TrueCrypt

Разработил: Стефан Манджуков

Факултетен номер: 13383

TrueCrypt е преустановена безплатна програма с достъпен код, позволяваща криптиране и декриптиране на файлове, дялове на дискове, или цели дискови утройства, давайки възможност за автентификация преди boot. Разработена през 2004г. от **TrueCrypt Foundation,** бива преустановена през 2014г. заради проблеми със сигурността[1].

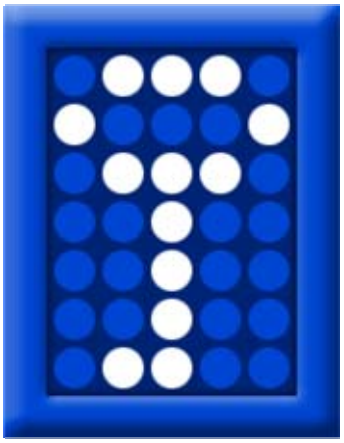
TrueCrypt създава *криптиран дял (или контейнер),* от който файловете се декриптират по време на изпълнението в системната памет. Това дава на потребителя удобството да монтира дяла, да го използва като нормален дял, след което да го размонтира, запазвайки целостта и сигурността на файловете вътре. **TrueCrypt** държи всички некриптирани файлове в паметта, и я почиства след себе си.

Предлагани криптографски шифри са **AES**, **Serpent**, и **Twofish.**
Serpent е най-силният от тях, но е също и най-бавен. AES е най-бързият от трите, но пък е по-слаб от Twofish и Serpent[2].

Предлагани хеширащи функции са **RIPEMD-160**, **SHA-512**, и **Whirlpool.** Тъй като SHA и Whirlpool са по-големи от RIPEMD, TrueCrypt ги използва само 1000 пъти при създаването на ключ, за разлика от 2000 пъти, когато се използва RIPEMD.

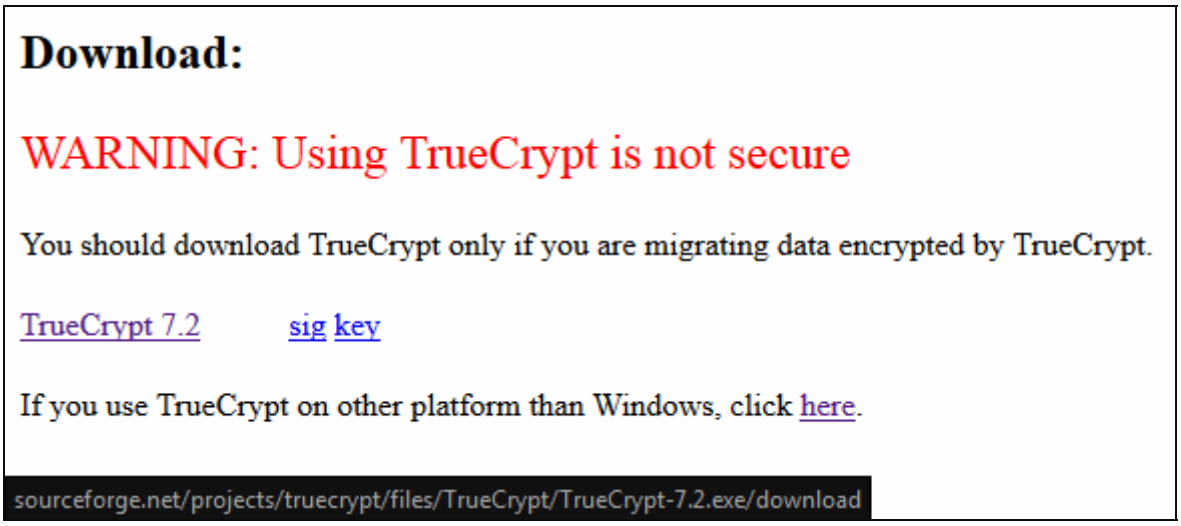
Поддържа се от Windows, OS X, Linux, FreeBSD, Android**.**

Не бива да се използва, освен за възстановяване на вече криптирана информация! Като алтернатива, разработчиците препоръчват **BitLocker** - вградена в Windows програма, извършваща криптиране на дисково ниво[3].

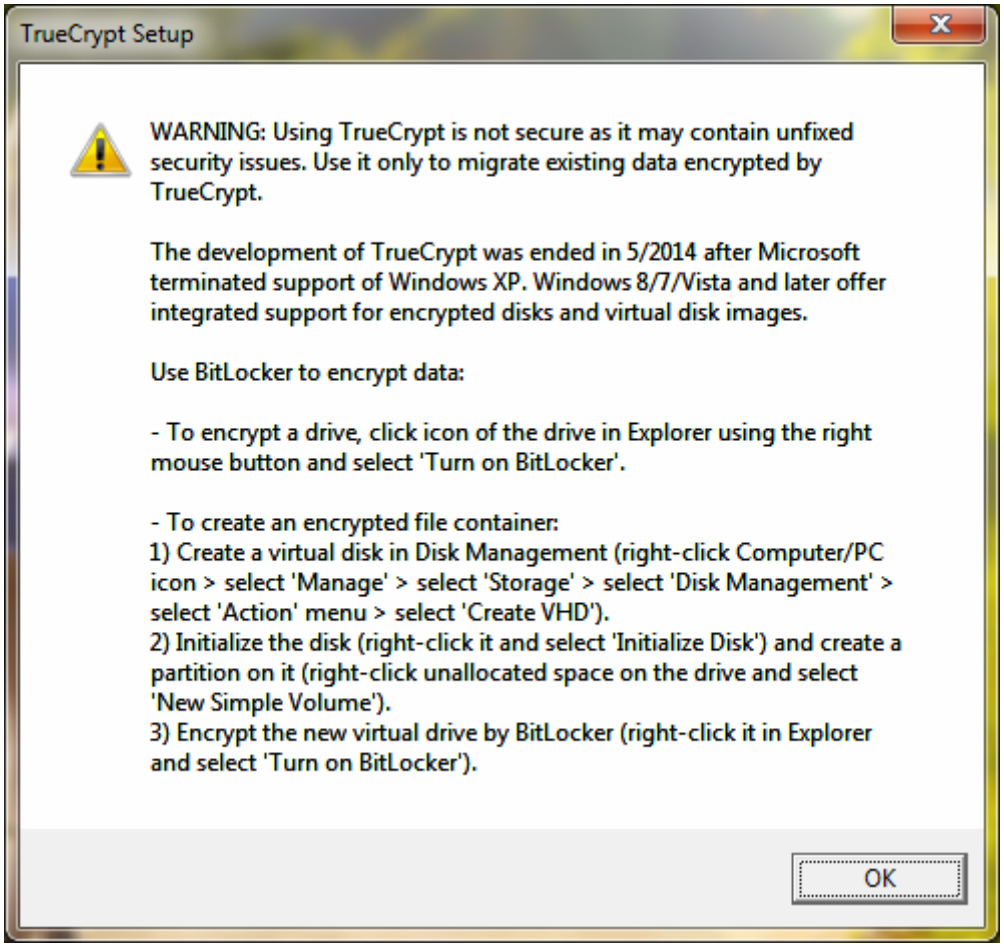


Фиг. 1. TrueCrypt - лого на програмата

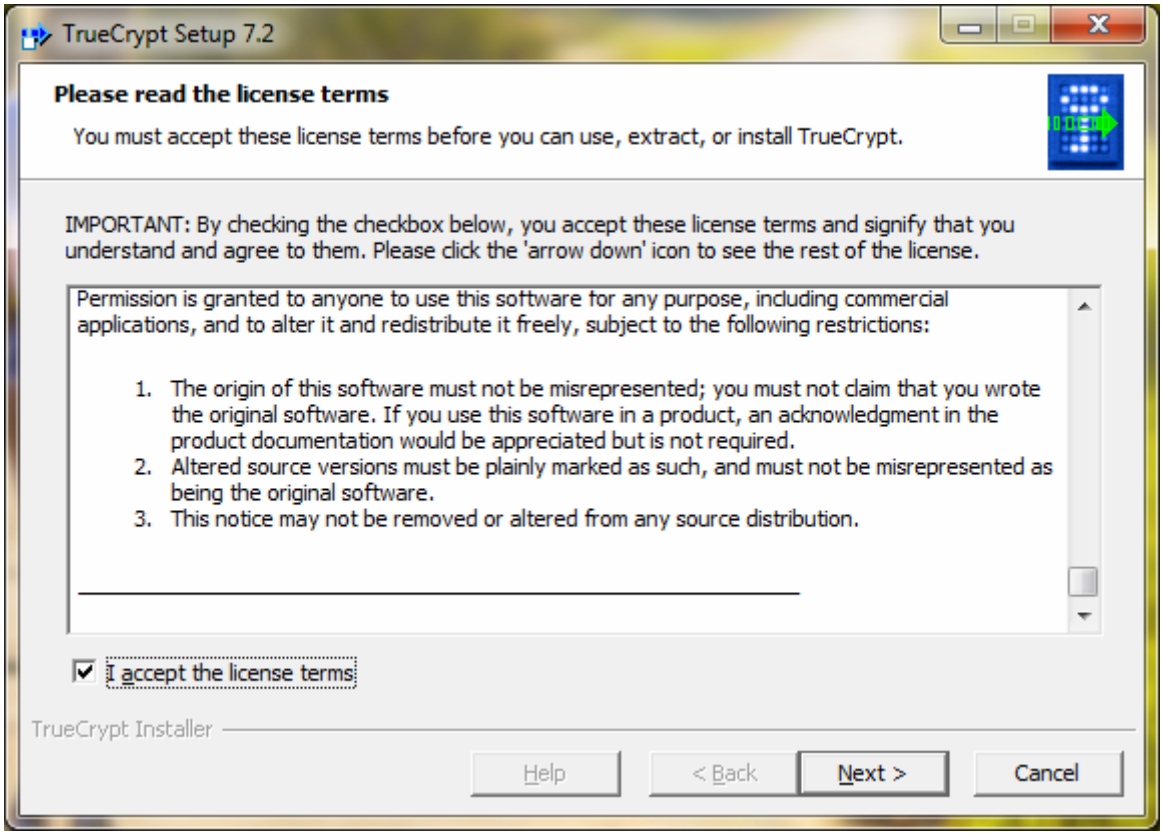
Инсталация



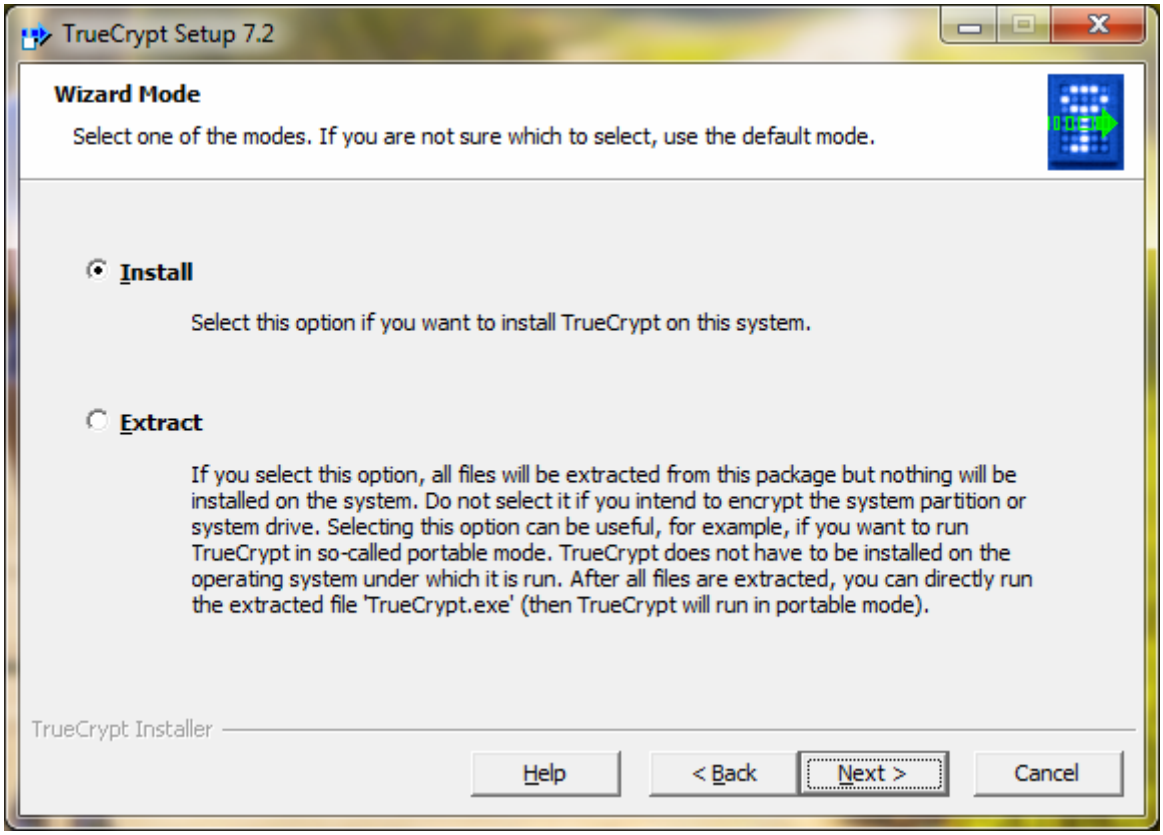
Фиг. 2. Изтегляне на програмата[4]



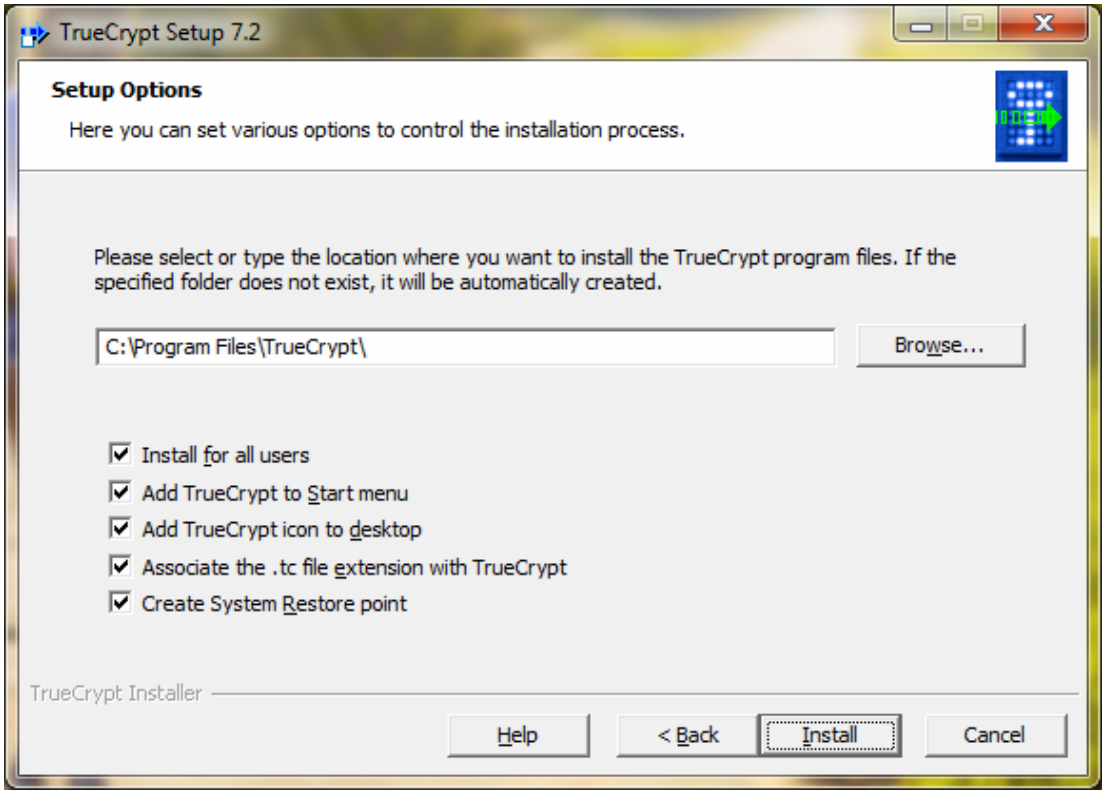
Фиг. 3. Предупреждение преди инсталация



Фиг. 4. Прочитане и съгласяване с лицензните условия

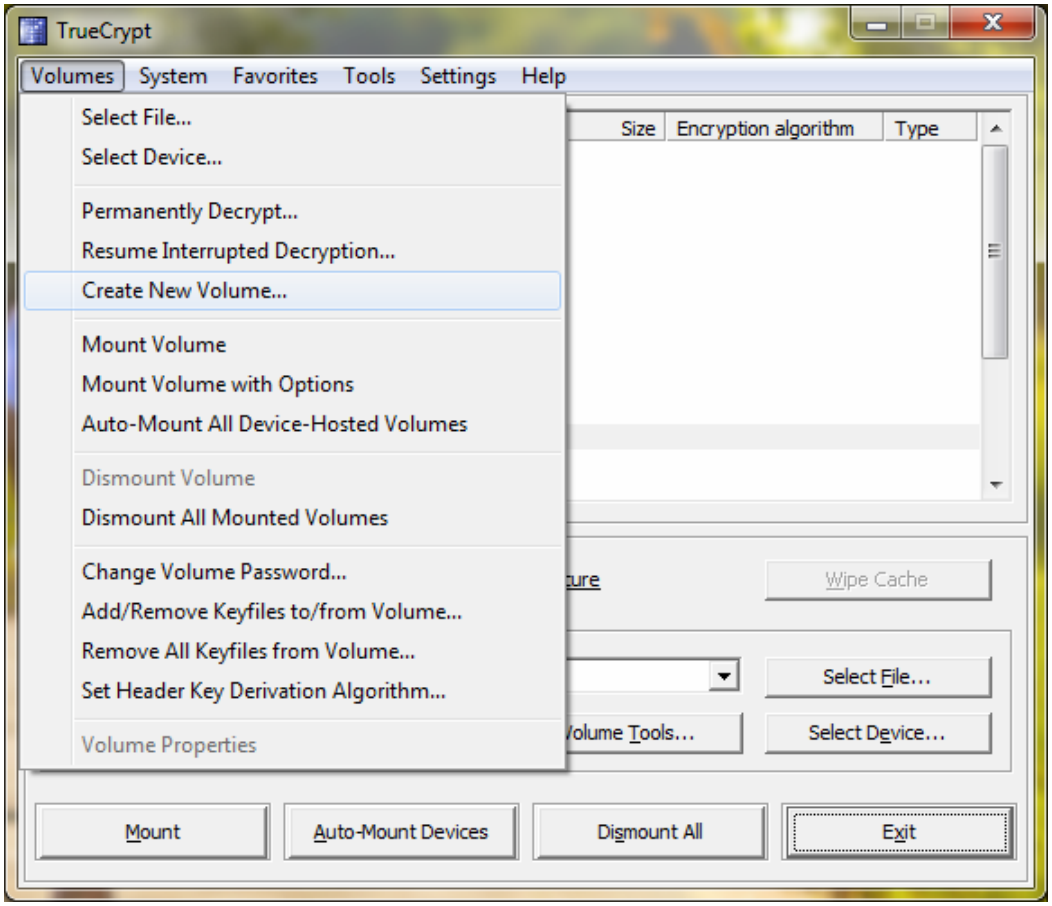


Фиг. 5. Избиране на начин на инсталация

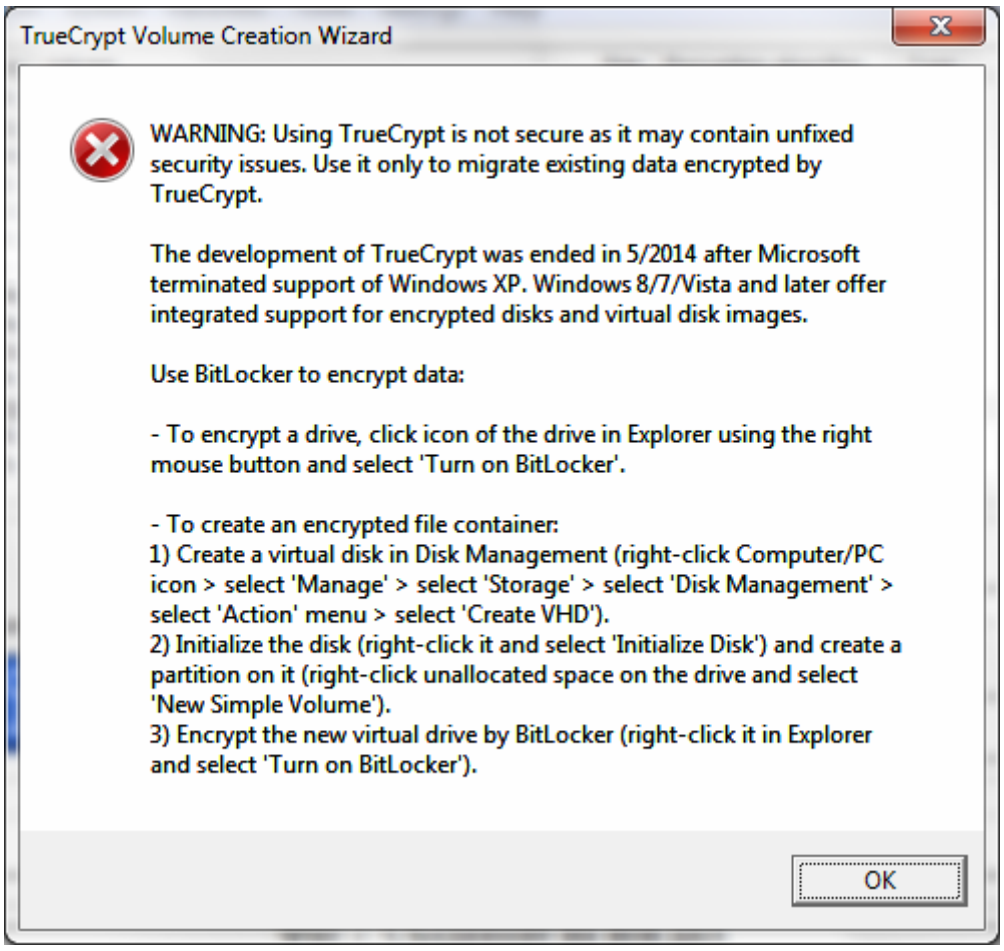


Фиг. 6. Указване на път и допълнителни опции към инсталацията

Използване на програмата



Фиг. 7. Създаване на нов дял



Фиг. 8. Фатална грешка

TrueCrypt не може и не бива да се използва за криптиране на информация, тъй като е несигурна.

Източници

1. http://www.darkreading.com/endpoint/the-mystery-of-the-truecrypt-encryption-software-shutdown-/d/d-id/1269323
2. http://www.reddit.com/r/crypto/comments/2wbrg1/aes_vs_twofish_vs_serpent/
3. http://www.howtogeek.com/192894/how-to-set-up-bitlocker-encryption-on-windows/
4. http://truecrypt.sourceforge.net/