REPUBLIC OF CAMEROON

PEACE-WORK-FATHERLAND

MINISTRY OF HIGHER EDUCATION

UNIVERSITY OF BUEA

REPUBLIQUE DU CAMEROUN

PAIX-TRAVAIL-PATRIE

MININSTERE DE L'ENSEIGNEMENT SUPERIEURE

UNIVERSITE DE BUEA

FACULTY OF ENGINEERING AND TECHNOLOGY (FET)

DEPARTMENT OF COMPUTER ENGINEERING

CEF 451: SECURITY OF INFORMATION SYSTEM AND CYBERSECURITY

PASSWORD SECURING AND FILE ENCRYPTION SOFTWARE

CASE STUDY: KeePassX and Veracrypt

Submitted by: QUINUEL TABOT NDIP-AGBOR

Matricule: FE21A300

Supervised by: Dr. TSAGUE Aline

I. IMPLEMENATION OF KEEPASS SOFTWARE:

Overview of KeePass Password Safe

With so many passwords to remember and the need to vary passwords to protect your valuable data, it's nice to have KeePass to manage your passwords securely. Password Safe puts all your passwords in a highly encrypted database and locks them with one master key or a key file.

As a result, you only have to remember one master password or select the key file to unlock the whole database. And the databases are encrypted using the best and most secure encryption algorithms currently known, AES and Twofish. KeePass is free, and more than that: it is opensource (OSI certified). You can look at its complete source and check whether the encryption algorithms are implemented correctly.

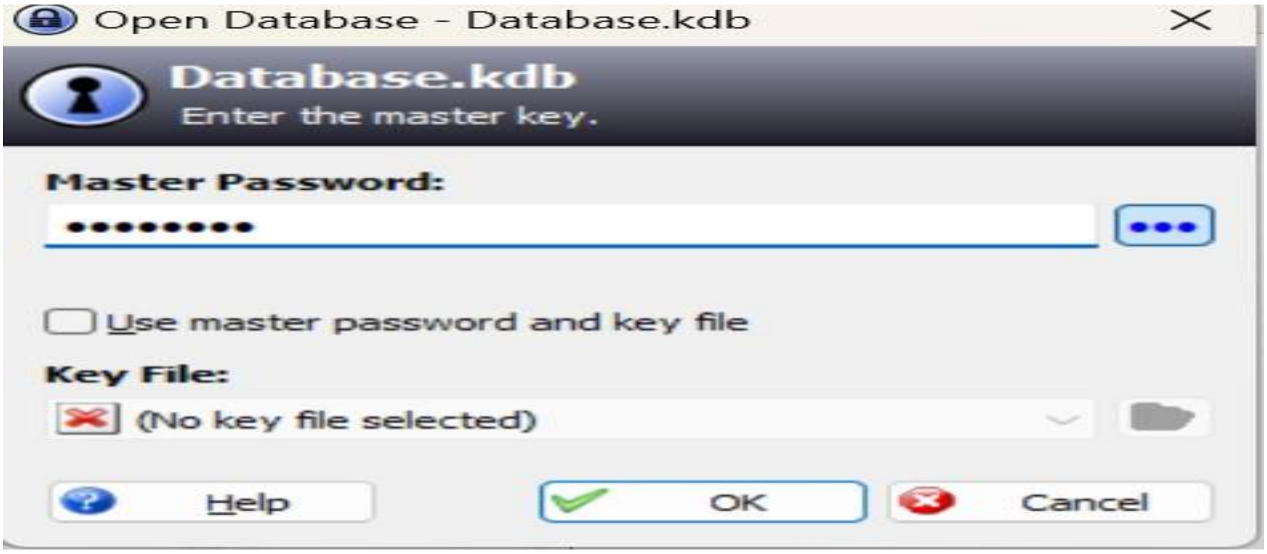
Working Principle

1. **Installation:**

Download and install KeePass from the official website https://keepass.info/
The installation process is typically straightforward, similar to installing other software.

2. **Creating a Password Database:**

Upon launching KeePass for the first time, you'll be prompted to create a new password database



Open Database - Database.kdb

Database.kdb
Enter the master key.

