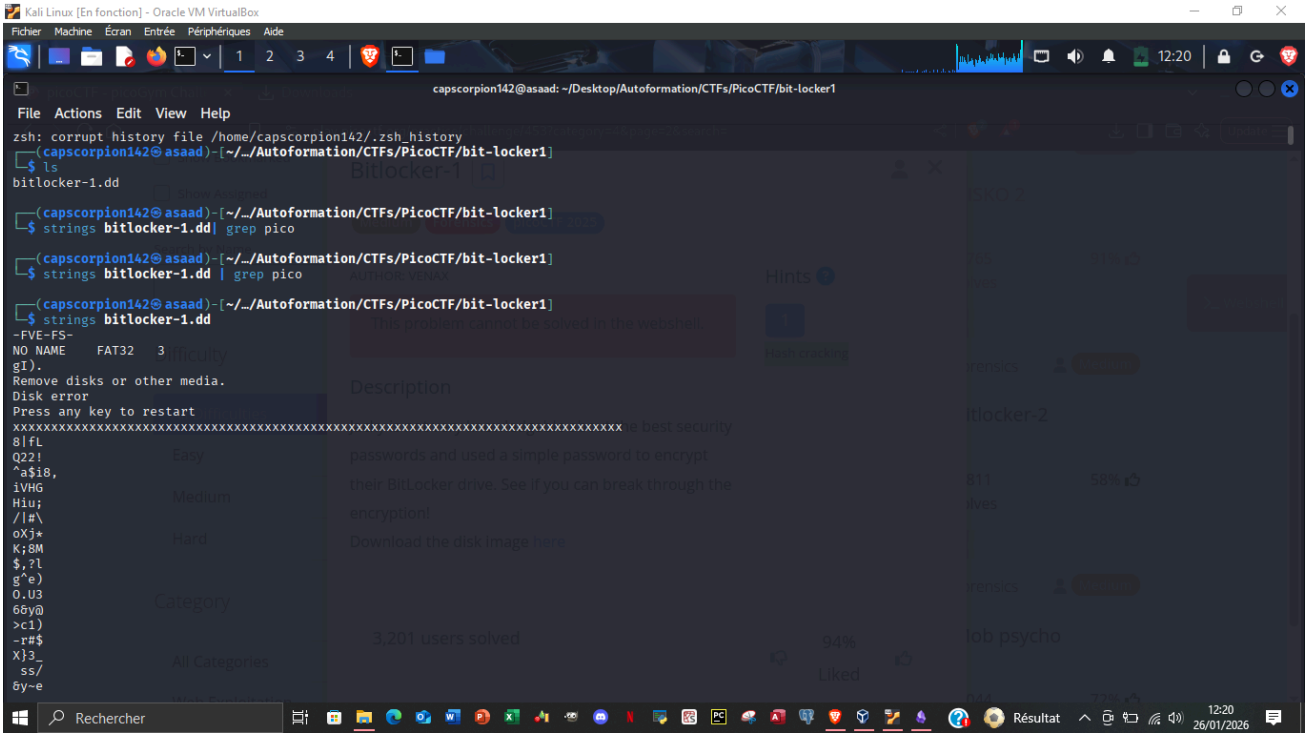
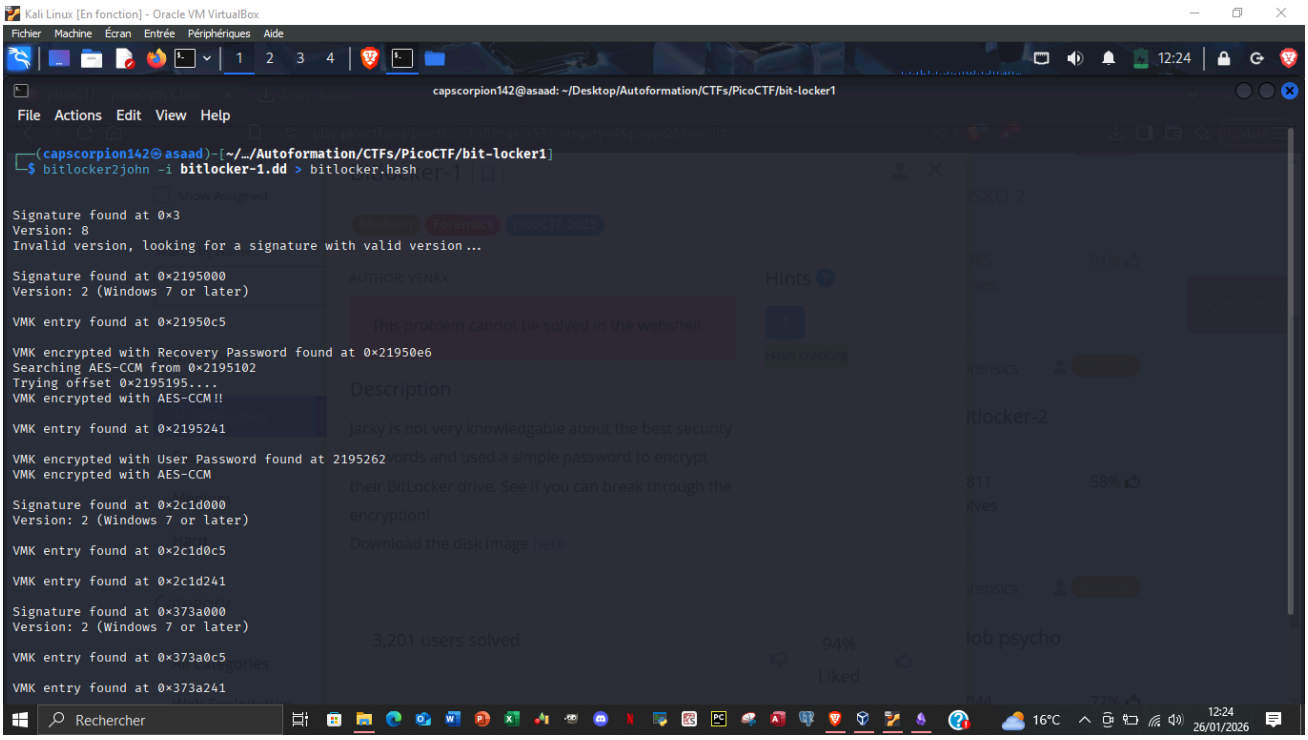
