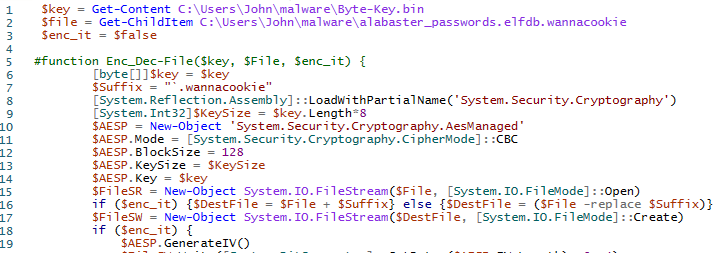
Objective--Recover Alabaster’s Password (Part 6)

# Decrypting Alabaster’s file

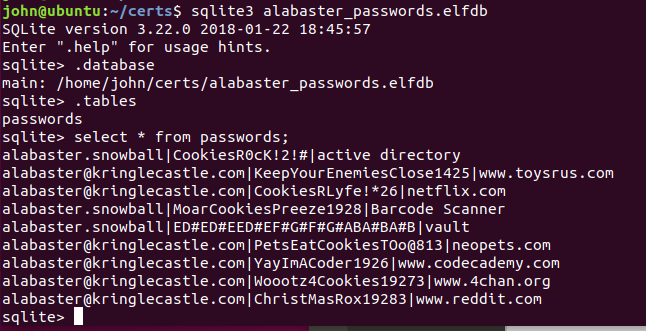
The code to decrypt Alabaster’s file is shown here. The key is the file we saved in the last lesson. Note that $file is the path to the wannacookie file, not the content; that’s why the line uses Get-Childitem (dir or ls) and not Get-Content. The variable $enc\_it is set to False to cause the file to be decrypted.  


The rest of the file is unchanged, except that the final “}” is commented out to match the one in line 5.

When we look in the directory where alabaster\_passwords.elfdb.wannacry used to be, we find it has been replaced by alabaster\_passwords.elfdb. Whew!



# Exploring the Database

It’s less work to paste Alabaster’s database file into a Linux VM that already has sqlite3 than to install sqlite3 on Windows, so that is what we will do. Then we can open the database.  


Alabaster’s vault password is ED#ED#EED#EF#G#F#G#ABA#BA#B.

We could also have used brute force. The string command works, it is just harder to read.  
