- Group policies:

  ```
  aws iam list-group-policies
  ```

- Create user:

  ```
  aws iam create-user
  ```

22. This concludes the demonstration of escalating IAM user privileges by exploiting a misconfigured user policy.
23. Close all open windows and document all the acquired information.
24. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all the results obtained in the lab exercise.

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

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

Cryptography

Module 20

Cryptography

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

ICON KEY

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

Lab Scenario

With the increasing adoption of the Internet for business and personal communication, securing sensitive information such as credit-card and personal identification numbers (PINs), bank account numbers, and private messages is becoming increasingly important, and yet, more difficult to achieve. Today's information-based organizations extensively use the Internet for e-commerce, market research, customer support, and a variety of other activities. Thus, data security is critical to online businesses and privacy of communication.

Cryptography and cryptographic ("crypto") systems help in securing data from interception and compromise during online transmissions. Cryptography enables one to secure transactions, communications, and other processes performed in the electronic world, and is additionally used to protect confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, etc.

As an ethical hacker or penetration tester, you should suggest to your client proper encryption techniques to protect data, both in storage and during transmission. The labs in this module demonstrate the use of encryption to protect information systems in organizations.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv10 Module 20 Cryptography

Lab Objectives

The objective of the lab is to use encryption to conceal data and perform other tasks that include, but is not limited to:

- Generate hashes and checksum files
- Calculate the encrypted value of the selected file
- Use encrypting/decrypting techniques
- Perform file and data encryption
- Create self-signed certificates
- Perform email encryption
- Perform disk encryption
- Perform cryptanalysis

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 110 Minutes

Overview of Cryptography

"Cryptography" comes from the Greek words ***kryptos***, meaning "concealed, hidden, veiled, secret, or mysterious," and ***graphia***, "writing"; thus, cryptography is "the art of secret writing."

Cryptography is the practice of concealing information by converting plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme: it is the process of the conversion of data into a scrambled code that is sent across a private or public network.

There are two types of cryptography, determined by the number of keys employed for encryption and decryption:

- **Symmetric Encryption**: Symmetric encryption (secret-key, shared-key, and private-key) uses the same key for encryption as it does for decryption
- **Asymmetric Encryption**: Asymmetric encryption (public-key) uses different encryption keys for encryption and decryption; these keys are known as public and private keys

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform cryptography to protect confidential data. Recommended labs that will assist you in learning various cryptography techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Encrypt the Information using Various Cryptography Tools	√	√	√
	1.1 Calculate One-way Hashes using HashCalc	√		√
	1.2 Calculate MD5 Hashes using MD5 Calculator		√	√
	1.3 Calculate MD5 Hashes using HashMyFiles		√	√
	1.4 Perform File and Text Message Encryption using CryptoForge	√		√

	1.5 Perform File Encryption using Advanced Encryption Package		√	
	1.6 Encrypt and Decrypt Data using BCTextEncoder		√	√
2	Create a Self-Signed Certificate	√		√
	2.1 Create and Use Self-signed Certificates	√		√
3	Perform Email Encryption		√	√
	3.1 Perform Email Encryption using Rmail		√	√
4	Perform Disk Encryption	√	√	√
	4.1 Perform Disk Encryption using VeraCrypt	√		√
	4.2 Perform Disk Encryption using BitLocker Drive Encryption		√	√
	4.3 Perform Disk Encryption using Rohos Disk Encryption		√	√
5	Perform Cryptanalysis using Various Cryptanalysis Tools		√	√
	5.1 Perform Cryptanalysis using CrypTool		√	√
	5.2 Perform Cryptanalysis using AlphaPeeler		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

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

Encrypt the Information using Various Cryptography Tools

Cryptography is used to encrypt sensitive data to protect it from unauthorized access by any party other than the person for whom it is intended.

ICON KEY

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

Lab Scenario

As a professional ethical hacker and penetration tester, you should use various cryptography techniques or tools to protect confidential data against unauthorized access. Cryptography protects confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, and many other kinds of communication. Encrypted messages can at times be decrypted by cryptanalysis (code breaking), although modern encryption techniques are virtually unbreakable.

The labs in this exercise demonstrate how you can use various cryptography tools to encrypt important information in the system.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

Lab Objectives

- Calculate one-way hashes using HashCalc
- Calculate MD5 hashes using MD5 Calculator
- Calculate MD5 hashes using HashMyFiles
- Perform file and text message encryption using CryptoForge
- Perform file encryption using advanced encryption package
- Encrypt and decrypt data using BCTextEncoder

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection

- Administrator privileges to run the tools
- HashCalc located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashCalc**
- MD5 Calculator located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\MD5 Calculator**
- HashMyFiles located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles**
- CryptoForge located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**
- Advanced Encryption Package located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package**
- BCTextEncoder located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\BCTextEncoder**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest versions, the screenshots shown in the lab might differ.

Lab Duration

Time: 35 Minutes

Overview of Cryptography Tools

System administrators use cryptography tools to encrypt system data within their network to prevent attackers from modifying the data or misusing it in other ways. Cryptography tools can also be used to calculate or decrypt hash functions available in MD4, MD5, SHA-1, SHA-256, etc.

Cryptography tools are used to convert the information present in plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme. The converted data are in the form of a scrambled code that is encrypted and sent across a private or public network.

Lab Tasks

TASK 1

Calculate One-way Hashes using HashCalc

Here, we will use the HashCalc tool to calculate one-way hashes.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Install & Launch HashCalc Tool

2. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashCalc** and double click **setup.exe**.

Note: If the **User Account Control** pop-up appears, click **Yes**.

3. **Setup - HashCalc** window appears, click **Next**.

Hash functions calculate a unique fixed-size bit string representation, called a message digest, of any arbitrary block of information. Message digest (One-way Hash) functions distill the information contained in a file (small or large) into a single fixed-length number, typically between 128 and 256 bits. If any given bit of the function's input is changed, every output bit has a 50% chance of changing. Given an input file and its corresponding message digest, it should be nearly impossible to find another file with the same message digest value, as it is computationally infeasible to have two files with the same message digest value.

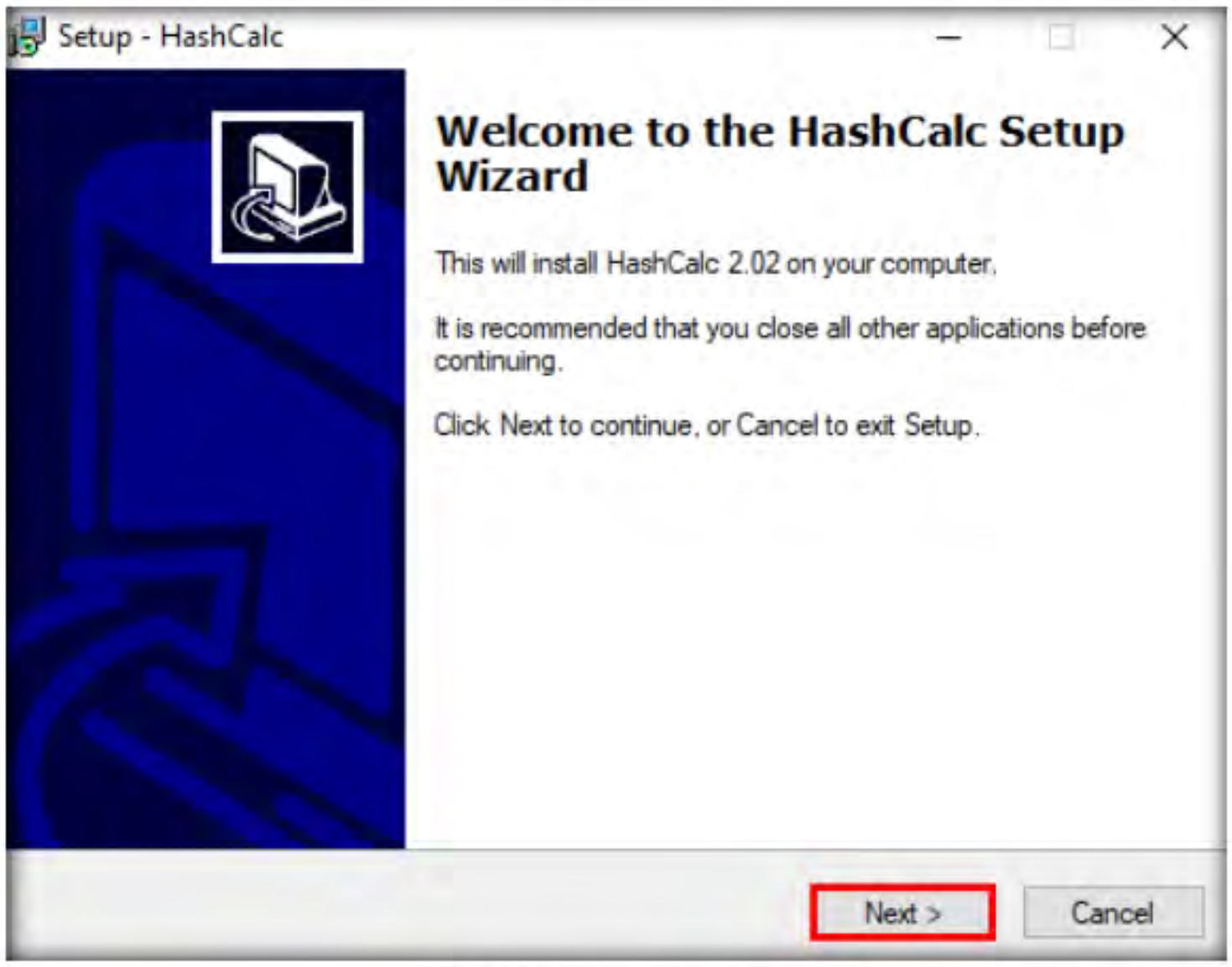


Figure 1.1.1: Setup - HashCalc window

4. Follow the installation wizard to install **HashCalc** using all default settings.
5. After the completion of the installation, **Completing the HashCalc Setup Wizard** appears. Uncheck the **View the README file** checkbox and click **Finish**.

HashCalc enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It supports the Secure Hash Algorithm family: MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, and the hash used in the peer-to-peer file sharing applications, eDonkey and eMule.

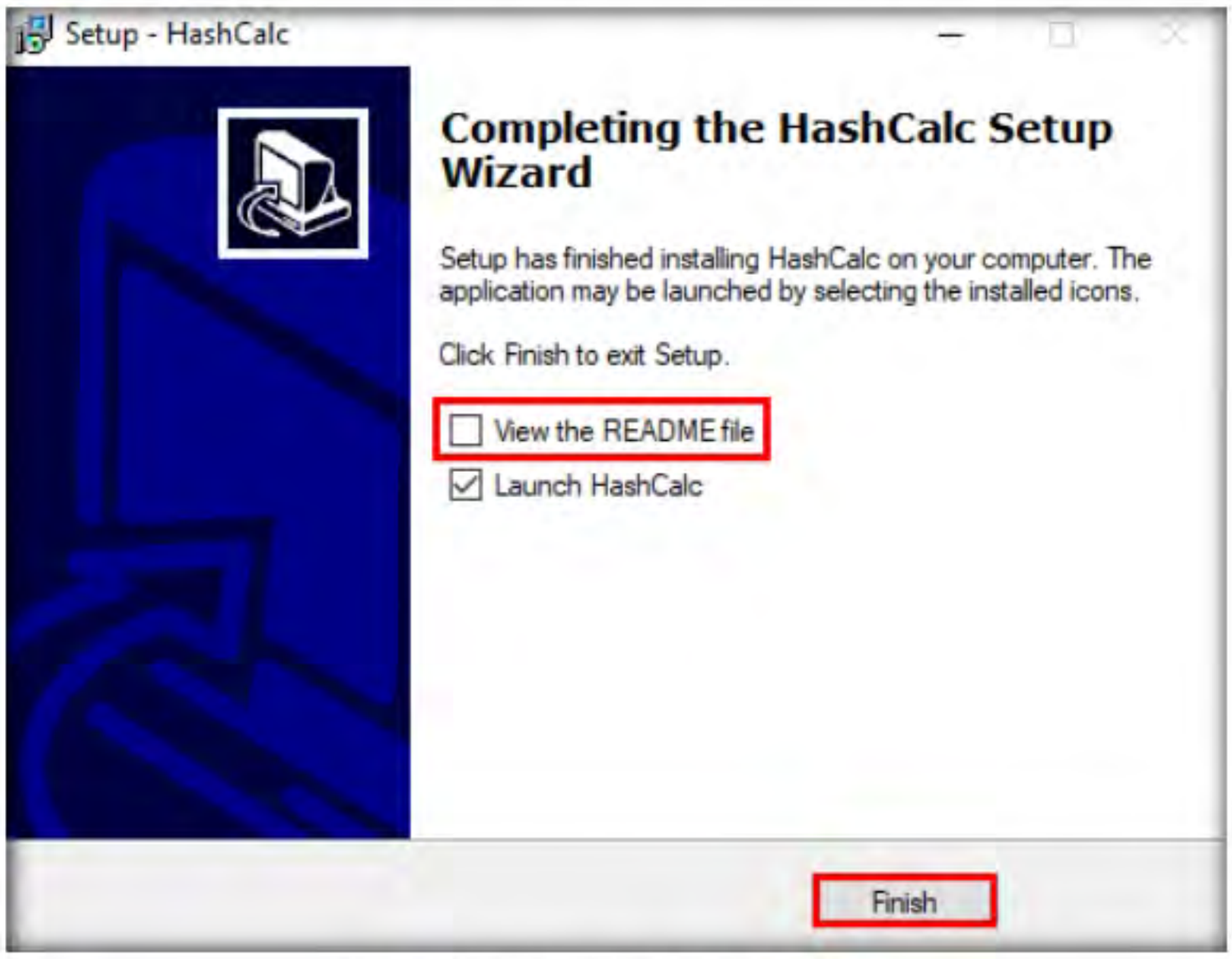


Figure 1.1.2: Setup: Completing HashCalc installation

6. The **HashCalc** main window appears, as shown in the screenshot.

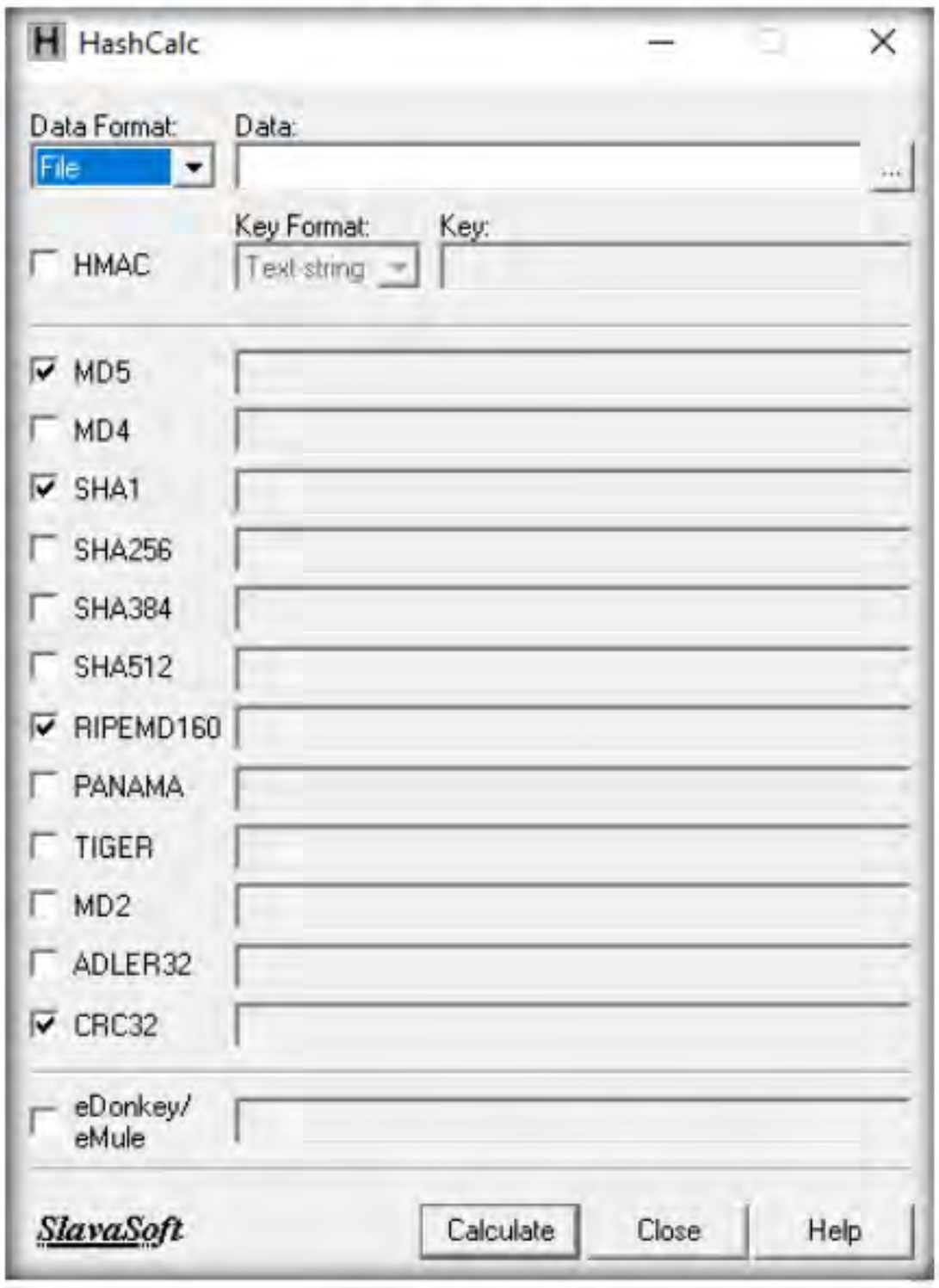


Figure 1.1.3: HashCalc Window

7. Minimize the **HashCalc** window. Navigate to **Desktop**, right-click on the **Desktop** window, and navigate to **New → Text Document** to create a new text file.

Note: You can create a text file at any location of your choice.

8. A newly created text file appears; rename it to **Test.txt** and open it. Write some text in it (here, **Hello World !!**) and press **Ctrl+S** to save the file. Close the text file.

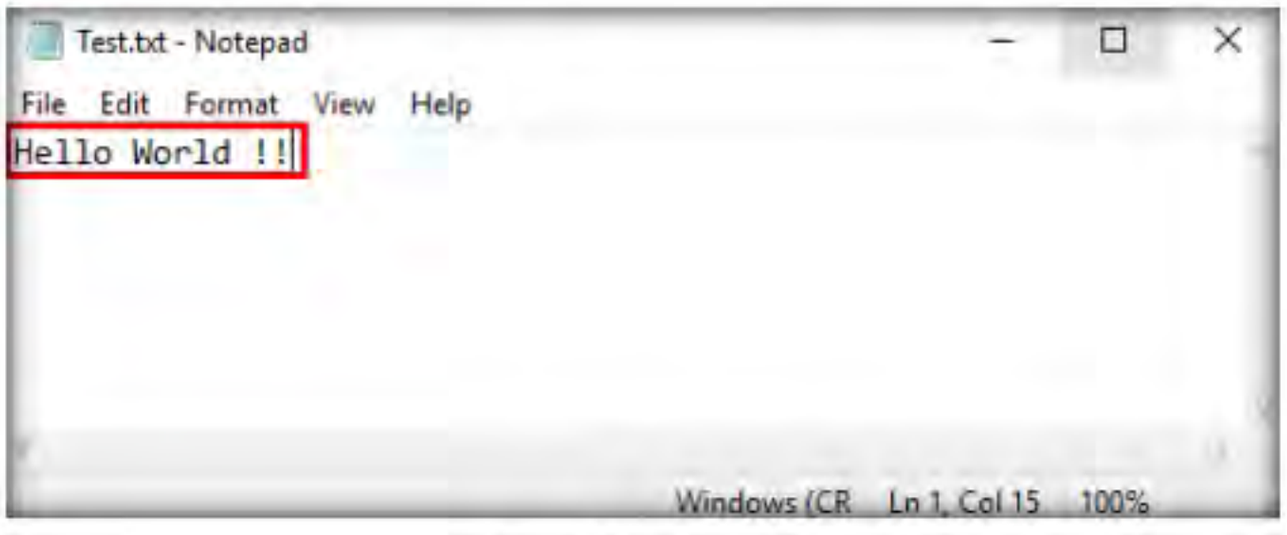


Figure 1.1.4: Test.txt file

TASK 1.2

Calculate Hash Values of a File

9. Now, switch back to the **HashCalc** window; ensure that the **File** option is selected in the **Data Format** field and click ellipsis icon ( ) under the **Data** filed.

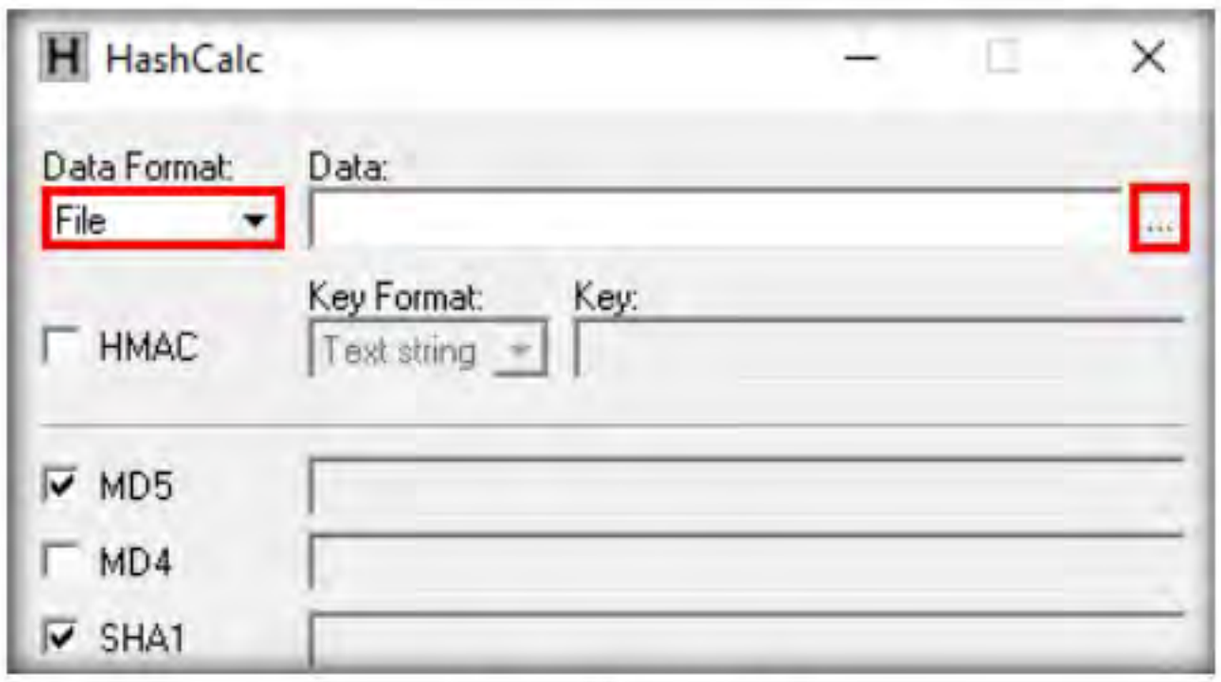


Figure 1.1.5: Open a text file

10. The **Find** window appears, navigate to the location where you saved the **Test.txt** file (here, **Desktop**) and click **Open**.

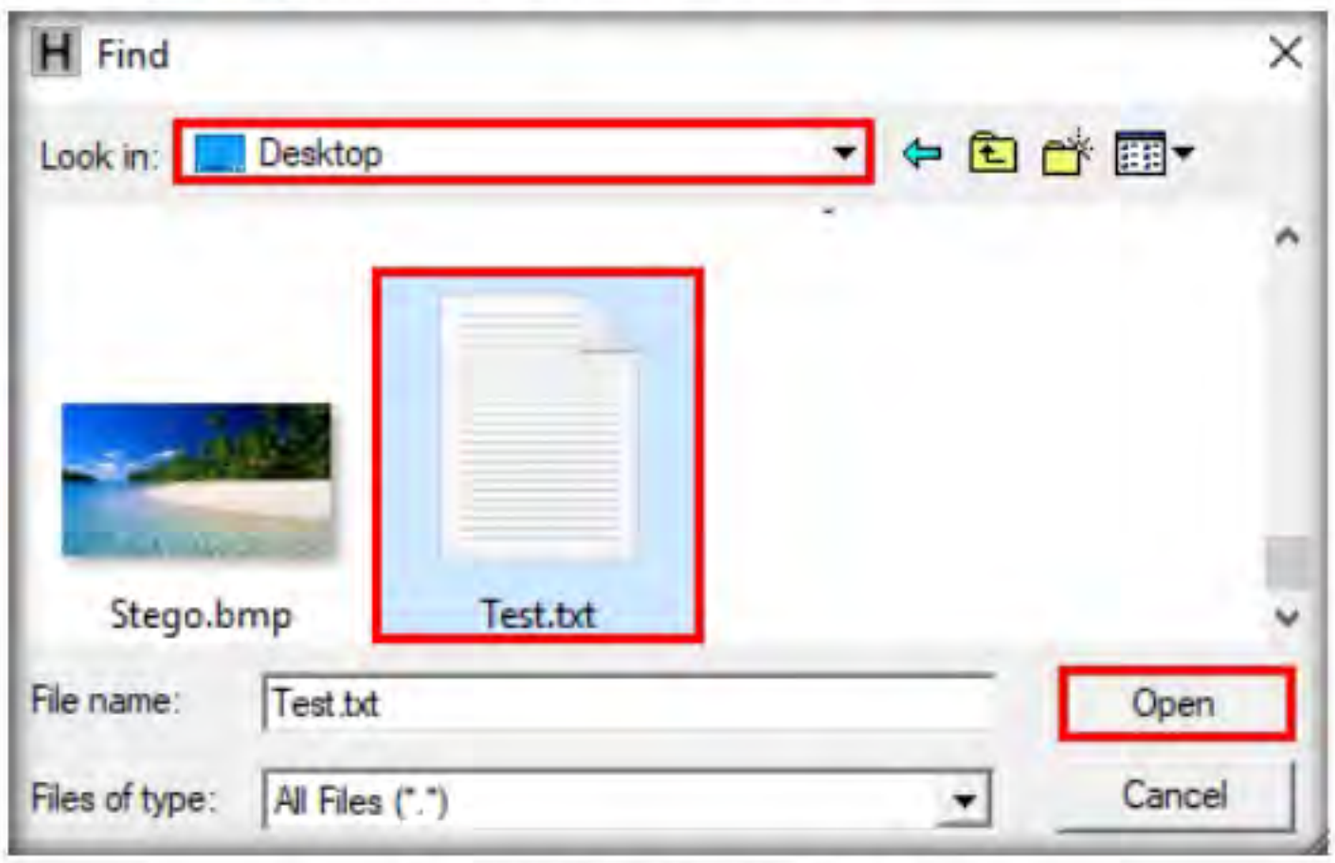


Figure 1.1.6: Find window: select Test.txt file

11. The path of the selected file (**Test.txt**) appears under the **Data** field. Ensure that the **MD5**, **SHA1**, **RIPEMD160**, and **CRC32** hash functions are selected. Click the **Calculate** button.

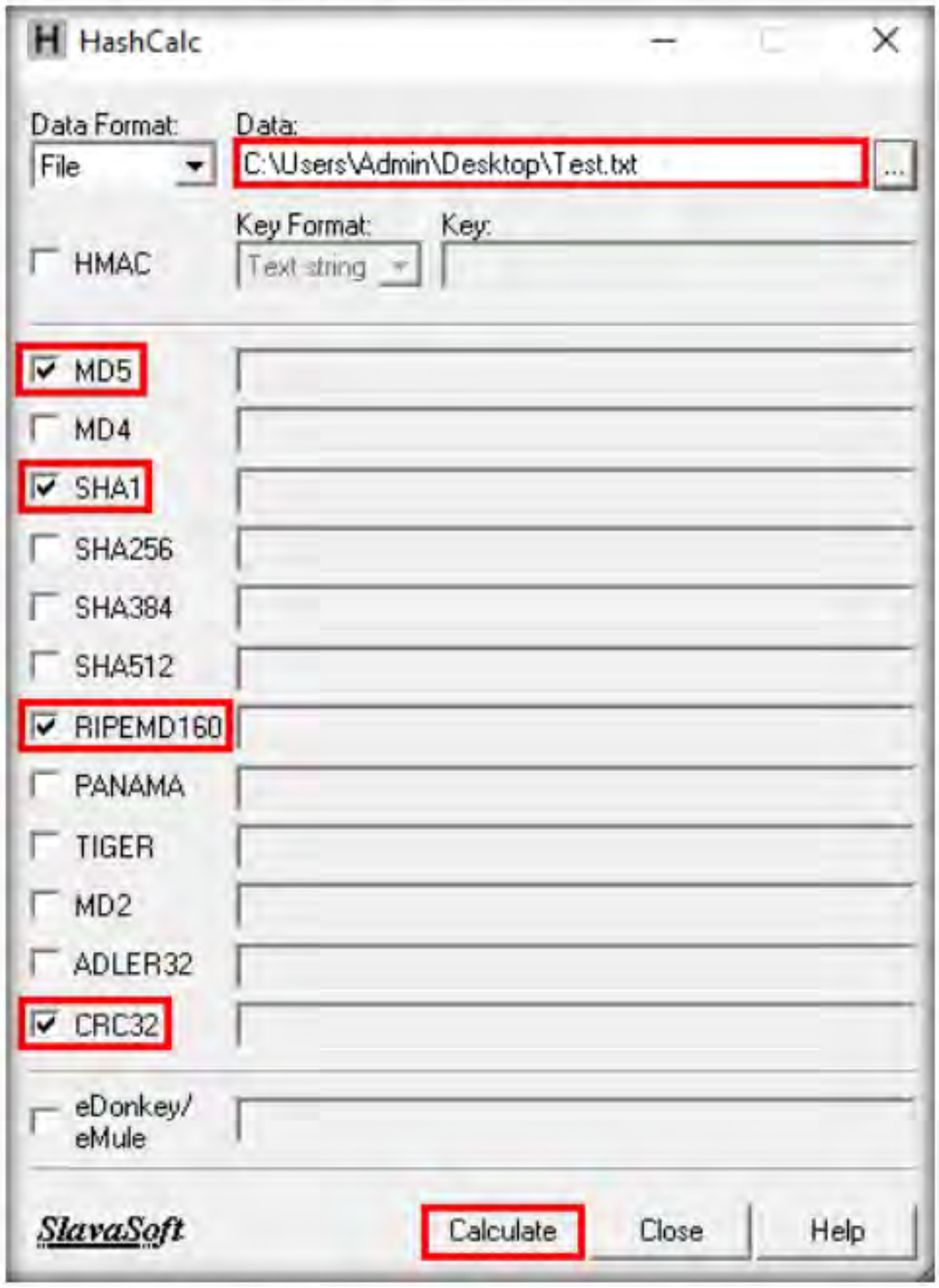


Figure 1.1.7: Calculate hash values of Test.txt file

12. The calculated hash values of the **Test.txt** file appears, as shown in the screenshot.

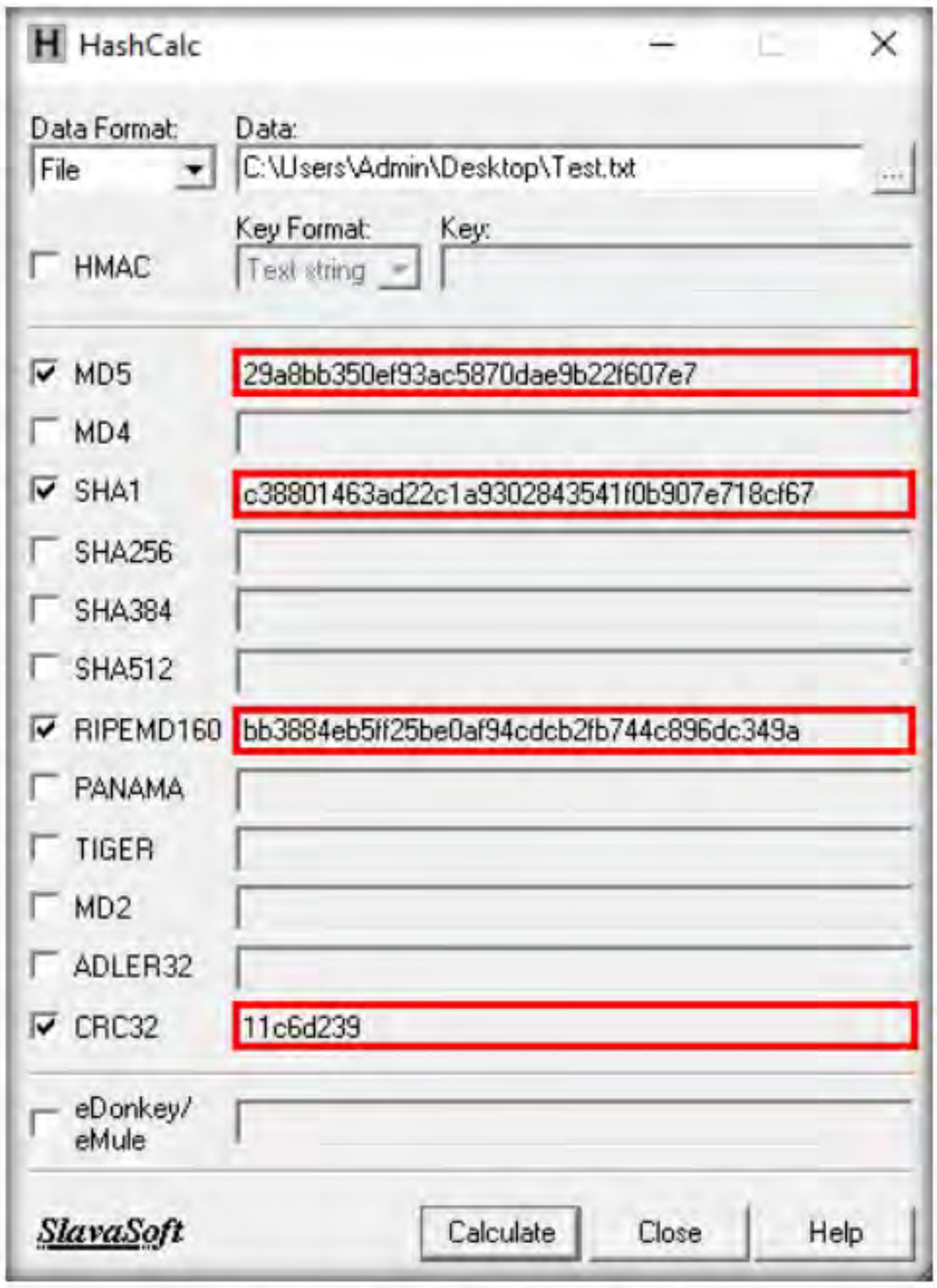


Figure 1.1.8: Calculated hash values of Test.txt file

TASK 1.3

Modify File Content

13. Minimize the **HashCalc** window, navigate to **Desktop**, and double-click the **Test.txt** file to open it. Modify the file content by writing some text (here, **Modified File ...!!!**) and press **Ctrl+S** to save it. Close the text file.

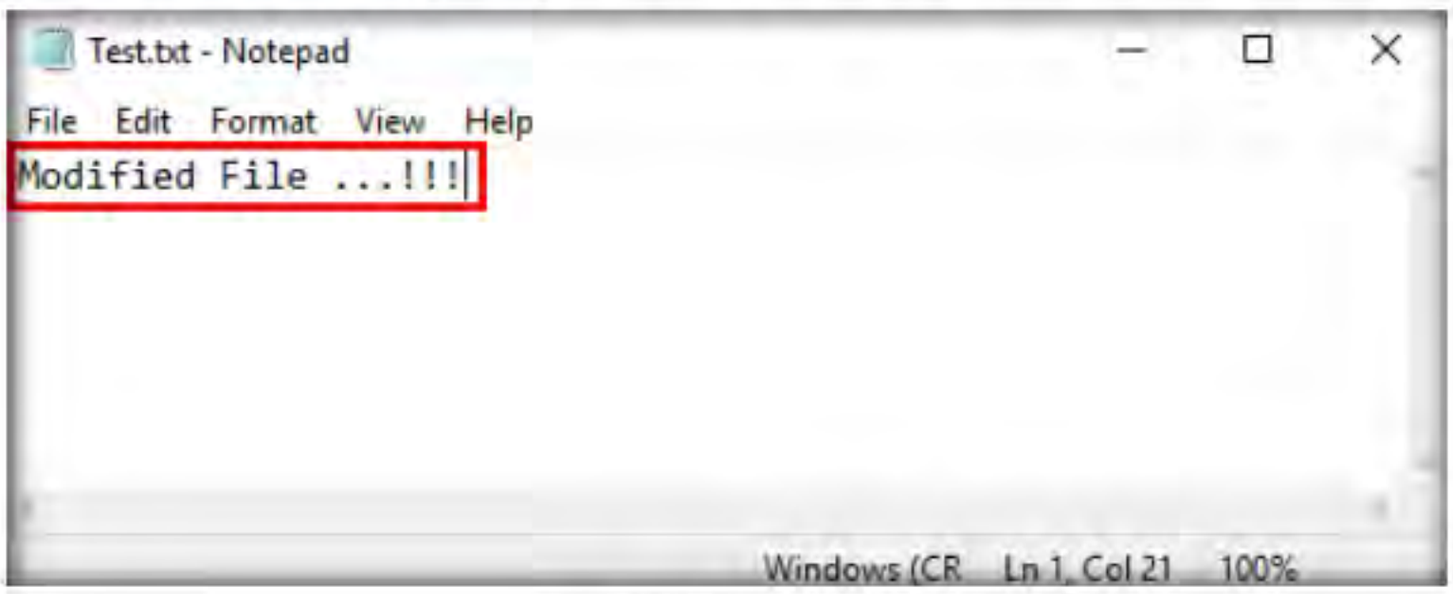


Figure 1.1.9: Modify text content

TASK 1.4

Compare Hash Values of Original and Modified File

14. Now, double-click **HashCalc** shortcut from **Desktop** to launch another HashCalc window.
15. A new **HashCalc** window appears, perform **Steps #9-12**.
16. Now, maximize the first **HashCalc** window and place it beside the second **HashCalc** window. You can observe changes in the hash values of the text file (**Test.txt**) before and after the modification, as shown in the screenshot.

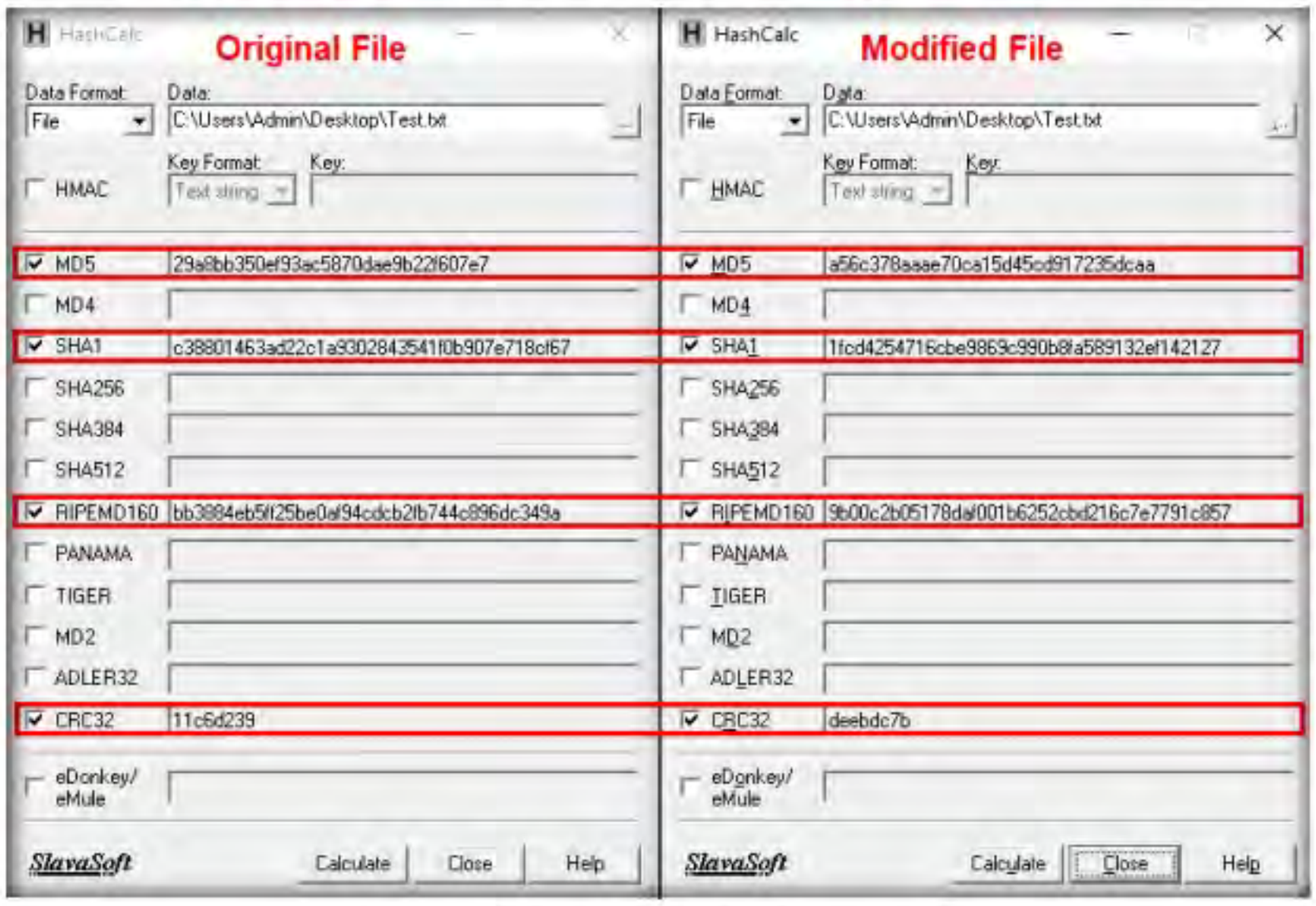


Figure 1.1.10: Difference in Hash values of the same text file

Note: In real-time, the HashCalc tool is used to check the integrity of a file where the changes in the hash values indicate that the file content has been modified.

17. This concludes the demonstration of calculating one-way hashes using HashCalc.
18. Close all open windows and document all the acquired information.

TASK 2

Calculate MD5 Hashes using MD5 Calculator

Here, we will use the MD5 Calculator tool to calculate MD5 hashes.

TASK 2.1

Install MD5 Calculator Tool

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\MD5 Calculator** and double-click **md5calc(1.0.0.0).msi**.
2. The **MD5 Calculator** setup window appears; click **Next**.

MD2, MD4, MD5, and MD6 are message digest algorithms used in digital signature applications to compress documents securely before the system signs it with a private key. The algorithms can be of variable length, but the resulting message digest is always 128 bits.

The MD5 algorithm is a widely used cryptographic hash function that takes a message of arbitrary length as input and outputs a 128-bit (16-byte) fingerprint or message digest of the input. The MD5 algorithm is used in a wide variety of cryptographic applications and is useful for digital signature applications, file integrity checking, and storing passwords.

MD5 Calculator is a simple application that calculates the MD5 hash of a given file, and it can be used with large files (e.g., multiple gigabytes). It features a progress counter and a text field from which the final MD5 hash can be easily copied to the clipboard. MD5 calculator can be used to check the integrity of a file.

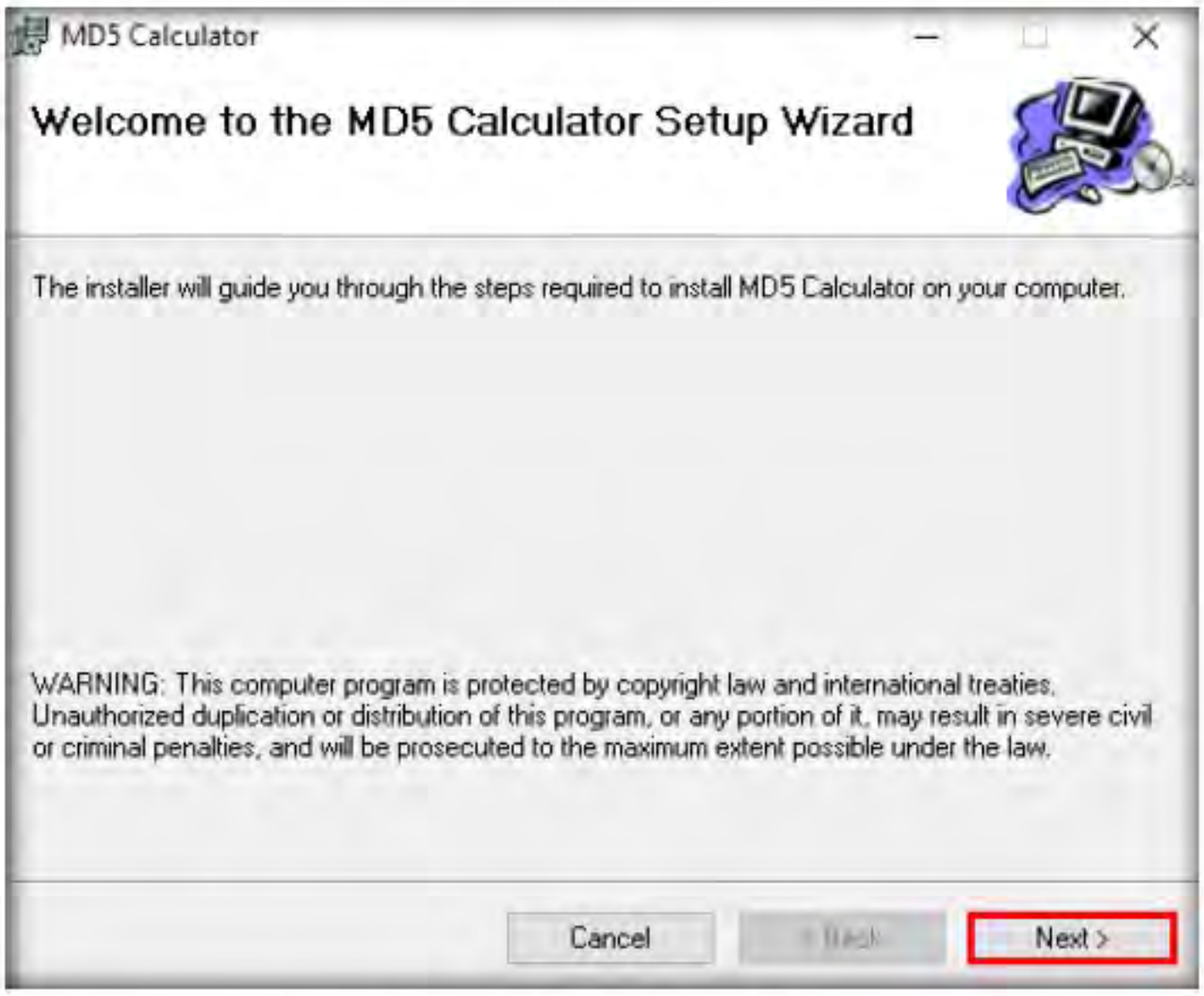


Figure 1.2.1: MD5 Calculator Window

3. Follow the installation wizard to install the **MD5 Calculator** using all default settings.

Note: If a **User Account Control** pop-up appears, click **Yes**.

4. After the completion of the installation, the **Installation Complete** wizard appears; click **Close**.

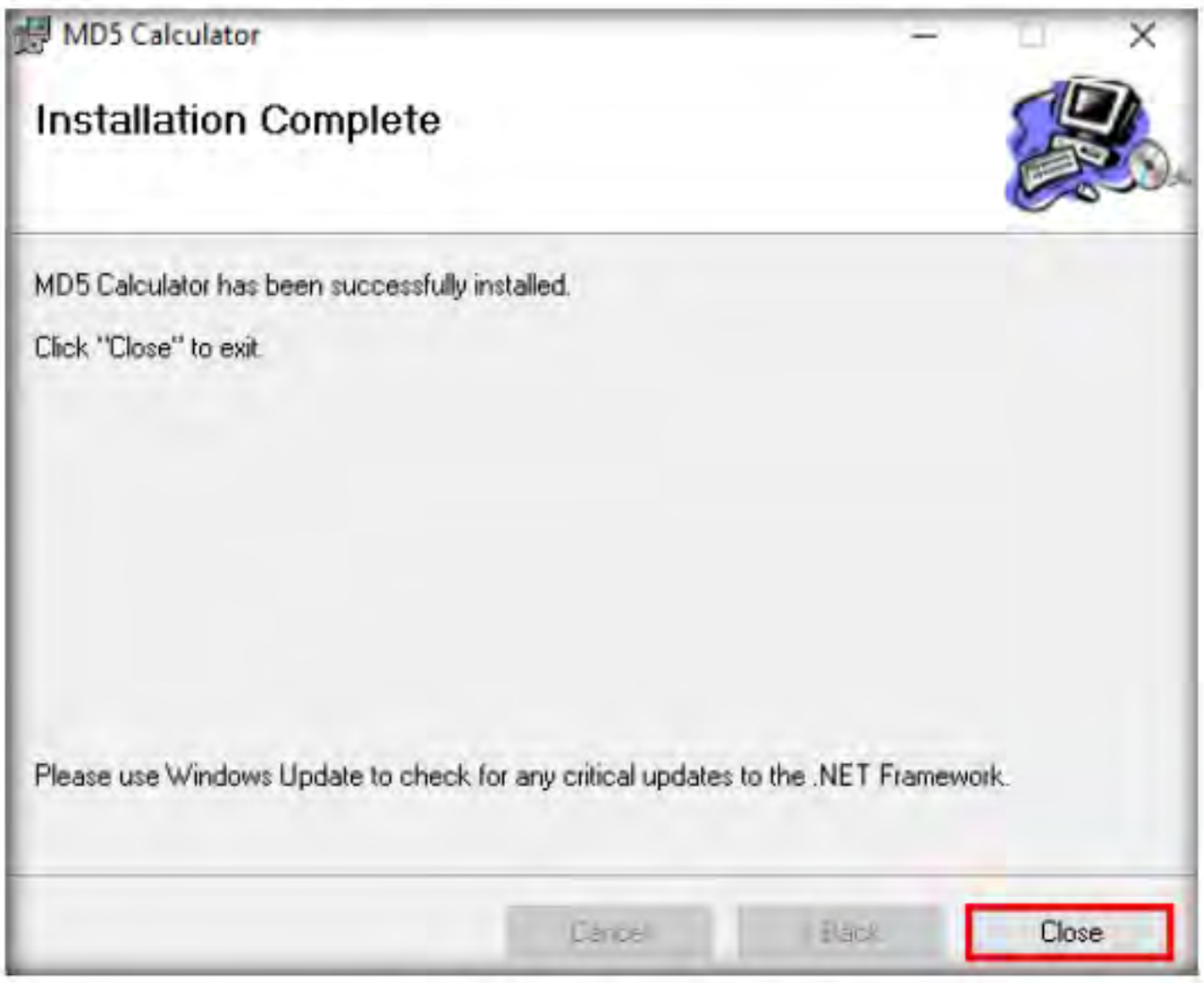


Figure 1.2.2: Installation Complete wizard

TASK 2.2

Calculate MD5 Value of an Original File

5. Navigate to **Desktop**, right-click on the text file (**Test.txt**) that we created in the previous task, and click **MD5 Calculator** from the context menu to calculate the MD5 hash of the file.

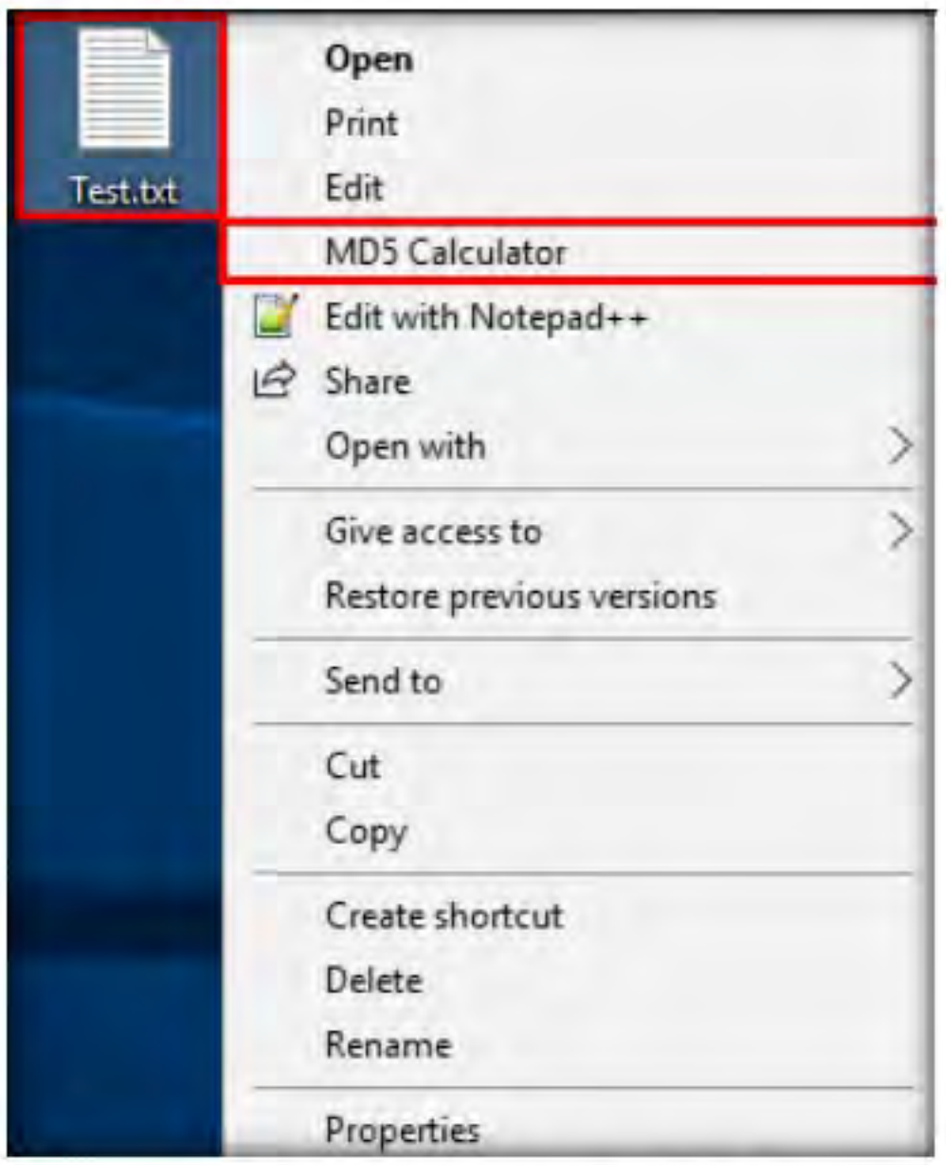


Figure 1.2.3: Calculate MD5 hash of Test.txt file

6. The **MD5 Calculator** window appears, with the path of file under the **File Name** field and MD5 hash value under the **MD5 Digest** field, as shown in the screenshot.
7. Copy the MD5 hash value from the **MD5 Digest** field.

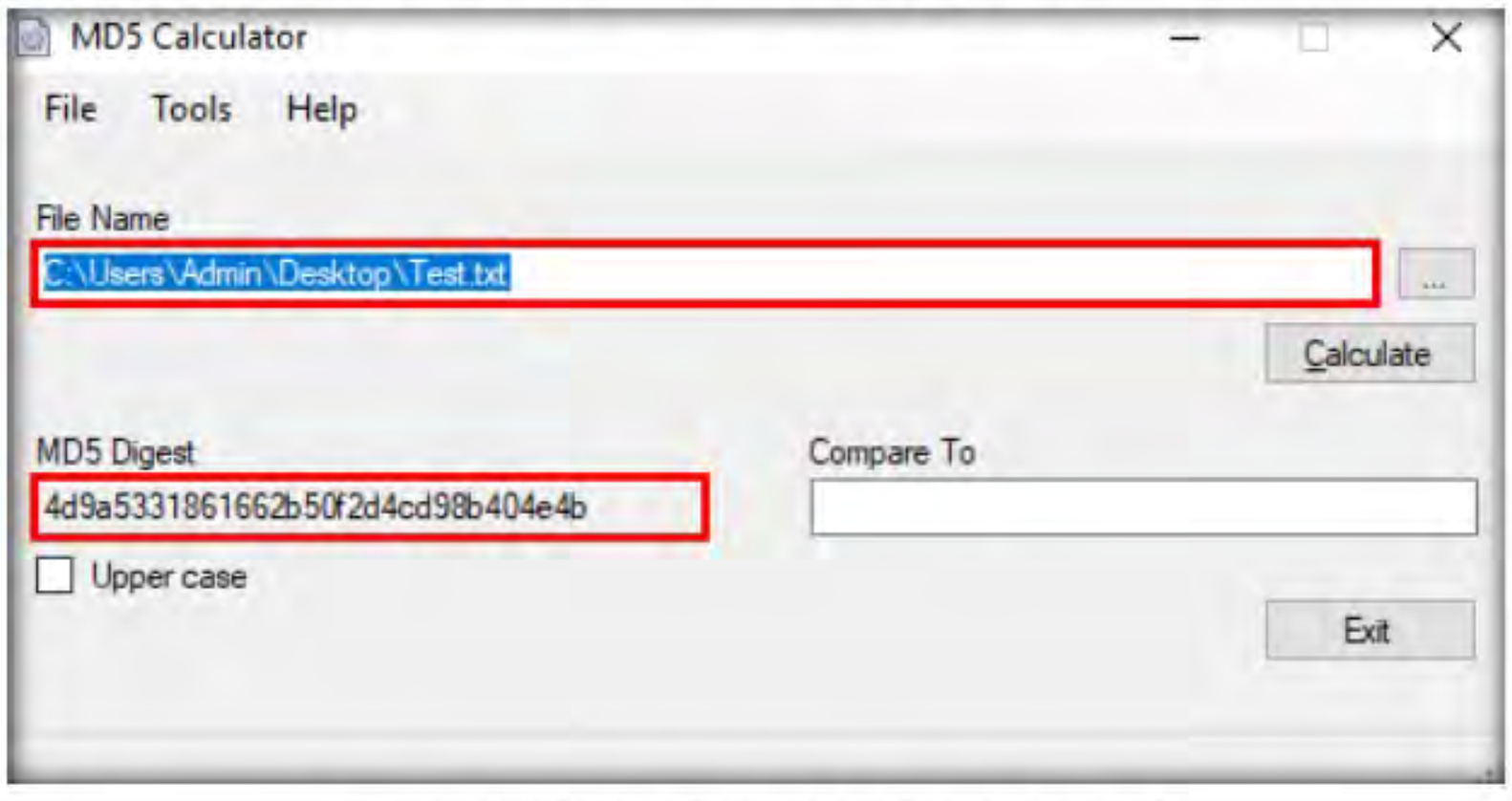


Figure 1.2.4: MD5 Calculator window with the MD5 hash value of the file

8. Now, double-click the **Test.txt** file from **Desktop** to open it and change the content of the file by inserting text within (here, **Hello World...!!!**). Save and close the **Test.txt** file.

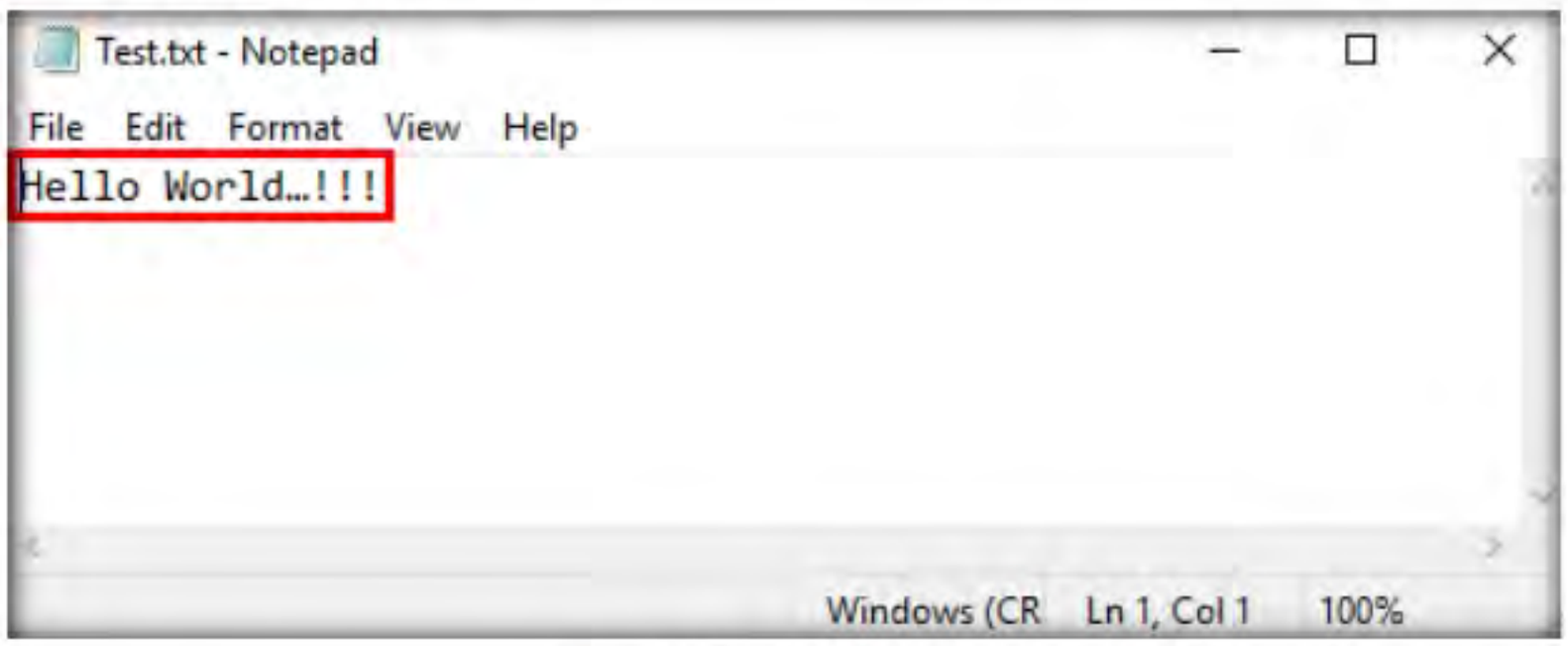


Figure 1.2.5: Modify the file content

9. After changing the file content, again right-click on the text file (**Test.txt**) and click **MD5 Calculator** from the context menu to calculate the MD5 hash of the file.

TASK 2.3

Analyze MD5 Values of Original and Modified File

10. A new **MD5 Calculator** window appears, with the MD5 hash value under the **MD5 Digest** field. In the **Compare To** field, paste the copied MD5 hash value of the file before it was modified.
11. The symbol (**<>**) between the **MD5 Digest** and **Compare To** fields indicates that the MD5 hash values of the file before modification is not equal to the MD5 hash value of the file after modification.

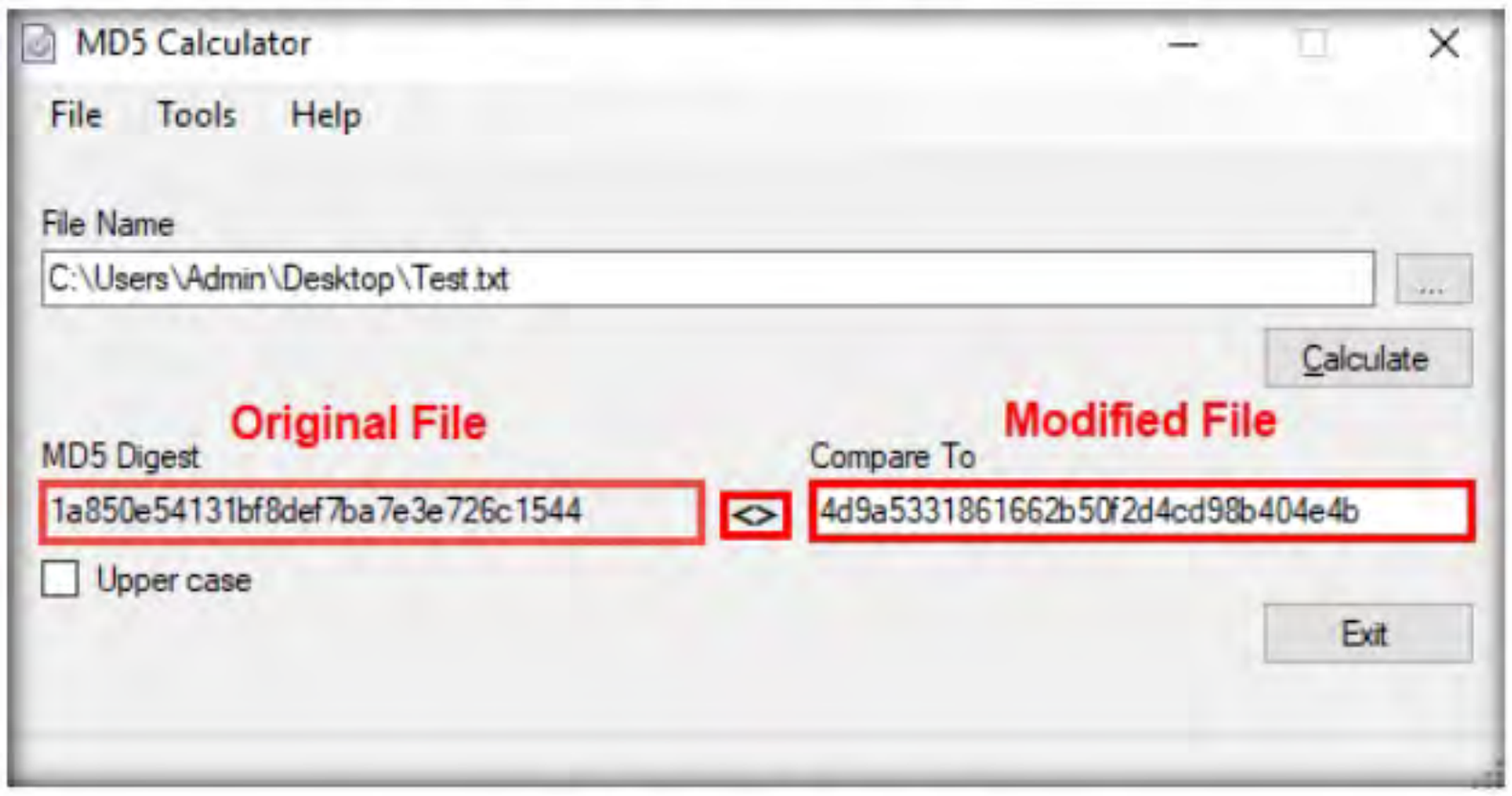


Figure 1.2.6: Modify the file content

Note: If a person wants to send a file to another person via a medium, they will calculate its hashes and send the file (along with the hash value) to the intended person. When the intended person receives the email, they will download the file and calculate its value using the MD5 Calculator.

The recipient compares the generated hash value with the hash value that was sent through email: if both tally, it is evident that they received the file without any modifications by a third person and that the integrity of the file is intact.

12. This concludes the demonstration of calculating MD5 hashes using MD5 Calculator.
13. Close all open windows and document all the acquired information.

TASK 3 — Calculate MD5 Hashes using HashMyFiles

Here, we will use the HashMyFiles tool to calculate MD5 hashes.

TASK 3.1 — Install HashMyFiles Tool

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles** and double-click **HashMyFiles.exe**.
2. The **HashMyFiles** main window appears, as shown in the screenshot.

HashMyFiles is a small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system: you can easily copy the MD5/SHA1 hashes list into the clipboard, or save them into text/html/xml file. HashMyFiles can also be launched from the context menu of Windows Explorer, and can display the MD5/SHA1 hashes of the selected file or folder.

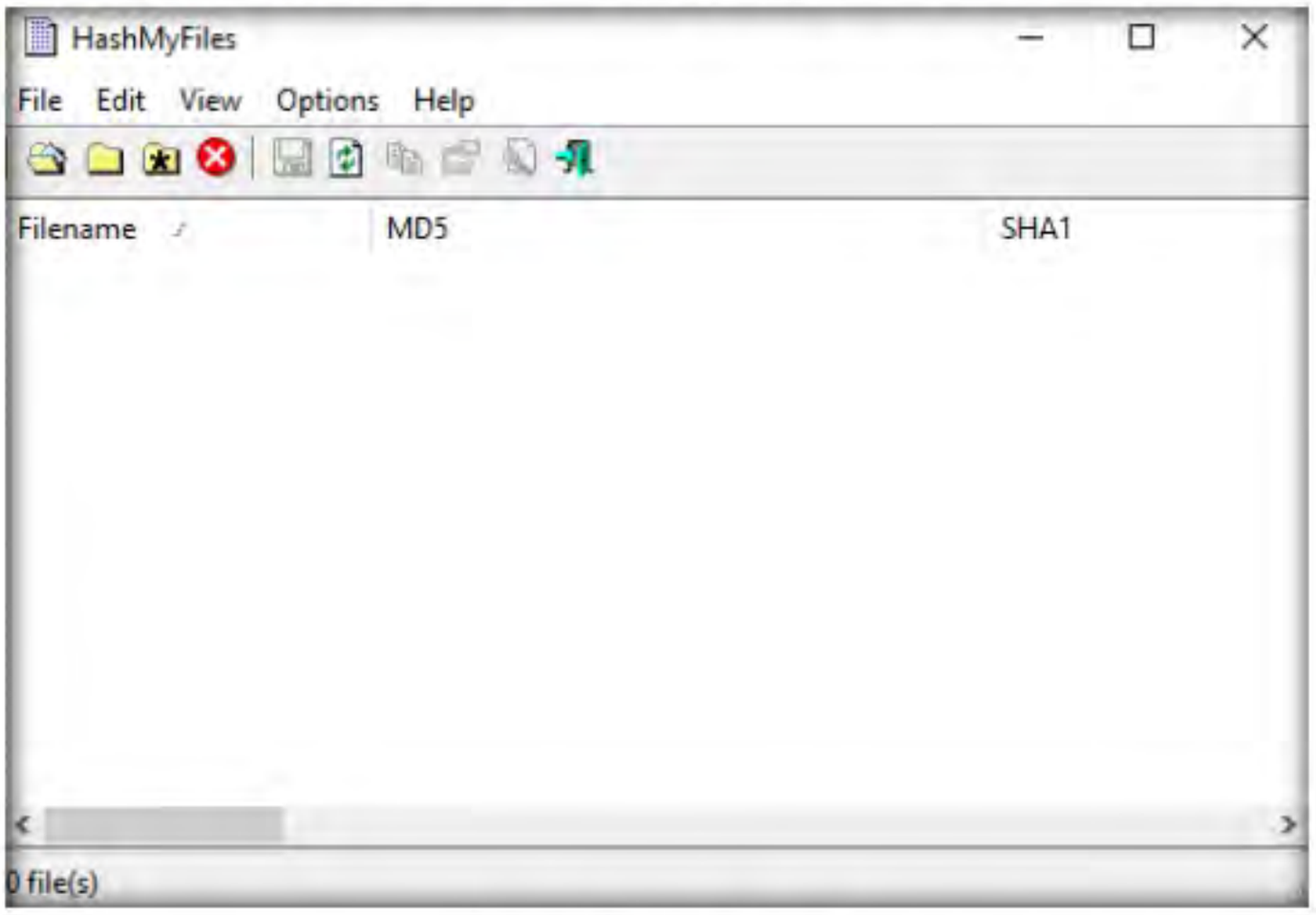


Figure 1.3.1 HashMyFiles window

3. In the **HashMyFiles** window, click **Files** from the menu bar. From the drop-down list, click the **Add Folder** option.

Note: You can also use the **Add Files** option to add multiple files.

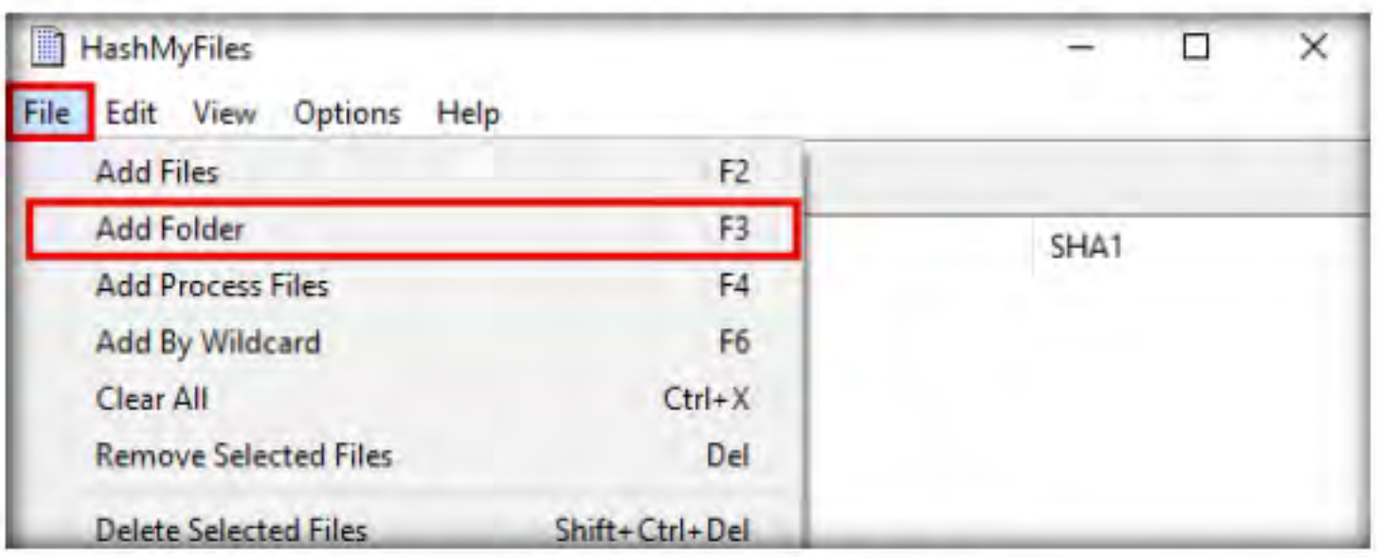


Figure 1.3.2: HashMyFiles window: File options

4. The **Select Folder** pop-up appears; click on the ellipsis icon (...) to select the folder you want to encrypt.

Figure 1.3.3: Select Folder pop-up

5. The **Browse for Folder** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles** and select the **Sample Files** folder; then, click **OK**.

Note: You can select any folder of your choice that you wish to encrypt.

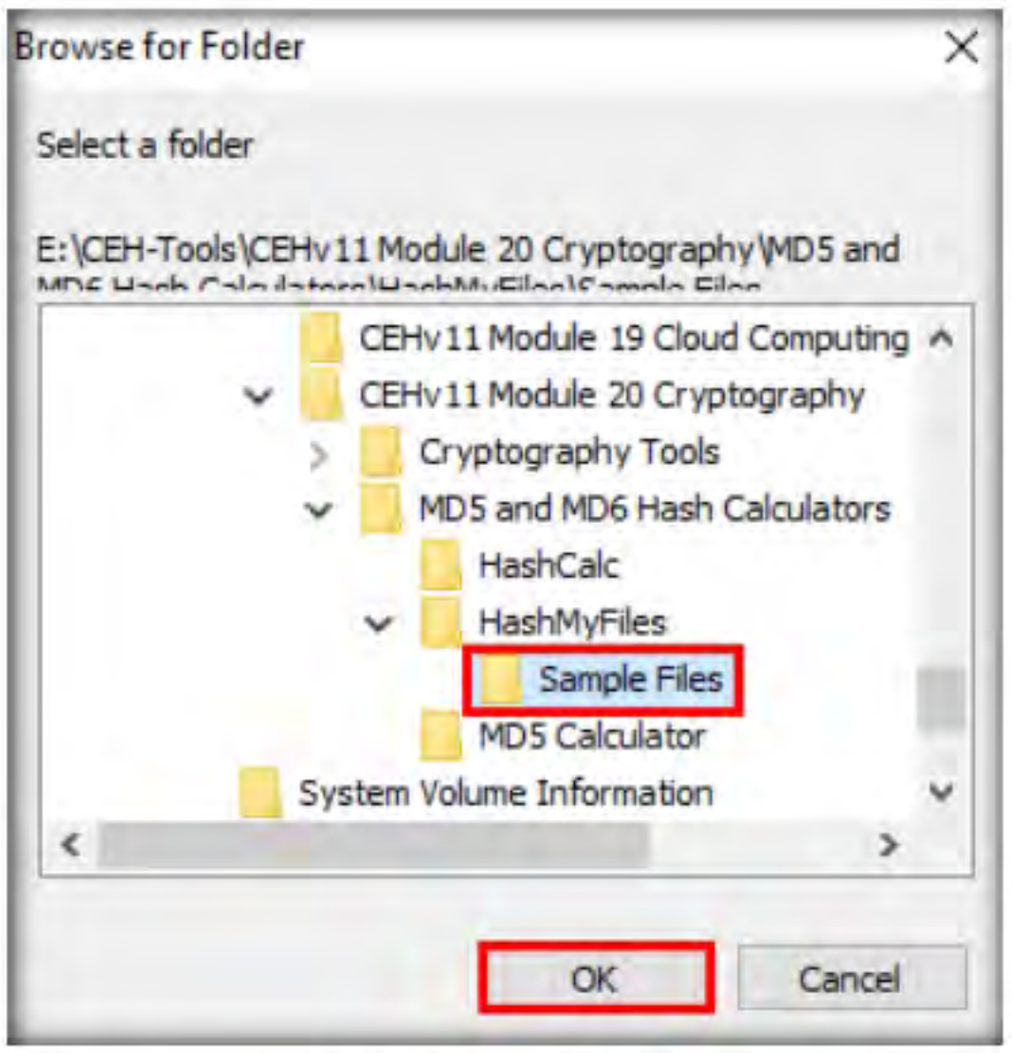


Figure 1.3.4: Browse for Folder

6. The location of the selected folder appears in the field; click **OK**.

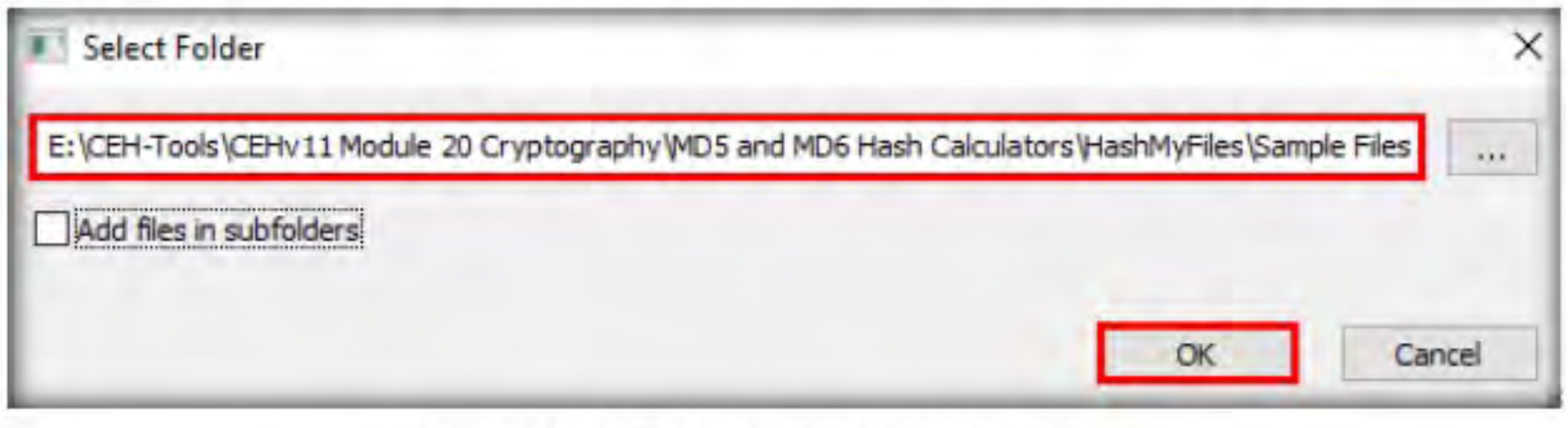


Figure 1.3.5: Select Folder pop-up: Selected folder's location

TASK 3.2

Analyze MD5 Values

7. A list of files contained in the folder appears, along with their various hash values such as **MD5**, **SHA1**, **CRC32**, etc.

