

```
kali_linux_Daniel_Salvador Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ zip2john /home/kali/Desktop/confi.zip
Created directory: /home/kali/.john
ver 2.0 efh 5455 efh 7875 confi.zip/confidencial.gif PKZIP Encr: TS_chk, cmplen=126, decmplen=116, crc=380A77C8 ts=9
3D6 cs=93d6 type=8
confi.zip/confidencial.gif:$pkzip$1*1*2*0*7e*74*380a77c8*0*4a*8*7e*93d6*2a7e4be3f4f978e2026a5856140c06cbcb2e8542b949
23fdc645e8cd94ef5ee5b849da69b3a0f89750e6a6d4ed69e680775e49188f006bde071a74b0dbcbd091bfc4f16e024d7f0d70d8d0fce345a2
43e23a77060c9c899ffeeb571ecd4a4f82613c810ee9eddb74173f2ebdb6e41f5f0ec5d957669d5df790165ddd*$ /pkzip$:confidencial.g
if:confi.zip::/home/kali/Desktop/confi.zip
(kali@kali)-[~]
$ zip2john /home/kali/Desktop/confi.zip > confi-Daniel_Salvador.txt
ver 2.0 efh 5455 efh 7875 confi.zip/confidencial.gif PKZIP Encr: TS_chk, cmplen=126, decmplen=116, crc=380A77C8 ts=9
3D6 cs=93d6 type=8
```

```
kali_linux_Daniel_Salvador Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
$ hashcat -h | grep -i zip
11600 | 7-Zip | Archive
17220 | PKZIP (Compressed Multi-File) | Archive
17200 | PKZIP (Compressed) | Archive
17225 | PKZIP (Mixed Multi-File) | Archive
17230 | PKZIP (Mixed Multi-File Checksum-Only) | Archive
17210 | PKZIP (Uncompressed) | Archive
20500 | PKZIP Master Key | Archive
20510 | PKZIP Master Key (6 byte optimization) | Archive
23001 | SecureZIP AES-128 | Archive
23002 | SecureZIP AES-192 | Archive
23003 | SecureZIP AES-256 | Archive
13600 | WinZip | Archive
(kali@kali)-[~]
```

```
kali_linux_Daniel_Salvador Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
[sudo] password for kali:
(kali@kali)-[~]
$ ls /usr/share/wordlists
amass dirbuster fern-wifi legion nmap.lst sqlmap.txt wifite.txt
dirb fasttrack.txt john.lst metasploit rockyou.txt wfuzz
(kali@kali)-[~]
$ hashcat -m CODI -a 0 confi-Daniel_Salvador.txt /usr/share/wordlists/rockyou.txt
The specified parameter cannot use 'CODI' as a value - must be a number.
```


File Machine View Input Devices Help

1 2 3 4

10:19

kali@kali: ~

File Actions Edit View Help

```

kali@kali:~$ hashcat -m 17220 -a 0 conf-Daniel_Salvador.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

```

```

OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEP, DISTRO, POCL_DEBUG) -
Platform #1 [The pocl project]

```

```

* Device #1: pthread-sandybridge-Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz, 2358/4781 MB (1024 MB allocatable), 2MCU

```

```

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
Rules: 1

```

```

Optimizers applied:

```

```

* Not-Iterated
* Single-Hash
* Single-Salt

```

```

Watchdog: Temperature abort trigger set to 90c

```

```

Host memory required for this attack: 0 MB

```

```

Dictionary cache built:

```

```

* Filename ..: /usr/share/wordlists/rockyou.txt
* Passwords..: 14344392
* Bytes.....: 139921507
* Keyspace...: 14344385
* Runtime ...: 1 sec

```

```

$pkzip$1*1*2*0*7e*7a*380a77c8*0*4a*8*7e*93d6*2a7e4be3f4f978e2026a5856140c06cbb2e8542b94923fdc645e8cdbc94ef5ee5b849d
a69b3a0f89750e6a6d4ed69e680775e49188f006bde071a74b0dbcbdb091bfc4f16e024d7f0d70d8d0fce345a243e23a77060c9c899ffeeb571ec
daa4f82613c810ee9eddb74173f2ebdb6e41f5f0ec5d957669d5df790165ddddd*$/pkzip$:P@ssw0rd!