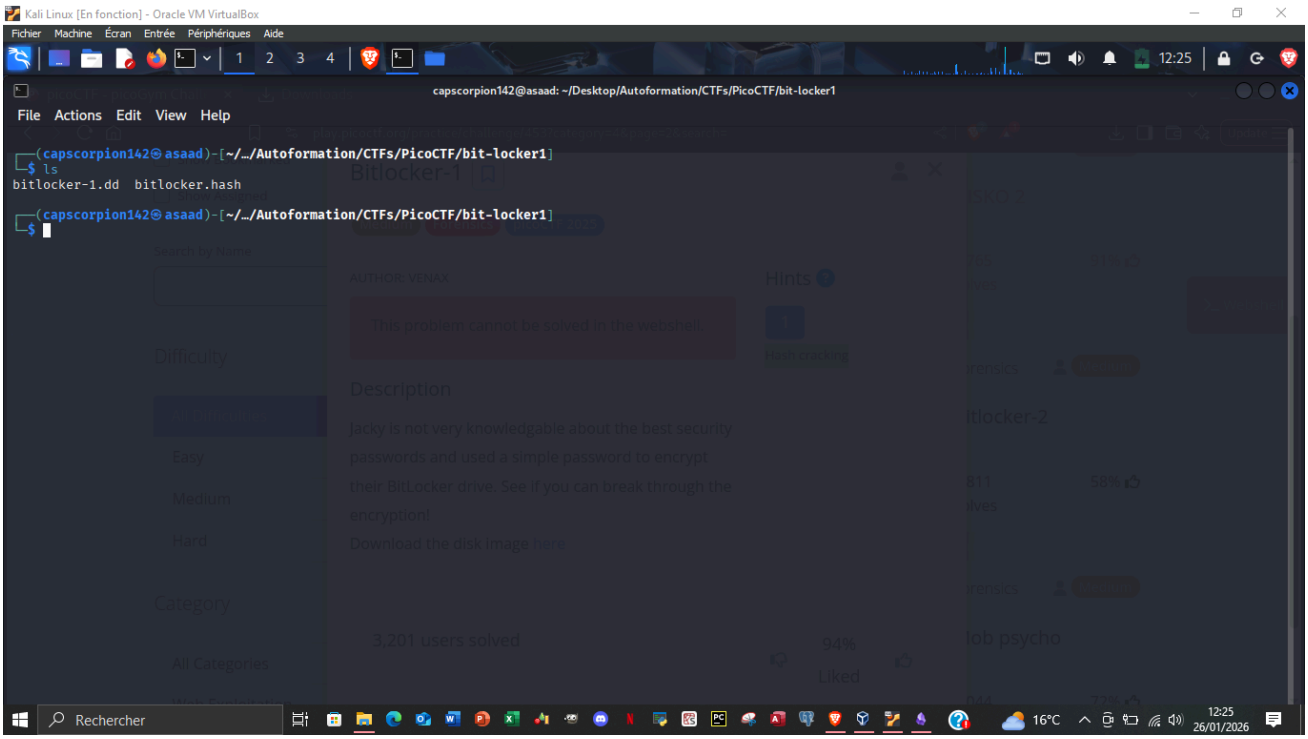
bit-locker1

