Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 3

*Metode și mijloace tehnice de protecție a informației.*

A efectuat: st. gr. SI-211 Chihai Adrian

A verificat: dr. conf.univ. Colesnic Victor

Chișinău – 2024

**Lucrare de laborator 3**

**Tema:** Criptarea datelor, fișierelor. BitLoker

**Scopul lucrării**: Studierea softului Dekart Private Disk (sau un alt soft similar, ex. VeraCrypt). Utilizarea BitLoker-ului.

**Instalează VeraCrypt**:

* Descarcă VeraCrypt de pe site-ul oficial (<https://www.veracrypt.fr>).
* Instalează aplicația pe sistemul tău, urmând instrucțiunile oferite de programul de instalare.

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Figura 1.1 – Instalarea VeraCrypt

**Deschide VeraCrypt**:

* După instalare, deschide aplicația VeraCrypt.

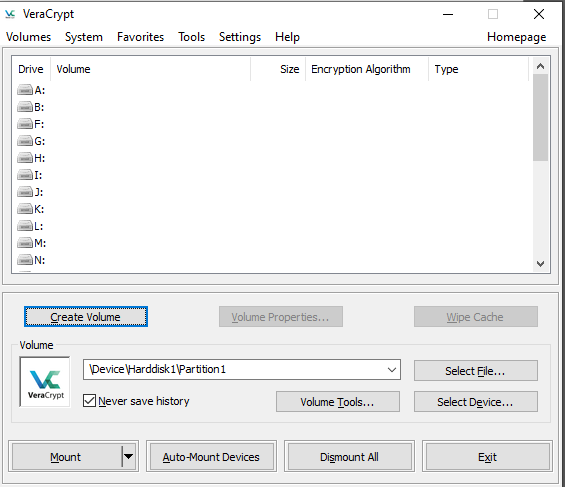


Figura 1.2 – GUI VeraCrypt

**Creează un nou container criptat**:

* În interfața principală, apasă pe butonul „**Create Volume**”.
* Selectează opțiunea „**Create an encrypted file container**” și apasă pe „Next”.

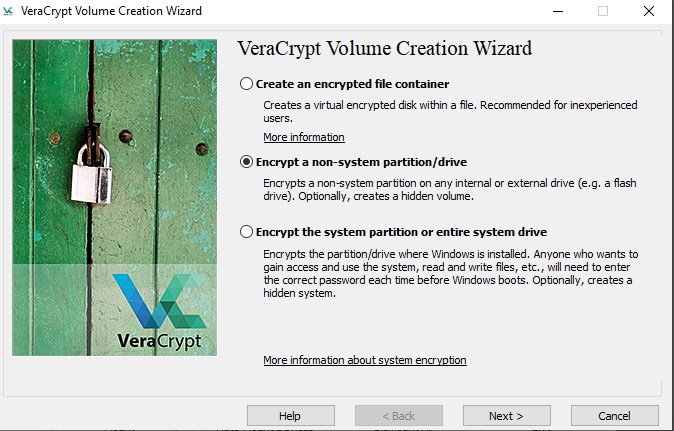


Figura 1.3 – Crearea unui nou container

**Alege tipul de volum**:

* Alege „**Standard VeraCrypt volume**” (dacă vrei un volum criptat simplu).
* Dacă vrei un volum ascuns, poți selecta „Hidden VeraCrypt volume”, dar pentru început e recomandat un volum standard.

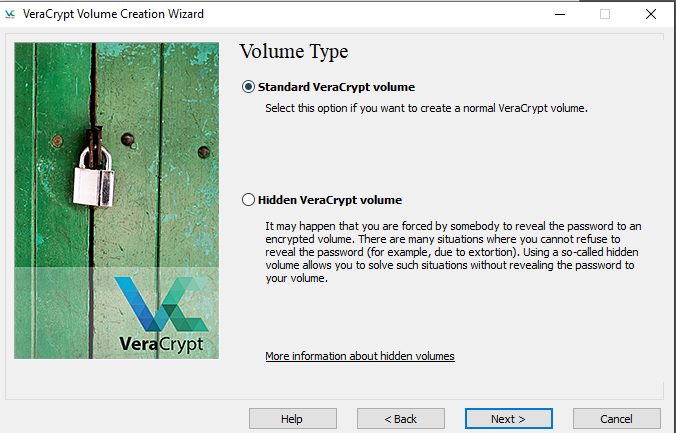


Figura 1.4 – Tipul de container

**Selectează locația fișierului container**:

* Alege locația unde vrei să creezi fișierul criptat. Apasă „**Select File**” și alege o locație și un nume pentru containerul tău.