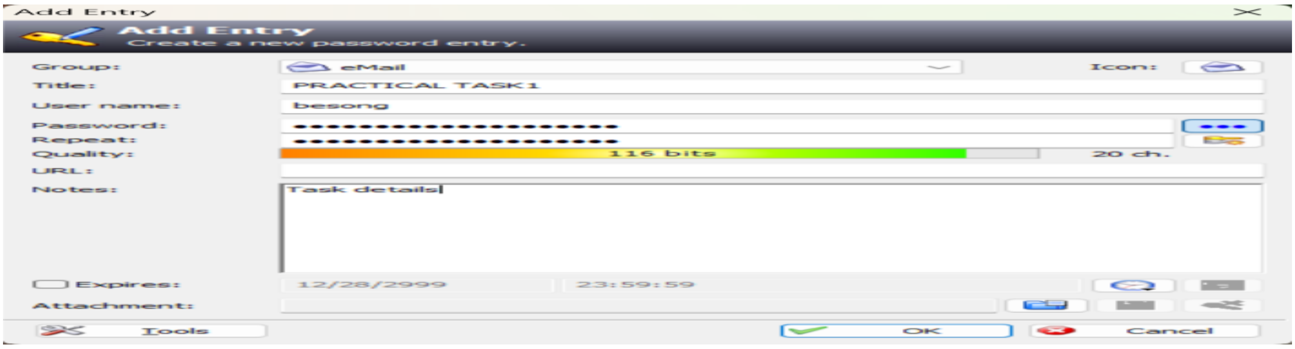
Master Password: •••••••••

□ Use master password and key file

Key File: (No key file selected)

3. Adding Entries:

After setting up the master password, you can start adding entries to your database. Entries typically include information such as website URLs, usernames, passwords, and additional notes.



Add Entry

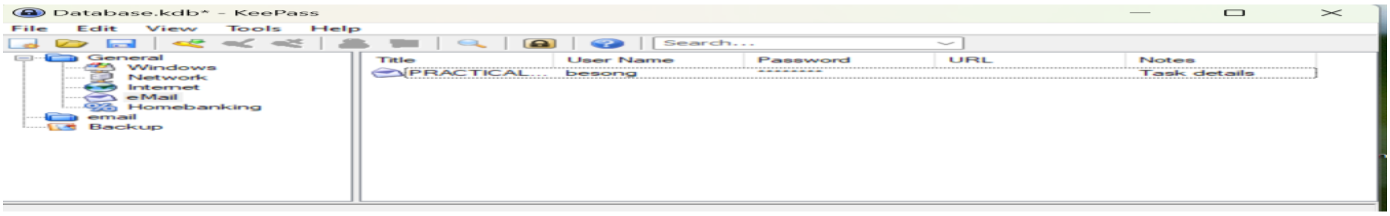
Add Entry
Create a new password entry.

Group: eMail
Icon:
Title: PRACTICAL TASK1
User name: besong
Password: •••••••••••••••••••••••
Repeat: •••••••••••••••••••••••
Quality: 116 bits 20 ch.
URL:
Notes: Task details

□ Expires: 12/28/2999 23:59:59
Attachment:

4. Organizing Entries:

KeePass allows users to organize their entries into groups or categories.
Users can create folders or use tags to further categorize and manage their passwords.



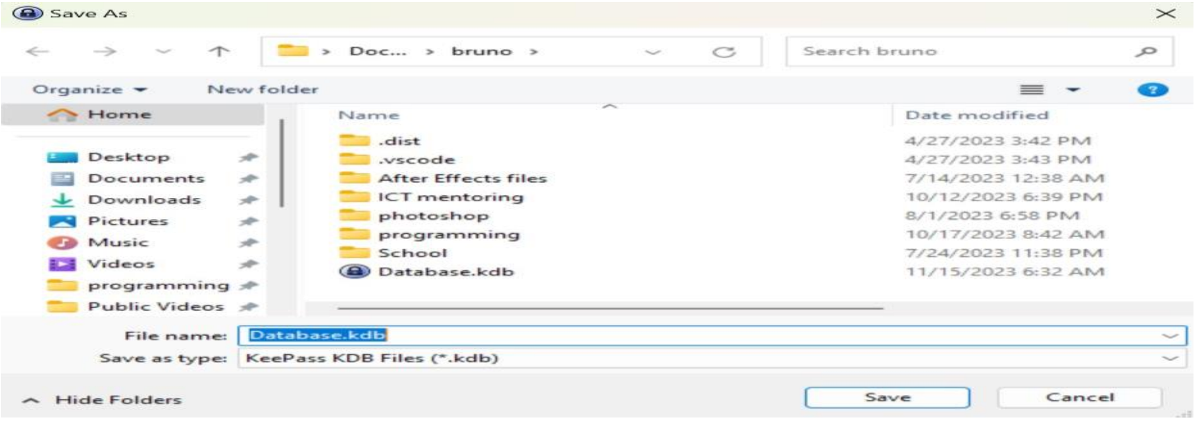
Database.kdb* - KeePass

- General
  - Windows
  - Network
  - Internet
  - eMail
  - Homebanking
- email
- Backup

Title	User Name	Password	URL	Notes
PRACTICAL...	besong	********		Task details

5.Backup and Sync:

Users are encouraged to regularly back up their KeePass database to prevent data loss.
The database file can be stored locally or synced across devices using secure cloud storage.



