WAN MUHAMMAD ISMAT WAN AZMY
B031920032 BITS DE

LAB REPORT

SECRET WRITING TOOLS

I. Introduction of Secret Writing

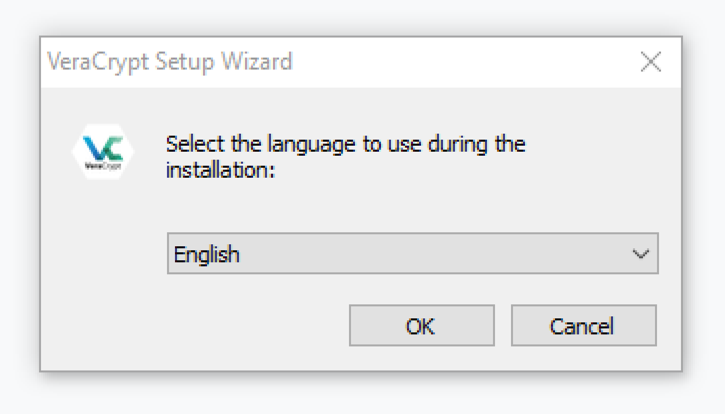
Secret Writing technique can be divided by to categories which are Cryptography and Steganography. Firstly, the explanation will be about cryptography. Basically, cryptography is by translating it into a type that unintended recipients do not understand, cryptography is the science of keeping information secure. In cryptography, by means of an algorithm, or sequence of mathematical operations, an initial human readable code, referred to as plaintext, is transformed into something that may look like gibberish to an uninformed observer; this gibberish is called ciphertext.

Today, there are five key cryptography features. They are Privacy /confidentiality: Ensuring that no one but the intended recipient can read the message; Authentication: The process of proving one 's identity; Integrity: Ensuring the recipient that the message received has not been changed in any way from the original; Non-repudiation: A procedure to prove that this message has actually been sent by the sender; and Key exchange: The system by which crypto keys are transmitted. Now we proceed to steganography explanation.

Steganography is the art of concealing a hidden message that is not secret inside (or even on top of) something. That anything can only be about whatever you want. Many examples of steganography these days include embedding a hidden piece of text within an image. Or inside a Word or Excel document to conceal a hidden message or script. Steganography is intended to conceal and deceive. It is a form of covert interaction and can involve the use of any medium to conceal messages. Because it does not involve scrambling data or using a key, it is not a form of cryptography. Instead, it is a type of hiding of information and can be executed in clever ways. Where cryptography is a science that allows privacy to a significant extent, steganography is a practice that allows secrecy and deceit.

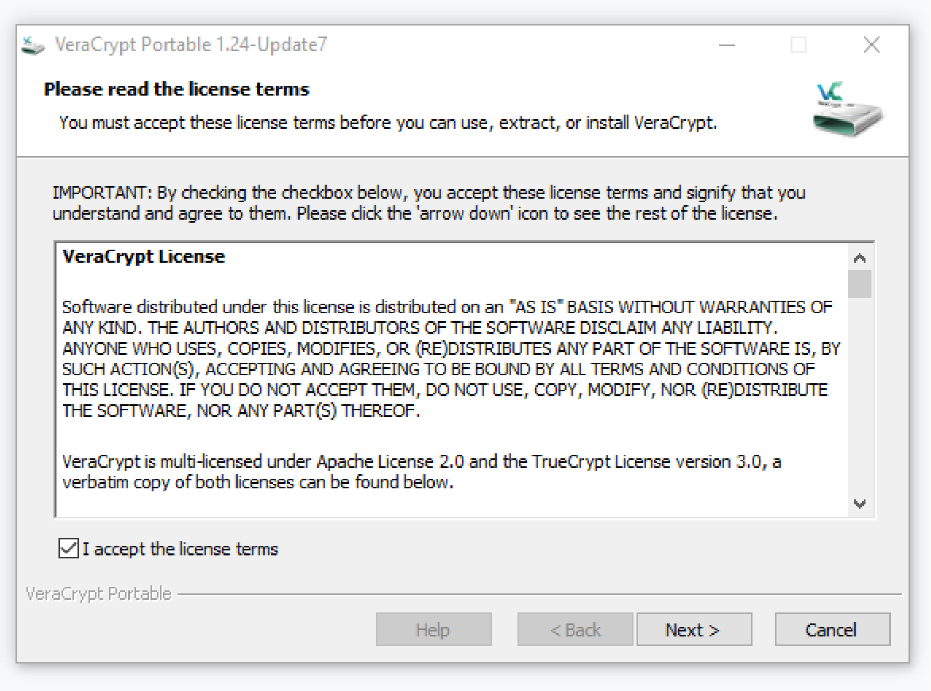
II. Cryptography

a. Installation manual for the tool



Select the language to use during the installation:

- Run the installation file, firstly it will ask to select the language to use during the installation. Click "OK" button to proceed after selecting the language.



Please read the license terms

You must accept these license terms before you can use, extract, or install VeraCrypt.

IMPORTANT: By checking the checkbox below, you accept these license terms and signify that you understand and agree to them. Please click the 'arrow down' icon to see the rest of the license.

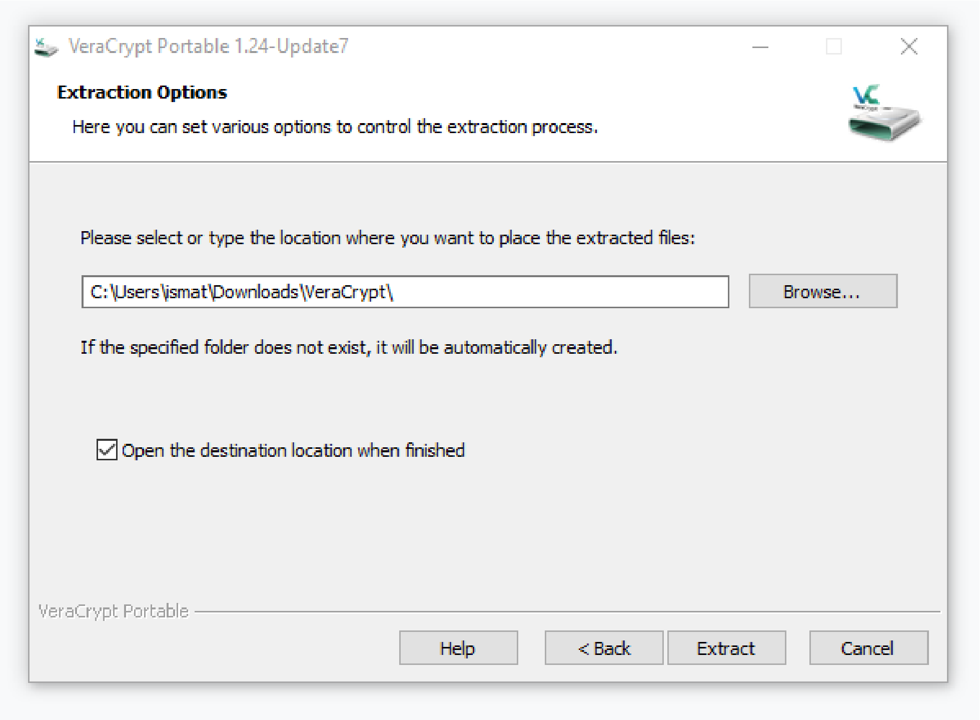
VeraCrypt License

Software distributed under this license is distributed on an "AS IS" BASIS WITHOUT WARRANTIES OF ANY KIND. THE AUTHORS AND DISTRIBUTORS OF THE SOFTWARE DISCLAIM ANY LIABILITY. ANYONE WHO USES, COPIES, MODIFIES, OR (RE)DISTRIBUTES ANY PART OF THE SOFTWARE IS, BY SUCH ACTION(S), ACCEPTING AND AGREEING TO BE BOUND BY ALL TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT ACCEPT THEM, DO NOT USE, COPY, MODIFY, NOR (RE)DISTRIBUTE THE SOFTWARE, NOR ANY PART(S) THEREOF.

VeraCrypt is multi-licensed under Apache License 2.0 and the TrueCrypt License version 3.0, a verbatim copy of both licenses can be found below.

☑ I accept the license terms

- Tick the "I accept the license terms" and click "Next" button.



Extraction Options

Here you can set various options to control the extraction process.

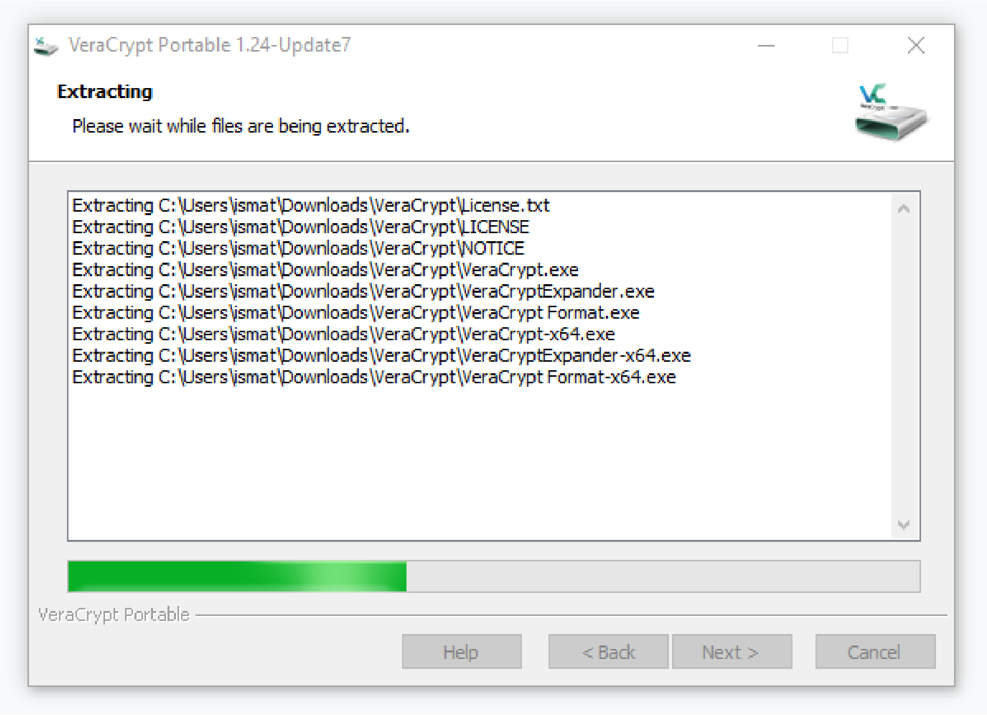
Please select or type the location where you want to place the extracted files:

C:\Users\ismat\Downloads\VeraCrypt\

If the specified folder does not exist, it will be automatically created.

☑ Open the destination location when finished

- Choose your installation folder, tick any necessary option then click Extract.

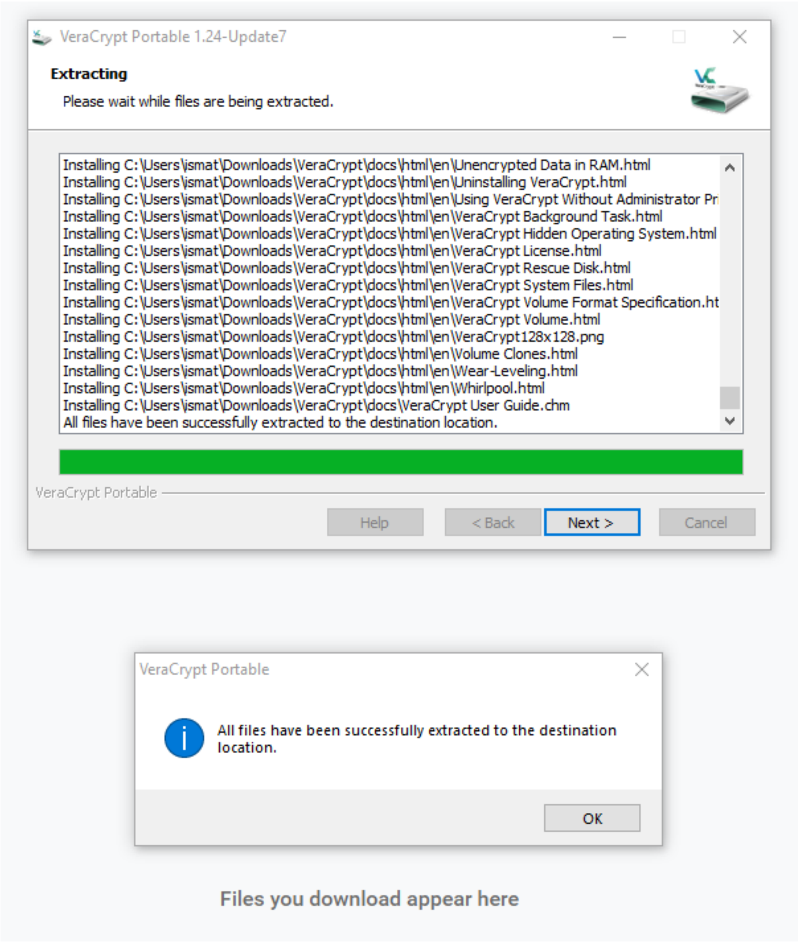


Extracting

Please wait while files are being extracted.

```
Extracting C:\Users\ismat\Downloads\VeraCrypt\License.txt
Extracting C:\Users\ismat\Downloads\VeraCrypt\LICENSE
Extracting C:\Users\ismat\Downloads\VeraCrypt\NOTICE
Extracting C:\Users\ismat\Downloads\VeraCrypt\VeraCrypt.exe
Extracting C:\Users\ismat\Downloads\VeraCrypt\VeraCryptExpander.exe
Extracting C:\Users\ismat\Downloads\VeraCrypt\VeraCrypt Format.exe
Extracting C:\Users\ismat\Downloads\VeraCrypt\VeraCrypt-x64.exe
Extracting C:\Users\ismat\Downloads\VeraCrypt\VeraCryptExpander-x64.exe
Extracting C:\Users\ismat\Downloads\VeraCrypt\VeraCrypt Format-x64.exe
```

- This is the installation progress screen; it will do the software installation.



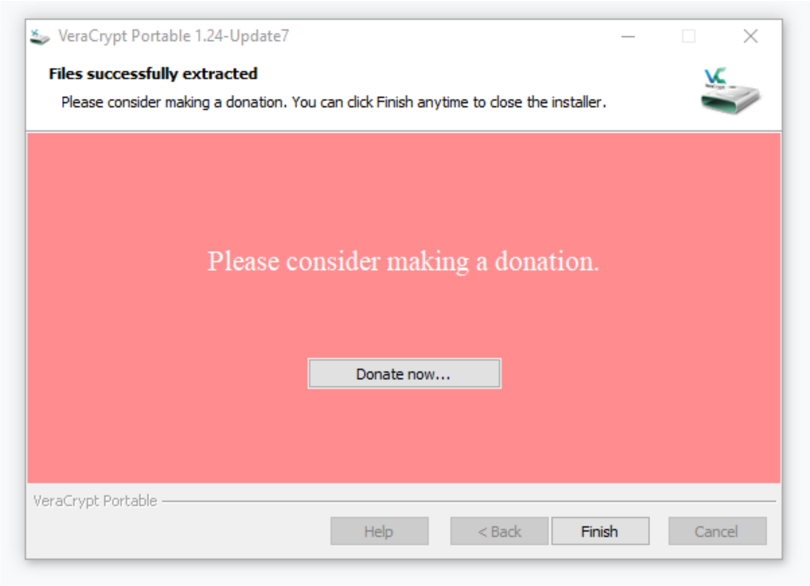
Extracting

Please wait while files are being extracted.

```
Installing C:\Users\ismat\Downloads\VeraCrypt\docs\html\en\Unencrypted Data in RAM.html
Installing C:\Users\ismat\Downloads\VeraCrypt\docs\html\en\Uninstalling VeraCrypt.html
Installing C:\Users\ismat\Downloads\VeraCrypt\docs\html\en\Using VeraCrypt Without Administrator Pr
Installing C:\Users\ismat\Downloads\VeraCrypt\docs\html\en\VeraCrypt Background Task.html
Installing C:\Users\ismat\Downloads\VeraCrypt\docs\html\en\VeraCrypt Hidden Operating System.html
Installing C:\Users\ismat\Downloads\VeraCrypt\docs\html\en\VeraCrypt License.html
Installing C:\Users\ismat\Downloads\VeraCrypt\docs\html\en\VeraCrypt Rescue Disk.html
Installing C:\Users\ismat\Downloads\VeraCrypt\docs\html\en\VeraCrypt System Files.html
Installing C:\Users\ismat\Downloads\VeraCrypt\docs\html\en\VeraCrypt Volume Format Specification.ht
Installing C:\Users\ismat\Downloads\VeraCrypt\docs\html\en\VeraCrypt Volume.html
Installing C:\Users\ismat\Downloads\VeraCrypt\docs\html\en\VeraCrypt128x128.png
Installing C:\Users\ismat\Downloads\VeraCrypt\docs\html\en\Volume Clones.html
Installing C:\Users\ismat\Downloads\VeraCrypt\docs\html\en\Wear-Leveling.html
Installing C:\Users\ismat\Downloads\VeraCrypt\docs\html\en\Whirlpool.html
Installing C:\Users\ismat\Downloads\VeraCrypt\docs\VeraCrypt User Guide.chm
All files have been successfully extracted to the destination location.
```

All files have been successfully extracted to the destination location.

OK
Files you download appear here



VeraCrypt Portable 1.24-Update7

Files successfully extracted

Please consider making a donation. You can click Finish anytime to close the installer.

Please consider making a donation.

Donate now...
VeraCrypt Portable
Help
< Back
Finish
Cancel

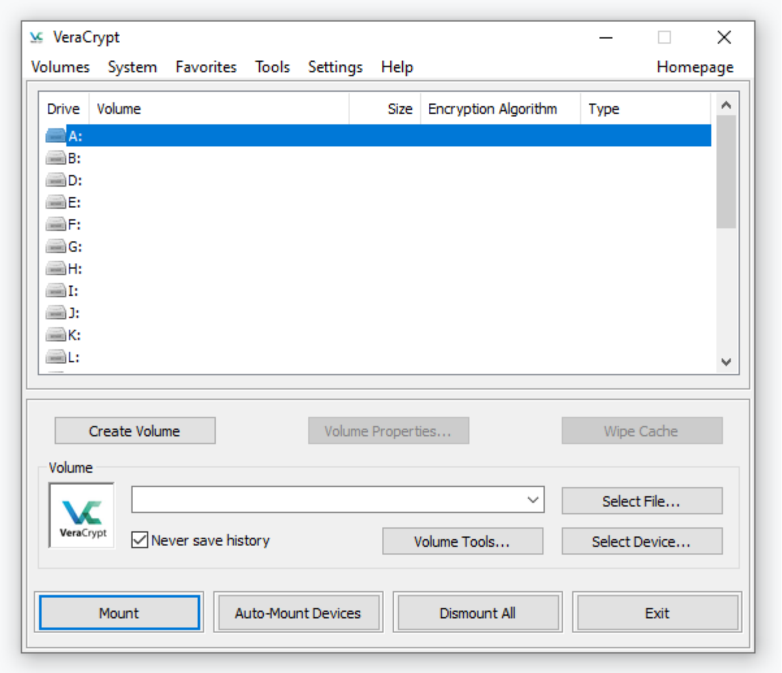
- After installation done, click "OK" button on prompt window and click "Finish" button.

b. Exploration of the tool features

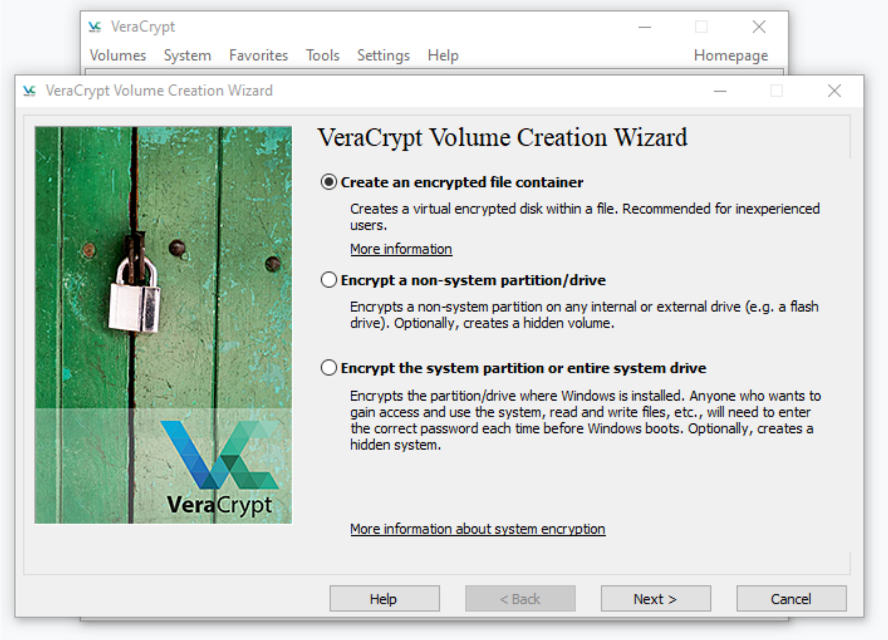
-

c. Some testing on the tool's capabilities

- Open the VeraCrypt by double click on the software. Click on "Create Volume" button to proceed to configure the system.



- Choose "Create an encrypted file container" to create a virtual encrypted disk within file. Then click "Next" button to proceed.


VeraCrypt
Volumes System Favorites Tools Settings Help
Homepage
VeraCrypt Volume Creation Wizard
VeraCrypt

VeraCrypt Volume Creation Wizard

● **Create an encrypted file container**

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

○ **Encrypt a non-system partition/drive**

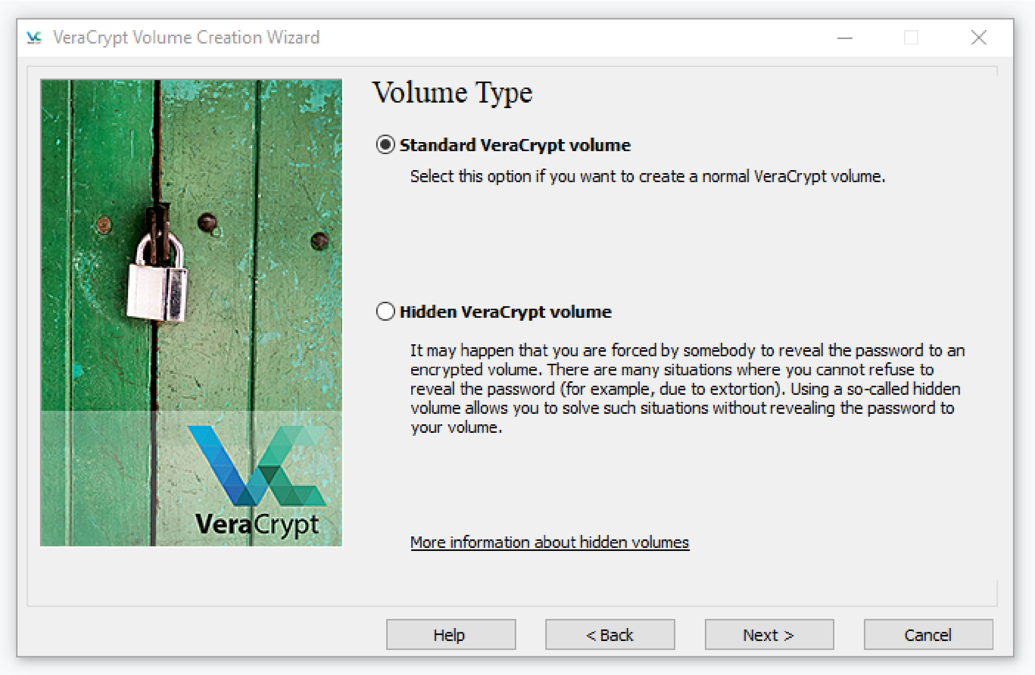
Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

○ **Encrypt the system partition or entire system drive**

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

More information about system encryption

- For Volume Type, choose “VeraCrypt volume” to create a normal VeraCrypt volume.



VeraCrypt Volume Creation Wizard

Volume Type

● **Standard VeraCrypt volume**

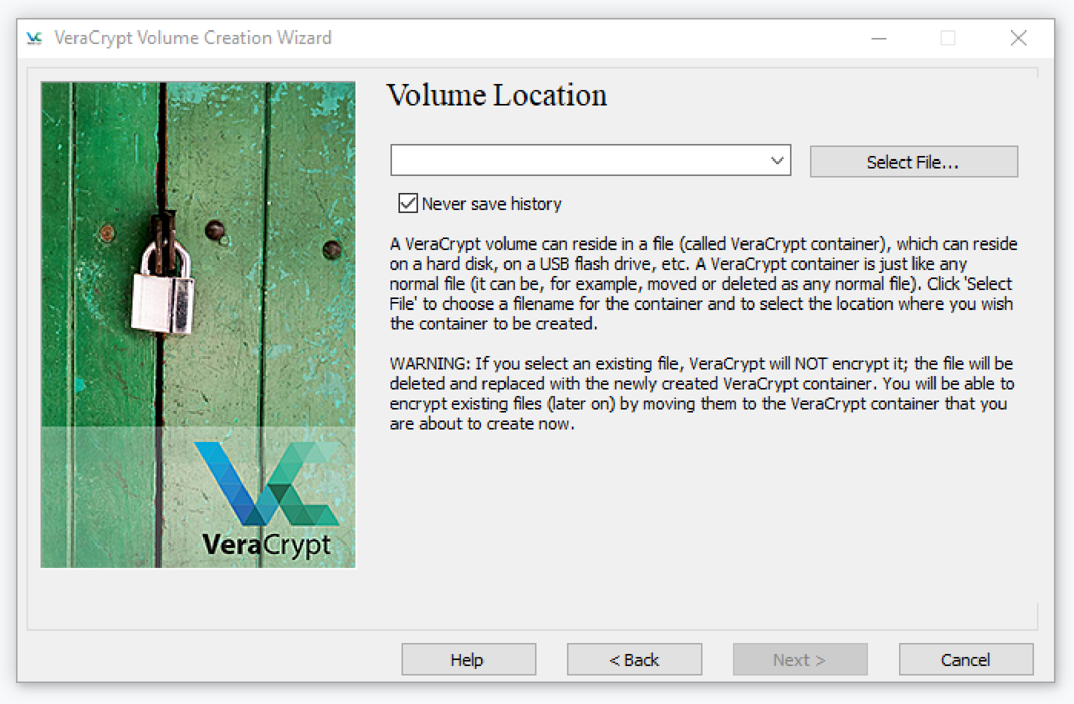
Select this option if you want to create a normal VeraCrypt volume.

○ **Hidden VeraCrypt volume**

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

More information about hidden volumes

- In this step, user need to clarify the volume location which is needed to create VeraCrypt volume (file container).



VeraCrypt Volume Creation Wizard

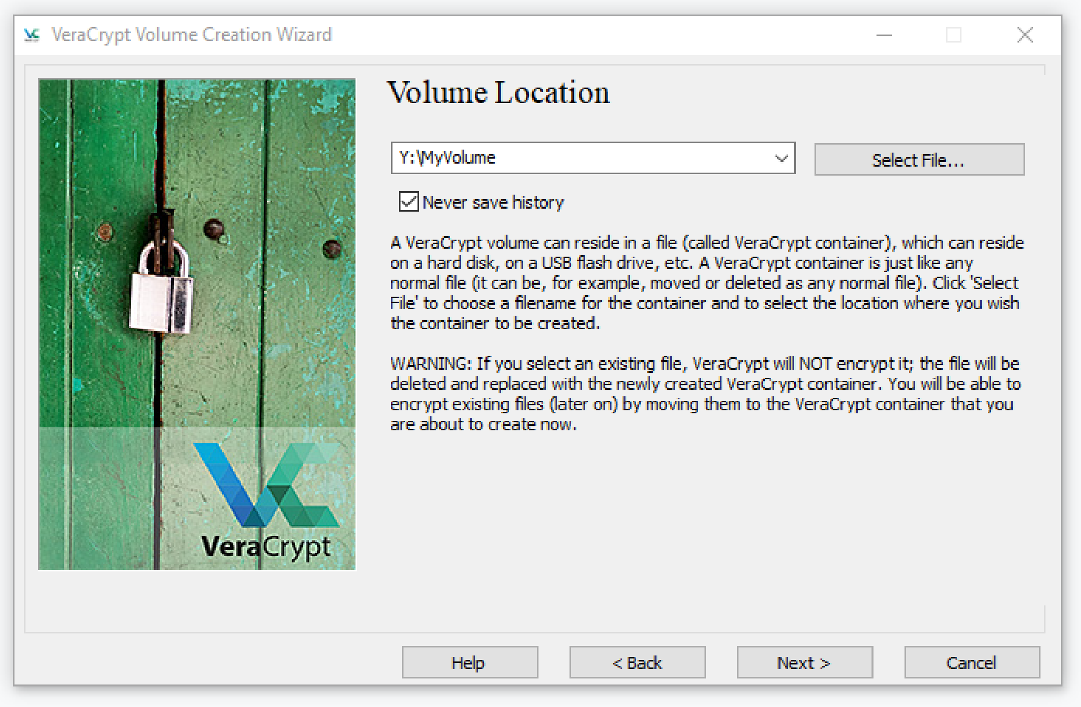
Volume Location

☑ Never save history

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 choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, VeraCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created VeraCrypt container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container that you are about to create now.

- The user can set the location for VeraCrypt volume in the folder Y:\ and set the file name as "My Volume". The user can set the location and rename the file name at will to desired location or name you like. Click "Next >" after done the above step.



Volume Location

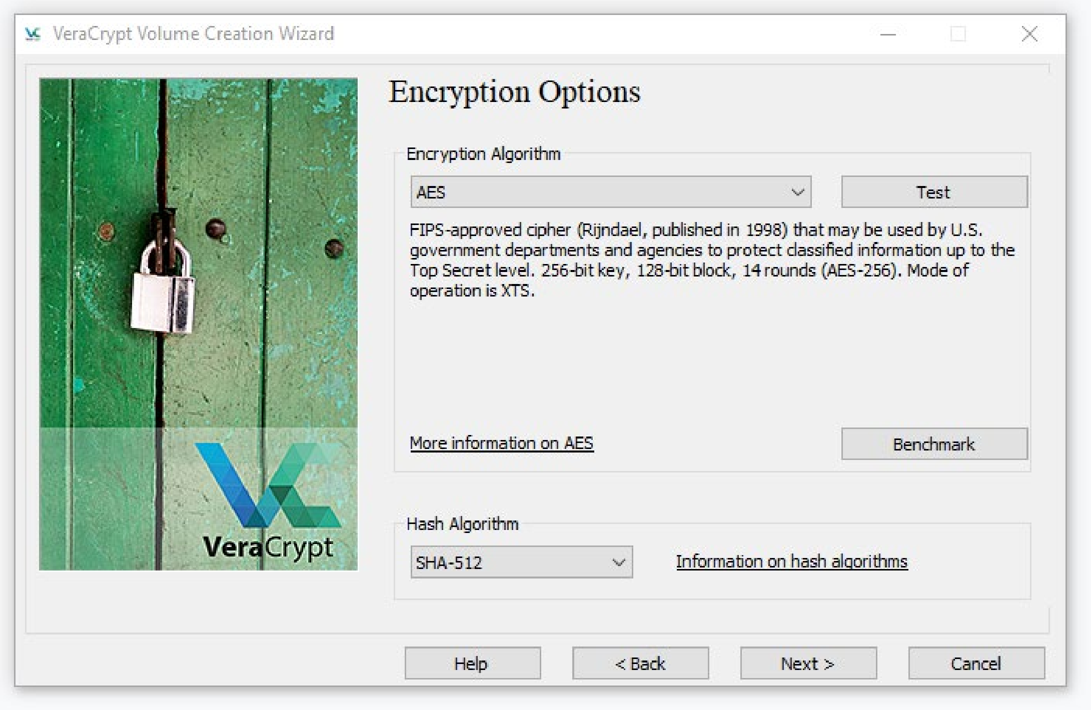
Y:\MyVolume

☑ Never save history

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 choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, VeraCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created VeraCrypt container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container that you are about to create now.

- Set Encryption Algorithm to "AES" and Hash Algorithm to "SHA-512" and click "Next" button to proceed.



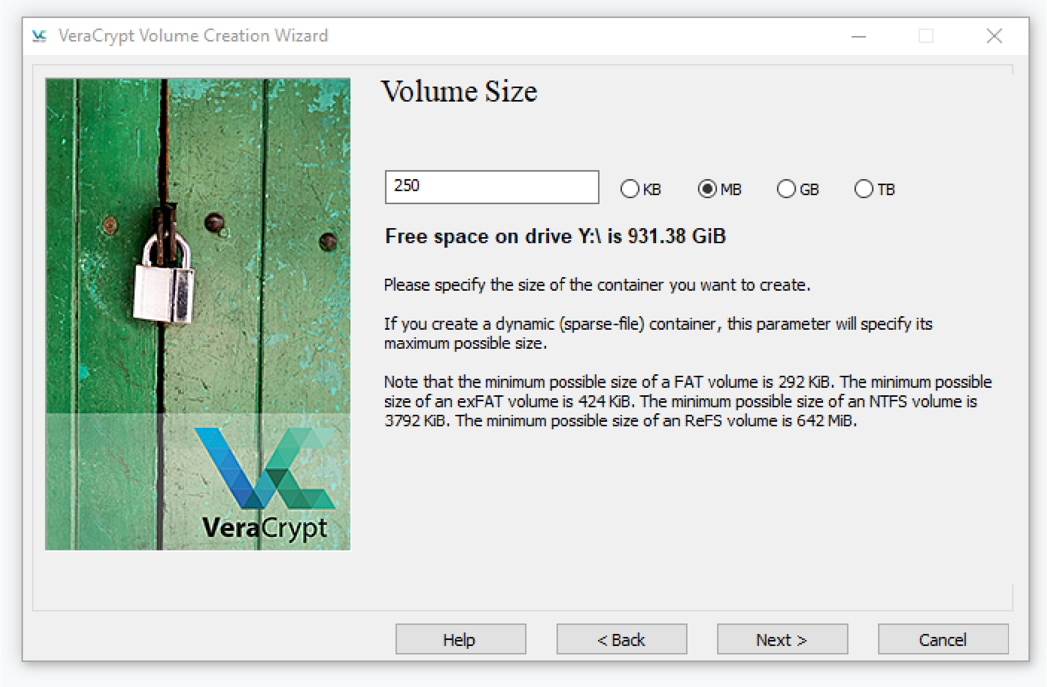
Encryption Options

Encryption Algorithm: AES

FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

Hash Algorithm: SHA-512

- Set size of VeraCrypt Container to 250MB. The size of container can be change to desired size you like.



Volume Size

250 ○ KB ● MB ○ GB ○ TB

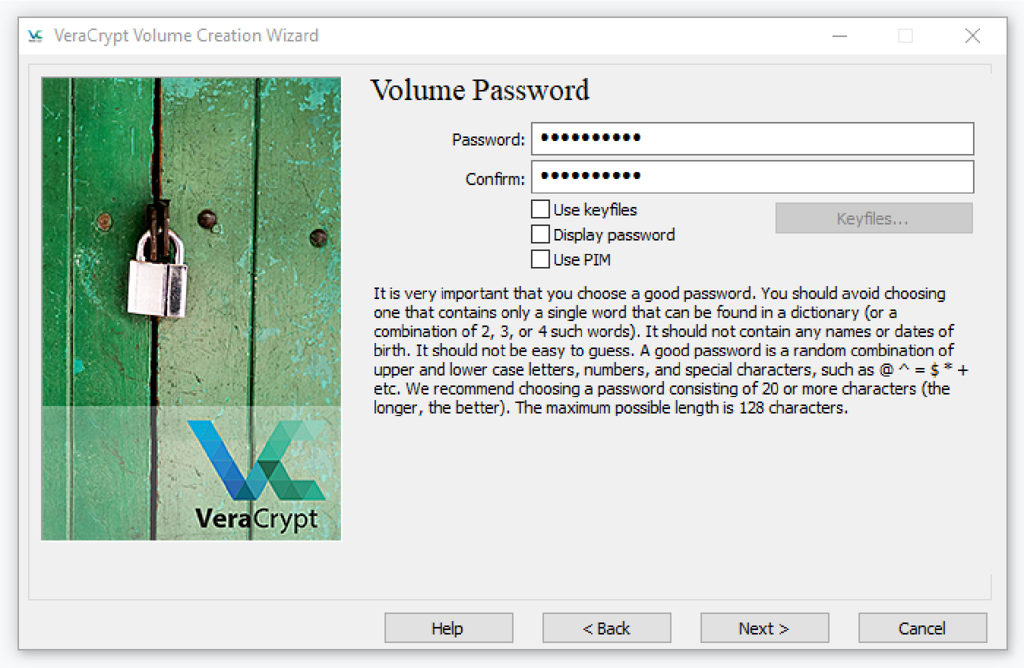
Free space on drive Y:\ is 931.38 GiB

Please specify the size of the container you want to create.

If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size.

Note that the minimum possible size of a FAT volume is 292 KiB. The minimum possible size of an exFAT volume is 424 KiB. The minimum possible size of an NTFS volume is 3792 KiB. The minimum possible size of an ReFS volume is 642 MiB.

- The user needs to set Password as an authentication when to use the VeraCrypt Container later. Users need to choose the good password to ensure the container is not easily to guess. This can prevent from the data inside the container to be access by people who does not have permission to use the container. Click “Next” button after done with fill the password on this system.



Volume Password

Password: ••••••••••

Confirm: ••••••••••

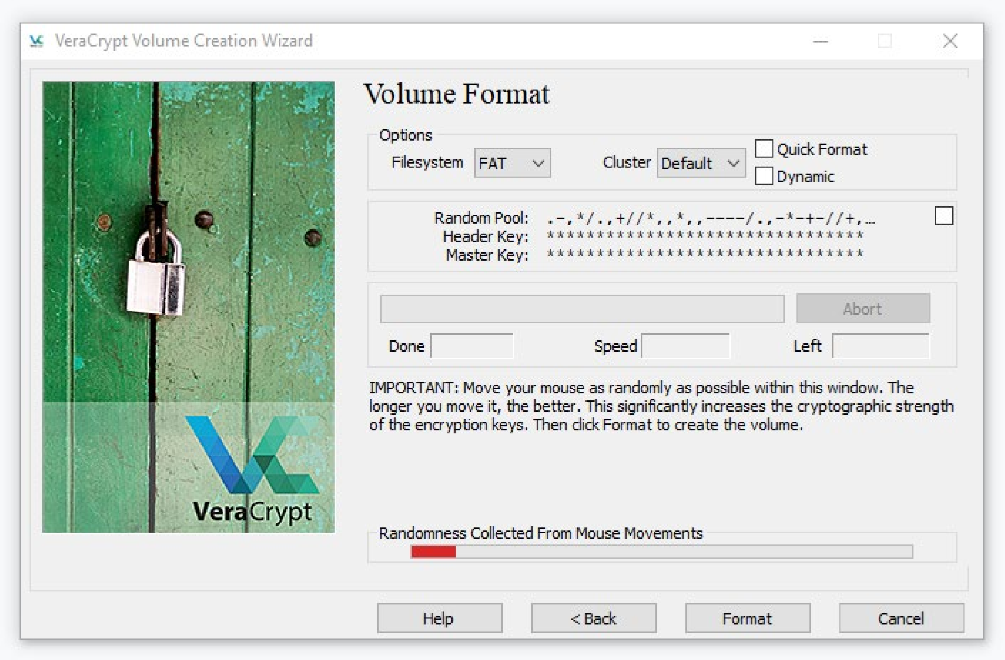
□ Use keyfiles

□ Display password

□ Use PIM

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 128 characters.

- In this step, the user needs to move the mouse to randomly within this interface to “Randomness Collected From Mouse Movements” indicator at less becomes green. This technique uses to increase the cryptographic strength of the encryption keys. Then, click “Format” to proceed the next step.



VeraCrypt Volume Creation Wizard

Volume Format

Options

Filesystem FAT

Cluster Default

□ Quick Format

□ Dynamic

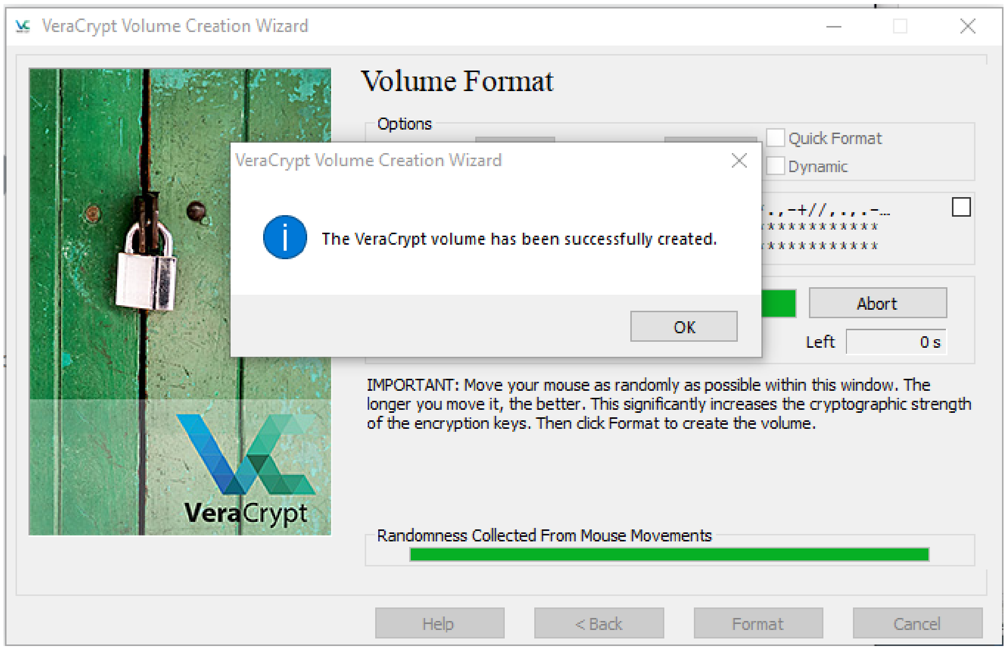
Random Pool: .-,*/.,+//*,,*,,----/.,-*-+-//+,...
Header Key: ********************************
Master Key: ********************************

Done
Speed
Left

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Randomness Collected From Mouse Movements

- This technique uses to increase the cryptographic strength of the encryption keys. Then, click “Format” to proceed the next step. After you done all the steps above, the system will show the pop up to tell the user the VeraCrypt volume is successful created. Click “OK” button to proceed.



VeraCrypt Volume Creation Wizard

Volume Format

Options

□ Quick Format

□ Dynamic

VeraCrypt Volume Creation Wizard

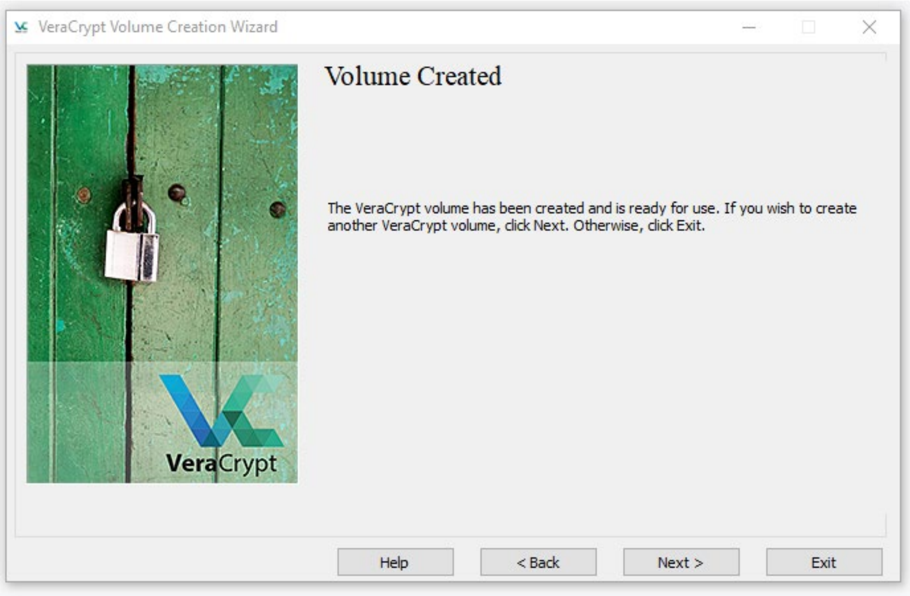
The VeraCrypt volume has been successfully created.

Left 0 s

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Randomness Collected From Mouse Movements

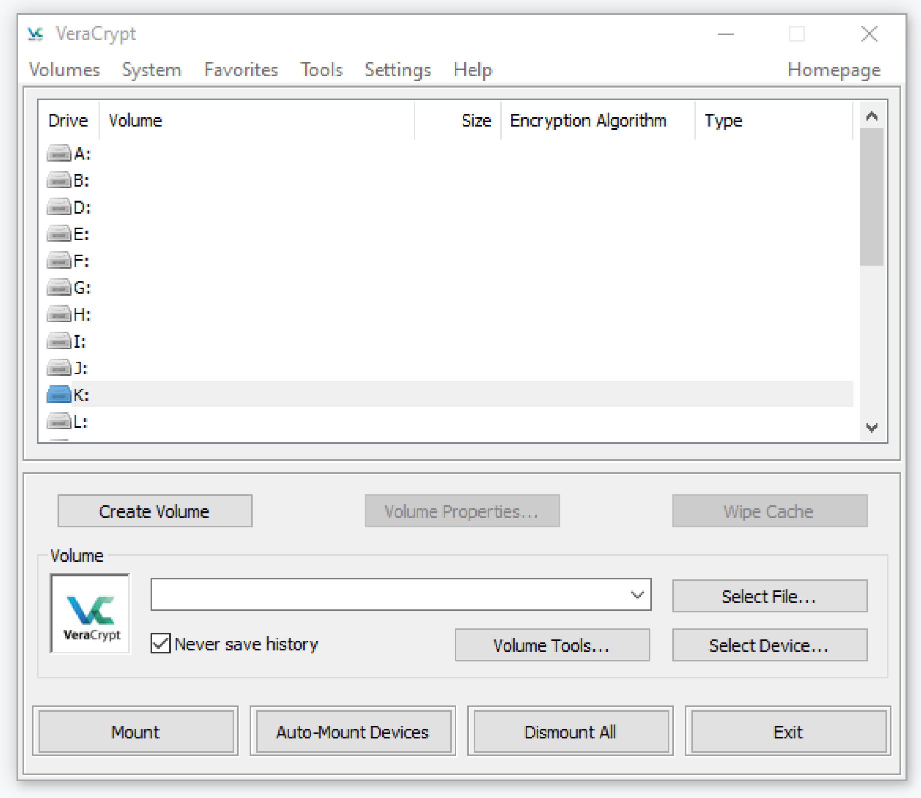
- Click “Exit” button to finish this step.



Volume Created

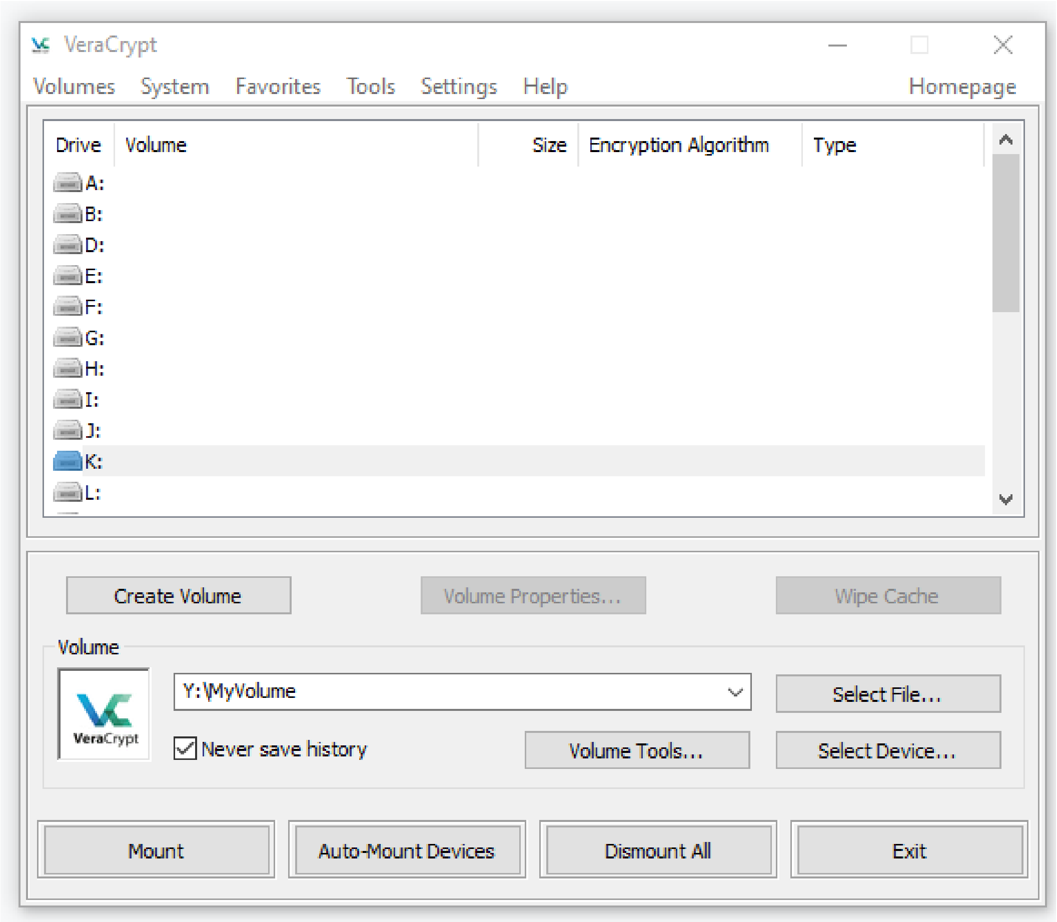
The VeraCrypt volume has been created and is ready for use. If you wish to create another VeraCrypt volume, click Next. Otherwise, click Exit.

- In this step, user need to choose one of this Drive to set to be partition of virtual drive for this system. User is freely to set the partition they want to act as new partition for this VeraCrypt container. For this tutorial, the user set the partition to K: drive. Then, click “Select File” button to choose the location of VeraCrypt that we just create before to load on this system.



☑ Never save history

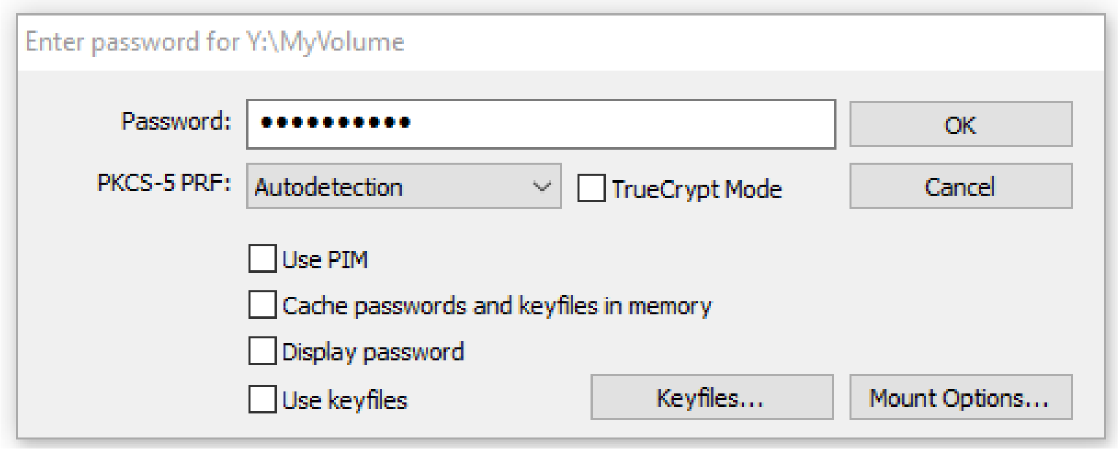
- Choose the location file that we make before. Form the user set before, “My Volume” will be used to load on this system. Click “Open” button to load that location. Then, press “mount” button to proceed.



Volume: Y:\MyVolume

☑ Never save history

- Put the password that user set before into this textbox and click “OK” button. Other options set to default.



Enter password for Y:\MyVolume

Password: ●●●●●●●●●●●

PKCS-5 PRF: Autodetection

□ TrueCrypt Mode

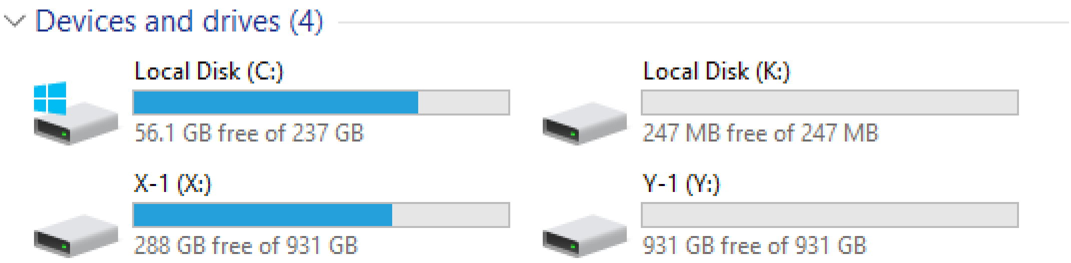
□ Use PIM

□ Cache passwords and keyfiles in memory

□ Display password

□ Use keyfiles

- The process to create VeraCrypt container is done. The user can check the virtual partition already run on the system. Open "My Computer" shortcut on the desktop to access the new partition that already done before. As the picture below, Local Disk (K:) was display as a new partition on this system.



Devices and drives (4)

Local Disk (C:)
56.1 GB free of 237 GB

Local Disk (K:)
247 MB free of 247 MB

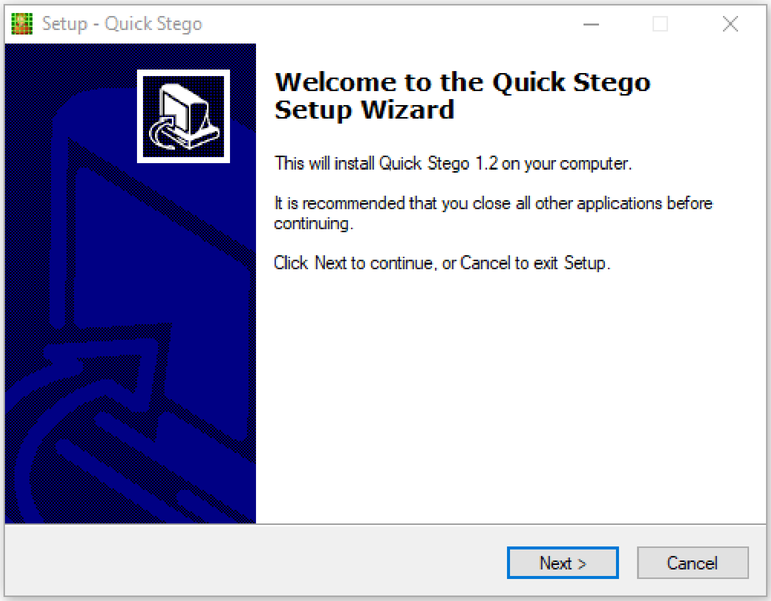
X-1 (X:)
288 GB free of 931 GB

Y-1 (Y:)
931 GB free of 931 GB

III. Steganography

a. Installation manual for the tool

- Download Quick Stegano from the internet. Extract the files, after extracted. Run the Setup. Proceed the Setup by clicking the "Next" button and then accept the agreement, choose the destination location to be install.



Welcome to the Quick Stego Setup Wizard

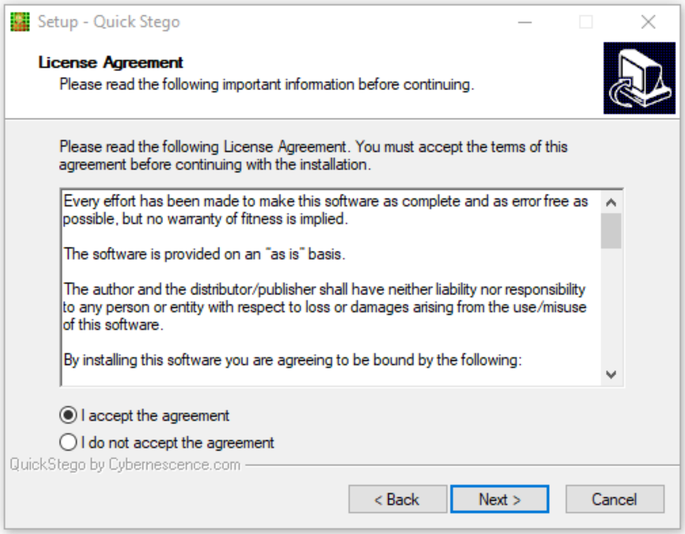
This will install Quick Stego 1.2 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

- Then select all as image bellow and "Finish" the setup. Then the application is ready to use.

WAN MUHAMMAD ISMAT WAN AZMY
B031920032 BITS DE



Setup - Quick Stego

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Every effort has been made to make this software as complete and as error free as possible, but no warranty of fitness is implied.

The software is provided on an "as is" basis.

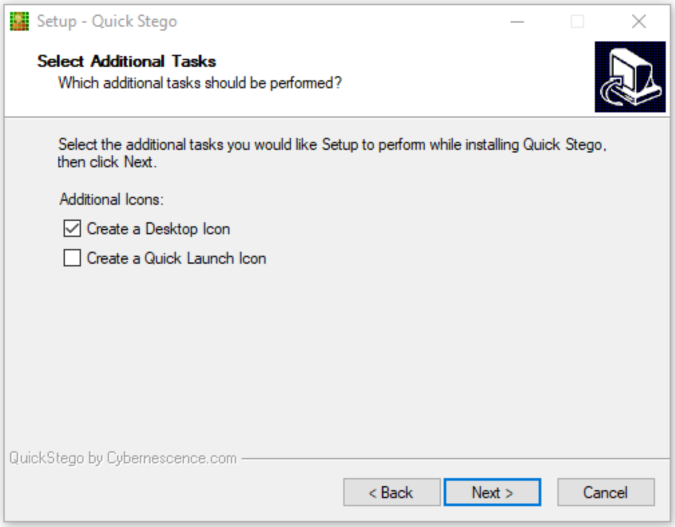
The author and the distributor/publisher shall have neither liability nor responsibility to any person or entity with respect to loss or damages arising from the use/misuse of this software.

By installing this software you are agreeing to be bound by the following:

● I accept the agreement

○ I do not accept the agreement

QuickStego by Cybernescence.com



Setup - Quick Stego

Select Additional Tasks

Which additional tasks should be performed?

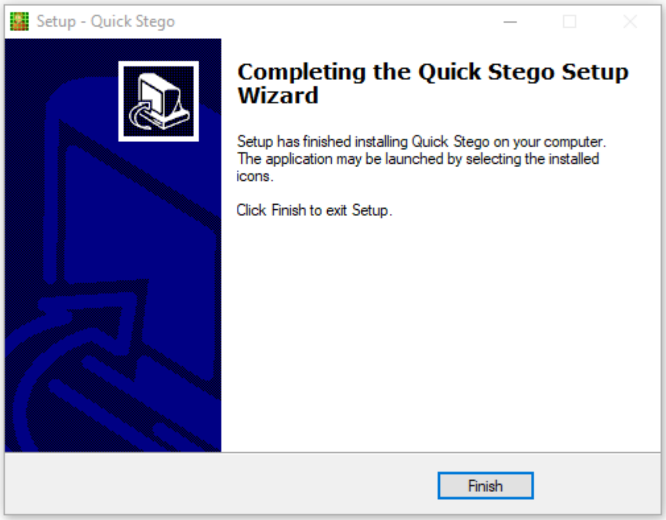
Select the additional tasks you would like Setup to perform while installing Quick Stego, then click Next.

Additional Icons:

☑ Create a Desktop Icon

□ Create a Quick Launch Icon

QuickStego by Cybernescence.com



Setup - Quick Stego

Completing the Quick Stego Setup Wizard

Setup has finished installing Quick Stego on your computer. The application may be launched by selecting the installed icons.

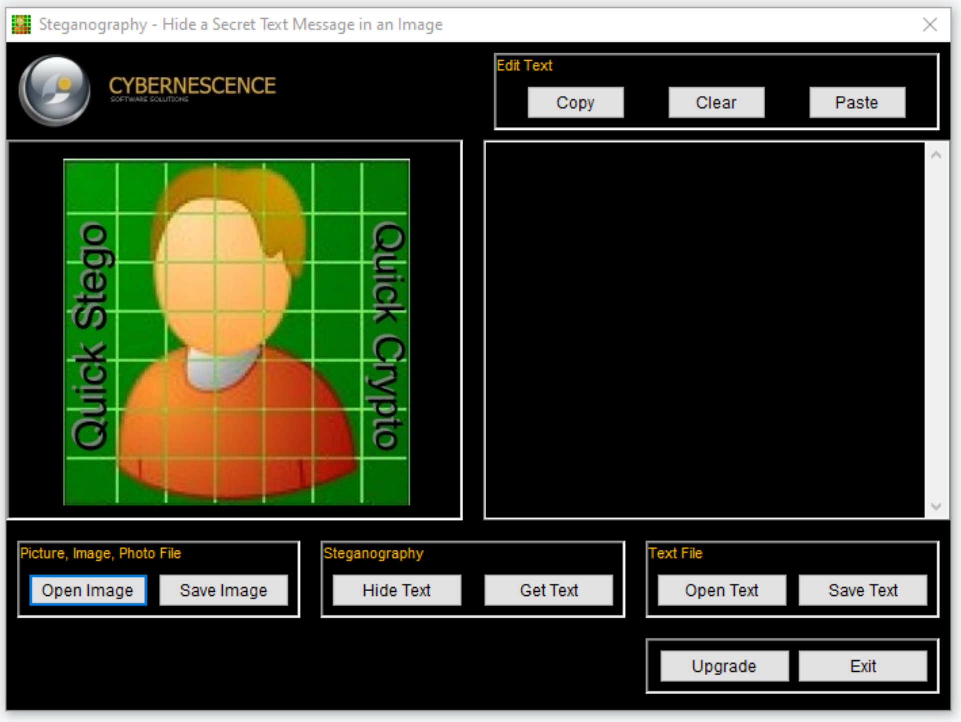
Click Finish to exit Setup.

b. Exploration of the tool features

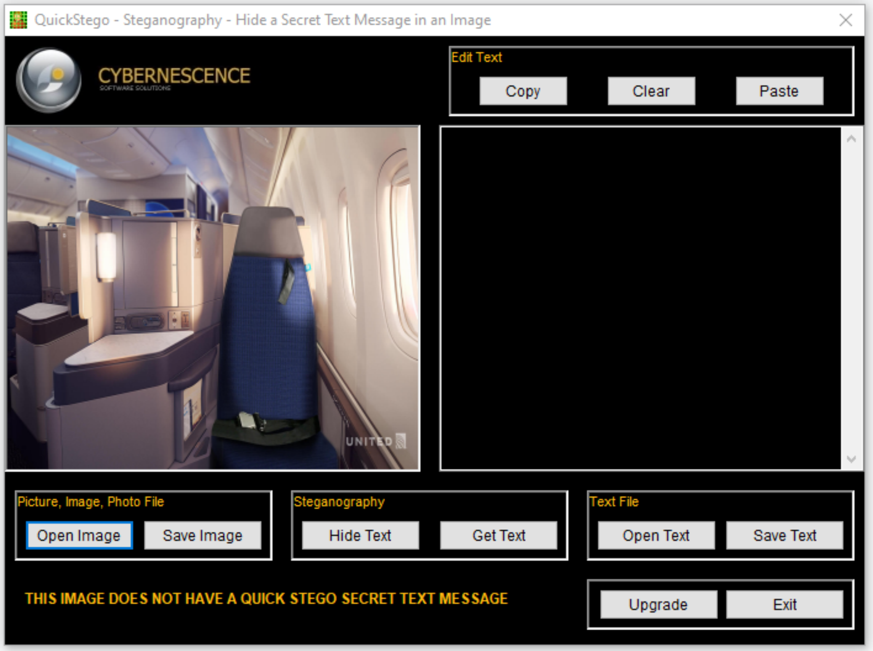
This tool gets the features to load the text image from text file format, this is other alternative to put the message directly to the text box. The system able to hide (encrypt) the message into image. So, to decrypt the message, the user needs to this system to decrypt the image.

c. Some testing on the tool's capabilities

- Open the application by double click on "Quick Stego" shortcut on the desktop. The software will show the interface as below. Then, click the "Open Image" button to load the image.

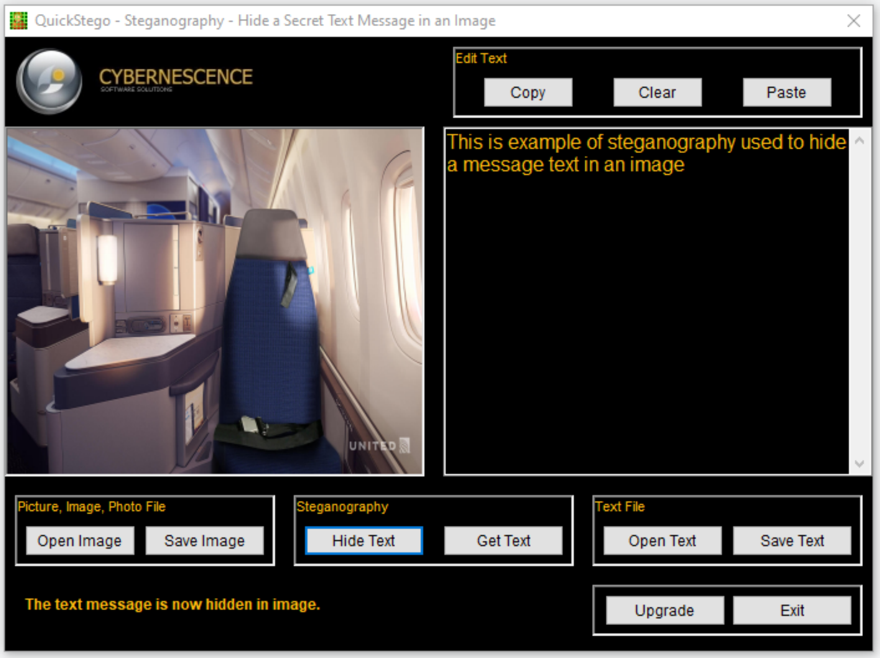


- The user needs to choose one picture to load in the system. Only image file format is accepted to use in this system to load. After the load, the picture is done, the interface will display the picture that the user chooses to load. The "THIS IMAGE DOES NOT HAVE A QUICK STEGO SECRET TEXT MESSAGE" message will show to inform the user that that picture does not have insert any hidden message.



THIS IMAGE DOES NOT HAVE A QUICK STEGO SECRET TEXT MESSAGE

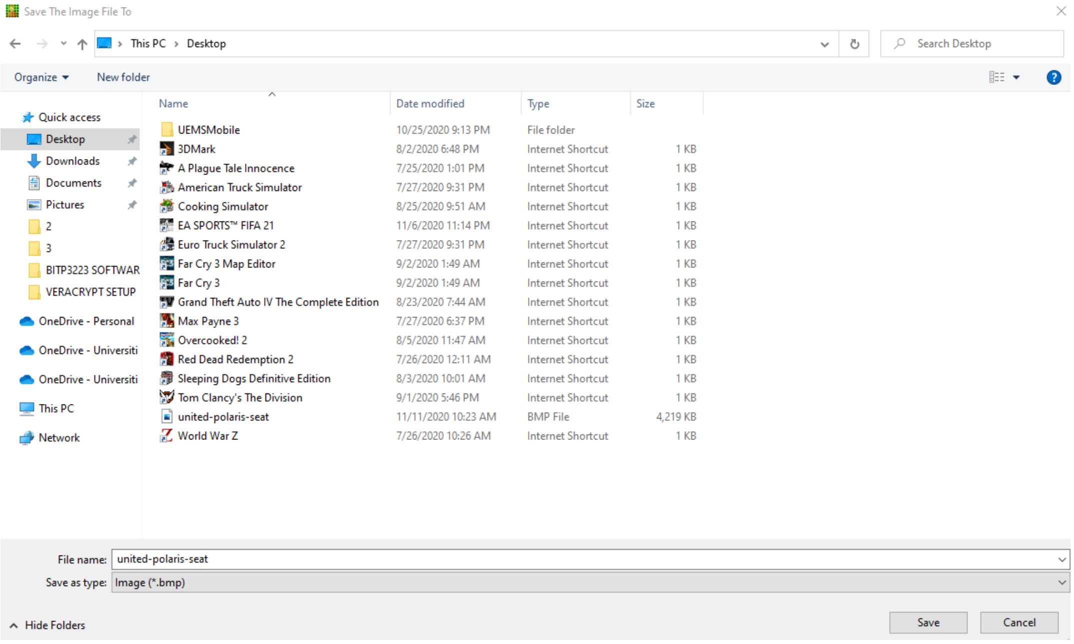
- Then, the user needs to put the text on the provided text box to insert a new message or copy from text file to load on this text box. The user needs to click on "Hide Text" button to insert the text into the image.



This is example of steganography used to hide a message text in an image

The text message is now hidden in image.

- After that, the user can save the image to send to another people to send this hidden message.

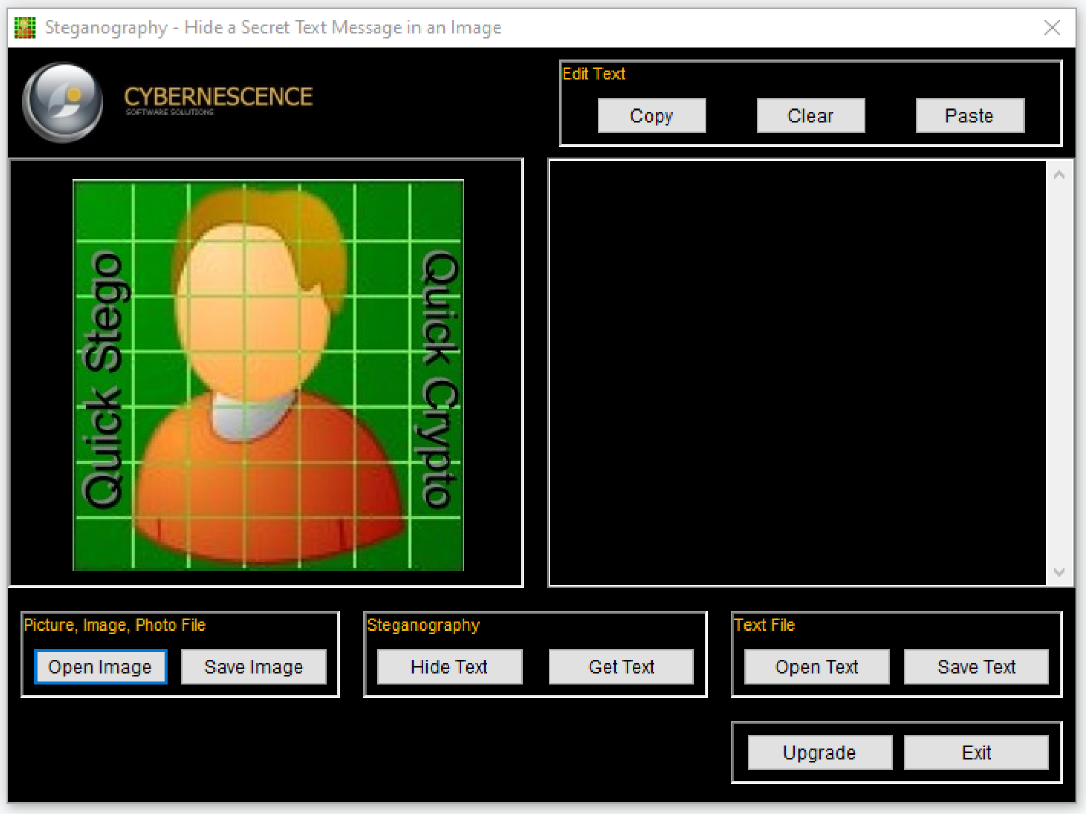


Name	Date modified	Type	Size
UEMSMobile	10/25/2020 9:13 PM	File folder	
3DMark	8/2/2020 6:48 PM	Internet Shortcut	1 KB
A Plague Tale Innocence	7/25/2020 1:01 PM	Internet Shortcut	1 KB
American Truck Simulator	7/27/2020 9:31 PM	Internet Shortcut	1 KB
Cooking Simulator	8/25/2020 9:51 AM	Internet Shortcut	1 KB
EA SPORTS™ FIFA 21	11/6/2020 11:14 PM	Internet Shortcut	1 KB
Euro Truck Simulator 2	7/27/2020 9:31 PM	Internet Shortcut	1 KB
Far Cry 3 Map Editor	9/2/2020 1:49 AM	Internet Shortcut	1 KB
Far Cry 3	9/2/2020 1:49 AM	Internet Shortcut	1 KB
Grand Theft Auto IV The Complete Edition	8/23/2020 7:44 AM	Internet Shortcut	1 KB
Max Payne 3	7/27/2020 6:37 PM	Internet Shortcut	1 KB
Overcooked! 2	8/5/2020 11:47 AM	Internet Shortcut	1 KB
Red Dead Redemption 2	7/26/2020 12:11 AM	Internet Shortcut	1 KB
Sleeping Dogs Definitive Edition	8/3/2020 10:01 AM	Internet Shortcut	1 KB
Tom Clancy's The Division	9/1/2020 5:46 PM	Internet Shortcut	1 KB
united-polaris-seat	11/11/2020 10:23 AM	BMP File	4,219 KB
World War Z	7/26/2020 10:26 AM	Internet Shortcut	1 KB

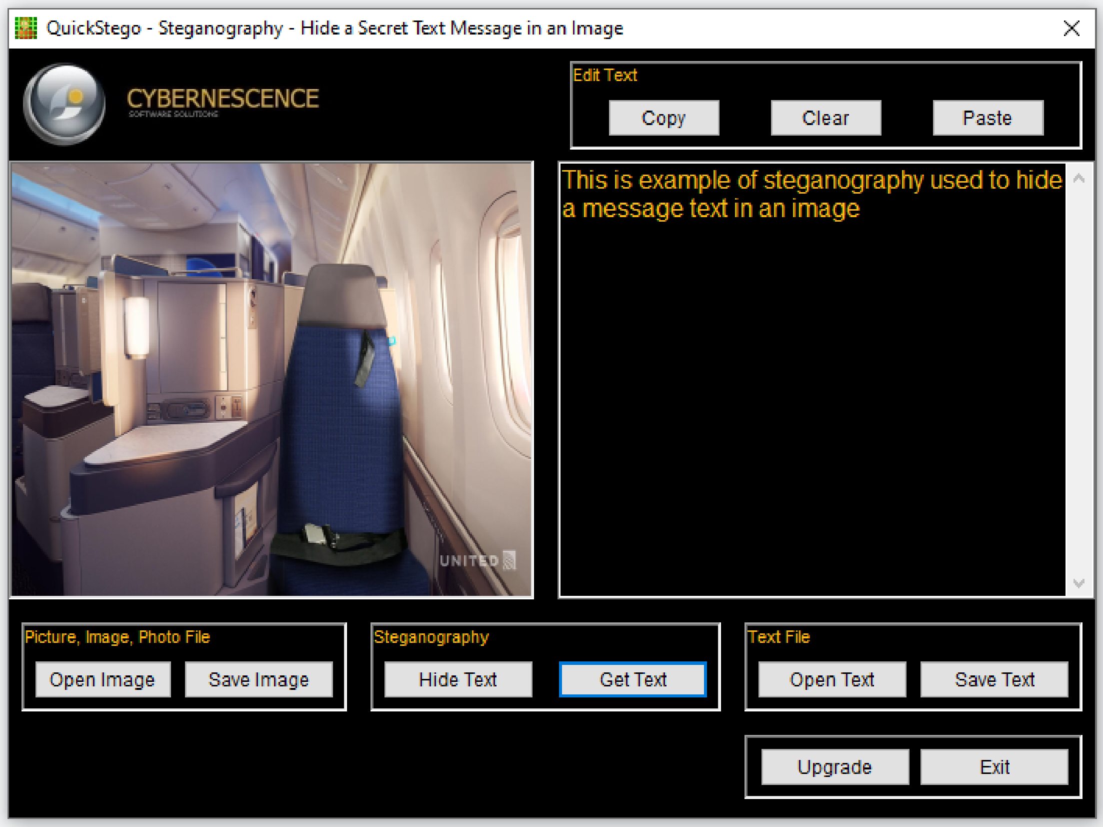
File name: united-polaris-seat

Save as type: Image (*.bmp)

- The receiver of this image also needs to use this software to be able the hidden message on this image appear.



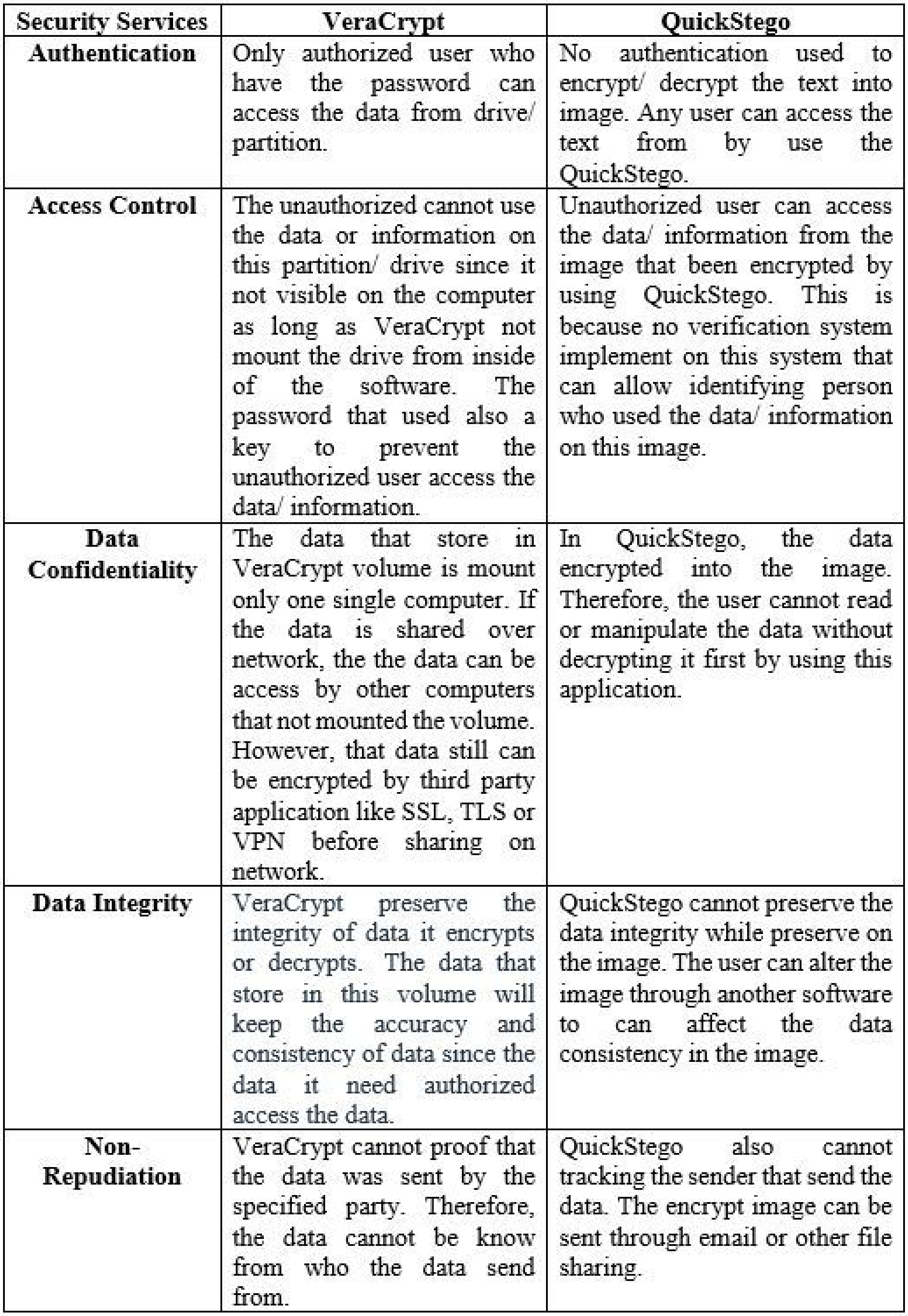
- The receiver needs to click on “Get Text” to decrypt the image to show the hidden message through the textbox.



QuickStego - Steganography - Hide a Secret Text Message in an Image

This is example of steganography used to hide a message text in an image

IV. Comparison Between Tools



Security Services	VeraCrypt	QuickStego
Authentication	Only authorized user who have the password can access the data from drive/ partition.	No authentication used to encrypt/ decrypt the text into image. Any user can access the text from by use the QuickStego.
Access Control	The unauthorized cannot use the data or information on this partition/ drive since it not visible on the computer as long as VeraCrypt not mount the drive from inside of the software. The password that used also a key to prevent the unauthorized user access the data/ information.	Unauthorized user can access the data/ information from the image that been encrypted by using QuickStego. This is because no verification system implement on this system that can allow identifying person who used the data/ information on this image.
Data Confidentiality	The data that store in VeraCrypt volume is mount only one single computer. If the data is shared over network, the the data can be access by other computers that not mounted the volume. However, that data still can be encrypted by third party application like SSL, TLS or VPN before sharing on network.	In QuickStego, the data encrypted into the image. Therefore, the user cannot read or manipulate the data without decrypting it first by using this application.
Data Integrity	VeraCrypt preserve the integrity of data it encrypts or decrypts. The data that store in this volume will keep the accuracy and consistency of data since the data it need authorized access the data.	QuickStego cannot preserve the data integrity while preserve on the image. The user can alter the image through another software to can affect the data consistency in the image.
Non-Repudiation	VeraCrypt cannot proof that the data was sent by the specified party. Therefore, the data cannot be know from who the data send from.	QuickStego also cannot tracking the sender that send the data. The encrypt image can be sent through email or other file sharing.

V. Conclusion

VeraCrypt is the best tool for the tools listed. This tool will ensure that a confidential framework is structured to prevent sensitive data from reaching the wrong person. Only a user who knows a password can install the volume / drive to the device to access the partition. QuickStego does not provide authentic authentication to prevent the data from being accessed by an unauthorized user. VeraCrypt 's integrity guarantees that the data can not be changed by an unauthorized user. This prevents unauthorized entities from getting file authorization and user access control. In addition, QuickStego has strong reputation to ensure data continuity, accuracy and trustworthiness. VeraCrypt 's availability shows good data protection which can be repaired quickly to ensure that the system operates properly and avoid system disputes.

As one of the security principles, QuickStego does not enforce accessibility to ensure that the application can provide good data maintenance, because encrypting the image without proper sharing can make it possible for the unauthorized user to access the data from that image.