Module 20: Cryptography

Lab 1: Encrypt the Information using Various Cryptography Tools

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.

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
- Encrypt and decrypt data using BCTextEncoder

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.

Task 1: Calculate One-way Hashes using HashCalc

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.

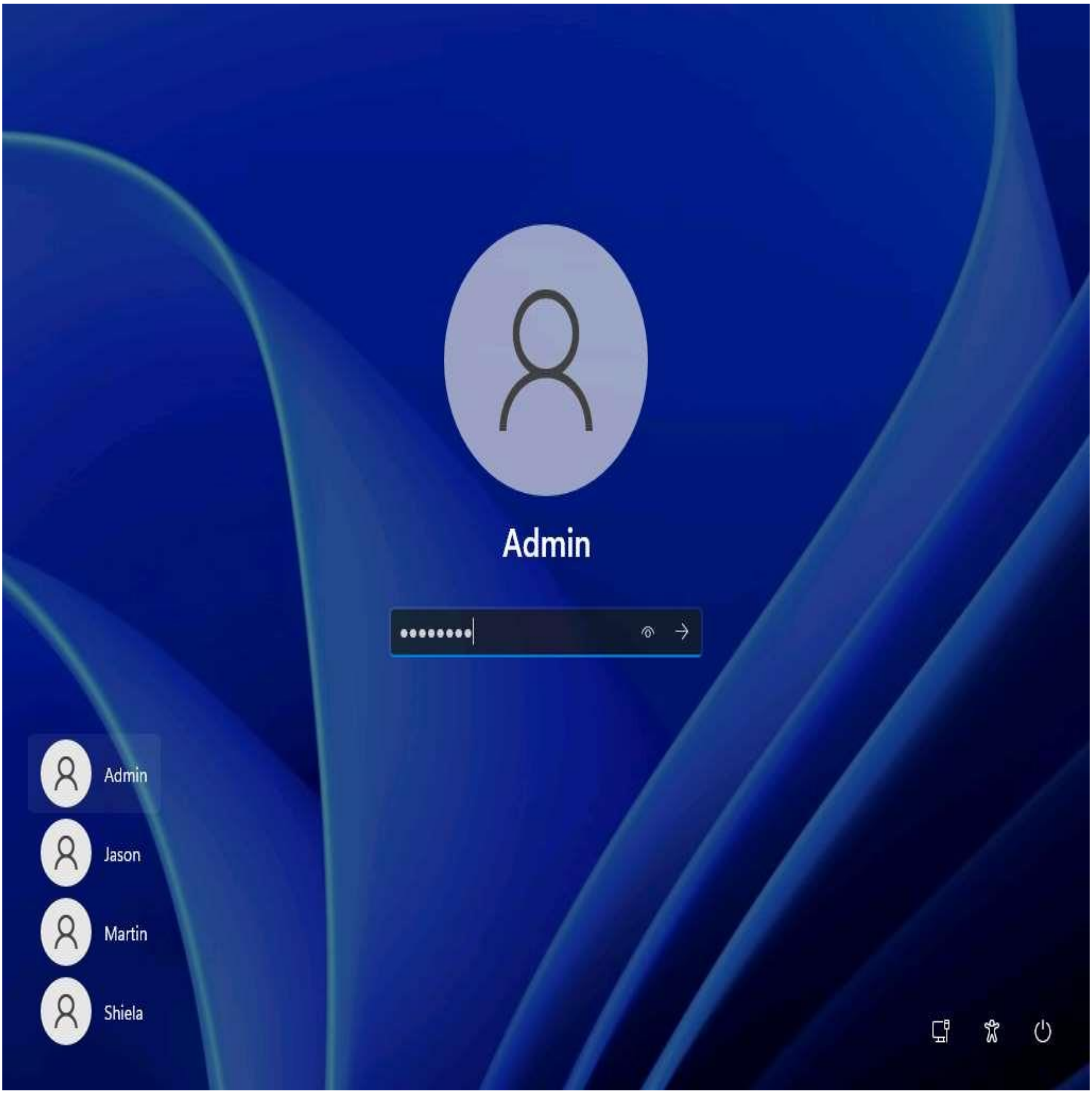
HashCalc enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It supports the Secure Hash Algorithm family: MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, and the hash used in the peer-to-peer file sharing applications,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

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

1. □ Click Windows 11 to switch to the **Windows 11** machine. click Ctrl+Alt+Delete to activate it. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

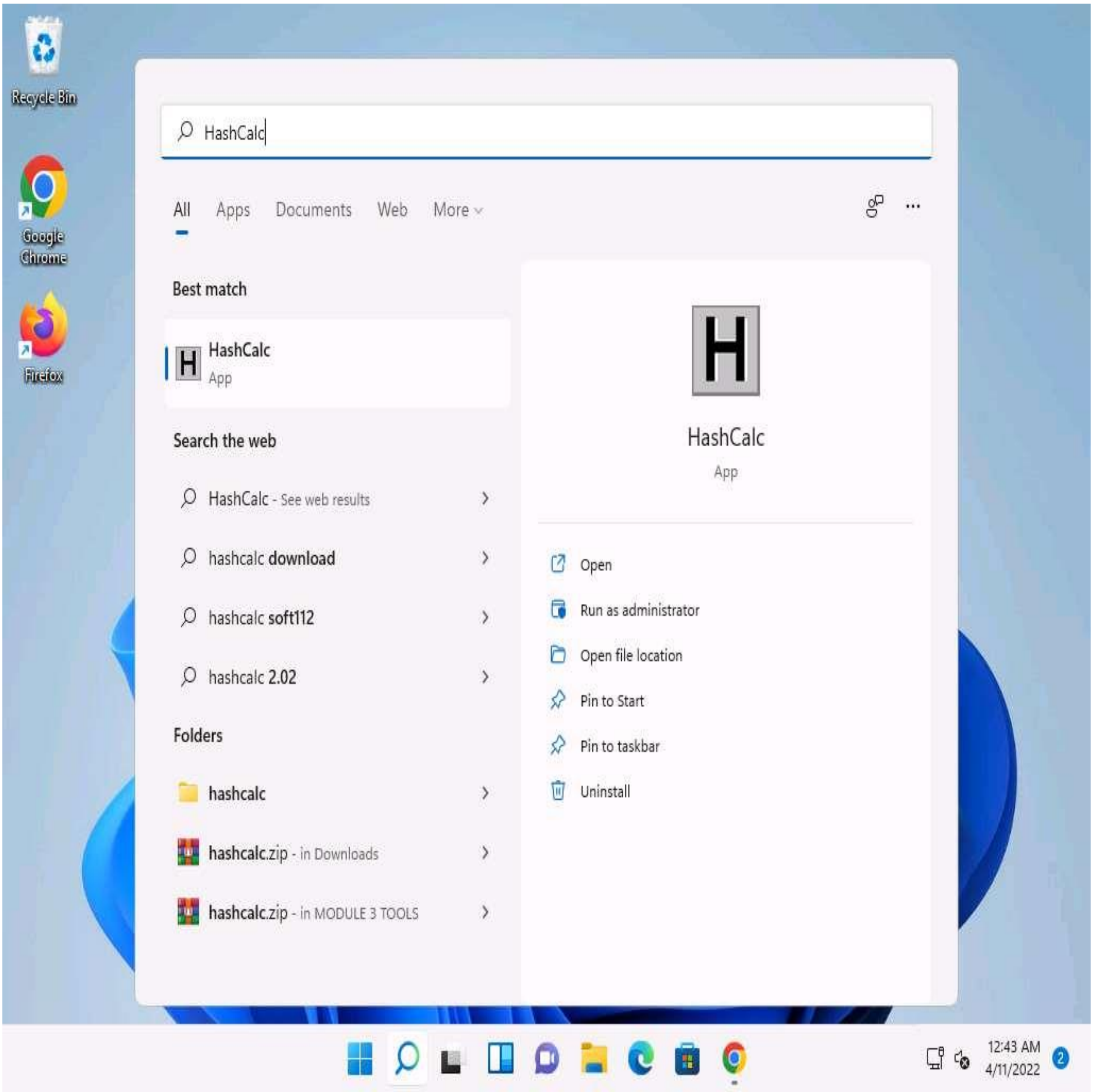
   Alternatively, you can also click **Pa$$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.
   If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

   Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



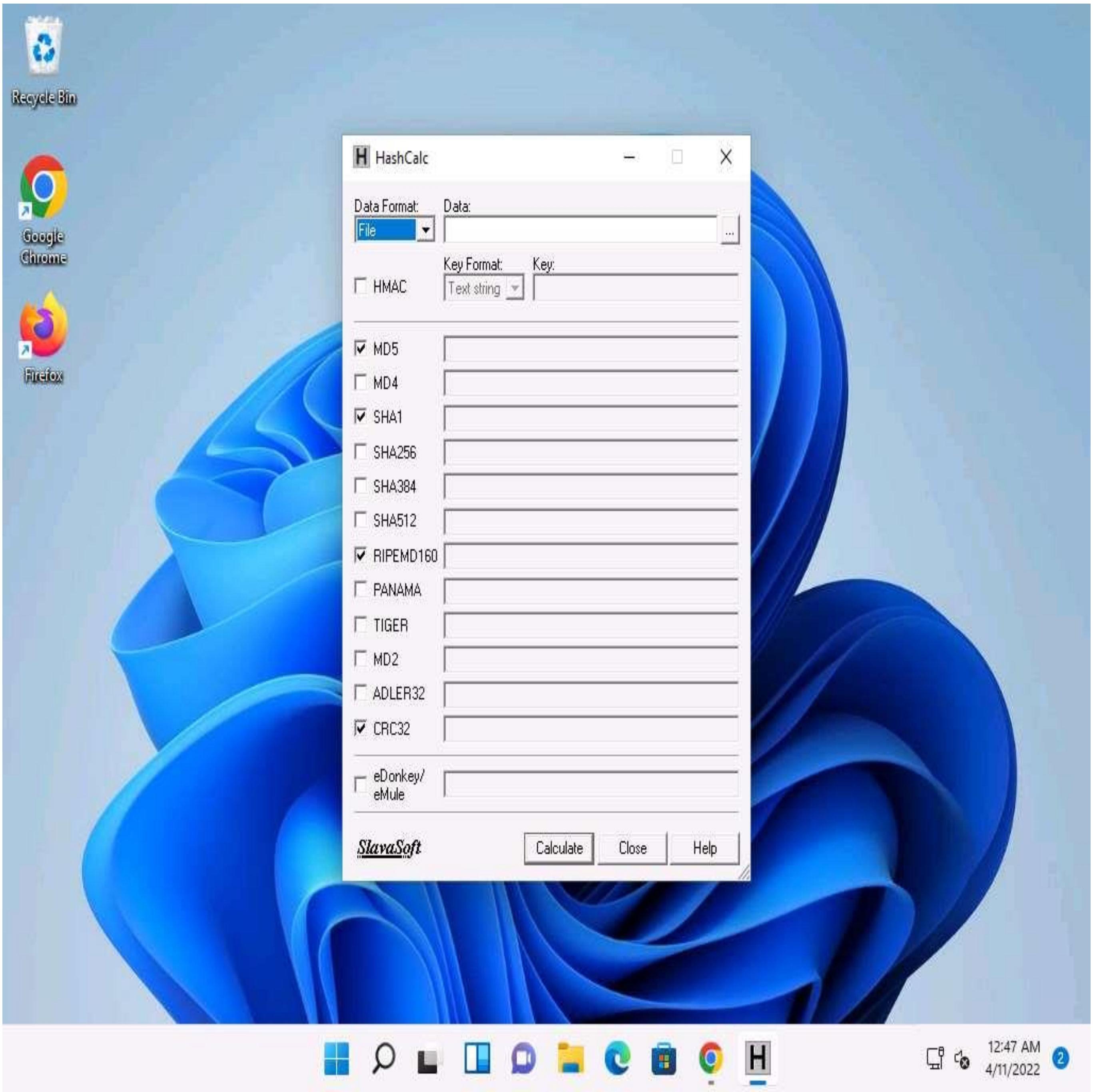
2. □ Click **Search** icon (🔍) on the **Desktop**. Type **HashCalc** in the search field, the **HashCalc** appears in the results, click **Open** to launch it.

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



HashCalc

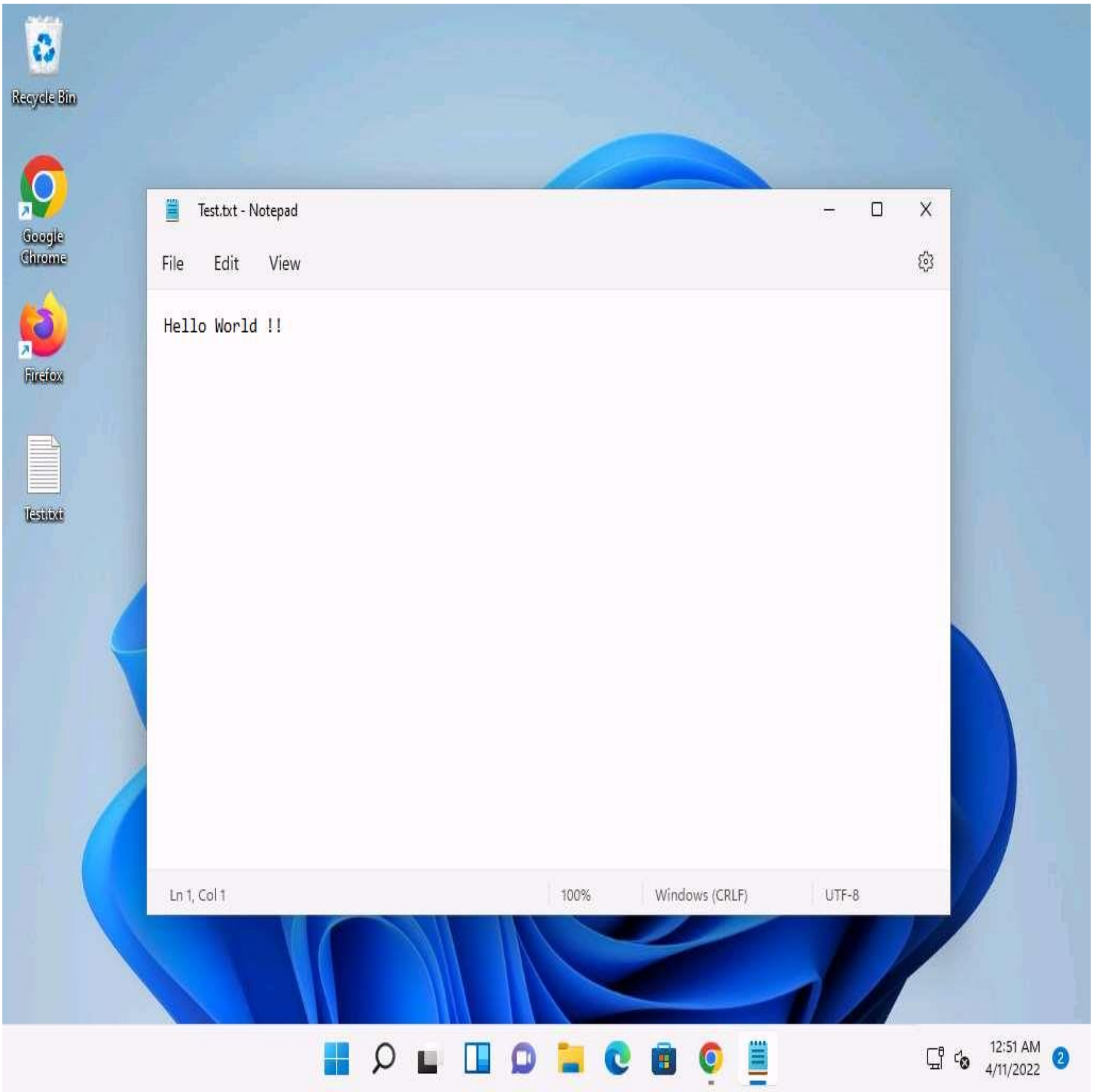
3. □ The **HashCalc** main window appears, as shown in the screenshot.



4. □ 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.

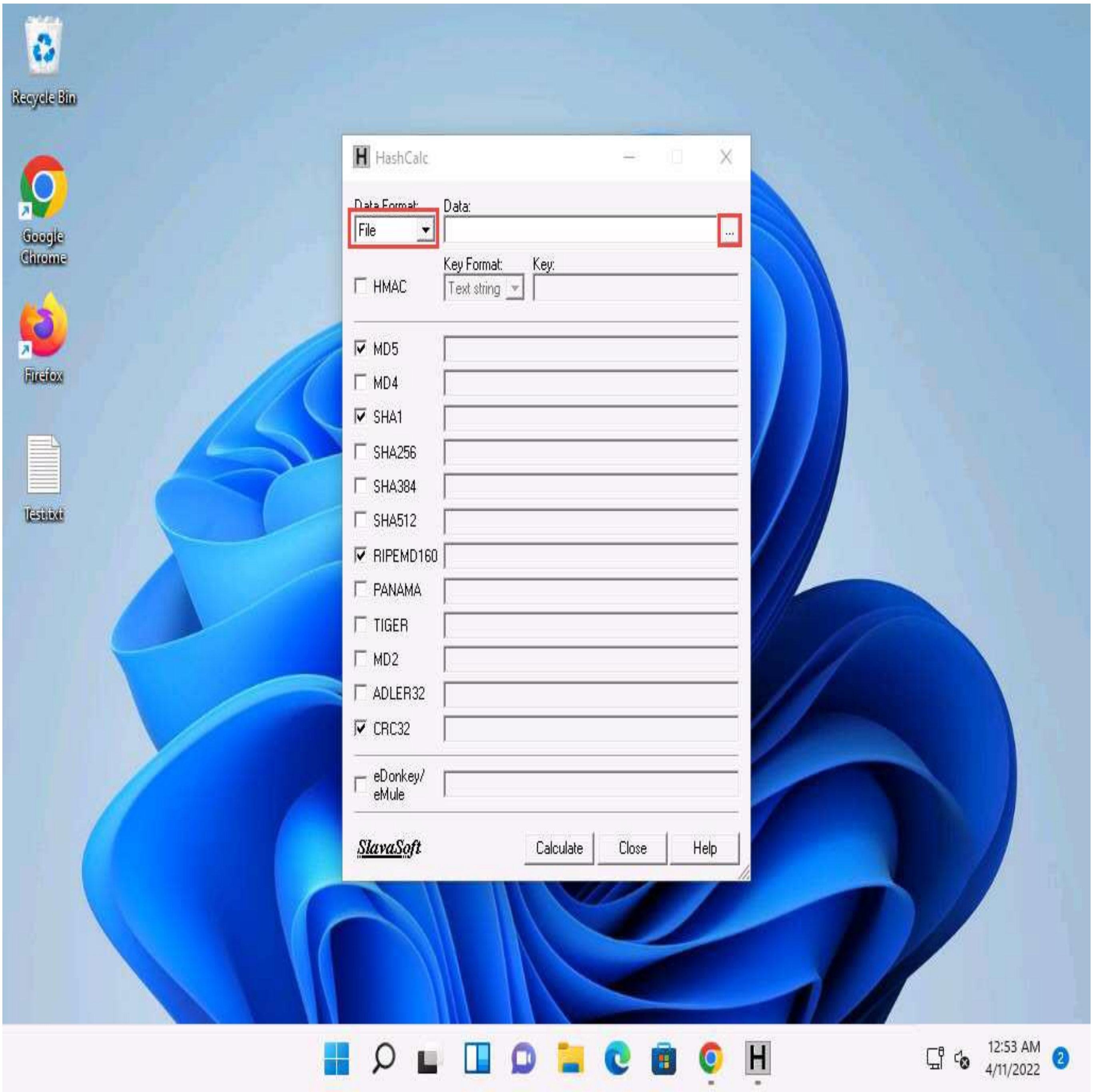
   You can create a text file at any location of your choice.

5. □ 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.



```
Hello World !!
```

6. □ 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.



HashCalc

Data Format: File

Data:

☐ HMAC Key Format: Text string Key:

☑ MD5

☐ MD4

☑ SHA1

☐ SHA256

☐ SHA384

☐ SHA512

☑ RIPEMD160

☐ PANAMA

☐ TIGER

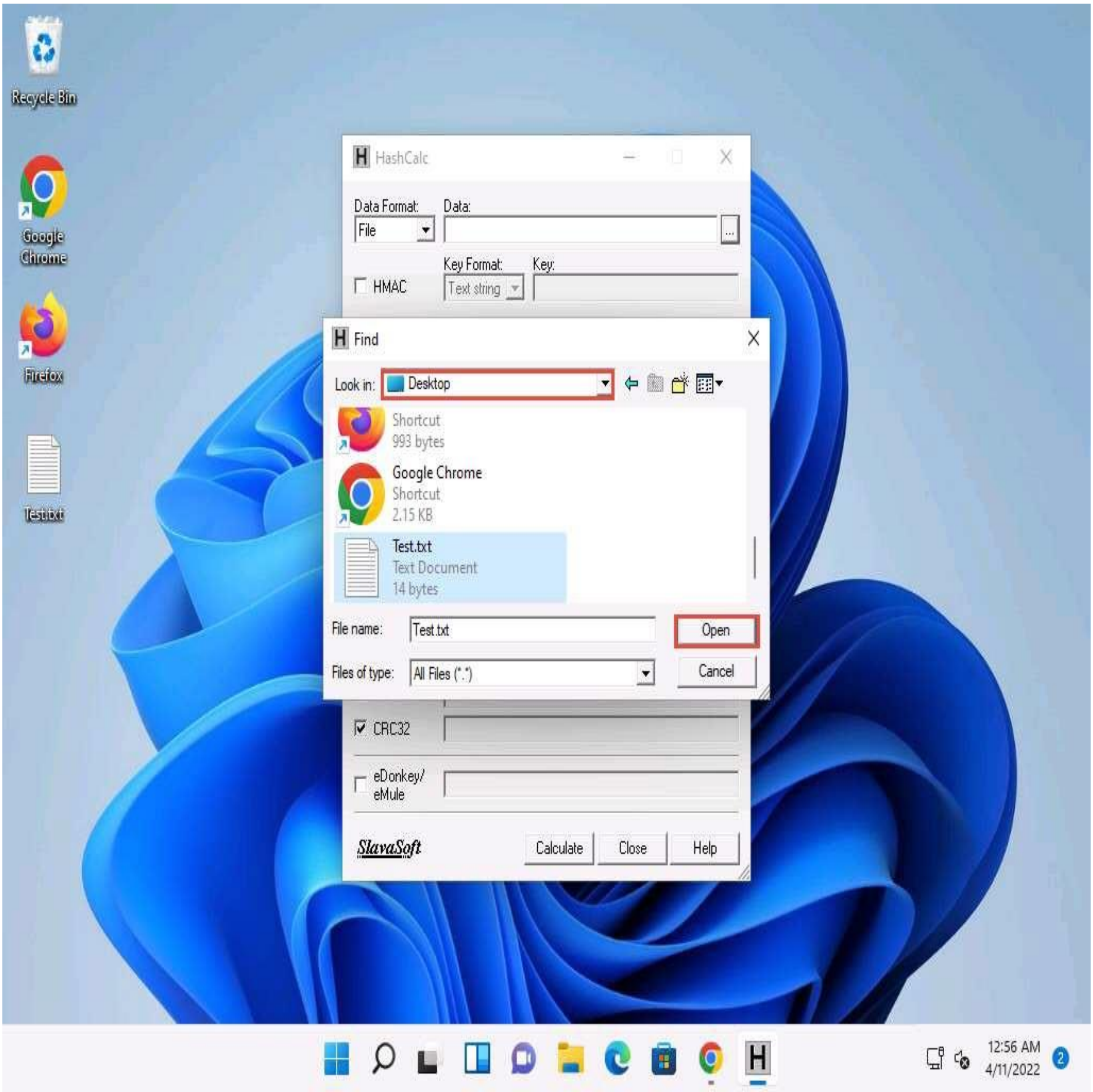
☐ MD2

☐ ADLER32

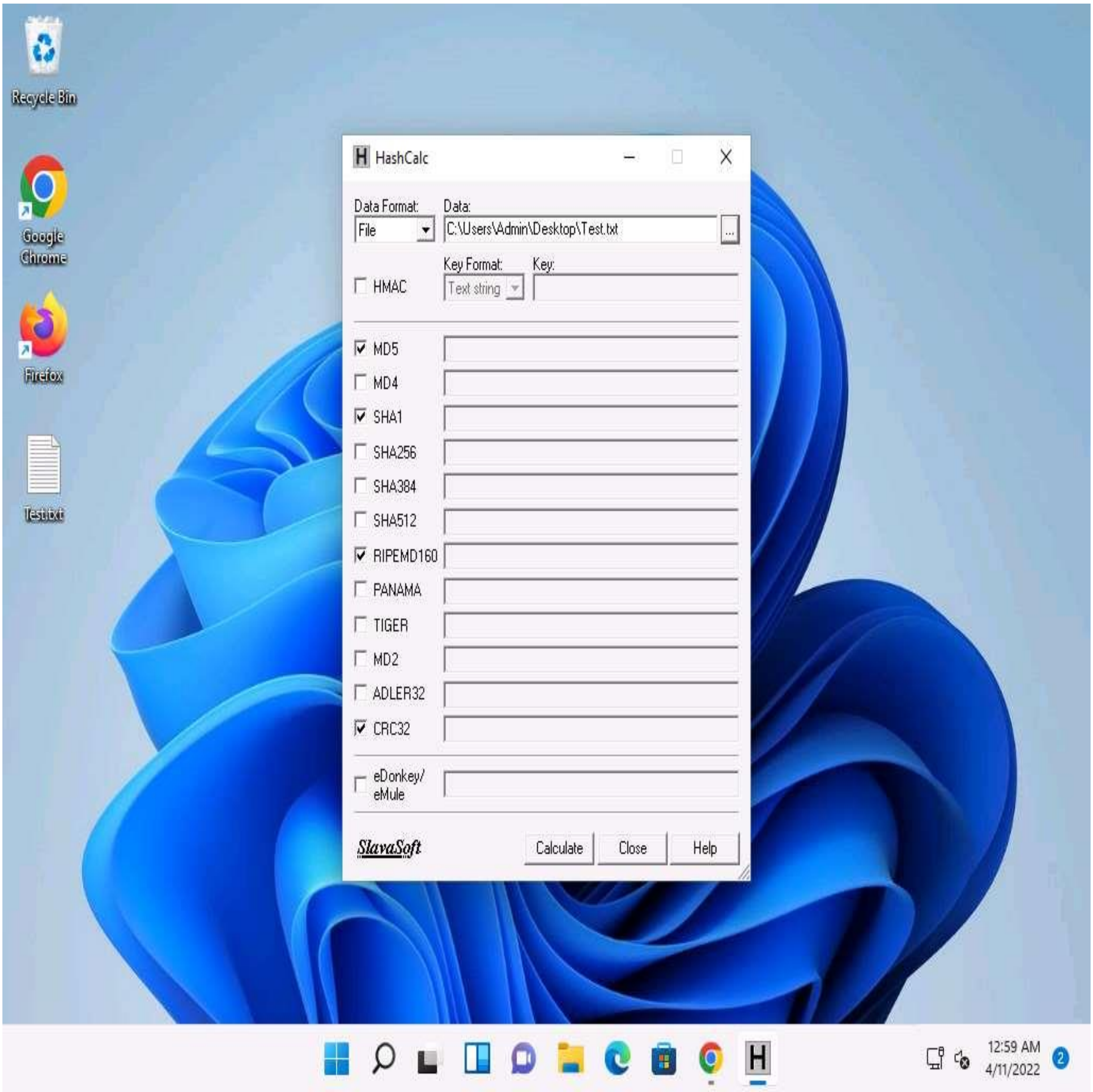
☑ CRC32

☐ eDonkey/ eMule

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



8. □ 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.