Save As

Name	Date modified
.dist	4/27/2023 3:42 PM
.vscode	4/27/2023 3:43 PM
After Effects files	7/14/2023 12:38 AM
ICT mentoring	10/12/2023 6:39 PM
photoshop	8/1/2023 6:58 PM
programming	10/17/2023 8:42 AM
School	7/24/2023 11:38 PM
Database.kdb	11/15/2023 6:32 AM

File name: Database.kdb
Save as type: KeePass KDB Files (*.kdb)

II. IMPLEMENATION OF ENCRPTION SOFTWARE (VERACRPT)

VERACRYPT Overview

1. **What is VeraCrypt?**

VeraCrypt is a free, open-source disk encryption software. It's designed to provide on-the-fly encryption for your data, allowing you to create encrypted volumes or encrypt entire storage devices.

2. **Encryption Features:**

On-the-Fly Encryption: VeraCrypt encrypts and decrypts data in real-time as it is read from or written to the disk.

Strong Encryption Algorithms: It supports various encryption algorithms such as AES, Serpent, and Twofish, and allows users to combine these for enhanced security.

3. **Supported Platforms:**

VeraCrypt is available for Windows, macOS, and Linux. This cross-platform support makes it versatile for users with different operating system preferences.

4. **Volume Types:**

VeraCrypt supports two main types of encrypted volumes:
File Containers: You can create an encrypted file container, which acts like a virtual encrypted disk within a file.
Full Disk Encryption: You can encrypt an entire disk partition or drive.

5. **Hidden Volumes and Plausible Deniability:**

VeraCrypt provides a unique feature known as hidden volumes. This allows users to create a decoy or outer volume and a hidden volume within it. The existence of the hidden volume cannot be proven, offering a layer of plausible deniability.

6. **Passwords and Keyfiles:**

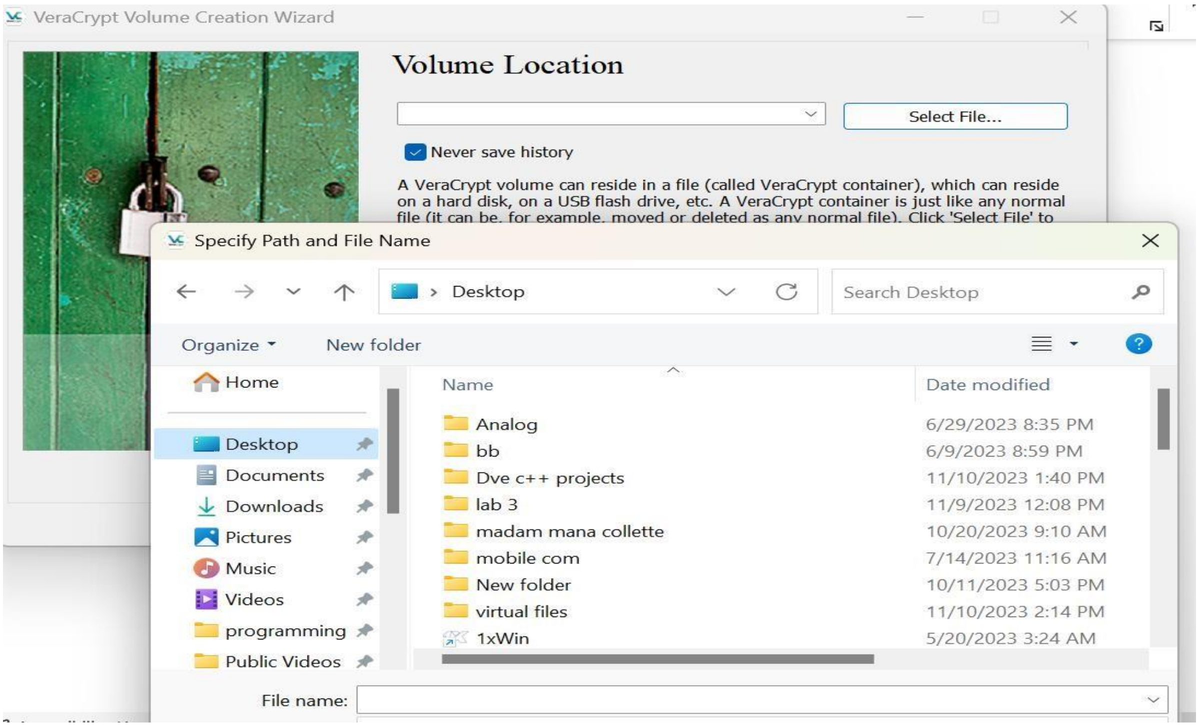
You can use passwords, keyfiles, or a combination of both for authentication. This adds an extra layer of security by requiring both something you know (password) and something you have (keyfile).

