A screenshot of a computer

Description automatically generatedJonah McKitty – LIS5775

1. Creating new Volume

A screenshot of a computer

Description automatically generated

2. New file transferred to new Drive

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

4. Eraser running

3. Text file with 20MB

1. What would you see if you opened the text file you used in this project?

I would likely find encrypted data or instructions related to encryption or secure deletion algorithms.

1. What is the purpose of a “hidden” volume? (This was an option when you created the first volume.)

The purpose of a "hidden" volume is to provide plausible deniability. It allows users to create an additional encrypted volume within an already encrypted volume.

1. What are keyfiles and how do they work?

Keyfiles are external files used as an additional authentication factor for accessing encrypted data. They work alongside passphrases or encryption keys to enhance security.

1. Can VeraCrypt encrypt an entire drive (e.g., an external hard drive)?

Yes, VeraCrypt can encrypt entire drives, including external hard drives, providing strong encryption to protect all data stored on the drive.

1. What methods does Eraser use to “shred” the files?

Eraser typically uses methods like overwriting data multiple times with random or specific bit patterns to securely delete files, ensuring they cannot be recovered through data recovery tools.

1. Can you right-click any file and shred it directly (or securely move it to another directory)?

Yes, with software like Eraser, you can right-click on a file or folder and choose an option to securely delete it, initiating the shredding process directly from the context menu.

1. Why does it take so long? Could it go faster?

Secure deletion processes can take longer because they involve overwriting data multiple times to ensure it can’t be recovered.

1. Why isn’t this functionality included with Windows?

Advanced file encryption and secure deletion functionalities are not included with Windows likely because they're not universally required by all users, and third-party software like VeraCrypt and Eraser offers more specialized and customizable solutions for those who need them.