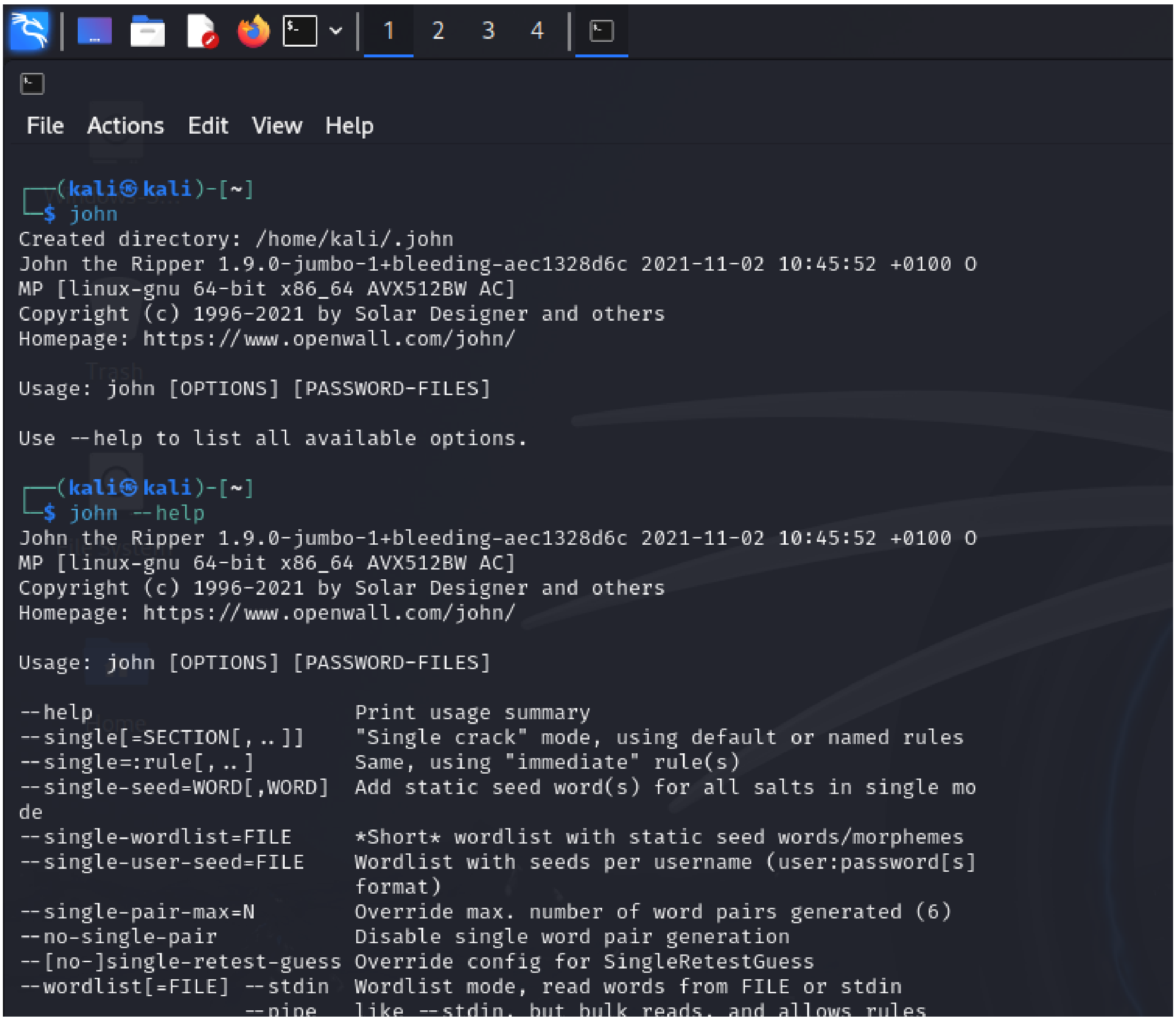
IS - IA-1: Screnshots of Demonstration

Team Members

- Hitanshi Patil - 16010122283
- Harikrishnan Gopal - 16010122284
- Aditya Raut - 16010122288
- Adhiraj Patole – 16010122294

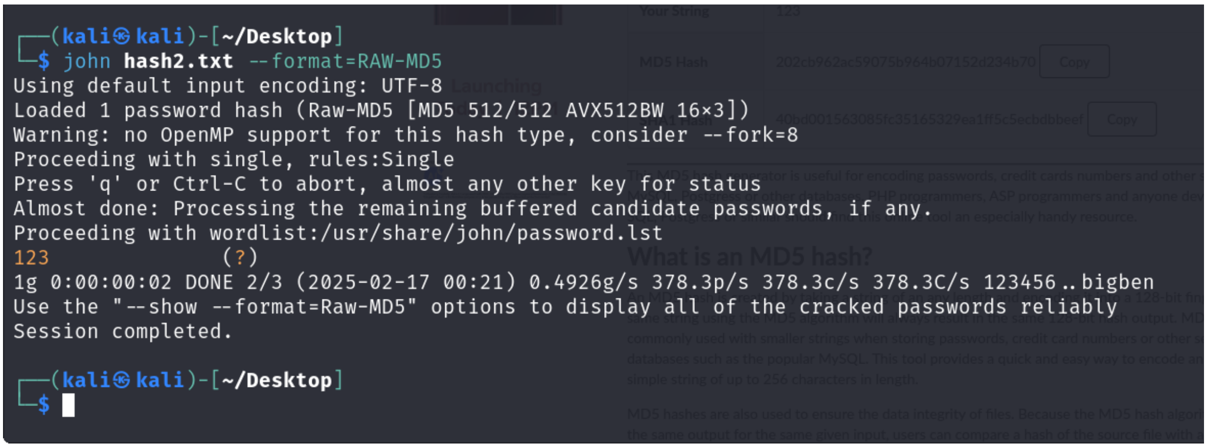
TY BTech Computer Engineering
B Division B-4 Batch

Introducing John the Ripper



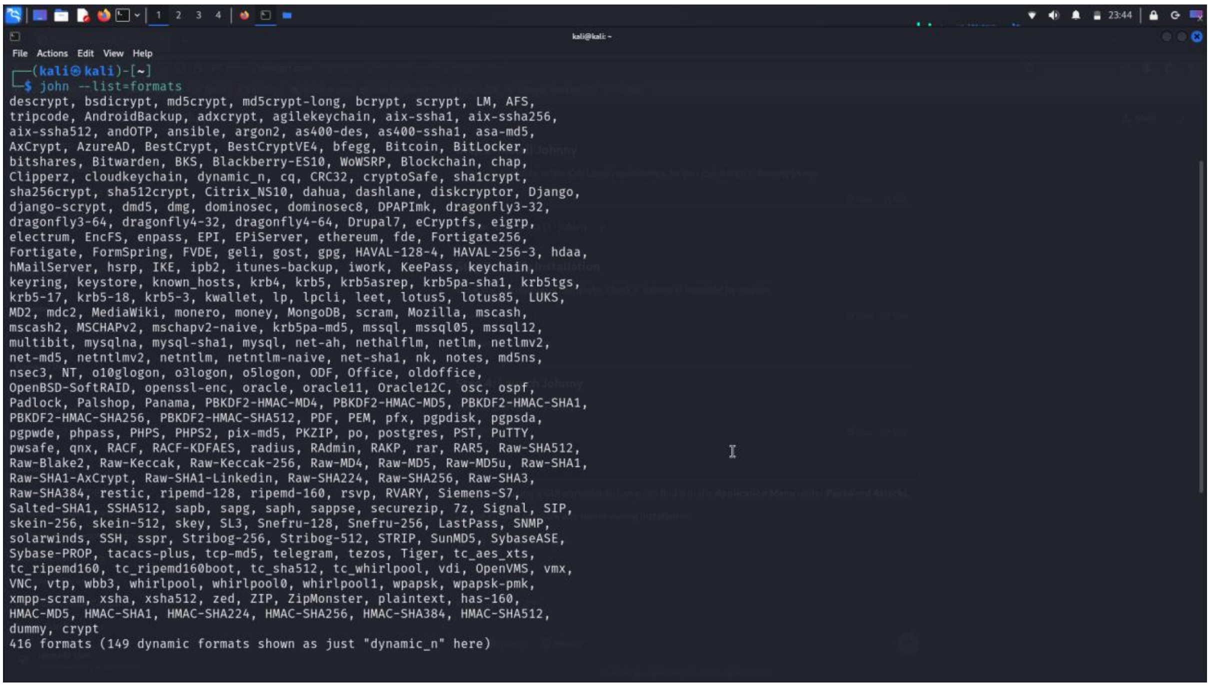
```
┌──(kali㉿kali)-[~]
└─$ john
Created directory: /home/kali/.john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 O
MP [linux-gnu 64-bit x86_64 AVX512BW AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.

┌──(kali㉿kali)-[~]
└─$ john --help
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 O
MP [linux-gnu 64-bit x86_64 AVX512BW AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

--help                     Print usage summary
--single[=SECTION[,..]]    "Single crack" mode, using default or named rules
--single=:rule[,..]        Same, using "immediate" rule(s)
--single-seed=WORD[,WORD]  Add static seed word(s) for all salts in single mo
de
--single-wordlist=FILE     *Short* wordlist with static seed words/morphemes
--single-user-seed=FILE    Wordlist with seeds per username (user:password[s]
                           format)
--single-pair-max=N        Override max. number of word pairs generated (6)
--no-single-pair           Disable single word pair generation
--[no-]single-retest-guess Override config for SingleRetestGuess
--wordlist[=FILE] --stdin  Wordlist mode, read words from FILE or stdin
                  --pipe   like --stdin, but bulk reads, and allows rules
```

Basic usage of John The Ripper:



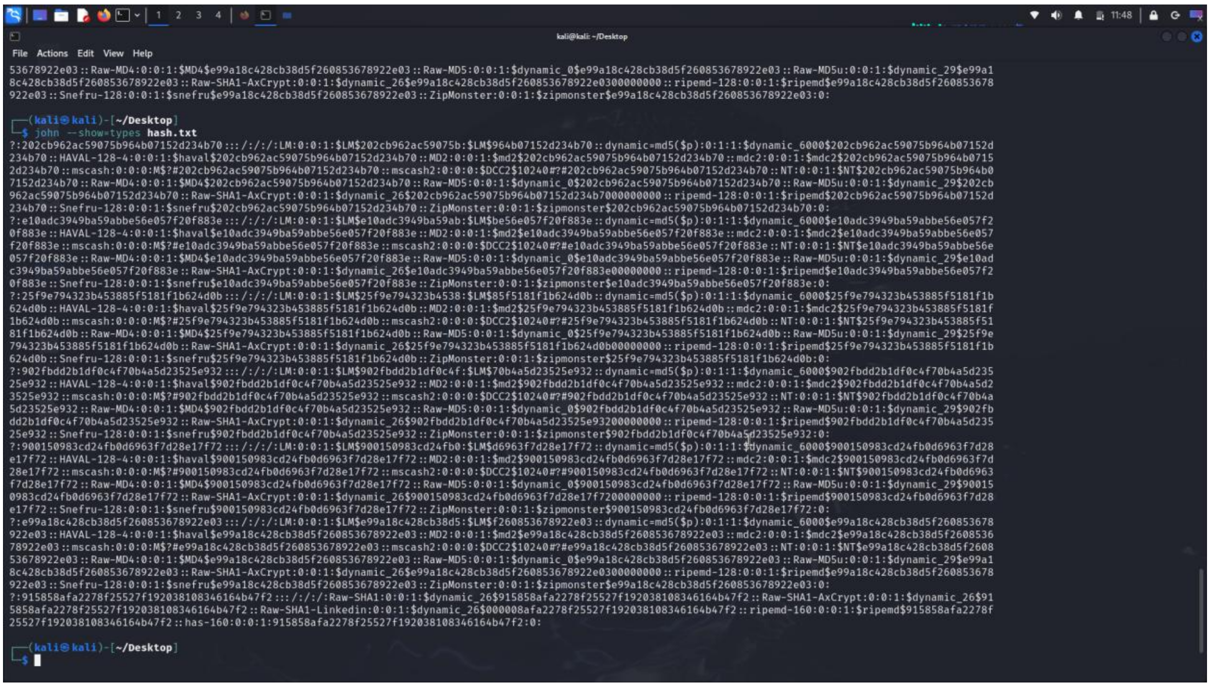
```
┌──(kali㉿kali)-[~/Desktop]
└─$ john hash2.txt --format=RAW-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=8
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123              (?)
1g 0:00:00:02 DONE 2/3 (2025-02-17 00:21) 0.4926g/s 378.3p/s 378.3c/s 378.3C/s 123456..bigben
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Formats Supported in John the Ripper



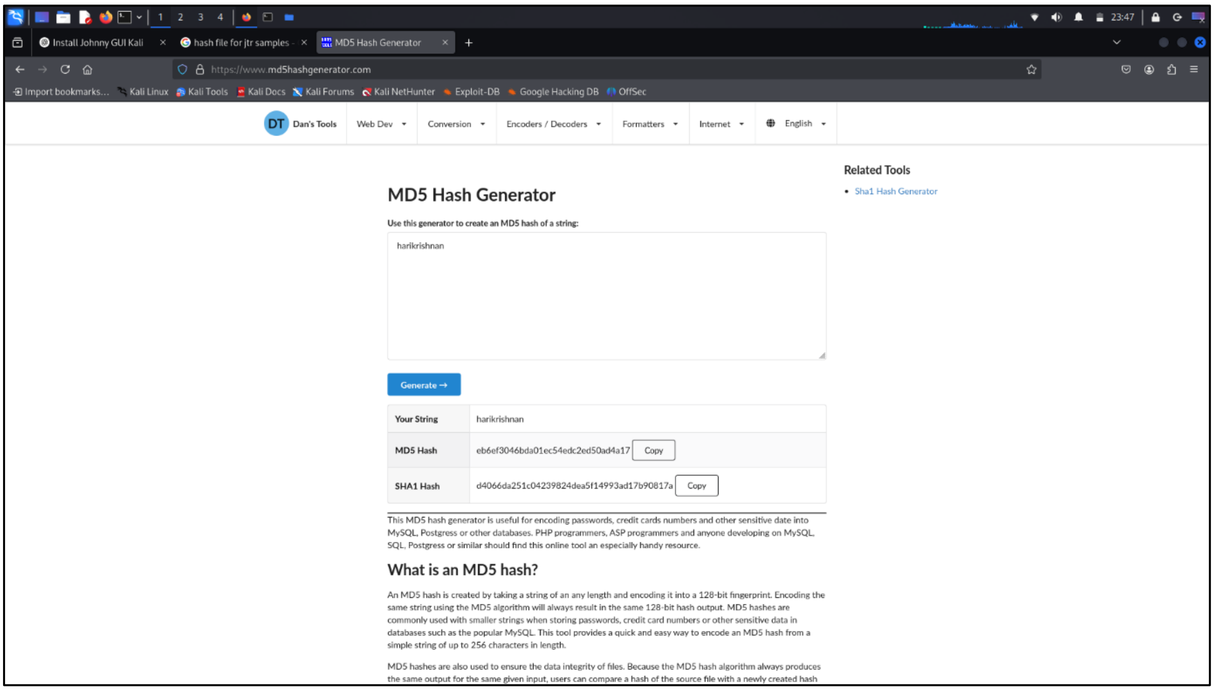
```
┌──(kali㉿kali)-[~]
└─$ john --list=formats
descrypt, bsdicrypt, md5crypt, md5crypt-long, bcrypt, scrypt, LM, AFS,
tripcode, AndroidBackup, adxcrypt, agilekeychain, aix-ssha1, aix-ssha256,
aix-ssha512, andOTP, ansible, argon2, as400-des, as400-ssha1, asa-md5,
AxCrypt, AzureAD, BestCrypt, BestCryptVE4, bfegg, Bitcoin, BitLocker,
bitshares, Bitwarden, BKS, Blackberry-ES10, WoWSRP, Blockchain, chap,
Clipperz, cloudkeychain, dynamic_n, cq, CRC32, cryptoSafe, sha1crypt,
sha256crypt, sha512crypt, Citrix_NS10, dahua, dashlane, diskcryptor, Django,
django-scrypt, dmd5, dmg, dominosec, dominosec8, DPAPImk, dragonfly3-32,
dragonfly3-64, dragonfly4-32, dragonfly4-64, Drupal7, eCryptfs, eigrp,
electrum, EncFS, enpass, EPI, EPiServer, ethereum, fde, Fortigate256,
Fortigate, FormSpring, FVDE, geli, gost, gpg, HAVAL-128-4, HAVAL-256-3, hdaa,
hMailServer, hsrp, IKE, ipb2, itunes-backup, iwork, KeePass, keychain,
keyring, keystore, known_hosts, krb4, krb5, krb5asrep, krb5pa-sha1, krb5tgs,
krb5-17, krb5-18, krb5-3, kwallet, lp, lpcli, leet, lotus5, lotus85, LUKS,
MD2, mdc2, MediaWiki, monero, money, MongoDB, scram, Mozilla, mscash,
mscash2, MSCHAPv2, mschapv2-naive, krb5pa-md5, mssql, mssql05, mssql12,
multibit, mysqlna, mysql-sha1, mysql, net-ah, nethalflm, netlm, netlmv2,
net-md5, netntlmv2, netntlm, netntlm-naive, net-sha1, nk, notes, md5ns,
nsec3, NT, o10glogon, o3logon, o5logon, ODF, Office, oldoffice,
OpenBSD-SoftRAID, openssl-enc, oracle, oracle11, Oracle12C, osc, ospf,
Padlock, Palshop, Panama, PBKDF2-HMAC-MD4, PBKDF2-HMAC-MD5, PBKDF2-HMAC-SHA1,
PBKDF2-HMAC-SHA256, PBKDF2-HMAC-SHA512, PDF, PEM, pfx, pgpdisk, pgpsda,
pgpwde, phpass, PHPS, PHPS2, pix-md5, PKZIP, po, postgres, PST, PuTTY,
pwsafe, qnx, RACF, RACF-KDFAES, radius, RAdmin, RAKP, rar, RAR5, Raw-SHA512,
Raw-Blake2, Raw-Keccak, Raw-Keccak-256, Raw-MD4, Raw-MD5, Raw-MD5u, Raw-SHA1,
Raw-SHA1-AxCrypt, Raw-SHA1-Linkedin, Raw-SHA224, Raw-SHA256, Raw-SHA3,
Raw-SHA384, restic, ripemd-128, ripemd-160, rsvp, RVARY, Siemens-S7,
Salted-SHA1, SSHA512, sapb, sapg, saph, sappse, securezip, 7z, Signal, SIP,
skein-256, skein-512, skey, SL3, Snefru-128, Snefru-256, LastPass, SNMP,
solarwinds, SSH, sspr, Stribog-256, Stribog-512, STRIP, SunMD5, SybaseASE,
Sybase-PROP, tacacs-plus, tcp-md5, telegram, tezos, Tiger, tc_aes_xts,
tc_ripemd160, tc_ripemd160boot, tc_sha512, tc_whirlpool, vdi, OpenVMS, vmx,
VNC, vtp, wbb3, whirlpool, whirlpool0, whirlpool1, wpapsk, wpapsk-pmk,
xmpp-scram, xsha, xsha512, zed, ZIP, ZipMonster, plaintext, has-160,
HMAC-MD5, HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512,
dummy, crypt
416 formats (149 dynamic formats shown as just "dynamic_n" here)
```

Find the Hash Format in files



```
53678922e03 :: Raw-MD4:0:0:1:$MD4$e99a18c428cb38d5f260853678922e03 :: Raw-MD5:0:0:1:$dynamic_0$e99a18c428cb38d5f260853678922e03 :: Raw-MD5u:0:0:1:$dynamic_29$e99a1
8c428cb38d5f260853678922e03 :: Raw-SHA1-AxCrypt:0:0:1:$dynamic_26$e99a18c428cb38d5f260853678922e0300000000 :: ripemd-128:0:0:1:$ripemd$e99a18c428cb38d5f260853678
922e03 :: Snefru-128:0:0:1:$snefru$e99a18c428cb38d5f260853678922e03 :: ZipMonster:0:0:1:$zipmonster$e99a18c428cb38d5f260853678922e03:0:

┌──(kali㉿kali)-[~/Desktop]
└─$ john --show=types hash.txt
?:202cb962ac59075b964b07152d234b70 ::: /:/:/:LM:0:0:1:$LM$202cb962ac59075b:$LM$964b07152d234b70 :: dynamic=md5($p):0:1:1:$dynamic_6000$202cb962ac59075b964b07152d
234b70 :: HAVAL-128-4:0:0:1:$haval$202cb962ac59075b964b07152d234b70 :: MD2:0:0:1:$md2$202cb962ac59075b964b07152d234b70 :: mdc2:0:0:1:$mdc2$202cb962ac59075b964b0715
2d234b70 :: mscash:0:0:0:M$?#202cb962ac59075b964b07152d234b70 :: mscash2:0:0:0:$DCC2$10240#?#202cb962ac59075b964b07152d234b70 :: NT:0:0:1:$NT$202cb962ac59075b964b0
7152d234b70 :: Raw-MD4:0:0:1:$MD4$202cb962ac59075b964b07152d234b70 :: Raw-MD5:0:0:1:$dynamic_0$202cb962ac59075b964b07152d234b70 :: Raw-MD5u:0:0:1:$dynamic_29$202cb
962ac59075b964b07152d234b70 :: Raw-SHA1-AxCrypt:0:0:1:$dynamic_26$202cb962ac59075b964b07152d234b7000000000 :: ripemd-128:0:0:1:$ripemd$202cb962ac59075b964b07152d
234b70 :: Snefru-128:0:0:1:$snefru$202cb962ac59075b964b07152d234b70 :: ZipMonster:0:0:1:$zipmonster$202cb962ac59075b964b07152d234b70:0:
?:e10adc3949ba59abbe56e057f20f883e ::: /:/:/:LM:0:0:1:$LM$e10adc3949ba59ab:$LM$be56e057f20f883e :: dynamic=md5($p):0:1:1:$dynamic_6000$e10adc3949ba59abbe56e057f2
0f883e :: HAVAL-128-4:0:0:1:$haval$e10adc3949ba59abbe56e057f20f883e :: MD2:0:0:1:$md2$e10adc3949ba59abbe56e057f20f883e :: mdc2:0:0:1:$mdc2$e10adc3949ba59abbe56e057
f20f883e :: mscash:0:0:0:M$?#e10adc3949ba59abbe56e057f20f883e :: mscash2:0:0:0:$DCC2$10240#?#e10adc3949ba59abbe56e057f20f883e :: NT:0:0:1:$NT$e10adc3949ba59abbe56e
057f20f883e :: Raw-MD4:0:0:1:$MD4$e10adc3949ba59abbe56e057f20f883e :: Raw-MD5:0:0:1:$dynamic_0$e10adc3949ba59abbe56e057f20f883e :: Raw-MD5u:0:0:1:$dynamic_29$e10ad
c3949ba59abbe56e057f20f883e :: Raw-SHA1-AxCrypt:0:0:1:$dynamic_26$e10adc3949ba59abbe56e057f20f883e00000000 :: ripemd-128:0:0:1:$ripemd$e10adc3949ba59abbe56e057f2
0f883e :: Snefru-128:0:0:1:$snefru$e10adc3949ba59abbe56e057f20f883e :: ZipMonster:0:0:1:$zipmonster$e10adc3949ba59abbe56e057f20f883e:0:
?:25f9e794323b453885f5181f1b624d0b ::: /:/:/:LM:0:0:1:$LM$25f9e794323b4538:$LM$85f5181f1b624d0b :: dynamic=md5($p):0:1:1:$dynamic_6000$25f9e794323b453885f5181f1b
624d0b :: HAVAL-128-4:0:0:1:$haval$25f9e794323b453885f5181f1b624d0b :: MD2:0:0:1:$md2$25f9e794323b453885f5181f1b624d0b :: mdc2:0:0:1:$mdc2$25f9e794323b453885f5181f
1b624d0b :: mscash:0:0:0:M$?#25f9e794323b453885f5181f1b624d0b :: mscash2:0:0:0:$DCC2$10240#?#25f9e794323b453885f5181f1b624d0b :: NT:0:0:1:$NT$25f9e794323b453885f51
81f1b624d0b :: Raw-MD4:0:0:1:$MD4$25f9e794323b453885f5181f1b624d0b :: Raw-MD5:0:0:1:$dynamic_0$25f9e794323b453885f5181f1b624d0b :: Raw-MD5u:0:0:1:$dynamic_29$25f9e
794323b453885f5181f1b624d0b :: Raw-SHA1-AxCrypt:0:0:1:$dynamic_26$25f9e794323b453885f5181f1b624d0b00000000 :: ripemd-128:0:0:1:$ripemd$25f9e794323b453885f5181f1b
624d0b :: Snefru-128:0:0:1:$snefru$25f9e794323b453885f5181f1b624d0b :: ZipMonster:0:0:1:$zipmonster$25f9e794323b453885f5181f1b624d0b:0:
?:902fbdd2b1df0c4f70b4a5d23525e932 ::: /:/:/:LM:0:0:1:$LM$902fbdd2b1df0c4f:$LM$70b4a5d23525e932 :: dynamic=md5($p):0:1:1:$dynamic_6000$902fbdd2b1df0c4f70b4a5d235
25e932 :: HAVAL-128-4:0:0:1:$haval$902fbdd2b1df0c4f70b4a5d23525e932 :: MD2:0:0:1:$md2$902fbdd2b1df0c4f70b4a5d23525e932 :: mdc2:0:0:1:$mdc2$902fbdd2b1df0c4f70b4a5d2
3525e932 :: mscash:0:0:0:M$?#902fbdd2b1df0c4f70b4a5d23525e932 :: mscash2:0:0:0:$DCC2$10240#?#902fbdd2b1df0c4f70b4a5d23525e932 :: NT:0:0:1:$NT$902fbdd2b1df0c4f70b4a
5d23525e932 :: Raw-MD4:0:0:1:$MD4$902fbdd2b1df0c4f70b4a5d23525e932 :: Raw-MD5:0:0:1:$dynamic_0$902fbdd2b1df0c4f70b4a5d23525e932 :: Raw-MD5u:0:0:1:$dynamic_29$902fb
dd2b1df0c4f70b4a5d23525e932 :: Raw-SHA1-AxCrypt:0:0:1:$dynamic_26$902fbdd2b1df0c4f70b4a5d23525e93200000000 :: ripemd-128:0:0:1:$ripemd$902fbdd2b1df0c4f70b4a5d235
25e932 :: Snefru-128:0:0:1:$snefru$902fbdd2b1df0c4f70b4a5d23525e932 :: ZipMonster:0:0:1:$zipmonster$902fbdd2b1df0c4f70b4a5d23525e932:0:
?:900150983cd24fb0d6963f7d28e17f72 ::: /:/:/:LM:0:0:1:$LM$900150983cd24fb0:$LM$d6963f7d28e17f72 :: dynamic=md5($p):0:1:1:$dynamic_6000$900150983cd24fb0d6963f7d28
e17f72 :: HAVAL-128-4:0:0:1:$haval$900150983cd24fb0d6963f7d28e17f72 :: MD2:0:0:1:$md2$900150983cd24fb0d6963f7d28e17f72 :: mdc2:0:0:1:$mdc2$900150983cd24fb0d6963f7d
28e17f72 :: mscash:0:0:0:M$?#900150983cd24fb0d6963f7d28e17f72 :: mscash2:0:0:0:$DCC2$10240#?#900150983cd24fb0d6963f7d28e17f72 :: NT:0:0:1:$NT$900150983cd24fb0d6963
f7d28e17f72 :: Raw-MD4:0:0:1:$MD4$900150983cd24fb0d6963f7d28e17f72 :: Raw-MD5:0:0:1:$dynamic_0$900150983cd24fb0d6963f7d28e17f72 :: Raw-MD5u:0:0:1:$dynamic_29$90015
0983cd24fb0d6963f7d28e17f72 :: Raw-SHA1-AxCrypt:0:0:1:$dynamic_26$900150983cd24fb0d6963f7d28e17f7200000000 :: ripemd-128:0:0:1:$ripemd$900150983cd24fb0d6963f7d28
e17f72 :: Snefru-128:0:0:1:$snefru$900150983cd24fb0d6963f7d28e17f72 :: ZipMonster:0:0:1:$zipmonster$900150983cd24fb0d6963f7d28e17f72:0:
?:e99a18c428cb38d5f260853678922e03 ::: /:/:/:LM:0:0:1:$LM$e99a18c428cb38d5:$LM$f260853678922e03 :: dynamic=md5($p):0:1:1:$dynamic_6000$e99a18c428cb38d5f260853678
922e03 :: HAVAL-128-4:0:0:1:$haval$e99a18c428cb38d5f260853678922e03 :: MD2:0:0:1:$md2$e99a18c428cb38d5f260853678922e03 :: mdc2:0:0:1:$mdc2$e99a18c428cb38d5f2608536
78922e03 :: mscash:0:0:0:M$?#e99a18c428cb38d5f260853678922e03 :: mscash2:0:0:0:$DCC2$10240#?#e99a18c428cb38d5f260853678922e03 :: NT:0:0:1:$NT$e99a18c428cb38d5f2608
53678922e03 :: Raw-MD4:0:0:1:$MD4$e99a18c428cb38d5f260853678922e03 :: Raw-MD5:0:0:1:$dynamic_0$e99a18c428cb38d5f260853678922e03 :: Raw-MD5u:0:0:1:$dynamic_29$e99a1
8c428cb38d5f260853678922e03 :: Raw-SHA1-AxCrypt:0:0:1:$dynamic_26$e99a18c428cb38d5f260853678922e0300000000 :: ripemd-128:0:0:1:$ripemd$e99a18c428cb38d5f260853678
922e03 :: Snefru-128:0:0:1:$snefru$e99a18c428cb38d5f260853678922e03 :: ZipMonster:0:0:1:$zipmonster$e99a18c428cb38d5f260853678922e03:0:
?:915858afa2278f25527f192038108346164b47f2 ::: /:/:/:Raw-SHA1:0:0:1:$dynamic_26$915858afa2278f25527f192038108346164b47f2 :: Raw-SHA1-AxCrypt:0:0:1:$dynamic_26$91
5858afa2278f25527f192038108346164b47f2 :: Raw-SHA1-Linkedin:0:0:1:$dynamic_26$000008afa2278f25527f192038108346164b47f2 :: ripemd-160:0:0:1:$ripemd$915858afa2278f
25527f192038108346164b47f2 :: has-160:0:0:1:915858afa2278f25527f192038108346164b47f2:0:

┌──(kali㉿kali)-[~/Desktop]
└─$ █
```

Hash generation:



MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

harikrishnan

Your String	harikrishnan
MD5 Hash	eb6ef3046bda01ec54edc2ed50ad4a17
SHA1 Hash	d4066da251c04239824dea5f14993ad17b90817a

This MD5 hash generator is useful for encoding passwords, credit cards numbers and other sensitive date into MySQL, Postgress or other databases. PHP programmers, ASP programmers and anyone developing on MySQL, SQL, Postgress or similar should find this online tool an especially handy resource.

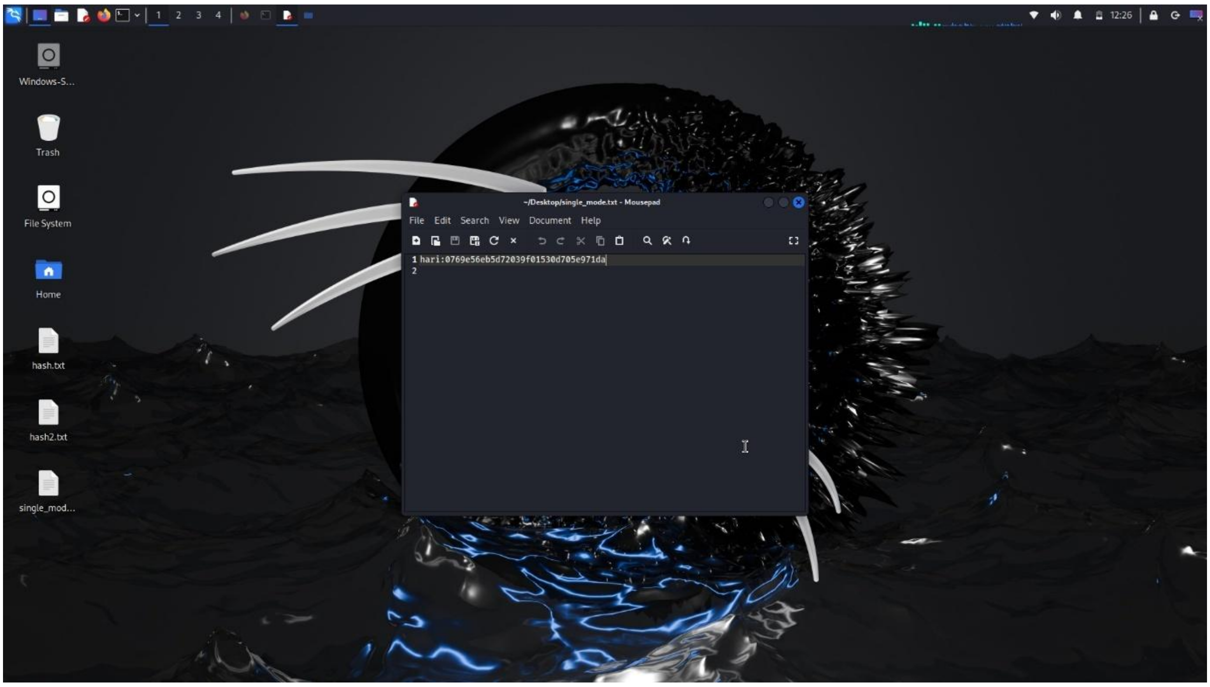
What is an MD5 hash?

An MD5 hash is created by taking a string of an any length and encoding it into a 128-bit fingerprint. Encoding the same string using the MD5 algorithm will always result in the same 128-bit hash output. MD5 hashes are commonly used with smaller strings when storing passwords, credit card numbers or other sensitive data in databases such as the popular MySQL. This tool provides a quick and easy way to encode an MD5 hash from a simple string of up to 256 characters in length.

MD5 hashes are also used to ensure the data integrity of files. Because the MD5 hash algorithm always produces the same output for the same given input, users can compare a hash of the source file with a newly created hash

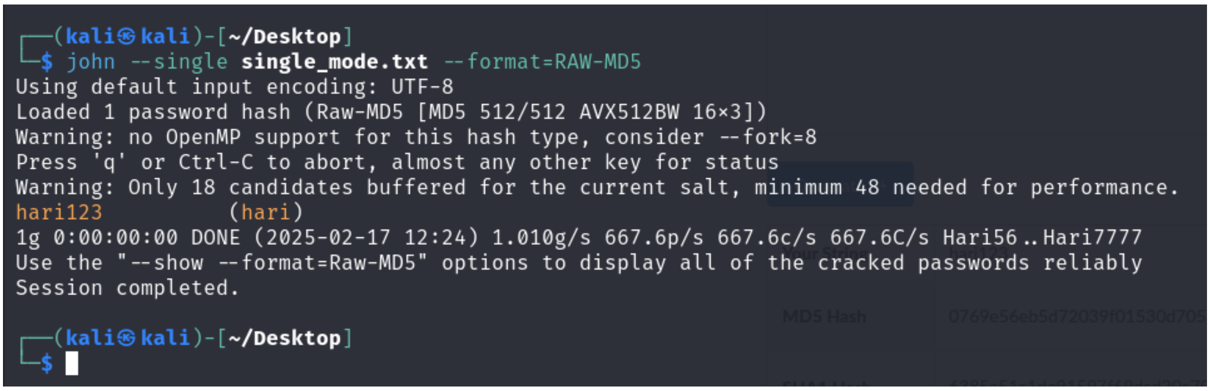
CLI: Single Crack Mode

Hash file creation (single_mode.txt)



```
hari:0769e56eb5d72039f01530d705e971da
```

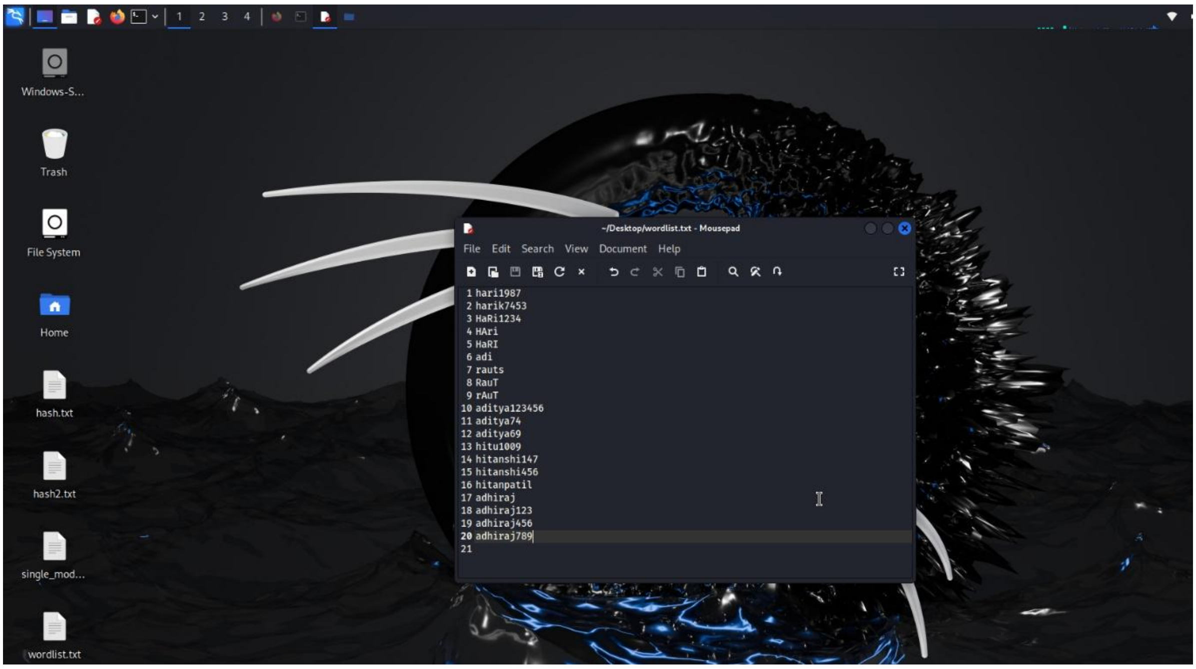
Single Crack mode:



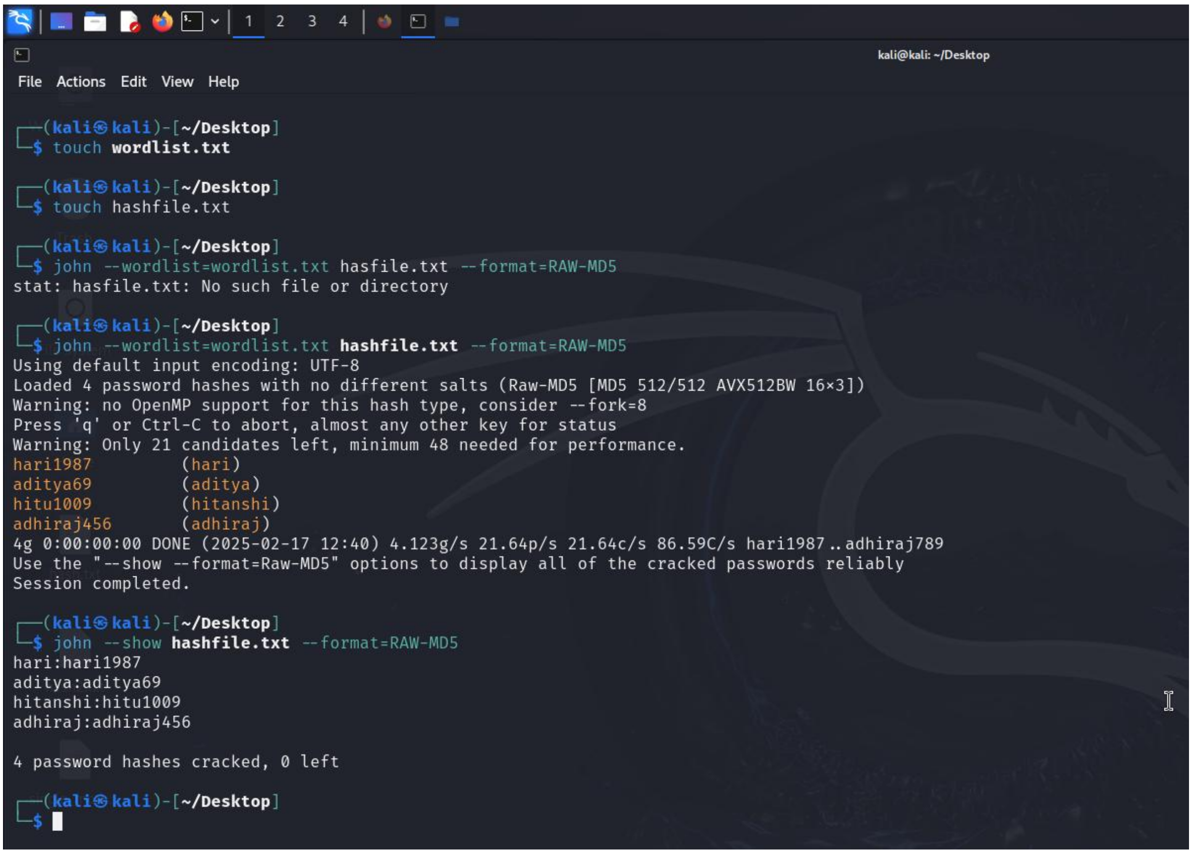
```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --single single_mode.txt --format=RAW-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 18 candidates buffered for the current salt, minimum 48 needed for performance.
hari123          (hari)
1g 0:00:00:00 DONE (2025-02-17 12:24) 1.010g/s 667.6p/s 667.6c/s 667.6C/s Hari56..Hari7777
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

CLI: Wordlist Mode

Wordlist Creation (wordlist.txt)



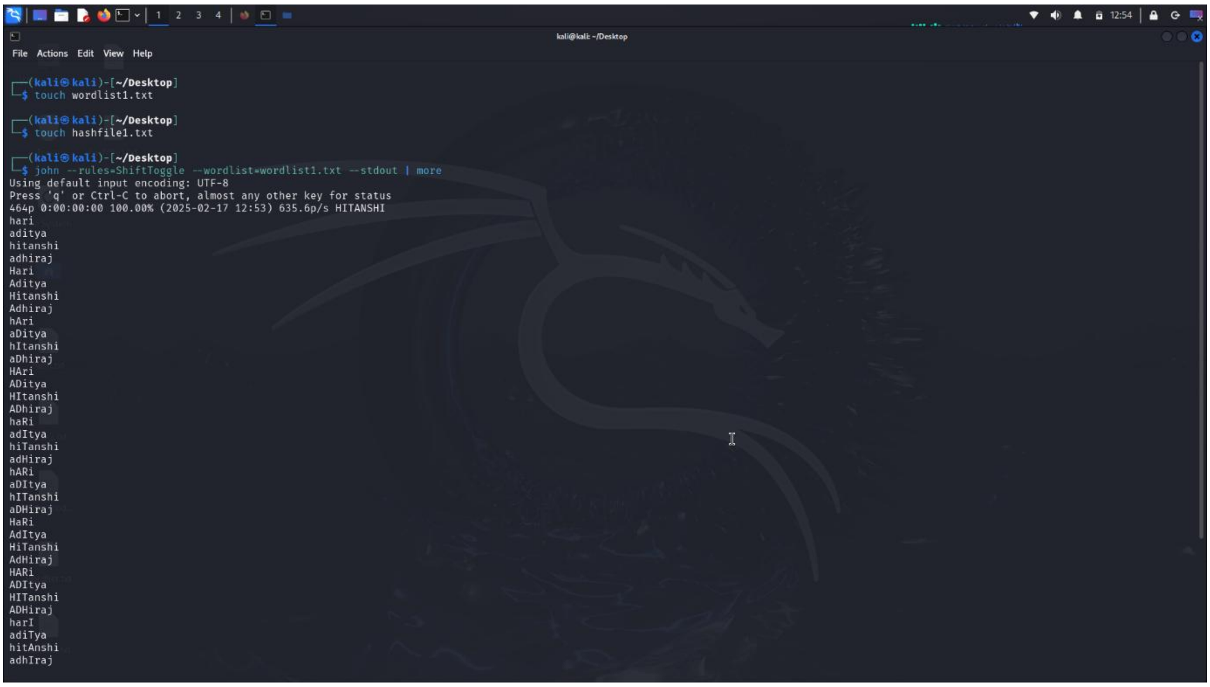
```
hari1987
harik7453
HaRi1234
HAri
HaRI
adi
rauts
RauT
rAuT
aditya123456
aditya74
aditya69
hitu1009
hitanshi147
hitanshi456
hitanpatil
adhiraj
adhiraj123
adhiraj456
adhiraj789
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ touch wordlist.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ touch hashfile.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=wordlist.txt hasfile.txt --format=RAW-MD5
stat: hasfile.txt: No such file or directory

┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=wordlist.txt hashfile.txt --format=RAW-MD5
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 21 candidates left, minimum 48 needed for performance.
hari1987         (hari)
aditya69         (aditya)
hitu1009         (hitanshi)
adhiraj456       (adhiraj)
4g 0:00:00:00 DONE (2025-02-17 12:40) 4.123g/s 21.64p/s 21.64c/s 86.59C/s hari1987..adhiraj789
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$ john --show hashfile.txt --format=RAW-MD5
hari:hari1987
aditya:aditya69
hitanshi:hitu1009
adhiraj:adhiraj456

4 password hashes cracked, 0 left

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

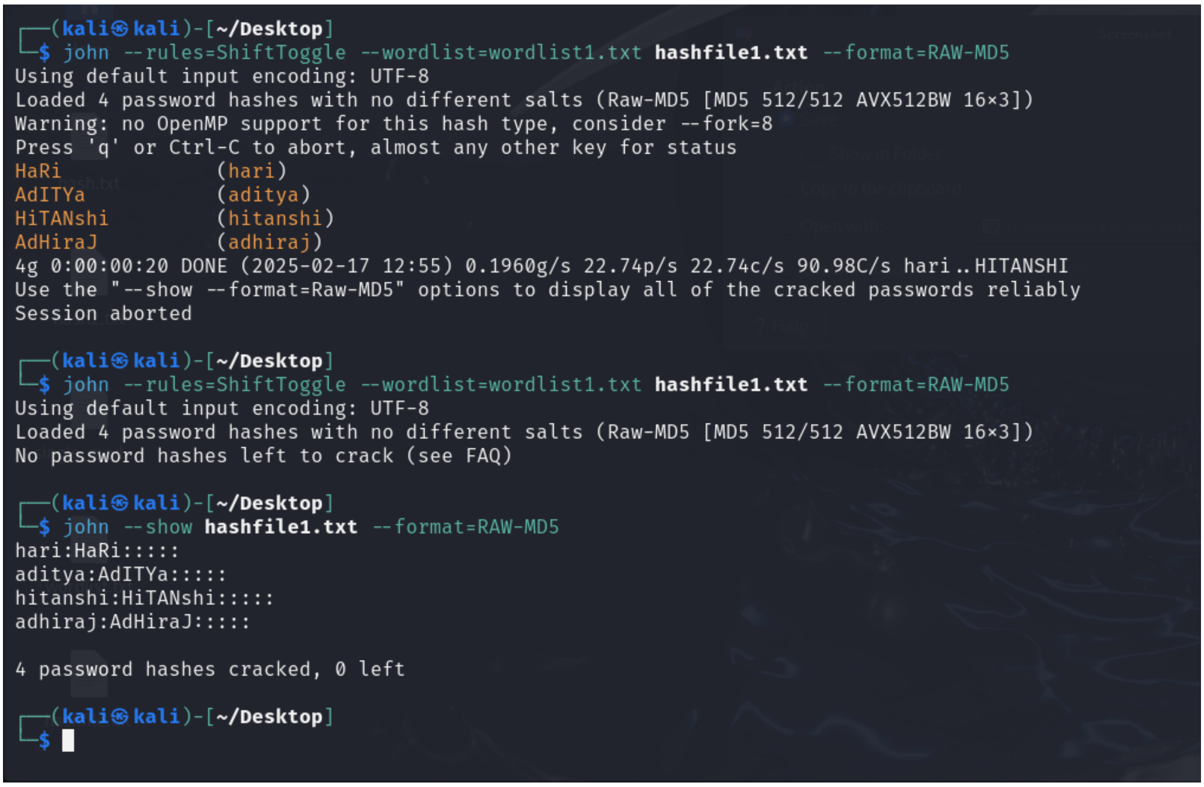
CLI: Incremental Mode

ShiftToggle in Incremental mode:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ touch wordlist1.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ touch hashfile1.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ john --rules=ShiftToggle --wordlist=wordlist1.txt --stdout | more
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
464p 0:00:00:00 100.00% (2025-02-17 12:53) 635.6p/s HITANSHI
hari
aditya
hitanshi
adhiraj
Hari
Aditya
Hitanshi
Adhiraj
hAri
aDitya
hItanshi
aDhiraj
HAri
ADitya
HItanshi
ADhiraj
haRi
adItya
hiTanshi
adHiraj
hARi
aDItya
hITanshi
aDHiraj
HaRi
AdItya
HiTanshi
AdHiraj
HARi
ADItya
HITanshi
ADHiraj
harI
adiTya
hitAnshi
adhIraj
```

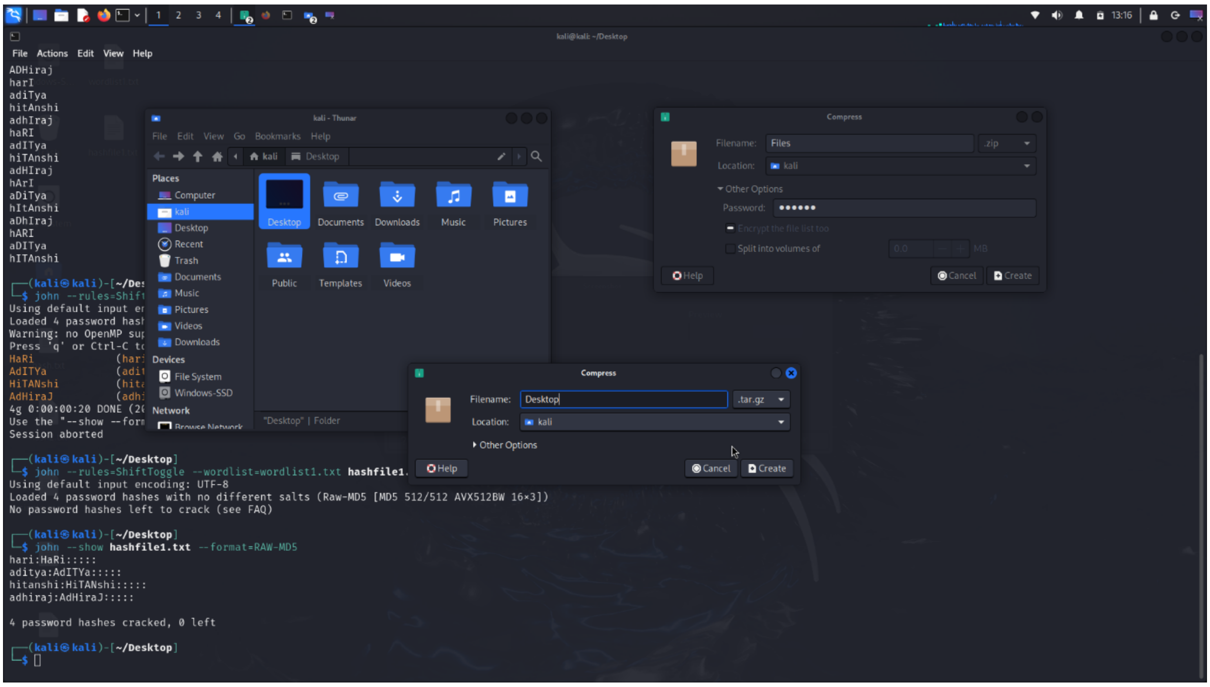
Incremental mode:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --rules=ShiftToggle --wordlist=wordlist1.txt hashfile1.txt --format=RAW-MD5
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
HaRi             (hari)
AdITYa           (aditya)
HiTANshi         (hitanshi)
AdHiraJ          (adhiraj)
4g 0:00:00:20 DONE (2025-02-17 12:55) 0.1960g/s 22.74p/s 22.74c/s 90.98C/s hari..HITANSHI
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session aborted

┌──(kali㉿kali)-[~/Desktop]
└─$ john --rules=ShiftToggle --wordlist=wordlist1.txt hashfile1.txt --format=RAW-MD5
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 512/512 AVX512BW 16×3])
No password hashes left to crack (see FAQ)

┌──(kali㉿kali)-[~/Desktop]
└─$ john --show hashfile1.txt --format=RAW-MD5
hari:HaRi::::
aditya:AdITYa::::
hitanshi:HiTANshi::::
adhiraj:AdHiraJ::::

4 password hashes cracked, 0 left

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

CLI: Password cracking of ZIP file

Password protected ZIP file creation (Files.zip):



```
ADHiraj
harI
adiTya
hitAnshi
adhIraj
haRI
adITya
hiTAnshi
adHIraj
hArI
aDiTya
hItAnshi
aDhIraj
hARI
aDITya
hITAnshi

┌──(kali㉿kali)-[~/Des
└─$ john --rules=Shift
Using default input en
Loaded 4 password hash
Warning: no OpenMP sup
Press 'q' or Ctrl-C to
HaRi             (hari
AdITYa           (adit
HiTANshi         (hita
AdHiraJ          (adhi
4g 0:00:00:20 DONE (20
Use the "--show --form
Session aborted

┌──(kali㉿kali)-[~/Desktop]
└─$ john --rules=ShiftToggle --wordlist=wordlist1.txt hashfile1.
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 512/512 AVX512BW 16×3])
No password hashes left to crack (see FAQ)

┌──(kali㉿kali)-[~/Desktop]
└─$ john --show hashfile1.txt --format=RAW-MD5
hari:HaRi:::::
aditya:AdITYa:::::
hitanshi:HiTANshi:::::
adhiraj:AdHiraJ:::::

4 password hashes cracked, 0 left

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Compress

Filename: Files .zip

Location: kali

Other Options

Password: ••••••

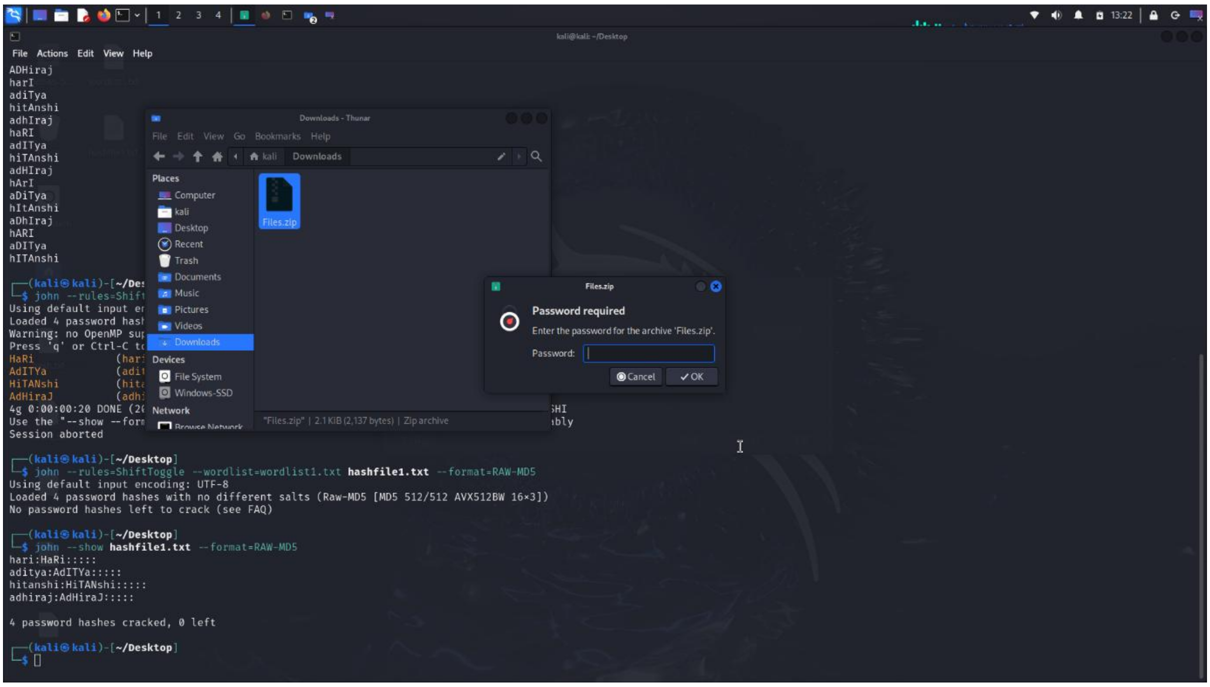
☐ Encrypt the file list too

☐ Split into volumes of 0.0 MB

Compress

Filename: Desktop .tar.gz

Location: kali



```
ADHiraj
harI
adiTya
hitAnshi
adhIraj
haRI
adITya
hiTAnshi
adHIraj
hArI
aDiTya
hItAnshi
aDhIraj
hARI
aDITya
hITAnshi

┌──(kali㉿kali)-[~/Des
└─$ john --rules=Shift
Using default input en
Loaded 4 password hash
Warning: no OpenMP sup
Press 'q' or Ctrl-C to
HaRi             (hari
AdITYa           (adit
HiTANshi         (hita
AdHiraJ          (adhi
4g 0:00:00:20 DONE (20
Use the "--show --form
Session aborted

┌──(kali㉿kali)-[~/Desktop]
└─$ john --rules=ShiftToggle --wordlist=wordlist1.txt hashfile1.txt --format=RAW-MD5
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 512/512 AVX512BW 16×3])
No password hashes left to crack (see FAQ)

┌──(kali㉿kali)-[~/Desktop]
└─$ john --show hashfile1.txt --format=RAW-MD5
hari:HaRi:::::
aditya:AdITYa:::::
hitanshi:HiTANshi:::::
adhiraj:AdHiraJ:::::

4 password hashes cracked, 0 left

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Files.zip

Password required

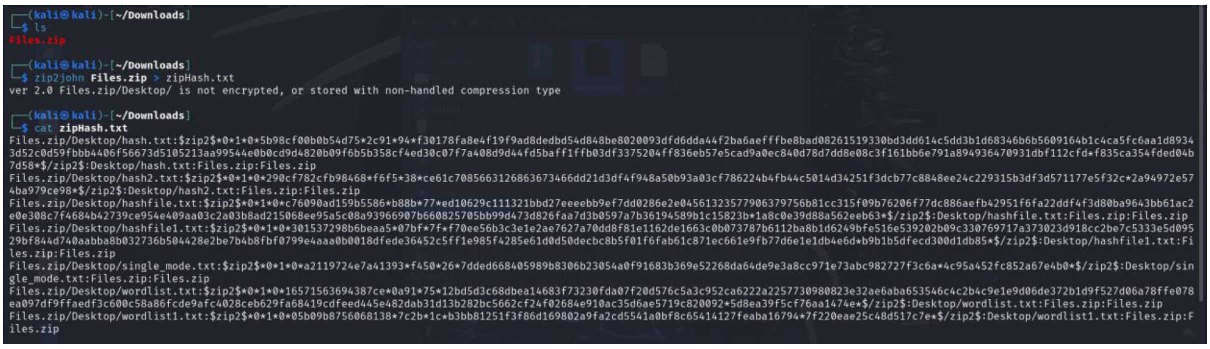
Enter the password for the archive 'Files.zip'.

Password:

"Files.zip" | 2.1 KiB (2,137 bytes) | Zip archive

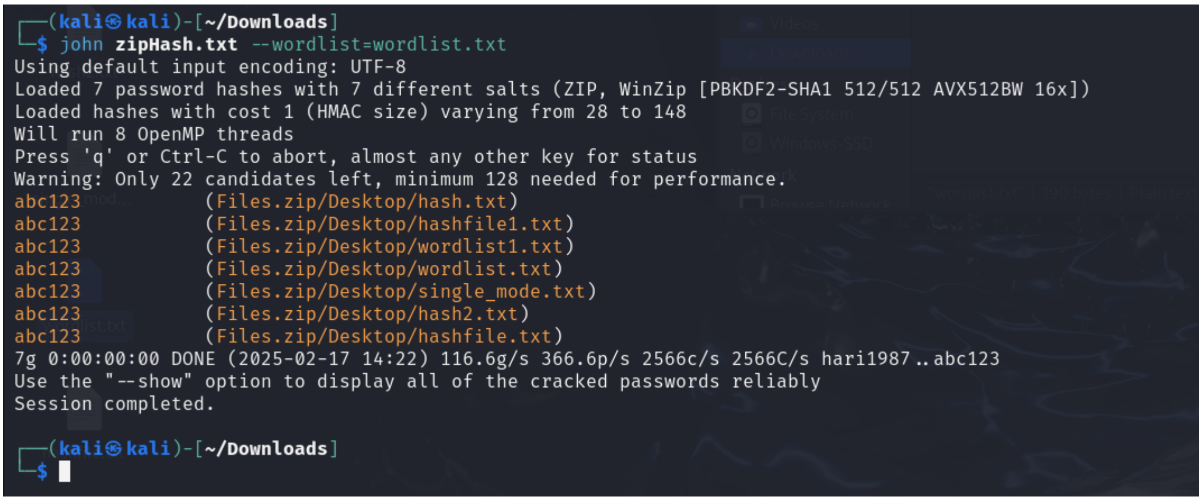
Password cracking on zip files:

Zip file hash:



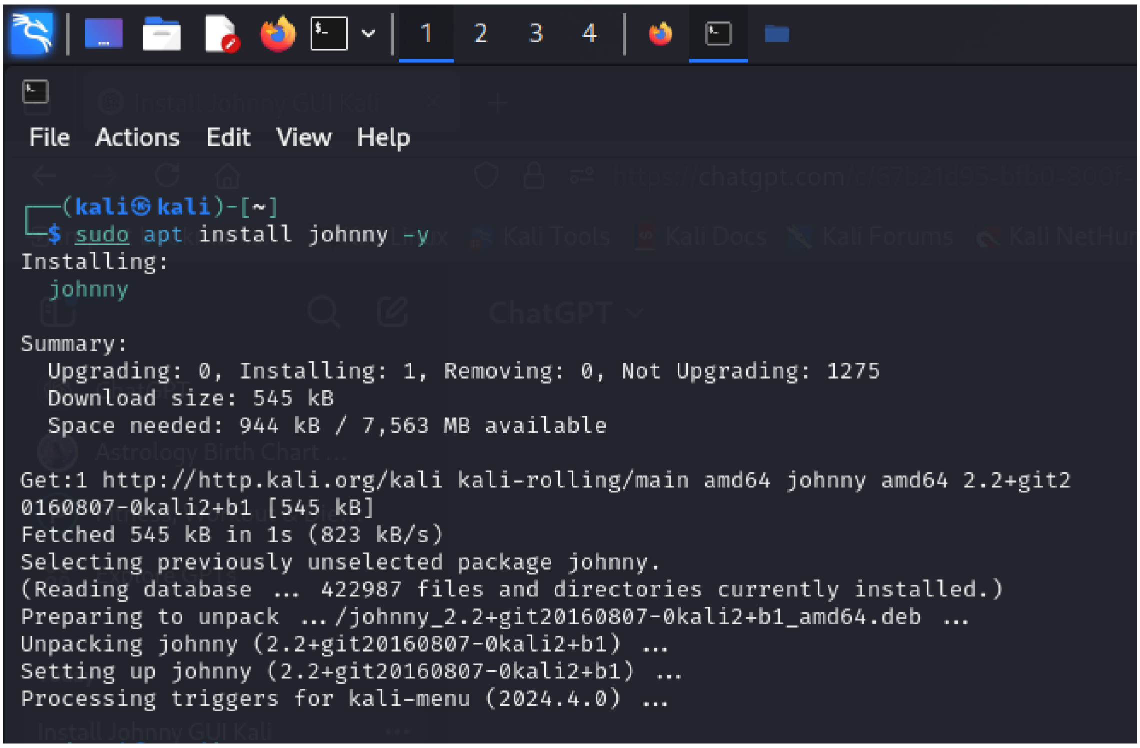
```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
Files.zip

┌──(kali㉿kali)-[~/Downloads]
└─$ zip2john Files.zip > zipHash.txt
ver 2.0 Files.zip/Desktop/ is not encrypted, or stored with non-handled compression type

┌──(kali㉿kali)-[~/Downloads]
└─$ cat zipHash.txt
Files.zip/Desktop/hash.txt:$zip2$*0*1*0*5b98cf00b0b54d75*2c91*94*f30178fa8e4f19f9ad8dedbd54d848be8020093dfd6dda44f2ba6aefffbe8bad08261519330bd3dd614c5dd3b1d68346b6b5609164b1c4ca5fc6aa1d8934
3d52c0d59fbbb4406f56673d5105213aa99544e0b0cd9d4820b09f6b5b358cf4ed30c07f7a408d9d44fd5baff1ffb03df3375204ff836eb57e5cad9a0ec840d78d7dd8e08c3f161bb6e791a894936470931dbf112cfd*f835ca354fded04b
7d58*$/zip2$:Desktop/hash.txt:Files.zip:Files.zip
Files.zip/Desktop/hash2.txt:$zip2$*0*1*0*290cf782cfb98468*f6f5*38*ce61c7085663126863673466dd21d3df4f948a50b93a03cf786224b4fb44c5014d34251f3dcb77c8848ee24c229315b3df3d571177e5f32c*2a94972e57
4ba979ce98*$/zip2$:Desktop/hash2.txt:Files.zip:Files.zip
Files.zip/Desktop/hashfile.txt:$zip2$*0*1*0*c76090ad159b5586*b88b*77*ed10629c111321bbd27eeeebb9ef7dd0286e2e04561323577906379756b81cc315f09b76206f77dc886aefb42951f6fa22ddf4f3d80ba9643bb61ac2
e0e308c7f4684b42739ce954e409aa03c2a03b8ad215068ee95a5c08a93966907b660825705bb99d473d826faa7d3b0597a7b36194589b1c15823b*1a8c0e39d88a562eeb63*$/zip2$:Desktop/hashfile.txt:Files.zip:Files.zip
Files.zip/Desktop/hashfile1.txt:$zip2$*0*1*0*301537298b6beaa5*07bf*7f*f70ee56b3c3e1e2ae7627a70dd8f81e1162de1663c0b073787b6112ba8b1d6249bfe516e539202b09c330769717a373023d918cc2be7c5333e5d095
29bf844d740aabba8b032736b504428e2be7b4b8fbf0799e4aaa0b0018dfede36452c5ff1e985f4285e61d0d50decbc8b5f01f6fab61c871ec661e9fb77d6e1e1db4e6d*b9b1b5dfecd300d1db85*$/zip2$:Desktop/hashfile1.txt:Fi
les.zip:Files.zip
Files.zip/Desktop/single_mode.txt:$zip2$*0*1*0*a2119724e7a41393*f450*26*7dded668405989b8306b23054a0f91683b369e52268da64de9e3a8cc971e73abc982727f3c6a*4c95a452fc852a67e4b0*$/zip2$:Desktop/sin
gle_mode.txt:Files.zip:Files.zip
Files.zip/Desktop/wordlist.txt:$zip2$*0*1*0*16571563694387ce*0a91*75*12bd5d3c68dbea14683f73230fda07f20d576c5a3c952ca6222a2257730980823e32ae6aba653546c4c2b4c9e1e9d06de372b1d9f527d06a78ffe078
ea097df9ffaedf3c600c58a86fcde9afc4028ceb629fa68419cdfeed445e482dab31d13b282bc5662cf24f02684e910ac35d6ae5719c820092*5d8ea39f5cf76aa1474e*$/zip2$:Desktop/wordlist.txt:Files.zip:Files.zip
Files.zip/Desktop/wordlist1.txt:$zip2$*0*1*0*05b09b8756068138*7c2b*1c*b3bb81251f3f86d169802a9fa2cd5541a0bf8c65414127feaba16794*7f220eae25c48d517c7e*$/zip2$:Desktop/wordlist1.txt:Files.zip:F
iles.zip
```

Password cracking on zip files:



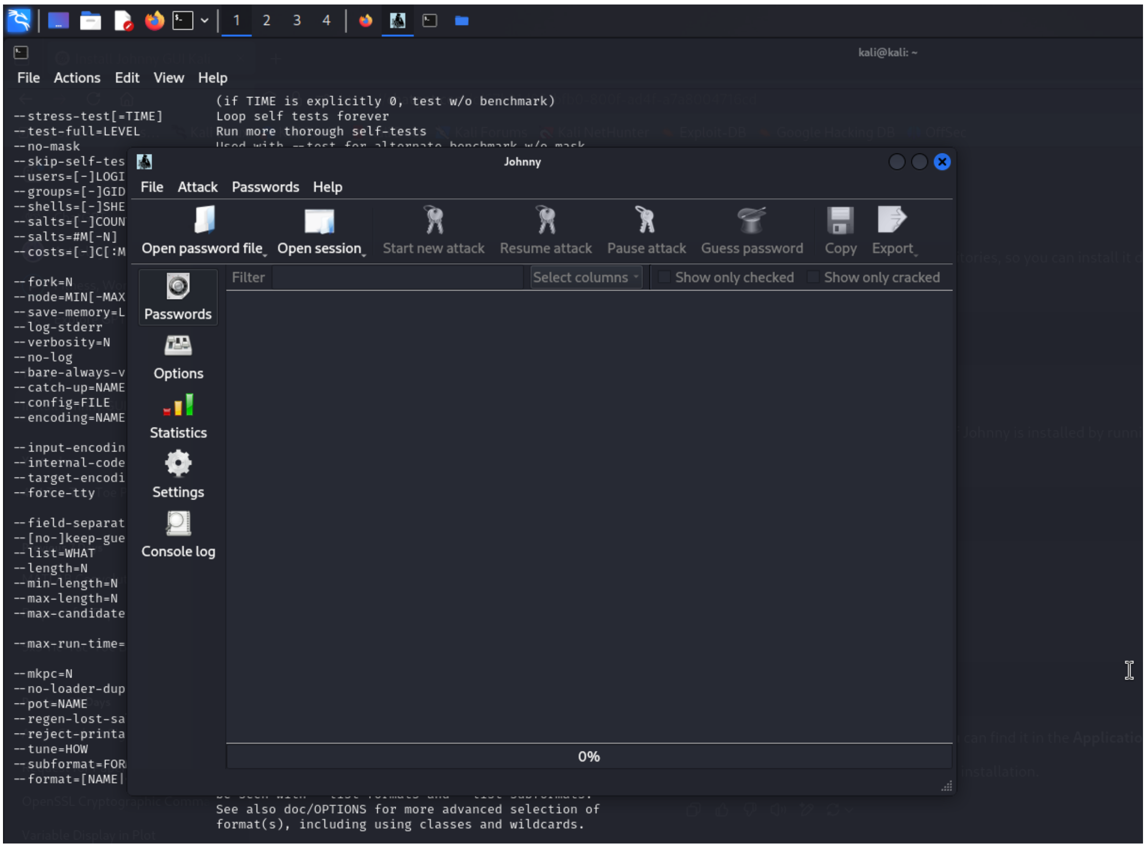
```
┌──(kali㉿kali)-[~/Downloads]
└─$ john zipHash.txt --wordlist=wordlist.txt
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (ZIP, WinZip [PBKDF2-SHA1 512/512 AVX512BW 16x])
Loaded hashes with cost 1 (HMAC size) varying from 28 to 148
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 22 candidates left, minimum 128 needed for performance.
abc123           (Files.zip/Desktop/hash.txt)
abc123           (Files.zip/Desktop/hashfile1.txt)
abc123           (Files.zip/Desktop/wordlist1.txt)
abc123           (Files.zip/Desktop/wordlist.txt)
abc123           (Files.zip/Desktop/single_mode.txt)
abc123           (Files.zip/Desktop/hash2.txt)
abc123           (Files.zip/Desktop/hashfile.txt)
7g 0:00:00:00 DONE (2025-02-17 14:22) 116.6g/s 366.6p/s 2566c/s 2566C/s hari1987..abc123
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

Exploring the John the Ripper GUI

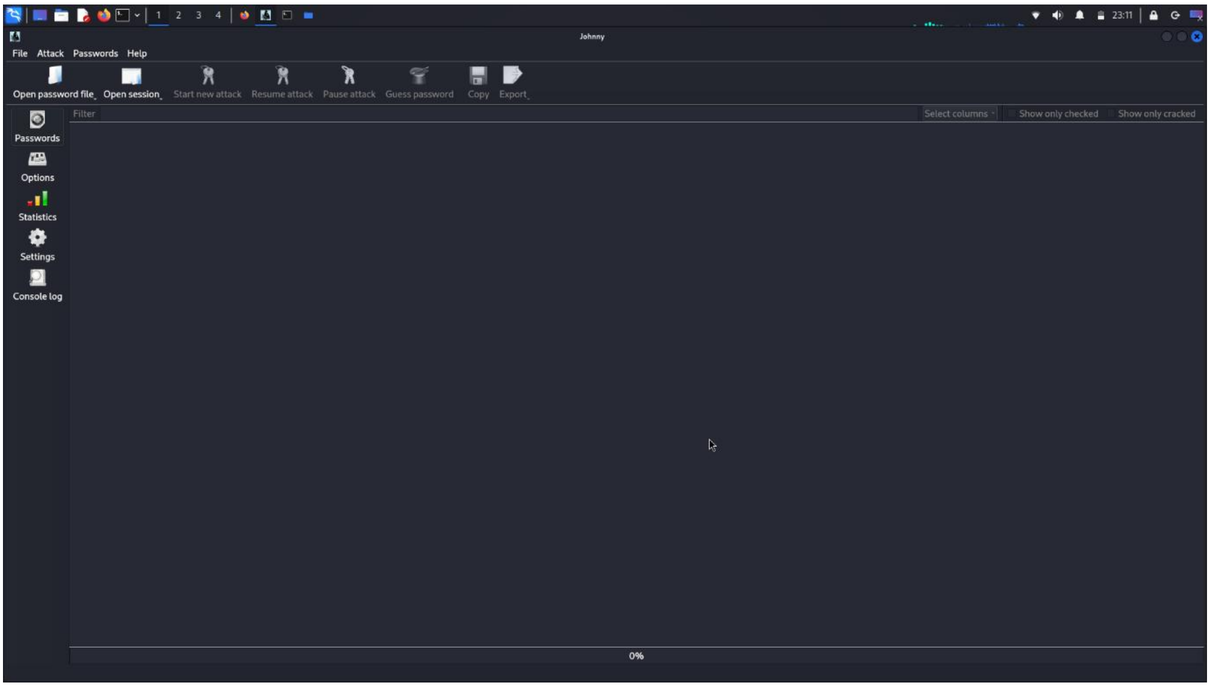


```
┌──(kali㉿kali)-[~]
└─$ sudo apt install johnny -y
Installing:
  johnny

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1275
  Download size: 545 kB
  Space needed: 944 kB / 7,563 MB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 johnny amd64 2.2+git2
0160807-0kali2+b1 [545 kB]
Fetched 545 kB in 1s (823 kB/s)
Selecting previously unselected package johnny.
(Reading database ... 422987 files and directories currently installed.)
Preparing to unpack .../johnny_2.2+git20160807-0kali2+b1_amd64.deb ...
Unpacking johnny (2.2+git20160807-0kali2+b1) ...
Setting up johnny (2.2+git20160807-0kali2+b1) ...
Processing triggers for kali-menu (2024.4.0) ...
```

GUI:



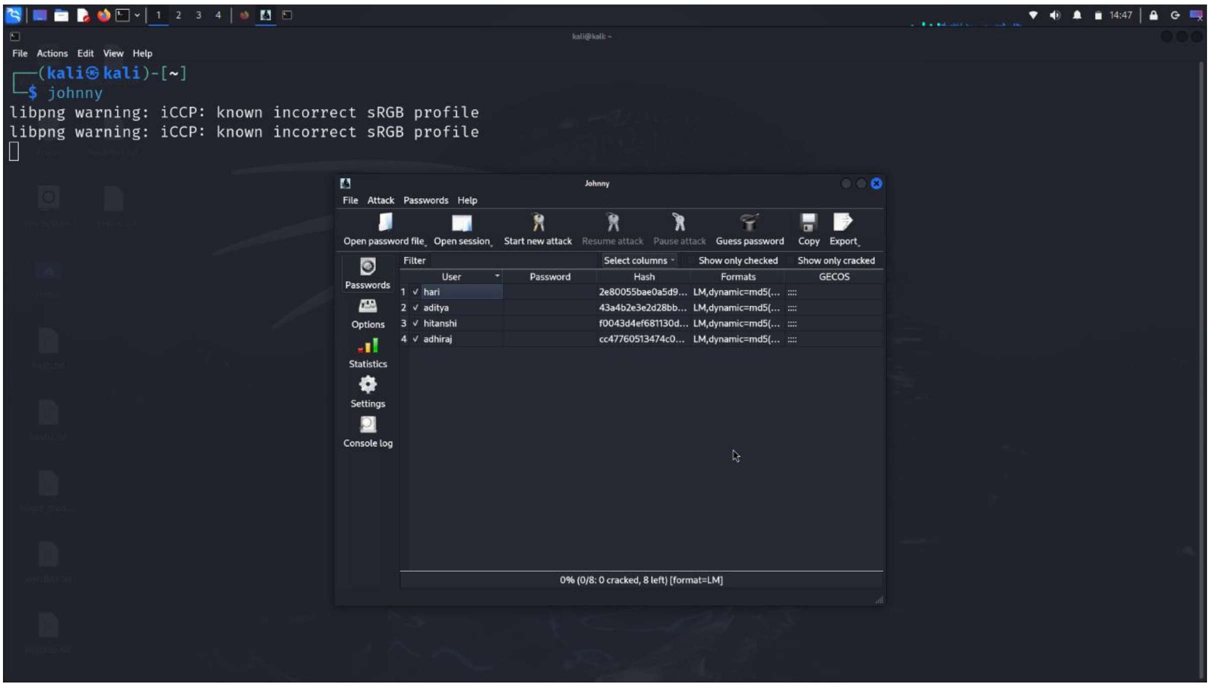
```
                                (if TIME is explicitly 0, test w/o benchmark)
--stress-test[=TIME]            Loop self tests forever
--test-full=LEVEL               Run more thorough self-tests
--no-mask
--skip-self-tes
--users=[-]LOGI
--groups=[-]GID
--shells=[-]SHE
--salts=[-]COUN
--salts=#M[-N]
--costs=[-]C[:M

--fork=N
--node=MIN[-MAX
--save-memory=L
--log-stderr
--verbosity=N
--no-log
--bare-always-v
--catch-up=NAME
--config=FILE
--encoding=NAME

--input-encodin
--internal-code
--target-encodi
--force-tty

--field-separat
--[no-]keep-gue
--list=WHAT
--length=N
--min-length=N
--max-length=N
--max-candidate

--max-run-time=

--mkpc=N
--no-loader-dup
--pot=NAME
--regen-lost-sa
--reject-printa
--tune=HOW
--subformat=FOR
--format=[NAME|
                                See also doc/OPTIONS for more advanced selection of
                                format(s), including using classes and wildcards.
```


Johnny
File Attack Passwords Help
Open password file Open session Start new attack Resume attack Pause attack Guess password Copy Export
Passwords
Options
Statistics
Settings
Console log
Filter
Select columns
Show only checked
Show only cracked

0%

GUI Mode: Multi-Mode Demonstration

Open Password file:

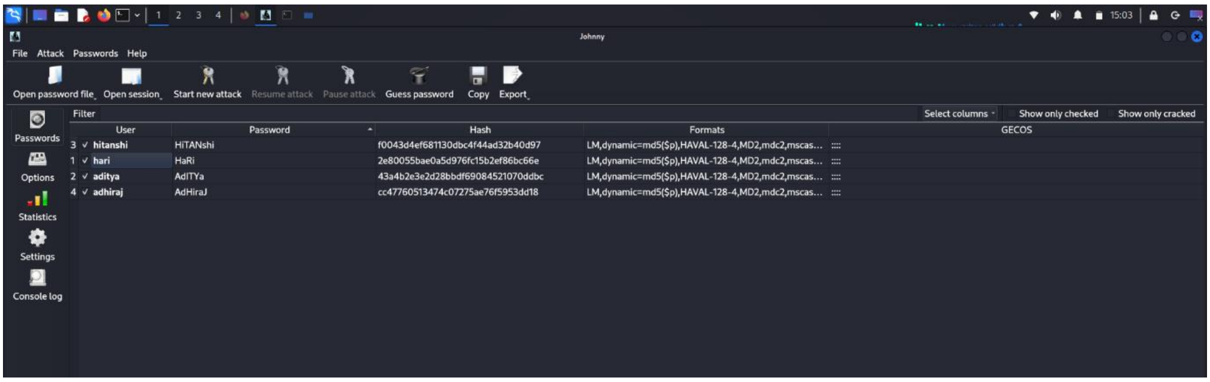

File Actions Edit View Help
Johnny
File Attack Passwords Help
Open password file Open session Start new attack Resume attack Pause attack Guess password Copy Export
Passwords
Options
Statistics
Settings
Console log
Filter
Select columns
Show only checked
Show only cracked

```
┌──(kali㉿kali)-[~]
└─$ johnny
libpng warning: iCCP: known incorrect sRGB profile
libpng warning: iCCP: known incorrect sRGB profile
```

		User	Password	Hash	Formats	GECOS
1	✓	hari		2e80055bae0a5d9…	LM,dynamic=md5(…	::::
2	✓	aditya		43a4b2e3e2d28bb…	LM,dynamic=md5(…	::::
3	✓	hitanshi		f0043d4ef681130d…	LM,dynamic=md5(…	::::
4	✓	adhiraj		cc47760513474c0…	LM,dynamic=md5(…	::::

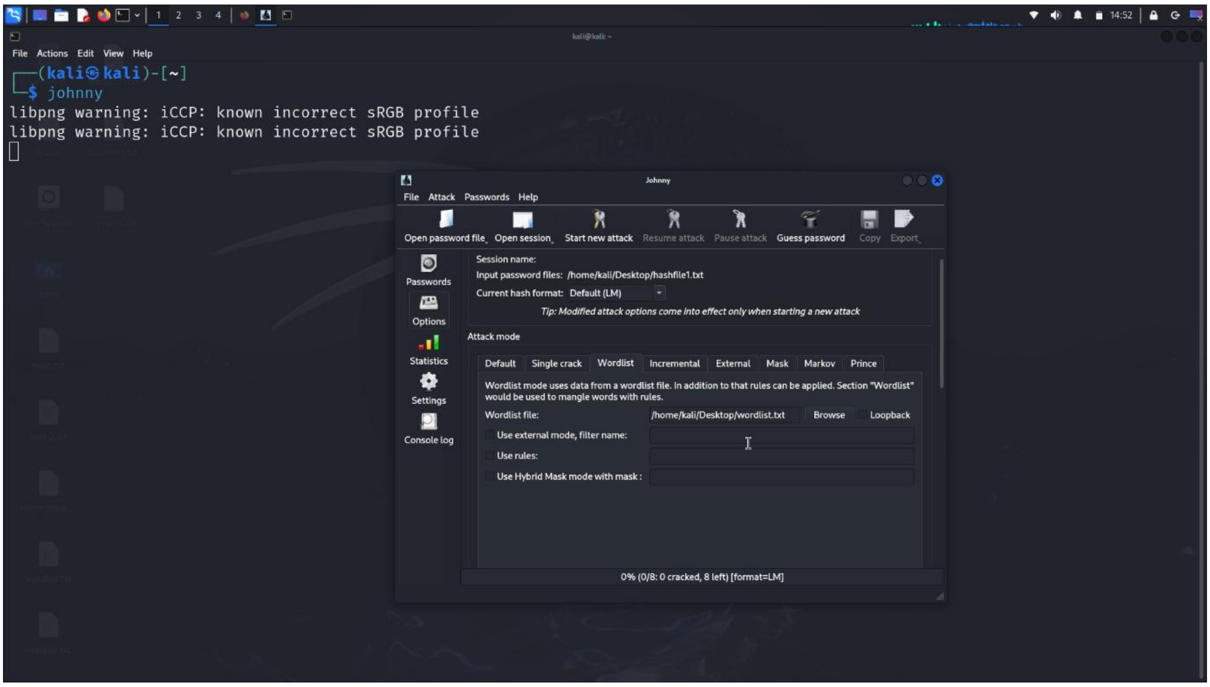
0% (0/8: 0 cracked, 8 left) [format=LM]

Using Single Crack mode:


Johnny
File Attack Passwords Help
Open password file Open session Start new attack Resume attack Pause attack Guess password Copy Export
Passwords
Options
Statistics
Settings
Console log
Filter
Select columns
Show only checked
Show only cracked

		User	Password	Hash	Formats	GECOS
3	✓	hitanshi	HiTANshi	f0043d4ef681130dbc4f44ad32b40d97	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	::::
1	✓	hari	HaRi	2e80055bae0a5d976fc15b2ef86bc66e	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	::::
2	✓	aditya	AdITYa	43a4b2e3e2d28bbdf69084521070ddbc	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	::::
4	✓	adhiraj	AdHiraJ	cc47760513474c07275ae76f5953dd18	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	::::

Open wordlist file:


kali@kali: ~
File Actions Edit View Help
Johnny
File Attack Passwords Help
Open password file Open session Start new attack Resume attack Pause attack Guess password Copy Export
Passwords
Options
Statistics
Settings
Console log
Attack mode
Default Single crack Wordlist Incremental External Mask Markov Prince
Browse

