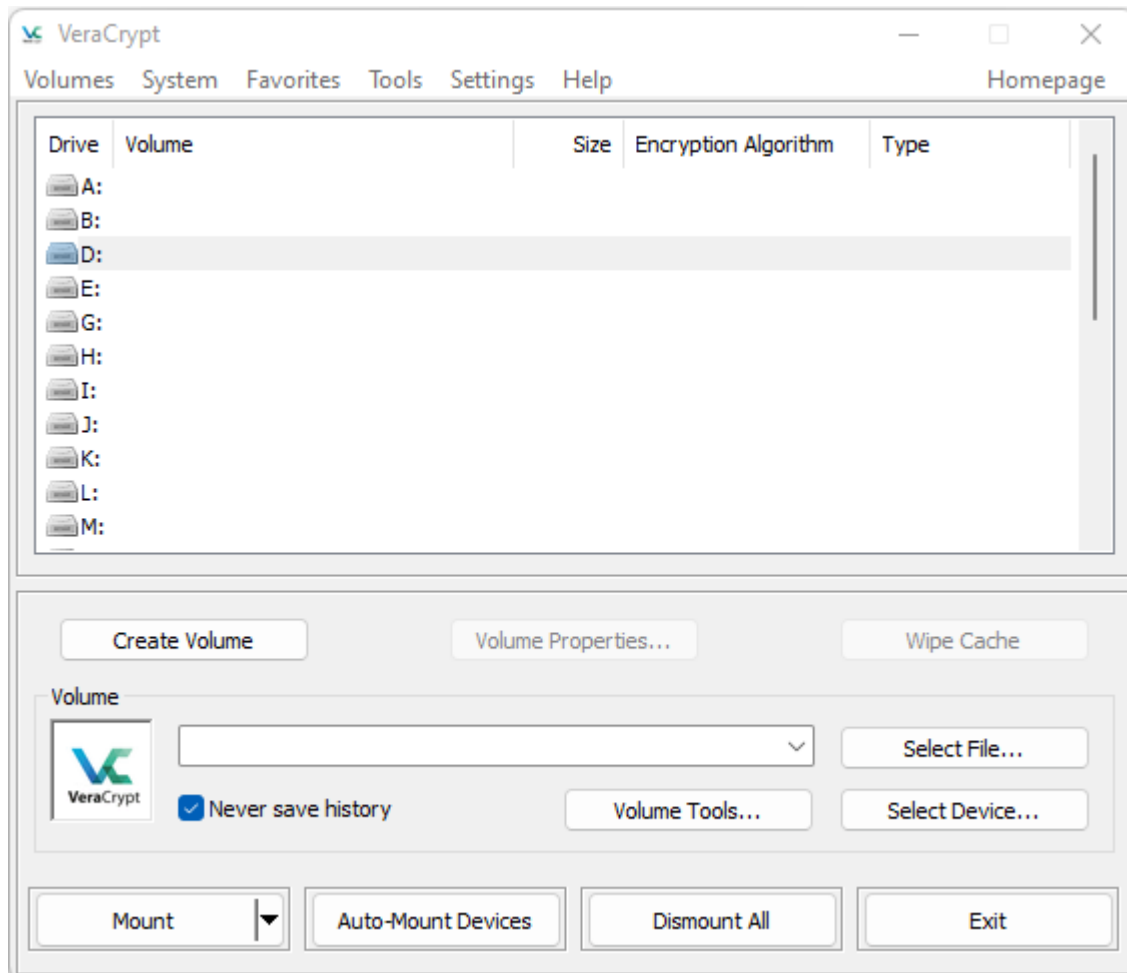


Cyber Security and Digital Forensics

Practical No. 10

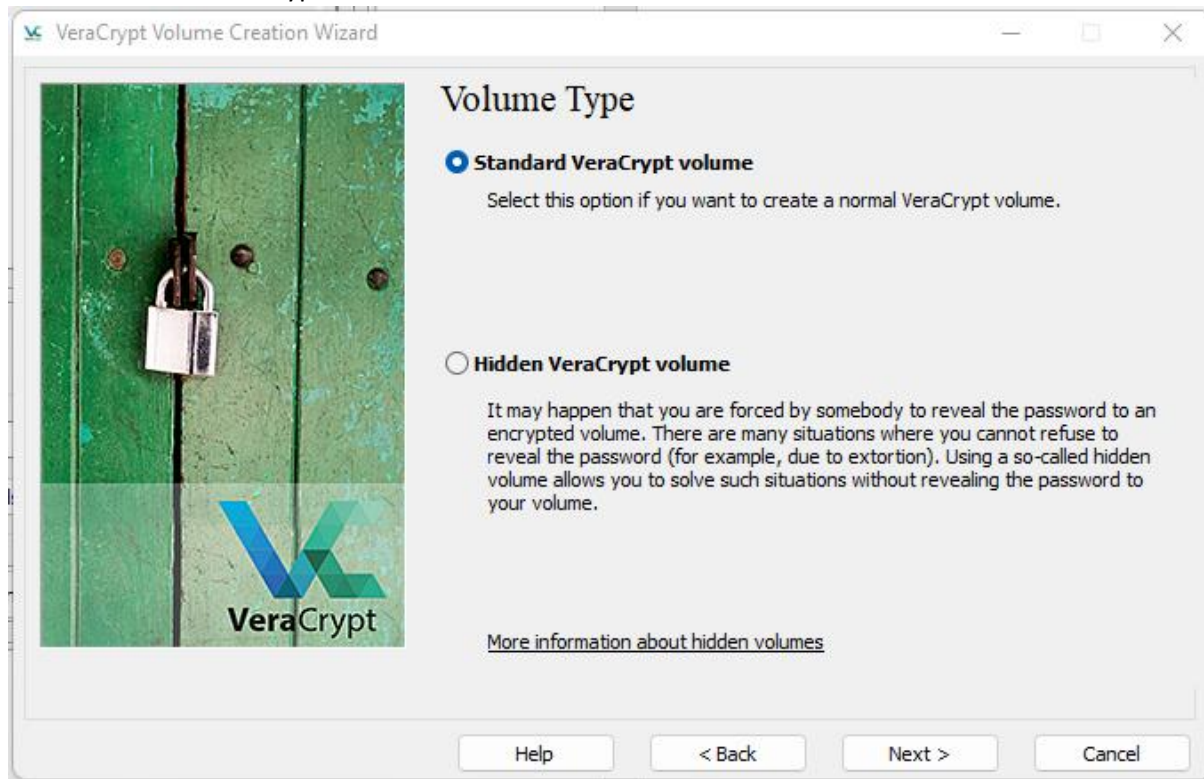
1. Download veraCrypt



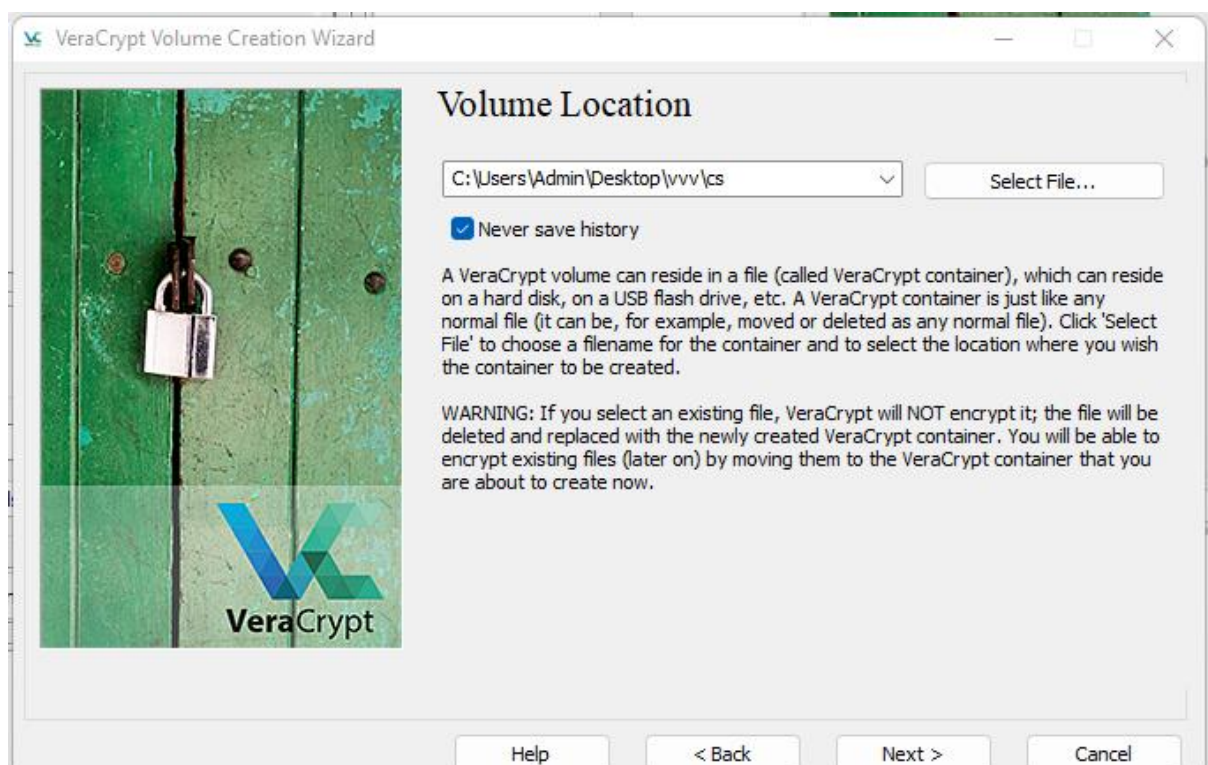
