Cryptography

Module 19

Cryptography

Cryptography is the study and art of hiding information in human unreadable format.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

The ability to protect and secure information is vital to the growth of electronic commerce and to the growth of the Internet itself. Many people need or want to use communications and data security in different areas. Encrypting the data plays a major role in security. For example, banks use encryption methods around the world to process financial transactions. This involves the transfer of large amounts of money from one bank to another. Banks also use encryption methods to protect their customers ID numbers at bank automated teller machines. There are many companies and even shopping malls selling anything from flowers to bottles of wines over the Internet and these transactions are made by the use of credit cards and secure Internet browsers, including encryption techniques. Customers using the Internet would like to know the connection is secure when sending their credit card information and other financial details related to them over a multi-national environment This will only work with the use of strong and unforgeable encryption methods. Since you are an expert ethical hacker and penetration tester, your IT director will instruct you to encrypt data using various encrypting algorithms in order to secure the organization's information.

Lab Objectives

This lab will show you how to encrypt data and how to use it. It will teach you how to:

- Use encrypting/decrypting commands
- Generate hashes and checksum files

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

To carry out the lab, you need:

- A computer running **Window Server 2012**
- A web browser with Internet access

Lab Duration

Time: 50 Minutes

Overview of Cryptography

Cryptography is the practice and study of **hiding** information. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering.

Cryptology prior to the modern age was almost synonymous with **encryption**, the **conversion** of information from a readable state to one apparently without sense.

TASK 1

Overview

Lab Tasks

Recommended labs to assist you in Cryptography:

- Basic Data Encrypting Using **HashCalc**
- Basic Data Encrypting Using **MD5 Calculator**
- Basic Data Encrypting Using **Advance Encryption Package**
- Basic Data Encrypting Using **TrueCrypt**
- Basic Data Encrypting Using **CrypTool**
- Encrypting and Decrypting the Data Using **BCTextEncoder**
- Basic Data Encrypting Using **Rohos Disk Encryption**

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Basic Data Encrypting Using HashCalc

HashCalc enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It supports MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, and the hash used in eDonkey and eMule tools.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Laptops are highly susceptible to theft and frequently contain valuable data. Boot disk encryption requires a key in order to start the operating system and access the storage media. Disk encryption encrypts all data on a system, including files, folders, and the operating system. This is most appropriate when the physical security of the system is not assured. Examples include traveling laptops or desktops that are not in a physically secured area. When properly implemented, encryption provides an enhanced level of assurance to the data, while encrypted, cannot be viewed or otherwise discovered by unauthorized parties in the event of theft, loss, or interception. In order to be an expert ethical hacker and penetration tester, you must understand data encryption using encrypting algorithms.

Lab Objectives

This lab will show you how to encrypt data and how to use it. It will teach you how to:

- Use encrypting/decrypting command
- Generate hashes and checksum files

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

Lab Environment

To carry out the lab, you need:

- **HashCalc** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\MD5 Hash Calculators\HashCalc**

- You can also download the latest version of **HashCalc** from the link http://www.slavasoft.com/hashcalc/
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Follow the wizard driven installation instructions
- Run this tool in **Windows Server 2012**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Hash

HashCalc is a fast and easy-to-use calculator that allows computing message **digests, checksums,** and **HMACs for files**, as well as for **text and hex strings**. It offers a choice of 13 of the most popular hash and checksum algorithms for calculations.

TASK 1

Lab Tasks

Calculate the Hash

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

You can also download HashCalc from http://www.slavasoft.com

FIGURE 1.1: Windows Server 2012 – Desktop view

2. Click the **HashCalc** app to open the **HashCalc** window.

HashCalc simple dialog-size interface dispenses with glitz to plainly list input and results.

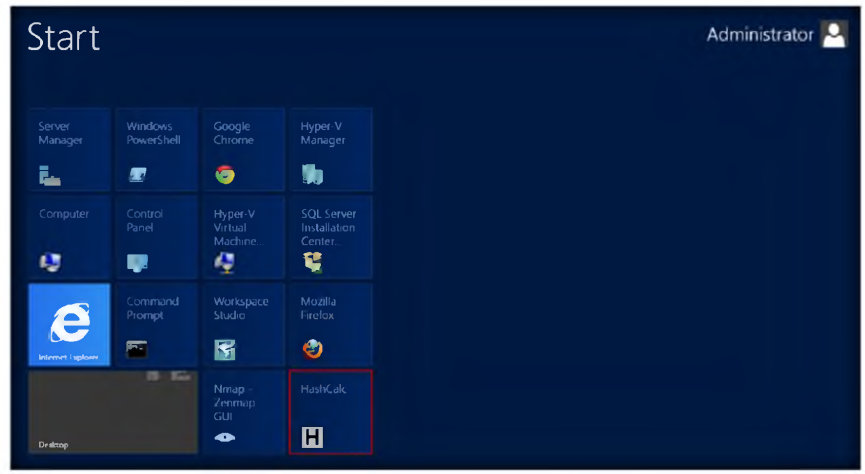


FIGURE 1.2: Windows Server 2012 – Apps

3. The main window of **HashCalc** appears as shown in the following figure.
4. From the **Data Format** drop-down list, select **File**.

Hash algorithms support three input data formats: file, text string, and hexadecimal string.

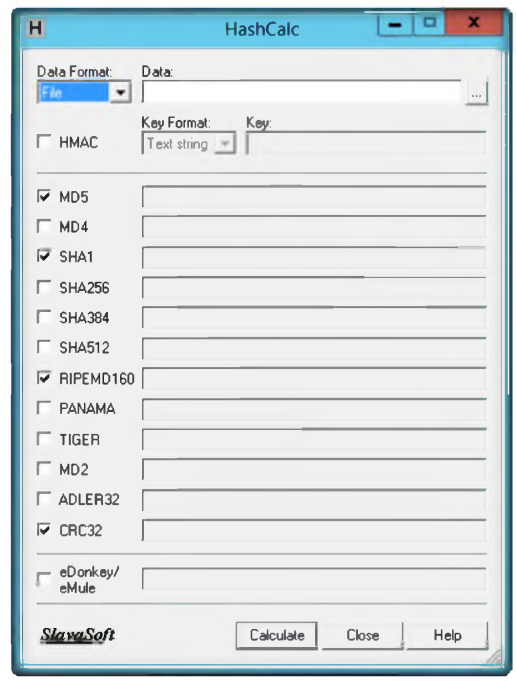


FIGURE 1.3: HashCalc main window

5. Enter/Browse the data to calculate.
6. Choose the appropriate **Hash algorithms** and check the check boxes.
7. Now, click **Calculate**.

HashCalc is used to generate crypting text.

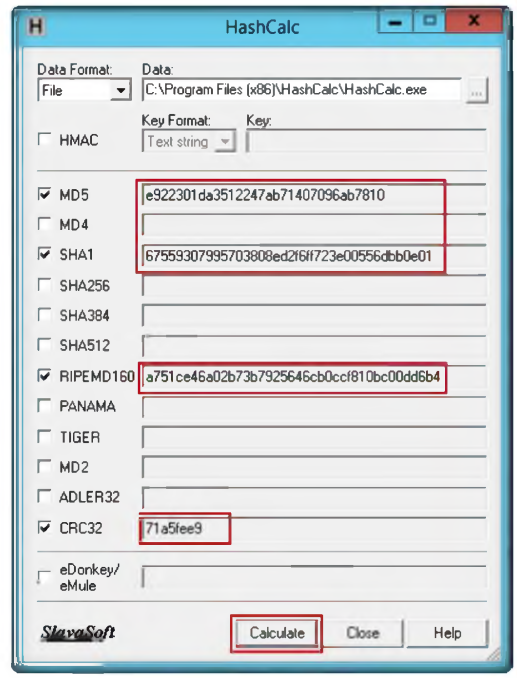


FIGURE 1.4: Hash is generated for chosen hash string

Lab Analysis

Document all Hash, MD5, and CRC values for further reference.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
HashCalc	**Output:** Generated Hashes for ▪ MD5 ▪ SHA1 ▪ RIPEMD160 ▪ CEC32

Questions

1. Determine how to calculate multiple checksums simultaneously.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 2

Basic Data Encrypting Using MD5 Calculator

MD5 Calculator is a simple application that calculates the MD5 hash of a given file. It can be used with big files (some GB). It features a progress counter and a text field from which the final MD5 hash can be easily copied to the clipboard.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

There has been a need to protect information from "prying eyes." In the electronic age, information that could otherwise benefit or educate a group or individual can also be used against such groups or individuals. Industrial espionage among highly competitive businesses often requires that extensive security measures be put into place. And, those who wish to exercise their personal freedom, outside of the oppressive nature of governments, may also wish to encrypt certain information to avoid suffering the penalties of going against the wishes of those who attempt to control. Still, the method of data encryption and decryption are relatively straightforward; encryption algorithms are used to encrypt the data and it stores system information files on the system, safe from prying eyes. In order to be an expert ethical hacker and penetration tester, you must understand data encryption using encrypting algorithms.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

- Use encrypting/decrypting commands
- Calculate the MD5 value of the selected file

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

Lab Environment

To carry out the lab, you need:

- **MD5 Calculator** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\MD5 Hash Calculators\MD5 Calculator**
- You can also download the latest version of **MD5 Calculator** from the link http://www.bullzip.com/products/md5/info.php
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Follow the wizard driven installation instructions
- Run this tool in **Windows Server 2012**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of MD5 Calculator

MD5 Calculator is a bare-bones program for **calculating and comparing** MD5 files. While its layout leaves something to be desired, its results are fast and simple.

Lab Tasks

TASK 1

Calculate MD5 Checksum

1. To find MD5 Hash of any file, right-click the file and select **MD5 Calculator** from the context menu.

MD5 checksum is used to generate MD5 hash.

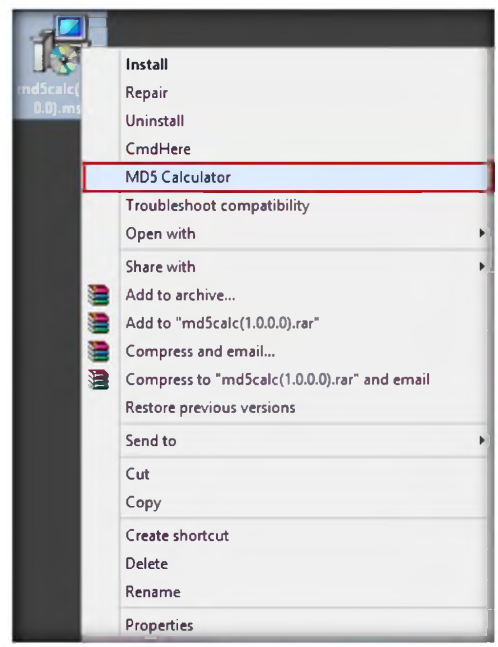


FIGURE 2.1: MD5 option in context menu

2. **MD5 Calculator** shows the MD5 digest of the selected file.

Note: Alternatively, you can browse any file to calculate the MD5 hash and click the **Calculate** button to calculate the MD5 hash of the file.

MD5 hash (or checksum) functions as a compact digital fingerprint of a file.

