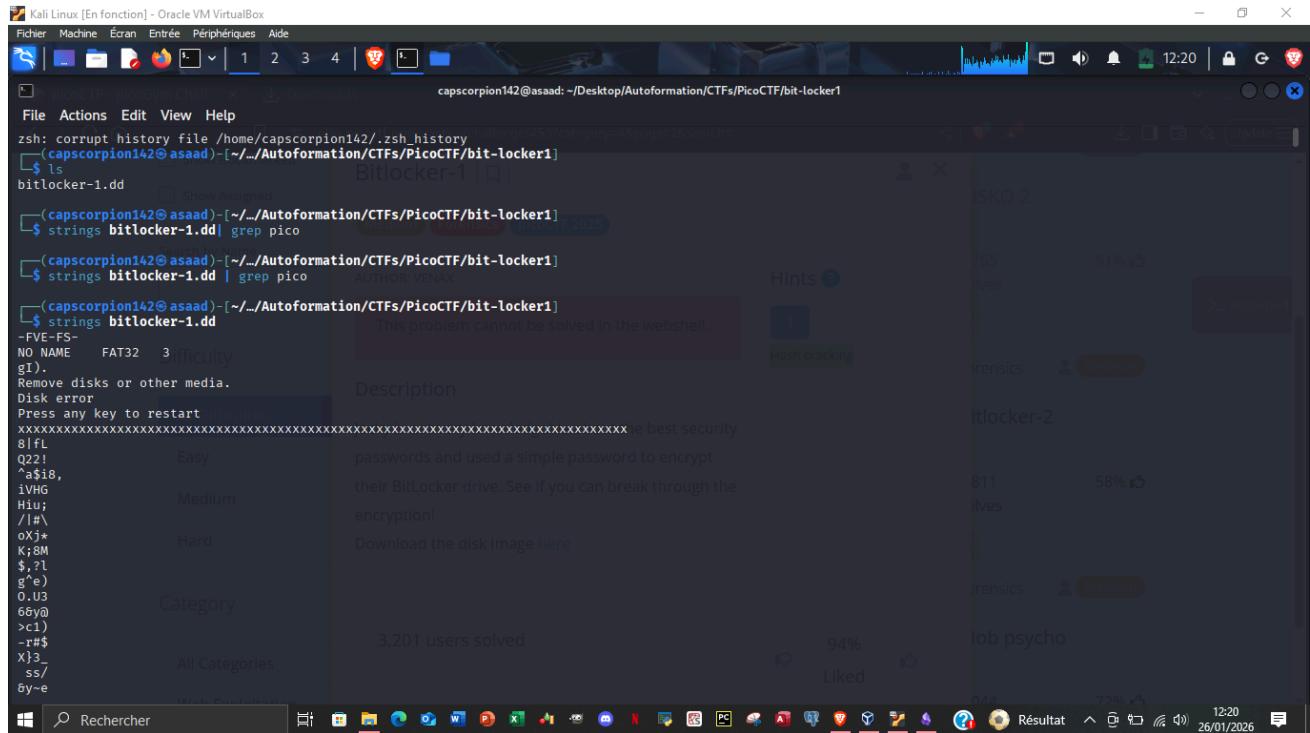


bit-locker1

- We download the disk image
- We try the strings command and this is what we get:



Kali Linux [En fonction] - Oracle VM VirtualBox

```
File Actions Edit View Help
zsh: corrupt history file /home/capscorpion142/.zsh_history
(capscorpion142@asaad:[~/Autoformation/CTFs/PicoCTF/bit-locker1]
$ ls
bitlocker-1.dd
(capscorpion142@asaad:[~/Autoformation/CTFs/PicoCTF/bit-locker1]
$ strings bitlocker-1.dd | grep pico
(capscorpion142@asaad:[~/Autoformation/CTFs/PicoCTF/bit-locker1]
$ strings bitlocker-1.dd | grep pico
(capscorpion142@asaad:[~/Autoformation/CTFs/PicoCTF/bit-locker1]
$ strings bitlocker-1.dd
This problem cannot be solved in the webshell.
```