2. create volume



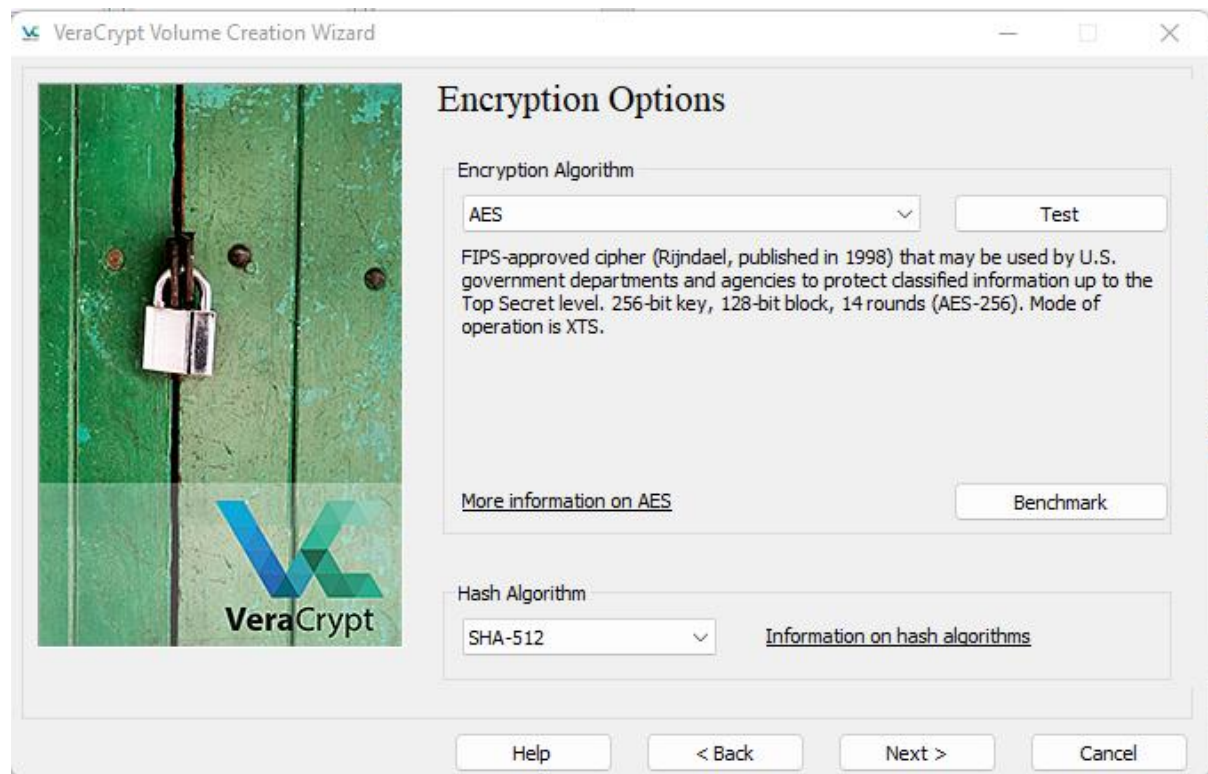
3. select volume type



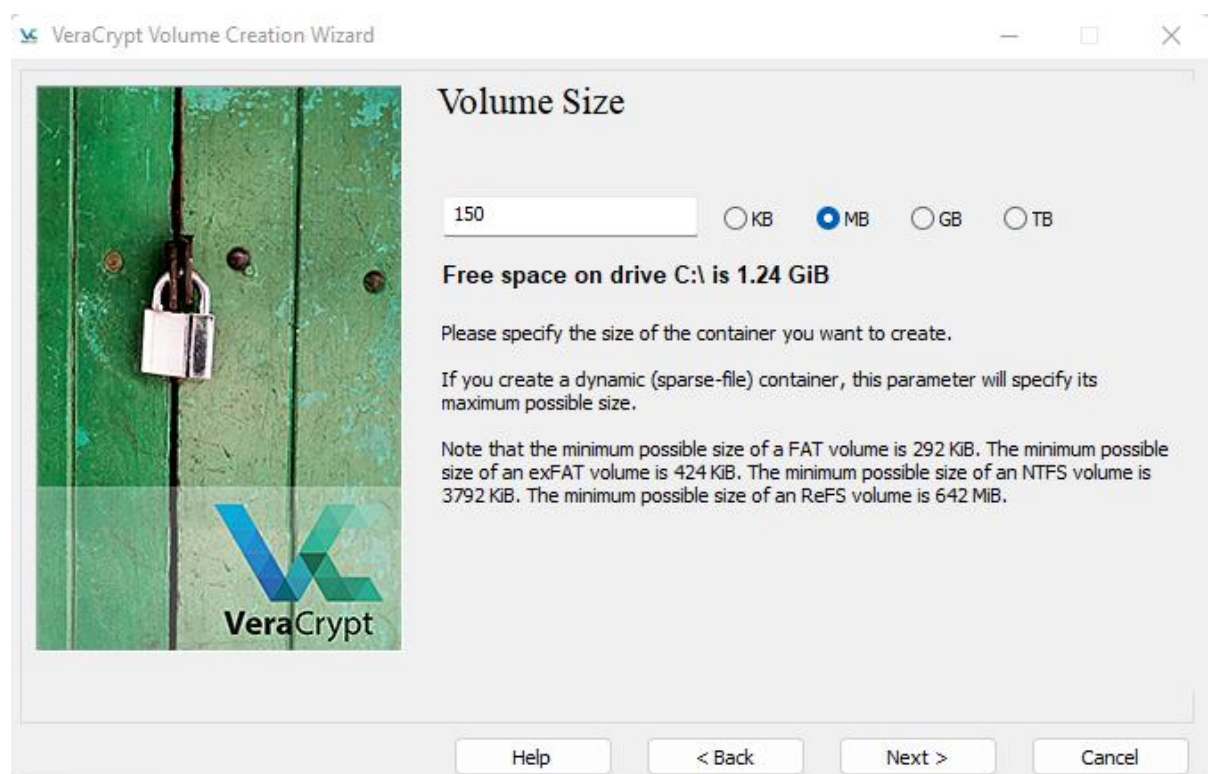
5. select location



6. select encryption option



7. select volume size



8. set password

VeraCrypt Volume Creation Wizard

Volume Password

Password: 1234
Confirm: 1234

☐ Use keyfiles ☒ Display password ☐ Use PIM

Keyfiles...

