BitLocker 1

GOALS : *Crack the dd file password for get access to disk storaged in file bitlocker-1.dd*

1. found 1 file thats it `exiftool bitlocker-1.dd`

```
bitlocker-1.dd
ExifTool Version Number : 12.76
File Name : bitlocker-1.dd
Directory : .
File Size : 105 MB
File Modification Date/Time : 2026:01:18 11:31:27+07:00
File Access Date/Time : 2026:01:27 10:43:13+07:00
File Inode Change Date/Time : 2026:01:18 11:31:29+07:00
File Permissions : -rw-rw-r--
Error : Unknown file type
```

//ekstras hashes password to txt file !

2. Untuk melakukan identifikasi pasword pengguna yang terdapat pada file dd kita bisa menggunaka tools yang namanya adalah *bitlocker2john*

penggunaan bitlocker2john untuk mengekstrak hash yang ada pada dd file
`bitlocker2john -i bitlocker-1.dd > bitlocker.txt`

```
cat bitlocker.txt
Encrypted device bitlocker-1.dd opened, size 100MB
Salt: 2b71884a0ef66f0b9de049a82a39d15b
RP Nonce: 00be8a46ead6da0106000000
RP MAC: a28f1a60db3e3fe4049a821c3aea5e4b
RP VMK:
a1957baea68cd29488c0f3f6efcd4689e43f8ba3120a33048b2ef2c9702e298e4c260743126ec8b
d29bc6d58

UP Nonce: d04d9c58eed6da010a000000
UP MAC: 68156e51e53f0a01c076a32ba2b2999a
UP VMK:
fffce8530fbe5d84b4c19ac71f6c79375b87d40c2d871ed2b7b5559d71ba31b6779c6f41412fd68
69442d66d

User Password hash:
$bitlocker$0$16$cb4809fe9628471a411f8380e0f668db$1048576$12$d04d9c58eed6da010a0
00000$60$68156e51e53f0a01c076a32ba2b2999afffce8530fbe5d84b4c19ac71f6c79375b87d4
0c2d871ed2b7b5559d71ba31b6779c6f41412fd6869442d66d
Hash type: User Password with MAC verification (slower solution, no false
positives)
```

`$bitlocker$1$16$cb4809fe9628471a411f8380e0f668db$1048576$12$d04d9c58eed6da010a000000$60$68156e51e53f0a01c076a32ba2b2999afffce8530fbe5d84b4c19ac71f6c79375b87d40c2d871ed2b7b5559d71ba31b6779c6f41412fd6869442d66d`
`Hash type: Recovery Password fast attack`
`$bitlocker$2$16$2b71884a0ef66f0b9de049a82a39d15b$1048576$12$00be8a46ead6da0106000000$60$a28f1a60db3e3fe4049a821c3aea5e4ba1957baea68cd29488c0f3f6efcd4689e43f8ba3120a33048b2ef2c9702e298e4c260743126ec8bd29bc6d58`
`Hash type: Recovery Password with MAC verification (slower solution, no false positives)`
`$bitlocker$3$16$2b71884a0ef66f0b9de049a82a39d15b$1048576$12$00be8a46ead6da0106000000$60$a28f1a60db3e3fe4049a821c3aea5e4ba1957baea68cd29488c0f3f6efcd4689e43f8ba3120a33048b2ef2c9702e298e4c260743126ec8bd29bc6d58`

//creating dictionary !

3. kita akan coba menggunakan hashcat untuk melakukan craking pada hash tersebut, namun sebelum itu kita wajib untuk menyusun dictionary terlebuh dahulu, kami menggunakan rockyou untuk menyusun diksi yang kami butuhkan.

```
head -n 10000 /usr/share/wordlists/rockyou.txt > dictionary.txt
```

(digunakan untuk memilih diksi dari 0 hingga 1000 yang ada pada rockyou)
diksi itu kayak:
mis: akmal
akmal
akmal1
akmal2
akmal3
nah ini diksi nya (4)