```
┌──(kali㉿kali)-[~]
└─$ johnny
libpng warning: iCCP: known incorrect sRGB profile
libpng warning: iCCP: known incorrect sRGB profile
```

Session name:

Input password files: /home/kali/Desktop/hashfile1.txt

Current hash format: Default (LM)

Tip: Modified attack options come into effect only when starting a new attack

Wordlist mode uses data from a wordlist file. In addition to that rules can be applied. Section "Wordlist" would be used to mangle words with rules.

Wordlist file: /home/kali/Desktop/wordlist.txt

□ Loopback

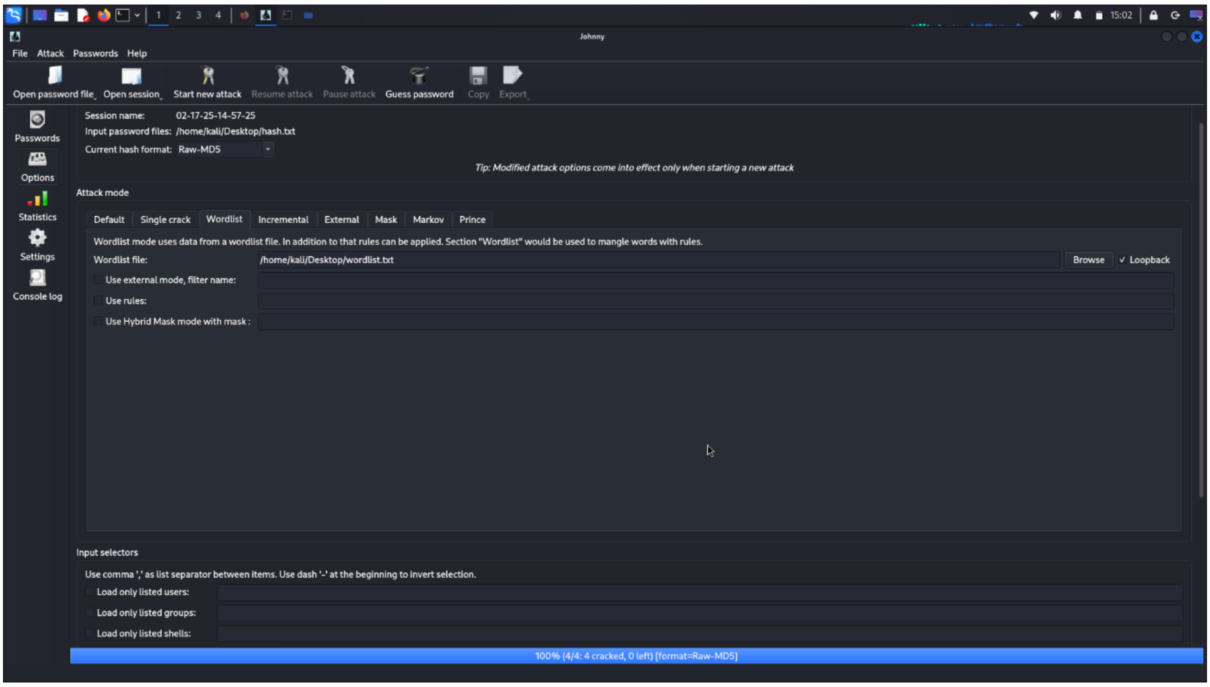
□ Use external mode, filter name:

□ Use rules:

□ Use Hybrid Mask mode with mask :

0% (0/8: 0 cracked, 8 left) [format=LM]

Using wordlist mode:



Session name: 02-17-25-14-57-25
Input password files: /home/kali/Desktop/hash.txt
Current hash format: Raw-MD5

Tip: Modified attack options come into effect only when starting a new attack

Attack mode

Default | Single crack | Wordlist | Incremental | External | Mask | Markov | Prince

Wordlist mode uses data from a wordlist file. In addition to that rules can be applied. Section "Wordlist" would be used to mangle words with rules.

Wordlist file: /home/kali/Desktop/wordlist.txt Browse ✓ Loopback

□ Use external mode, filter name:

□ Use rules:

□ Use Hybrid Mask mode with mask :

Input selectors

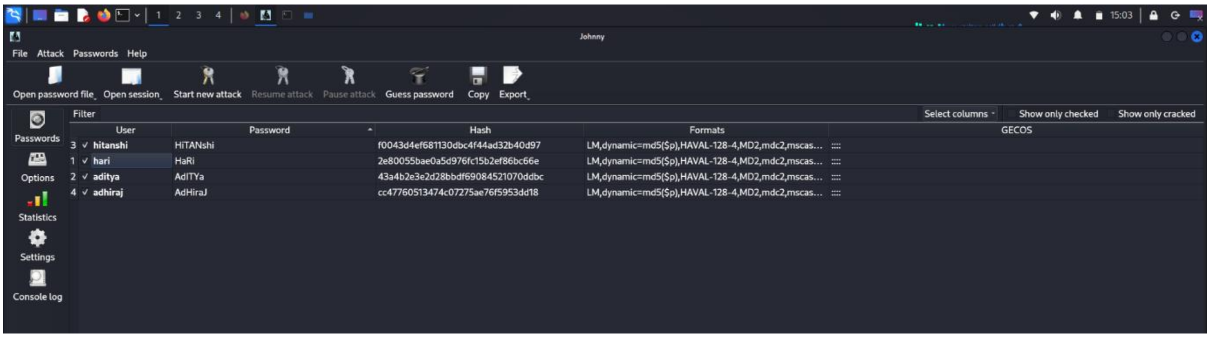
Use comma ',' as list separator between items. Use dash '-' at the beginning to invert selection.

□ Load only listed users:

□ Load only listed groups:

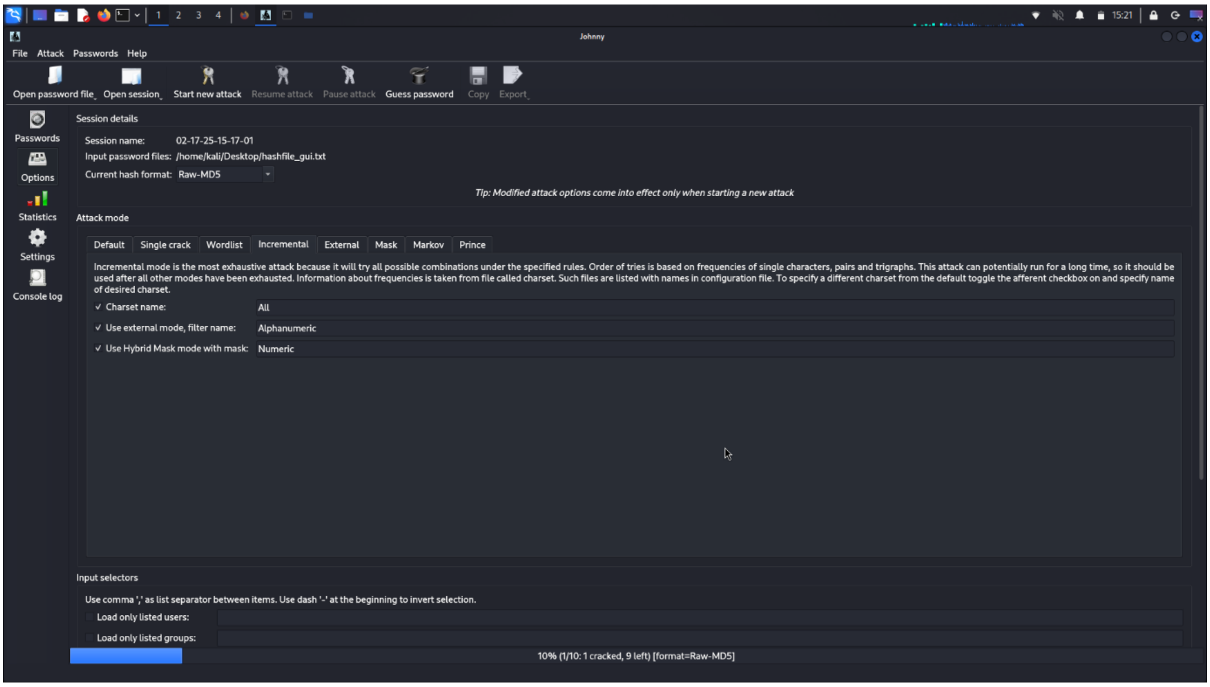
□ Load only listed shells:

100% (4/4: 4 cracked, 0 left) [format=Raw-MD5]



		User	Password	Hash	Formats	GECOS
3	✓	hitanshi	HiTANshi	f0043d4ef681130dbc4f44ad32b40d97	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	::::
1	✓	hari	HaRi	2e80055bae0a5d976fc15b2ef86bc66e	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	::::
2	✓	aditya	AdITYa	43a4b2e3e2d28bbdf69084521070ddbc	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	::::
4	✓	adhiraj	AdHiraJ	cc47760513474c07275ae76f5953dd18	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	::::

Using Incremental mode:


Johnny
File Attack Passwords Help
Open password file Open session Start new attack Resume attack Pause attack Guess password Copy Export
Passwords
Options
Statistics
Settings
Console log

Session details

Session name: 02-17-25-15-17-01
Input password files: /home/kali/Desktop/hashfile_gui.txt
Current hash format: Raw-MD5

Tip: Modified attack options come into effect only when starting a new attack

Attack mode

Default | Single crack | Wordlist | Incremental | External | Mask | Markov | Prince

Incremental mode is the most exhaustive attack because it will try all possible combinations under the specified rules. Order of tries is based on frequencies of single characters, pairs and trigraphs. This attack can potentially run for a long time, so it should be used after all other modes have been exhausted. Information about frequencies is taken from file called charset. Such files are listed with names in configuration file. To specify a different charset from the default toggle the afferent checkbox on and specify name of desired charset.

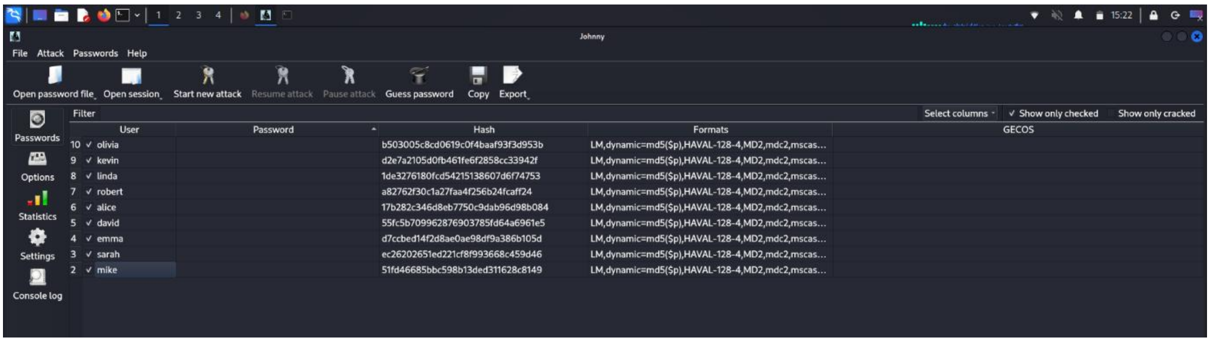
✓ Charset name: All
✓ Use external mode, filter name: Alphanumeric
✓ Use Hybrid Mask mode with mask: Numeric

Input selectors

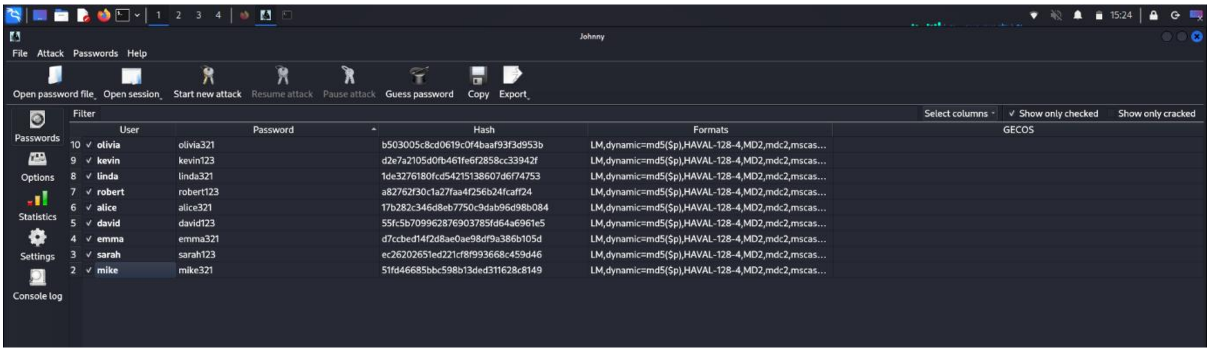
Use comma ',' as list separator between items. Use dash '-' at the beginning to invert selection.

□ Load only listed users:
□ Load only listed groups:

10% (1/10: 1 cracked, 9 left) [format=Raw-MD5]


Johnny
File Attack Passwords Help
Open password file Open session Start new attack Resume attack Pause attack Guess password Copy Export
Passwords
Options
Statistics
Settings
Console log
Filter
Select columns
✓ Show only checked
Show only cracked

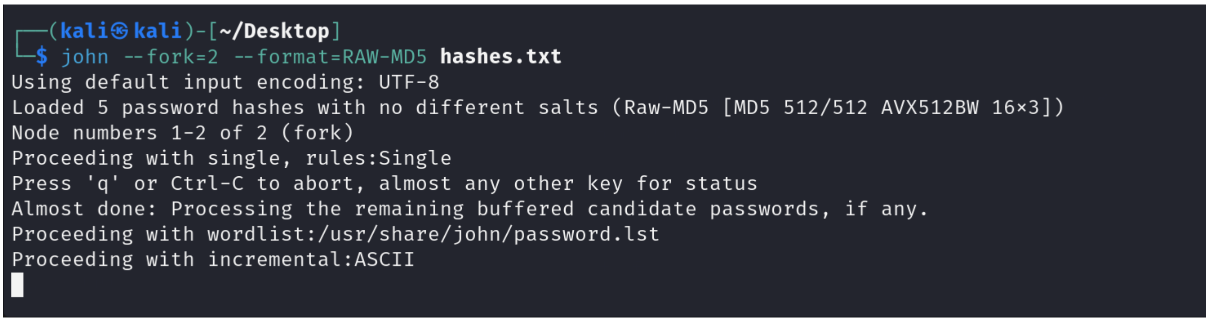
		User	Password	Hash	Formats	GECOS
10	✓	olivia		b503005c8cd0619c0f4baaf93f3d953b	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
9	✓	kevin		d2e7a2105d0fb461fe6f2858cc33942f	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
8	✓	linda		1de3276180fcd54215138607d6f74753	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
7	✓	robert		a82762f30c1a27faa4f256b24fcaff24	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
6	✓	alice		17b282c346d8eb7750c9dab96d98b084	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
5	✓	david		55fc5b709962876903785fd64a6961e5	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
4	✓	emma		d7ccbed14f2d8ae0ae98df9a386b105d	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
3	✓	sarah		ec26202651ed221cf8f993668c459d46	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
2	✓	mike		51fd46685bbc598b13ded311628c8149	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	


Johnny
File Attack Passwords Help
Open password file Open session Start new attack Resume attack Pause attack Guess password Copy Export
Passwords
Options
Statistics
Settings
Console log
Filter
Select columns
✓ Show only checked
Show only cracked

		User	Password	Hash	Formats	GECOS
10	✓	olivia	olivia321	b503005c8cd0619c0f4baaf93f3d953b	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
9	✓	kevin	kevin123	d2e7a2105d0fb461fe6f2858cc33942f	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
8	✓	linda	linda321	1de3276180fcd54215138607d6f74753	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
7	✓	robert	robert123	a82762f30c1a27faa4f256b24fcaff24	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
6	✓	alice	alice321	17b282c346d8eb7750c9dab96d98b084	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
5	✓	david	david123	55fc5b709962876903785fd64a6961e5	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
4	✓	emma	emma321	d7ccbed14f2d8ae0ae98df9a386b105d	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
3	✓	sarah	sarah123	ec26202651ed221cf8f993668c459d46	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	
2	✓	mike	mike321	51fd46685bbc598b13ded311628c8149	LM,dynamic=md5($p),HAVAL-128-4,MD2,mdc2,mscas...	

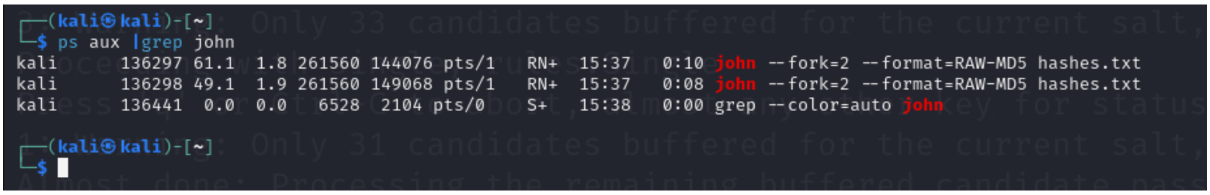
Implementing fork() for Multiprocessing

Using 2 Forks:



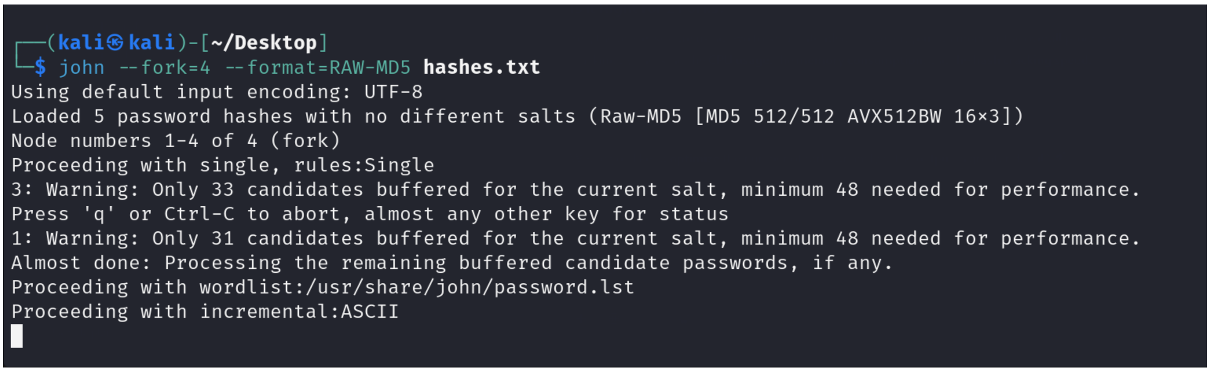
```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --fork=2 --format=RAW-MD5 hashes.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 512/512 AVX512BW 16×3])
Node numbers 1-2 of 2 (fork)
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost 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
█
```

Verifying Forked John the Ripper Processes with ps aux:



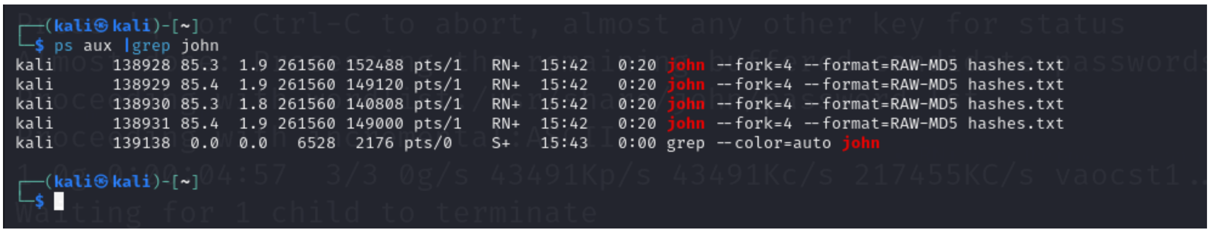
```
┌──(kali㉿kali)-[~]
└─$ ps aux |grep john
kali      136297 61.1  1.8 261560 144076 pts/1   RN+  15:37   0:10 john --fork=2 --format=RAW-MD5 hashes.txt
kali      136298 49.1  1.9 261560 149068 pts/1   RN+  15:37   0:08 john --fork=2 --format=RAW-MD5 hashes.txt
kali      136441  0.0  0.0   6528  2104 pts/0    S+   15:38   0:00 grep --color=auto john