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = \$ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 128 characters.

Help < Back Next > Cancel

9. format volume key

VeraCrypt Volume Creation Wizard

Volume Format

Options
Filesystem FAT Cluster Default Full Format
☐ Dynamic

Random Pool: *./...+.,,/-,*,,-*+*+.../*,---*-...
Header Key: *****
Master Key: *****

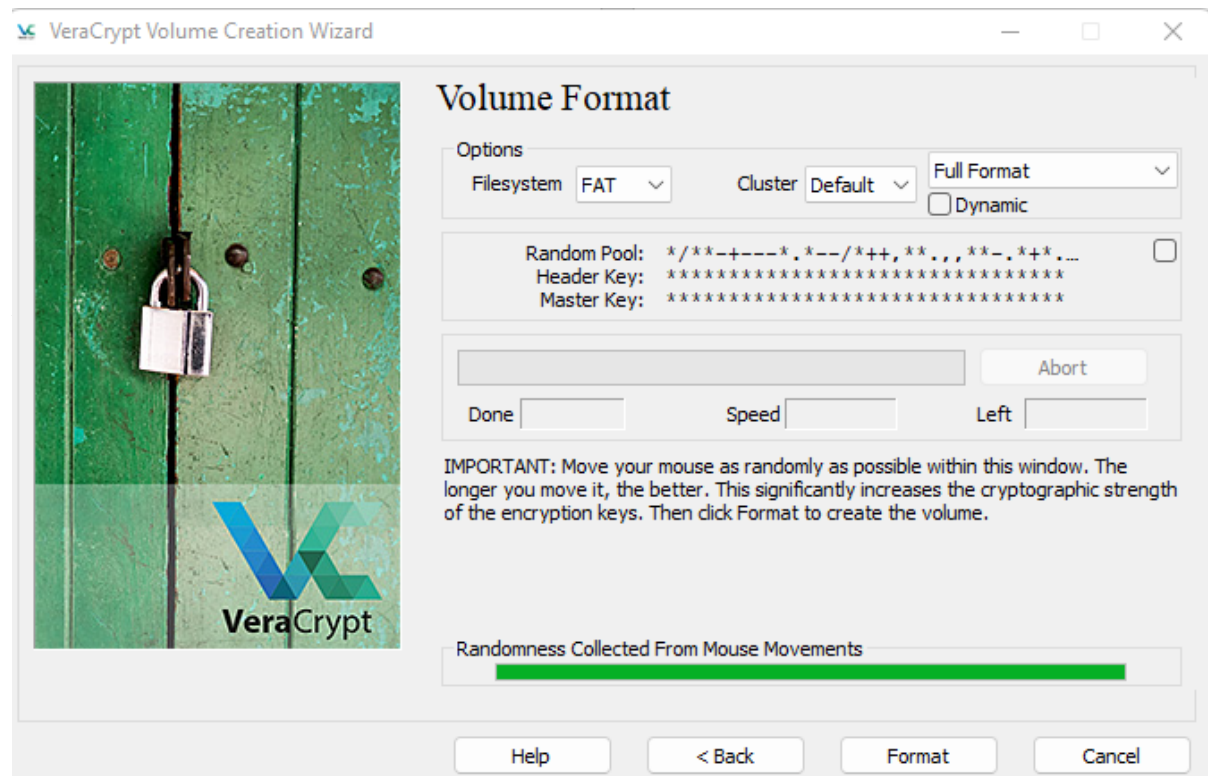
Done Speed Left

Abort

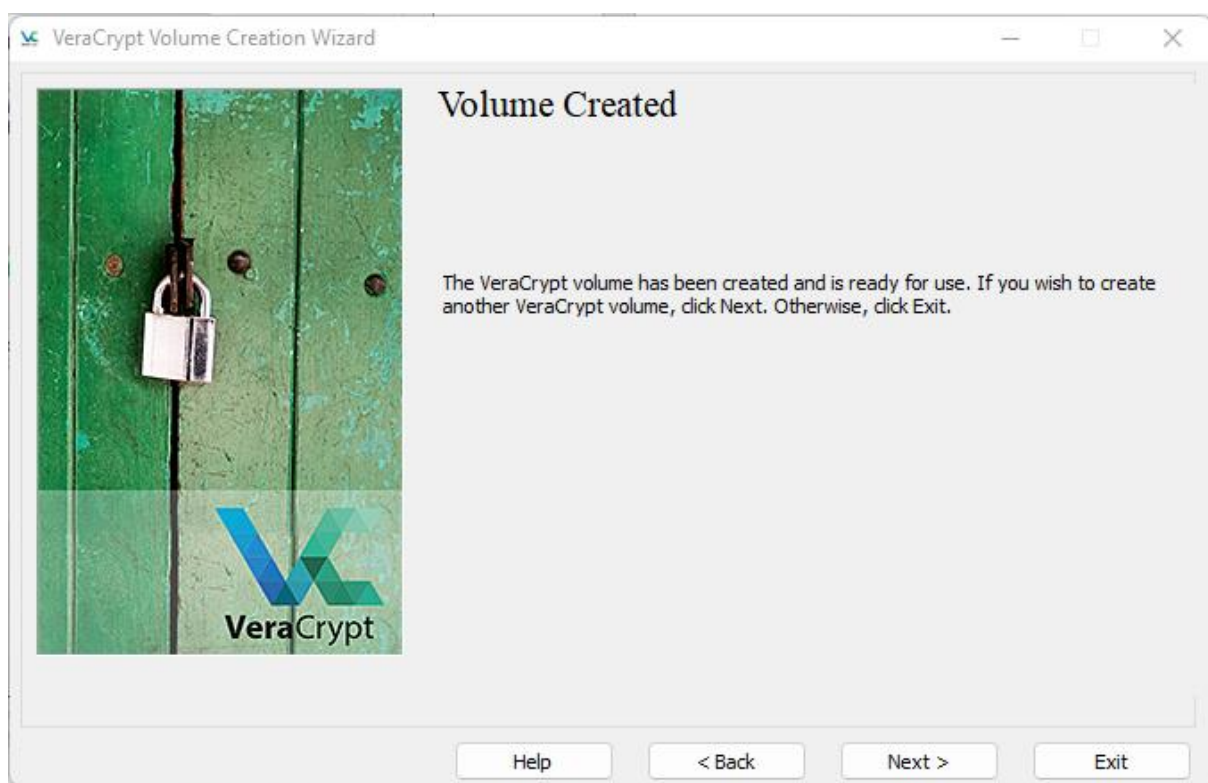
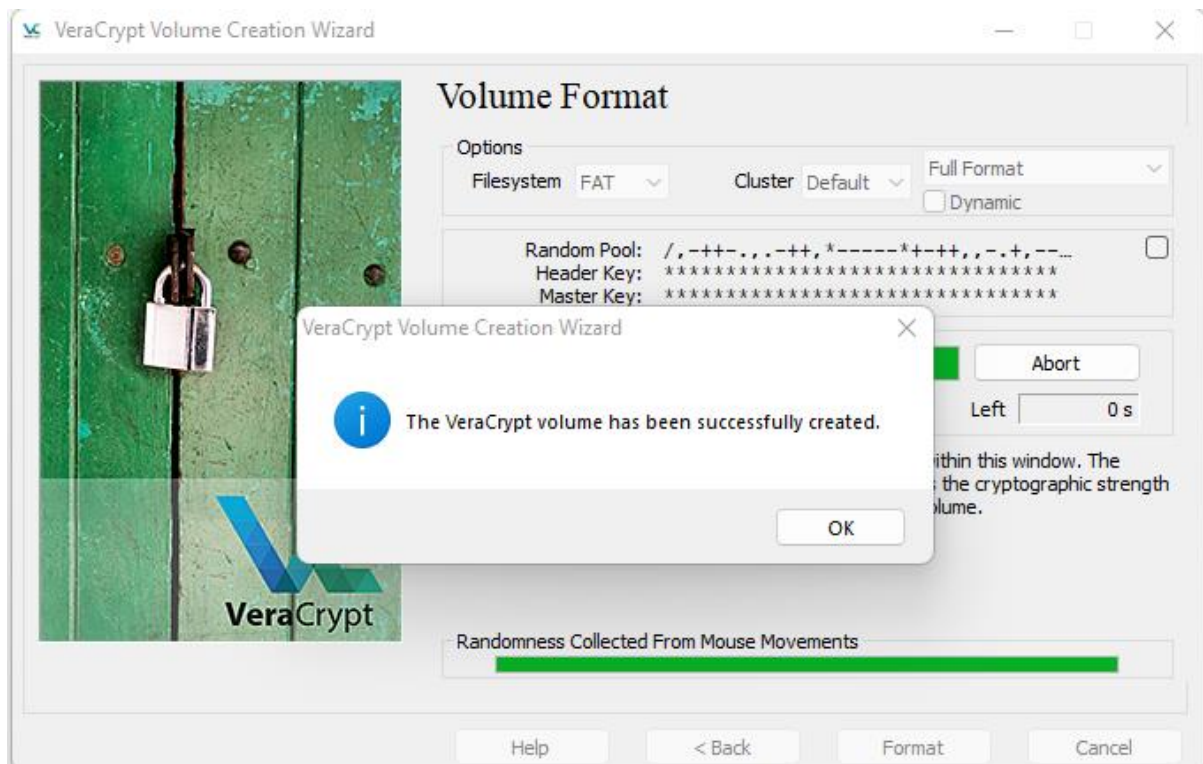
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Randomness Collected From Mouse Movements

