Testing & Evaluation Sheet

VeraCrypt

1. Tool Overview

Name:	VeraCrypt
Category:	Encryption
Purpose:	VeraCrypt is a free, open-source disk encryption software that uses strong encryption techniques to protect individual files, folders, and whole drives.
Date Tested	4/22/25
Status:	Deployed ☑ Operational - Actively running/maintained ☐ In Testing - Currently being evaluated or piloted ☐ Inactive/Deprecated - No longer maintained or functional
Deployment Architecture:	☑ A standalone software - Runs entirely locally (e.g., runs on computer and doesn't depend on external server) ☐ A locally hosted service with separate server and client component - Run both backend/frontend yourself (e.g., backend could be on a local network, or self-hosted on cloud) ☐ A service with a local client that's hosted by a third party - You install a client on your device, but it connects to and depends on a remote server (e.g., Signal: install app (client), but Signal's servers handle message relaying, etc.) ☐ A service that is hosted by a third party but can also be self-hosted
Version:	1.26.20

2. Installation & Setup

OS Compatibility	Windows, macOS (Monterey 12 and later), Linux, FreeBSD
Installation Manual:	Yes
Installation Steps:	● Download installer from the official VeraCrypt website. ● Run the installer and follow GUI prompts. ● Optional: Reboot (Windows) if driver installation is required.

	● Launch VeraCrypt.
Mention if command-line setup or special configurations are needed	No command line setup or special configurations required (can use command line instead of GUI and has documentation but is more complex and less intuitive).
Common Installation Issues & Fixes:	● Driver signature errors (Windows): Disable secure boot or manually allow drivers. ● Missing dependencies (Linux): Install using official packages or install required libraries (e.g., wxWidgets). ● macOS permissions issue: Grant full disk access to VeraCrypt under System Preferences > Security & Privacy. ● More limitations/issues
User Documentation:	Yes (Comprehensive user guides and FAQs available on official site)
Required Technical Knowledge	Intermediate (Easy setup but may require technical knowledge for the different encryption methods but there is some documentation for it)

3. Testing & Evaluation

Category	Details	Score
Operational Functionality:	**Functionality** ● Test Steps: Verify the tool's core features by using all major functions, tracking any failures or bugs. □ The tool is mostly non-functional with many broken features and bugs. □ Several broken features or bugs □ Minor bugs or issues □ Mostly functional with few bugs or no bugs ☑ Fully functional with no bugs **Internet Dependence:** ● Once installed, no internet required. Fully offline tool. **Localization & Language Support** ● 40+ languages, including Simplified & Traditional Chinese, Japanese, Korean. Community translation support exists. **Mobile Accessibility**	4.3

	● VeraCrypt is not mobile accessible and they do not plan to make it accessible either. ● They do provide other options for iOS and Android in their documentation.	
Usability for Non-Technical Users	**Ease of Installation & Deployment** ● 5–10 minutes installation time. GUI installer available. May take longer to download based off specs of device (can only use desktop) ● Setup Complexity: Not one-click install, but minimal setup process. ● Documentation: Available and frequently updated. There is extensive documentation on all security and cryptographic features. **User Onboarding Experience** ● Have an entire dedicated beginner's tutorial with extensive tutorial on how to use VeraCrypt. After downloading VeraCrypt it provides a message recommending reading it and links it directly to the tutorial. **Technical Experience Level Required** ● Intermediate – GUI is user-friendly but concepts of encryption, volumes, and keyfiles may require some understanding.	4.7
Security & Privacy Strength	**Encryption Standards** ● Includes many encryption algorithms: ○ AES, Camellia, Kuznyechik, Serpent, Twofish, Cascades of ciphers (different combinations of the other encryption algorithms) ● End-to-End Encryption for volume data **Hash Algorithms:** ● **BLAKE2s-256** ● **SHA-256** ● **SHA-512** ● **Whirlpool** ● **Streebog** ● Hash algorithm is used for VeraCrypt's Random Number Generator (unpredictable and secure keys for encrypting data safely) and header key derivation (turns password into a key that can decrypt those secure keys) **Known Strength resilience** ● The encryption software is usable in regions with heavy censorship and surveillance (like China)	5.0

because it works completely offline and cannot be detected.