Diction > Dictionary
kata > Kamus

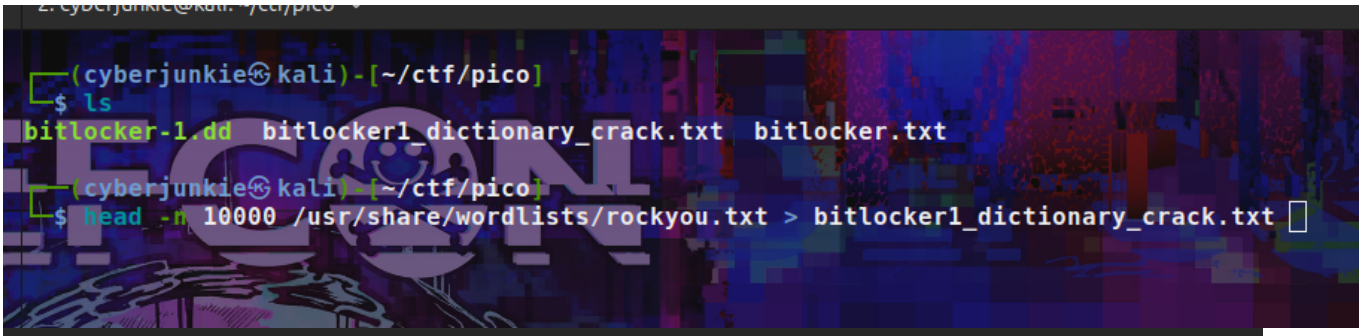
nah ini yang bakal kita gunain untuk melakukan penebakan pada sandi, jadi kita akan memulaii melakukan penyusunan pada wordlist yang akan kita gunakan menggunakan head -n 10000, maka yang akan diambil adalah kata dari 0 - 10000, pada susunan kata rockyou.

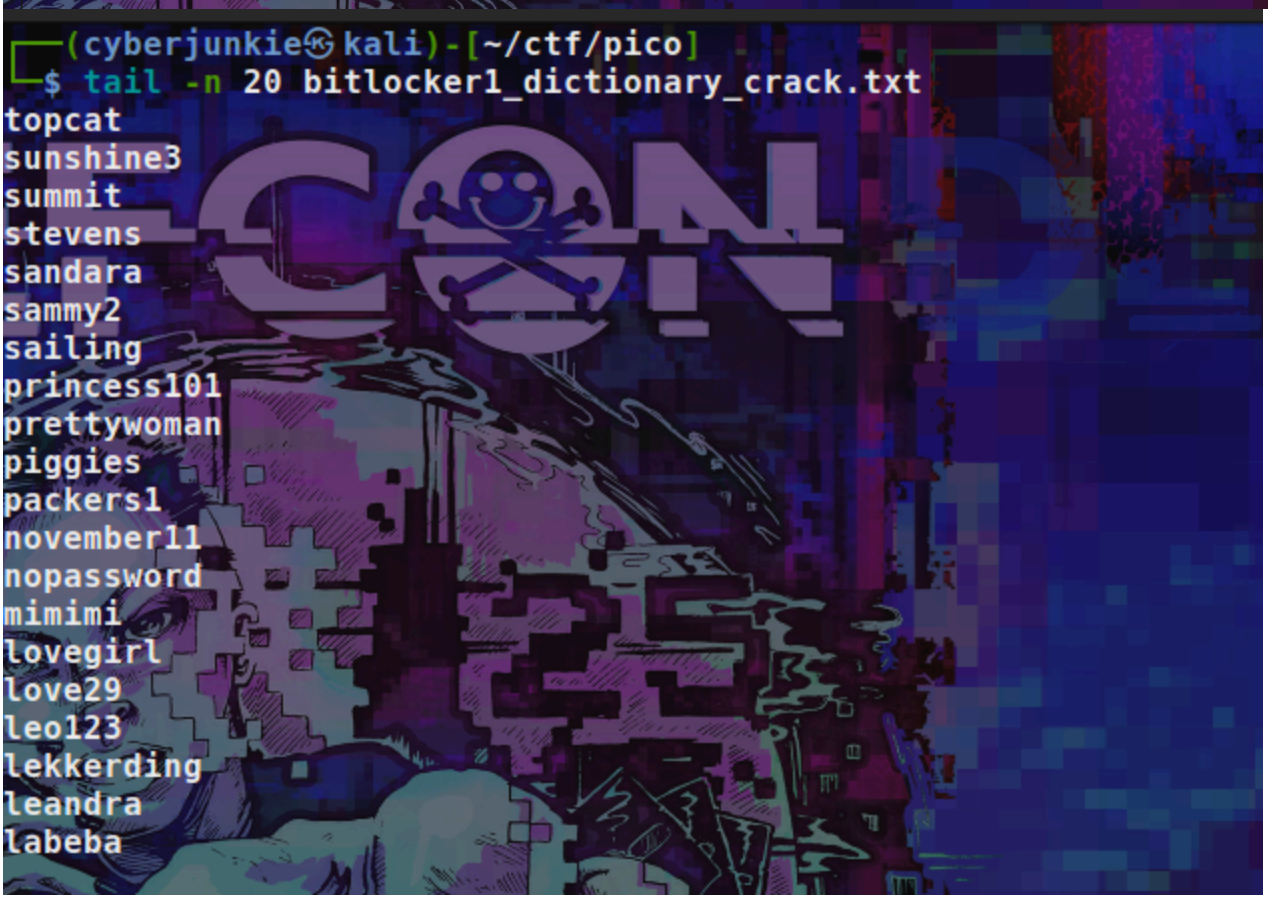
setelah dictionary atau kamus sudah tersusun, kita bisa *Send hashed passwords* kedalam hash file yang sudah berhasil di ekstrak via bitlocker2john, menggunakan tools yang bernama hashcat.