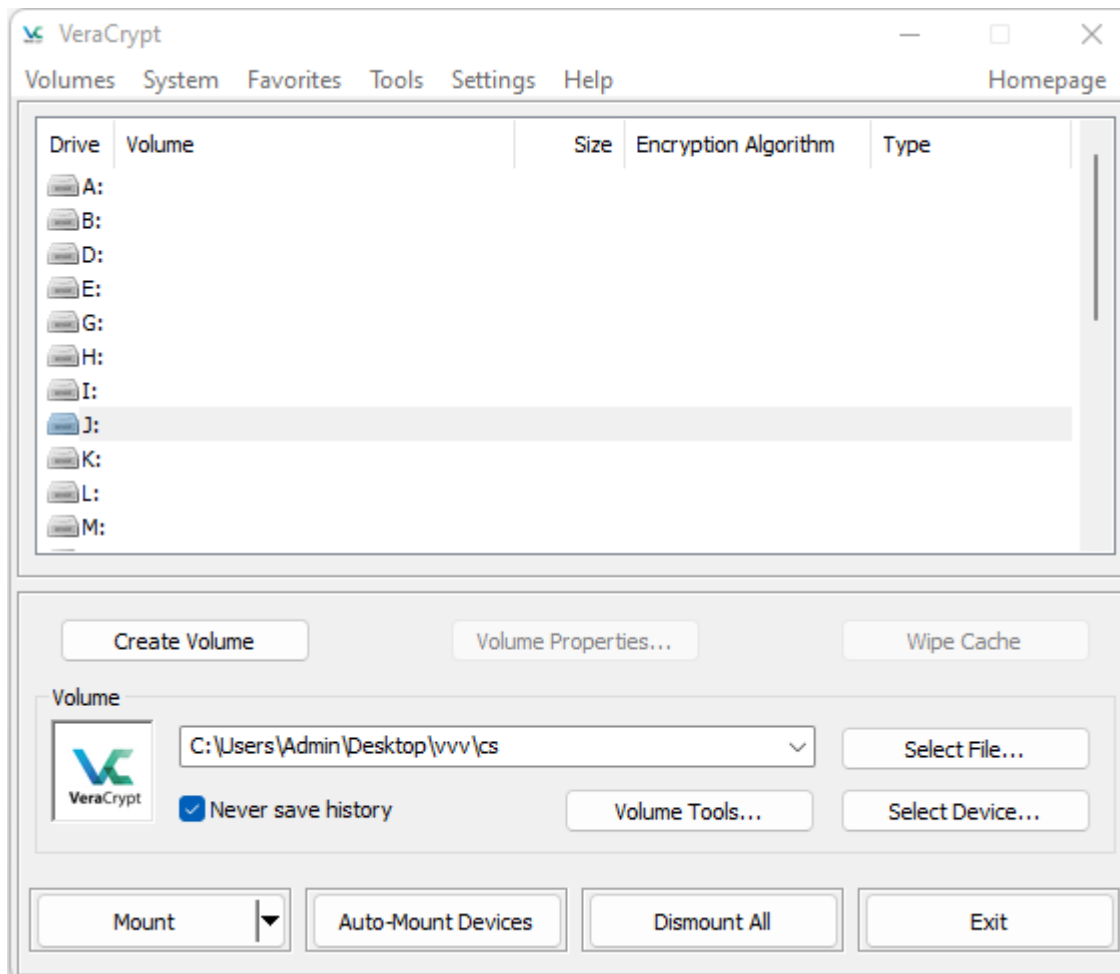
Help < Back Format Cancel



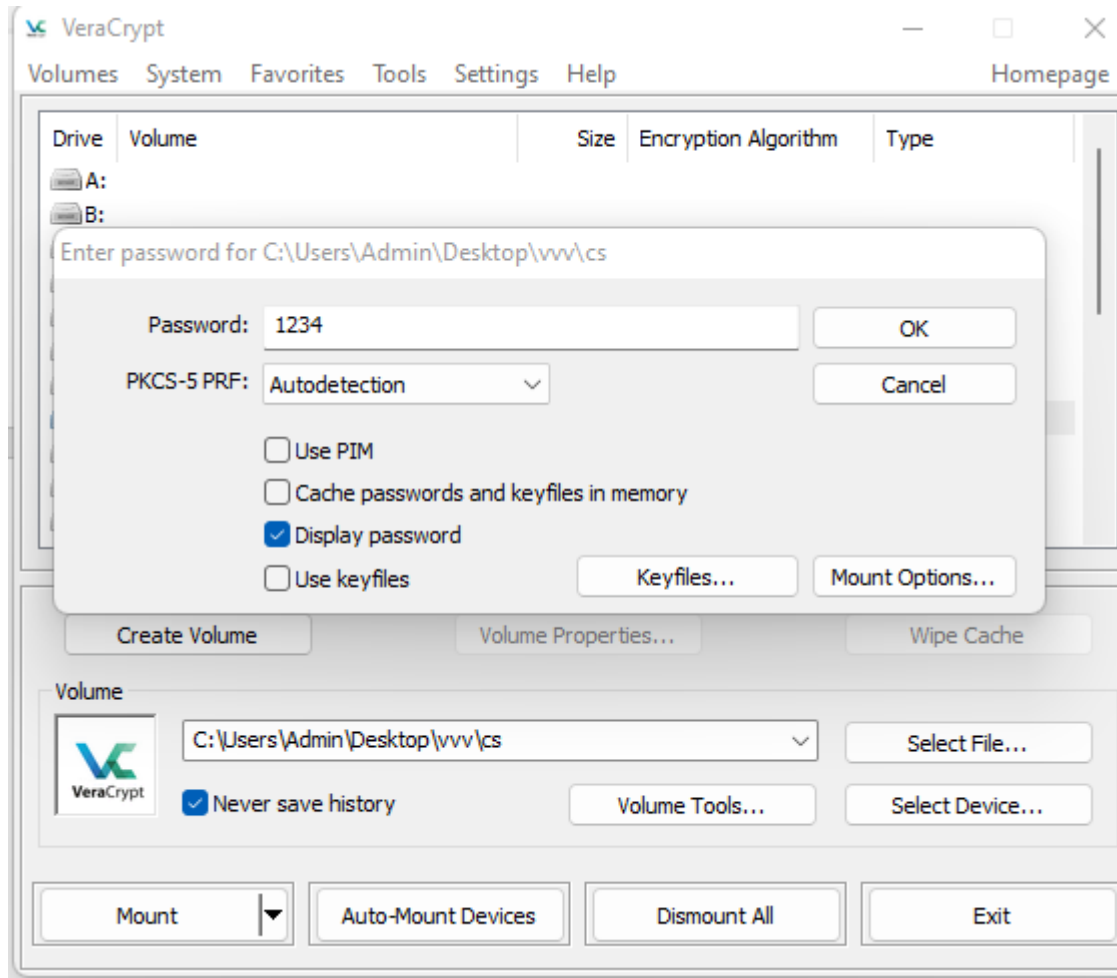
10. volume is created



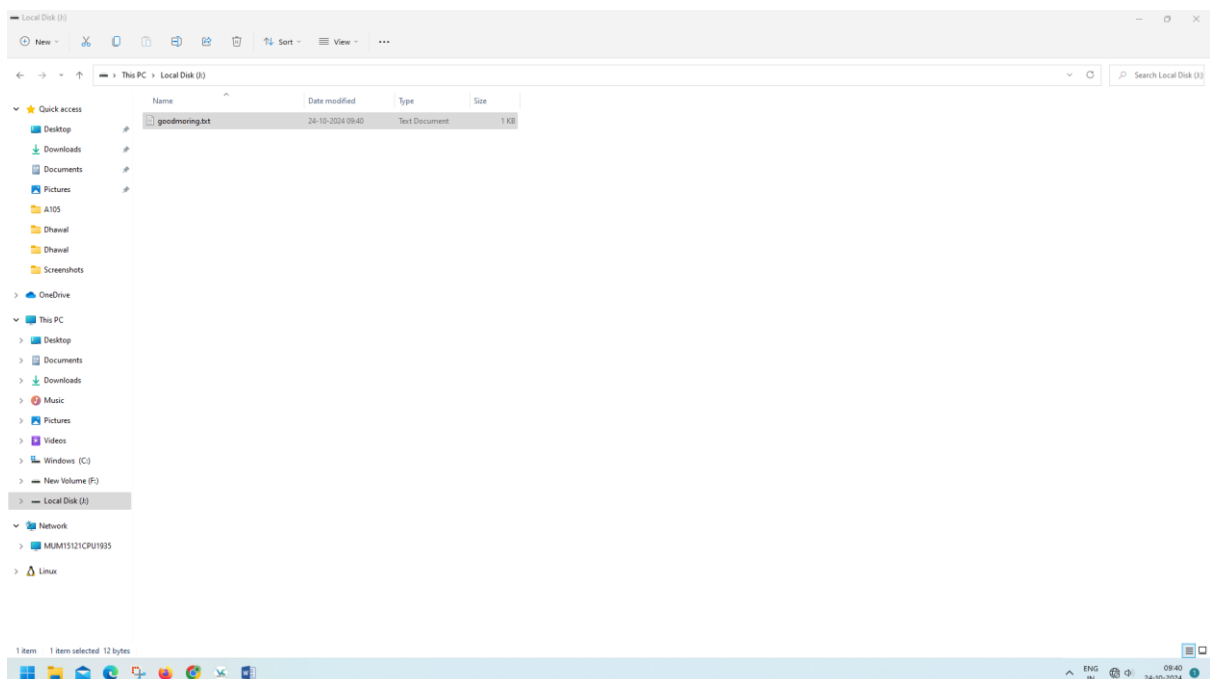
