

TrueCrypt and Friends

Dipl.-Inform. Volker Kamin

Aachen 2014

Why would you do that?

- Defect
- Theft
- Privacy (e.g., cloud storage)
- Seizure

What types are there?

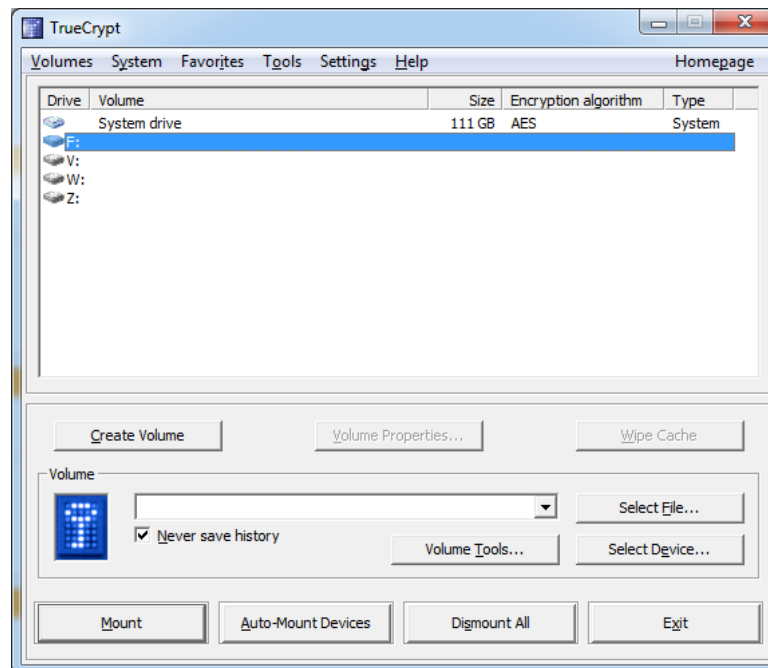
- File encryption
- Container encryption
- Partition encryption
- Drive encryption
- Full system encryption
- *Hidden volumes (not steganography)*

Alternatives

- TrueCrypt
 - Windows / Linux / Mac
 - Hidden volumes
 - Disclosed source, but not really Open Source
- LUKS (dm-crypt extension)
 - Open source
 - FreeOTFE for Windows
- BitLocker
 - Windows on-board
 - Closed source
- iOS & Android on-board encryption

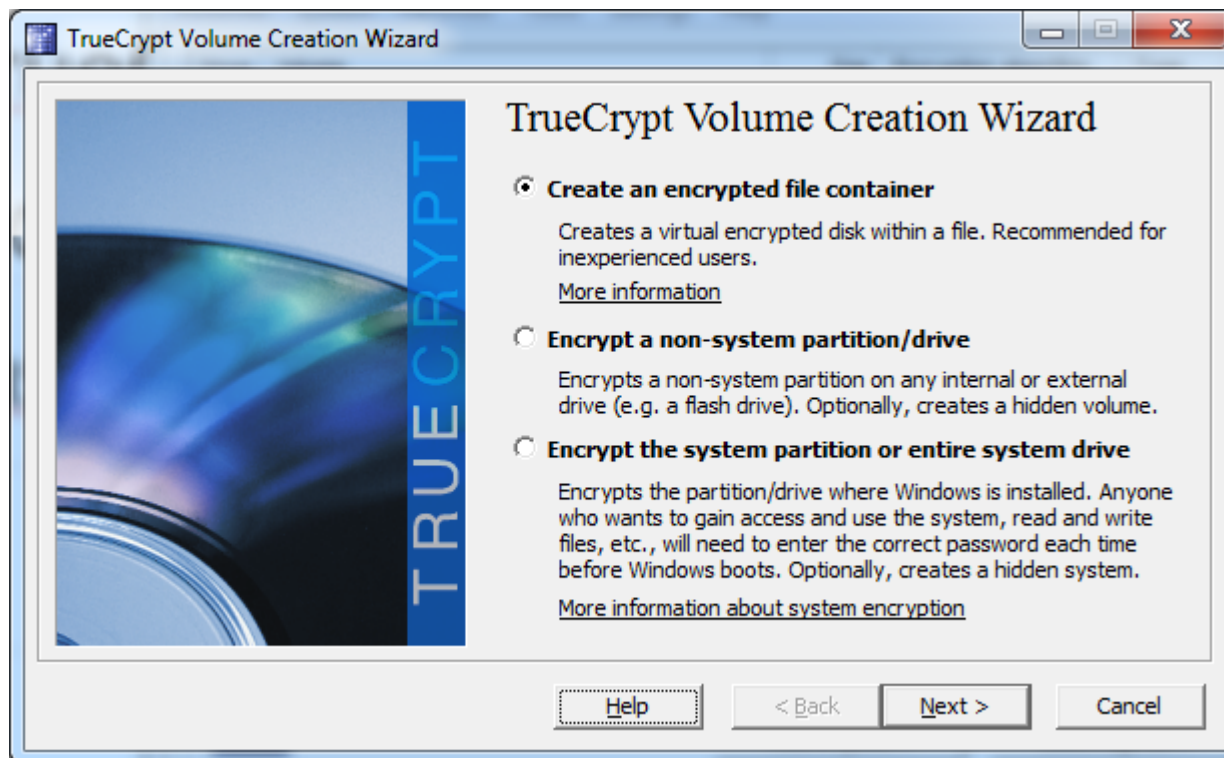
Quick Tour

- TrueCrypt for Windows
- Download installer from truecrypt.org
- Install like any other windows program



Create a volume

- Volumes → Create New Volume...
- The assistant will guide you



Choices

- Standard vs. Hidden
- Location and name of container
- Cipher: AES, Serpent, Twofish, combinations
 - 256 bit key, 128 bit block, XTS
- Hash algorithm: RIPEMD-160, SHA-512, Whirlpool
- Size
- Password & Keyfiles
- Filesystem, cluster size, dynamic

System encryption

- Just like creating a container
- Mandatory header backup
 - Must create rescue disk
 - Great when working with children or parents
 - Virtual disks surface
- Can be done „on the fly“
- Pre-boot authentication

Weaknesses

- Malware on the system
- Password guessing
- Password brute-forcing
- Password logging, sniffing, extortion
- Bad implementation
- Broken crypto