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

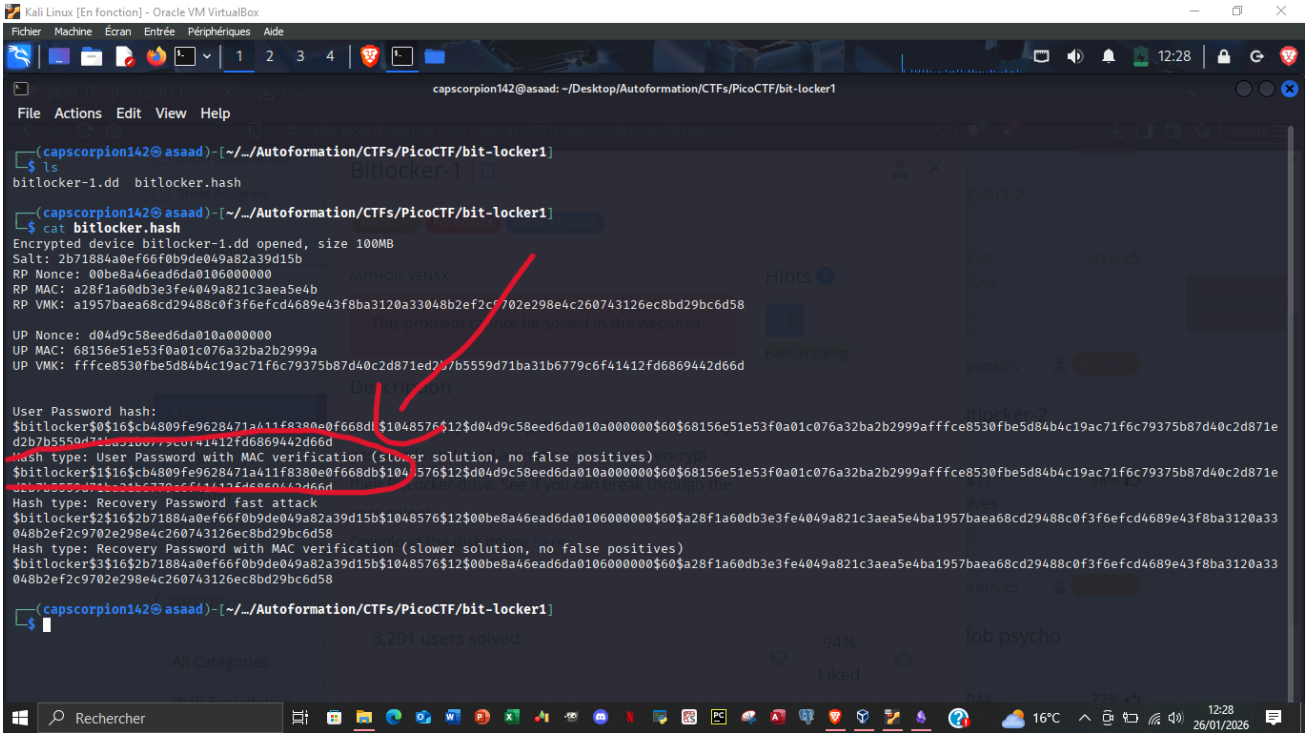


- A long file
- So we use a tool called john for bitlockers (we must hash it)
- And we do this command : "bitlocker2john -i bitlocker-1.dd > bitlocker.hash"