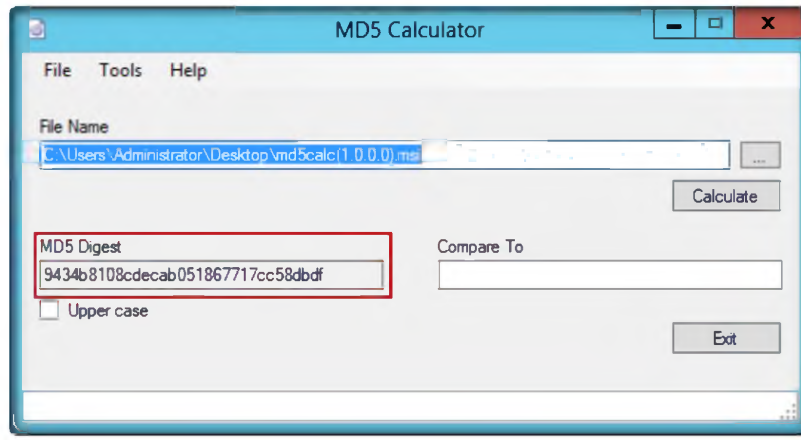


FIGURE 2.2: MD5 is generate for the chosen file

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
MD5 Calculator	**Output:** MD5 Hashes for selected software

Questions

1. What are the alternatives to the MD5 sum calculator?
2. Is the MD5 (Message-Digest algorithm 5) calculator a widely used cryptographic hash function with a 128-bit hash value?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 3

Basic Data Encrypting Using Advanced Encryption Package

Advanced Encryption Package is most noteworthy for its flexibility; not only can you encrypt files for your own protection, but you can easily create "self-decrypting" versions of your files that others can run without needing this or any other software.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Data encryption and decryption operations are major security applications to secure data. Most systems use block ciphers, such as public AES standard. However, implementations of block ciphers such as AES, as well as other cryptographic algorithms, are subject to side-channel attacks. These attacks allow adversaries to extract secret keys from devices by passively monitoring power consumption, other side channels. Countermeasures are required for applications where side-channel attacks are a threat. These include several military and aerospace applications where program information, classified data, algorithms, and secret keys reside on assets that may not always be physically protected. In order to be an expert ethical hacker and penetration tester, you must understand data encrypted over files.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

- Use encrypting/decrypting commands
- Calculate the encrypted value of the selected file

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

Lab Environment

To carry out the lab, you need:

- **Advanced Encryption Package** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Cryptography Tools\Advanced Encryption Package**

- You can also download the latest version of **Advanced Encryption Package** from the link http://www.secureaction.com/encryption_pro/
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Follow the wizard-driven installation instructions
- Run this tool in **Windows Server 2012**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Advanced Encryption Package

Advanced Encryption Package includes a **file shredder** that wipes out the contents of your original files. It also integrates nicely with **Windows Explorer**, allowing you to use Explorer's context menus and avoid having another **window** clutter your screen.

Lab Tasks

TASK 1

Encrypting a File

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

FIGURE 3.1: Windows Server 2012 – Desktop view

You can also download Advance Encryption Package from http://www.secureaction.com

2. Click the **Advanced Encryption Package** app to open the **Advanced Encryption Package** window.

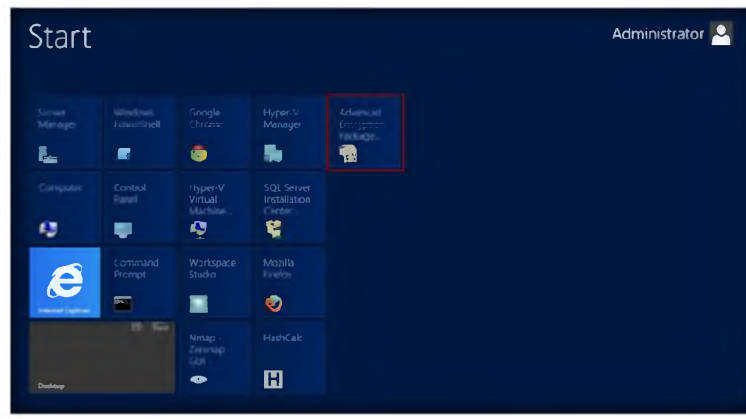


FIGURE 3.2: Windows Server 2012 – Apps

3. The **Register Advanced Encryption Package 2013** trial period window appears. Click **Try Now!**.

FIGURE 3.3: Activation Window

4. The main window of **Advanced Encryption Package** appears, as show in the following figure.

Advance Encryption Package is easy to use for novices.

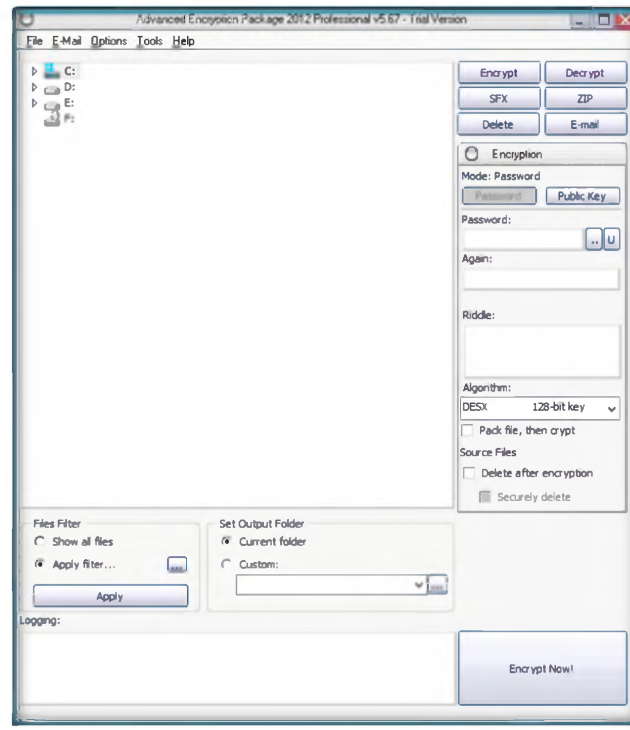


FIGURE 3.4: Welcome screen of Advance Encryption Package

Advanced Encryption Package is a symmetric-key encryption comprising three block ciphers, AES-128, AES-192 and AES-256.

5. Select the sample file to encrypt. The file is located **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Cryptography Tools\Advanced Encryption Package**.
6. Click **Encrypt**. It will ask you to enter the password. Type the password in the **Password** field, and again type the password in the **Again** field.
7. Click **Encrypt Now!**.

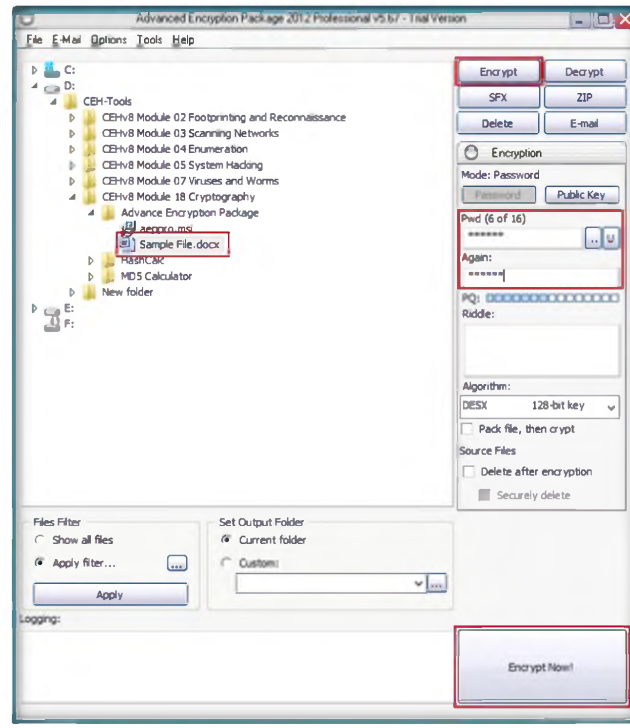


FIGURE 3.5: Welcome screen of Advance Encryption Package

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

8. The encrypted sample file can be shown in the same location of the original file, as shown in the following figure.

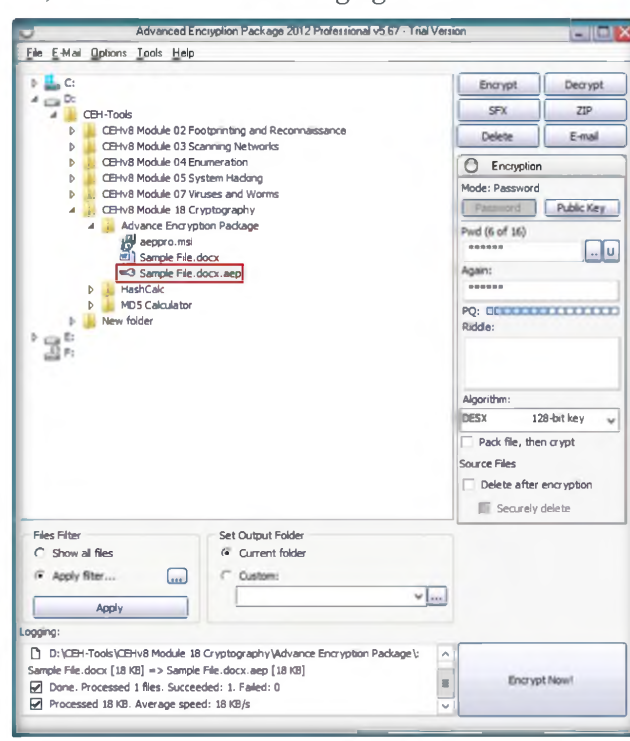


FIGURE 3.6: Encrypting the selected file

9. To decrypt the file, first select the encrypted file. Click **Decrypt**; it will prompt you to enter the password.
10. Click **Decrypt Now!**.

It creates encrypted self-extracting files to send as email attachments.

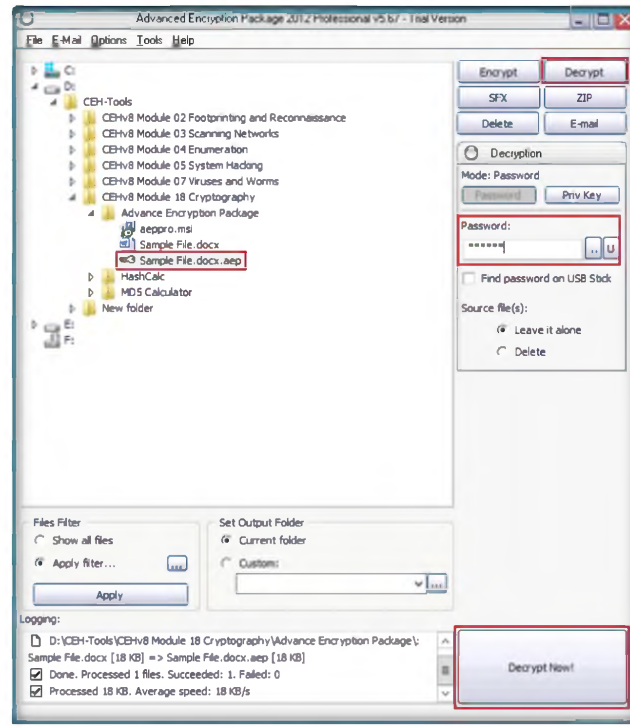


FIGURE 3.7: Decrypting the selected file

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Advance Encryption	**Output:** Encrypted simple File.docx.ape

Package	

Questions

1. Which algorithm does Advanced Encryption Package use to protect sensitive documents?
2. Is there any other way to protect the use of private key file with a password?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 4

Basic Data Encrypting Using TrueCrypt

TrueCrypt is a software system for establishing and maintaining an on-the-fly encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted or decrypted right before it is loaded or saved, without any user intervention.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

CiTx is a billion-dollar company and does not want to take chances or risk the data stored on its laptops. These laptops contain proprietary partner information, customer data, and financial information. CiTx cannot afford its data to be lost to any of its competitors. The CiTx Company started using full disk encryption to protect its data from preying eyes. Full disk encryption encrypts all data on a system, including files, folders and the operating system. This is most appropriate when the physical security of the system is not assured. Encryption uses one or more cryptographic keys to encrypt and decrypt the data that they protect.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

- Use encrypting/decrypting commands
- Create a virtual encrypted disk with a file

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

Lab Environment

To carry out the lab, you need:

- **TrueCrypt** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Disk Encryption Tools\TrueCrypt**
- You can also download the latest version of **TrueCrypt** from the link http://www.truecrypt.org/downloads

- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Follow the **wizard-driven installation** instructions
- Run this tool in **Windows Server 2012**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of TrueCrypt

TrueCrypt is a software application used for on-the-fly encryption (OTFE). It is distributed without cost, and the source code is available. It can create a **virtual encrypted disk** within a file or encrypt a partition or an entire storage device.