kegunaan hashcat:

| + | Features

```
  1 | Send hashed passwords
  2 | Send attack positions
  3 | Send hashed passwords and attack positions
```





4. Kami sudah memiliki kamus dan banyak kata untuk kami kirimkan ke hash file yang masih berbentuk hash tersebut, yang kami perlu lakukan selanjutnya hanyalah menggunakan hashcat untuk menebak password yang digunakan untuk mengamankan file *bitlocker-1.dd*

Akhirnya kami menumukan pasword yang berhasil di tebak dan di pecahkan yaitu

```
Hashes: 2 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
```

- `Single-Hash`
- `Single-Salt`
- `Slow-Hash-SIMD-LOOP`

`Watchdog: Temperature abort trigger set to 90c`

`Host memory allocated for this attack: 512 MB (8677 MB free)`

`Dictionary cache hit:`

- `Filename..: bitlocker1_dictionary_crack.txt`
- `Passwords.: 10000`
- `Bytes.....: 80577`
- `Keyspace..: 10000`

`$bitlocker$0$16$cb4809fe9628471a411f8380e0f668db$1048576$12$d04d9c58eed6da010a0`
`00000$60$68156e51e53f0a01c076a32ba2b2999afffce8530fbe5d84b4c19ac71f6c79375b87d4`
`0c2d871ed2b7b5559d71ba31b6779c6f41412fd6869442d66d:**jacqueline` **

```
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 22100 (BitLocker)
Hash.Target......: $bitlocker$0$16$cb4809fe9628471a411f8380e0f668db$10...42d66d
Time.Started.....: Tue Jan 27 14:24:59 2026 (7 mins, 41 secs)
Time.Estimated...: Tue Jan 27 14:32:40 2026 (0 secs)
Kernel.Feature...: Pure Kernel (password length 6-256 bytes)
Guess.Base.......: File (bitlocker1_dictionary_crack.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........: 5 H/s (149.03ms) @ Accel:367 Loops:1024 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2419/10000 (24.19%)
Rejected.........: 217/2419 (8.97%)
Restore.Point....: 1606/10000 (16.06%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1 Iteration:1047552-1048576
Candidate.Engine.: Device Generator
Candidates.#01...: poopie -> jimenez
Hardware.Mon.#01.: Util: 95%

Started: Tue Jan 27 14:24:51 2026
Stopped: Tue Jan 27 14:32:42 2026
```