Data Format: File

Data: C:\Users\Admin\Desktop\Test.txt

□ HMAC Key Format: Text string Key:

☑ MD5

□ MD4

☑ SHA1

□ SHA256

□ SHA384

□ SHA512

☑ RIPEMD160

□ PANAMA

□ TIGER

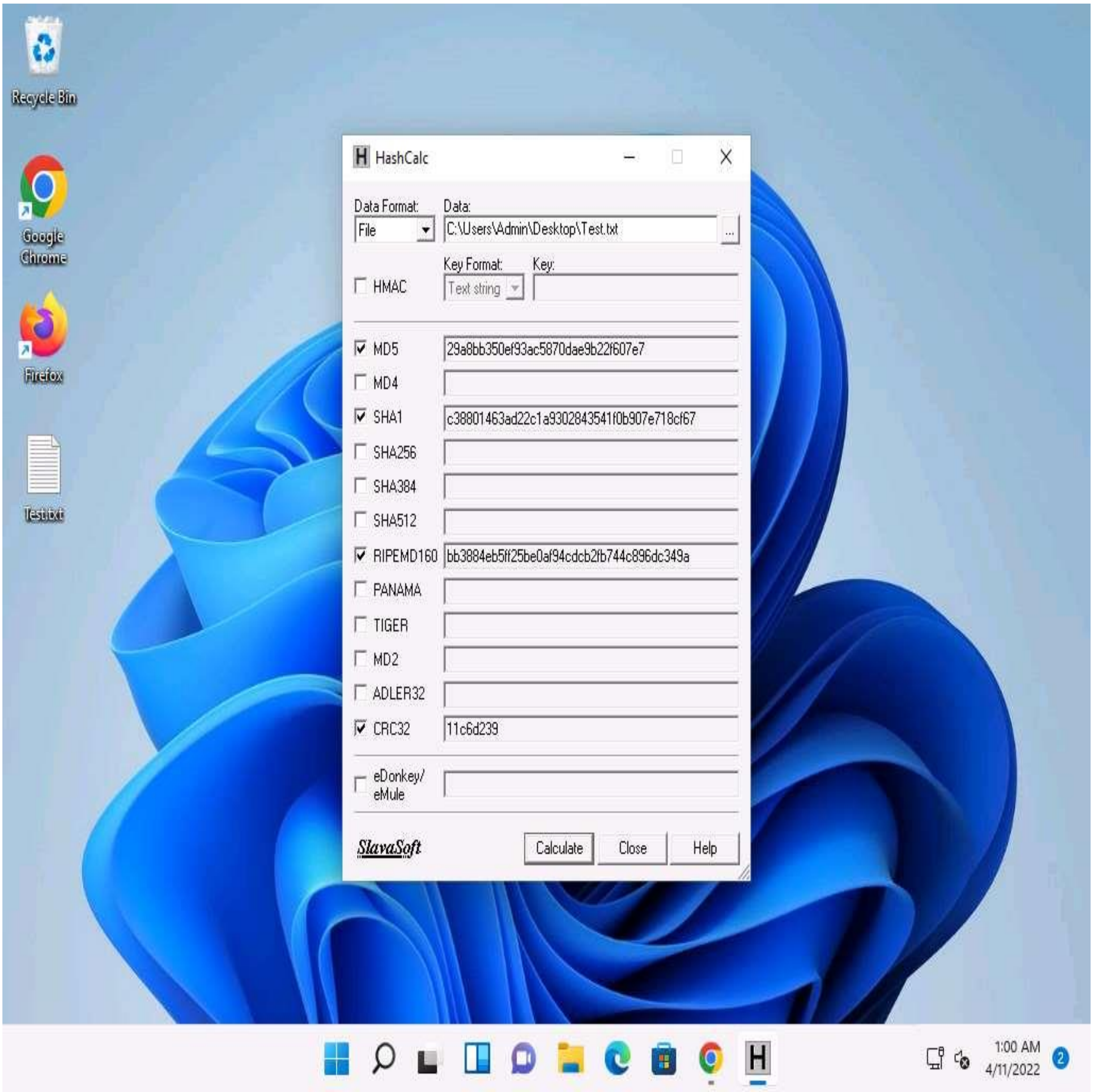
□ MD2

□ ADLER32

☑ CRC32

□ eDonkey/ eMule

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



Data Format: File

Data: C:\Users\Admin\Desktop\Test.txt

□ HMAC Key Format: Text string Key:

☑ MD5 29a8bb350ef93ac5870dae9b22f607e7

□ MD4

☑ SHA1 c38801463ad22c1a9302843541f0b907e718cf67

□ SHA256

□ SHA384

□ SHA512

☑ RIPEMD160 bb3884eb5ff25be0af94cdcb2fb744c896dc349a

□ PANAMA

□ TIGER

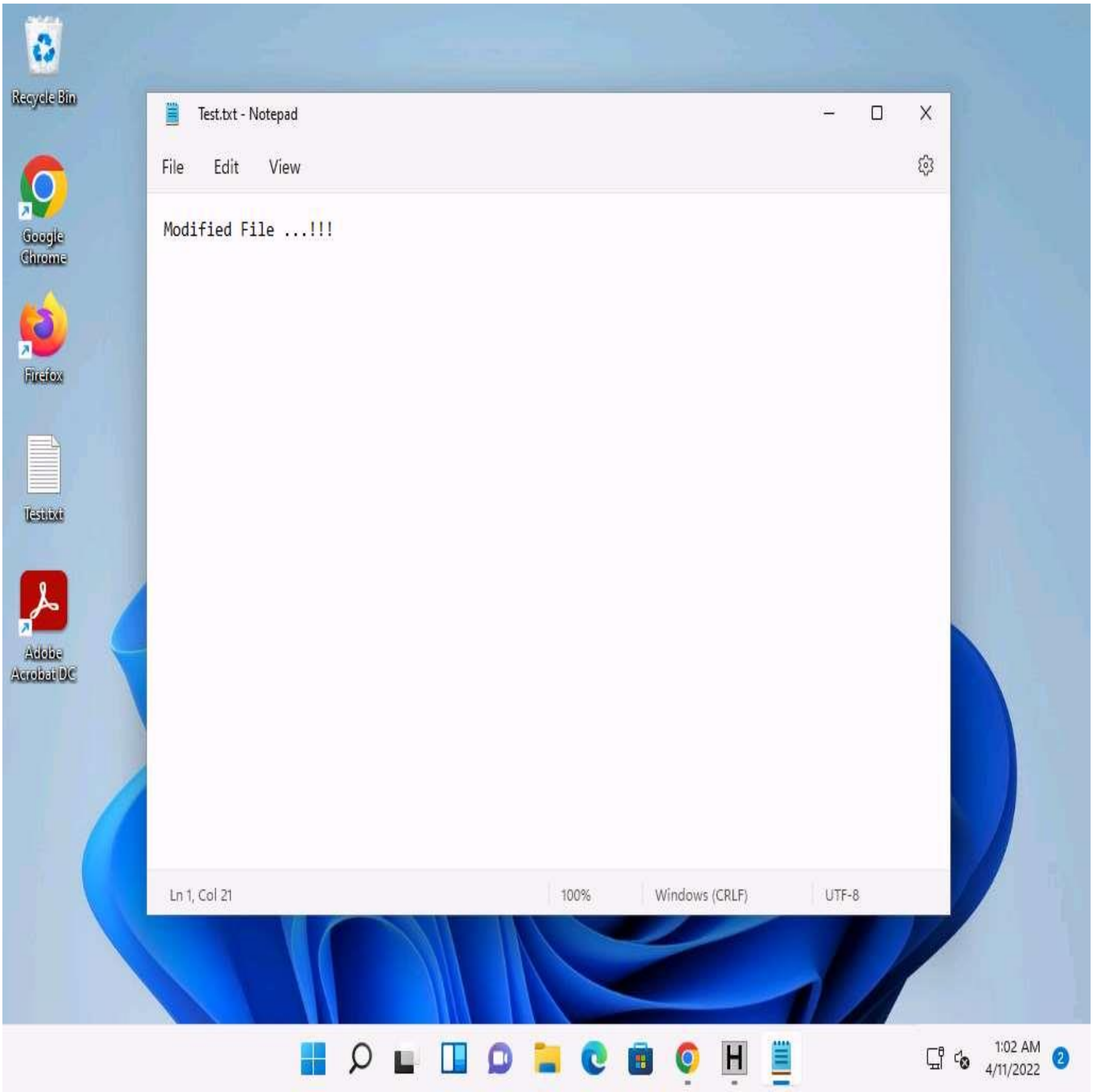
□ MD2

□ ADLER32

☑ CRC32 11c6d239

□ eDonkey/ eMule

10. □ 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.

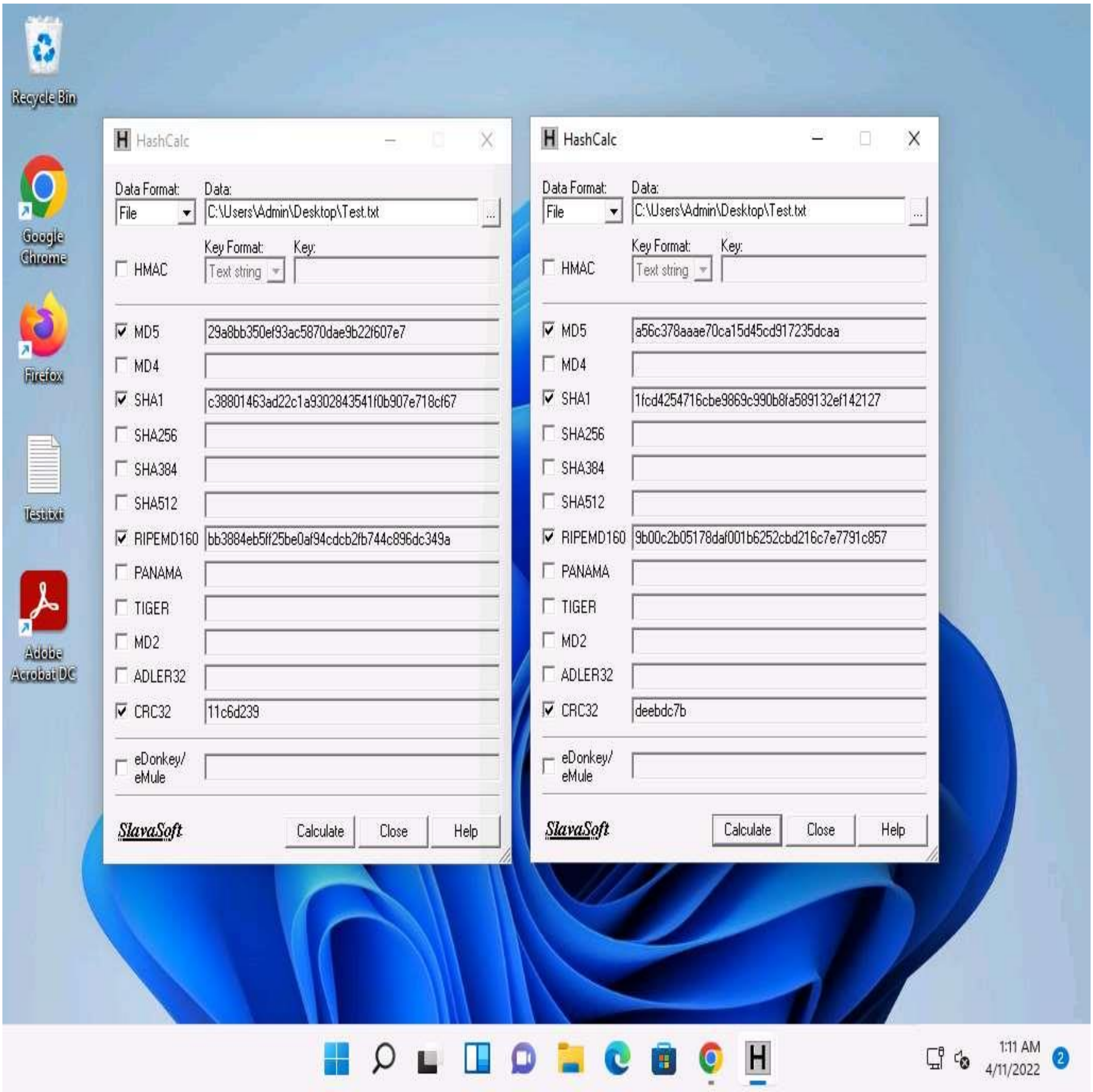


Modified File ...!!!

11. □ Click **Search** icon (🔍) on the **Desktop**. Type **HashCalc** in the search field, the **HashCalc** appears in the results, click **Open** to launch it.

12. □ A new **HashCalc** window appears, perform **Steps #6-9**

13. □ 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.



HashCalc

Data Format: File
Data: C:\Users\Admin\Desktop\Test.txt
☐ HMAC Key Format: Text string Key:
☑ MD5 29a8bb350ef93ac5870dae9b22f607e7
☐ MD4
☑ SHA1 c38801463ad22c1a9302843541f0b907e718cf67
☐ SHA256
☐ SHA384
☐ SHA512
☑ RIPEMD160 bb3884eb5ff25be0af94cdcb2fb744c896dc349a
☐ PANAMA
☐ TIGER
☐ MD2
☐ ADLER32
☑ CRC32 11c6d239
☐ eDonkey/eMule

HashCalc

Data Format: File
Data: C:\Users\Admin\Desktop\Test.txt
☐ HMAC Key Format: Text string Key:
☑ MD5 a56c378aaae70ca15d45cd917235dcaa
☐ MD4
☑ SHA1 1fcd4254716cbe9869c990b8fa589132ef142127
☐ SHA256
☐ SHA384
☐ SHA512
☑ RIPEMD160 9b00c2b05178daf001b6252cbd216c7e7791c857
☐ PANAMA
☐ TIGER
☐ MD2
☐ ADLER32
☑ CRC32 deebdc7b
☐ eDonkey/eMule

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.

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

Task 2: Calculate MD5 Hashes using MD5 Calculator

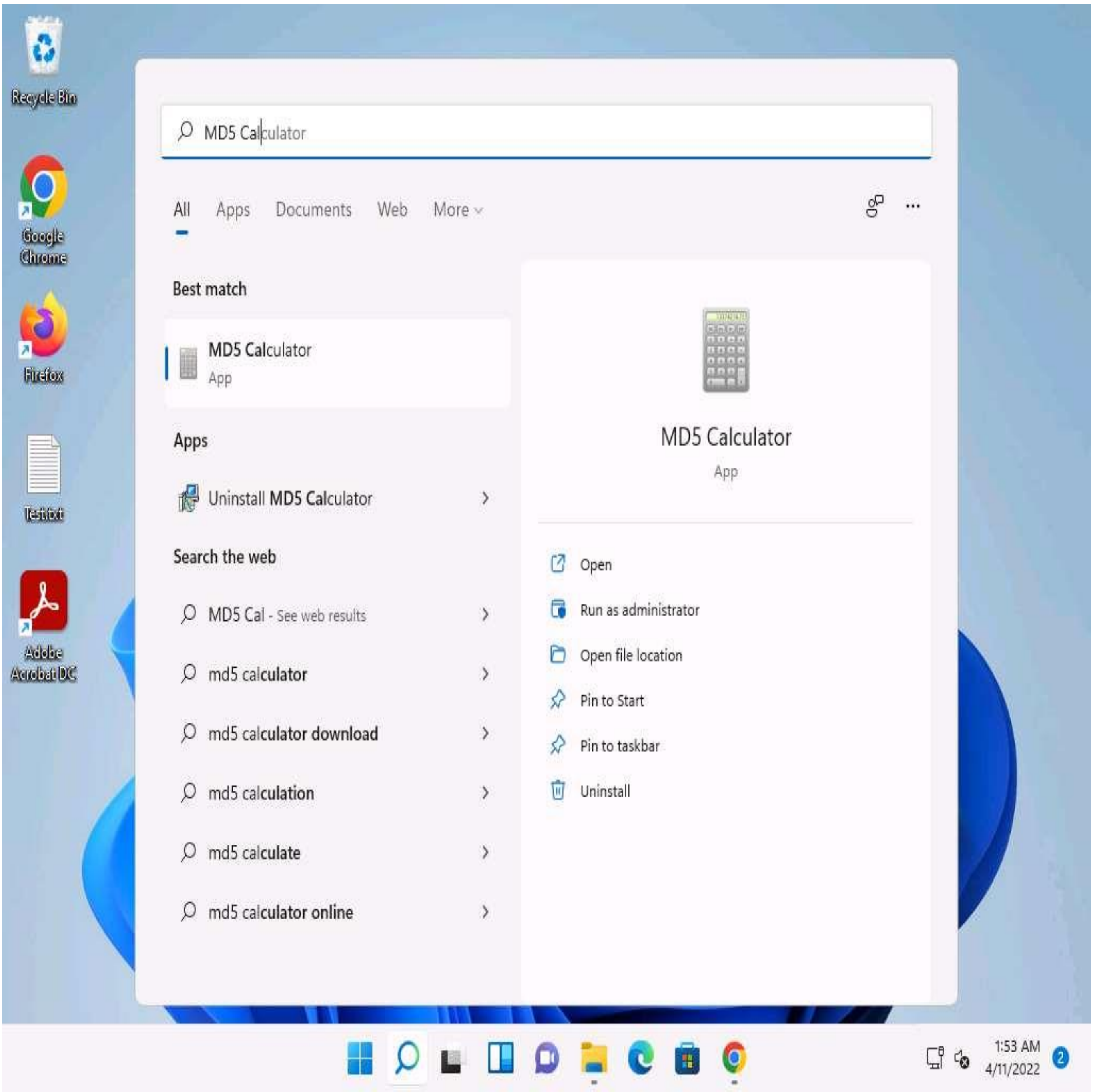
MD2, MD4, MD5, and MD6 are message digest algorithms used in digital signature applications to compress documents securely before the system signs it with a private key. The algorithms can be of variable length, but the resulting message digest is always 128 bits.

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.

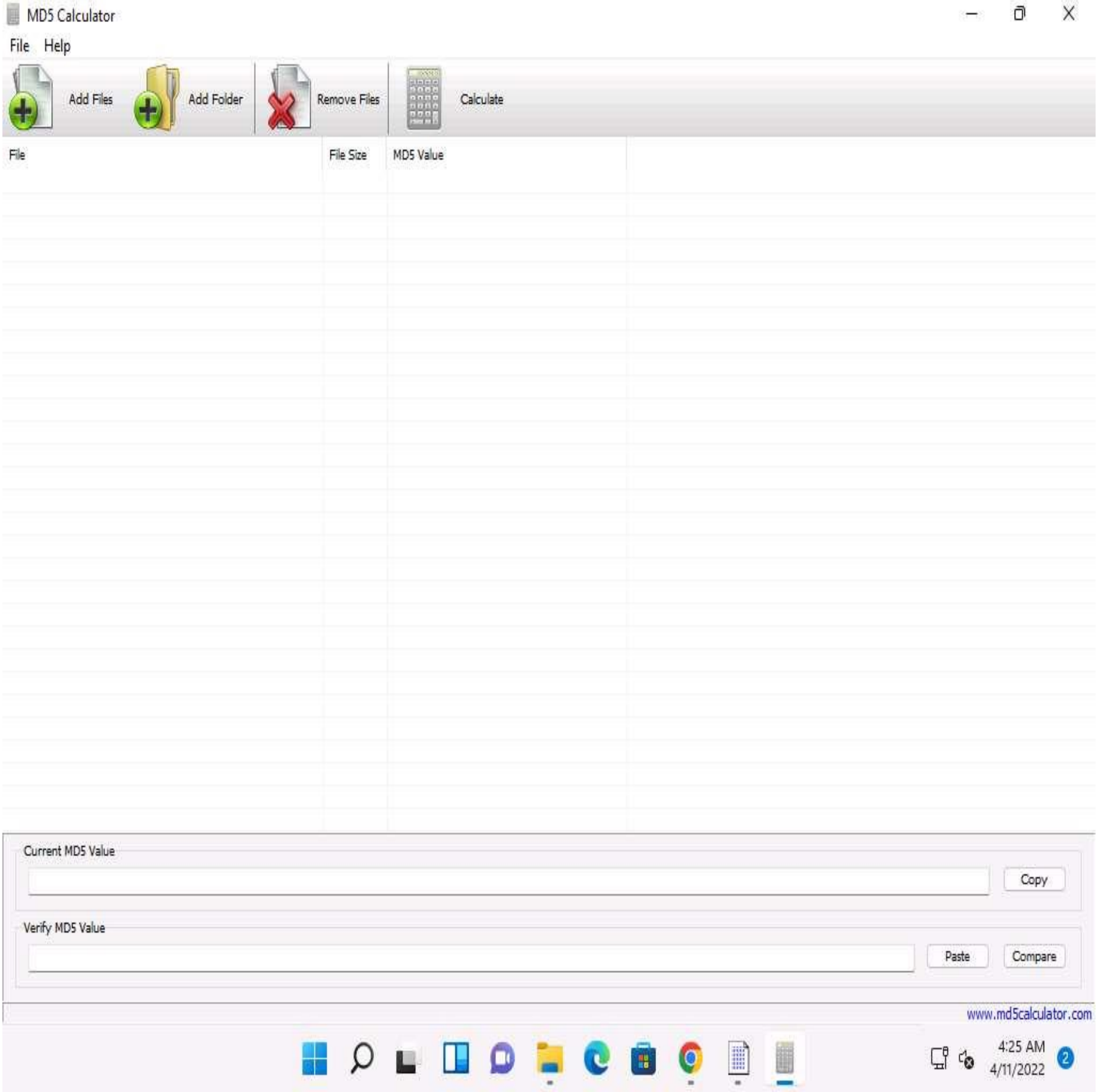
Here, we will use the MD5 Calculator tool to calculate MD5 hashes.

1. □ Click **Search** icon (🔍) on the **Desktop**. Type **MD5 Cal** in the search field, the **MD5 Calculator** appears in the results, click **Open** to launch it.

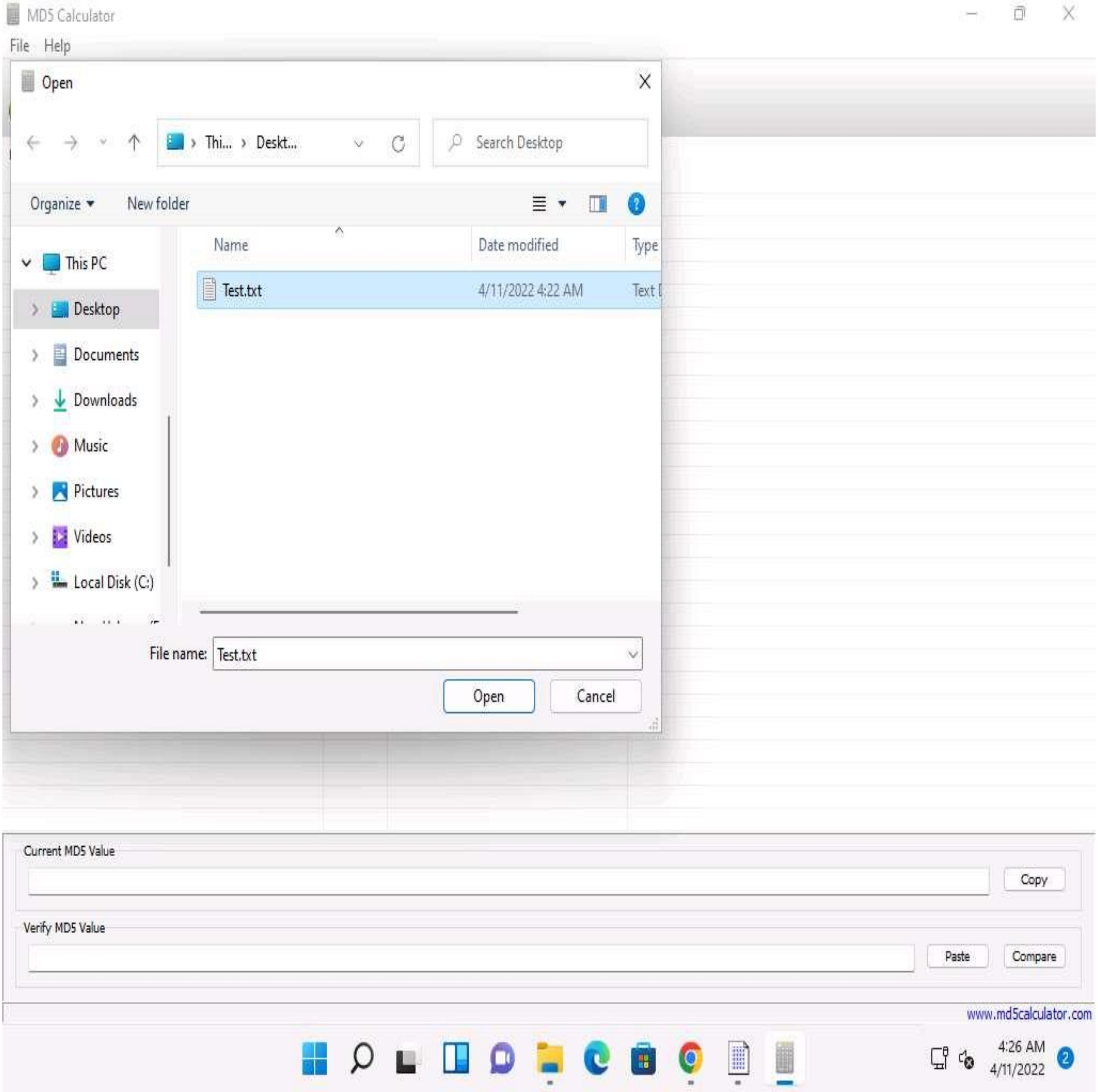


MD5 Calculator

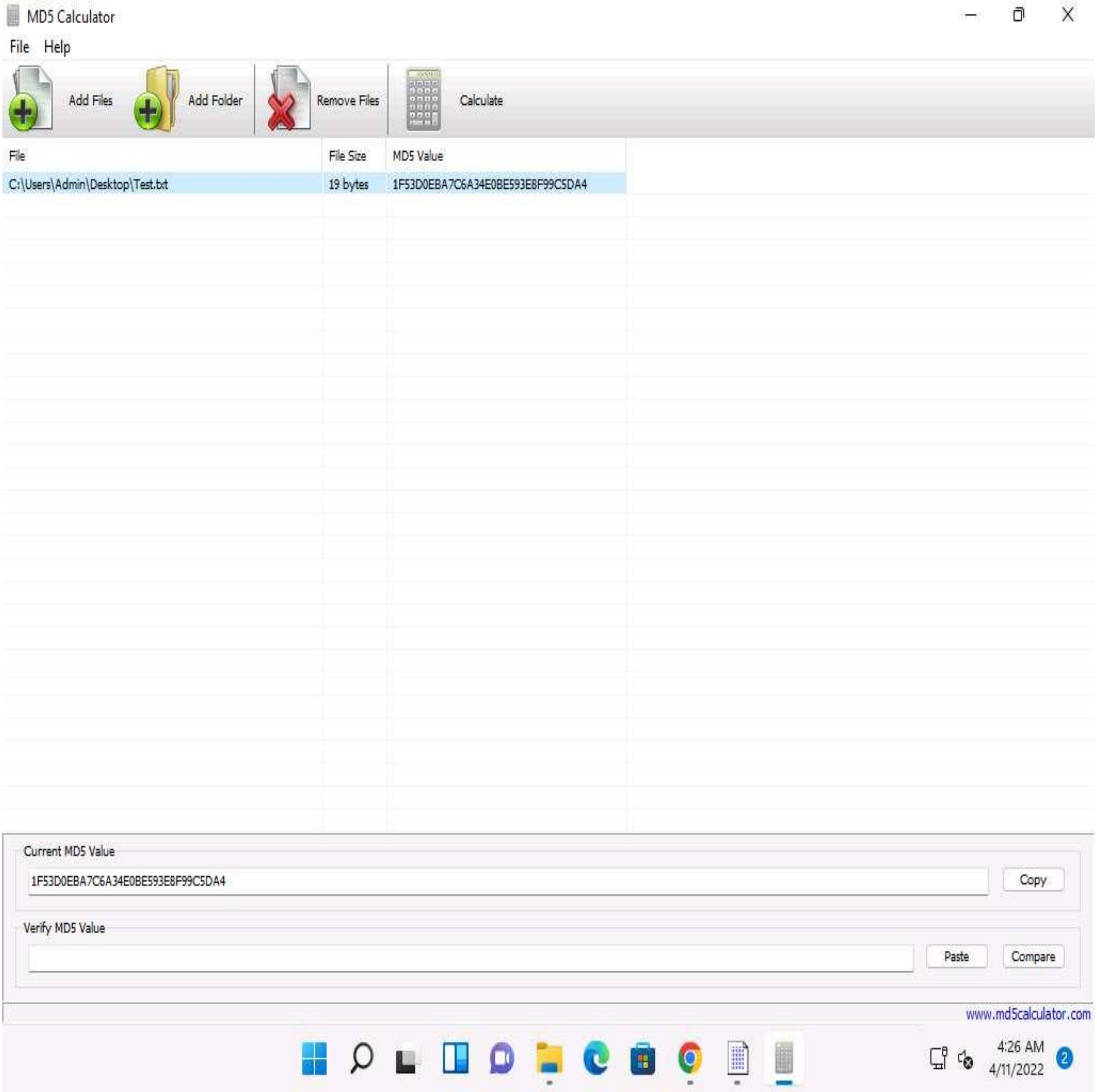
2. □ The **MD5 Calculator** main window appears, as shown in the screenshot.