TASK 1

Create a Volume

Lab Tasks

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

FIGURE 4.1: Windows Server 2012 – Desktop view

2. Click the **TrueCrypt** app to open the **TrueCrypt** window.

You can also download Truecrypt from http://www.truecrypt.org

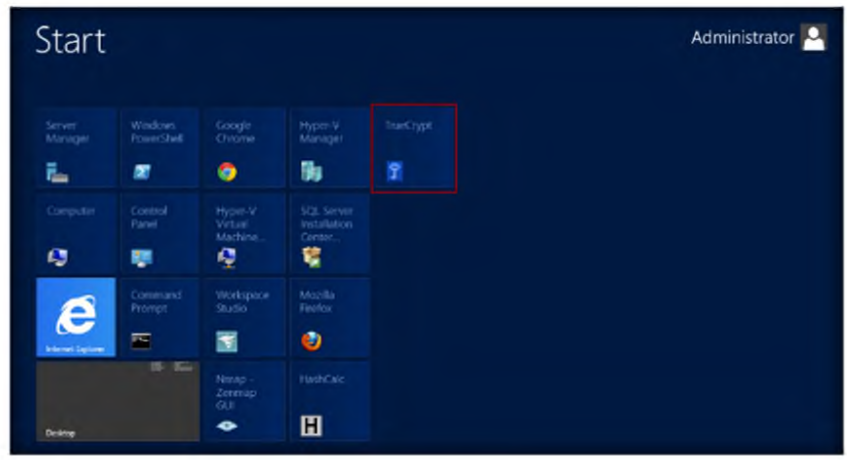


FIGURE 4.2: Windows Server 2012 – Apps

3. The **TrueCrypt** main window appears.

4. Select the desired volume to be encrypted and click **Create Volume**.

TrueCrypt is a software application used for on-the-fly encryption (OTFE). It is distributed without cost and the source code is available.

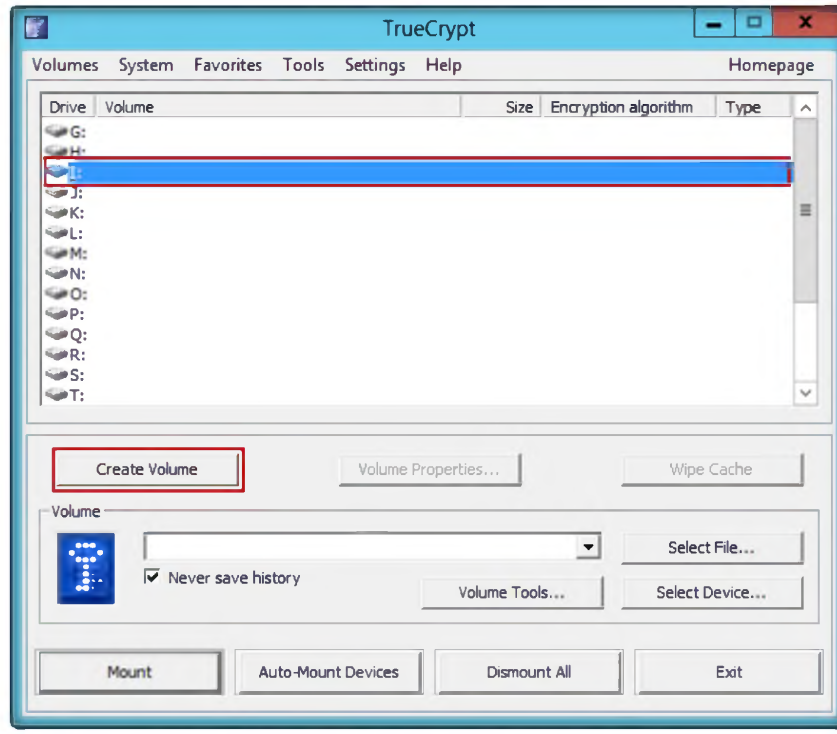


FIGURE 4.3: TrueCrypt Main Window With Create Volume Option

TrueCrypt have the ability to create and run a hidden encrypted operating system whose existence may be denied.

5. The **TrueCrypt Volume Creation Wizard** window appears.
6. Select the **Create an encrypted file container** option. This option creates a virtual encrypted disk within a file.
7. By default, the **Create an encrypted file container** option is selected. Click **Next** to proceed.

IMPORTANT: Note that TrueCrypt will not encrypt any existing files (when creating a TrueCrypt file container). If you select an existing file in this step, it will be overwritten and replaced by the newly created volume (so the overwritten file will be lost, not encrypted). You will be able to encrypt existing files (later on) by moving them to the TrueCrypt volume that we are creating now.

FIGURE 4.4: TrueCrypt Volume Creation Wizard-Create Encrypted File Container

8. In the next step of the wizard, choose the type of volume.
9. Select **Standard TrueCrypt volume**; this creates a **normal** TrueCrypt volume.
10. Click **Next** to proceed.

Note: After you copy existing unencrypted files to a TrueCrypt volume, you should securely erase (wipe) the original unencrypted files. There are software tools that can be used for the purpose of secure erasure (many of them are free).

FIGURE 4.5: TrueCrypt Volume Creation Wizard-Volume Type

11. In the next wizard, select the **Volume Location**.
12. Click **Select File...**.

TrueCrypt supports a concept called plausible deniability.

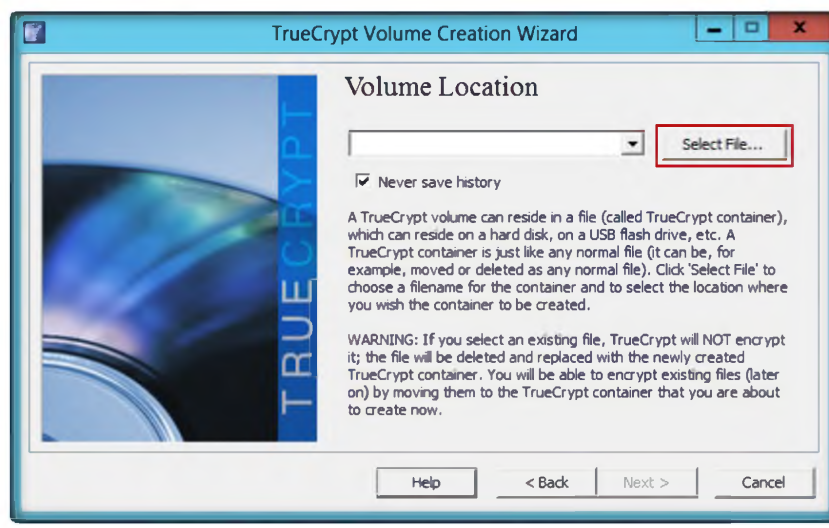


FIGURE 4.6: TrueCrypt Volume Creation Wizard-Volume Location

13. The standard Windows file selector appears. The **TrueCrypt Volume Creation Wizard** window remains open in the background.
14. Select a desired **location**; provide a **File name** and **Save** it.

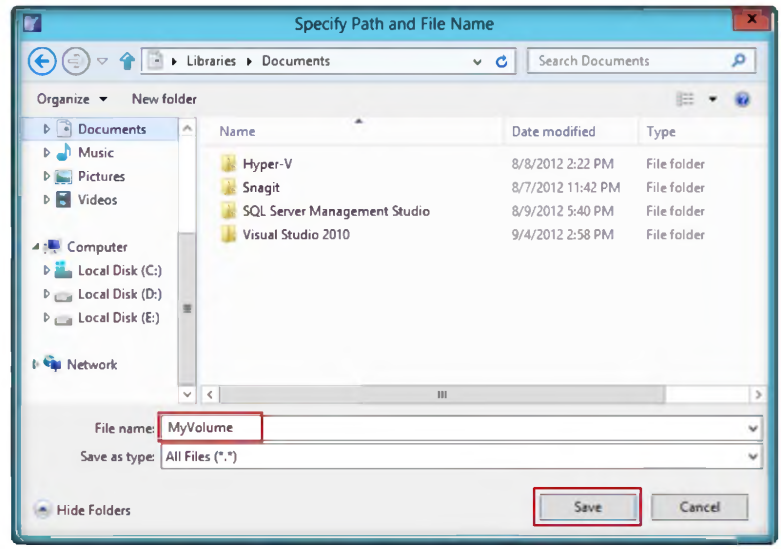


FIGURE 4.7: Windows Standard-Specify Path and File Name Window

The mode of operation used by TrueCrypt for encrypted partitions, drives, and virtual volumes is XTS.

15. After saving the file, the **Volume Location** wizard continues. Click **Next** to proceed.

FIGURE 4.8: TrueCrypt Volume Creation Wizard-Volume Location

TrueCrypt volumes do not contain known file headers and their content is indistinguishable from random data.

16. **Encryption Options** appear in the wizard.
17. Select **AES Encryption Algorithm** and **RIPEMD-160 Hash Algorithm** and click **Next**.

TrueCrypt currently supports the following hash algorithms:

- RIPEMD-160
- SHA-512
- Whirlpool

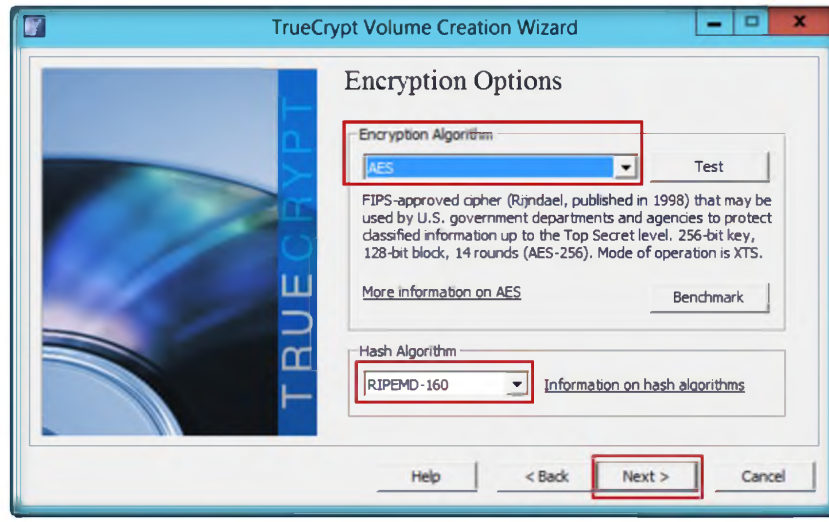


FIGURE 4.9: TrueCrypt Volume Creation Wizard-Encryption Options

18. In the next step, **Volume Size** option appears.
19. Specify the size of the TrueCrypt container to be **2** megabyte and click **Next**.