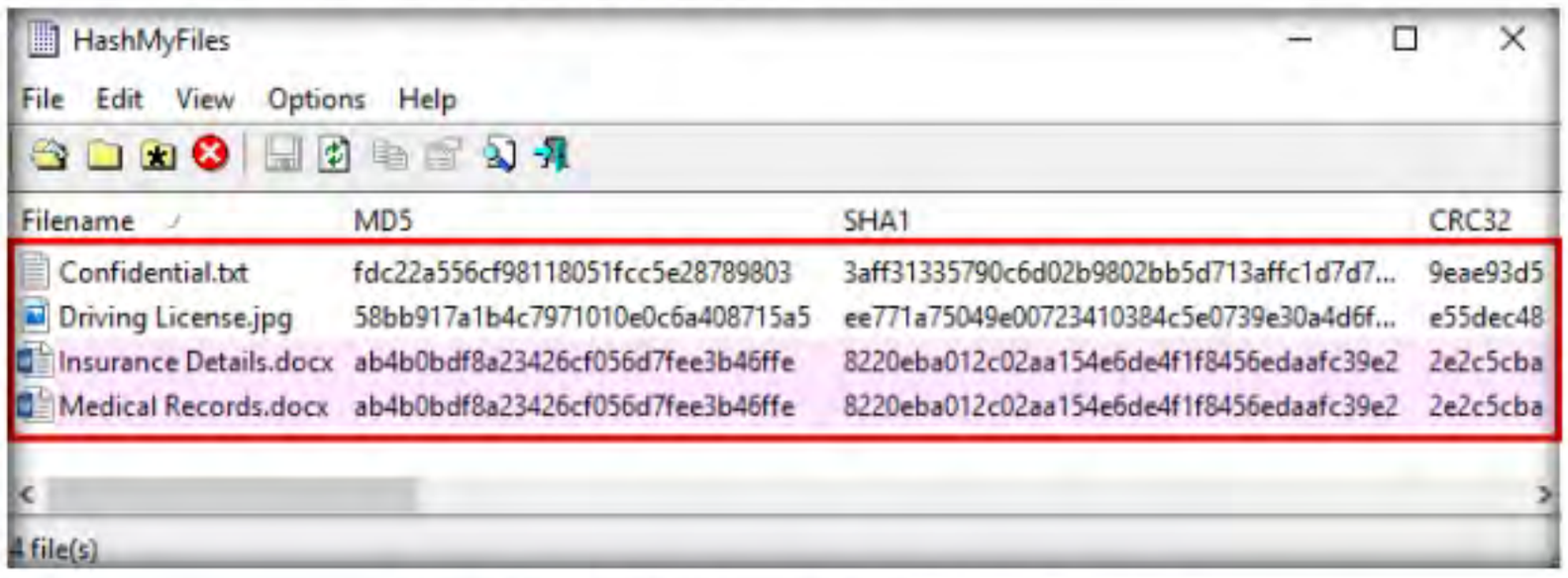


Figure 1.3.6: HashMyFiles window: list of files with hash values

You can also use other MD5 and MD6 hash calculators such as **MD6 Hash Generator** (https://www.browserling.com), **All Hash Generator** (https://www.browserling.com), **MD6 Hash Generator** (https://convert-tool.com), and **md5 hash calculator** (https://onlinehashtools.com) to calculate MD5 and MD6 hashes.

8. In the **HashMyFiles** window, click **Options** from the menu bar and choose **Hash Types** from the options. You can observe a list of hash functions such as **MD5**, **SHA1**, **CRC32**, **SHA-256**, **SHA-512**, and **SHA-384**, which you can choose (here, the MD5, SHA1, and CRC32 hash functions were selected).

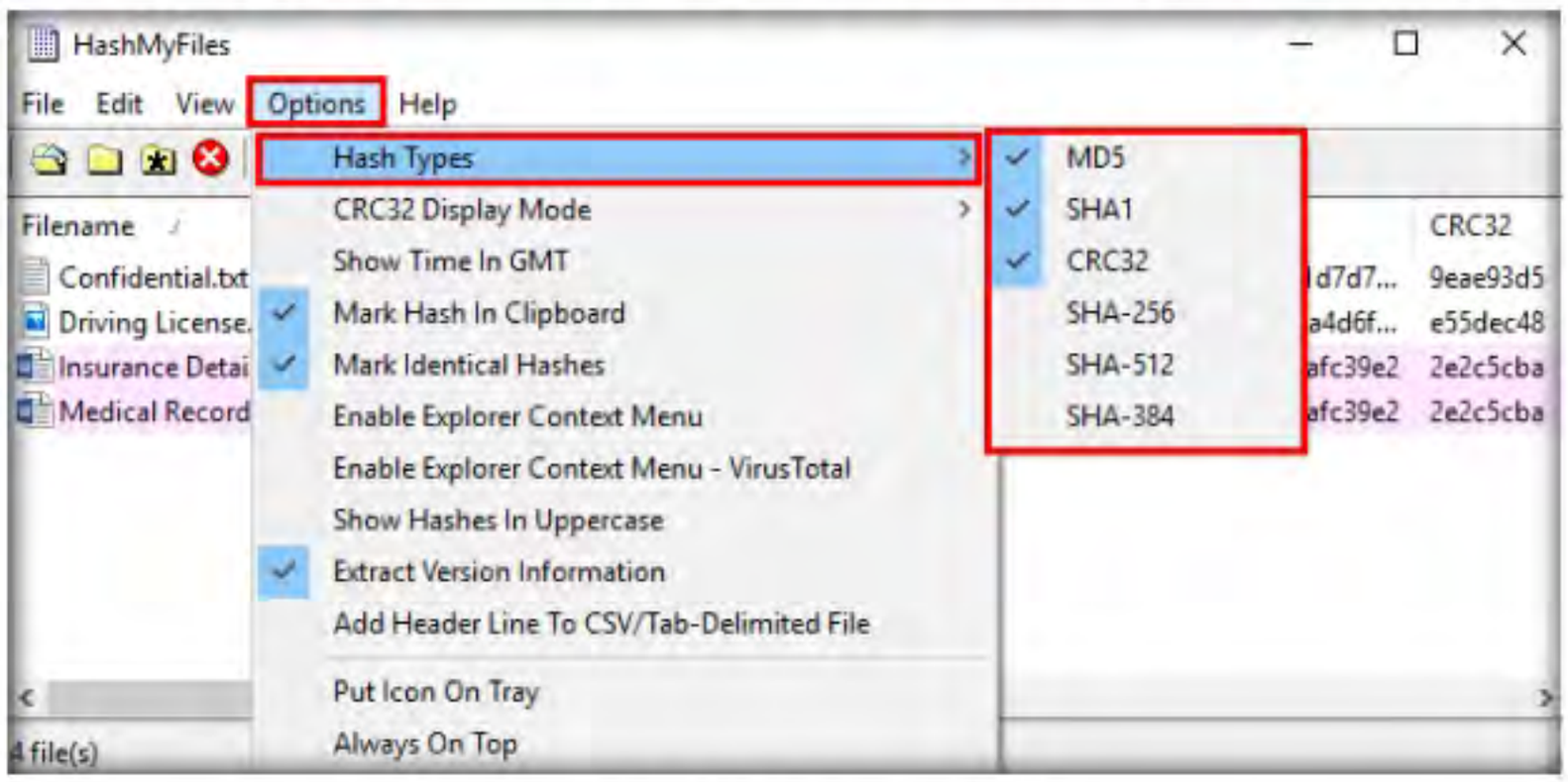


Figure 1.3.7: HashMyFiles window: Options list

Note: In real-time, you may share confidential information in the folder in an encrypted form to maintain its integrity.

9. This concludes the demonstration of calculating MD5 hashes using HashMyFiles.
10. Close all open windows and document all the acquired information.

TASK 4

Perform File and Text Message Encryption using CryptoForge

Here, we will use the CryptoForge tool to encrypt a file and text message.

Note: Ensure that the **Windows 10** virtual machine is running.

1. Turn on the **Windows Server 2019** virtual machine; log in with the credentials **Administrator**/**Pa$$w0rd**.

TASK 4.1

Install CryptoForge

CryptoForge is a file encryption software for personal and professional data security. It allows you to protect the privacy of sensitive files, folders, or email messages by encrypting them with strong encryption algorithms. Once the information has been encrypted, it can be stored on insecure media or transmitted on an insecure network—such as the Internet—and remain private. Later, the information can be decrypted into its original form.

2. Navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge** and double-click **CryptoForge.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

3. The **CryptoForge Installation** window appears; click **Next**.

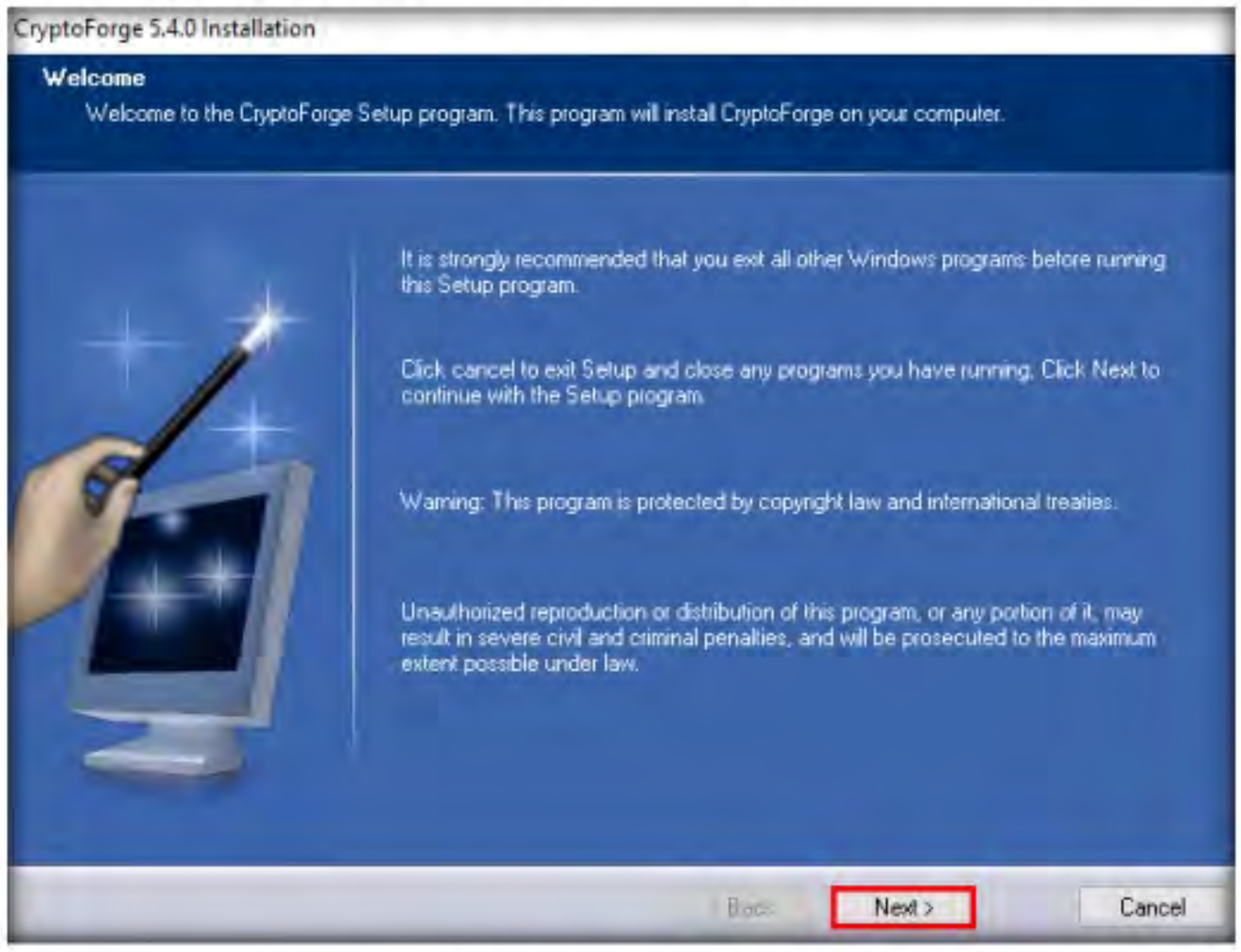


Figure 1.4.1: CryptoForge Installation window

4. Follow the installation steps to install the application using all default settings.

5. After completion of the installation, **CryptoForge installation successful** wizard appears; click **Finish**.

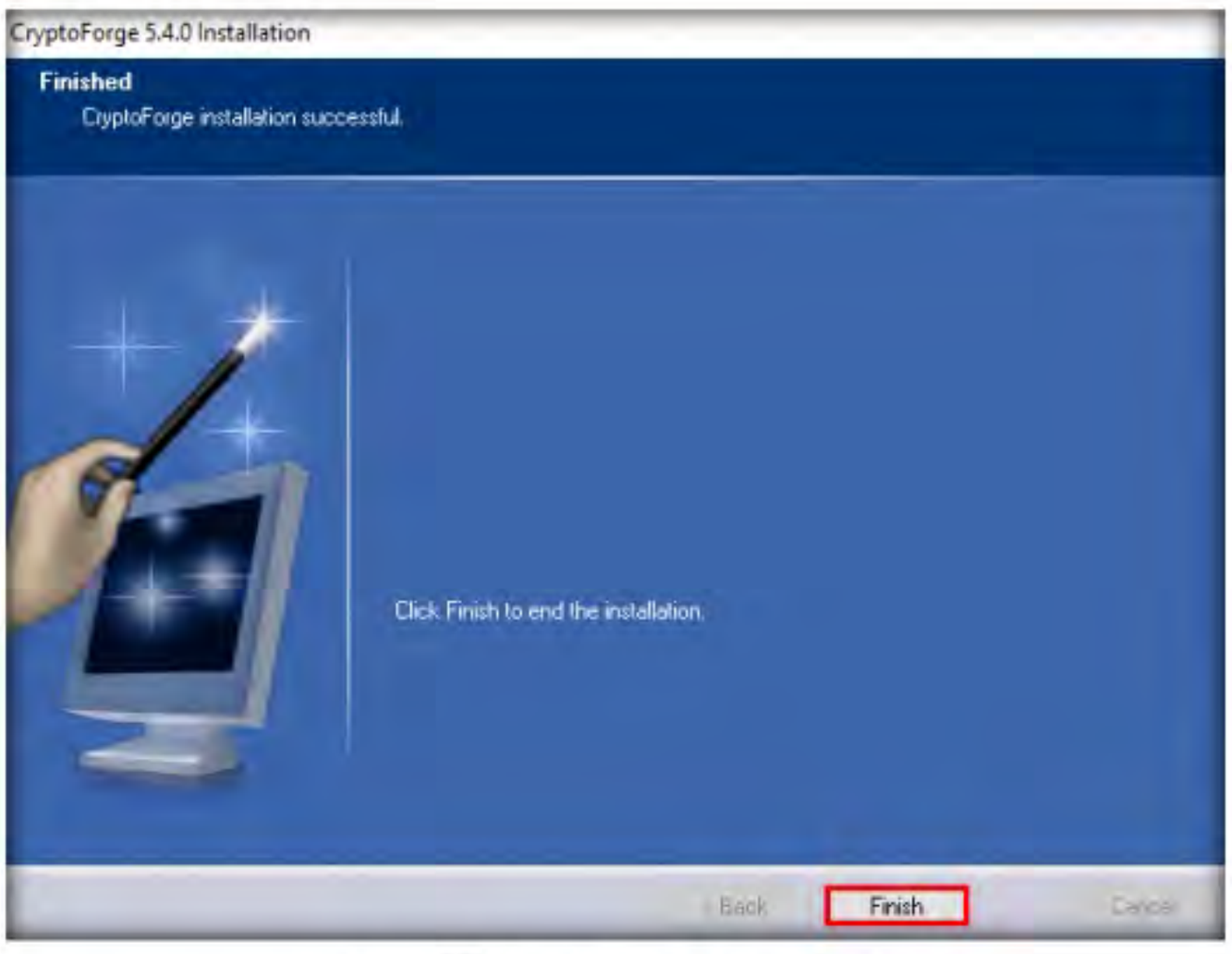


Figure 1.4.2: CryptoForge installation successful

6. Now, switch to the **Windows 10** virtual machine.
7. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**, double-click **CryptoForge.exe**, and follow the steps to install the application using default settings.

TASK 4.2

Encrypt a File

8. Right-click the **Confidential.txt** file located at the same location (**E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**) and select **Encrypt** from the context menu.

Note: In this task, we are encrypting the **Confidential.txt** file, although you can encrypt any file of your choice.

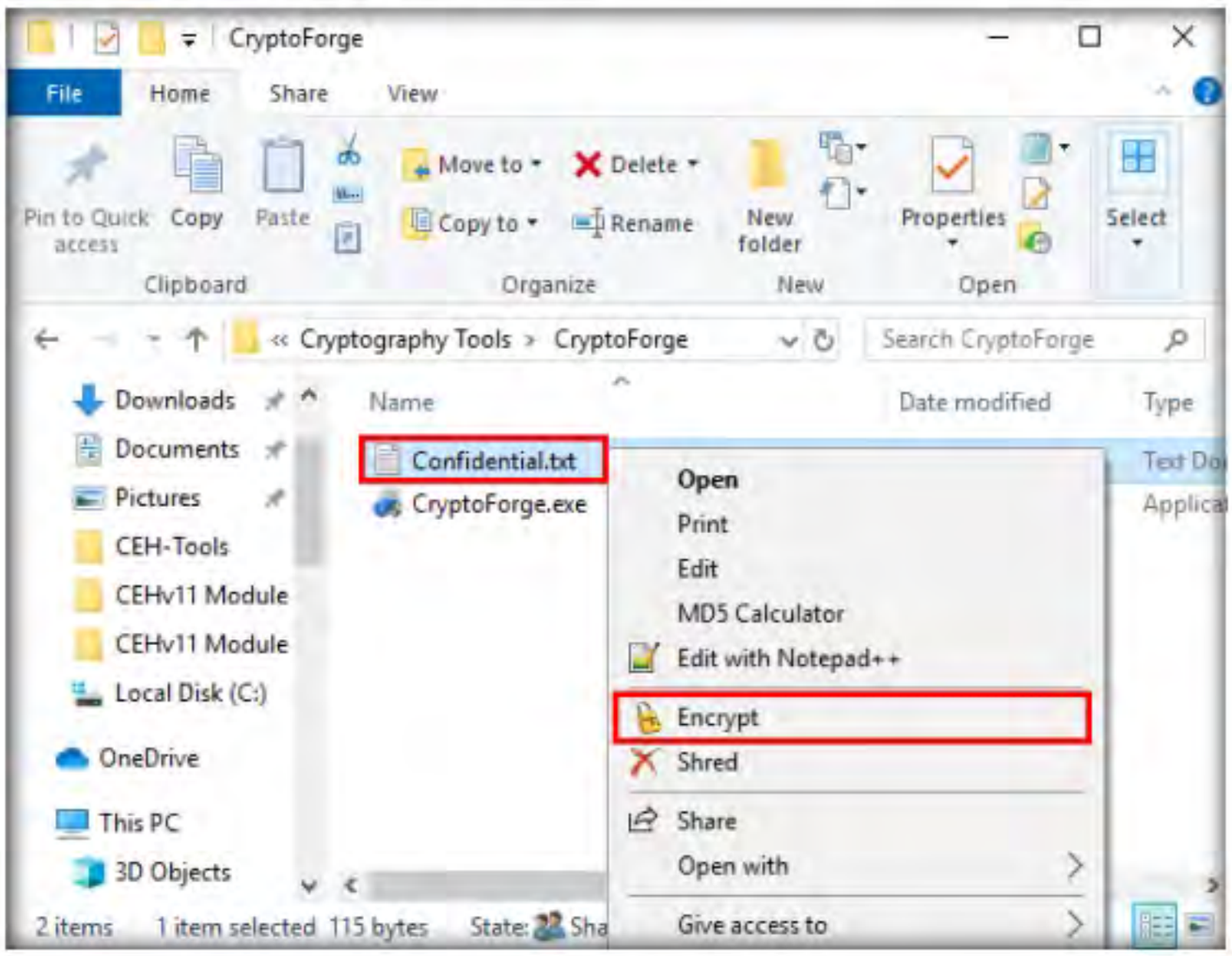


Figure 1.4.3: Encrypting a File

9. The **Enter Passphrase - CryptoForge Files** dialog-box appears; type a password in the **Passphrase** field, retype it in the **Confirm** field, and click **OK**. The password used in this lab is **qwerty@1234**.

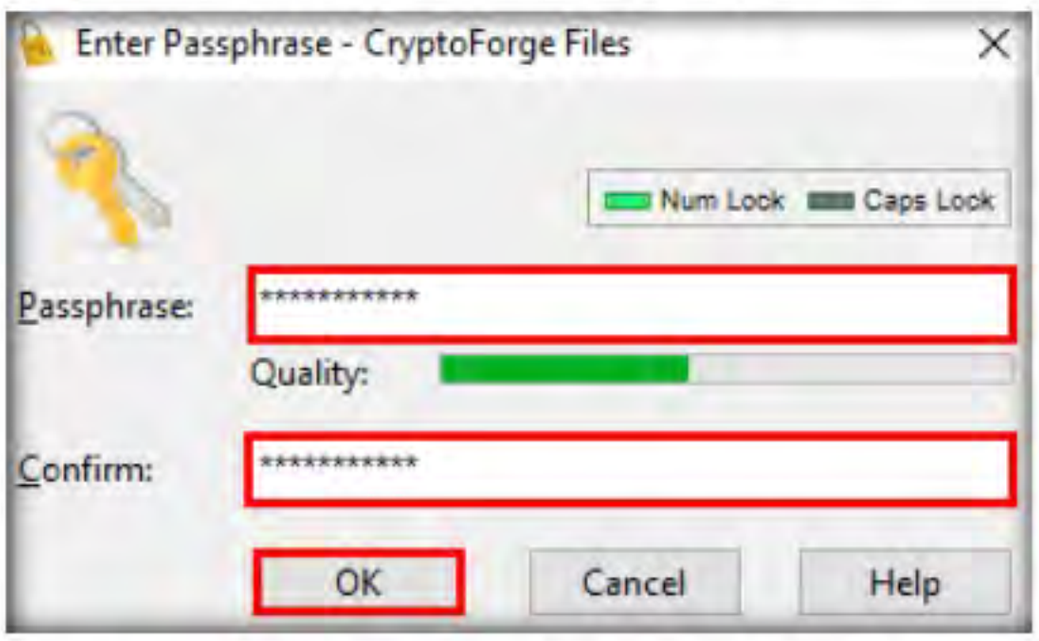


Figure 1.4.4: Enter Passphrase - CryptoForge Files Dialog-Box

10. Now, the file will be encrypted in the same location, and the old file will be deleted automatically, as shown in the screenshot.

Note: No one can access this file unless the user provides the password for the encrypted file. You will have to share the password with the user through message, email, or any other means.

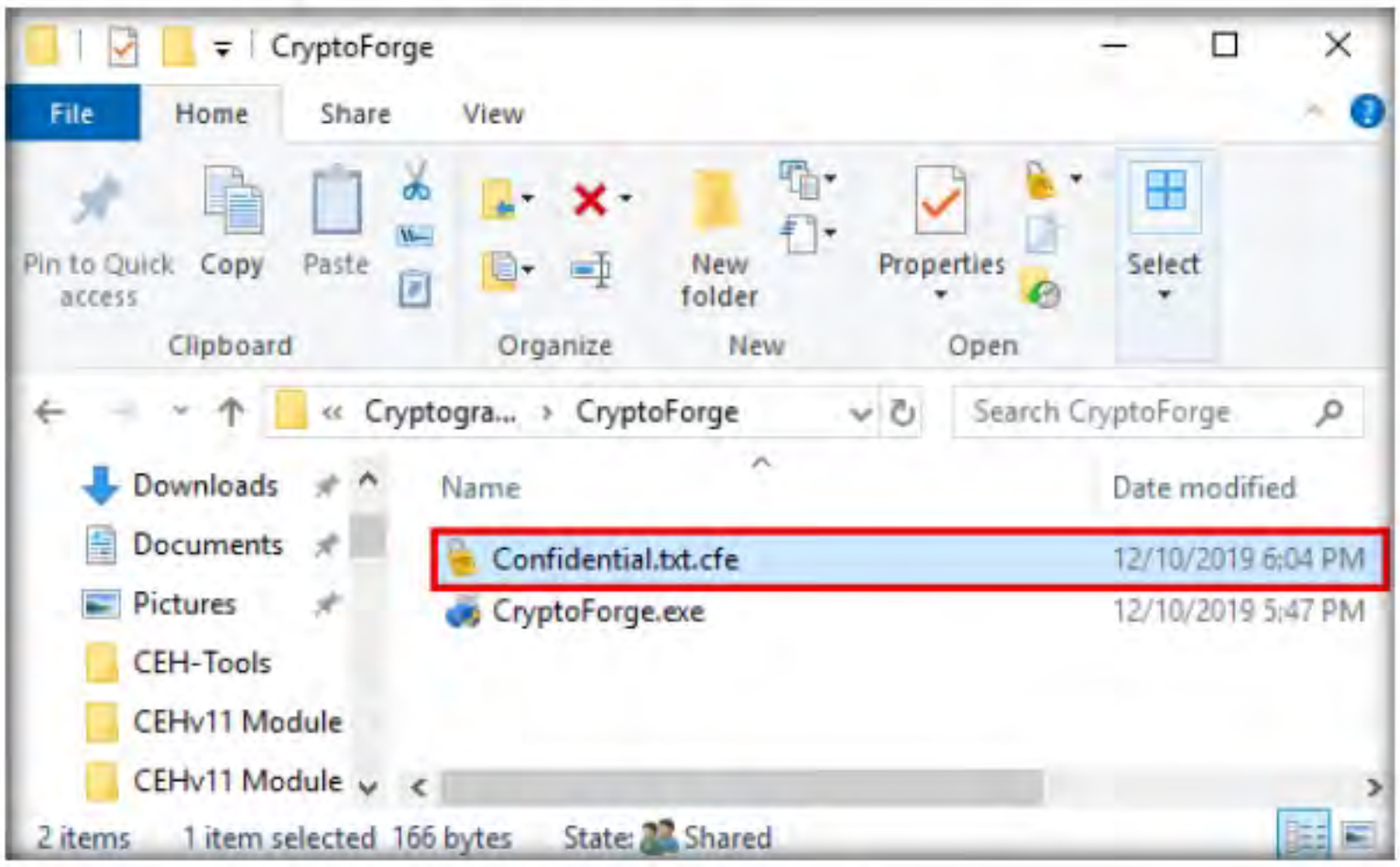


Figure 1.4.5: File Encrypted

TASK 4.3

Decrypt the Encrypted File

11. Let us assume that you shared this file through a shared network drive.
12. Now, switch to the **Windows Server 2019** virtual machine and navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**. You will observe the encrypted file in this location.
13. Double-click the encrypted file to decrypt it and view its contents.

Figure 1.4.6: Decrypted the Encrypted File

14. The **Enter Passphrase - CryptoForge Files** dialog-box appears; enter the password that you have provided in **Step#9** to encrypt the file and click **OK**.

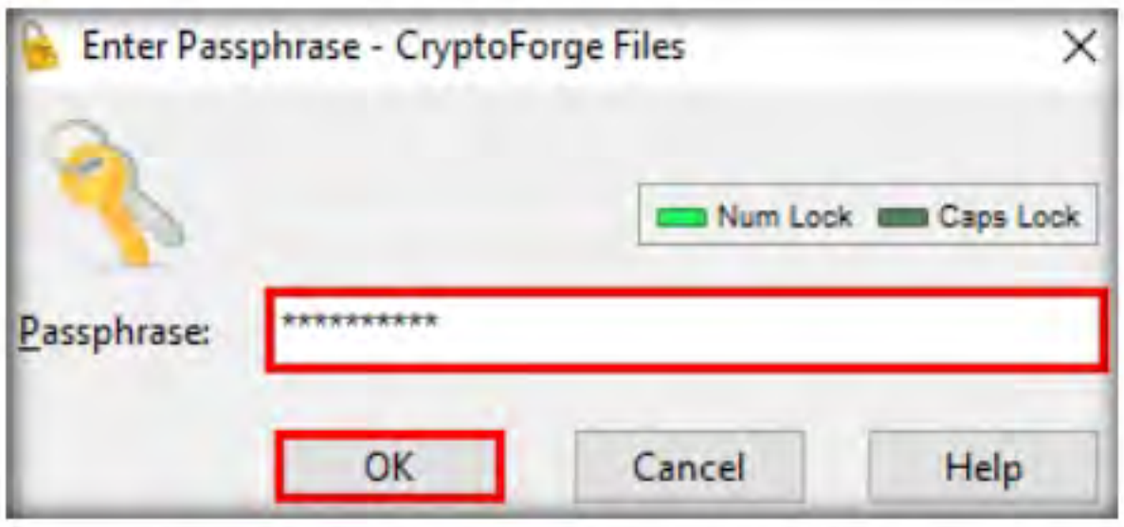


Figure 1.4.7: Enter Passphrase - CryptoForge Files Dialog-Box

15. Upon entering the password, the file will be successfully decrypted. You may now double-click the text file to view its contents.

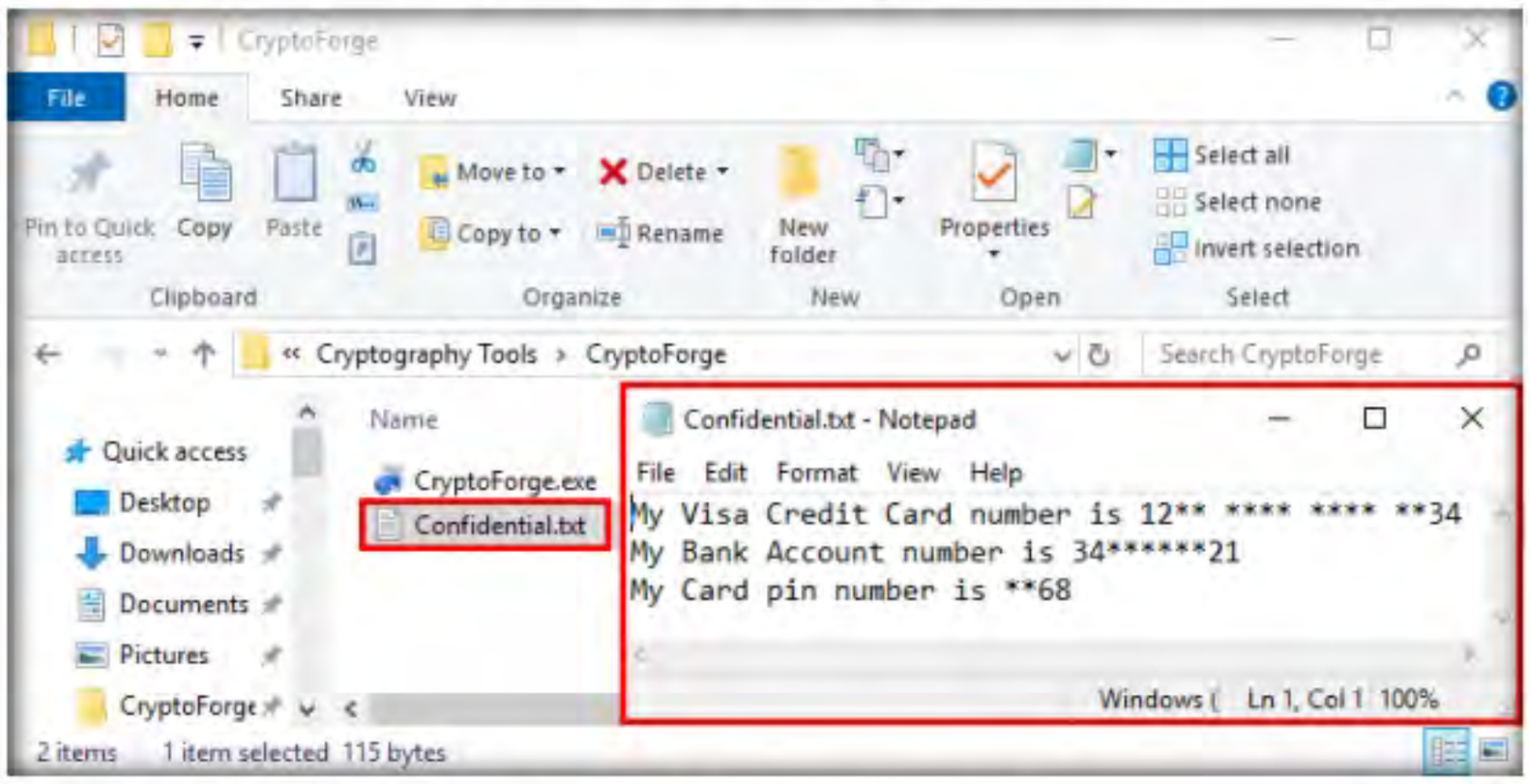


Figure 1.4.8: File Decrypted Successfully

16. So far, you have seen how to encrypt a file and share it with the intended user. Now, we shall share an encrypted message with a user.

TASK 4.4

Encrypt a Message

17. In the **Windows Server 2019** machine, click the **Start** icon present in the bottom-left corner of **Desktop** and click **CryptoForge Text** from the apps to launch the application.
18. The **CryptoForge Text** window appears; type a message and click **Encrypt** from the toolbar.

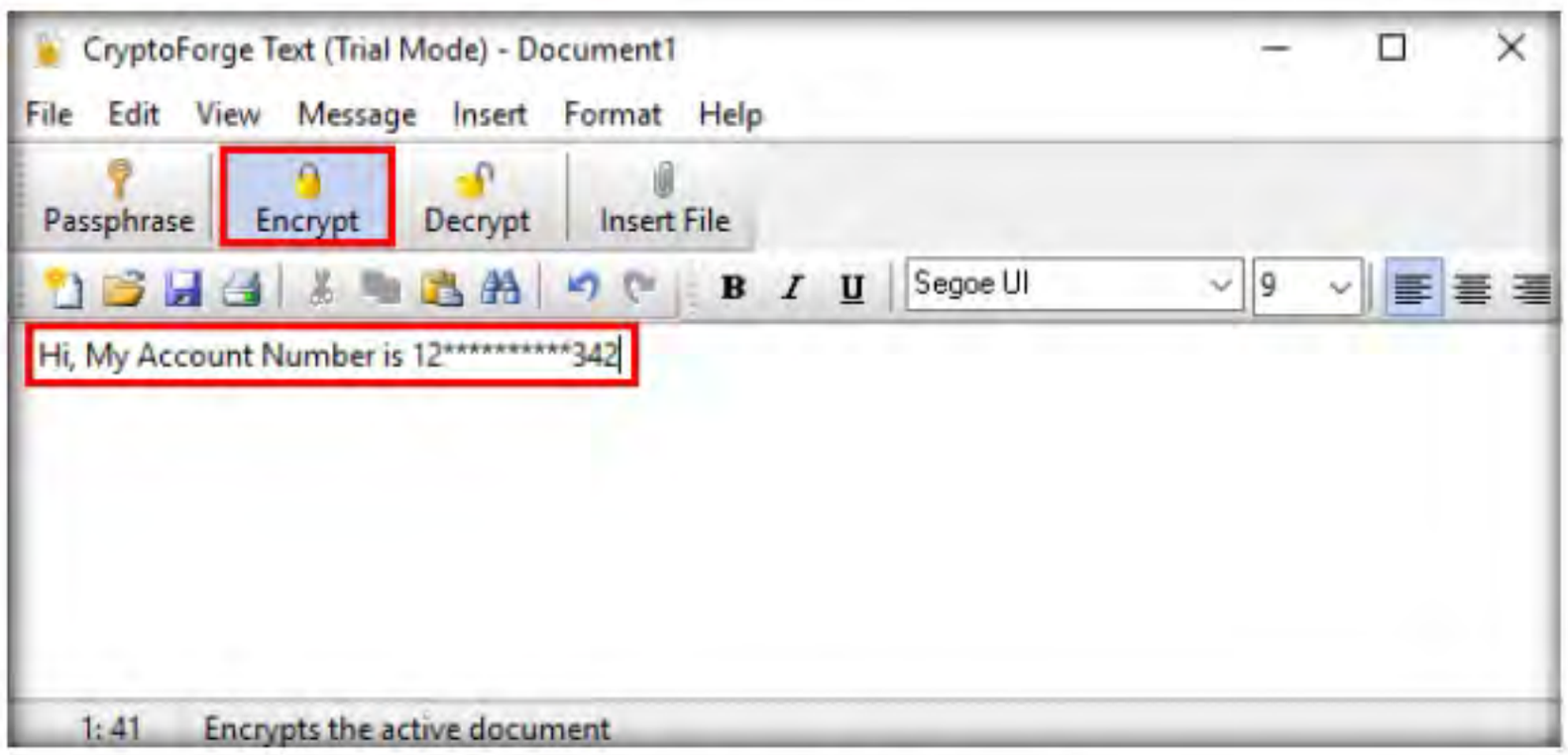


Figure 1.4.9: Encrypting a Text Message

19. The **Enter Passphrase - CryptoForge Text** dialog-box appears; type a password in the **Passphrase** field, retype it in the **Confirm** field, and click **OK**. The password used in this lab is **test@123**.

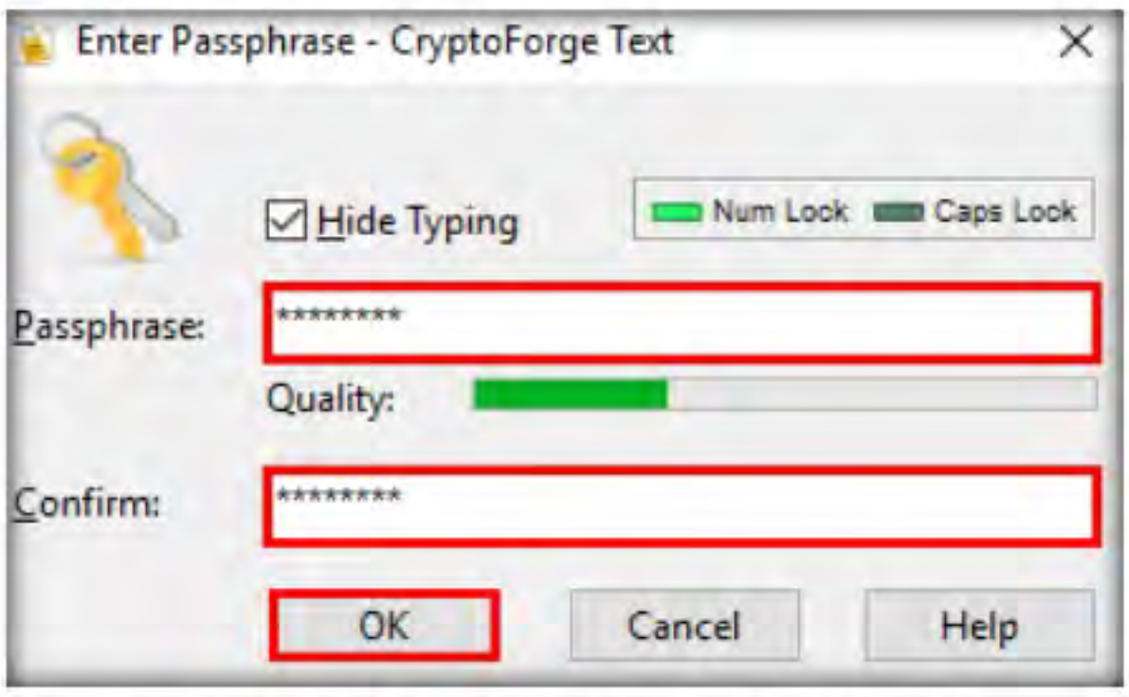


Figure 1.4.10: Enter Passphrase - CryptoForge Text Dialog-Box

20. The message that you have typed will be encrypted, as shown in the screenshot.

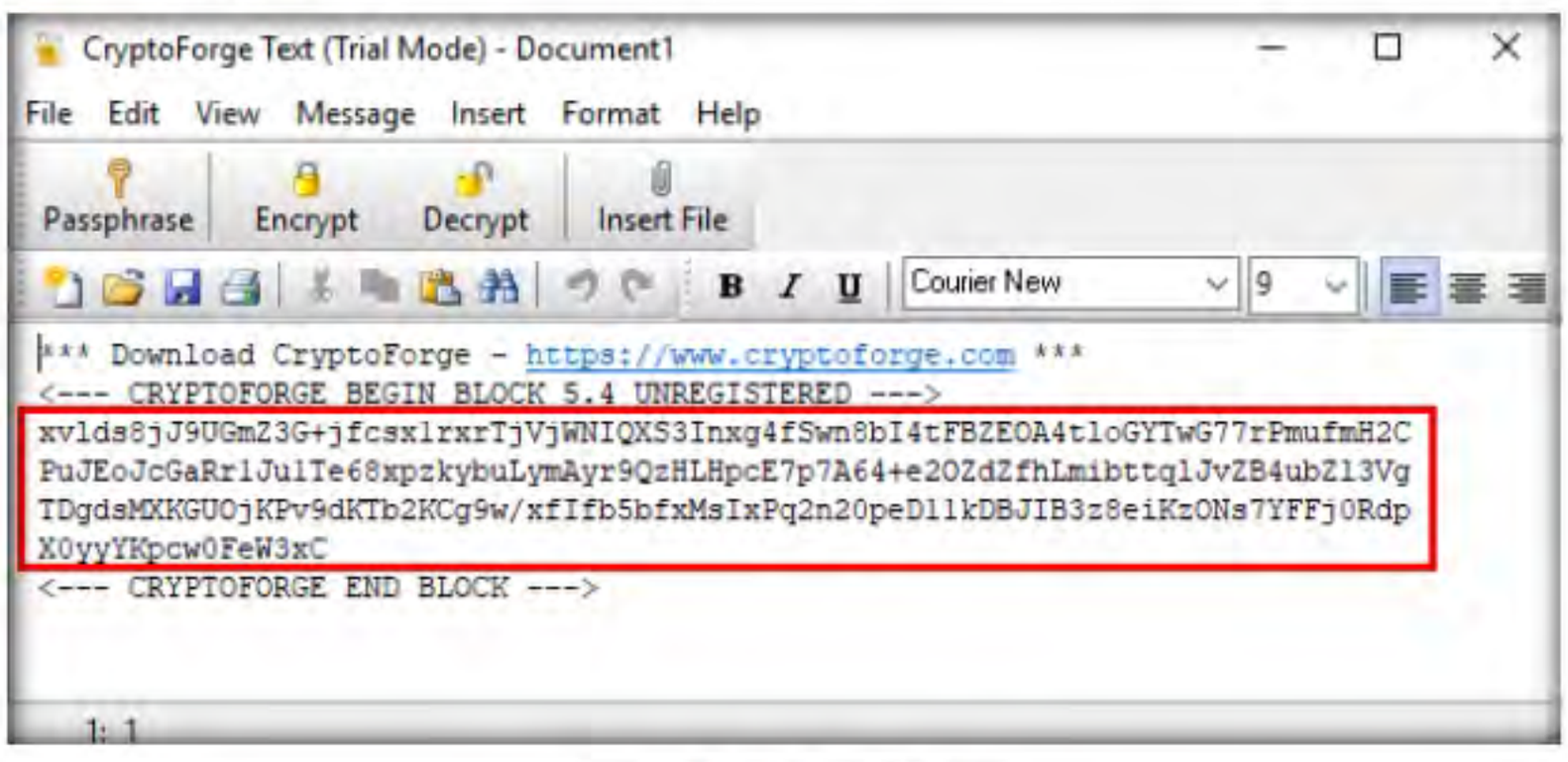


Figure 1.4.11: Encrypted Message

21. Now, you need to save the file. Click **File** in the menu bar and click **Save**.

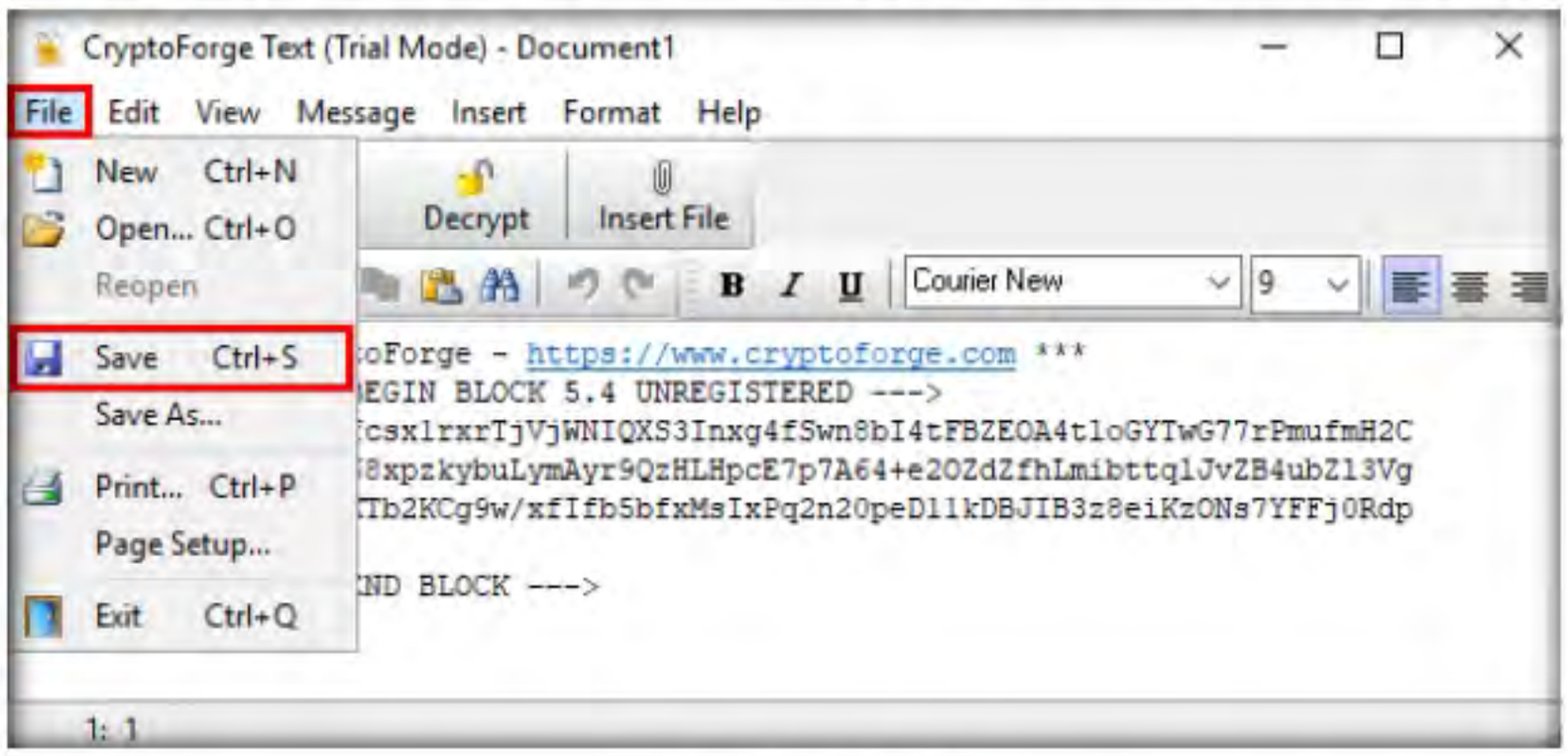


Figure 1.4.12: Saving the File

22. The **Save As** window appears; navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**, specify the file name as **Secret Message.cfd**, and click **Save**.

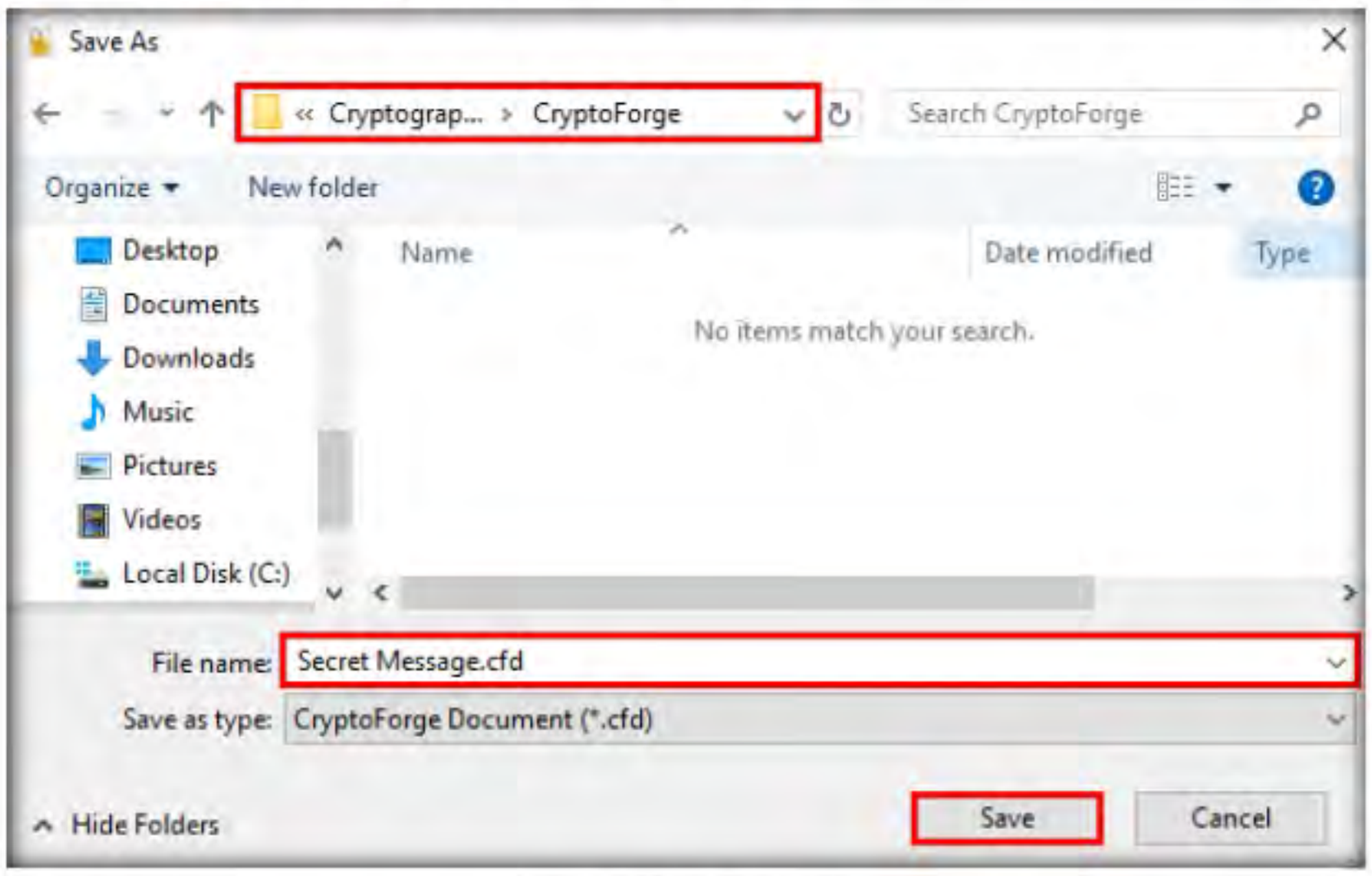


Figure 1.4.13: Saving the File

23. Close the **CryptoForge Text** window.
24. Now, let us assume that you shared the file through the mapped network drive and shared the password to decrypt the file in an email message or through some other means.

TASK 4.5

Decrypt the Encrypted Message

25. Switch to the **Windows 10** virtual machine and navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**.

26. You will observe the encrypted file in this location; double-click the file **Secret Message.cfd**.

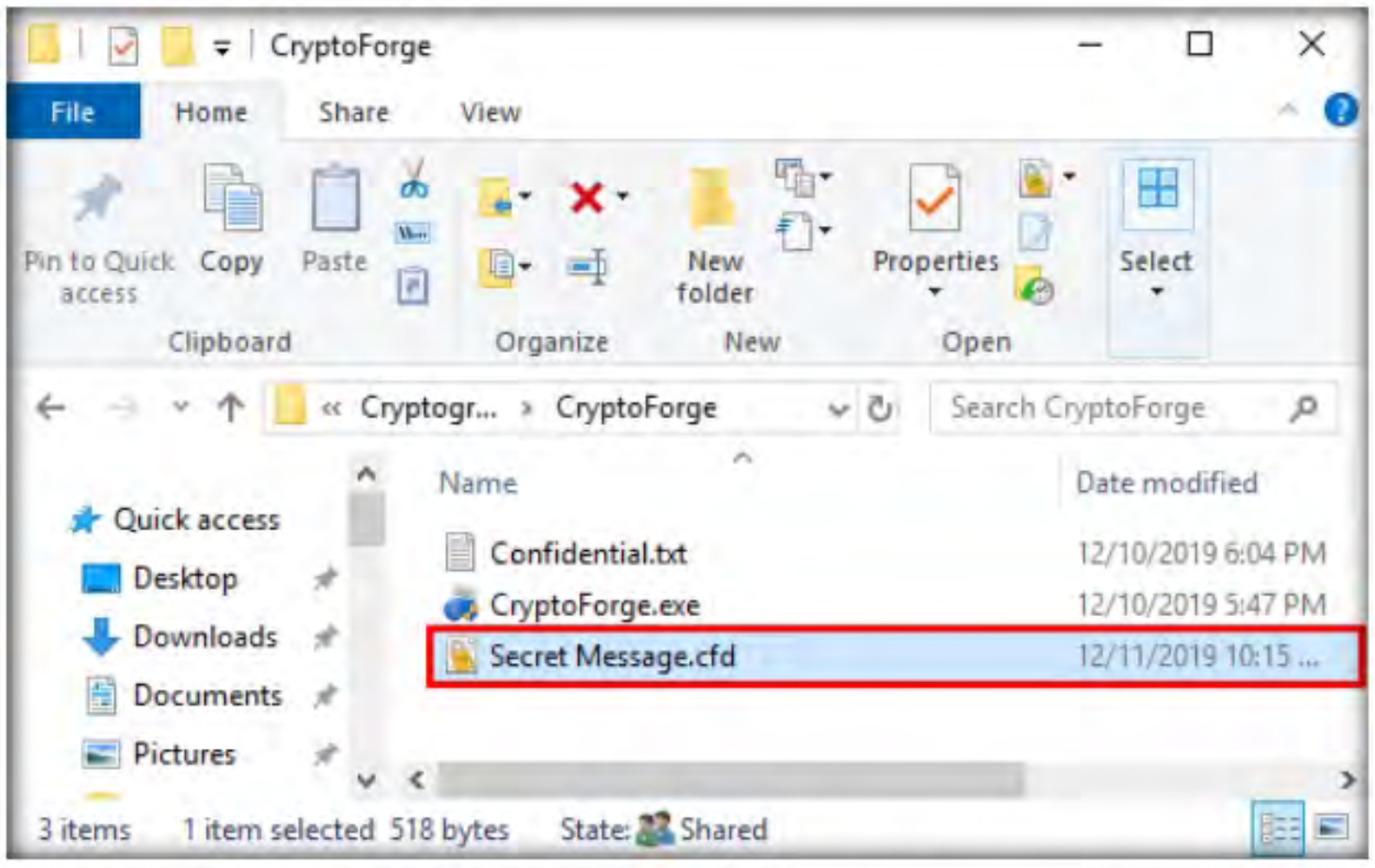


Figure 1.4.14: Viewing the Encrypted File

27. The **CryptoForge Text** window appears, displaying the message in an encrypted format. Click **Decrypt** from the toolbar to decrypt it.

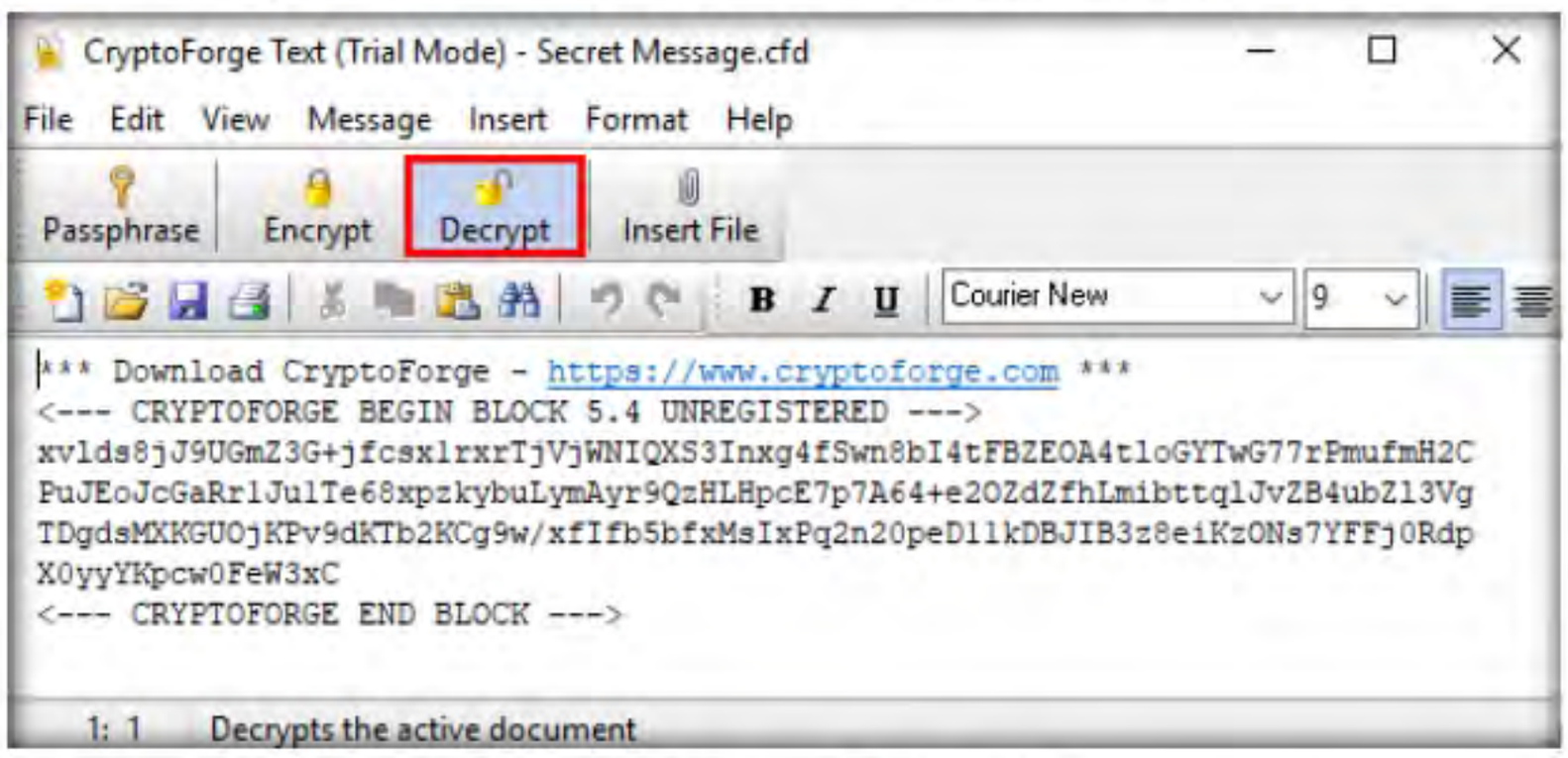


Figure 1.4.15: Decrypting the Encrypted File

28. The **Enter Passphrase - CryptoForge Text** dialog-box appears; enter the password you provided in **Step#19** to decrypt the message in the **Passphrase** field and click **OK**.

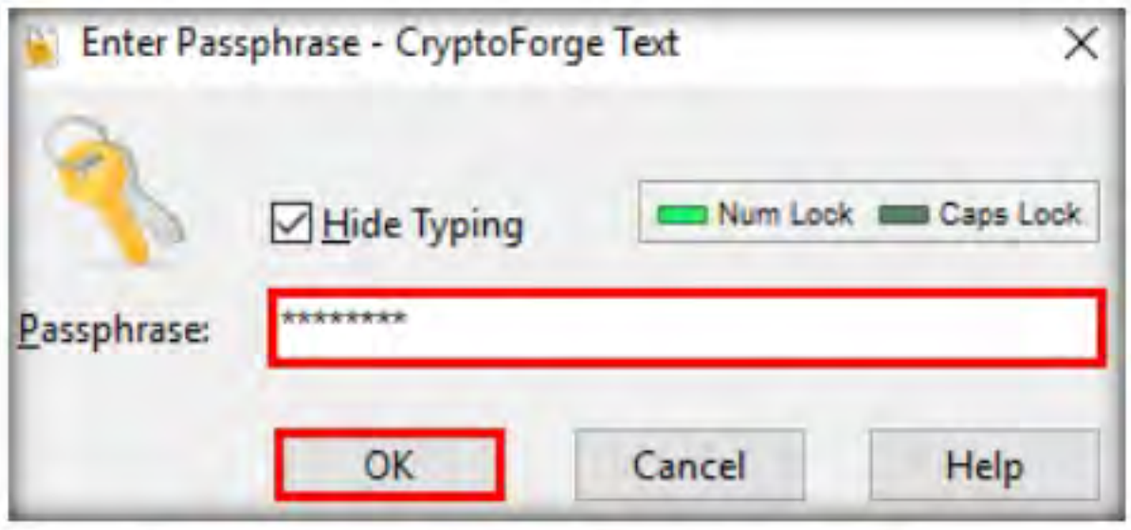


Figure 1.4.16: Enter Passphrase - CryptoForge Text Dialog-Box

29. The **CryptoForge Text** window appears, displaying the message in plain-text format, as shown in the screenshot.

Figure 1.4.17: Message Decrypted Successfully

Note: In real-time, you may share sensitive information through email by encrypting data using CryptoForge.

30. This concludes the demonstration of performing file and text message encryption using CryptoForge.
31. Close all open windows and document all the acquired information.
32. Turn off the **Windows Server 2019** virtual machine.

TASK 5 — Perform File Encryption using Advanced Encryption Package

Here, we will use the Advanced Encryption Package tool to perform file encryption.

TASK 5.1 — Install Advanced Encryption Package

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package** and double-click **aep.msi**.
2. **Windows Installer** initializes and the **Advanced Encryption Package Setup** window appears; click the **I accept the terms in the License Agreement** checkbox; then, click **Install**.

Advanced Encryption Package is a file encryption software for Windows used for secure file transfer, batch file encryption, and encrypted backups. It supports file and/or text encryption, performs secure file deletion, and creates an encrypted self-extracting file to send as an email attachment.

Note: If a **User Account Control** pop-up appears, click **Yes**.

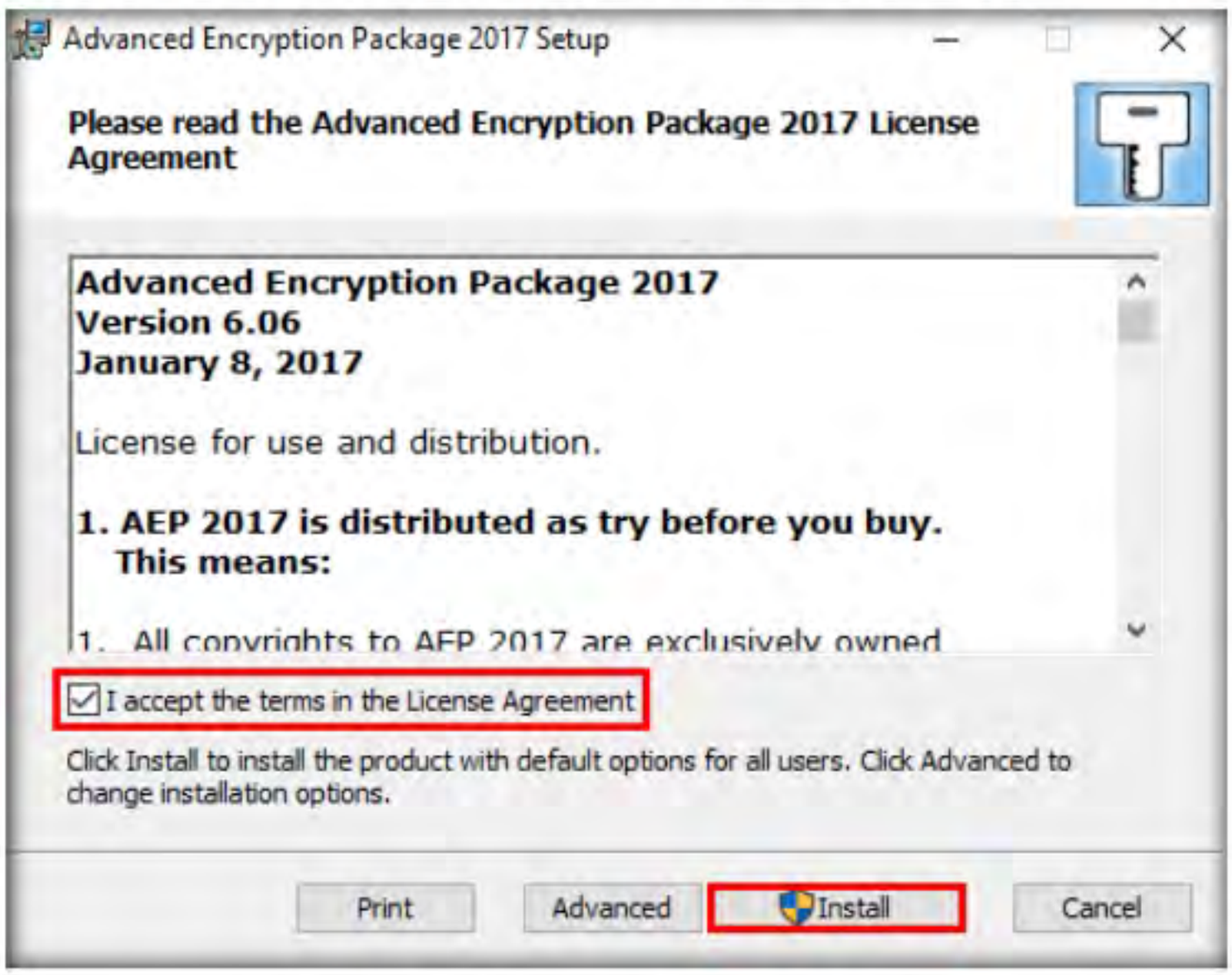


Figure 1.5.1: Advanced Encryption Package Setup window

3. Follow the steps to install the application with default settings.
4. After the completion of the installation, **Completed the Advanced Encryption Package Setup Wizard** appears; then, click **Finish**.

Figure 1.5.2: Advanced Encryption Package Setup window

5. Now, click the **Start** icon from the bottom-left corner of **Desktop**; and from the list of **Recently added** applications, click **Advanced Encryption Package 2017** to launch the application.

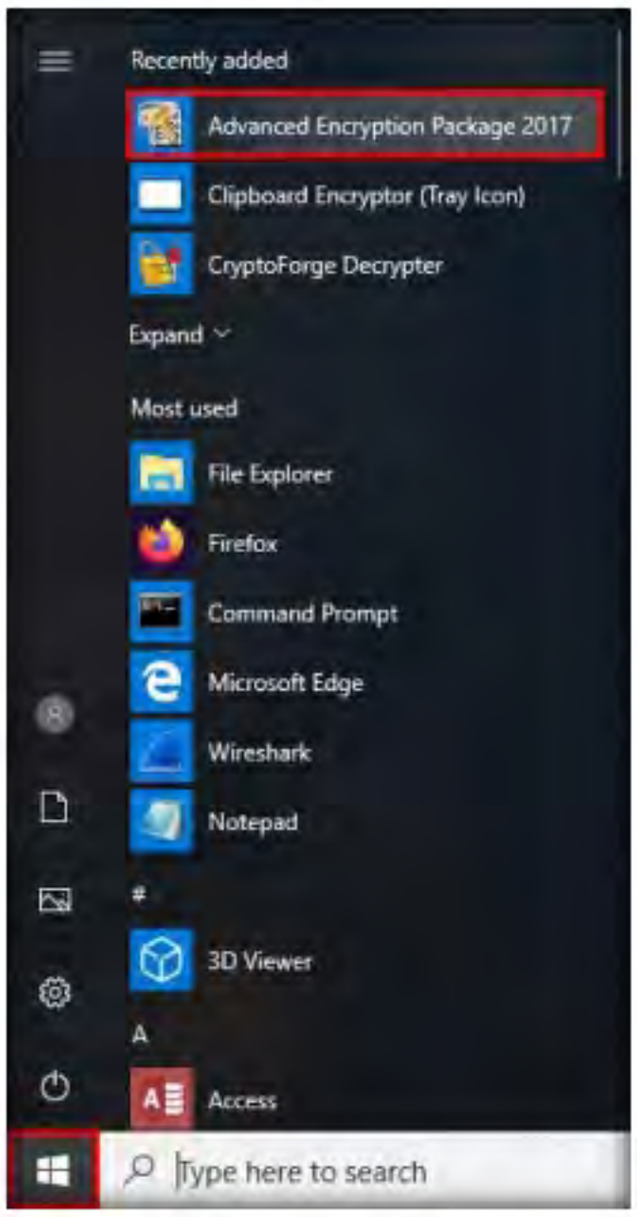


Figure 1.5.3: Launching Advanced Encryption Package application from the Apps screen

6. The **Advanced Encryption Package - License Manager** window appears. Under the **License Manager** section, select the **Start free 30-day trial** radio button and click **Next**.

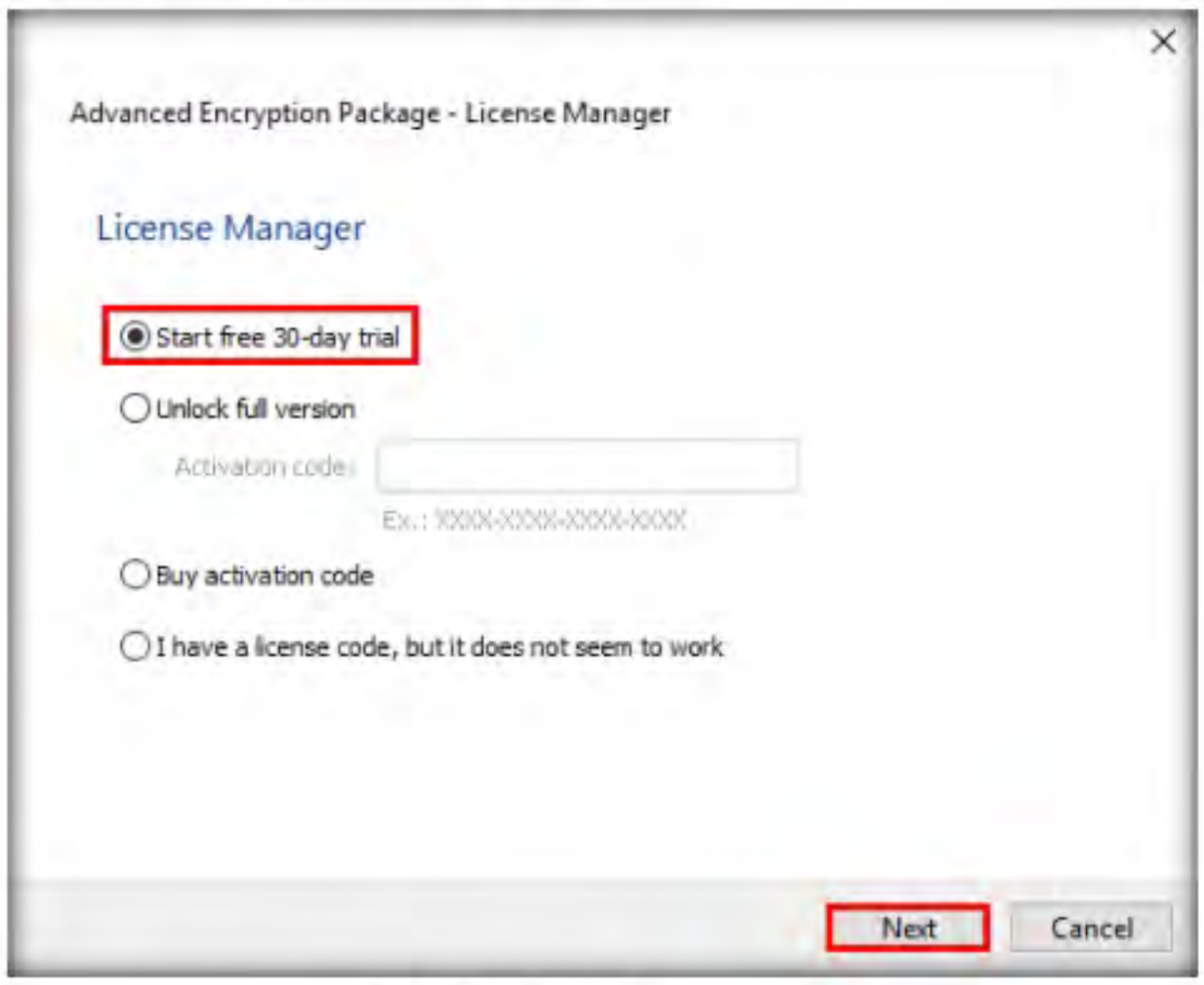


Figure 1.5.4: License Manager window

7. The **Activating** step appears displaying a **Success!** message; then, click **Next**.

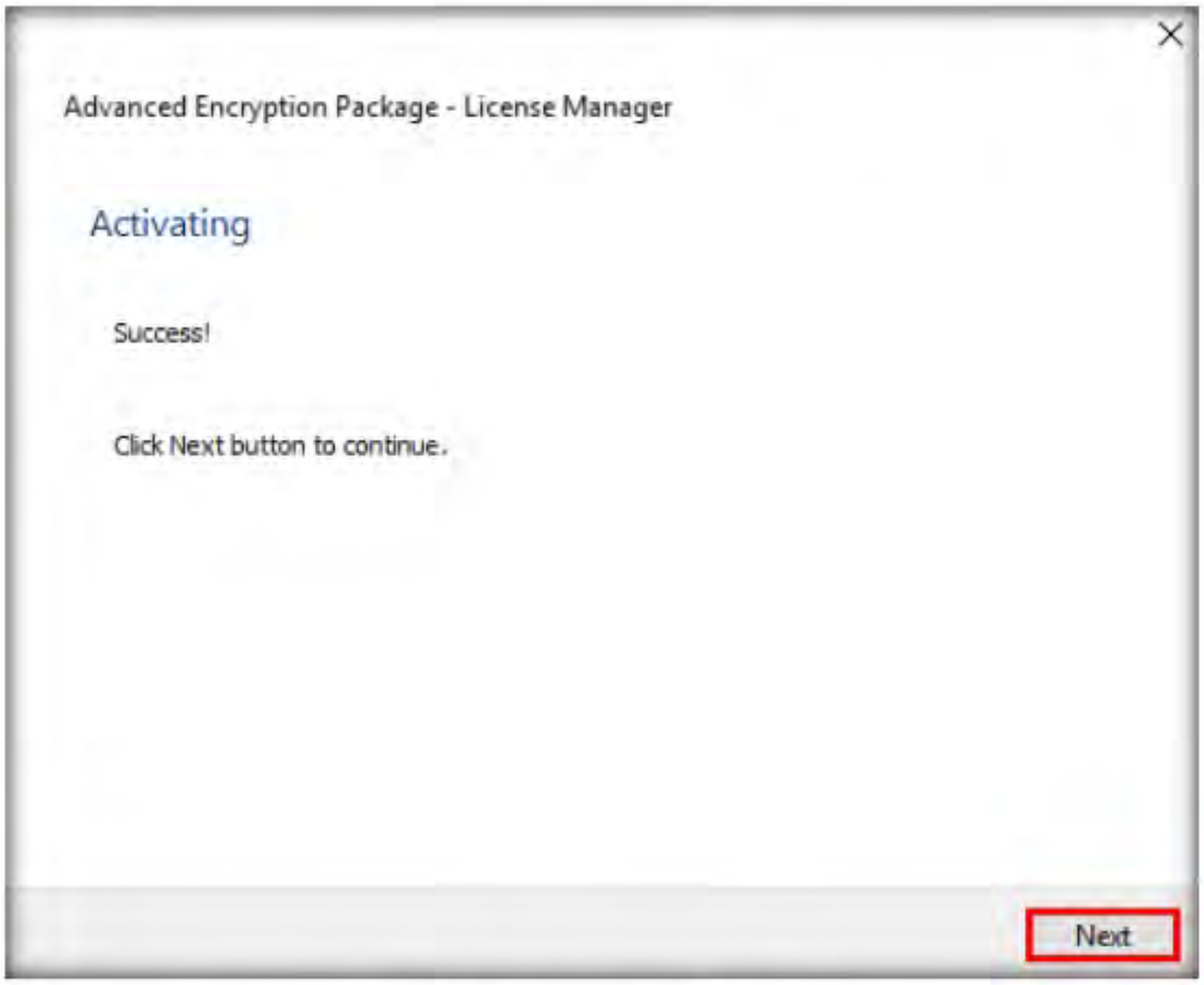


Figure 1.5.5: Activation Window

8. Leave all options set to default in the **License Information** step and click **Finish**.

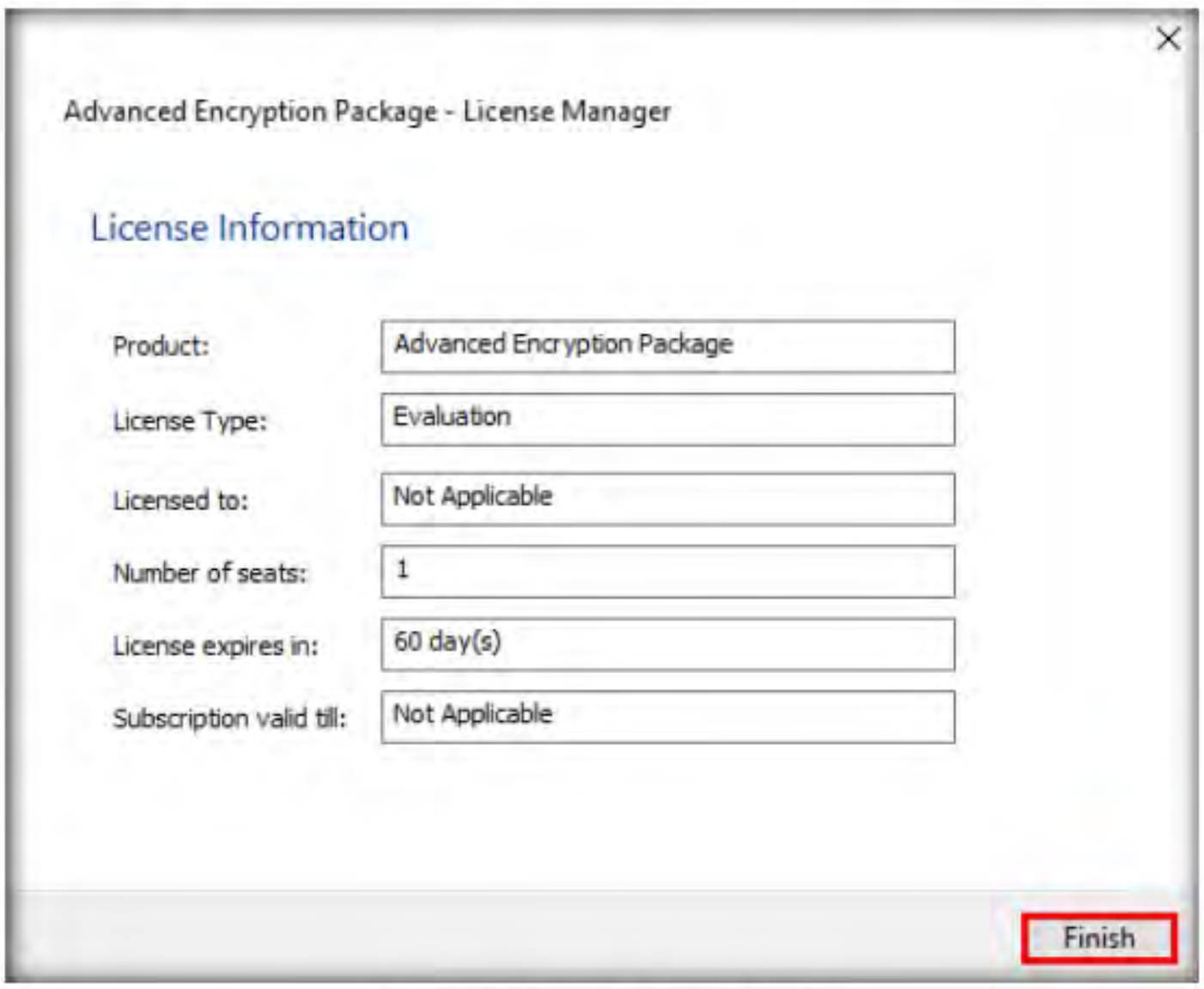


Figure 1.5.6: License Information section

9. The **Advanced Encryption Package** main window appears, as shown in the screenshot.

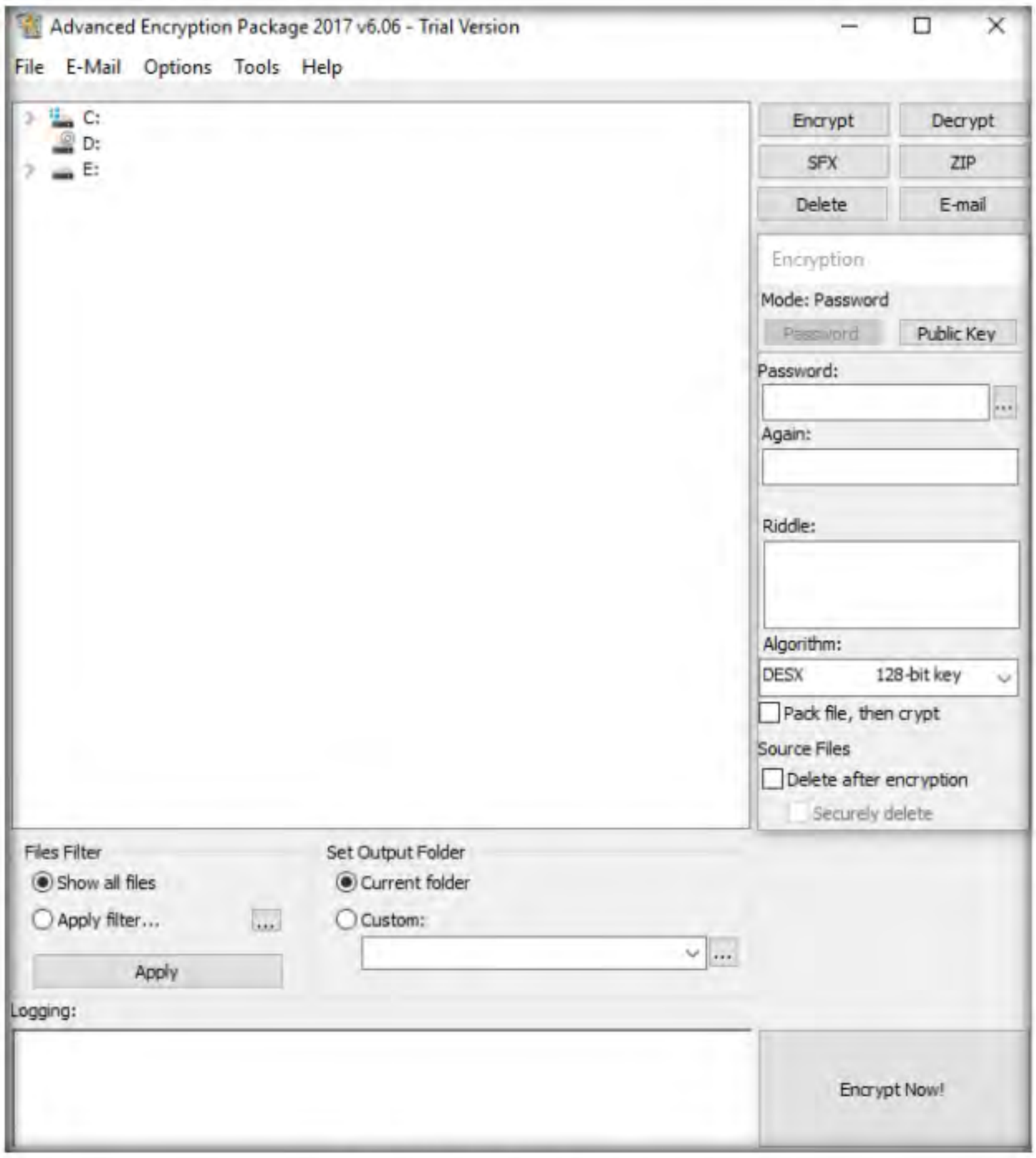


Figure 1.5.7: License Information section

TASK 5.2

Encrypt a File

10. In the **Advanced Encryption Package** window, expand **E:** drive and navigate to **CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package**. Select the **Sample.docx** file located in the given location and click **Encrypt** in the toolbar

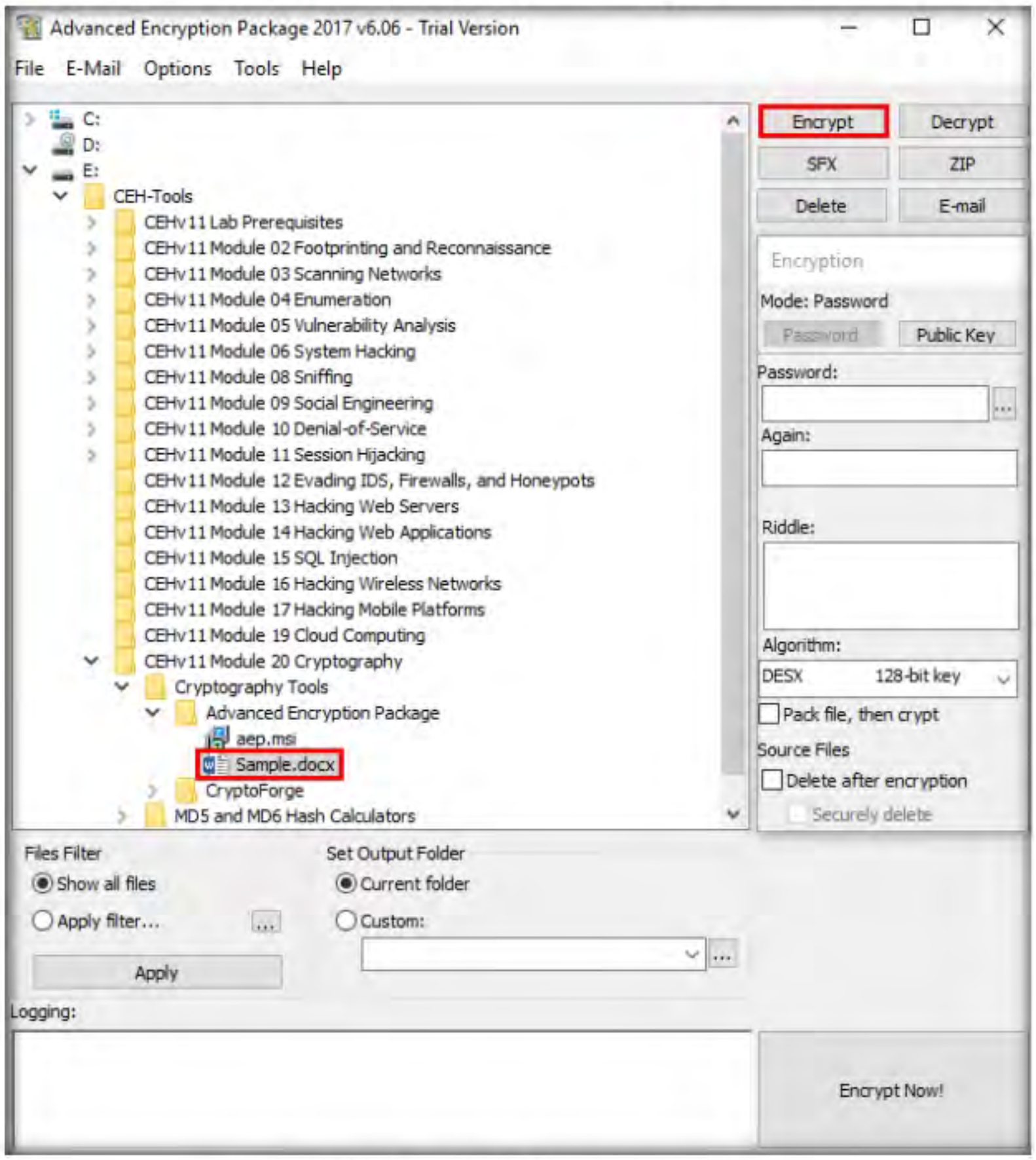


Figure 1.5.8: Main window of Advance Encryption Package

11. You need to provide a password for encryption. In the right-hand pane, enter the password into the **Pwd** field, retype it in the **Again** field, and click **Encrypt Now!** button (Here, the password provided is **test@123**).