How Veracrypt Works

1. **Installation**
   - Download and install Veracrypt from the official website: https://veracrypt.fr/en/Downloads.html
   - The installation process is similar to installing other software

2. **Creating an Encrypted Volume**
   - Launch Veracrypt and click on "Create Volume."
   - Choose whether you want to create an encrypted file container or encrypt a non-system partition/drive.

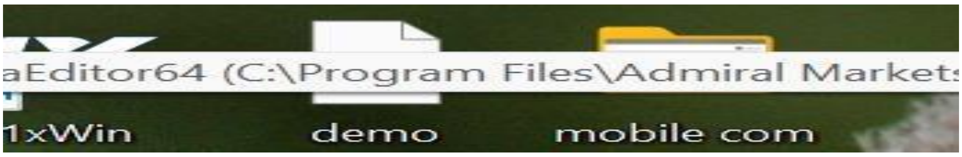
3. **Encrypting a File Container:**
   - If you choose to create an encrypted file container:
   - Select a location to save the container file.
   - Define the size of the container.
   - Choose a strong password, keyfiles, or a combination for added security



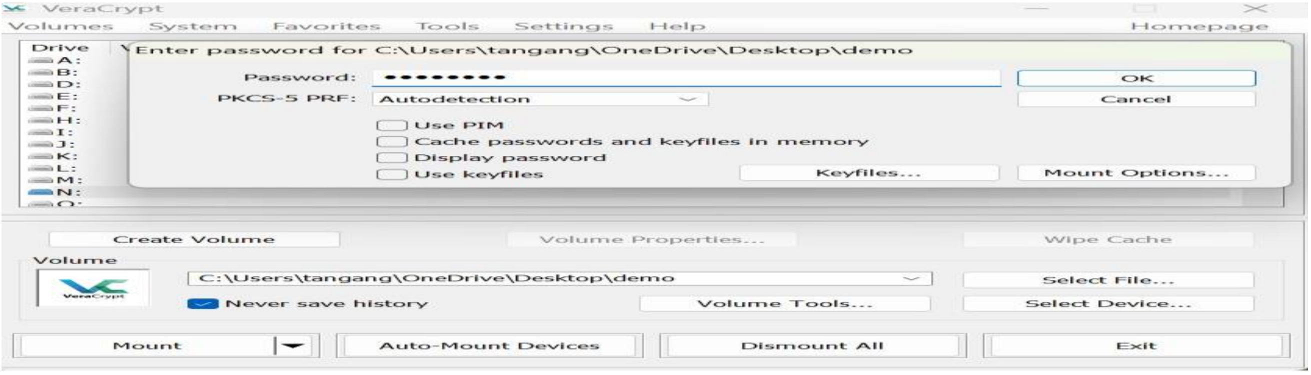
A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to

Name	Date modified
Analog	6/29/2023 8:35 PM
bb	6/9/2023 8:59 PM
Dve c++ projects	11/10/2023 1:40 PM
lab 3	11/9/2023 12:08 PM
madam mana collette	10/20/2023 9:10 AM
mobile com	7/14/2023 11:16 AM
New folder	10/11/2023 5:03 PM
virtual files	11/10/2023 2:14 PM
1xWin	5/20/2023 3:24 AM

A demo file is created on the desktop



4. **Encrypting a File Container:**
   - If you choose to create an encrypted file container: Select a location to save the container file.
   - Define the size of the container.
   - Choose a strong password, keyfiles, or a combination for added security.