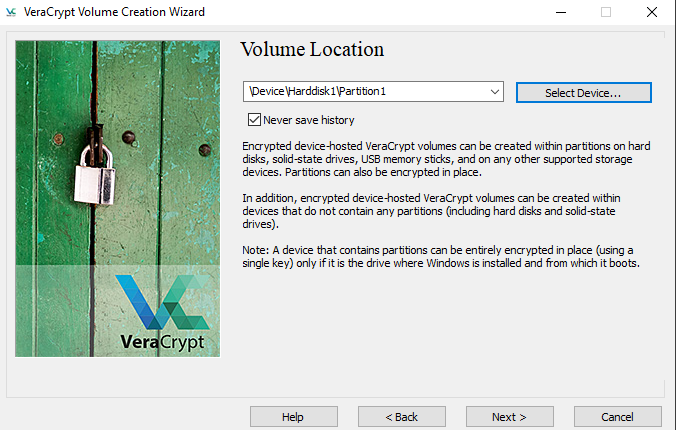
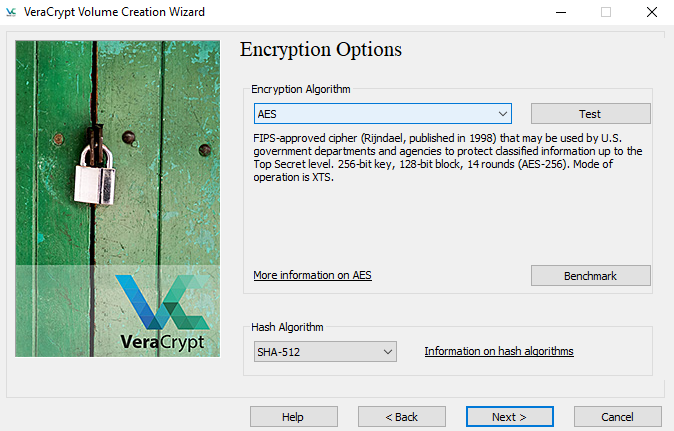


Figura 1.5 – Locatia fisierului



**Alege algoritmii de criptare**:

* Alege algoritmul de criptare și cel de hash. Algoritmii disponibili includ **AES**, **Serpent**, **Twofish**, iar pentru hash-uri sunt disponibile opțiuni ca **SHA-512** sau **Whirlpool**.
* Dacă nu ești sigur, AES este o alegere sigură și eficientă pentru majoritatea utilizatorilor. Apasă „Next” după selecție.

**Setează dimensiunea containerului**:

* Alege dimensiunea containerului (în MB sau GB) în funcție de cât spațiu vrei să aloci fișierelor criptate.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Figura 1.6 – Alegerea dimensiunea containerului

**Setează o parolă**:

* Introdu o parolă puternică pentru containerul criptat. Asigură-te că parola este lungă și complexă (combinație de litere mari și mici, cifre, simboluri).
* Dacă parola este prea scurtă, VeraCrypt te va avertiza că o parolă slabă poate compromite securitatea datelor.

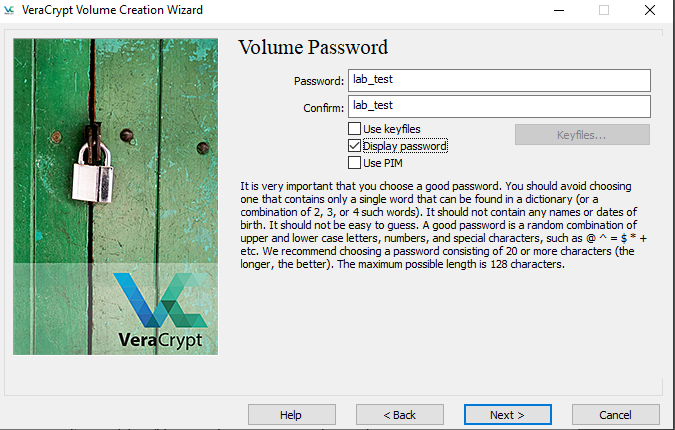


Figura 1.7 – Setez o parola

**Formatarea containerului**:

* Alege sistemul de fișiere (de obicei **FAT** sau **exFAT** pentru compatibilitate largă, sau **NTFS** pentru fișiere mai mari).
* Mișcă mouse-ul într-un mod aleatoriu în fereastra de formatare pentru a crește calitatea criptării. Apasă „**Format**” după ce ai terminat.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Figura 1.8 – Generarea intropiei

**Montează containerul criptat**:

* După ce containerul este creat, revino la fereastra principală VeraCrypt.
* Apasă „**Select File**” pentru a alege fișierul containerului criptat.
* Alege o literă de unitate (drive letter) liberă, apoi apasă „**Mount**”.
* Introdu parola și containerul va fi montat ca o unitate virtuală în Windows.

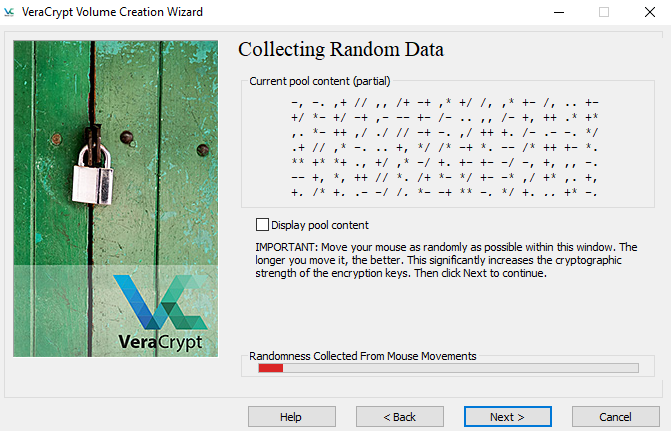


Figura 1.9 – Criptarea tomului

**Utilizează containerul**:

* Acum poți accesa containerul ca pe orice altă unitate din „My Computer” (sau „This PC”).
* Poți copia fișiere în și din container în siguranță. După ce ai terminat, trebuie să „unmount” containerul pentru a-l bloca și securiza.

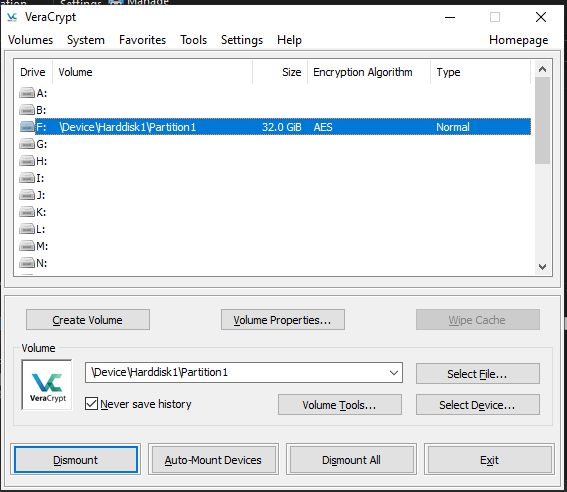


Figura 1.20 – Montarea tomului

**Demontarea containerului criptat**:

* Când ai terminat de folosit containerul, deschide VeraCrypt și apasă „**Dismount**” pentru a închide accesul la fișierele criptate.

Concluzie: În urma criptării unui container cu VeraCrypt, putem concluziona că acest proces oferă un nivel ridicat de securitate pentru protejarea datelor sensibile. Prin utilizarea algoritmilor avansați de criptare, precum AES sau Serpent, informațiile stocate în container devin inaccesibile pentru persoanele neautorizate, chiar dacă acestea au acces la fișierul containerului.

VeraCrypt este o soluție flexibilă, permițând criptarea unui volum într-un mod relativ simplu și eficient. Totuși, succesul acestei metode depinde în mare măsură de alegerea unei parole puternice și de gestionarea corespunzătoare a accesului la volum. De asemenea, măsura suplimentară de demontare a volumului atunci când nu este utilizat garantează că datele rămân protejate în orice situație.