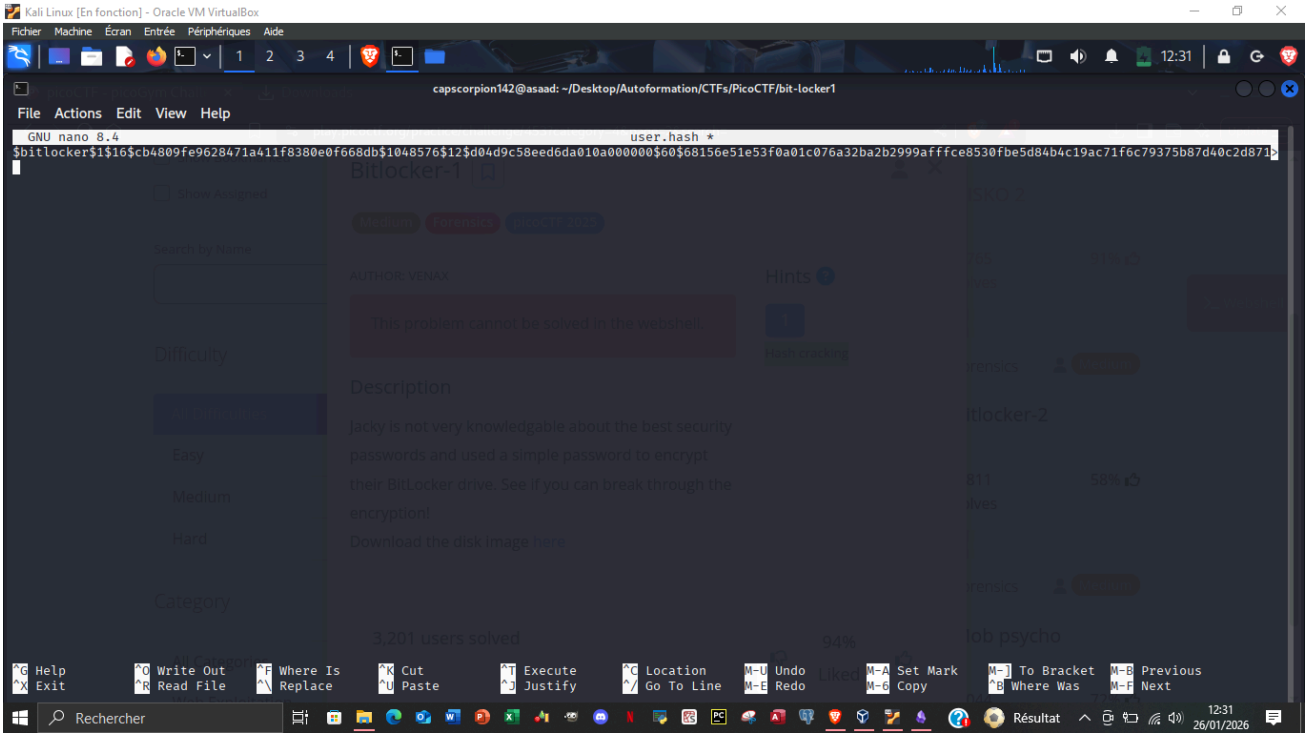


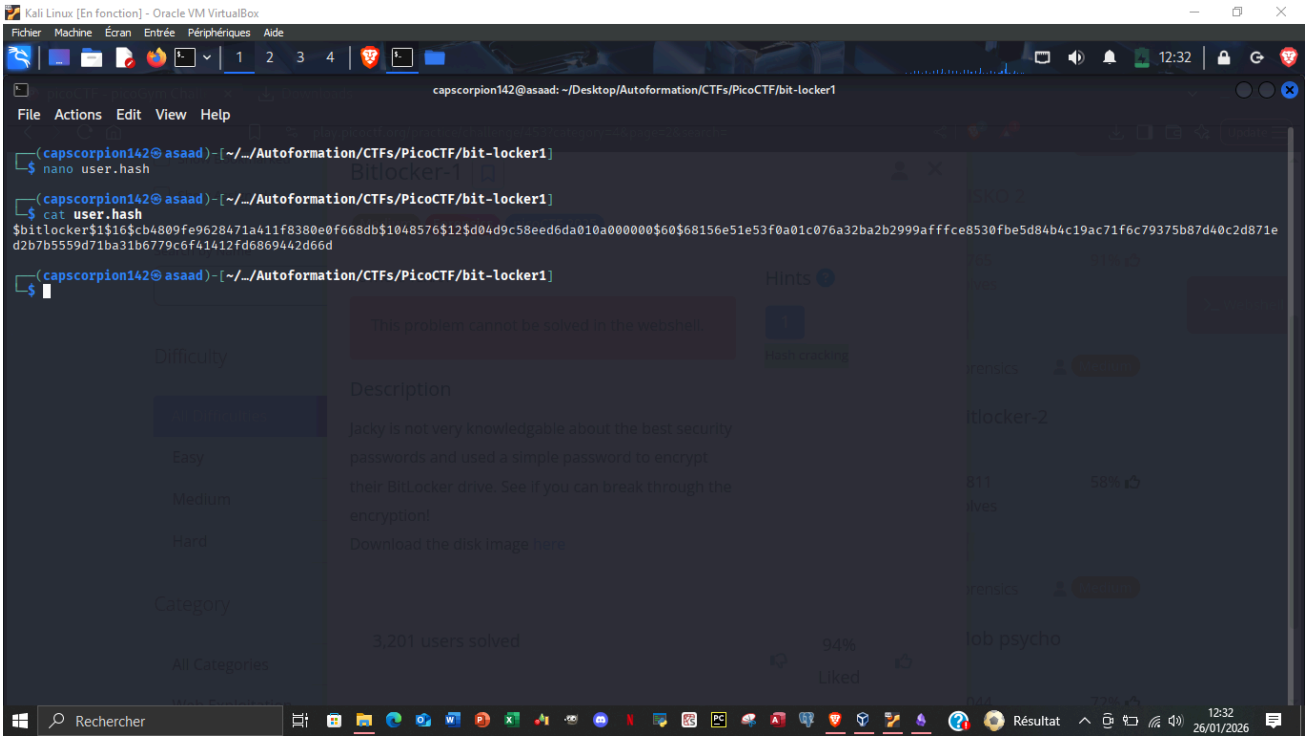


- We take this password with $1:



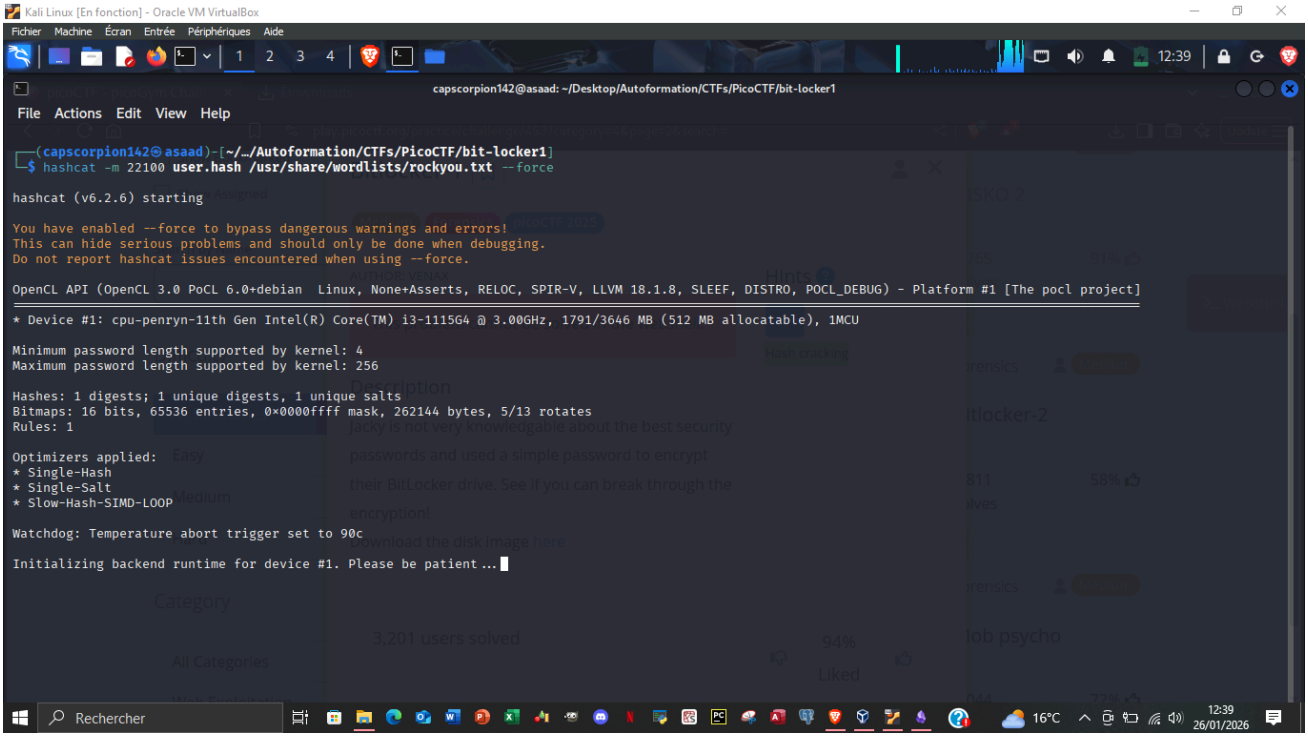
- We put that only line in .hash file to use later:



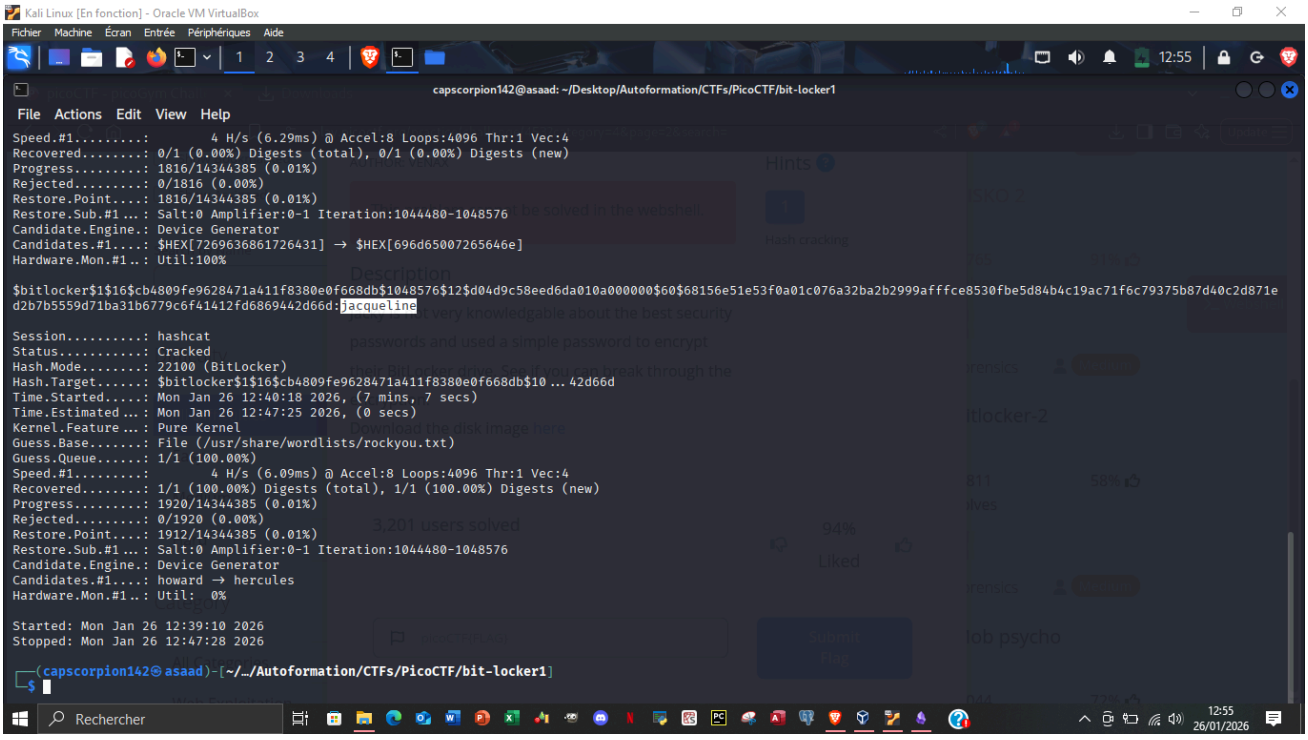


- So now, we'll use our file user.hash with a wordlist with this command "hashcat -m 22100 user.hash /usr/share/wordlists/rockyou.txt --force
"

- It is processing:



- We found the password:




```
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"