Note: The button "Next" will be disabled until passwords in both input fields are the same.

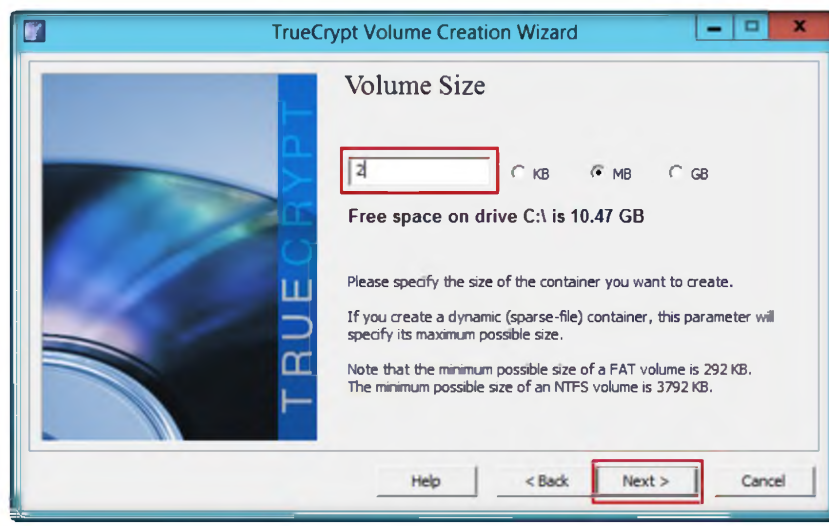


FIGURE 4.10: TrueCrypt Volume Creation Wizard-Volume Size

20. The **Volume Password** option appears. This is one of the most important steps. Read the information displayed in the wizard window on what is considered a good password carefully.
21. Provide a good password in the first input field, re-type it in the **Confirm** field, and click **Next**.

FIGURE 4.11: TrueCrypt Volume Creation Wizard-Volume Password

The longer you move the mouse, the better. This significantly increases the **cryptographic strength** of the encryption keys.

22. The **Volume Format** option appears. Select **FAT Filesystem**, and set the cluster to **Default**.
23. Move your mouse as randomly as possible within the **Volume Creation** Wizard window at least for 30 seconds.
24. Click **Format**.

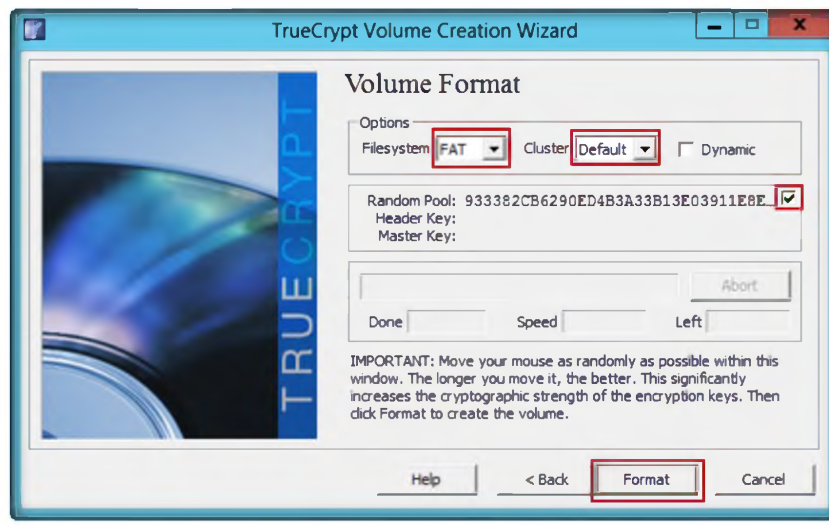


FIGURE 4.12: TrueCrypt Volume Creation Wizard-Volume Format

TrueCrypt volumes have no "signature" or ID strings. Until decrypted, they appear to consist solely of random data.

25. After clicking **Format** volume creation begins. TrueCrypt will now create a file called **MyVolume** in the provided folder. This file depends on the TrueCrypt container (it will contain the encrypted TrueCrypt volume).
26. Depending on the size of the volume, the volume creation may take a long time. After it finishes, the following dialog box appears.

Free space on each TrueCrypt volume is filled with random data when the volume is created.

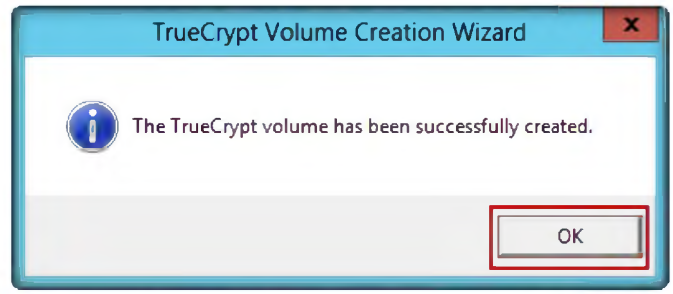


FIGURE 4.13: TrueCrypt Volume Creation Wizard- Volume Successfully Created Dialog Box

27. Click **OK** to close the dialog box.
28. You have successfully created a TrueCrypt volume (file container).
29. In the **TrueCrypt Volume Creation** wizard window, click **Exit**.

TrueCrypt is unable to secure data on a computer if an attacker physically accessed it and TrueCrypt is used on the compromised computer by the user again.

FIGURE 4.14: TrueCrypt Volume Creation Wizard-Volume Created

TASK 2

Mount a Volume

30. To mount a volume, launch **TrueCrypt**.
31. In the main window of **TrueCrypt**, click **Select File...**

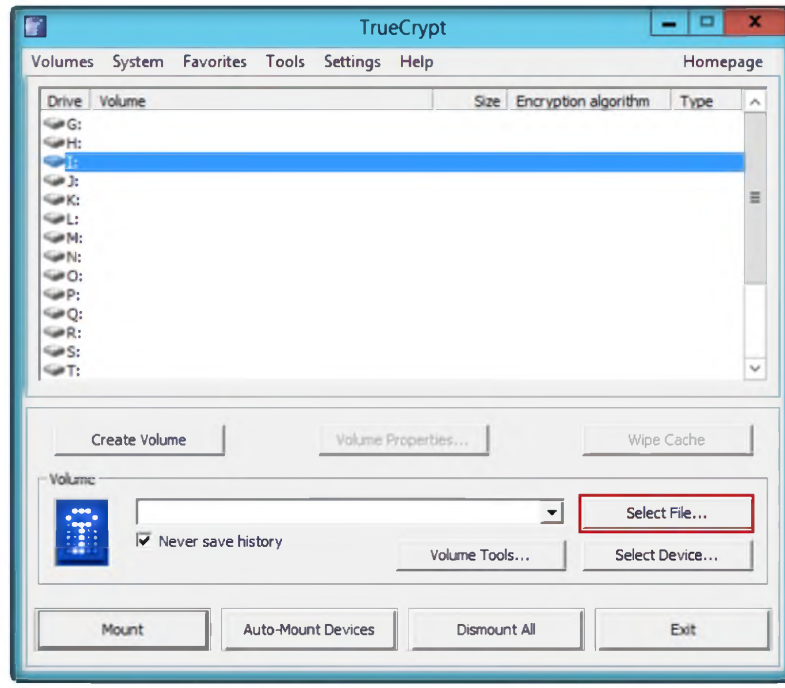
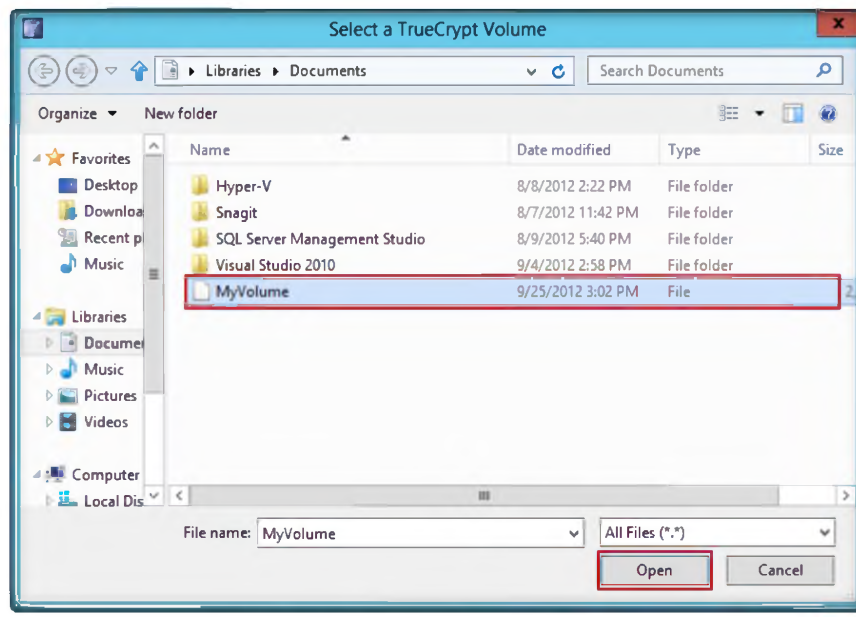


FIGURE 4.15: TrueCrypt Main Window with Select File Button

Mount options affect the parameters of the volume being mounted. The Mount Options dialog can be opened by clicking on the Mount Options button in the password entry dialog.

32. The standard file selector window appears.
33. In the file selector, browse to the container file, select the file, and click **Open**.



Default mount options can be configured in the main program preferences (Settings → Preferences).

FIGURE 4.16: Windows Standard File Selector Window

34. The file selector window disappears and returns to the main **TrueCrypt** window.

35. In the main **TrueCrypt** window, click **Mount**.

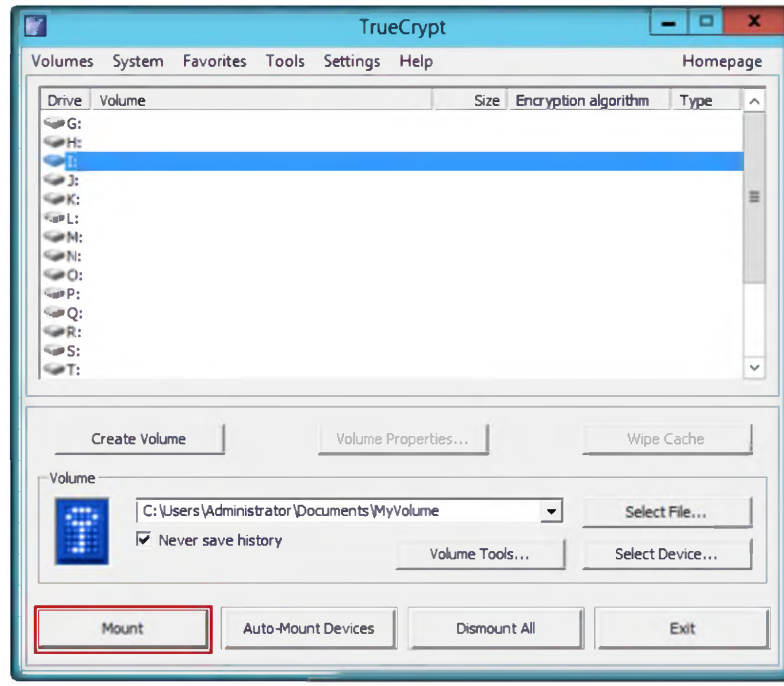


FIGURE 4.17: TrueCrypt Main Window with Mount Button

This option can be set in the password entry dialog so that it will apply only to that particular mount attempt. It can also be set as default in the Preferences.