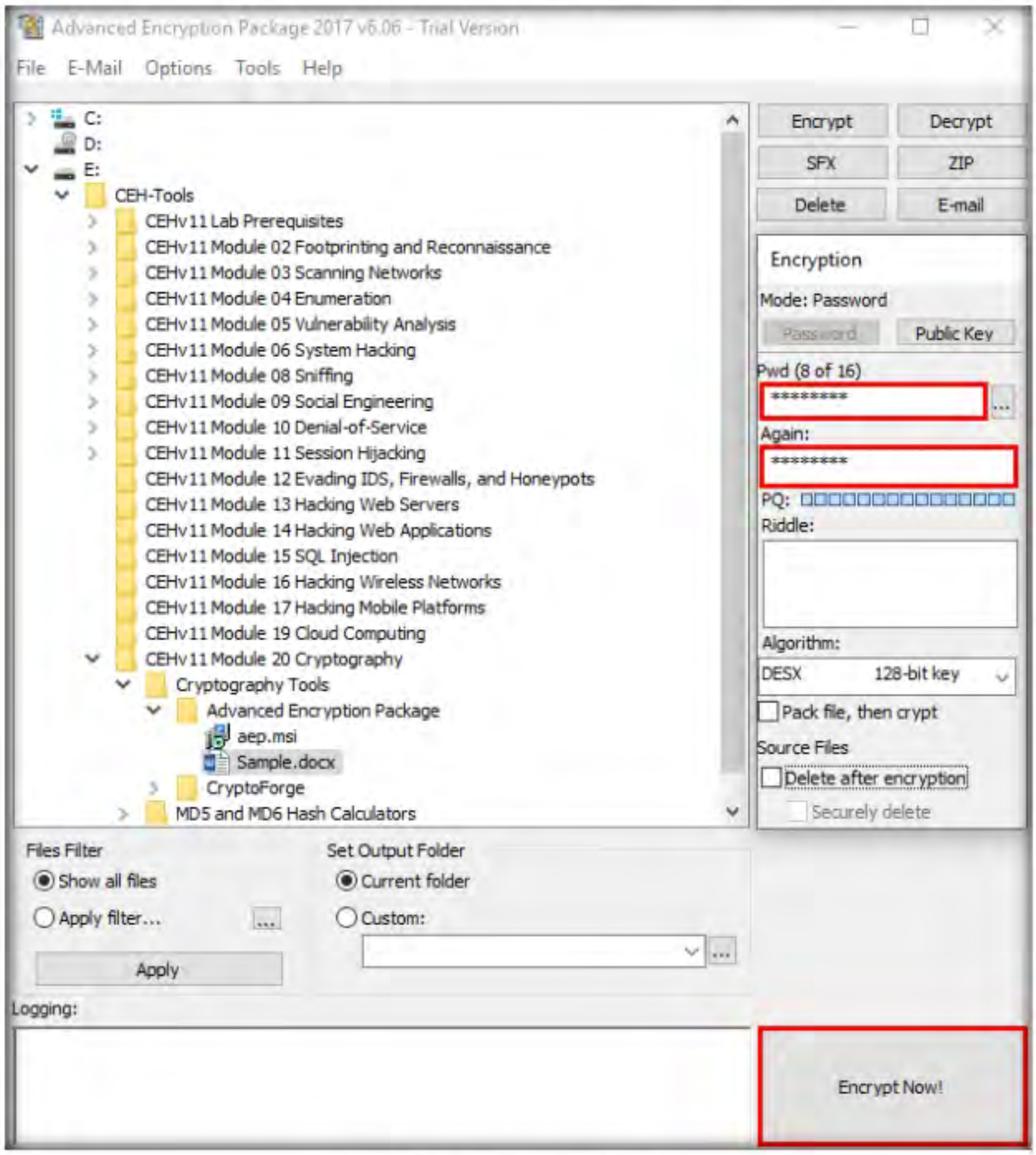


Figure 1.5.9: Encrypting the selected file

12. The encrypted **Sample.docx.aep** file appears in the same location as the original file (i.e., **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package**).
13. To decrypt the file, first, select the encrypted file and click on **Decrypt**.

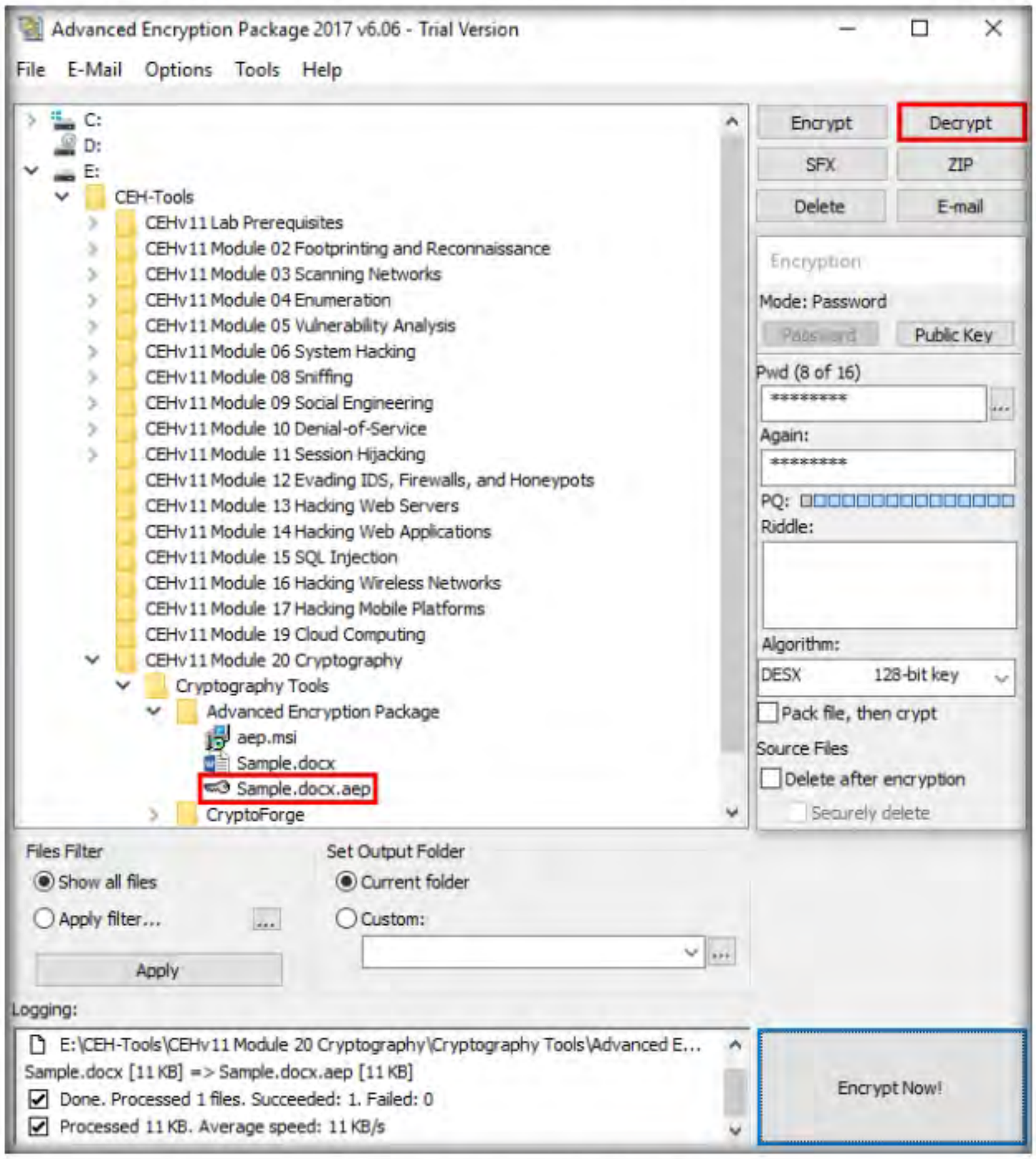


Figure 1.5.10: Decrypting the selected file

14. You will be prompted to enter the password. In the right-hand pane, under the **Password** field, enter the password that you have provided in **Step#11**.
15. Under the **Source file(s)** section in the right-pane, click the **Delete** radio-button to delete the source file **Sample.docx**; then, click **Decrypt Now!**.

TASK 5.3

Decrypt a File

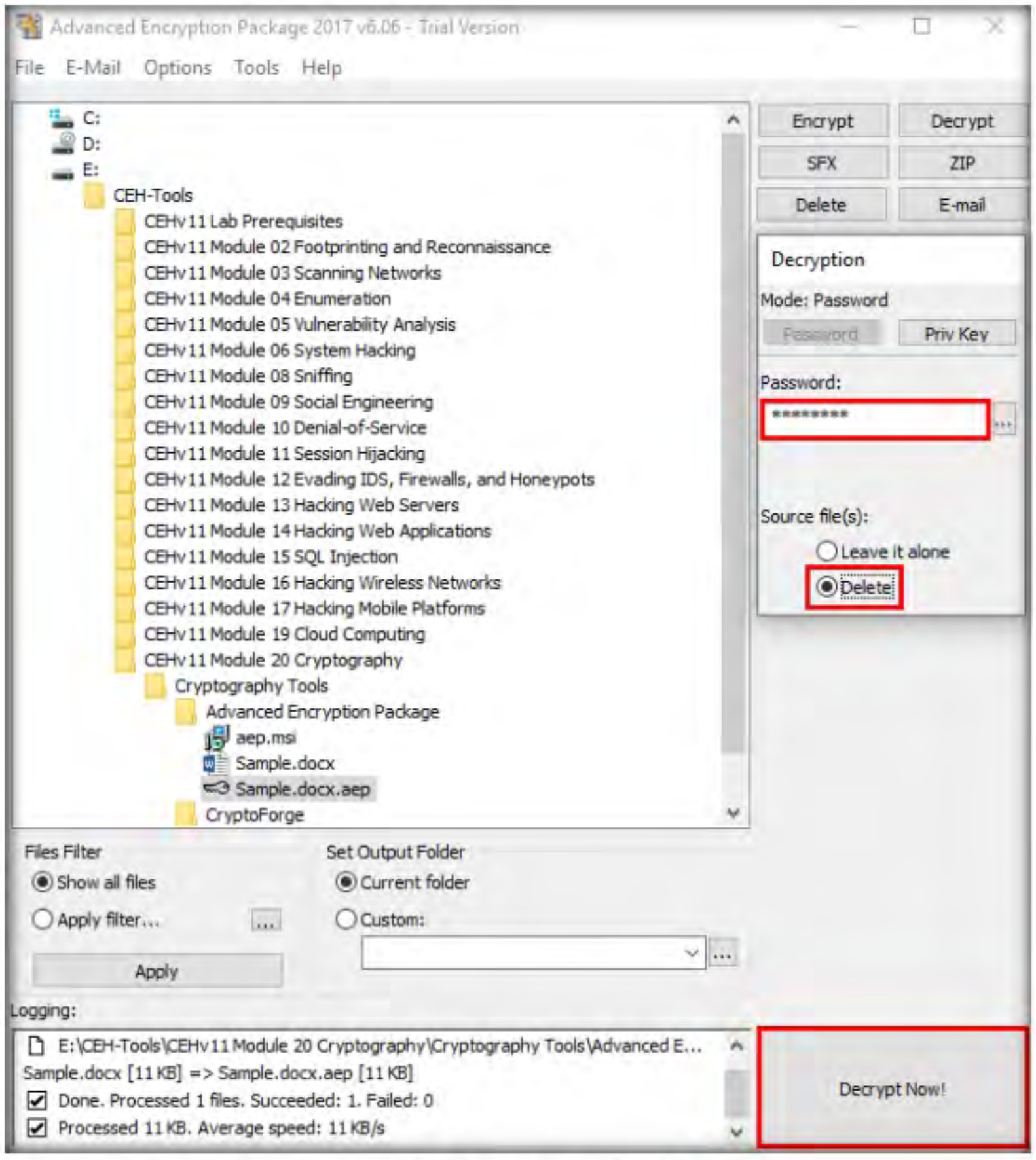


Figure 1.5.11: Decrypting the selected file

16. The **File exists already...** pop-up appears, click **Yes**.

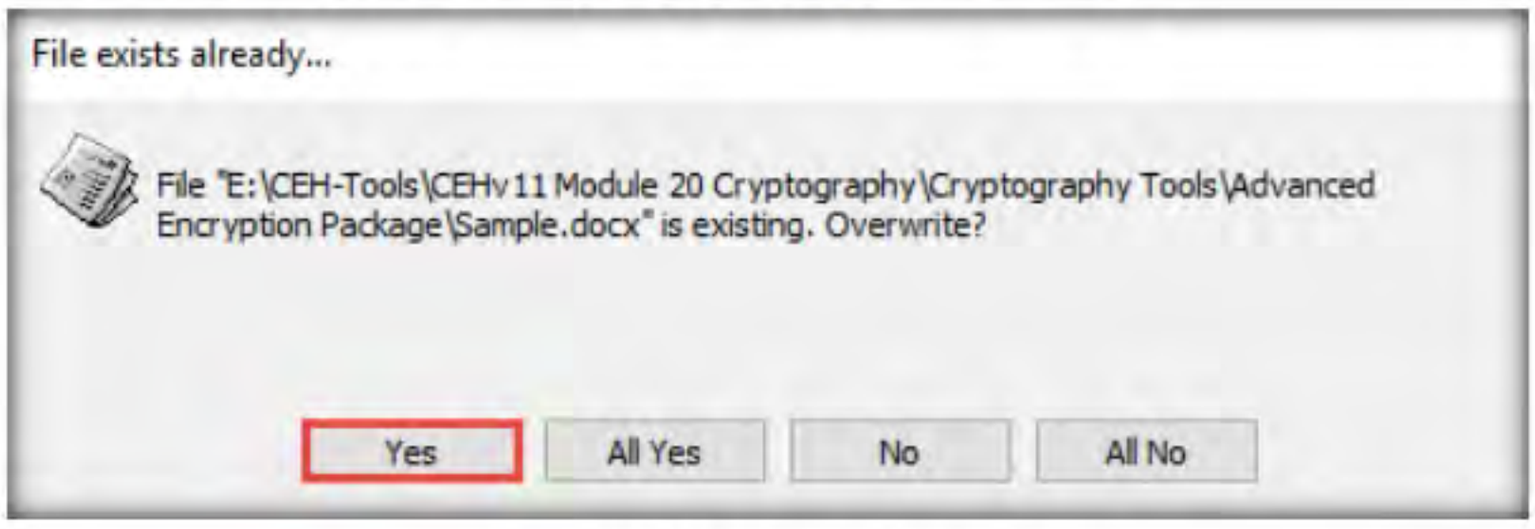


Figure 1.5.12: File exists already… pop-up

17. The decrypted file (**Sample.docx**) appears in the same location, as shown in the screenshot.

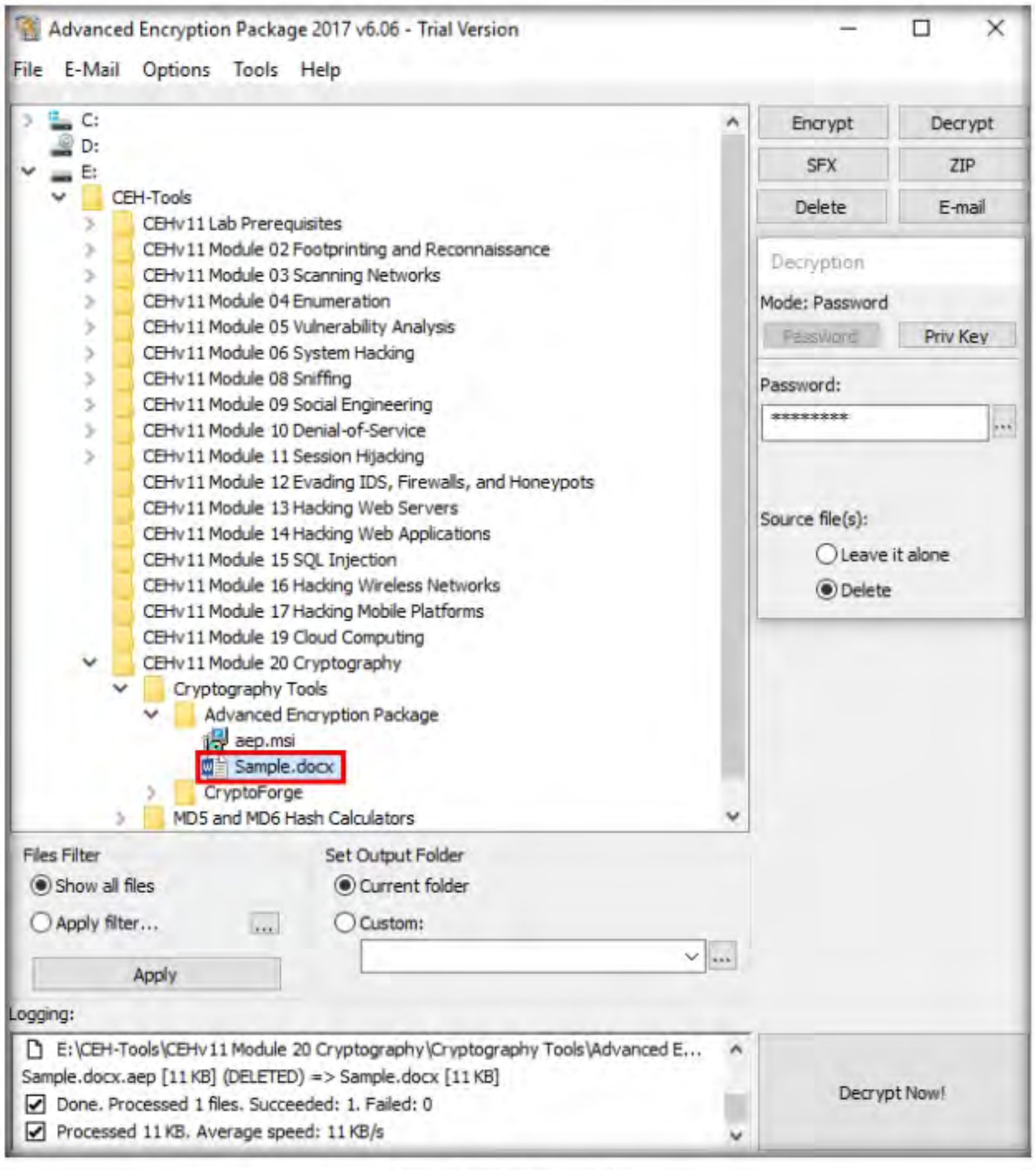


Figure 1.5.13: Decrypted file

Note: In real time, network administrators or ethical hackers use this tool to encrypt files and send it to the intended persons to safeguard the integrity of the files.

18. This concludes the demonstration of performing data encryption using the Advanced Encryption Package.
19. Close all open windows and document all the acquired information.

TASK 6 Encrypt and Decrypt Data using BCTextEncoder

Here, we will use the BCTextEncoder tool to encrypt and decrypt data.

TASK 6.1 Encrypt the Data

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\BCTextEncoder** and double click **BCTextEncoder_v.1.03.2.1.exe**.
2. The **BCTextEncoder Utility** window appears, as shown in the screenshot.

BCTextEncoder simplifies encoding and decoding text data. Plain text data are compressed, encrypted, and converted to text format, which can then be easily copied to the clipboard or saved as a text file. This utility software uses public key encryption methods and password-based encryption, as well as strong and approved symmetric and public key algorithms for data encryption.

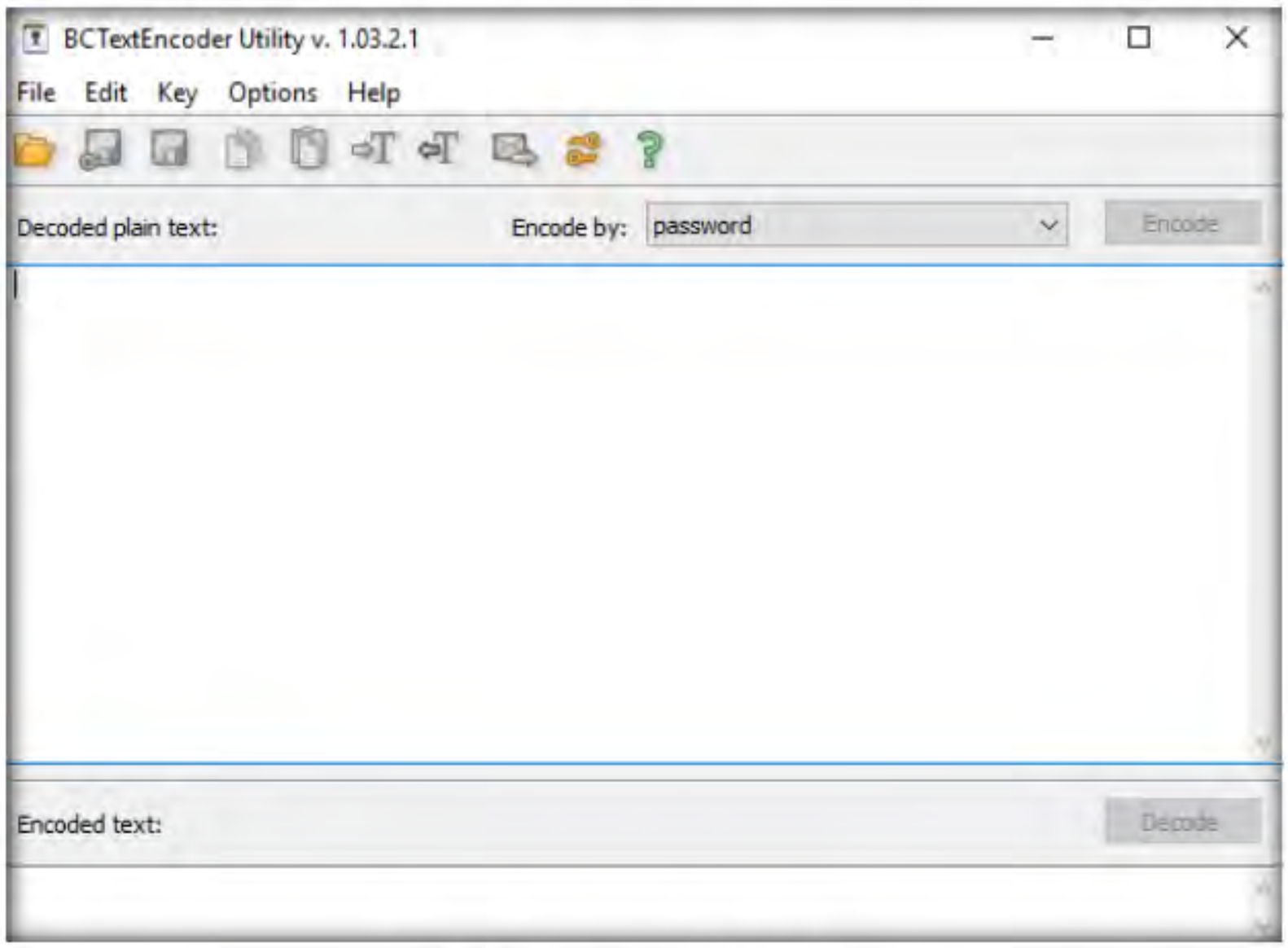


Figure 1.6.1: Main window of BCTextEncoder

3. To encrypt the text, insert text in the clipboard.

Or

Select the data that you want to encode and paste it to the clipboard by pressing **Ctrl+V**.

4. Ensure that the **password** option is selected in the **Encode by** field and click **Encode**.

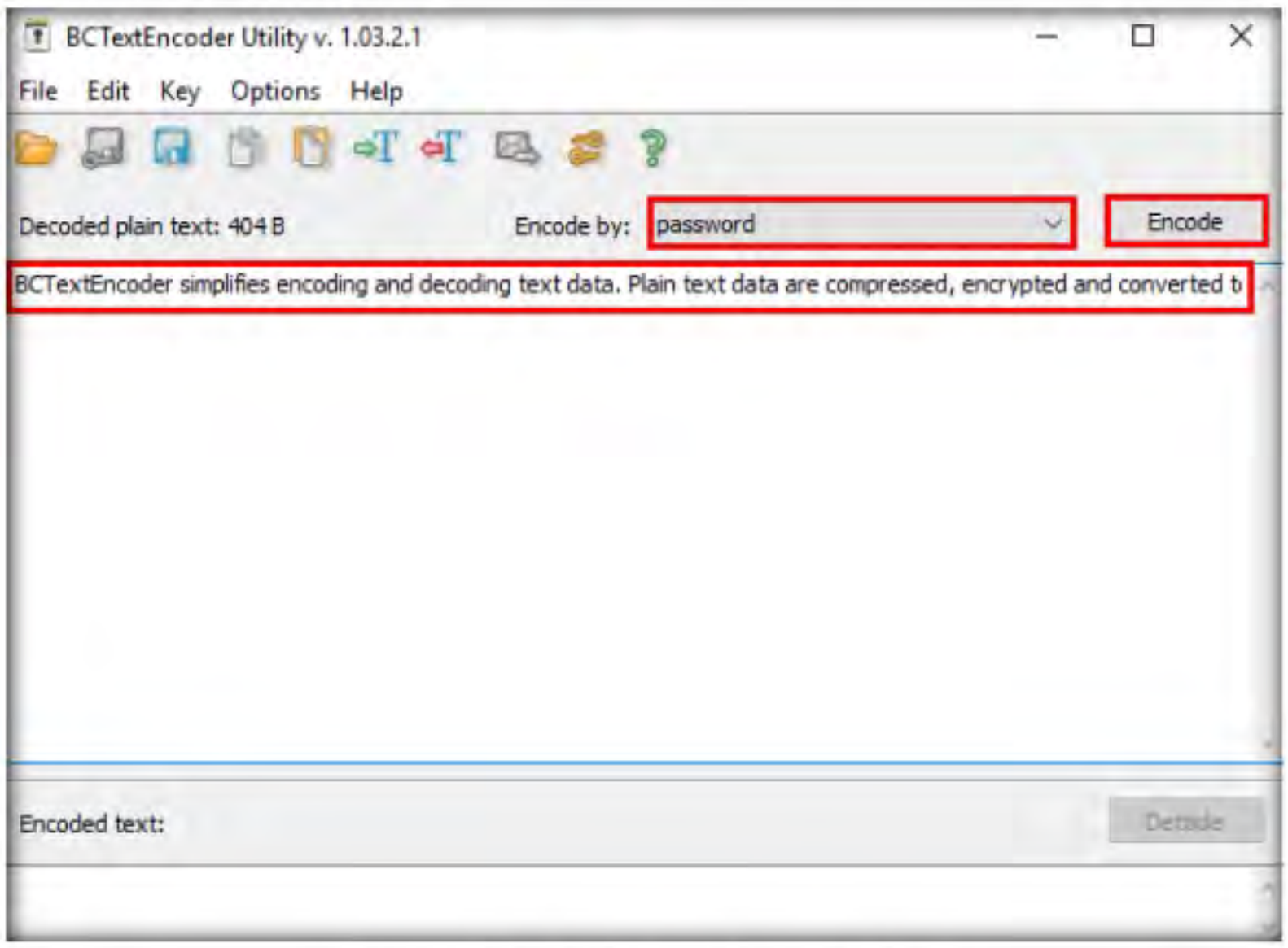


Figure 1.6.2: BCTextEncoder: Secret information in clipboard

5. The **Enter password** pop-up appears; enter the password into the **Password** field and retype it in the **Confirm** field; then, click **OK**. Here, we use the password **test@123**.

Figure 1.6.3: Set the password for encryption

6. **BCTextEncoder** encodes the text and displays it in under the **Encoded text** section, as shown in the screenshot.

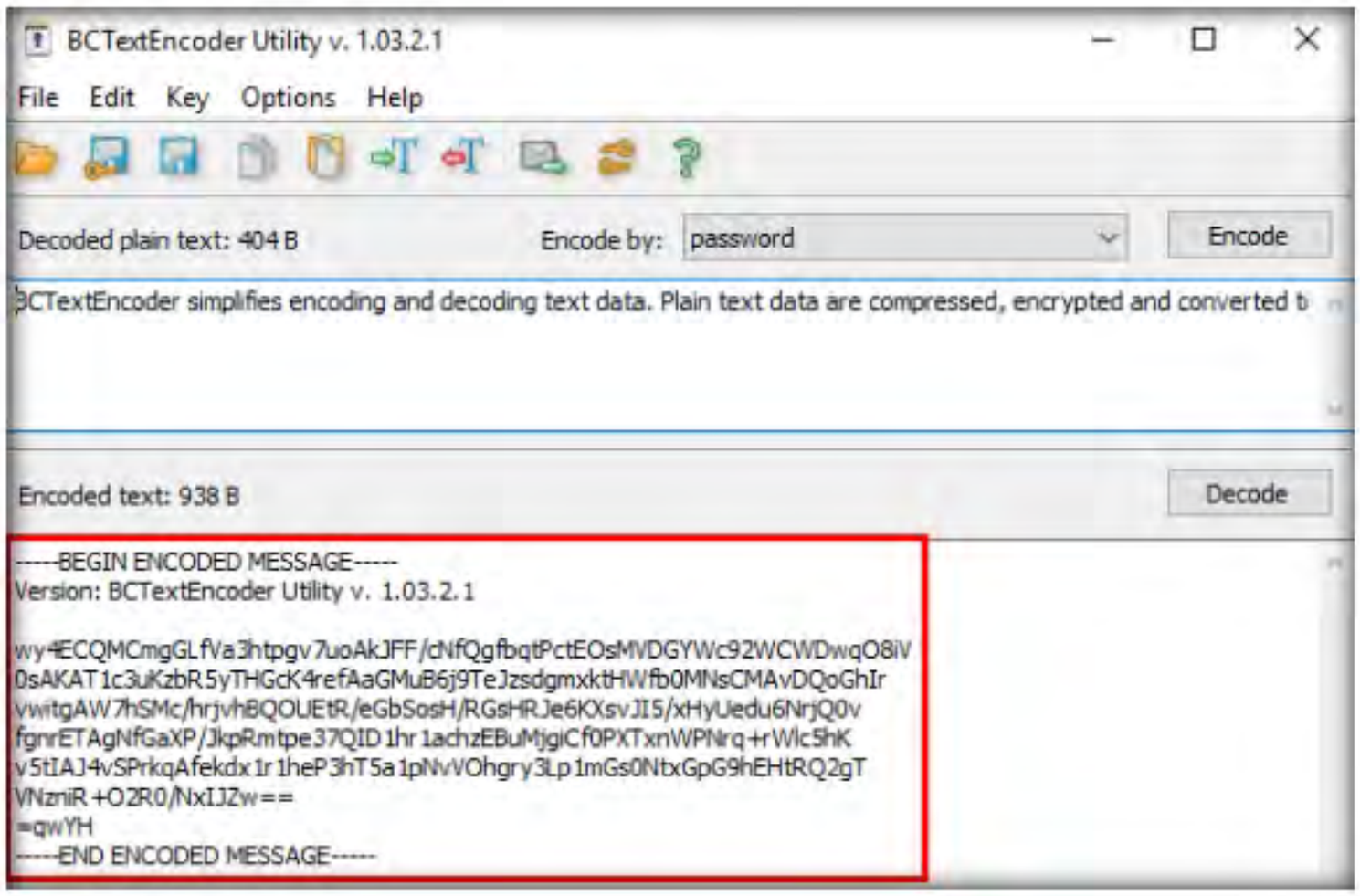


Figure 1.6.4: Encoded text

TASK 6.2

Decrypt the Data

7. To decrypt the data, first, you need to clean the **Decoded plain text** in the clipboard, and then click the **Decode** button.

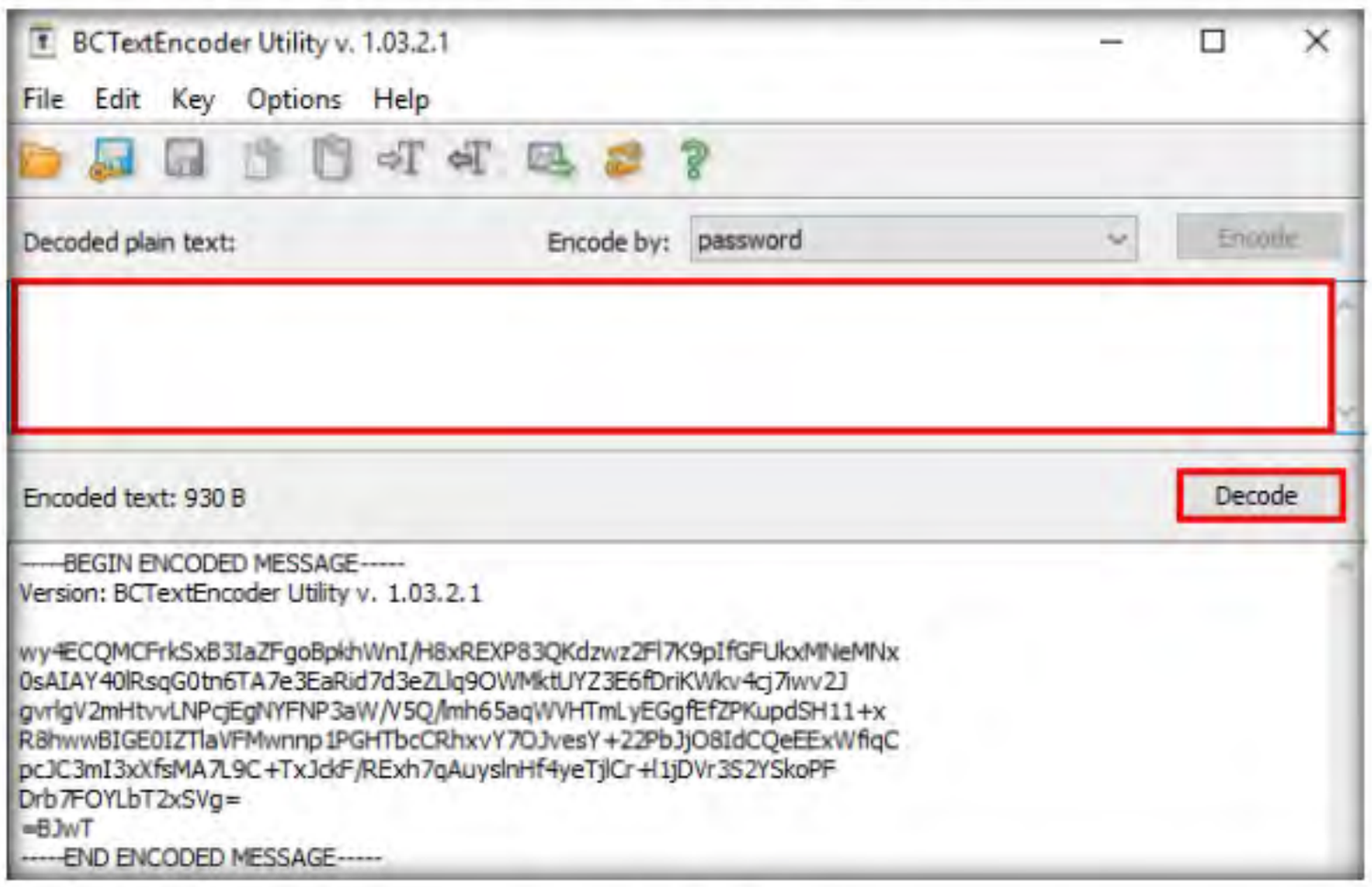


Figure 1.6.5: Decoding data

8. The **Enter password for encoding text** dialog-box appears; insert the **Password** (**test@123**) into the password field and click **OK**.

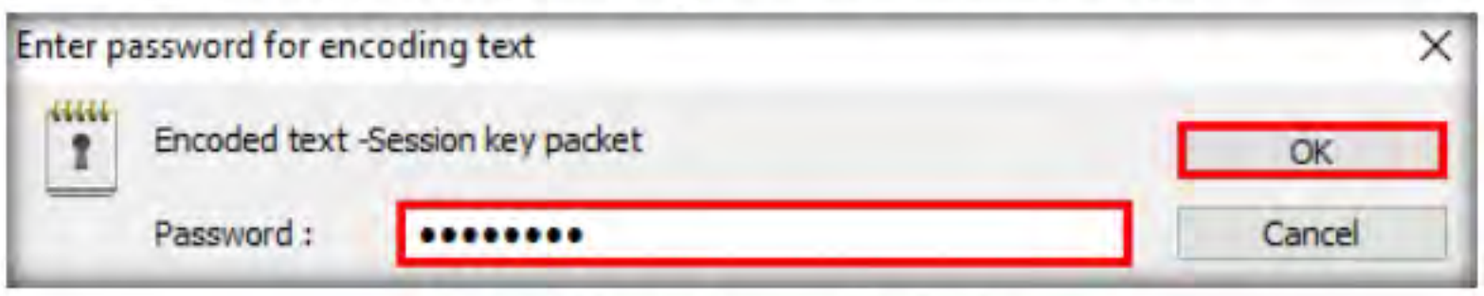


Figure 1.6.6: Enter the password for decoding

You can also use other cryptography tools such as **AxCrypt** (https://www.axcrypt.net), **Microsoft Cryptography Tools** (https://docs.microsoft.com), and **Concealer** (https://www.belightsoft.com) to encrypt confidential data.

9. The decoded plain text appears under the **Decoded plain text** section, as shown in the screenshot.

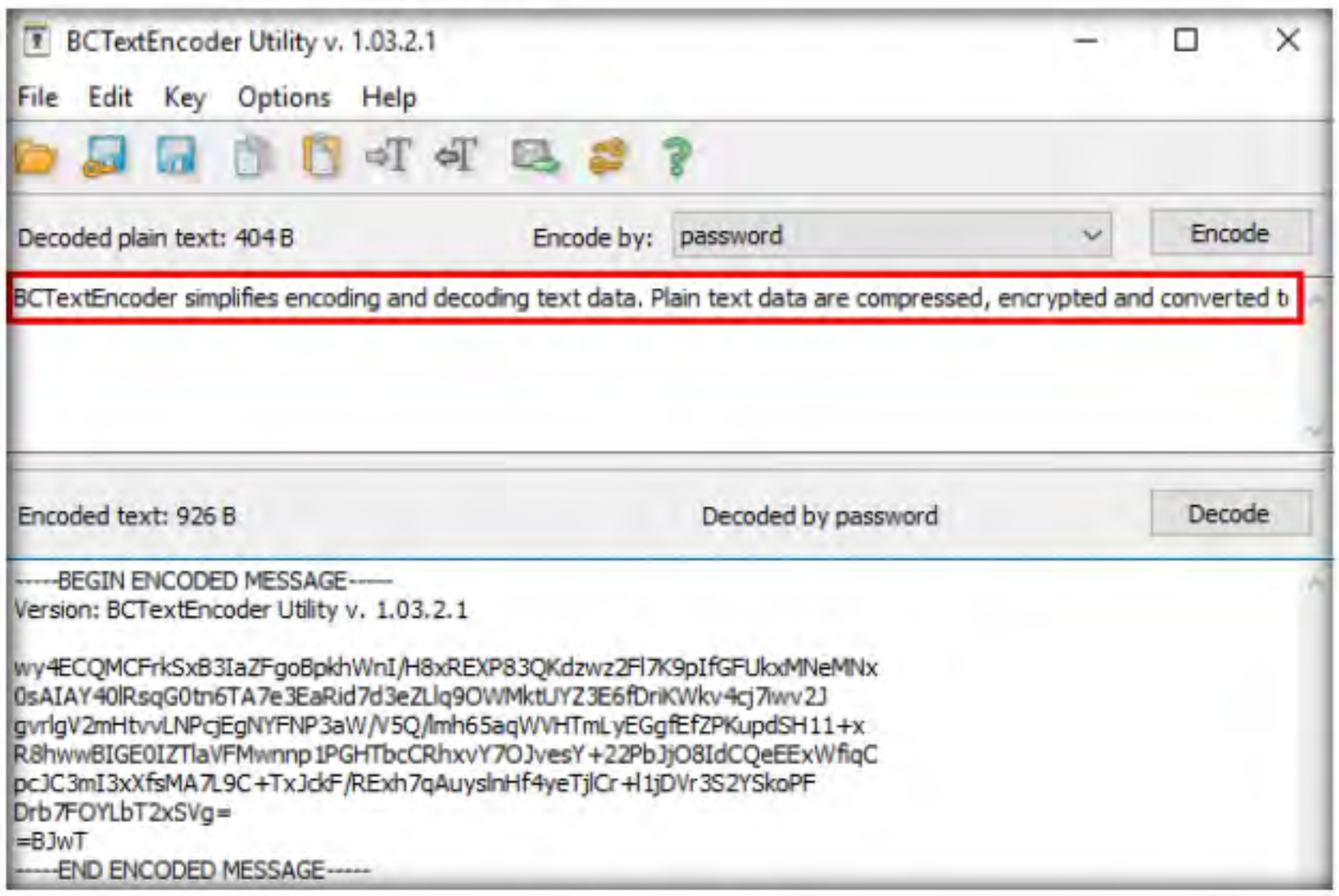


Figure 1.6.7: Output decoded text

Note: In real-time, using this procedure, you can encode the text while sending it to the intended user along with the password used for encryption. The user for whom the text is intended should have the BCTextEncoder application installed on his/her machine. He/she will have to paste the encoded text into the **Encoded text** section and use the password you shared, to decode it to plain text.

10. This concludes the demonstration of encrypting and decrypting the data using BCTextEncoder.
11. Close all open windows and document all the acquired information.
12. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

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

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

Lab 2

Create a Self-signed Certificate

A self-signed certificate is an identity certificate signed by the same entity whose identity it verifies.

ICON KEY

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

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

Lab Scenario

As a professional ethical hacker and penetration tester, you must possess a proper knowledge of creating this certificate as it validates the public key contained within the certificate belonging to the person, company, server, or other entity mentioned.

The labs in this exercise demonstrate the creation of a self-signed certificate.

Lab Objectives

- Create and use self-signed certificates

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Self-signed Certificate

In cryptography and computer security, a self-signed certificate is an identity certificate signed by the same entity whose identity it verifies. However, the term is unrelated to the identity of the person or organization that actually performs the signing procedure.

Lab Tasks

TASK 1

Create and Use Self-signed Certificates

Here, we will create a self-signed certificate in Windows Server 2019.

1. Turn on the **Windows Server 2019** and log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 1.1

Verify Self-Signed Certificate

2. Before you start this task, you will need to check with your local sites whether they include a self-signed certificate.
3. Launch any web browser (here, **Google Chrome**), type **https://www.goodshopping.com** in the address bar, and press **Enter**.
4. As you are using an https channel to browse the website, it displays a page stating that **This site can't be reached**.
5. As the site does not have a self-signed certificate, it displays a connection refused message, as shown in the screenshot. Close the web browser.

Self-signed certificates are widely used for testing servers. In self-signed certificates, a user creates a pair of public and private keys using a certificate creation tool such as Adobe Acrobat Reader, Java's keytool, Apple's Keychain, etc. and signs the document with the public key.

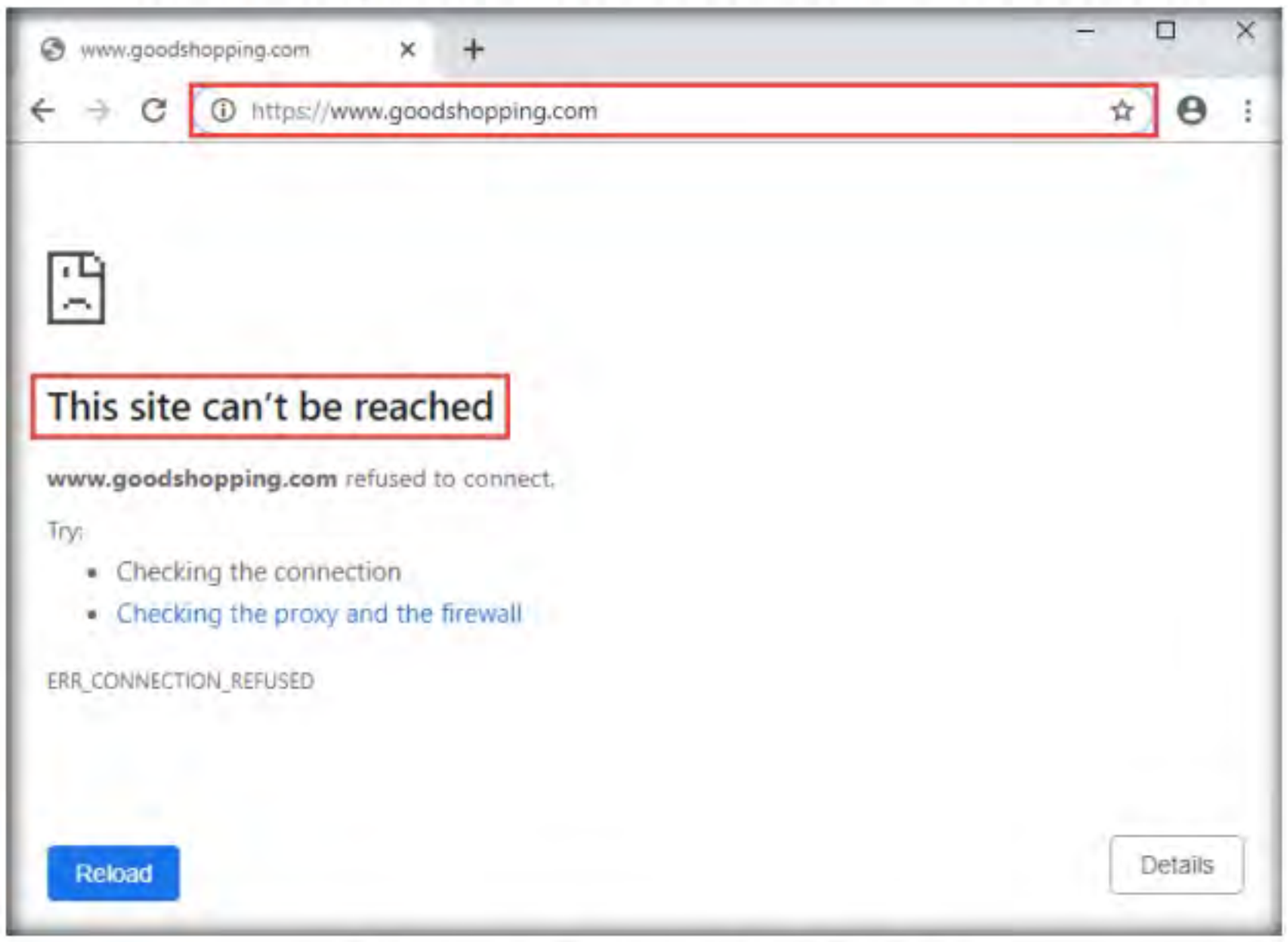


Figure 2.1.1: www.goodshopping.com before adding Certificate

TASK 1.2

Launch IIS Manager

6. Click the **Type here to search** icon ( ) present in the bottom-left of **Desktop** and type **iis**. Select **Internet Information Services (IIS) Manager** from the results.

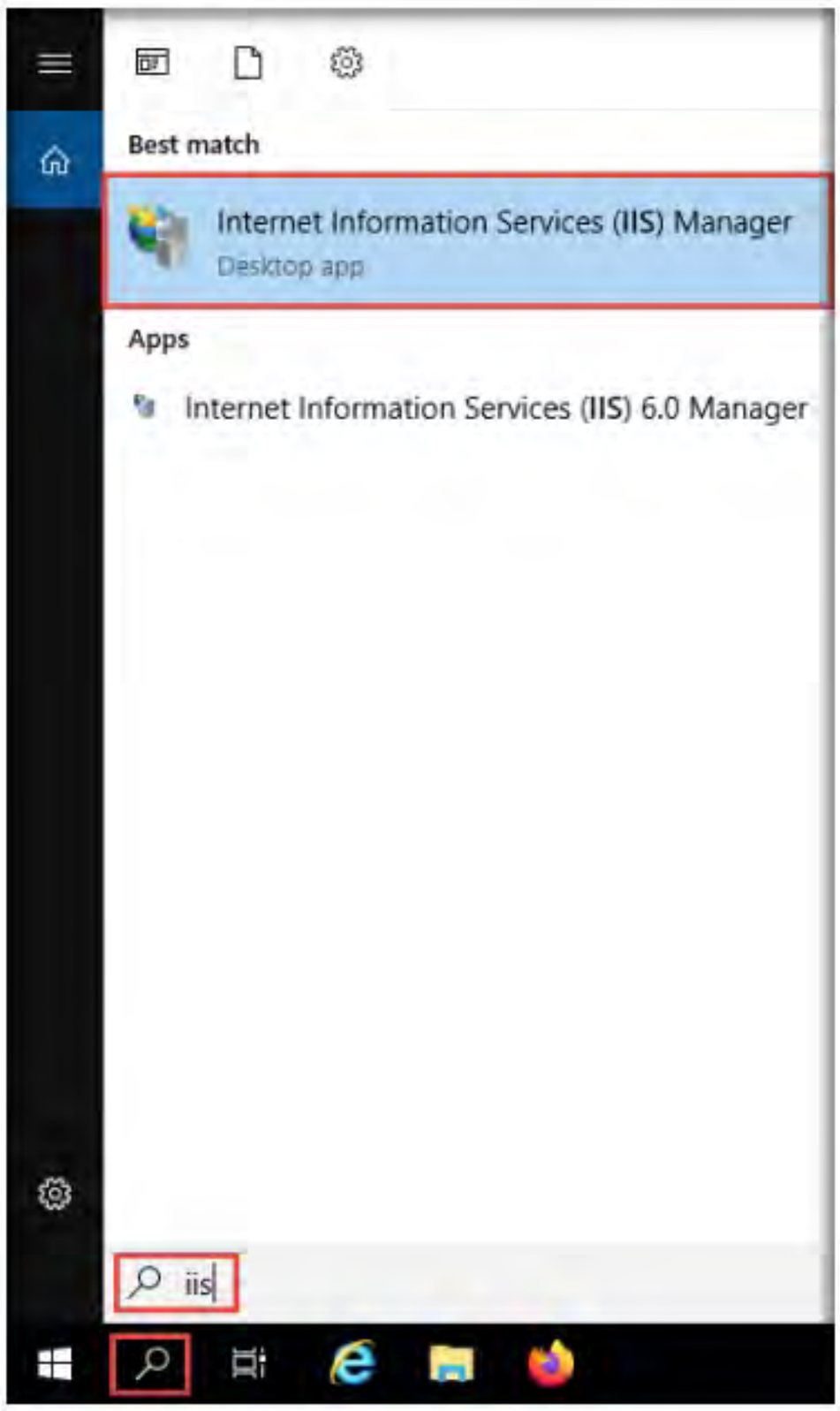


Figure 2.1.2: Launch IIS Manager

The recipient requests the private key from the sender in order to verify the certificate. However, certificate verification rarely occurs due to the necessity of disclosing the private key: this makes self-signed certificates useful only in a self-controlled testing environment.

TASK 1.3

Configure Server Certificates

7. The **Internet Information Services (IIS) Manager** window appears; click the machine name (**SERVER2019 (SERVER2019\Administrator)**) under the **Connections** section from the left-hand pane.

8. In **SERVER2019 Home**, double-click **Server Certificates** in the **IIS** section.

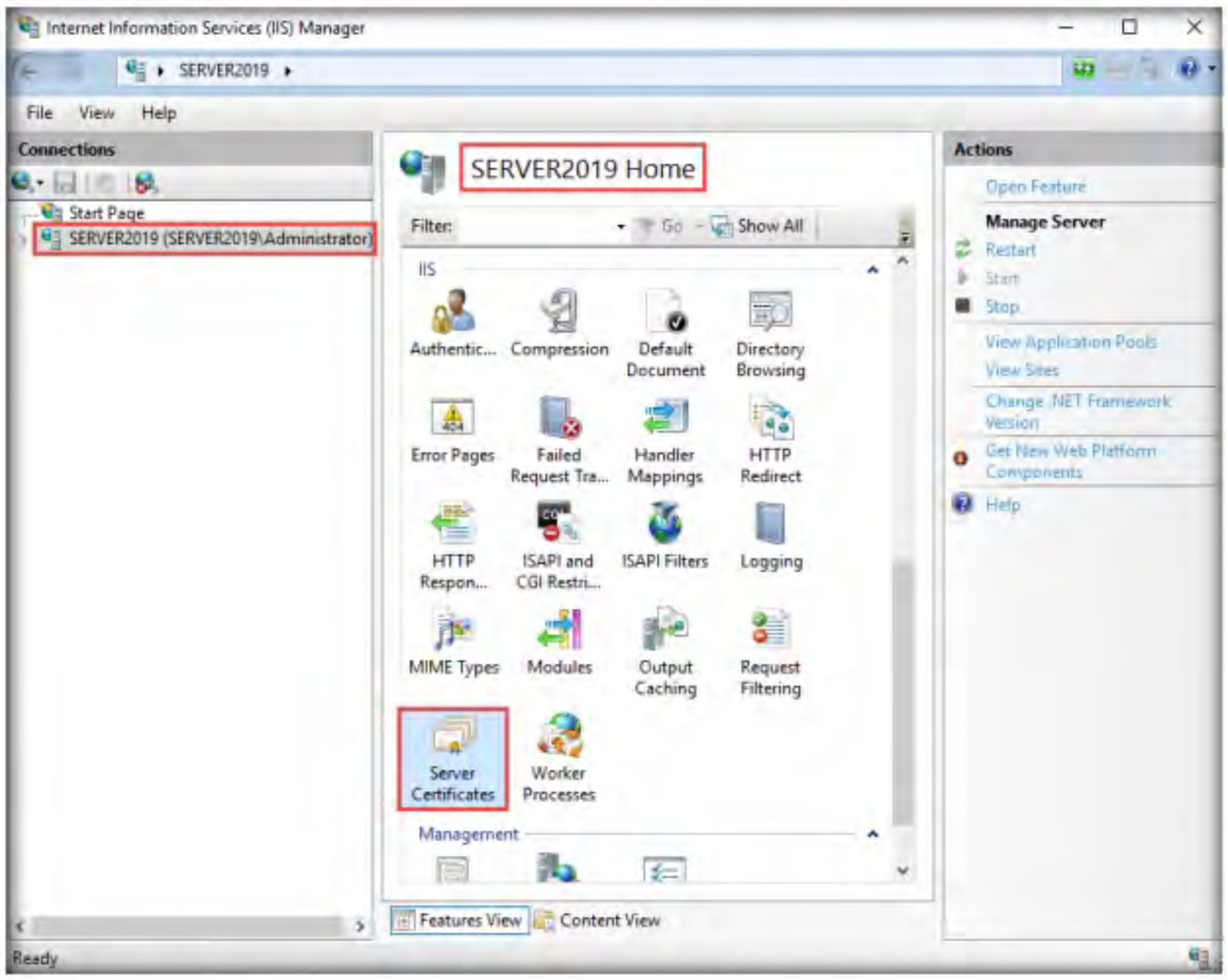


Figure 2.1.3: IIS Manager Server Certificates

TASK 1.4

Create a Self-signed Certificate

9. The **Server Certificates** wizard appears; click **Create Self-Signed Certificate...** from the right-hand pane in the **Actions** section.

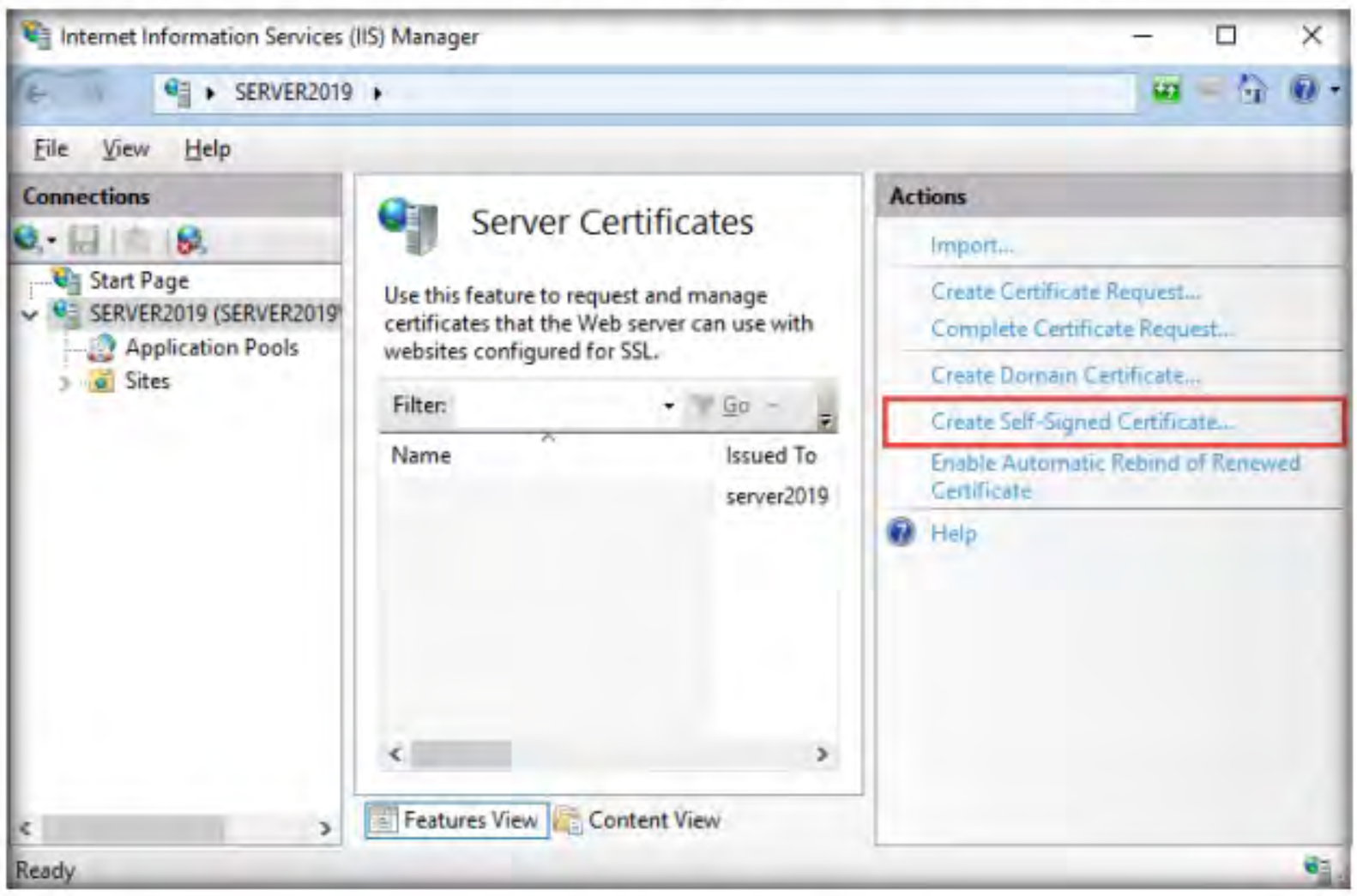


Figure 2.1.4: Server Certificates

10. The **Create Self-Signed Certificate** window appears; type **GoodShopping** in the **Specify a friendly name for the certificate** field. Ensure that the **Personal** option is selected in the **Select a certificate store for the new certificate** field; then, click **OK**.

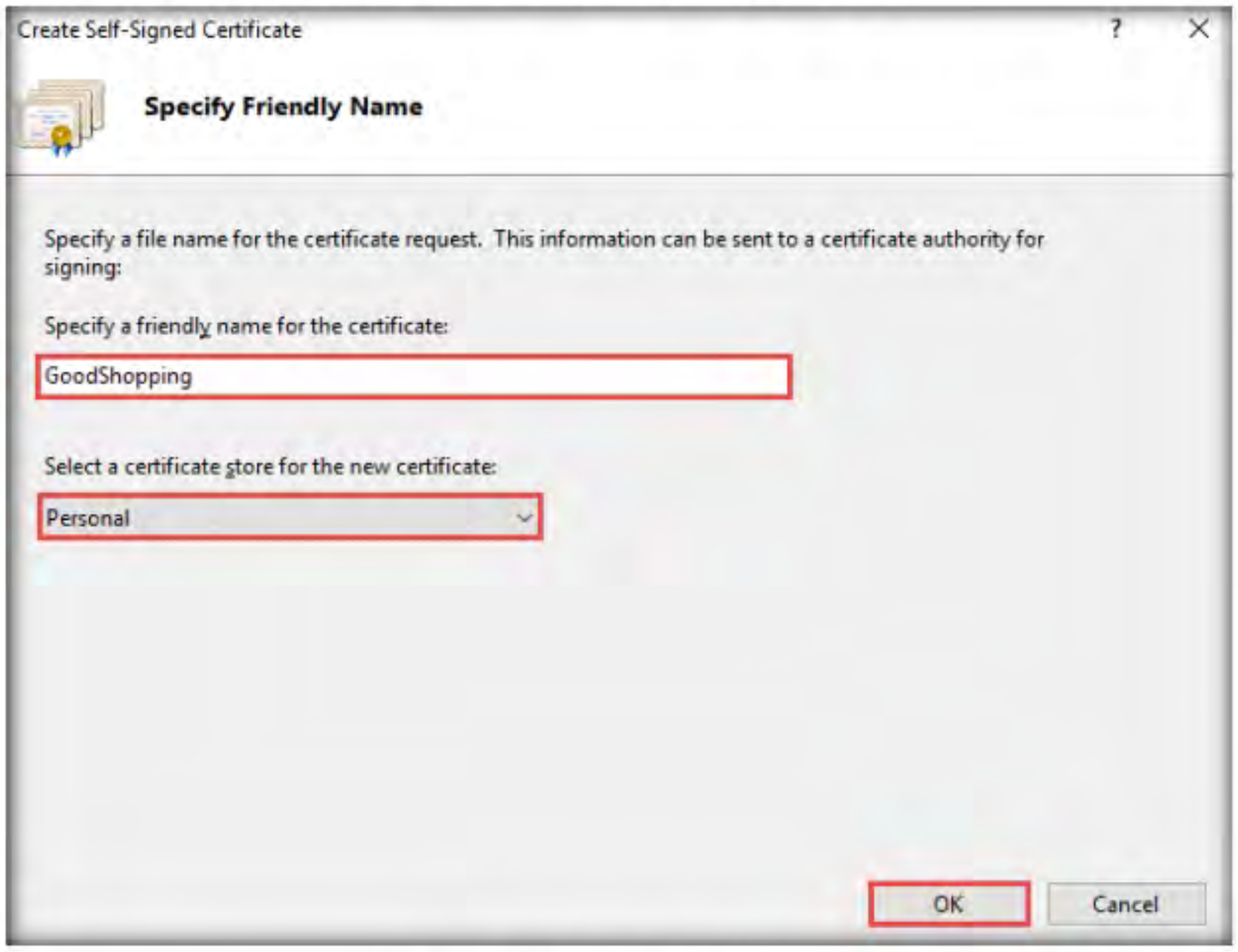


Figure 2.1.5: Specify Friendly Name

11. A newly created self-signed certificate will be displayed in the **Server Certificates** pane, as shown in the screenshot.

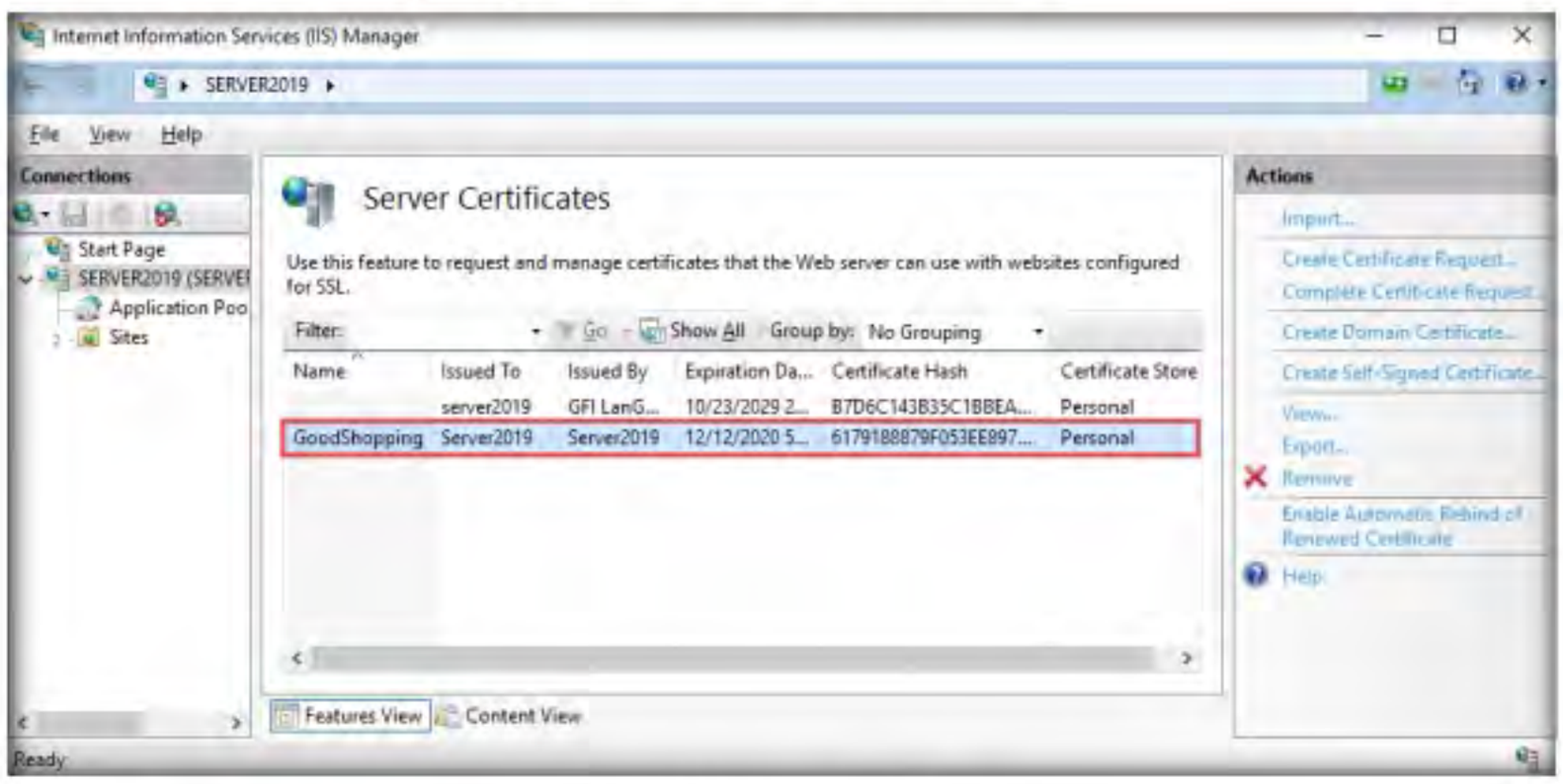


Figure 2.1.6: Server Certificates

TASK 1.5

Edit Bindings

12. Expand the **Sites** node from the left-hand pane, and select **GoodShopping** from the available sites. Click **Bindings...** from the right-hand pane in the **Actions** section.

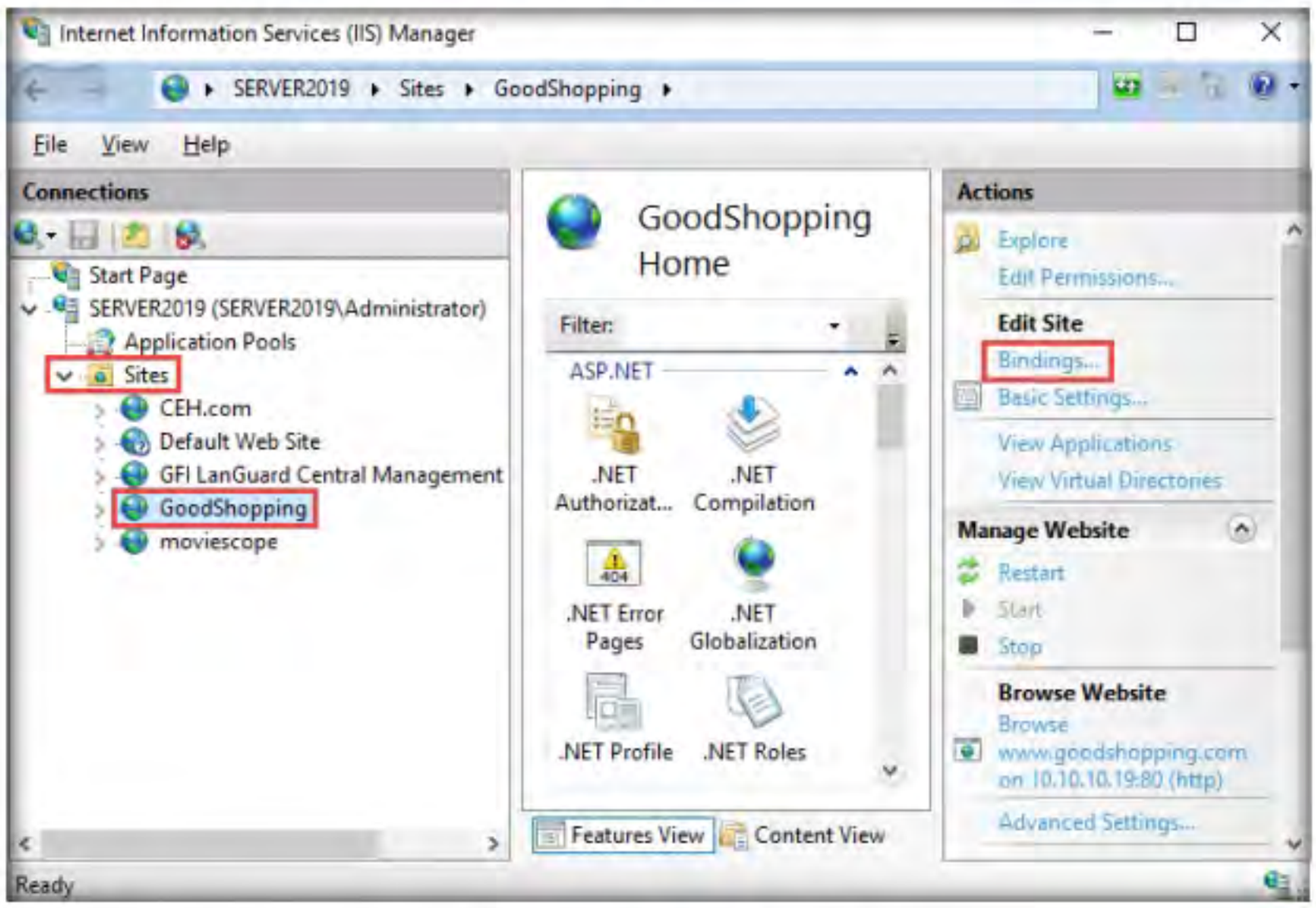


Figure 2.1.7: Editing Site Bindings

13. The **Site Bindings** window appears; click **Add...**.

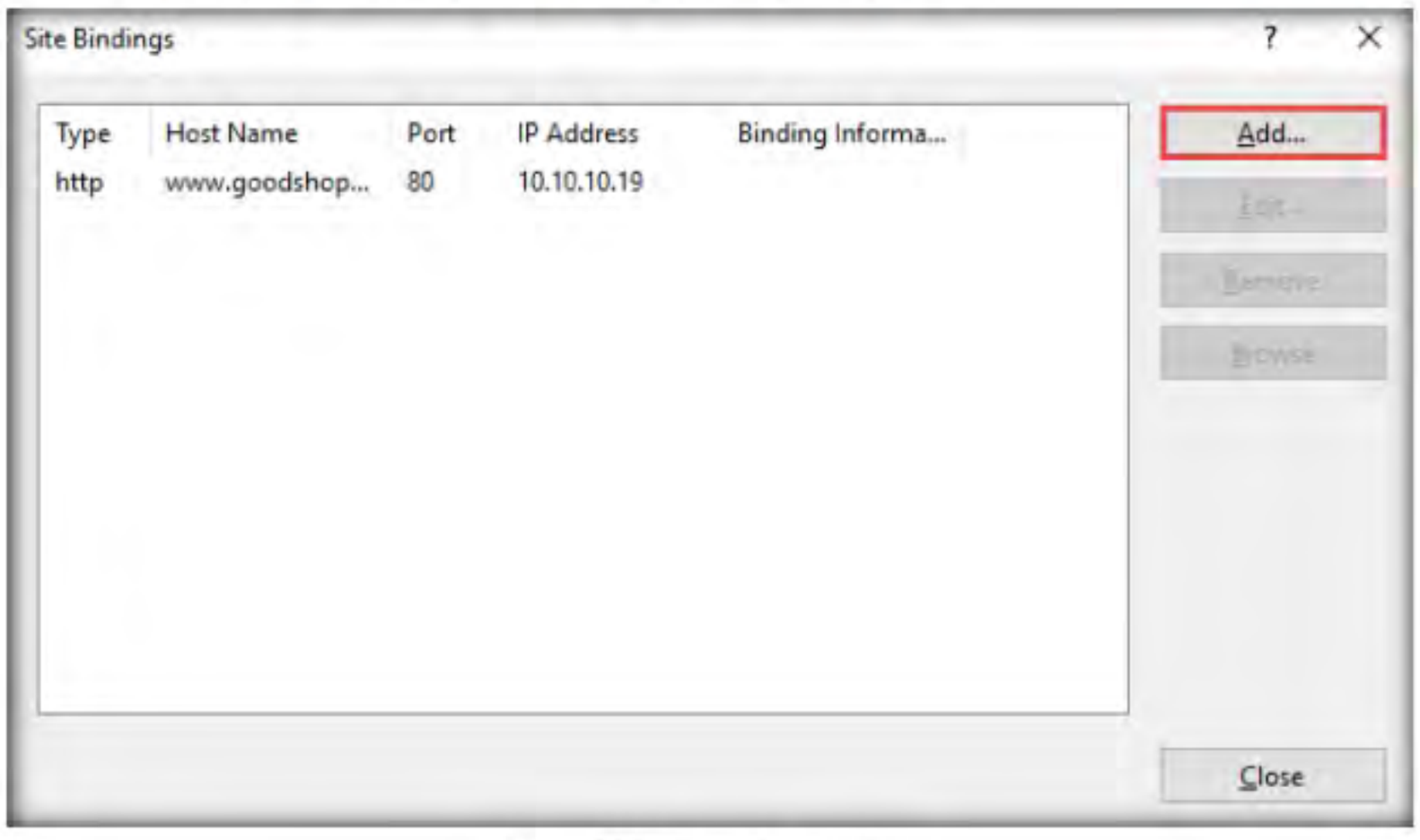


Figure 2.1.8: Site Bindings window

14. The **Add Site Binding** window appears; choose **https** from the **Type** field drop-down list. Once you choose the https type, the port number in the **Port** field automatically changes to **443** (the channel on which HTTPS runs).
15. Choose the **IP address** on which the site is hosted (here, **10.10.10.19**).
16. Under the **Host name** field, type **www.goodshopping.com**. Under the **SSL certificate** field, select **GoodShopping** from the drop-down list, and click **OK**.