11. select the volume file location



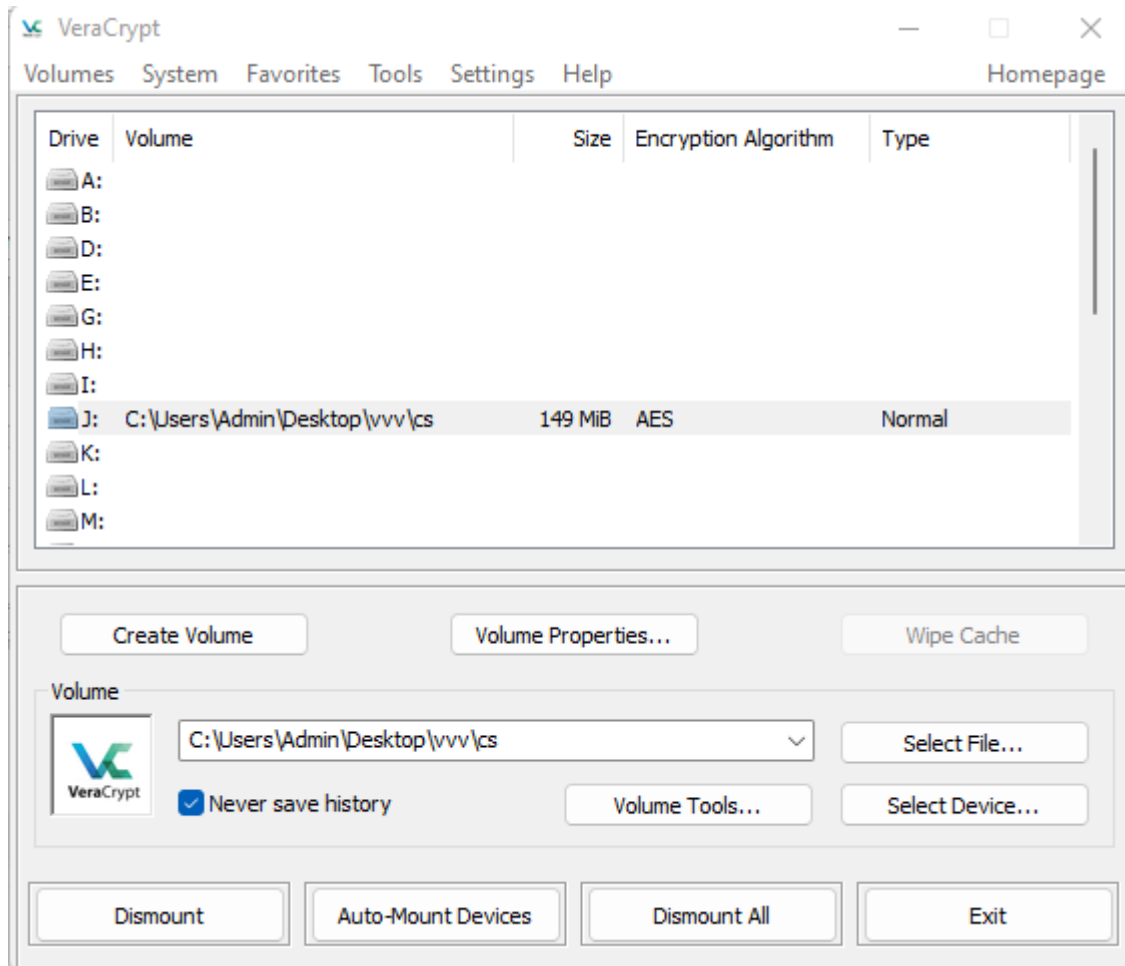
12. select mount and enter password