```

```

Session.....: hashcat

```

```

Status.....: Cracked

```

```

Hash.Mode.....: 17220 (PKZIP (Compressed Multi-File))

```

```

Hash.Target.....: $pkzip$1*1*2*0*7e*7a*380a77c8*0*4a*8*7e*93d6*2a7e4b ... pkzip$

```

```

Time.Started.....: Wed Sep 27 10:02:43 2023 (1 sec)

```

```

Time.Estimated...: Wed Sep 27 10:02:44 2023 (0 secs)

```

```

Kernel.Feature...: Pure Kernel

```

```

Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)

```

```

Guess.Queue.....: 1/1 (100.00%)

```

```

Speed.#1.....: 2299.5 kH/s (0.26ms) @ Accel:512 Loops:1 Thr:1 Vec:8

```

```

Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)

```

```

Progress.....: 2106368/14344385 (14.68%)

```

```

Rejected.....: 0/2106368 (0.00%)

```

```

Restore.Point...: 2105344/14344385 (14.68%)

```

```

Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1

```

```

Candidate.Engine.: Device Generator

```

```

Candidates.#1...: PECKHAM -> Olguin!

```

```

Hardware.Mon.#1..: Util: 80%

```

```

Started: Wed Sep 27 10:02:07 2023

```

```

Stopped: Wed Sep 27 10:02:46 2023

```

```

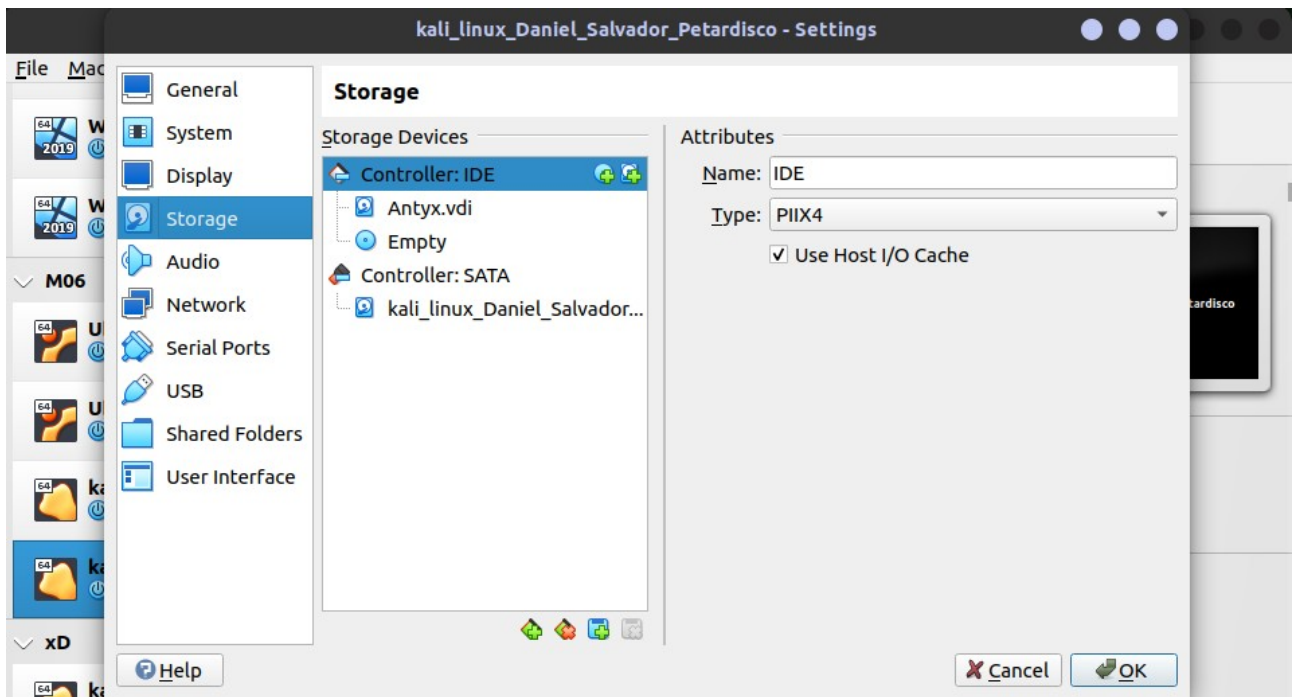
kali@kali:~$ hashcat --show -m 17220 -a 0 conf-Daniel_Salvador.txt /usr/share/wordlists/rockyou.txt

```

```

$pkzip$1*1*2*0*7e*7a*380a77c8*0*4a*8*7e*93d6*2a7e4be3f4f978e2026a5856140c06cbb2e8542b94923fdc645e8cdbc94ef5ee5b849d
a69b3a0f89750e6a6d4ed69e680775e49188f006bde071a74b0dbcbdb091bfc4f16e024d7f0d70d8d0fce345a243e23a77060c9c899ffeeb571ec
daa4f82613c810ee9eddb74173f2ebdb6e41f5f0ec5d957669d5df790165ddddd*$/pkzip$:P@ssw0rd!