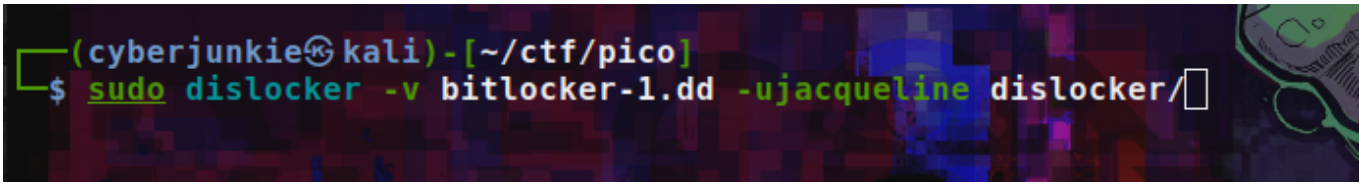
5. setelah itu kami akan menggunakan dislocker untuk memaksa akses ke file dd yang masih di enkrip menggunakan bitlocker.

dengan itu kami bisa menggunakan password yang sudah kami tebak untuk bisa memecahkan keamanan enkripsi bitlocker, namun untuk bisa mengakses dengan leluasa

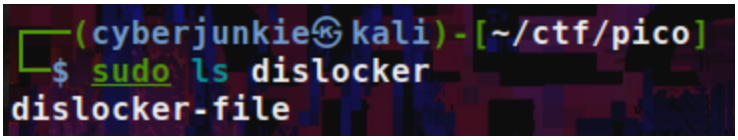
kami butuh folder yang baru untuk bisa menyimpan hasil dari dislocker.

mkdir dislocker
/dislocker

setlah itu kami akan mencoba memecahkan keamanan bitlocker dengan menggunakan command dislocker dan memasukan hasil nya kedalam folder dislocker yang telah kami buat sebelumnya.



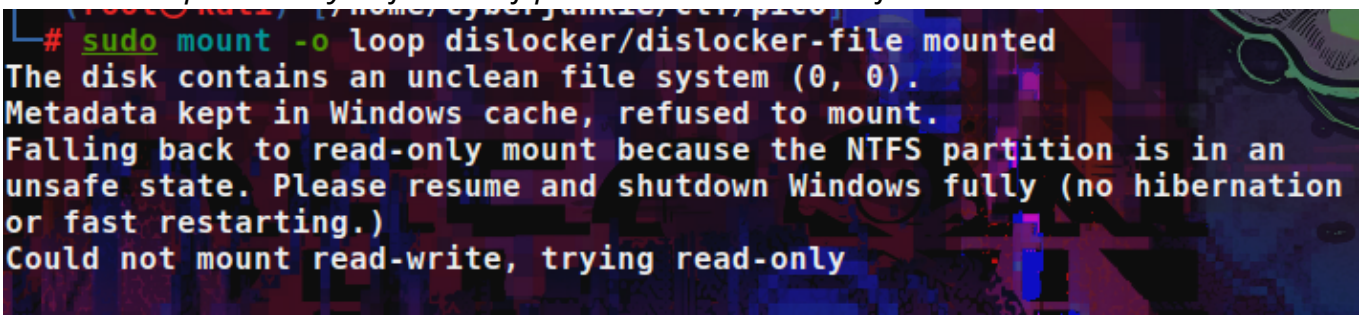
maka nanti akan menghasilkan sebuah file yang bernama



langakah terakhirnya kita hanya perlu melakukan mounting untuk media yang sudah kita hasilkan dari dislocker, langkah selanjutnya buat mount folder untuk mount point yang baru