- The encryption algorithms used are very high-brute force resistant and would require even powerful state actors a lot of time and prove extremely difficult.
- An extremely good feature is the hidden volume and hidden OS which support “plausible deniability” (way to reveal something under pressure without giving up everything)
    - Hidden Volumes:
        - Can create hidden volumes in regularly encrypted volumes
        - Can set up volume with two passwords where one is decoy volume and other is the hidden volume containing sensitive data
        - There is no way to tell if the hidden volume exists
    - Hidden OS (Operating System):
        - Same idea as hidden volume but booting up an entire operating system
        - Different passwords for Decoy OS, which has harmless files, and Hidden OS, which has real work
        - Only you know which one is real.
        -

Weaknesses:

- No file level encryption (encrypt entire folders, partitions, or virtual devices—not individual files)
    - To encrypt an individual file, you would need to mount a entire volume and to unlock it you would need to unlock entire vault (less convenient)
- No file sharing or syncing capabilities
    - Can store encrypted volumes in Dropbox/Google Drive but will not sync/update automatically
    - Hard to collaborate across devices
- If someone accesses your computer and installs a keylogger or watches your device, they can suspect something and act accordingly.

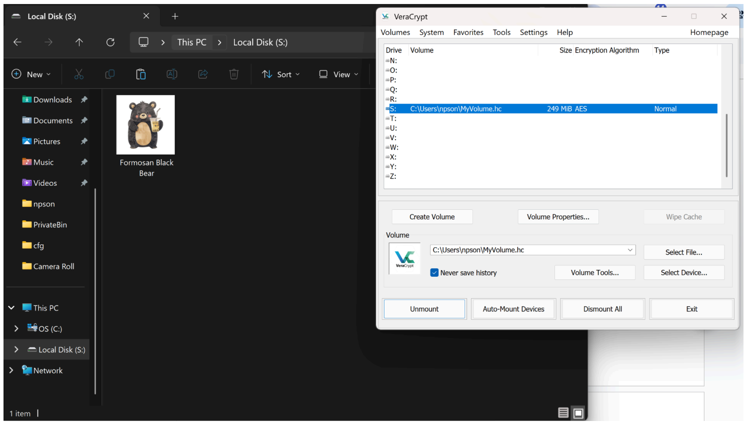
Comparison with Known Standards

	● Exceeds many privacy tool standards. ● It is used and trusted by many security professionals. ● One of the best encryption tools available. **Data Minimization** ● Collects no user data as it is entirely offline (no risk of any data tracked through network/internet). **Privacy Policy** ● No clear privacy policy but it is transparent and open source (does not collect data so no risk in that aspect)	
Maintenance/Sustainability	**Community support** ● Active community on public forums and GitHub. ● Has over 100 contributors. ● Can contact the development team if anyone has questions on contributions with contact information on their website. **Development active status** ● It is frequently updated with updates nearly every month. ● The development team is responsive and clearly looks at new contributions and approves if they are acceptable. **Funding and Sponsorship** ● Amount of funding not publicly known. ● Independent project without any major sponsors. ● VeraCrypt is actively involved in funding campaigns and other initiatives to support it. ● Users will see requests for donations on websites to help maintain the project.	4.3
Performance / Effectiveness & Reliability	**Testing Environment Setup:** ● **Device:** Dell XPS 15 ● **OS:** Windows ● **Network:** Not required (offline) **User Experience Observations** ● The tool feels really smooth from an user standpoint. ● VeraCrypt was quite responsive when being tested. ● A lot of the steps were very intuitive because there were pop up messages with important information and steps. **Speed & Responsiveness:** ● Minimal lag even with encrypted large volume. ● Slight delay when mounting and unmounting volume which is to be expected.	5.0

