Veracrypt Encryption

Notes created on July 10, 2025 at 10:05 AM by Minutes AI

Introduction to Veracrypt

• Veracrypt is a tool for encrypting information that can be shared across different operating systems and is open source.

• It is described as a "shield" for sensitive data.

• Veracrypt is an open-source encryption tool, meaning its source code is available for examination and auditing.

Key Features of Veracrypt

• Veracrypt utilizes robust encryption algorithms like AES, Serpent, or Chuffys.

• It is a multiplatform tool available for Windows, Mac, and most Linux distributions.

• It allows the creation of hidden volumes within encrypted volumes, adding an extra layer of security.

• Veracrypt can be used on USB drives and other removable devices.

Veracrypt Installation (Windows 11)

• The presenter is using Windows 11 and has the Veracrypt website open.

• The website displays the main features, access to the source code, documentation, forums, and the download section.

• Different installation options are available depending on the OS: exe, msi, and portable versions for Windows; version 12 or higher and an osx fuse dependency for Mac; and Debian, Ubuntu, rpm packages for Linux.

• The presenter downloads the exe installer for Windows.

• The installation process includes accepting the conditions, choosing to install or extract for portable use, installing for all users, adding a Start menu item and desktop icon, and associating the .hc extension with Veracrypt.

• The installer is left with all the default options.

• After installation, a message appears about donations, and the tutorial is skipped.

Fast Startup and VeraCrypt Interface

• Fast startup can be disabled, and a computer restart is recommended but not immediately necessary.

• VeraCrypt's interface displays volume options from a to z, indicating its focus on creating virtual volumes.

• Options include creating a volume, selecting an existing one to mount, viewing properties, clearing cache, auto-mounting, dismounting all, and exiting the application.

Creating a New Volume

• The process will start in Windows and then transition to a Linux OS.

• Users can create a file to contain encrypted content as a virtual volume, encrypt a drive like a USB, or encrypt a system partition.

• The presenter will create a file to contain all encrypted information.

Volume Types and Encryption Settings

• VeraCrypt offers standard and hidden volume types; hidden volumes use two passwords to access different sets of documents, useful for plausible deniability.

• The presenter will use the standard volume type for this demonstration.

• The file will be saved on the desktop as "test.VC".

• Default encryption and hashing algorithms are sufficient, but many options are available.

Volume Size, Password, and Formatting

• The virtual volume size will be set to 5 MB for testing purposes.

• A password will be used, but a file can also serve as a password.

• A warning is given that the password is short and a password of 20 or more characters is recommended.

• The process involves generating entropy for key creation, indicated by a green bar, before formatting.

• The VeraCrypt volume has been created successfully.

VeraCrypt File Properties

• The created container occupies the size specified (50 MB in this case).

• All data added will be integrated within this file.

Mounting the Volume

• Select the file (testvc) in VeraCrypt.

• Choose a drive letter (A in this example).

• Enter the password to mount the volume.

• A WordPad document is created, saved to the desktop as "document", then dragged to the mounted drive.

Dismounting and Remounting

• Dismount the drive.

• Double-clicking the file mounts it directly to the selected drive (A).

• Enter the password again to remount and access the "document" file.

Transfer to Linux

• Dismount all units and exit VeraCrypt.

• Transfer the "testvc" file to a Linux system with VeraCrypt installed.

VeraCrypt on Linux (Ubuntu)

• The "testvc" file is prepared for mounting in VeraCrypt on Ubuntu.

• VeraCrypt installers for Linux distributions (Debian, Ubuntu, Fedora, CentOS) are available on the official website.

    - GUI and console versions are available.
    - A generic installer detects the system.
- Installation via APT is also an option.

- To install Veracrypt on Ubuntu, the speaker first opens the terminal and runs `sudo apt update` to update the repositories.
- If the Veracrypt repository is not installed, running `sudo apt install veracrypt` will not find the package.
- The speaker adds the repository, runs `sudo apt update` again, and then installs Veracrypt.
- Veracrypt's graphical interface is the same across Windows and Mac.
- A new volume is created, a file named "testvc" is selected from the desktop, and it's mounted on slot number one.
- The password for the virtual hard drive is required, as well as the administrator password for privileges.
- The volume is mounted in `/media/veracrypt`.
- A document opened from the mounted volume may not display correctly due to formatting issues (RTF).
- The key is to protect the Veracrypt file, which can be moved between operating systems.

Conclusions on Veracrypt

- Veracrypt offers solid security for encrypting sensitive data across different platforms (Windows, Mac, Linux).
- "Veracrypt cuenta con algoritmos de cifrado robustos y con una amplia gama de funcionalidades y por tanto podemos destacar Veracrypt como una herramienta esencial en la protección de la información confidencial."
- Veracrypt is recommended for personal and business use due to its versatility and reliability.
- Veracrypt adapts to different security needs, offering a range of features and configuration options for users to customize their security approach.