Description

Difficulty: 3

Category: Hash cracking

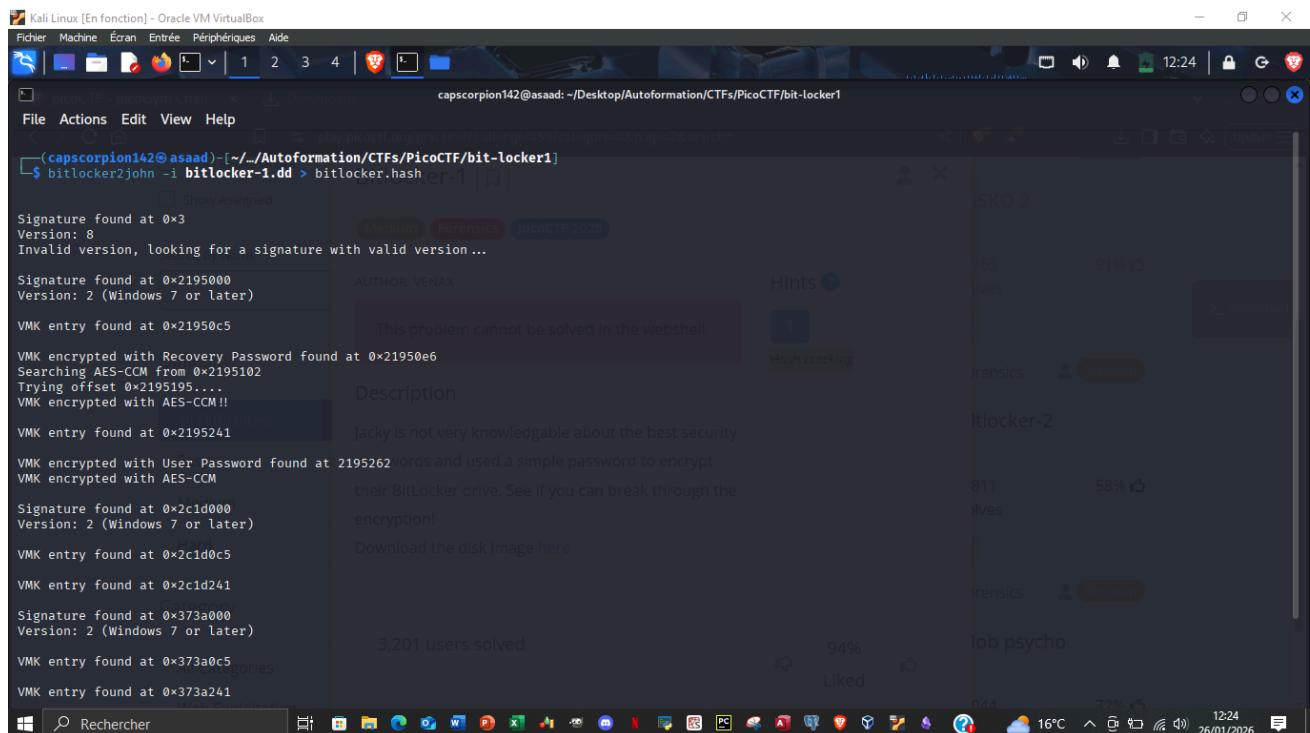
3,201 users solved

94% Liked

724x576 12:20 26/01/2026

The terminal shows the user running the strings command on the file 'bitlocker-1.dd' and filtering for the string 'pico'. The output of the strings command is displayed in the terminal window.

- A long file
- So we use a tool called john for bitlockers (we must hash it)
- And we do this command : "bitlocker2john -i bitlocker-1.dd > bitlocker.hash"



Kali Linux [En fonction] - Oracle VM VirtualBox

```
File Actions Edit View Help
(capscorpion142@asaad:[~/Autoformation/CTFs/PicoCTF/bit-locker1]
$ bitlocker2john -i bitlocker-1.dd > bitlocker.hash
Signature found at 0x3
Version: 8
Invalid version, looking for a signature with valid version ...
Signature found at 0x2195000
Version: 2 (Windows 7 or later)
VMK entry found at 0x21950c5
VMK encrypted with Recovery Password found at 0x21950e6
Searching AES-CCM from 0x2195102
Trying offset 0x2195195...
VMK encrypted with AES-CCM!!
VMK entry found at 0x2195241
VMK encrypted with User Password found at 2195262
VMK encrypted with AES-CCM
Signature found at 0x2c1d000
Version: 2 (Windows 7 or later)
VMK entry found at 0x2c1d0c5
VMK entry found at 0x2c1d241
Signature found at 0x373a000
Version: 2 (Windows 7 or later)
VMK entry found at 0x373a0c5
VMK entry found at 0x373a241
```