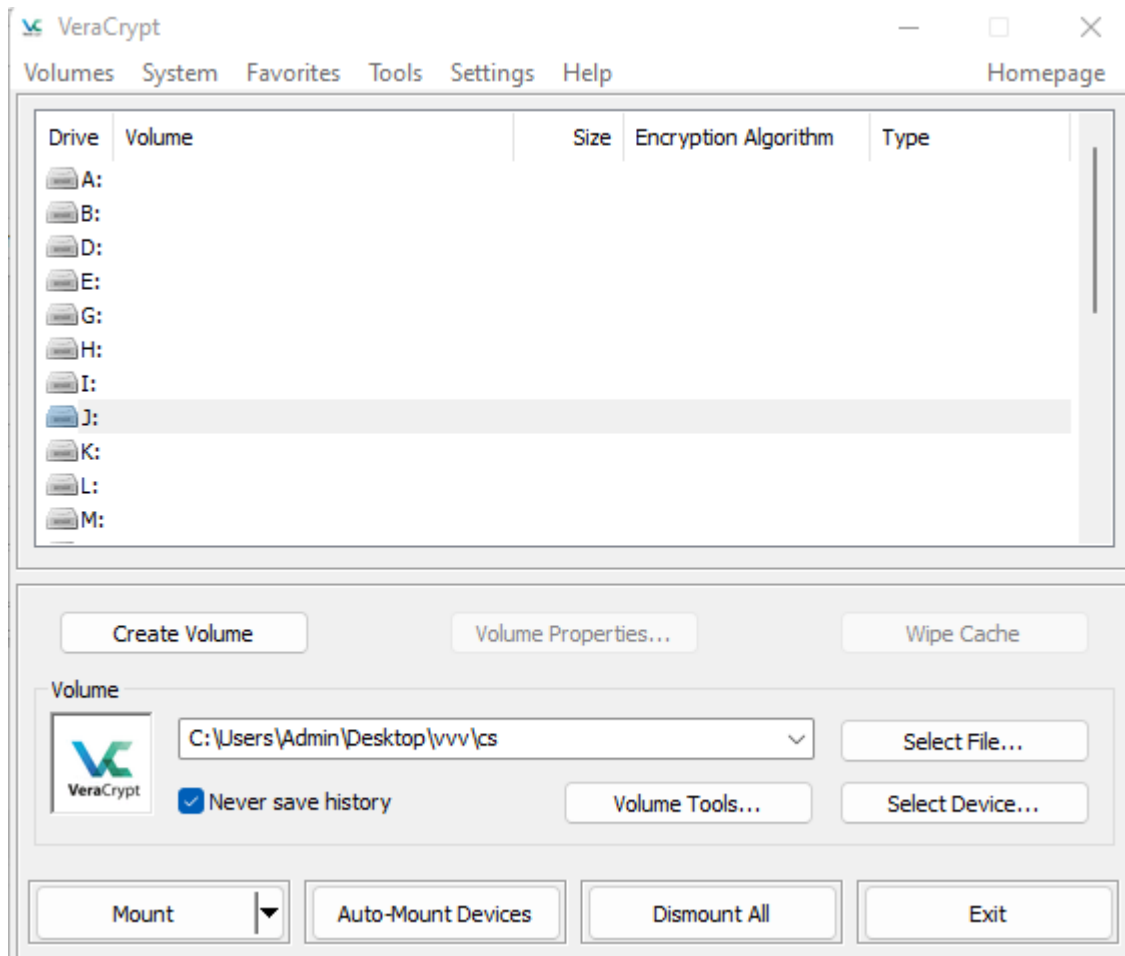
13. create a file in the create volume



14. it is visible that j is created



15. Now dismount the volume



16. J is not available