Enter password for C:\Users\tangang\OneDrive\Desktop\demo

Password: ••••••••

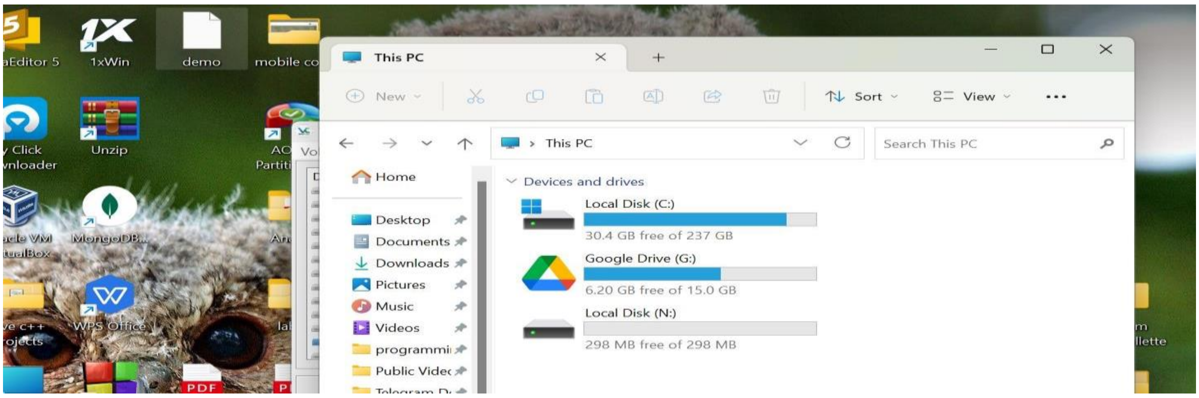
PKCS-5 PRF: Autodetection

□ Use PIM
□ Cache passwords and keyfiles in memory
□ Display password
□ Use keyfiles

Volume: C:\Users\tangang\OneDrive\Desktop\demo

☑ Never save history

The encrypted file is now moved to the newly created volume

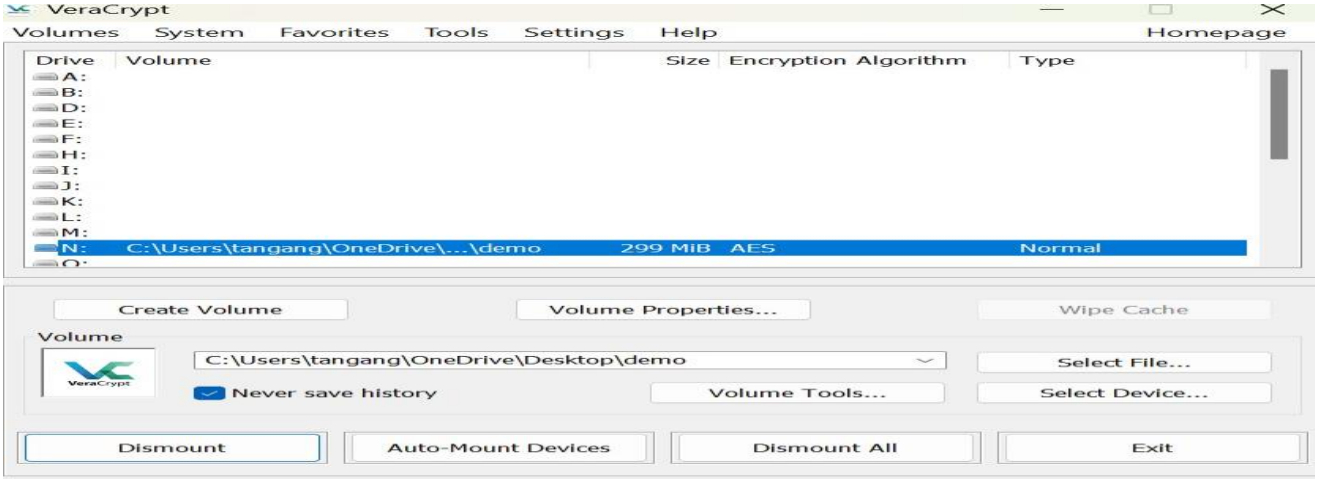


This PC > Devices and drives

Local Disk (C:)	30.4 GB free of 237 GB
Google Drive (G:)	6.20 GB free of 15.0 GB
Local Disk (N:)	298 MB free of 298 MB

5. Dismounting the Volume:

To secure your data, dismount the encrypted volume when you're done using it. This makes the data inaccessible until you mount it again



Drive	Volume	Size	Encryption Algorithm	Type
A:				
B:				
D:				
E:				
F:				
H:				
I:				
J:				
K:				
L:				
M:				
N:	C:\Users\tangang\OneDrive\...\demo	299 MiB	AES	Normal
O:				

Volume: C:\Users\tangang\OneDrive\Desktop\demo

☑ Never save history

Conclusion:

VeraCrypt is a powerful software tool that provides robust disk encryption and data protection. Its encryption methods, including system encryption and hidden volumes, offer versatile security options. The ability to encrypt individual files and folders enhances flexibility and convenience. By employing strong encryption algorithms and comprehensive security features, VeraCrypt ensures the confidentiality and integrity of sensitive data. Its usage promotes data privacy and protects against unauthorized access or data breaches.

The encrypted file can now be accessed by clicking on the volume.