	○ Extremely large volume: Tested a 100GB volume and it takes roughly 1 minute to collect random mouse data (to format volume) and then about 800MB/s-1GB/s to actually create it (roughly 2 minutes). **Resource Usage:** ● Low usage during volume mounting (varies for size of volume but relatively low regardless). ● RAM Usage is low even for large volumes (~15MB) ● Disk Usage was roughly 800MB/s when formatting the volume. **Network Performance:** ● Not applicable—tool is completely offline (advantage) **Reliability** ● A 2016 audit by OSTIF and Quarkslab found and helped patch several issues, greatly improving reliability. ● No backdoors or fatal flaws were found in the cryptographic design. ● Particularly among societies that prioritize privacy, VeraCrypt is regarded as extremely reliable in terms of both security and functionality. ● Rarely fails when used properly.	
Deployment Considerations:	**Open Source & Transparency:** ● The source code is open for independent verification. **Cloud vs. Local Deployment:** ● Entirely local **Dependencies:** ● Minor dependencies required (if any)– Installer handles nearly all of them. On Linux, some GUI dependencies like **libwxgtk** may be needed. **Post-Deployment Maintenance** ● After potential deployment, the tool is easy to maintain (deploying it can be very complex and not necessary as there are audited released versions available). **Merge/Sustainability:** ● Actively accepts pull requests and improvements while having a criteria for contribution listed on the README section IV.	

4. Testing Scenarios

- **Scenario 1**
  Create and Mount Standard Encrypted Volume

- 

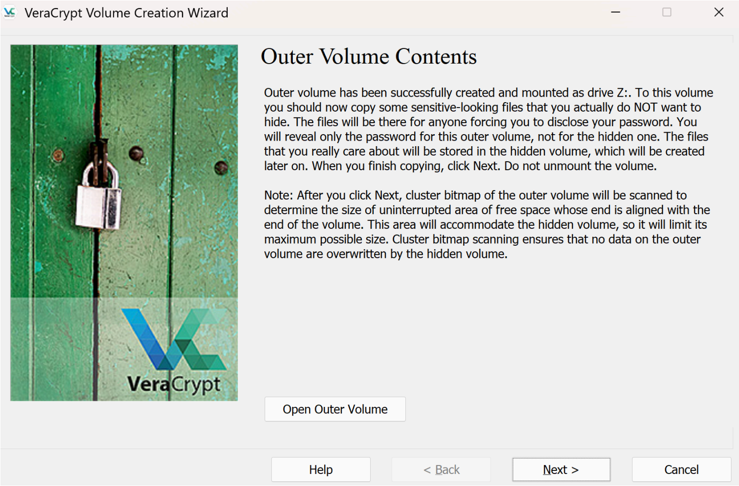
Drive	Volume	Size	Encryption Algorithm	Type
N:				
O:				
P:				
Q:				
R:				
S:	C:\Users\npson\MyVolume.hc	249 MiB	AES	Normal
T:				
U:				
V:				
W:				
X:				
Y:				
Z:				

Volume: C:\Users\npson\MyVolume.hc

☑ Never save history

- Following the beginner's tutorial on the VeraCrypt site, creating and mounting standard encrypted volumes is very straightforward.
- Sometimes an OS permissions error may show up. This just means the volume can not be located in a certain directory.

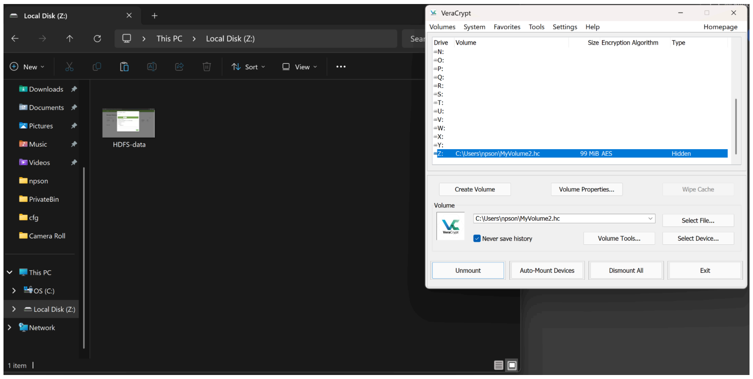
- **Scenario 2**
  Create and Mount Hidden Encrypted Volume

- 
VeraCrypt Volume Creation Wizard

Outer Volume Contents

Outer volume has been successfully created and mounted as drive Z:. To this volume you should now copy some sensitive-looking files that you actually do NOT want to hide. The files will be there for anyone forcing you to disclose your password. You will reveal only the password for this outer volume, not for the hidden one. The files that you really care about will be stored in the hidden volume, which will be created later on. When you finish copying, click Next. Do not unmount the volume.