3. □ Click on **Add Files** in **MD5 Calculator** window.
4. □ In the **Open** window, navigate to the Desktop and select **Test.txt** file and click **Open**.



5. □ You can observe the uploaded file path under **File** section, click on **Calculate** to get the hash value in **Current MD5 value** field at the bottom of the window.



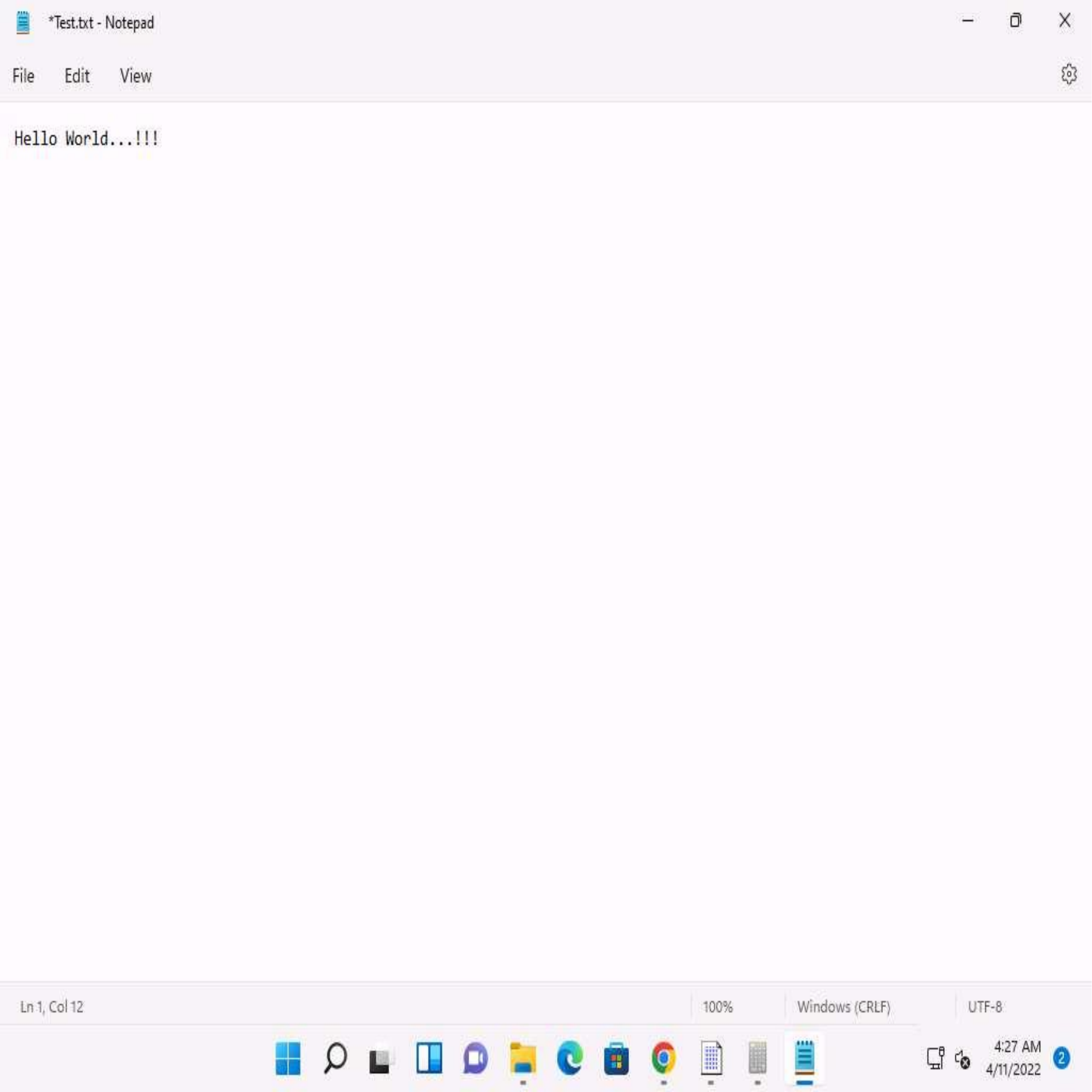
File	File Size	MD5 Value
C:\Users\Admin\Desktop\Test.txt	19 bytes	1F53D0EBA7C6A34E0BE593E8F99C5DA4

Current MD5 Value

1F53D0EBA7C6A34E0BE593E8F99C5DA4

Verify MD5 Value

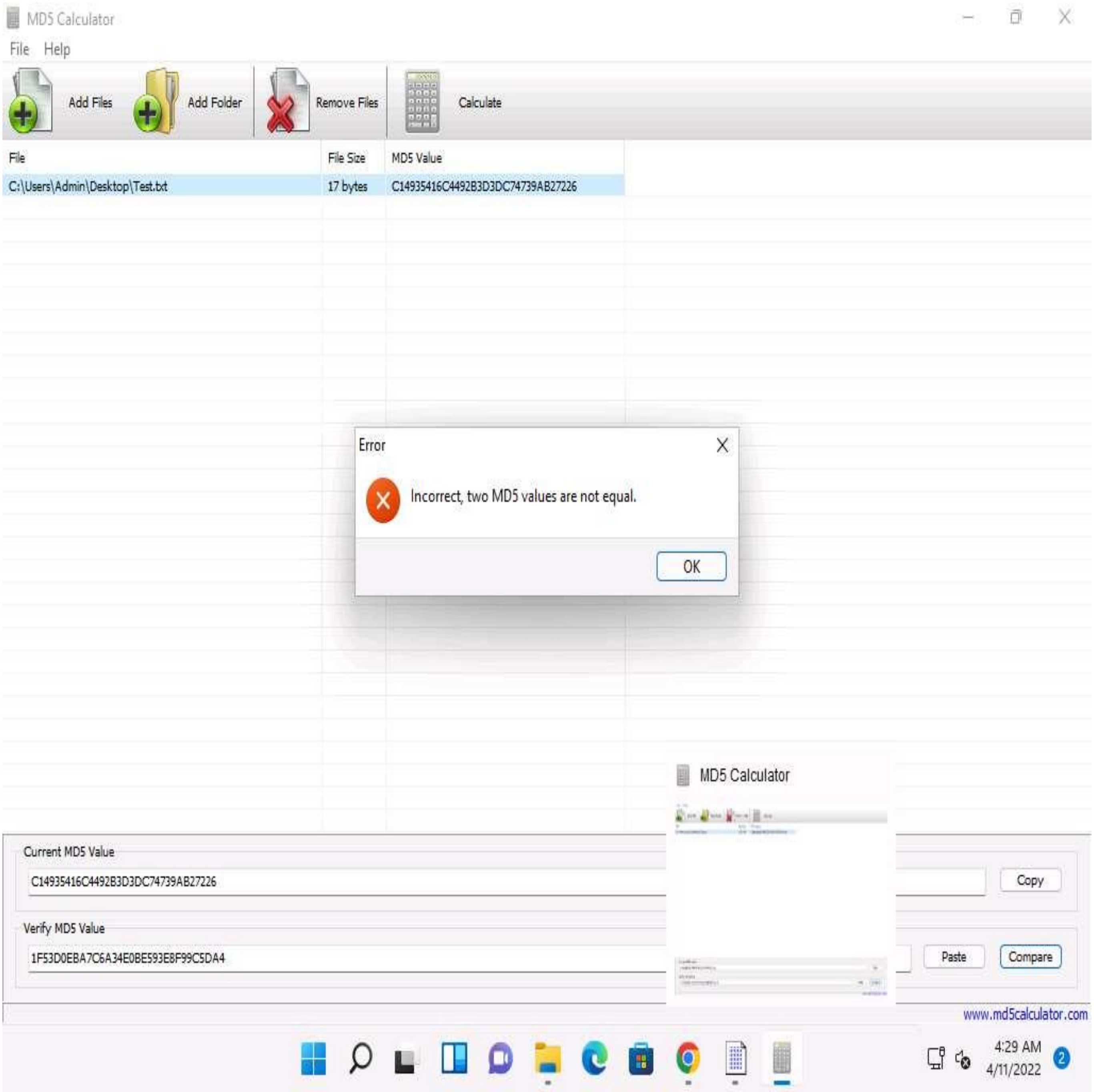
6. □ Now, click on **Copy** beside the MD5 value, to copy the hash value from **Current MD5 Value** field and click on **Remove Files** to clear the MD5 value.
7. □ Now, double-click the **Test.txt** file from **Desktop** to open it and change the content of the file by modifying text within (here, **Hello World...!!!**). Save and close the **Test.txt** file.



```
Hello World...!!!
```

8. □ In **MD5 Calculator** perform **Steps #2-5**.

9. □ Now, paste the previous hash value in the **Verify MD5 Value** field and click on **Compare** to compare the MD5 values.



File	File Size	MD5 Value
C:\Users\Admin\Desktop\Test.txt	17 bytes	C14935416C4492B3D3DC74739AB27226

Error

Incorrect, two MD5 values are not equal.

Current MD5 Value: C14935416C4492B3D3DC74739AB27226

Verify MD5 Value: 1F53D0EBA7C6A34E0BE593E8F99C5DA4

10. □ We can see that the MD5 hash values of the file before modification is not equal to the MD5 hash value of the file after modification.

    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.

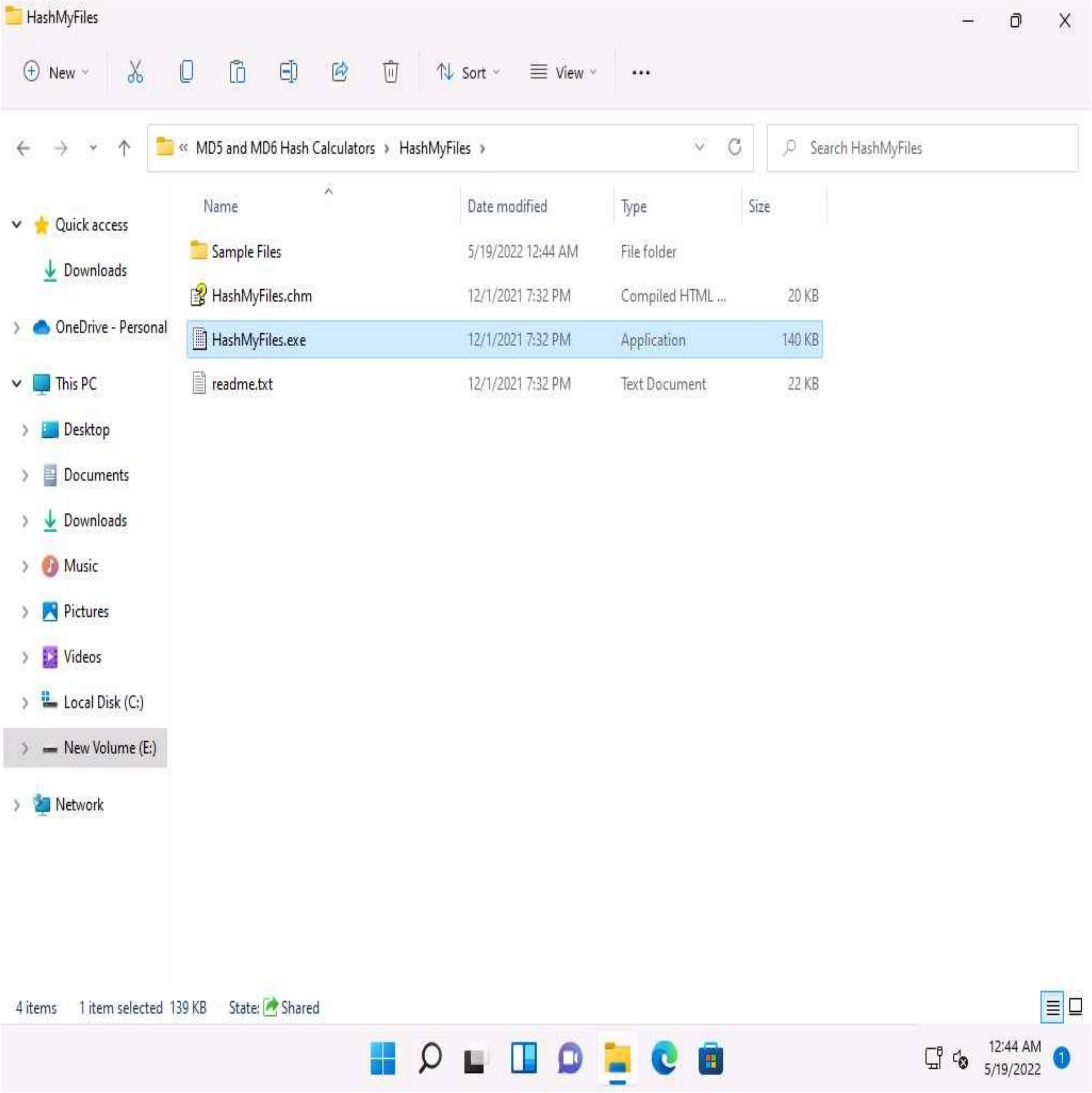
11. □ This concludes the demonstration of calculating MD5 hashes using MD5 Calculator.
12. □ Close all open windows and document all the acquired information.

Task 3: Calculate MD5 Hashes using HashMyFiles

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.

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

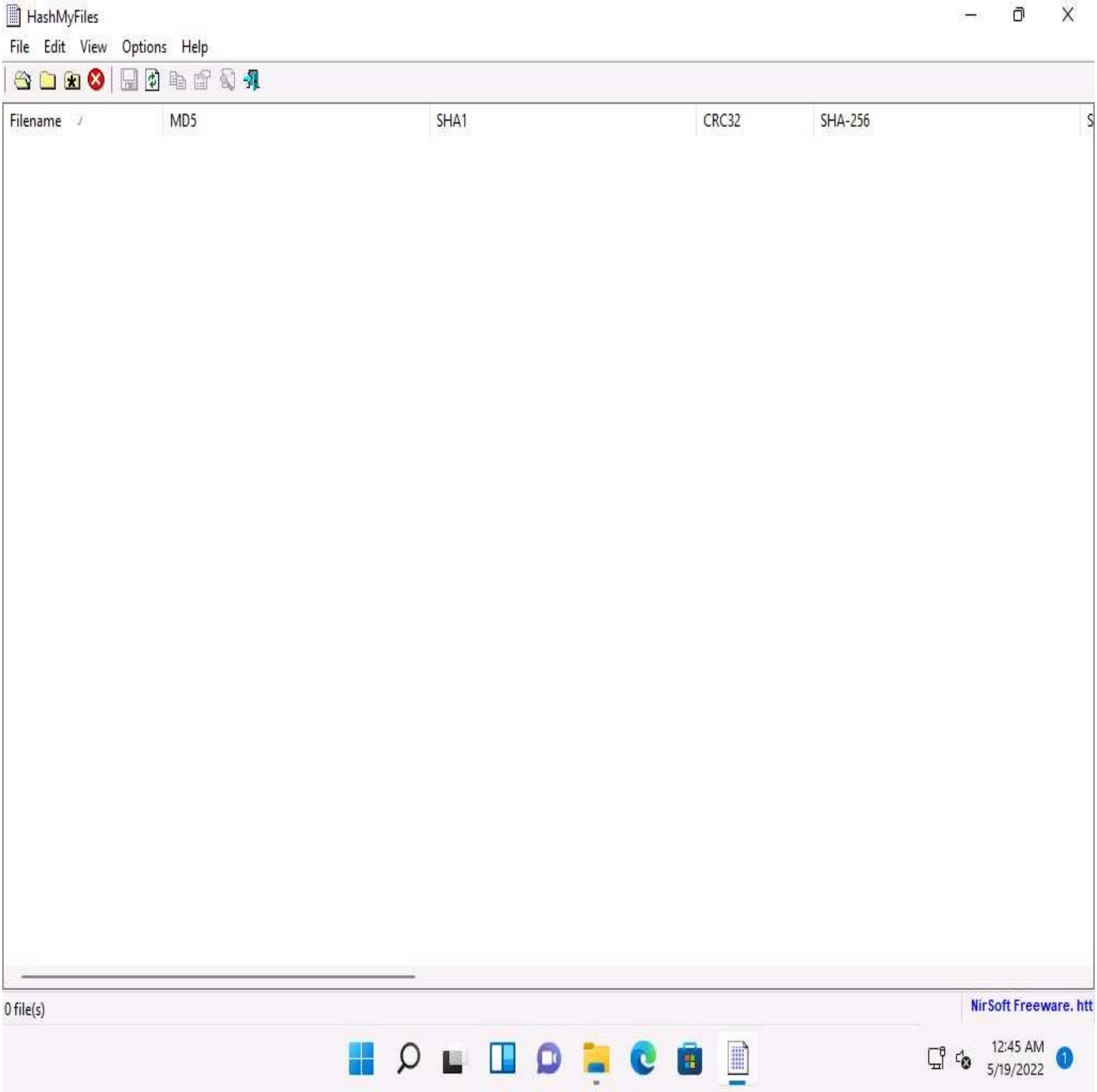
1. □ In **Windows 11** machine navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles** and double click **HashMyFiles.exe**.



Name	Date modified	Type	Size
Sample Files	5/19/2022 12:44 AM	File folder	
HashMyFiles.chm	12/1/2021 7:32 PM	Compiled HTML ...	20 KB
HashMyFiles.exe	12/1/2021 7:32 PM	Application	140 KB
readme.txt	12/1/2021 7:32 PM	Text Document	22 KB

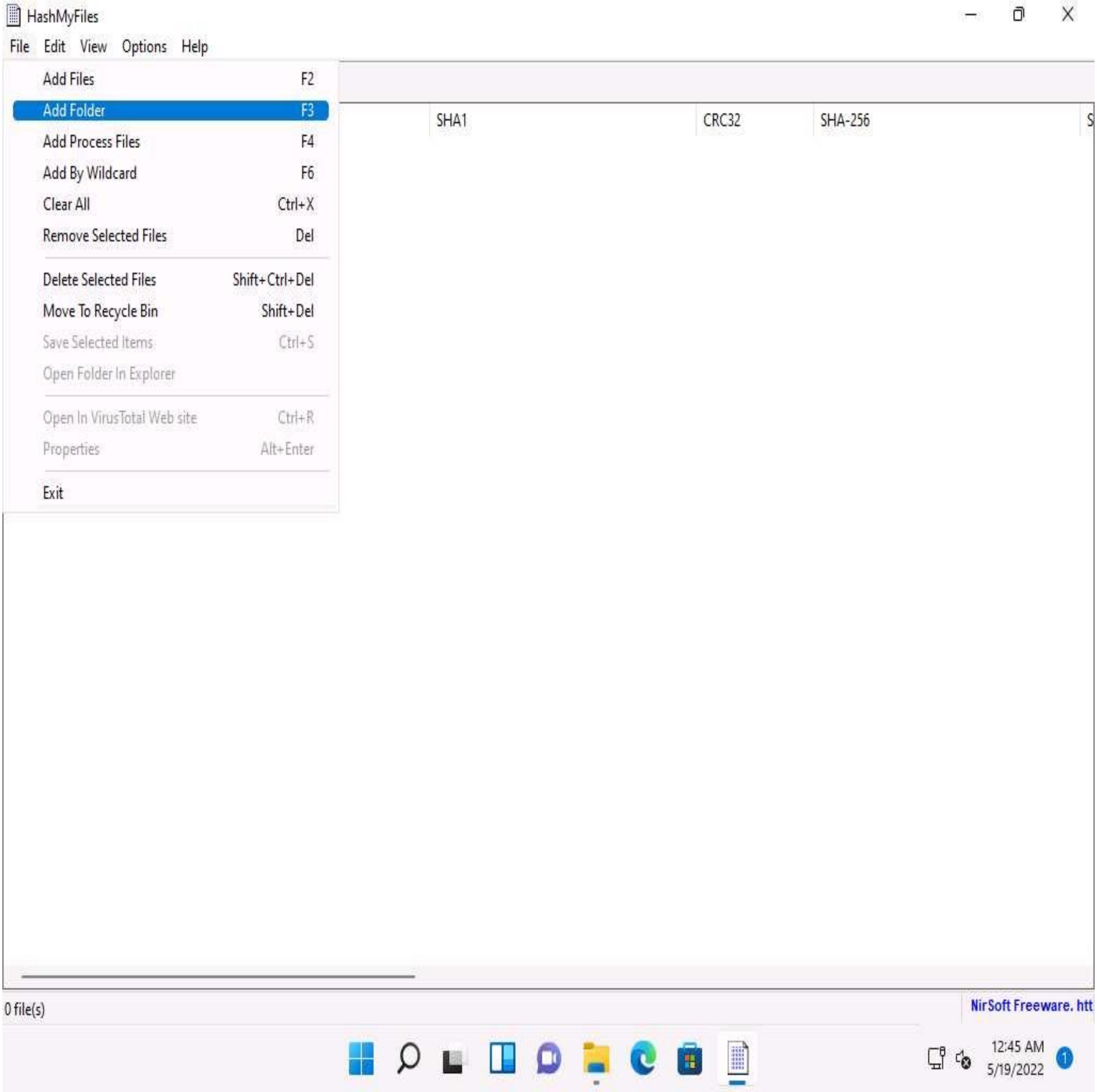
If the **Open File - Security Warning** pop-up appears, click **Run**.

2. □ The **HashMyFiles** main window appears, as shown in the screenshot.

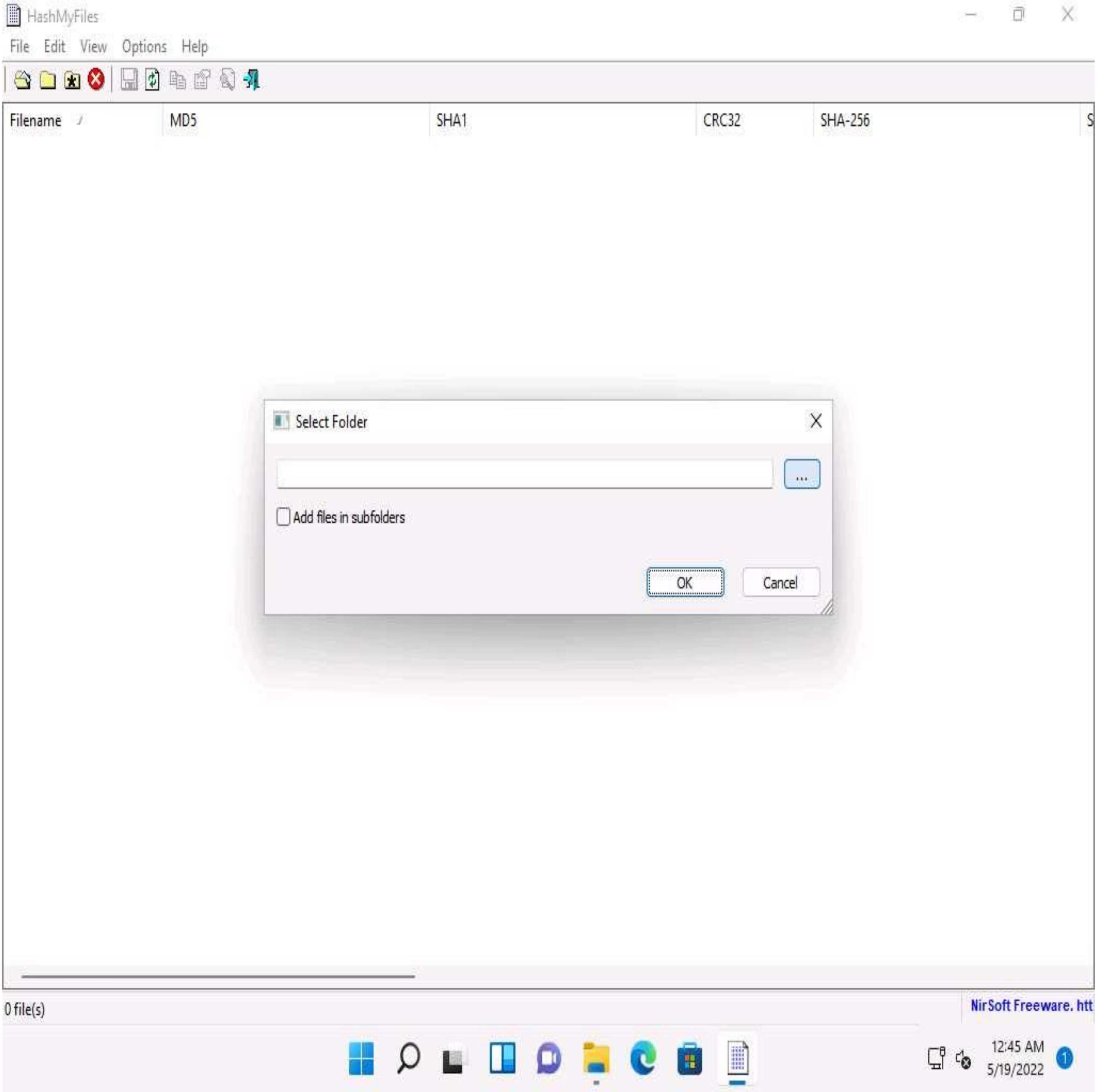


3. □ In the **HashMyFiles** window, click **File** from the menu bar. From the drop-down list, click the **Add Folder** option.