┌──(kali㉿kali)-[~]
└─$ █
```

Using 4 Forks:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --fork=4 --format=RAW-MD5 hashes.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 512/512 AVX512BW 16×3])
Node numbers 1-4 of 4 (fork)
Proceeding with single, rules:Single
3: Warning: Only 33 candidates buffered for the current salt, minimum 48 needed for performance.
Press 'q' or Ctrl-C to abort, almost any other key for status
1: Warning: Only 31 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
█
```

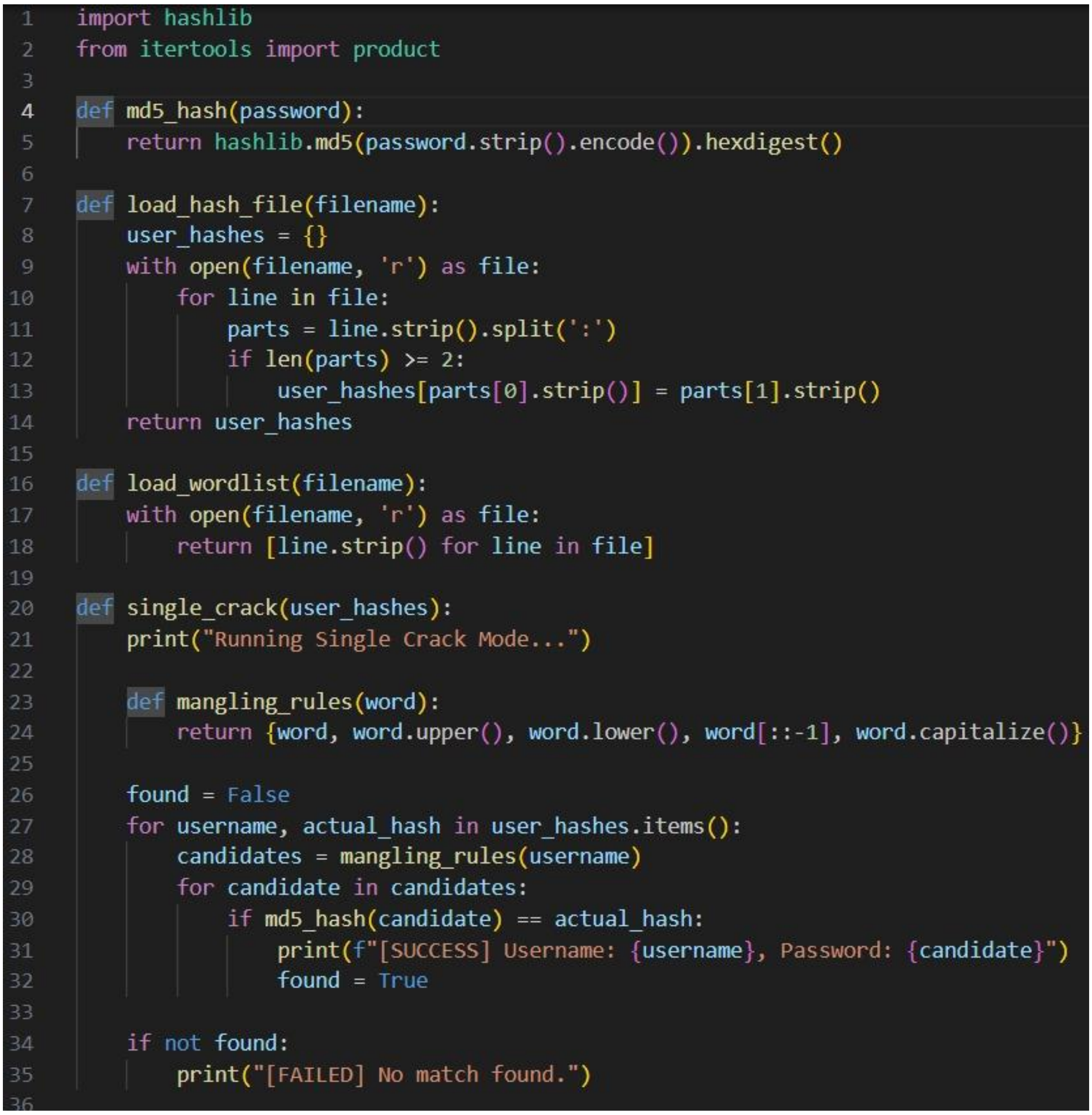
Verifying Forked John the Ripper Processes with ps aux:



```
┌──(kali㉿kali)-[~]
└─$ ps aux |grep john
kali      138928 85.3  1.9 261560 152488 pts/1   RN+  15:42   0:20 john --fork=4 --format=RAW-MD5 hashes.txt
kali      138929 85.4  1.9 261560 149120 pts/1   RN+  15:42   0:20 john --fork=4 --format=RAW-MD5 hashes.txt
kali      138930 85.3  1.8 261560 140808 pts/1   RN+  15:42   0:20 john --fork=4 --format=RAW-MD5 hashes.txt
kali      138931 85.4  1.9 261560 149000 pts/1   RN+  15:42   0:20 john --fork=4 --format=RAW-MD5 hashes.txt
kali      139138  0.0  0.0   6528  2176 pts/0    S+   15:43   0:00 grep --color=auto john

┌──(kali㉿kali)-[~]
└─$ █
```

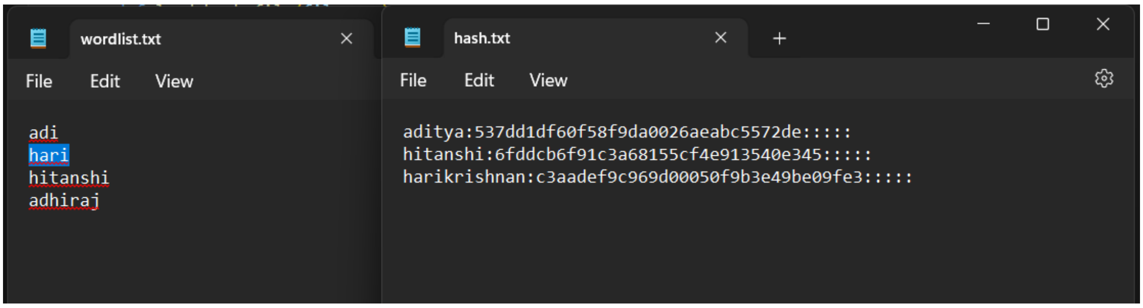
Basic Implementation of John the Ripper in Python

Python code (Full code Uploaded on GitHub):



```python
import hashlib
from itertools import product

def md5_hash(password):
    return hashlib.md5(password.strip().encode()).hexdigest()

def load_hash_file(filename):
    user_hashes = {}
    with open(filename, 'r') as file:
        for line in file:
            parts = line.strip().split(':')
            if len(parts) >= 2:
                user_hashes[parts[0].strip()] = parts[1].strip()
    return user_hashes

def load_wordlist(filename):
    with open(filename, 'r') as file:
        return [line.strip() for line in file]

def single_crack(user_hashes):
    print("Running Single Crack Mode...")

    def mangling_rules(word):
        return {word, word.upper(), word.lower(), word[::-1], word.capitalize()}

    found = False
    for username, actual_hash in user_hashes.items():
        candidates = mangling_rules(username)
        for candidate in candidates:
            if md5_hash(candidate) == actual_hash:
                print(f"[SUCCESS] Username: {username}, Password: {candidate}")
                found = True

    if not found:
        print("[FAILED] No match found.")
```

Files:

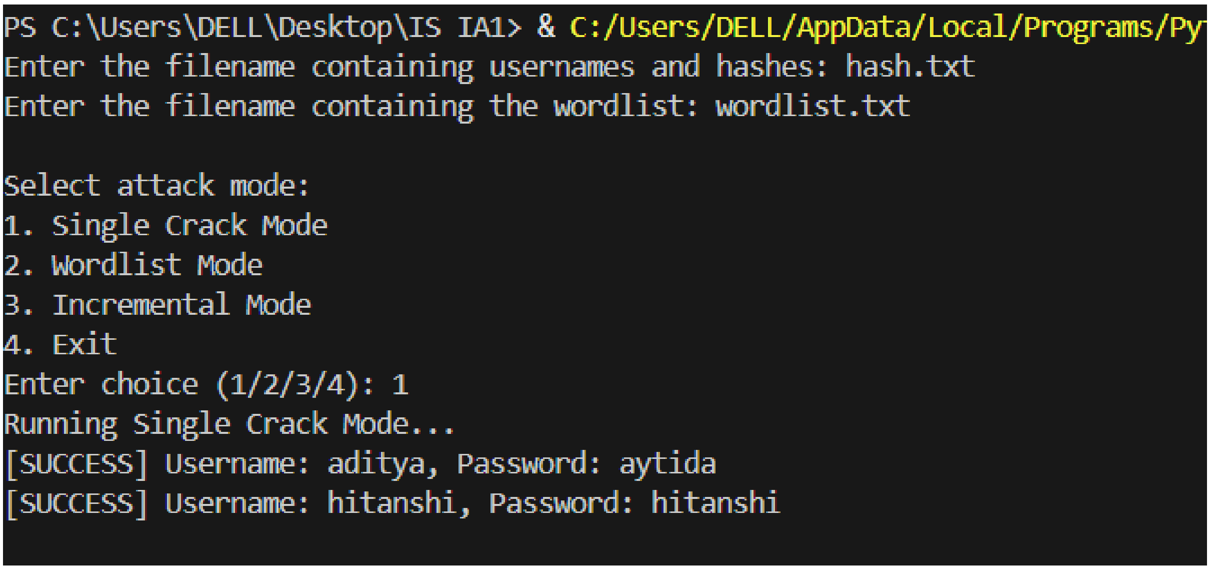


```
adi
hari
hitanshi
adhiraj
```

```
aditya:537dd1df60f58f9da0026aeabc5572de:::::
hitanshi:6fddcb6f91c3a68155cf4e913540e345:::::
harikrishnan:c3aadef9c969d00050f9b3e49be09fe3:::::
```

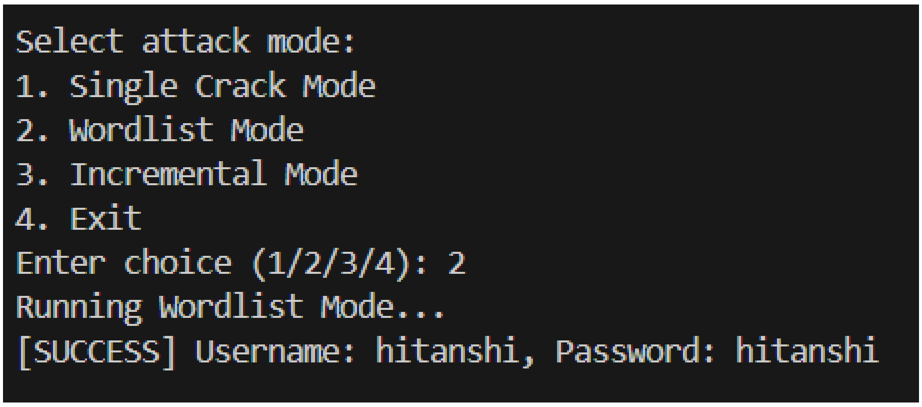
Output:

Using Single Crack Mode:



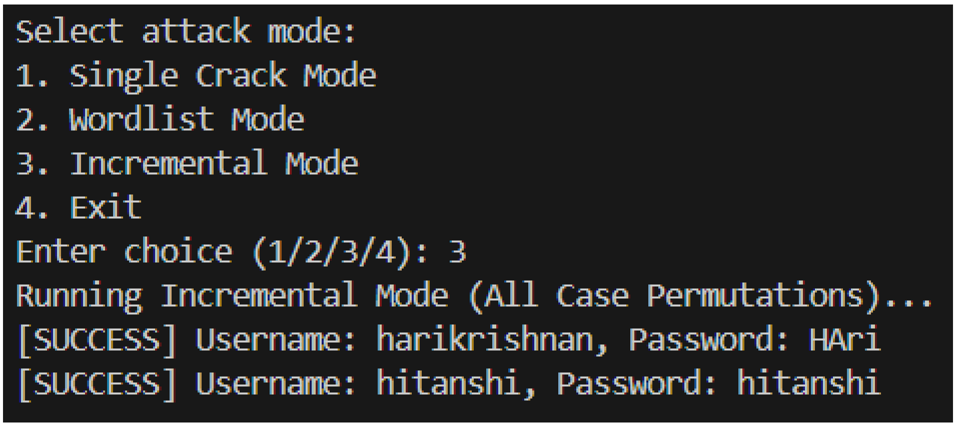
```
PS C:\Users\DELL\Desktop\IS IA1> & C:/Users/DELL/AppData/Local/Programs/Py
Enter the filename containing usernames and hashes: hash.txt
Enter the filename containing the wordlist: wordlist.txt

Select attack mode:
1. Single Crack Mode
2. Wordlist Mode
3. Incremental Mode
4. Exit
Enter choice (1/2/3/4): 1
Running Single Crack Mode...
[SUCCESS] Username: aditya, Password: aytida
[SUCCESS] Username: hitanshi, Password: hitanshi
```

Using Wordlist mode:



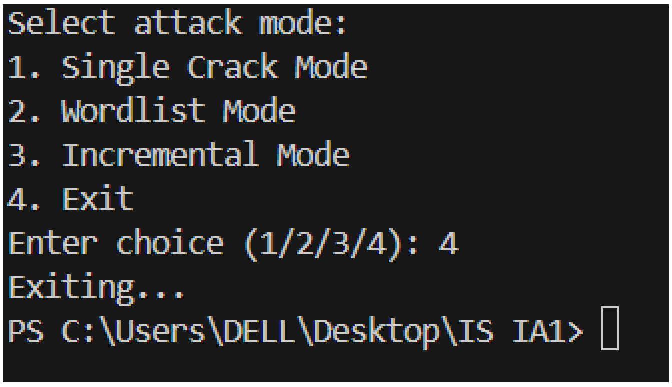
```
Select attack mode:
1. Single Crack Mode
2. Wordlist Mode
3. Incremental Mode
4. Exit
Enter choice (1/2/3/4): 2
Running Wordlist Mode...
[SUCCESS] Username: hitanshi, Password: hitanshi
```

Using Incremental mode:



```
Select attack mode:
1. Single Crack Mode
2. Wordlist Mode
3. Incremental Mode
4. Exit
Enter choice (1/2/3/4): 3
Running Incremental Mode (All Case Permutations)...
[SUCCESS] Username: harikrishnan, Password: HAri
[SUCCESS] Username: hitanshi, Password: hitanshi
```

Exit:



```
Select attack mode:
1. Single Crack Mode
2. Wordlist Mode
3. Incremental Mode
4. Exit
Enter choice (1/2/3/4): 4
Exiting...
PS C:\Users\DELL\Desktop\IS IA1>
```