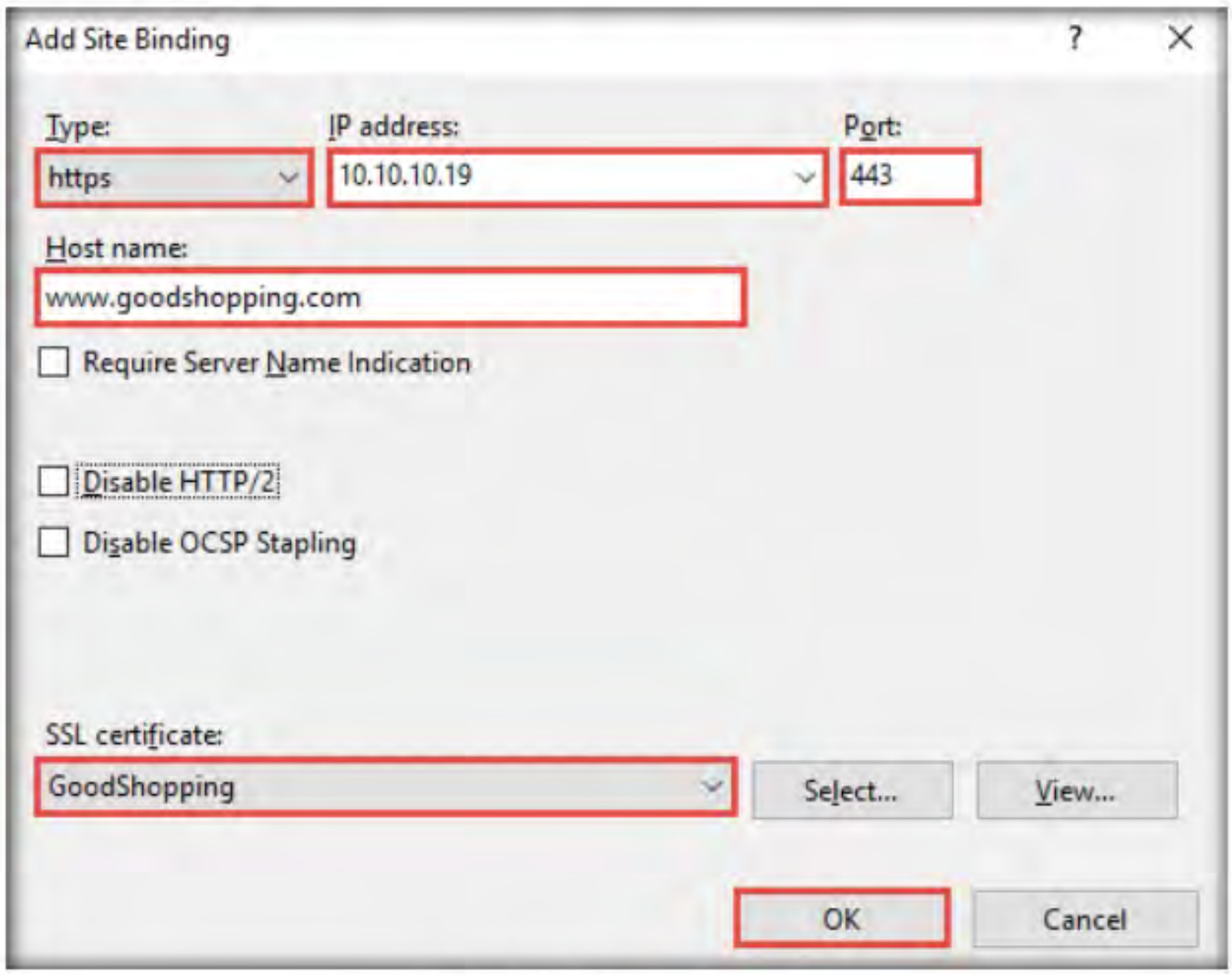


Figure 2.1.9: Adding Site Binding

17. The newly created SSL certificate is added to the **Site Bindings** window; then, click **Close**.

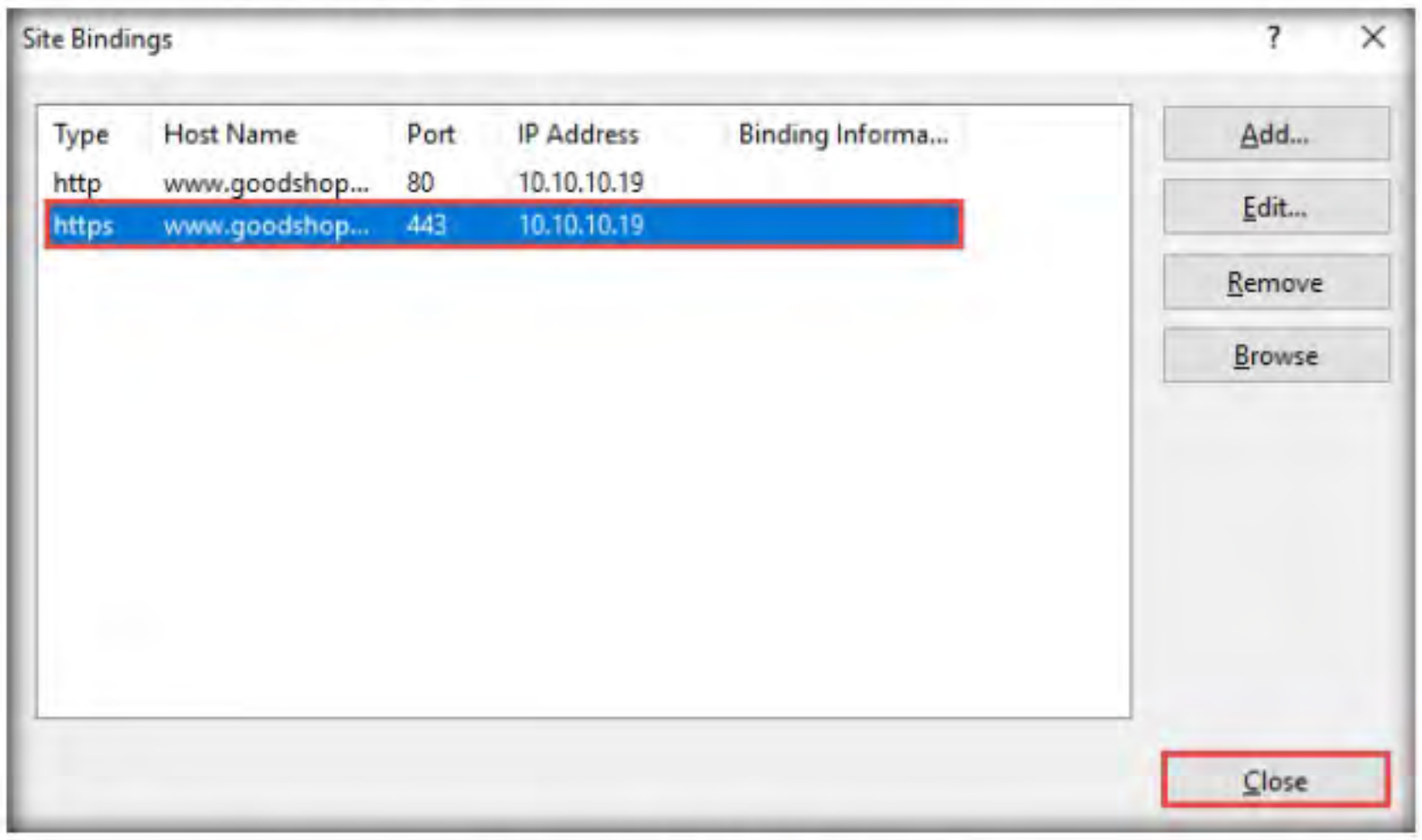


Figure 2.1.10: Added HTTPS Channel

18. Now, right-click the name of the site for which you have created the self-signed certificate (here, **GoodShopping**) and click **Refresh** from the context menu.

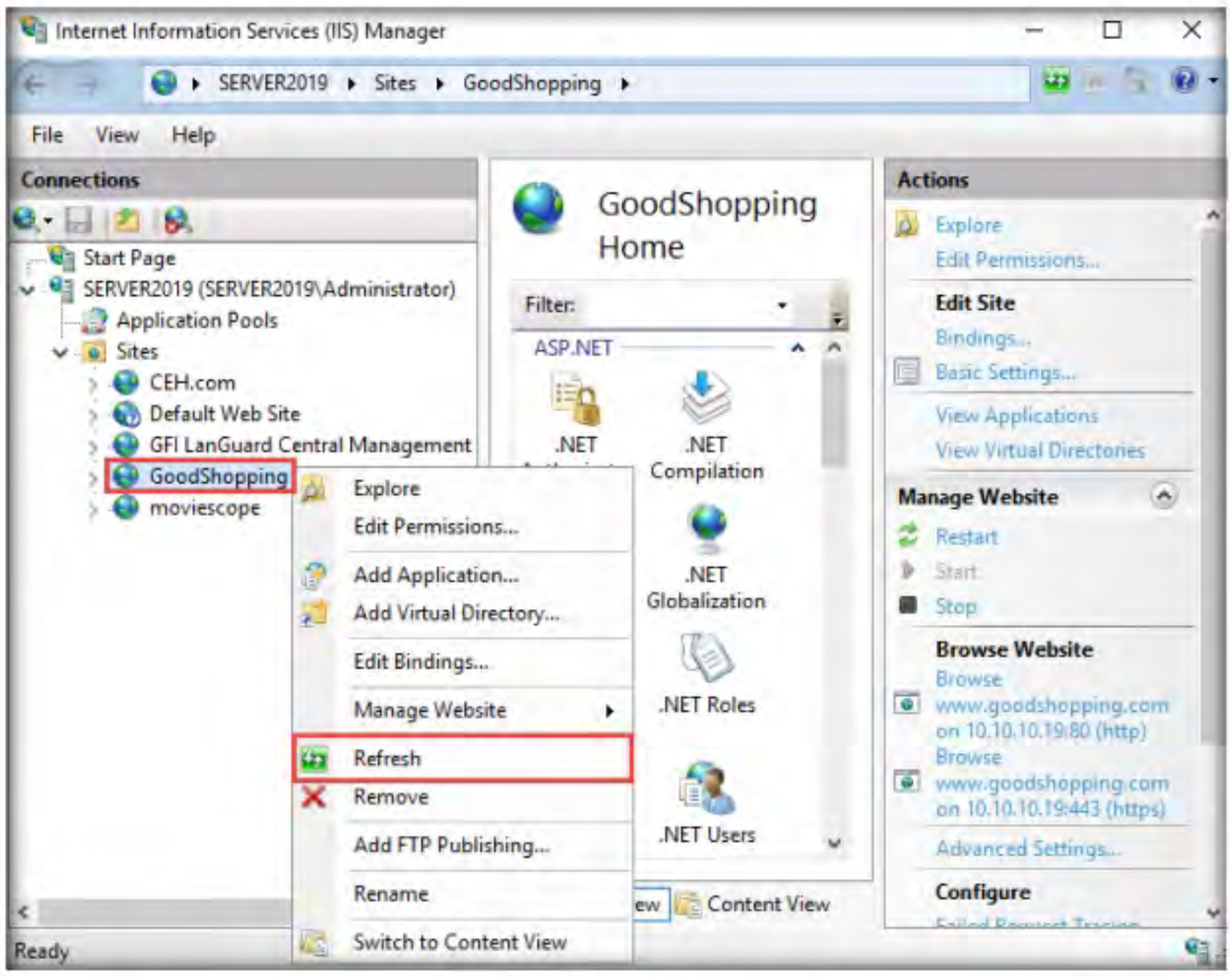


Figure 2.1.11: Added HTTPS Channel

19. Minimize the **Internet Information Services (IIS) Manager** window.

TASK 1.6

Open SSL Website

20. Open the **Google Chrome** browser, type **https://www.goodshopping.com** in the address bar, and press **Enter**.
21. The **Your connection is not private** message appears, click **ADVANCED** to proceed.

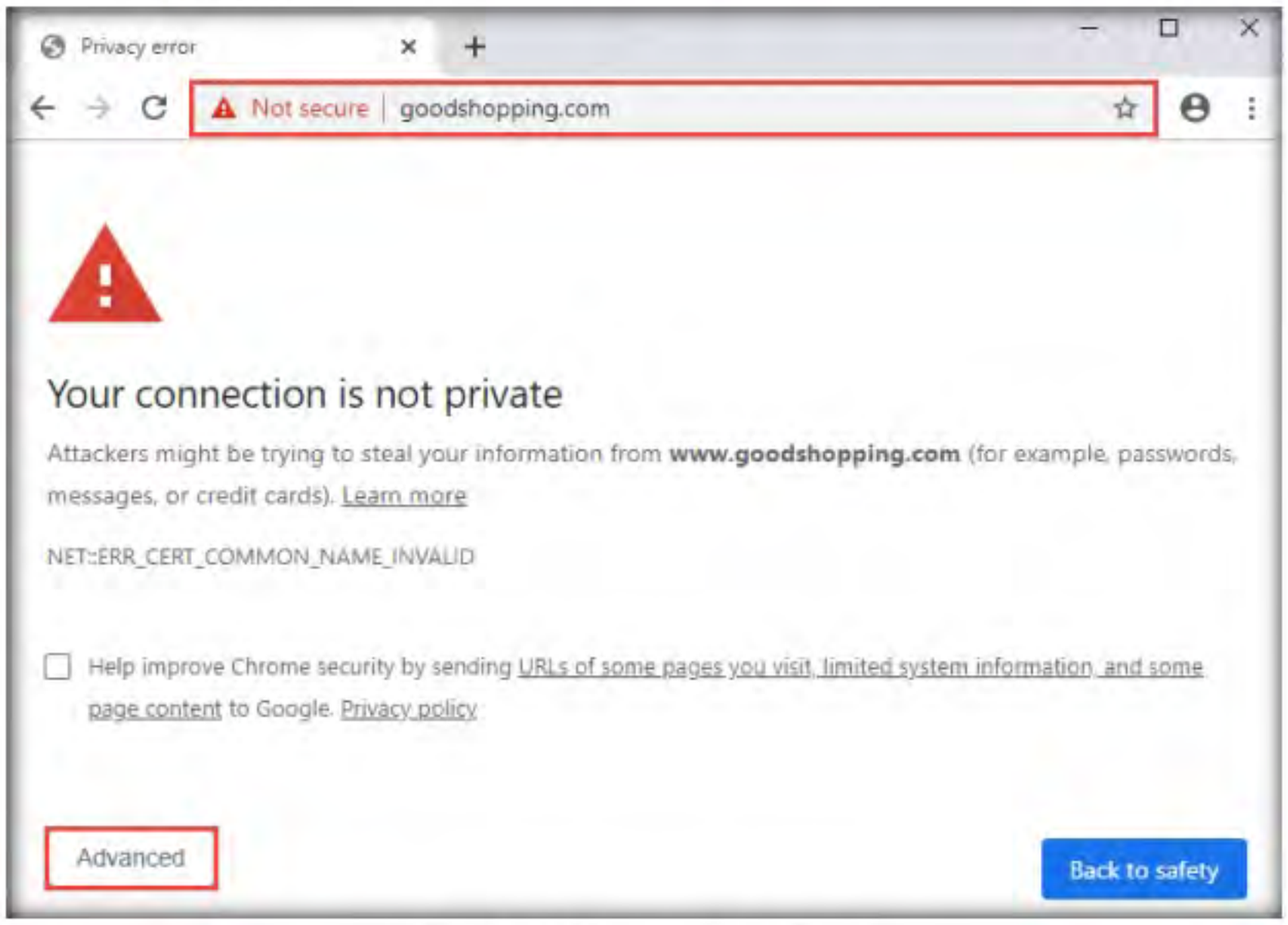


Figure 2.1.12: Connection is not Private

22. Click **Proceed to www.goodshopping.com (unsafe)**.

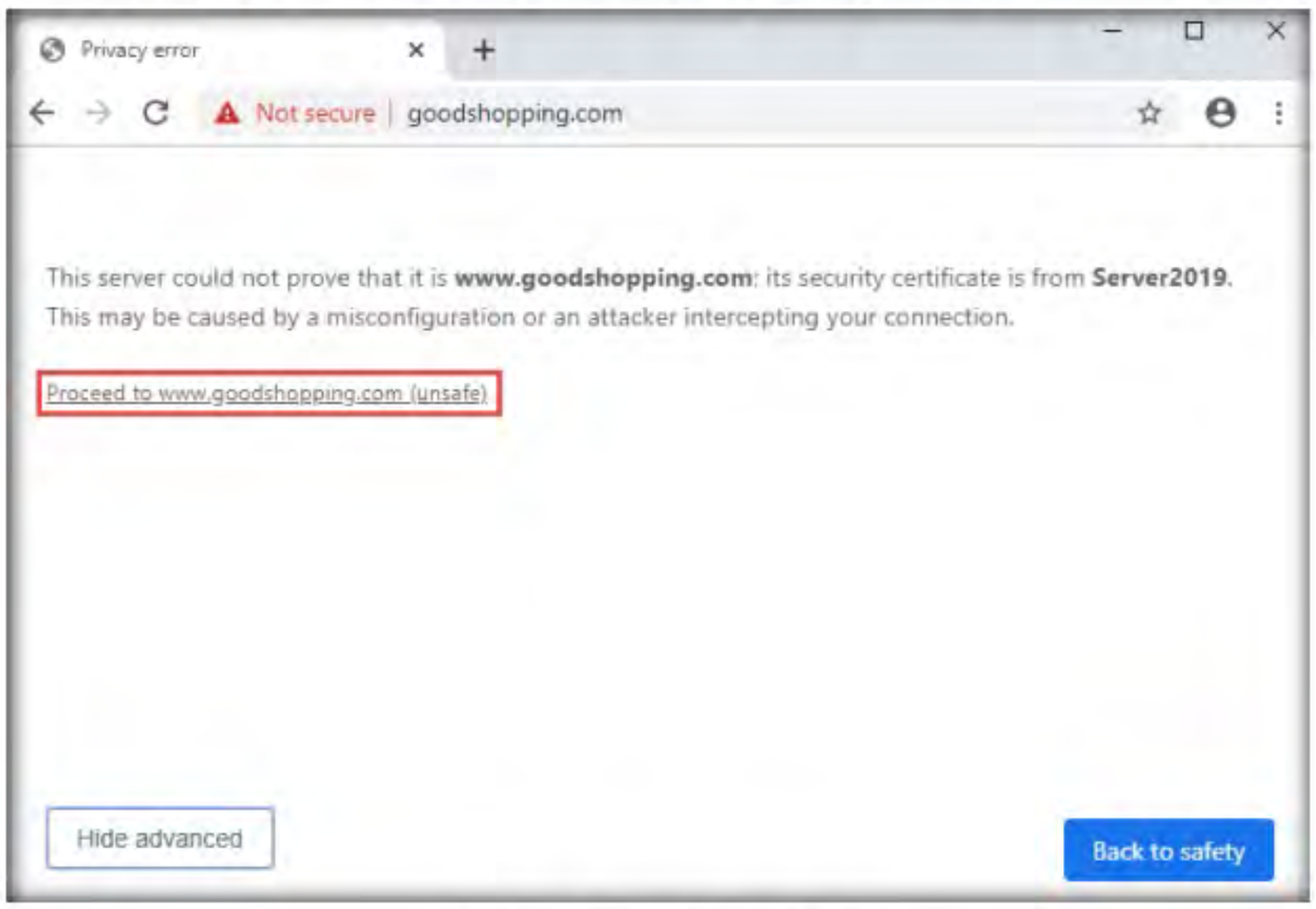


Figure 2.1.13: Proceed to Unsafe Page

23. Now you can see **Goodshopping webpage** with **ssl certificate** assigned to it, as shown in the screenshot.

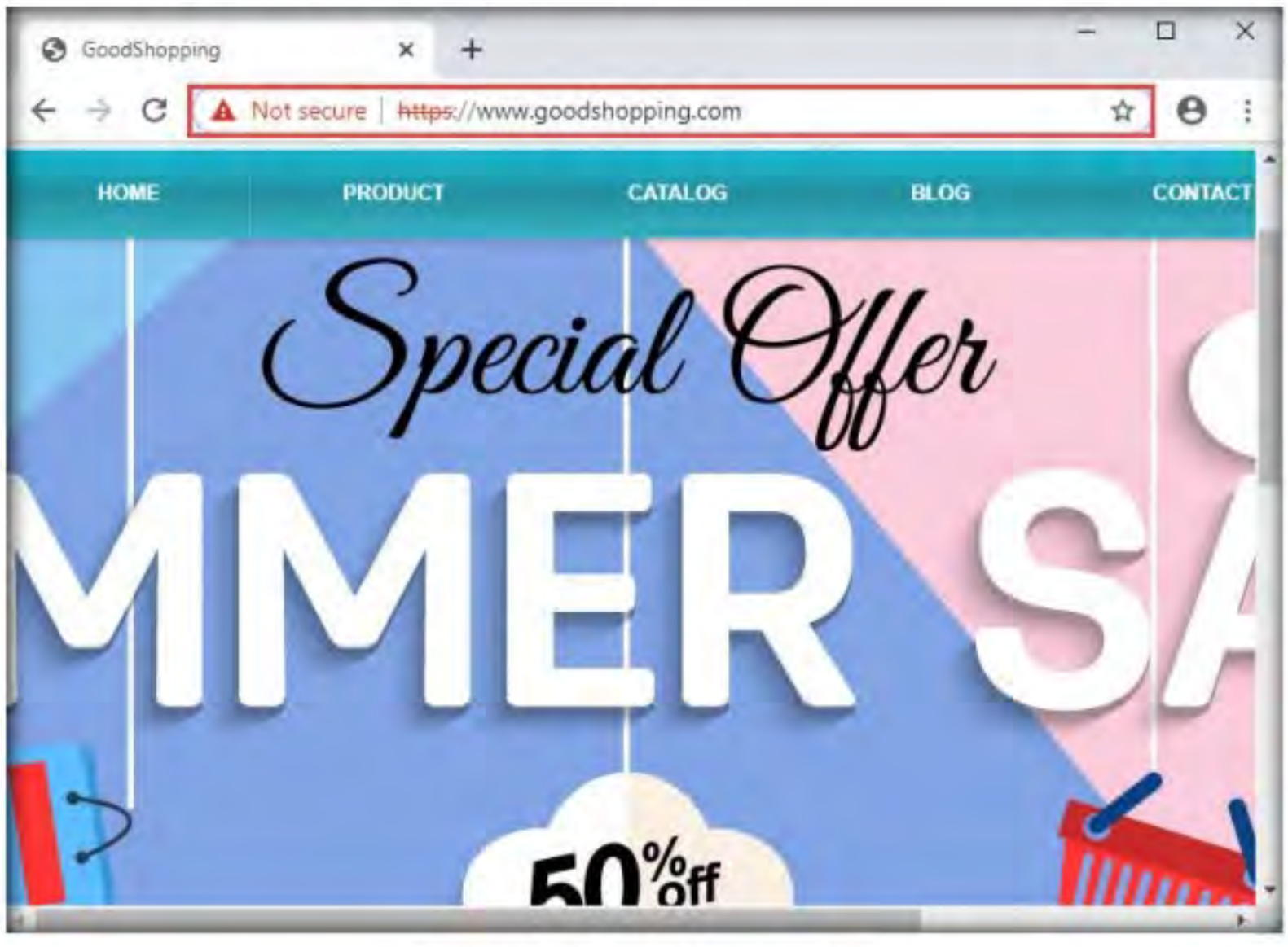


Figure 2.1.14: Self-signed Certificate Page

24. This concludes the demonstration of creating and using a self-signed certificate.
25. Close all open windows and document all the acquired information.
26. Turn off the **Windows Server 2019** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

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

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

Lab 3

Perform Email Encryption

Email encryption is the process of encrypting email messages to protect the content from being viewed by entities other than the intended recipients.

ICON KEY

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

Lab Scenario

Currently, the majority of businesses use email as their primary source of communication, as it is simple and easy to communicate or share information. Emails can contain sensitive information about an organization such as projects, upcoming news, and financial data, which, when accessed by the wrong person, can cause huge losses to the organization. One can protect emails containing sensitive information by encrypting them.

As a professional ethical hacker and penetration tester, you must have proper knowledge of encrypting email messages so that sensitive information sent through emails remain intact. This lab will demonstrate how to encrypt email messages using various email encryption tools.

Lab Objectives

- Perform email encryption using RMail

Lab Environment

To carry out this lab, you need:

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Email Encryption

Email encryption hides the email content from eavesdroppers by encrypting it into an unreadable form. Emails can be encrypted and decrypted by means of a digital signature mechanism that uses public and private keys: the public key is shared, while the private key is kept private.

There are numerous methods that can be employed for email encryption, including:

- **Digital Signature**: Uses asymmetric cryptography to simulate the security properties of a signature in digital, rather than written form
- **Secure Sockets Layer (SSL)**: Uses RSA asymmetric (public key) encryption to encrypt data transferred over SSL connections
- **Transport Layer Security (TLS)**: Uses a symmetric key for bulk encryption, an asymmetric key for authentication and key exchange, and message authentication codes for message integrity
- **Pretty Good Privacy (PGP)**: Used to encrypt and decrypt data that provides authentication and cryptographic privacy
- **GNU Privacy Guard (GPG)**: Software replacement of PGP and free implementation of the OpenPGP standard that is used to encrypt and decrypt data

Lab Tasks

TASK 1

Perform Email Encryption using RMail

Here, we will use the RMail tool to perform email encryption.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Create an Account in the RMail Website

3. Open any web browser (here, **Google Chrome**), type **https://www.rmail.com/free-trial/** in the address bar, and press **Enter**.
4. The **RMail FREE TRIAL** webpage appears, as well as the registration form. Fill in the required personal details.

RMail is an email security tool that provides open tracking, proof of delivery, email encryption, electronic signatures, large file transfer functionality, etc. RMail works seamlessly with users' existing email platforms, including Microsoft Outlook and Gmail, amongst others. Using this tool, you can encrypt sensitive emails and attachments for security or legal compliance.

5. Check the **I'm not a robot** checkbox and click **Start Free Trial**.

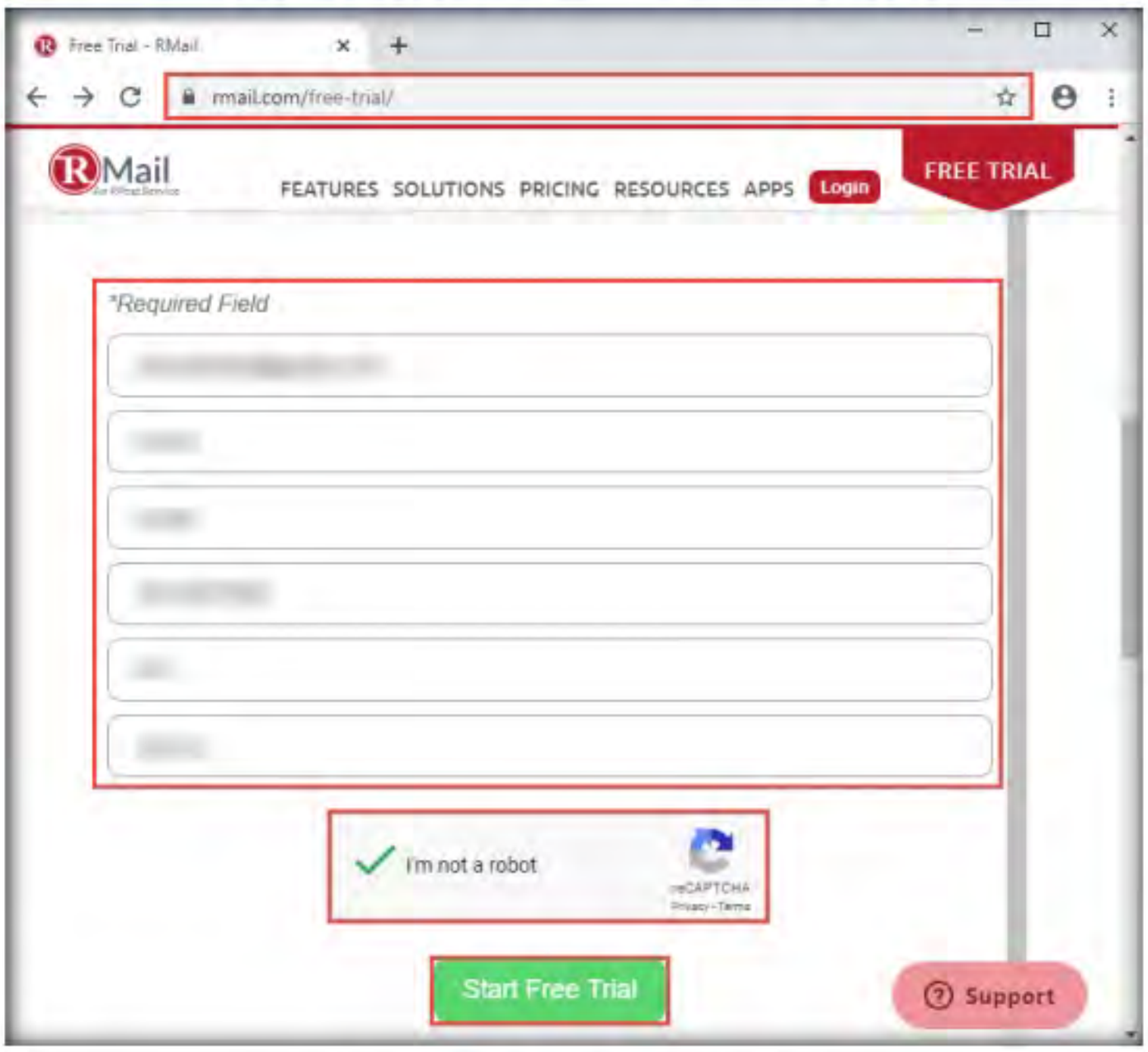


Figure 3.1.1: FREE TRIAL registration form

6. The **FREE TRIAL - GETTING STARTED** page appears; click **Apps page** hyperlink.

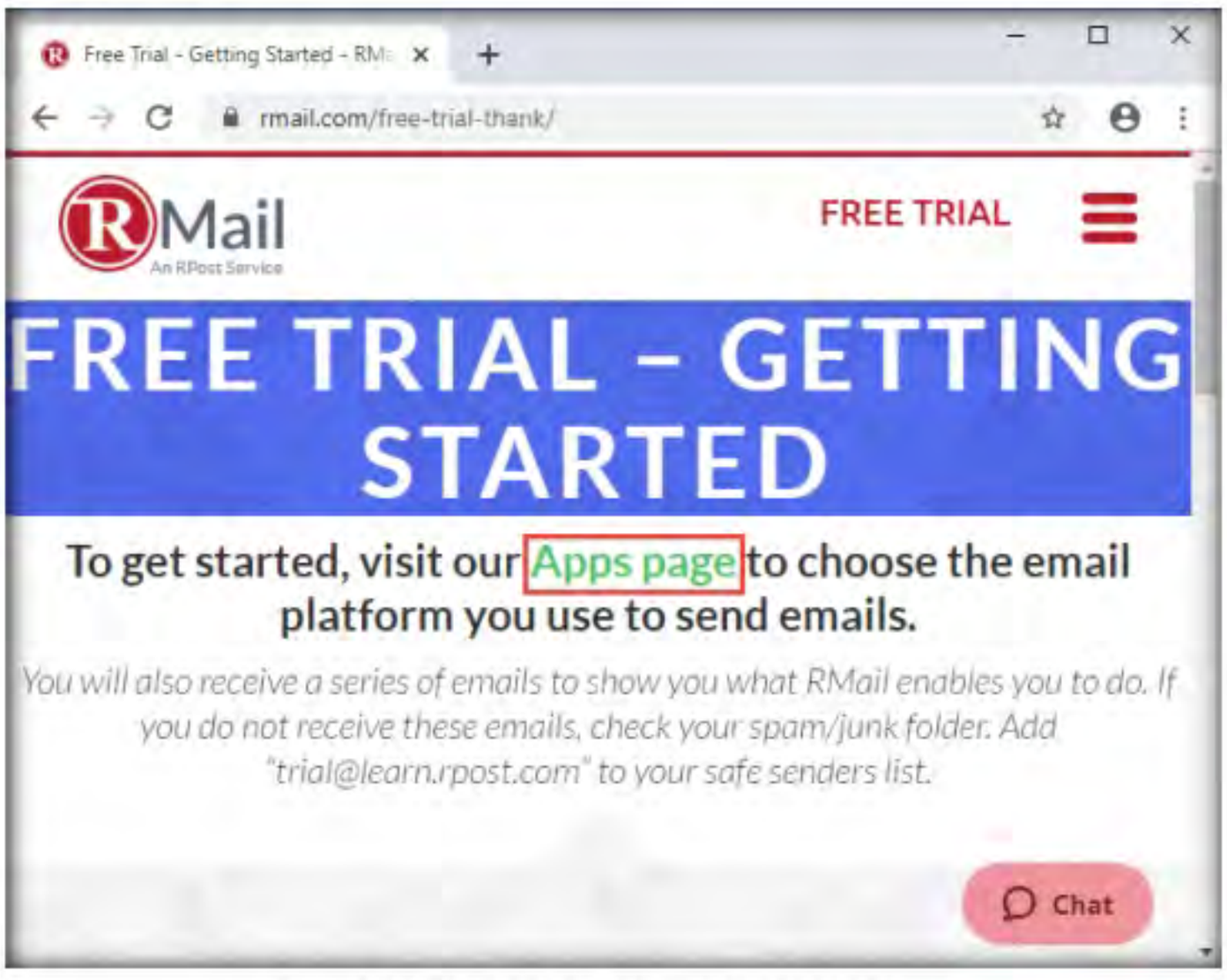


Figure 3.1.2: FREE TRIAL - GETTING STARTED page

TASK 1.2

Add RMail to the Gmail

7. The **APPS & DOWNLOADS** page appears; click the **RMail for Gmail (Chrome)** option from the available platforms.

Note: In this task, we will be using the Gmail platform to demonstrate the working of RMail. However, you can use RMail on the platform of your choice.

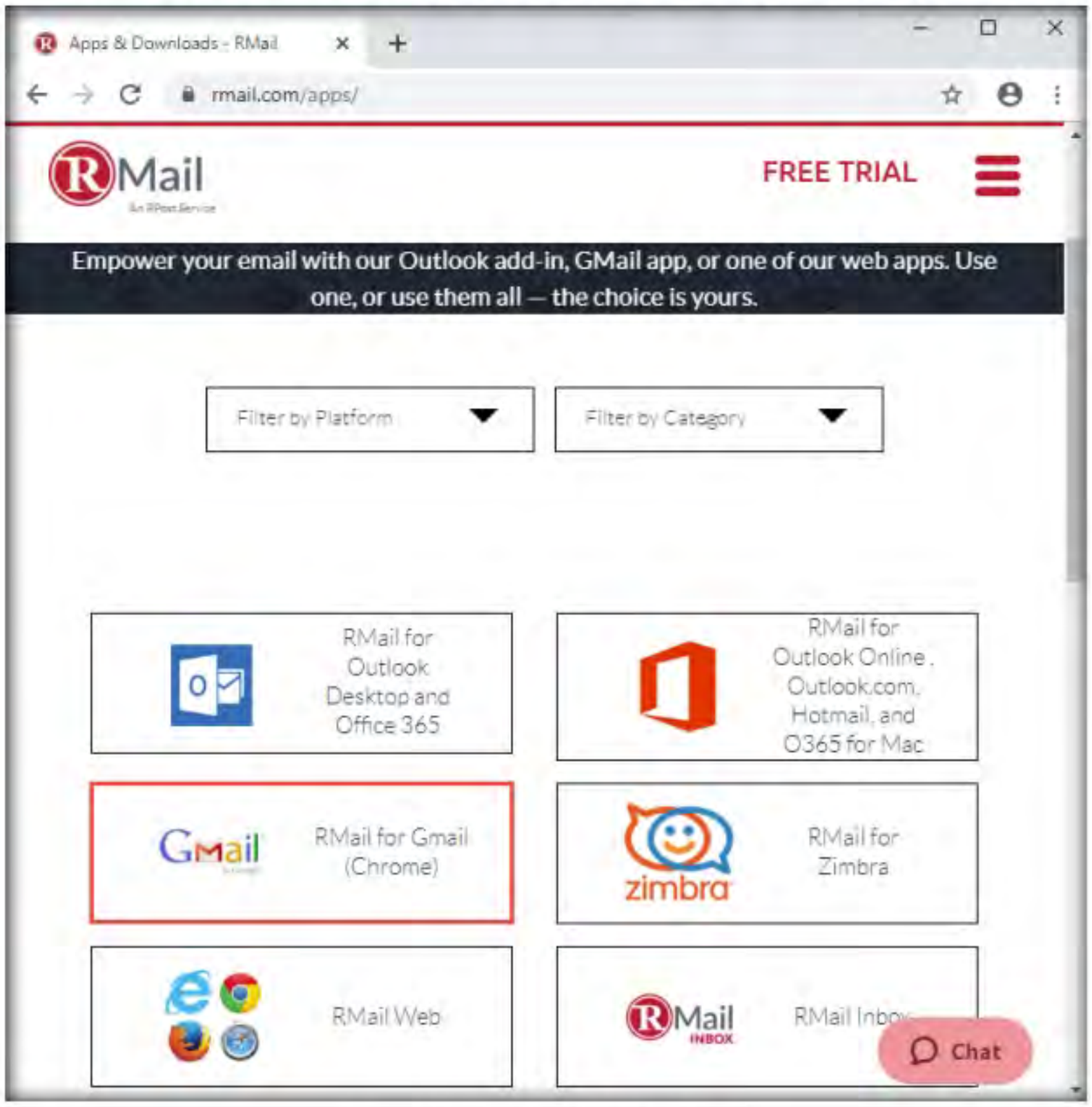


Figure 3.1.3: APPS & DOWNLOADS page

8. The **RMAIL FOR GMAIL (GOOGLE CHROME)** page appears; scroll down and click the **ADD TO CHROME** button.

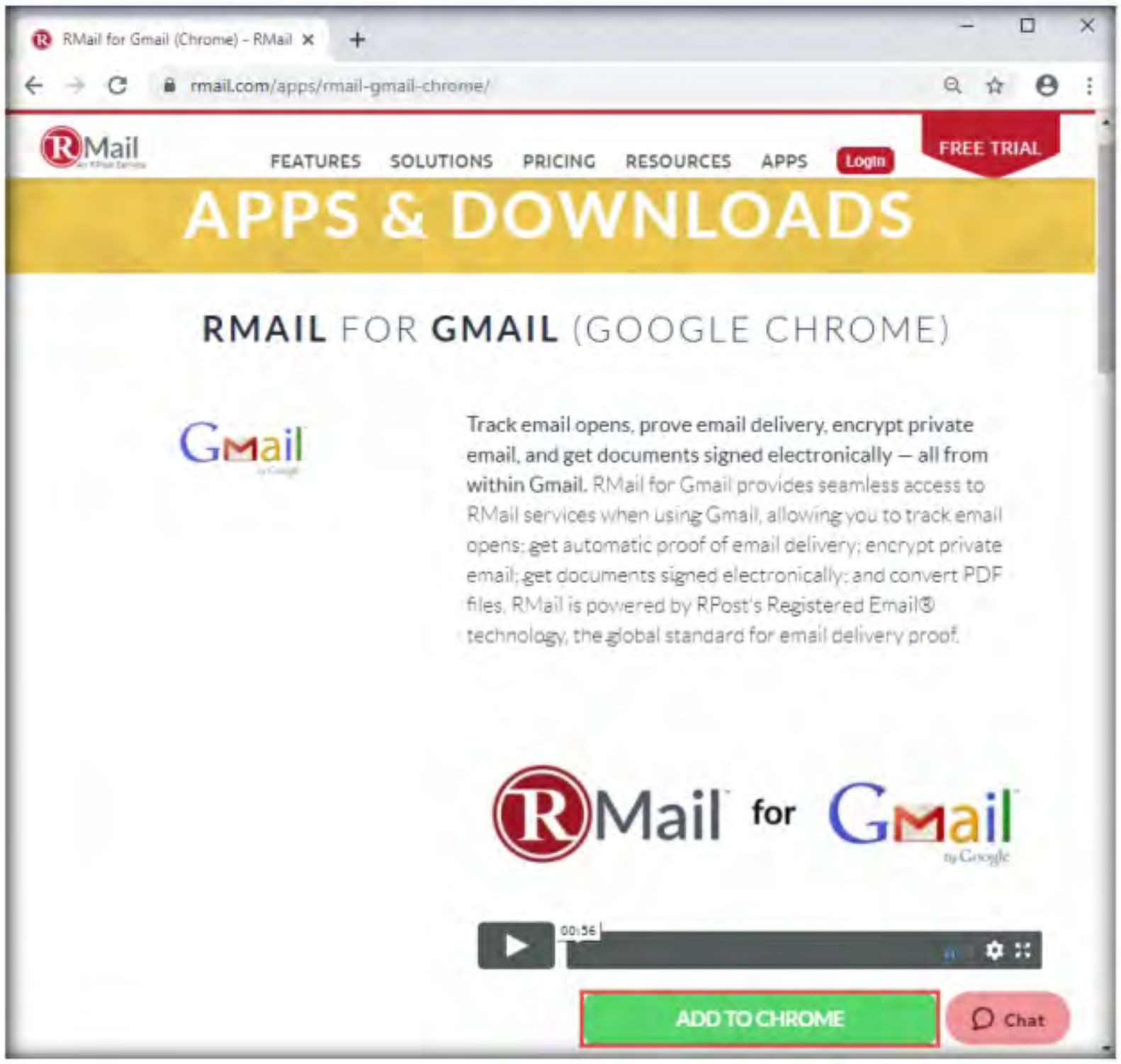


Figure 3.1.4: RMAIL FOR GMAIL (GOOGLE CHROME) page

9. A **chrome web store** page appears; click the **Add to Chrome** button under the **RPost for Gmail** option.

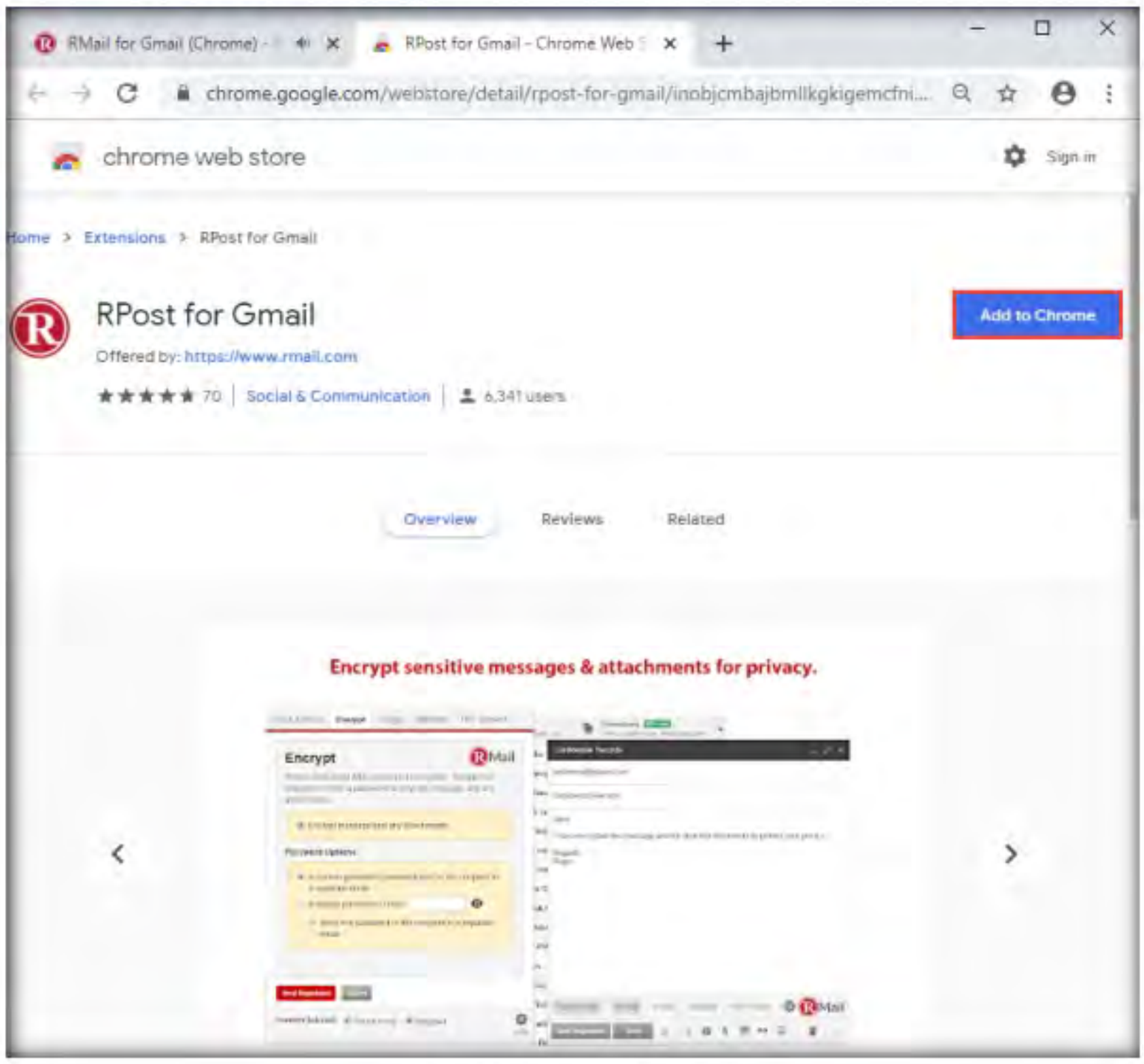


Figure 3.1.5: chrome web store page

10. The **Add "RPost for Gmail"?** notification appears; click **Add extension**.

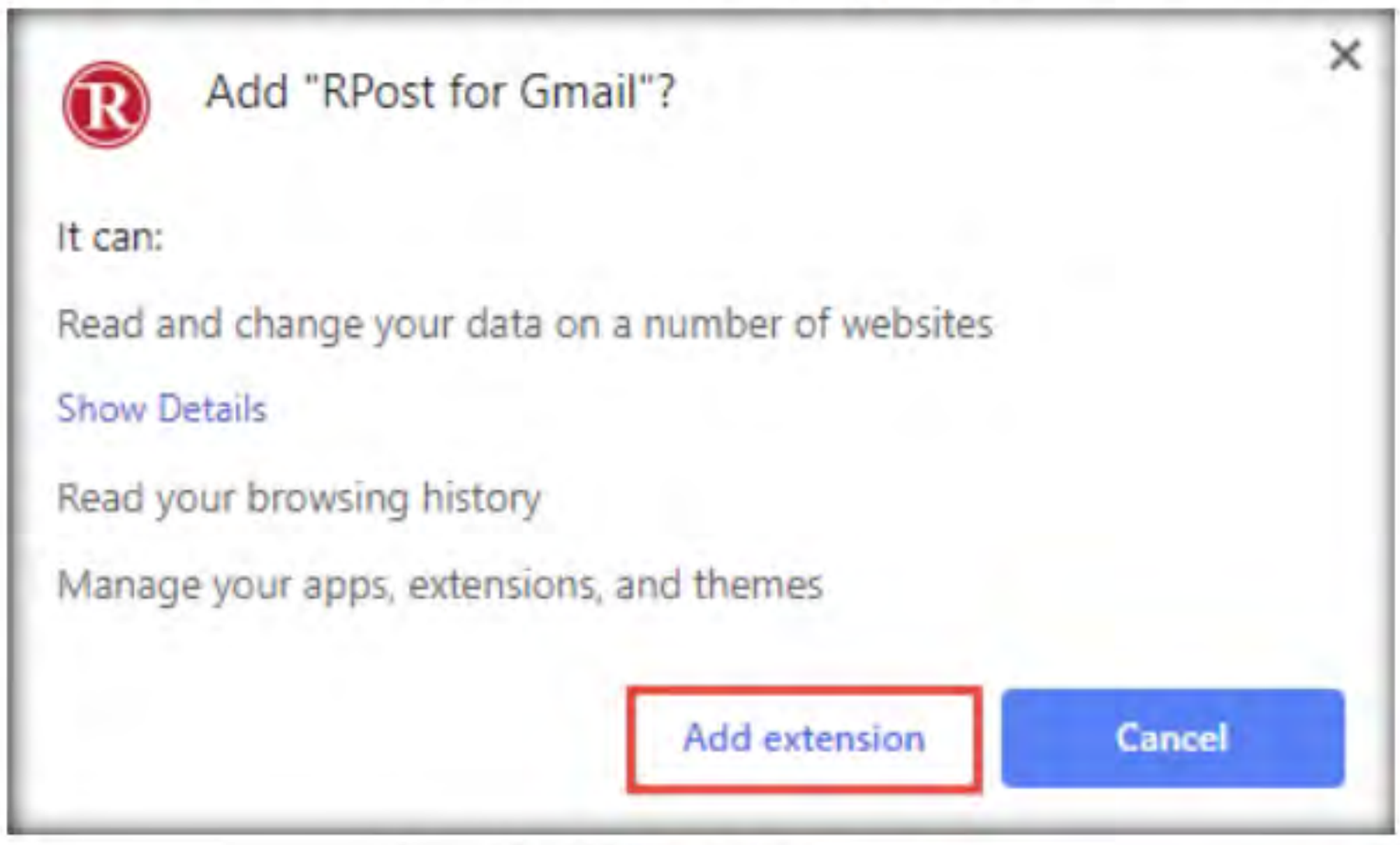


Figure 3.1.6: Add "RPost for Gmail"? notification

TASK 1.3

Set RMail in your Gmail Account

11. **RPost** is added to the browser and an **RPost for Gmail has been added to Chrome** notification appears.
12. Now, open a new tab in the browser and open the **Gmail** account within which you wish to implement email encryption.
13. Once you log in to your **Gmail** account, the **RMail** pop-up appears. Click the **Activate** button.

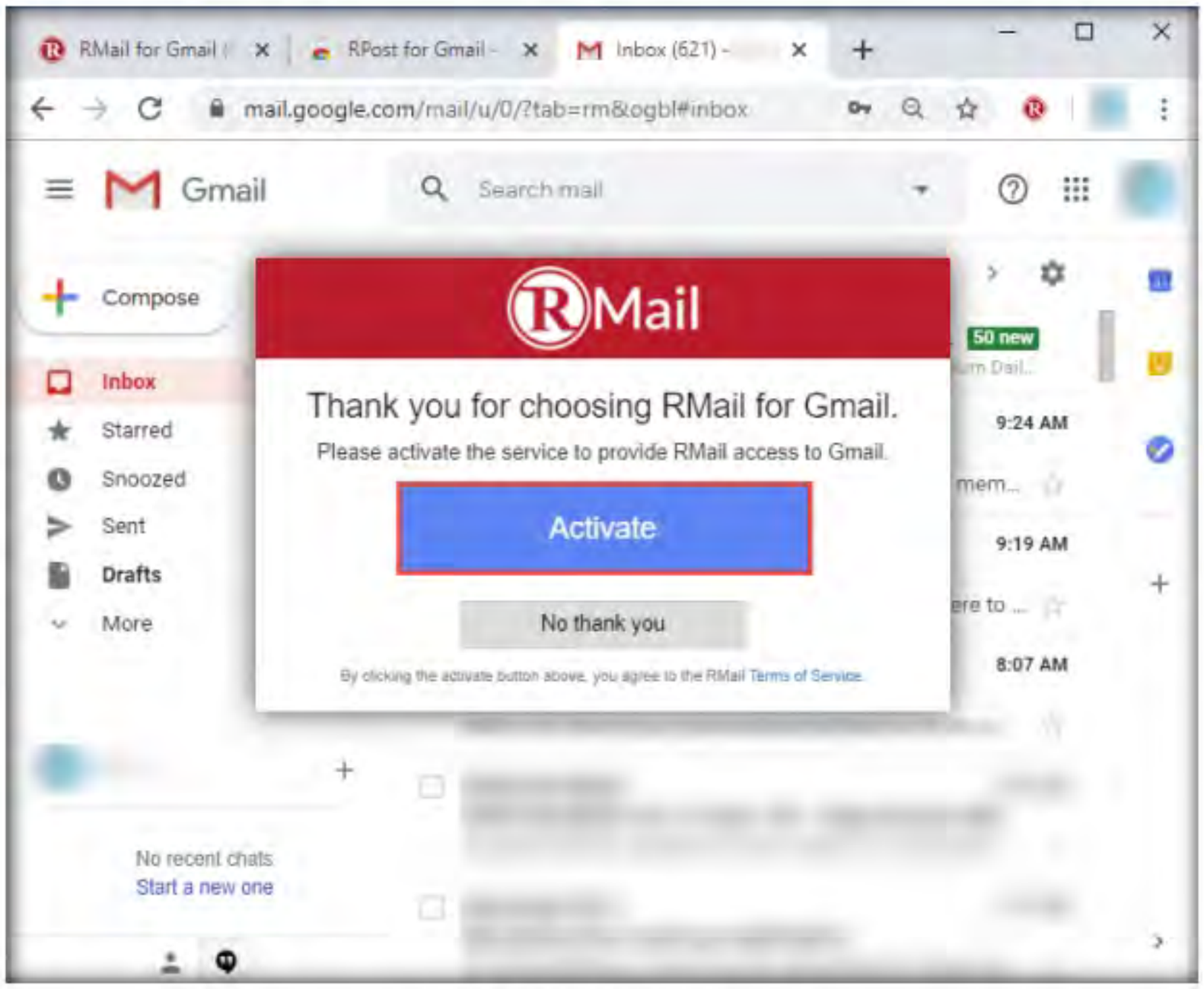


Figure 3.1.7: Adding RMail to the account

14. The **Sign in - Google Accounts** page appears; under the **Choose an account**, click on your account.

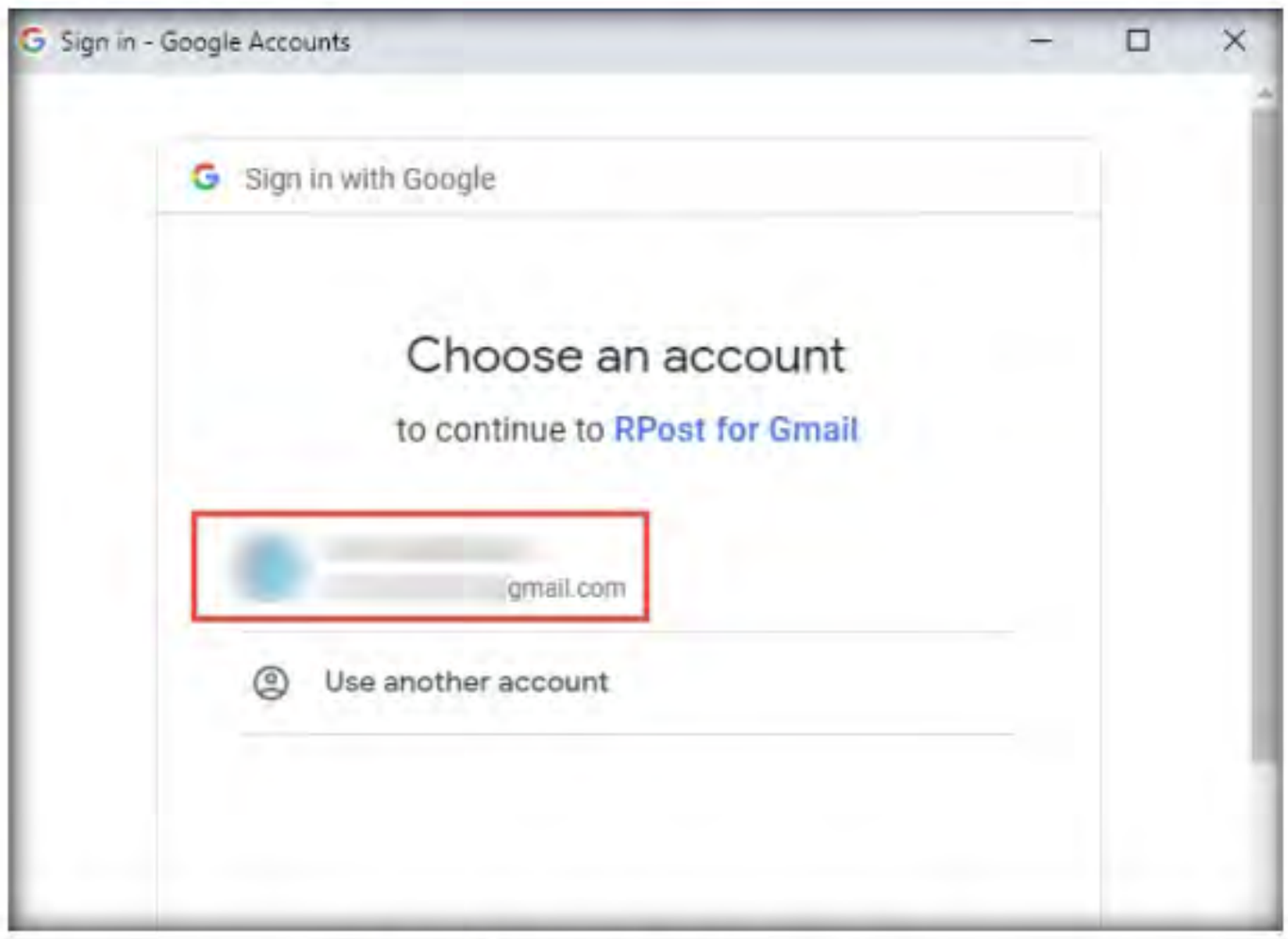


Figure 3.1.8: Sign in - Google Account page

15. The **RPost for Gmail wants to access your Google Account** wizard appears; click the **Allow** button.

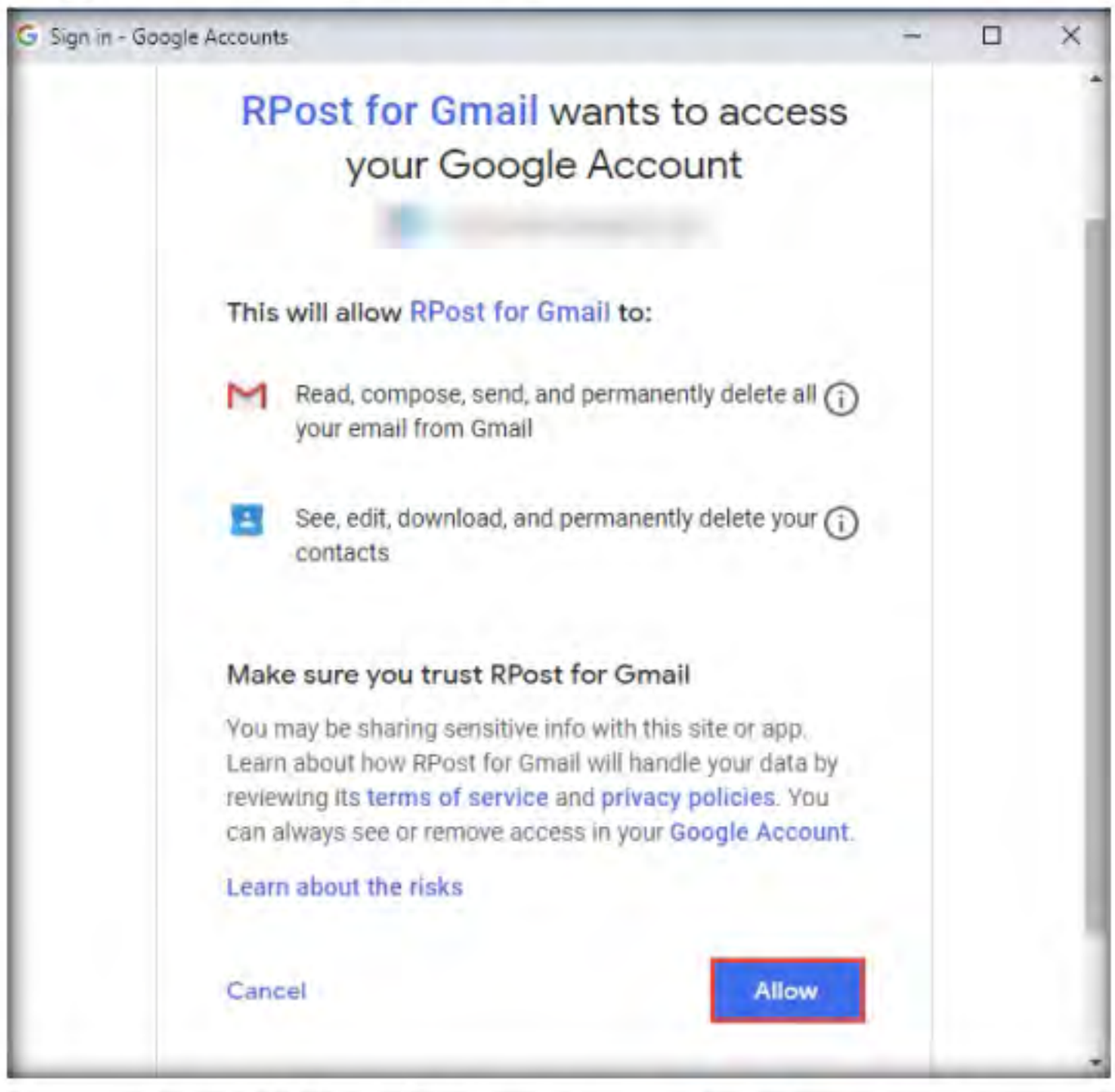


Figure 3.1.9: RPost for Gmail wants to access your Google Account wizard

TASK 1.4

Compose an Email

16. The **Thank you For Choosing RMail** page appears. Close the tab and navigate back to your **Gmail** account page.
17. Click **Compose** from the left-hand pane; the email body appears. Compose an email and click **Send Registered**.

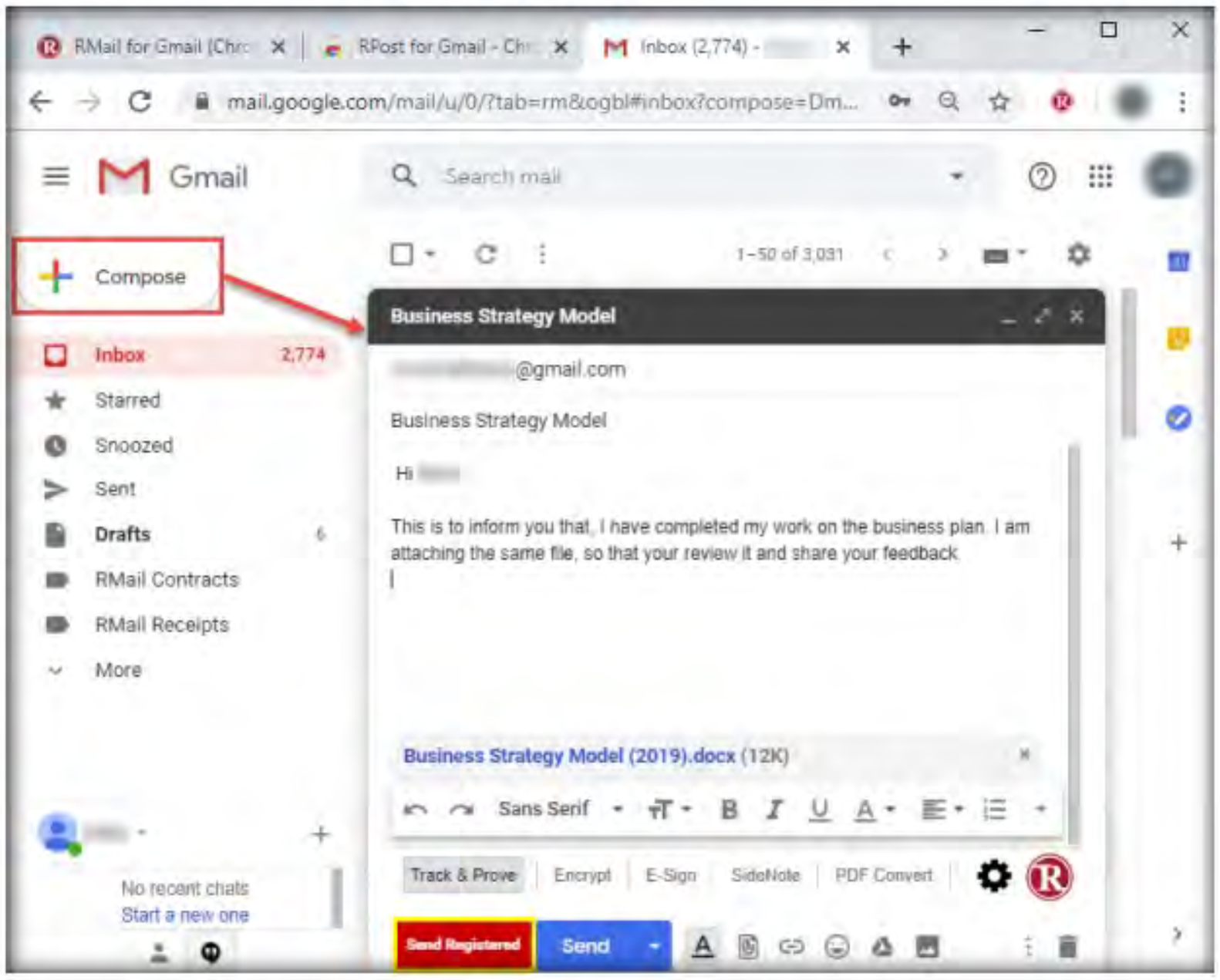


Figure 3.1.10: Compose an email

TASK 1.5

Set RMail Options and Sent an Email

18. The RMail **Track & Prove** pop-up appears; ensure that the **Marked** radio button is selected. Under the **Register Replies** section, check the **Receive proof of content and time of replies to this message** checkbox. Then, click the **Encrypt** tab.

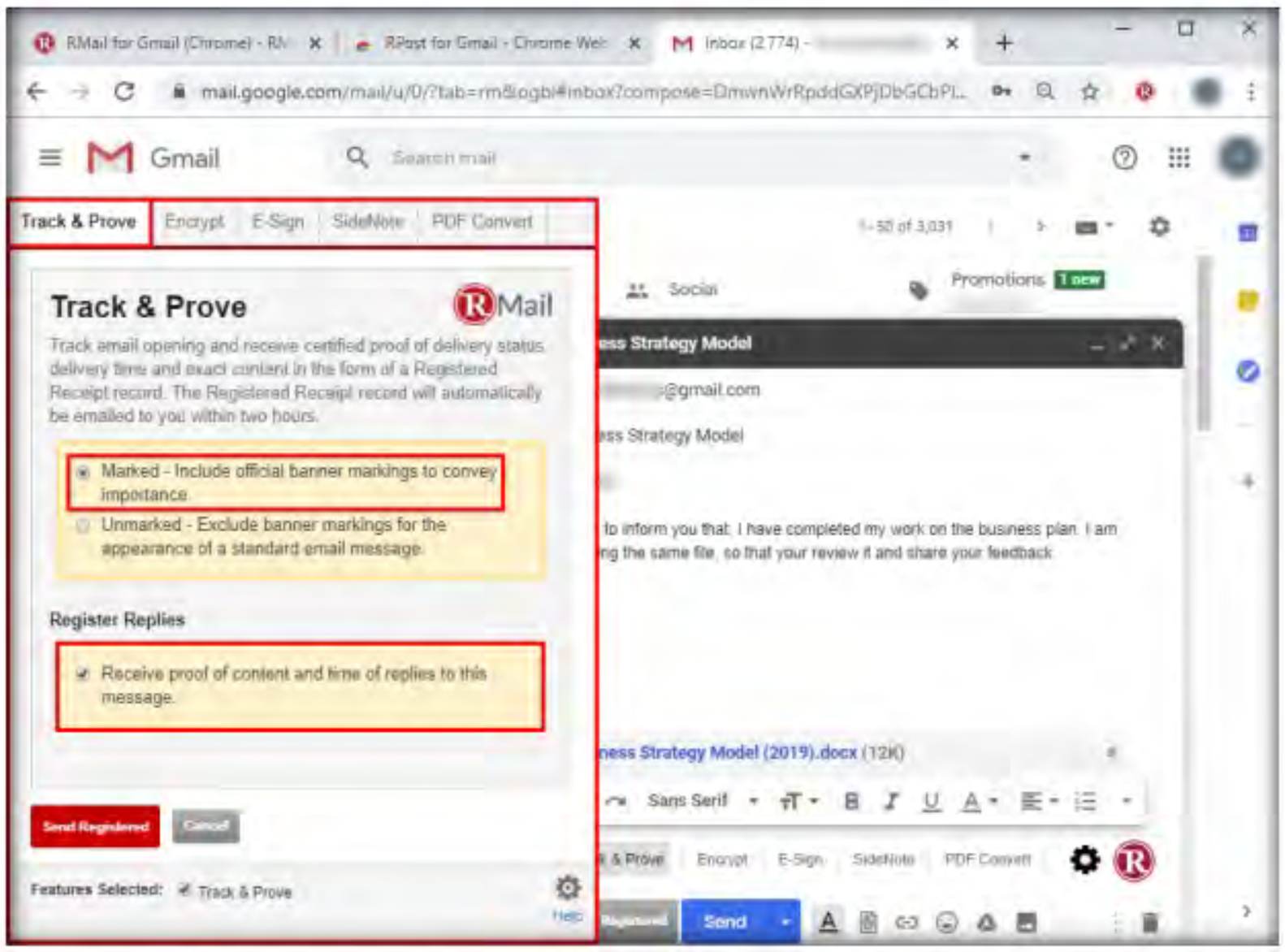


Figure 3.1.11: Track & Prove tab

19. In the **Encrypt** tab, check the **Encrypt message and any attachments** checkbox and click the **E-sign** tab.

Figure 3.1.12: Encrypt tab

20. In the **E-Sign** tab, check both the **Send your attachments for electronic signature** and **Send e-sign request encrypted** checkboxes. Click the **Send Registered** button.

Figure 3.1.13: E-Sign tab

21. In the **Inbox**, you can observe an **Acknowledgement** email with **Proof of Sending**.
22. In this task, for the purpose of demonstration, we will open the recipient's account and view the email.

TASK 1.6

Login as Recipient

23. To do so, switch to the **Windows Server 2019** virtual machine and log in with **Administrator/Pa$$w0rd**.
24. Open any web browser (here, **Google Chrome**) and log in to the **Gmail** account of the recipient. Open the email from the sender.
25. You can observe that the email received is tagged as a registered email wherein a document has been sent for the recipient to review and electronically sign to confirm his/her identity.

26. Click the **View & Sign Document** button to sign an agreement.

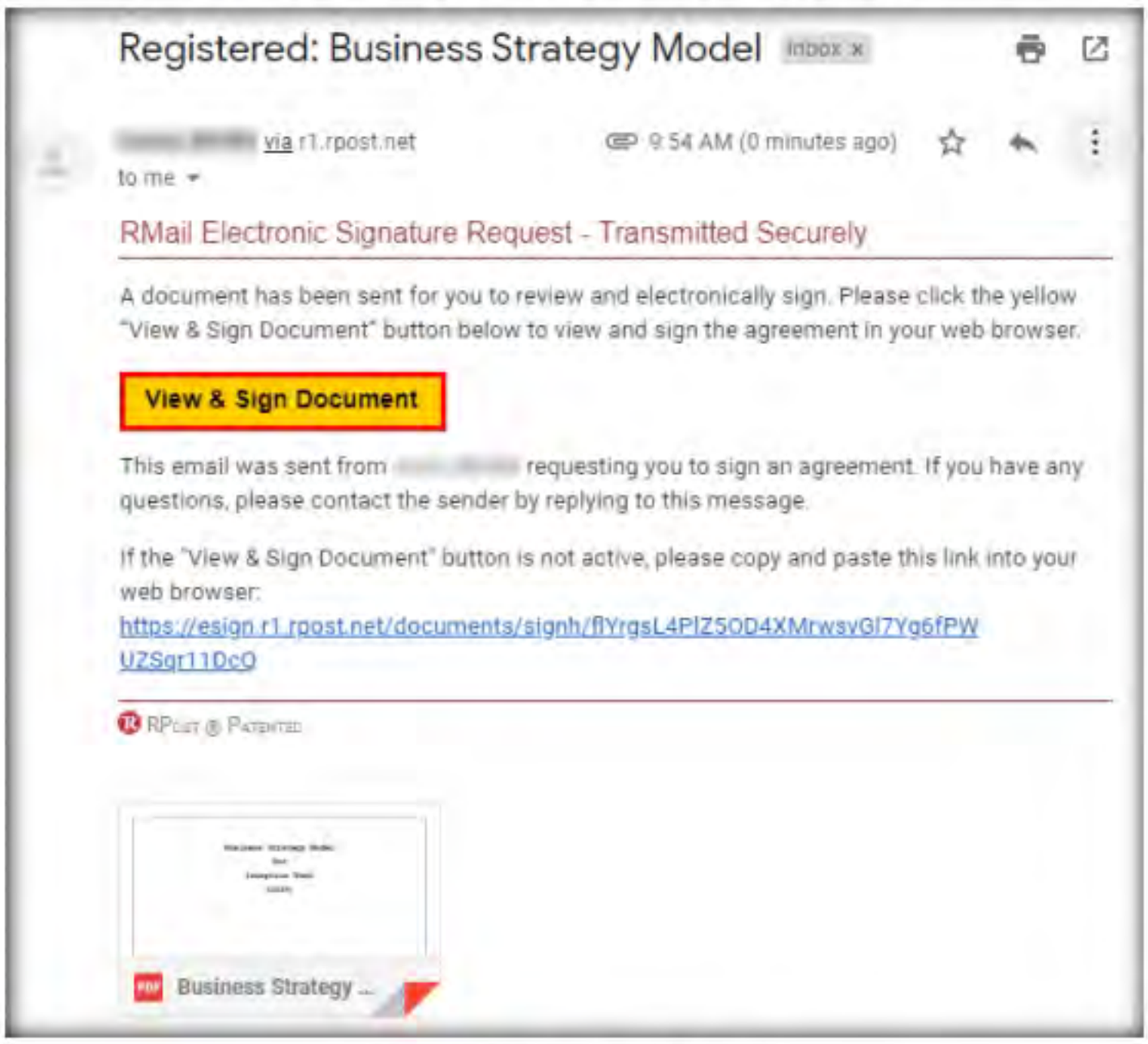


Figure 3.1.14: Email from the sender

TASK 1.7

E-Sign to Confirm Identity

27. A new **E-Sign** webpage appears displaying the email content; click **CONTINUE**.

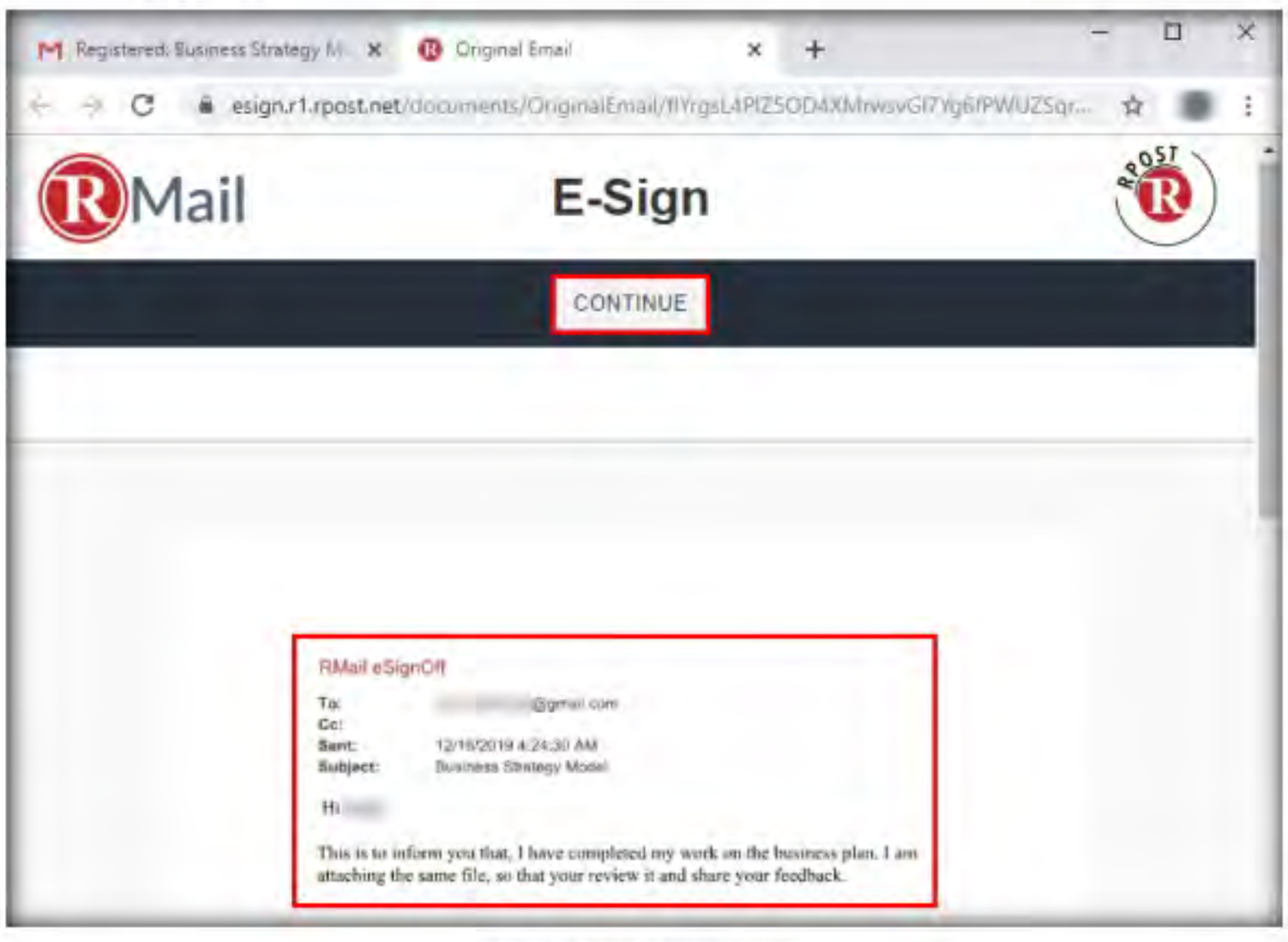


Figure 3.1.15: E-Sign page

28. The **Instructions: How To E-Sign** page appears; read the instructions carefully and click **CONTINUE**.

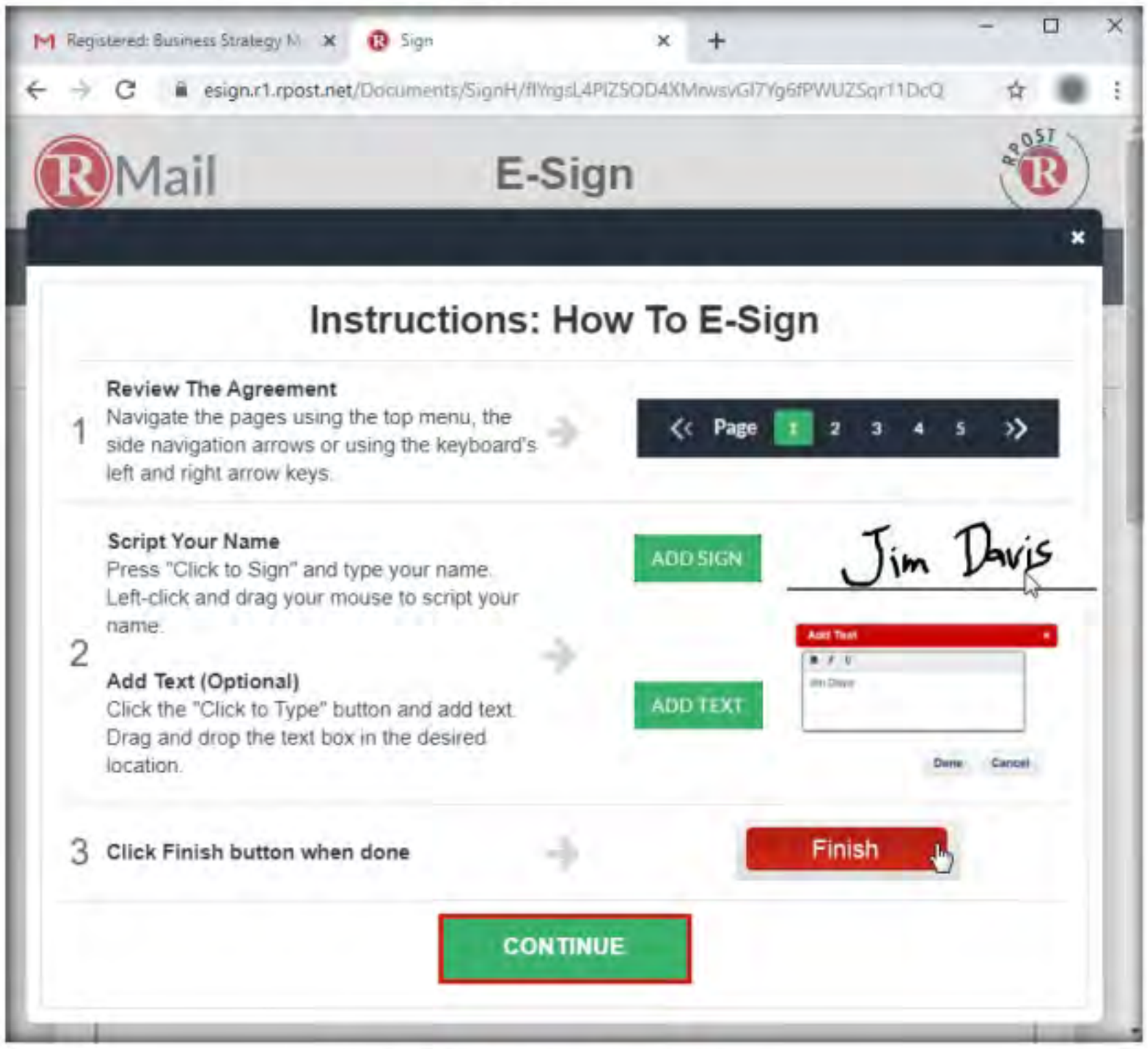


Figure 3.1.16: Instructions: How To E-Sign page

29. The attached document to the email (**Business Strategy Model (2019)**) appears, as shown in the screenshot.
30. After viewing the attached document, click **FINISH**.