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

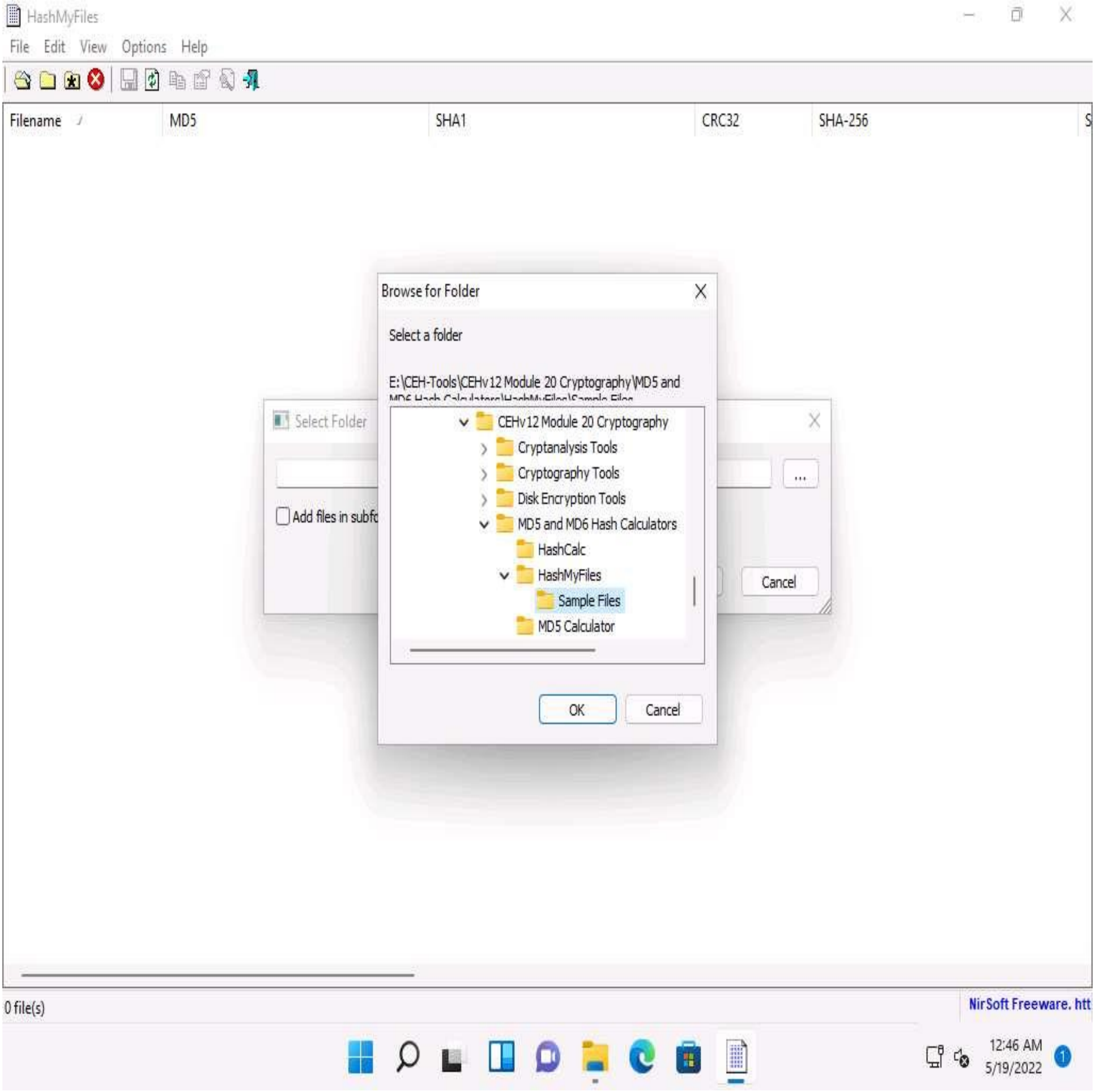


4. □ The **Select Folder** pop-up appears; click on the ellipsis icon to select the folder you want to encrypt.



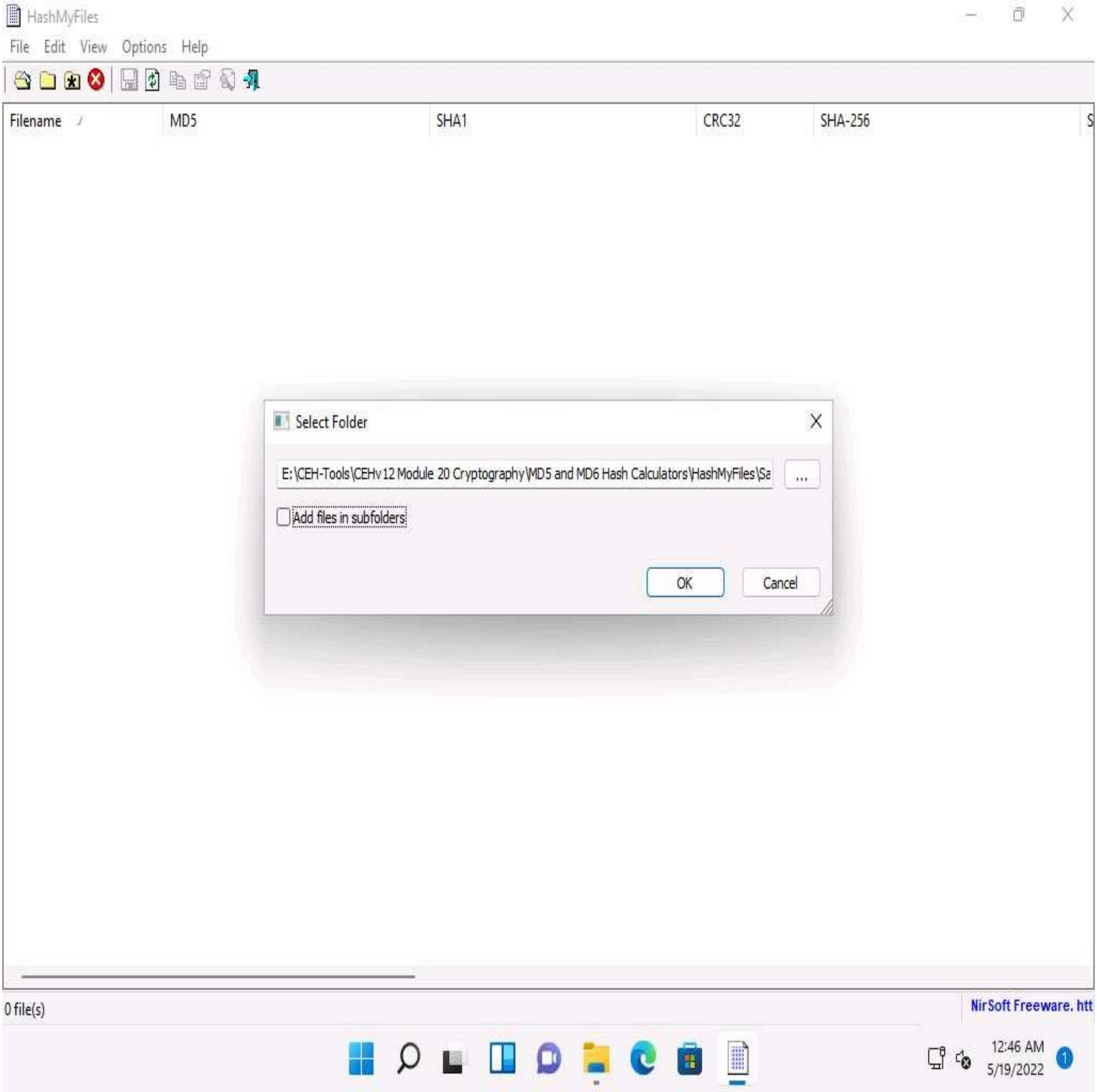
5. □ The **Browse for Folder** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles** and select the **Sample Files** folder; then, click **OK**.

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



E:\CEH-Tools\CEHv12 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles\Sample Files

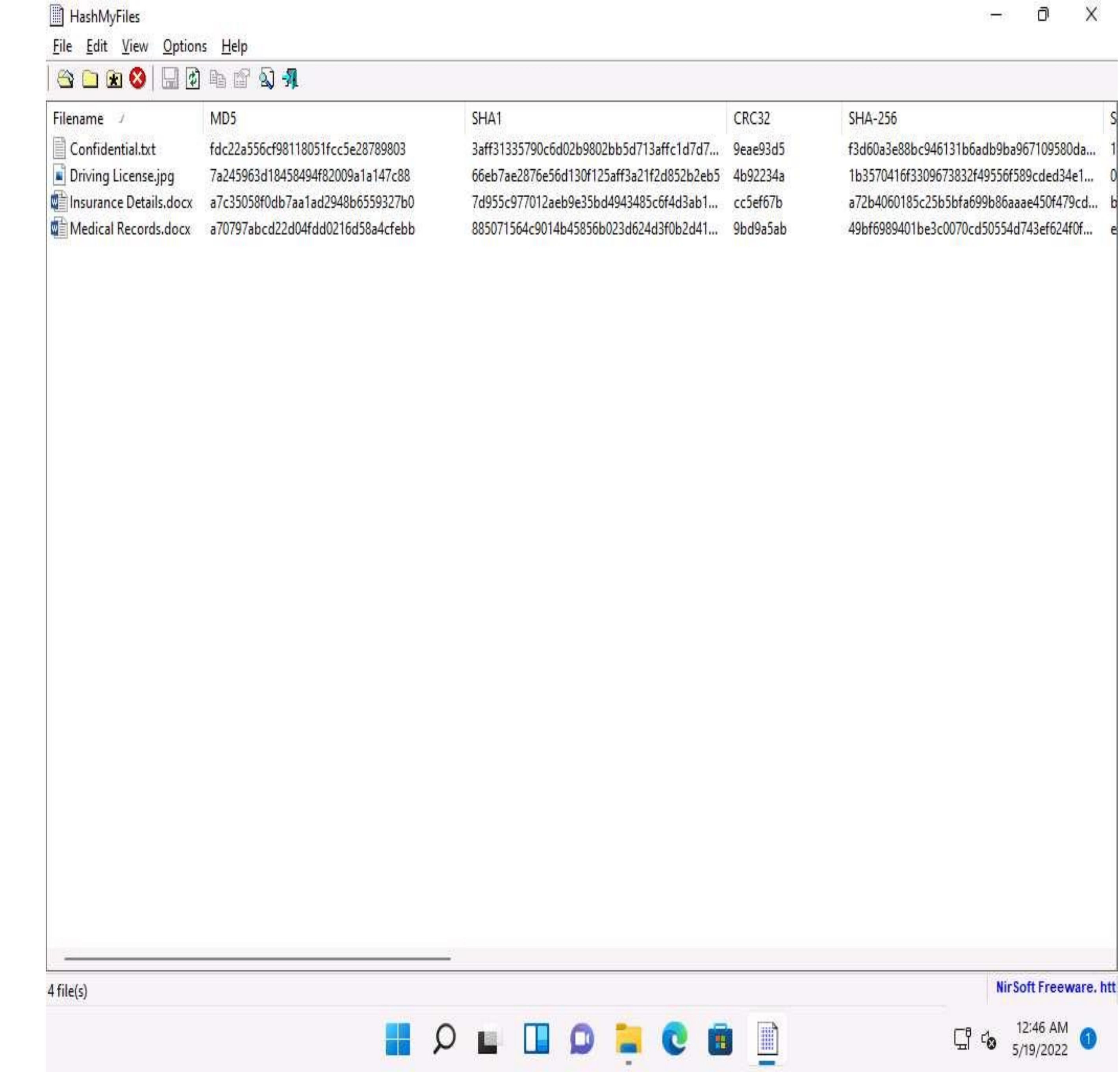
6. □ The location of the selected folder appears in the field; click **OK**.



E:\CEH-Tools\CEHv12 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles\Sa

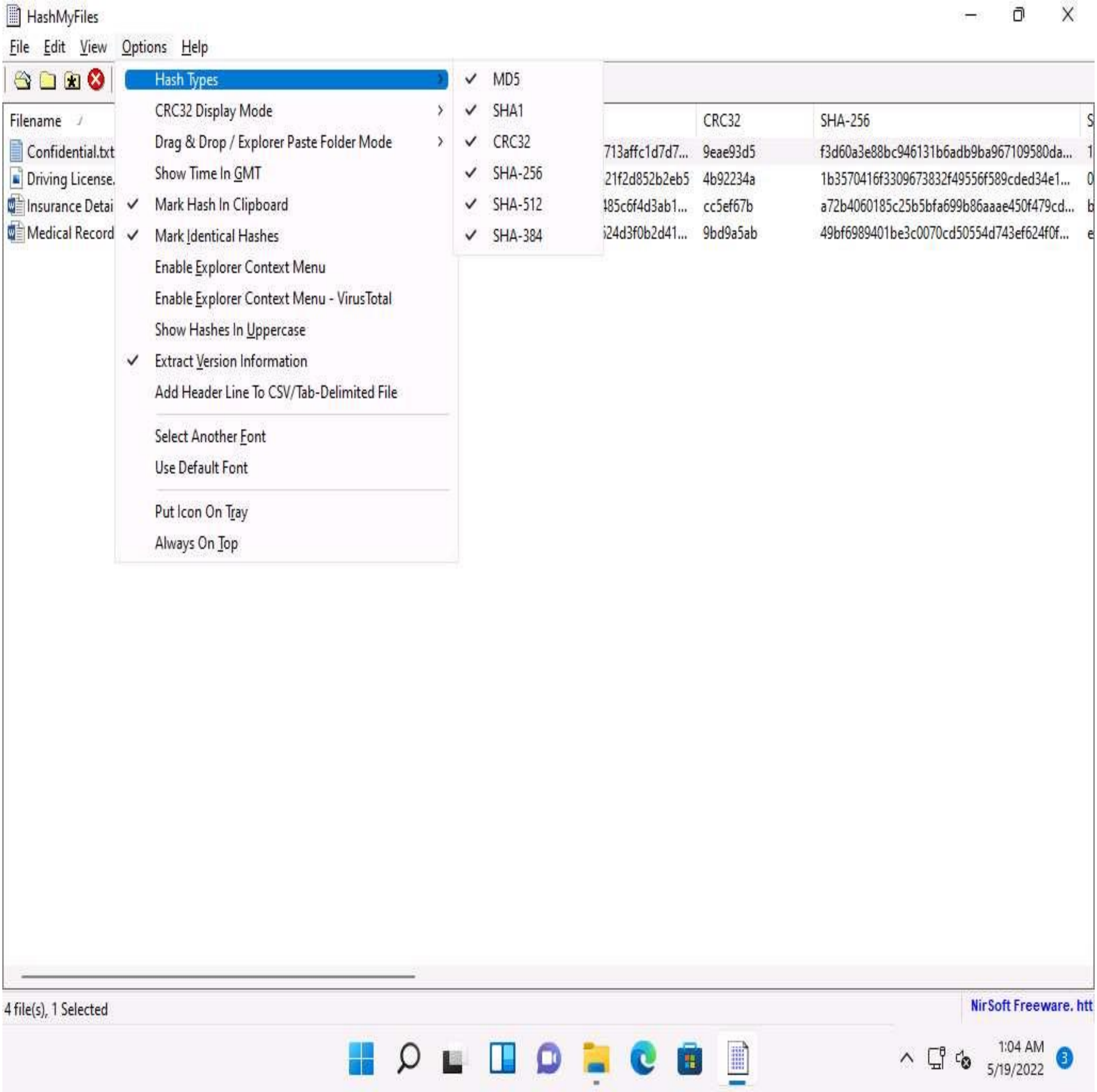
□ Add files in subfolders

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



Filename	MD5	SHA1	CRC32	SHA-256	S
Confidential.txt	fdc22a556cf98118051fcc5e28789803	3aff31335790c6d02b9802bb5d713affc1d7d7...	9eae93d5	f3d60a3e88bc946131b6adb9ba967109580da...	1
Driving License.jpg	7a245963d18458494f82009a1a147c88	66eb7ae2876e56d130f125aff3a21f2d852b2eb5	4b92234a	1b3570416f3309673832f49556f589cded34e1...	0
Insurance Details.docx	a7c35058f0db7aa1ad2948b6559327b0	7d955c977012aeb9e35bd4943485c6f4d3ab1...	cc5ef67b	a72b4060185c25b5bfa699b86aaae450f479cd...	b
Medical Records.docx	a70797abcd22d04fdd0216d58a4cfebb	885071564c9014b45856b023d624d3f0b2d41...	9bd9a5ab	49bf6989401be3c0070cd50554d743ef624f0f...	e

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**.

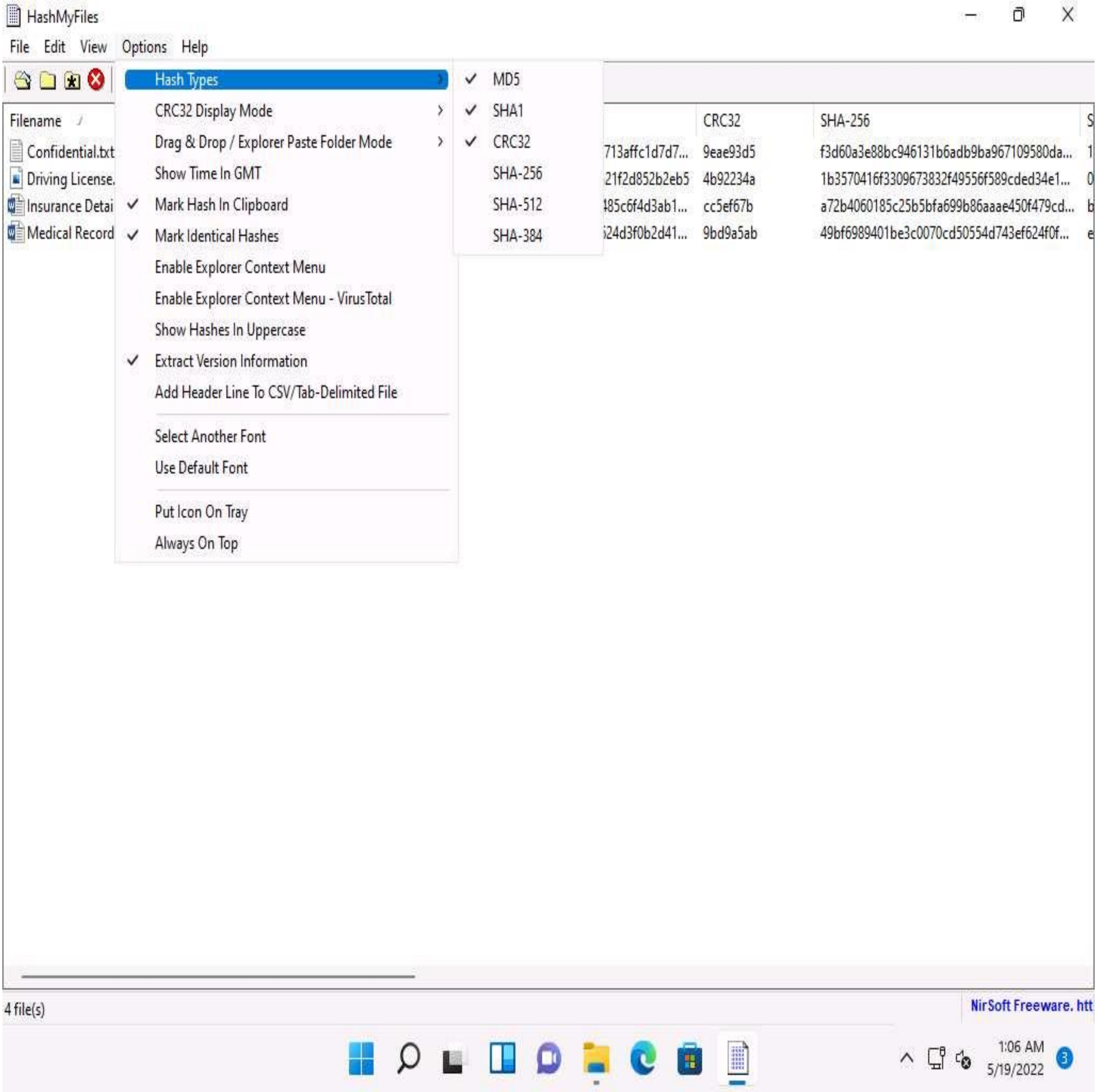


Filename		CRC32	SHA-256	S
Confidential.txt	713affc1d7d7...	9eae93d5	f3d60a3e88bc946131b6adb9ba967109580da...	1
Driving License.	21f2d852b2eb5	4b92234a	1b3570416f3309673832f49556f589cded34e1...	0
Insurance Detai	185c6f4d3ab1...	cc5ef67b	a72b4060185c25b5bfa699b86aaae450f479cd...	b
Medical Record	24d3f0b2d41...	9bd9a5ab	49bf6989401be3c0070cd50554d743ef624f0f...	e

4 file(s), 1 Selected

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

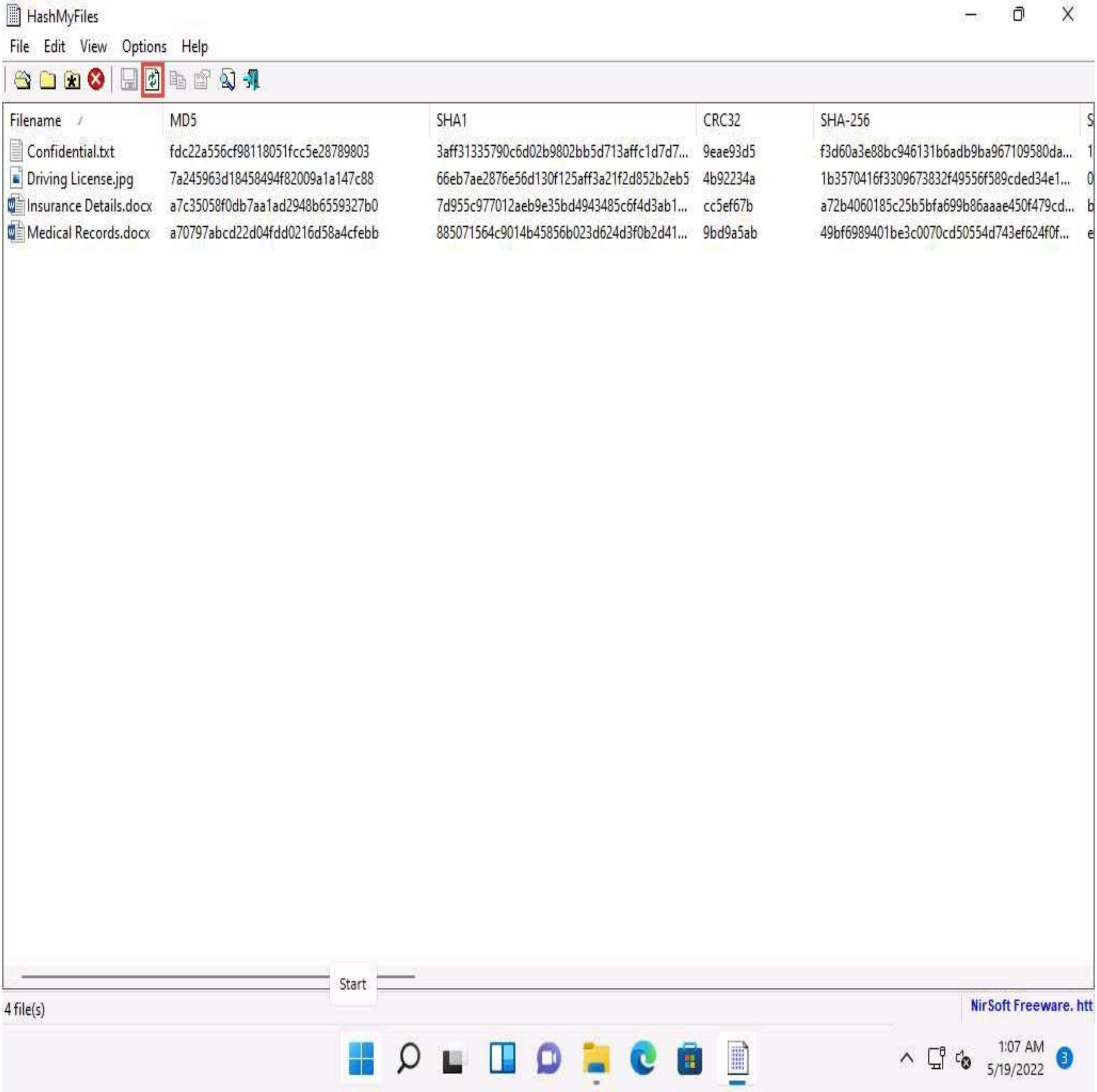
9. □ From the list of hash functions, unselect **SHA-256**, **SHA-512** and **SHA-384** hash types one by one.



Filename		CRC32	SHA-256	S
Confidential.txt	713affc1d7d7...	9eae93d5	f3d60a3e88bc946131b6adb9ba967109580da...	1
Driving License.	21f2d852b2eb5	4b92234a	1b3570416f3309673832f49556f589cded34e1...	0
Insurance Detai	485c6f4d3ab1...	cc5ef67b	a72b4060185c25b5bfa699b86aaae450f479cd...	b
Medical Record	524d3f0b2d41...	9bd9a5ab	49bf6989401be3c0070cd50554d743ef624f0f...	e

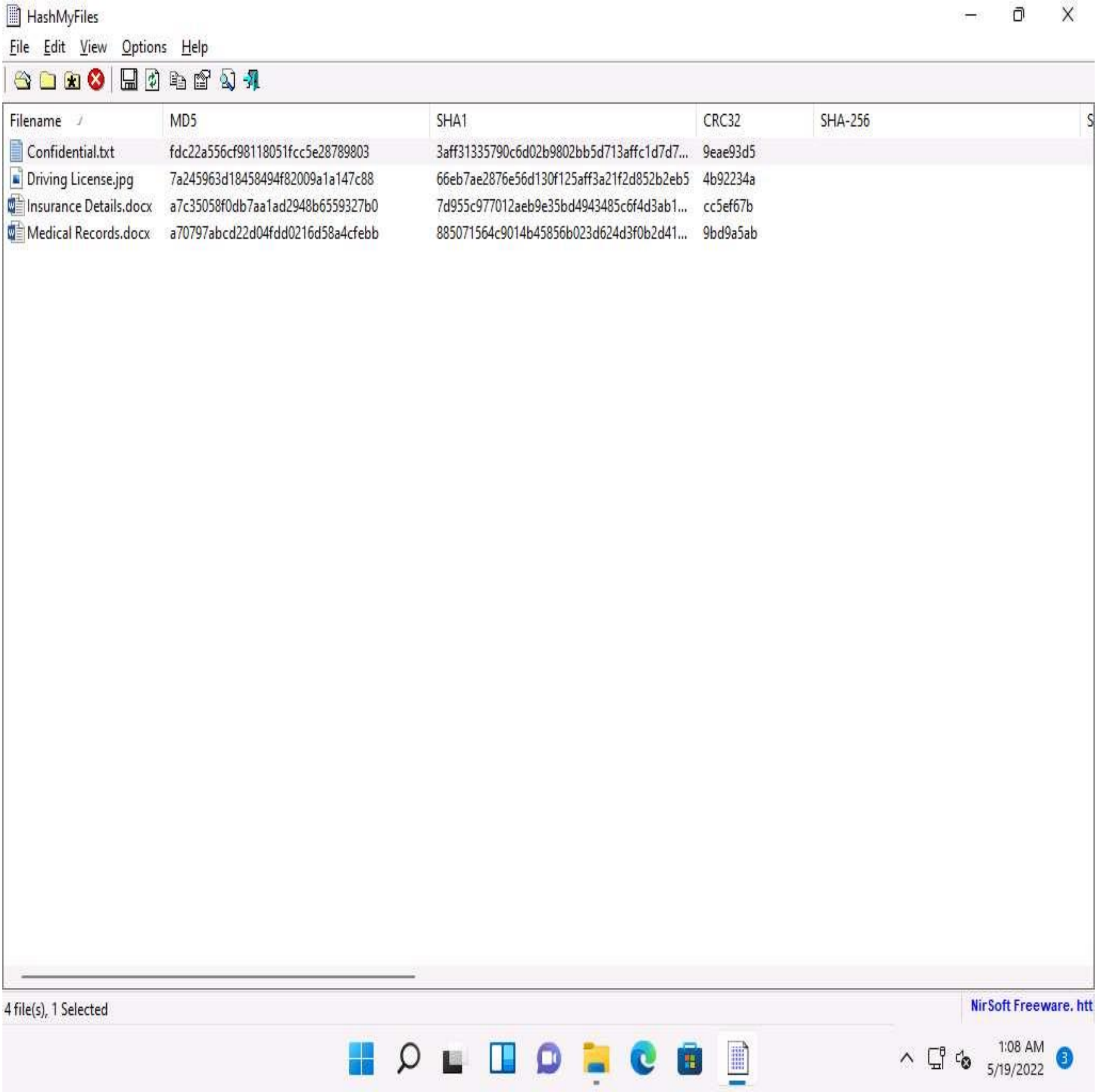
Here, we will calculate **MD5**, **SHA1** and **CRC32 Hash Types**.

10. □ After selecting the hash functions to be displayed, click **Refresh** icon from the menu bar to view the selected hash functions.



Filename	MD5	SHA1	CRC32	SHA-256	S
Confidential.txt	fdc22a556cf98118051fcc5e28789803	3aff31335790c6d02b9802bb5d713affc1d7d7...	9eae93d5	f3d60a3e88bc946131b6adb9ba967109580da...	1
Driving License.jpg	7a245963d18458494f82009a1a147c88	66eb7ae2876e56d130f125aff3a21f2d852b2eb5	4b92234a	1b3570416f3309673832f49556f589cded34e1...	0
Insurance Details.docx	a7c35058f0db7aa1ad2948b6559327b0	7d955c977012aeb9e35bd4943485c6f4d3ab1...	cc5ef67b	a72b4060185c25b5bfa699b86aaae450f479cd...	b
Medical Records.docx	a70797abcd22d04fdd0216d58a4cfebb	885071564c9014b45856b023d624d3f0b2d41...	9bd9a5ab	49bf6989401be3c0070cd50554d743ef624f0f...	e

4 file(s)



Filename	MD5	SHA1	CRC32	SHA-256	S
Confidential.txt	fdc22a556cf98118051fcc5e28789803	3aff31335790c6d02b9802bb5d713affc1d7d7...	9eae93d5		
Driving License.jpg	7a245963d18458494f82009a1a147c88	66eb7ae2876e56d130f125aff3a21f2d852b2eb5	4b92234a		
Insurance Details.docx	a7c35058f0db7aa1ad2948b6559327b0	7d955c977012aeb9e35bd4943485c6f4d3ab1...	cc5ef67b		
Medical Records.docx	a70797abcd22d04fdd0216d58a4cfebb	885071564c9014b45856b023d624d3f0b2d41...	9bd9a5ab		

4 file(s), 1 Selected

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

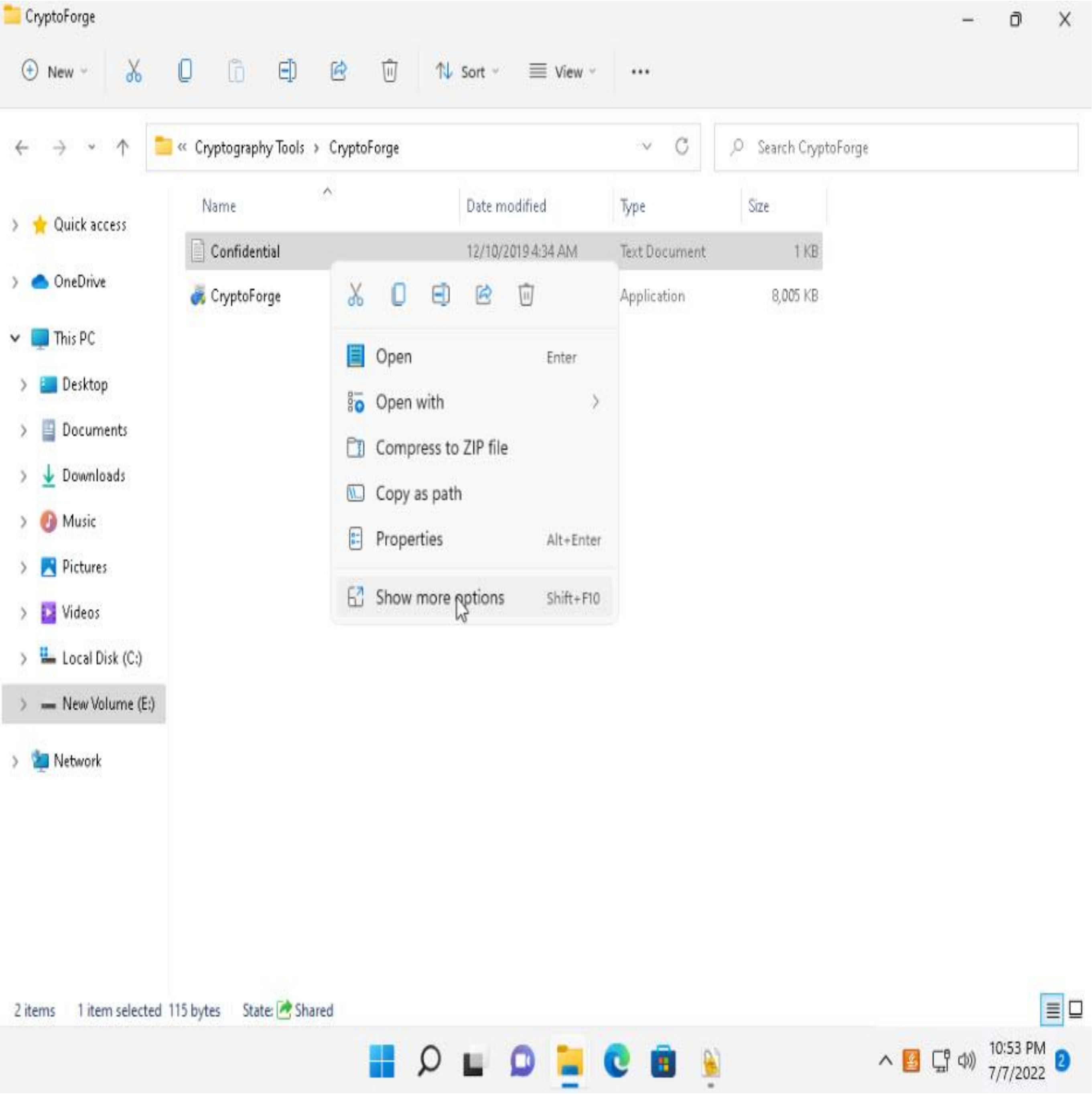
Task 4: Perform File and Text Message Encryption using CryptoForge

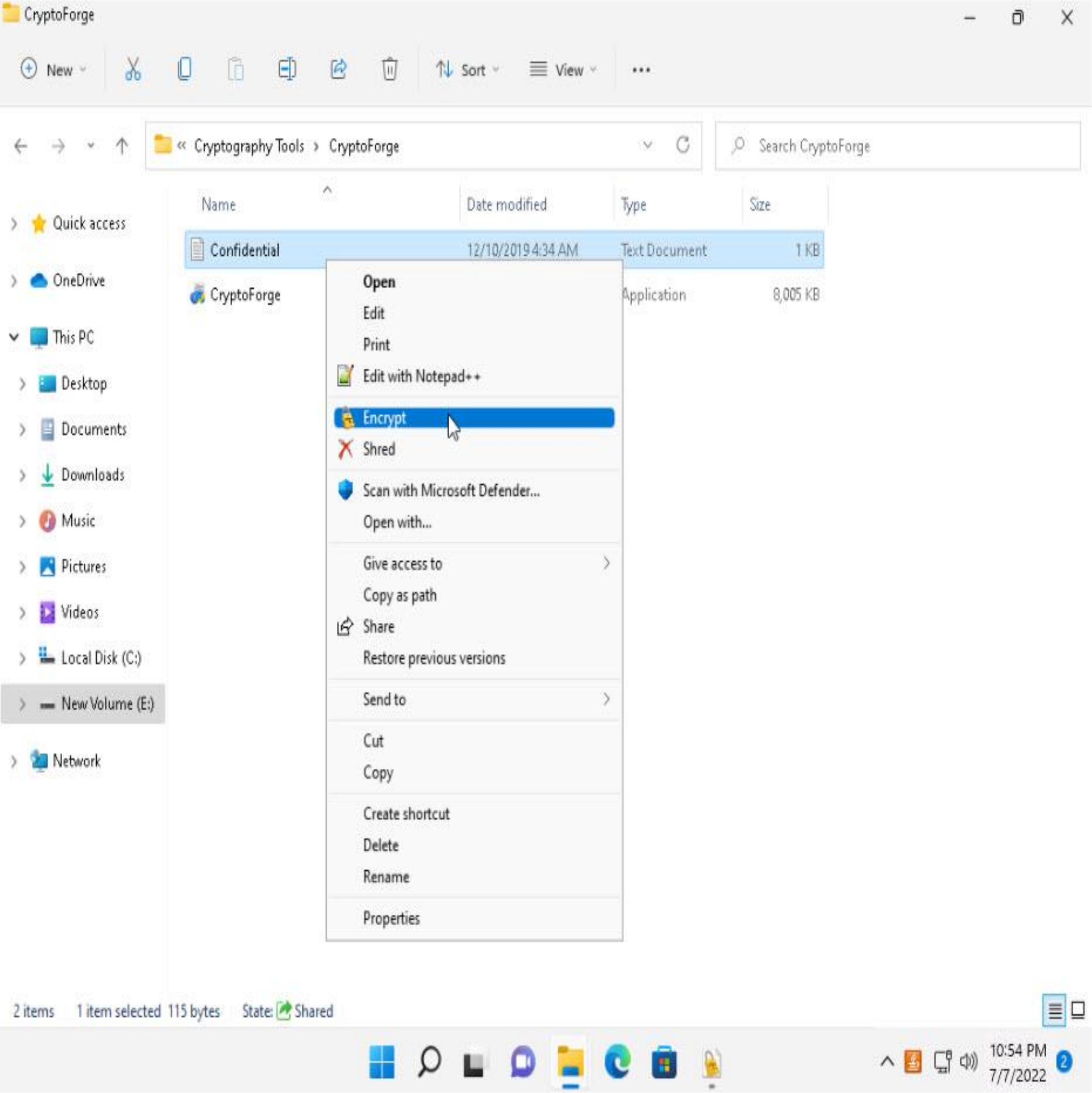
CryptoForge is a file encryption software for personal and professional data security. It allows you to protect the privacy of sensitive files, folders, or email messages by encrypting them with strong encryption algorithms. Once the information has been encrypted, it can be stored on insecure media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

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

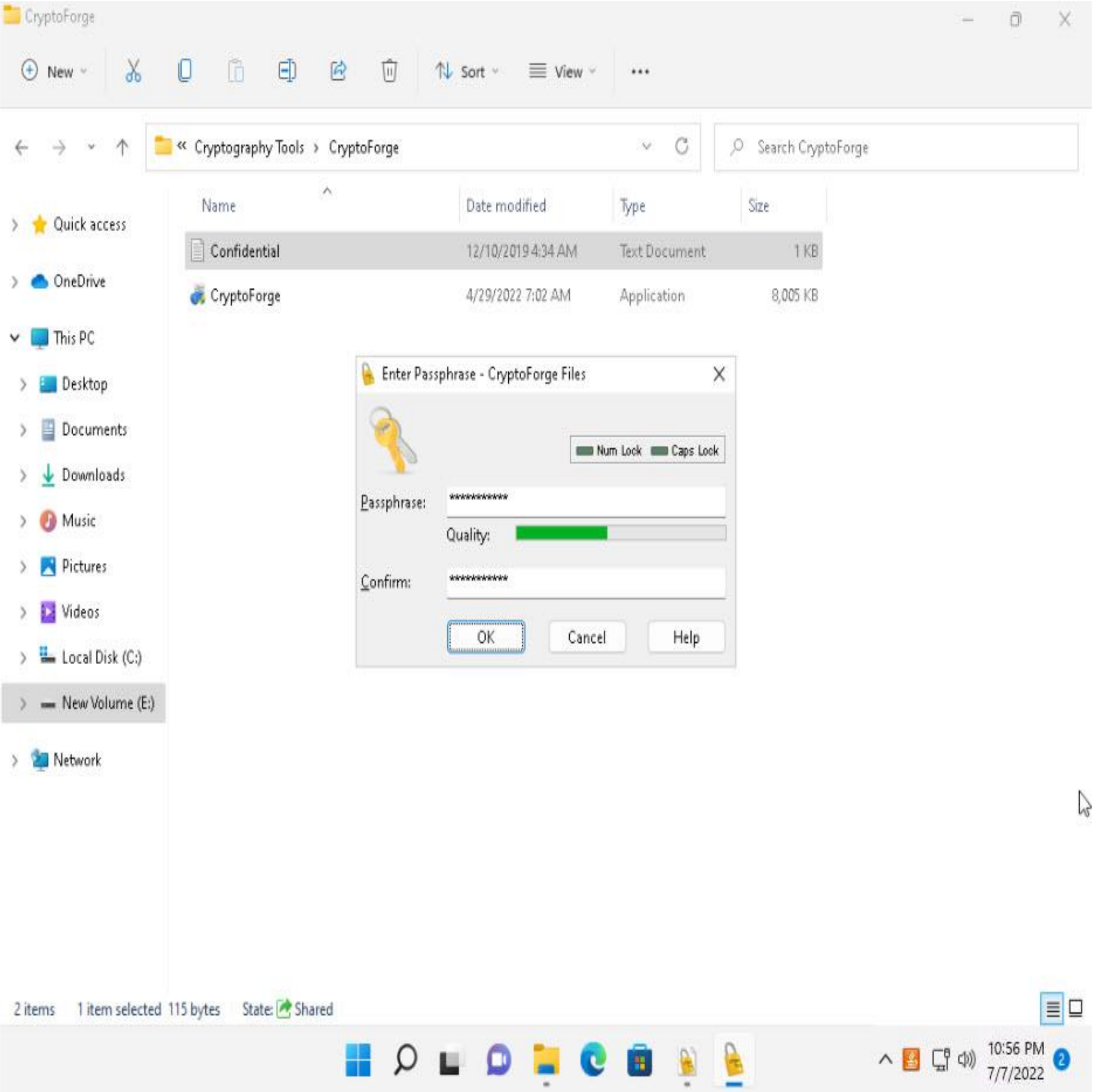
1. □ Click on Windows 11 to switch to the **Windows 11** machine. Navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\CryptoForge**. Right-click the **Confidential.txt** file and click **Show more options** and select **Encrypt** from the context menu

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





2. □ 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**.



Name	Date modified	Type	Size
Confidential	12/10/2019 4:34 AM	Text Document	1 KB
CryptoForge	4/29/2022 7:02 AM	Application	8,005 KB

Enter Passphrase - CryptoForge Files

Passphrase: ************

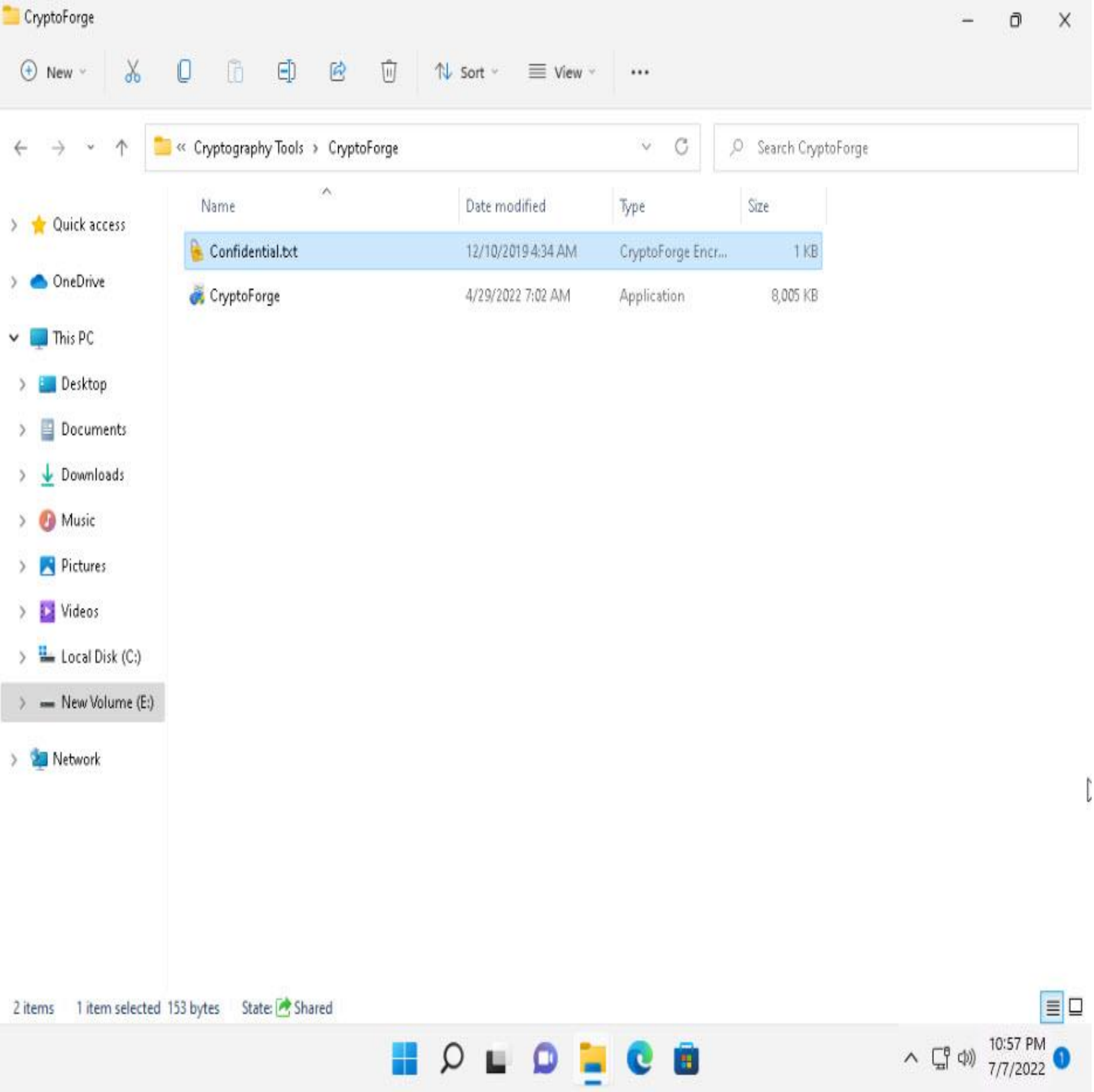
Quality:

Confirm: ************

2 items 1 item selected 115 bytes State: Shared

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

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.



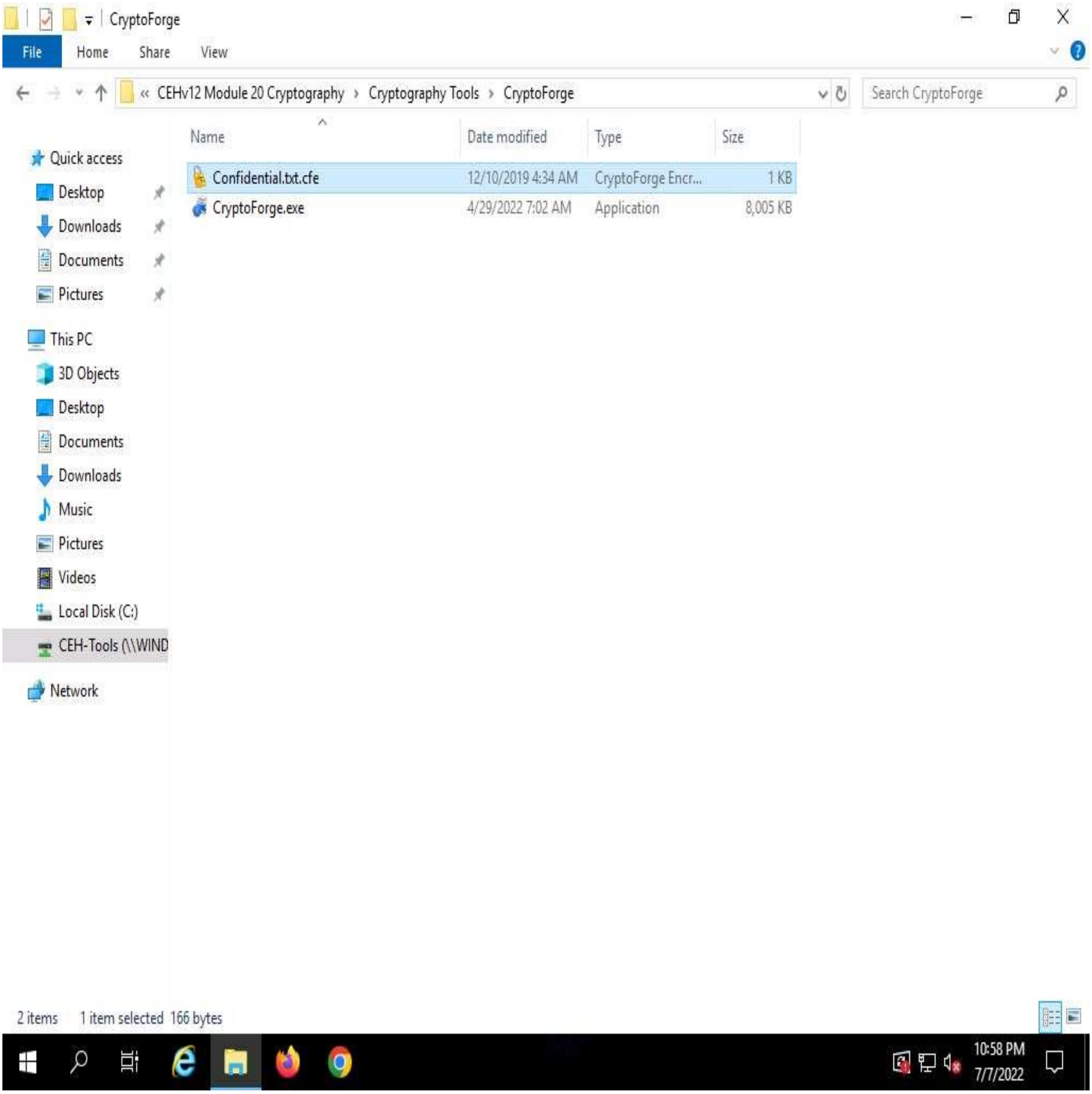
Name	Date modified	Type	Size
Confidential.txt	12/10/2019 4:34 AM	CryptoForge Encr...	1 KB
CryptoForge	4/29/2022 7:02 AM	Application	8,005 KB

4. □ Let us assume that you shared this file through a shared network drive.

5. □ Now, click on Windows Server 2019 to switch to the **Windows Server 2019**, click Ctrl+Alt+Delete to activate the machine. By default, **Administrator** profile is selected, type **Pa$$w0rd** to enter password in the Password field and press **Enter** to login.

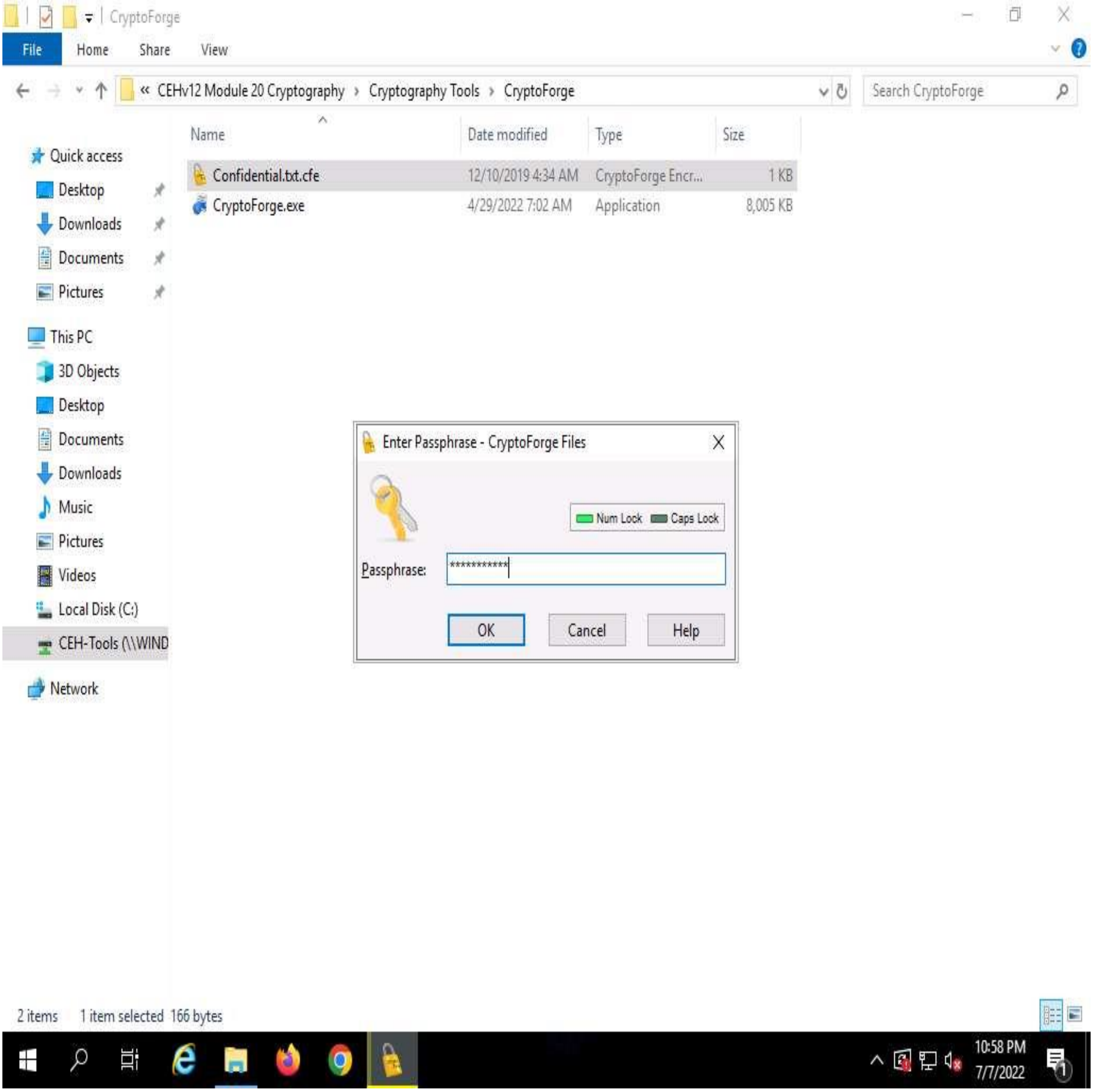
6. □ Navigate to **Z:\CEHv12 Module 20 Cryptography\Cryptography Tools\CryptoForge**. You will observe the encrypted file in this location.

7. □ Double-click the encrypted file to decrypt it and view its contents.



Name	Date modified	Type	Size
Confidential.txt.cfe	12/10/2019 4:34 AM	CryptoForge Encr...	1 KB
CryptoForge.exe	4/29/2022 7:02 AM	Application	8,005 KB

8. □ The **Enter Passphrase - CryptoForge Files** dialog-box appears; enter the password that you have provided in **Step#2** to encrypt the file and click **OK**.

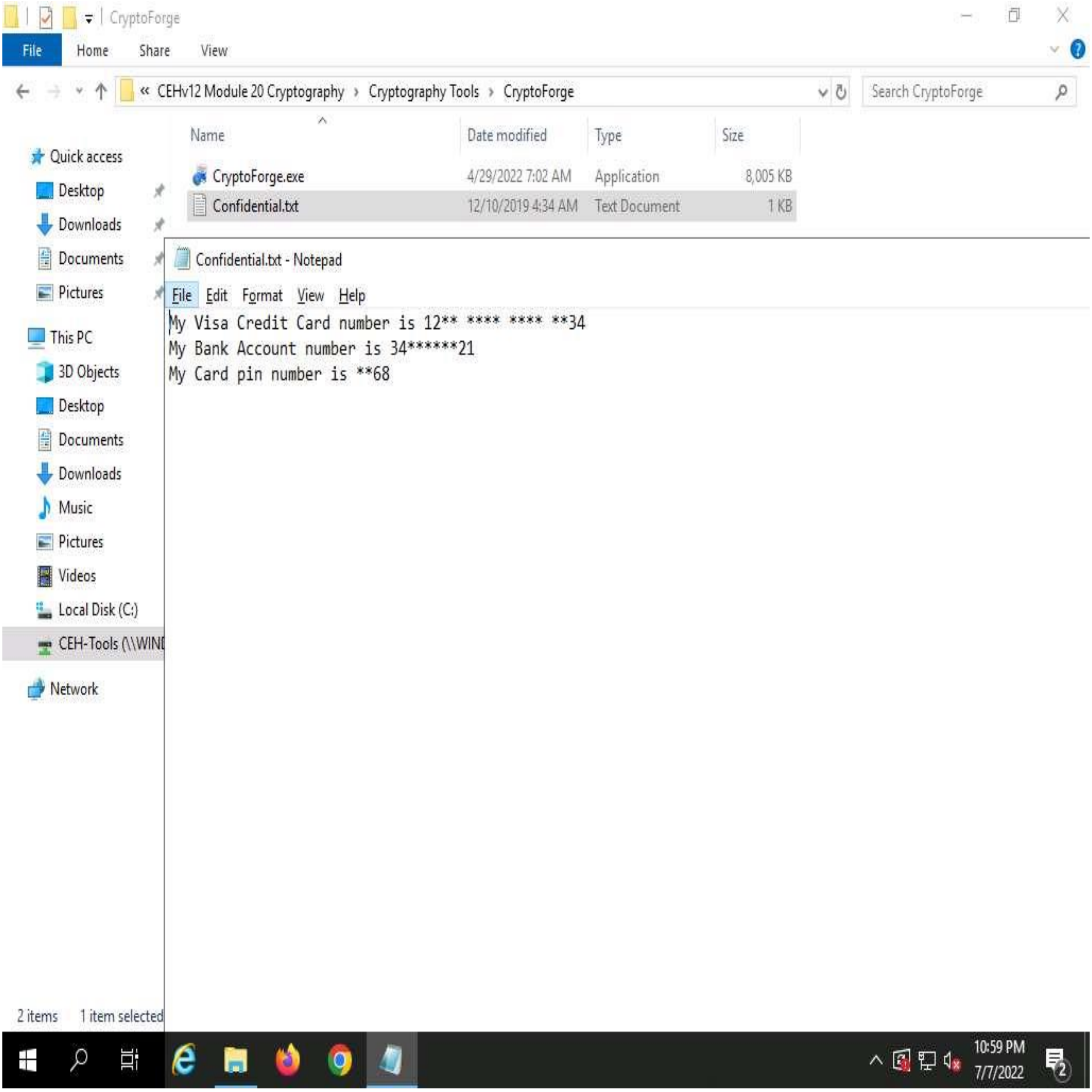


Name	Date modified	Type	Size
Confidential.txt.cfe	12/10/2019 4:34 AM	CryptoForge Encr...	1 KB
CryptoForge.exe	4/29/2022 7:02 AM	Application	8,005 KB

Passphrase: ***********

2 items 1 item selected 166 bytes

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



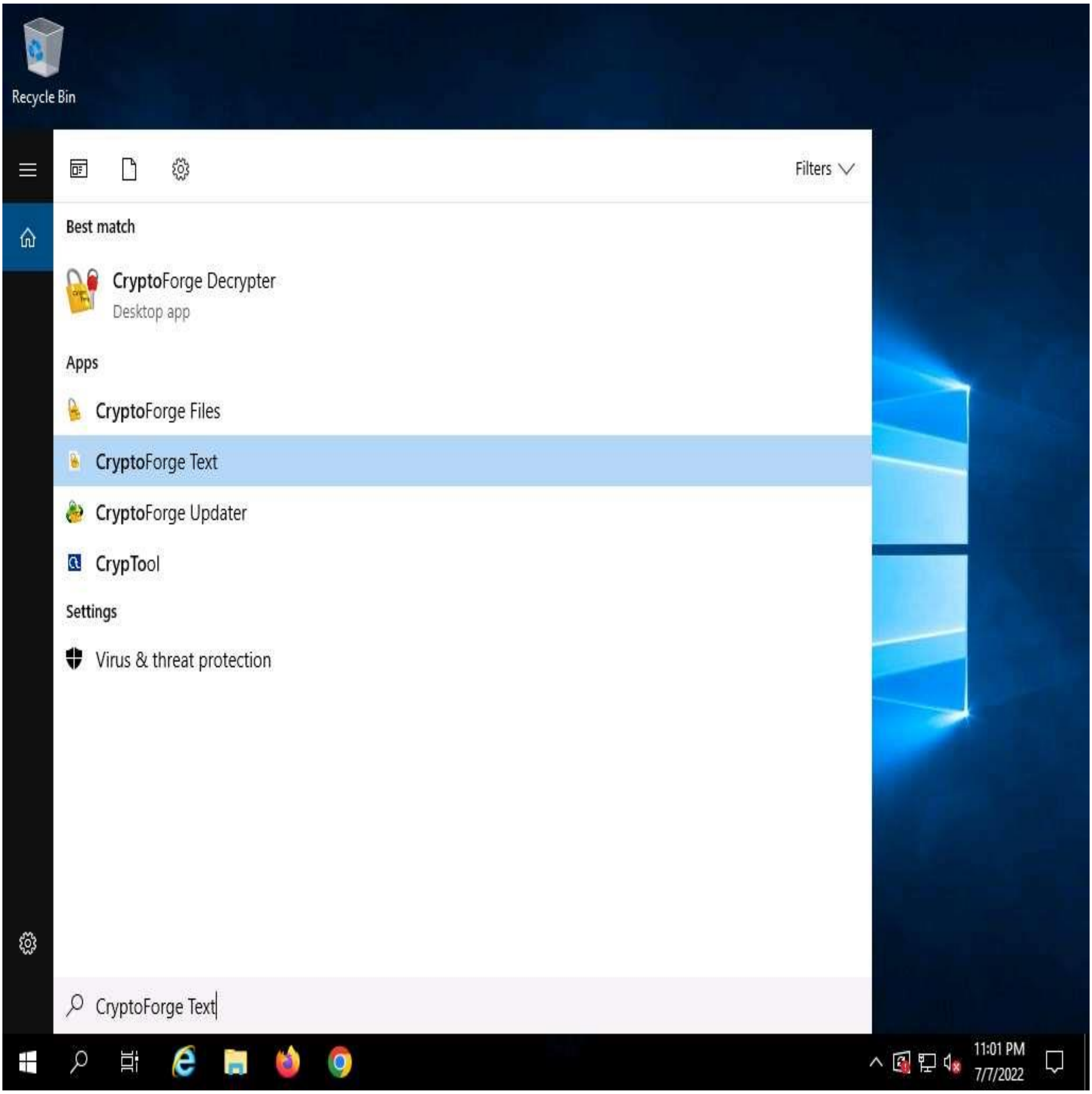
Name	Date modified	Type	Size
CryptoForge.exe	4/29/2022 7:02 AM	Application	8,005 KB
Confidential.txt	12/10/2019 4:34 AM	Text Document	1 KB

Confidential.txt - Notepad

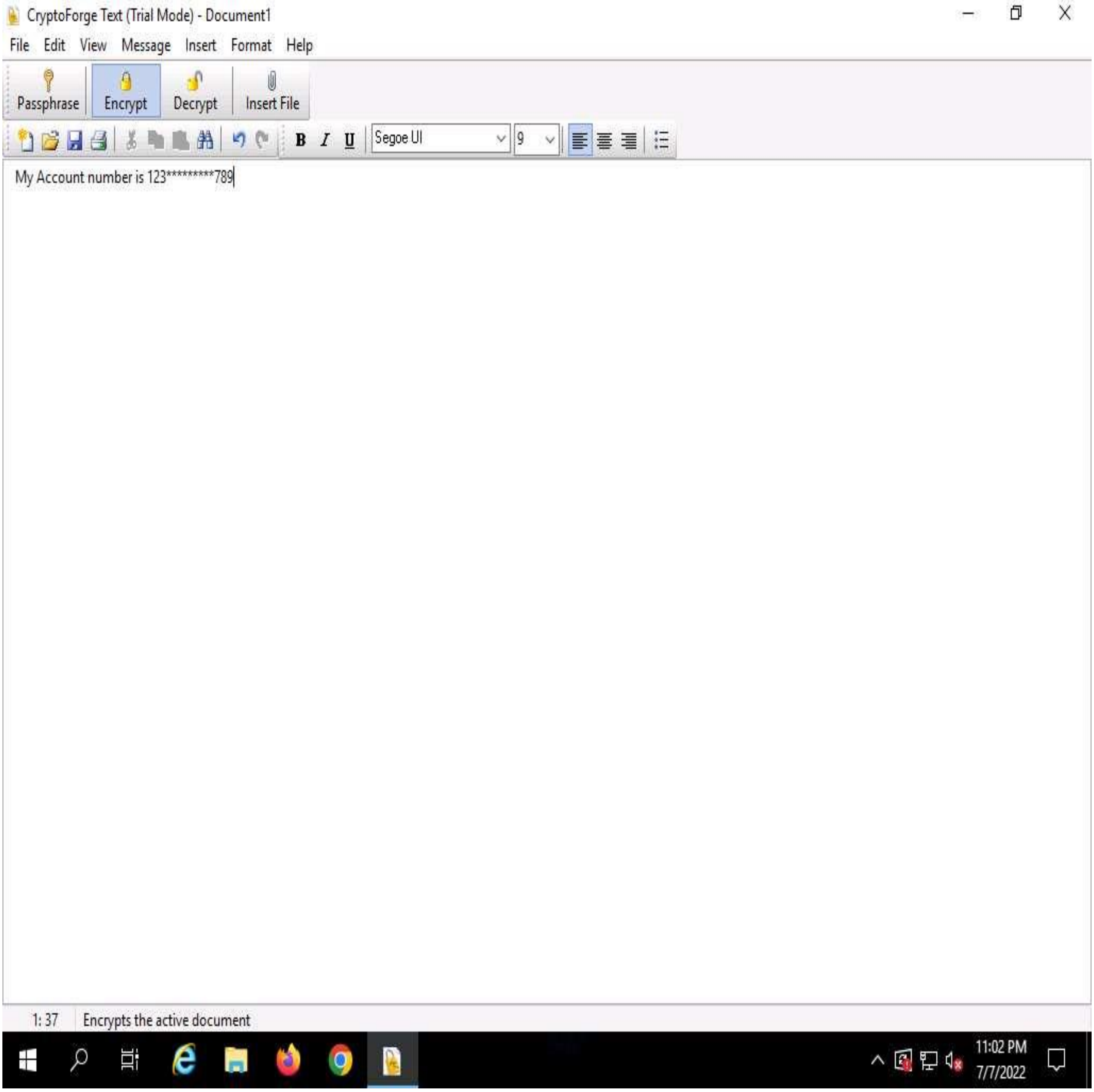
```
My Visa Credit Card number is 12** **** **** **34
My Bank Account number is 34******21
My Card pin number is **68
```

10. □ 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.

11. □ In the **Windows Server 2019** machine, click the **Type here to search** icon present in the bottom-left corner of **Desktop**, type **crypto** in the search field and click **CryptoForge Text** from the apps to launch the application.



12. □ The **CryptoForge Text** window appears; type a message and click **Encrypt** from the toolbar.

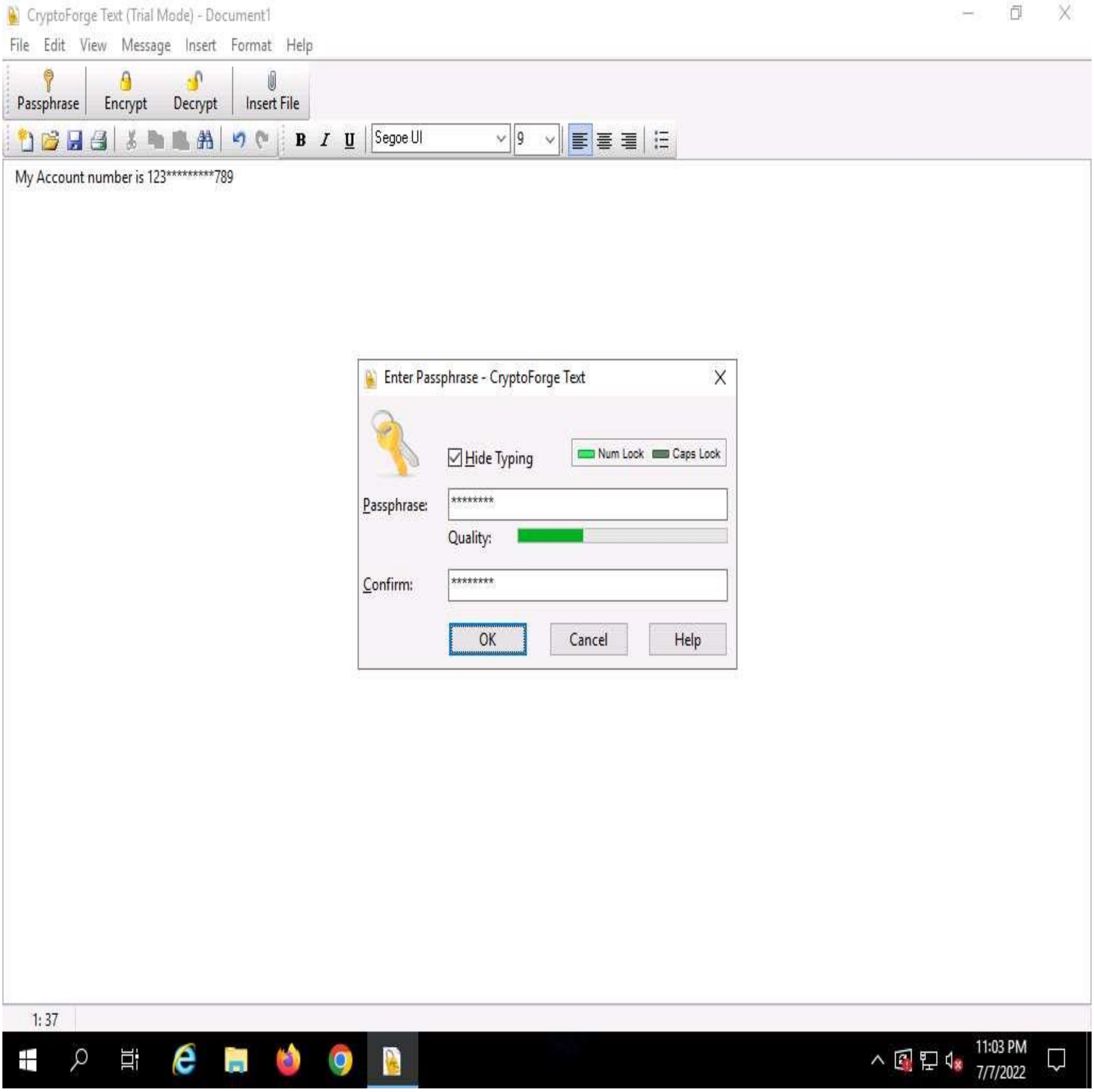


CryptoForge Text (Trial Mode) - Document1
File Edit View Message Insert Format Help
Passphrase
Encrypt
Decrypt
Insert File
Segoe UI
9

My Account number is 123*********789

1: 37 Encrypts the active document

13. □ 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**.



CryptoForge Text (Trial Mode) - Document1
File Edit View Message Insert Format Help
Passphrase
Encrypt
Decrypt
Insert File
Segoe UI
9

My Account number is 123*********789

Enter Passphrase - CryptoForge Text
☑ Hide Typing
Num Lock
Caps Lock

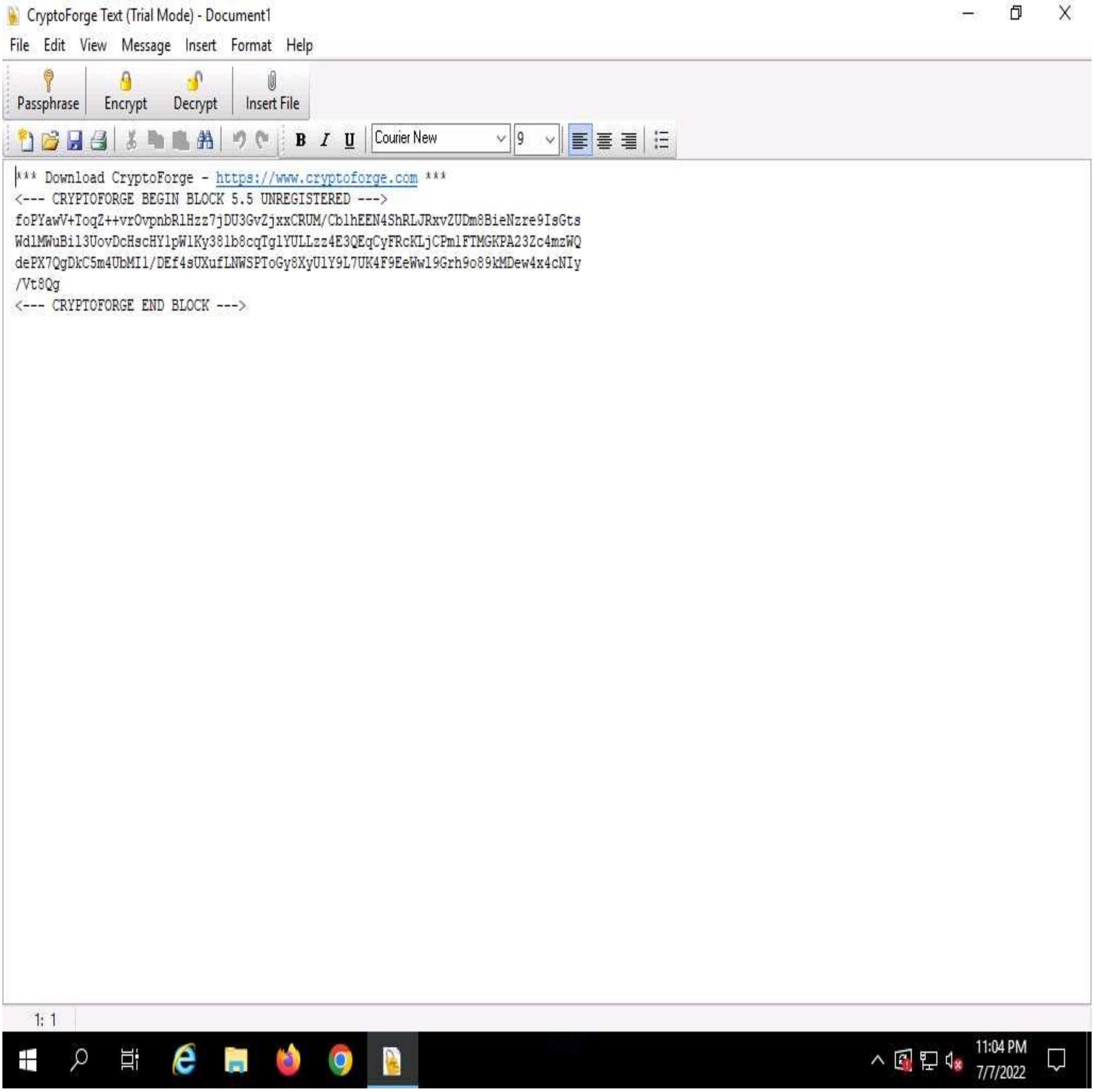
Passphrase: ********

Quality:

Confirm: ********

OK
Cancel
Help
1: 37
11:03 PM
7/7/2022

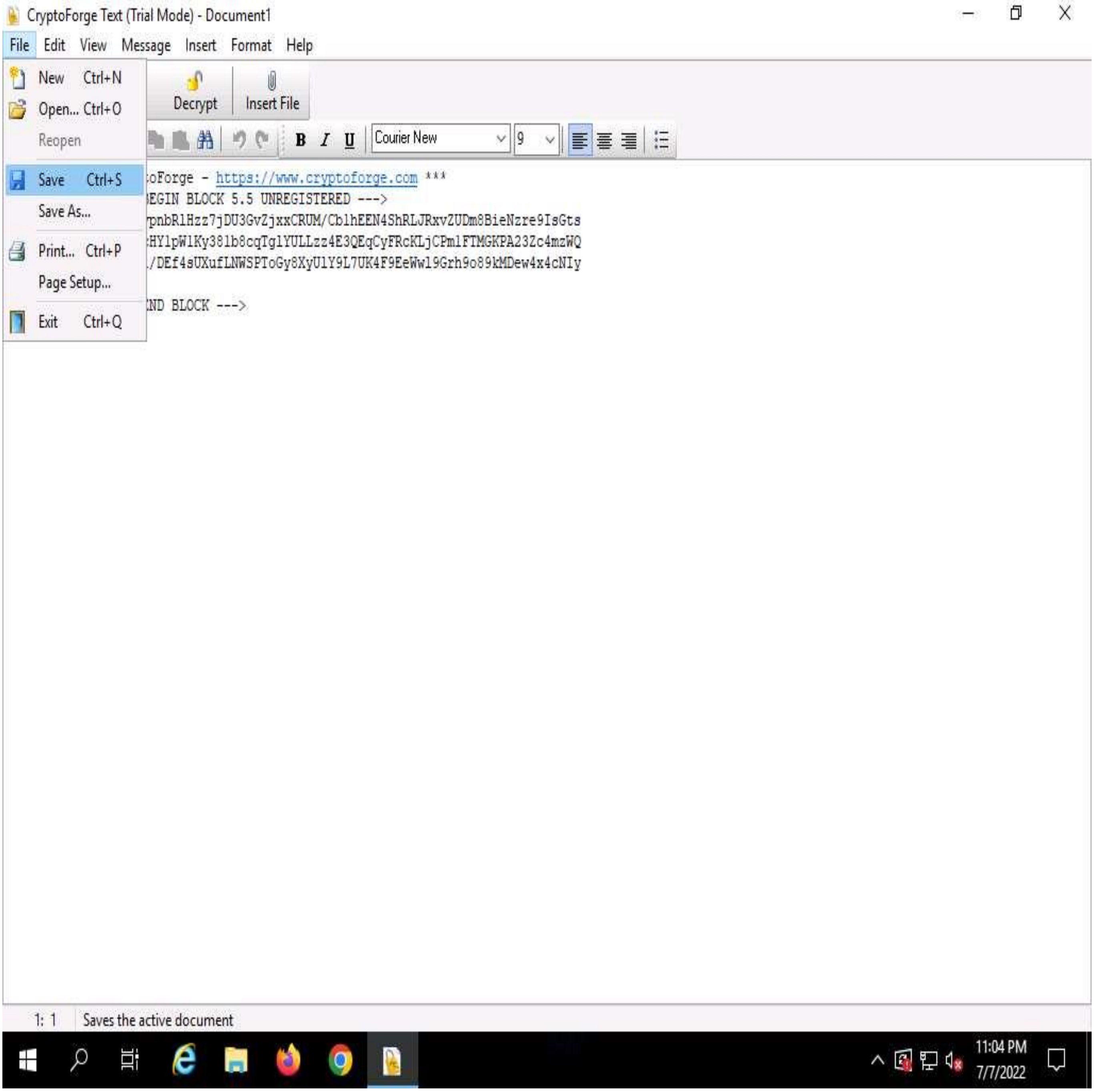
14. □ The message that you have typed will be encrypted, as shown in the screenshot.



CryptoForge Text (Trial Mode) - Document1
File Edit View Message Insert Format Help
Passphrase
Encrypt
Decrypt
Insert File
Courier New
9
1: 1
11:04 PM
7/7/2022

```
*** Download CryptoForge - https://www.cryptoforge.com ***
<--- CRYPTOFORGE BEGIN BLOCK 5.5 UNREGISTERED --->
foPYawV+ToqZ++vrOvpnbRlHzz7jDU3GvZjxxCRUM/CblhEEN4ShRLJRxvZUDm8BieNzre9IsGts
WdlMWuBil3UovDcHscHYlpWlKy381b8cqTglYULLzz4E3QEqCyFRcKLjCPmlFTMGKPA23Zc4mzWQ
dePX7QgDkC5m4UbMIl/DEf4sUXufLNWSPToGy8XyUlY9L7UK4F9EeWwl9Grh9o89kMDew4x4cNIy
/Vt8Qg
<--- CRYPTOFORGE END BLOCK --->
```

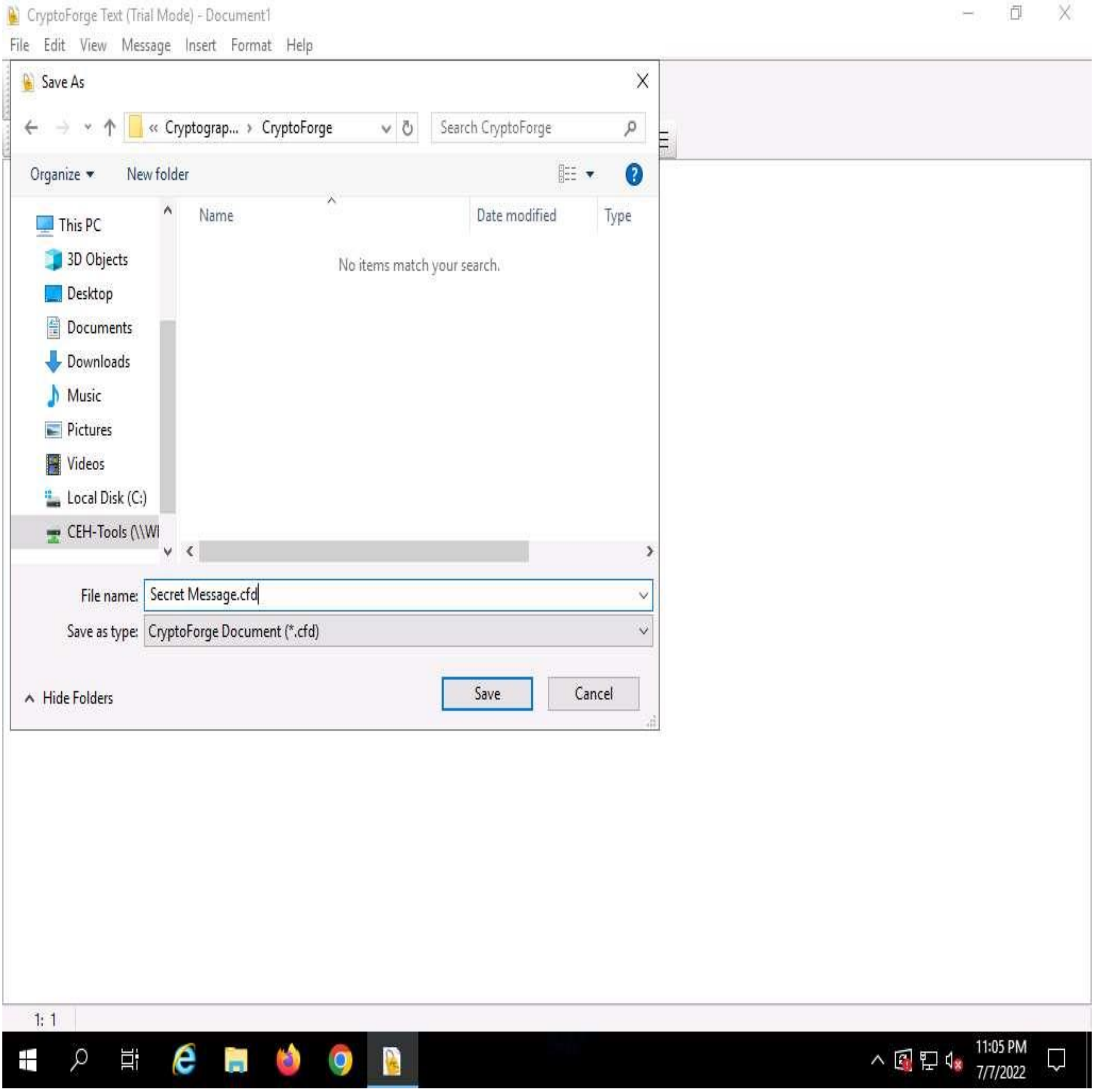
15. □ Now, you need to save the file. Click **File** in the menu bar and click **Save**.



```
oForge - https://www.cryptoforge.com ***
EGIN BLOCK 5.5 UNREGISTERED --->
pnbRlHzz7jDU3GvZjxxCRUM/CblhEEN4ShRLJRxvZUDm8BieNzre9IsGts
HYlpWlKy38lb8cqTglYULLzz4E3QEqCyFRcKLjCPmlFTMGKPA23Zc4mzWQ
/DEf4sUXufLNWSPToGy8XyUlY9L7UK4F9EeWwl9Grh9o89kMDew4x4cNIy

ND BLOCK --->
```

16. □ The **Save As** window appears; navigate to **Z:\CEHv12 Module 20 Cryptography\Cryptography Tools\CryptoForge**, specify the file name as **Secret Message.cfd**, and click **Save**.



CryptoForge Text (Trial Mode) - Document1

Save As

No items match your search.

File name: Secret Message.cfd

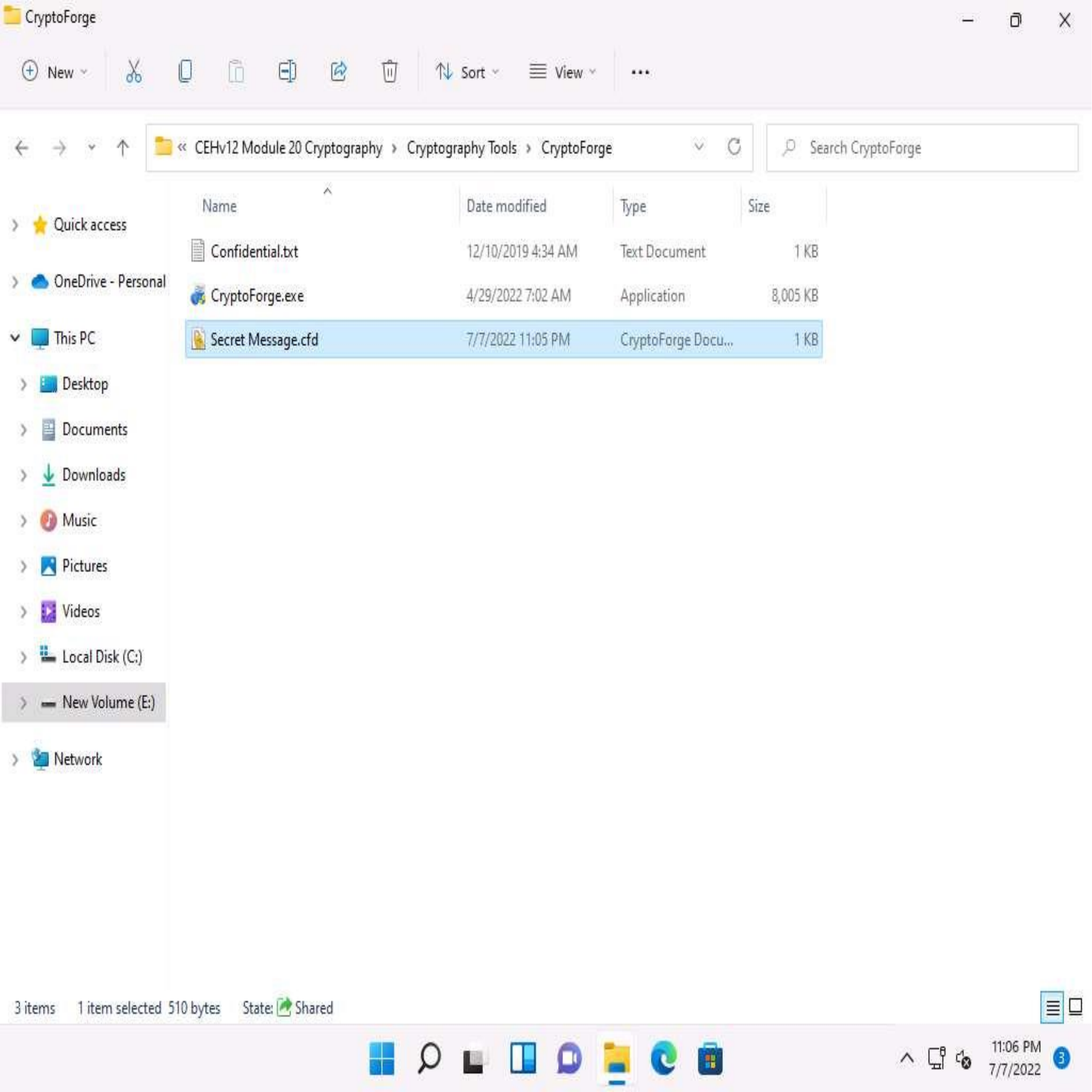
Save as type: CryptoForge Document (*.cfd)

17. □ Close the **CryptoForge Text** window.

18. □ 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.

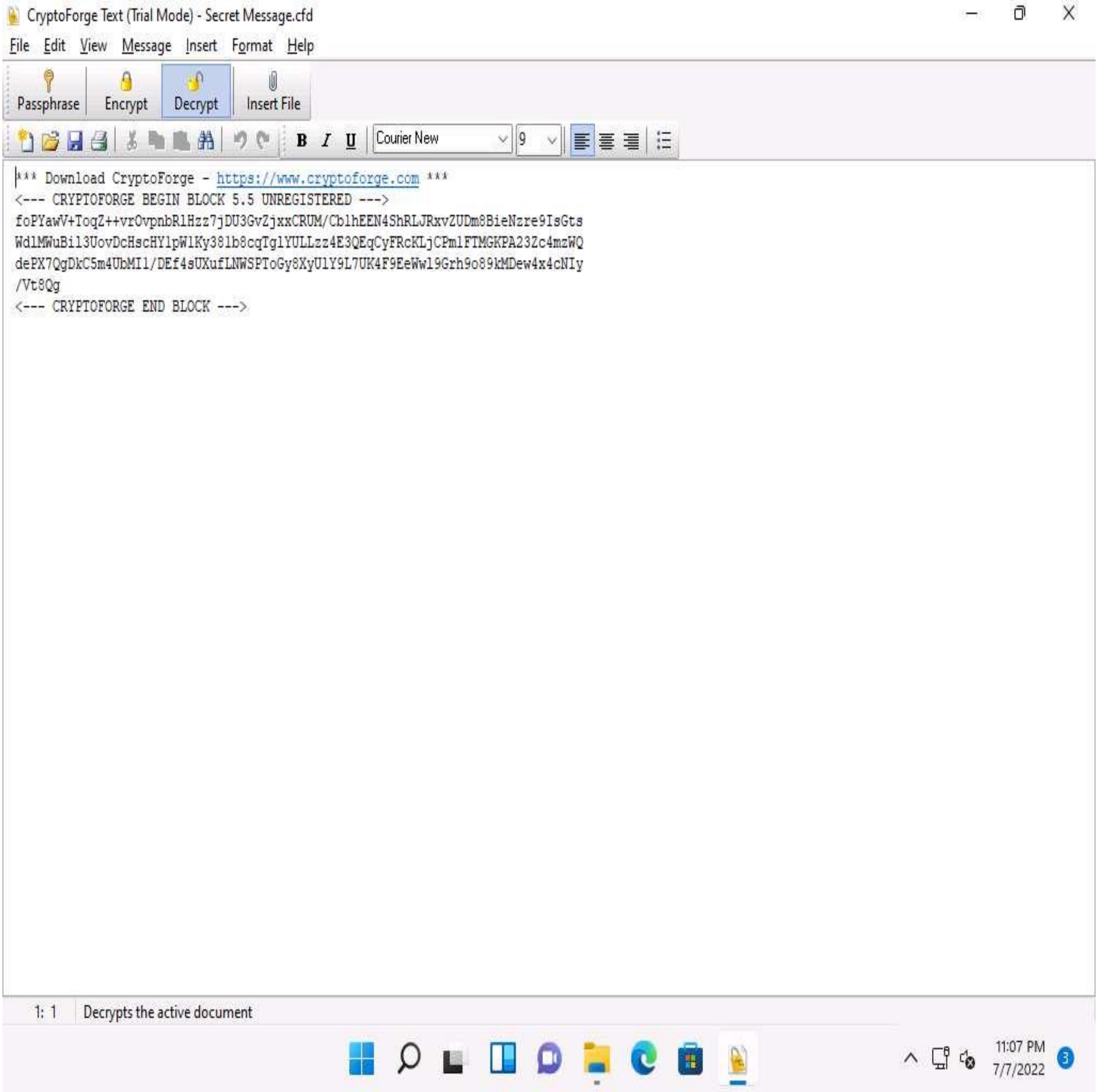
19. □ Click on Windows 11 to switch to the **Windows 11** machine and navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\CryptoForge**.

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



Name	Date modified	Type	Size
Confidential.txt	12/10/2019 4:34 AM	Text Document	1 KB
CryptoForge.exe	4/29/2022 7:02 AM	Application	8,005 KB
Secret Message.cfd	7/7/2022 11:05 PM	CryptoForge Docu...	1 KB

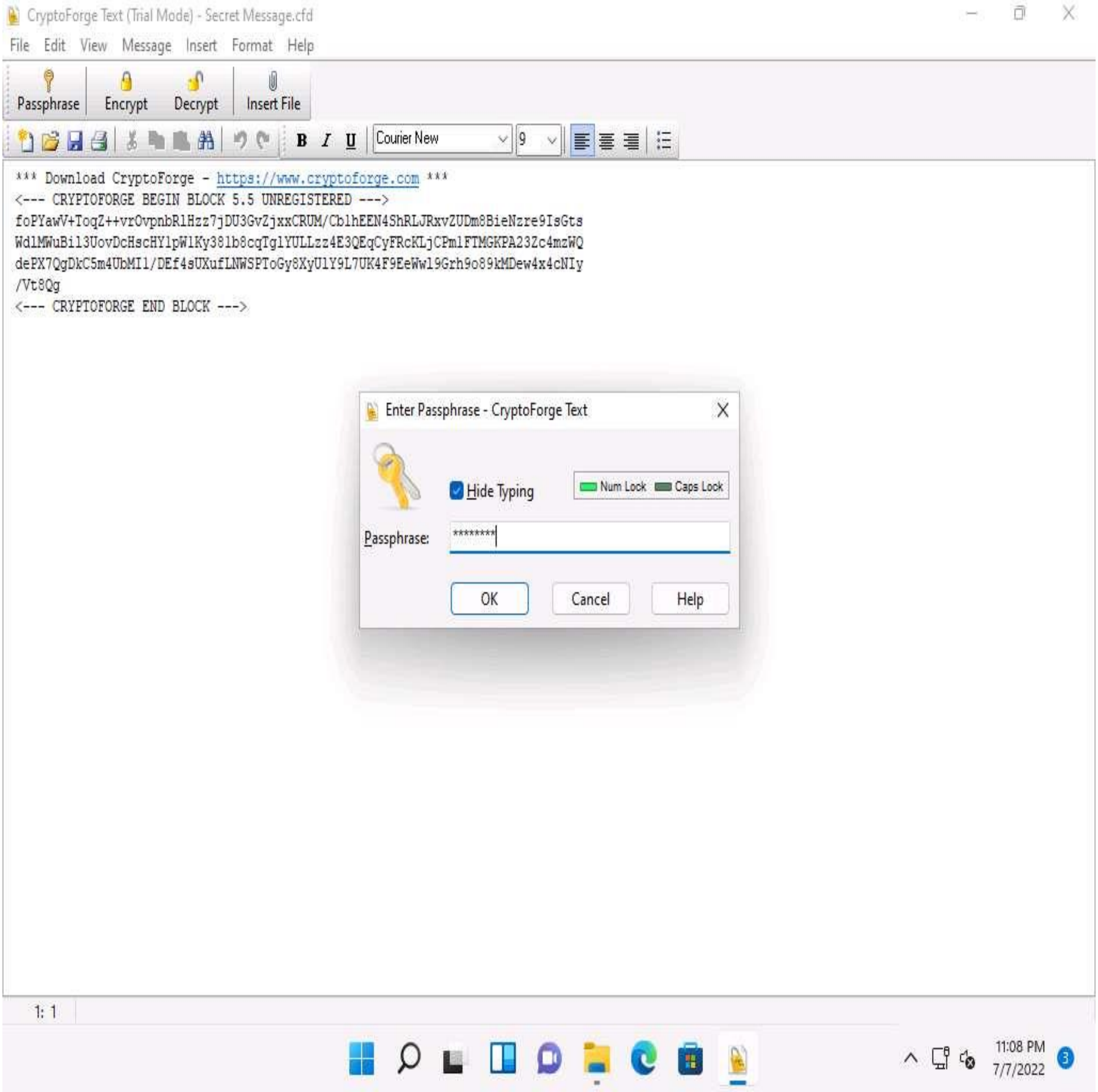
21. □ The **CryptoForge Text** window appears, displaying the message in an encrypted format. Click **Decrypt** from the toolbar to decrypt it.



CryptoForge Text (Trial Mode) - Secret Message.cfd
File Edit View Message Insert Format Help
Passphrase
Encrypt
Decrypt
Insert File
B I U
Courier New
9

```
*** Download CryptoForge - https://www.cryptoforge.com ***
<--- CRYPTOFORGE BEGIN BLOCK 5.5 UNREGISTERED --->
foPYawV+ToqZ++vrOvpnbRlHzz7jDU3GvZjxxCRUM/CblhEEN4ShRLJRxvZUDm8BieNzre9IsGts
WdlMWuBil3UovDcHscHYlpWlKy38lb8cqTglYULLzz4E3QEqCyFRcKLjCPmlFTMGKPA23Zc4mzWQ
dePX7QgDkC5m4UbMIl/DEf4sUXufLNWSPToGy8XyUlY9L7UK4F9EeWwl9Grh9o89kMDew4x4cNIy
/Vt8Qg
<--- CRYPTOFORGE END BLOCK --->
```

22. □ The **Enter Passphrase - CryptoForge Text** dialog-box appears; enter the password you provided in **Step#13** to decrypt the message in the **Passphrase** field and click **OK**.


CryptoForge Text (Trial Mode) - Secret Message.cfd
File Edit View Message Insert Format Help
Passphrase
Encrypt
Decrypt
Insert File
Courier New
9
1: 1
11:08 PM
7/7/2022

```
*** Download CryptoForge - https://www.cryptoforge.com ***
<--- CRYPTOFORGE BEGIN BLOCK 5.5 UNREGISTERED --->
foPYawV+ToqZ++vrOvpnbRlHzz7jDU3GvZjxxCRUM/CblhEEN4ShRLJRxvZUDm8BieNzre9IsGts
WdlMWuBil3UovDcHscHYlpWlKy38lb8cqTglYULLzz4E3QEqCyFRcKLjCPmlFTMGKPA23Zc4mzWQ
dePX7QgDkC5m4UbMIl/DEf4sUXufLNWSPToGy8XyUlY9L7UK4F9EeWwl9Grh9o89kMDew4x4cNIy
/Vt8Qg
<--- CRYPTOFORGE END BLOCK --->
```

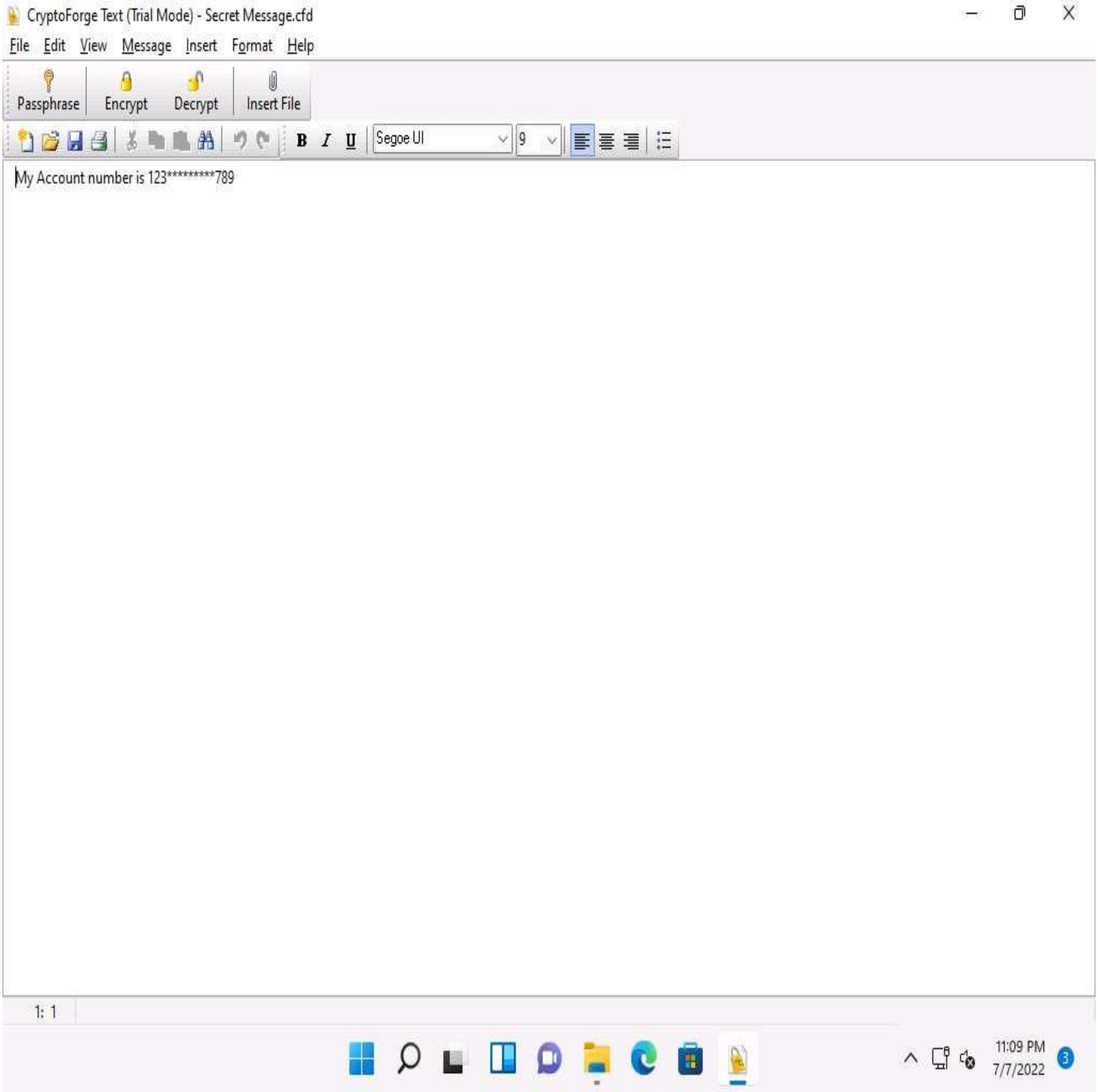
Enter Passphrase - CryptoForge Text

☑ Hide Typing

Passphrase: ********

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

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


CryptoForge Text (Trial Mode) - Secret Message.cfd
File Edit View Message Insert Format Help
Passphrase
Encrypt
Decrypt
Insert File
Segoe UI
9
1: 1
11:09 PM
7/7/2022

My Account number is 123*********789

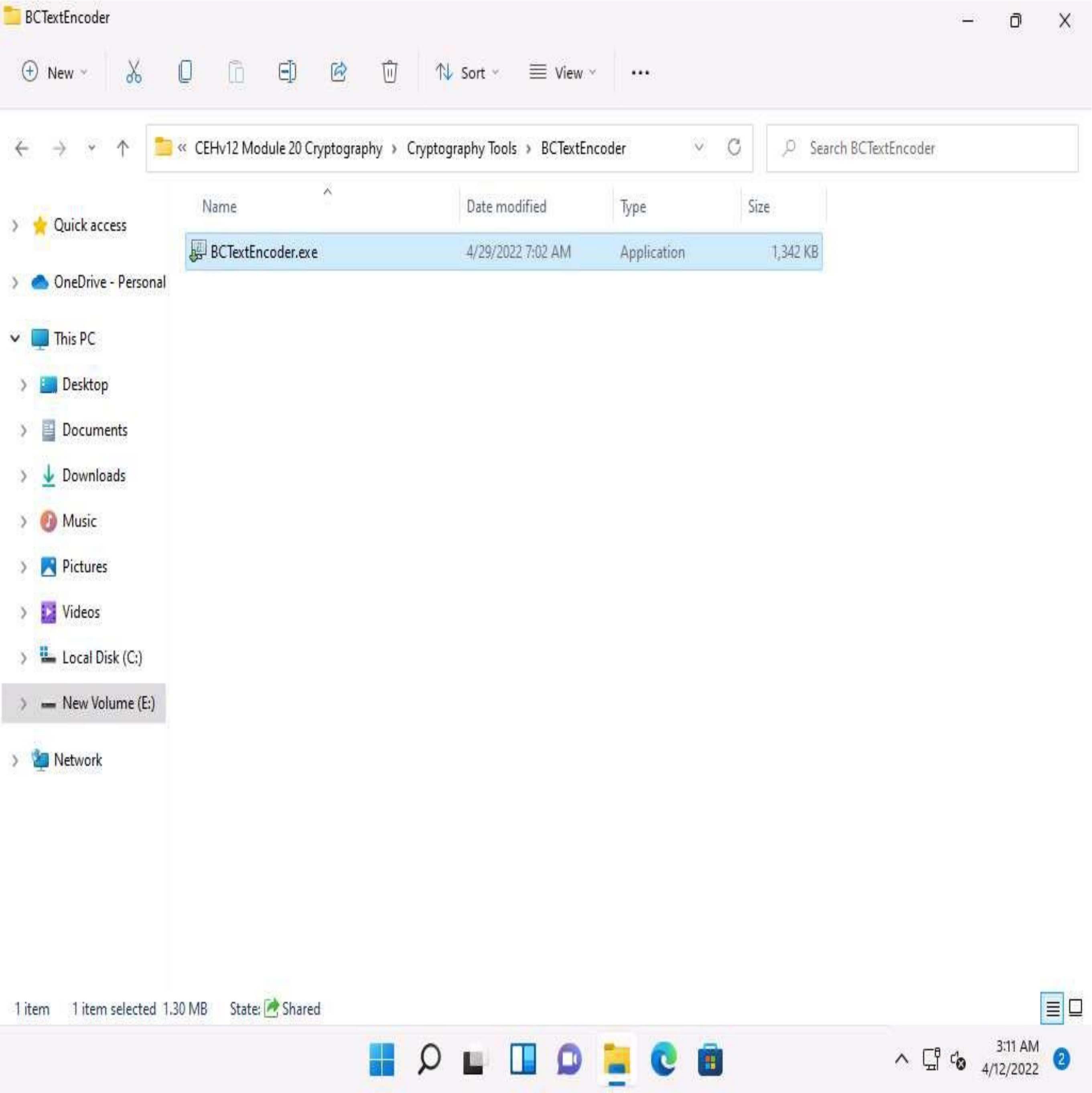
24. □ This concludes the demonstration of performing file and text message encryption using CryptoForge.
25. □ Close all open windows and document all the acquired information.

Task 5: Encrypt and Decrypt Data using BCTextEncoder

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.

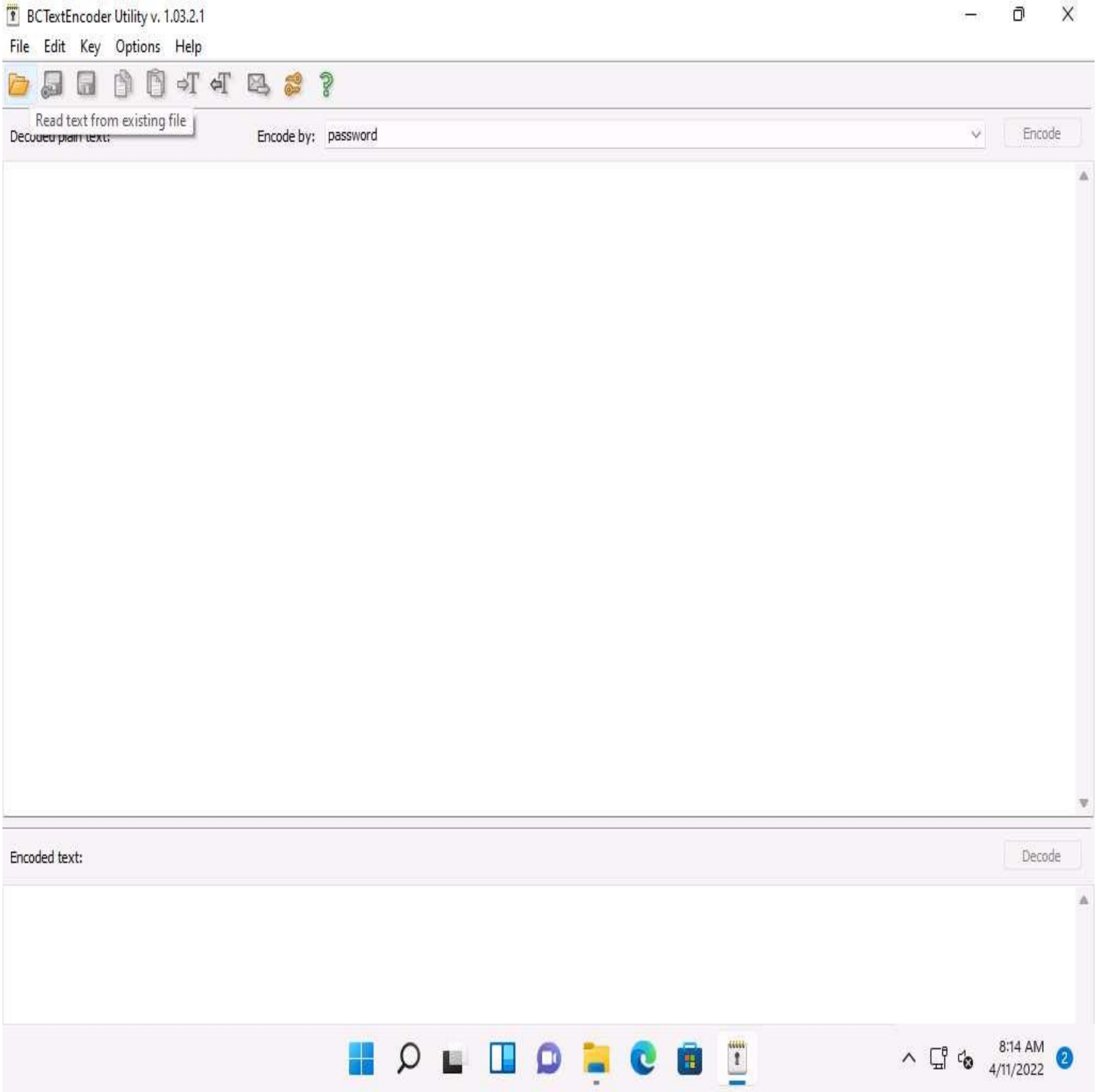
Here, we will use the BCTextEncoder tool to encrypt and decrypt data.