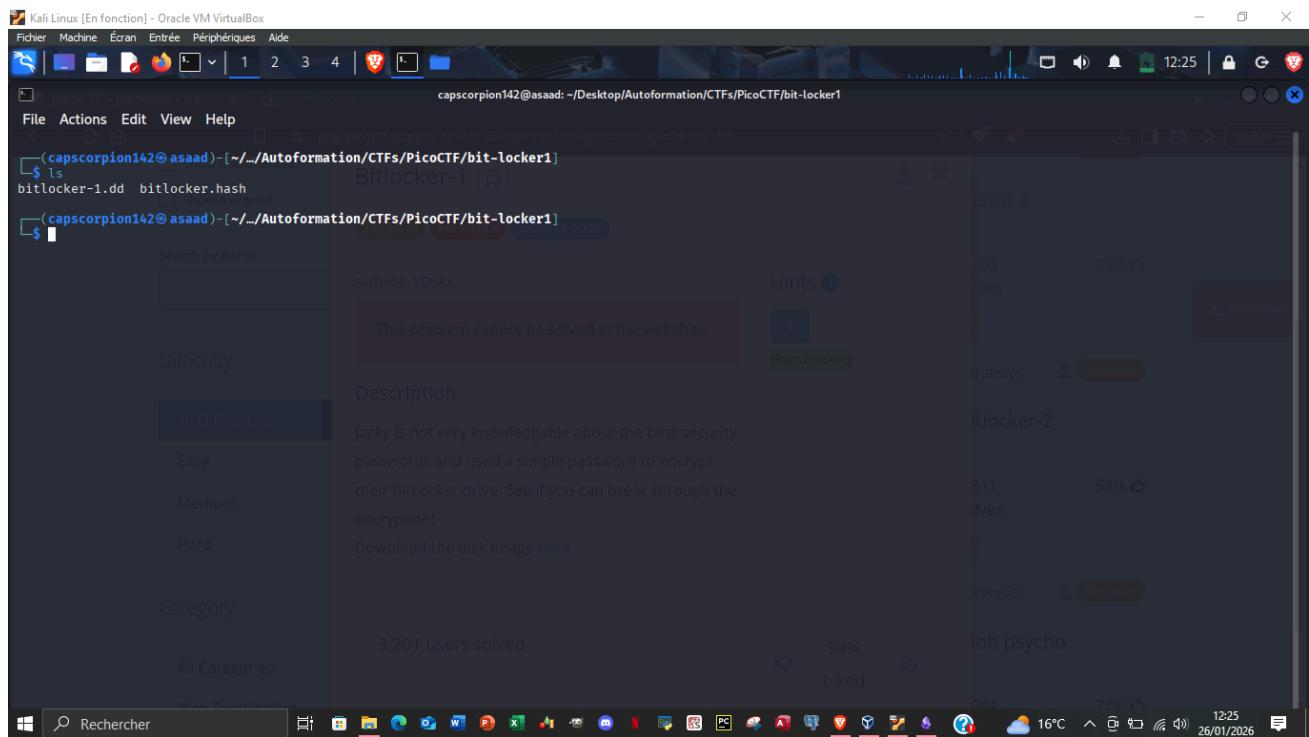
Description

3,201 users solved

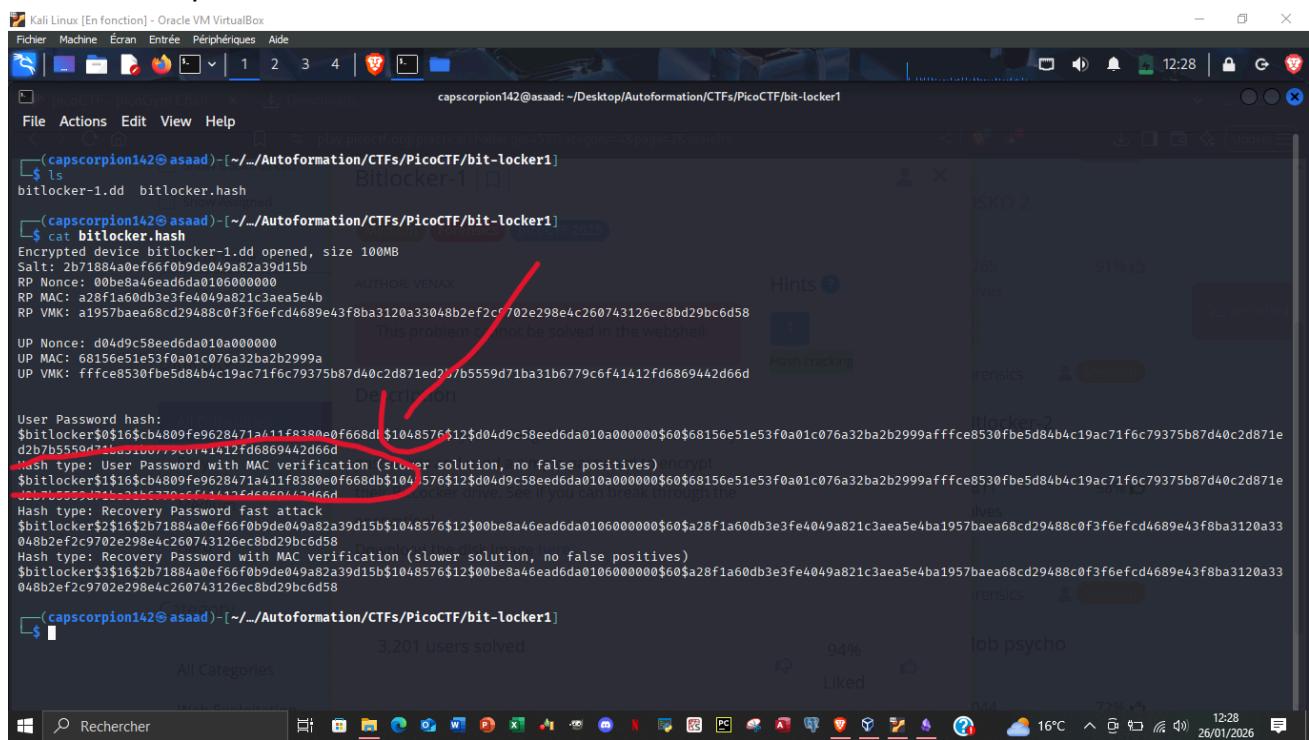
94% Liked

724x576 12:24 26/01/2026

The terminal shows the user running the 'bitlocker2john -i bitlocker-1.dd > bitlocker.hash' command. The output of the command is displayed in the terminal window, showing various encryption signatures and versions found in the file.



- We take this password with \$1:



- We put that only line in .hash file to use later:

A screenshot of a Kali Linux desktop environment. The terminal window shows a challenge from a CTF competition. The command run is `nano 8.4 user.hash *` and the output is a long string of hex bytes representing a hash. The terminal title is "BitLocker-1". The desktop background features a dark theme with various icons and windows visible, including another terminal window titled "BitLocker-2". A sidebar on the left lists challenges by category: All Challenges, Easy, Medium, Hard, and Forensics. The challenge details for "BitLocker-1" show it's a medium difficulty challenge authored by VENAX. The description states: "Jacky is not very knowledgeable about the best security passwords and used a simple password to encrypt their BitLocker drive. See if you can break through the encryption!" It also provides a link to download the disk image.

The screenshot shows a Kali Linux desktop environment running in Oracle VM VirtualBox. The terminal window displays a user's session on a CTF challenge:

```
(capscorpion142㉿asaad) [~/..../Autoformation/CTFs/PicoCTF/bit-locker1]
$ nano user.hash
(capscorpion142㉿asaad) [~/..../Autoformation/CTFs/PicoCTF/bit-locker1]
$ cat user.hash
$bitlocker$1$16$cb4809fe9628471a411f8380e$0f668db$1048576$12$d04d9c58eed6da010a000000$60$68156e51e53f0a01c076a32ba2b2999affce8530fbe5d84b4c19ac71f6c79375b87d40c2d871e
d2b7b5559d71ba31b6779c6f41412fd6869442d66d
```

The challenge details are visible on the right side of the screen:

- Difficulty:** All difficulties
- Description:** Jacky is not very knowledgeable about the best security passwords and used a simple password to encrypt their BitLocker drive. See if you can break through the encryption!
- Category:** Hash cracking
- Solved:** 3,201 users solved
- Completion:** 94% Liked

- So now, we'll use our file user.hash with a wordlist with this command "hashcat -m 22100 user.hash /usr/share/wordlists/rockyou.txt --force