```



kali@kali: ~

File Actions Edit View Help

Disk identifier: 0xdcf83301

Device	Boot	Start	End	Sectors	Size	Id	Type
/dev/sda1	*	2048	102856703	102854656	49G	83	Linux
/dev/sda2		102858750	104855551	1996802	975M	f	W95 Ext'd (LBA)
/dev/sda5		102858752	104855551	1996800	975M	82	Linux swap / Solaris

Disk /dev/sdb: 8 GiB, 8589934592 bytes, 16777216 sectors

Disk model: VBOX HARDDISK

Units: sectors of 1 * 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes

Disklabel type: dos

Disk identifier: 0xfb6f555a

Device	Boot	Start	End	Sectors	Size	Id	Type
/dev/sdb1		2048	16777215	16775168	8G	83	Linux

(kali@kali)-[~]

\$

Screenshot taken

View image

Screenshot taken

View image

KALI LINUX

"the quieter you become, the more you are able to hear"


```
kali_linux_Daniel_Salvador_Petardisco [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 2
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ history
1 hashcat -h | grep -i zip
2 ls Desktop
3 cd /media/kali
4 ls
5 cd rootantiX19
6 ls
7 ls /etc/passwd
8 ls etc/passwd
9 ls /media/kali/rootantiX19/etc/passwd
10 less /media/kali/rootantiX19/etc/passwd
11 sudo cp /media/kali/rootantiX19/etc/passwd /home/kali/Desktop
12 less /media/kali/rootantiX19/etc/shadow
13 sudo less /media/kali/rootantiX19/etc/shadow
14 sudo cp /media/kali/rootantiX19/etc/shadow /home/kali/Desktop
(kali@kali)-[~]
```

```
kali_linux_Daniel_Salvador_Petardisco [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 2
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo unshadow Desktop/passwd_DanielSlavador Desktop/shadow_DanielSalvador > passwords-DanielSalvador
(kali@kali)-[~]
$
File System
Home
```

```
kali_linux_Daniel_Salvador_Petardisco [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo unshadow Desktop/passwd_DanielSlavador Desktop/shadow_DanielSalvador > passwords-DanielSalvador

(kali@kali)-[~]
$ john --wordlist=/usr/share/wordlists/500-worst-passwords.txt --rules passwords-DanielSalvador
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
```

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo unshadow Desktop/passwd_DanielSlavador Desktop/shadow_DanielSalvador > passwords-DanielSalvador

(kali@kali)-[~]
$ john --wordlist=/usr/share/wordlists/500-worst-passwords.txt --rules passwords-DanielSalvador
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
packers1 (albert)
1g 0:00:00:31 25.29% (ETA: 13:55:01) 0.03213g/s 189.2p/s 1390c/s 1390C/s orange9..zxcvbn9
1g 0:00:00:33 26.79% (ETA: 13:55:02) 0.03023g/s 189.6p/s 1389c/s 1389C/s music9..booboo5
1g 0:00:00:35 28.28% (ETA: 13:55:02) 0.02849g/s 189.6p/s 1389c/s 1389C/s naked5..heather4
1g 0:00:00:39 31.22% (ETA: 13:55:03) 0.02561g/s 190.1p/s 1390c/s 1390C/s bronco8..movie8
1g 0:00:01:14 63.64% (ETA: 13:54:55) 0.01350g/s 195.2p/s 1392c/s 1392C/s Scorpion9..xxxxxx5
1g 0:00:01:49 90.34% (ETA: 13:54:59) 0.009170g/s 196.0p/s 1394c/s 1394C/s wizarded..zzzzzzed
1g 0:00:01:57 DONE (2023-09-29 13:54) 0.008540g/s 197.0p/s 1394c/s 1394C/s Animaling..Alberting
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~]
$
```

Invalid options combination: "--show"

```
(kali㉿kali)-[~]  
$ john --show passwords-DanielSalvador  
albert:packers1:1004:1004:,,,:/home/albert:/bin/bash
```

1 password hash cracked, 7 left

```
(kali㉿kali)-[~]  
$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
```

```
(kali㉿kali)-[~]  
$ john --show --wordlist=/usr/share/wordlists/rockyou.txt passwords-DanielSalvador  
Invalid options combination: "--show"
```

```
(kali㉿kali)-[~]  
$ john --wordlist=/usr/share/wordlists/rockyou.txt --rules passwords-DanielSalvador  
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"  
Use the "--format=HMAC-SHA256" option to force loading these as that type instead  
Using default input encoding: UTF-8  
Loaded 8 password hashes with 8 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])  
Remaining 7 password hashes with 7 different salts  
Cost 1 (iteration count) is 5000 for all loaded hashes  
Press 'q' or Ctrl-C to abort, almost any other key for status  
maria (maria)  
█
```