Note: After you click Next, cluster bitmap of the outer volume will be scanned to determine the size of uninterrupted area of free space whose end is aligned with the end of the volume. This area will accommodate the hidden volume, so it will limit its maximum possible size. Cluster bitmap scanning ensures that no data on the outer volume are overwritten by the hidden volume.

- 

Drive	Volume	Size	Encryption Algorithm	Type
N:				
O:				
P:				
Q:				
R:				
S:				
T:				
U:				
V:				
W:				
X:				
Y:				
Z:	C:\Users\npson\MyVolume2.hc	99 MiB	AES	Hidden

Volume: C:\Users\npson\MyVolume2.hc

☑ Never save history

	● This scenario is also straightforward and steps are very similar to a standard encrypted volume. However it is important to read this documentation on how to protect the hidden volume when making changes to the outer volume. ● This is a very good feature for plausible deniability as individuals can “give up” a decoy volume when necessary, while keeping real information safe. Also there is no way to know of the existence of a hidden volume.

5. Insights & Recommendations

Key Findings	**Strengths:** ● VeraCrypt uses strong encryption standards such as AES256, Serpent, and Twofish. They even provide protection against advanced forensic-level attacks. ● Tool is open source and has gone through independent security audits to make it more secure and improve other features while addressing vulnerabilities. ● VeraCrypt operates fully locally and doesn't require an internet connection, it may be used with air-gapped computers and removes the possibility of data breaches through online services. ● Supports hidden volumes and hidden operating systems, allowing users to deny existence of encrypted data under duress or interrogation. **Weaknesses:** ● VeraCrypt is currently not available for iOS or Android, limiting accessibility for users who rely heavily on mobile devices. Workarounds involve using third-party tools, which may introduce security risks. ● VeraCrypt does not encrypt individual files; it encrypts whole disks or partitions. Even for small files, users must maintain containers and files must be transferred inside the volume to be secure. Individual files cannot be encrypted in real time until the entire container is mounted. ● Must mount volume manually for every time it needs to be used (might be less seamless).
Suggested Improvements	● Develop a mobile-compatible version (already stated they do not plan to) ● Add file-level encryption
Alternative Tools:	Cryptomator, GnuPG (GPG), Age

License	Apache License 2.0
Cost/Resource Implications	**Total Cost of Ownership:** ● The tool is completely free to use. ● Users may donate (if they wish to/not necessary) to help improve and maintain VeraCrypt ● There are no hidden costs for maintenance, third-party integrations, or updates.
Why is this useful to civil societies in authoritarian environments?	VeraCrypt is extremely useful to civil society organizations and human rights defenders in authoritarian environments. This is because of the advanced encryption and hash algorithms that secure sensitive data of journalists, activists, whistleblowers etc. Furthermore, one of the best features is plausible deniability. Even under forced decryption or inspection, you can plausibly deny the existence of the hidden OS or volume as it's not visible on the disk. For example, if a journalist is working on a very dangerous political topic and has sensitive data, they can create a hidden volume and store it there. The journalist also adds realistic files to the outer volume. If this journalist is then stopped by Chinese officials and forced to give up their password (say, at a border checkpoint or under interrogation), they can give Password A (password for outer volume). The officials can open it, see “innocent” data, and have no way to know there’s more. Because VeraCrypt's hidden volumes are encrypted inside the primary volume's free space and show up as random data, they are undetectable without the right password, offering plausible deniability even in the event that the primary disk is examined. This guarantees that without the password for the hidden volume, its presence cannot be proved. Note: It is important, however, to ensure there is nobody watching the computer all the time or something like a keylogger being installed. Under these circumstances of surveillance, those people can track file changes or see your password being typed, which can cause them to believe you are hiding something or uncover the hidden volume. Other than that, the hidden volume can not be accessed.