mkdir mounted
/mounted

mount -o loop /home/cyberjunkie/ctf/pico/dislocker/dislocker-file mounted



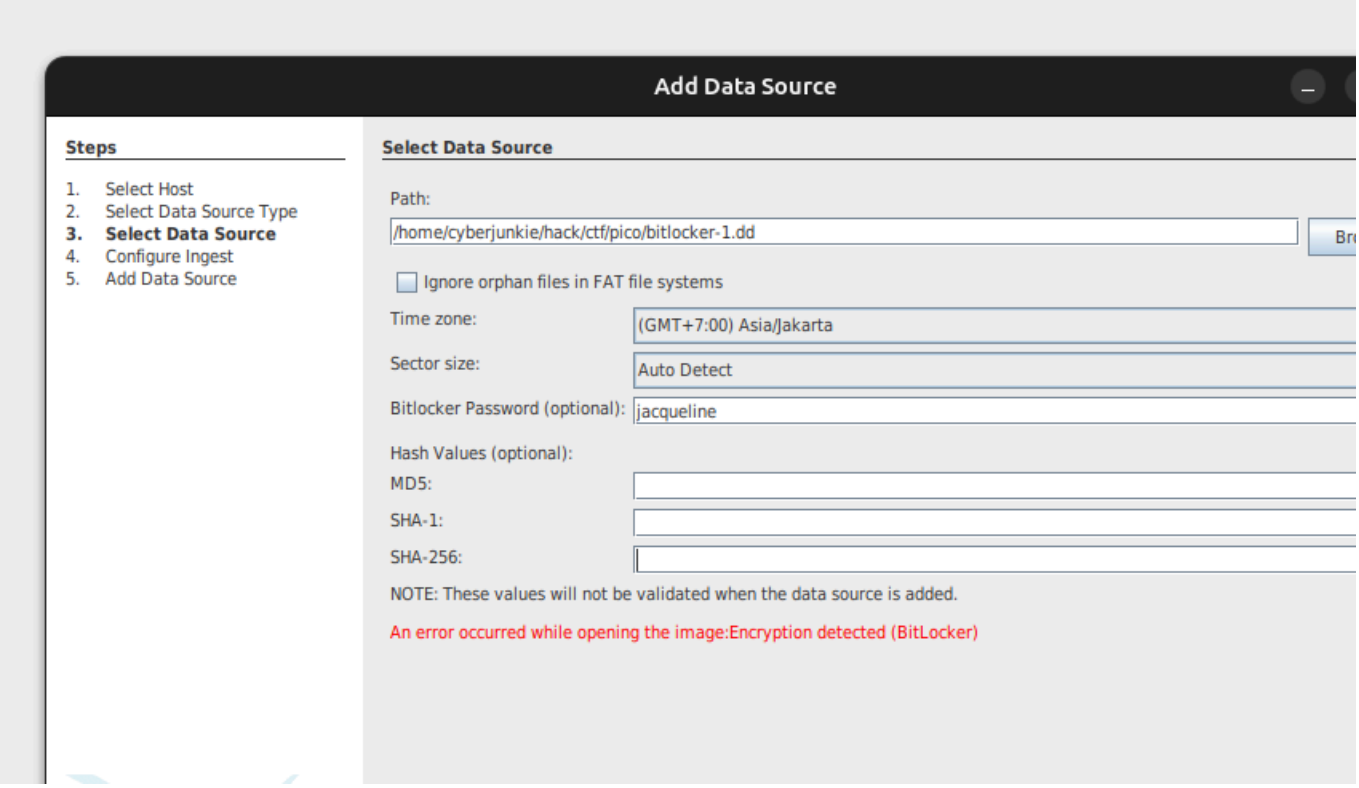
dan kami berhasil menemukan flag.txt yang kami cari pada chall kali ini

RESOURCES :

https://medium.com/@erichdryn/bitlocker-1-picoctf-writeup-c0b5e4e3ec9b (Walkthrough)
https://www.freecodecamp.org/news/hacking-with-hashcat-a-practical-guide/ (Hashcat Methode)

NOTES :

Autopsy memiliki keterbatasan dalam mendekripsi BitLocker - Autopsy tidak selalu bisa mendekripsi BitLocker secara langsung, bahkan dengan password yang benar. Fitur dekripsi BitLocker di Autopsy masih terbatas. (alasan mengapa kita tidak menggunakan autopsy)



oleh sebab itu kita diharuskan untuk menggunakan dislocker untuk bisa mengakses media storaged yang masih diamankan menggunakan btilocker tersebut.