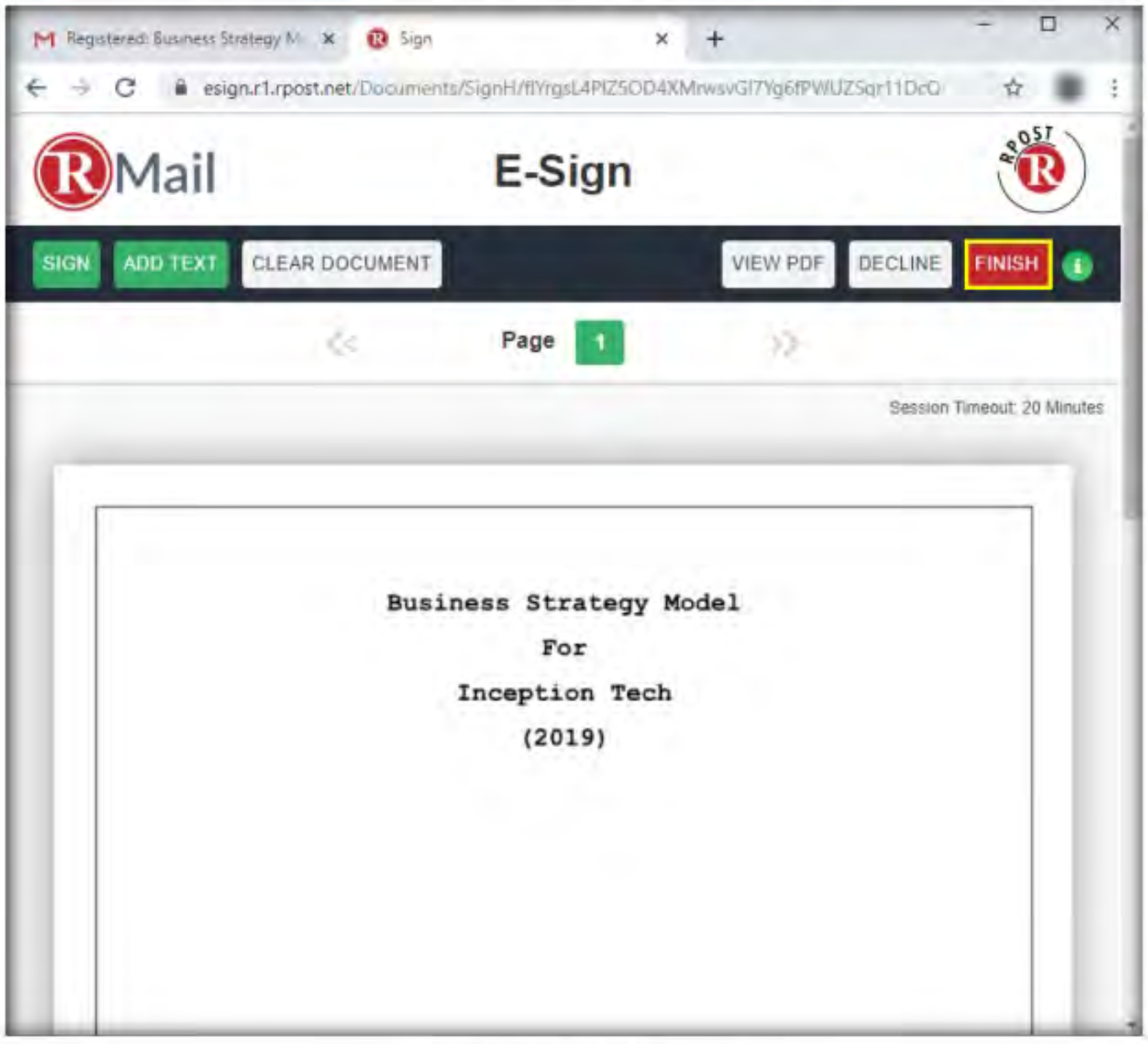


Figure 3.1.17: Attached document

31. The **Final Step - Please Complete the Information Below** page appears with the **Document Signature** form. In the **Please enter your name** field, enter your name (Recipient's name) and leave the **Title** field blank.
32. Click the **Draw It** tab, sign in the field below and click the **Click to Sign** button.

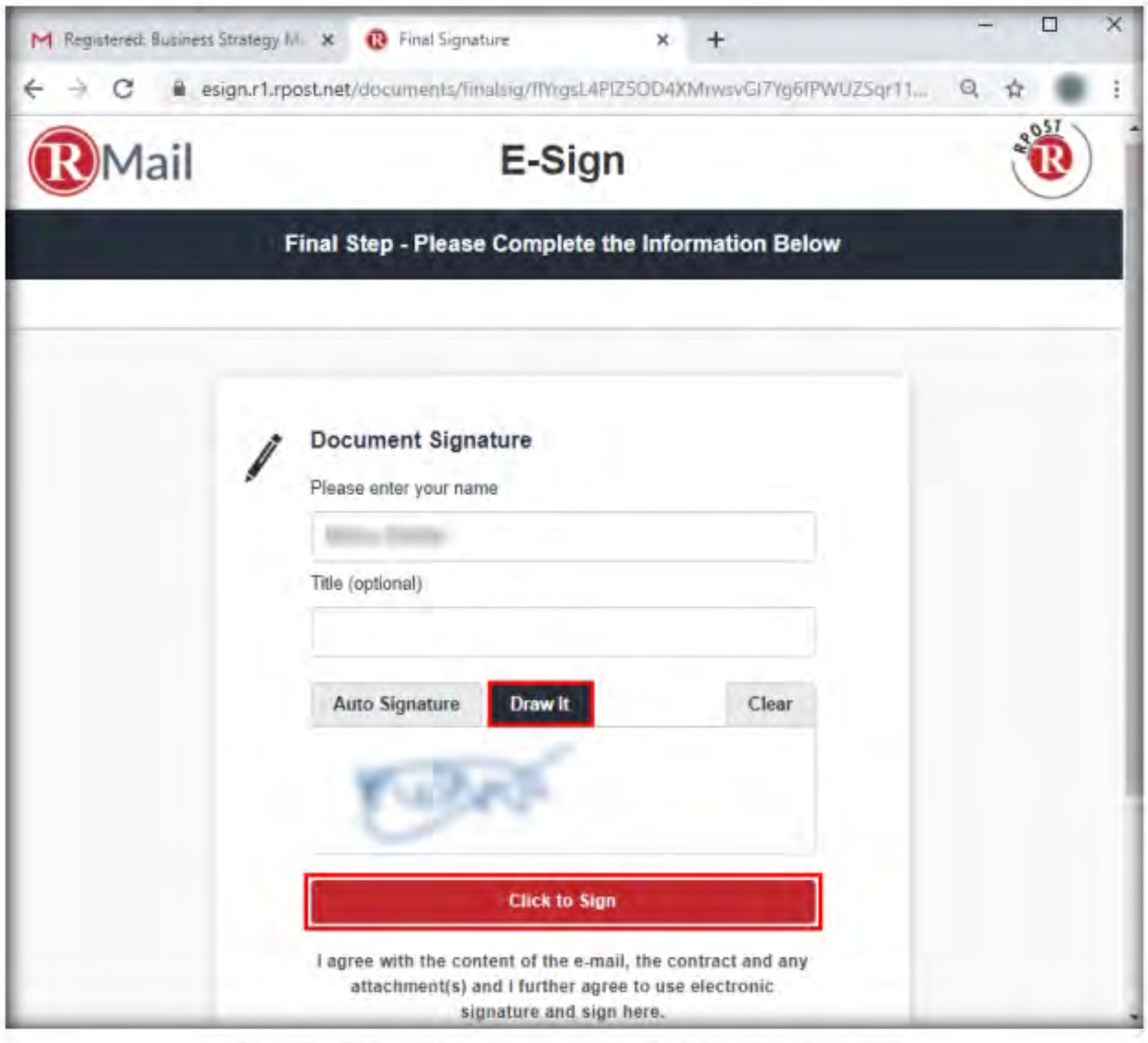


Figure 3.1.18: Final Step: Please Complete the Information Below page

33. The **YOU'RE ALL DONE!** page appears; close the current tab to return to the opened email. Click **Inbox** from the left-hand pane to navigate to the inbox.

34. Open an email from **RPost eSignOff Service**. You can observe that it is an acknowledgment email from RPost along with various details such as **Signed By**, **Date**, **Time**, **Original Recipient**, **IP**, **Message Id**, etc.

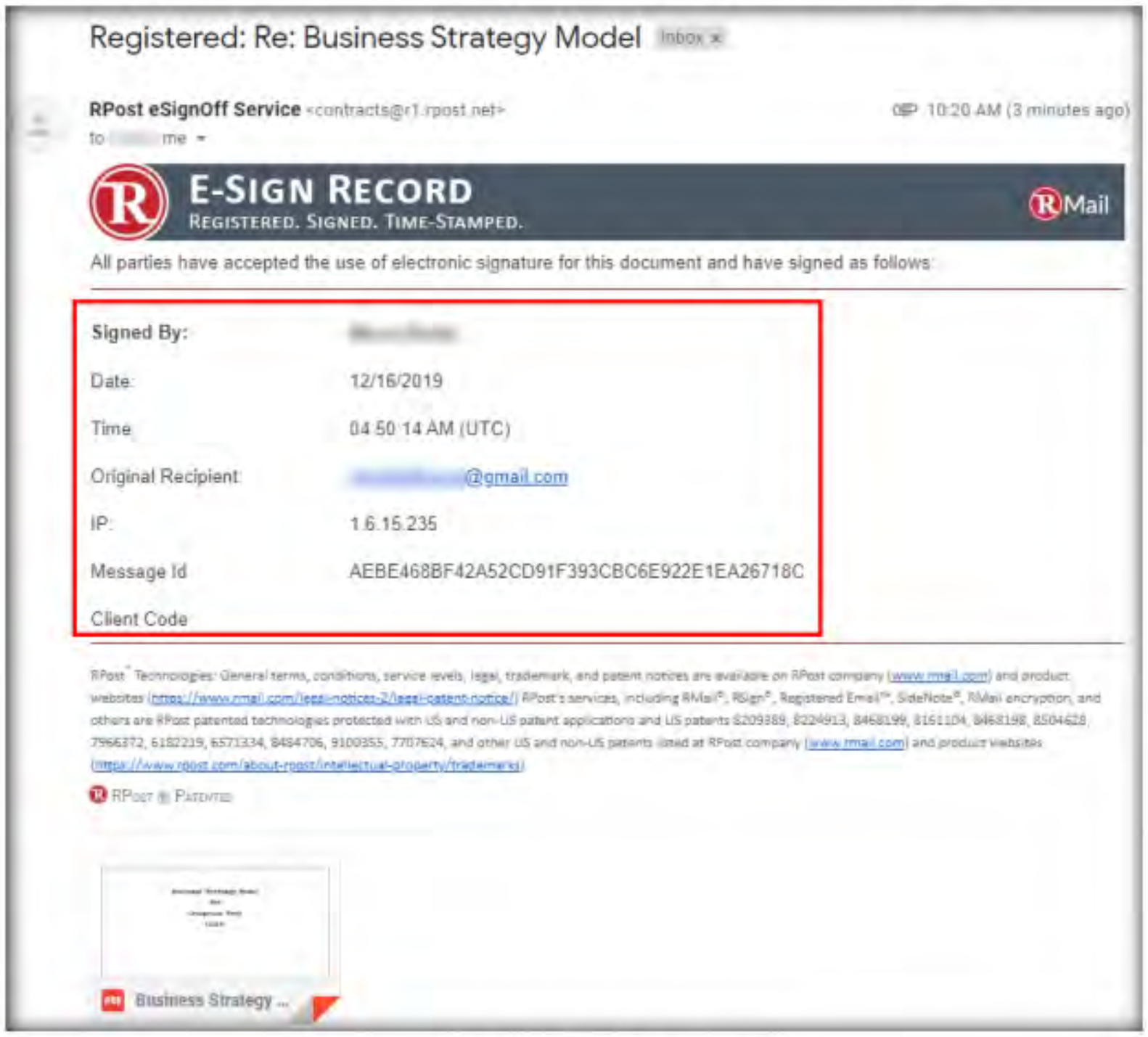


Figure 3.1.19: RPost eSignOff Service email

TASK 1.8

View Acknowledgement Emails as a Sender

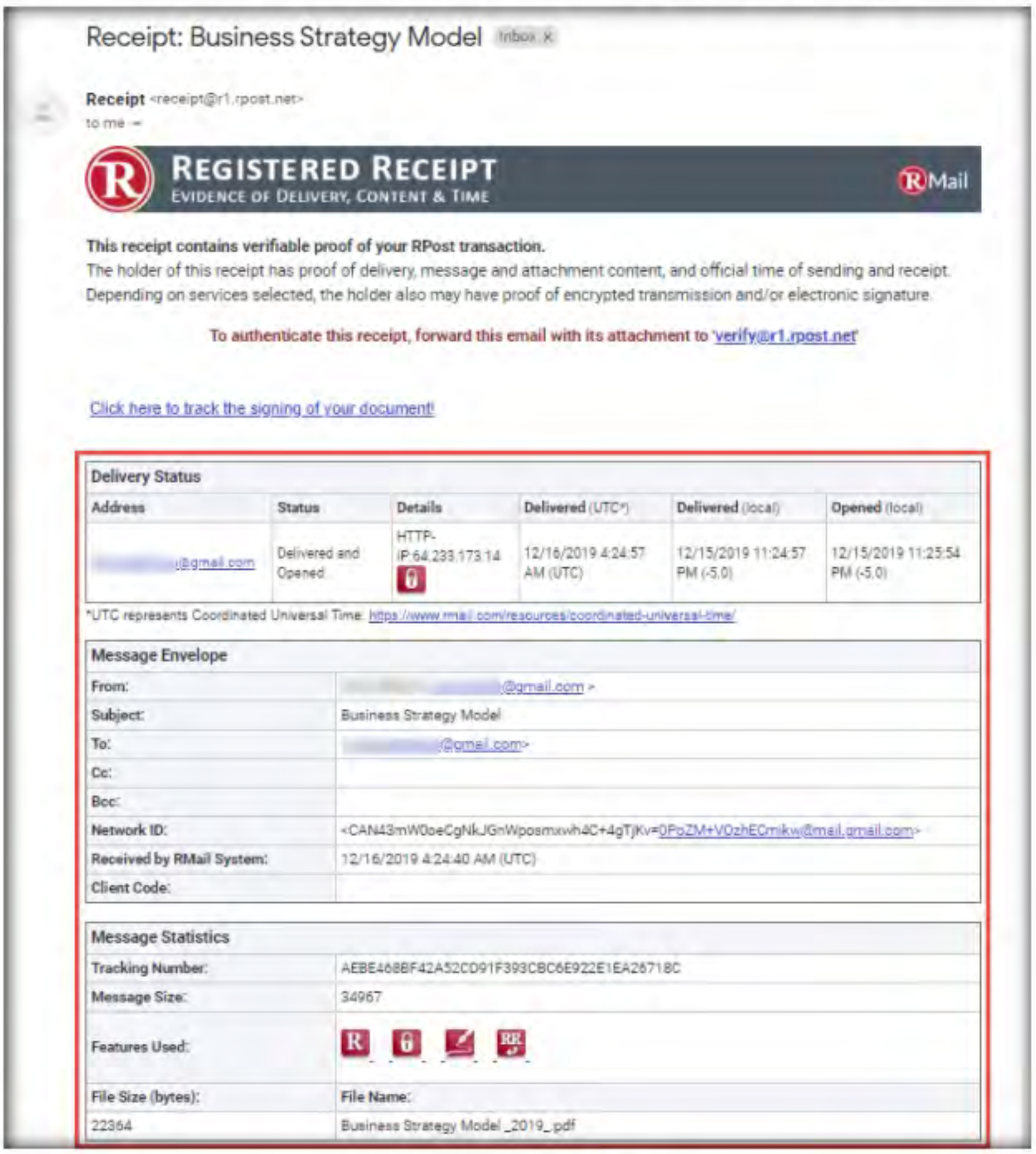
35. Now, return to the **Windows 10** virtual machine, where the sender's account is opened. In **Inbox**, you can observe two emails (**Receipt** and **RPost eSignOff Service**). Click to open the **Receipt** email.

Note: You might receive a **Receipt** mail in the **RMail Receipts** inbox folder present in the left-hand pane.

36. The **Receipt** email contains information about the **Delivery Status**, **Message Envelope**, and **Message Statistics** of the sent email, as shown in the screenshot.

37. The **Receipt** email also includes the **DeliveryReceipt** and **HtmlReceipt** attachments containing detailed information regarding the sent email.

You can also use other email encryption tools such as **Virtru** (https://www.virtru.com), **ZixMail** (https://www.zixcorp.com), **Egress Secure Email and File Transfer** (https://www.egress.com), and **Proofpoint Email Protection** (https://www.proofpoint.com) to perform email encryption.



Receipt: Business Strategy Model Inbox x

Receipt <receipt@r1.rpost.net>
to me

REGISTERED RECEIPT
EVIDENCE OF DELIVERY, CONTENT & TIME
RMail

This receipt contains verifiable proof of your RPost transaction.
The holder of this receipt has proof of delivery, message and attachment content, and official time of sending and receipt. Depending on services selected, the holder also may have proof of encrypted transmission and/or electronic signature.

To authenticate this receipt, forward this email with its attachment to 'verify@r1.rpost.net'

Click here to track the signing of your document!

Delivery Status

Address	Status	Details	Delivered (UTC*)	Delivered (local)	Opened (local)
[redacted]@gmail.com	Delivered and Opened	HTTP-IP:64.233.173.14	12/16/2019 4:24:57 AM (UTC)	12/15/2019 11:24:57 PM (-5.0)	12/15/2019 11:25:54 PM (-5.0)

*UTC represents Coordinated Universal Time. https://www.rmail.com/resources/coordinated-universal-time/

Message Envelope

From:	[redacted]@gmail.com >
Subject:	Business Strategy Model
To:	[redacted]@gmail.com>
Cc:	
Bcc:	
Network ID:	<CAN43mW0oeCgNkJGnWposmxwh4C+4gTjKv=0PoZM+V0zhECmikw@mail.gmail.com>
Received by RMail System:	12/16/2019 4:24:40 AM (UTC)
Client Code:	

Message Statistics

Tracking Number:	AEBE468BF42A52CD91F393CBC6E922E1EA26718C
Message Size:	34967
Features Used:	
File Size (bytes):	File Name:
22364	Business Strategy Model _2019_.pdf

Figure 3.1.20: Receipt email

38. Now, navigate back to the **Inbox** and open an email from **RPost eSignOff Service**. This email contains the same information as the email received from **RPost eSignOff Service** by the recipient.

39. This concludes the demonstration of performing email encryption using RMail.
40. Close all open windows and document all the acquired information.
41. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

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

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

Lab 4

Perform Disk Encryption

Disk encryption encrypts every bit and byte of data stored on a disk or a disk volume, thus preventing illegal access to data storage.

Lab Scenario

ICON KEY

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

Disk encryption is a technology that protects the confidentiality of the data stored on a disk by converting it into an unreadable code using disk encryption software or hardware, thus preventing unauthorized users from accessing it. Disk encryption provides confidentiality and privacy using passphrases and hidden volumes. As a professional ethical hacker or pen tester, you should perform disk encryption in order to prevent sensitive information from unauthorized access.

Disk encryption works in a manner similar to text-message encryption and protects data even when the OS is not active. By using an encryption program for the user's disk (Blue Ray, DVD, USB flash drive, External HDD, and Backup), the user can safeguard any or all information burned onto the disk and thus prevent it from falling into the wrong hands. Disk-encryption software scrambles the information burned on the disk into an illegible code. It is only after decryption of the disk information that one can read and use it.

This lab will demonstrate the use of various disk encryption tools to perform this technique.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

Lab Objectives

- Perform disk encryption using VeraCrypt
- Perform disk encryption using BitLocker Drive Encryption
- Perform disk encryption using Rohos Disk Encryption

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection

- VeraCrypt located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\VeraCrypt**
- Rohos Disk Encryption located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\Rohos Disk Encryption**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest versions, the screenshots shown in the lab might differ.

Lab Duration

Time: 30 Minutes

Overview of Disk Encryption

Disk encryption is useful when the user needs to send sensitive information through email. In addition, disk encryption can prevent the real-time exchange of information from threats. When users exchange encrypted information, it minimizes the chances of compromising the data; the only way an attacker could access the information is by decrypting the message. Furthermore, encryption software installed on a user's system ensures the security of the system. Install encryption software on any systems that hold valuable information or on those exposed to unlimited data transfer.

Lab Tasks

TASK 1

Perform Disk Encryption using VeraCrypt

Here, we will use the VeraCrypt tool to perform disk encryption.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Install and Launch VeraCrypt

2. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\VeraCrypt** and double-click **VeraCrypt Setup 1.24-Hotfix1.exe**.

Note: If the **User Account Control** pop-up appears, click **Yes**.

3. **VeraCrypt Setup Wizard** appears, click **OK**.

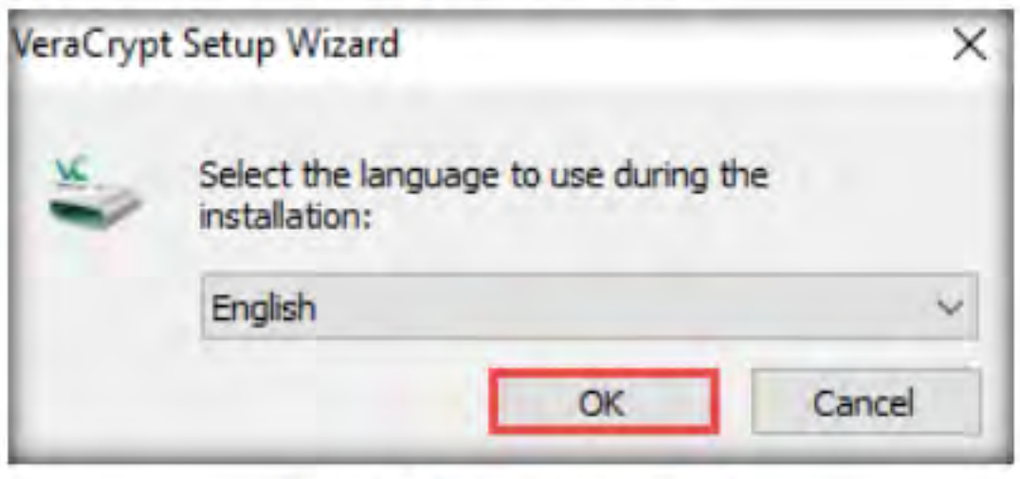


Figure 4.1.1: VeraCrypt Setup Wizard

4. Follow the steps to install the application using all default settings.

VeraCrypt is a software used for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved, and decrypted just after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).

5. After the completion of the installation, the **VeraCrypt has been successfully installed** wizard appears; then, click **Finish**.

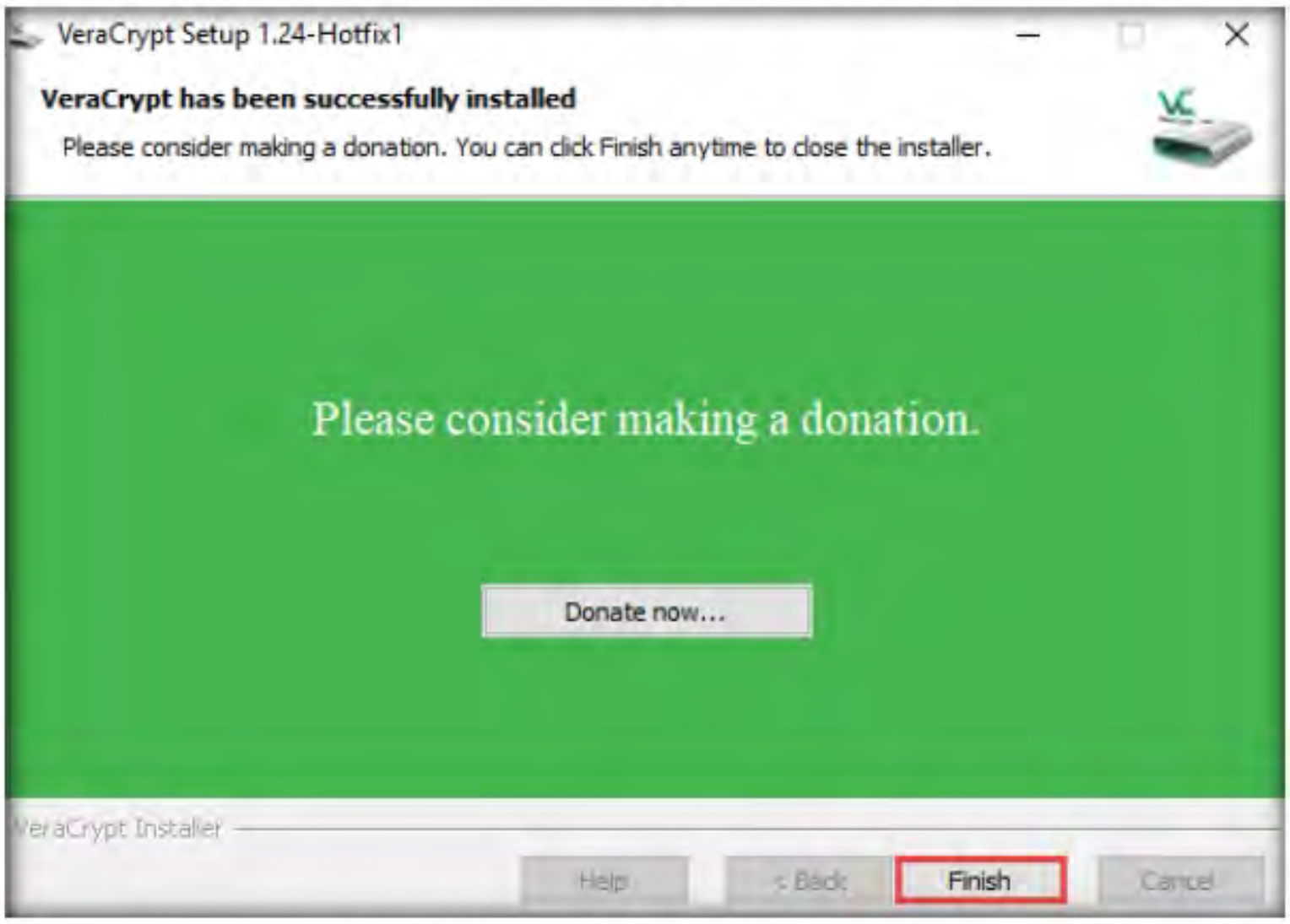


Figure 4.1.2: VeraCrypt has been successfully installed wizard

6. A **VeraCrypt Setup** notification appears; then, click **No**.
7. Click the **Start** icon in the bottom-left corner of **Desktop** and click **VeraCrypt** from the applications to launch VeraCrypt.

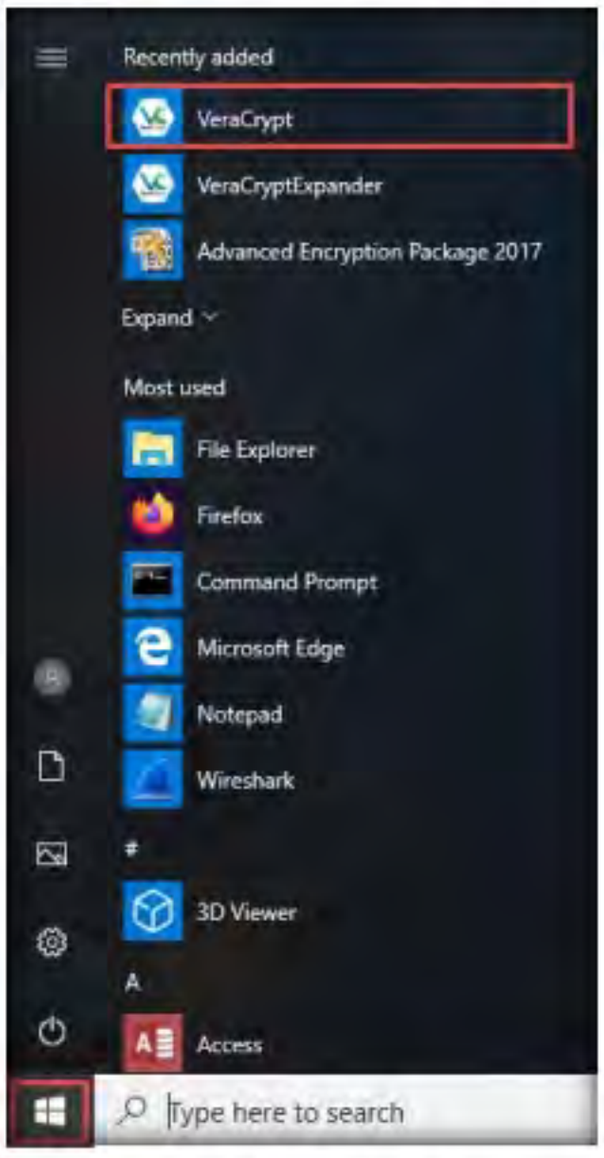


Figure 4.1.3: Launch VeraCrypt

TASK 1.2

Create a Volume

8. The **VeraCrypt** main window appears; click the **Create Volume** button.

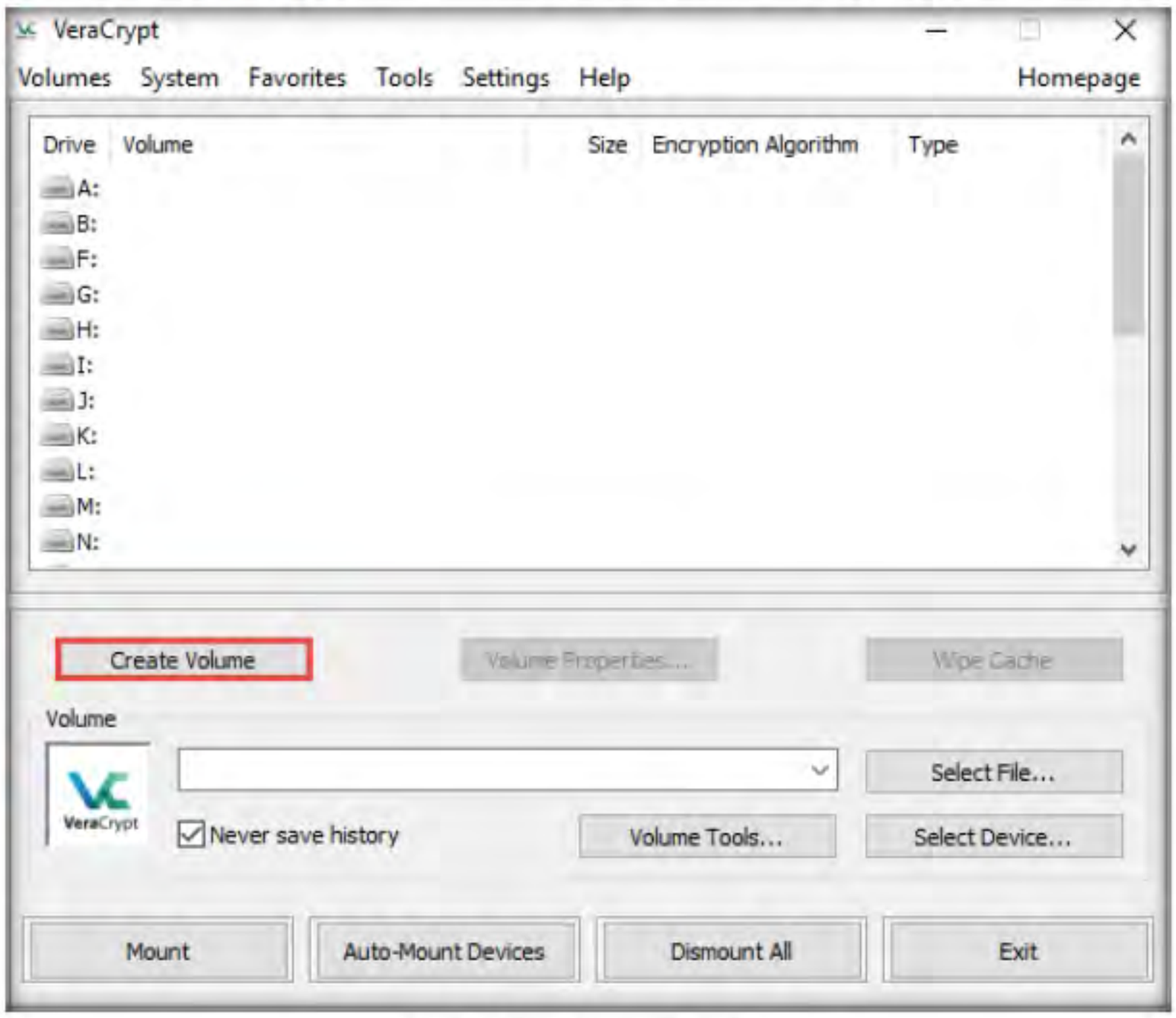


Figure 4.1.4: VeraCrypt main window

9. The **VeraCrypt Volume Creation Wizard** window appears. Ensure that the **Create an encrypted file container** radio-button is selected and click **Next** to proceed.

Figure 4.1.5: VeraCrypt Volume Creation Wizard

10. In the **Volume Type** wizard, keep the default settings and click **Next**.
11. In the **Volume Location** wizard, click **Select File...**.

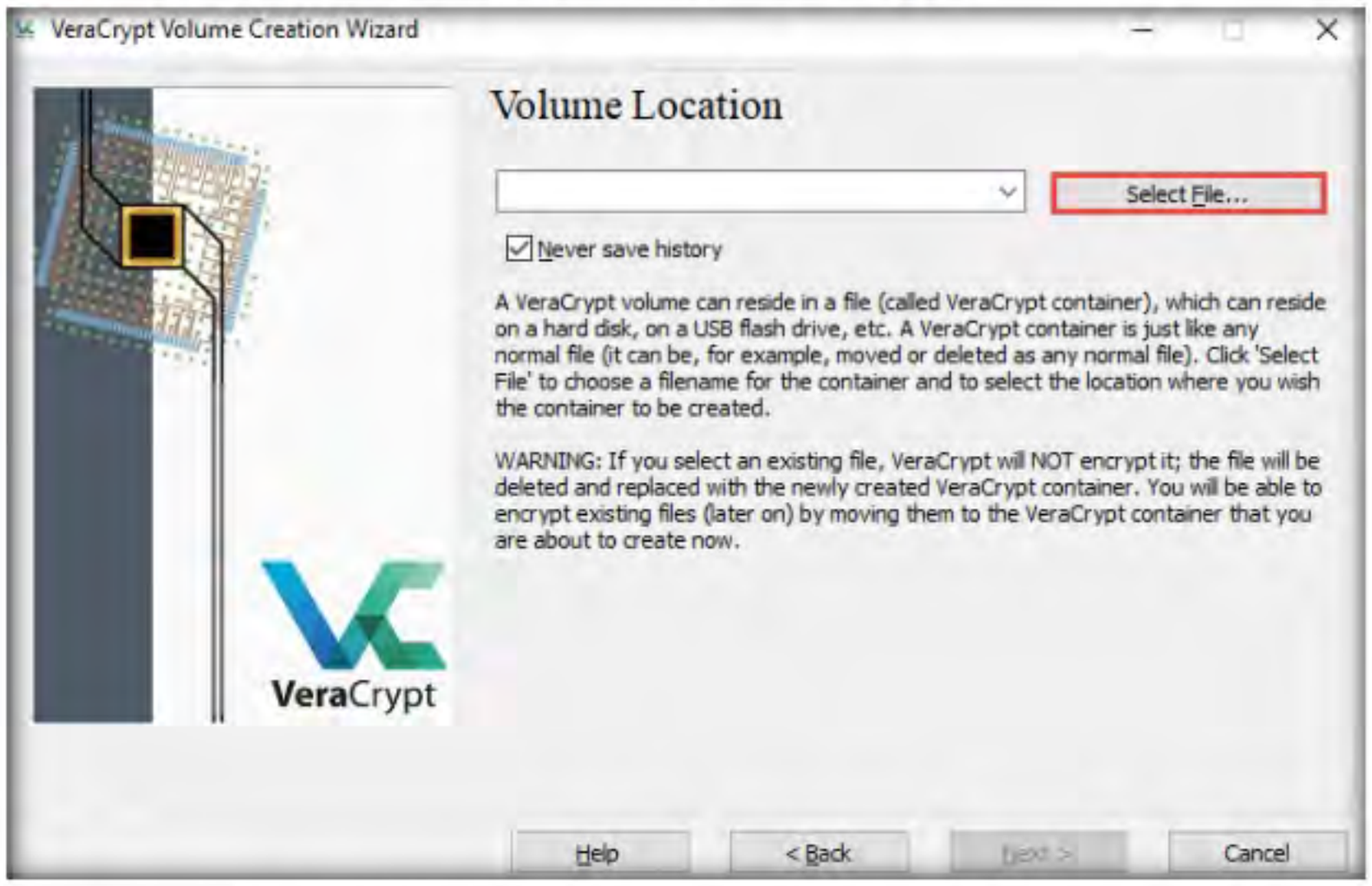


Figure 4.1.6: VeraCrypt Volume Creation Wizard-Volume Location

12. The **Specify Path and File Name** window appears; navigate to the desired location (here, **Desktop**), provide the **File name** as **My Volume**, and click **Save**.

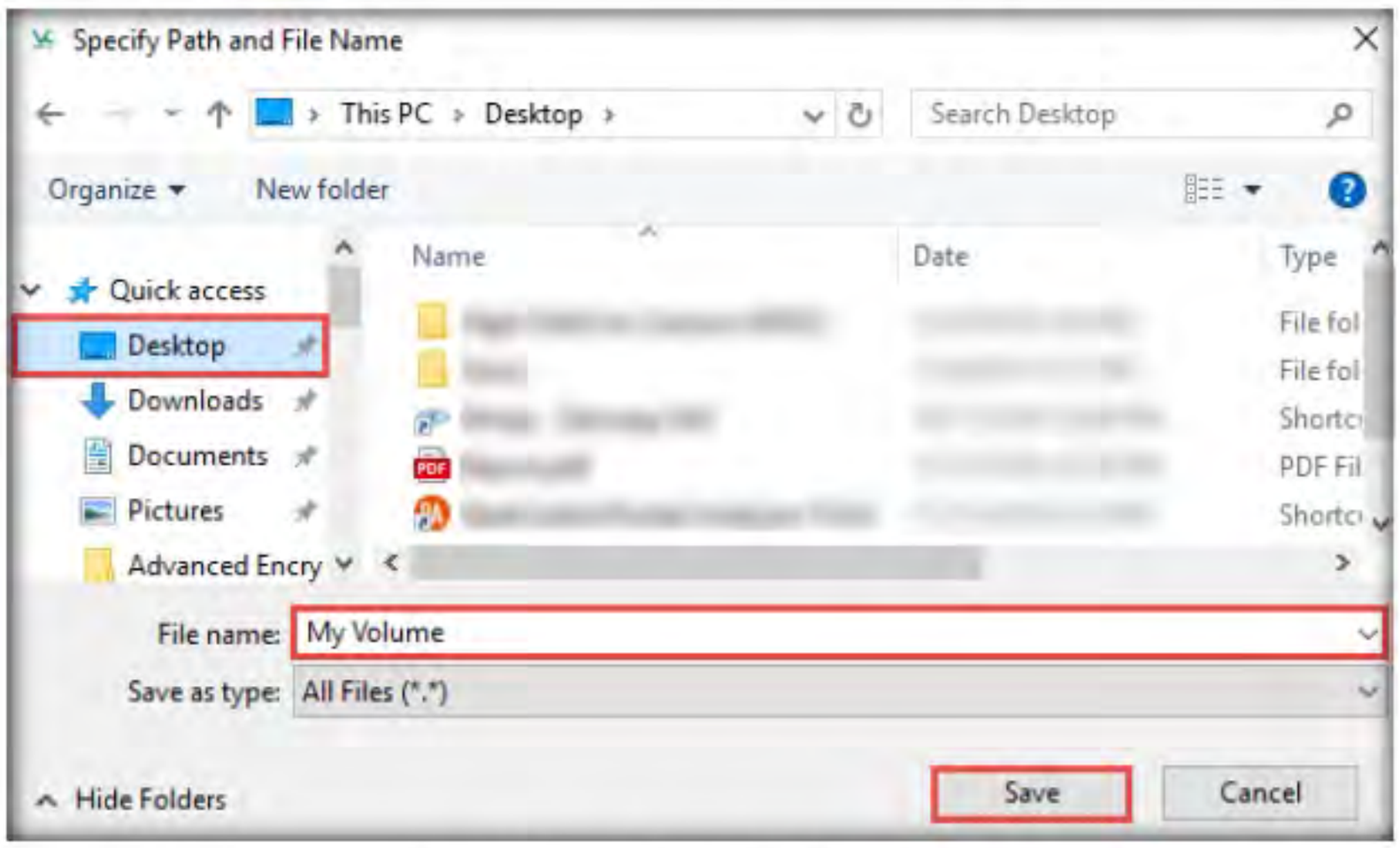


Figure 4.1.7: Specify Path and File Name Window

13. After saving the file, the location of a file containing the **VeraCrypt** volume appears under the **Volume Location** field; then, click **Next**.

Figure 4.1.8: VeraCrypt Volume Creation Wizard: Volume Location

14. In the **Encryption Options** wizard, keep the default settings and click **Next**.
15. In the **Volume Size** wizard, ensure that the **MB** radio-button is selected and specify the size of the VeraCrypt container as **5**; then, click **Next**.

Figure 4.1.9: VeraCrypt Volume Creation Wizard-Volume Size

16. The **Volume Password** wizard appears; provide a strong password in the **Password** field, retype in the **Confirm** field, and click **Next**. The password provided in this lab is **qwerty@123**.

Figure 4.1.10: VeraCrypt Volume Creation Wizard: Volume Password

Note: A **VeraCrypt Volume Creation Wizard** warning pop-up appears; then, click **Yes**.

17. The **Volume Format** wizard appears; ensure that **FAT** is selected in the **Filesystem** option and **Default** is selected in **Cluster** option.
18. Check the checkbox under the **Random Pool**, **Header Key**, and **Master Key** section.
19. Move your mouse as randomly as possible within the **Volume Creation Wizard** window for at least **30 seconds** and click the **Format** button.

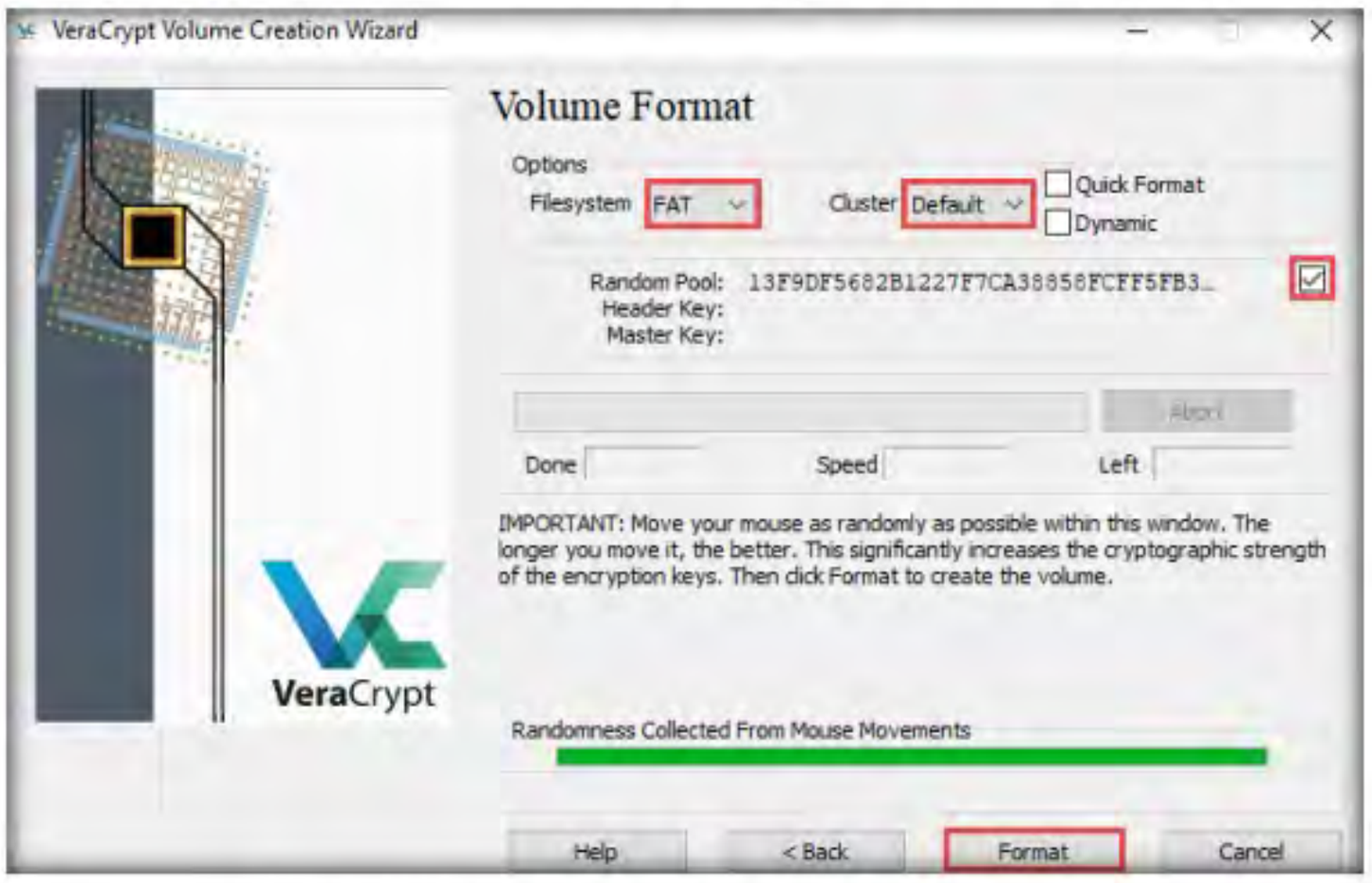


Figure 4.1.11: VeraCrypt Volume Creation Wizard-Volume Format

20. After clicking **Format**, VeraCrypt will create a file called **My Volume** in the provided folder. This file depends on the VeraCrypt container (it will contain the encrypted VeraCrypt volume).
21. Depending on the size of the volume, volume creation may take some time.
22. Once the volume is created, a **VeraCrypt Volume Creation Wizard** dialog-box appears; click **OK**.

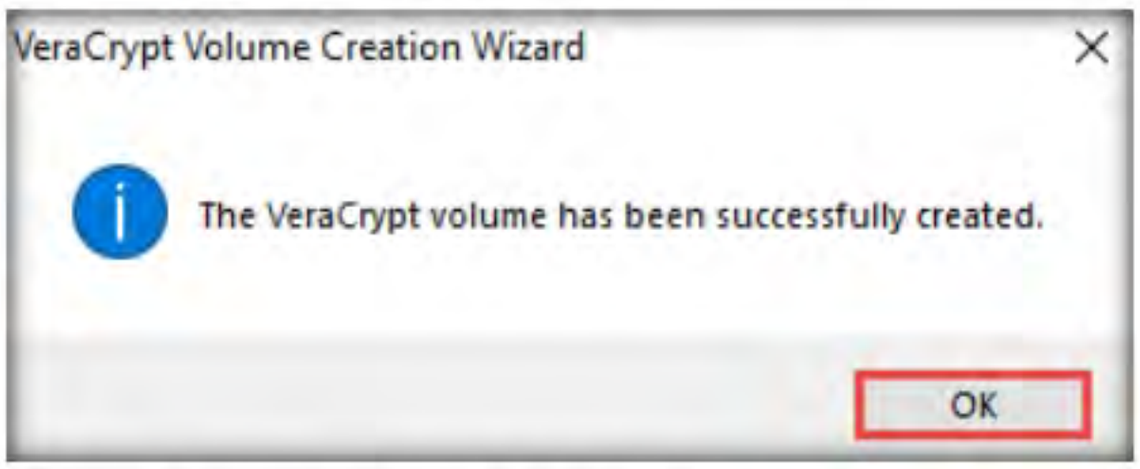


Figure 4.1.12: VeraCrypt Volume Creation Wizard Dialog Box

23. In the **VeraCrypt Volume Creation Wizard** window, a **Volume Created** message appears; then, click **Exit**.

Figure 4.1.13: VeraCrypt Volume Creation Wizard-Volume Created

TASK 1.3

Mount a Volume

24. The **VeraCrypt** main window appears; select a drive (here, **I:**) and click **Select File...**.

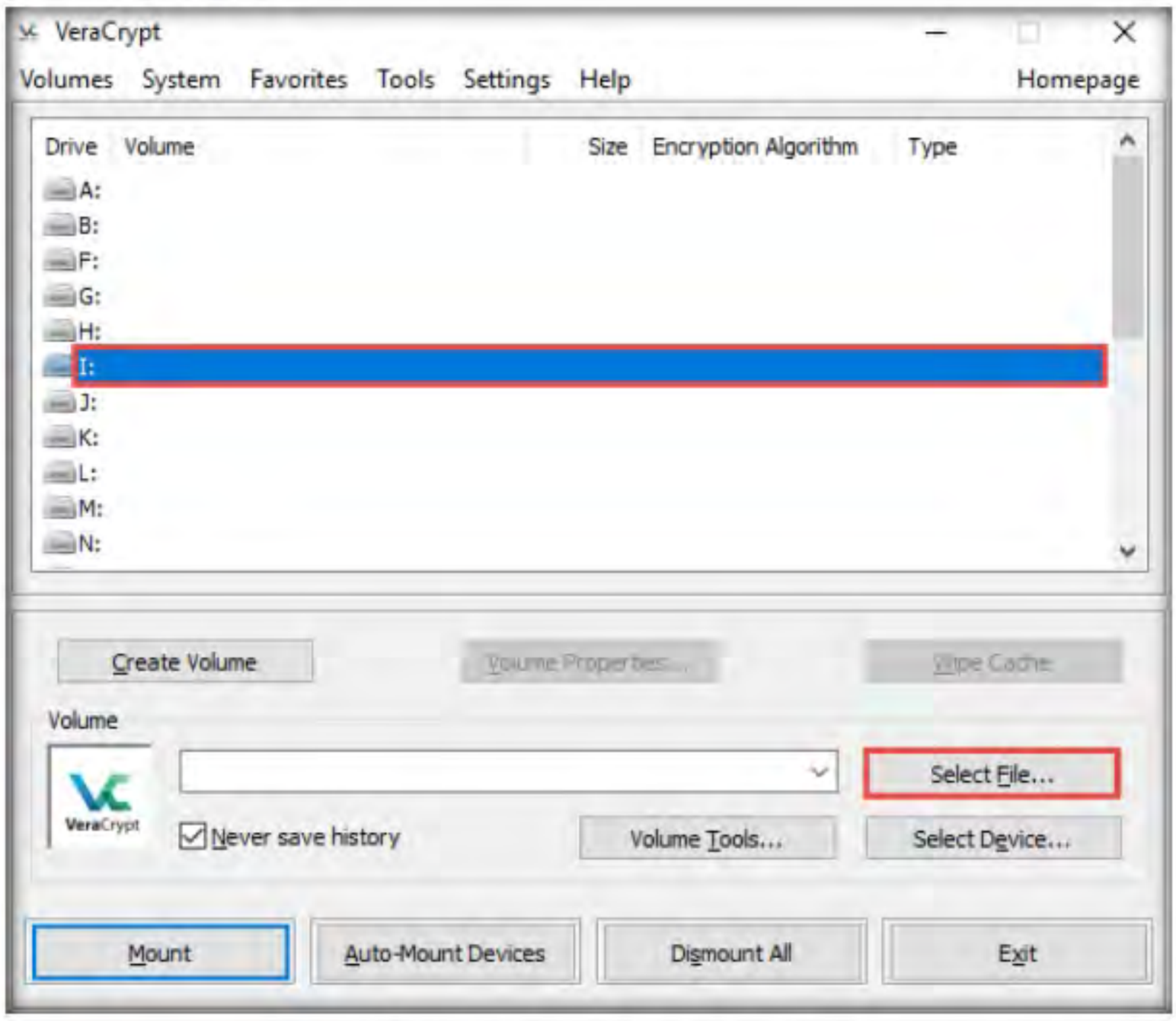


Figure 4.1.14: VeraCrypt Main Window with Select File Button

25. The **Select a VeraCrypt Volume** window appears; navigate to **Desktop**, click **My Volume**, and click **Open**.

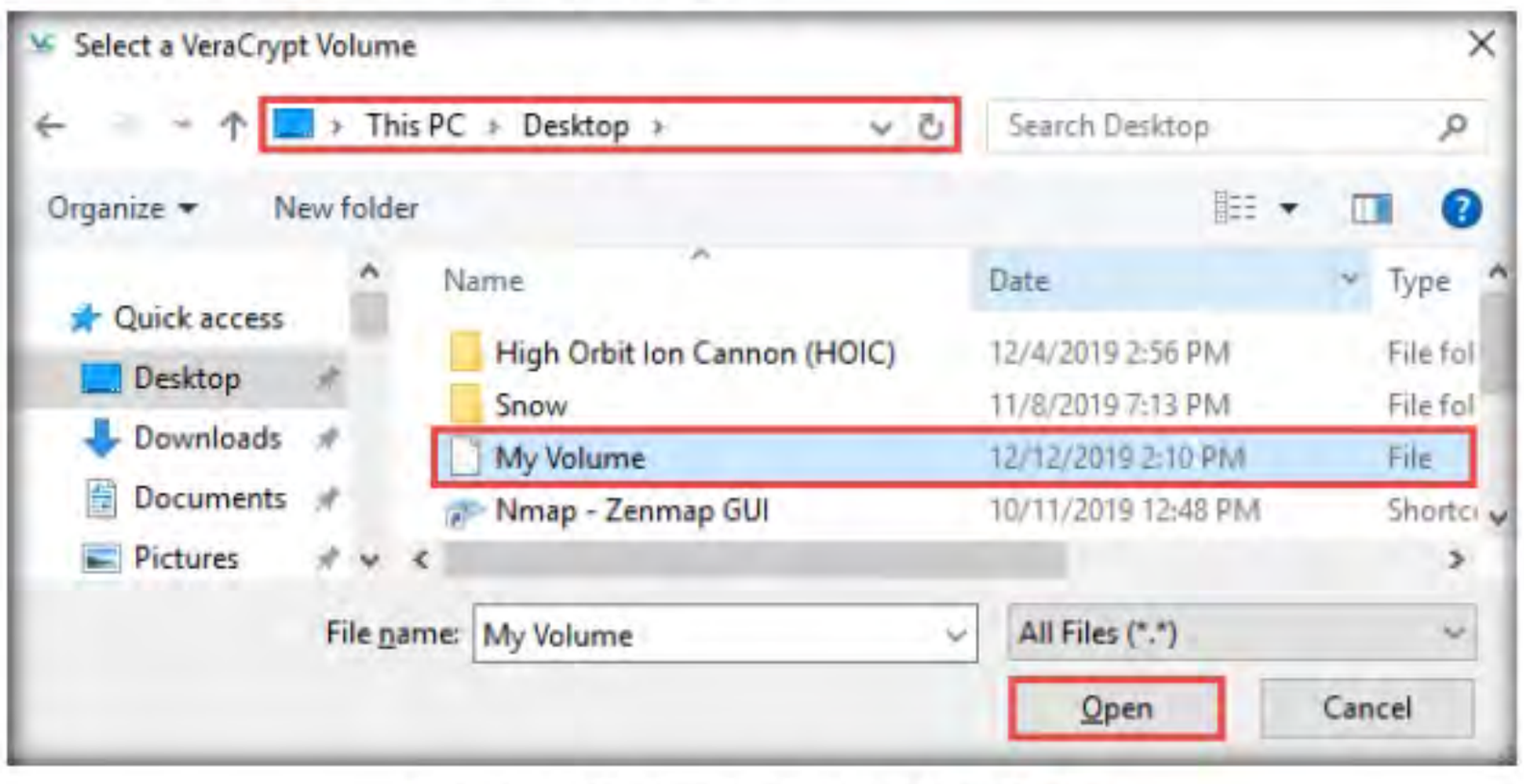


Figure 4.1.15: Windows Standard File Selector Window

26. The window closes, and the **VeraCrypt** window appears displaying the location of selected volume under the **Volume** field; then, click **Mount**.

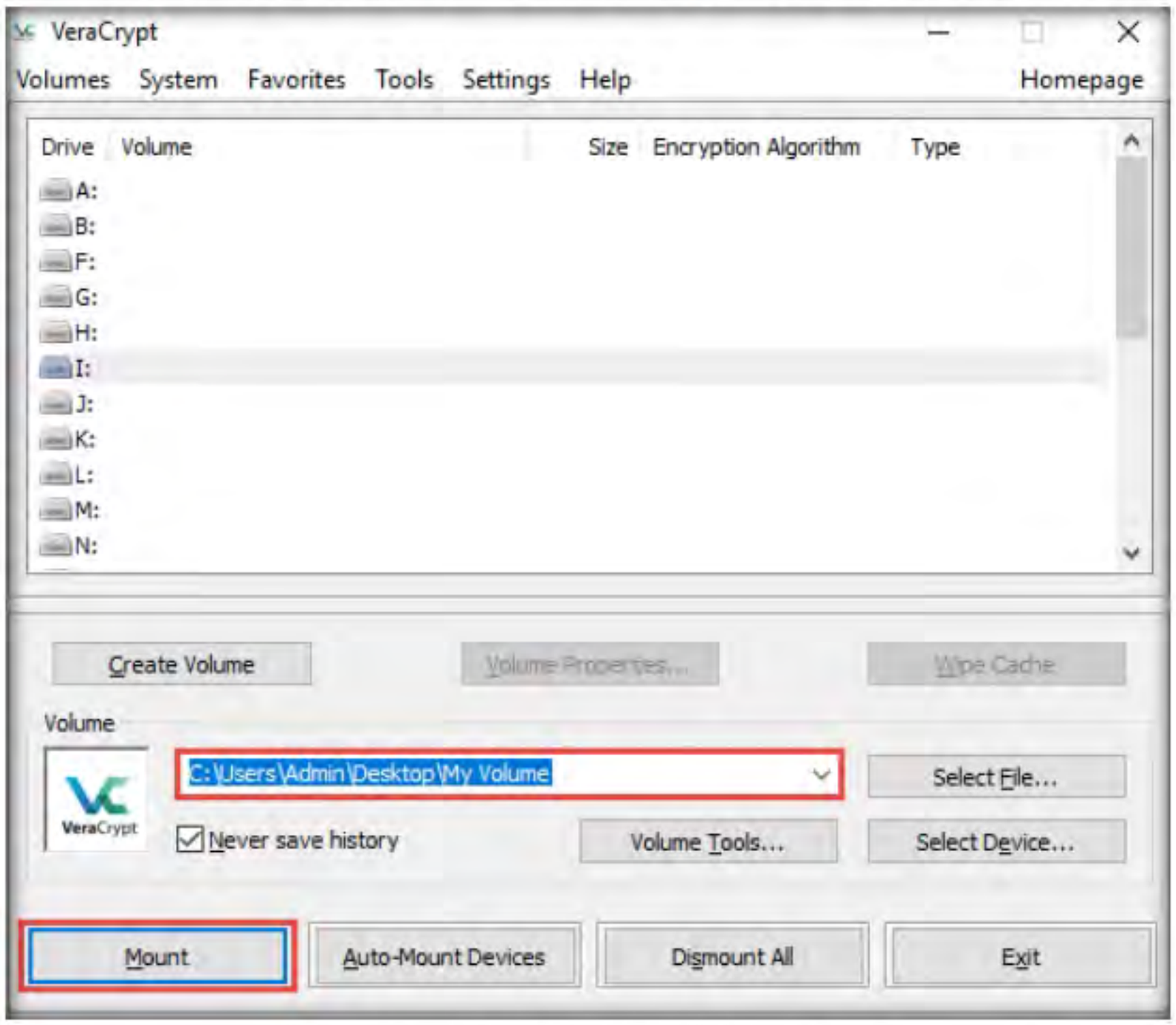


Figure 4.1.16: VeraCrypt Main Window with Mount Button

27. The **Enter password** dialog-box appears; type the password you specified in **Step#16** into the **Password** field and click **OK**.

Note: The password specified in this task is **qwerty@123**.

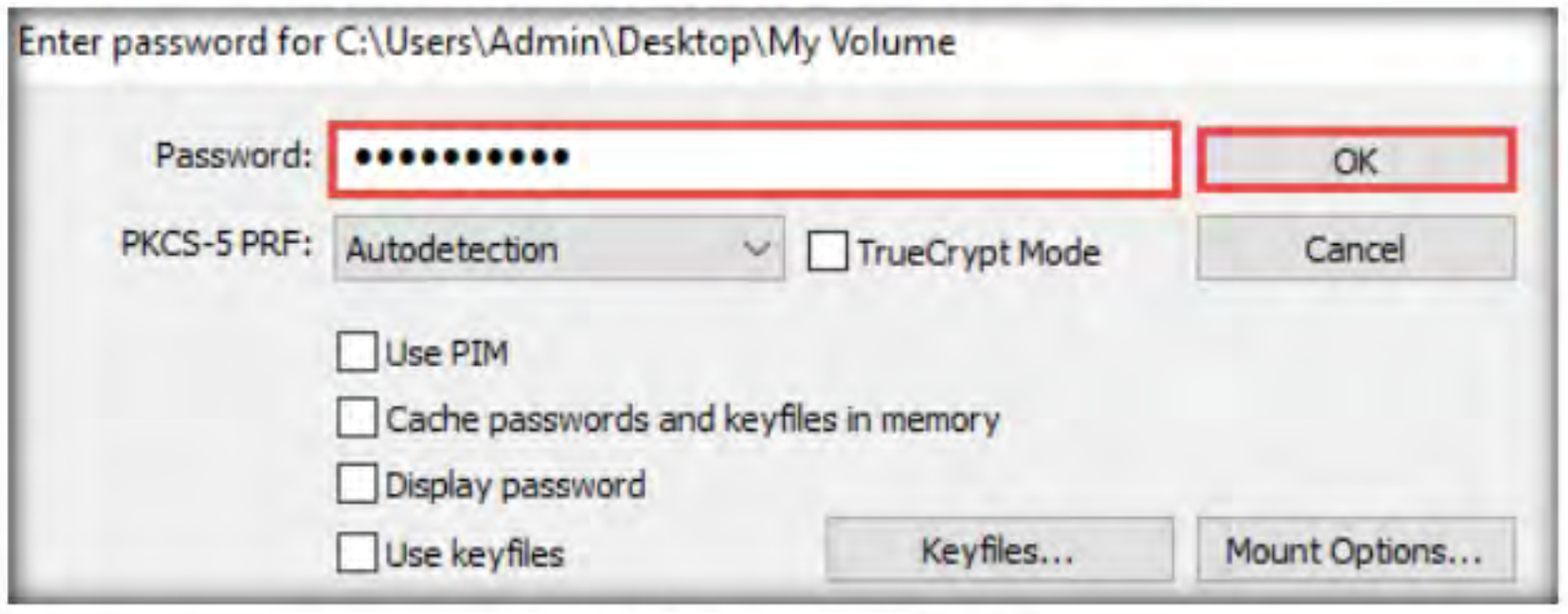


Figure 4.1.17: VeraCrypt Enter password

28. After the password is verified, **VeraCrypt** will mount the volume in **I:** drive, as shown in the screenshot:

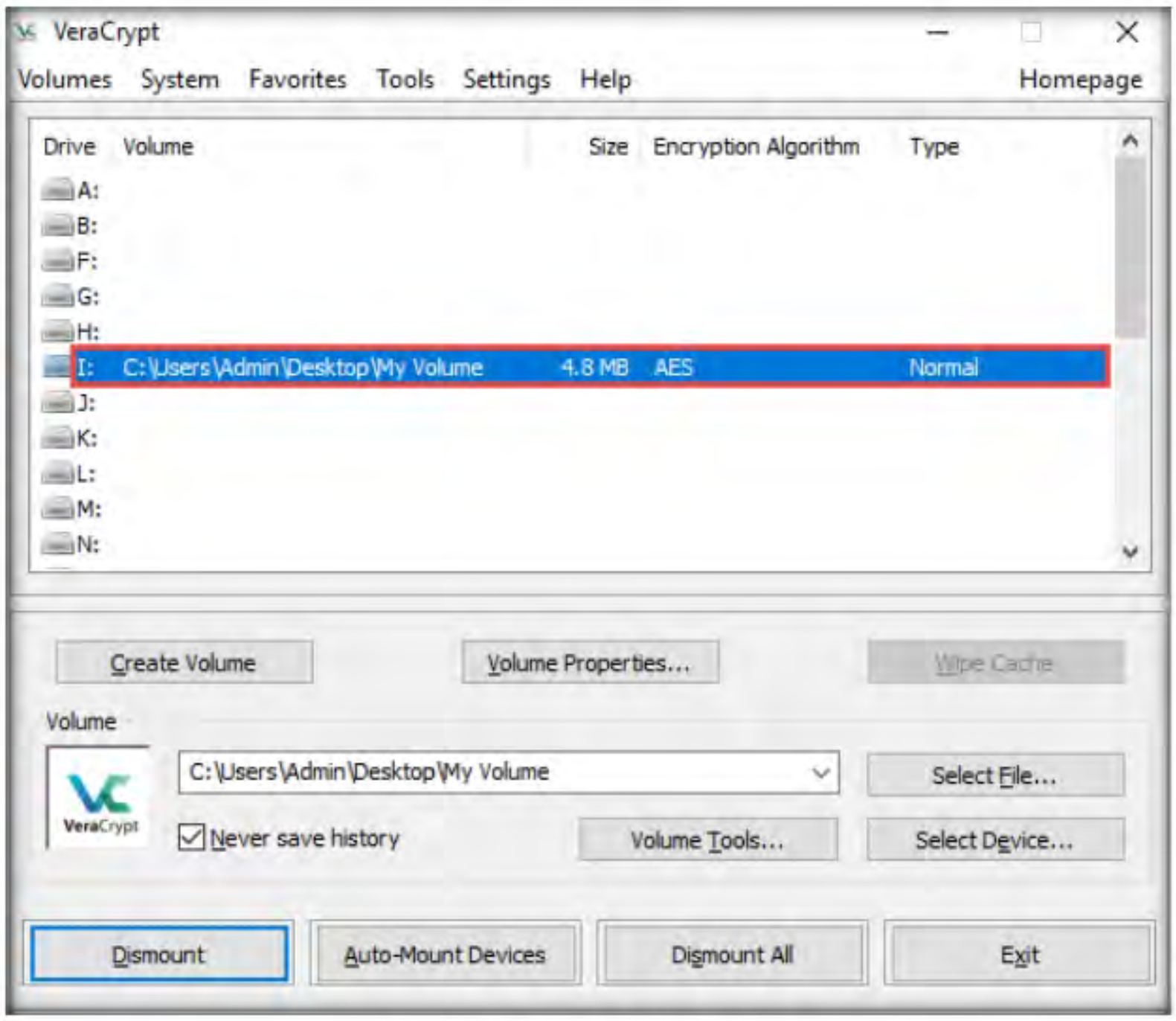


Figure 4.1.18: VeraCrypt Main Window

29. **My Volume** has successfully mounted the container as a virtual disk (**I:**). The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves similarly to a real disk. You can copy or move files to this virtual disk to encrypt them.
30. Create a text file on **Desktop** and name it **Test**. Open the text file and insert text.
31. Click **File** in the menu bar and click **Save**.

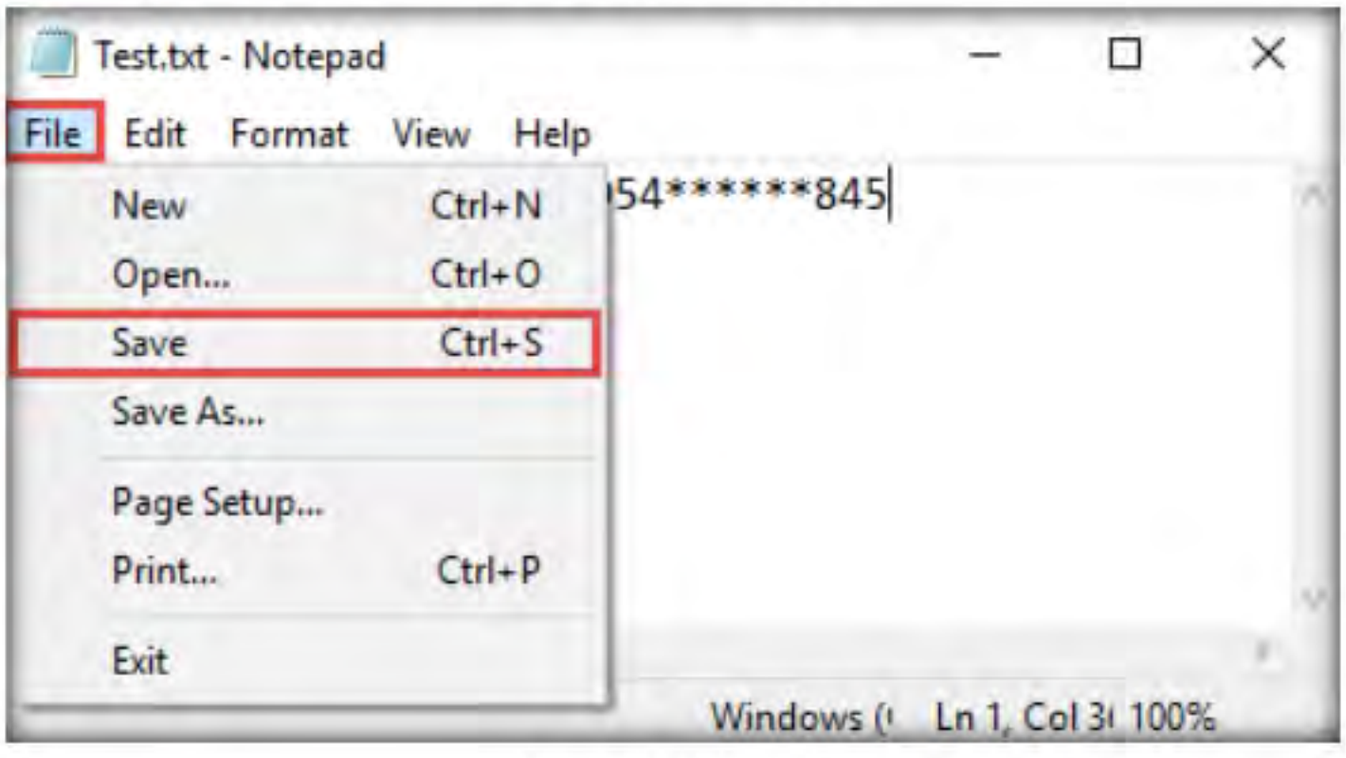


Figure 4.1.19: Text file

32. Copy the file from **Desktop** and paste it into **Local Disk (I:)**. Close the window.

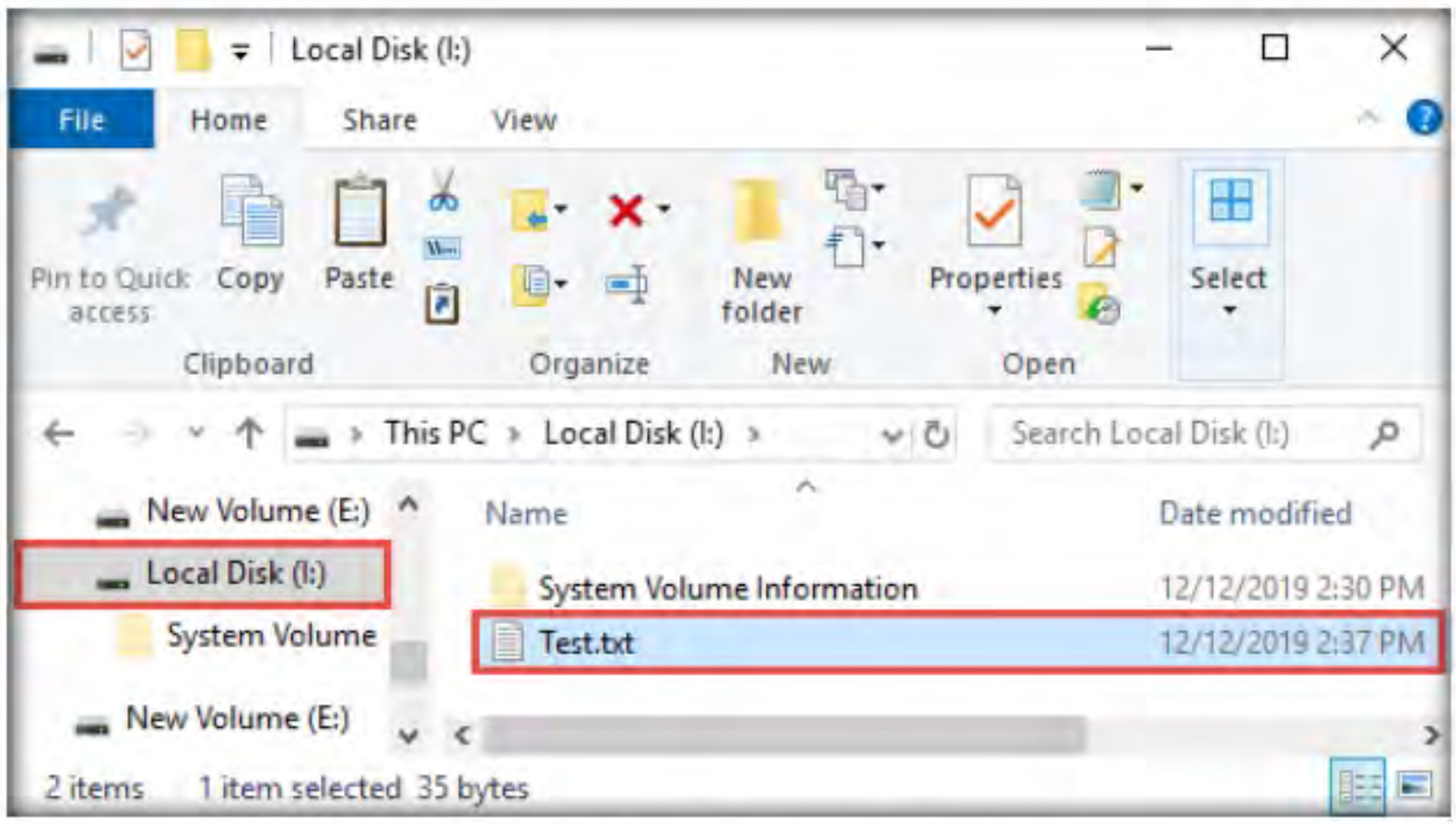


Figure 4.1.20: Test.txt file in Encrypted Container

TASK 1.4

Dismount a Volume

33. Switch to the **VeraCrypt** window, click **Dismount**, and then click **Exit**.

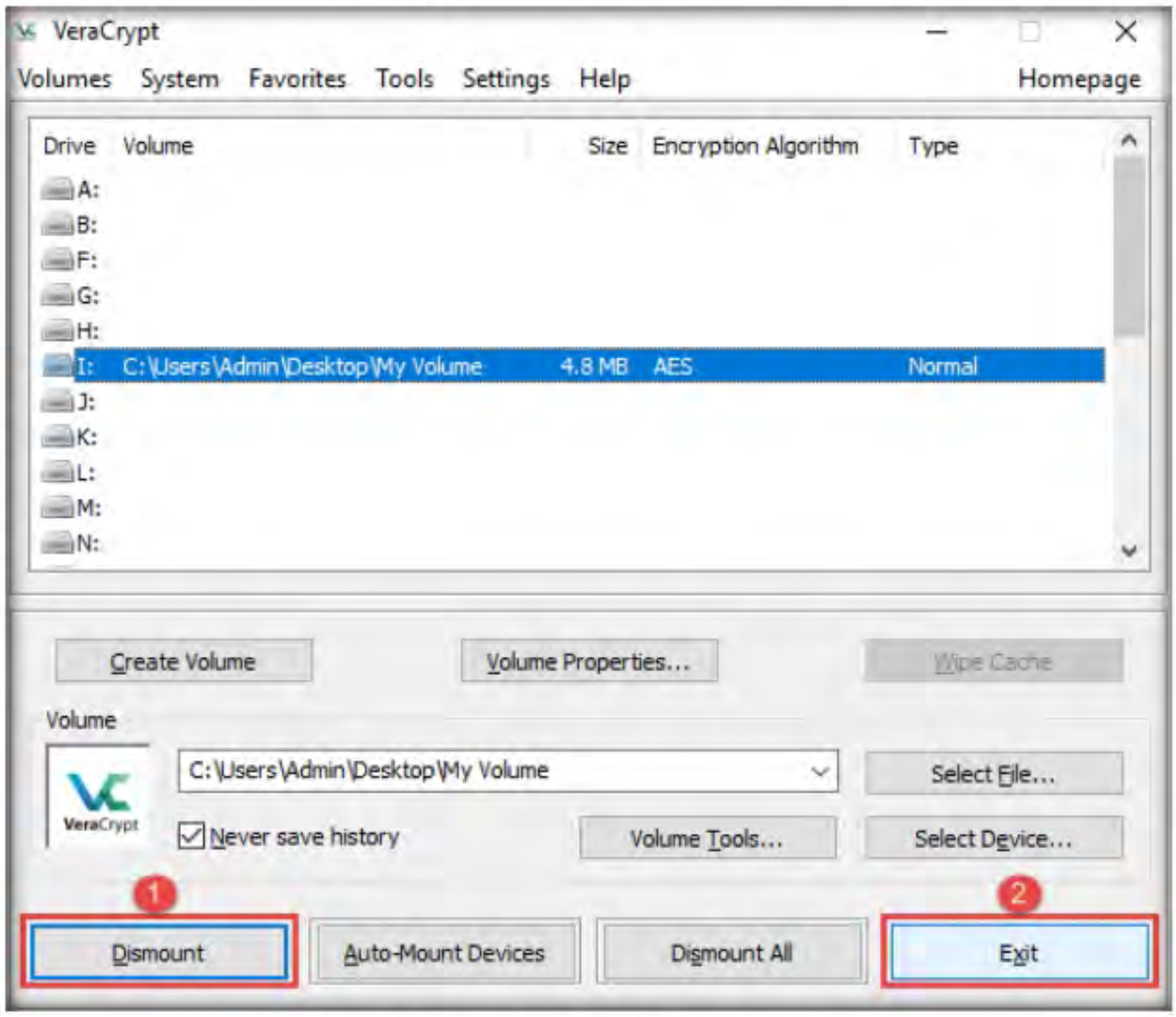


Figure 4.1.21: VeraCrypt Main Window with Dismount Button

34. The **I:** drive located in **This PC** disappears.

Note: This lab is used to demonstrate that, in cases of system hacks, if an attacker manages to gain remote access or complete access to the machine, he/she will not be able to find the encrypted volume—including its files—unless he/she is able to obtain the password. Thus, all sensitive information located on the encrypted volume is safeguarded.

