Ethan Walton

28 September 2025

Ms. Emond

## VeraCrypt – Intro to Encrypted Volumes

### Lab Purpose

The purpose of this lab was to learn how to use VeraCrypt to create encrypted volumes for securing sensitive data. By following the tutorial, I practiced setting up a standard encrypted container, mounting it for use, and later creating a hidden volume within it. This lab is designed to demonstrate how hard drive encryption protects files and how VeraCrypt provides flexibility through both visible and concealed encrypted storage options.

### Tools & Resources

* VeraCrypt 1.25.9
* Windows 11
* VeraCrypt Beginner’s Tutorial
* File Explorer

### Lab Procedures

1. Launched VeraCrypt and selected “Create Volume”
2. Choose the option to create a volume within a file. This allows secure storage in a single file in the filesystem
3. Create a Standard VeraCrypt Volume
4. Chose a location to save the encrypted file container
5. Chose the encryption algorithm and hash algorithm, I just used the default
6. Set the container size to 200 mb to keep it simple and light
7. Created a volume password
8. Performed random mouse movements inside the wizard to strengthen the cryptographic key generation as recommended by VeraCrypt.
9. Chose the filesystem type for the new encrypted volume. I selected NTFS to support larger files, though FAT would also work for smaller use cases.
10. Completed the process by clicking Format. VeraCrypt successfully created the encrypted file container.
11. Returned to the main VeraCrypt interface and clicked Select File to choose the encrypted file container.
12. Assigned a virtual drive letter (for example, drive Z:) and clicked Mount. After entering the password, the container appeared as a mounted drive in File Explorer.
13. Transferred several test files (text documents and an image) into the encrypted container to confirm secure storage.
14. Un-mounted container from VeraCrypt.
15. Restarted the wizard to explore creation of a Hidden Volume within the original container. Selected the existing LabContainer.vc and followed prompts to define a secondary hidden partition inside it. This required setting a second password unique to the hidden volume.
16. Mounted the container again and tested accessing first the standard volume (using the original password) and then the hidden volume (using the hidden volume password). Both worked successfully, confirming VeraCrypt’s hidden volume support.

### Observations

Through this lab, I learned how VeraCrypt allows secure file storage through encrypted containers. The software’s interface emphasizes security best practices, such as random mouse movement to strengthen entropy during encryption key creation. I also observed that using different passwords determines whether the standard or hidden volume is accessed, which provides an additional layer of plausible deniability. A key takeaway is the importance of strong, unique passwords to maintain encryption security. Additionally, the hidden volume concept was particularly interesting, as it demonstrates how data can be concealed inside another encrypted volume to protect sensitive information further.

### Reflection Questions

1. **Why use a hidden volume instead of just a standard volume?**

Hidden volumes add a layer of plausible deniability. If a user is forced to reveal a password, they can provide the standard volume’s password, while still keeping the hidden volume secret.

1. **What are some practical scenarios for encrypted containers?**

They are useful for securely storing sensitive personal documents, research data, or work files on shared machines. They are also valuable for protecting external drives or USB devices in case they are lost or stolen.

1. **What risks remain even if files are encrypted with VeraCrypt?**

Risks include weak or reused passwords, malware capturing keystrokes, or users forgetting their password (which makes recovery impossible). Encryption mitigates data-at-rest attacks, but proper digital hygiene is still needed.

### Pictures/Screenshots

A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.