

Now, Click on other options where you can see the password field type password you want, and click on create.



Compress

Filename: john1.png .zip

Location: Desktop

▾ Other Options

Password: ••••••

Encrypt the file list too

□ Split into volumes of 0.1 MB

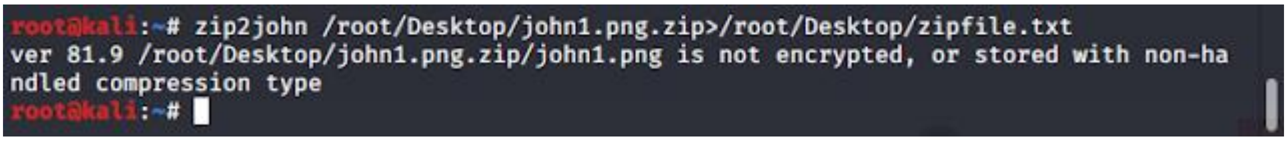
So this is how you can create a password-protected ZIP file in Kali Linux.

We created a password-protected Zip file now we will Decrypt it using John The Ripper.

Firstly we need to Export hashes to .txt file using this command.

# zip2john [Zipfile]>zipfile.txt

This command will export zip keys to .txt file which we will feed to John The Ripper. in my case.

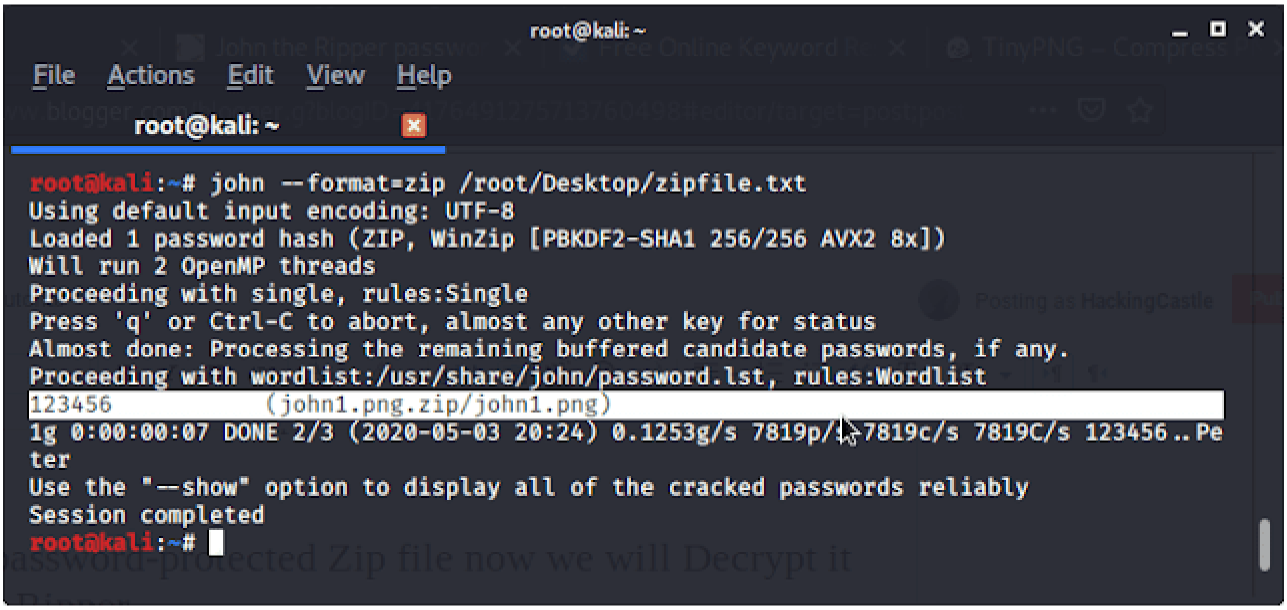


```
root@kali:~# zip2john /root/Desktop/john1.png.zip>/root/Desktop/zipfile.txt
ver 81.9 /root/Desktop/john1.png.zip/john1.png is not encrypted, or stored with non-ha
ndled compression type
root@kali:~# █
```

It's okay if this shows that, if you check zipfile.txt or cat it you will see their zip keys are exported successfully.

Now use this command to crack those keys in john. or **Crack Zip password in John the Ripper**

# john --format=zip [zip.txt]



```
root@kali:~# john --format=zip /root/Desktop/zipfile.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
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
123456           (john1.png.zip/john1.png)
1g 0:00:00:07 DONE 2/3 (2020-05-03 20:24) 0.1253g/s 7819p/s 7819c/s 7819C/s 123456..Pe
ter
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```

As you can see the password is decrypted successfully. This is a **John the Ripper Zip crack**.

If you want to **crack a password of RAR with John the Ripper** then Use the command.

# rar2john [zipfile]>zipkey.txt

Cracking windows user password:

In this **John The Ripper Tutorial** we will crack Windows password stored in SAM and SYSTEM files located in

C:\Windows\System32\Config

Just copy these files using CMD type these commands

reg save hklm\SYSTEM   (for SYSTEM file)

reg save hklm\SAM   (for SAM file)

Now take these files in Kali Linux and need to extract Windows keys so we can crack them use this command

# samdump2 SYSTEM SAM>keys.txt

Details of windows users' passwords will be saved in keys.txt and now we can feed it to John the ripper so it can crack it.

# john --format=LM --user=administrator keys.txt

you can choose the username you want to crack simply specify there instead of an administrator. and john will crack those passwords for you.

If you want to use a custom wordlist then use this command.

# john --wordlist=[wordlist.txt] --user=administrator keys.txt

Cracking WPA/WPA2 handshake using John The Ripper.

Here in this **John the Ripper Tutorial** will only show you how to crack WPA/WPA2 handshake not to capture it. (that's for another day)

The captured handshake must be in .hccap file it not then convert it.

now use this command to export keys in a handshake.

```
# hccap2john [capture]>keys.txt
```

now keys will be exported to keys.txt so we will crack this handshake using a custom wordlist.
use this command.

```
# john --wordlist=[wordlist.txt] /keys.txt
```

and john will start cracking process, a succession of attack depends upon password must be present in wordlist if that wordlist was not worked try a different one.

This is how you can crack various password hashes, encryptions, and user passwords using John the Ripper.

Conclusion:

These are the most common password encryptions you will encounter many times in your experience with hacking and penetration testing and john the ripper is here to help you with every one of them. you will get pretty much ideas about how to crack other password encryptions using John The Ripper.

sometimes it takes too much time to crack a password or it gets failed of password not found in many cases than using custom wordlists can help you here but the cracking password is dependent upon password complexity and a number of character used.

Such as using variables like (!@#$%^&*_<>) and combining it with lowercase and uppercase with more than 12 characters long passwords can make password cracking insanely difficult.