35. This concludes the demonstration of performing disk encryption using VeraCrypt.
36. Close all open windows and document all the acquired information.

TASK 2 Perform Disk Encryption using BitLocker Drive Encryption

Here, we will perform disk encryption using BitLocker Drive Encryption.

TASK 2.1 Launch BitLocker

1. In the **Windows 10** virtual machine, click the **Type here to search** field present at the bottom-left corner of **Desktop** and type **bitlocker**. Select **Manage BitLocker** from the search results.

BitLocker provides offline-data and OS protection for your computer, and helps to ensure that data stored on a computer that is running Windows® is not revealed if the computer is tampered with when the installed OS is offline. BitLocker uses a microchip that is called a Trusted Platform Module (TPM) to provide enhanced protection for your data and to preserve early boot-component integrity. The TPM can help protect your data from theft or unauthorized viewing by encrypting the entire Windows volumes.

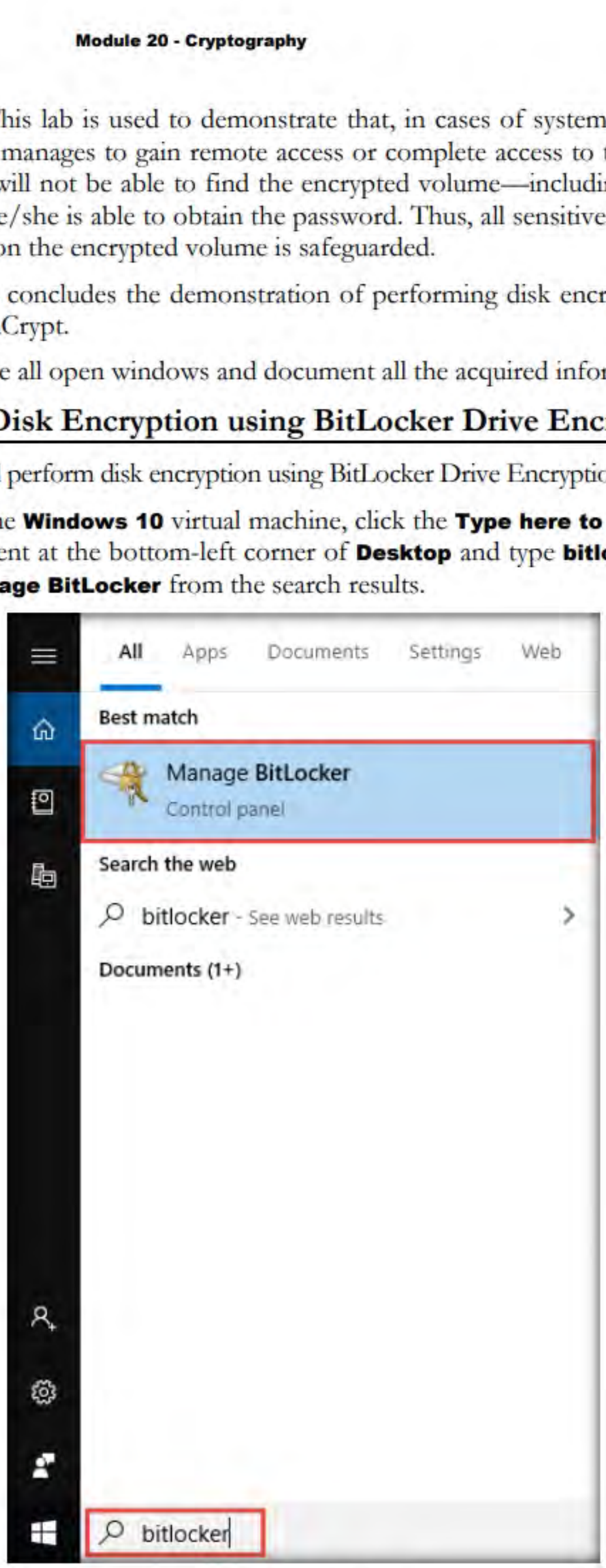


Figure 4.2.1: Launch BitLocker

2. The **BitLocker Drive Encryption** window appears; click the **New Volume (E:) BitLocker off** option under the **Removable data drives - BitLocker To Go** section.

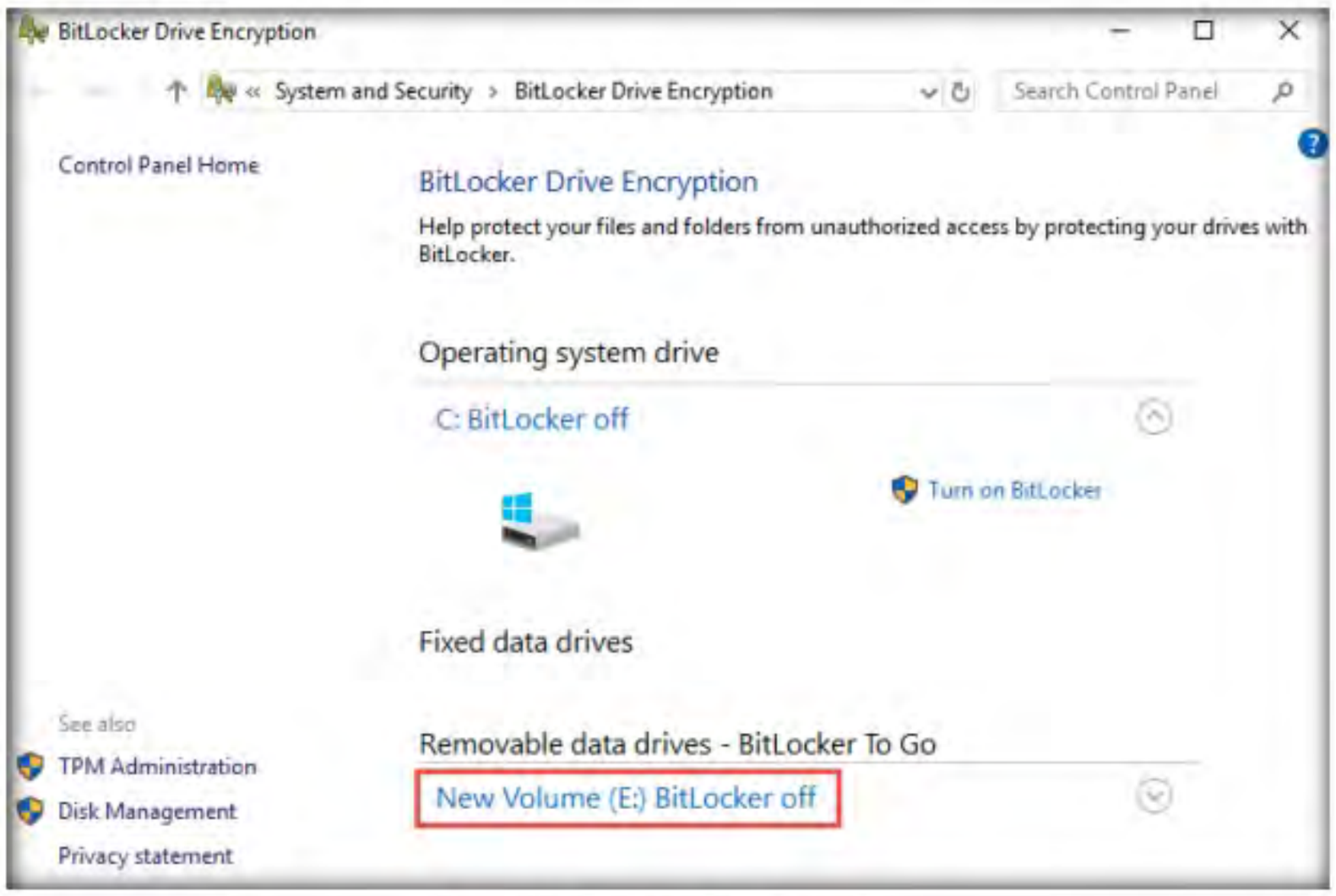


Figure 4.2.2: BitLocker Drive Encryption

TASK 2.2

Encrypt the Drive

3. Click the **Turn on BitLocker** option under **New Volume (E:) BitLocker off**.

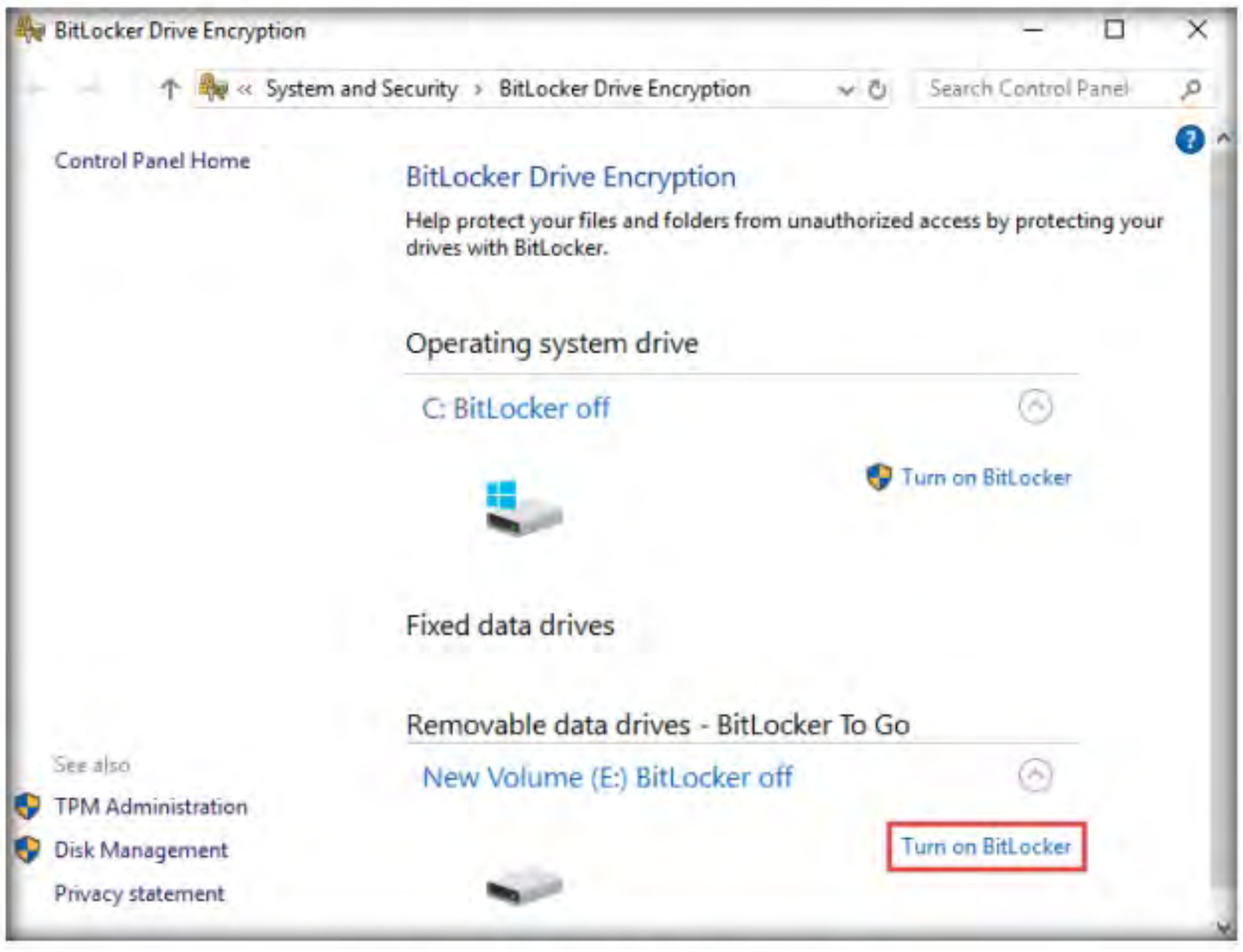


Figure 4.2.3: Turn on BitLocker option

4. The **BitLocker Drive Encryption (E:)** wizard appears; check the **Use a password to unlock the drive** checkbox.
5. Type the password in the **Enter your password** field and re-type the password in the **Reenter your password** field; then, click **Next** (Here, the password entered is **test@123**).

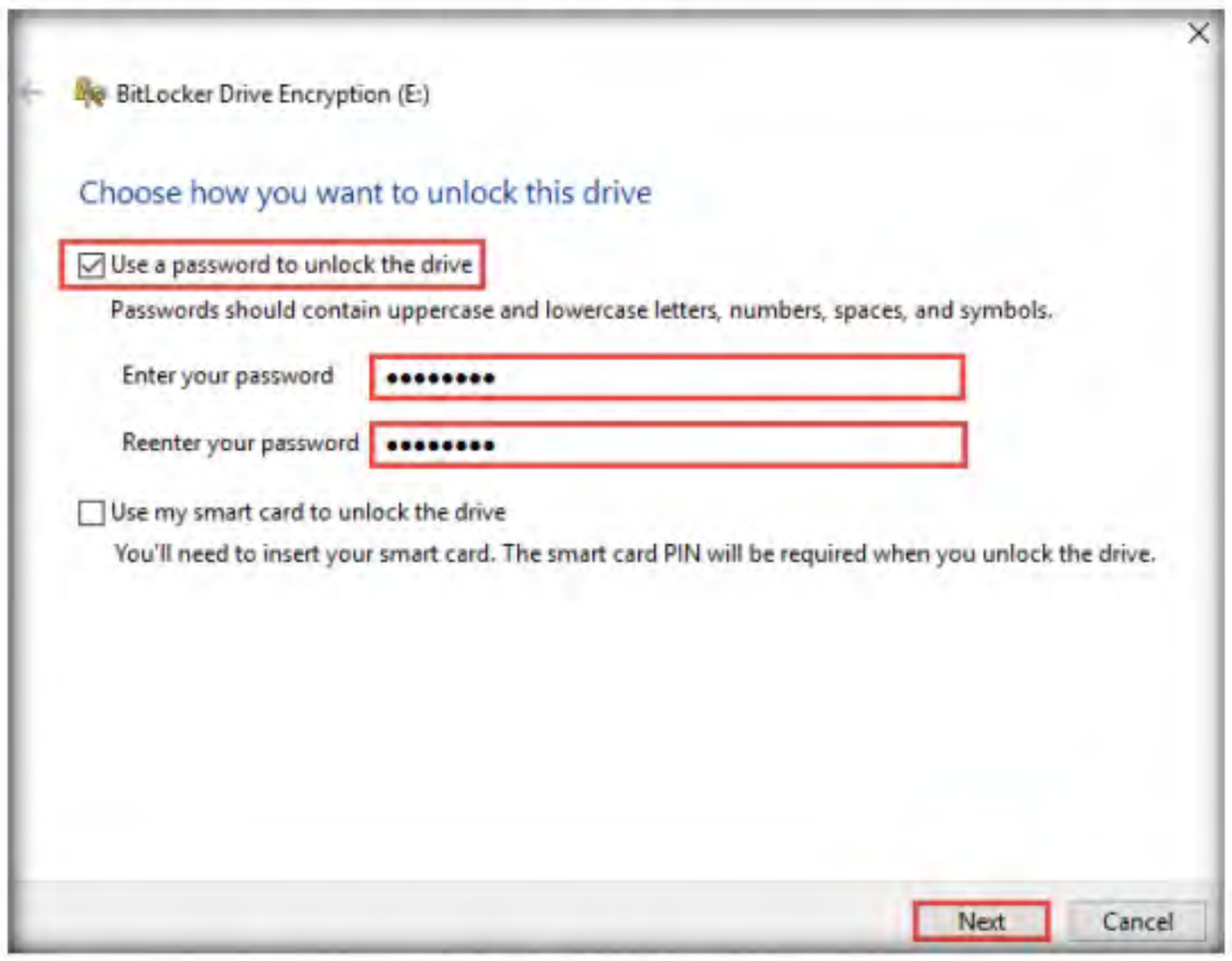


Figure 4.2.4: BitLocker Drive Encryption (E:) wizard

6. The **How do you want to back up your recovery key?** step appears; click **Save to a file** from the available options.

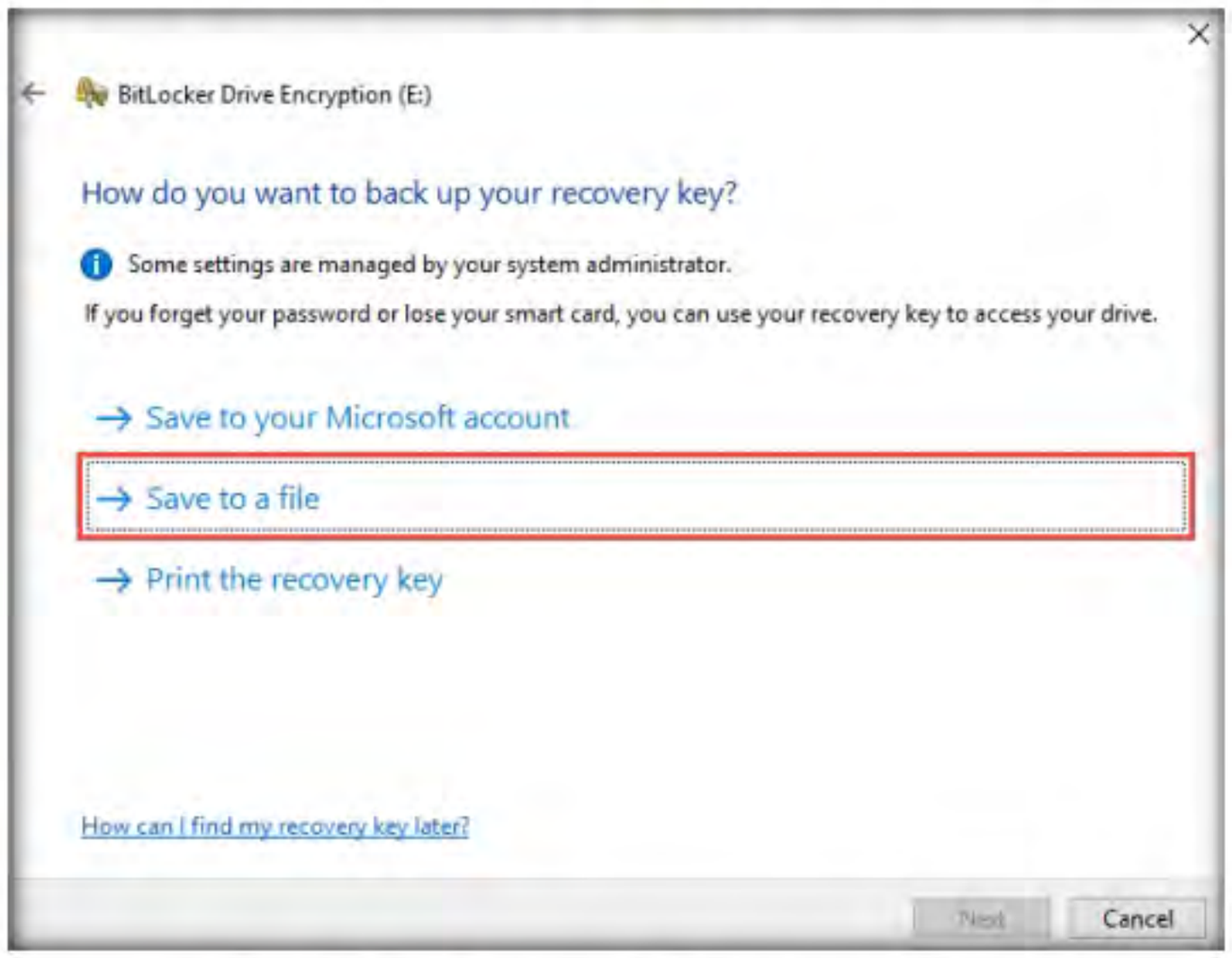


Figure 4.2.5: How do you want to back up your recovery key? step

7. The **Save BitLocker recovery key as** window appears; keep the save location set to default and click **Save**.

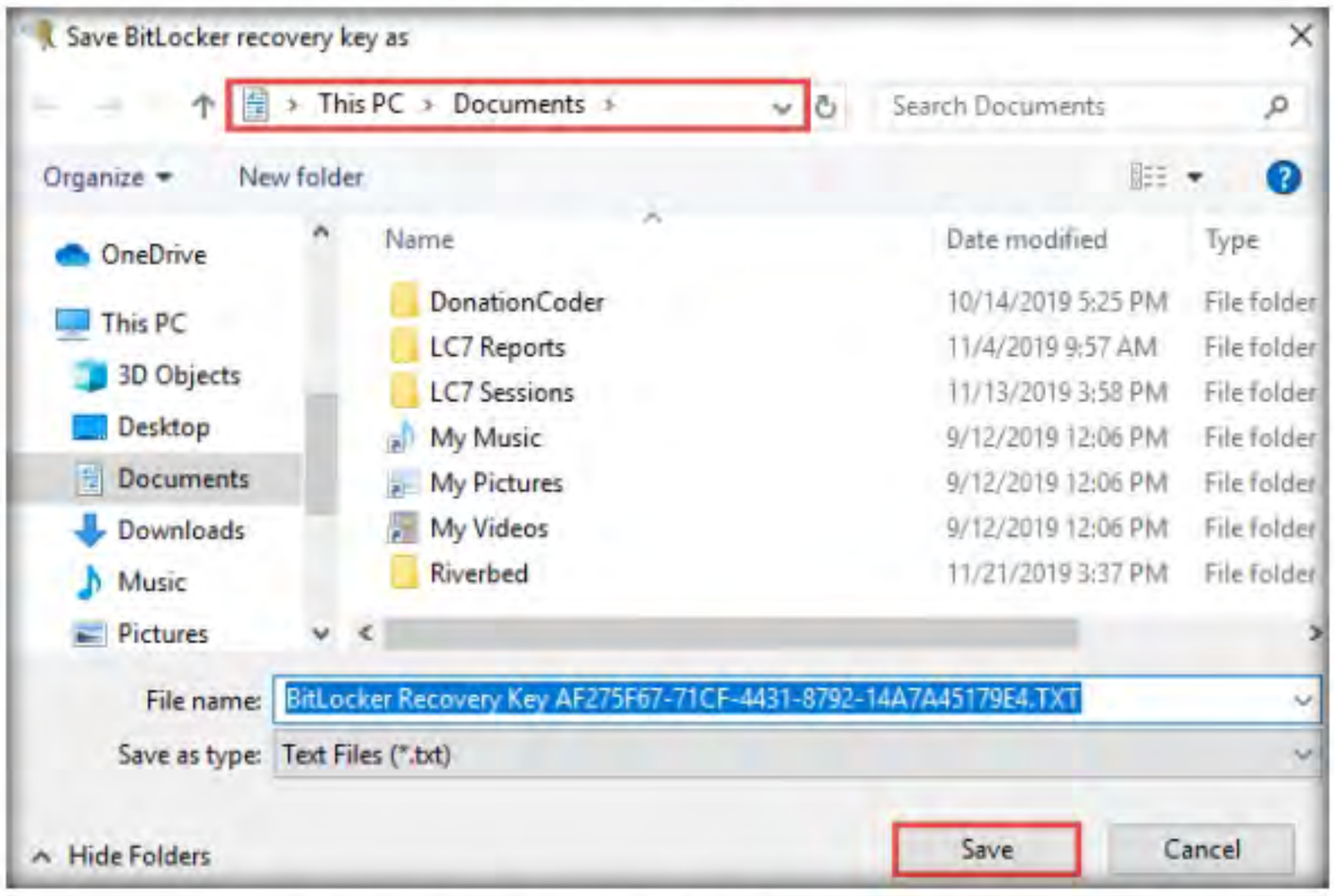


Figure 4.2.6: How do you want to back up your recovery key? step

8. Click **Next** in the **How do you want to back up your recovery key?** step.
9. In the **Choose how much of your drive to encrypt** step, select the **Encrypt entire drive (slower but best for PCs and drives already in use)** button, and click **Next**.

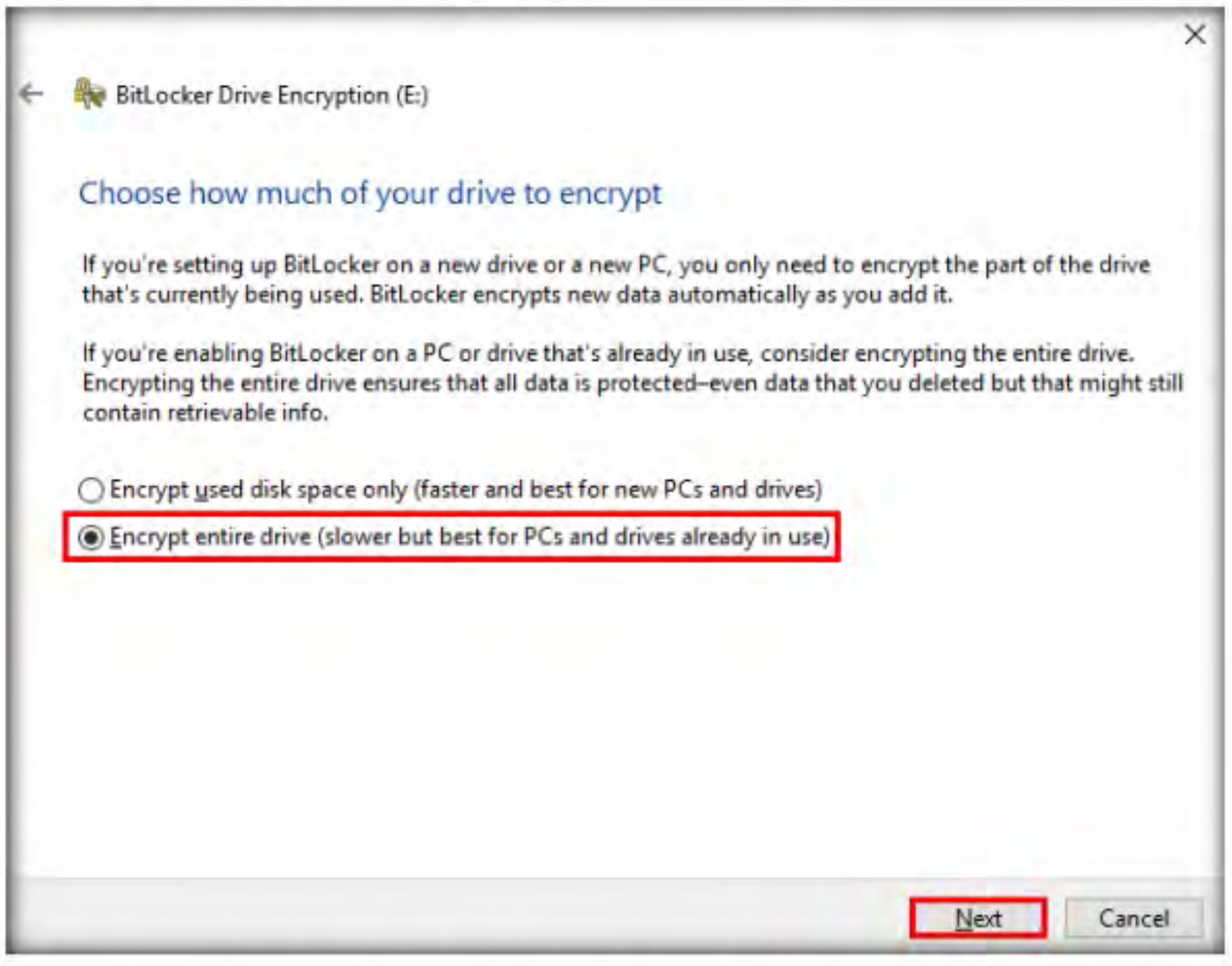


Figure 4.2.7: Choose how much of your drive to encrypt step

10. In the **Choose which encryption mode to use** step, ensure that the **Compatible mode (best for drives that can be moved from this device)** option is selected, and click **Next**.

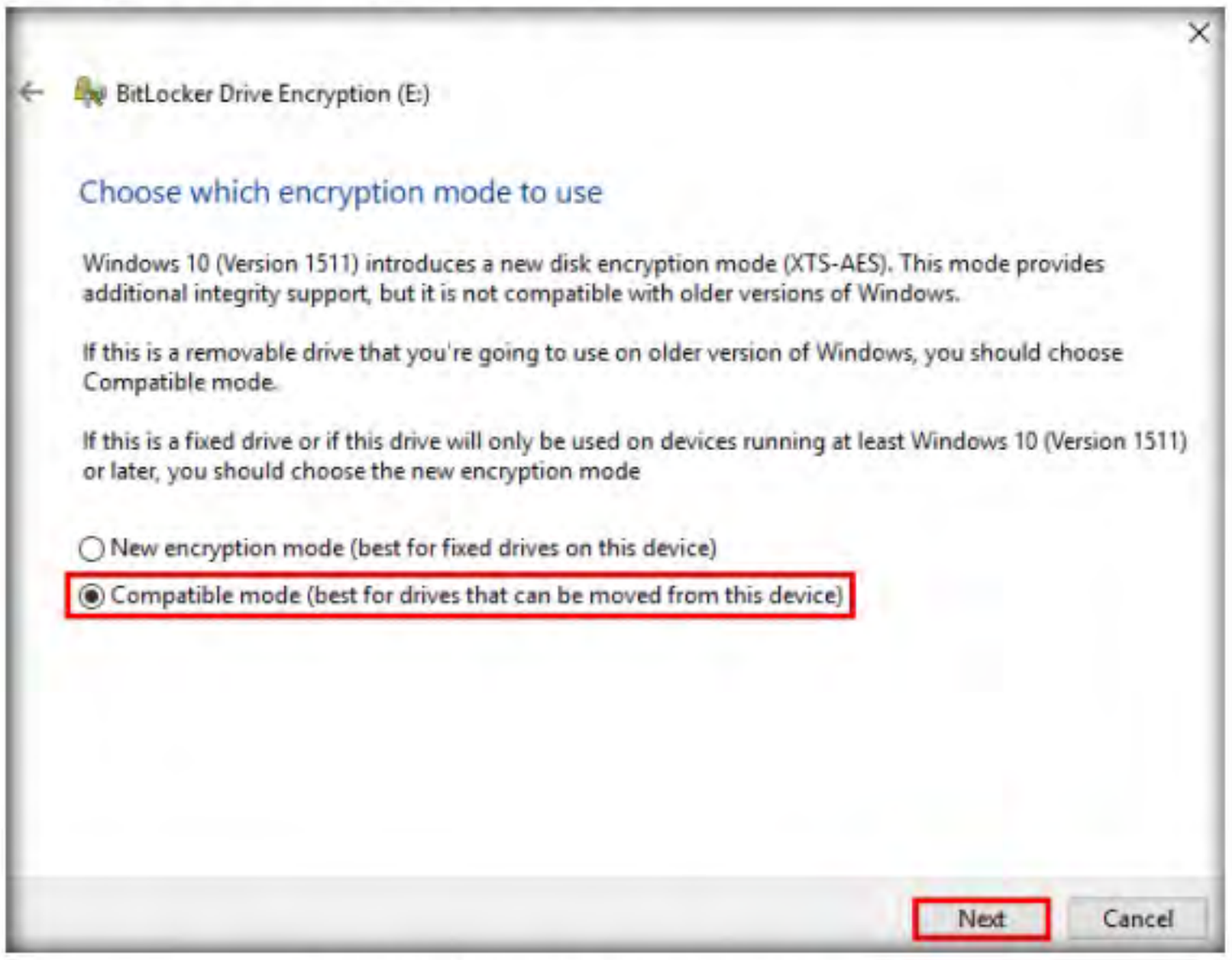


Figure 4.2.8: Choose which encryption mode to use step

11. In the **Are you ready to encrypt this drive?** step, click **Start encrypting** to encrypt the selected drive.

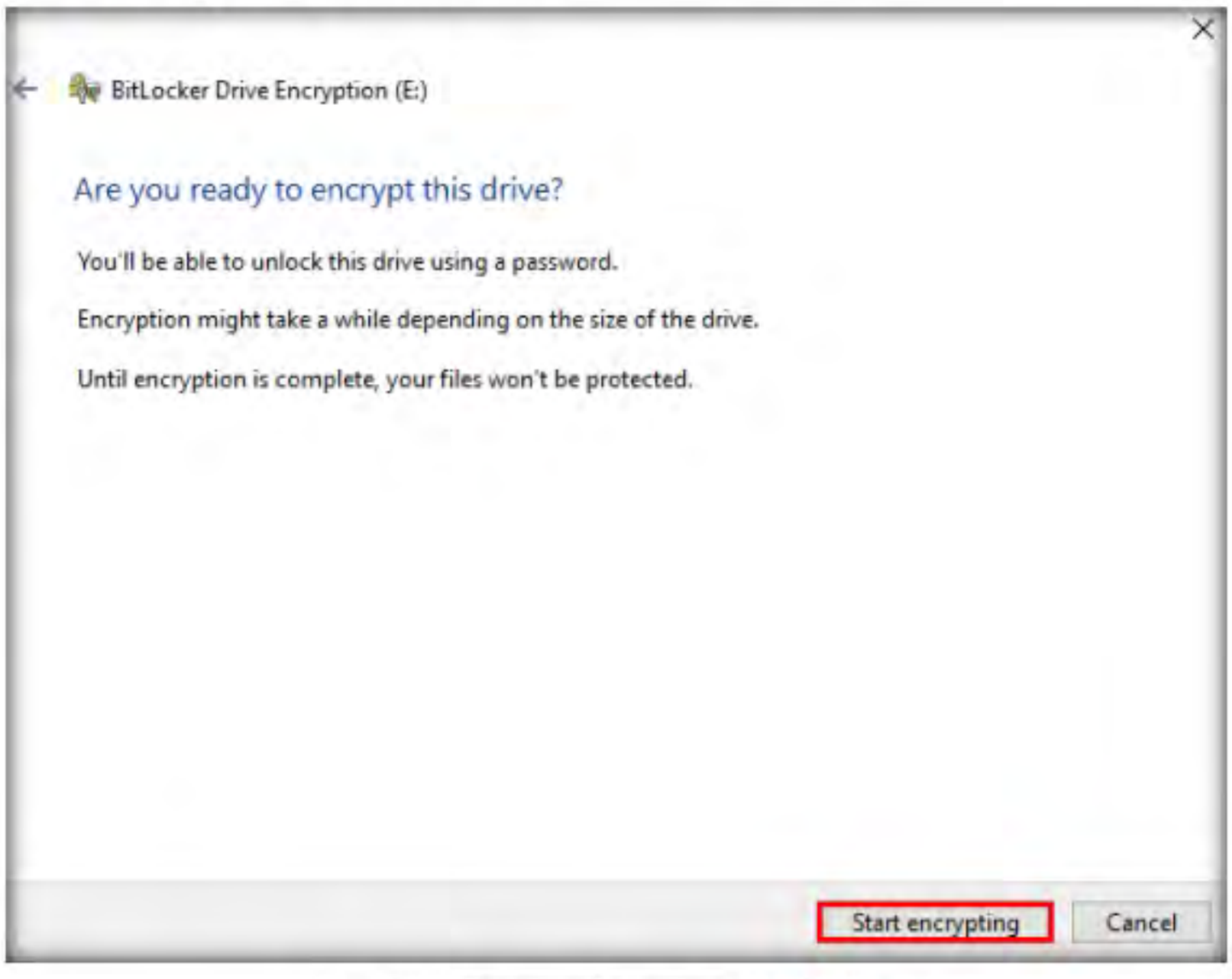


Figure 4.2.9: Are you ready to encrypt this drive? steps

12. The **BitLocker Drive Encryption** pop-up appears, showing the **Encrypting...** status.

Figure 4.2.10: Encrypting pop-up

13. After the completion of the encryption process, the **Encryption of E: is complete** notification appears; click **Close** and **Restart** the virtual machine.

Figure 4.2.11: Encryption of E: is complete notification

14. After the system reboots, log in with the credentials **Admin**/**Pa$$w0rd**.

TASK 2.3

Access the Encrypted Disk

15. Open **File Explorer** and click **This PC** from the left pane.
16. You can observe that **Local Disk (E:)** is now encrypted; double-click and the **BitLocker (E:)** security pop-up appears at the top-right corner of **Desktop**.
17. Type the password you provided in **Step#5** and click **Unlock**.

Note: Here, the password is **test@123**.

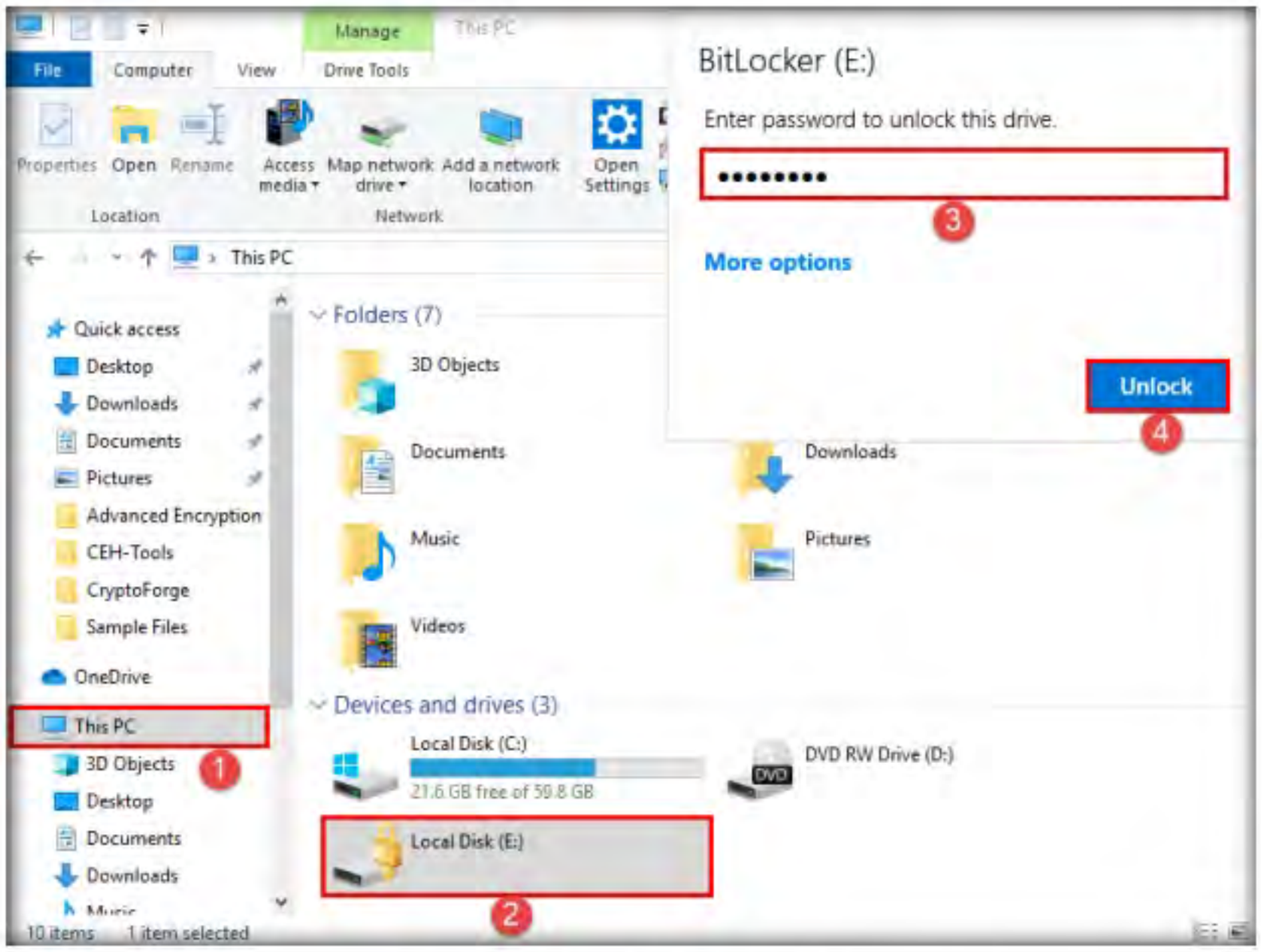


Figure 4.2.12: Accessing the encrypted disk

18. The **New Volume (E:)** pop-up appears at the top-right corner of the window. Click the **Open folder to view files** option to view the disk content.

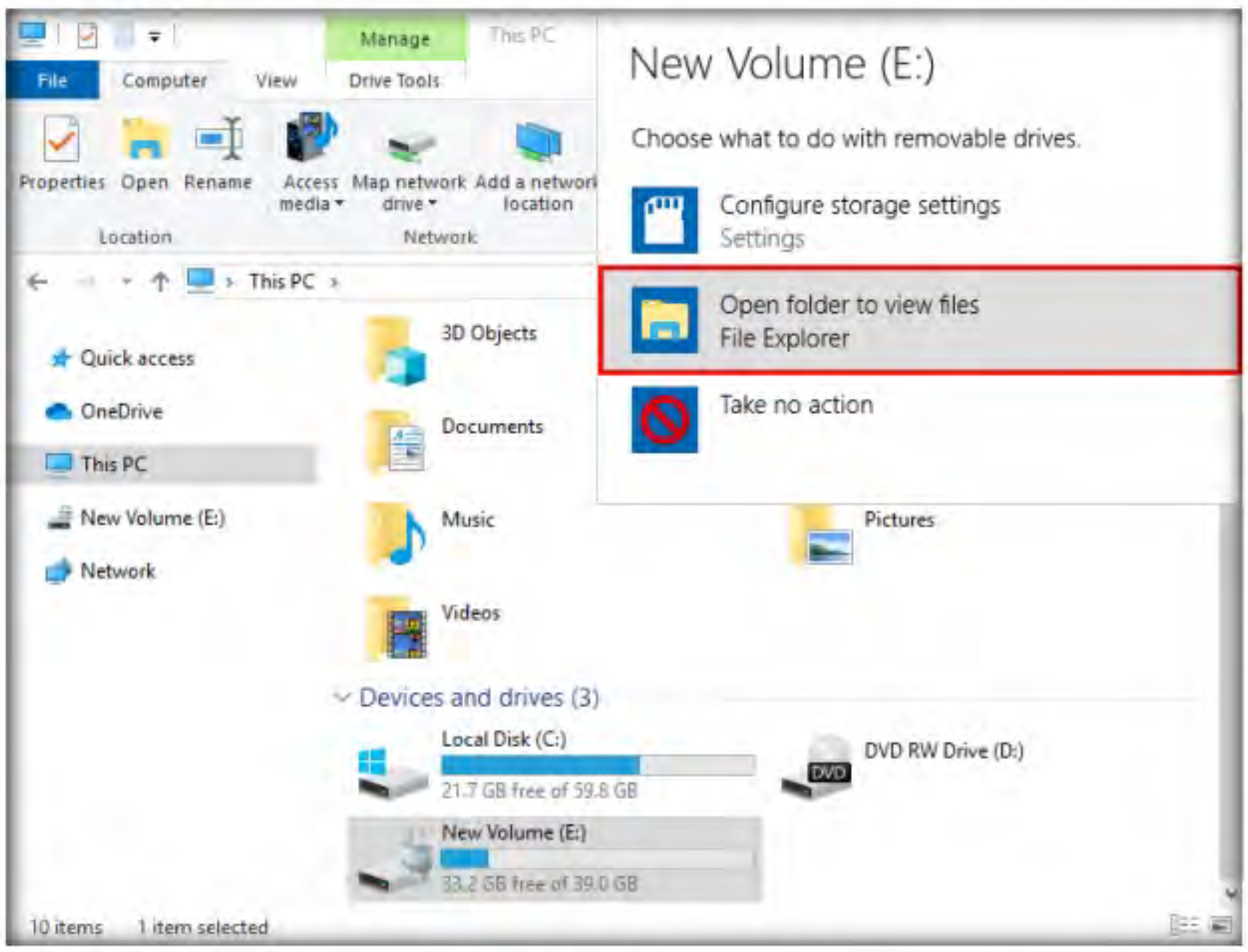


Figure 4.2.13: New Volume (E:) pop-up

19. The **New Volume (E:)** window appears displaying the disk content, as shown in the screenshot.

Note: The disk will remain unlocked until the next time you restart the system.

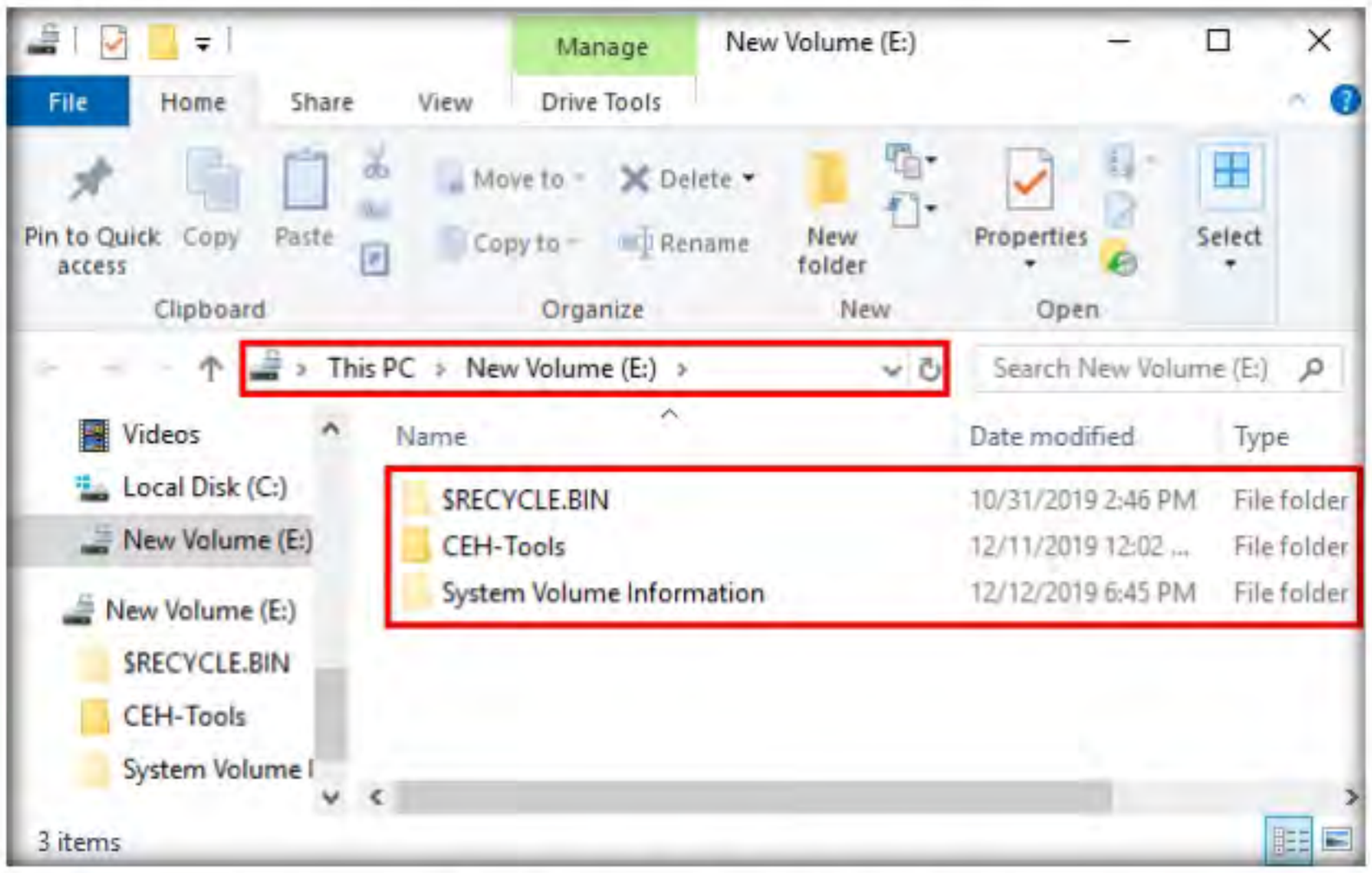


Figure 4.2.14: New Volume (E:) disk content

20. This concludes the demonstration of performing disk encryption using BitLocker Drive Encryption.
21. Once, you are done with this task; you must turn off BitLocker to decrypt the **New Volume (E:)** disk.

TASK 2.4

Turn off BitLocker

22. To do so, open the **BitLocker Drive Encryption** window, click **New Volume (E:) BitLocker on** and from the options click **Turn off BitLocker**.

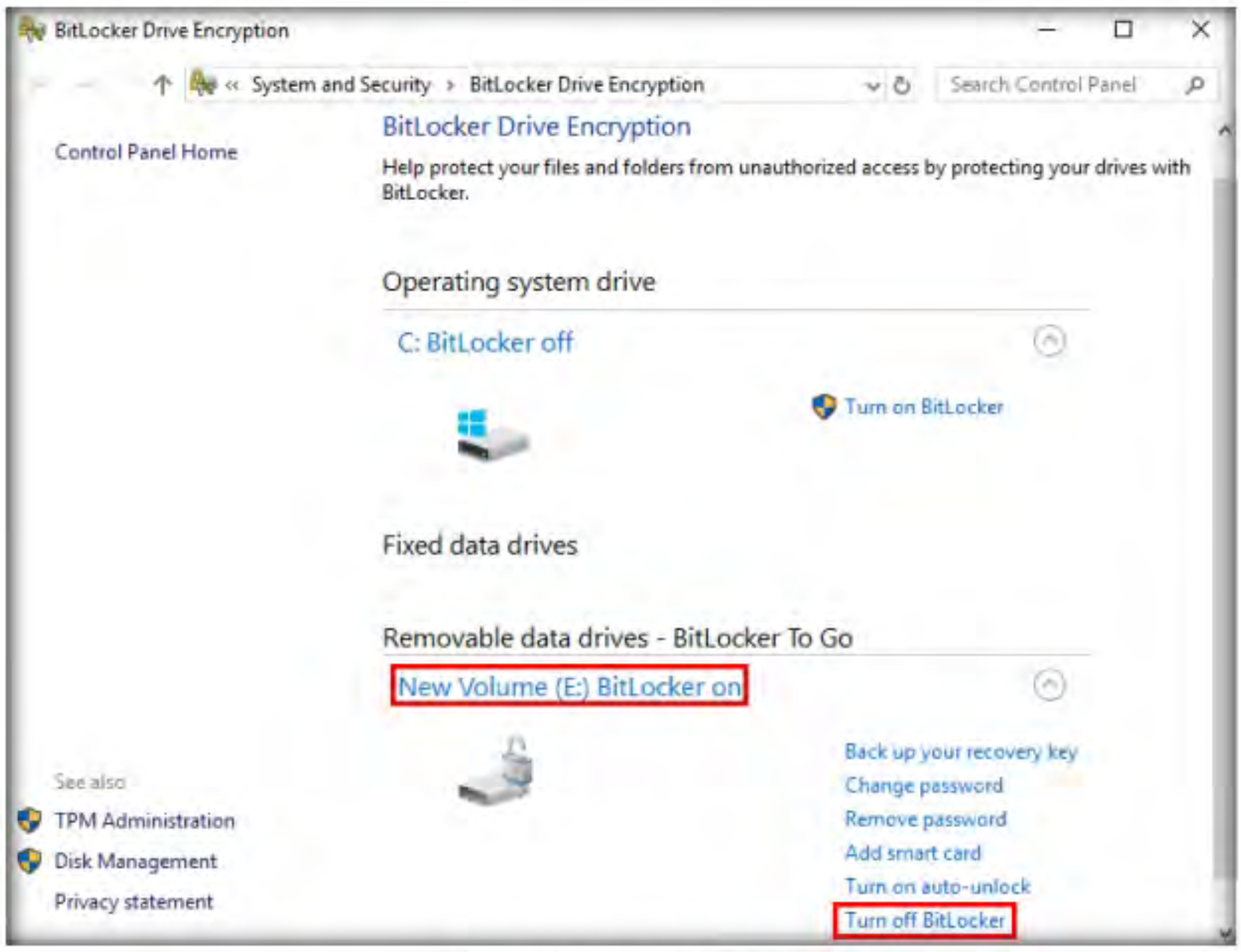


Figure 4.2.15: Turn off BitLocker

23. The **BitLocker Drive Encryption** pop-up appears; click **Turn off BitLocker**.

Figure 4.2.16: BitLocker Drive Encryption pop-up

24. **BitLocker** initiates the decryption process. Wait for it to complete.

Figure 4.2.17: BitLocker Decrypting drive

25. After the completion of decryption process, the **Decryption of E: is complete** pop-up appears; click **Close**.

Figure 4.2.18: Decryption of E: is complete pop-up

26. The **New Volume (E:)** decrypts successfully.
27. Close all open windows and document all the acquired information.

TASK 3 Perform Disk Encryption using Rohos Disk Encryption

Here, we will use the Rohos Disk Encryption tool to perform disk encryption.

TASK 3.1 Install and Launch Rohos Disk Encryption

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\Rohos Disk Encryption** and double-click **rohos.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

2. The **Select Setup Language** dialog box appears; click **OK**.

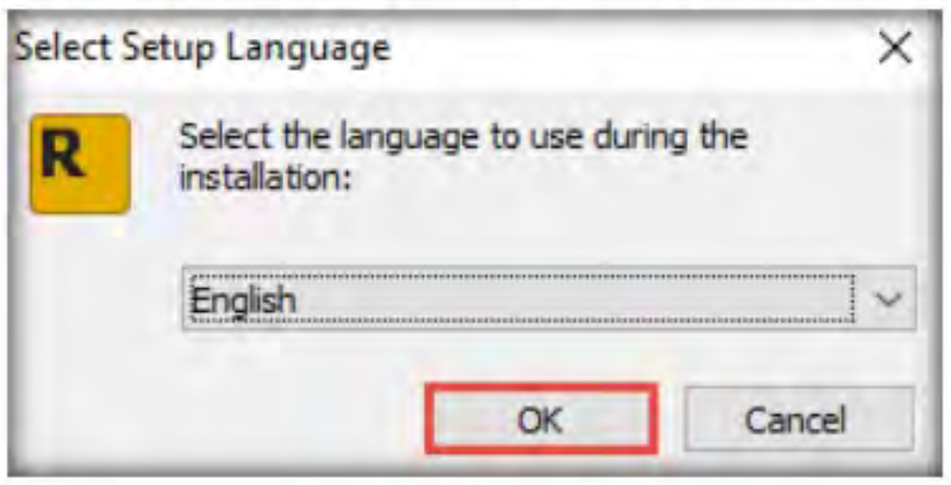


Figure 4.3.1: Select the Language

Rohos Disk Encryption creates hidden and password-protected partitions on a computer or USB flash drive, and password protects/locks access to your Internet applications. It uses a NIST-approved AES encryption algorithm with a 256-bit encryption key length. Encryption is automatic and on-the-fly.

3. The **Setup - Rohos Disk Encryption** window appears; read the instruction and click **Next**.

Figure 4.3.2: Rohos setup wizard

4. Follow the steps and install the application using all default settings.
5. After the completion of the installation, **Completing the Rohos Disk Encryption Setup Wizard** appears; ensure that the **Launch Rohos Disk** checkbox is checked and click **Finish**.

Figure 4.3.3: License agreement window

TASK 3.2

Create an Encrypted Disk for Local Machine

6. The **Rohos Disk Encryption** main window appears; click **Create new disk...**

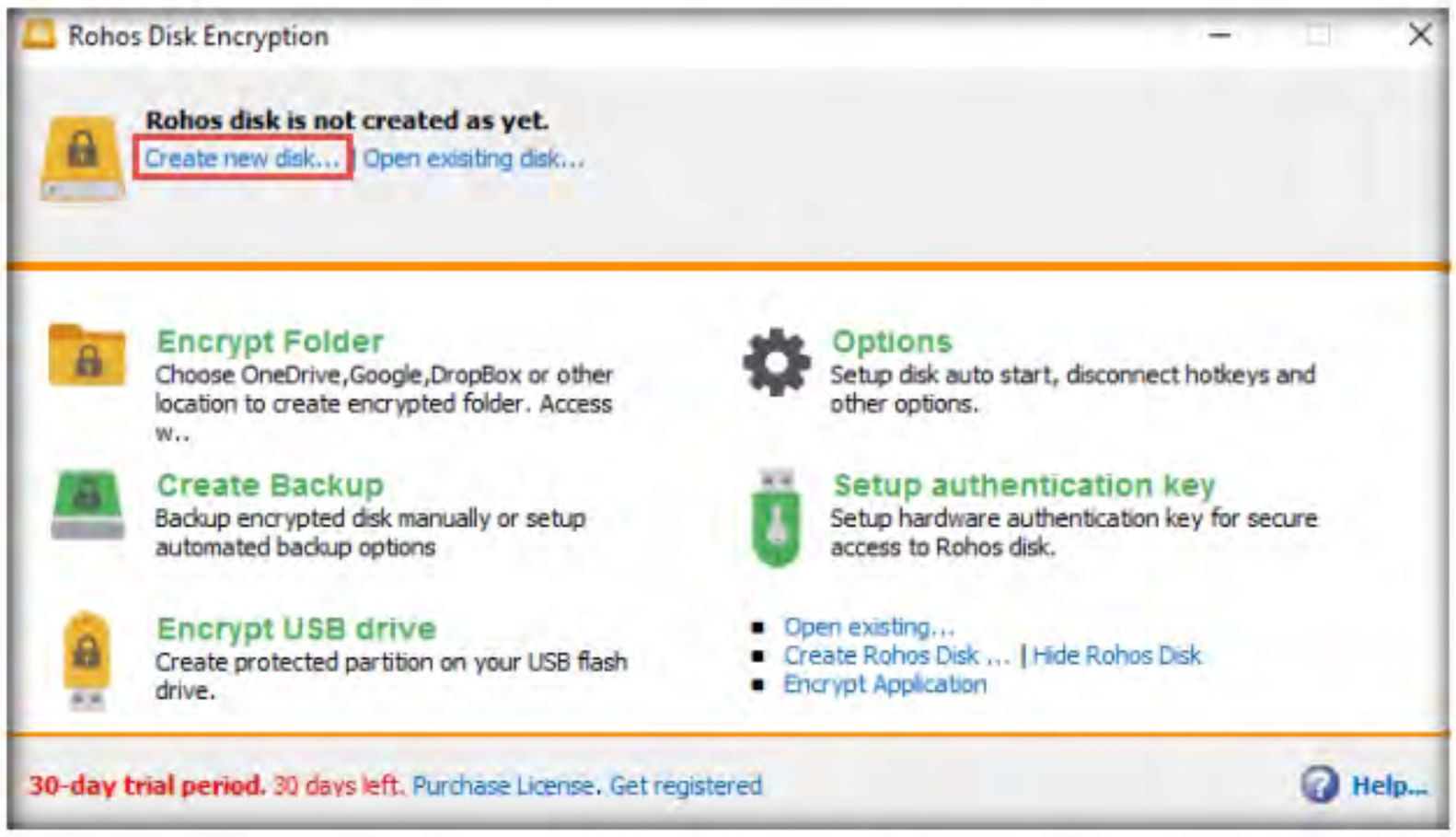


Figure 4.3.4: Create new disk

7. The **Create new Rohos disk** window appears; click **Change...** to modify the size of the encrypted disk.

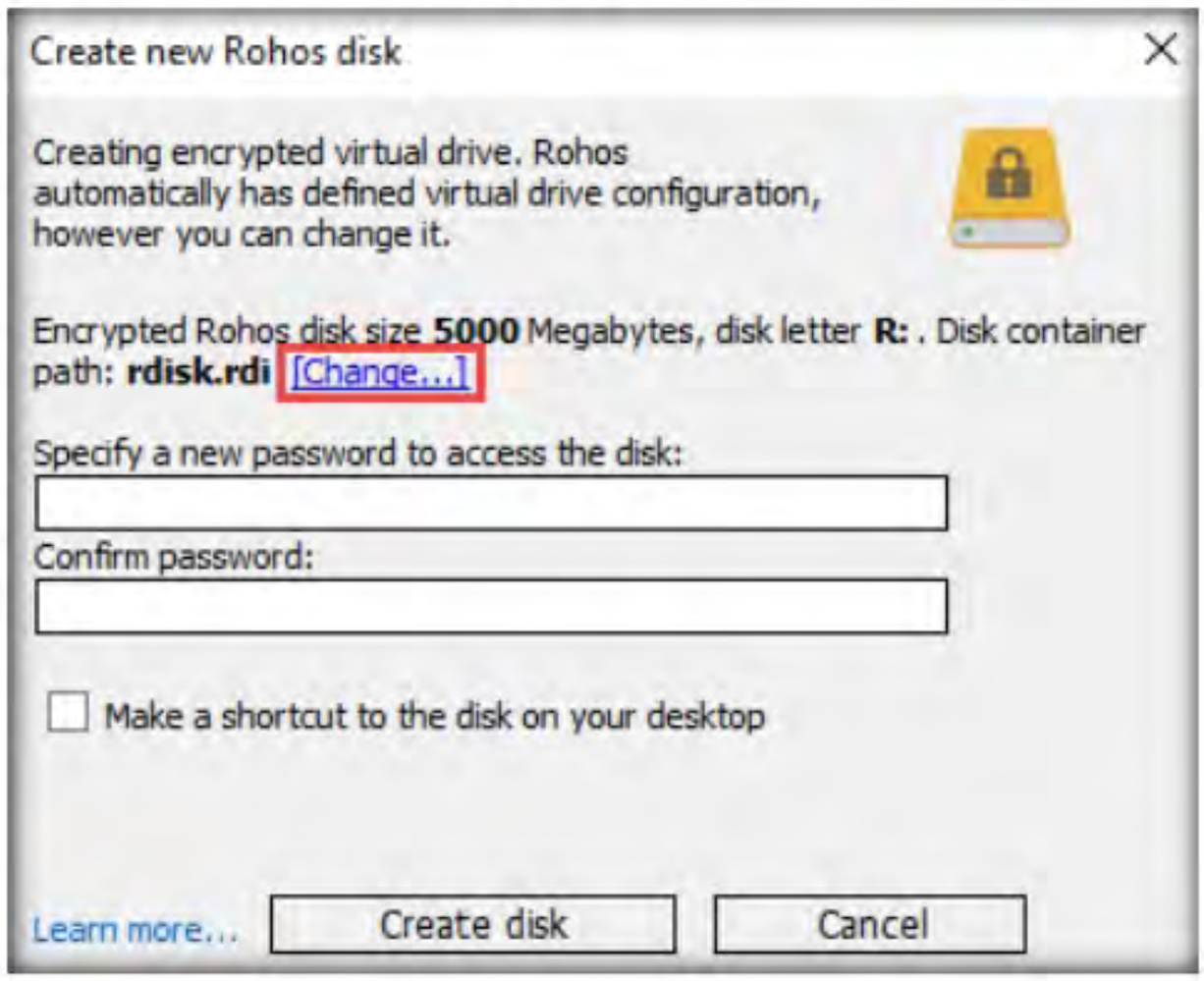


Figure 4.3.5: Create new Rohos disk window

8. The **Disk details** wizard appears; modify the disk size to **10** in the **Disk Size (in Megabytes)** field and leave all other settings to default; then, click **OK**.

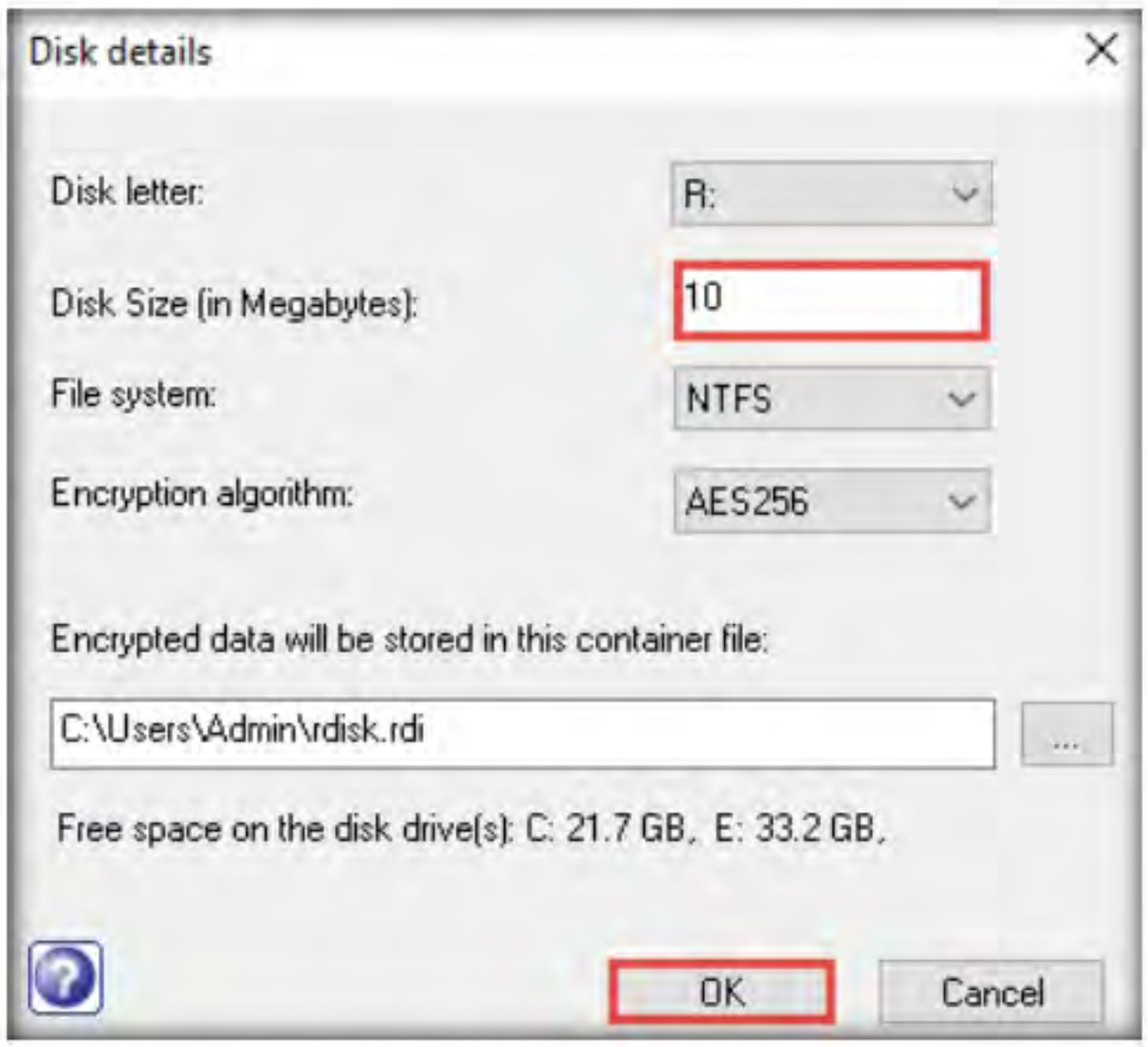


Figure 4.3.6: Disk details window

9. Provide a password in the **Specify a new password to access the disk** field and retype it into the **Confirm password** field; then, click **Create disk** button (Here, the password provided is **test@123**).

Figure 4.3.7: Specify password

10. Wait until the encrypted volume is created. The time to create the encrypted volume depends upon the size you specified under the **Disk Size** option: if large, it will take a long time to create the volume.
11. On creating the encrypted volume, the **Encrypted Disk (R:)** window appears, displaying the default disk content, as shown in the screenshot.

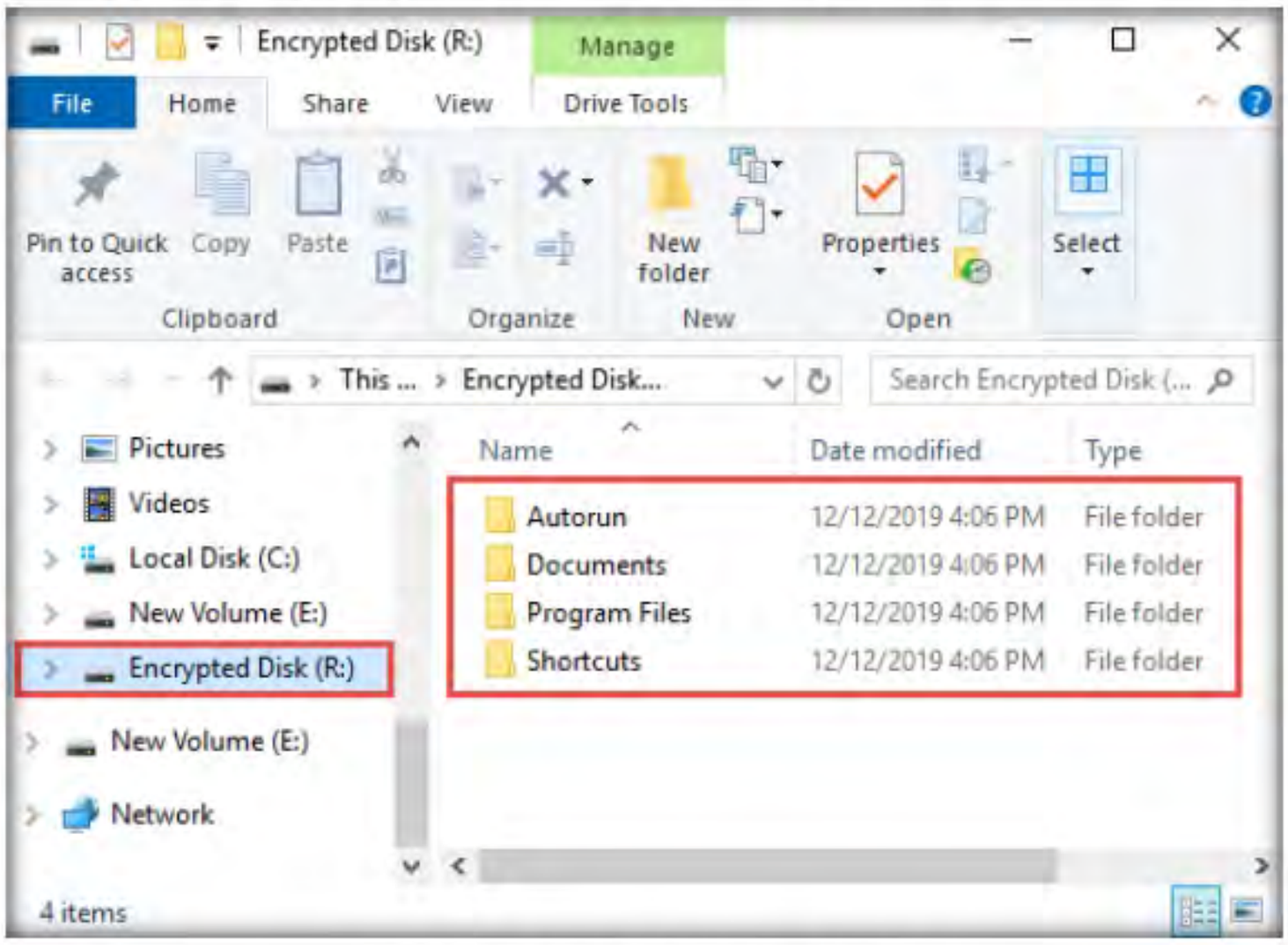


Figure 4.3.8: Encrypted disk successfully created

12. The **Disk is connected** notification appears at the top section of the **Rohos Disk Encryption** window.

Note: This drive appears only when you are connected to Rohos Disk Encryption, and disappears when you exit.

Figure 4.3.9: Disk is connected notification

TASK 3.3

Create a File and Save it in Encrypted Disk

13. If you wish to conceal any important files/directories from anyone accessing your system, you can place them in this drive and access them whenever required (by launching Rohos and entering the password).
14. Now, we shall place a text file in **Encrypted disk (R:)**. To do so, create a text file on **Desktop** and name it **Test**. Open the file and insert text.
15. Click **File** in the menu bar and click **Save**.

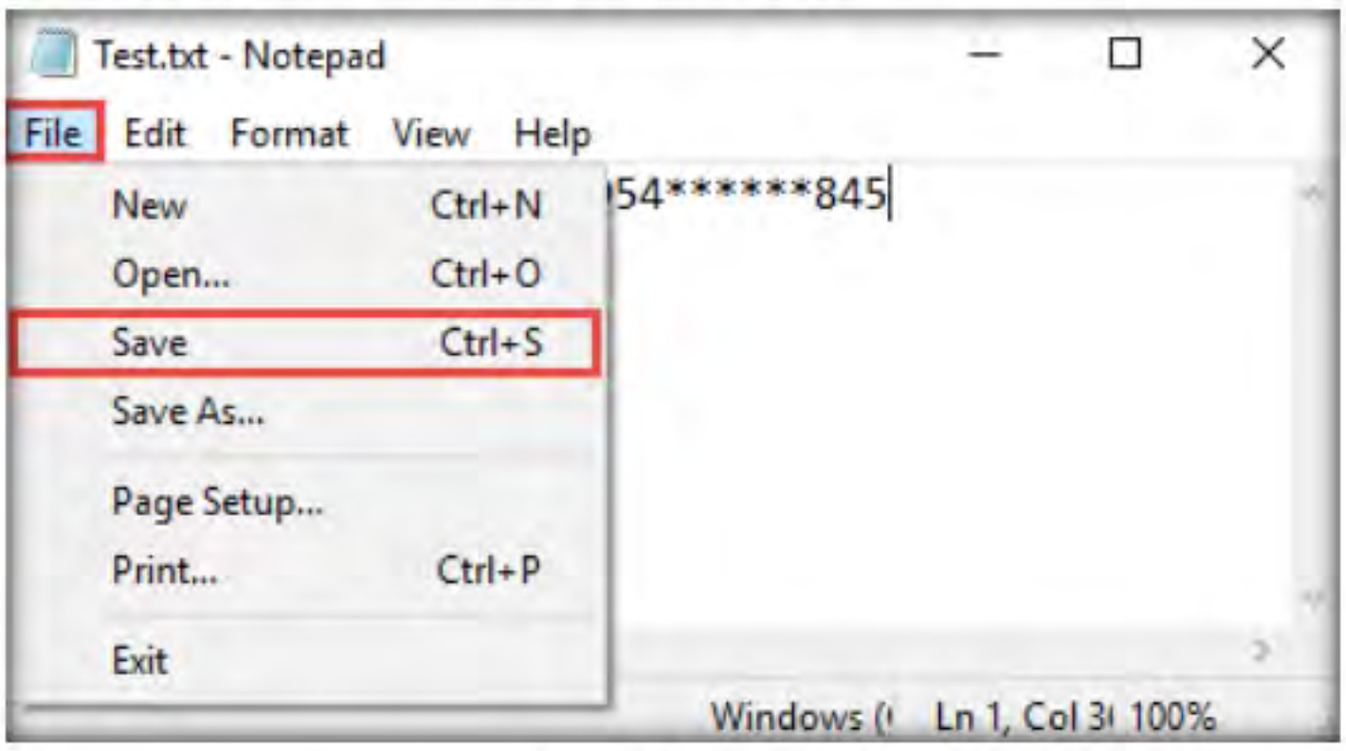


Figure 4.3.10: Text file

16. Copy the file from **Desktop** and paste into **Encrypted Disk (R:)**. Close the window.

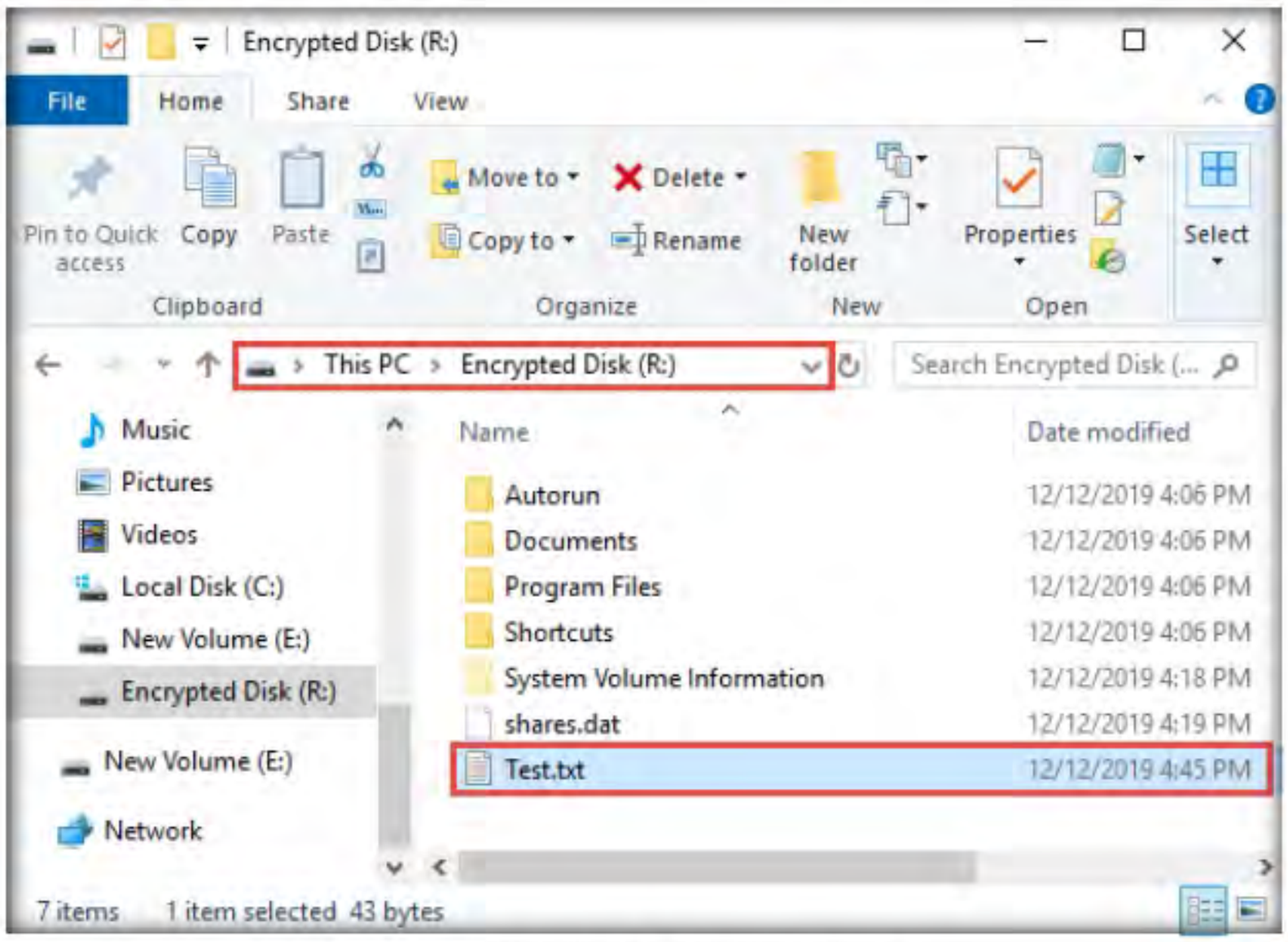


Figure 4.3.11: Test.txt file in Encrypted Container

17. Switch to the **Rohos Disk Encryption** window and click **Disconnect** to dismount **Encrypted disk (R:)**.

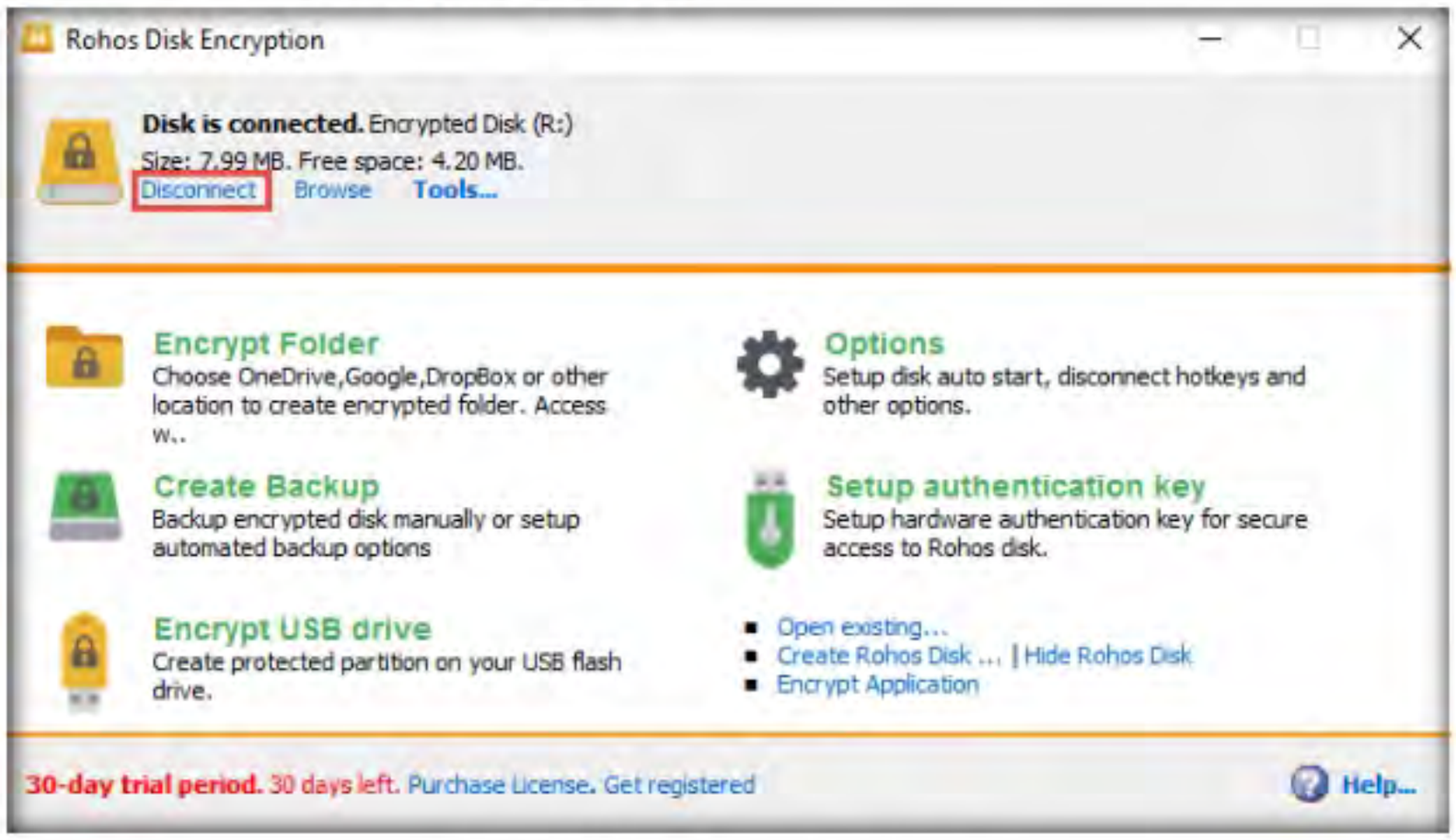


Figure 4.3.12: Click Disconnect to dismount

18. A notification appears stating **Primary Rohos disk is not connected** at the top of the **Rohos Disk Encryption** window. To mount the disk again, click the **Connect disk** option.

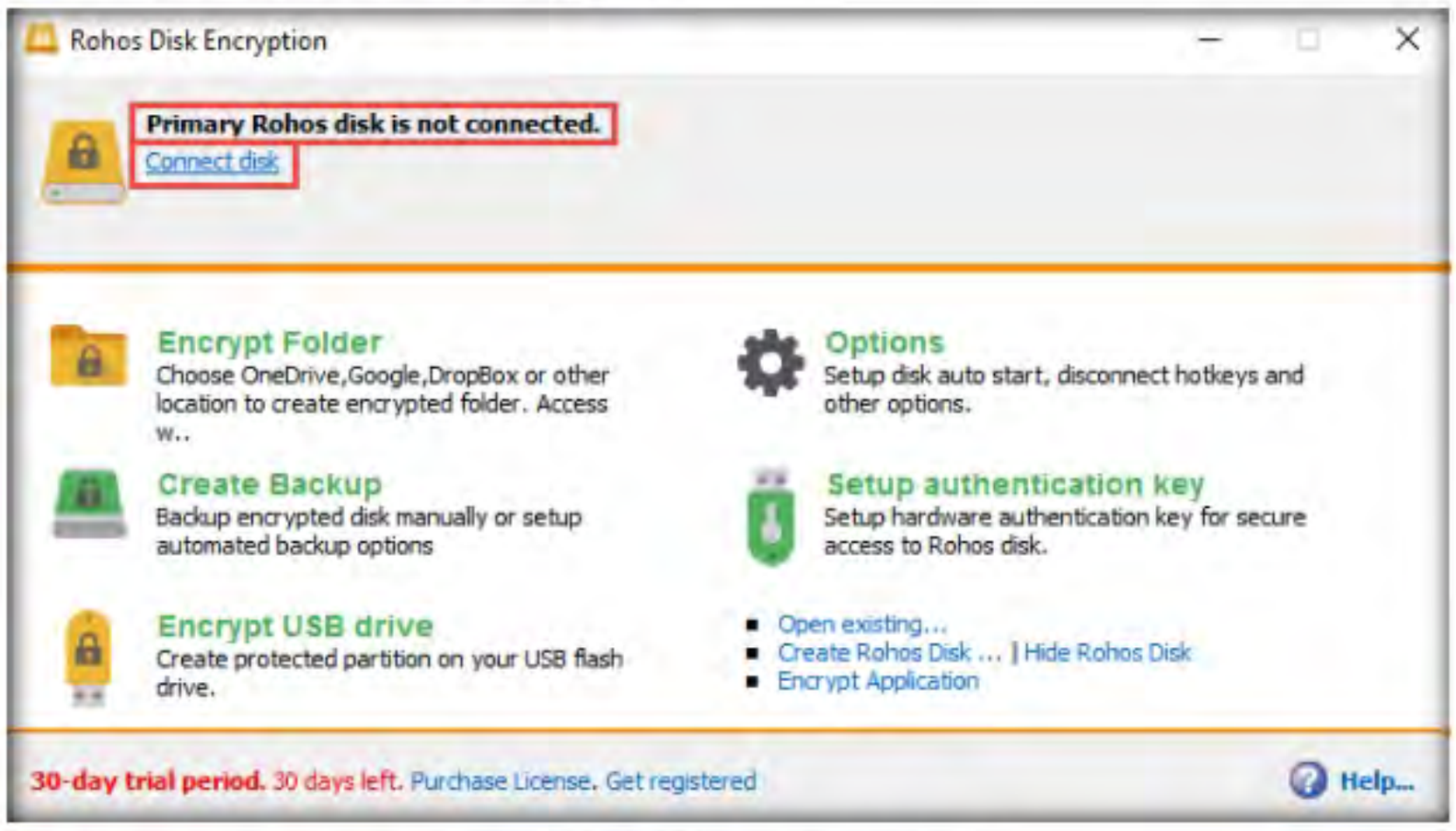


Figure 4.3.13: Click Connect to mount the disk

TASK 3.4

Access Files in the Encrypted Disk

19. The **Rohos** pop-up appears; type the password you provided in **Step#9** into the **Enter password to access Rohos disk** field and click **OK**.

Note: Here, the password is **test@123**.

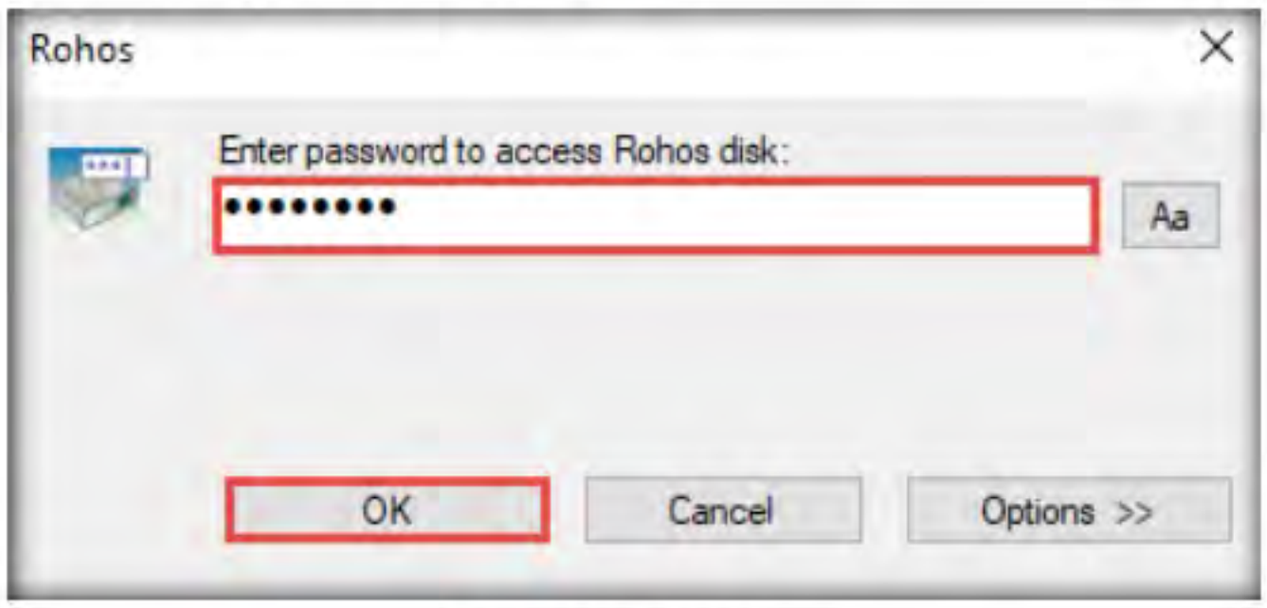


Figure 4.3.14: Rohos pop-up

20. The **Disk is connected** notification appears in the **Rohos Disk Encryption** window. Click **Browse** to explore the disk content.

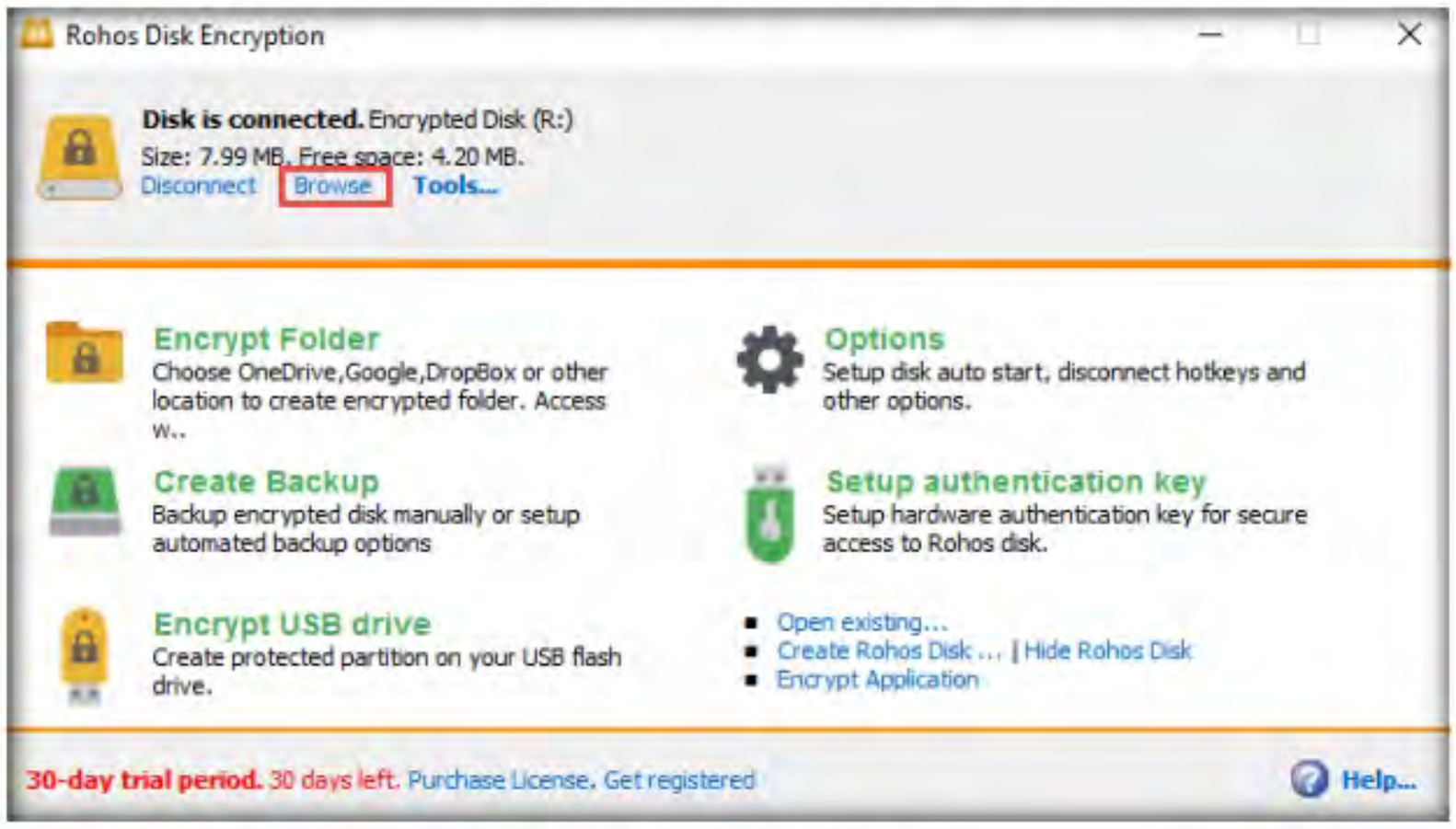


Figure 4.3.15: Disk is connected

21. The **Encrypted Disk (R:)** window appears; you can see the **Test.txt** file that was pasted onto the disk earlier, as shown in the screenshot.

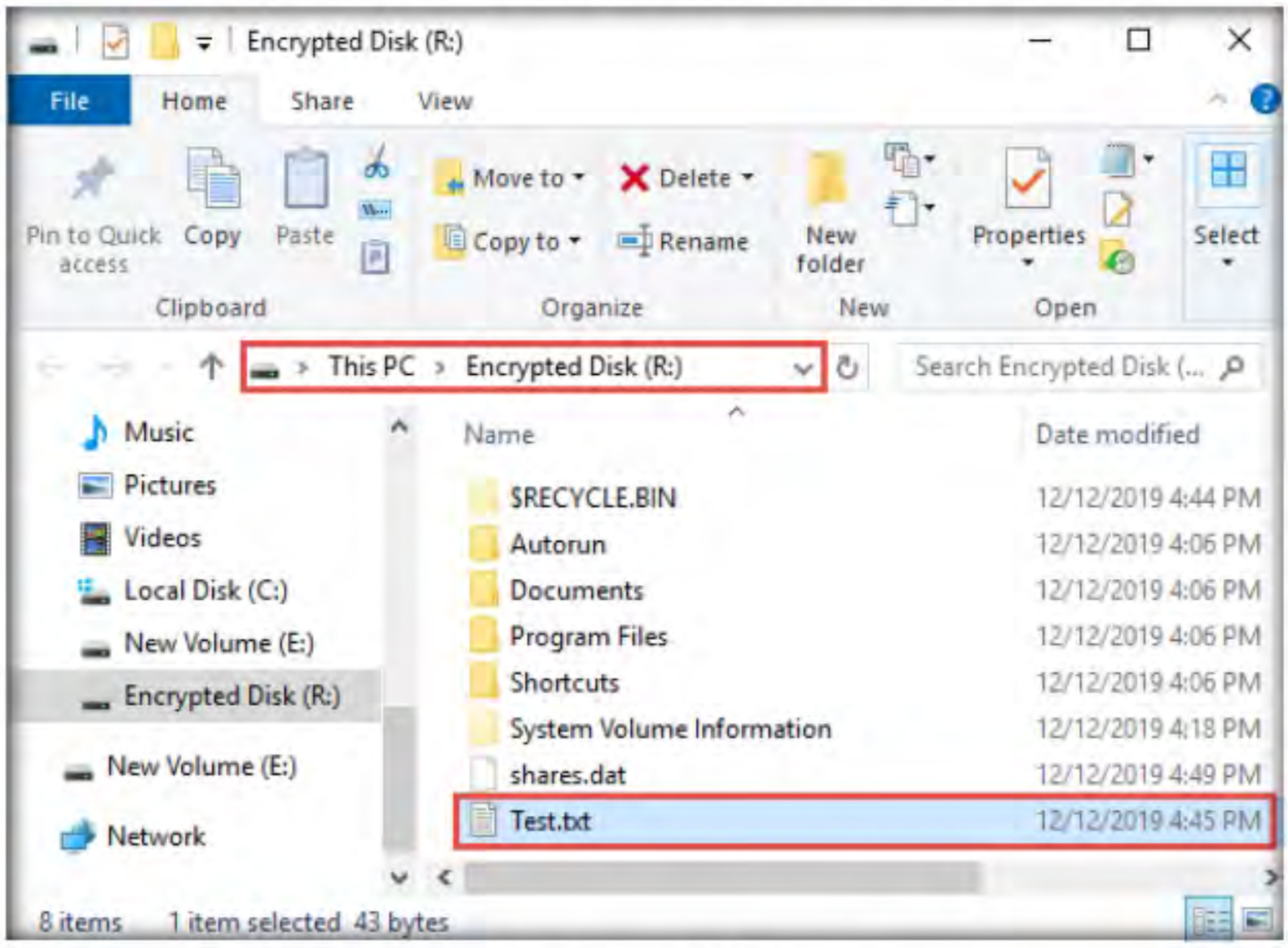


Figure 4.3.16: Encrypted disk (R:) content

22. You can access the disk content and further add, delete, and modify the files. After making the intended changes, click **Disconnect** again in the **Rohos Disk Encryption** window to dismount the disk.

You can also use other disk encryption tools such as **FinalCrypt** (http://www.finalcrypt.org), **Seqrite Encryption Manager** (https://www.seqrite.com), **FileVault** (https://support.apple.com), and **Gillsoft Full Disk Encryption** (http://www.gilisoft.com) to perform disk encryption.

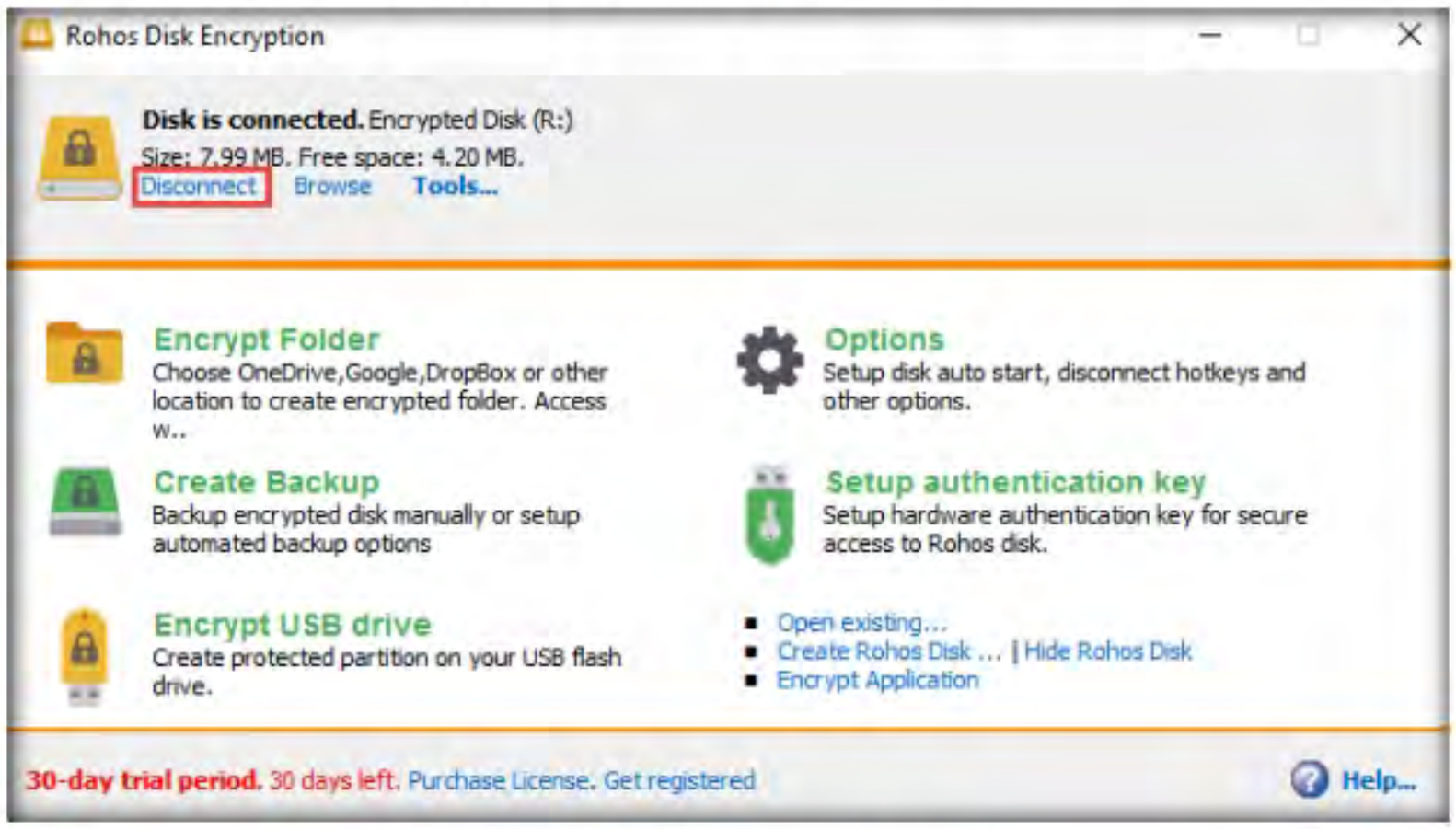


Figure 4.3.17: Disconnect to dismount

Note: You can also use the Encrypt USB drive option to share sensible information with someone via USB. You can use this application to store the files in an encrypted disk and share the password with that person. The person with whom you want to share the files can access them only after entering the correct password. This way, you can protect the files from being viewed by a third person and thereby safeguard them.

23. This concludes the demonstration of performing disk encryption using Rohos Disk Encryption.
24. Close all open windows and document all the acquired information
25. Turn off **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

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

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

Lab 5

Perform Cryptanalysis using Various Cryptanalysis Tools

Cryptanalysis is the study of ciphers, cipher text, or cryptosystems with the ability to identify vulnerabilities that allows extraction of plaintext from the ciphertext, even if the cryptographic key or algorithm used to encrypt the plaintext is unknown.

Lab Scenario

ICON KEY

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

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

Attackers tend to focus on easy to compromise targets. Therefore, in order to attain maximum network security, strong encryption is needed for all the traffic placed onto the transmission media, no matter the type and location: if an attacker wishes to break into an encrypted network, he/she faces decrypting a whole slew of encrypted packets, which is a difficult task. Therefore, the attacker is likely to try and find another target that is easy to compromise or will simply abort the attempt. Using the latest encryption algorithms provides a strong layer of security to an organization.

As a professional ethical hacker or pen tester, you should possess the required knowledge to investigate the security of cryptographic systems. In order to confirm the security of the cryptographic systems, you must implement various cryptography attacks to evade the system's security by exploiting vulnerabilities in codes, ciphers, cryptographic protocols, or key management schemes.

In this lab, you will learn how to compromise cryptographic systems using various cryptanalysis techniques and tools that help in breaching cryptographic security.

Lab Objectives

- Perform cryptanalysis using CrypTool
- Perform cryptanalysis using AlphaPeeler

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

- Windows Server 2019 virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection
- CrypTool located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**
- AlphaPeeler located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**
- You can also download the latest version of the above-mentioned tools from their official website. If you decide to download the latest versions, the screenshots shown in the lab might differ.

Lab Duration

Time: 25 Minutes

Overview of Cryptanalysis

Cryptanalysis can be performed using various methods, including the following:

- **Linear Cryptanalysis**: A known plaintext attack that uses a linear approximation to describe the behavior of the block cipher
- **Differential Cryptanalysis**: The examination of differences in an input and how this affects the resultant difference in the output
- **Integral Cryptanalysis**: This attack is useful against block ciphers based on substitution-permutation networks and is an extension of differential cryptanalysis

Lab Tasks

TASK 1

Perform Cryptanalysis using CrypTool

Here, we will use the CrypTool tool to perform cryptanalysis.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Install and Launch CrypTool

3. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool** and double-click **SetupCrypTool_1_4_41_en.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

CrypTool is a freeware program that enables you to apply and analyze cryptographic mechanisms, and has the typical look and feel of a modern Windows application. CrypTool includes a multitude of state-of-the-art cryptographic functions and allows you to both learn and use cryptography within the same environment. CrypTool is a free, open-source e-learning application used in the implementation and analysis of cryptographic algorithms.

4. The **CrypTool Setup** window appears; then, click **Next**.

Figure 5.1.1: CrypTool Setup window

5. Follow the wizard-driven installation steps to install the application using all default settings.
6. After the completion of the installation, the **Completing CrypTool Setup** wizard appears; uncheck the **Show Readme** checkbox and click **Finish**.

Figure 5.1.2: Completing CrypTool Setup window

7. The **CrypTool** main window appears with a **How to Start** window. Check the **Don't show this dialog again** checkbox and click **Close**.

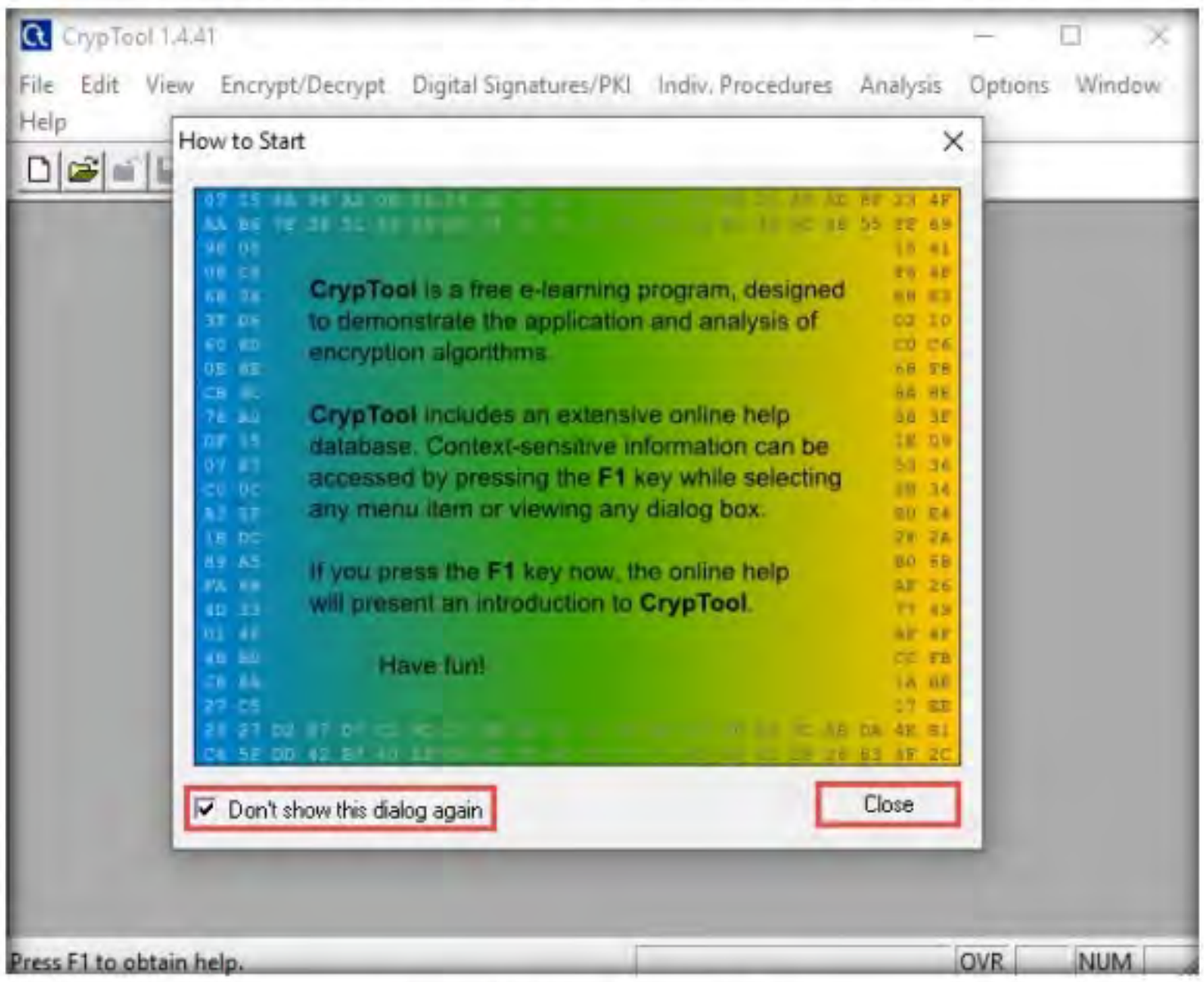


Figure 5.1.3: How to Start Dialog box

8. The **CrypTool** window appears; close the **startingexample-en.txt** window.

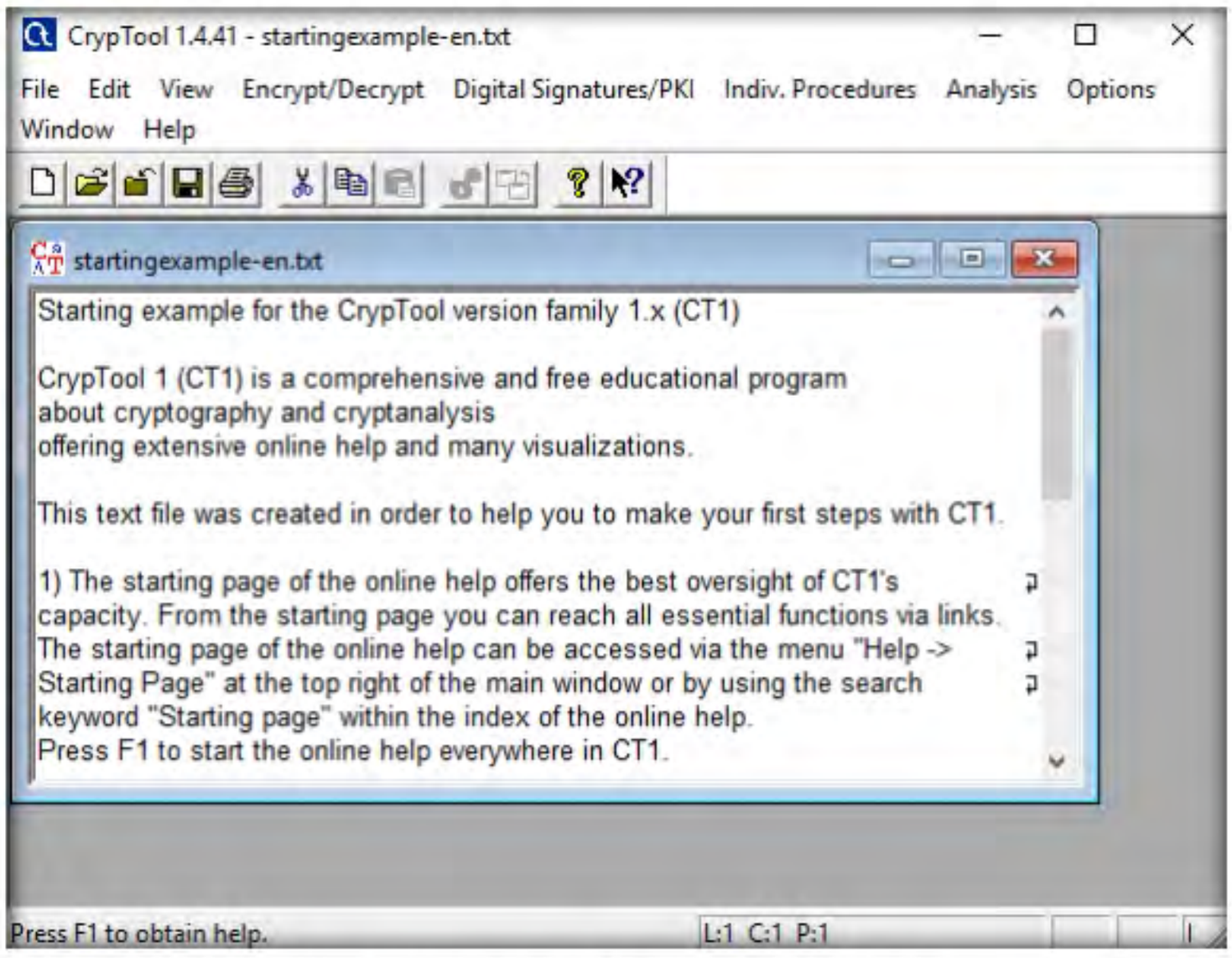


Figure 5.1.4: startingexample-en.txt window in CrypTool

9. Click the **File** option from the menu bar and select **New** to create encrypted data.

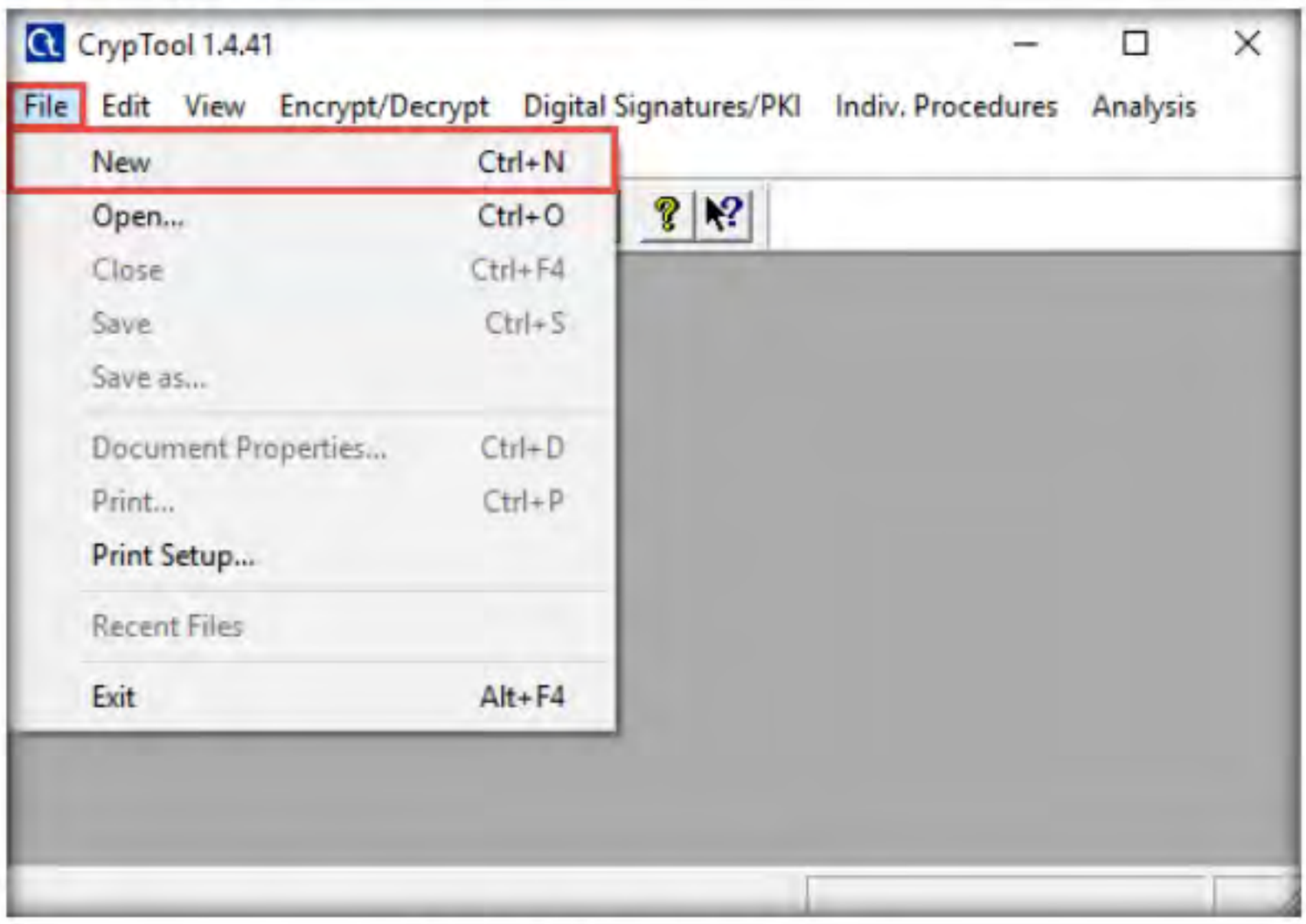


Figure 5.1.5: Choosing a new file to crypt

10. The **Unnamed1** notepad appears; insert some text into the file. You will be encrypting this content.

TASK 1.2

Encrypt the Data using RC2 Encryption

11. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → RC2...**.

Note: RC2 is a symmetric-key block cipher. It is a 64-bit block cipher with variable key size and uses 18 rounds.

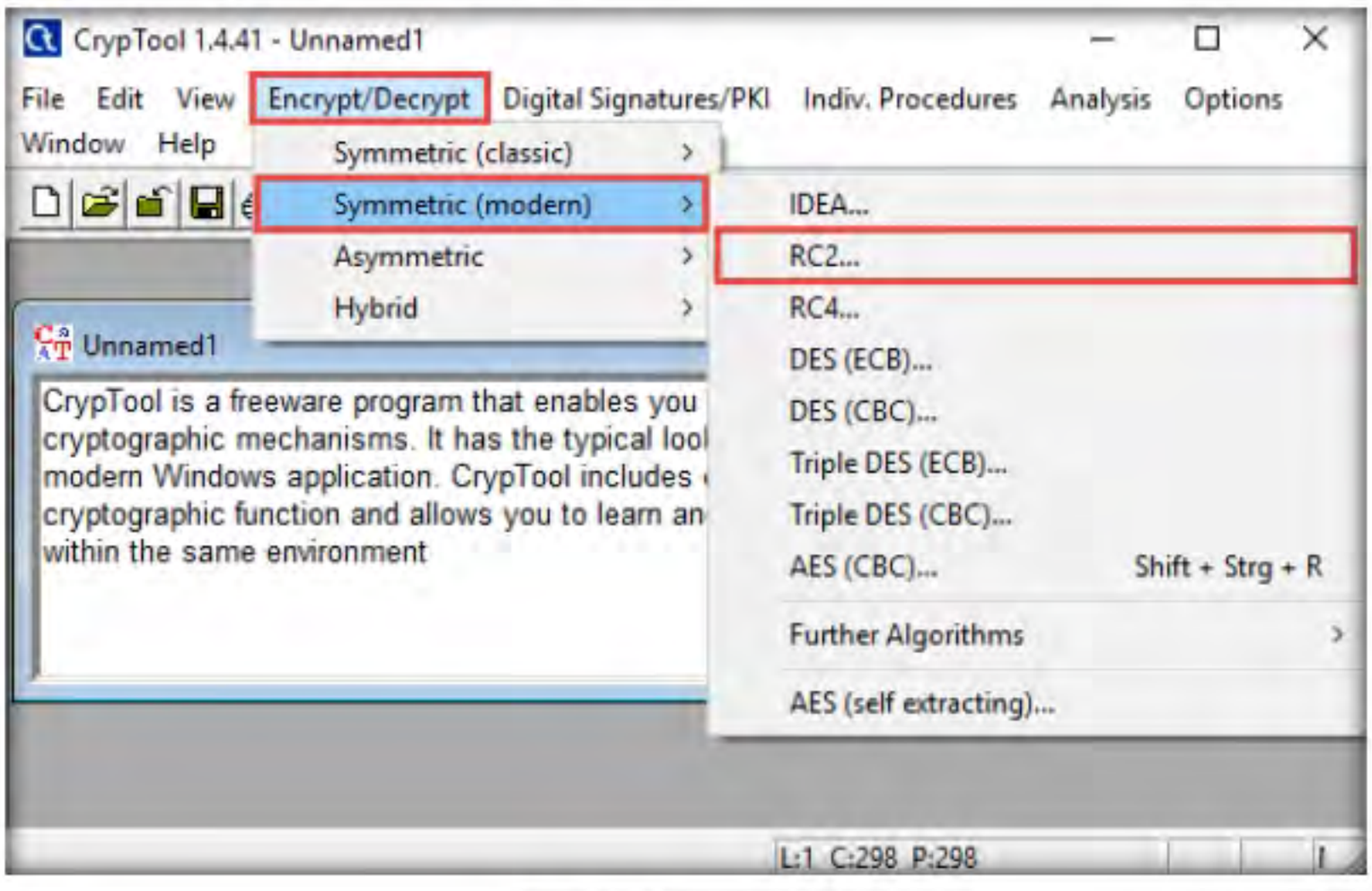


Figure 5.1.6: Encrypting the file

12. The **Key Entry: RC2** dialog box appears; keep the **Key length** set to default (**8 bits**).
13. In the text field below **Key length**, enter **05** as **hexadecimal characters**, and click **Encrypt**.

Note: The chosen hexadecimal character acts as a key that you must send to the intended user along with the encrypted file.

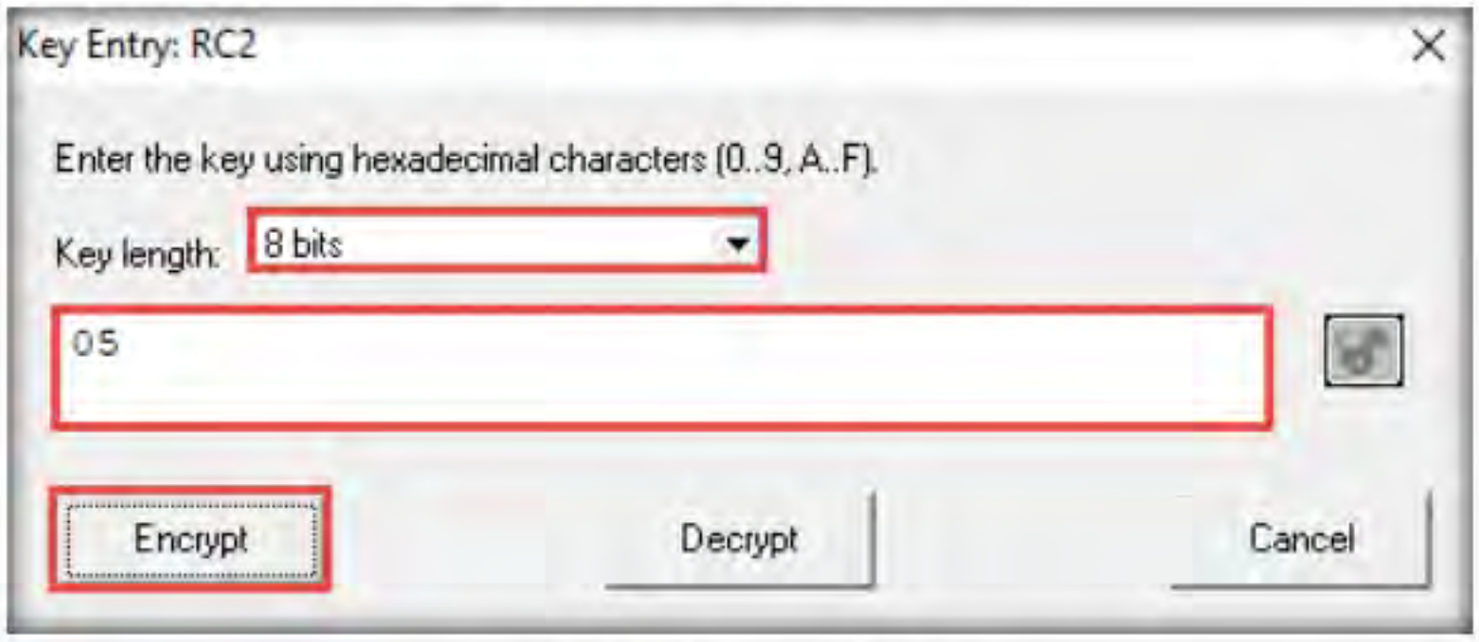


Figure 5.1.7: Encrypting the file

14. The **RC encryption of Unnamed1** notepad file appears, as shown in the screenshot.

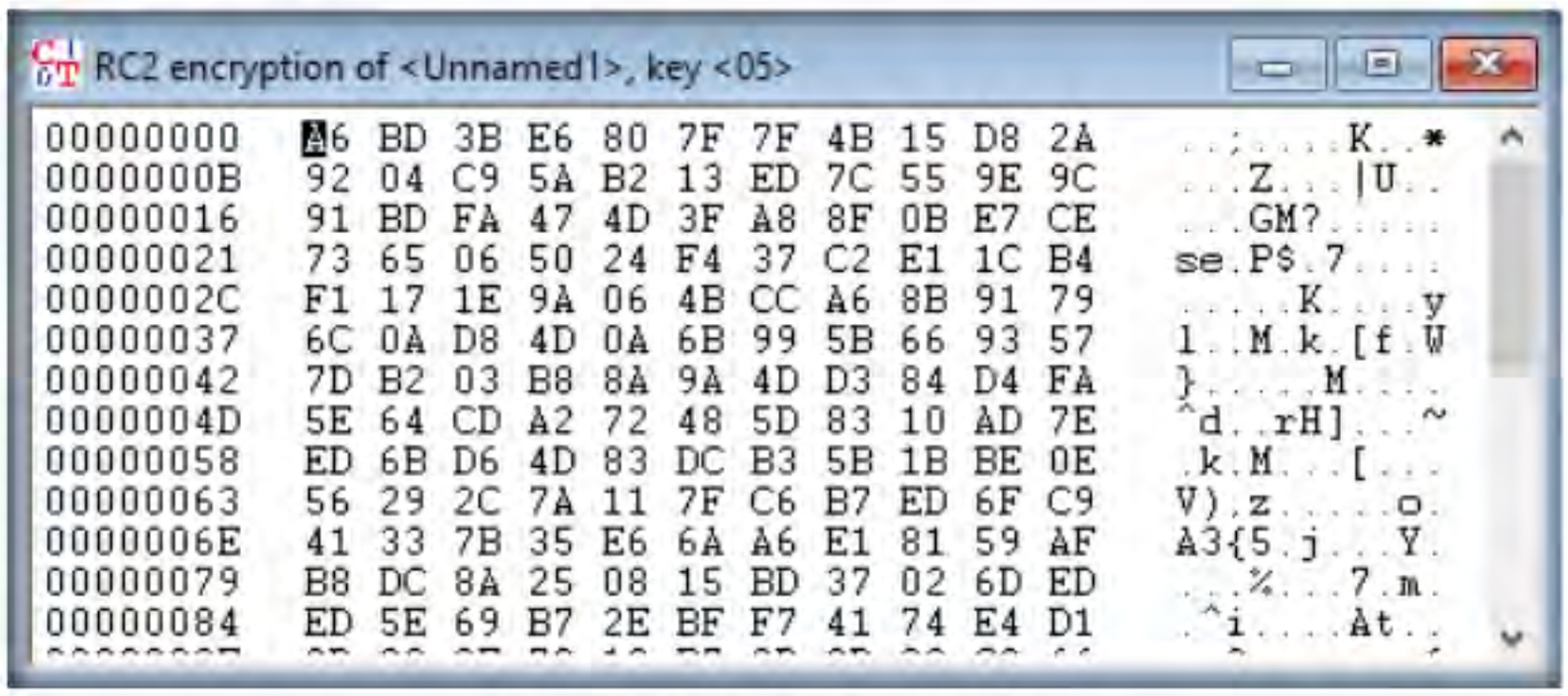


Figure 5.1.8: Output of RC2: encrypted data

15. To save, click **File** in the menu bar and select **Save**.

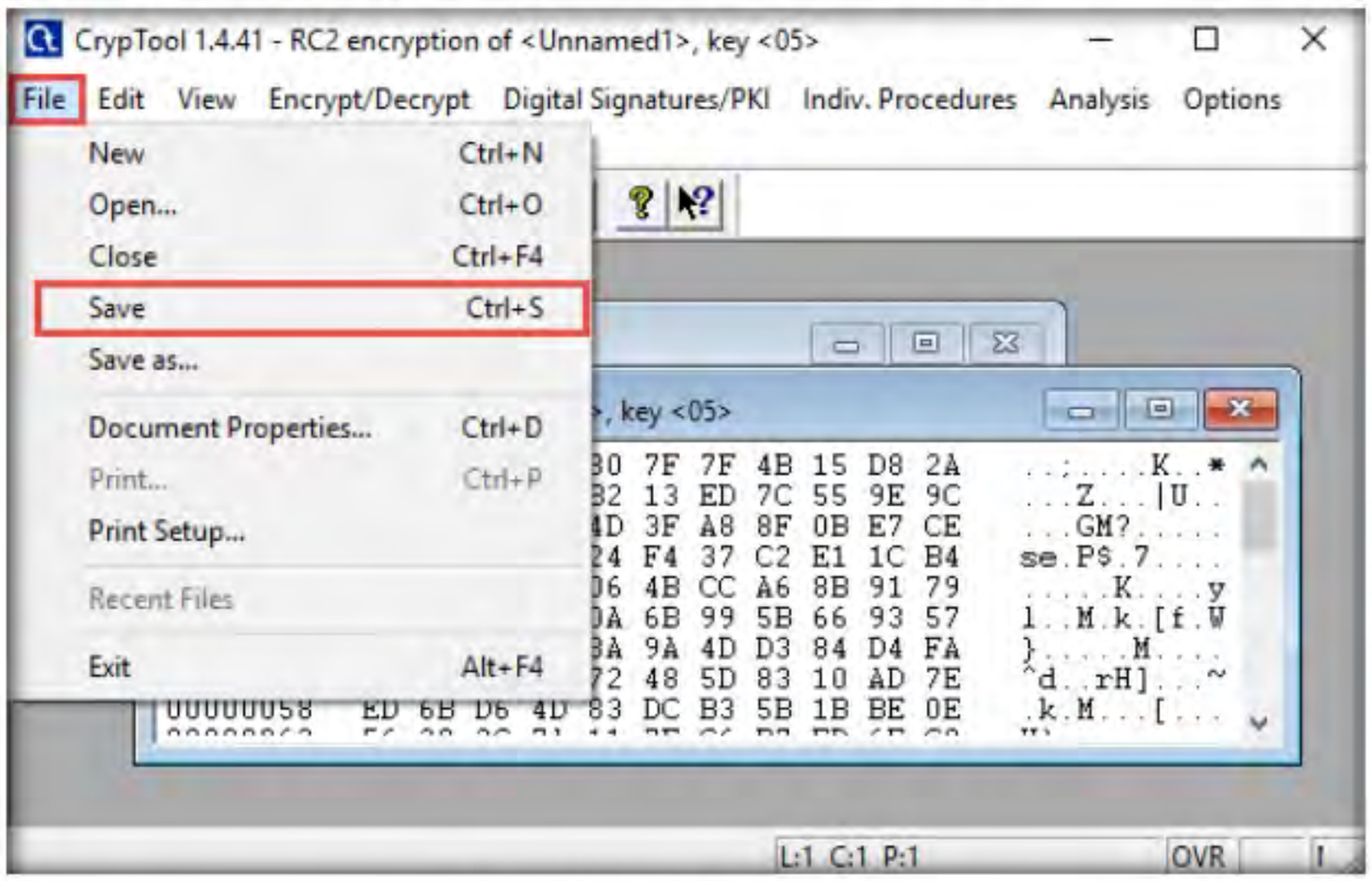


Figure 5.1.9: Saving the encrypted file

16. The **Save As** window appears; choose the save location (here, **Desktop**) and click **Save**.

Note: The file name may differ in your lab environment.

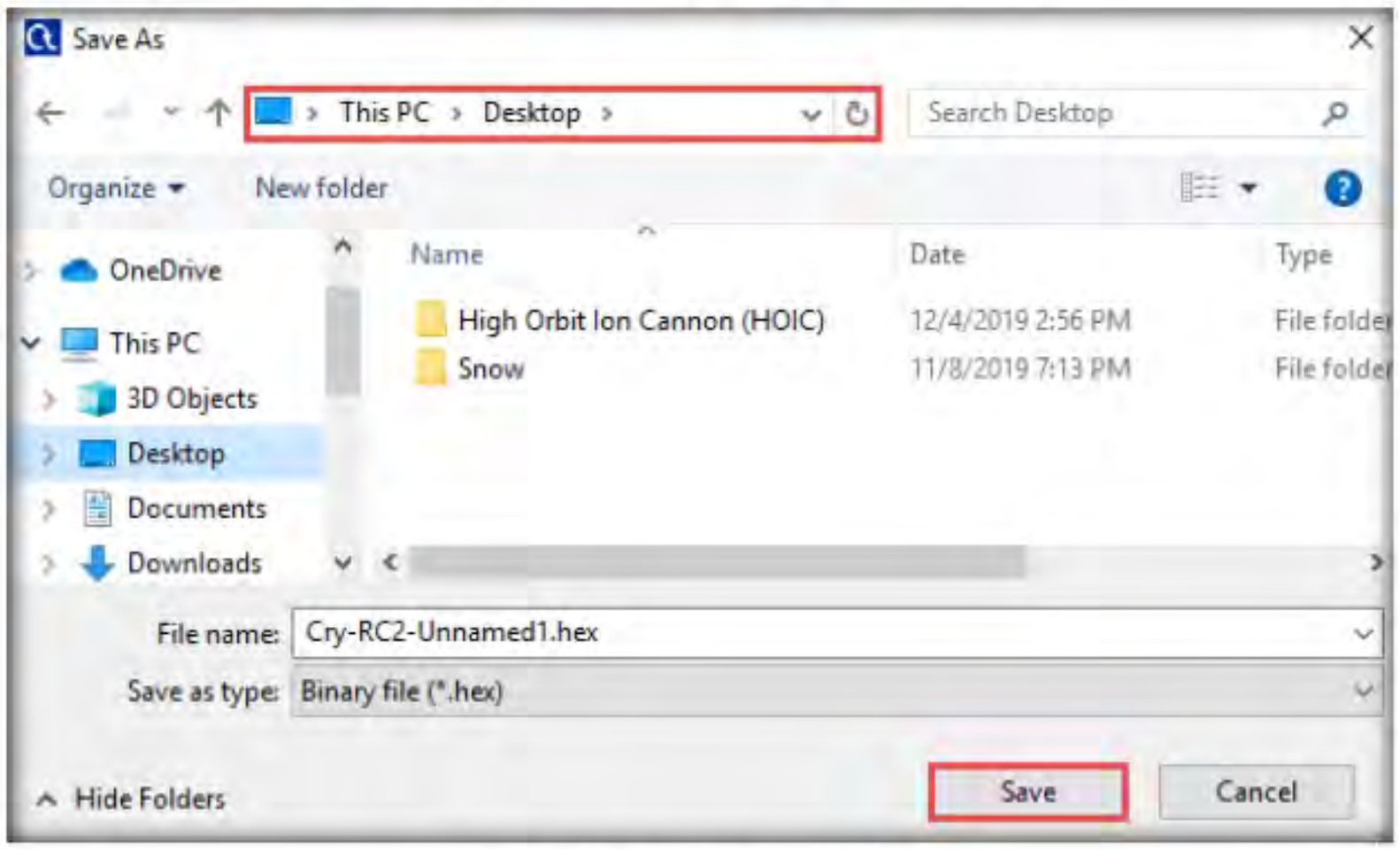


Figure 5.1.10: Saving the encrypted file

17. Now, you can send this file to the intended person by email or any other means and provide him/her with the hex value, which will be used to decrypt the file.

18. To share the file, you may copy the encrypted file (**Cry-RC2-Unnamed1.hex**) from **Desktop** to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**.
19. Assume that you are the intended recipient (working on Windows Server 2019) of the encrypted file through the shared network drive and the key to open the encrypted data was sent to you via an email. Using this, you can decrypt the encrypted data and see the data in plain-text.

TASK 1.3

Decrypt the Data

20. Switch to **Windows Server 2019** and log in with the credentials **Administrator** and **Pa$$w0rd**.
21. Navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**, double-click **SetupCrypTool_1_4_41_en.exe**, and follow the steps to install the application using all default settings.
22. After the installation finishes, launch the **CrypTool** application.

Note: In the **How to Start** dialog-box; check **Don't show this dialog again** and click **Close**.

23. The **CrypTool** main window appears; close the **startingexample-en.txt** window.
24. Now, copy the encrypted hex file (**Cry-RC2-Unnamed1.hex**) from **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool** and paste it on **Desktop**.
25. Switch to the **CrypTool** window; click **File** in the menu bar and select **Open...**

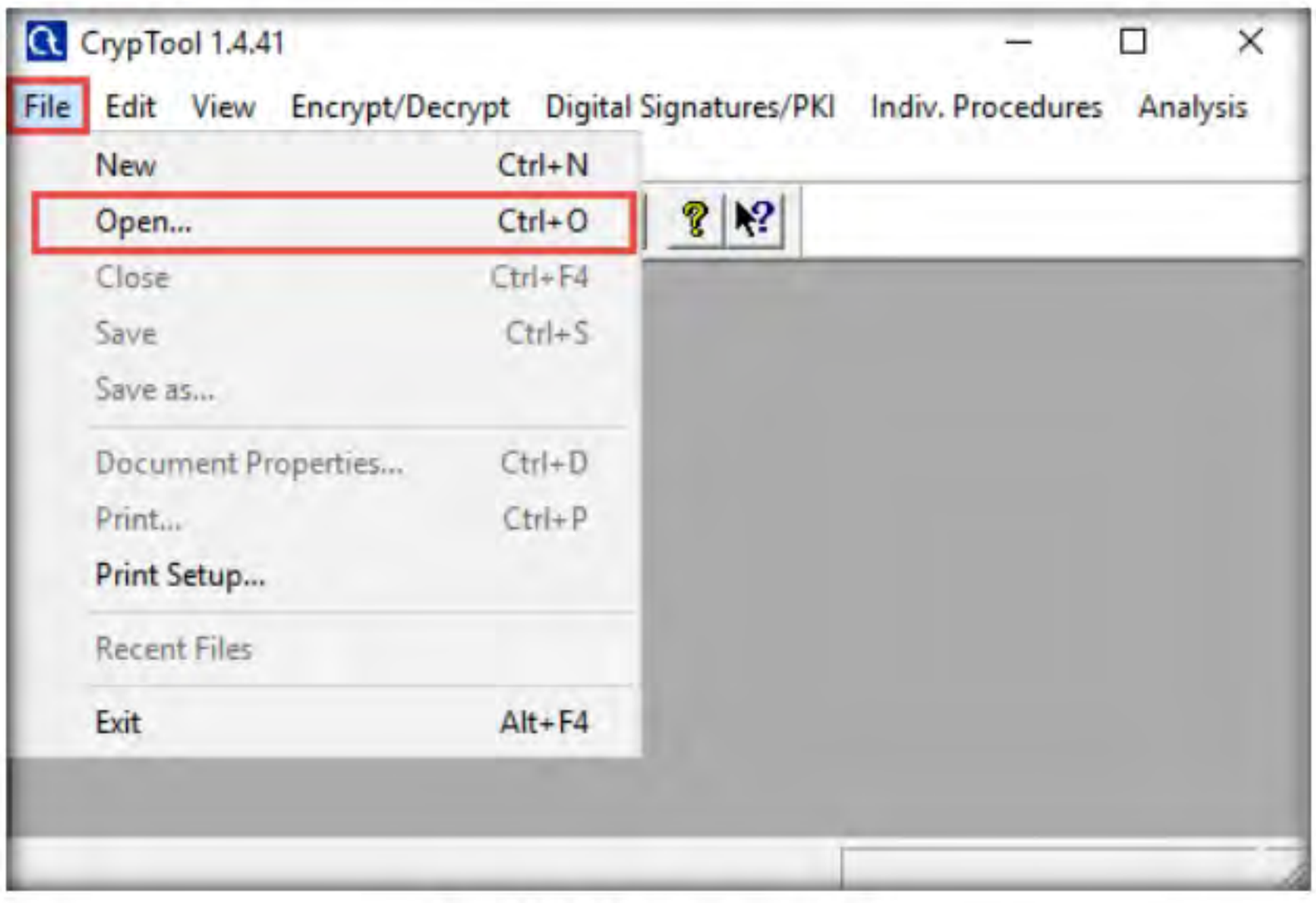


Figure 5.1.11: Opening an encrypted file

26. The **Open** window appears; select **Binary file (*.hex)** from the drop-down list in the file type option, navigate to the location of the file (here, **Desktop**), select, and then click **Open**.

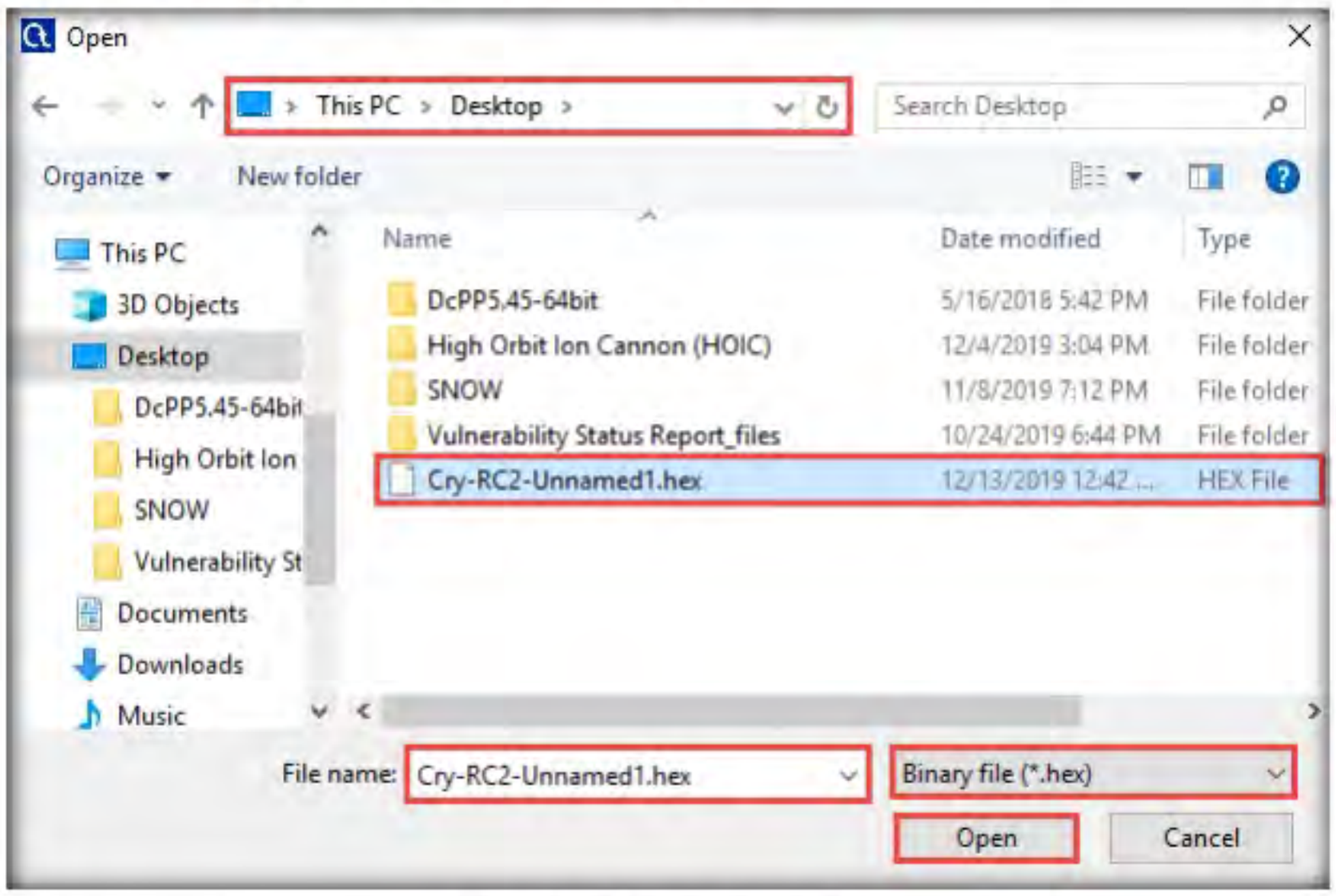


Figure 5.1.12: Opening a Crypted file

27. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → RC2...**

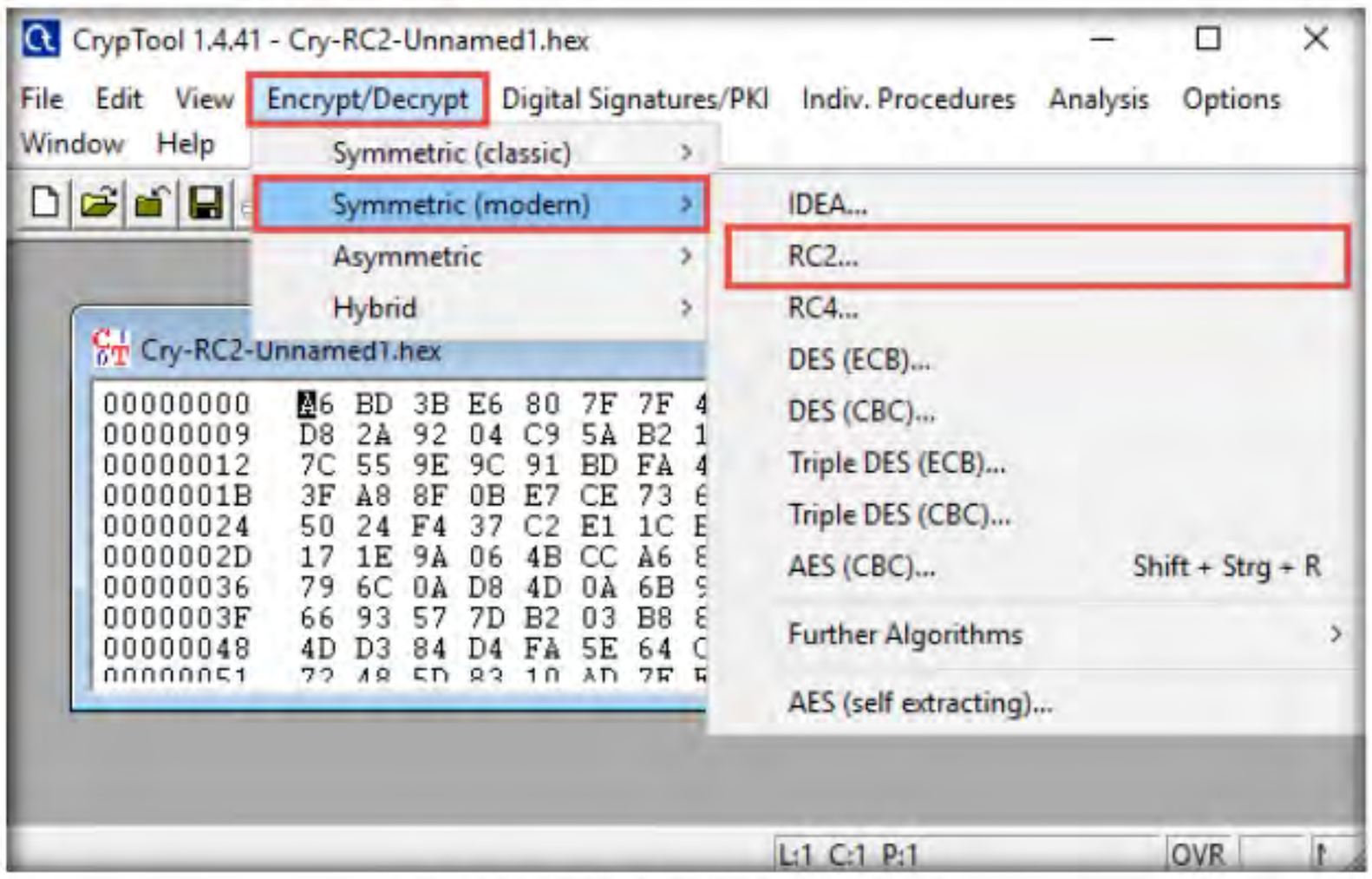


Figure 5.1.13: Select the RC2 Encryption algorithm

28. The **Key Entry: RC2** dialog box appears; leave the **Key length** set to default (**8 bits**).
29. In the text field below **Key length**, enter **05** as **hexadecimal characters**, and click **Decrypt**.

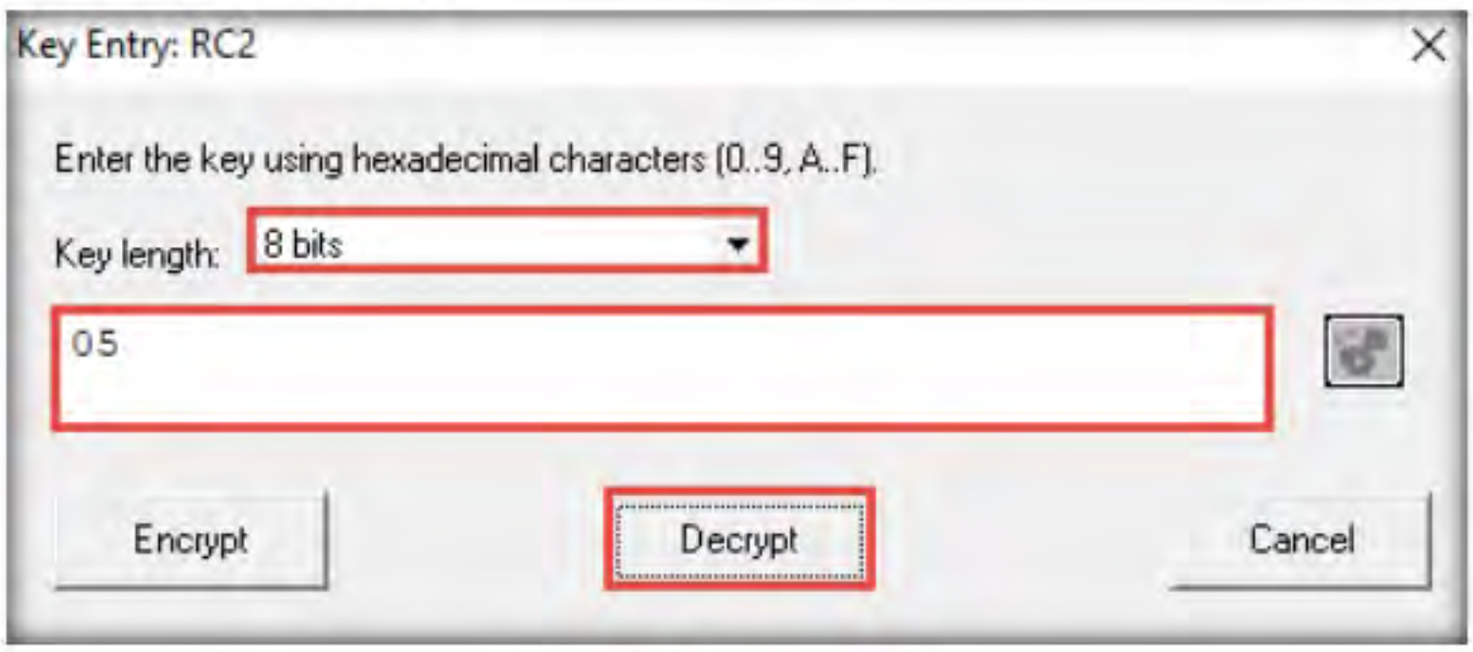


Figure 5.1.14: Decrypting the file

30. The decrypted text appears, as shown in the screenshot:

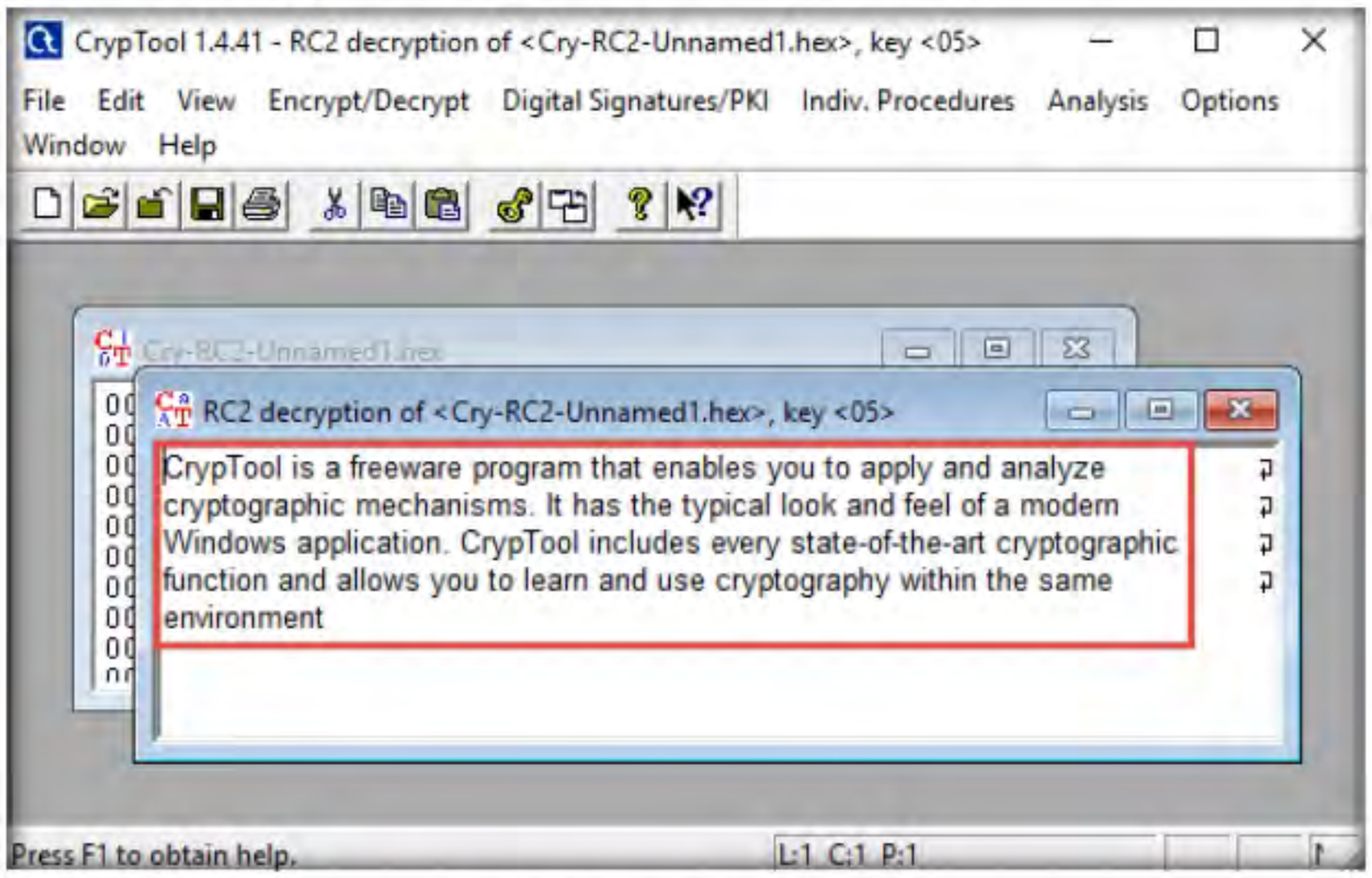


Figure 5.1.15: Decrypted the file successfully

31. Now, we shall encrypt the data using Triple DES encryption.
32. Switch back to the **Windows 10** virtual machine.

TASK 1.4

Encrypt the Data using Triple DES Encryption

33. In the **CrypTool** window, close **Cry-RC2-Unnamed1.hex** window. Leave the **Unnamed1** notepad window open.
34. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → Triple DES (ECB)...**

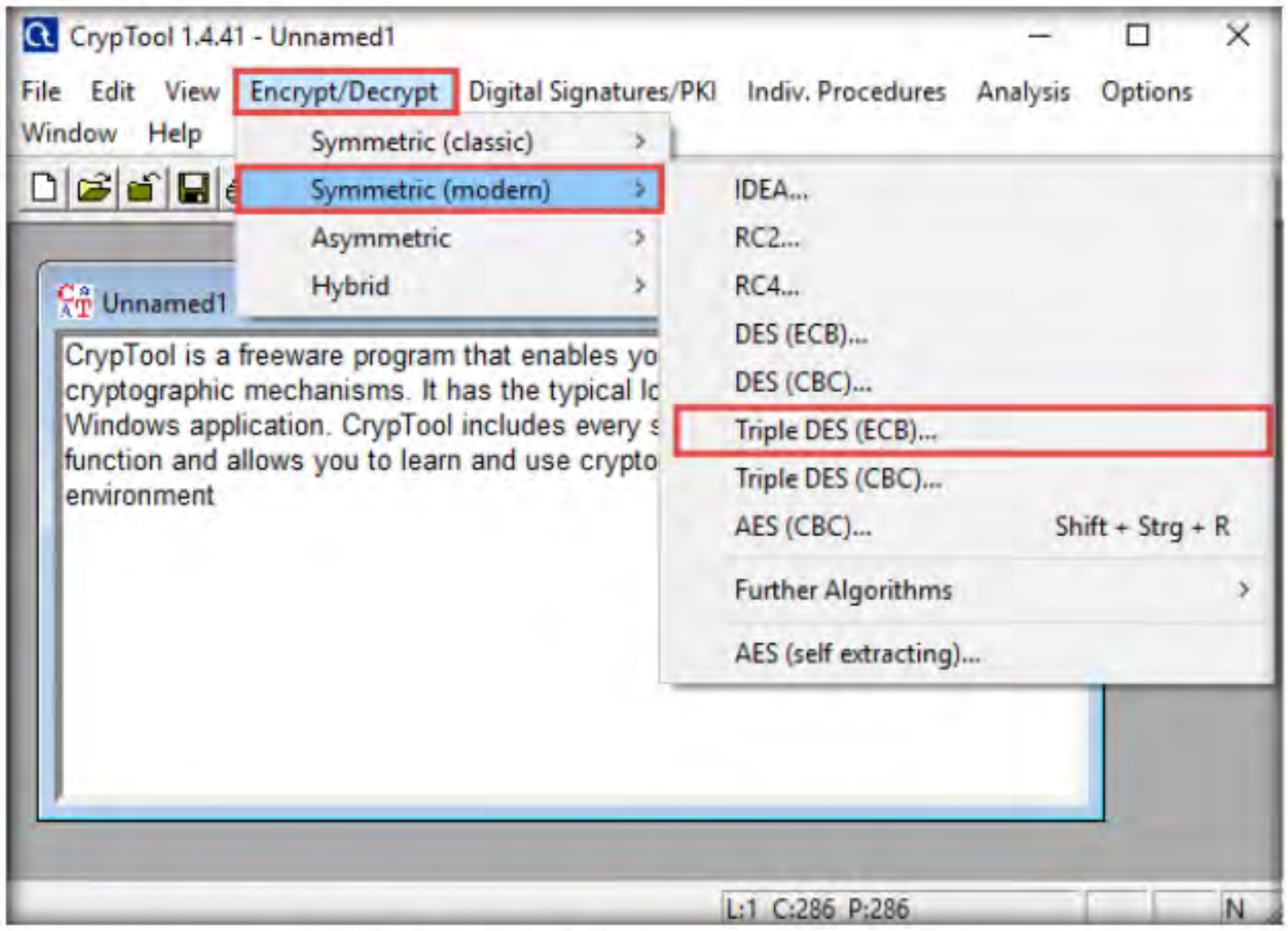


Figure 5.1.16: Select the Triple DES (ECB) Encryption algorithm

35. The **Key Entry: Triple DES (ECB)** dialog-box appears; leave the **Key length** set to default (**128 bits (effectively 112 bits)**).
36. In the text field below **Key length**, enter the combinations of **12** as **hexadecimal characters**, and click **Encrypt**.

Note: The chosen hexadecimal characters act like a key that you must send to the intended user along with the encrypted file.