36. The **Password prompt** dialog window appears.

37. Type the password (which you specified earlier for this volume) in the **Password** input field and click **OK**.

When a correct password is cached, volumes are automatically mounted after you click Mount. If you need to change mount options for a volume being mounted using a cached password, hold down the Control (Ctrl) key while clicking Mount, or select Mount with Options from the Volumes menu.

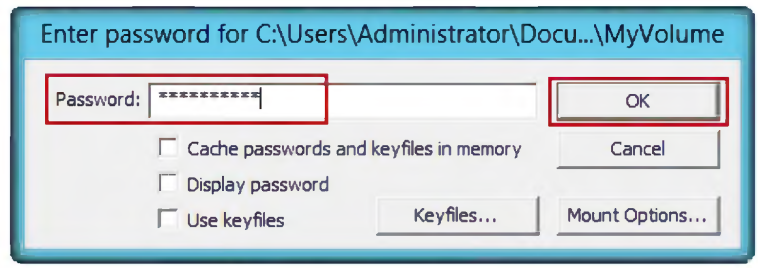


FIGURE 4.18: TrueCrypt Password Window

38. TrueCrypt now attempts to mount the volume. After the password is verified, TrueCrypt will mount the volume.

No data stored on an encrypted volume can be read (decrypted) without using the correct password or correct encryption key.

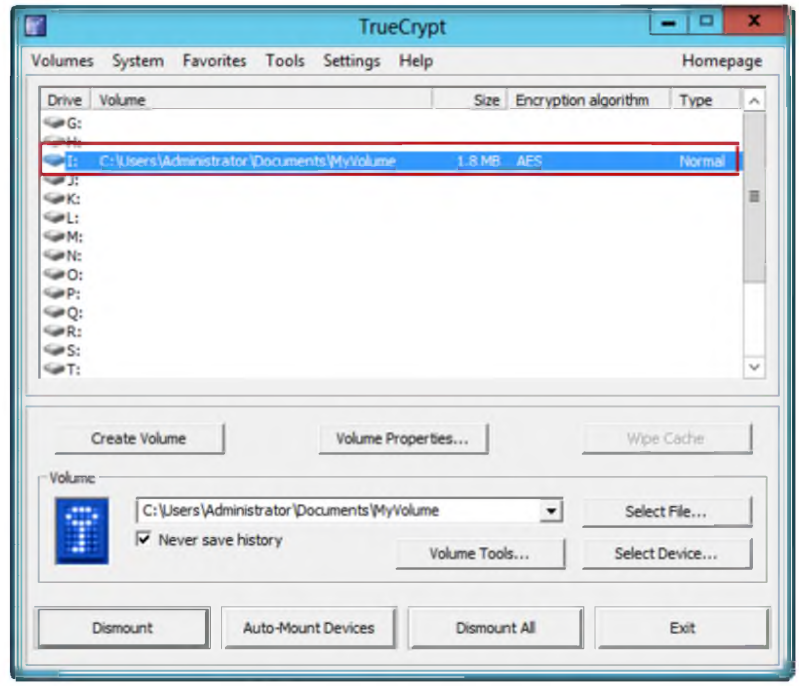


FIGURE 4.19: TrueCrypt Main Window

39. MyVolume has successfully mounted the container as a virtual disk I:.
40. The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves like a real disk.
41. You can save (or copy, move, etc.) files to this virtual disk and they will be encrypted on the fly as they are being written.
42. To dismount a volume, select the volume to dismount and click **Dismount**. The volume is dismounted.

TrueCrypt cannot automatically dismount all mounted TrueCrypt volumes on system shutdown/restart.

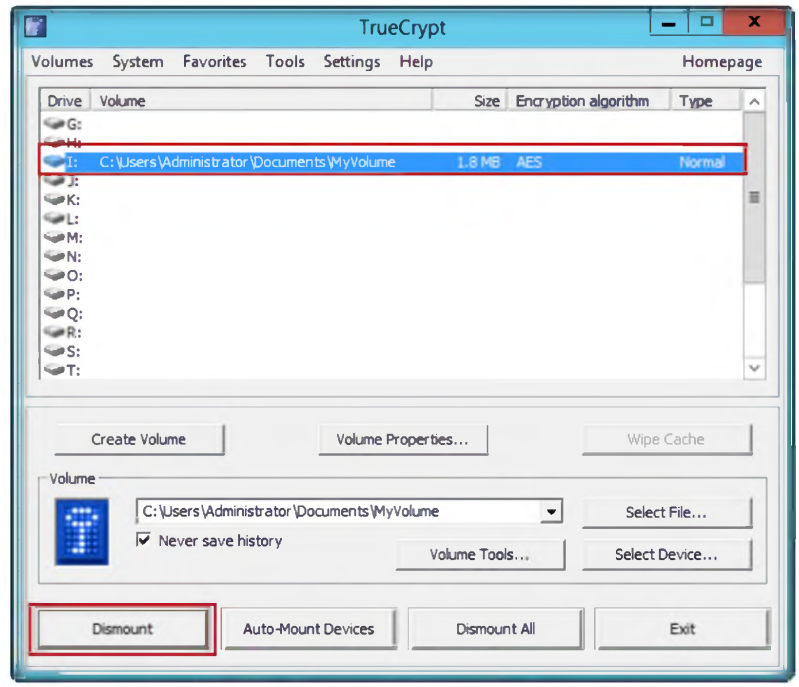


FIGURE 4.20: TrueCrypt Main Window with Dismount Button

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
TrueCrypt	**Encrypted Volume:** I
	Volume File System: FAT

Questions

1. Determine whether there is any way to recover the files from the TrueCrypt volume if you forget the volume password.
2. Evaluate whether TrueCrypt uses any trusted program module (TPM) to prevent attacks. If yes, find out the relevant TPM.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 5

Basic Data Encrypting Using CrypTool

CrypTool is a freeware program that enables you to apply and analyze cryptographic mechanisms. It has the typical look and feel of a modern Windows application. CrypTool includes every state-of-the-art cryptographic function and allows you to learn and use cryptography within the same environment.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Most security initiatives are defensive strategies aimed at protecting the perimeter of the network. But these efforts may ignore a crucial vulnerability: sensitive data stored on networked servers is at risk from attackers who only need to find one way inside the network to access this confidential information. Additionally, perimeter defenses like firewalls cannot protect stored sensitive data from the internal threat of employees with the means to access and exploit this data. Encryption can provide strong security for sensitive data stored on local or network servers. In order to be an expert ethical hacker and penetration tester, you must have knowledge of cryptography functions.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

- Use encrypting/decrypting commands
- Visualize several algorithms
- Calculate hash values and analysis

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

Lab Environment

To carry out the lab, you need:

- **CrypTool** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Cryptanalysis Tools\CrypTool**

- You can also download the latest version of **CrypTool** from the link http://www.cryptool.org/en/download-ct1-en
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Follow the **wizard-driven installation** instructions
- Run this tool on **Windows Server 2012** host machine
- Administrative privileges to run the tool

CrypTool is a free e-learning application for Windows.

Lab Duration

Time: 10 Minutes

Overview of CrypTool

CrypTool is a free, open-source **e-learning application** used in the implementation and analysis of **cryptographic algorithms**. It was originally designed for internal **business application** for information **security** training.

Lab Tasks

TASK 1

Encrypting the Data

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

FIGURE 5.1: Windows Server 2012 – Desktop view

2. Click the **CrypTool** app to open the **CrypTool** window.

You can also download CrypTool from http://www.cryptool.org

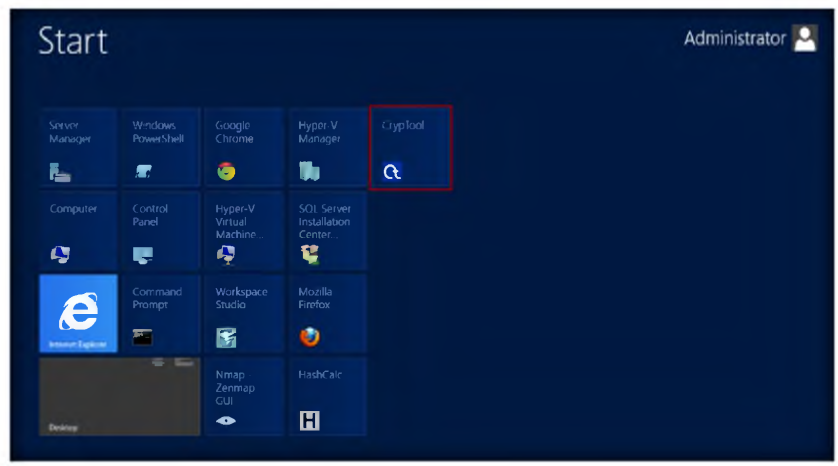


FIGURE 5.2: Windows Server 2012 – Apps

3. The **How to Start** dialog box appears. Check **Don't show this dialog again** and click **Close**.

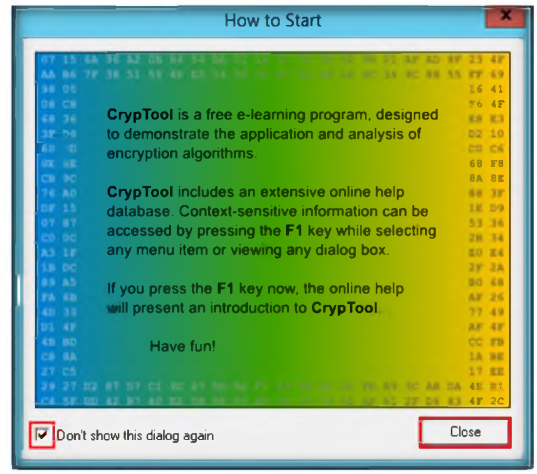


FIGURE 5.3: How to Start Dialog Window

CrypTool Online provides an exciting insight into the world of cryptology with a variety of ciphers and encryption methods.

4. The main window of **CrypTool** appears, as shown in the following figure. Close the **startingexample-en.txt** window in **CrypTool**.