- It is processing:

- We found the password:

Kali Linux [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

File Actions Edit View Help

Speed.#1.....: 4 H/s (6.29ms) @ Accel:8 Loops:4096 Thr:1 Vec:4
Recovered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.....: 1816/14344385 (0.01%)
Rejected.....: 0/1816 (0.00%)
Restore.Point.: 1816/14344385 (0.01%)
Restore.Sub.#1.: Salt:0 Amplifier:0-1 Iteration:1044480-1048576
Candidate.Engine.: Device Generator
Candidates.#1...: \$HEX[729636861726431] → \$HEX[696d65007265646e]
Hardware.Mon.#1.: Util:100%

Description: bitlocker\$#1\$16\$cba4809fe9628471a41f8380e0f668db\$1048576\$12\$d04d9c58eed6da010a000000\$60\$68156e51e53f0a01c076a32ba2b2999afffce8530fbe5d84b4c19ac71f6c79375b87d40c2d871e d2b7b5559d71ba31b6779c6f1412fd6869442d66d:jacqueline very knowledgeable about the best security

Session.....: hashcat passwords and used a simple password to encrypt
Status.....: Cracked
Hash.Mode....: 22900 (BitLocker) their BitLocker drive. See if you can break through the
Hash.Target....: \$bitlocker\$#1\$16\$cba4809fe9628471a41f8380e0f668db\$10 ... 42d66d
Time.Started...: Mon Jan 26 12:40:18 2026, (7 mins, 7 secs)
Time.Estimated.: Mon Jan 26 12:47:25 2026, (0 secs)
Kernel.Feature.: Pure Kernel
Guess.Base....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 4 H/s (6.09ms) @ Accel:8 Loops:4096 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 1920/14344385 (0.01%)
Rejected.....: 0/1920 (0.00%)
Restore.Point.: 1920/14344385 (0.01%)
Restore.Sub.#1.: Salt:0 Amplifier:0-1 Iteration:1044480-1048576
Candidate.Engine.: Device Generator
Candidates.#1...: howard → hercules
Hardware.Mon.#1.: Util: 94% Liked
Started: Mon Jan 26 12:39:10 2026
Stopped: Mon Jan 26 12:47:28 2026

(capscorpion142@asaad)-[~/Autoformation/CTFs/PicoCTF/bit-locker1]

```
sudo apt install dislocker  
mkdir bitlocker decrypted  
sudo dislocker -V bitlocker-1.dd -uPASSWORD_FOUND -- bitlocker  
sudo mount -o loop bitlocker/dislocker-file decrypted  
ls decrypted
```

- Use this command for the before last one : "sudo mount -o ro,loop bitlocker/dislocker-file decrypted"

```
(capscorpion142㉿asaad) [~/../Autoformation/CTFs/PicoCTF/bit-locker1]
$ ls decrypted
'$RECYCLE.BIN'  flag.txt 'System Volume Information'

(capscorpion142㉿asaad) [~/../Autoformation/CTFs/PicoCTF/bit-locker1]olved in the webshell.
```

Difficulty: All difficulties

Description: Jacky is not very knowledgeable about the best security passwords and used a simple password to encrypt their BitLocker drive. See if you can break through the encryption!

Download the disk image [here](#)

3,201 users solved

94% Liked

Submit Flag

Category: All Categories

Power Manager: Your Battery is charging

```
(capscorpion142㉿asaad) [~/../Autoformation/CTFs/PicoCTF/bit-locker1]
$ ls decrypted
'$RECYCLE.BIN'  flag.txt 'System Volume Information'

(capscorpion142㉿asaad) [~/../Autoformation/CTFs/PicoCTF/bit-locker1]olved in the webshell.

(capscorpion142㉿asaad) [~/../Autoformation/CTFs/PicoCTF/bit-locker1]
$ cat decrypted/flag.txt
picoCTF{us3_b3tt3r_p4ssw0rd5_pl5!_3242adb1}

(capscorpion142㉿asaad) [~/../Autoformation/CTFs/PicoCTF/bit-locker1]
```

Difficulty: All difficulties

Description: Jacky is not very knowledgeable about the best security passwords and used a simple password to encrypt their BitLocker drive. See if you can break through the encryption!

Download the disk image [here](#)

3,201 users solved

94% Liked

Submit Flag

Category: All Categories