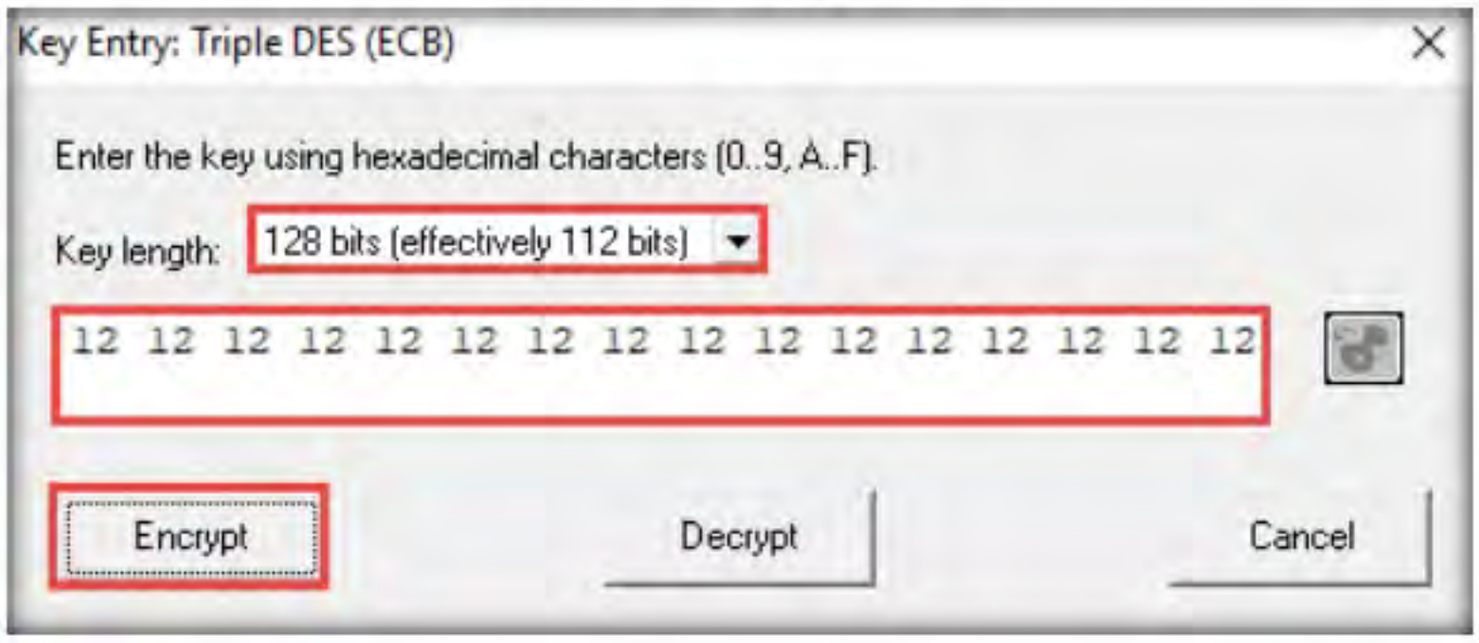


Figure 5.1.17: Key Entry: Triple DES (ECB) dialog-box

37. The **Triple DES (ECB) encryption of Unnamed1** notepad appears, as shown in the screenshot.

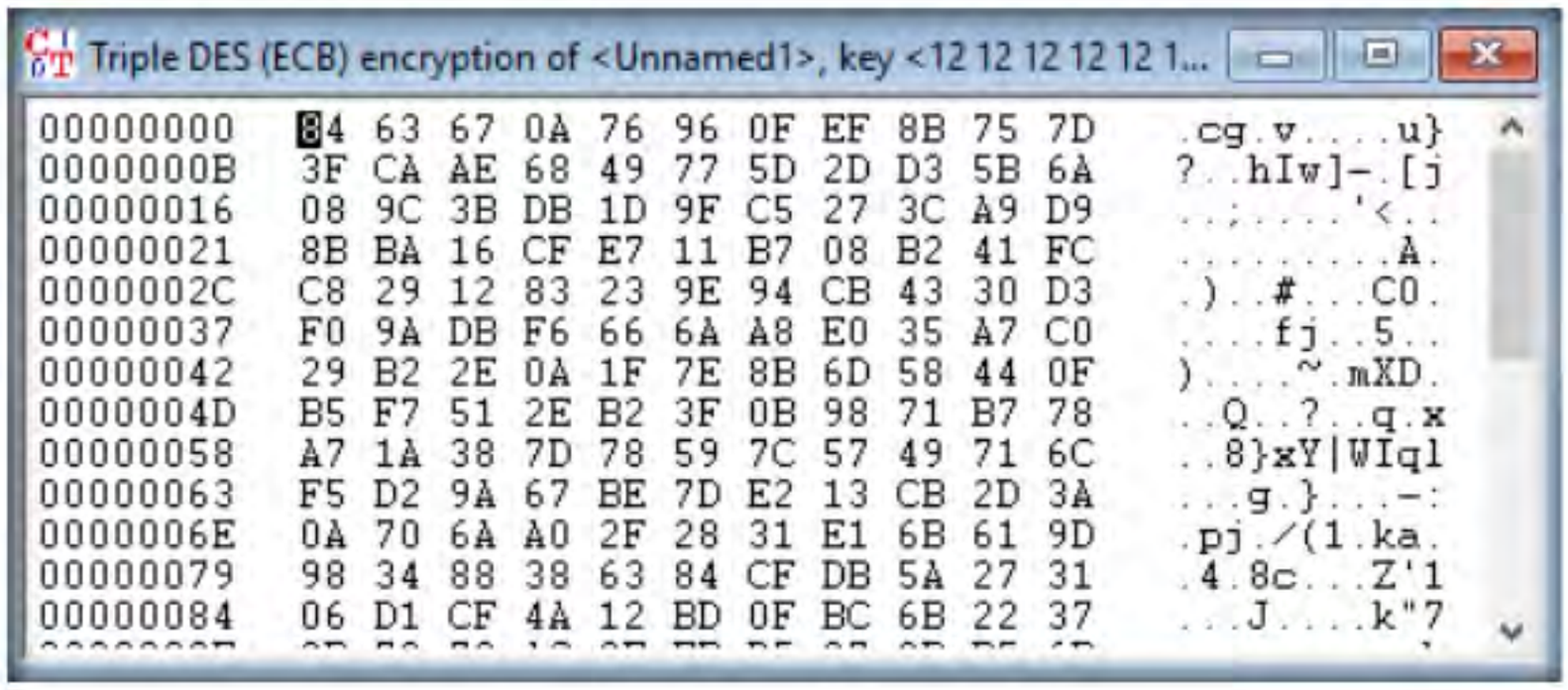


Figure 5.1.18: Output of RC2: encrypted data

38. To save the file, click **File** in the menu bar and select **Save**.
39. The **Save As** window appears; choose the save location (here, **Desktop**) and click **Save**.

Note: The file name may differ in your lab environment.

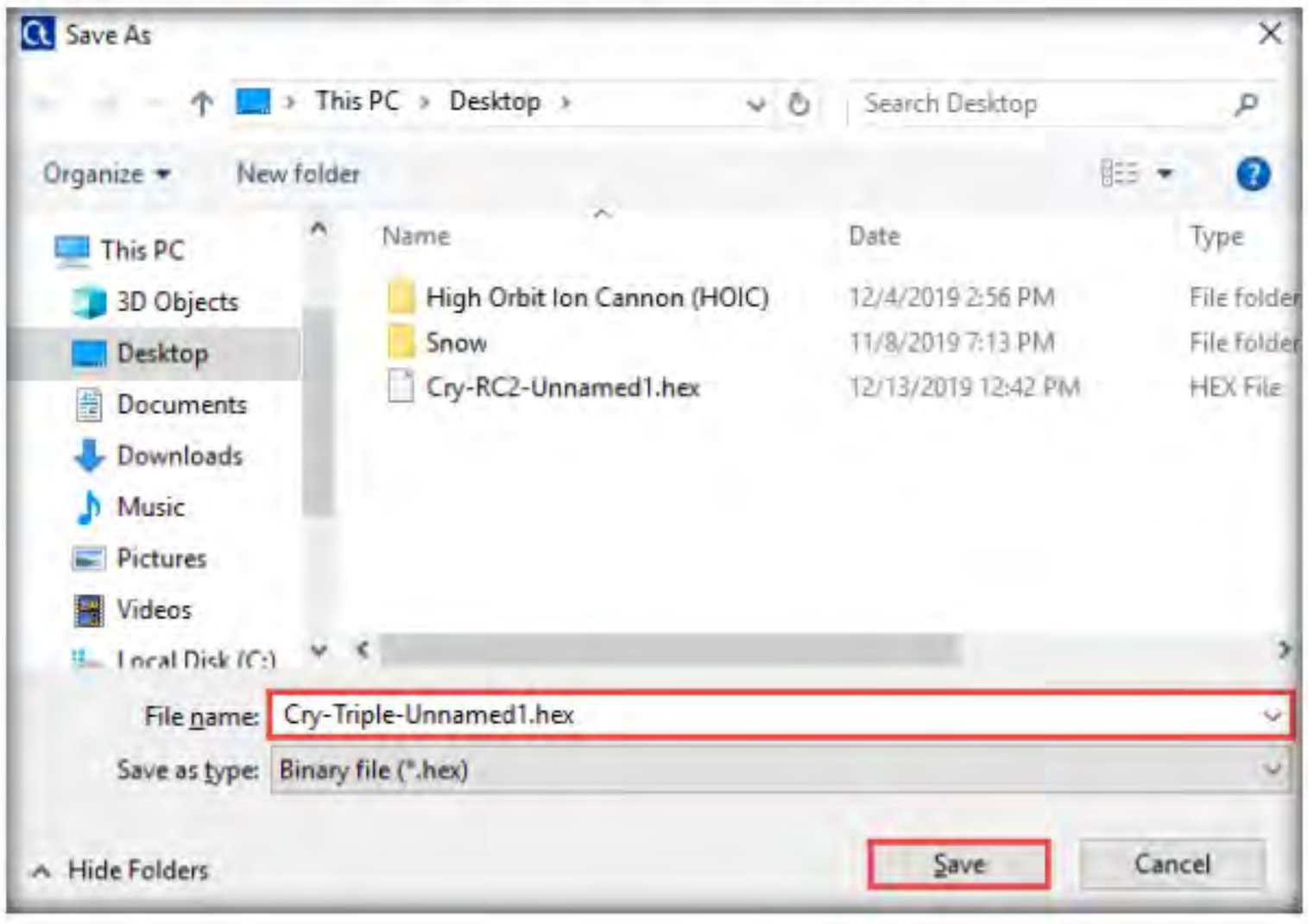


Figure 5.1.19: Save As window

40. To share the file, you may copy the encrypted file (**Cry-Triple-Unnamed1.hex**) from **Desktop** to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**.

TASK 1.5

Decrypt the Data

41. Switch to **Windows Server 2019**; copy the encrypted hex file (**Cry-Triple-Unnamed1.hex**) from **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool** and paste on **Desktop**.

42. Switch to the **CrypTool** window to **decrypt** the data; click **File** in the menu bar and select **Open...**

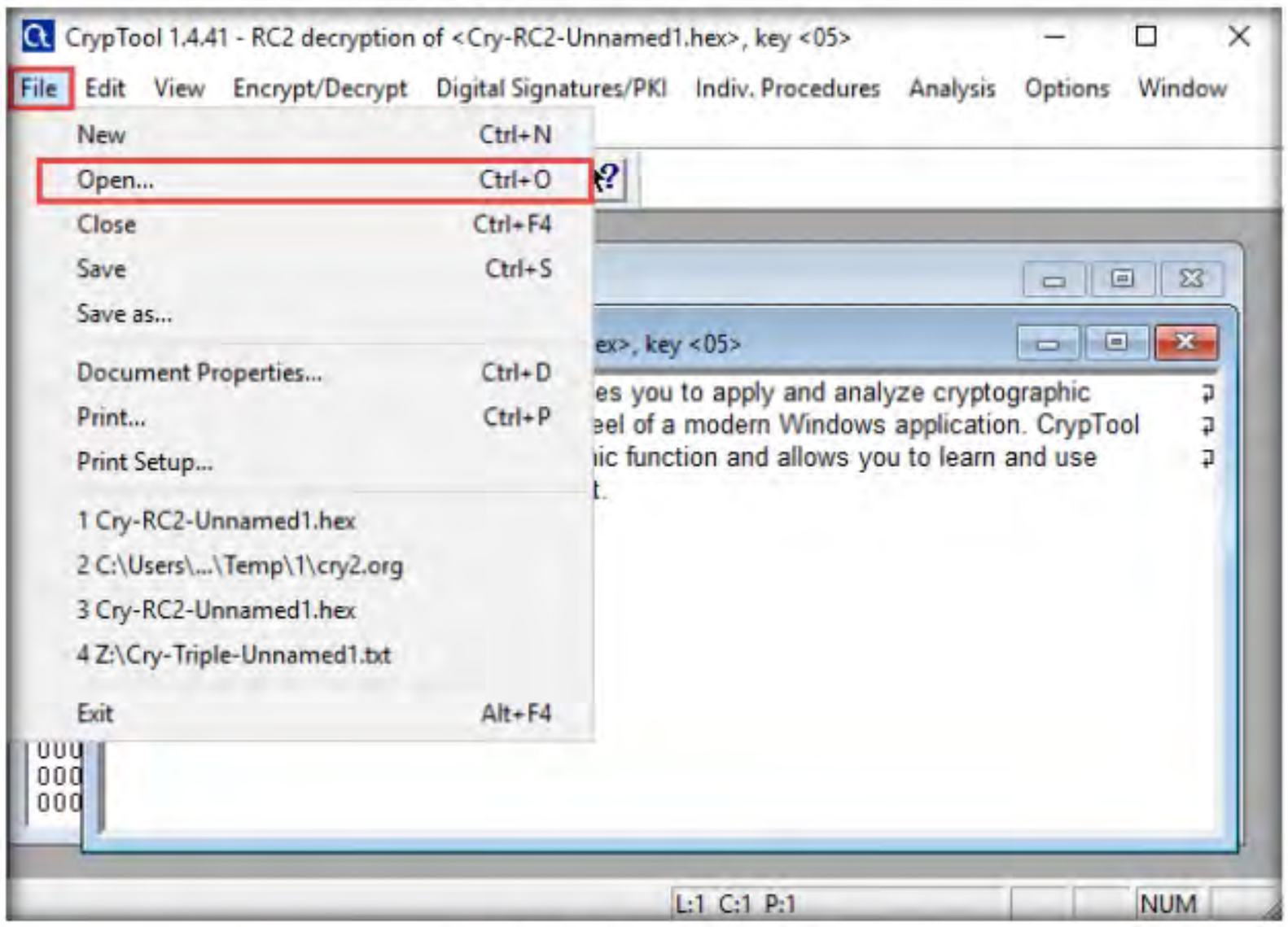


Figure 5.1.20: Opening a Crypted file

43. The **Open** window appears; select **Binary file (*.hex)** from the drop-down list in the file type option, navigate to the location of the file (here, **Desktop**), select, and click **Open**.

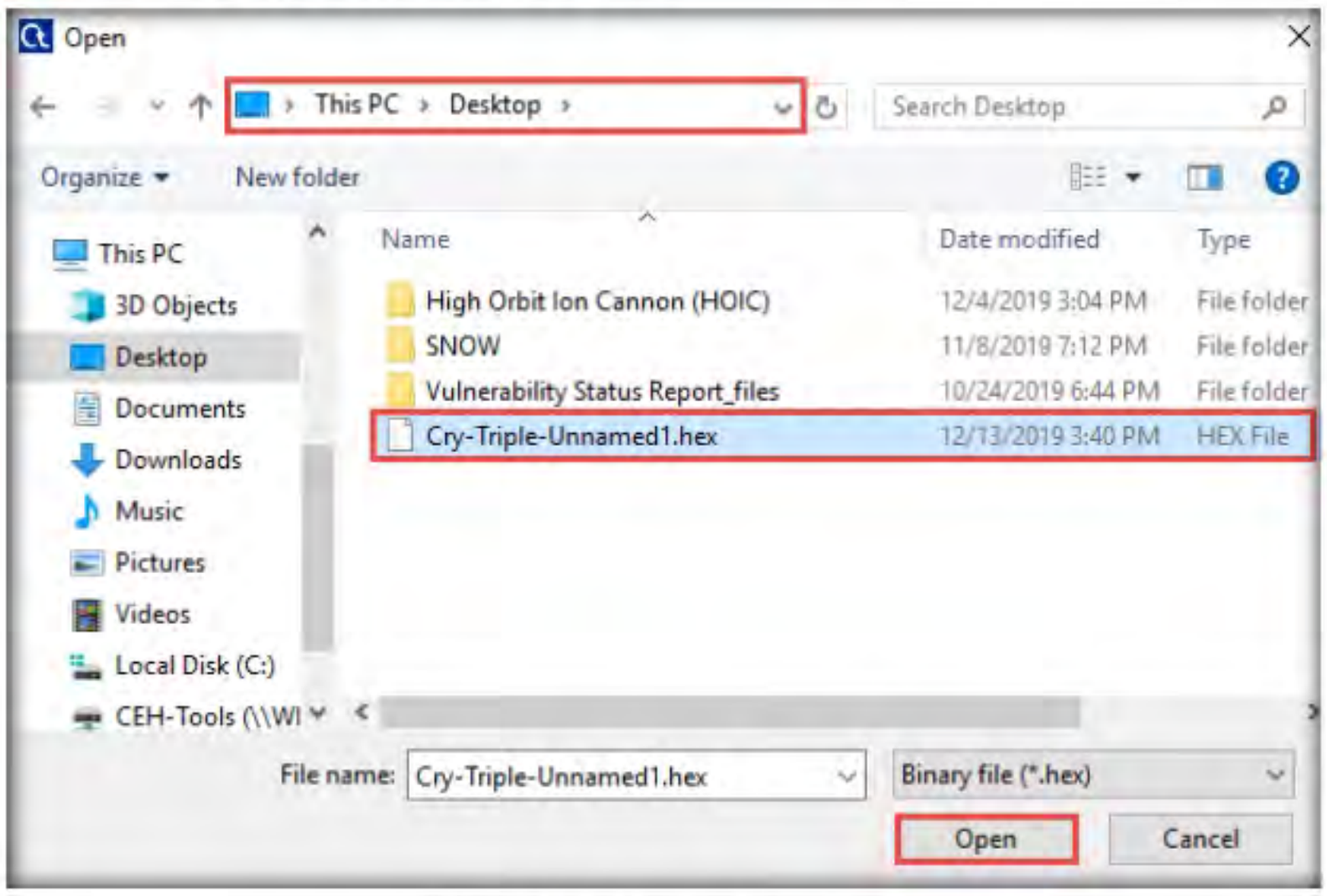


Figure 5.1.21: Opening a Crypted file

44. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → Triple DES (ECB)...**

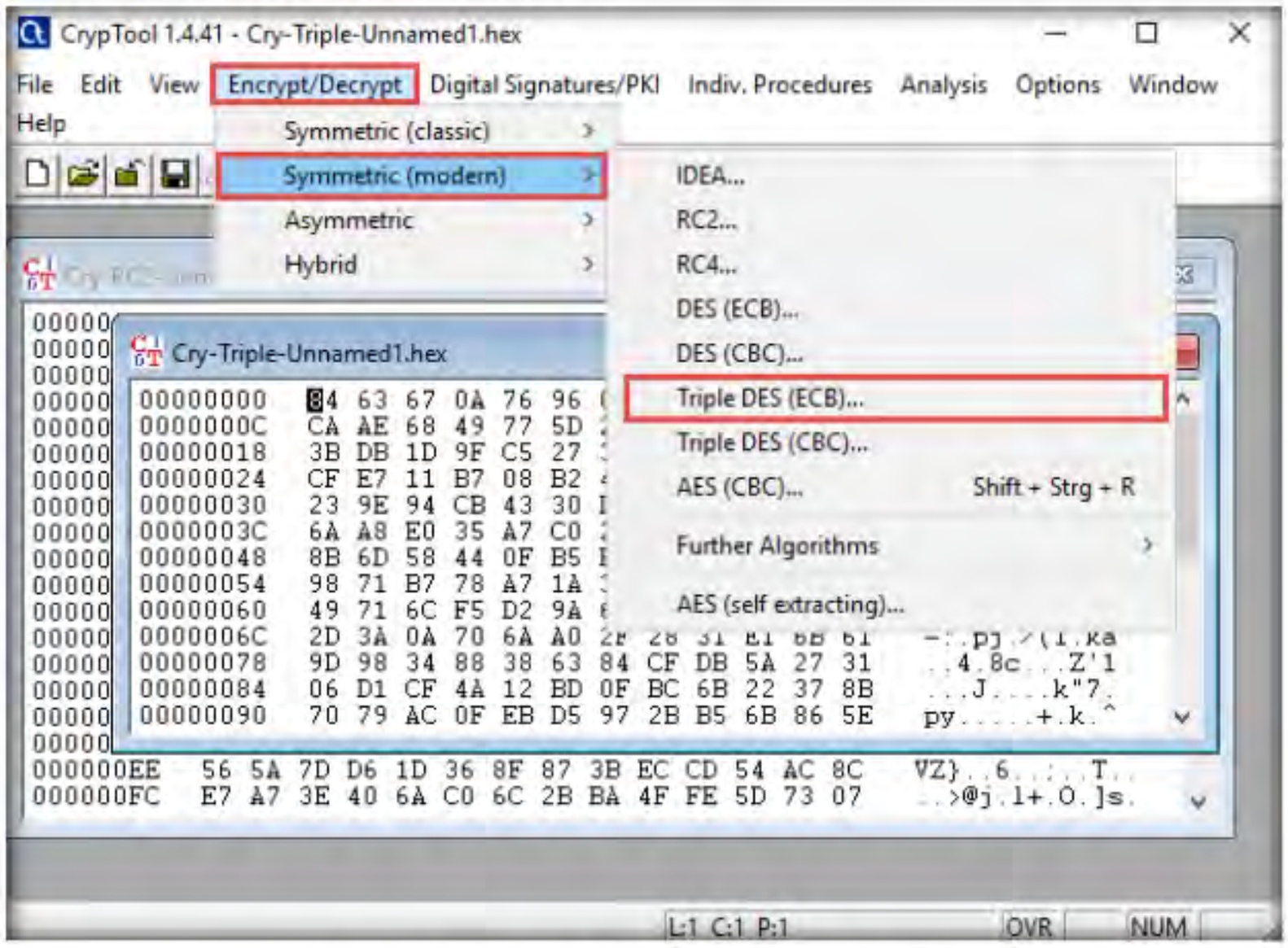


Figure 5.1.22: Select the Triple DES Encryption algorithm

45. The **Key Entry: Triple DES (ECB)** dialog-box appears; keep the **Key length** set to default (**128 bits (effectively 112 bits)**).

46. In the text field below **Key length**, enter the combinations of **12** as **hexadecimal characters** and click **Decrypt**.

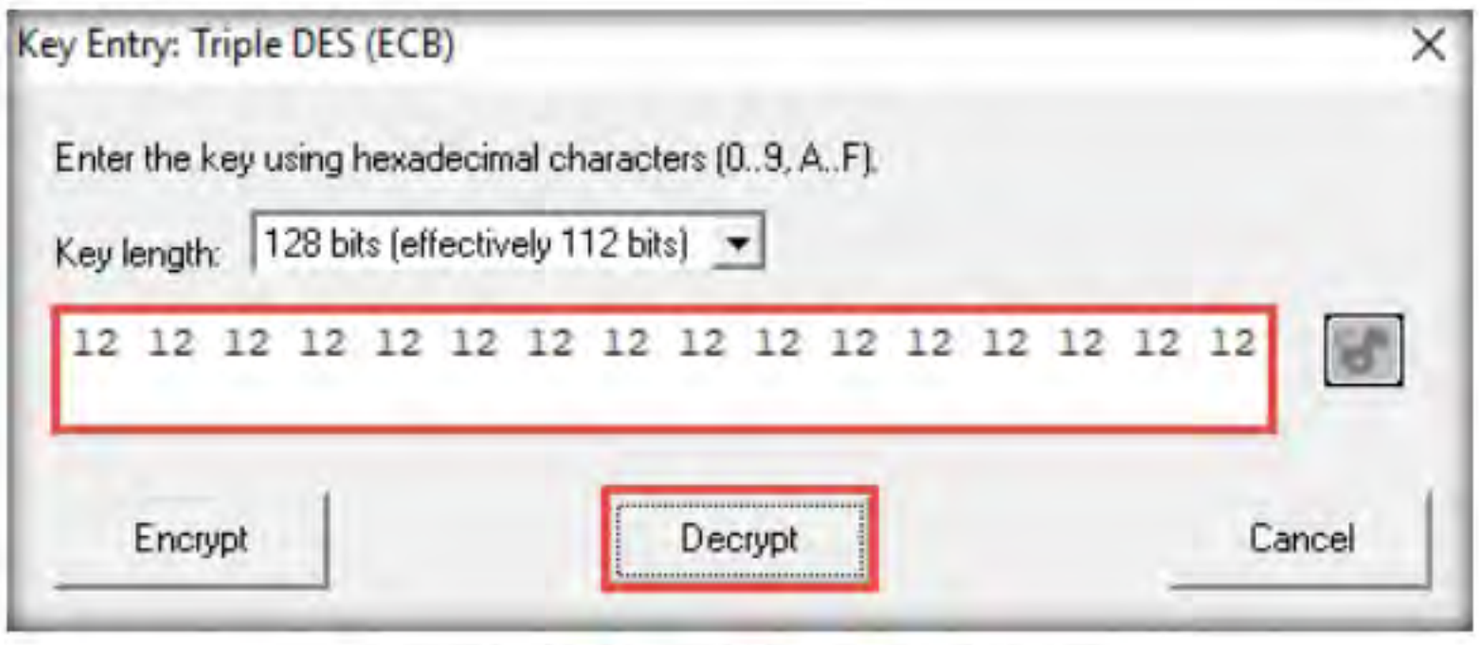


Figure 5.1.23: Key Entry: Triple DES (ECB) dialog-box

47. The decrypted text appears, as shown in the screenshot.

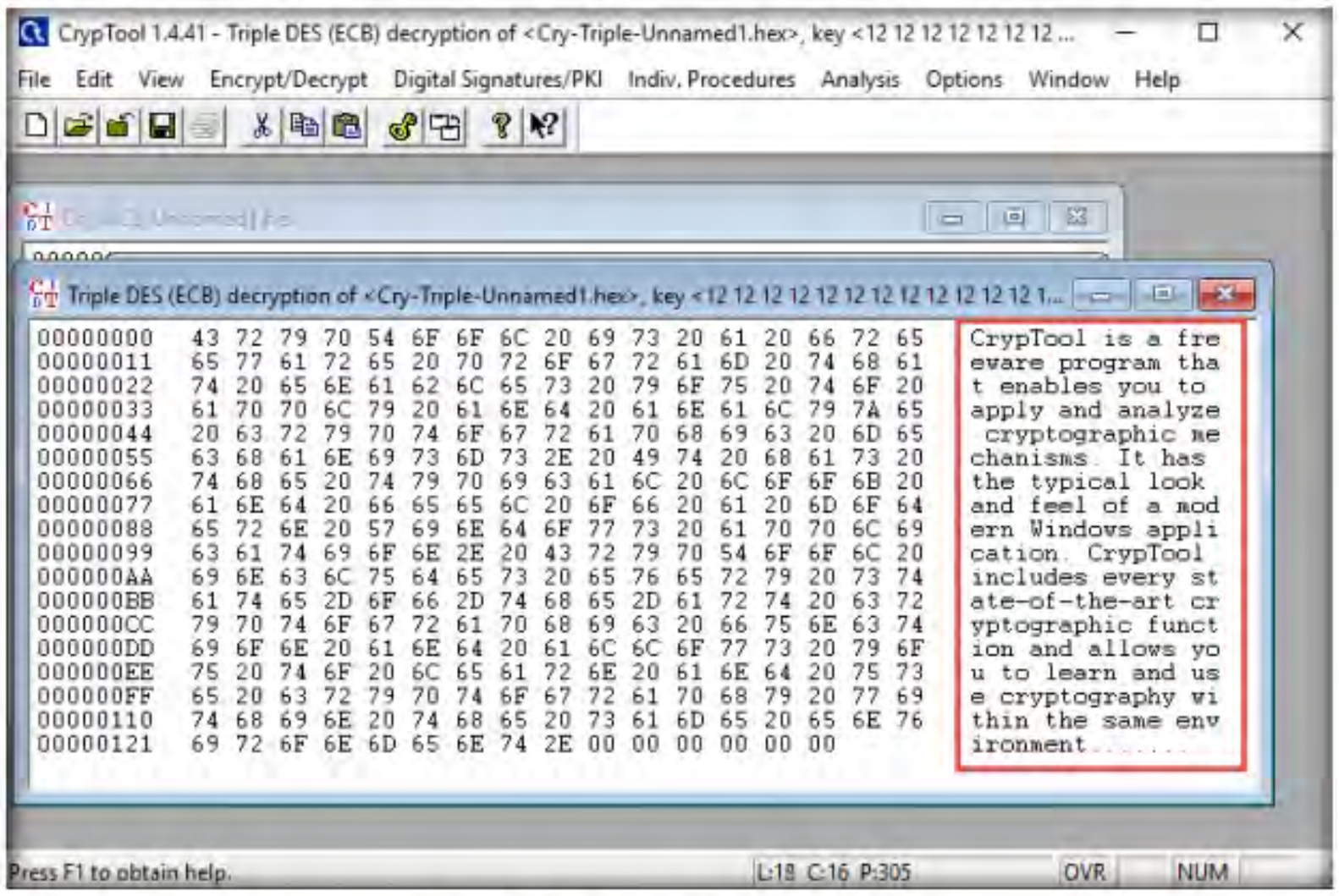


Figure 5.1.24: Decrypted the file successfully

48. Using this method, files can be encrypted using CrypTool and shared with an individual in a secure manner, so that no one can intercept the data.
49. This concludes the demonstration of performing cryptanalysis using CrypTool.
50. Close all open windows and document all the acquired information.

TASK 2 Perform Cryptanalysis using AlphaPeeler

Here, we will use the AlphaPeeler tool to perform cryptanalysis.

TASK 2.1

Install and Launch AlphaPeeler

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and double-click **AlphaPeelerPro1.3wse.exe**.

   Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

AlphaPeeler is a powerful tool for learning cryptology. It can be useful as an instructor's teaching aid and to create assignments for classical cryptography. You can easily learn classical techniques such as frequency analysis of alphabets, mono-alphabetic substitution, Caesar cipher, transposition cipher, Vigenere cipher, and Playfair cipher.

2. The **AlphaPeeler Professional** window appears; click **Accept**.

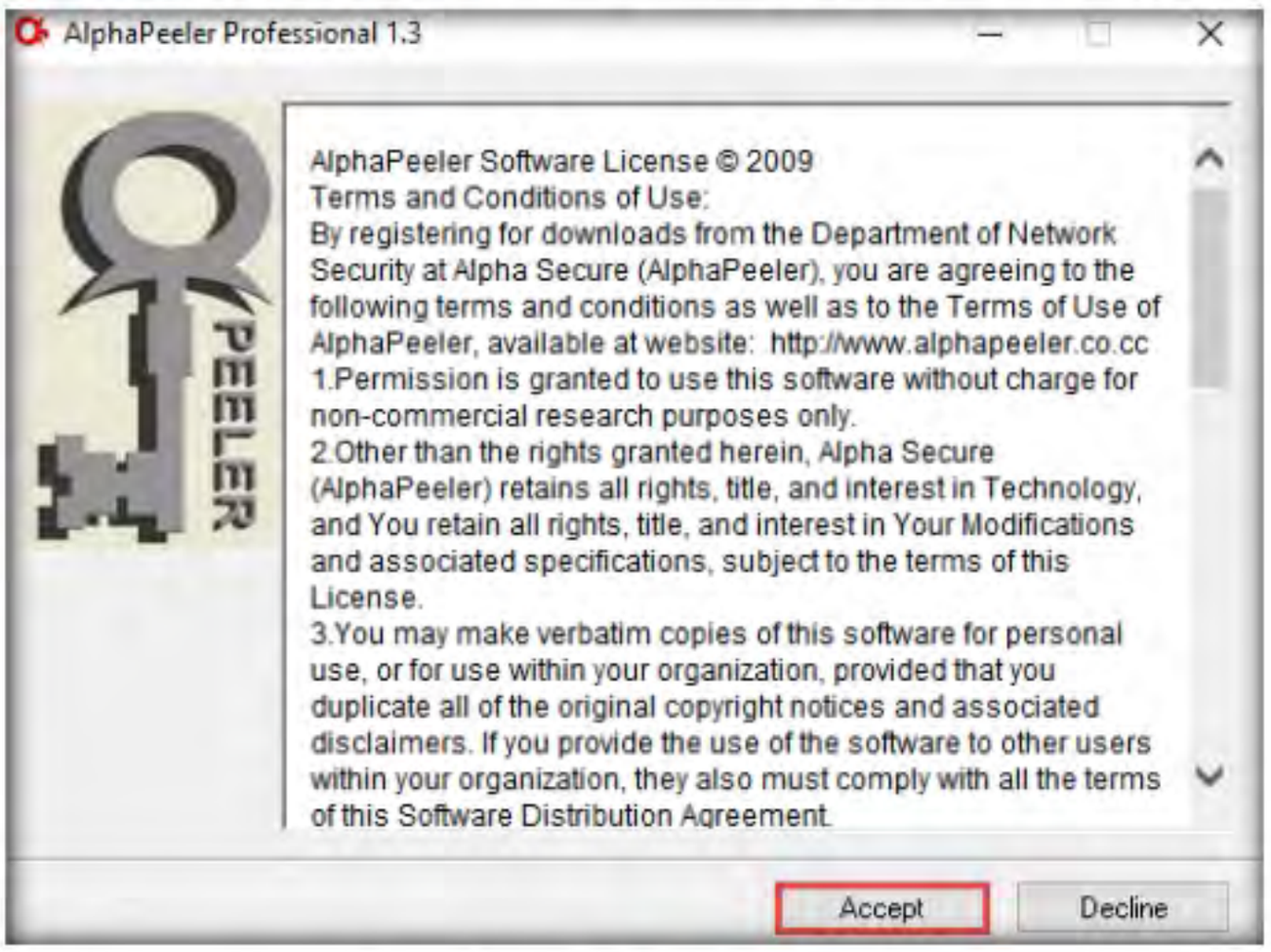


Figure 5.2.1: AlphaPeeler Professional setup

3. Follow the steps in the wizard and install the application using all default settings.

AlphaPeeler Professional (powered by crypto++ library) also includes DES, Gzip/Gunzip, MD5, SHA-1, SHA-256, RIPEMD-16, RSA key generation, RSA crypto, RSA signature & validation, and generation of secret share files.

4. After the completion of the installation, click the **Start** icon from the bottom-left corner of **Desktop** and click **AlphaPeeler** from the applications.

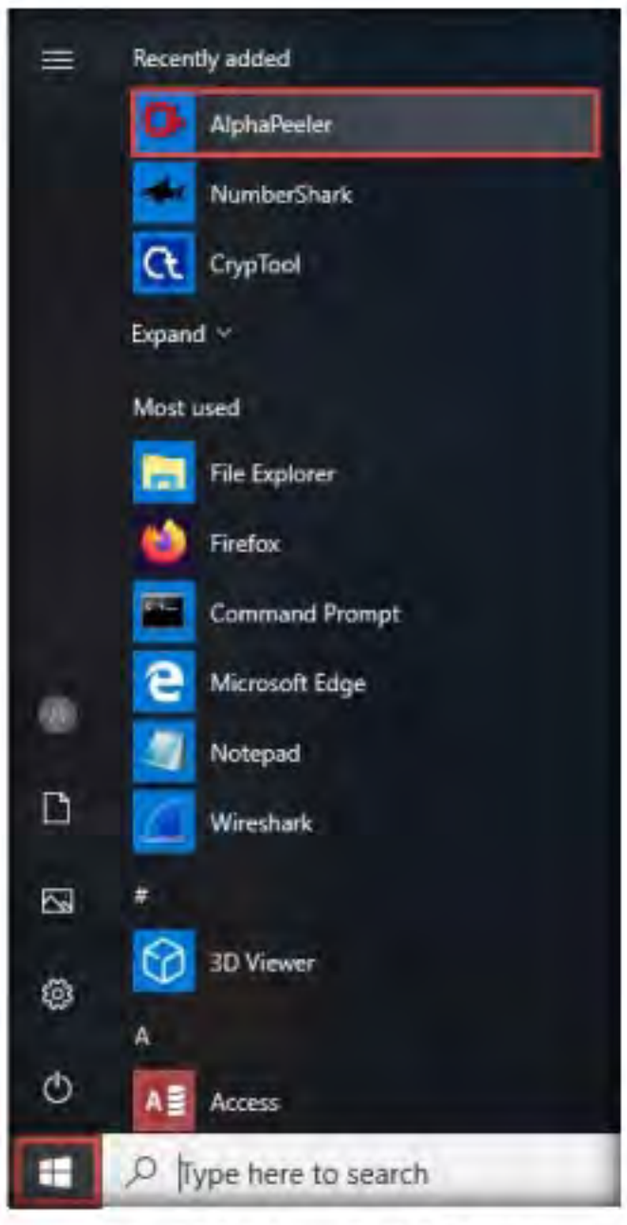


Figure 5.2.2: Launch AlphaPeeler

5. **AlphaPeeler Professional** initializes and the **AlphaPeeler** main window appears, as shown in the screenshot.

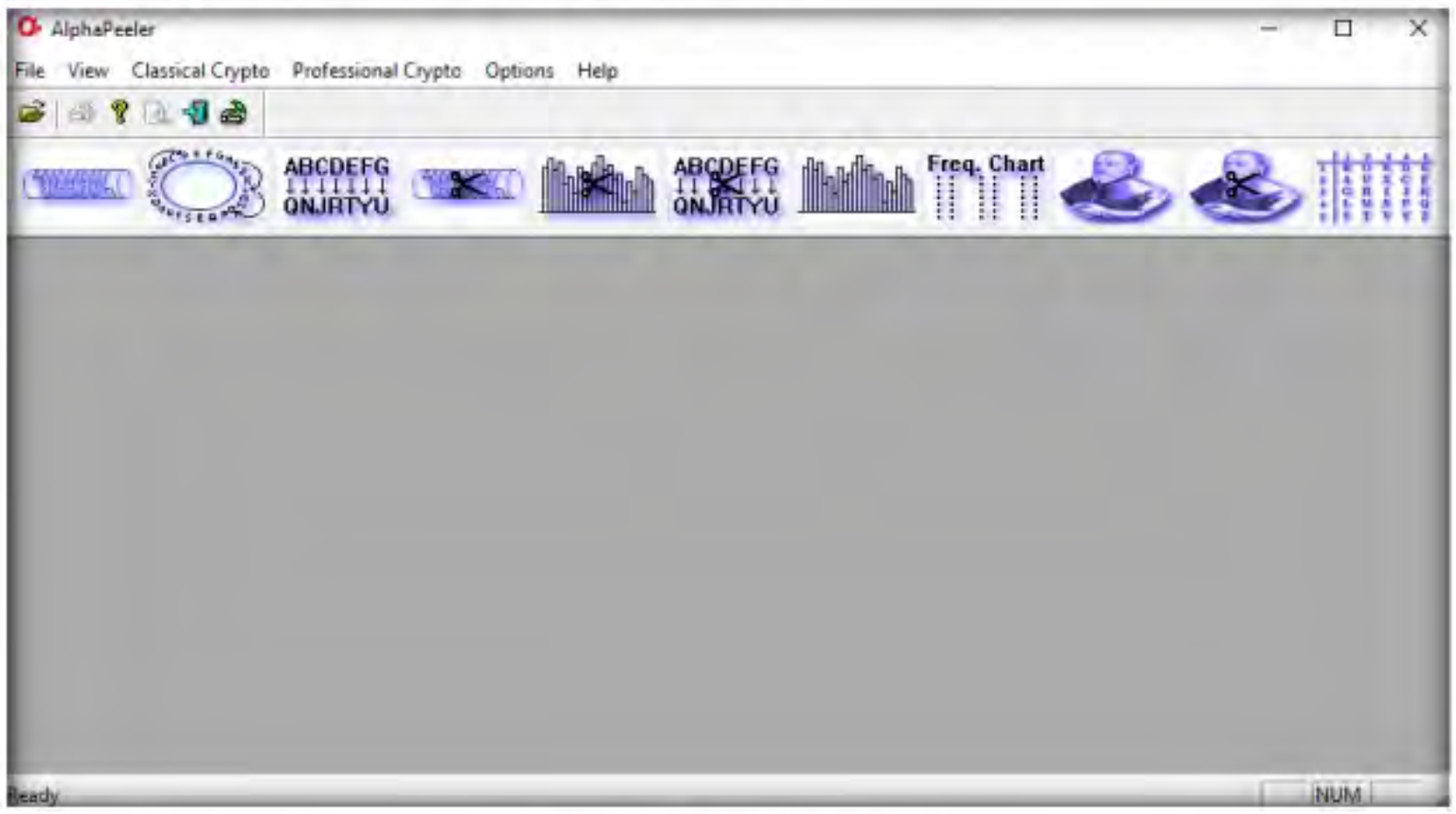


Figure 5.2.3: AlphaPeeler window

6. Now, minimize the AlphaPeeler window and create a text file on **Desktop**. Name it **Test**, open the file, and insert some text.
7. Click **File** in the menu bar and click **Save**.

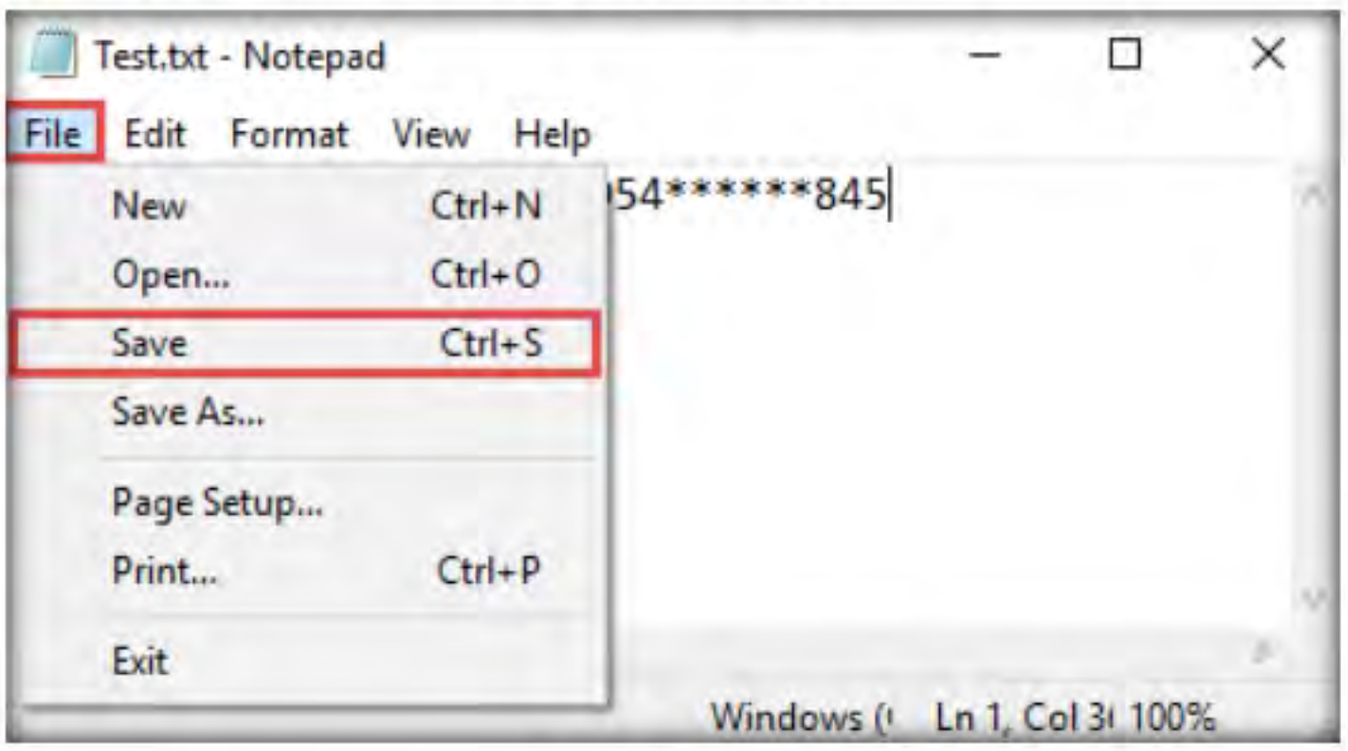


Figure 5.2.4: Text file

TASK 2.2

Encrypt a Data File

8. Switch back to the **AlphaPeeler** window; click **Professional Crypto** from the menu bar and select **DES crypto** from the options.

Figure 5.2.5: Selecting DES crypto

9. The **DES crypto** pop-up appears; click the ellipsis icon (...) under the **Plain text file** option.

Figure 5.2.6: Selecting DES crypto

10. The **Open** window appears; navigate to **Desktop** and select **Test.txt** file; then, click **Open**.

Note: Here, we are selecting the file that we will encrypt and this will act as an input file.

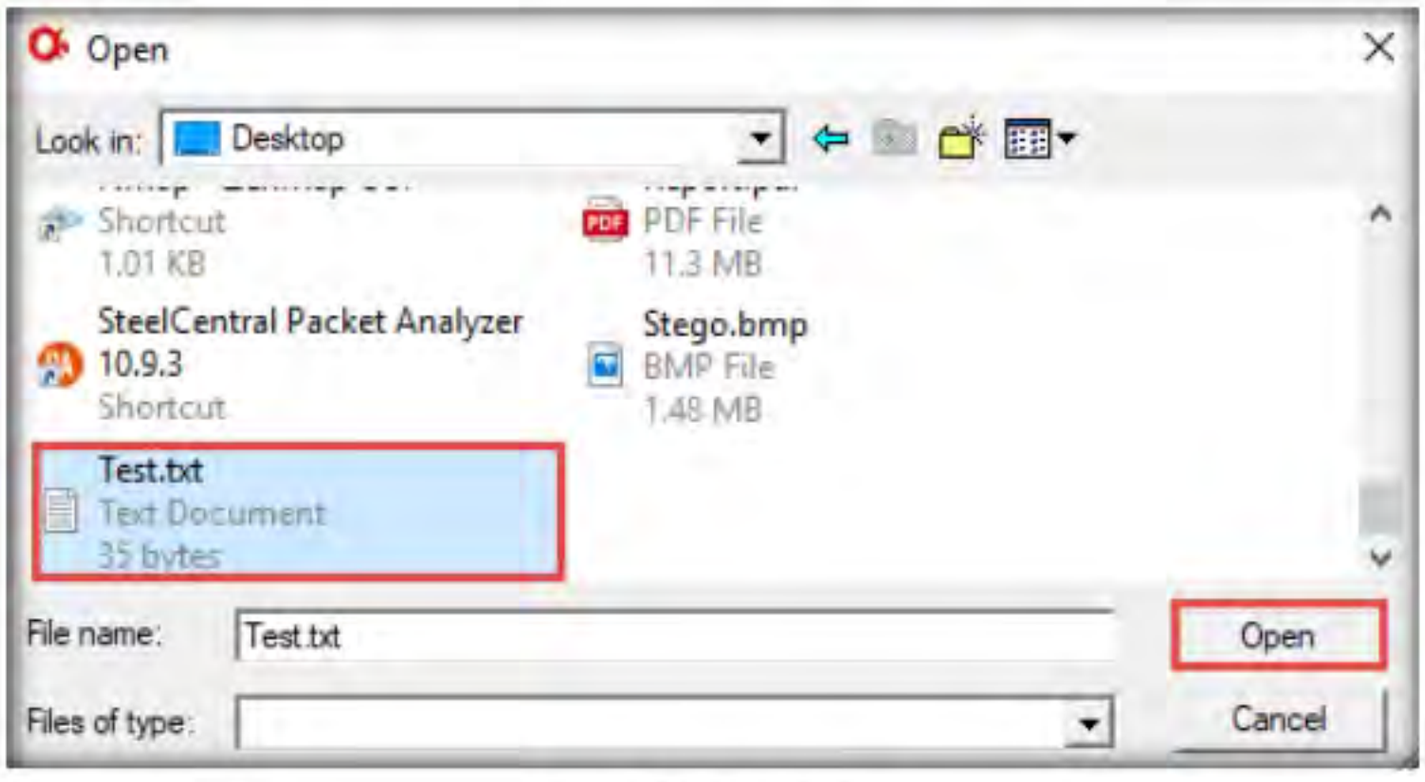


Figure 5.2.7: Open window

11. In the **DES crypto** pop-up; click the ellipsis icon ( ) under the **Cipher text file** option.
12. The **Open** window appears; select the save location (here, **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**) and name the file as **Confidential.txt**; then, click **Open**.

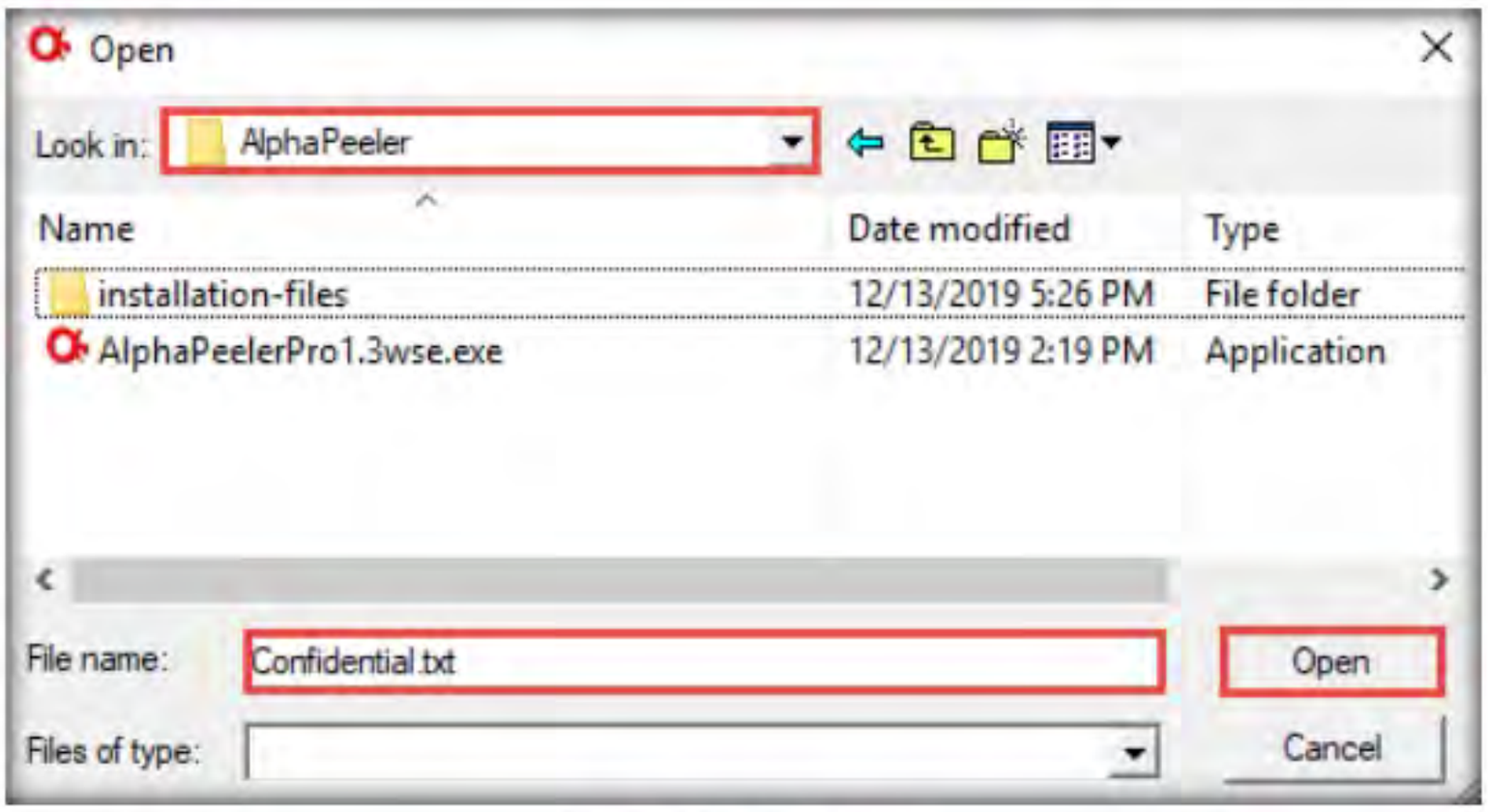


Figure 5.2.8: Open window

13. In the **DES crypto** pop-up; insert the password into the **Pass phrase** field and click **DES-EDE (CBC)** to encrypt the text file.

Note: Here, the password provided is **test@123**.

Figure 5.2.9: DES crypto

14. A new file **Confidential.txt** appears at location **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**, as shown in the screenshot.
15. Double-click **Confidential.txt** to open, and you can observe that the file's content is encrypted.

Note: Here, the encrypted file is shared through shared network drive **E\CEH-Tools\ CEHv11 Module 20 Cryptography** and the key to open the encrypted data was sent to you via an email. Using this, you can decrypt the encrypted data and view the data in plain-text.

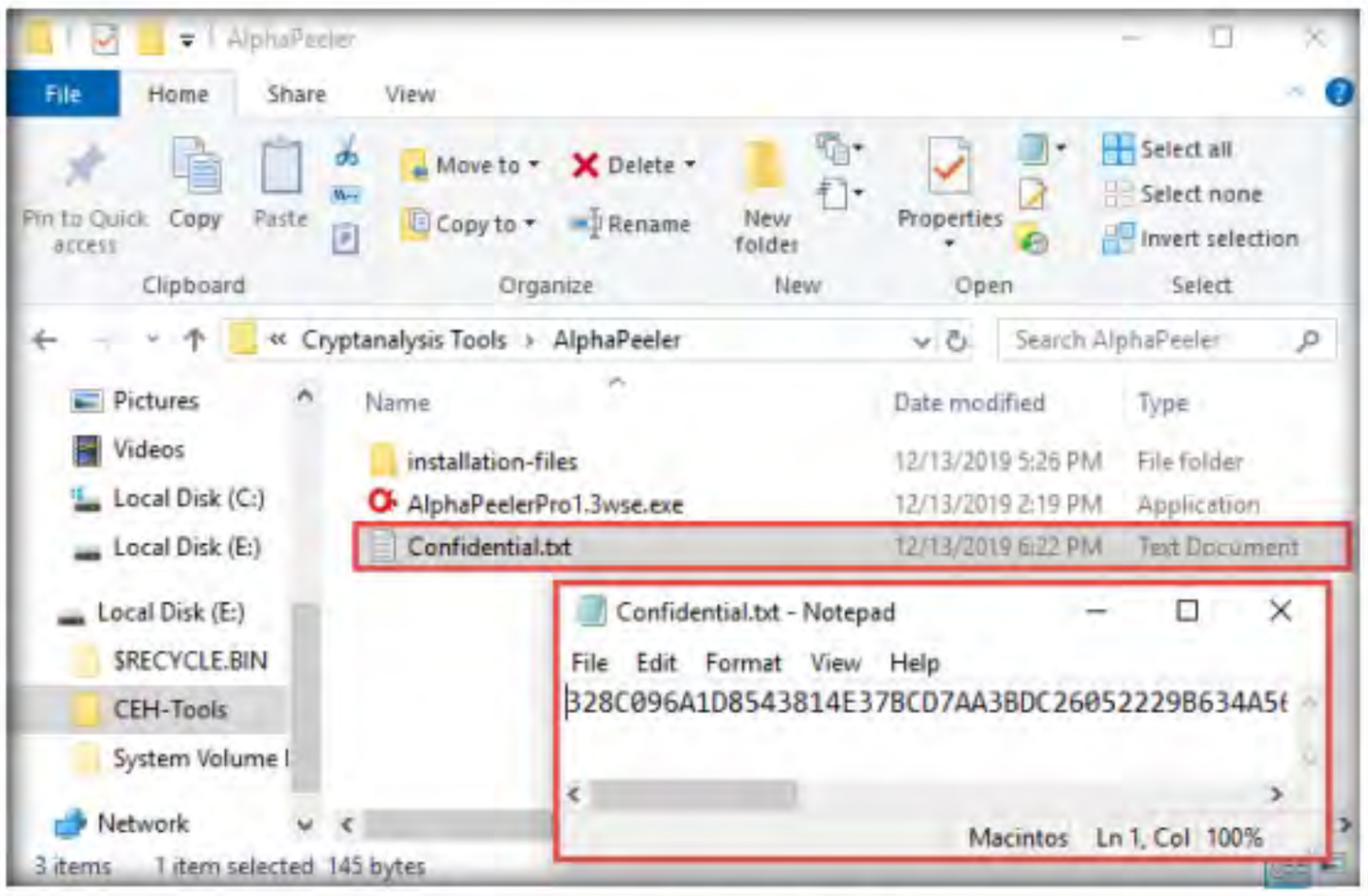


Figure 5.2.10: Confidential.txt file

16. Close the **DES crypto** pop-up and the **AlphaPeeler** window.
17. Switch to **Windows Server 2019**; navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and copy the **AlphaPeelerPro1.3wse.exe** file on **Desktop**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

18. Follow the steps in the wizard and install the application using all default settings.
19. After completion of the installation; click the **Start** icon from the bottom-right corner of **Desktop** and click **AlphaPeeler** from the applications.

TASK 2.3

Decrypt a Data File

20. The **AlphaPeeler** main window appears; click **File** from the menu bar and click **Open...**

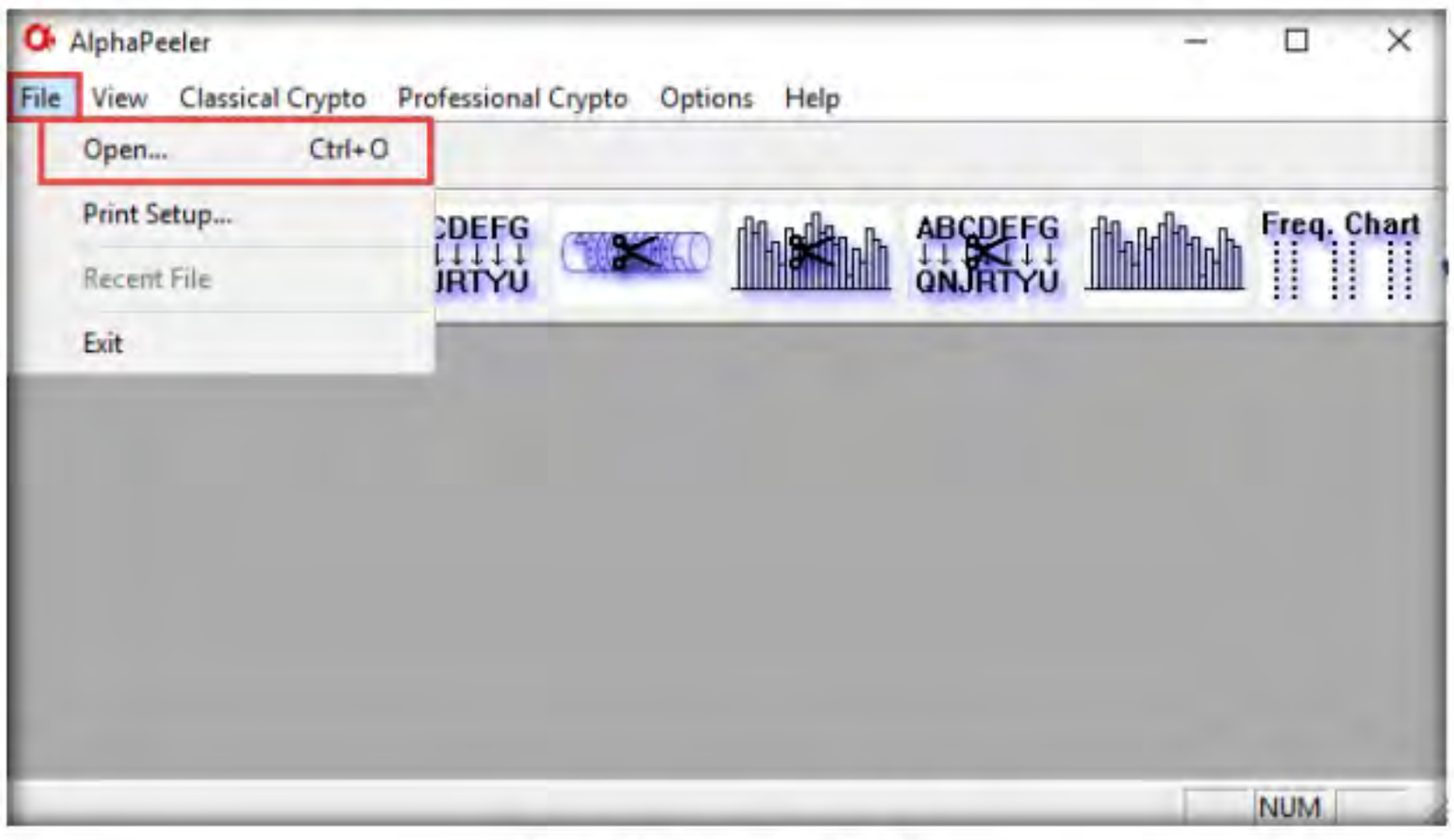


Figure 5.2.11: Confidential.txt file

21. The **Open** window appears; in the **Look in** field, navigate to the location of **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and select **Confidential.txt** file; then, click **Open**.

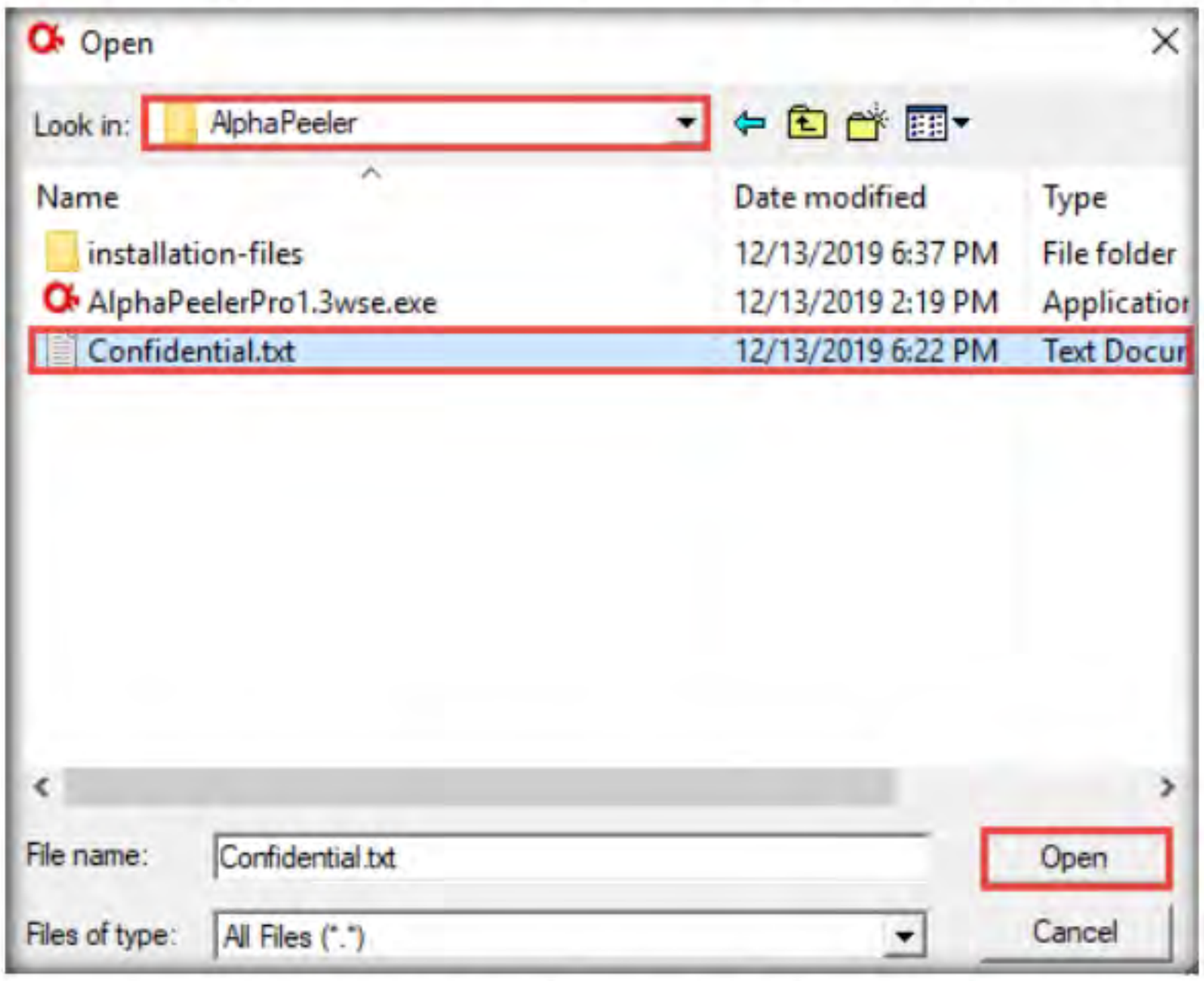


Figure 5.2.12: Open window select Confidential.txt file

22. The **Confidential.txt** file appears; click **Professional crypto** from the menu bar and select the **DES crypto** option.

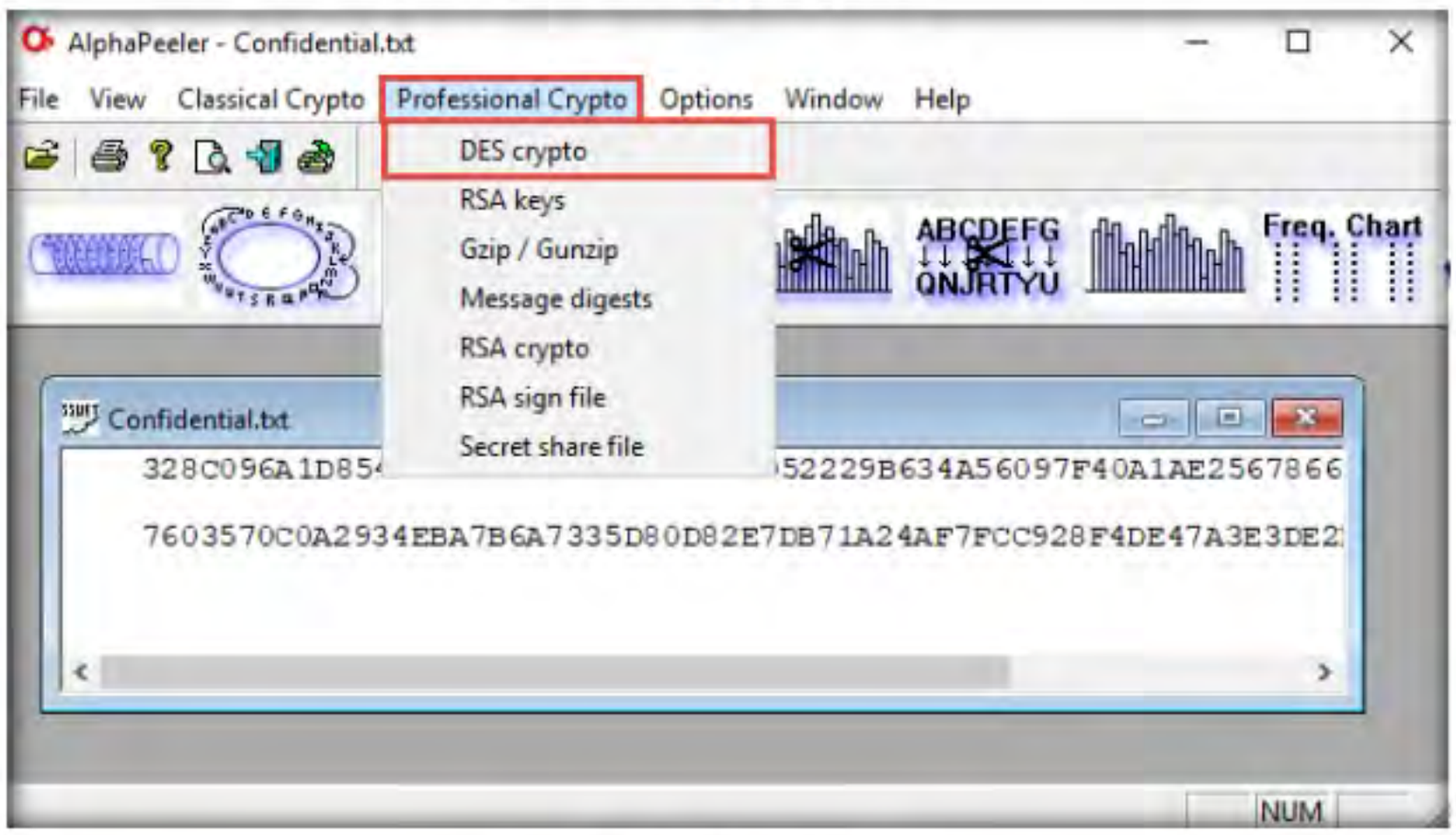


Figure 5.2.13: Selecting DES crypto

23. The **DES crypto** pop-up appears; click the ellipsis icon ( ) next to the **Plain text file** option.

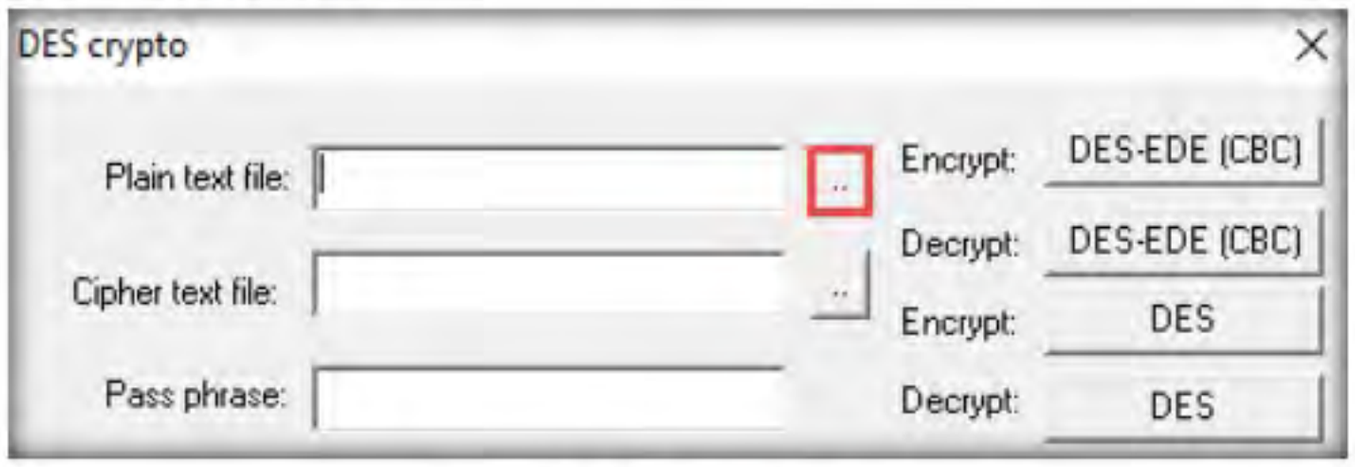


Figure 5.2.14: Selecting DES crypto

24. The **Open** window appears; navigate to **Desktop** and name the file **Result.txt**; then, click **Open**.

Note: Here, we are creating an output file that will be in plain-text.

25. In the **DES crypto** pop-up; click the ellipsis icon ( ) under the **Cipher text file** option.
26. The **Open** window appears; select the encrypted file (**Confidential.txt**) located at **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and click **Open**.

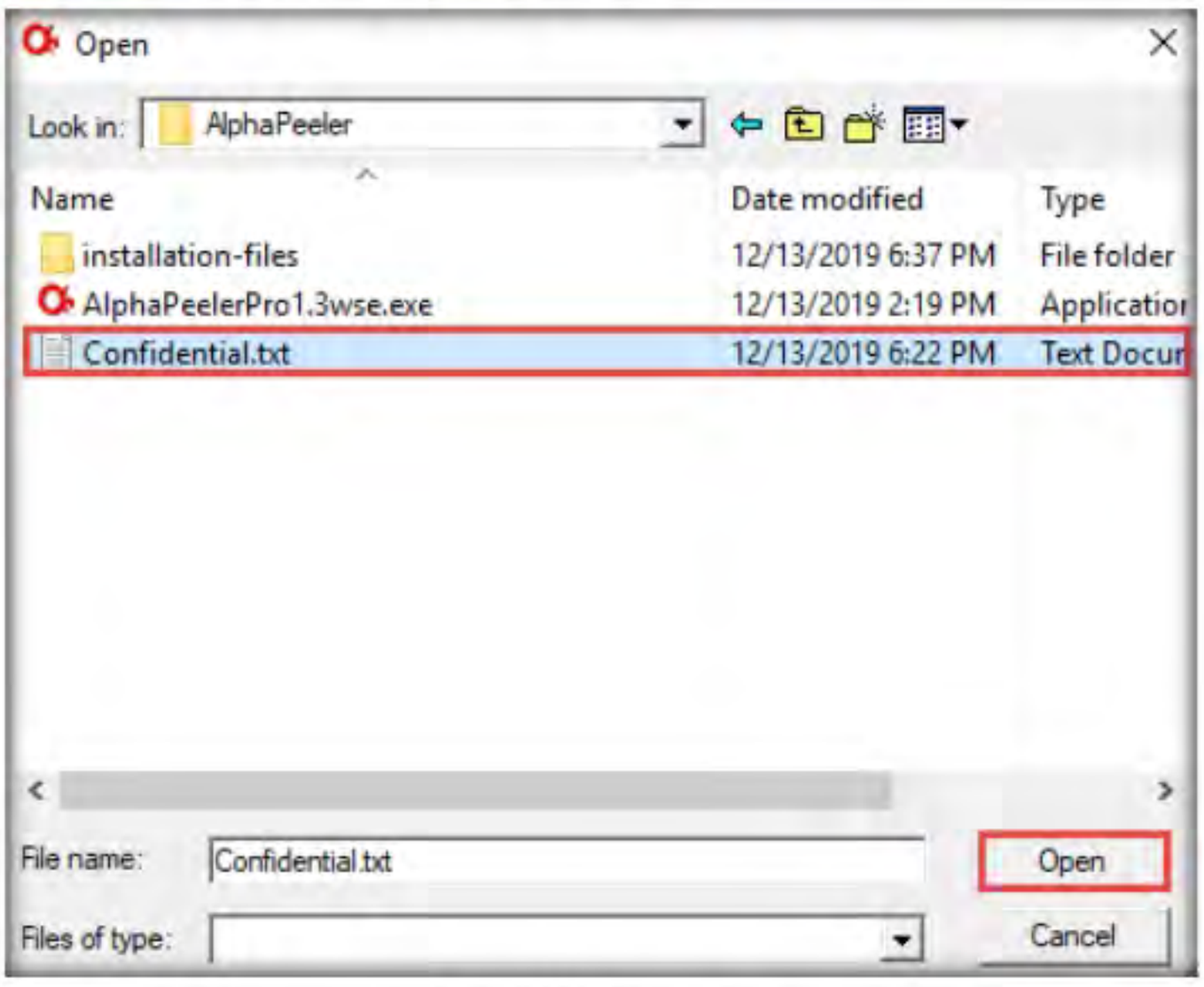


Figure 5.2.15: Open window

27. In the **DES crypto** pop-up, enter the password that you provided in **Step#13** into the **Pass phrase** field and click the **DES-EDE (CBC)** button next to **Decrypt** to decrypt the text file.

Note: Here, the password provided is **test@123**.

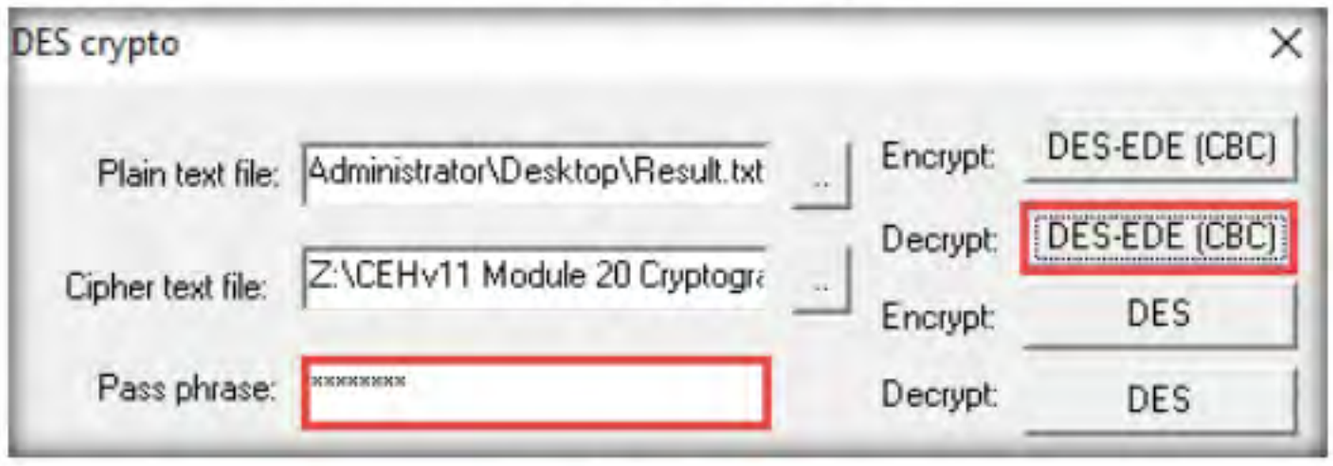


Figure 5.2.16: DES crypto

You can also use other cryptanalysis tools such as **Cryptosense** (https://cryptosense.com) , **RsaCtfTool** (https://github.com), **Msieve** (https://sourceforge.net), and **Cryptol** (https://cryptol.net) to perform cryptanalysis.

28. Navigate to **Desktop** and double click the **Result.txt** file. You can observe the file content in plain-text, as shown in the screenshot.

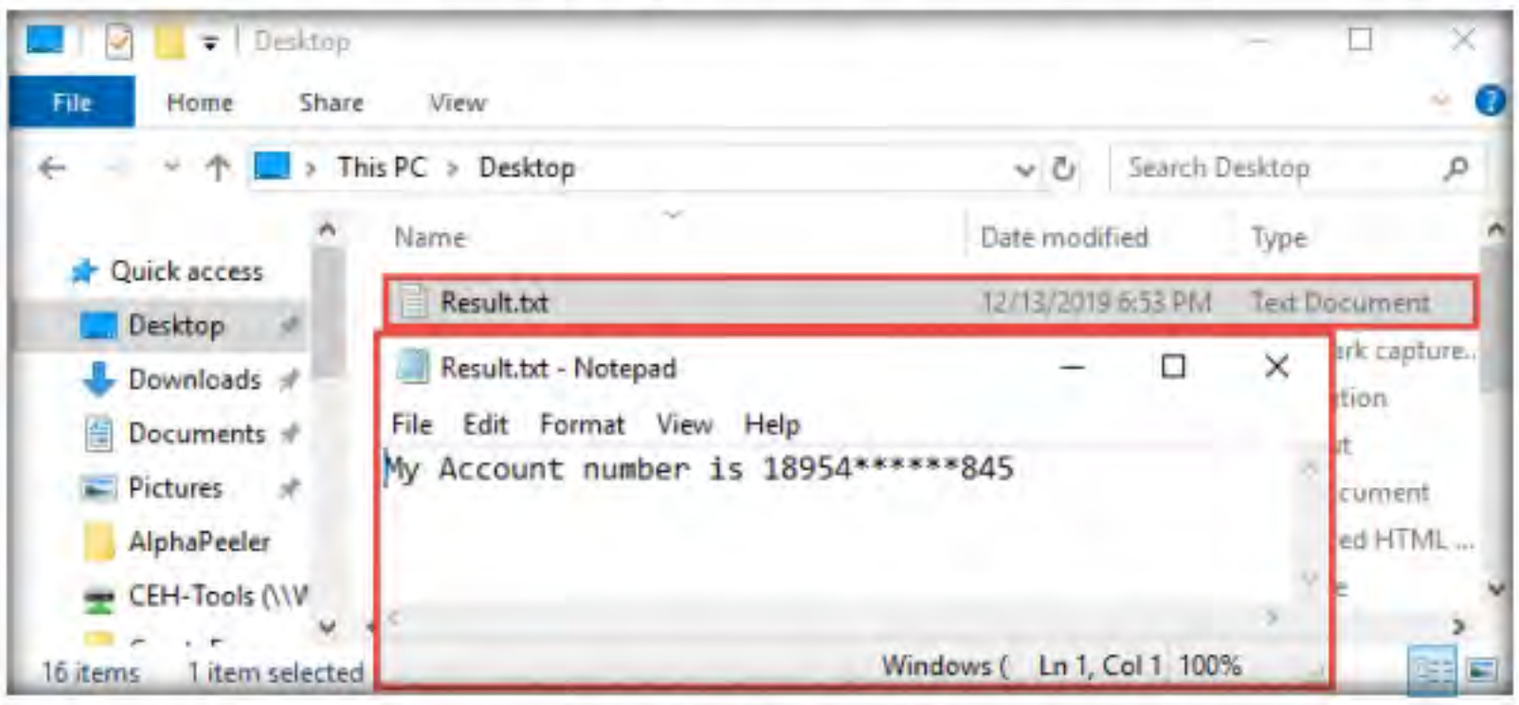


Figure 5.2.17: Decrypted file

29. This concludes the demonstration of performing cryptanalysis using AlphaPeeler.
30. Close all open windows and document all the acquired information.
31. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

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

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