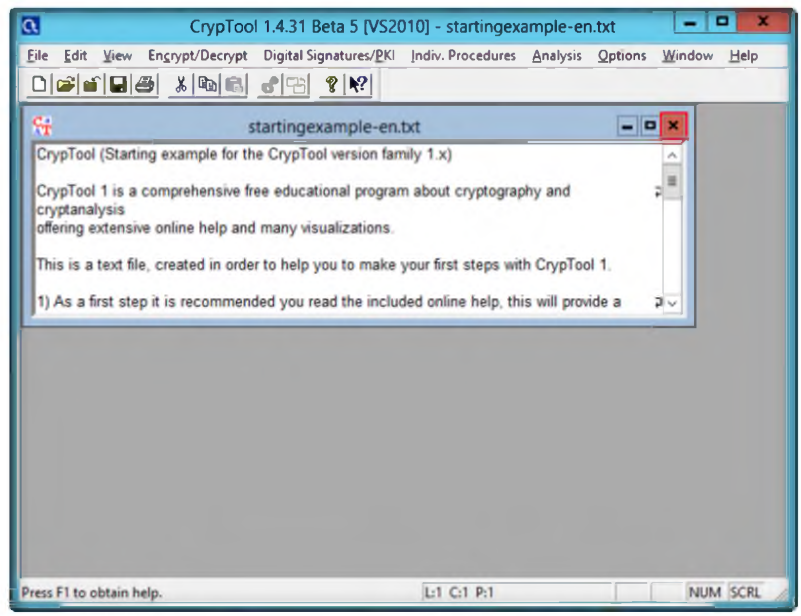


FIGURE 5.4: startingexample-en.txt window in CrypTool

5. To encrypt the desired data, click the **File** option and select **New** from the menu bar.

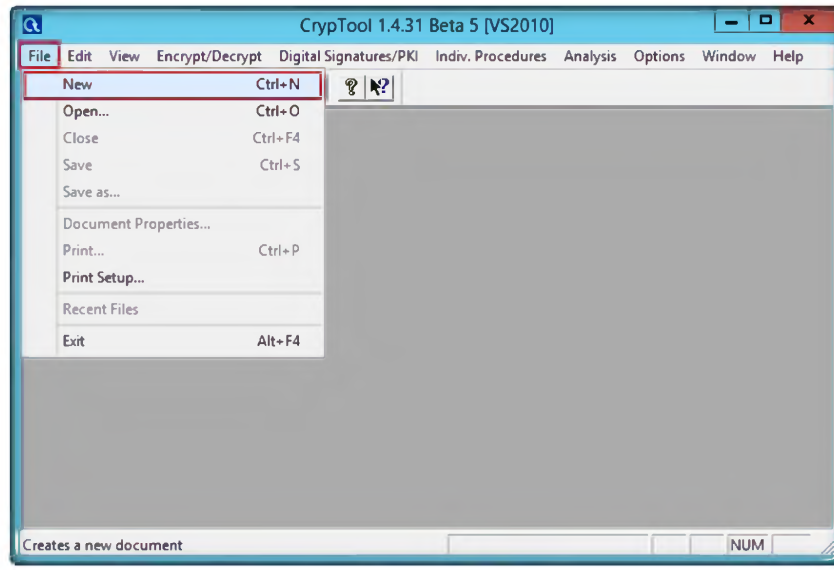


FIGURE 5.5: CrypTool Main Window

CrypTool was originally designed for internal business application for information security.

6. Type a few lines in the opened **Unnamed1 Notepad** of **CrypTool**.
7. On the menu bar, select **Encrypt/Decrypt**, **Symmetric (modern)**, and select any encrypting algorithm.
8. Select the **RC2** encrypting algorithm.

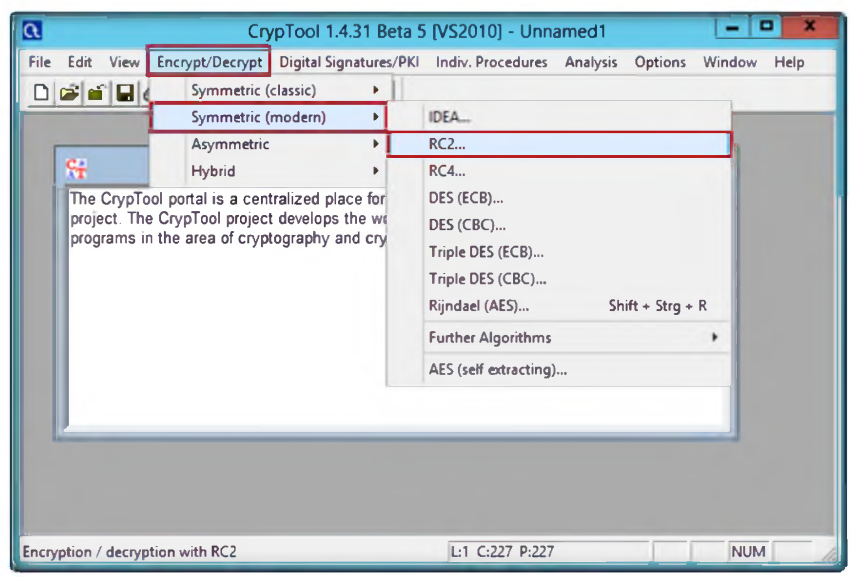


FIGURE 5.6: Select the RC2 Encrypt algorithm

9. In the **Key Entry: RC2** wizard, select **Key length** from the drop-down list
10. Enter the key using hexadecimal characters and click **Encrypt**.

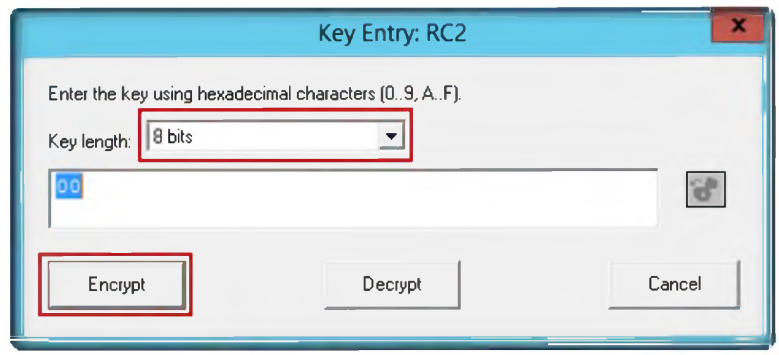


FIGURE 5.7: Selecting Key Length in the hexadecimal character

11. RC2 encryption of Unnamed1 notepad will appear as shown in the following figure.

CrypTool includes every state-of-the-art cryptographic function and allows you to learn and use cryptography within the same environment.

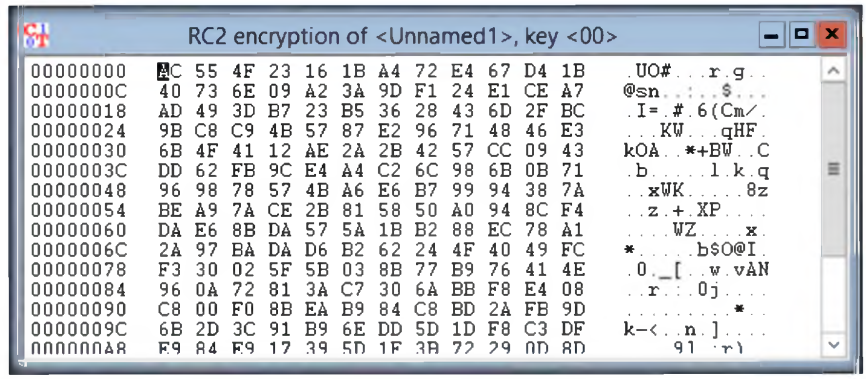


FIGURE 5.8: Output of RC2 encrypted data

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
CrypTool	**Encrypted Algorithm:** RC2
	Result: Encrypted data for selected text

Questions

1. What are the alternatives to CrypTool for encrypting data?
2. How can you differentiate between encrypting data in CrypTool and other encrypting tools?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 6

Encrypting and Decrypting Data Using BCTextEncoder

BCTextEncoder simplifies encoding and decoding text data. Plaintext data is compressed, encrypted, and converted to text format, which can then be easily copied to the clipboard or saved as a text file.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In order to be an **expert ethical hacker** and **penetration tester**, you must have knowledge of cryptography functions.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

- Use encode/decode text data encrypted with a password

Lab Environment

To carry out the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

- **BCTextEncoder** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Cryptography Tools\BCTextEncoder**
- You can also download the latest version of **BCTextEncoder** from the link http://www.jetico.com/encryption-bctextencoder/
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Run this tool on **Windows Server 2012** host machine
- Administrative privileges to run the tool

Lab Duration

Time: 10 Minutes

Overview of BCTextEncoder

BCTextEncoder uses **public key encryption** methods as well as password-based encryption. This utility software uses strong and approved **symmetric** and **public key** algorithms for data encryption.

Lab Tasks

TASK 1

Encrypting the Data

1. Double-click the **BCTextEncoder.exe** file. The main window of BCTextEncoder appears, as displayed in the following figure.

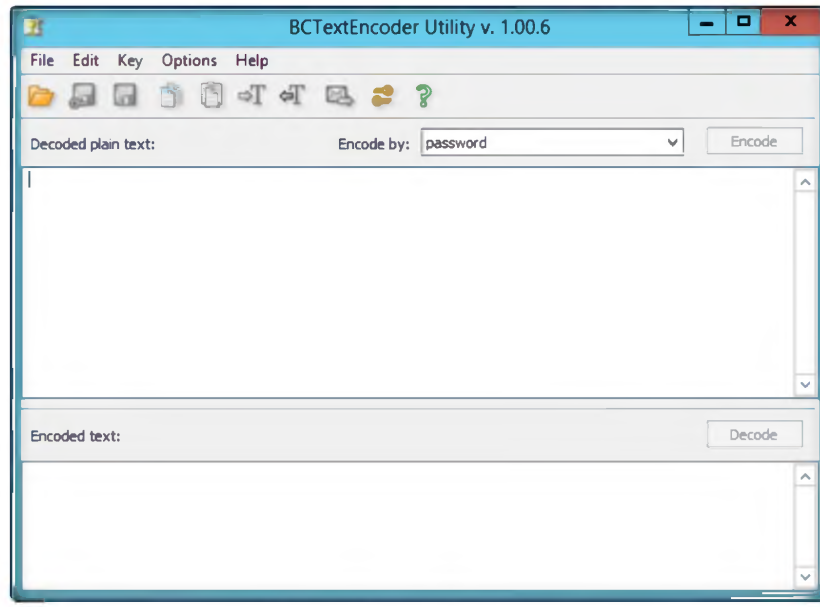


FIGURE 6.1: Main window of BCTextEncoder

2. To encrypt the text, type the text in **Clipboard** (OR) select the secret data and put it to clipboard with **Ctrl+V**.

You can also download BCTextEncoder from http://www.jetico.com

BCTextEncoder utilizes the following encryption algorithms:

- ZLIB compression algorithm
- AES (Rijndael) encryption algorithm for password based encryption
- RSA asymmetric encryption algorithm for public key encryption

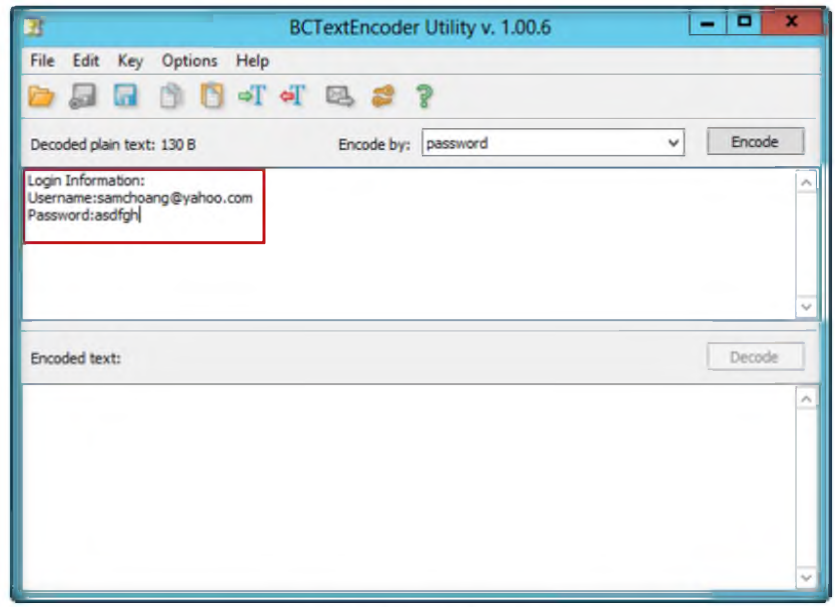


FIGURE 6.2: Secret information in clipboard

3. Click **Encode**. The **Enter Password** window will appear. Set the password and confirm the same password in the respective fields.
4. Click **OK**.