1. □ In **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\BCTextEncoder** and double click **BCTextEncoder.exe**.



Name	Date modified	Type	Size
BCTextEncoder.exe	4/29/2022 7:02 AM	Application	1,342 KB

2. □ The **BCTextEncoder Utility** window appears, as shown in the screenshot.



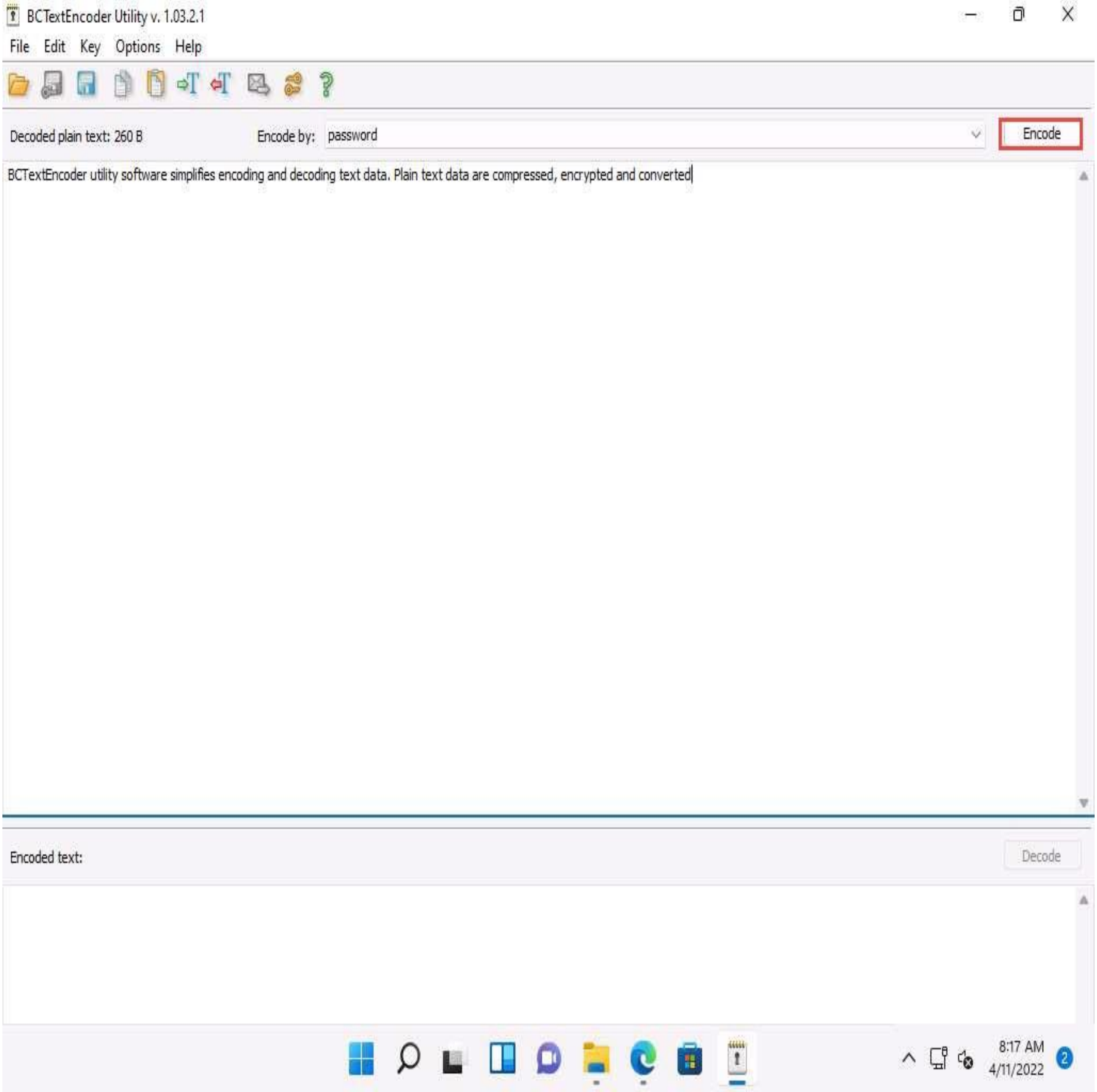
Encode by: password

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

Or

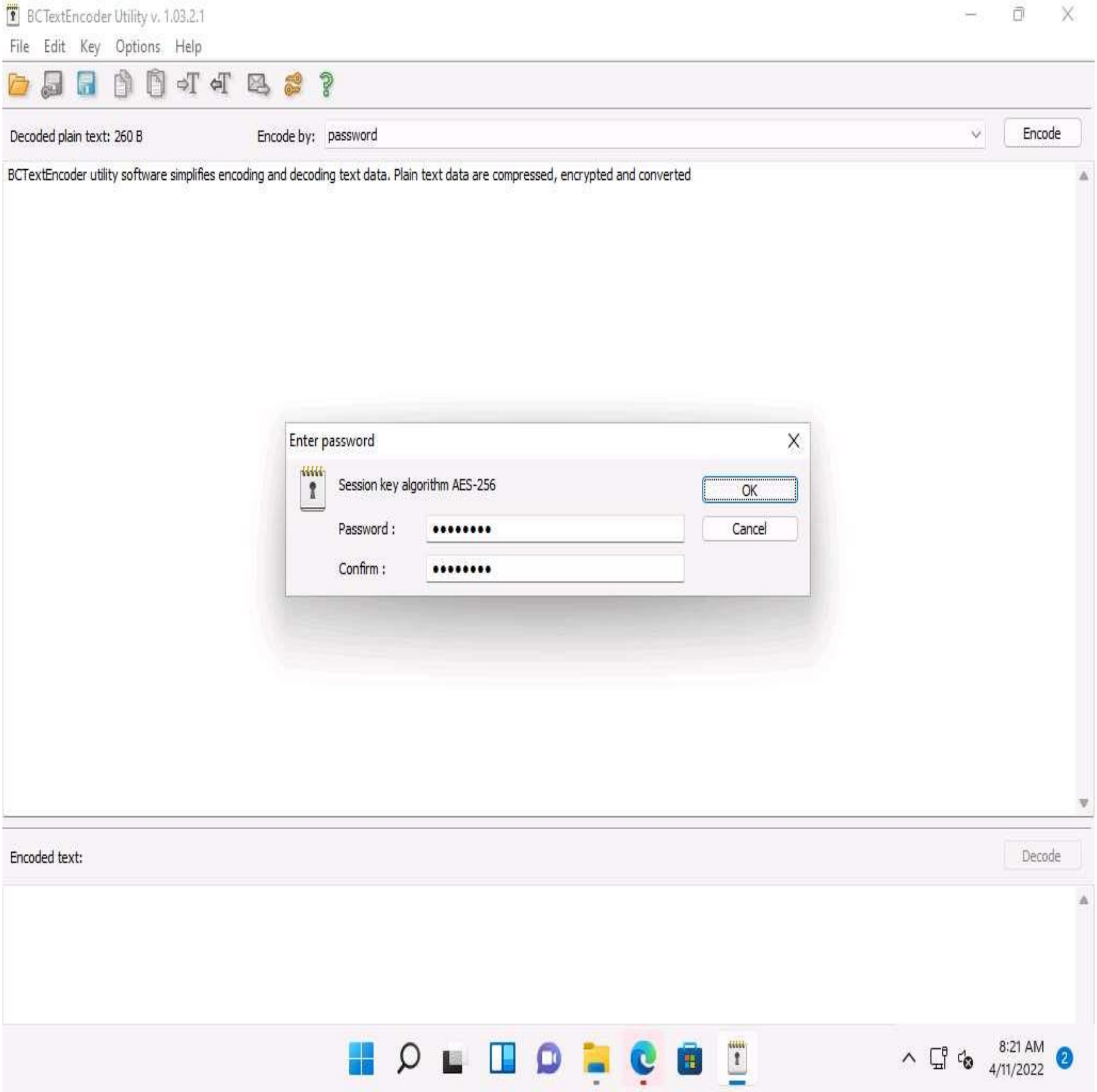
Select the data that you want to encode and paste it to the clipboard by pressing **Ctrl+V**.

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



BCTextEncoder utility software simplifies encoding and decoding text data. Plain text data are compressed, encrypted and converted

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**).



Decoded plain text: 260 B

Encode by: password

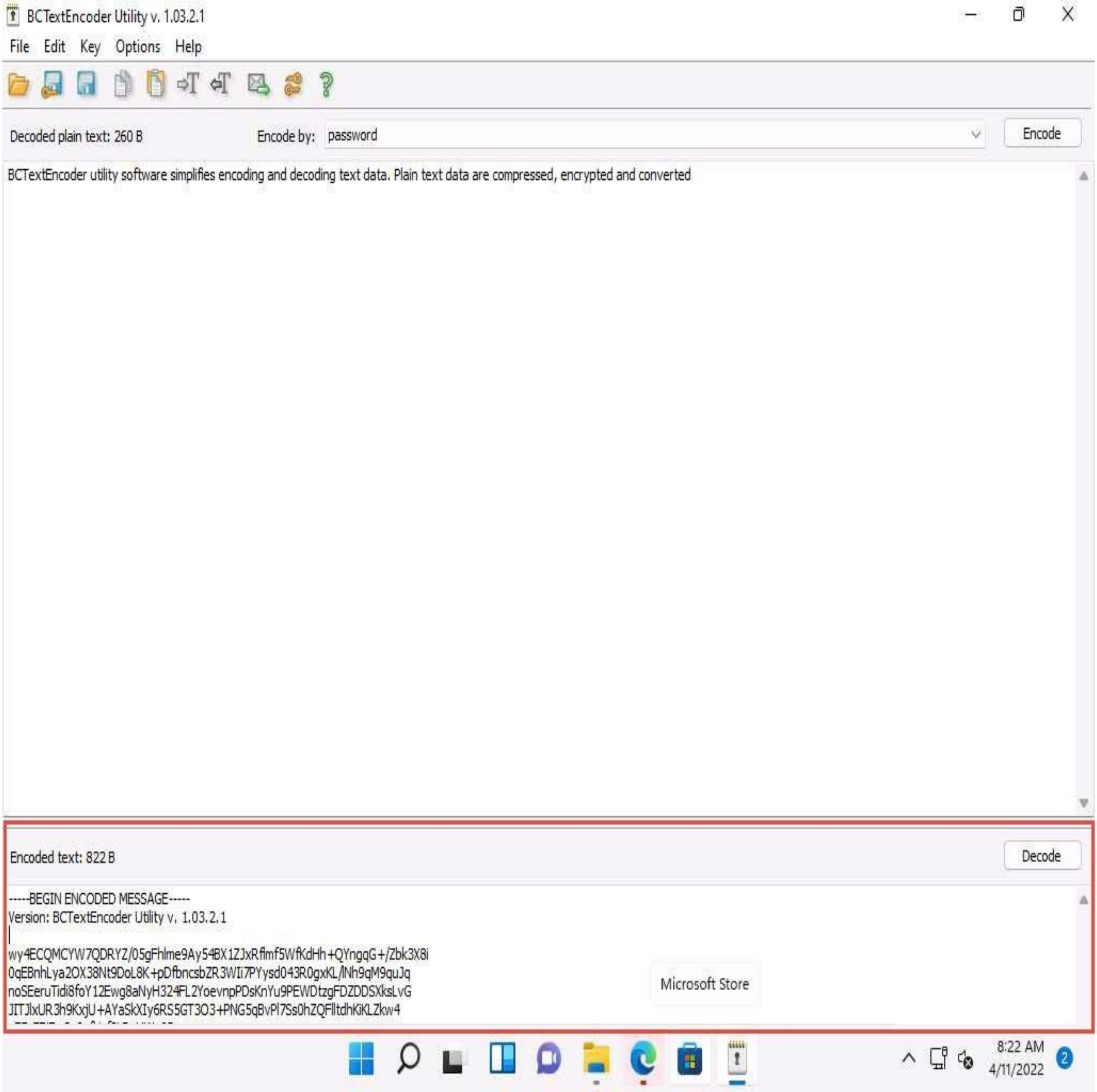
BCTextEncoder utility software simplifies encoding and decoding text data. Plain text data are compressed, encrypted and converted

Session key algorithm AES-256

Password : •••••••••

Confirm : •••••••••

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



Decoded plain text: 260 B

Encode by: password

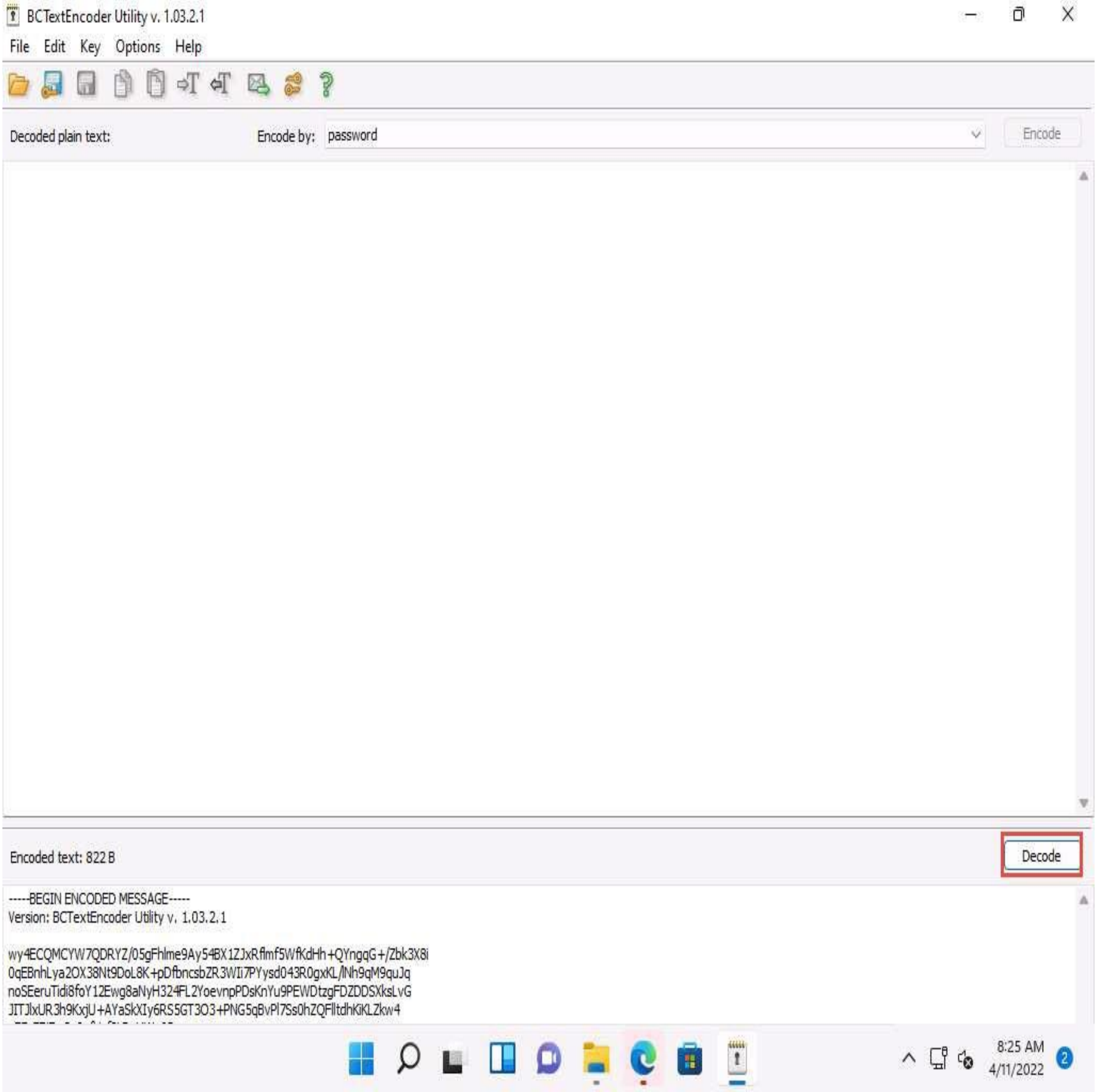
BCTextEncoder utility software simplifies encoding and decoding text data. Plain text data are compressed, encrypted and converted

Encoded text: 822 B

```
-----BEGIN ENCODED MESSAGE-----
Version: BCTextEncoder Utility v. 1.03.2.1

wy4ECQMCYW7QDRYZ/05gFhlme9Ay54BX1ZJxRflmf5WfKdHh+QYngqG+/Zbk3X8i
0qEBnhLya2OX38Nt9DoL8K+pDfbncsbZR3WIi7PYysd043R0gxKL/lNh9qM9quJq
noSEeruTidi8foY12Ewg8aNyH324FL2YoevnpPDsKnYu9PEWDtzgFDZDDSXksLvG
JITJlxUR3h9KxjU+AYaSkXIy6RS5GT3O3+PNG5qBvPl7Ss0hZQFlltdhKiKLZkw4
```

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

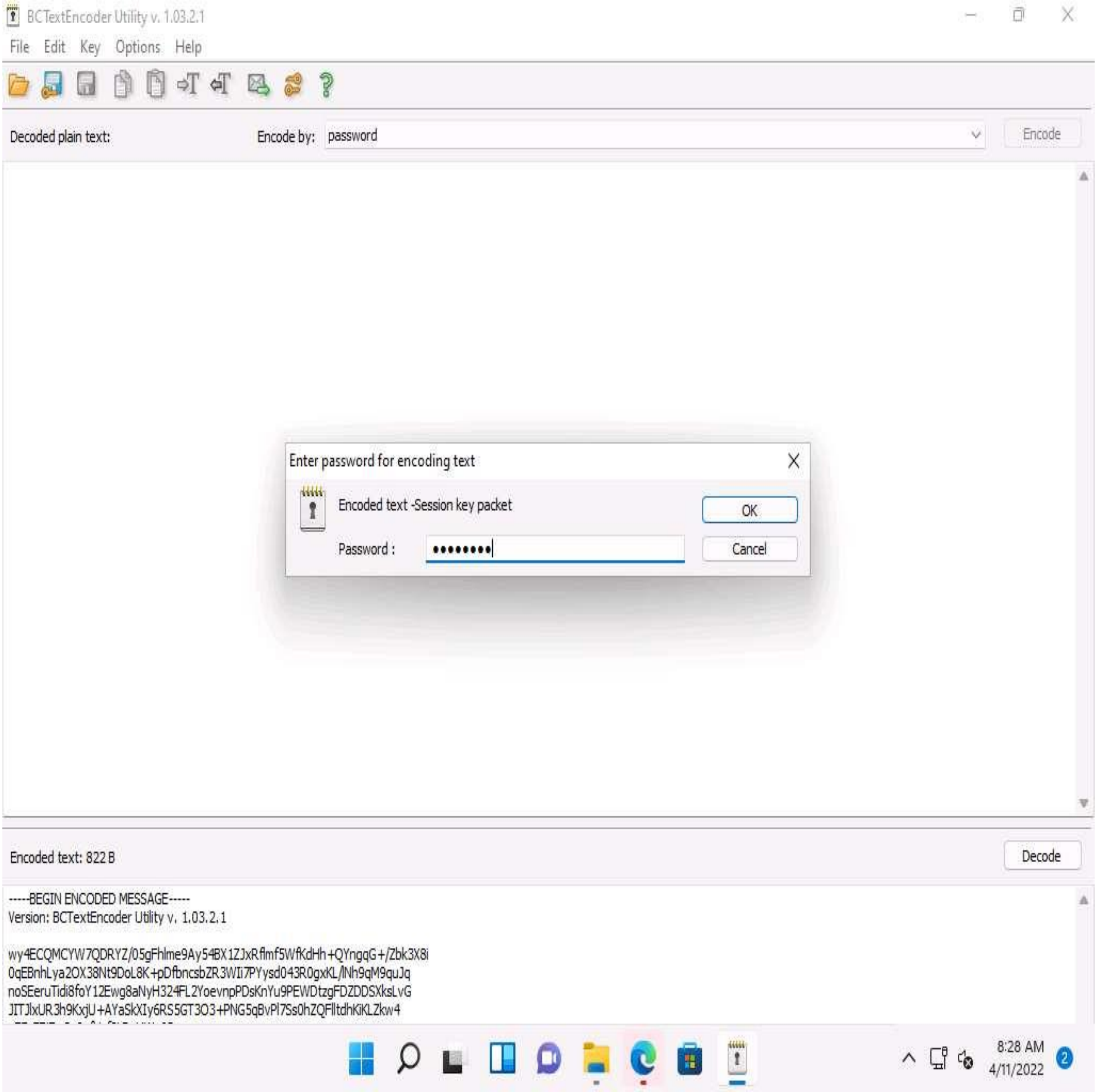


Encoded text: 822 B

```
-----BEGIN ENCODED MESSAGE-----
Version: BCTextEncoder Utility v. 1.03.2.1

wy4ECQMCYW7QDRYZ/05gFhlme9Ay54BX1ZJxRflmf5WfKdHh+QYngqG+/Zbk3X8i
0qEBnhLya2OX38Nt9DoL8K+pDfbncsbZR3WIi7PYysd043R0gxKL/lNh9qM9quJq
noSEeruTidi8foY12Ewg8aNyH324FL2YoevnpPDsKnYu9PEWDtzgFDZDDSXksLvG
JITJlxUR3h9KxjU+AYaSkXIy6RS5GT3O3+PNG5qBvPl7Ss0hZQFlltdhKiKLZkw4
```

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

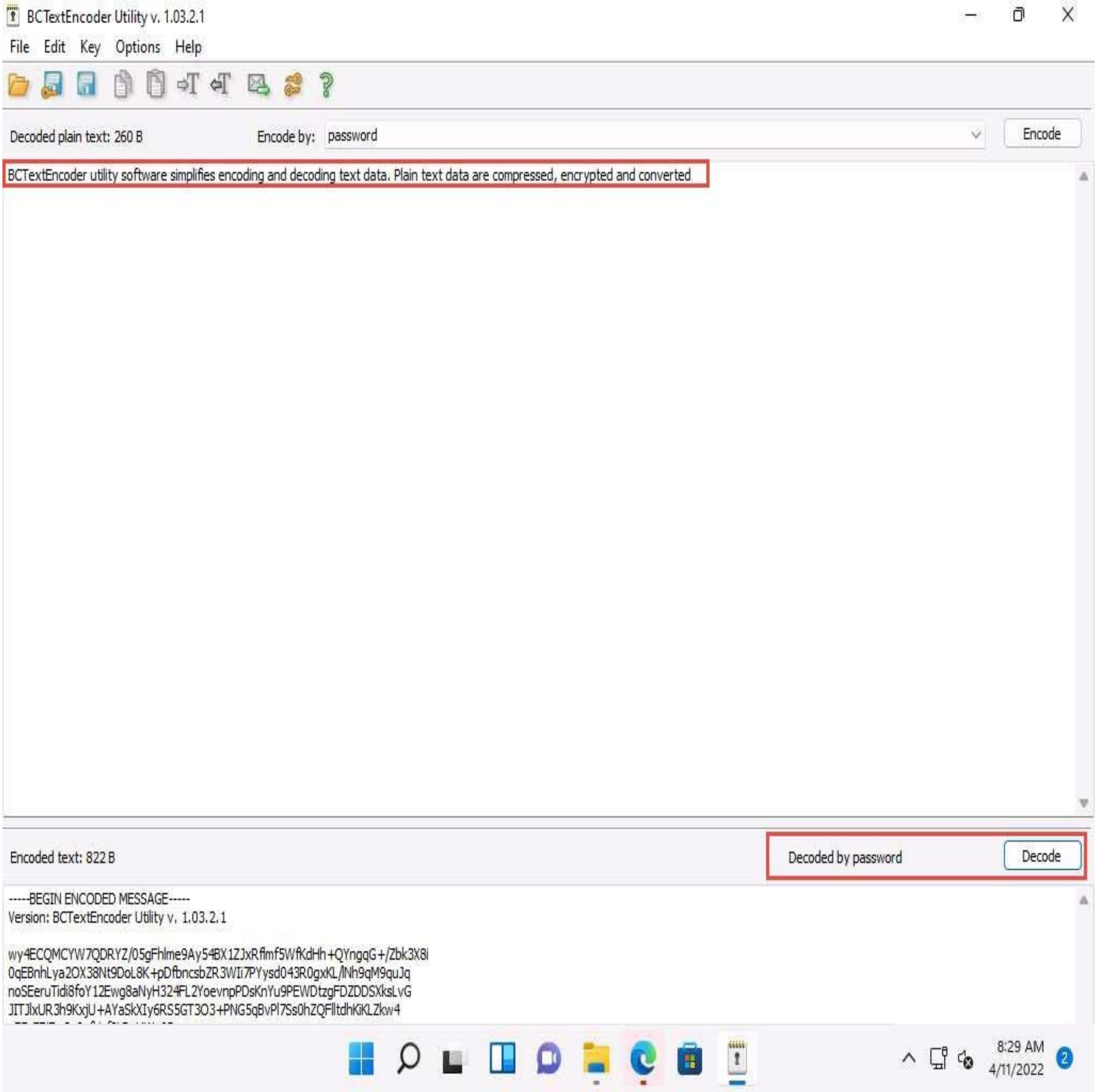


BCTextEncoder Utility v. 1.03.2.1
File Edit Key Options Help
Decoded plain text:
Encode by: password
Encode
Enter password for encoding text
Encoded text -Session key packet
Password : ••••••••
OK
Cancel
Encoded text: 822 B
Decode
8:28 AM
4/11/2022

```
-----BEGIN ENCODED MESSAGE-----
Version: BCTextEncoder Utility v. 1.03.2.1

wy4ECQMCYW7QDRYZ/05gFhlme9Ay54BX1ZJxRflmf5WfKdHh+QYngqG+/Zbk3X8i
0qEBnhLya2OX38Nt9DoL8K+pDfbncsbZR3WIi7PYysd043R0gxKL/lNh9qM9quJq
noSEeruTidi8foY12Ewg8aNyH324FL2YoevnpPDsKnYu9PEWDtzgFDZDDSXksLvG
JITJlxUR3h9KxjU+AYaSkXIy6RS5GT3O3+PNG5qBvPl7Ss0hZQFlltdhKiKLZkw4
```

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



Decoded plain text: 260 B

Encode by: password

BCTextEncoder utility software simplifies encoding and decoding text data. Plain text data are compressed, encrypted and converted

Encoded text: 822 B

Decoded by password

```
-----BEGIN ENCODED MESSAGE-----
Version: BCTextEncoder Utility v. 1.03.2.1

wy4ECQMCYW7QDRYZ/05gFhlme9Ay54BX1ZJxRflmf5WfKdHh+QYngqG+/Zbk3X8i
0qEBnhLya2OX38Nt9DoL8K+pDfbncsbZR3WIi7PYysd043R0gxKL/lNh9qM9quJq
noSEeruTidi8foY12Ewg8aNyH324FL2YoevnpPDsKnYu9PEWDtzgFDZDDSXksLvG
JITJlxUR3h9KxjU+AYaSkXIy6RS5GT3O3+PNG5qBvPl7Ss0hZQFlltdhKiKLZkw4
```

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. □ 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.
12. □ Close all open windows and document all the acquired information.