BCTextEncoder is intended for fast encoding and decoding text data

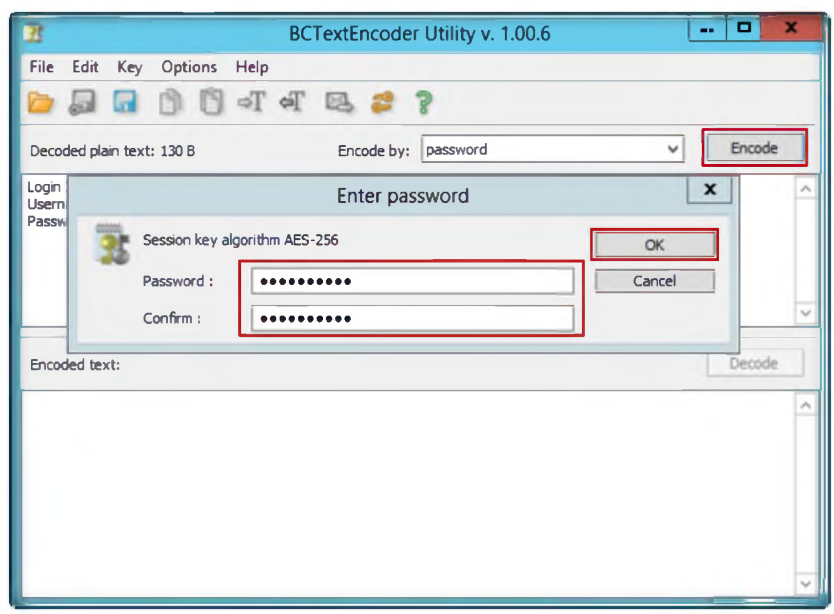


FIGURE 6.3: Set the password for encryption

5. The encoded text appears, as show in the following figure.

The main advantage of BCTextEncoder is support of public key encryption.

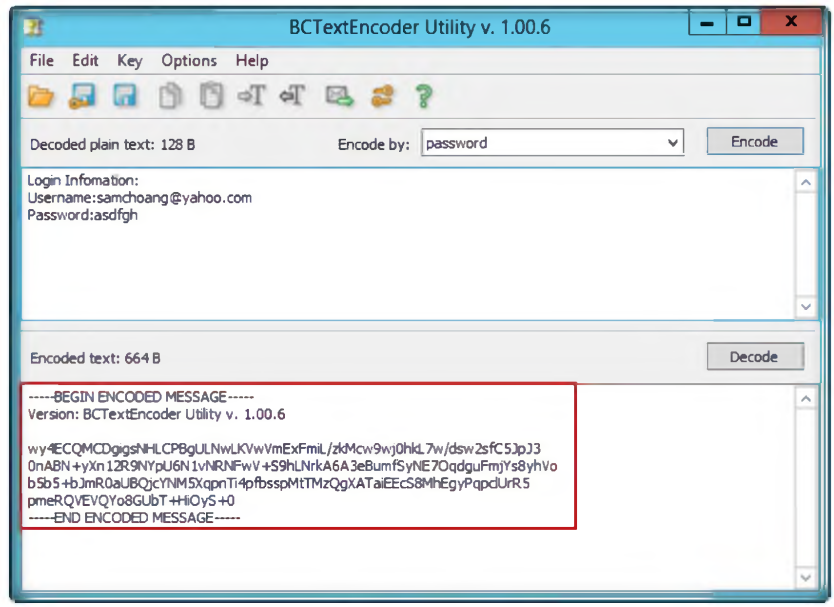


FIGURE 6.4: Encoded text

TASK 2

Decrypting the Data

6. To decrypt the data, you first clean the **Decoded plain text** clipboard.
7. Click the **Decode** button

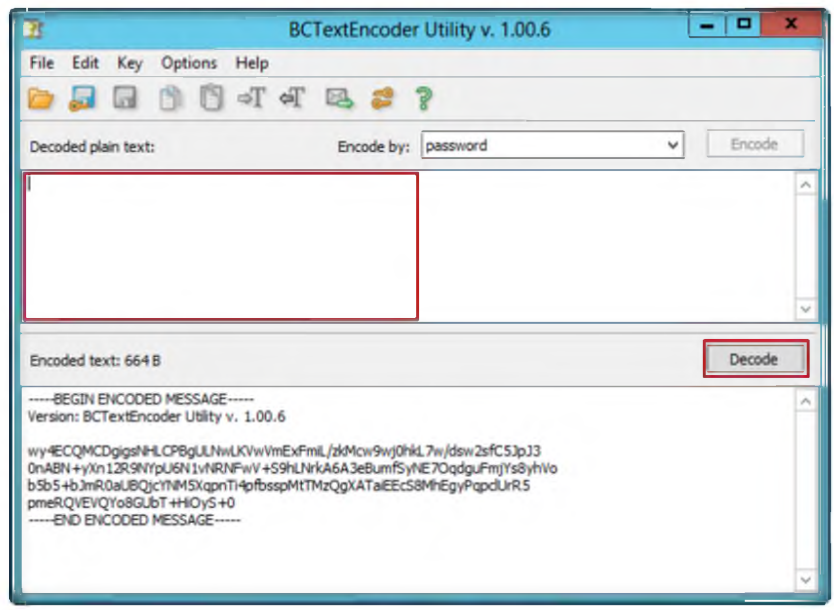


FIGURE 6.5: Decoding the data

8. **The Enter password for encoding text** widow will appear. Enter the password in the **Password** field, and click **OK**.

BCArchive includes the BC Key Manager utility to manage your own public/secret key pair as well as public keys you have received from other people

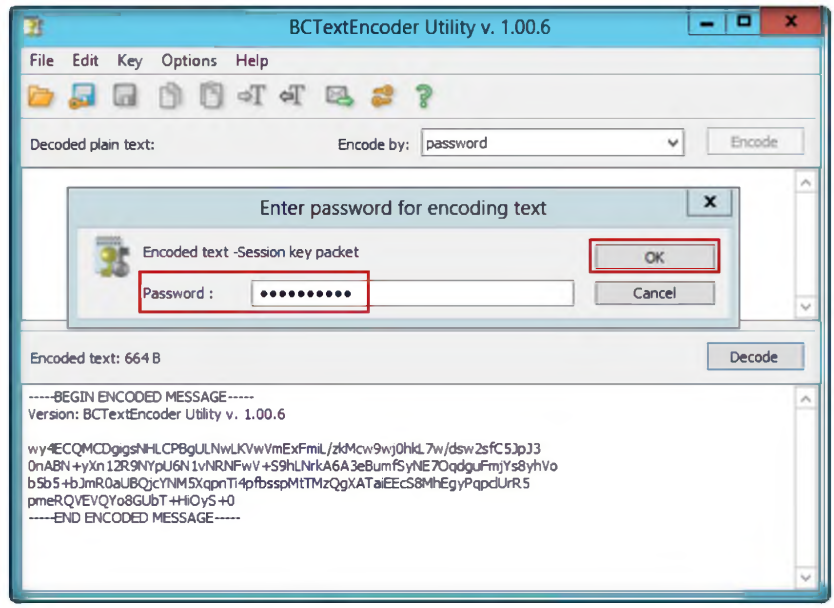


FIGURE 6.6: Enter the password for decoding

9. Decoded plaintext appears as shown in the following figure.

BCTextEncoder not only encrypts, but also compresses the data

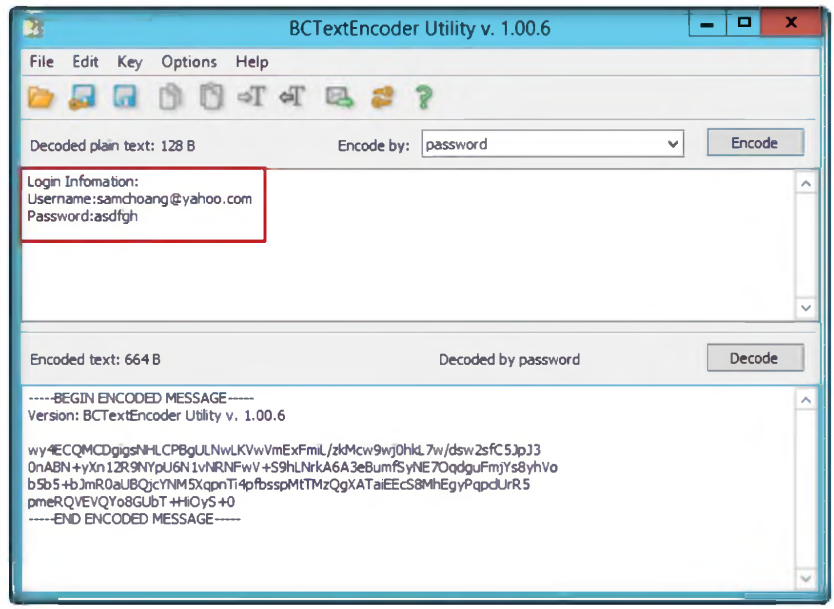


FIGURE 6.7: Output decoded text

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
BCTText Encoder	**Result:** Encoding and Decoding text for selected data

Questions

1. How can you differentiate between encrypting or decrypting the data in BCTextEncoder and other encrypting tools?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 7

Basic Data Encrypting Using Rohos Disk Encryption

The Rohos Disk Encryption- program creates hidden and protected partitions on the computer or USB flash drive and password protects/ locks access to your Internet applications.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Today's web browsers automatically encrypt text when making a connection to a secure server. This prevents intruders from listening in on private communications. Even if they are able to capture the message, encryption allows them to only view scrambled text or what many call unreadable gibberish. Upon arrival, the data is decrypted, allowing the intended recipient to view the message in its original form. In order to be an expert ethical hacker and penetration tester, you must have knowledge of cryptography functions.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

- Use encrypting/decrypting commands
- Create a virtual encrypted disk with a file

Lab Environment

To carry out the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

- **Rohos Disk Encryption** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Disk Encryption Tools\Rohos Disk Encryption**
- You can also download the latest version of **Rohos Disk Encryption** from the link http://www.rohos.com/products/rohos-disk-encryption/
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Follow the **wizard-driven installation** instructions

- Run this tool on **Windows Server 2012** host machine
- Administrative privileges to run the tool

Lab Duration

Time: 10 Minutes

Overview of Rohos Disk Encryption

Rohos Disk Encryption creates **hidden** and **password** protected partitions on the computer or **USB flash** drive with megabytes of sensitive files and private data on your computer or USB drive. Rohos Disk uses **NIST**-approved **AES** encryption algorithm, and **256** bit encryption key length. Encryption is automatic and on-the-fly.

Lab Tasks

TASK 1

Installation of Rohos Disk Encryption

1. To install Rohos Disk Encryption, navigate to **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Disk Encryption Tools\Rohos Disk Encryption**.
2. Double-click the **rohos.exe** file/ Select the language **English** and click **OK**.

FIGURE 7.1: Select the Language

You can also download Rohos from http://www.rohos.com

3. The **Setup** window appears. Read the instruction and click **Next**.

Portable Rohos Disk Browser allows to use encrypted partition on any PC without Admin rights, without install.

FIGURE 7.2: Rohos setup wizard

4. The **Licence Agreement** window will appear. Read the agreement carefully and select the **I accept the agreement** radio button
5. Click **Next**.

Encryption is automatic and on-the-fly. AES 256 bit key length. Using NIST compliant encryption standards

FIGURE 7.3: License agreement window

6. Click **Next**.

File Virtualization: prevents secret data leak outside encrypted disk on TEMP folders, Registry, Recent documents list, etc.

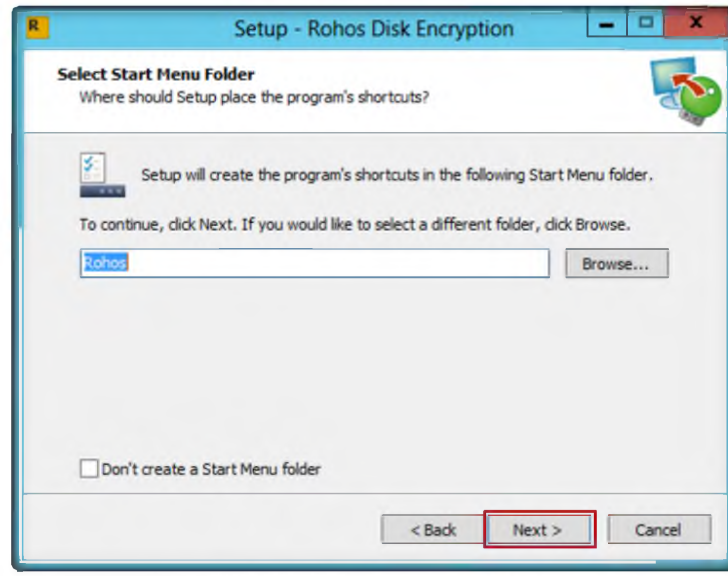


FIGURE 7.4: Select the destination folder

7. Check the **Create a desktop icon** check box, and click **Next**.

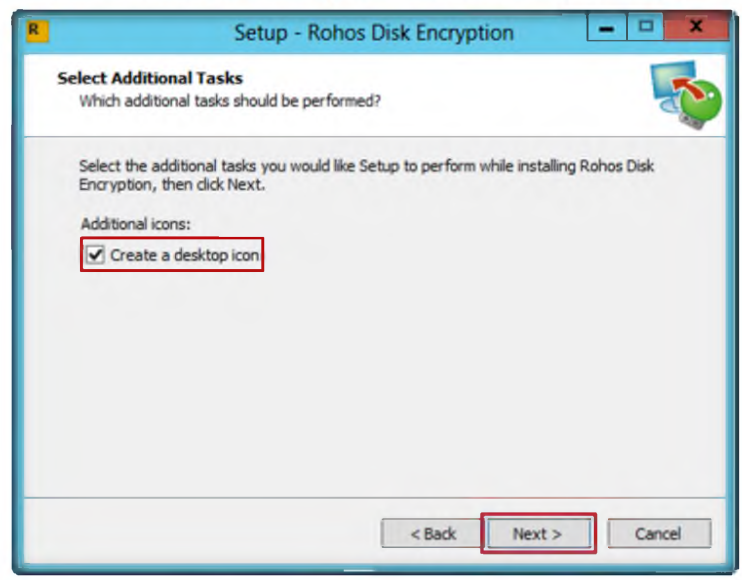


FIGURE 7.5: creating Rohos desktop icon

Any file or folder can be easily moved into Encrypted Rohos Disk with shredding afterwards.

8. Click **Install**. Rohos Disk Encryption is ready to install.

Secured virtual keyboard - protect encrypted disk password from a keylogger

FIGURE 7.6: Rohos disk encryption installation

9. Click **Finish**.

FIGURE 7.7: Complete installation of Rohos disk encryption

TASK 2

Disk Encryption

10. The **Rohos Get Ready Wizard** window will appear. Specify the password to access the disk in the respective field.
11. Click **Next**.
12. Alternatively, you can also launch the program from the **Start** menu apps of Windows Server 2012.

Rohos disk uses NIST approved AES encryption algorithm, 256 bit encryption key length.

FIGURE 7.8: Select password for access disk

13. The **Setup USB Key** window appears. Read the information, and click **Next**.

Rohos cares about usability: Your first Encrypted Drive can be turned on with a single click or automatically on system startup.

FIGURE 7.9: Select USB key device

14. The **Rohos Updates** window appears. Click **Finish**.

Partition password reset option allows creating a backup file to access your secured disk if you forgot your password or lost USB key.

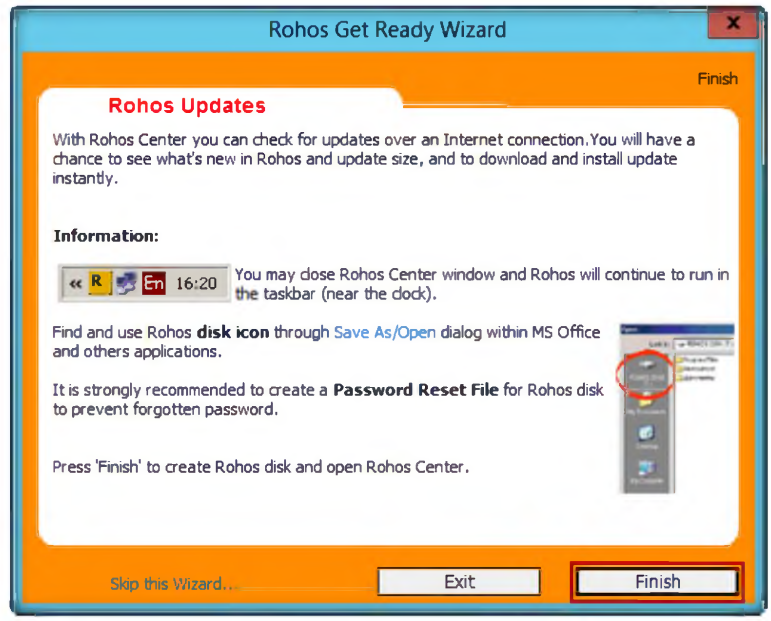


FIGURE 7.10: Rohos disk encryption update window

15. The encrypted disk is created successfully, as shown in following figure.

This option brings affordable and AES 256 strength encryption solution to improve security issues by preventing unauthorized access to your Internet apps, such as Google Chrome, Firefox

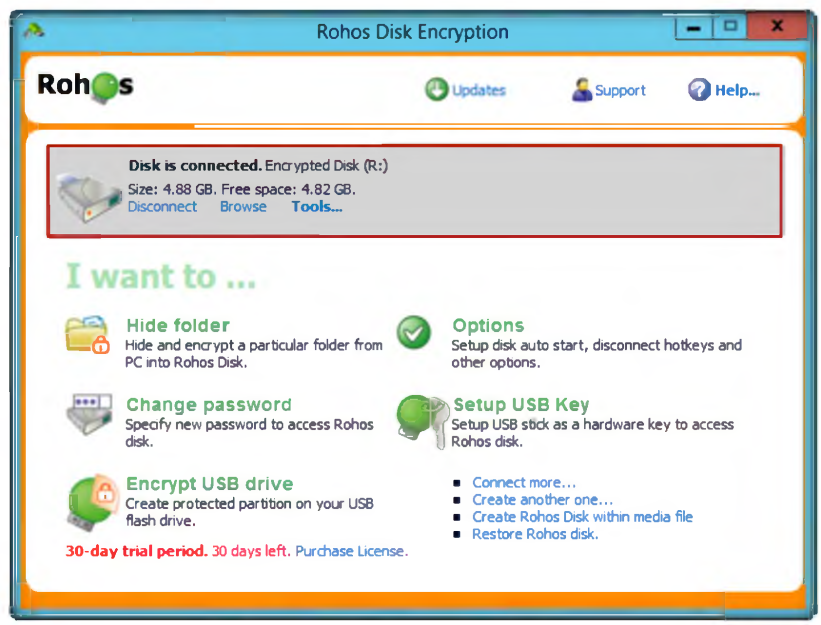


FIGURE 7.11: Successful creation of encrypted disk

16. To decrypt the disk, click **Disconnect**.

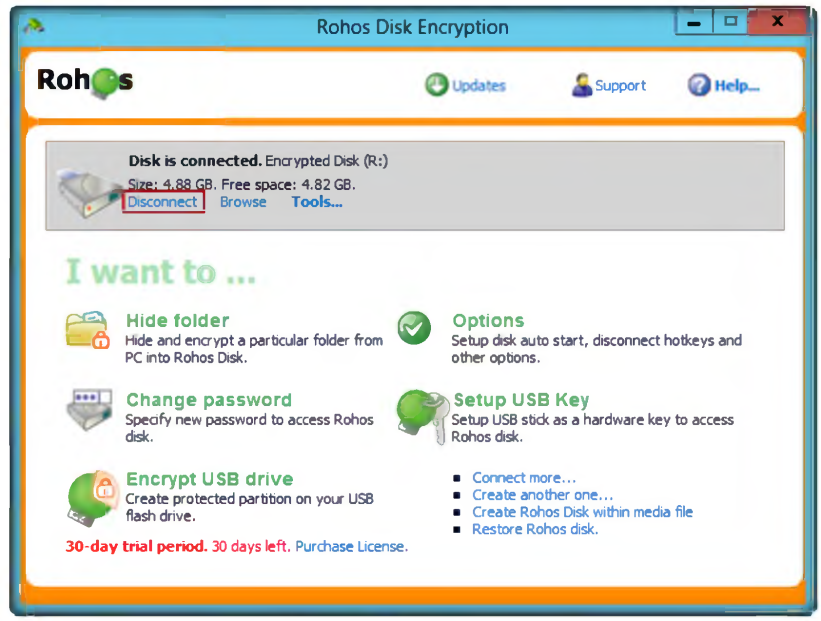


FIGURE 7.12: Decrypt the disk

You can open or Save your protected documents right from MS Word (Excel) by clicking on the personal disk icon.

17. After decrypting the disk, it will be displayed, as shown in the following figure.

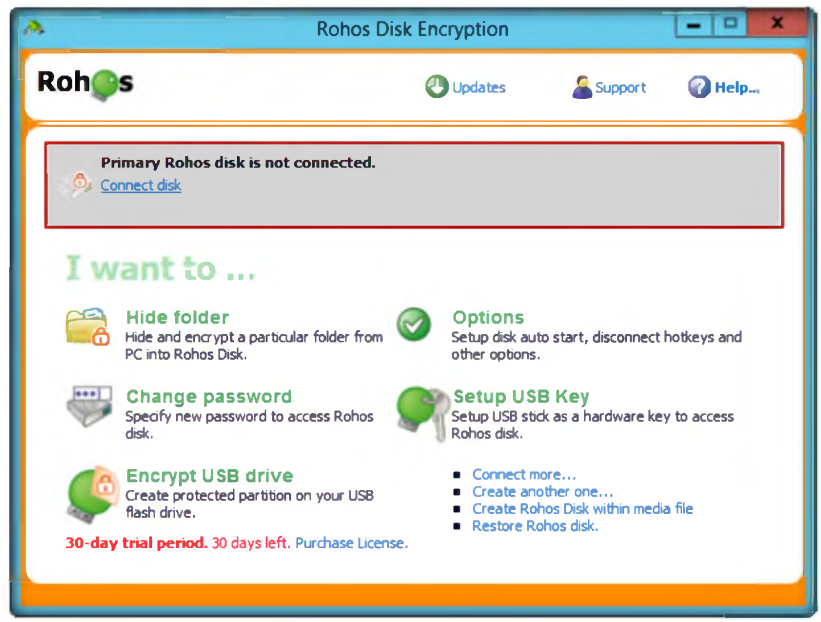


FIGURE 7.13: Decrypt the disk

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Rohos Disk Encryption	**Result:** Successful connection of encrypted disk

Questions

1. Determine whether there is any way to recover the files from Rohos Disk Encryption if you forget the volume password.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs