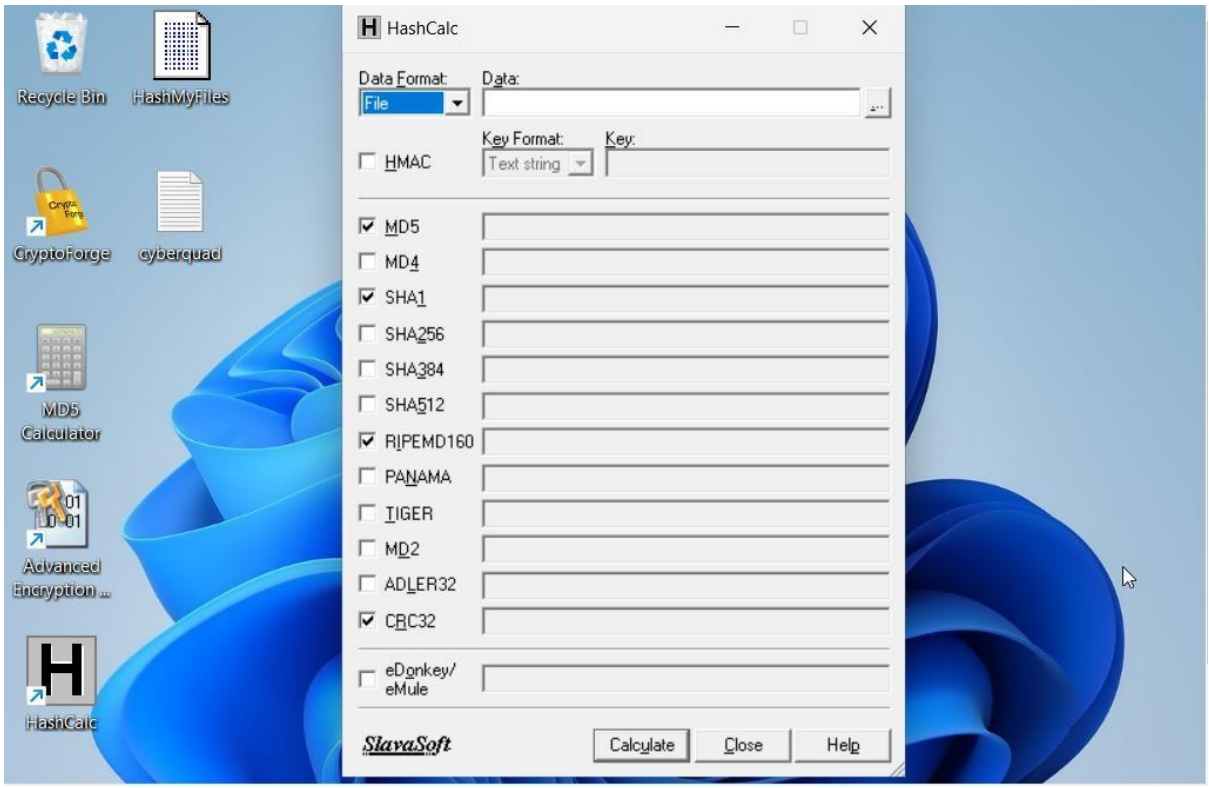
CRYPTOGRAPHY - BISF

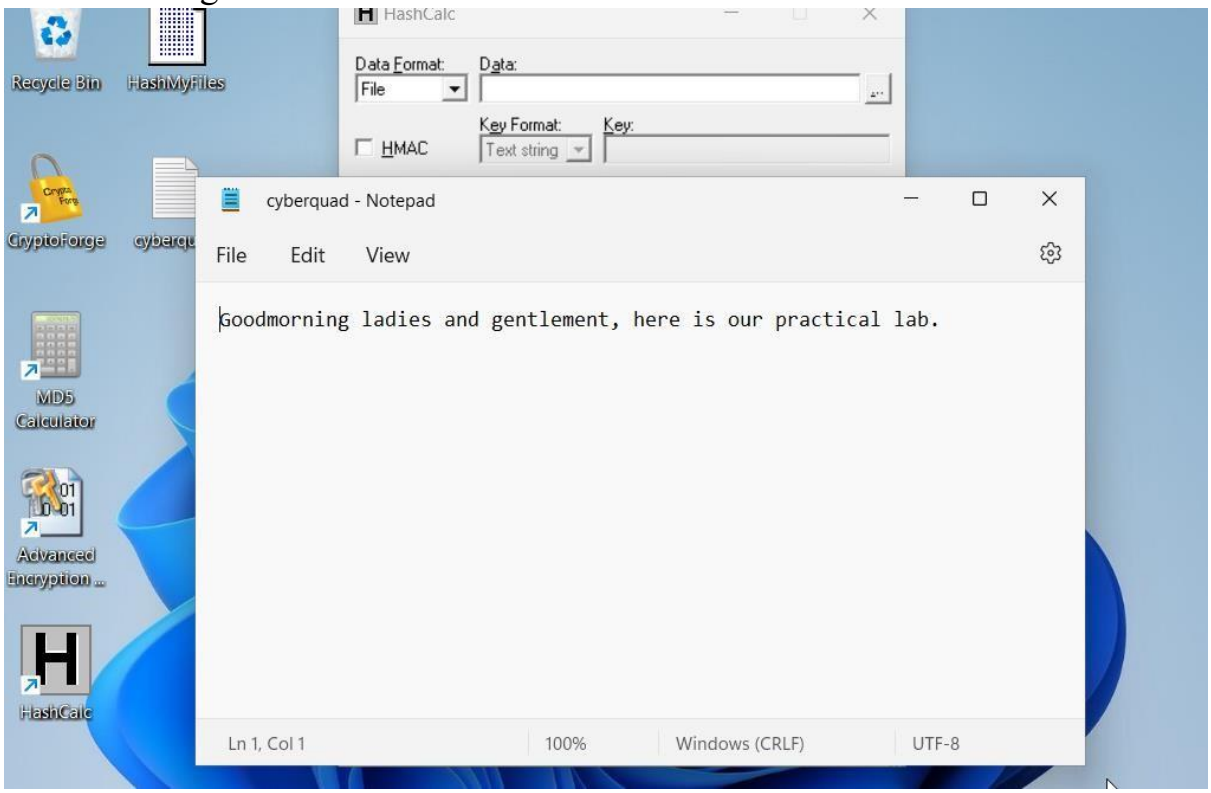
LAB 1

Task 1: Calculating one-way Hashes using HashCalc •

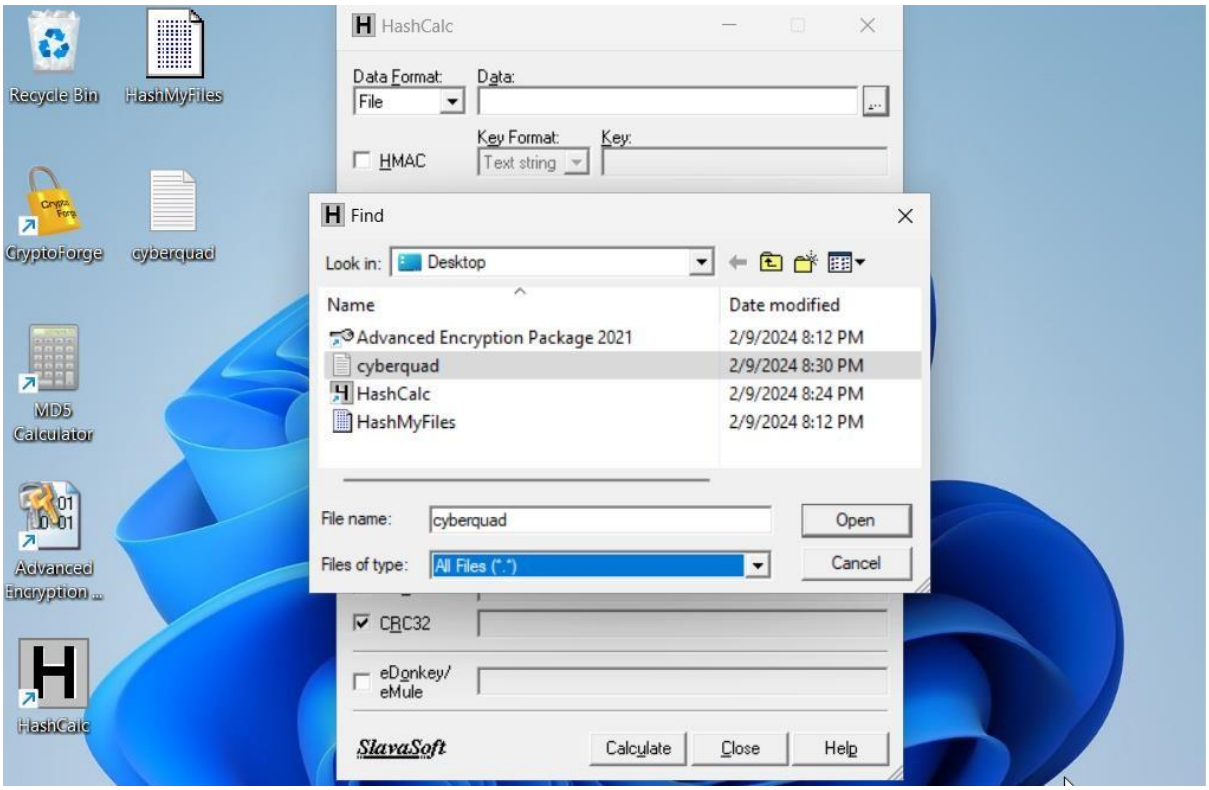
Launching HASHCALC.



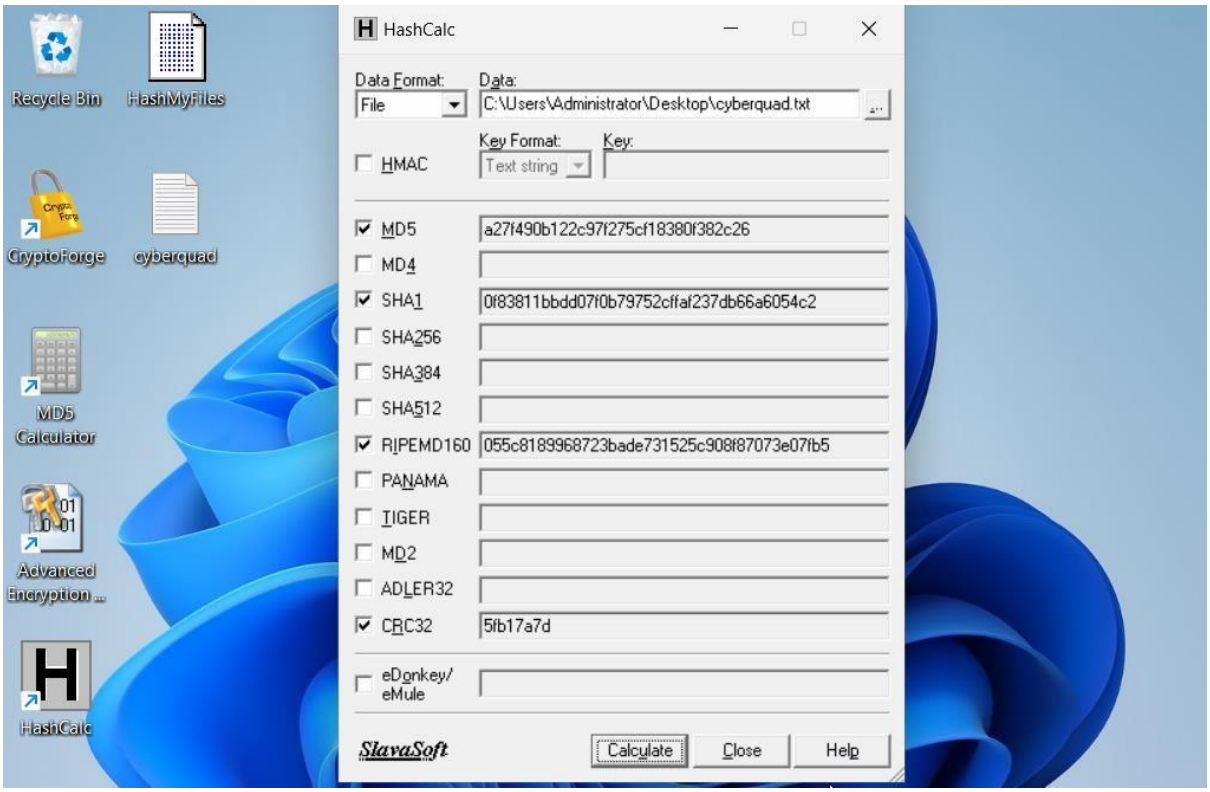
Creating a text file



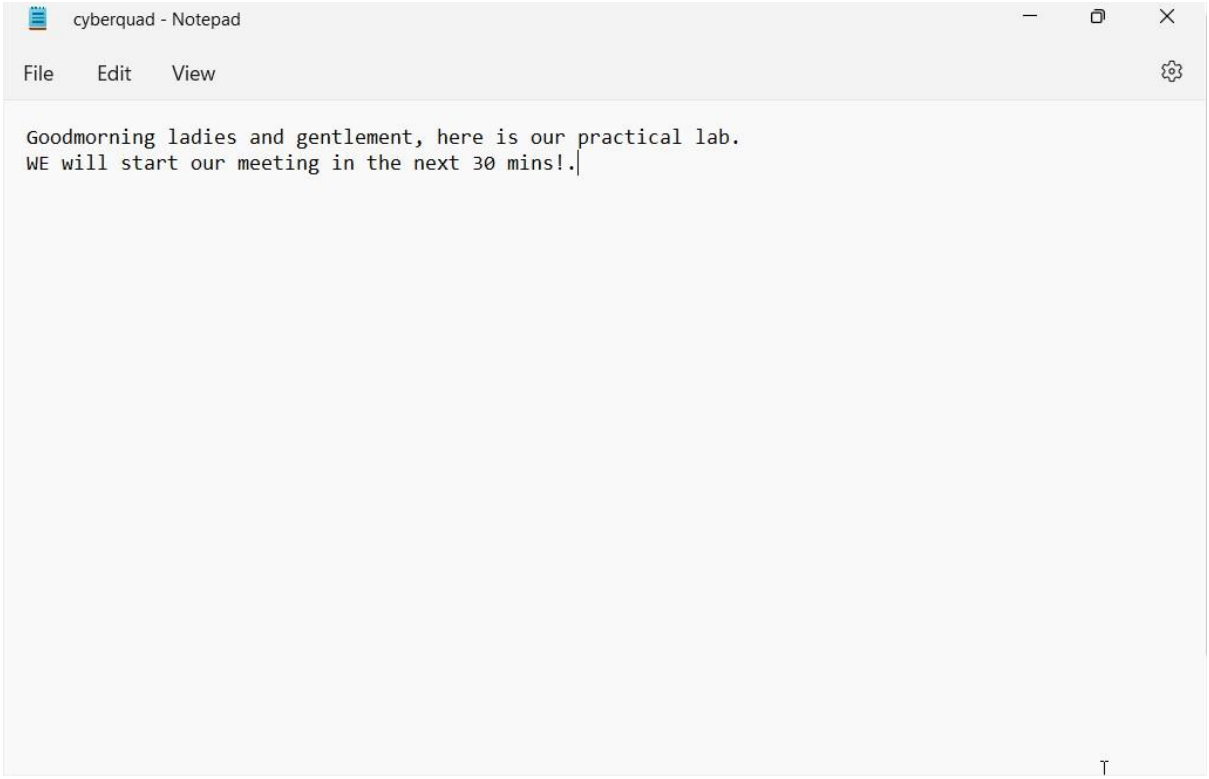
- Navigating to the location where the txt file is saved using HashCalc

- 
Recycle Bin
HashMyFiles
CryptoForge
cyberquad
MD5 Calculator
Advanced Encryption ...
HashCalc
HashCalc
Data Format:
File
Data:
HMAC
Key Format:
Text string
Key:
Find
Look in:
Desktop
Name
Date modified
Advanced Encryption Package 2021
2/9/2024 8:12 PM
cyberquad
2/9/2024 8:30 PM
HashCalc
2/9/2024 8:24 PM
HashMyFiles
2/9/2024 8:12 PM
File name:
cyberquad
Open
Files of type:
All Files (*.*)
Cancel
CRC32
eDonkey/ eMule
SlavaSoft
Calculate
Close
Help

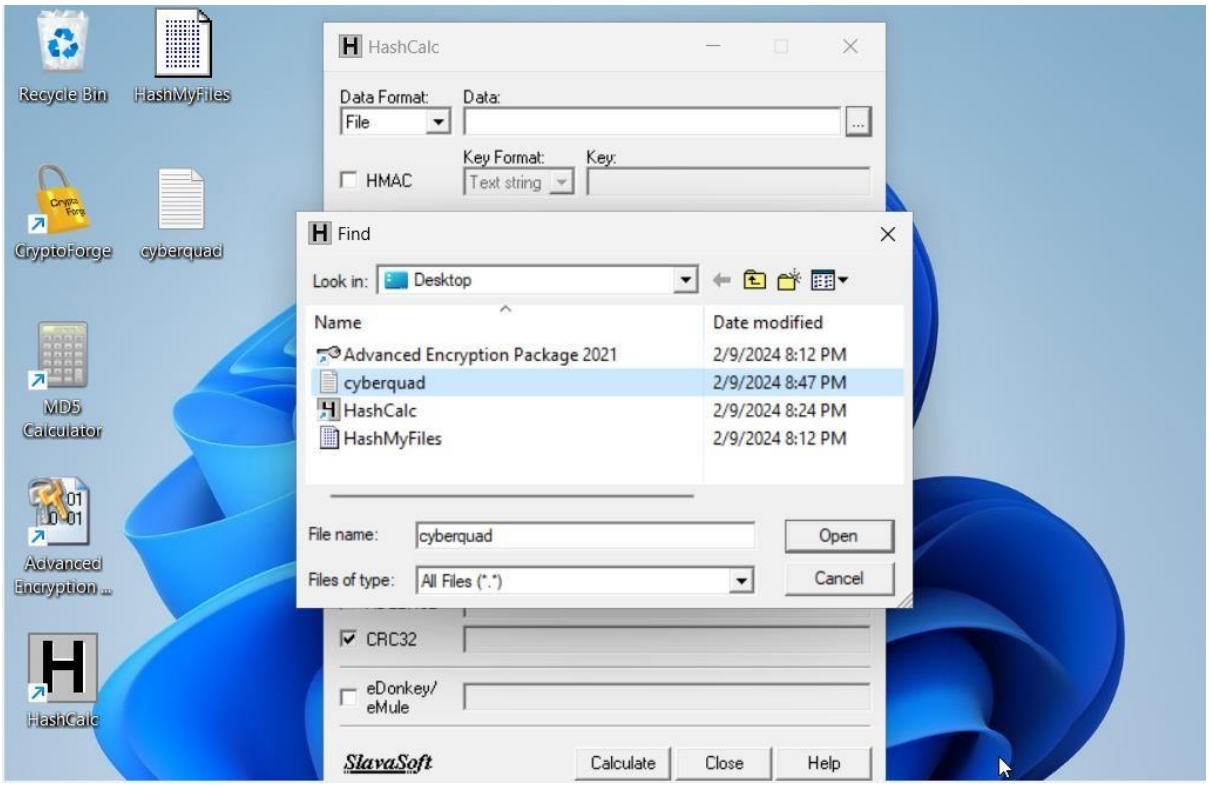
- Selecting Hash functions; MD5, SHA1, RIPEMD160, CRC32 and Calculate.

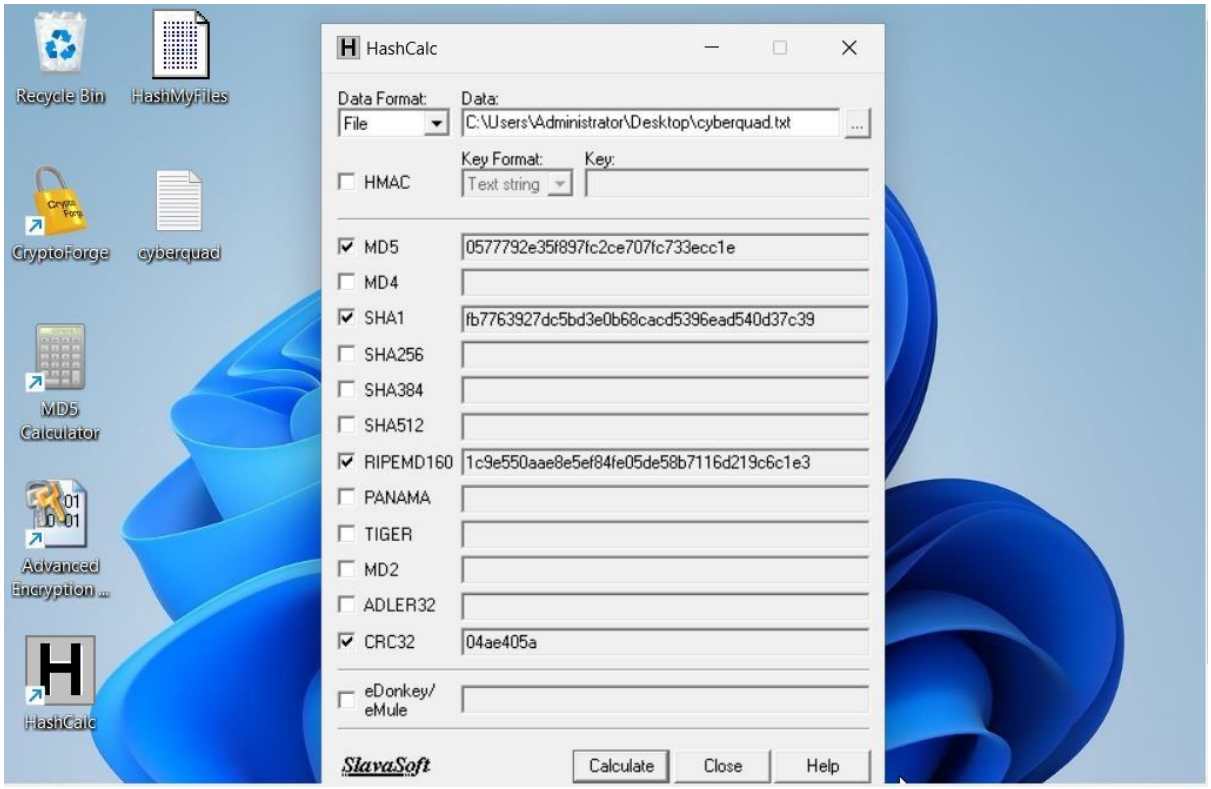


- Reopening the txt file and modify it by writing some text.

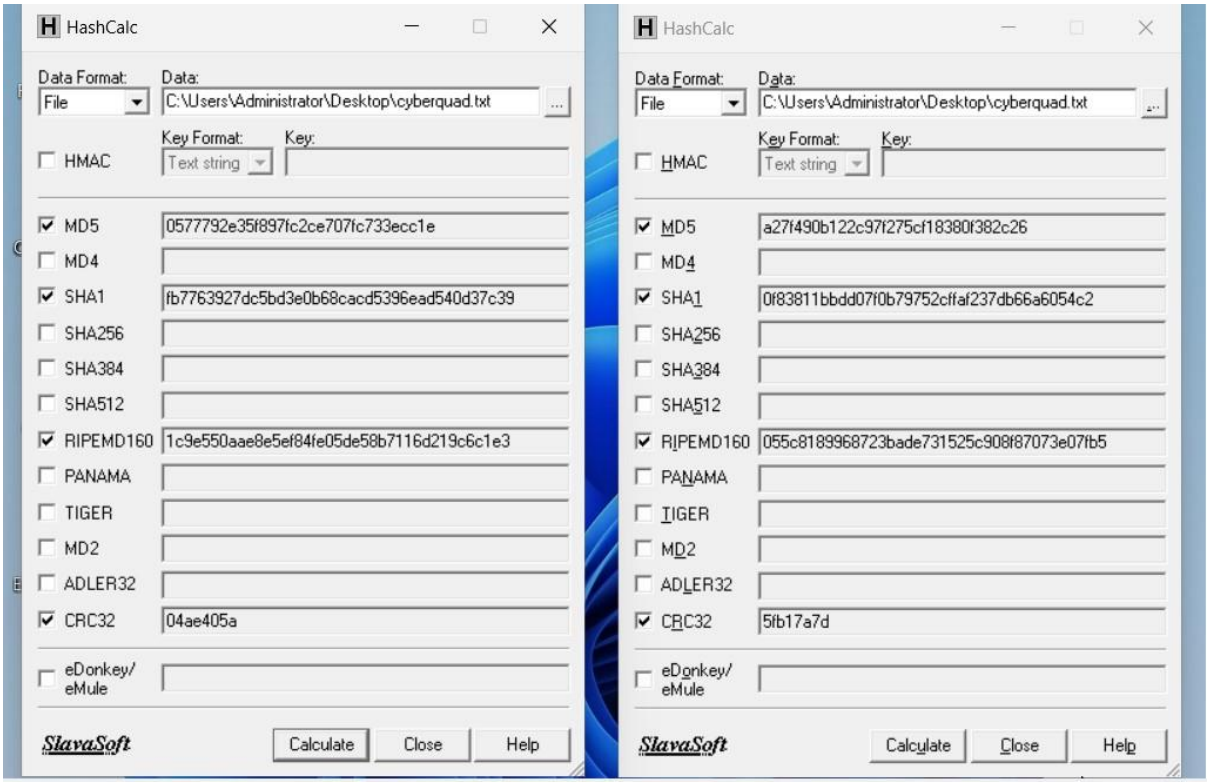
- 

Launching another HashCalc, Repeating the initial procedure.

- 
Recycle Bin
HashMyFiles
CryptoForge
cyberquad
MD5 Calculator
Advanced Encryption ...
HashCalc
HashCalc
Data Format:
File
Data:
HMAC
Key Format:
Text string
Key:
Find
Look in:
Desktop
Name
Date modified
Advanced Encryption Package 2021
2/9/2024 8:12 PM
cyberquad
2/9/2024 8:47 PM
HashCalc
2/9/2024 8:24 PM
HashMyFiles
2/9/2024 8:12 PM
File name:
cyberquad
Open
Files of type:
All Files (*.*)
Cancel
CRC32
eDonkey/ eMule
SlavaSoft
Calculate
Close
Help


Recycle Bin
HashMyFiles
CryptoForge
cyberquad
MD5 Calculator
Advanced Encryption ...
HashCalc
HashCalc
Data Format:
File
Data:
C:\Users\Administrator\Desktop\cyberquad.txt
HMAC
Key Format:
Text string
Key:
MD5
0577792e35f897fc2ce707fc733ecc1e
MD4
SHA1
fb7763927dc5bd3e0b68cacd5396ead540d37c39
SHA256
SHA384
SHA512
RIPEMD160
1c9e550aae8e5ef84fe05de58b7116d219c6c1e3
PANAMA
TIGER
MD2
ADLER32
CRC32
04ae405a
eDonkey/ eMule
SlavaSoft
Calculate
Close
Help

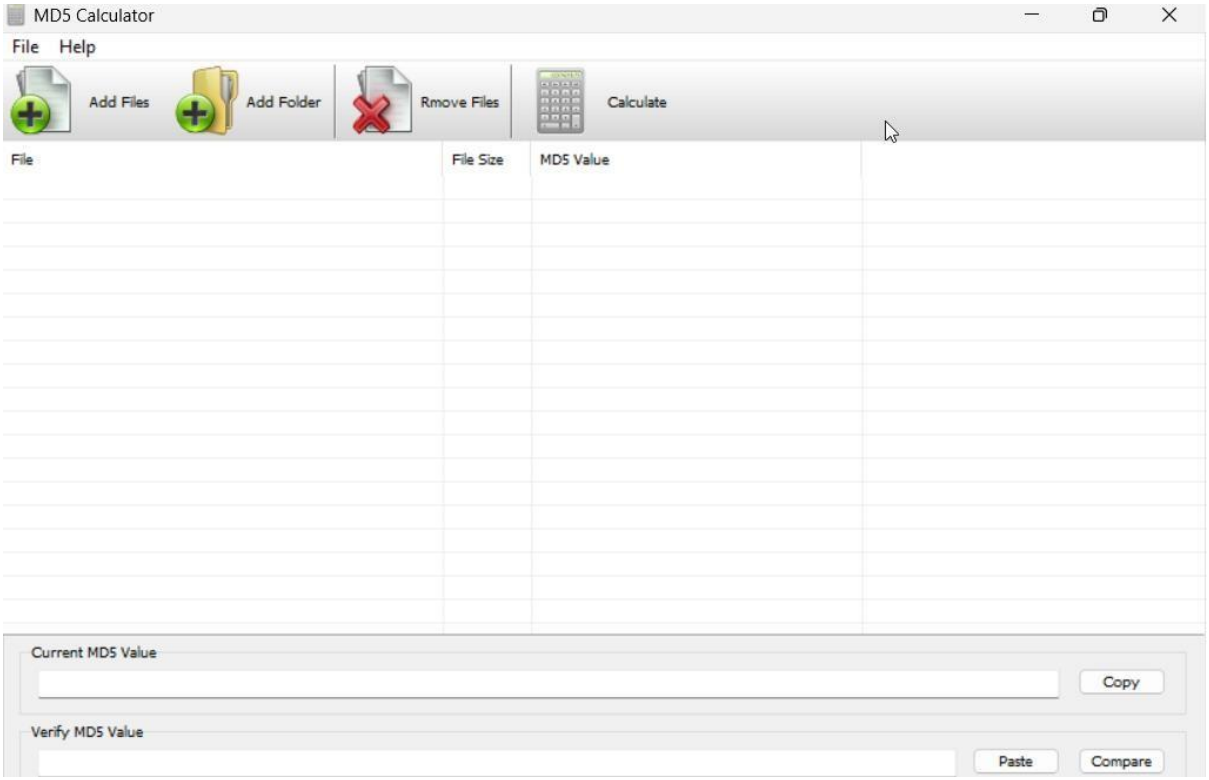
- Comparing the both outcomes of the hash values before and after modification.



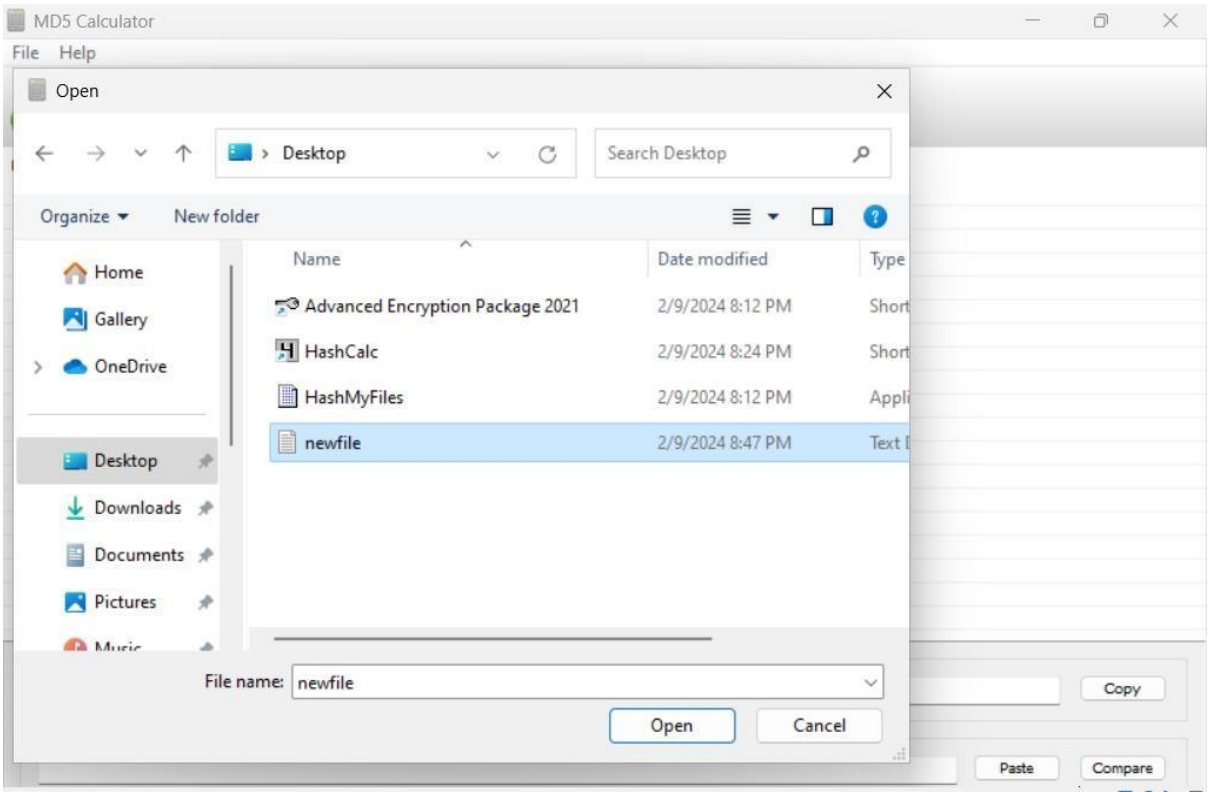
•

Task 2

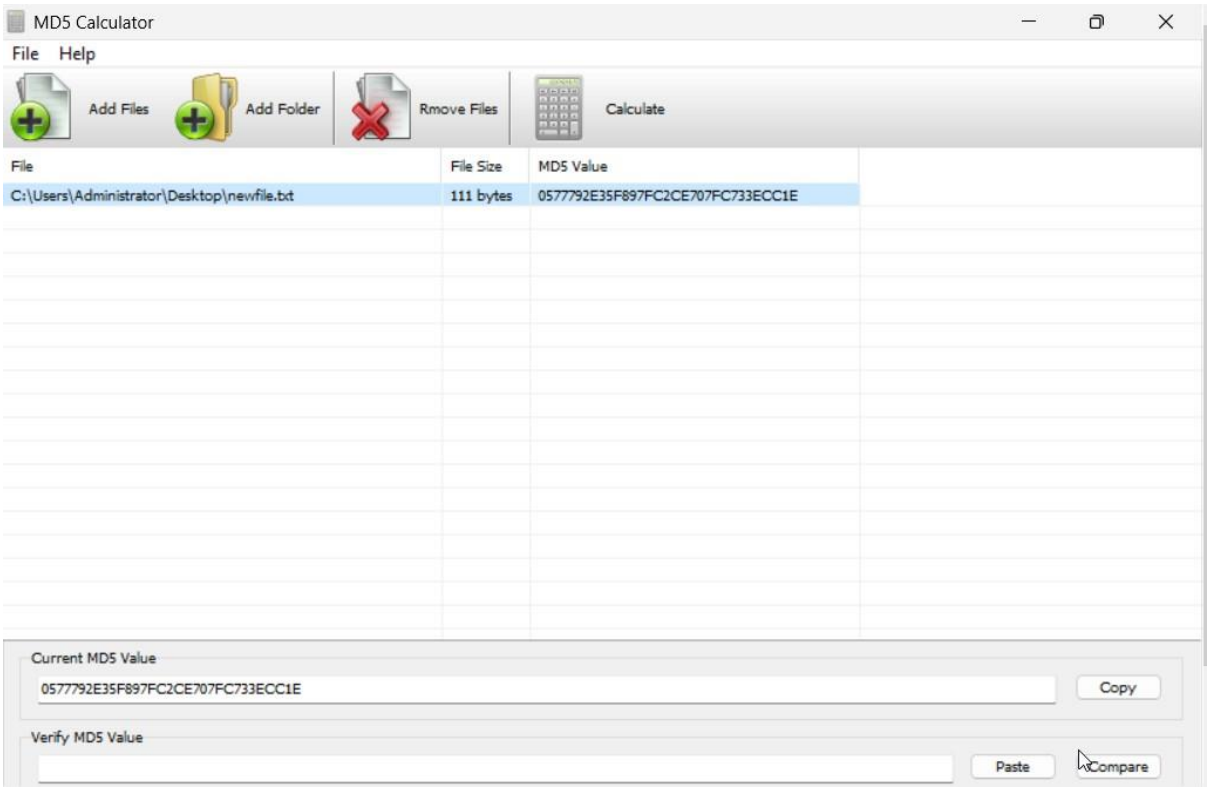
- Launching MD5 calc



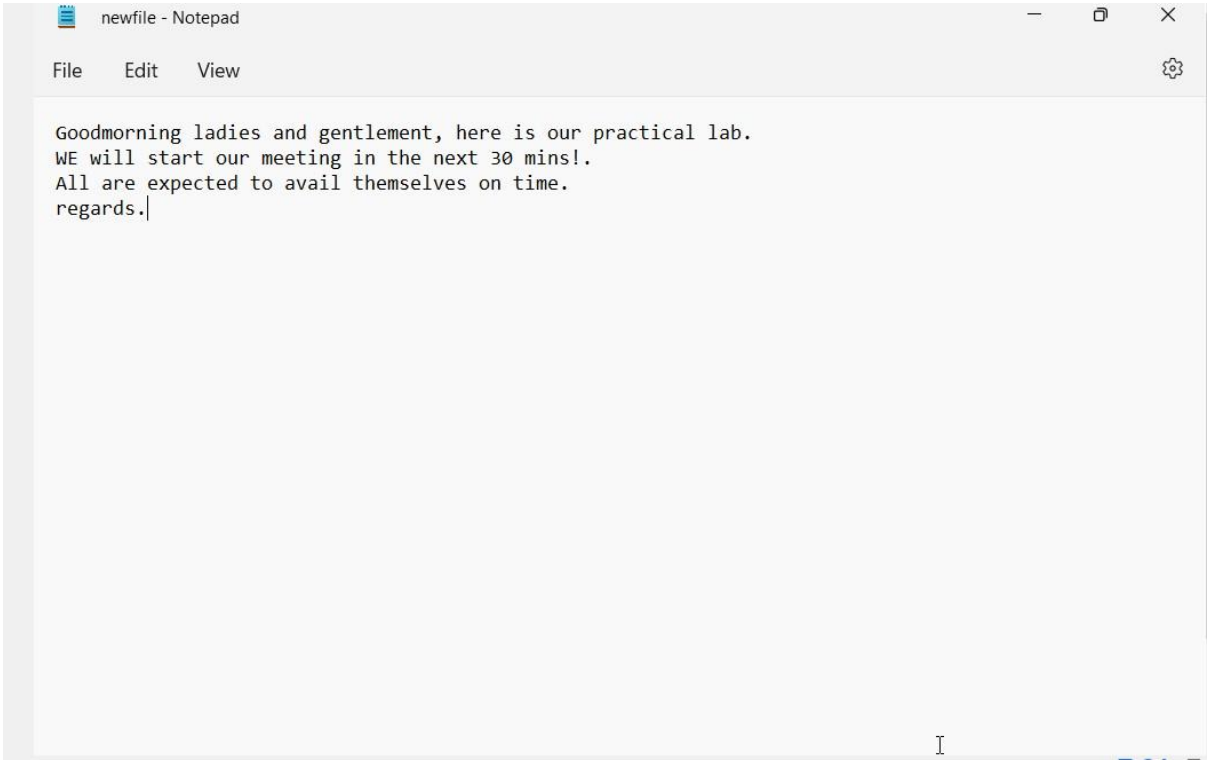
- Adding A file in MD5cal window



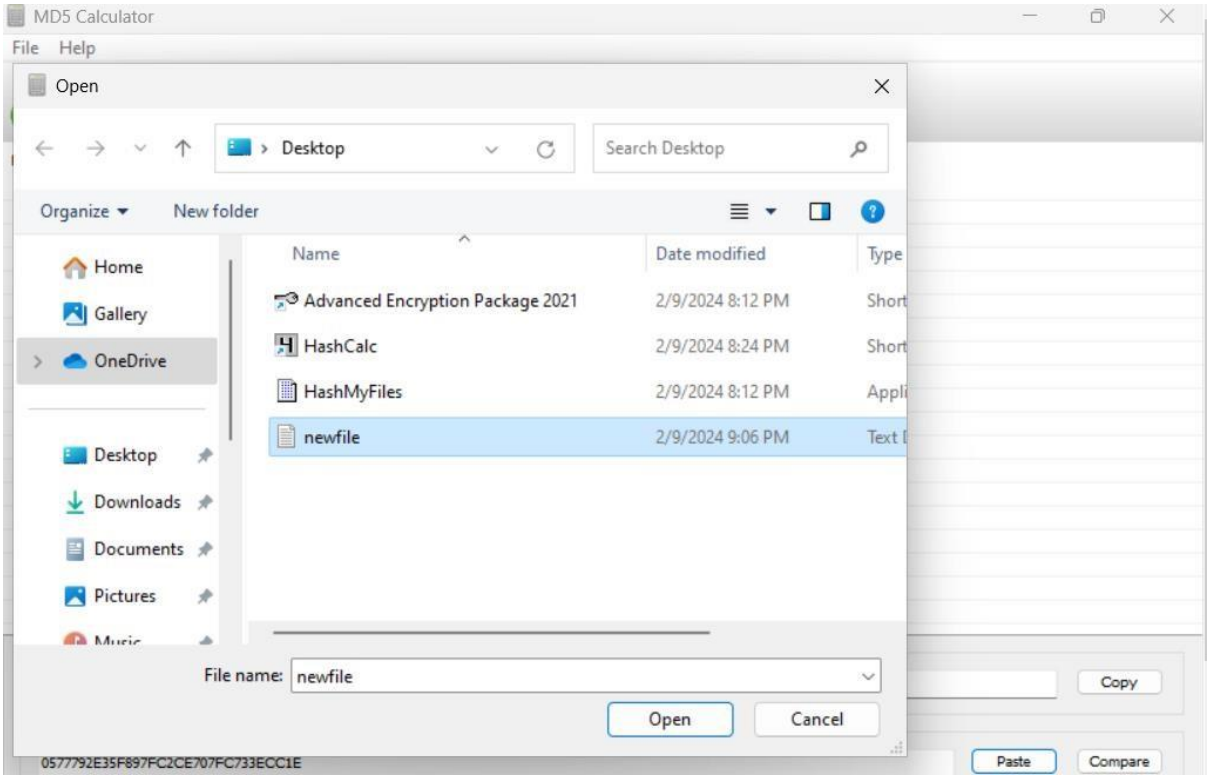
Calculating the Hash value on MD5 Calc

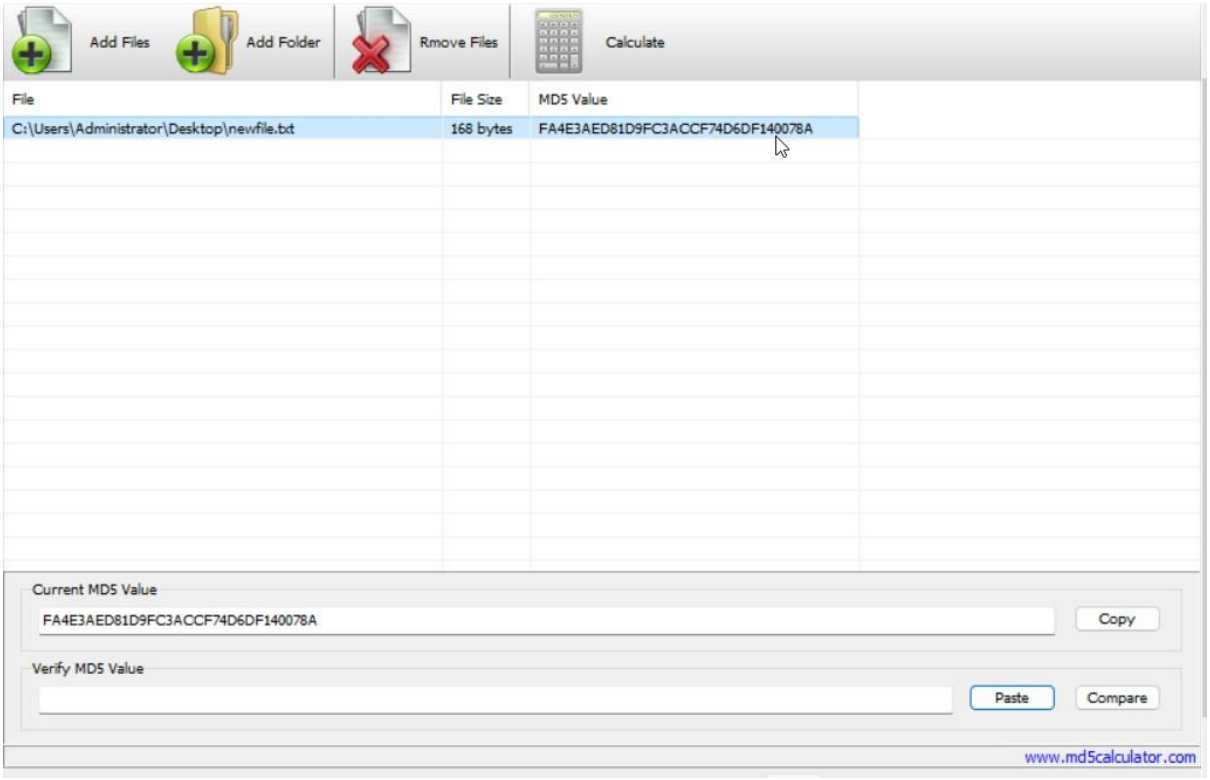


- Coping the calculated hash value and removing file from the MD5 calc.
- Open and modify the text file.

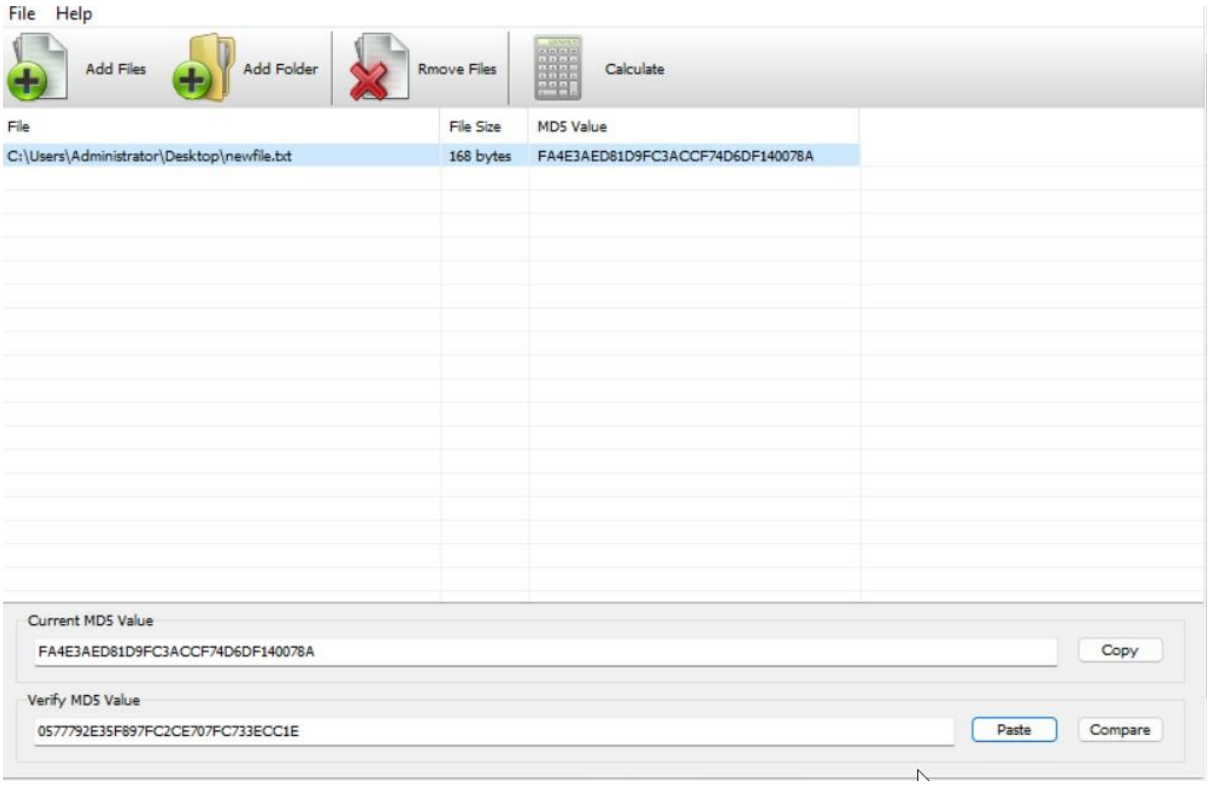


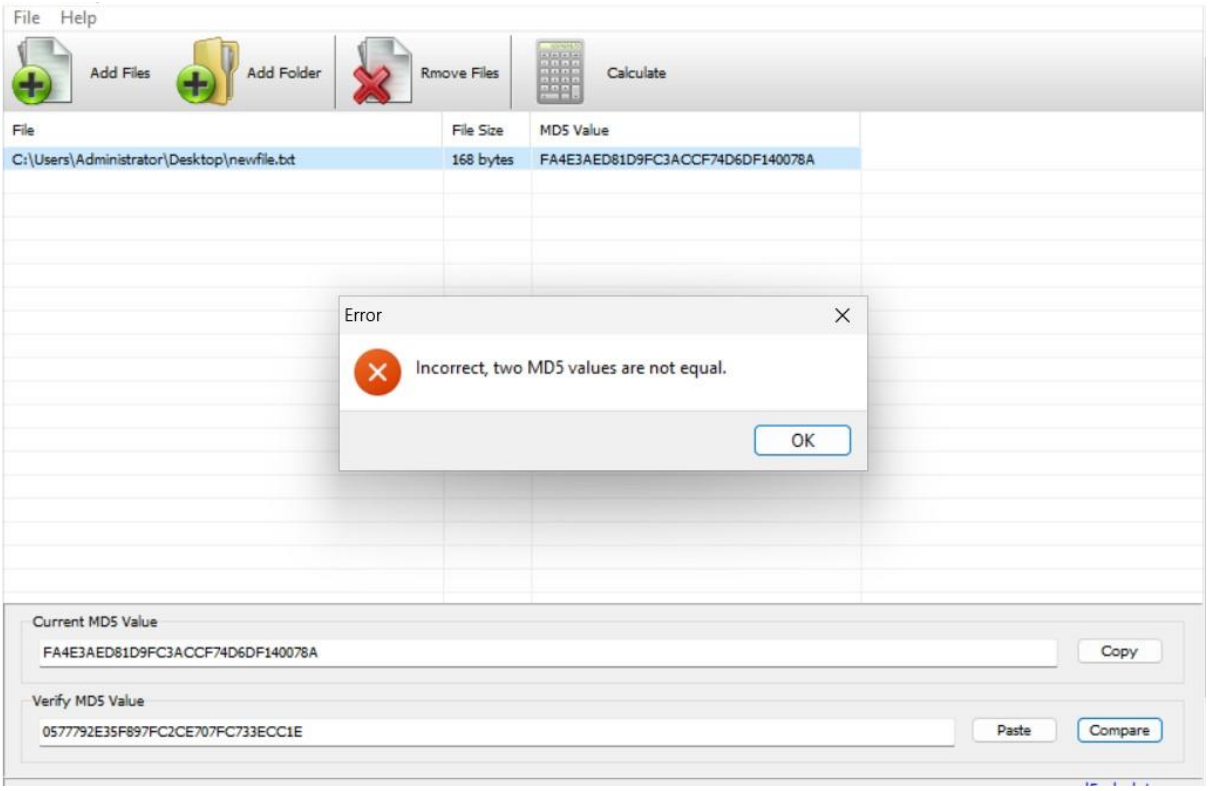
- Perform the previous steps.

- 



Comparing the previous and current generated hash values in the MD5 calculator.


File Help
Add Files
Add Folder
Rmove Files
Calculate
File
File Size
MD5 Value
C:\Users\Administrator\Desktop\newfile.txt
168 bytes
FA4E3AED81D9FC3ACCF74D6DF140078A
Current MD5 Value
FA4E3AED81D9FC3ACCF74D6DF140078A
Copy
Verify MD5 Value
0577792E35F897FC2CE707FC733ECC1E
Paste
Compare

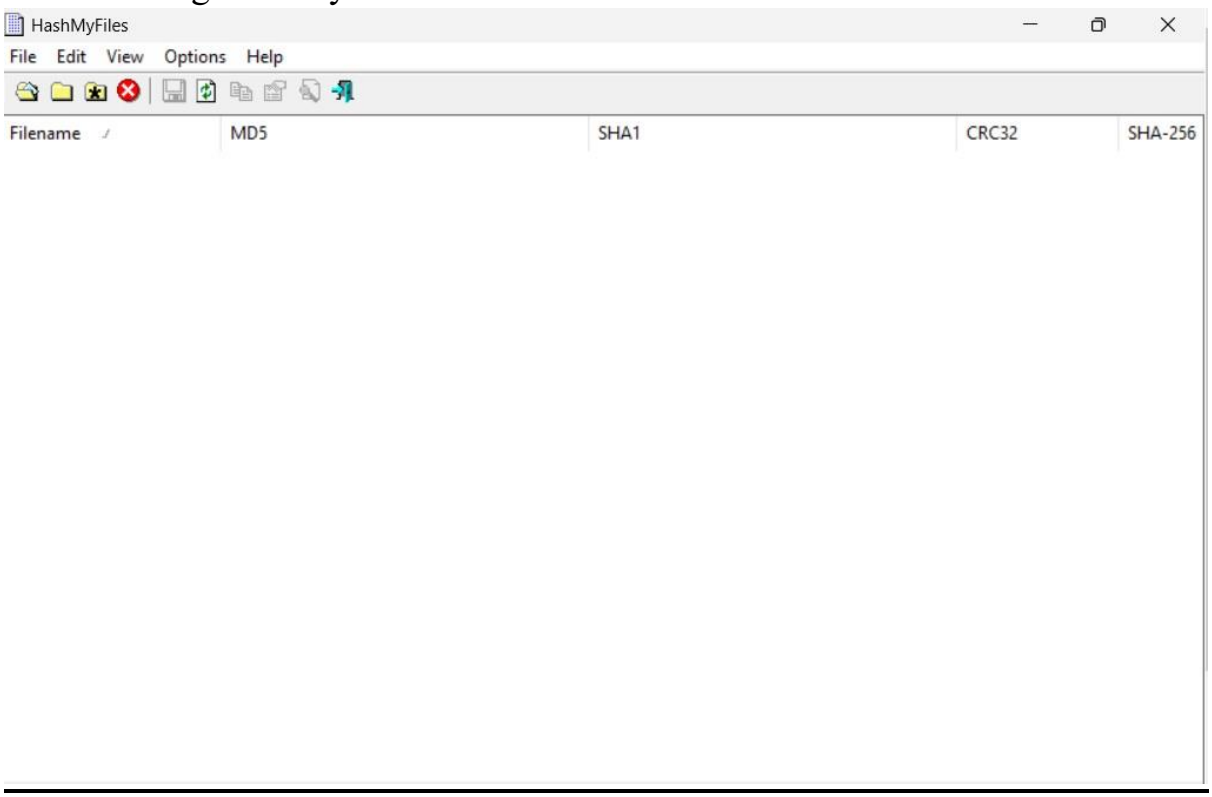

File Help
Add Files
Add Folder
Rmove Files
Calculate
File
File Size
MD5 Value
C:\Users\Administrator\Desktop\newfile.txt
168 bytes
FA4E3AED81D9FC3ACCF74D6DF140078A
Error
Incorrect, two MD5 values are not equal.
OK
Current MD5 Value
FA4E3AED81D9FC3ACCF74D6DF140078A
Copy
Verify MD5 Value
0577792E35F897FC2CE707FC733ECC1E
Paste
Compare

Task 3

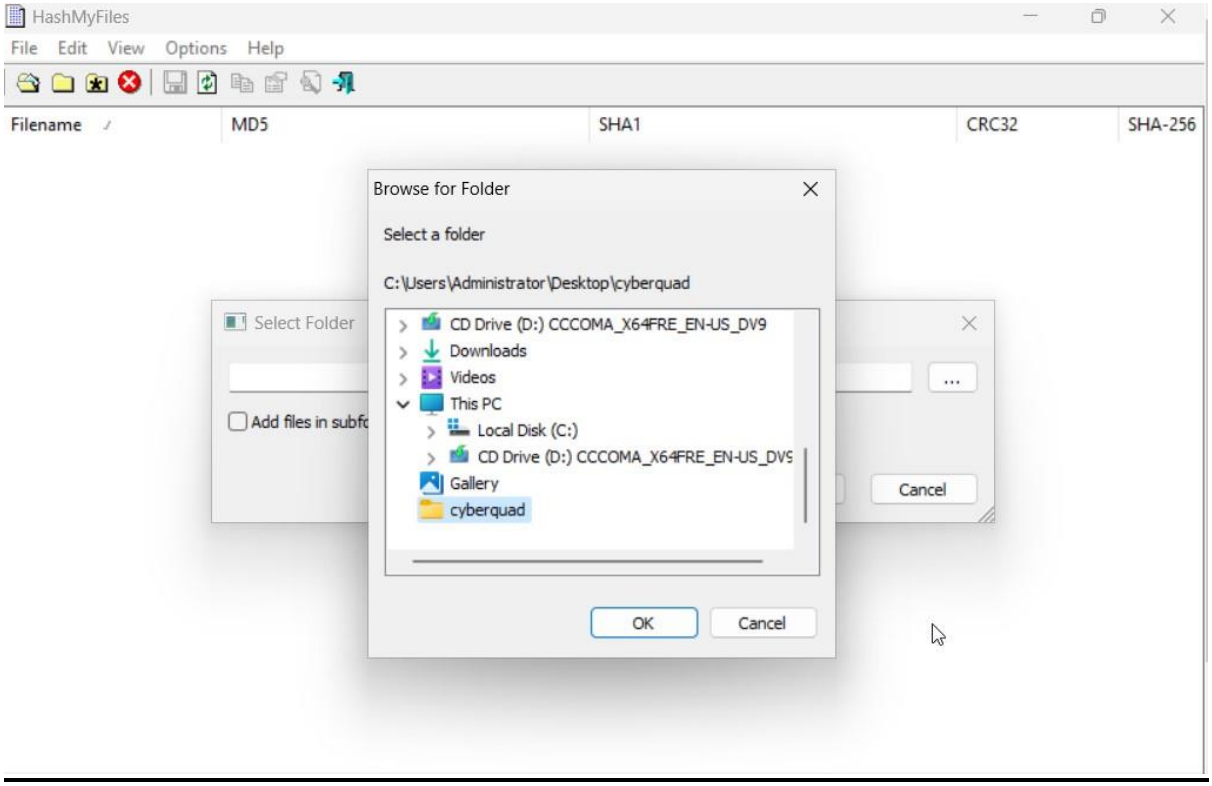
•

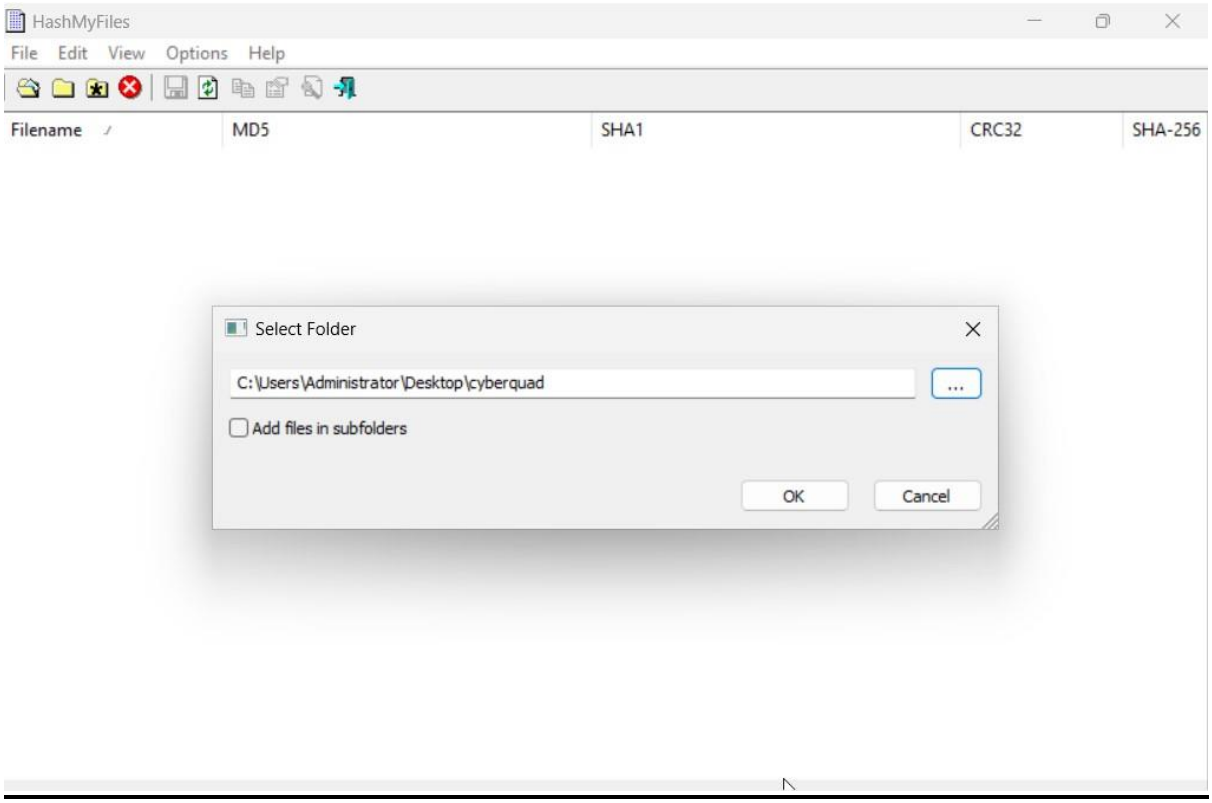
Calculating MD5 hashes using HashMyfile

- Launching HashMyfile



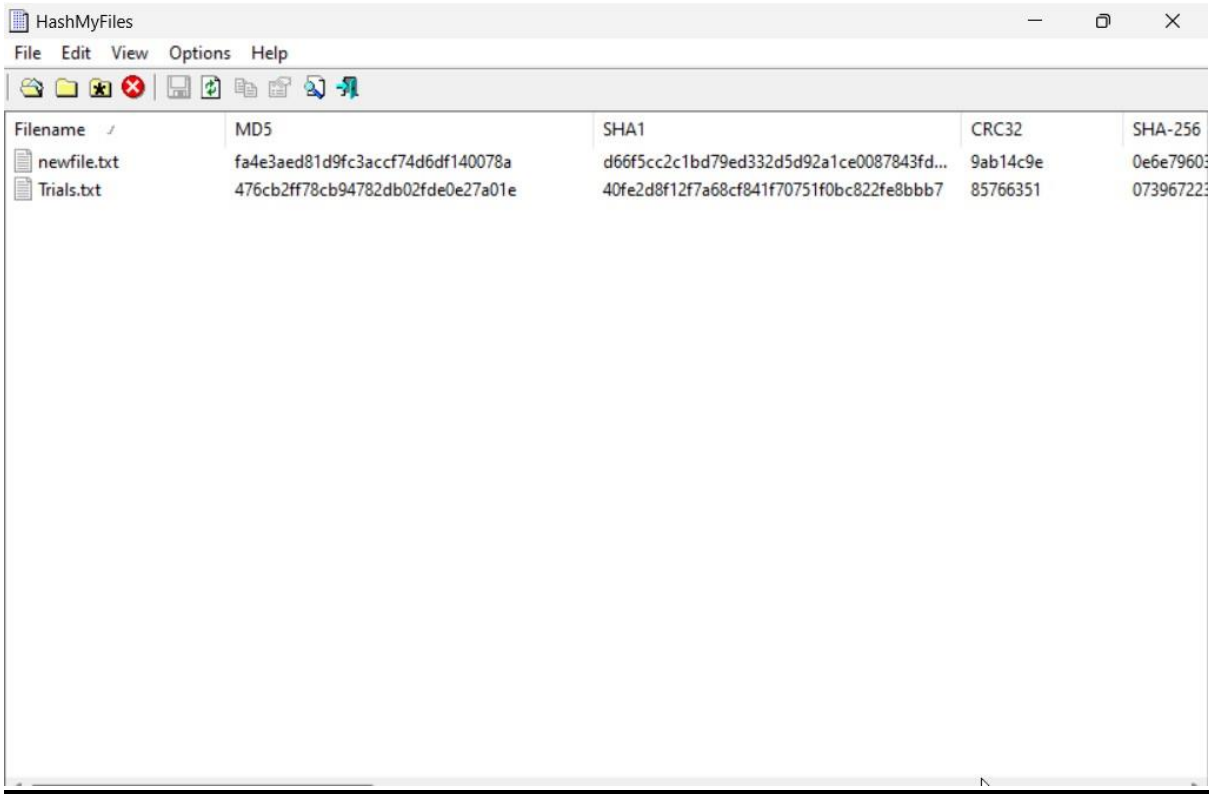
Navigating the folder to encrypt through HashMyfile



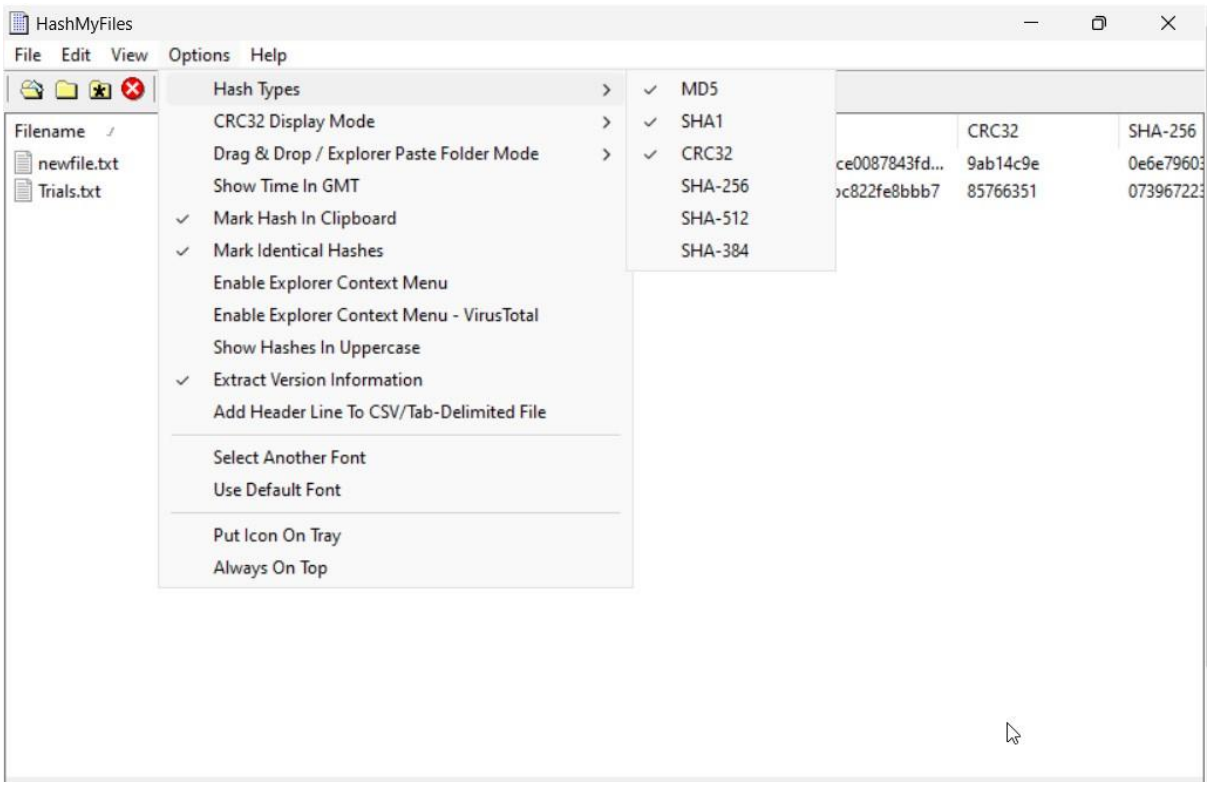


- Files from the folder appears along with their corresponding hash values.

•

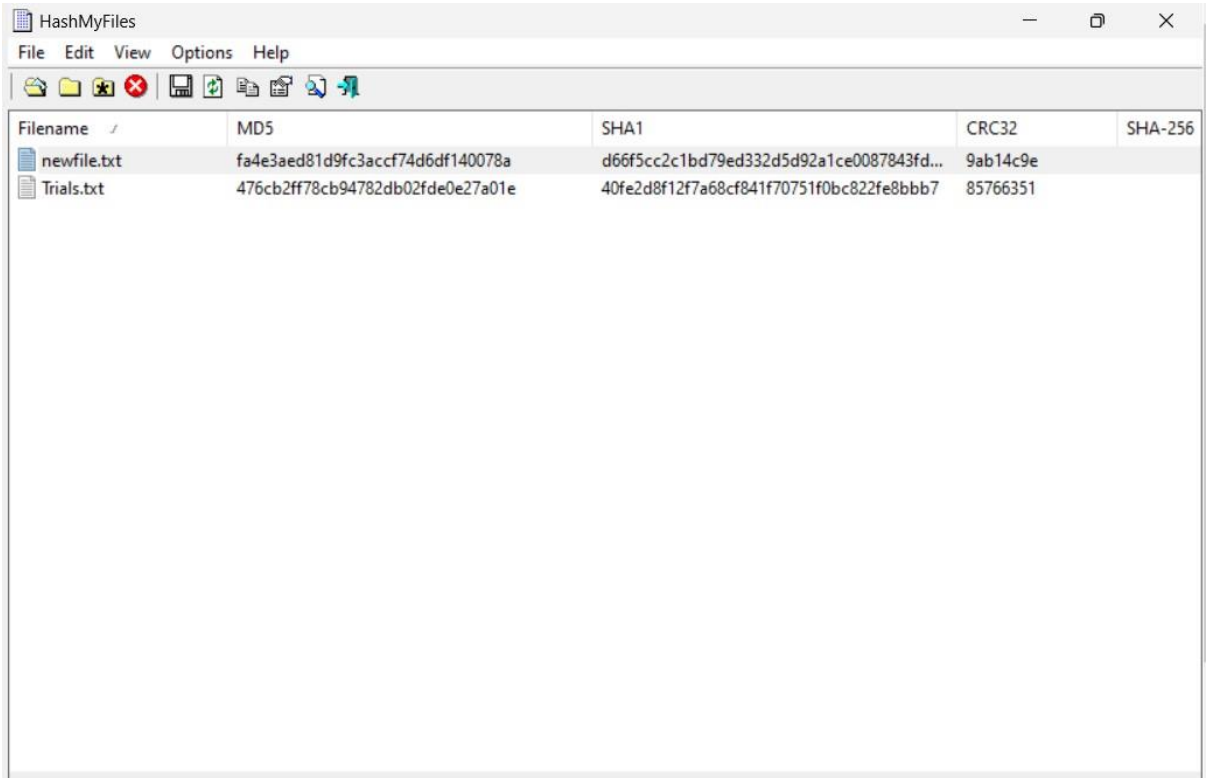


• Choosing hash types from HashMyfile.



Click refresh option from the menu

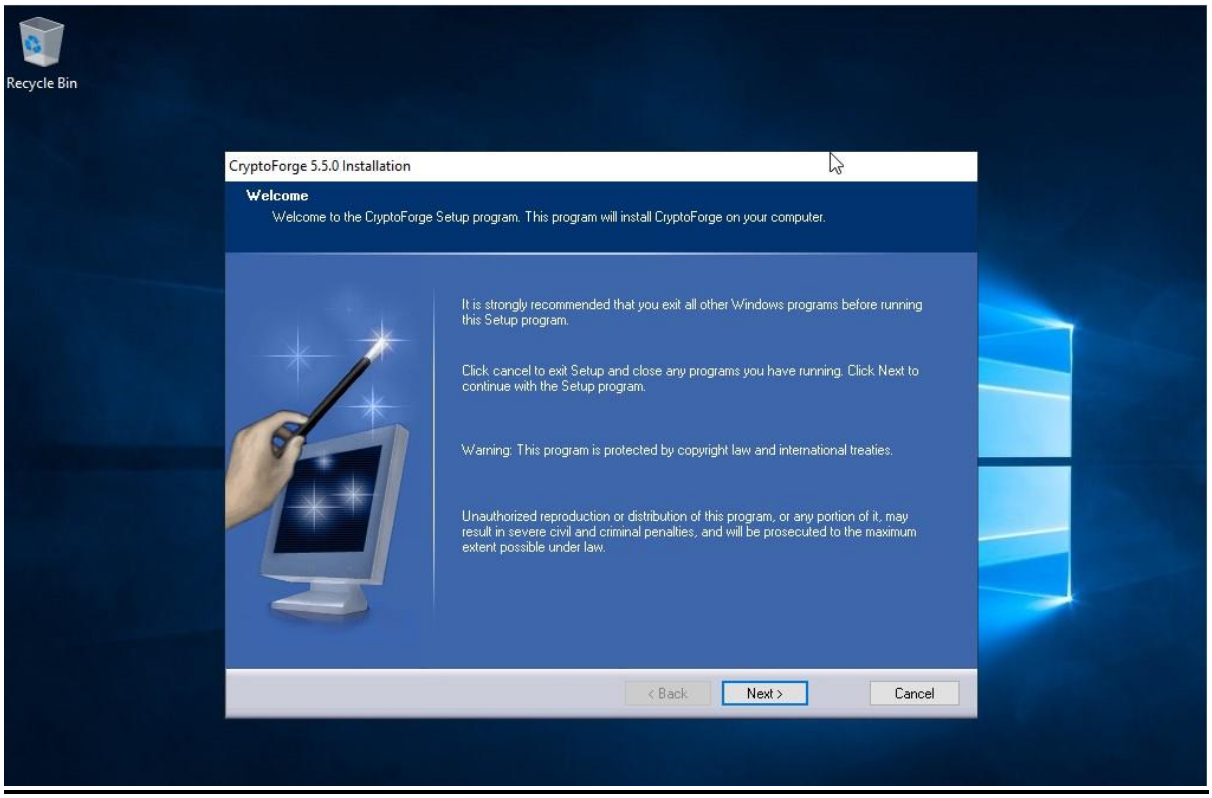
- Hash values of the selected hash types are displayed.

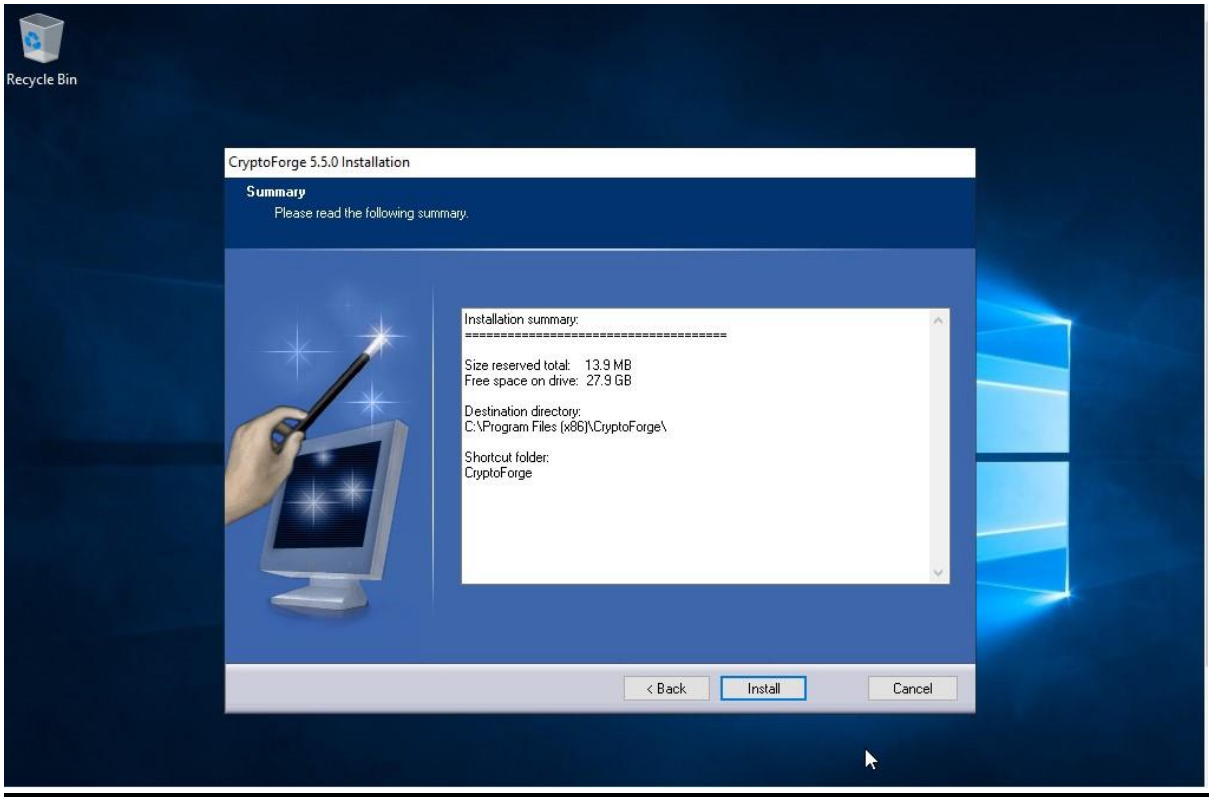


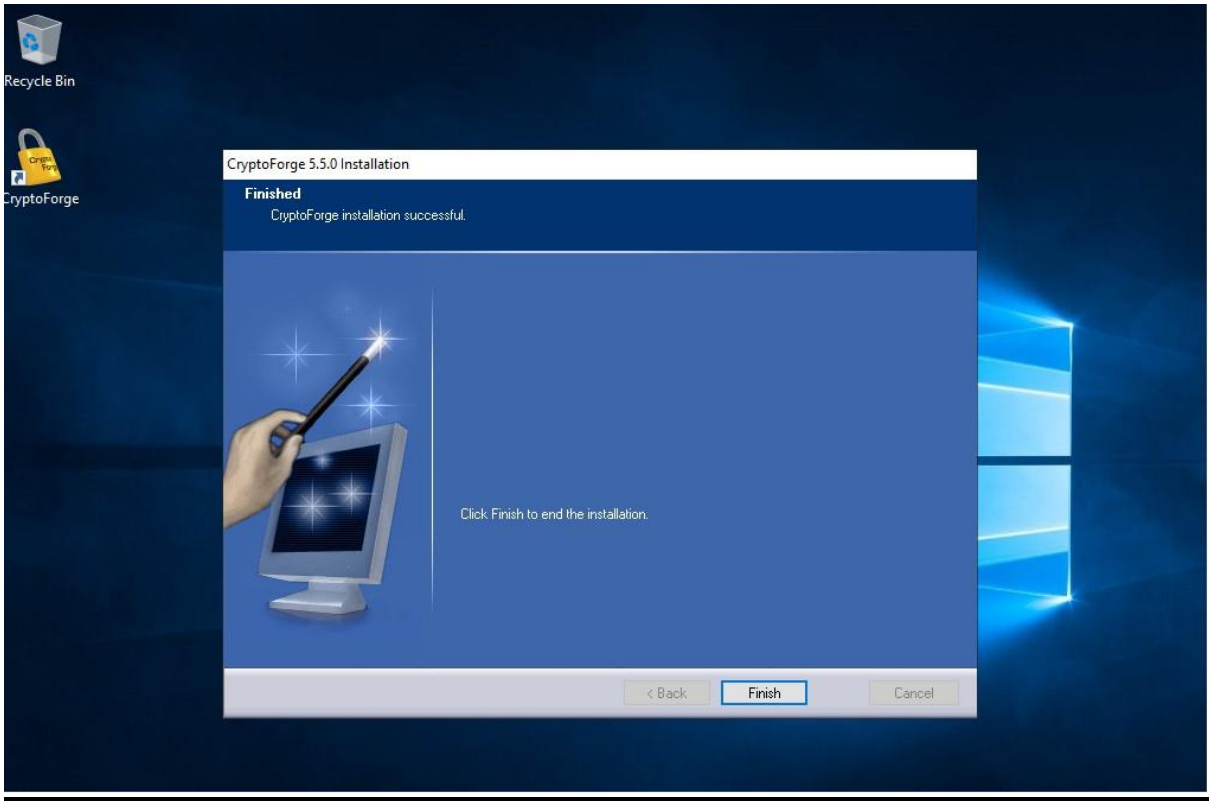
Task 4

Installing cryptoforge in both windows 11 and windows server virtual machines

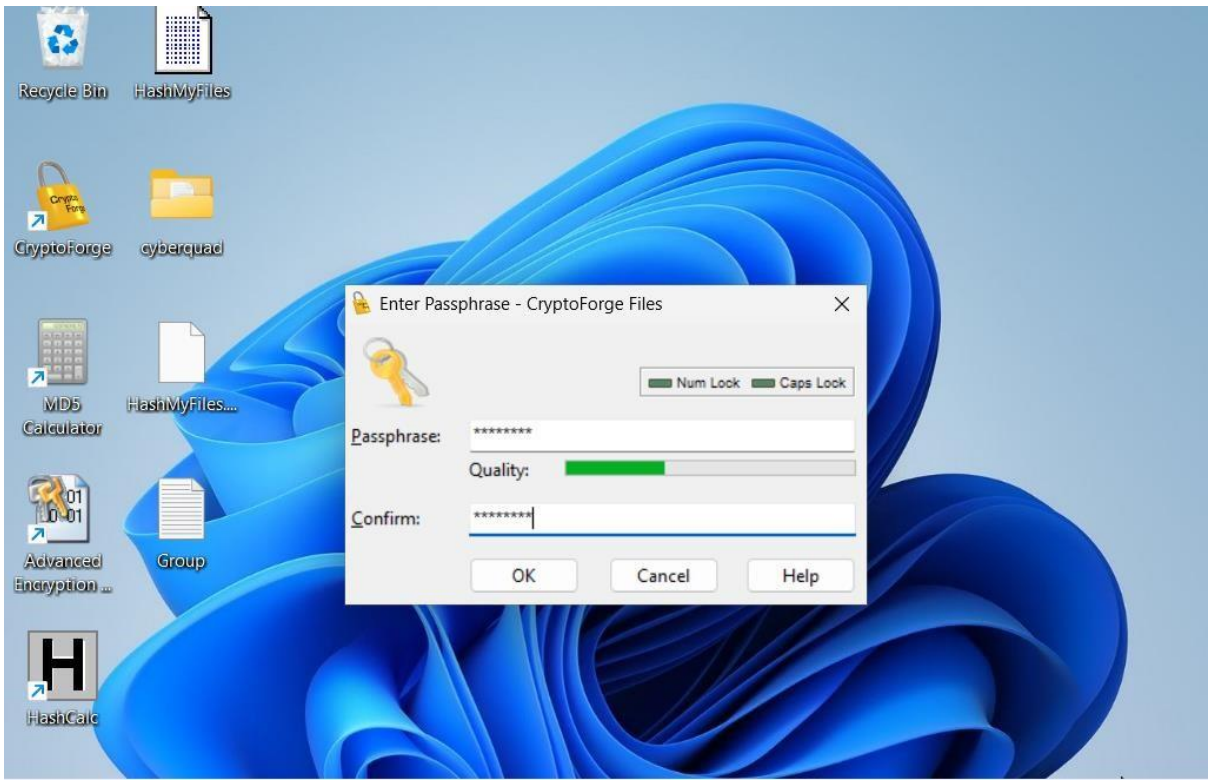
-


Recycle Bin
CryptoForge 5.5.0 Installation
Welcome
Welcome to the CryptoForge Setup program. This program will install CryptoForge on your computer.
It is strongly recommended that you exit all other Windows programs before running this Setup program.
Click cancel to exit Setup and close any programs you have running. Click Next to continue with the Setup program.
Warning: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
< Back
Next >
Cancel


Recycle Bin
CryptoForge 5.5.0 Installation
Summary
Please read the following summary.
Installation summary:
Size reserved total: 13.9 MB
Free space on drive: 27.9 GB
Destination directory:
C:\Program Files (x86)\CryptoForge\
Shortcut folder:
CryptoForge
< Back
Install
Cancel



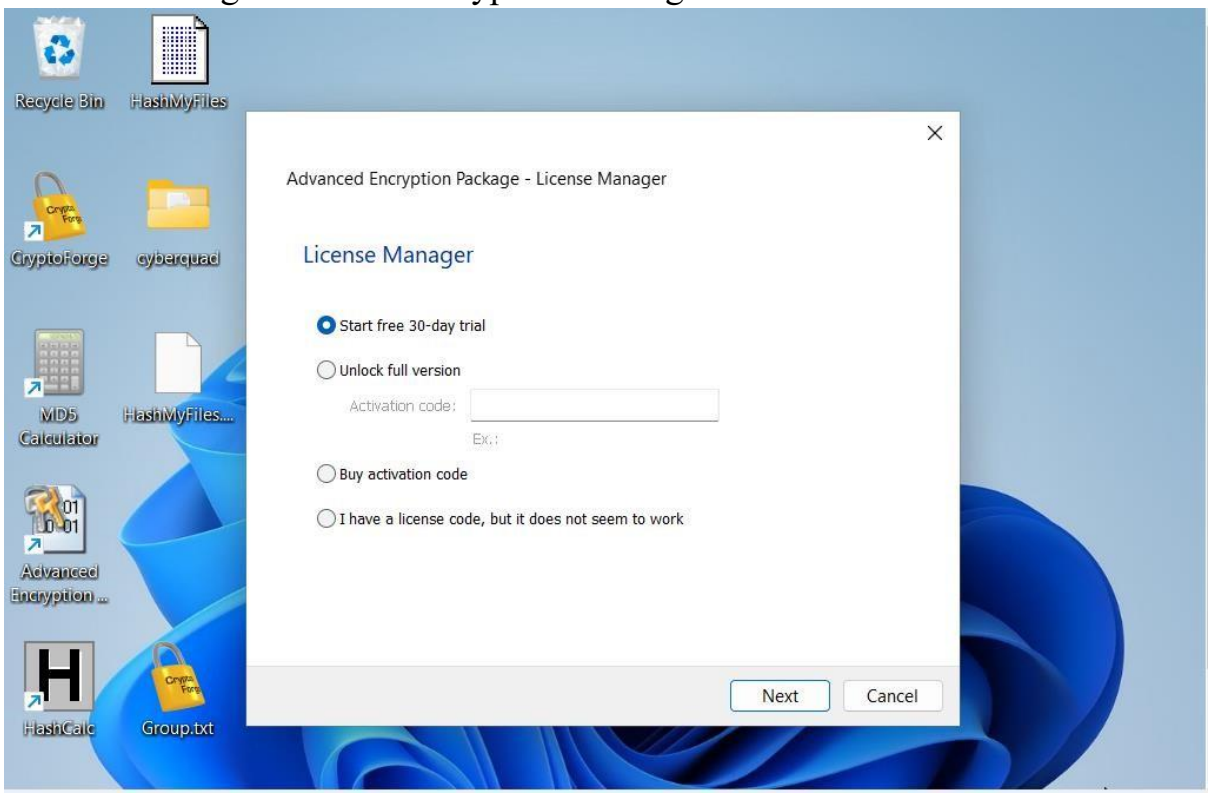
- Encrypting a txt file from widows 11 vm

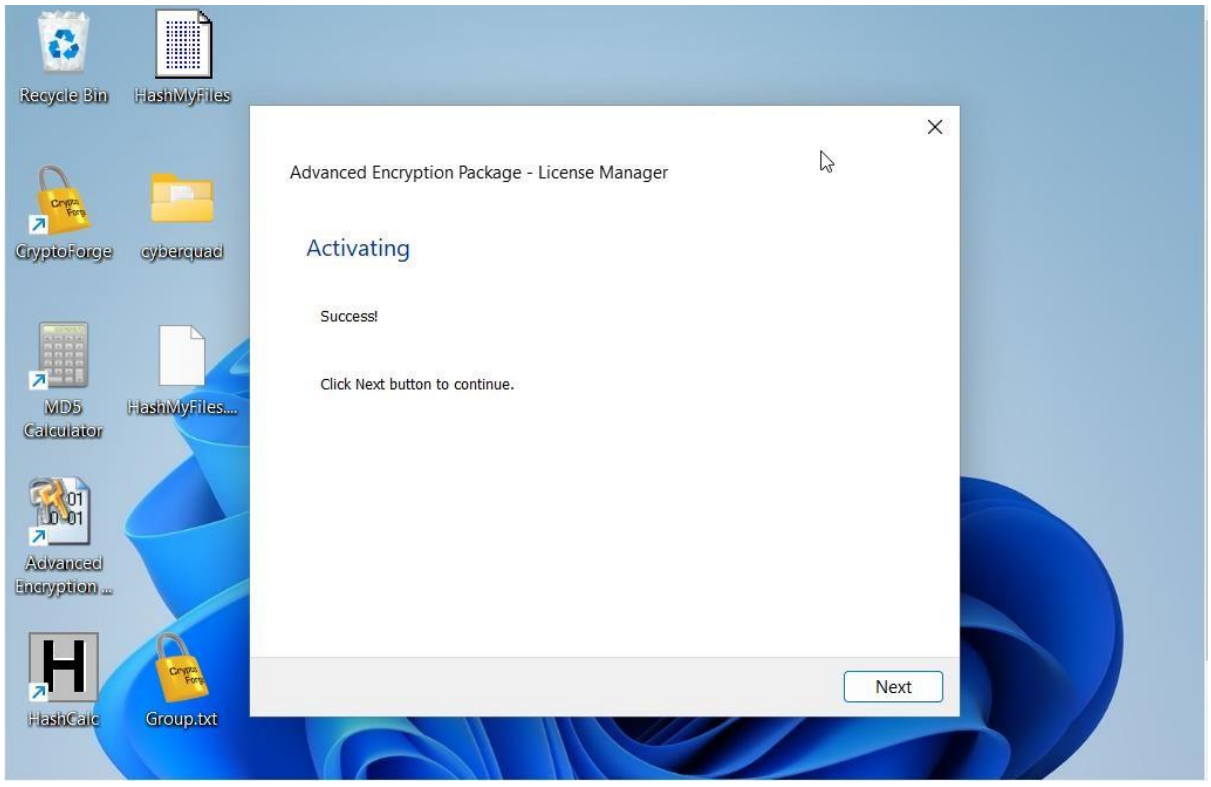


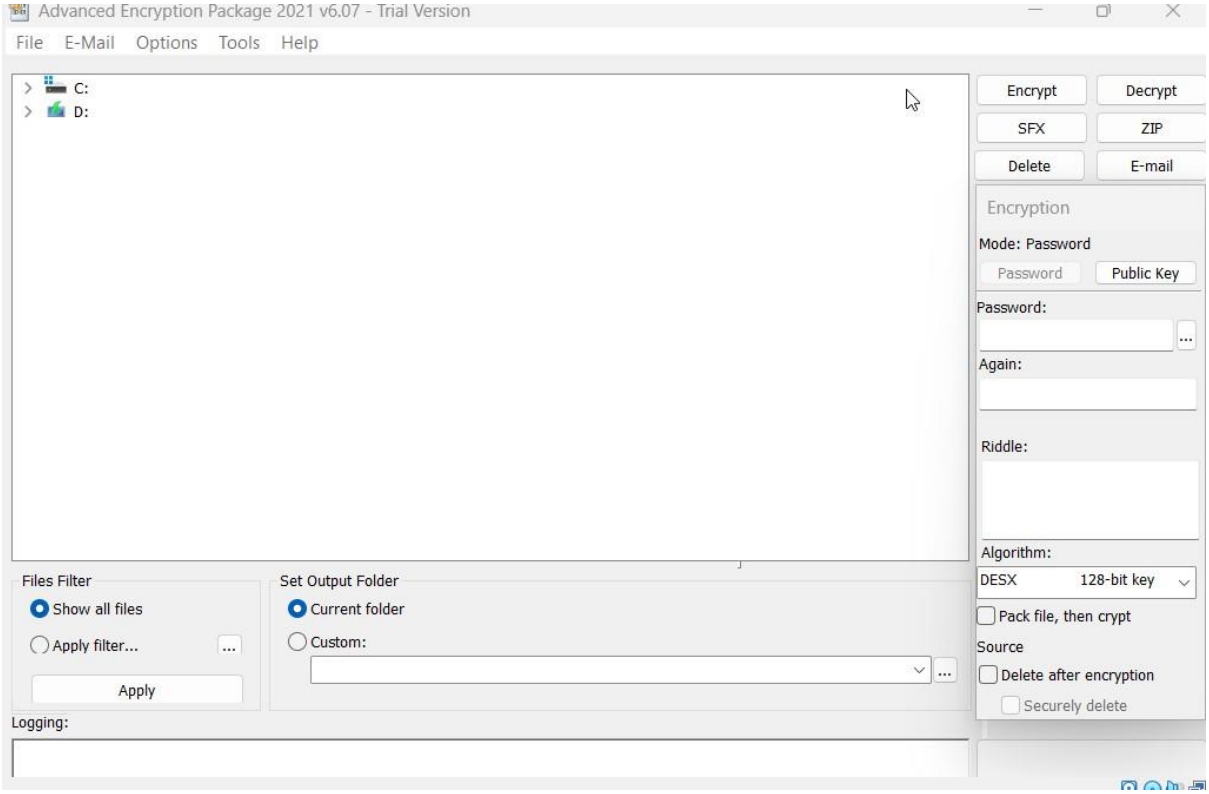
TASK 5

ENCRYPTION USING ADVANCED ENCRYPTION ADVANCED PACKAGE

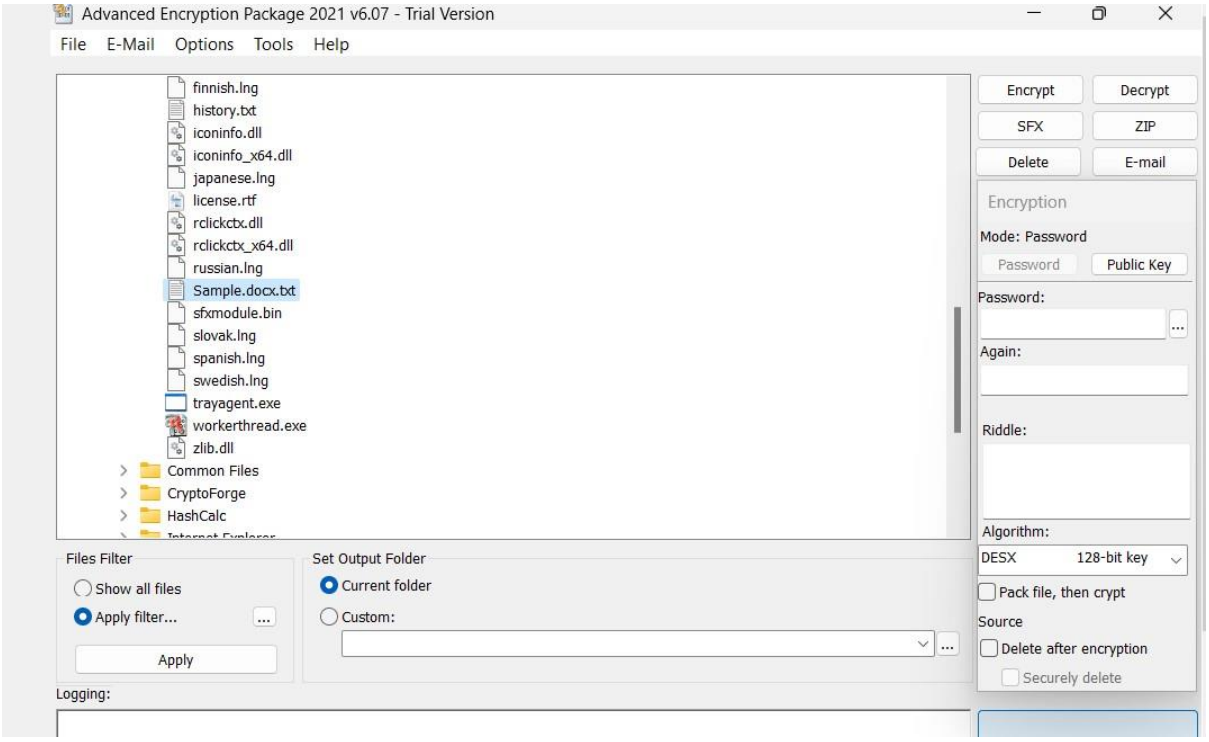
- Installing Advanced encryption Package

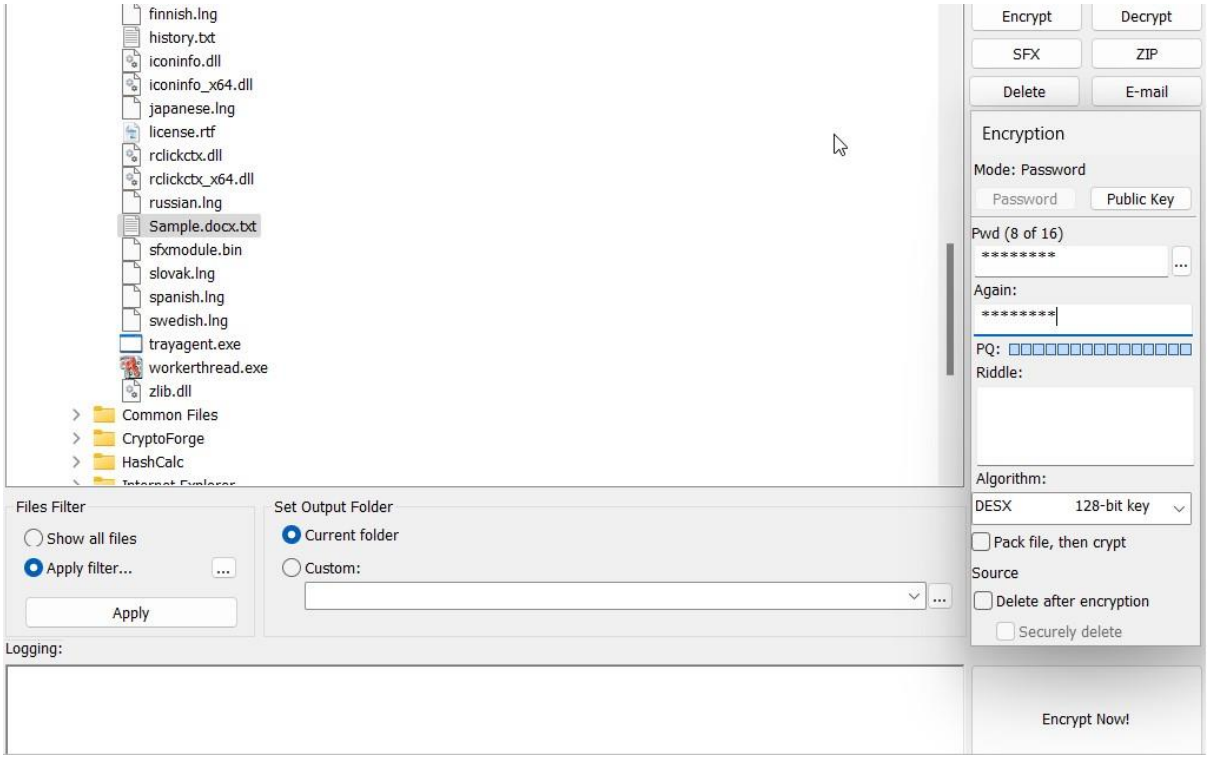


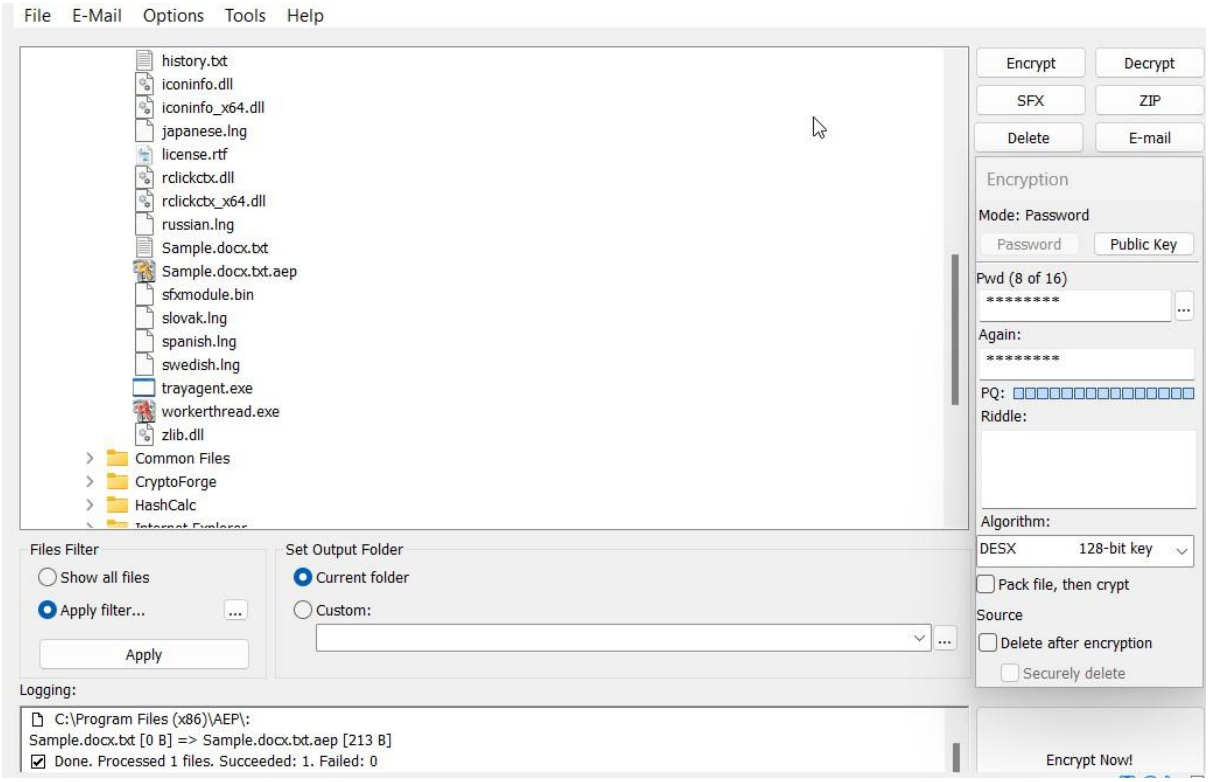




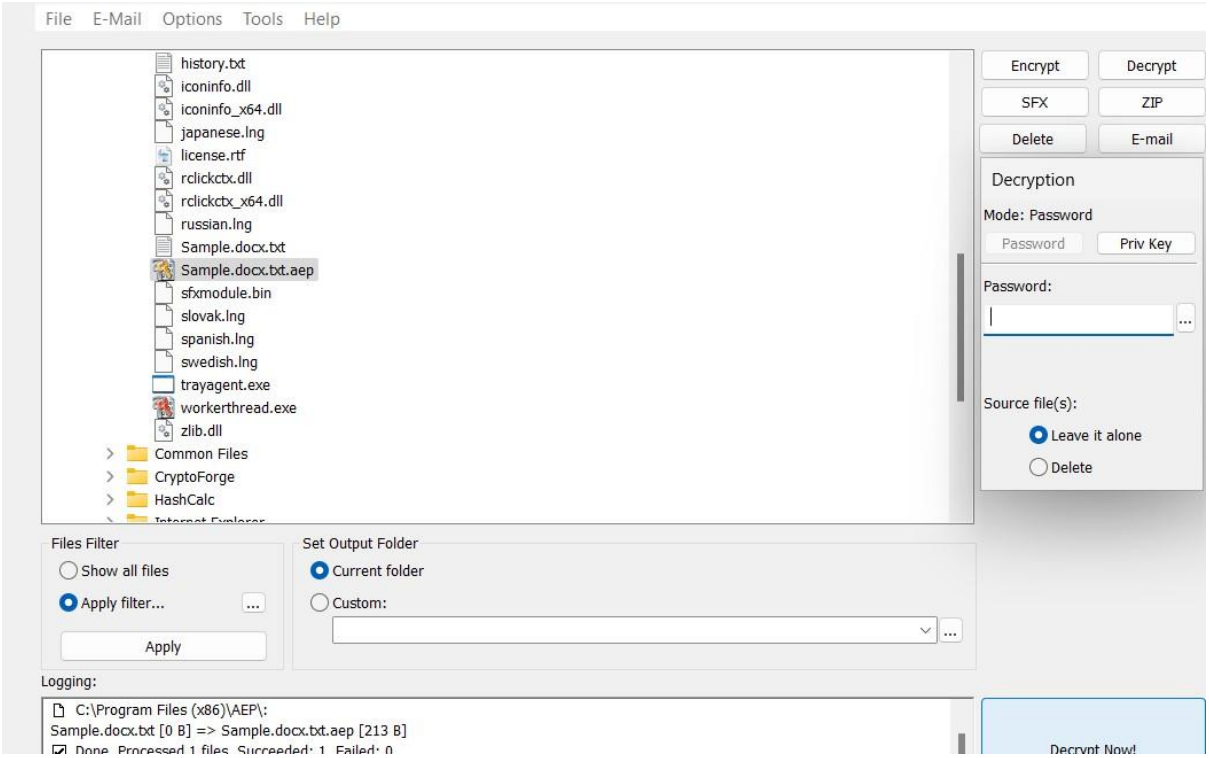
- Encrypting a sample file using Advanced Encryption Package.

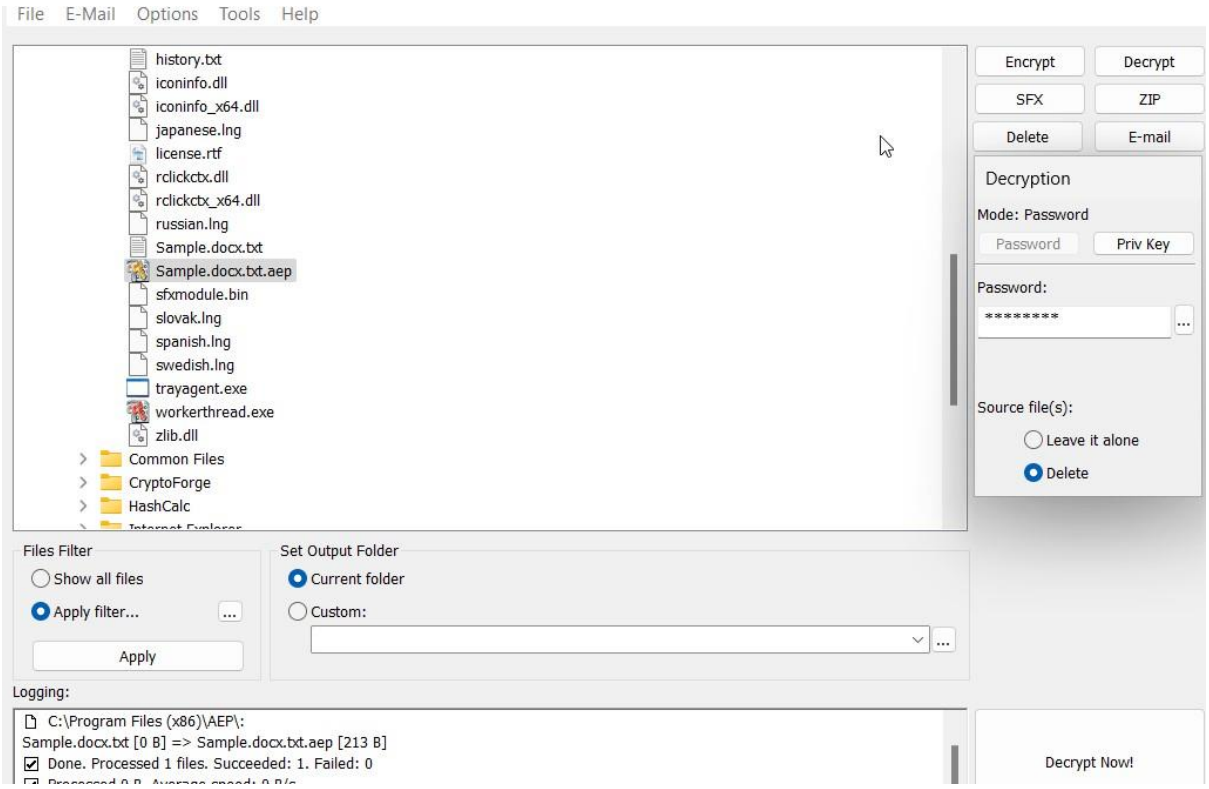


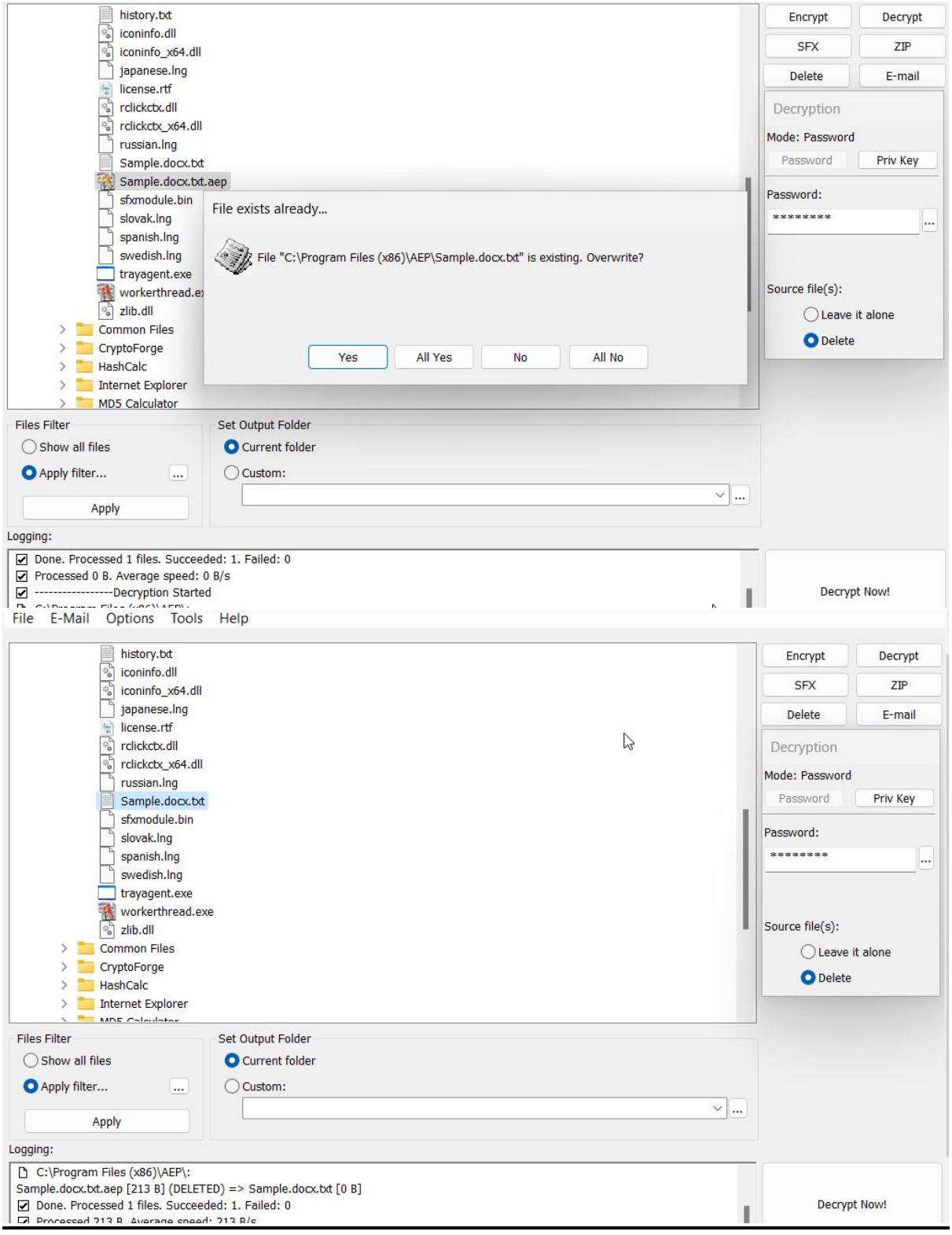




- Decrypting the Encrypted sample file


File E-Mail Options Tools Help
history.txt
iconinfo.dll
iconinfo_x64.dll
japanese.lng
license.rtf
rclickctx.dll
rclickctx_x64.dll
russian.lng
Sample.docx.txt
Sample.docx.txt.aep
sfxmodule.bin
slovak.lng
spanish.lng
swedish.lng
trayagent.exe
workerthread.exe
zlib.dll
Common Files
CryptoForge
HashCalc
Encrypt
Decrypt
SFX
ZIP
Delete
E-mail
Decryption
Mode: Password
Password
Priv Key
Password:
Source file(s):
Leave it alone
Delete
Files Filter
Show all files
Apply filter...
Apply
Set Output Folder
Current folder
Custom:
Logging:
C:\Program Files (x86)\AEP\:
Sample.docx.txt [0 B] => Sample.docx.txt.aep [213 B]
Decrypt Now!

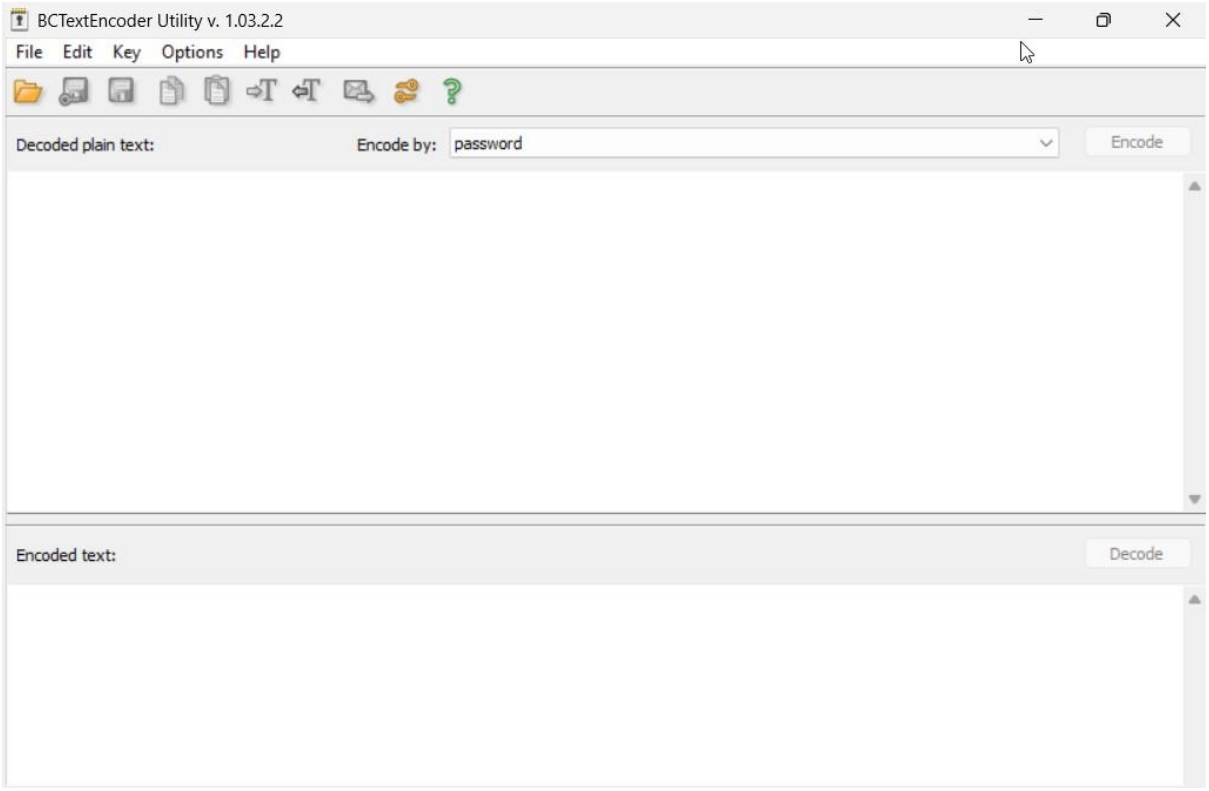

File E-Mail Options Tools Help
history.txt
iconinfo.dll
iconinfo_x64.dll
japanese.lng
license.rtf
rclickctx.dll
rclickctx_x64.dll
russian.lng
Sample.docx.txt
Sample.docx.txt.aep
sfxmodule.bin
slovak.lng
spanish.lng
swedish.lng
trayagent.exe
workerthread.exe
zlib.dll
Common Files
CryptoForge
HashCalc
Encrypt
Decrypt
SFX
ZIP
Delete
E-mail
Decryption
Mode: Password
Password
Priv Key
Password:
****
Source file(s):
Leave it alone
Delete
Files Filter
Show all files
Apply filter...
Apply
Set Output Folder
Current folder
Custom:
Logging:
C:\Program Files (x86)\AEP\:
Sample.docx.txt [0 B] => Sample.docx.txt.aep [213 B]
Done. Processed 1 files. Succeeded: 1. Failed: 0
Decrypt Now!


history.txt
iconinfo.dll
iconinfo_x64.dll
japanese.lng
license.rtf
rclickctx.dll
rclickctx_x64.dll
russian.lng
Sample.docx.txt
Sample.docx.txt.aep
sfxmodule.bin
slovak.lng
spanish.lng
swedish.lng
trayagent.exe
workerthread.exe
zlib.dll
Common Files
CryptoForge
HashCalc
Internet Explorer
MD5 Calculator
File exists already...
File "C:\Program Files (x86)\AEP\Sample.docx.txt" is existing. Overwrite?
Yes
All Yes
No
All No
Encrypt
Decrypt
SFX
ZIP
Delete
E-mail
Decryption
Mode: Password
Password
Priv Key
Password:
Source file(s):
Leave it alone
Delete
Files Filter
Show all files
Apply filter...
Apply
Set Output Folder
Current folder
Custom:
Logging:
Done. Processed 1 files. Succeeded: 1. Failed: 0
Processed 0 B. Average speed: 0 B/s
----------Decryption Started
Decrypt Now!
File E-Mail Options Tools Help
history.txt
iconinfo.dll
iconinfo_x64.dll
japanese.lng
license.rtf
rclickctx.dll
rclickctx_x64.dll
russian.lng
Sample.docx.txt
sfxmodule.bin
slovak.lng
spanish.lng
swedish.lng
trayagent.exe
workerthread.exe
zlib.dll
Common Files
CryptoForge
HashCalc
Internet Explorer
Encrypt
Decrypt
SFX
ZIP
Delete
E-mail
Decryption
Mode: Password
Password
Priv Key
Password:
Source file(s):
Leave it alone
Delete
Files Filter
Show all files
Apply filter...
Apply
Set Output Folder
Current folder
Custom:
Logging:
C:\Program Files (x86)\AEP\:
Sample.docx.txt.aep [213 B] (DELETED) => Sample.docx.txt [0 B]
Done. Processed 1 files. Succeeded: 1. Failed: 0
Decrypt Now!

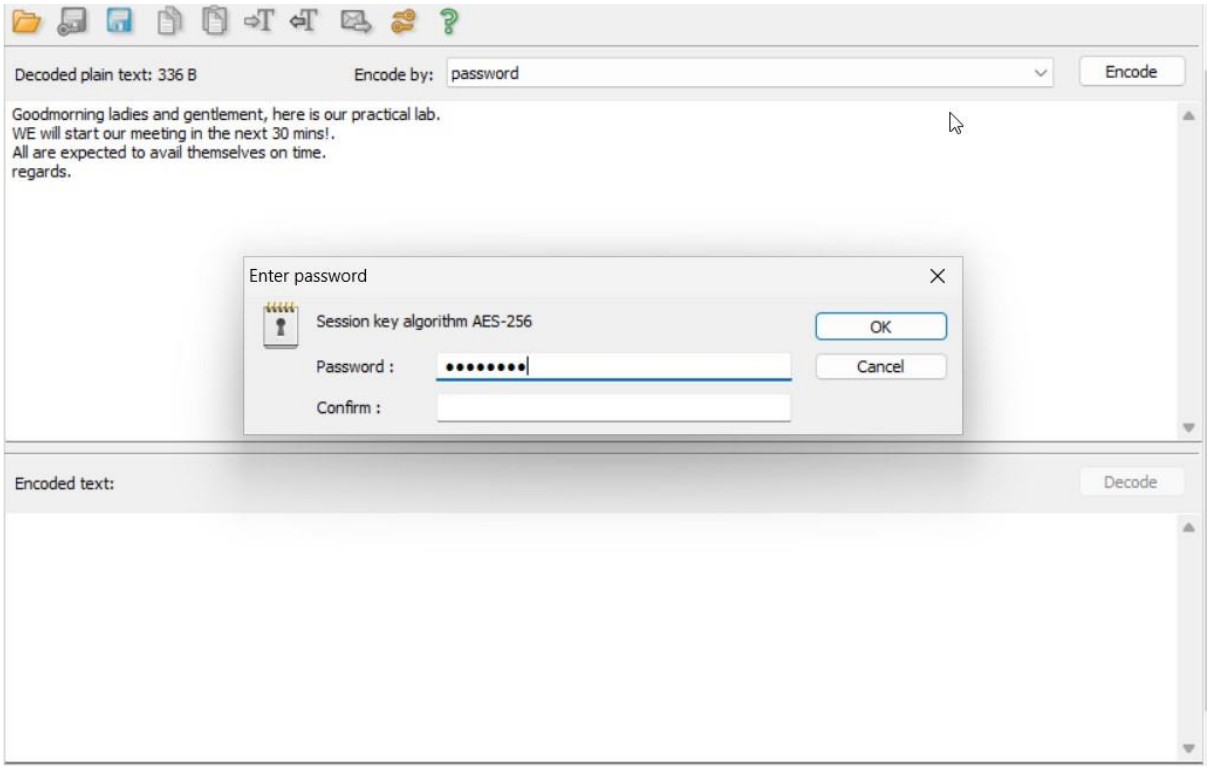
TASK 6

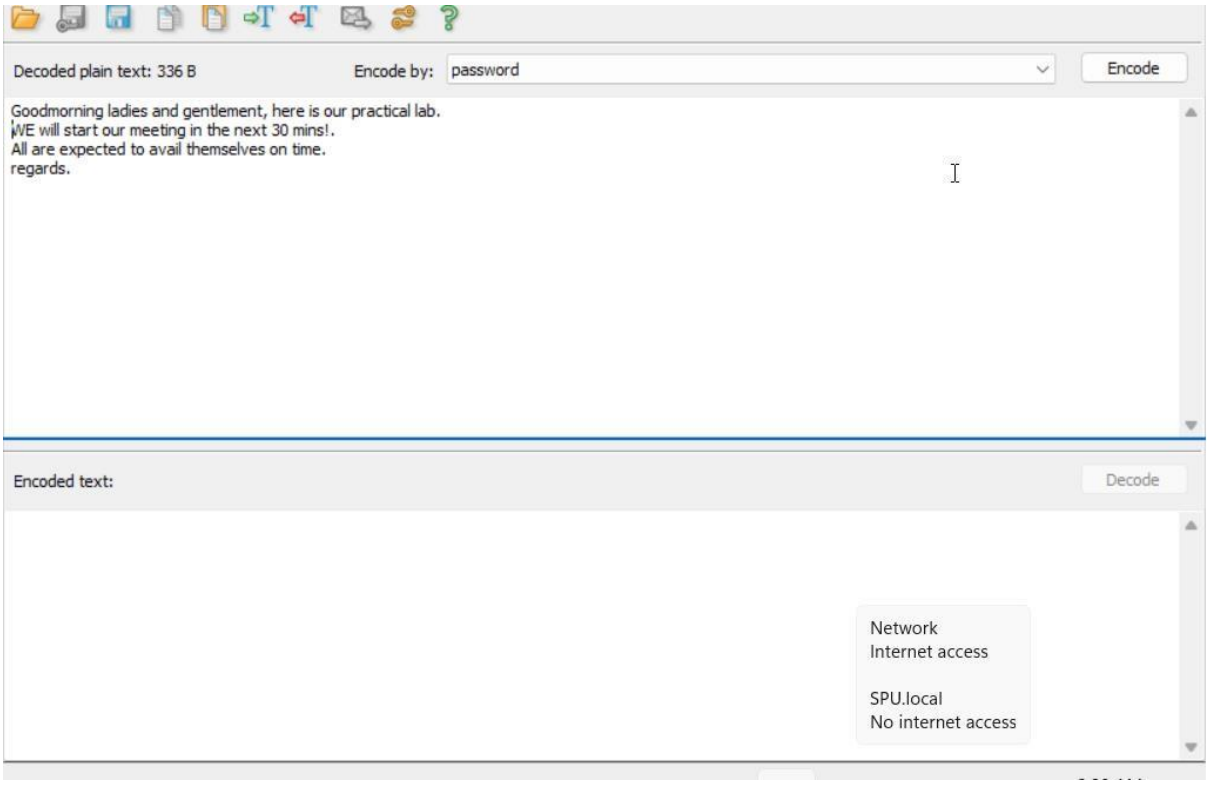
Encrypt and Decrypt data using BCTextEncoder

- BCTextEncoder appears as shown when opened

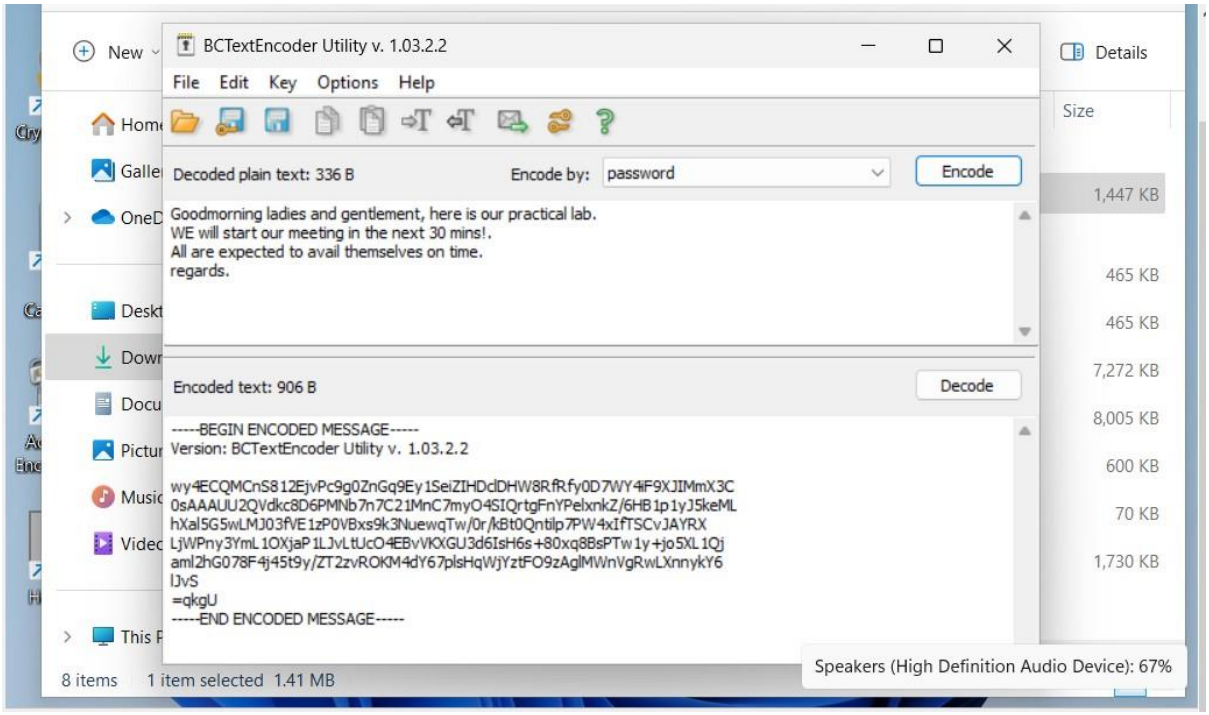


- Insert a text on the clipboard to encrypt, ensure the password tab is selected
- click on encode and input your password to encode the text.

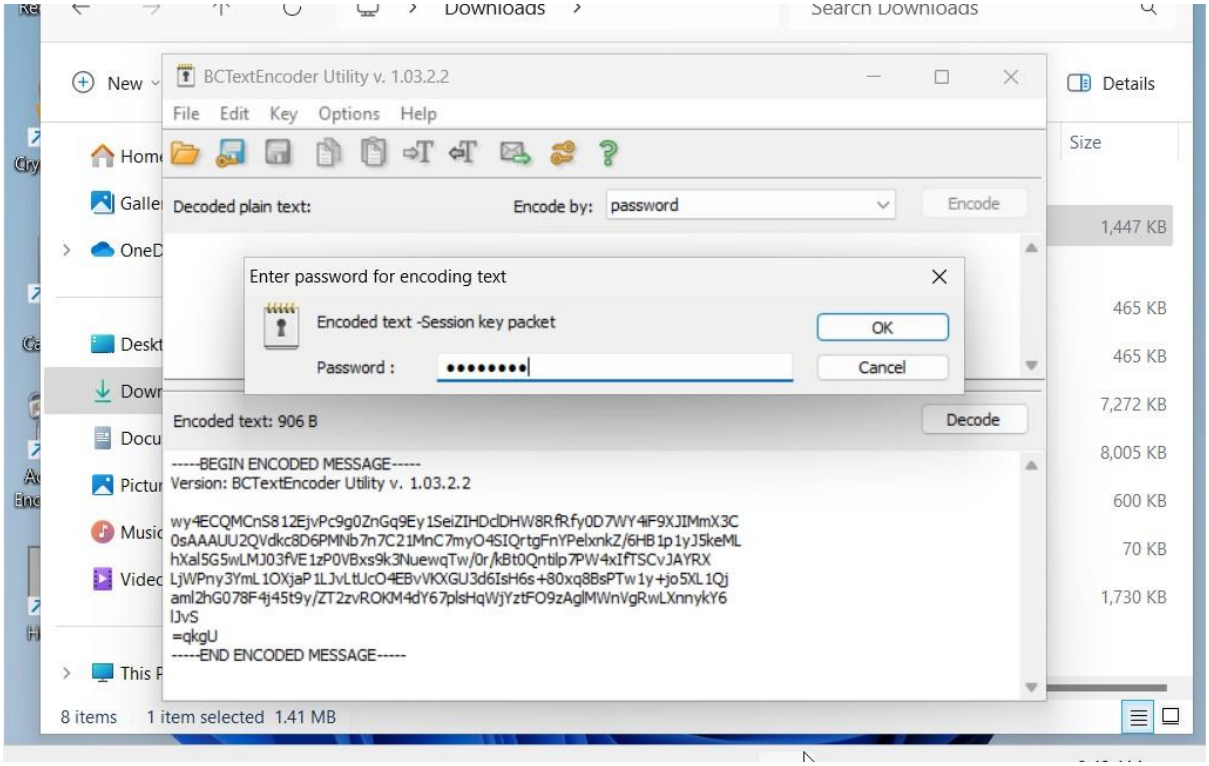




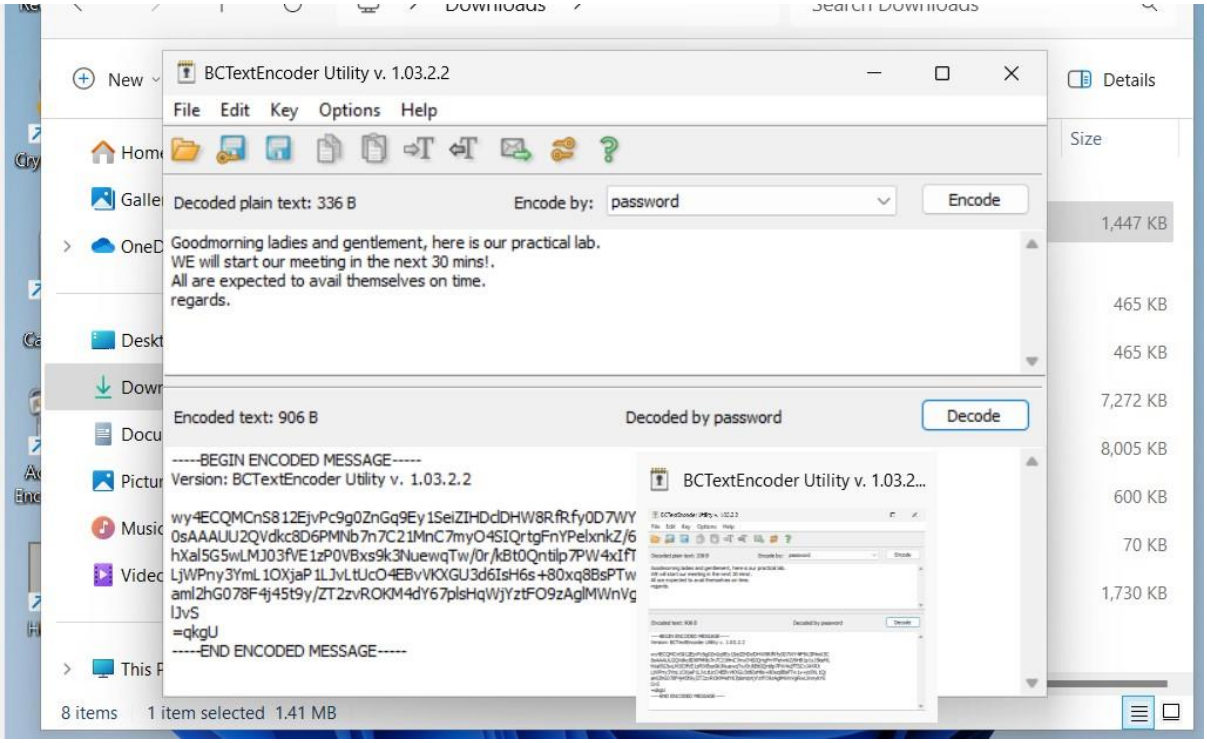
- The encode context is shown



- Decrypting the encoded text, you first need to clear the plain text, then click on the decode tab to decode the cipher text.
- A fill in your password message will pop, enter the password to decode the cipher text.



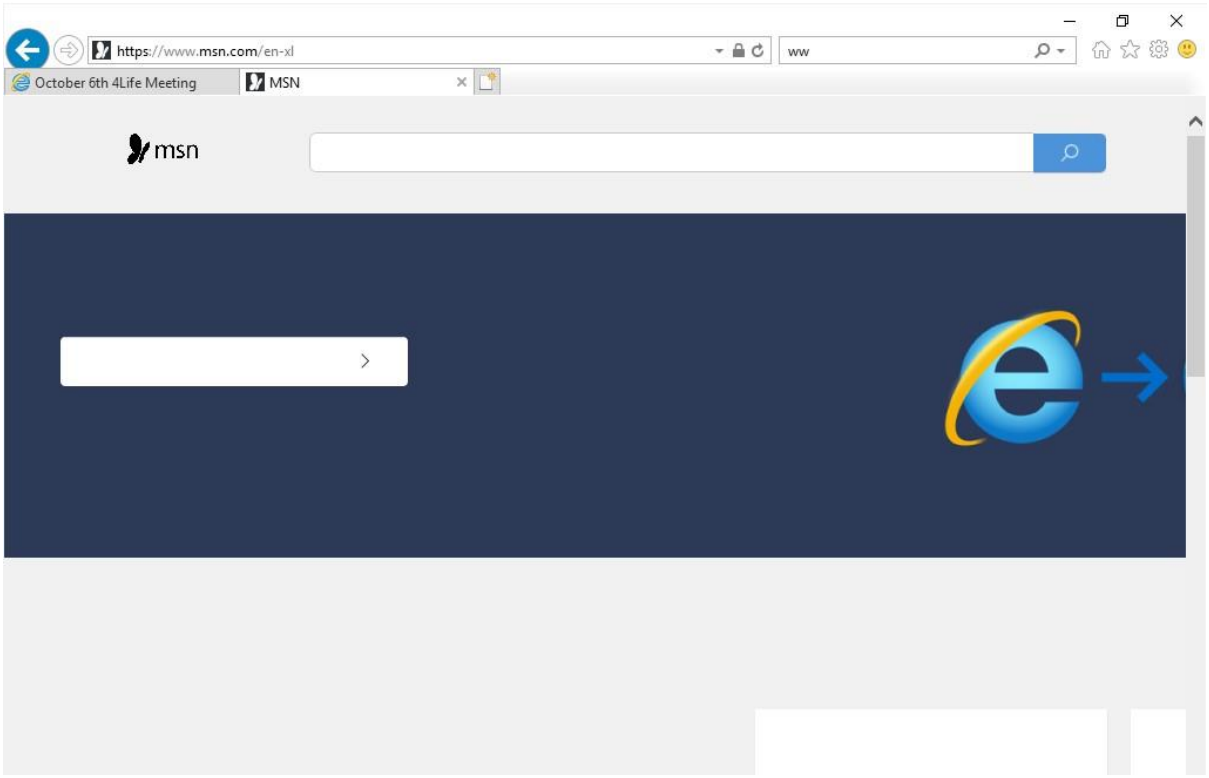
- Decoded plain text appears after you input the password.



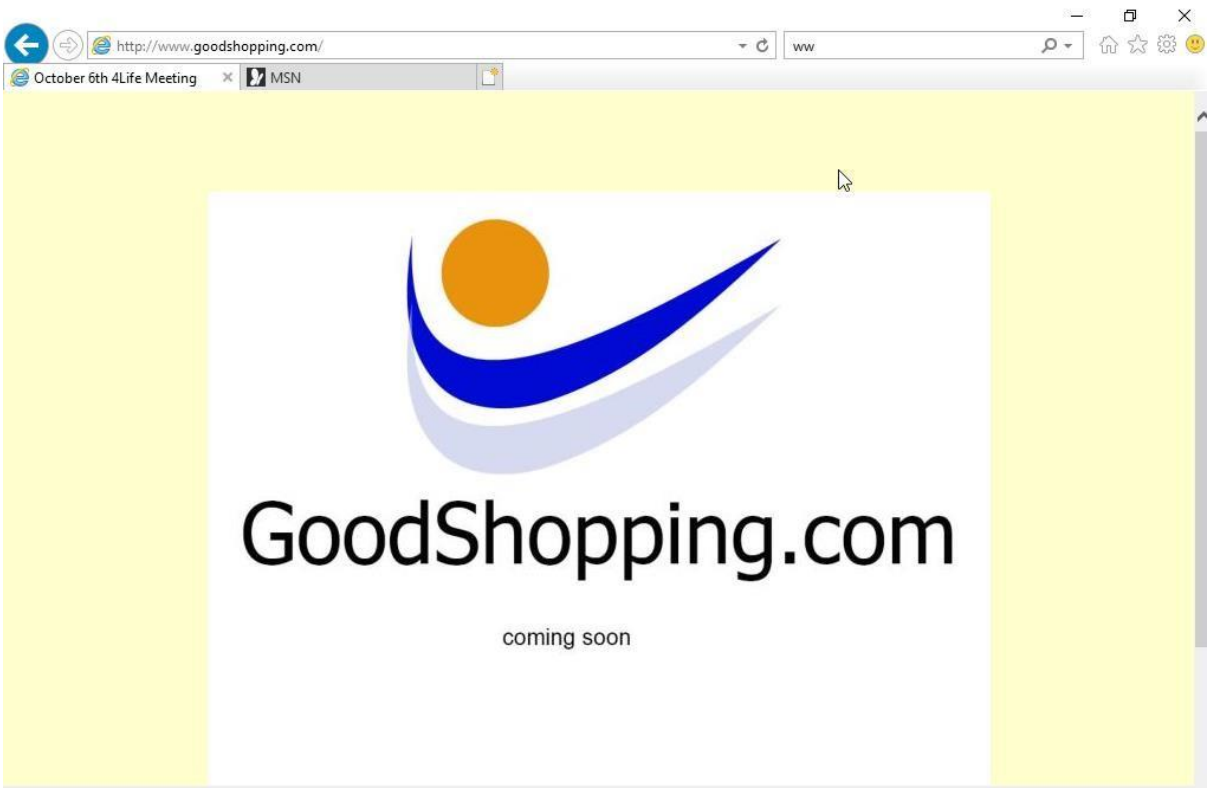
LAB 2

CREATING A SELF SIGNED CERTIFICATE

- Open your browser

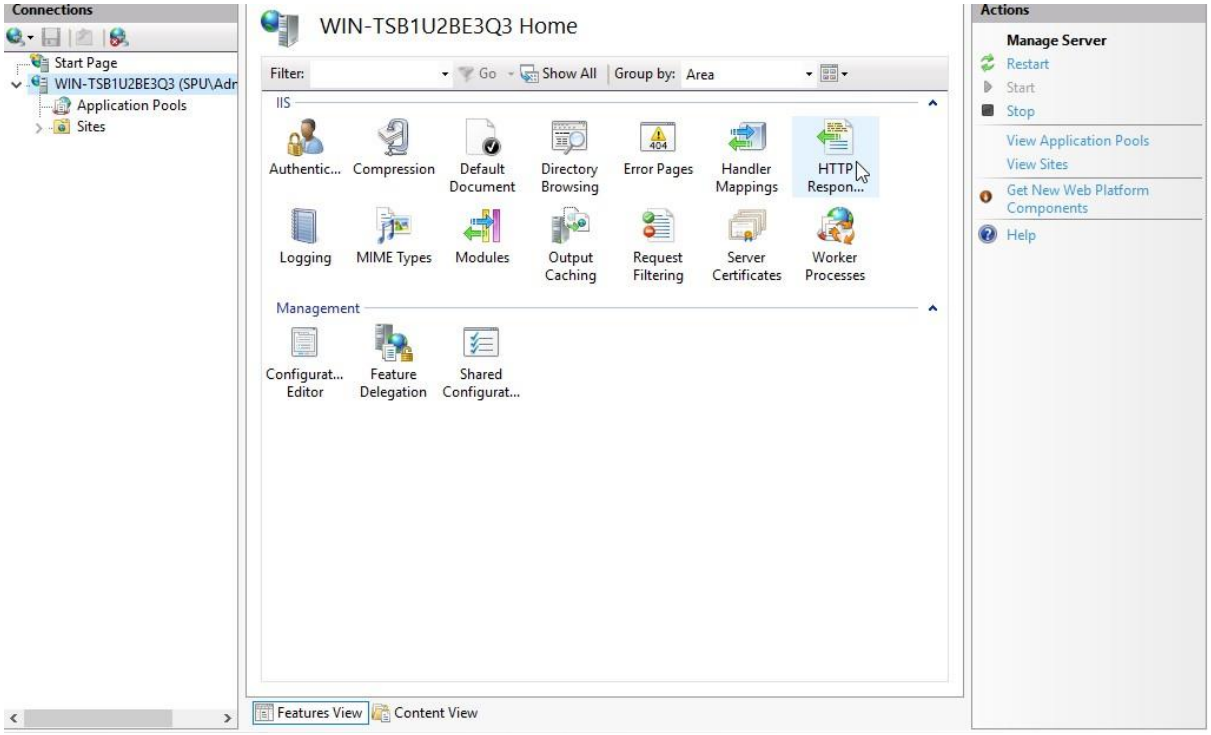


- Navigate to www.goodshopping.com

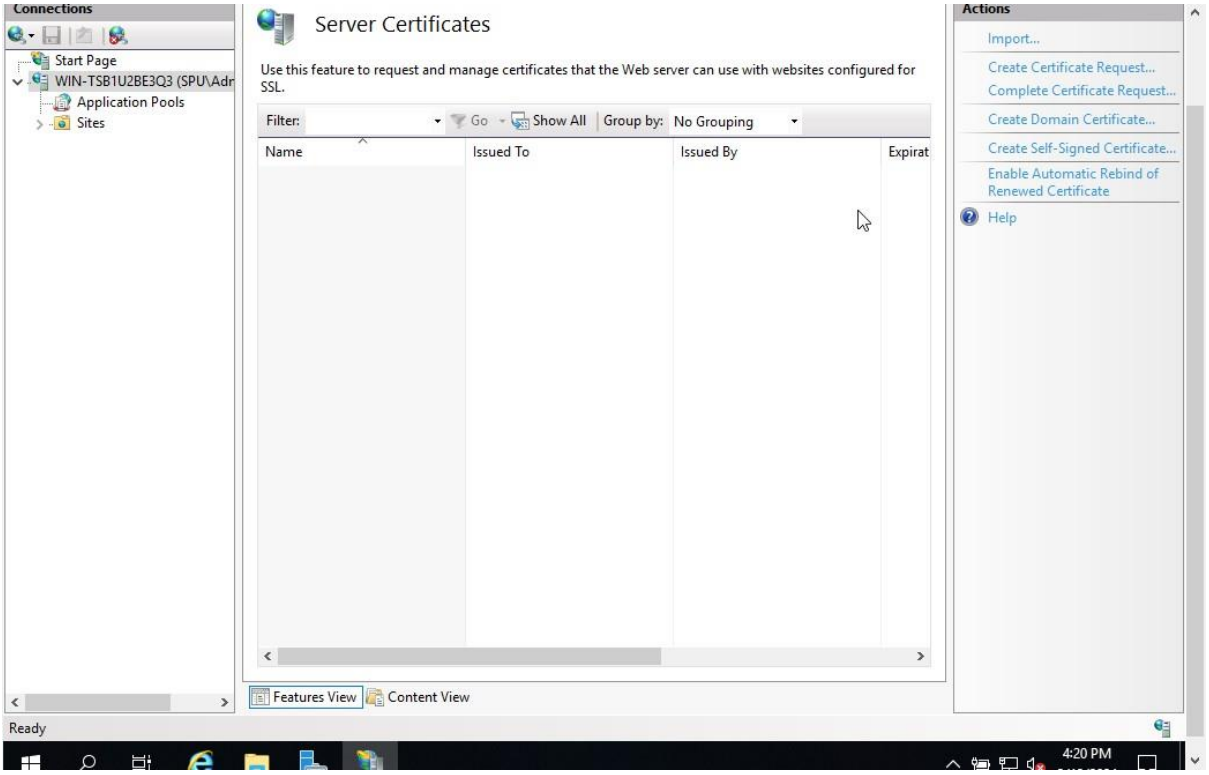


- Access the IIS manager

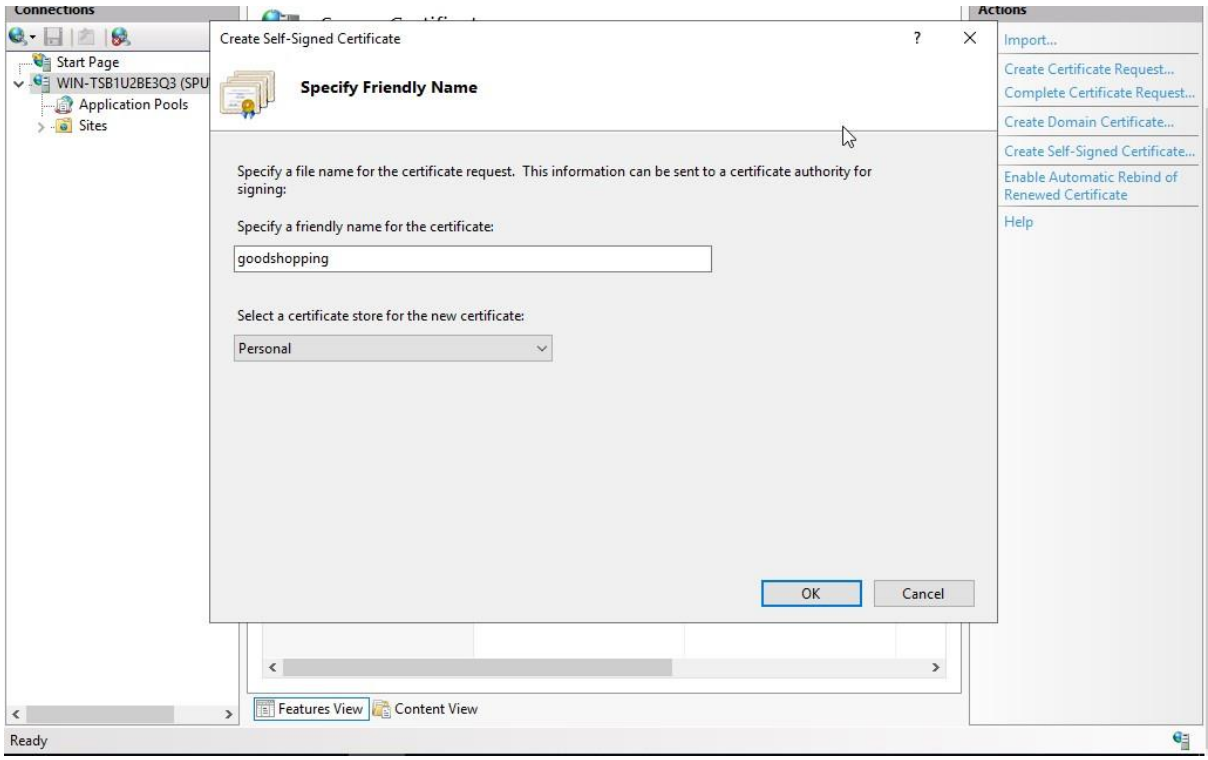
- Double click on the server certificate in the IIS section.



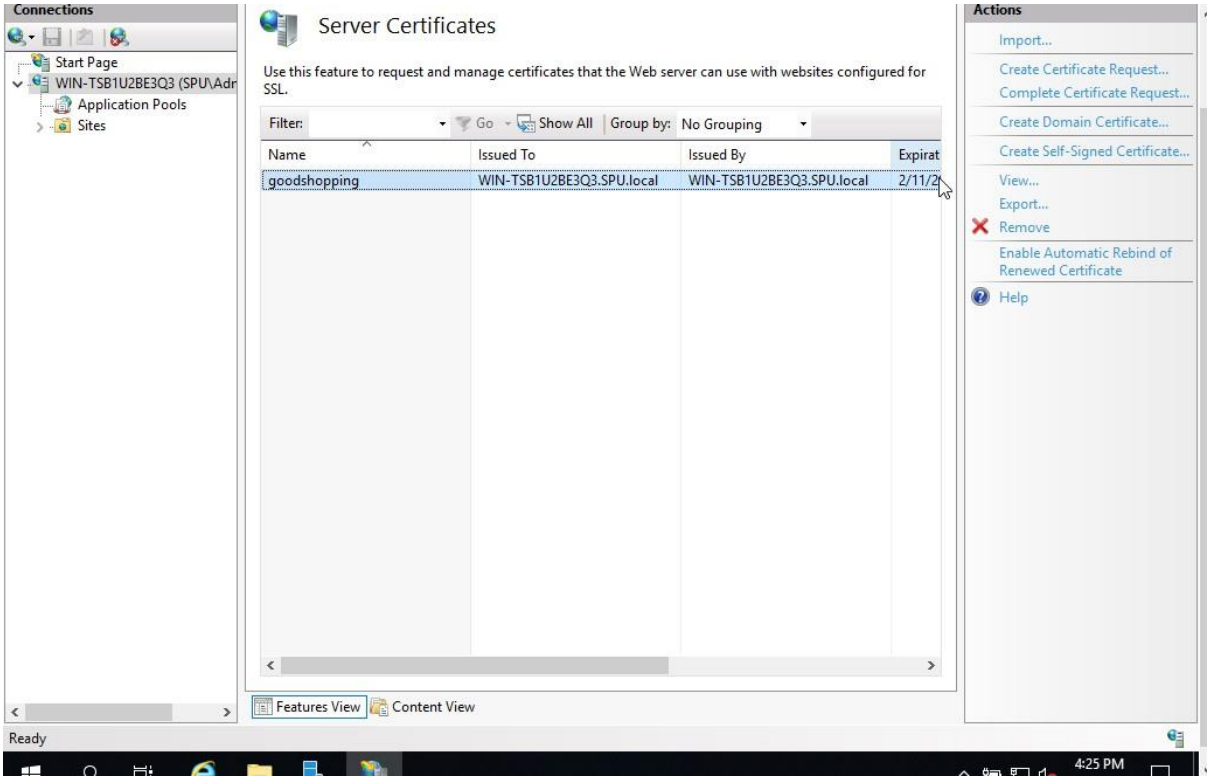
- Creating a self-signed certificate.



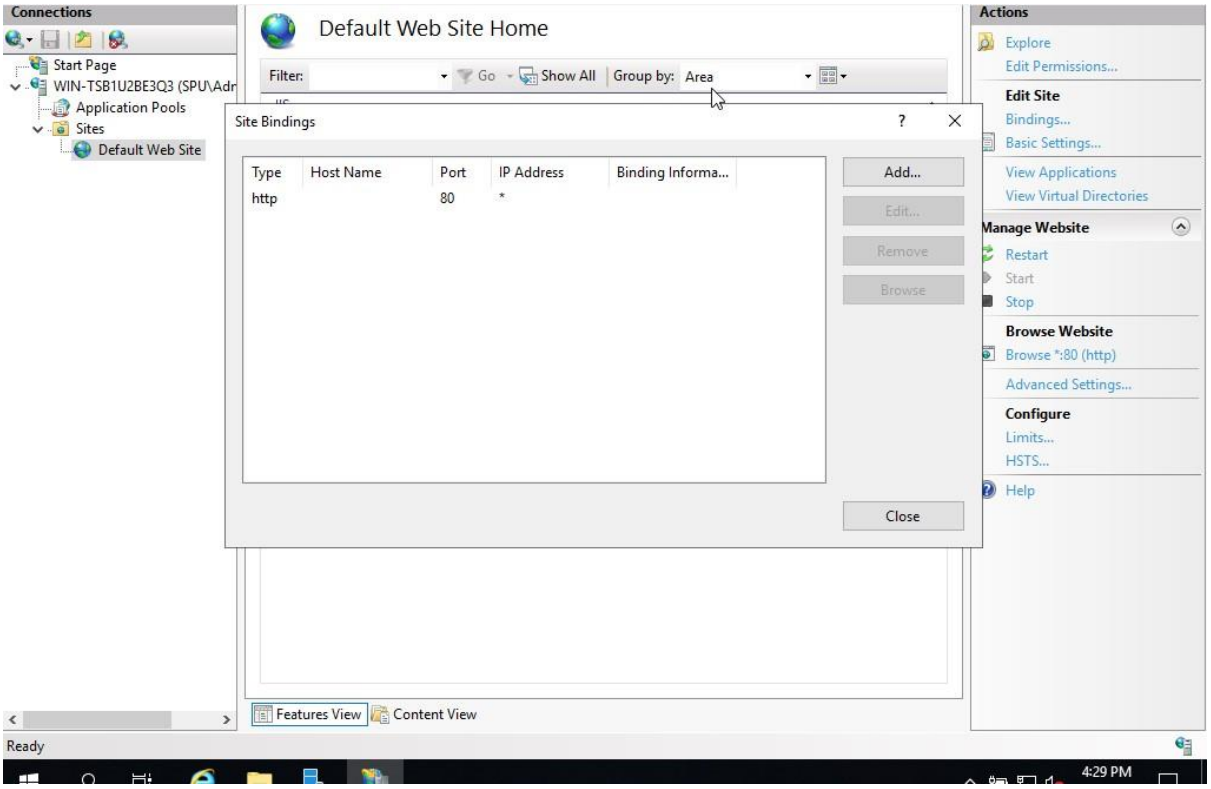
- Click on create signed certificate tab
- Specifying the details of the signed certificate



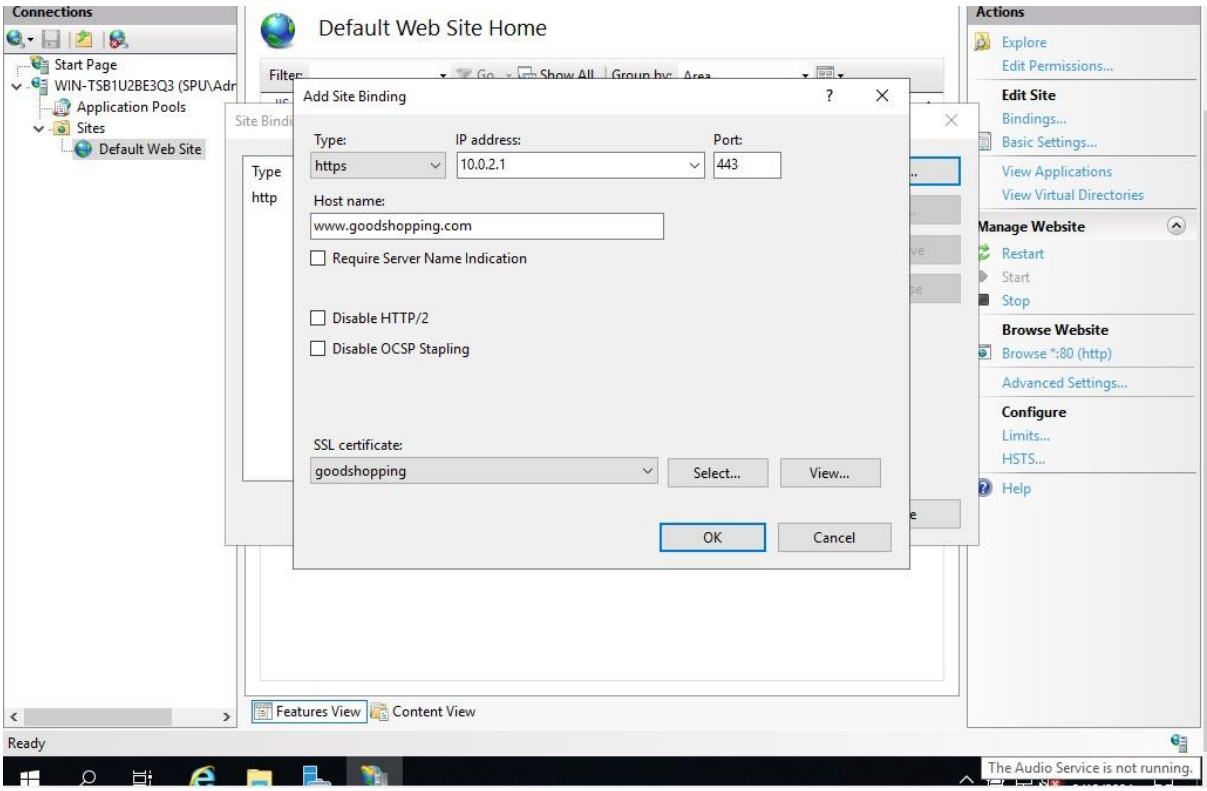
- The new created certificate

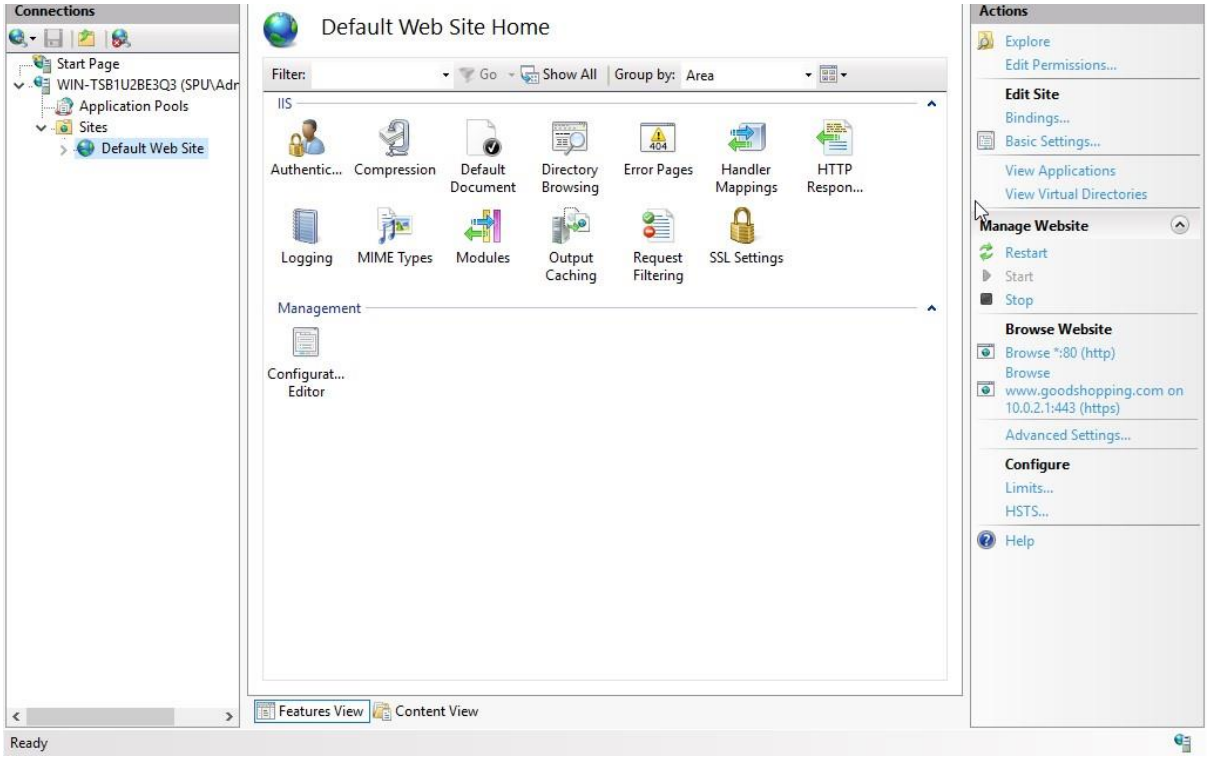


- Biding the newly created self-signed certificate

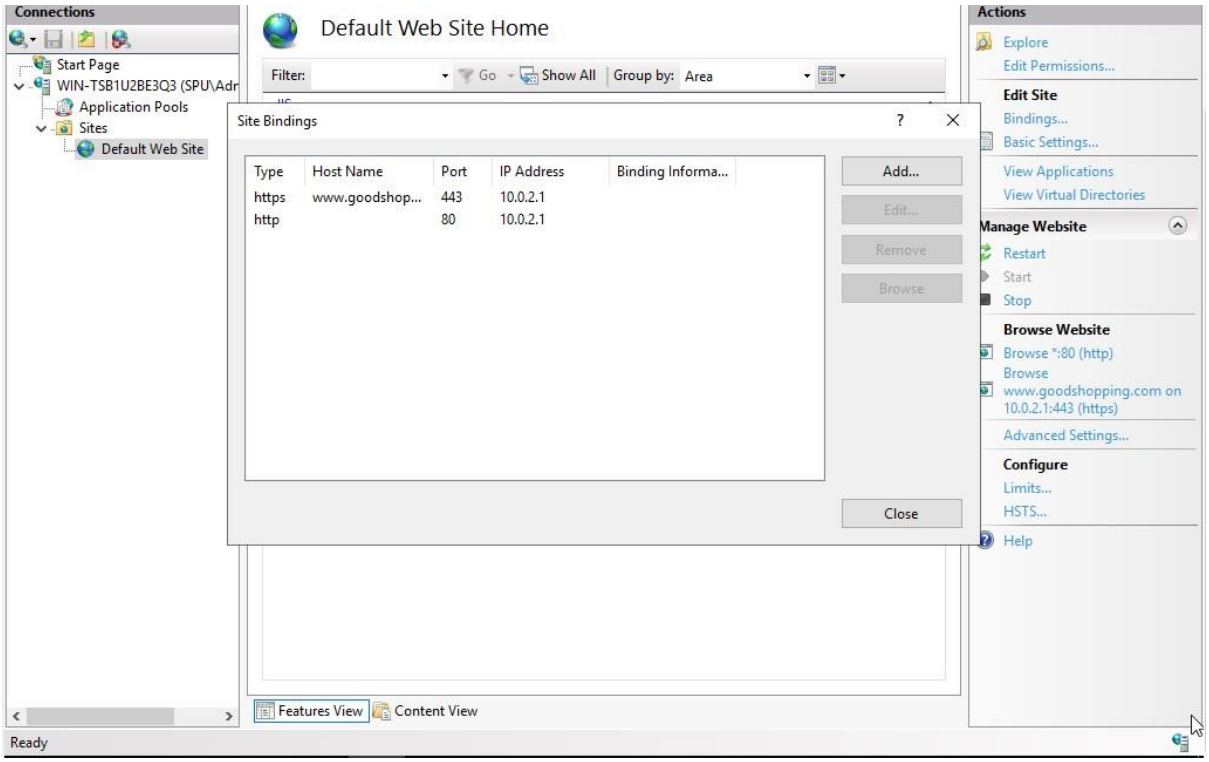


- Choose ip address on which the site is hosted
- Under Host name field type www.goodshopping.com and click ok





- The newly created certificate reflects



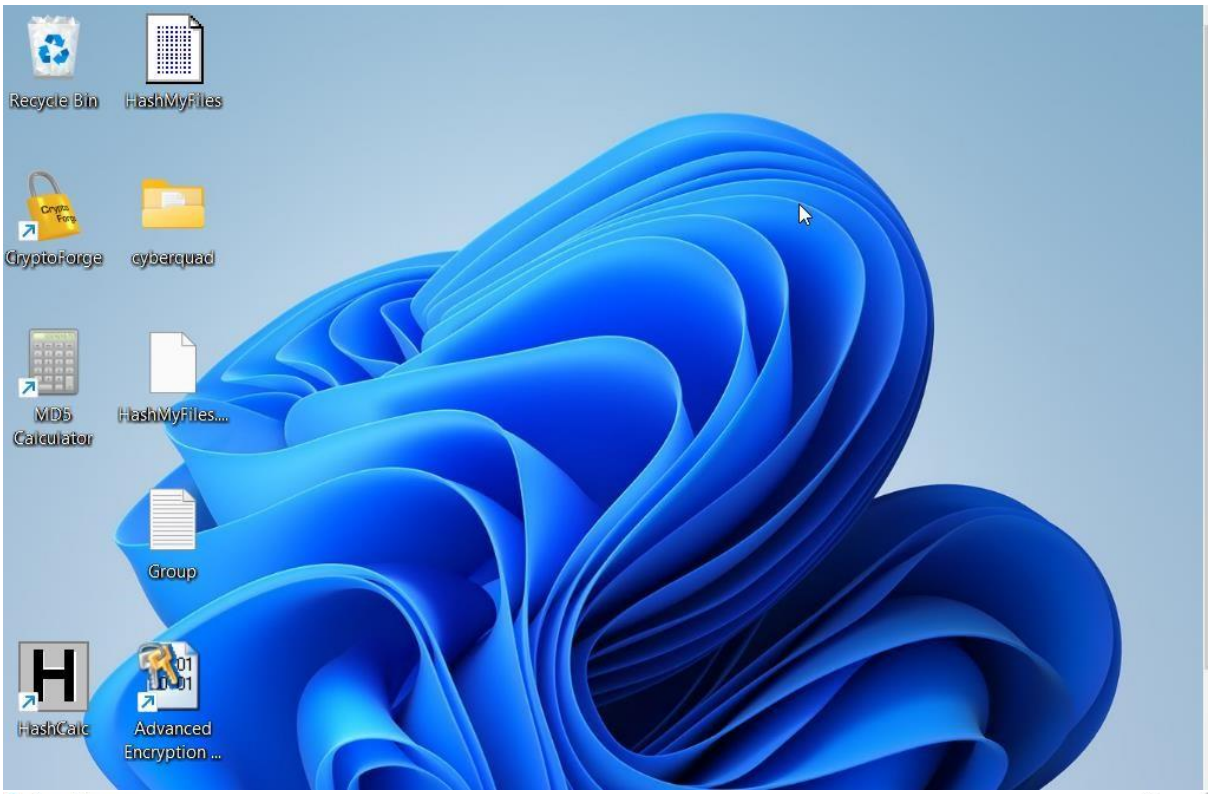
- Now navigate to the www.goodshopping.com site

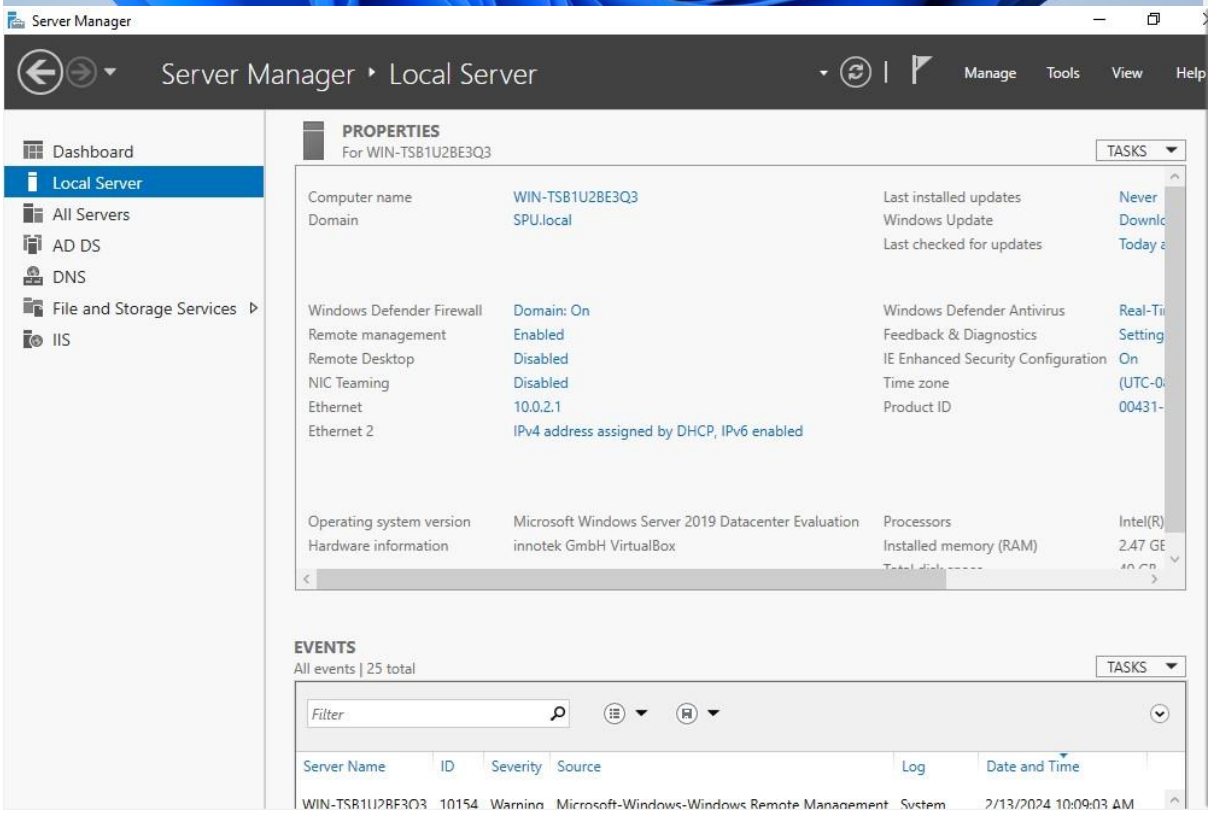
LAB 3

TASK 1

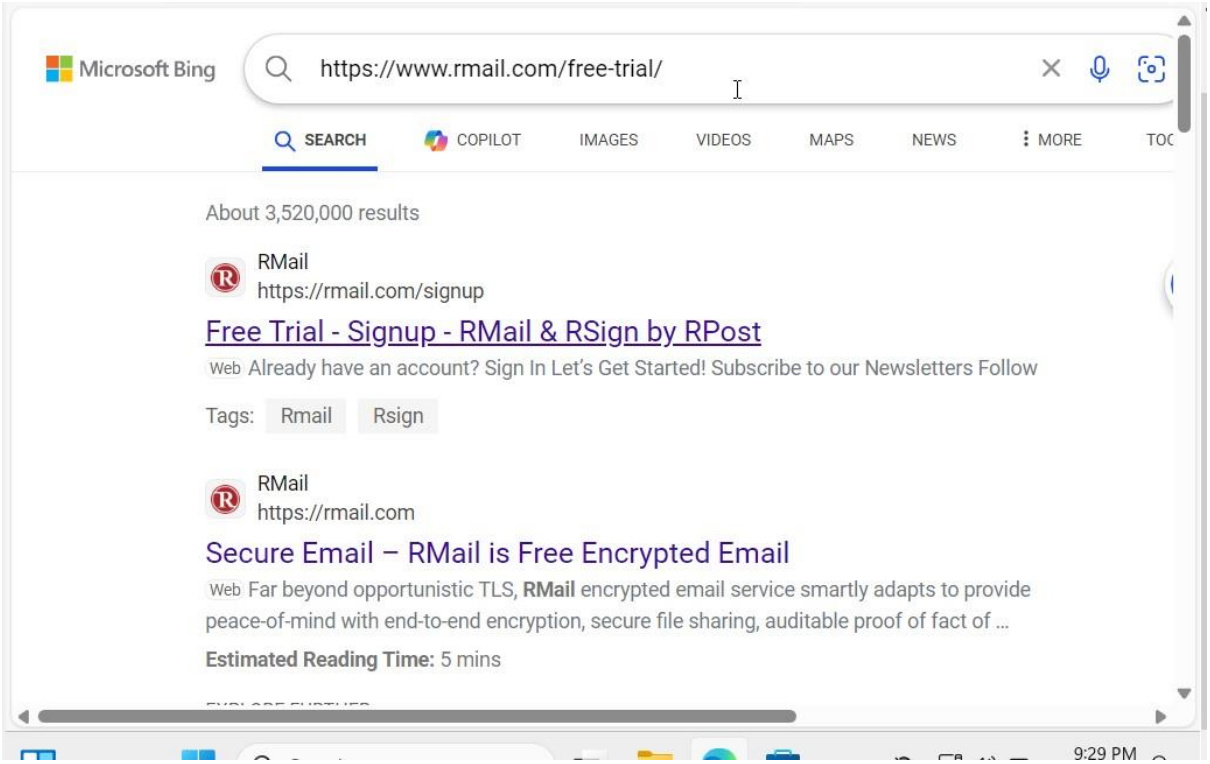
PERFORM EMAIL ENCRYPTION USING RMAIL

- Switch on both windows' server 2019 and windows 11 virtual machine

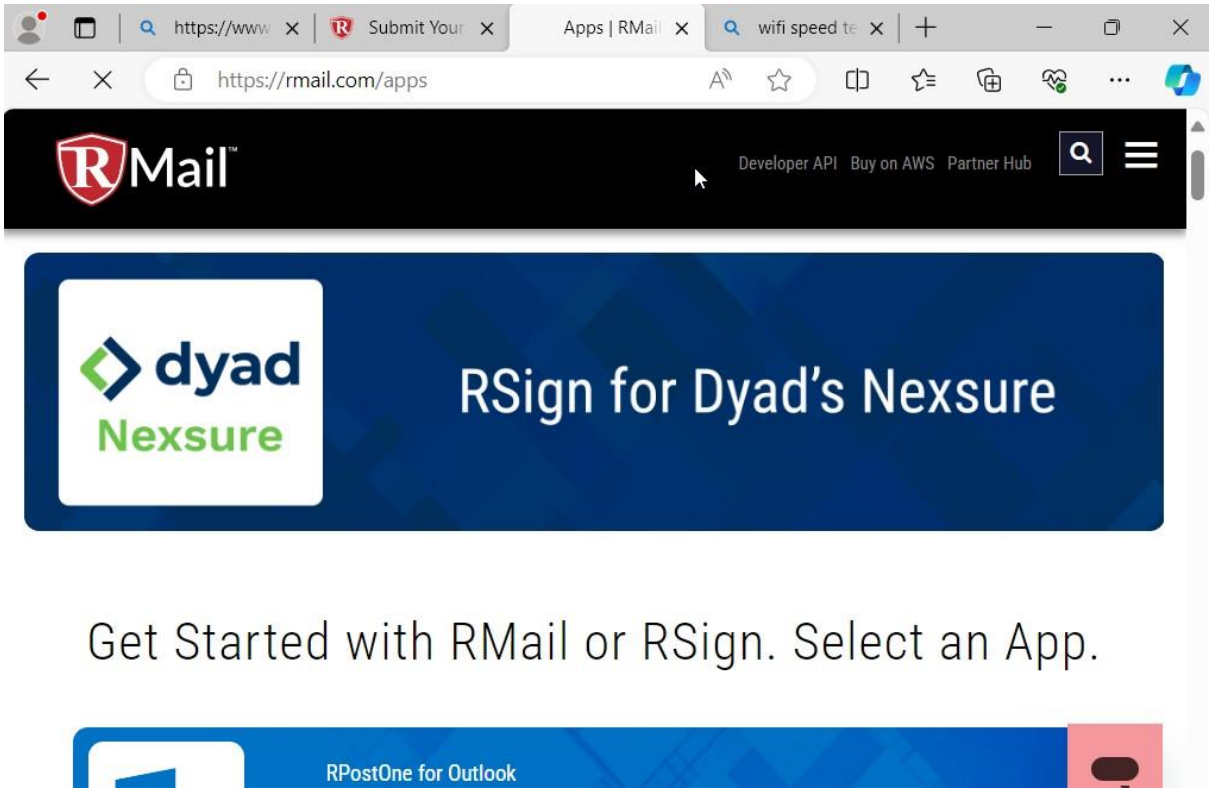




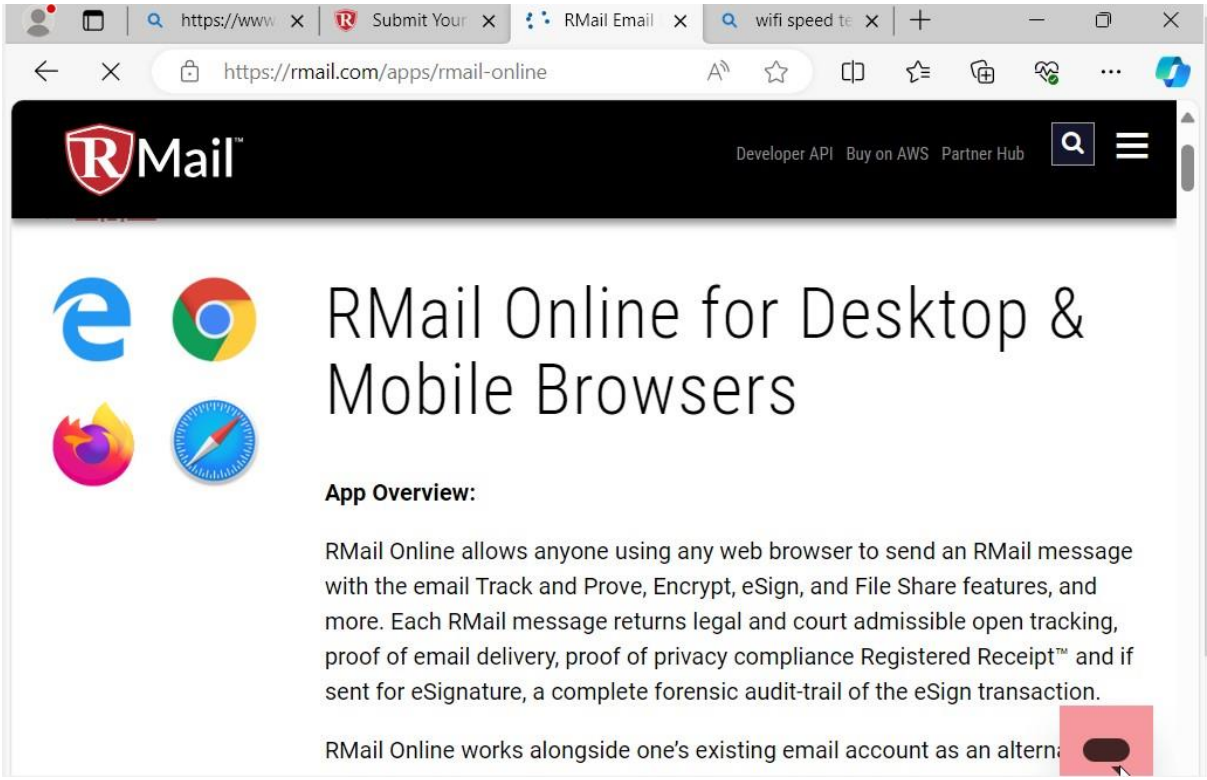
- Launch your browser and place the cursor in the address bar, type and press enter.



- Free trial window appears

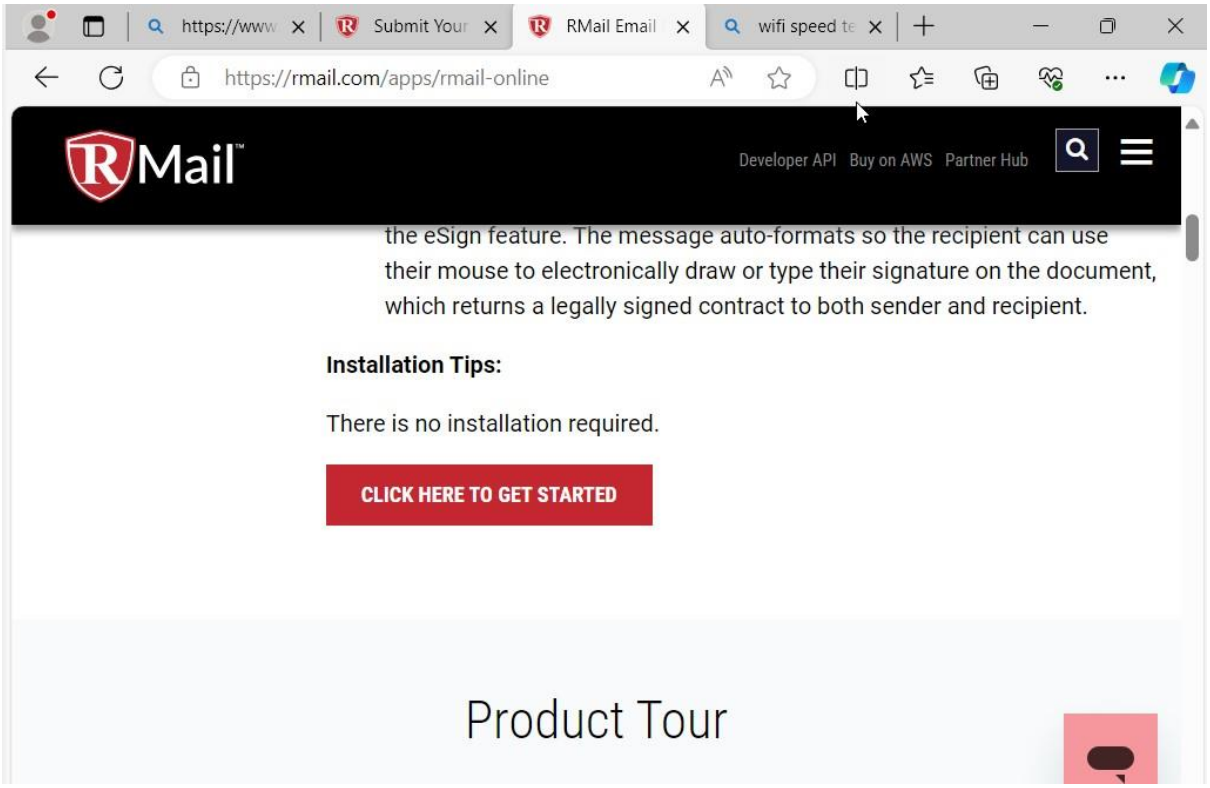


- On the app page, scroll down and click on Rmail online



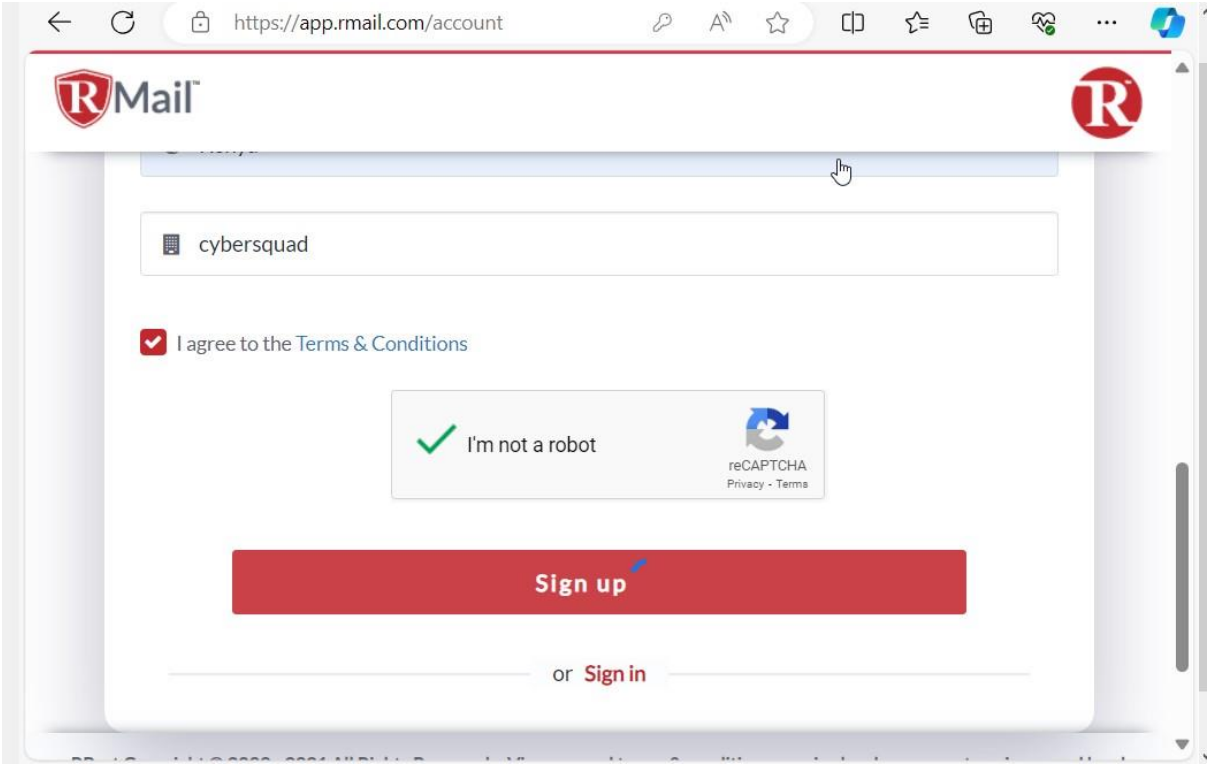
- Navigate through the page and clock on Click here to get started.

•

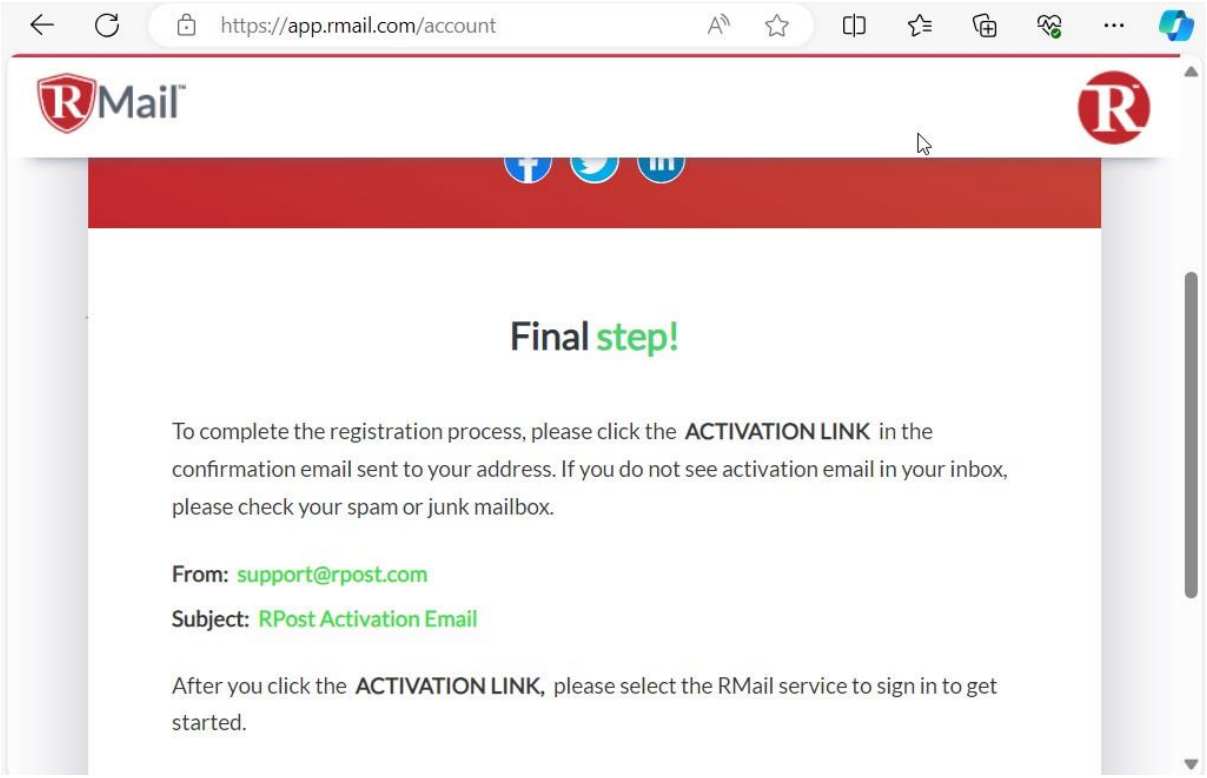


Click on create an account on the Rmail webpage

- Get started page appears, fill in the required Infor and click sign up

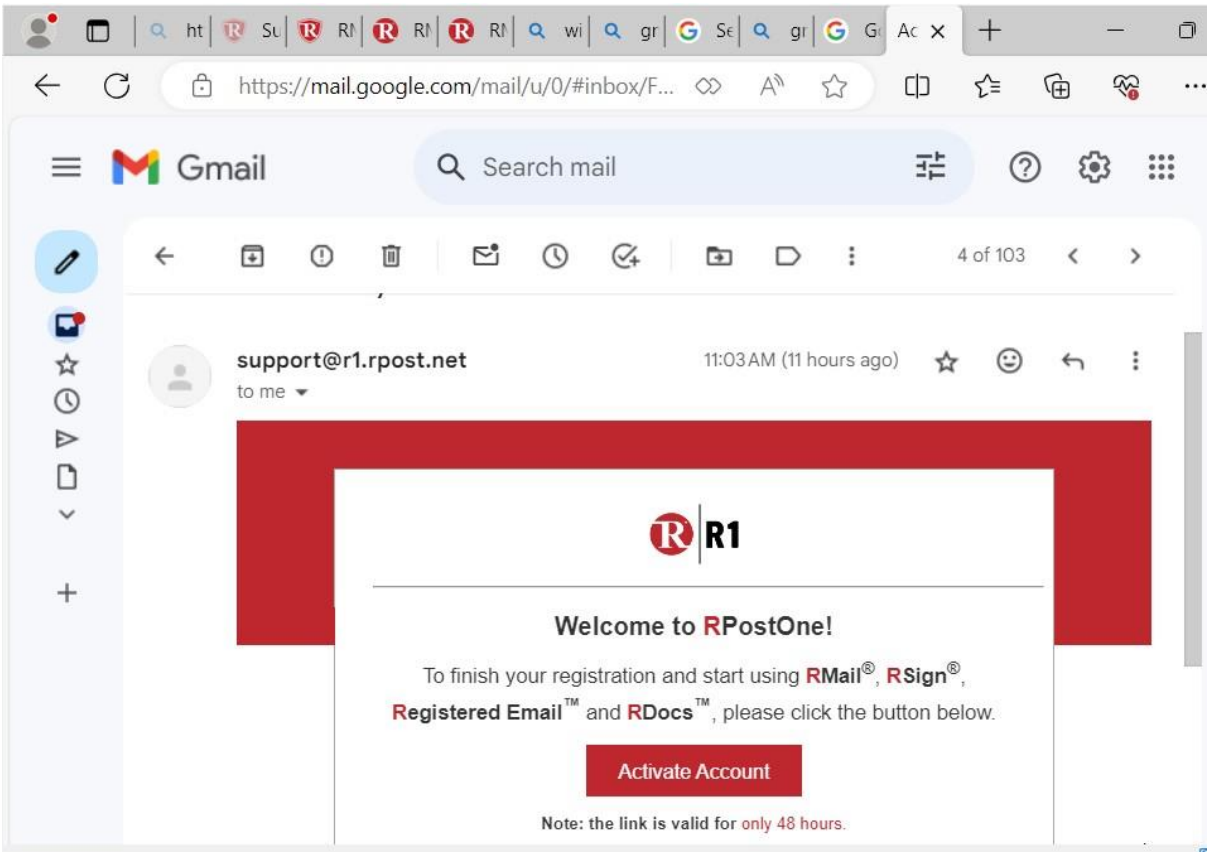


-
- Final step appears displaying that the activation link has been sent to the registered email address.

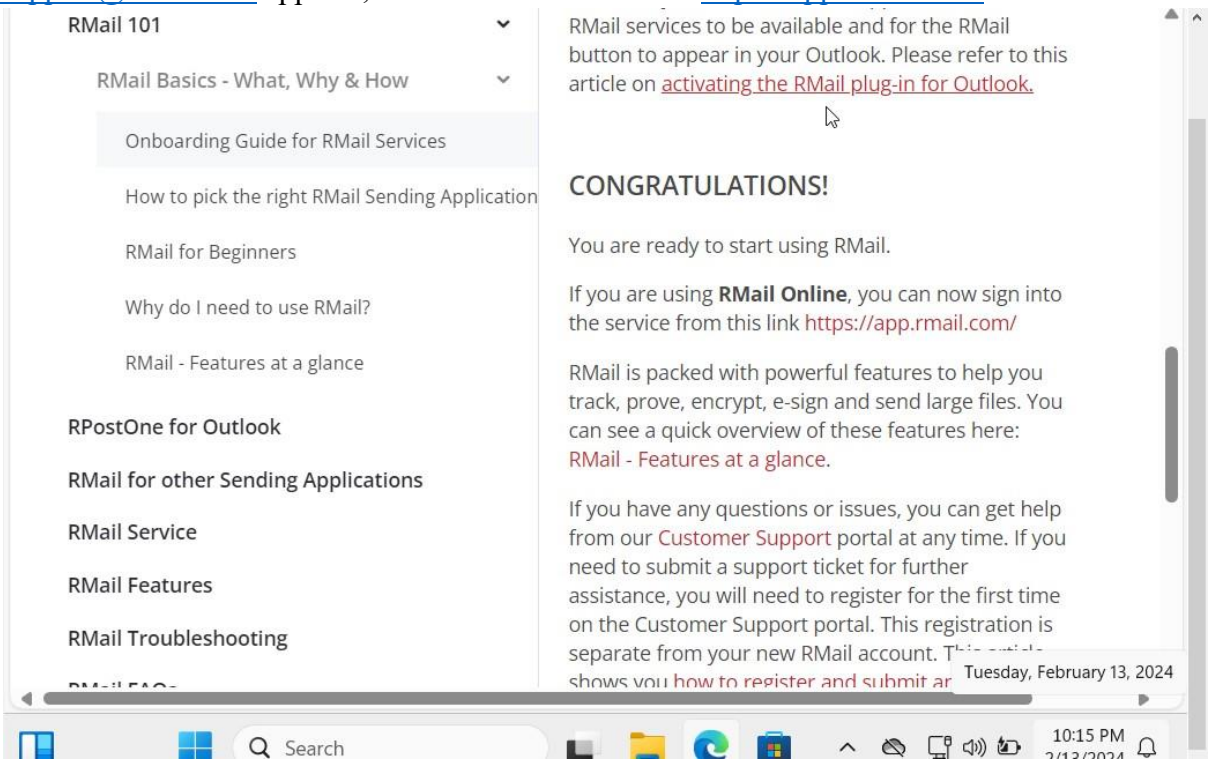


Open Gmail mail webpage on a new tab, on you Gmail account, click on support@rpost.com and then click on activation link to activate the account.

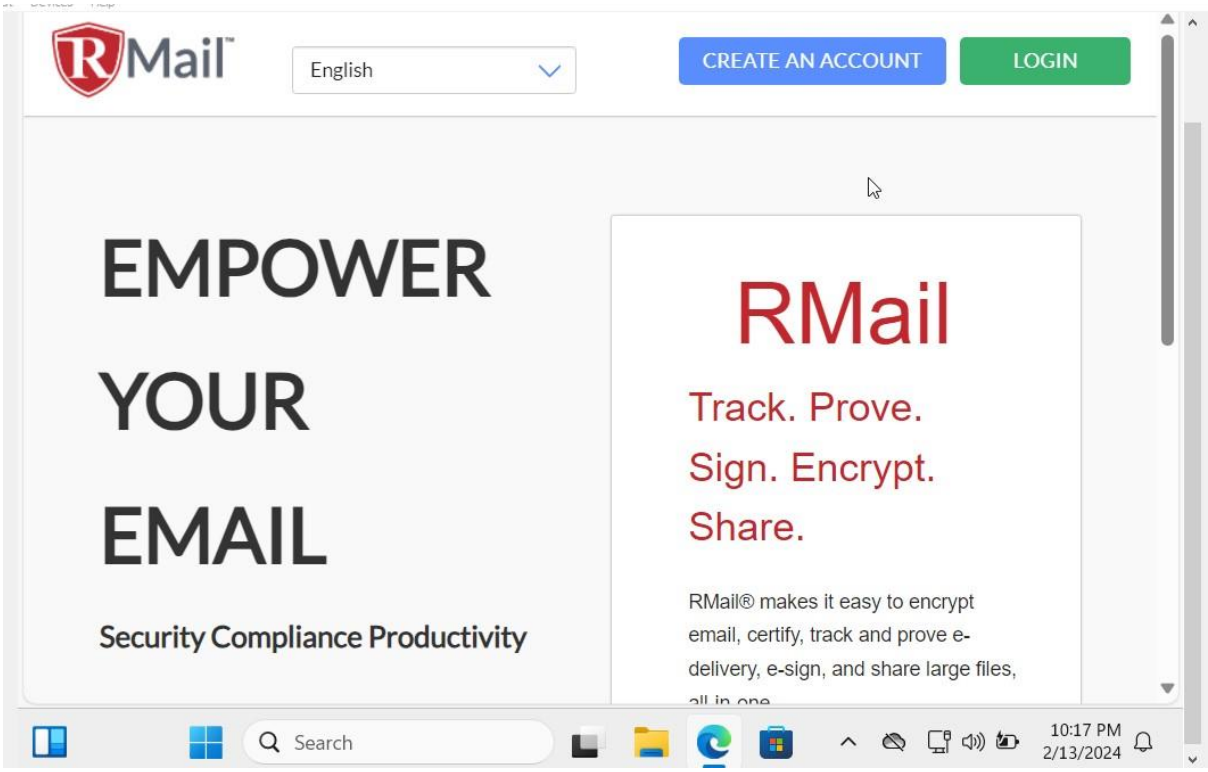
•



Support@rmail.com appears, scroll down and click on https://app.rmail.com/ link

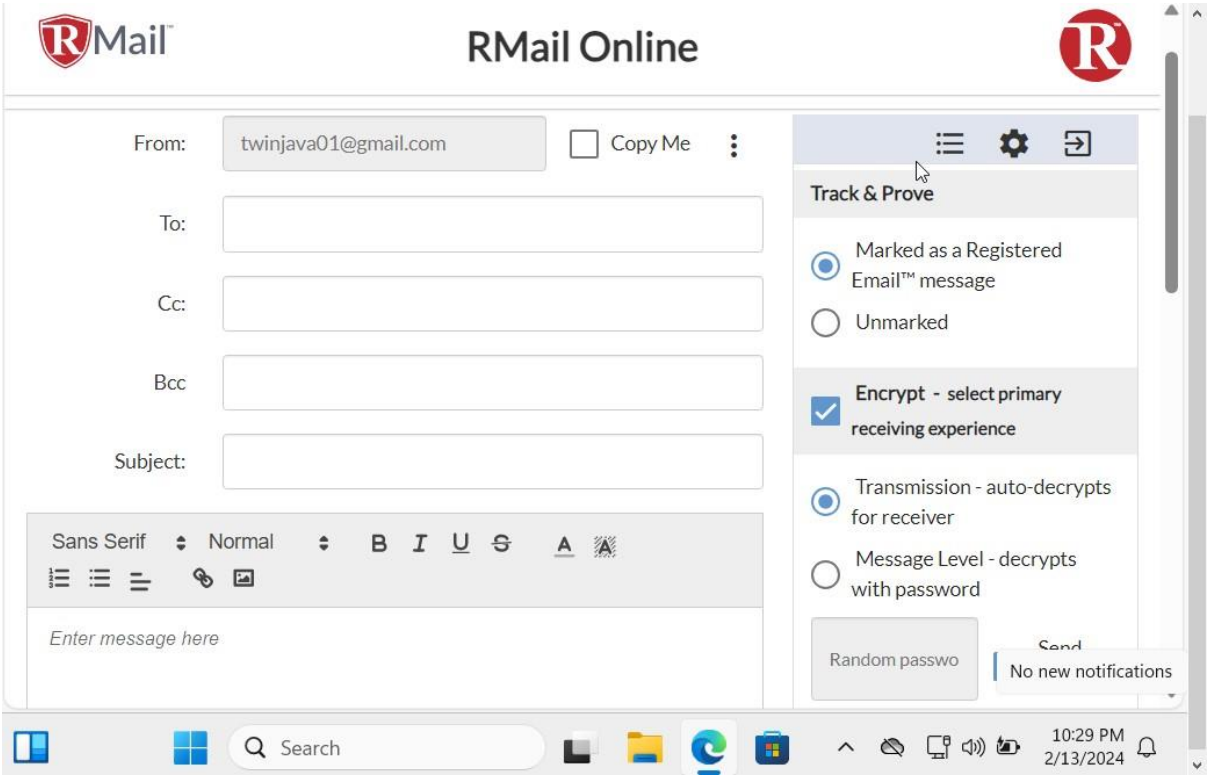


-
- When the app.rmail.com appears, click on login



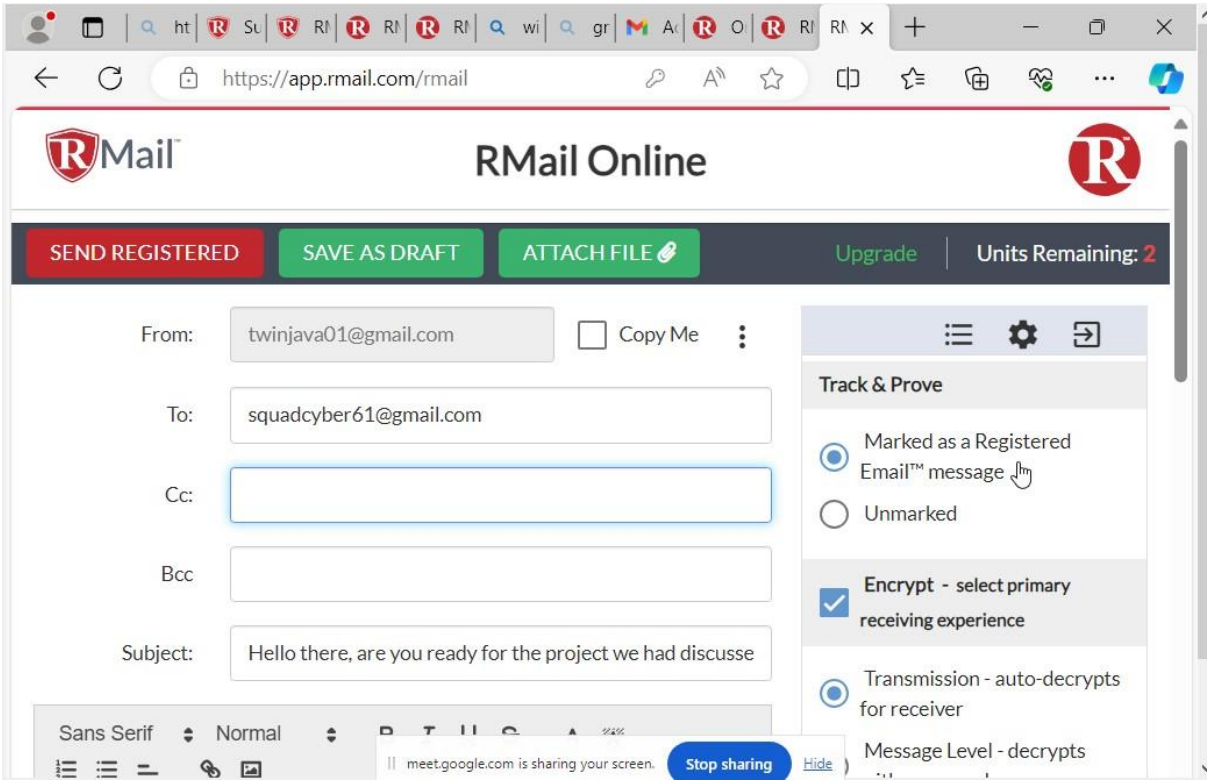
The Rmail web page appear, enter recipient address and ensure that

i. Marked as is selected under track & prove section
ii. Check the encrypt select primary encrypt receiving experience option
iii. Ensure that the transmission-auto decrypt for receiver radio button is selected
iv. Ensure that E-sign – send for signature checkbox is checked.
v. Ensure that web sign radio button is selected

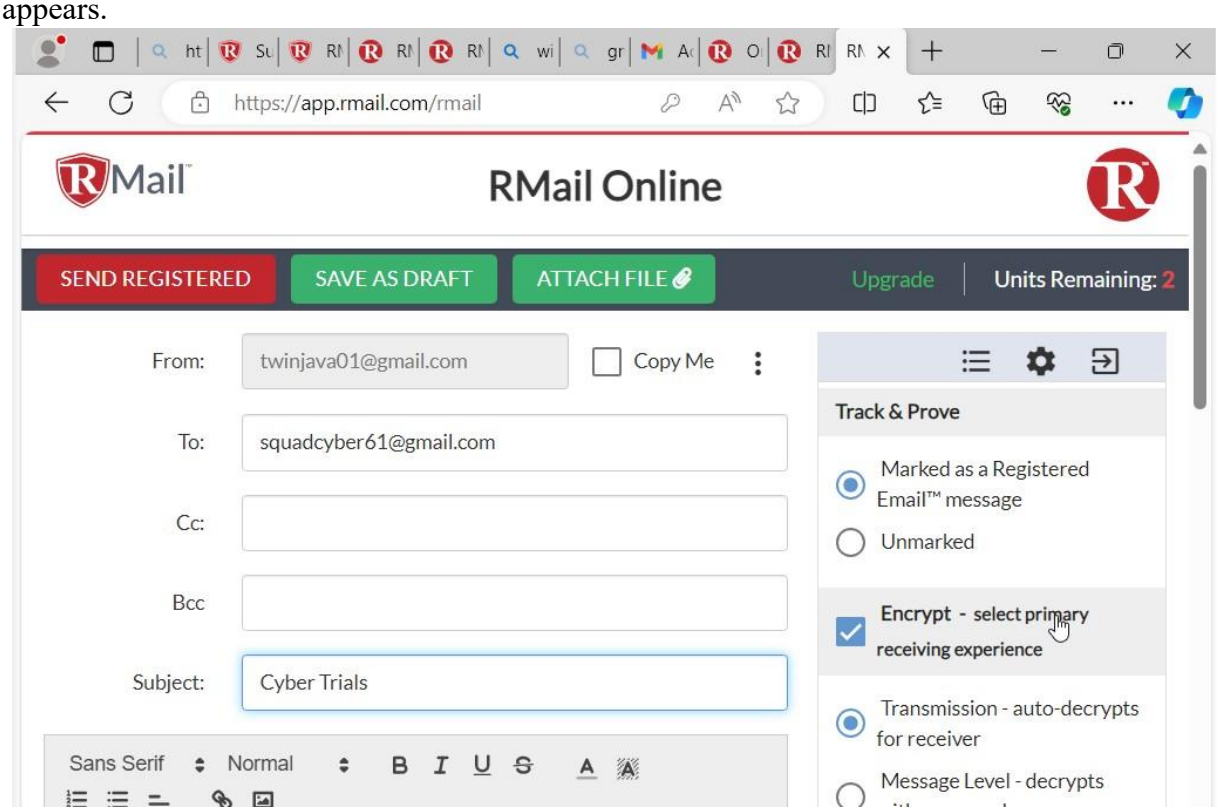


Enter message to be sent to the recipient

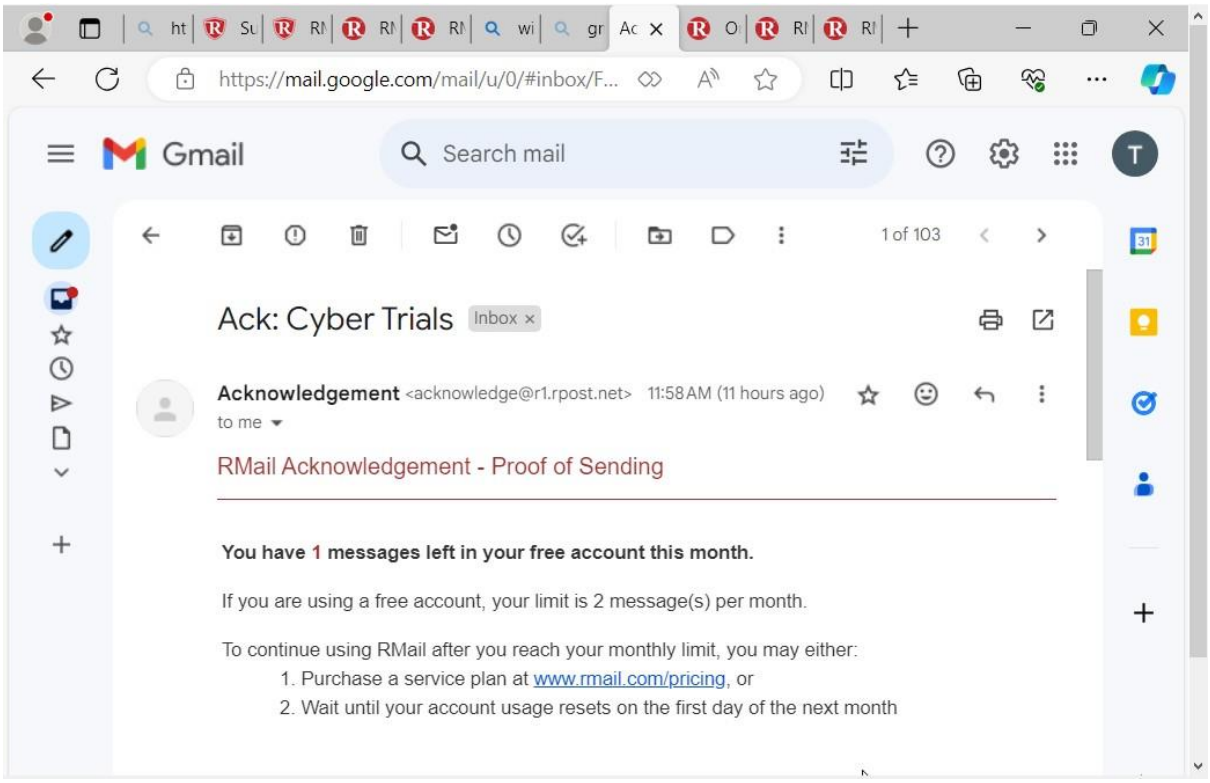
•



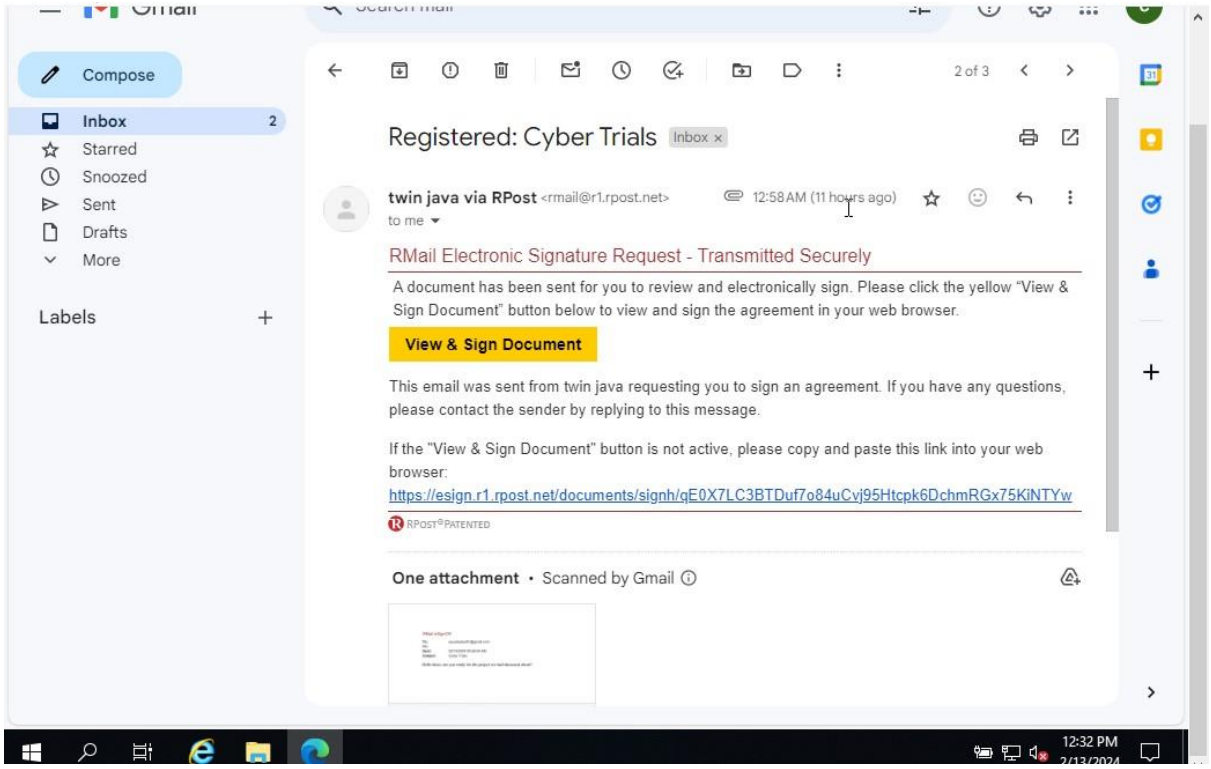
- After writing your message, click on sendregisterd tab, email sent pop up message appears.



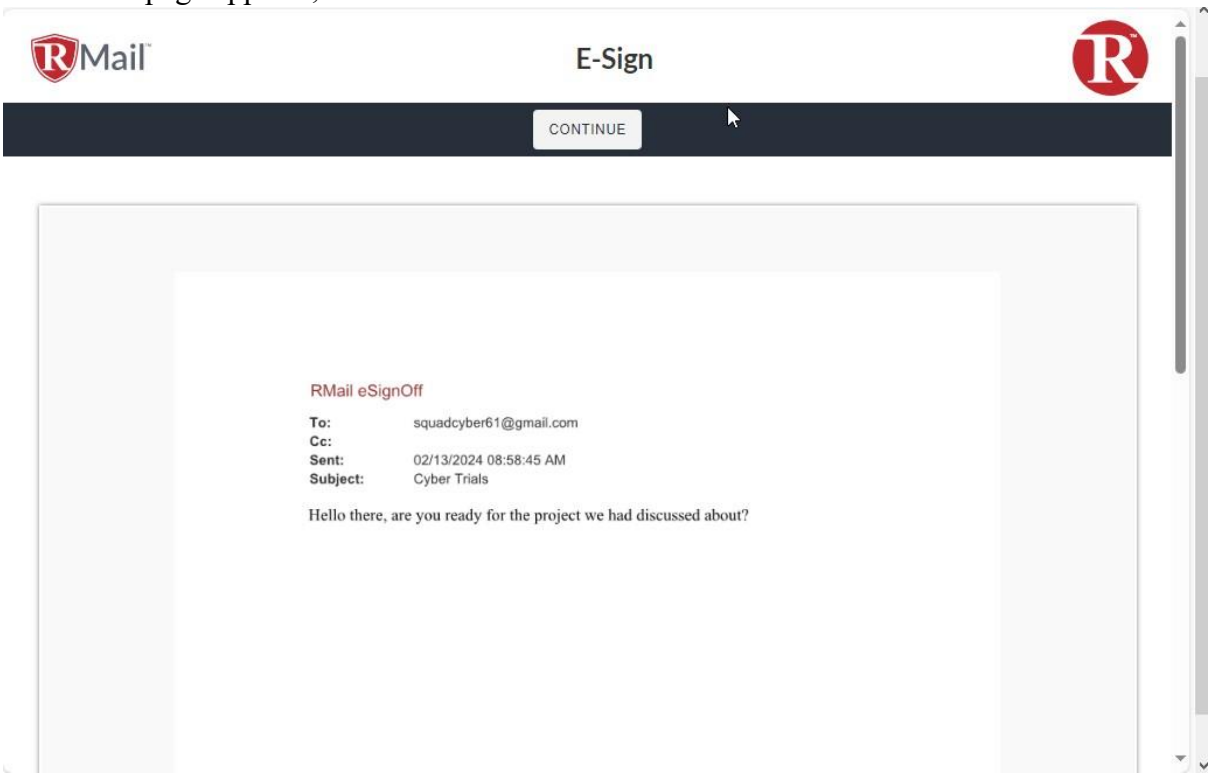
- You can observe acknowledgement email with proof of sending in Gmail



- Switch to your windows server 2019 vm machine, open your browser and navigate to the recipient Gmail account.
- Open the email from the sender
- You will observe that the email received is tagged as registered email, the recipient should review the document and electronically sign to confirm the identity.

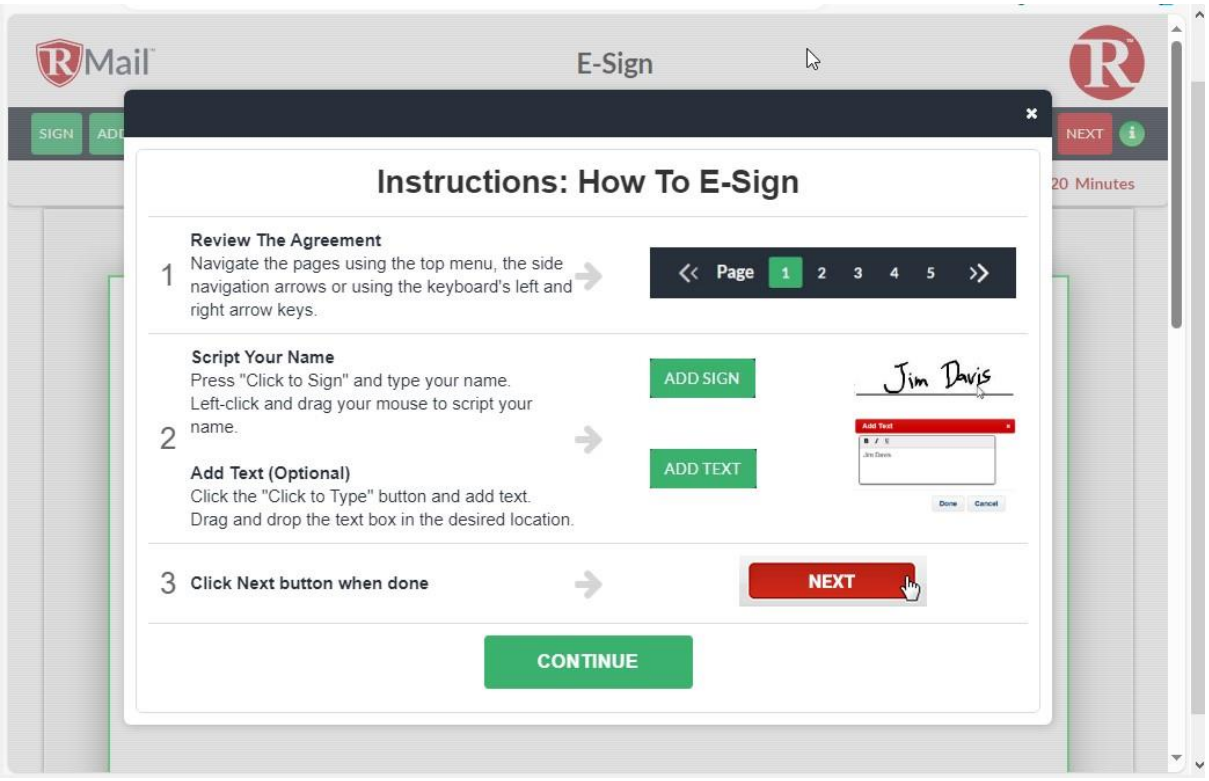


- Click on view and sign document button to sign an agreement.
- A new web page appears, click continue

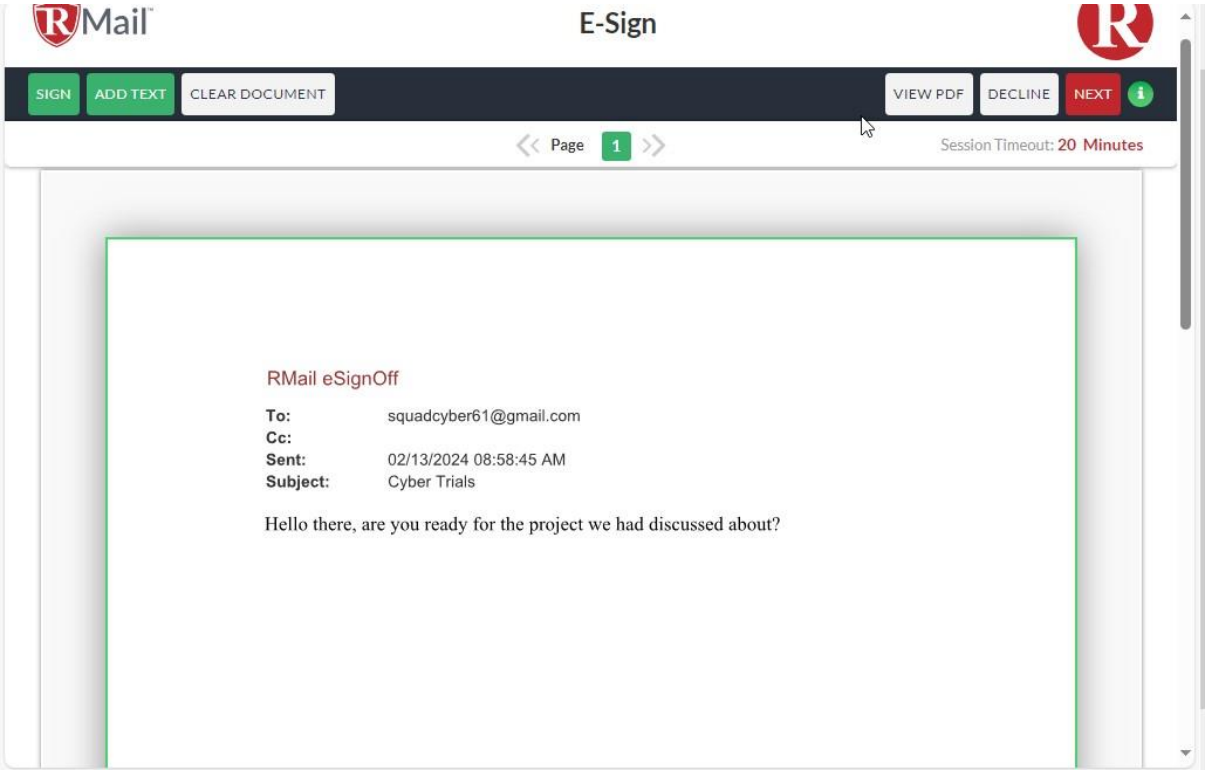


-

  The instructions: how to E-sign page appears, read the instructions carefully and click continue.

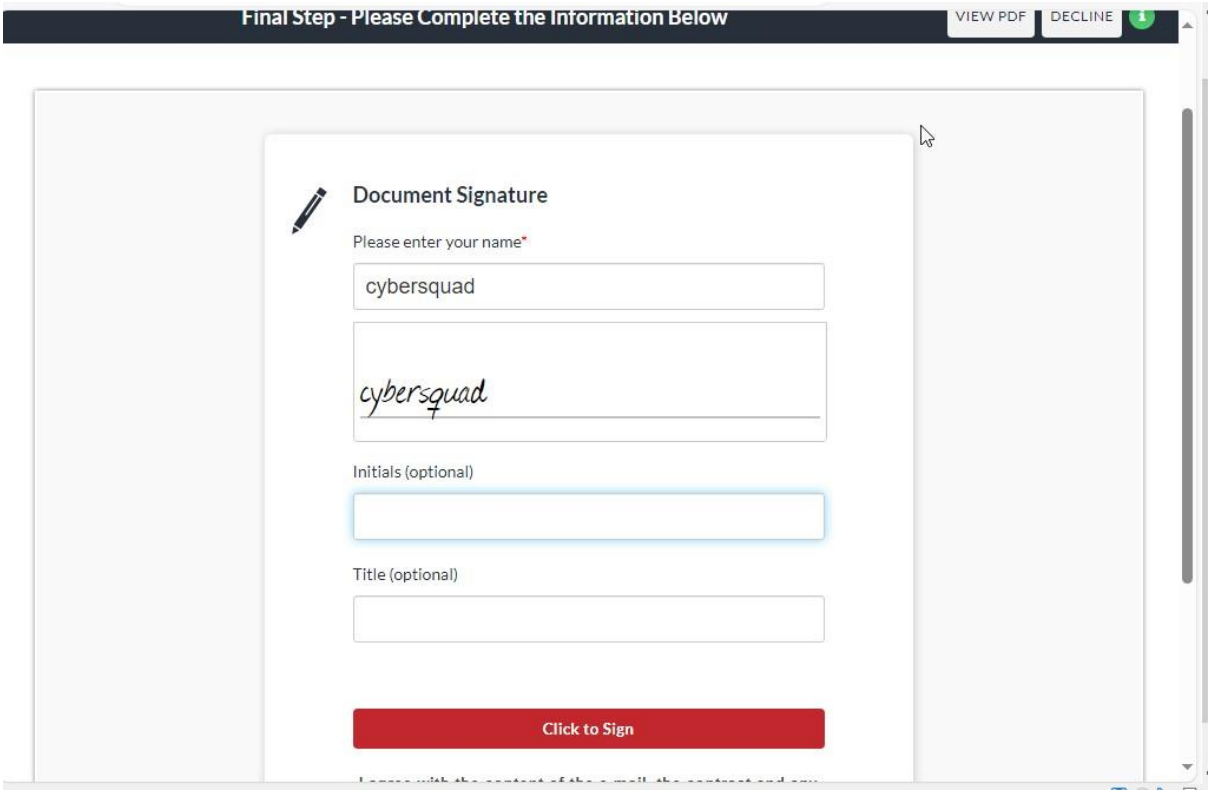


- Click next after viewing the email contents

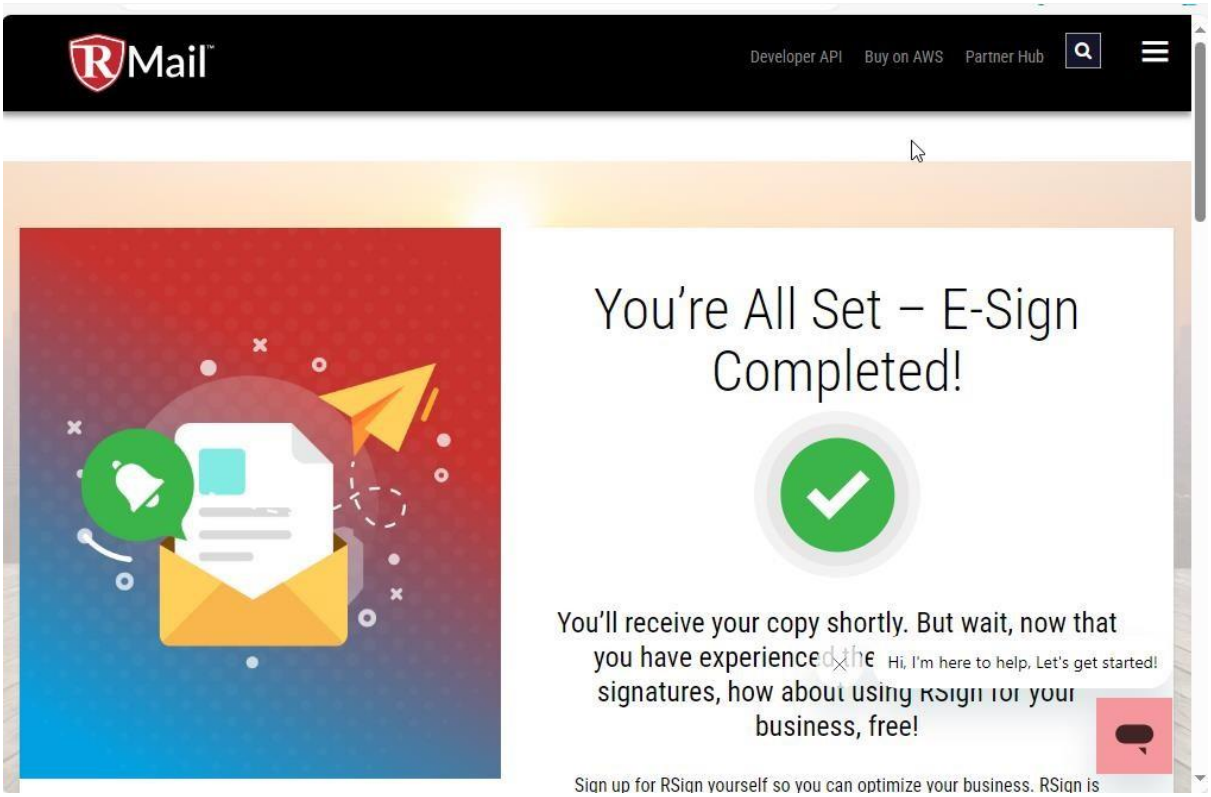


•

Document signature form appears, in the enter your name field, enter your name, and click to the sign in button.

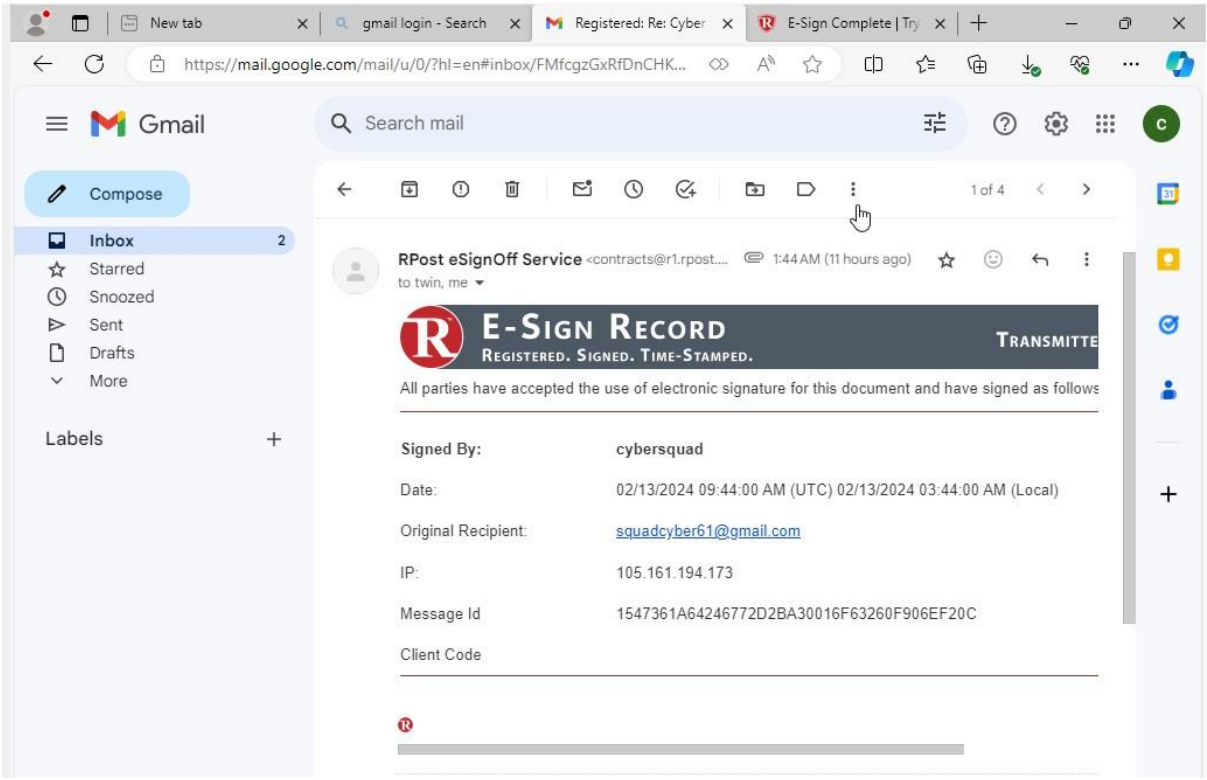


• E sign completed tab appears, close the current tab and return to the opened email.

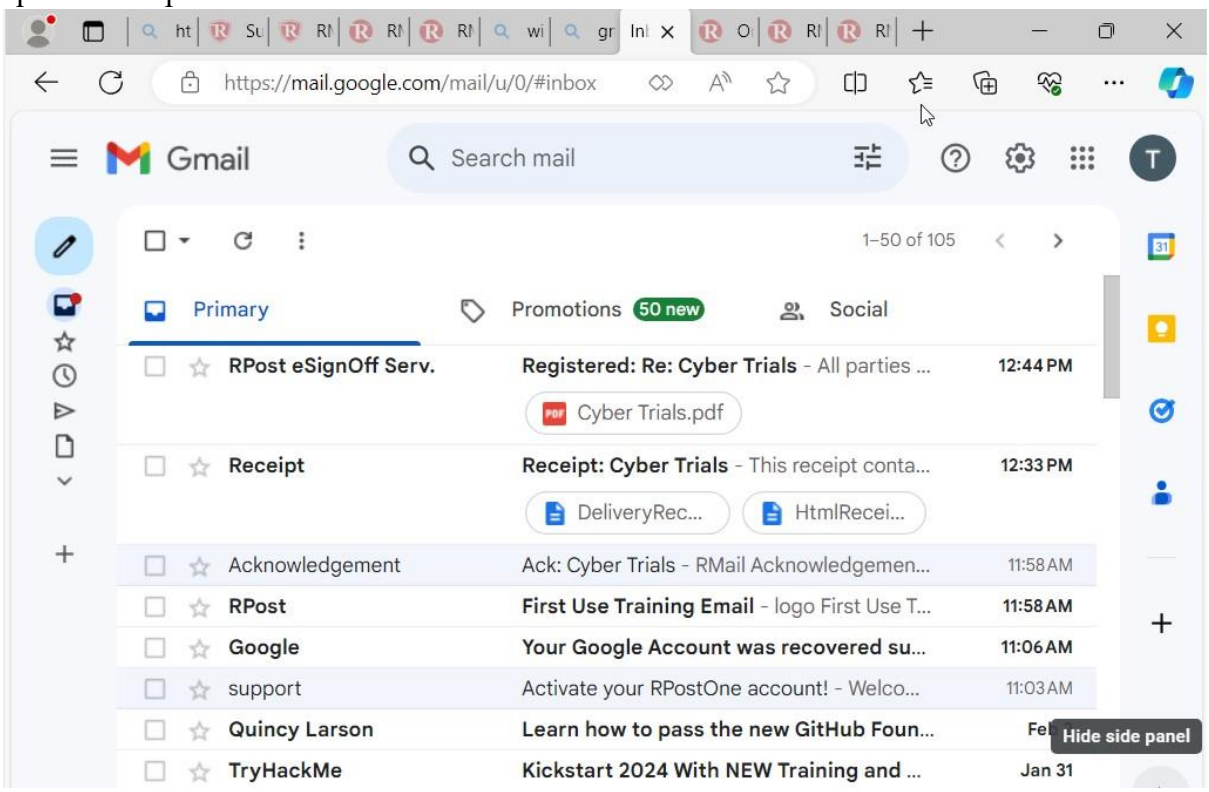


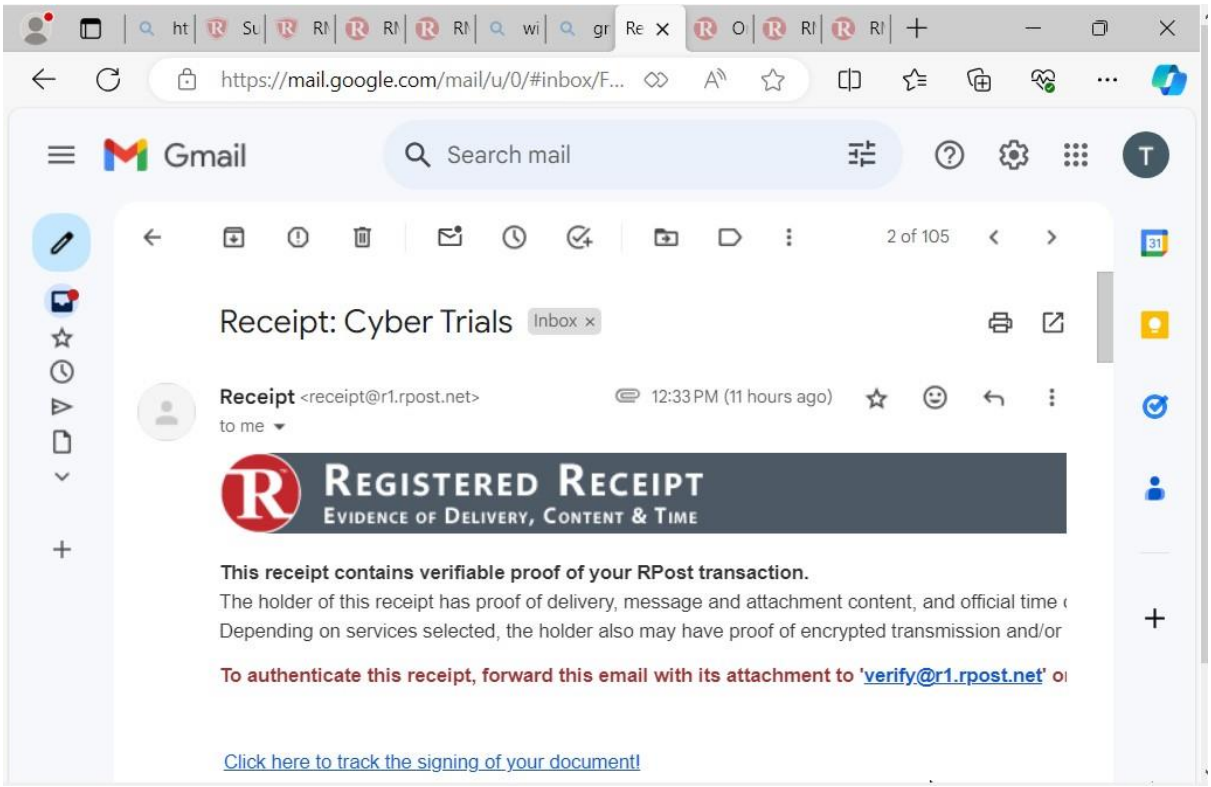
-

  Open an email from Rpost esignoff service, you can observe that is acknowledgement email from Rpost.



- Now switch to windows 11 virtual machine, to the senders Gmail account.
- You can observe two messages Recipient mails and Rpost eSignoff Service.
- Open the recipient email.

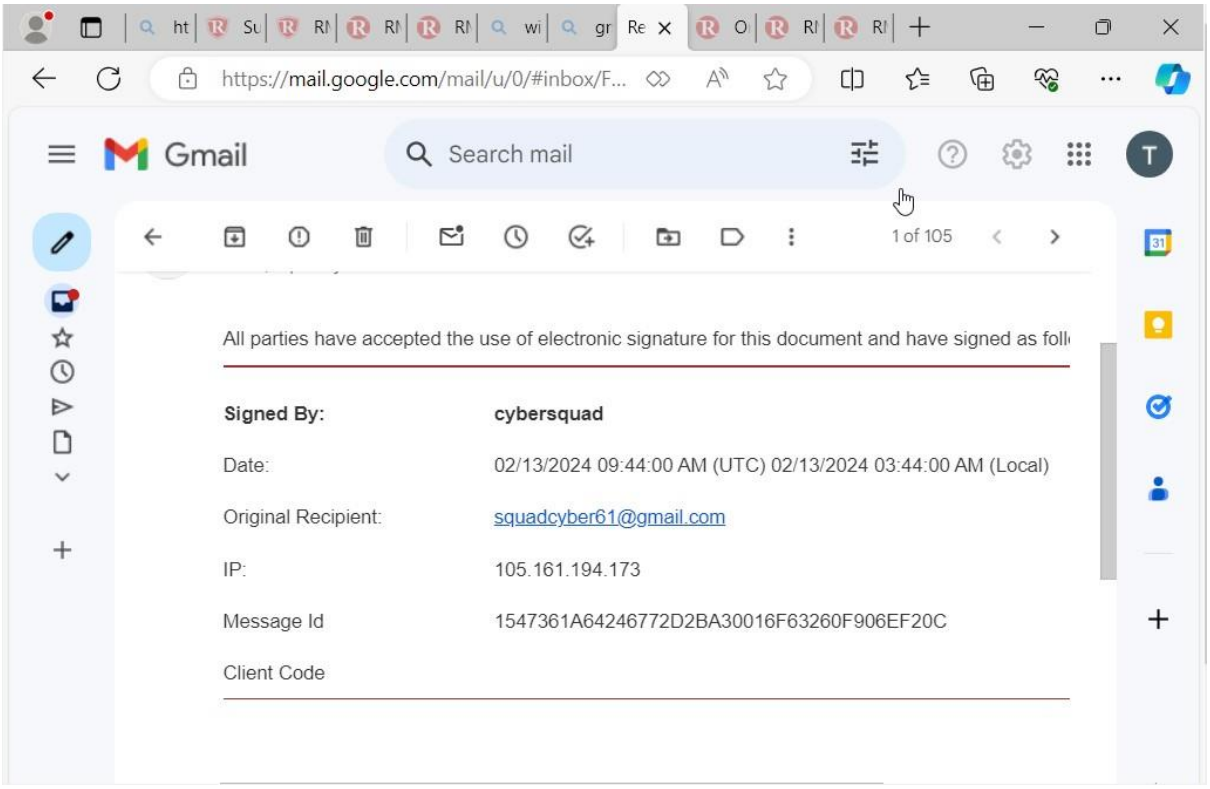




- Navigate back to the inbox and open Rpost eSignoff Services

NOTE!

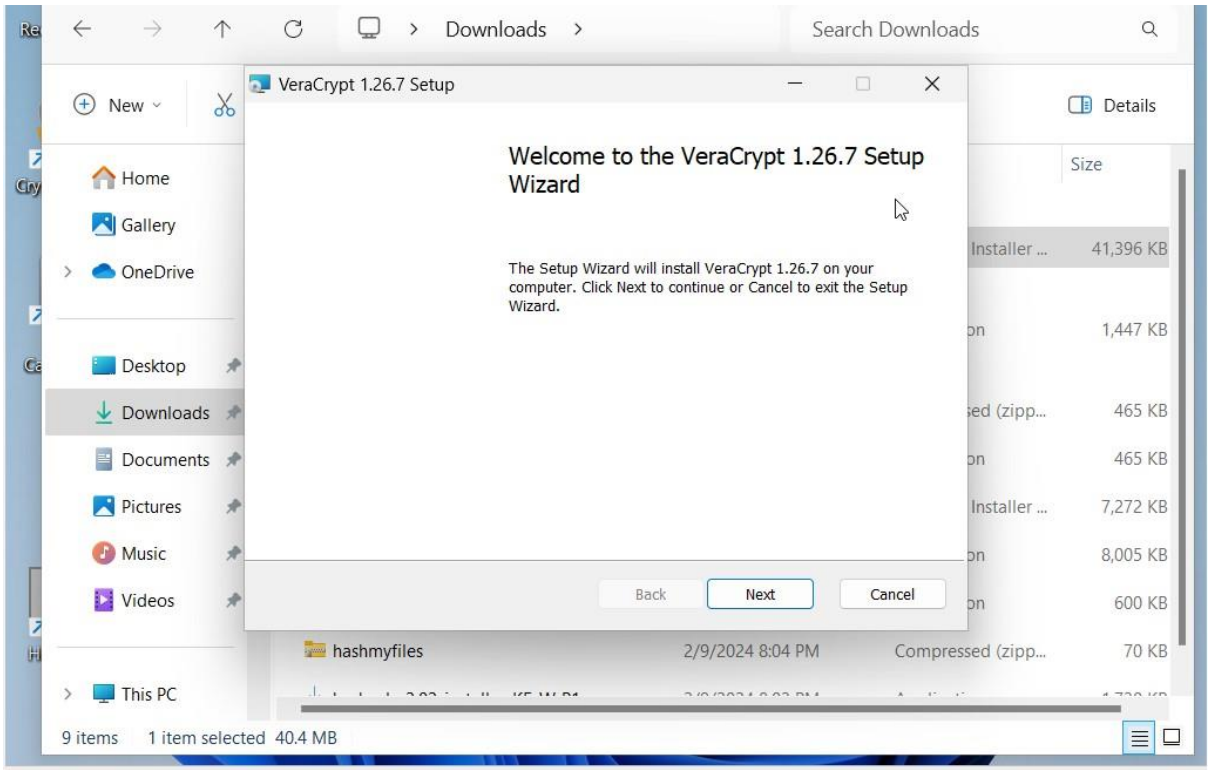
- This email contains the same information as the email received Rpost eSignoff Services by the recipient

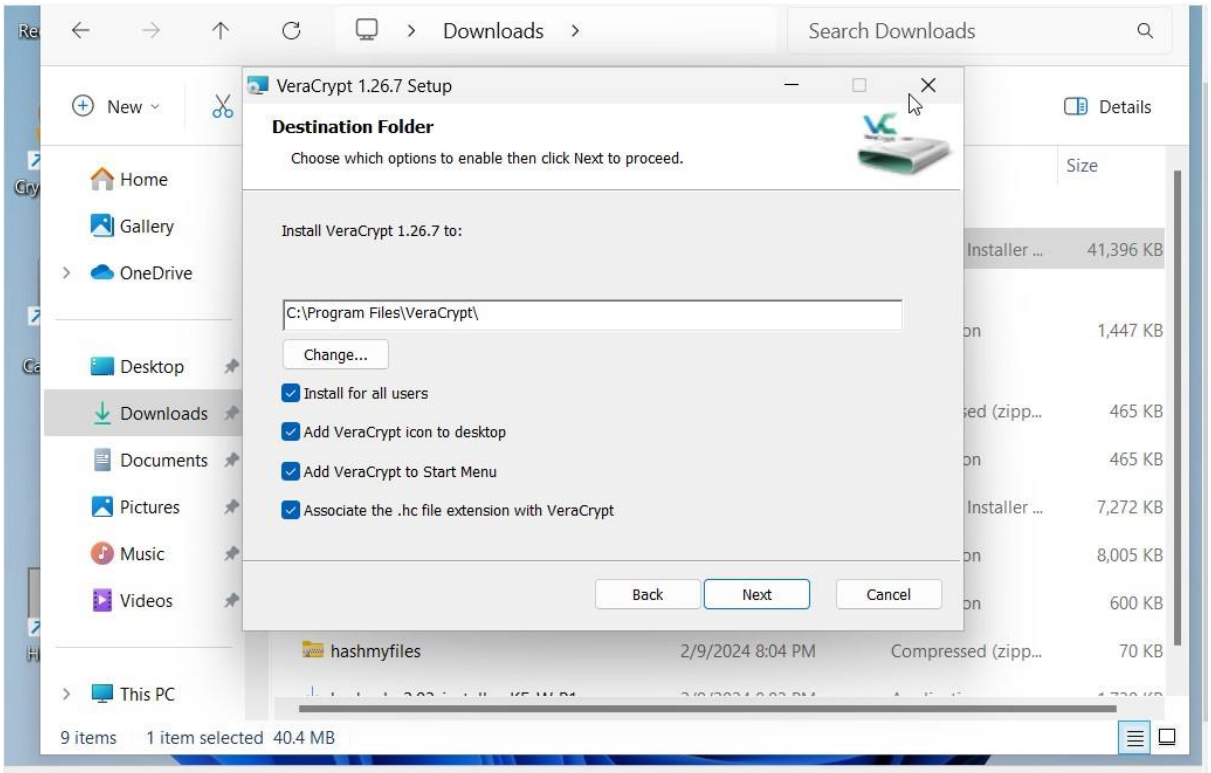

https://mail.google.com/mail/u/0/#inbox/F...
Gmail
Search mail
1 of 105
All parties have accepted the use of electronic signature for this document and have signed as foll
Signed By: cybersquad
Date: 02/13/2024 09:44:00 AM (UTC) 02/13/2024 03:44:00 AM (Local)
Original Recipient: squadcyber61@gmail.com
IP: 105.161.194.173
Message Id 1547361A64246772D2BA30016F63260F906EF20C
Client Code

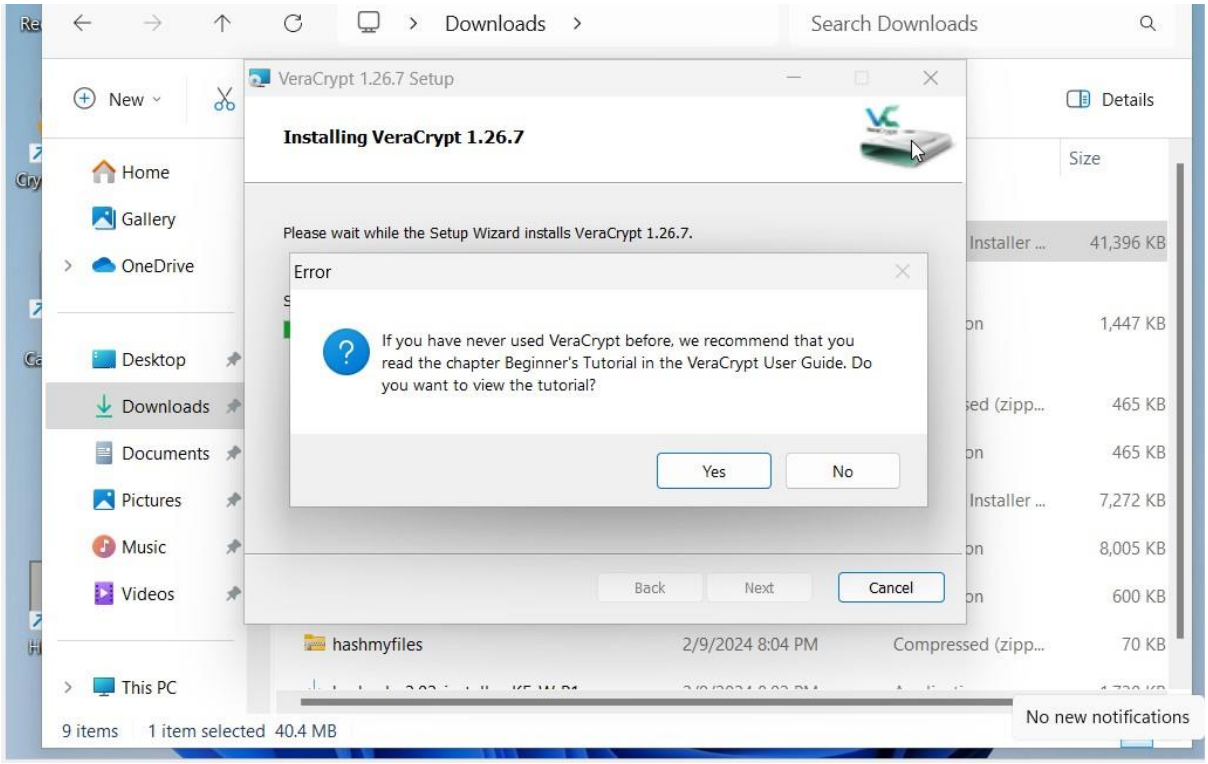
LAB 4:

TASK 1: Perform disk encryption using VeraCrypt.

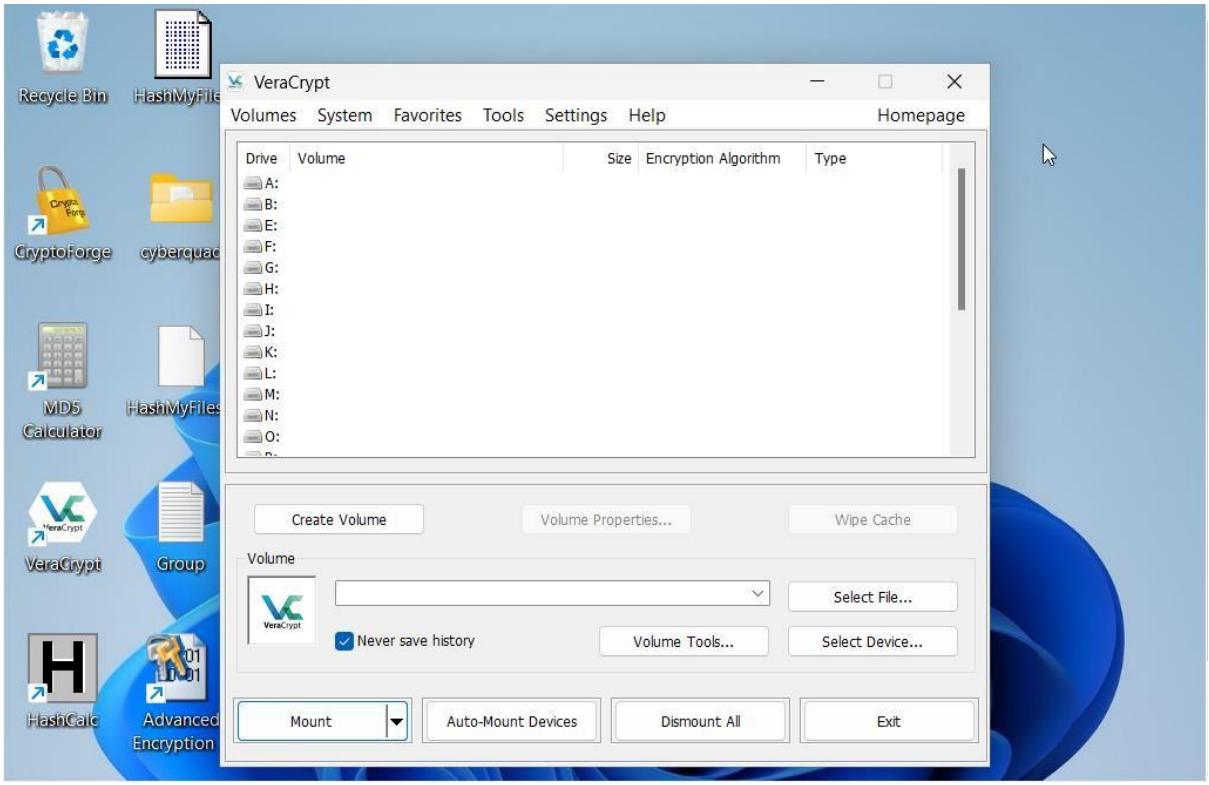
- Installation of VeraCrypt



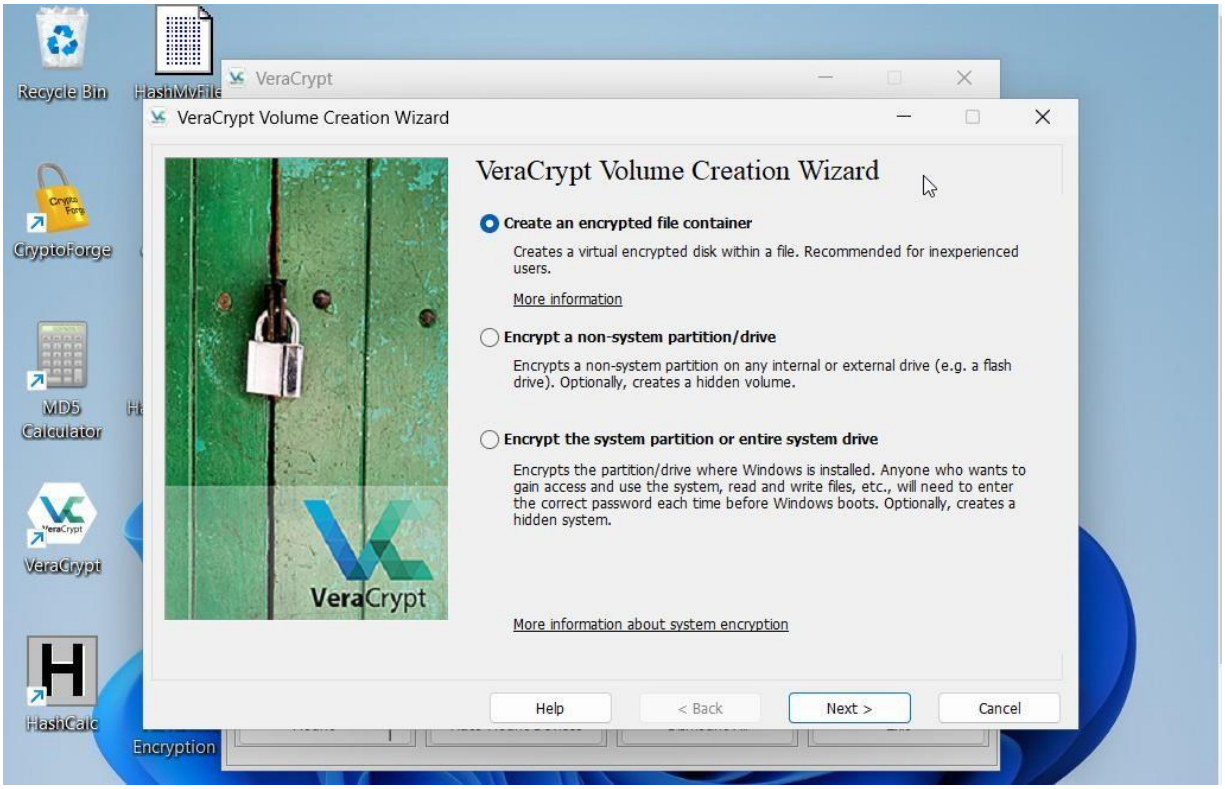



Downloads
Search Downloads
New
Details
Home
Gallery
OneDrive
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Size
VeraCrypt 1.26.7 Setup
Installing VeraCrypt 1.26.7
Please wait while the Setup Wizard installs VeraCrypt 1.26.7.
Error
If you have never used VeraCrypt before, we recommend that you read the chapter Beginner's Tutorial in the VeraCrypt User Guide. Do you want to view the tutorial?
Yes
No
Back
Next
Cancel
Installer ... 41,396 KB
1,447 KB
465 KB
465 KB
Installer ... 7,272 KB
8,005 KB
600 KB
hashmyfiles 2/9/2024 8:04 PM Compressed (zipp... 70 KB
9 items
1 item selected 40.4 MB
No new notifications

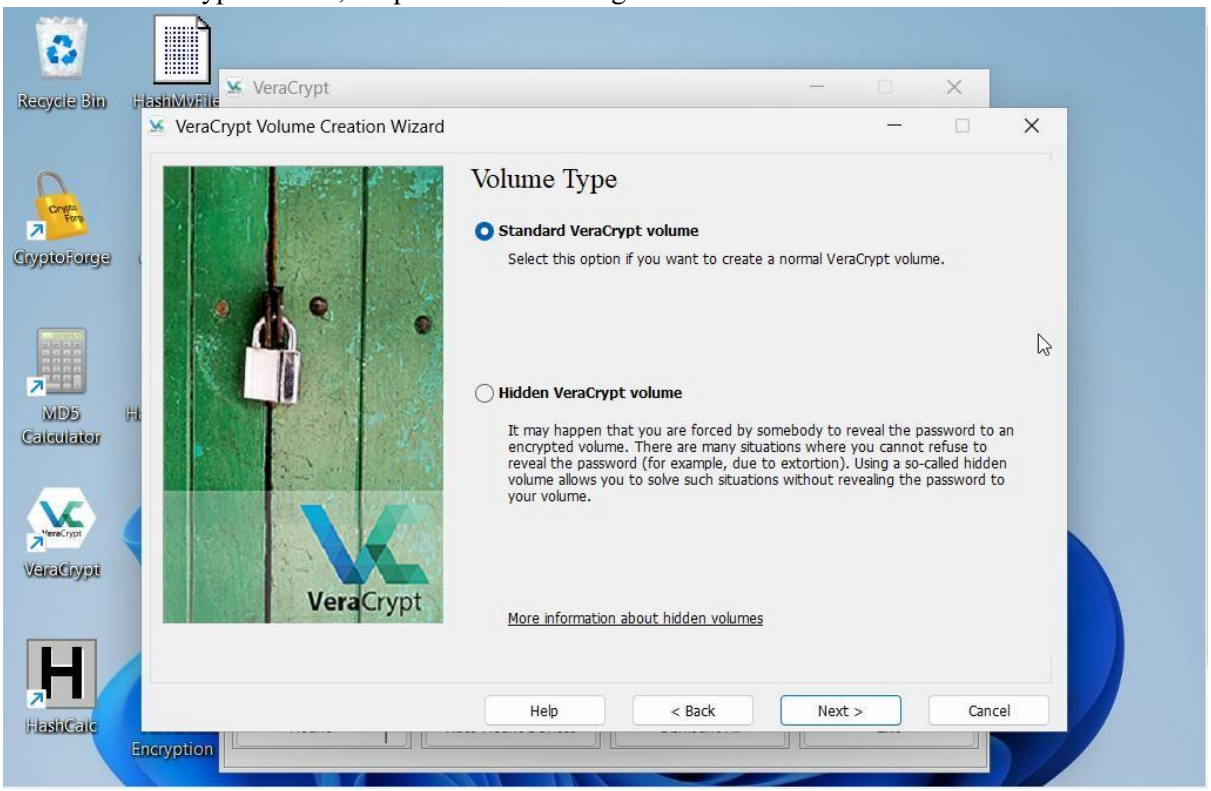
- After installation and launching, VeraCrypt windows appears as shown.



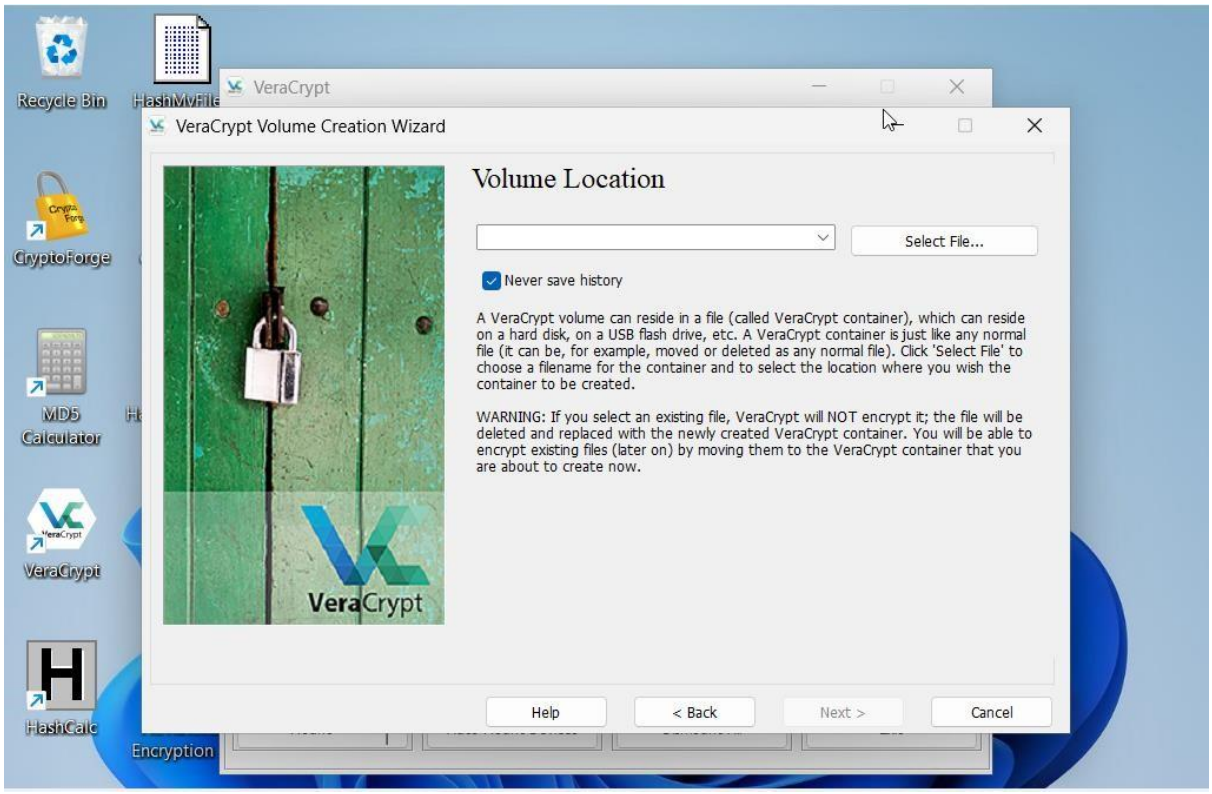
- Disk encryption process starts by clicking, create volume button.
- VeraCrypt Volume Creation Wizard appears, make sure you check on create an encrypted file container and click next.



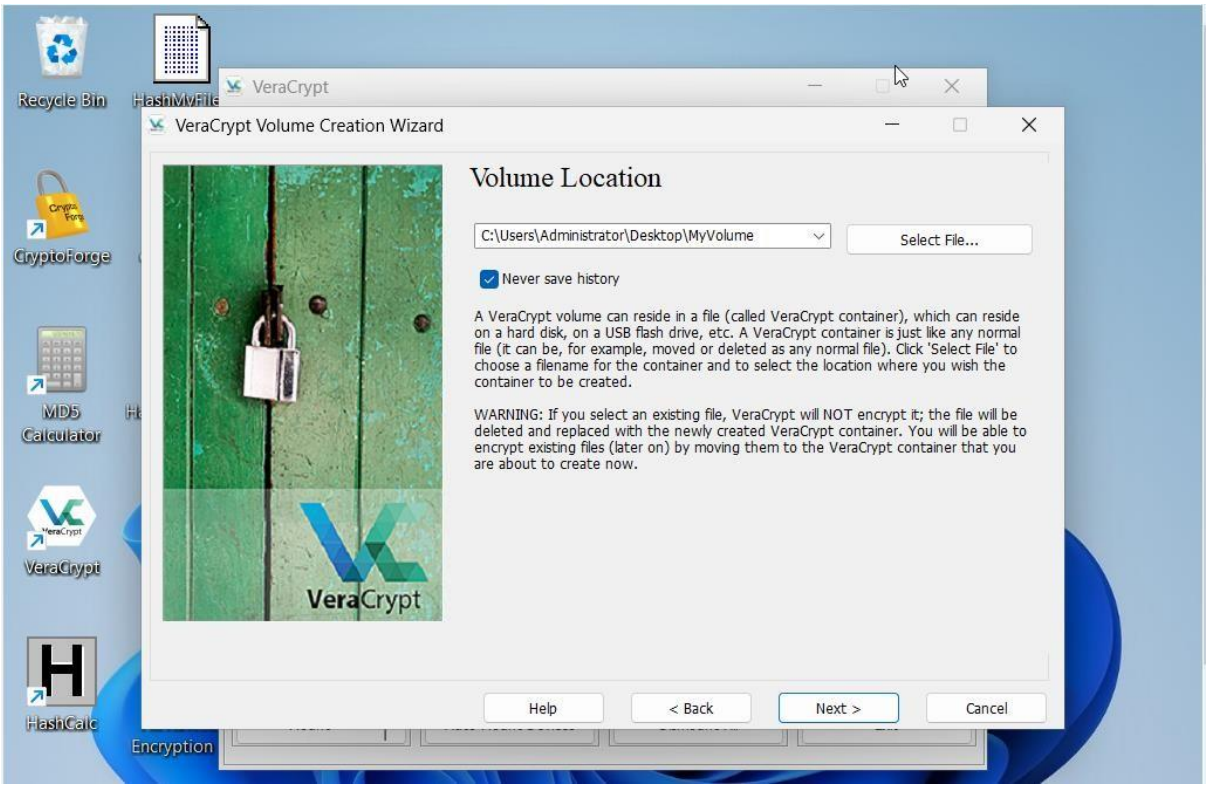
- In the volume type wizard , keep the default settings and Next.



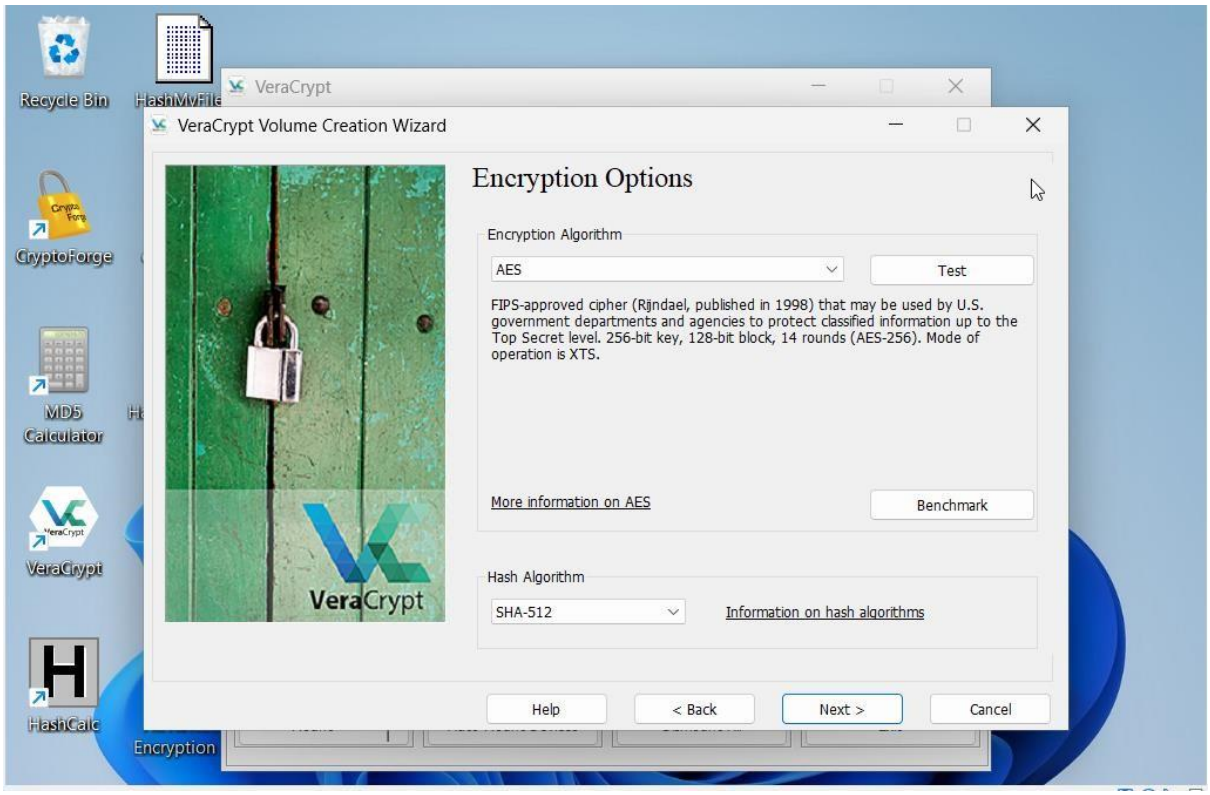
- In the Volume location wizard, click select file



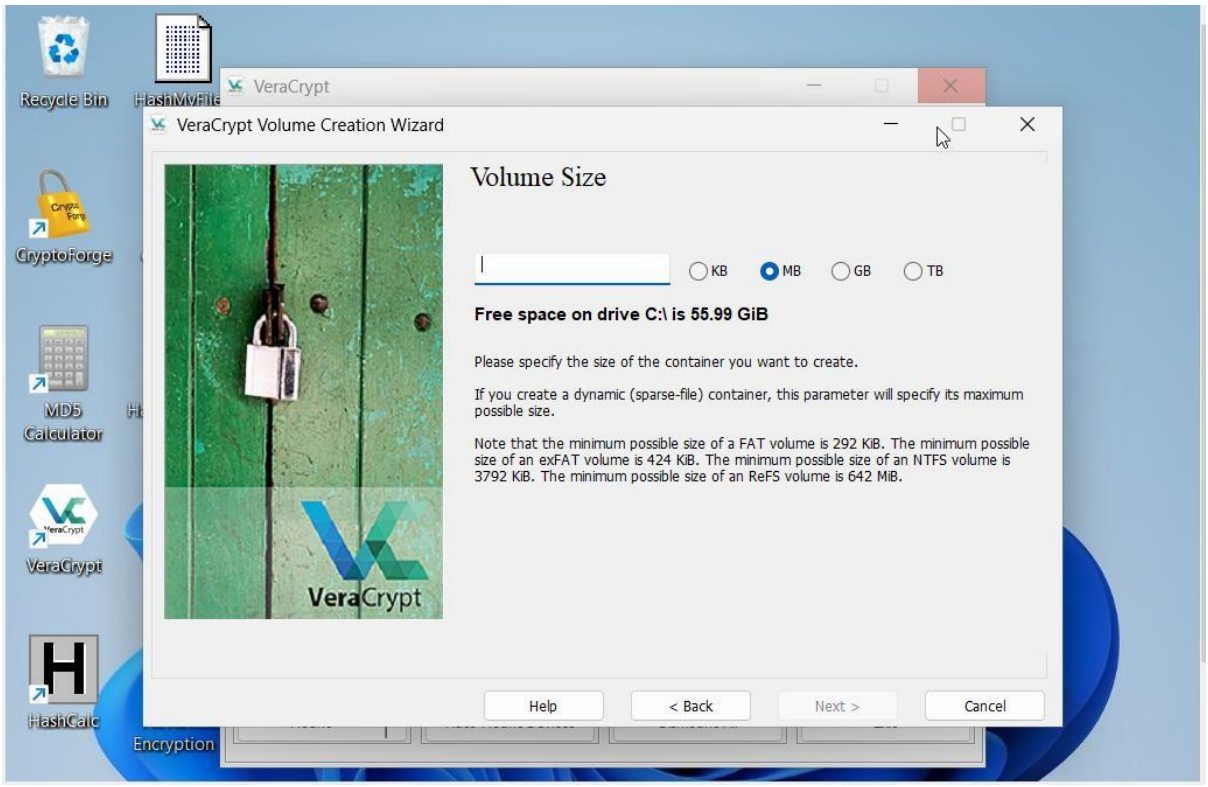
- Specify path and file windows appears, navigate to the desired location (Desktop), Provide the file name as My volume and click save
- The location of the file containing the VeraCrypt volume appears under the volume location field, Click next.



- In the Encryption Options, keep the default settings and click next.



In the Volume Size wizard, ensure that the MB radio button is selected and specify the size of the VeraCrypt container as 5, Click next

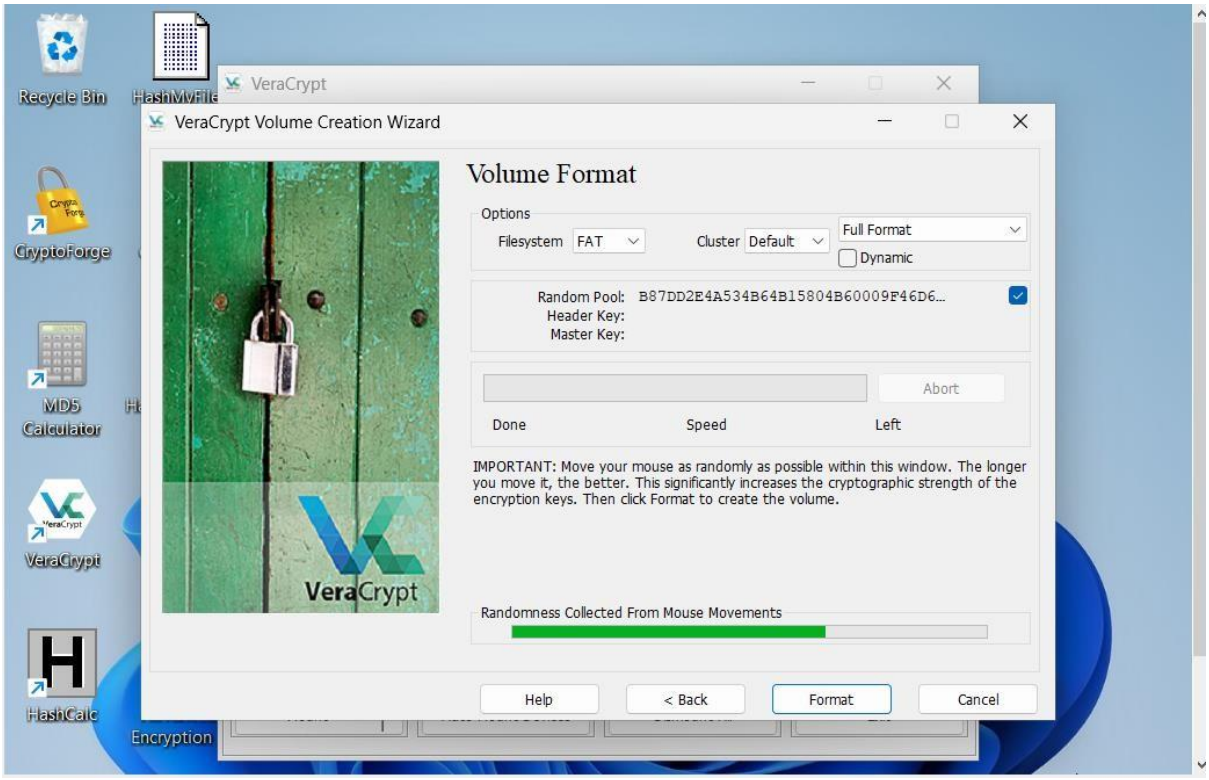


•

• In the Volume Password wizard, enter a strong password of your choice and click next • A VeraCrypt Volume Creation wizard appears, Click Yes.

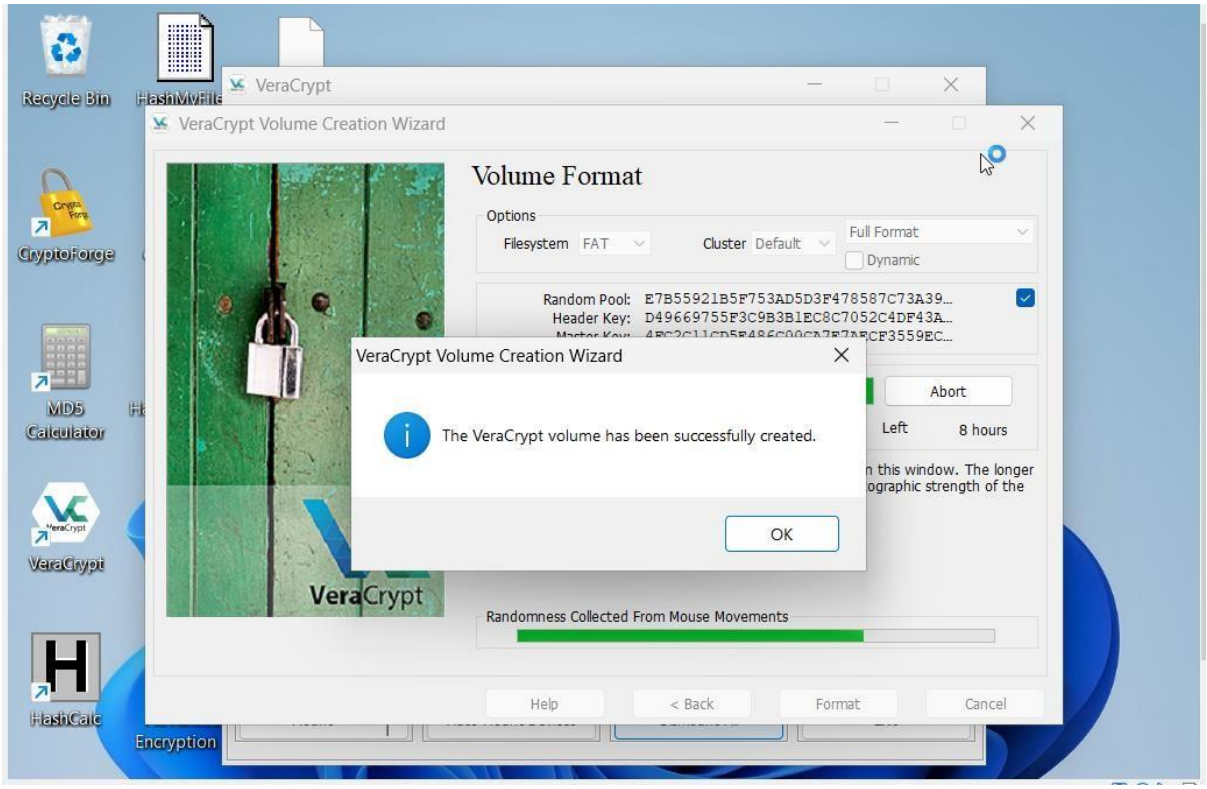
Check the check box under the Random pool, Header key and Master key section.

- Move mouse for 30 sec, within the Volume Creation Wizard and click the format button

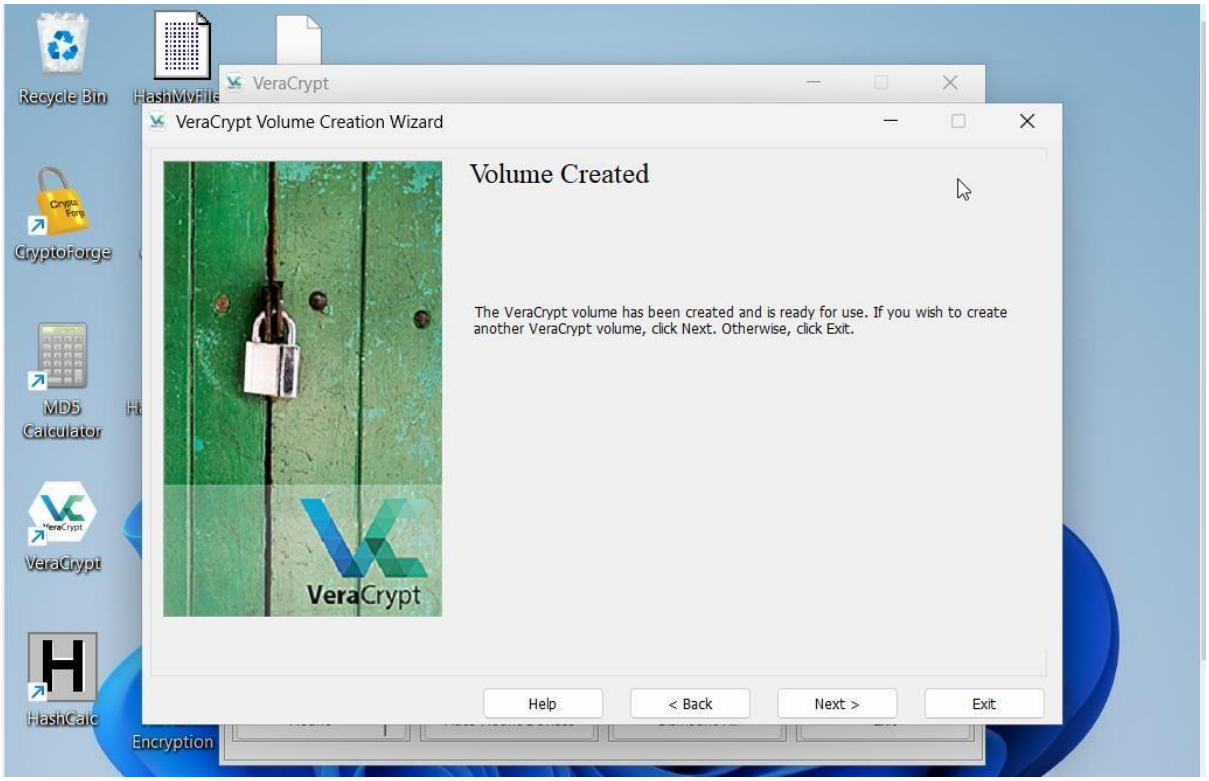


- Once the volume is created a VeraCyrpt Volume Creation Wizard dialog box appears, click okay.

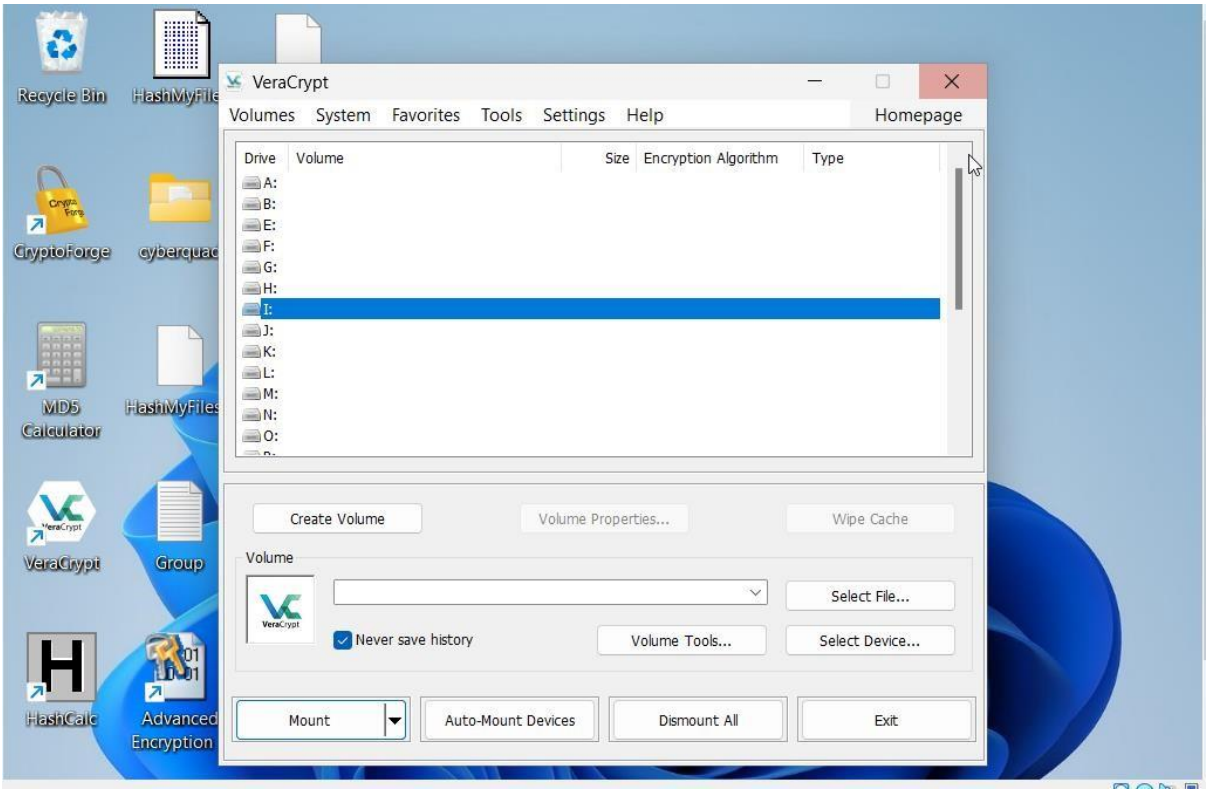
-


Recycle Bin
CryptoForge
MD5 Calculator
VeraCrypt
HashCalc
Encryption
VeraCrypt
VeraCrypt Volume Creation Wizard
Volume Format
Options
Filesystem FAT
Cluster Default
Full Format
Dynamic
Random Pool: E7B55921B5F753AD5D3F478587C73A39...
Header Key: D49669755F3C9B3B1EC8C7052C4DF43A...
Abort
Left 8 hours
this window. The longer
ographic strength of the
Randomness Collected From Mouse Movements
Help
< Back
Format
Cancel
VeraCrypt Volume Creation Wizard
The VeraCrypt volume has been successfully created.
OK

- Click exit on the Volume Created message that appear.

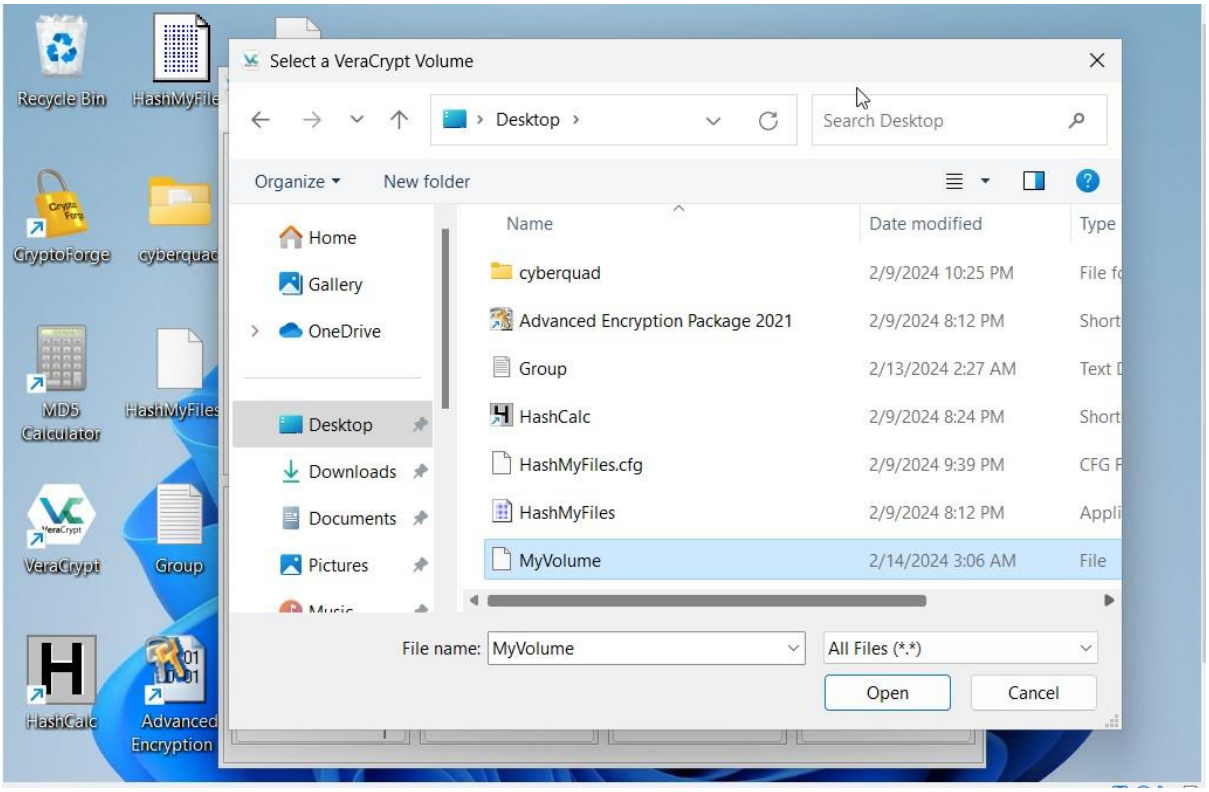


- Select a Drive I and click select file.

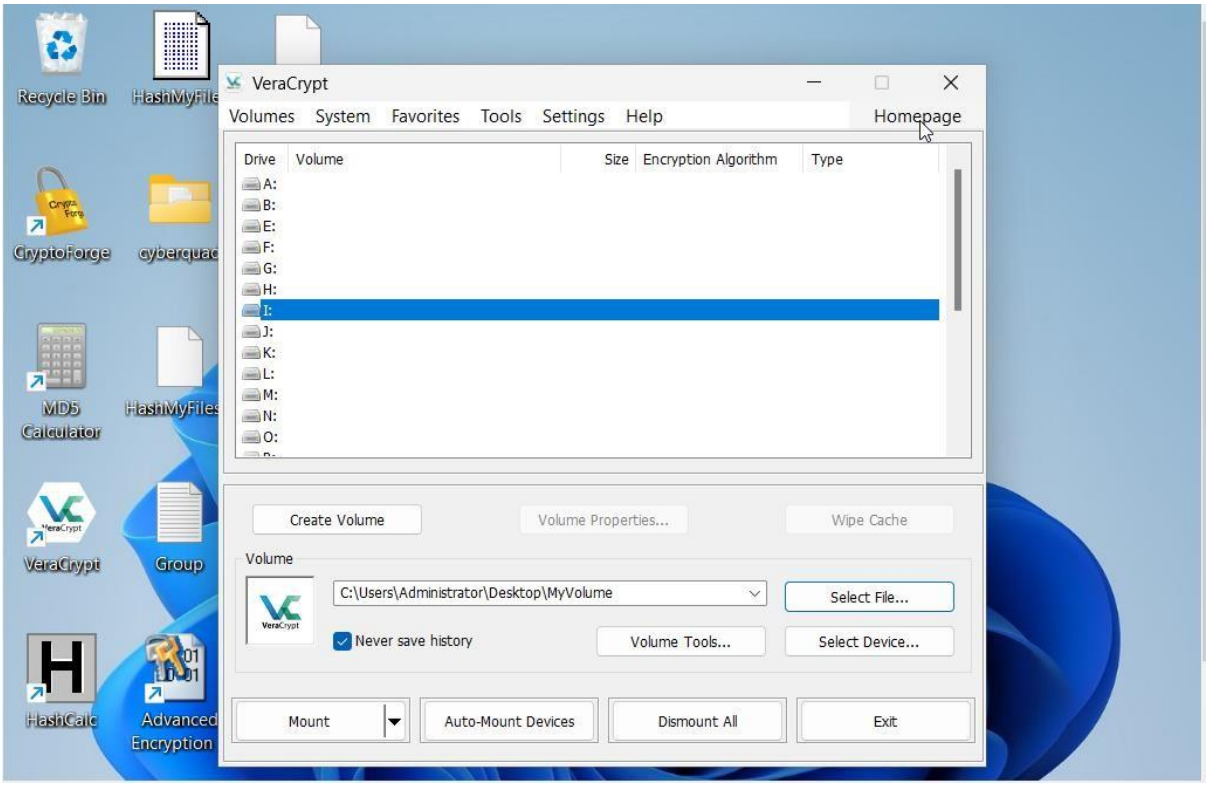


Navigate to desktop, click MyVolume and click open

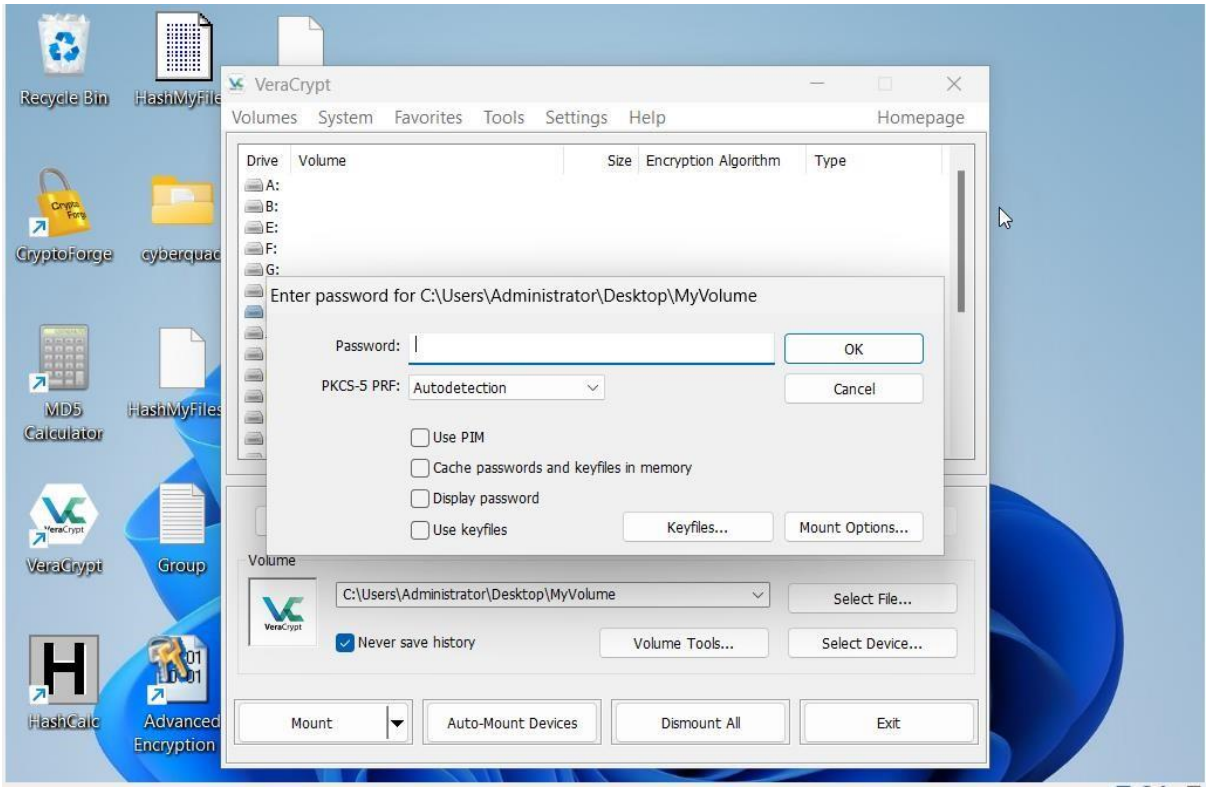
•

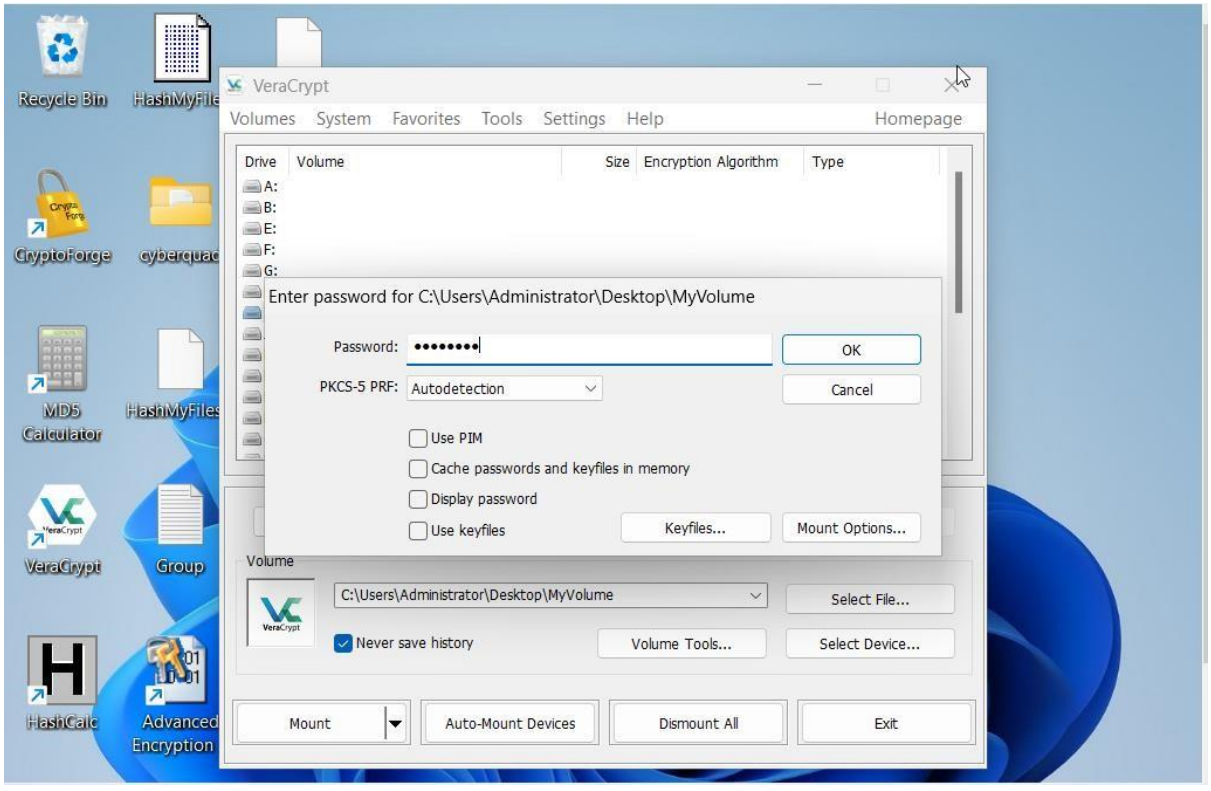


- VeraCrypt window appears displaying the location of the selected volume under the volume field then click mount.



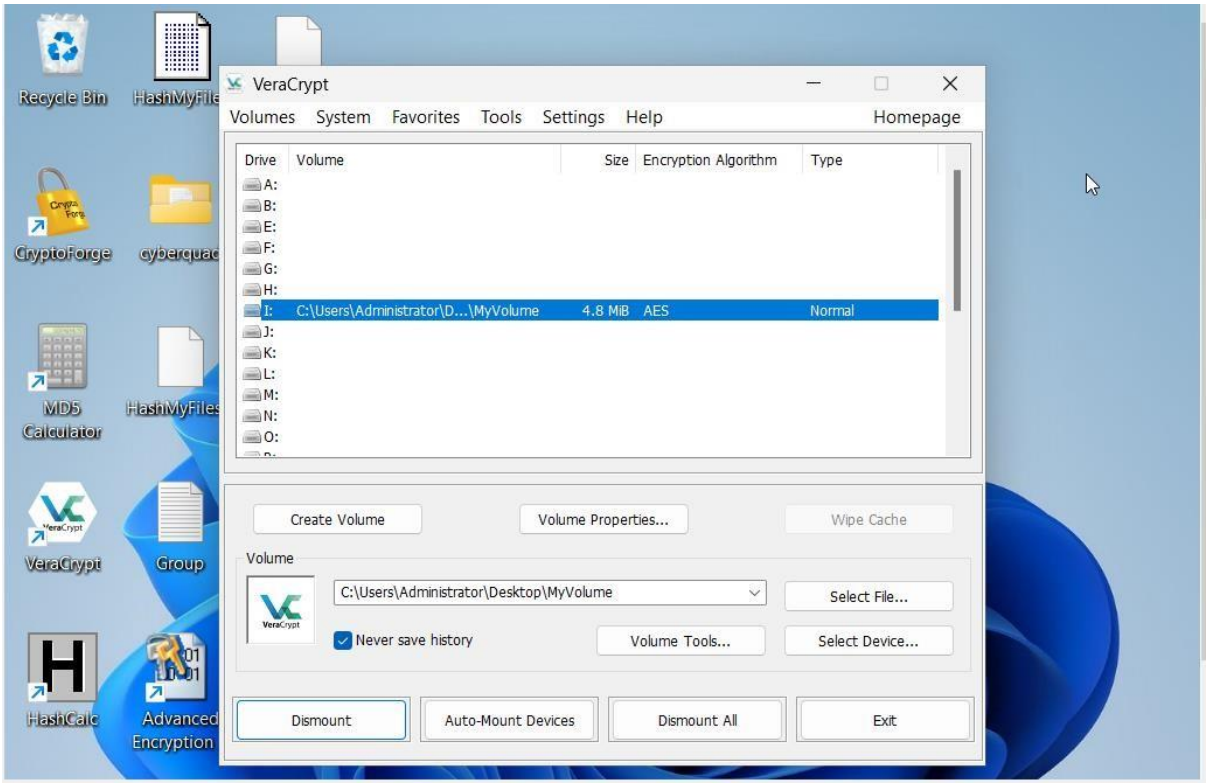
Type the password you specified in the Volume password then click okay

- 

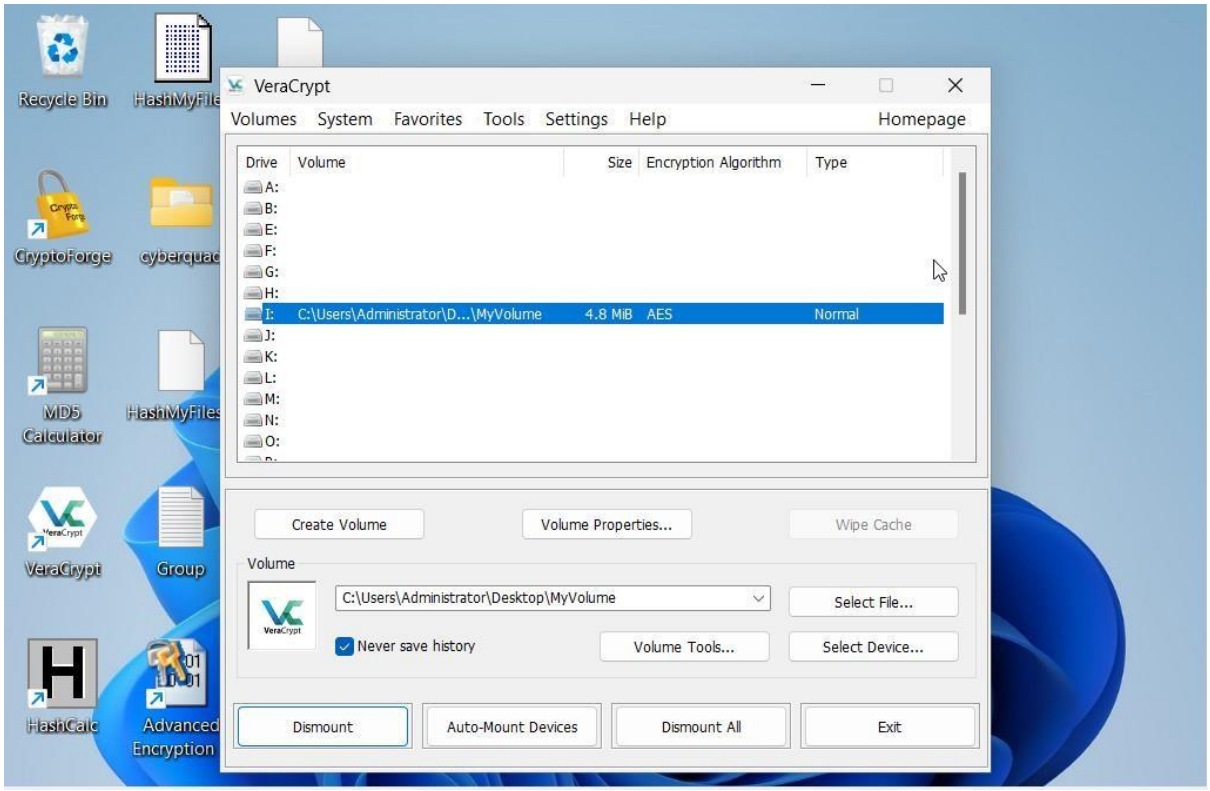


VeraCrypt will mount the volume in Drive I

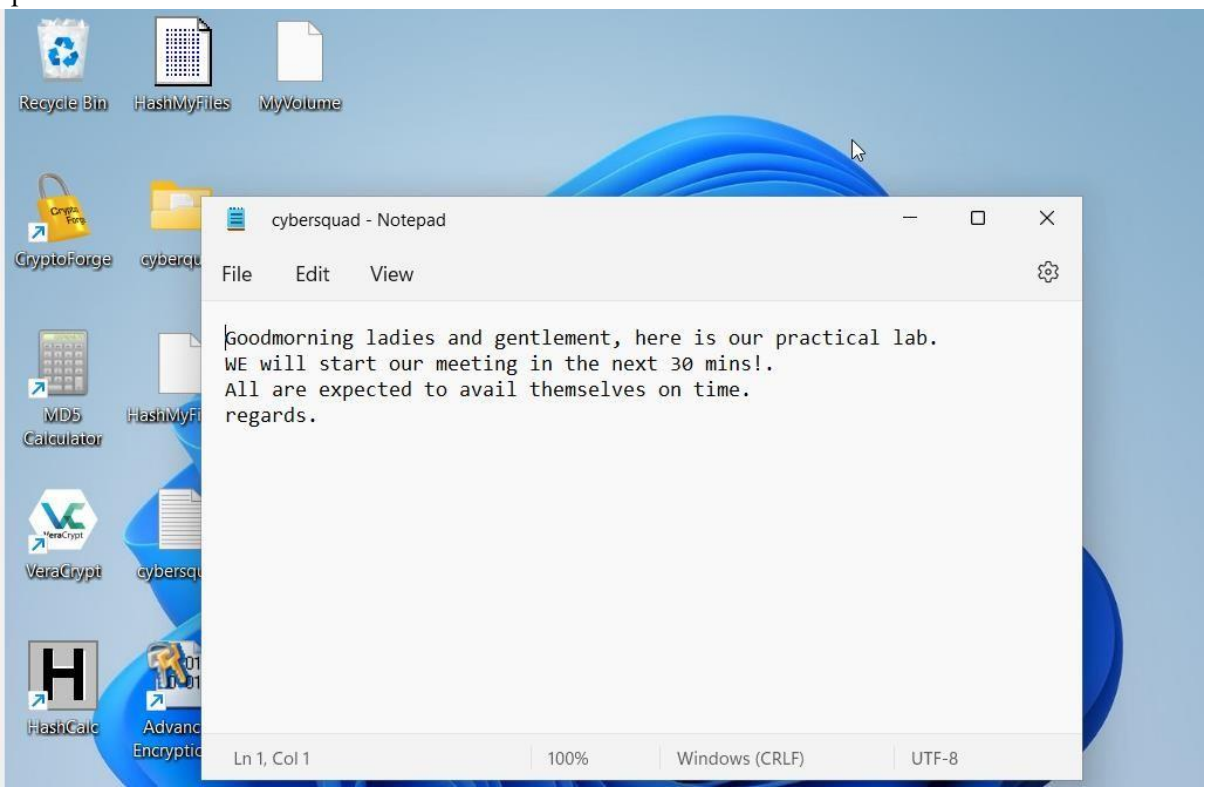
•



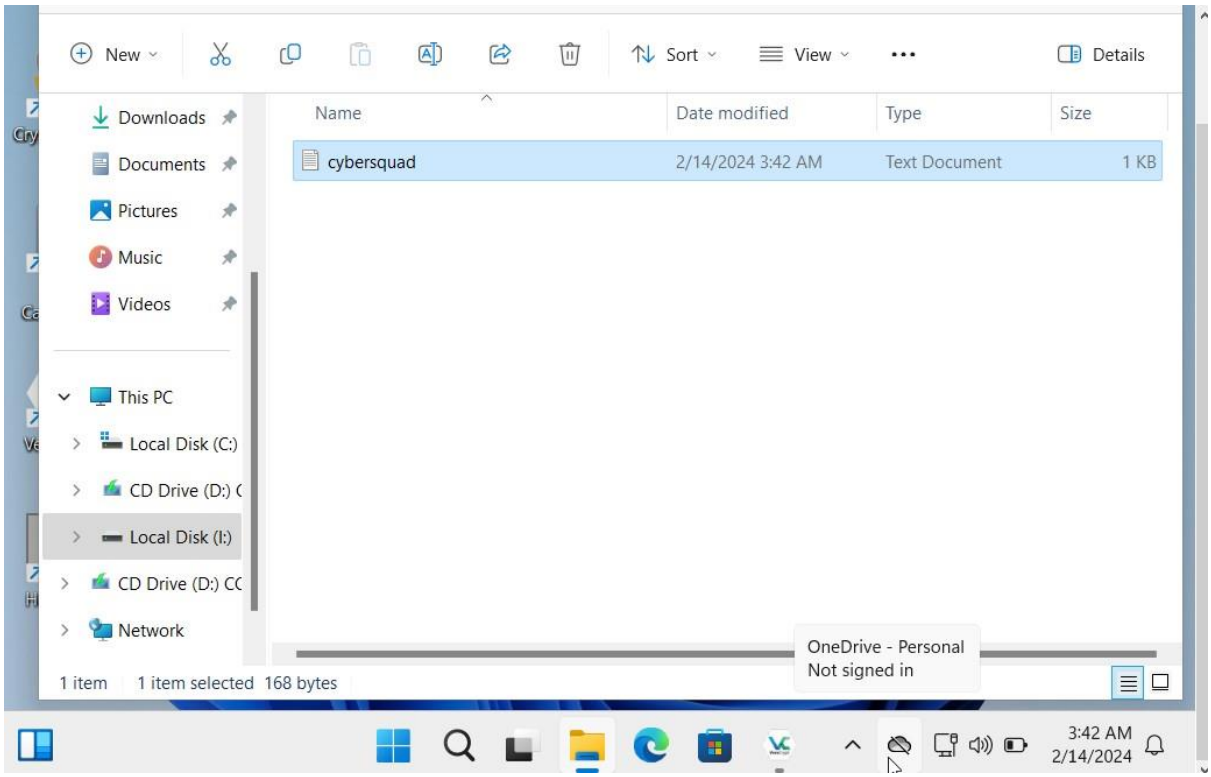
- MyVolume has been successfully mount as a virtual Disk I (entirely encrypted), and behave similarly to a real disk. You can copy or move files to this virtual disk for encryption.



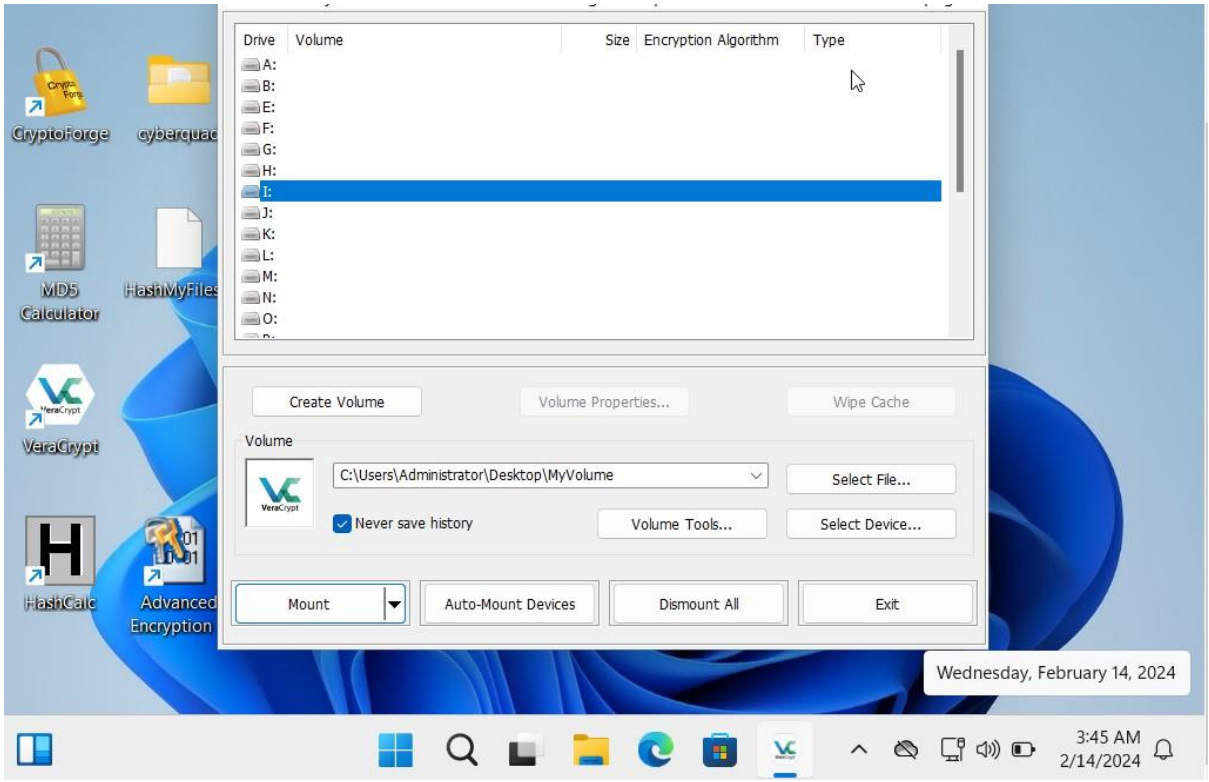
- Create a text file in the desktop and name it Cybersquad.
- Open the text file and insert text and save.



- Copy the file to the Desktop and paste to Local Disk and close the window.



Switch to the VeraCrypt window, click dismount and then click exit.

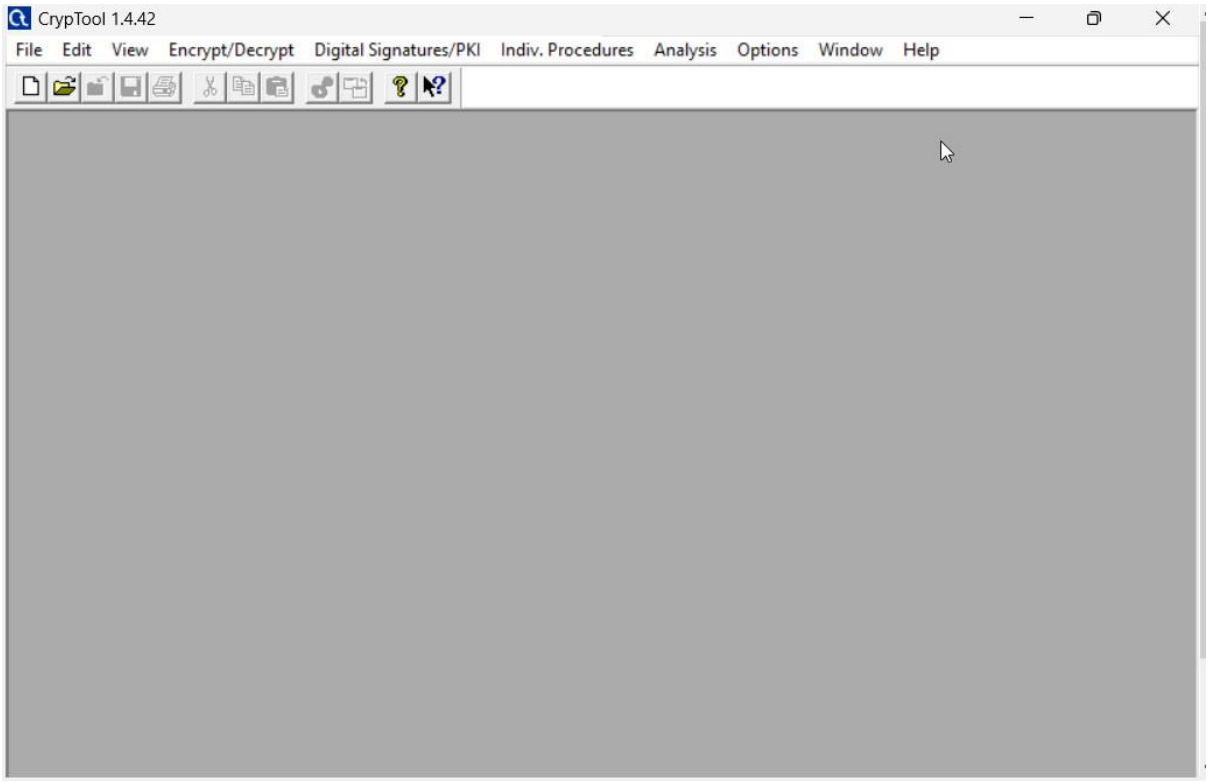


- The Drive I located in Disk C disappears.

Lab 5

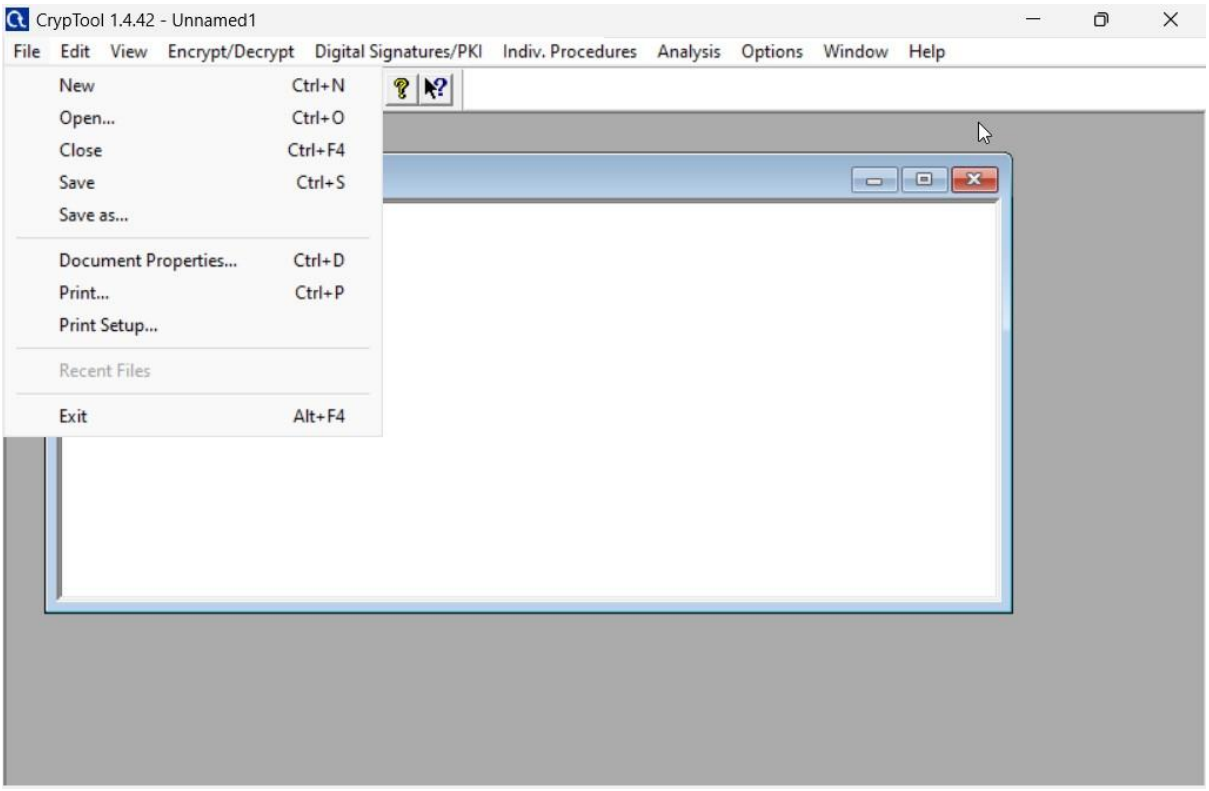
Task 2: Perform Crypto Analysis using CrypTool

- **Launching CrypTool**

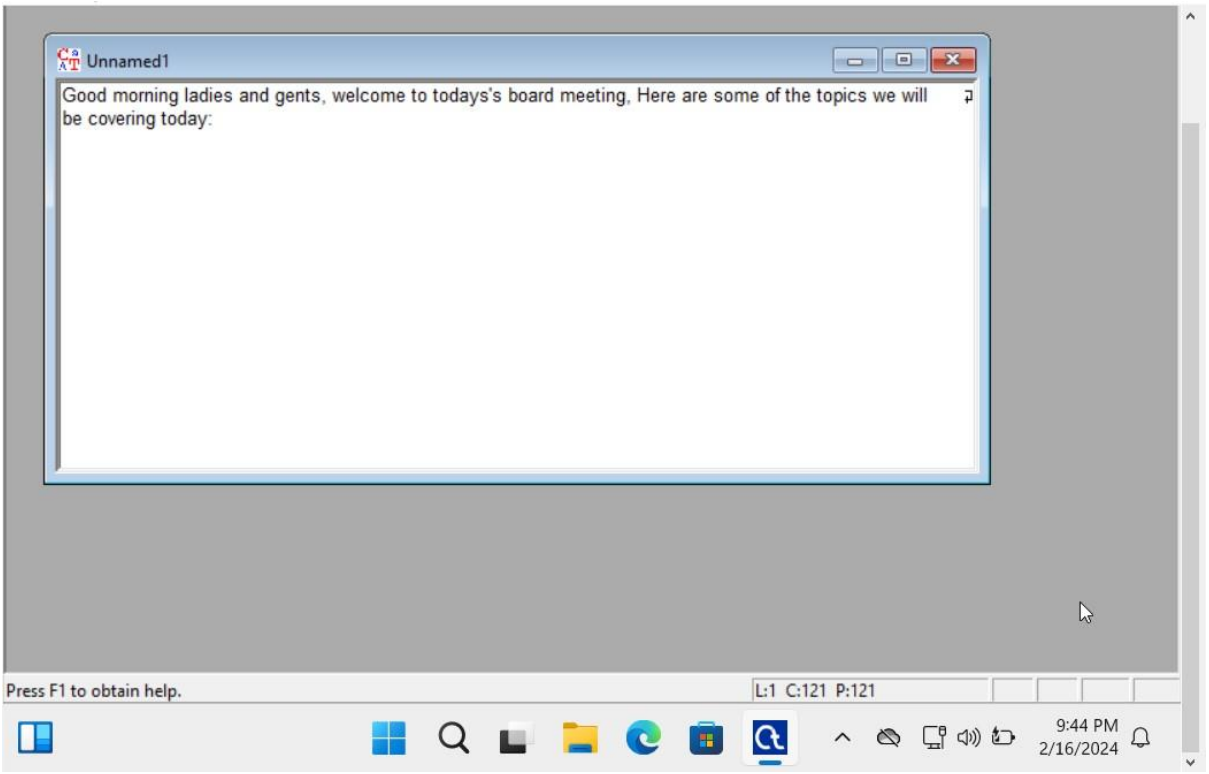


Click the file tab and select New to create encrypted data.

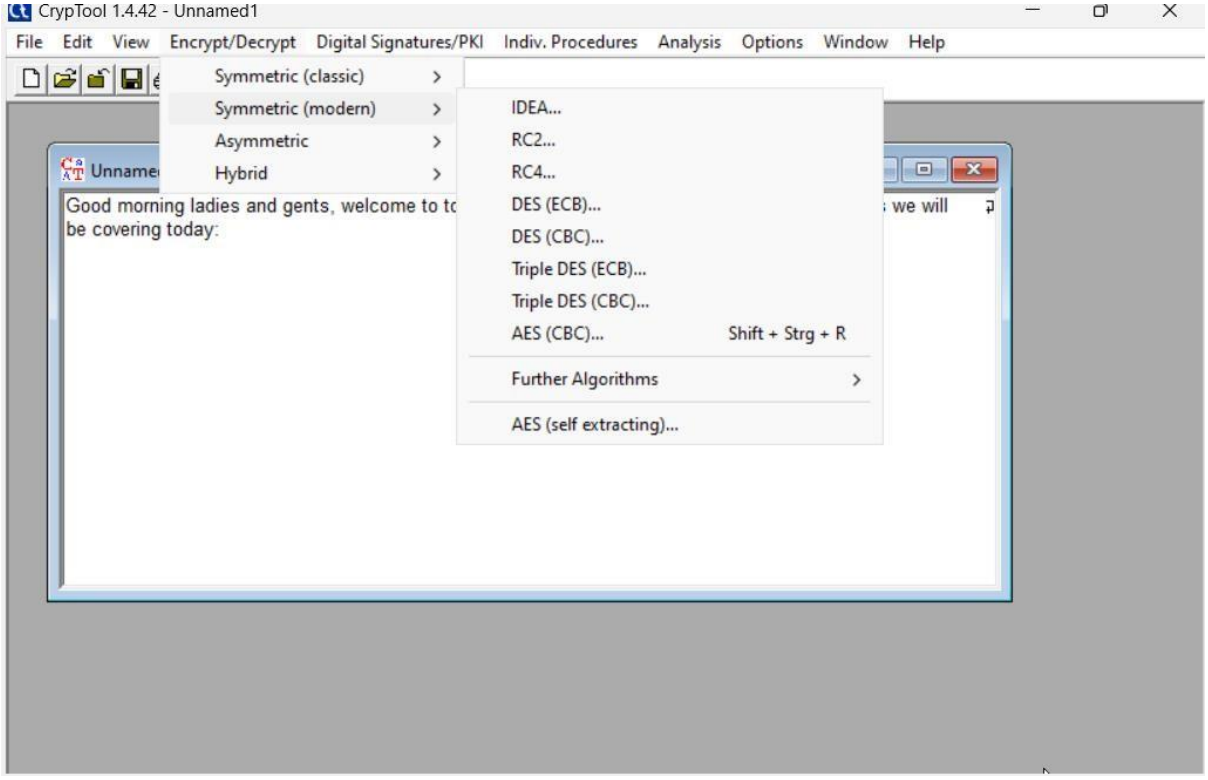
•



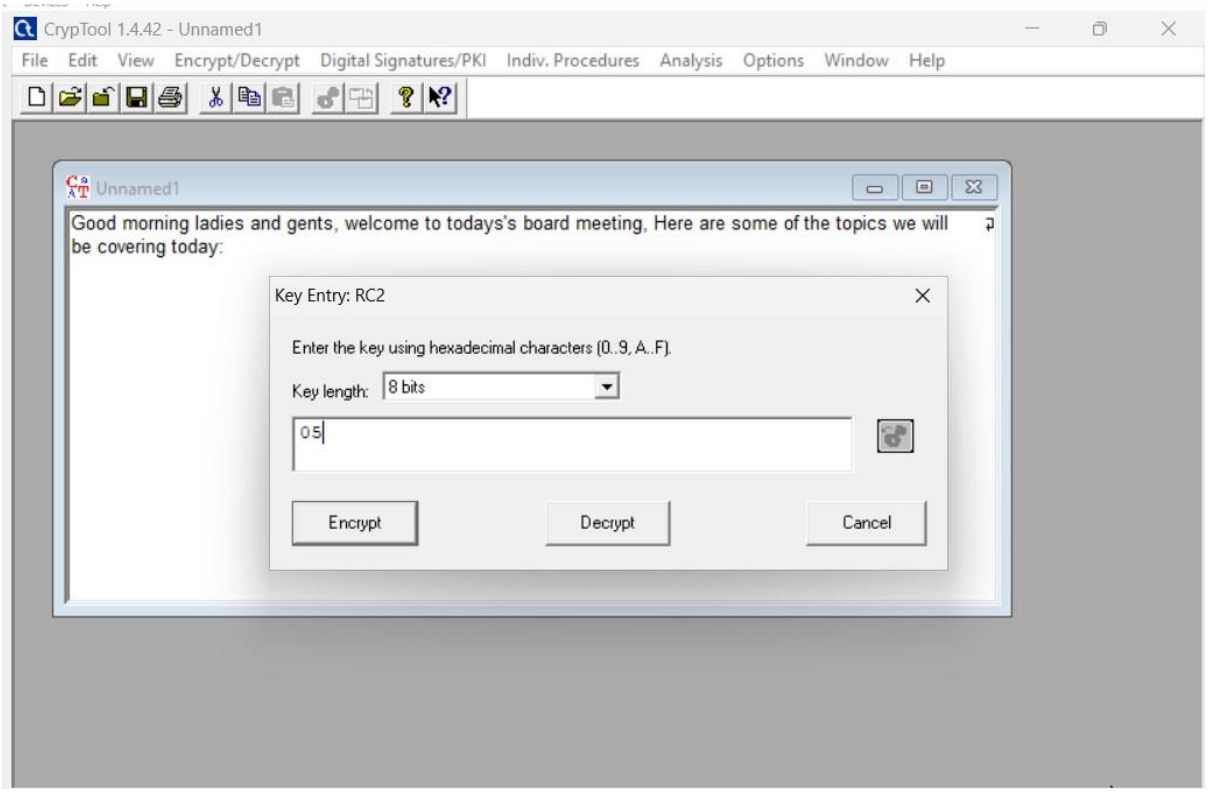
- **Insert some text into the file, you will be encrypting this content.**



- **From the menu bar, click Encrypt/decrypt and navigate to symmetric (modern), RC2.**

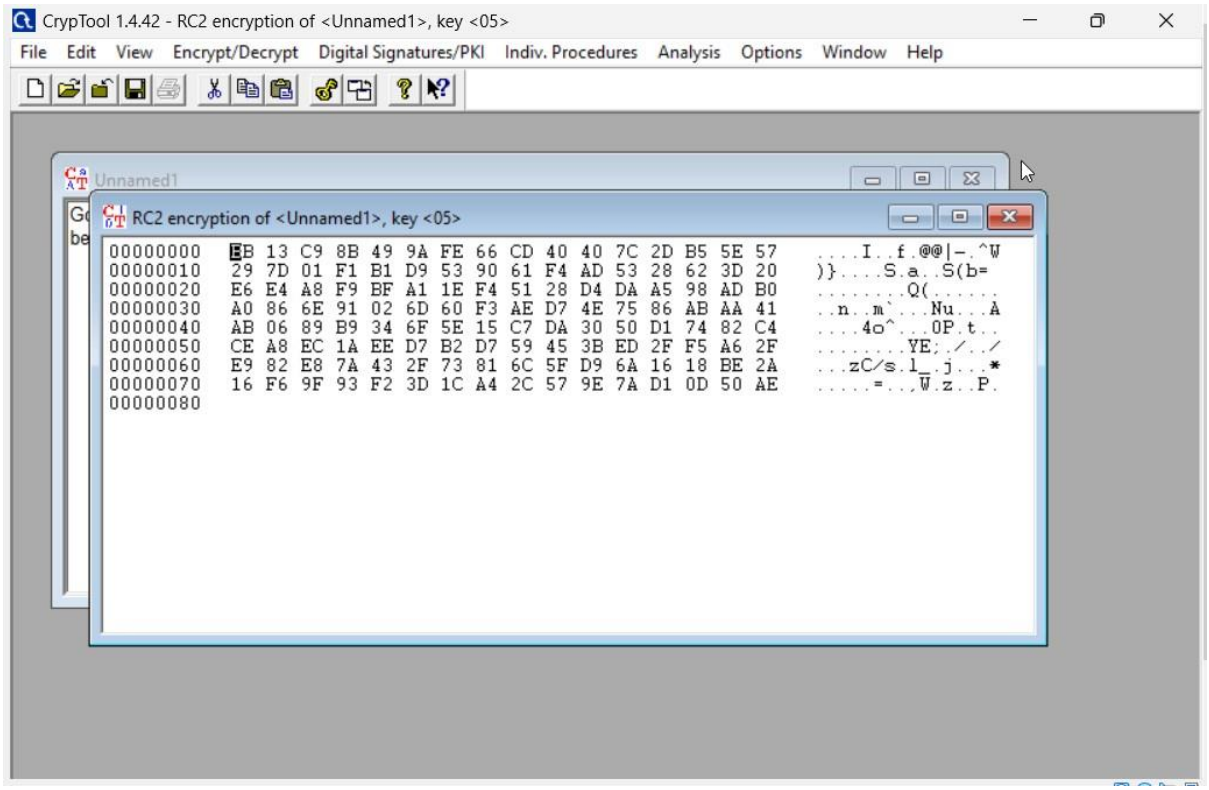


- **Keep the key length to default (8bits), then below the key length, enter 05 as hexadecimal characters and click encrypt.**

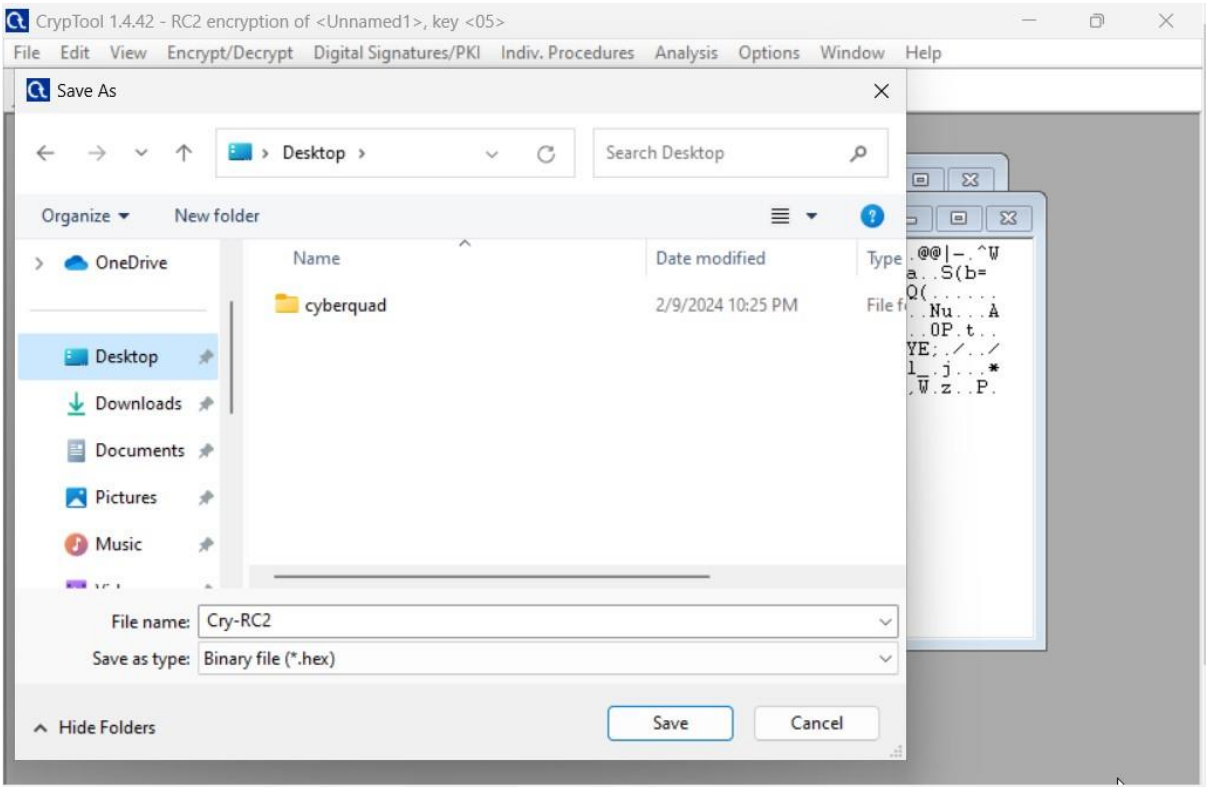


-

The output of the encrypted content appears.



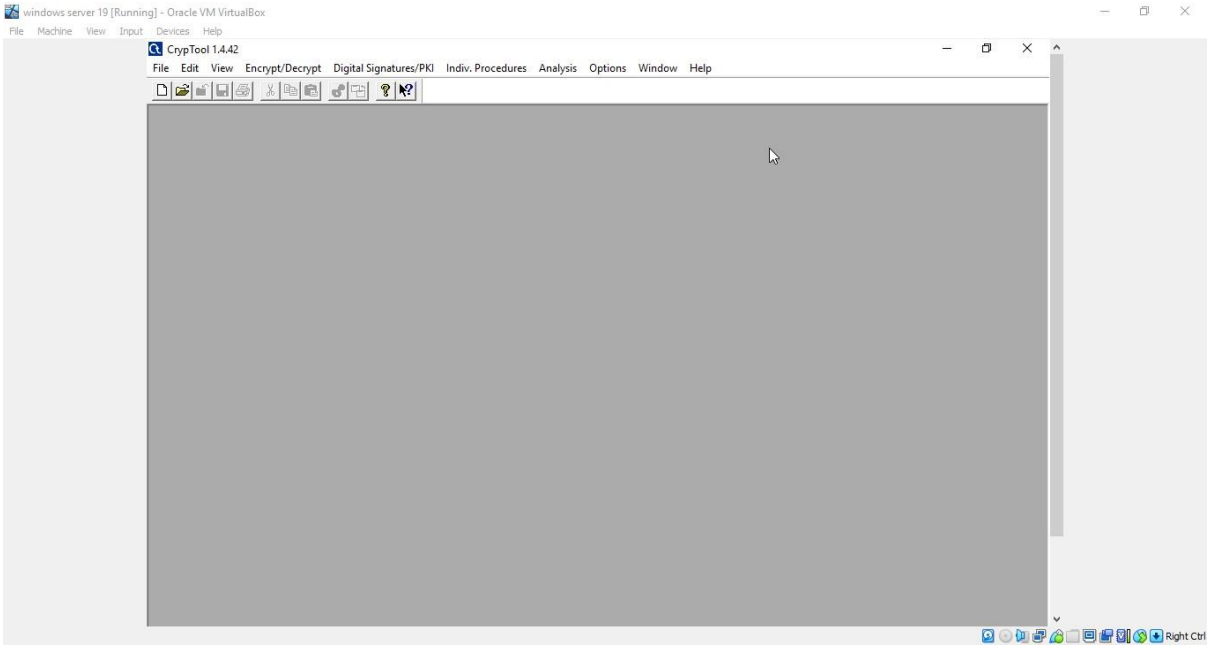
- **Save the cypher text by clicking file on the menu bar and click save.**



To share the file, copy the encrypted file (Cry-RC2) from Desktop.

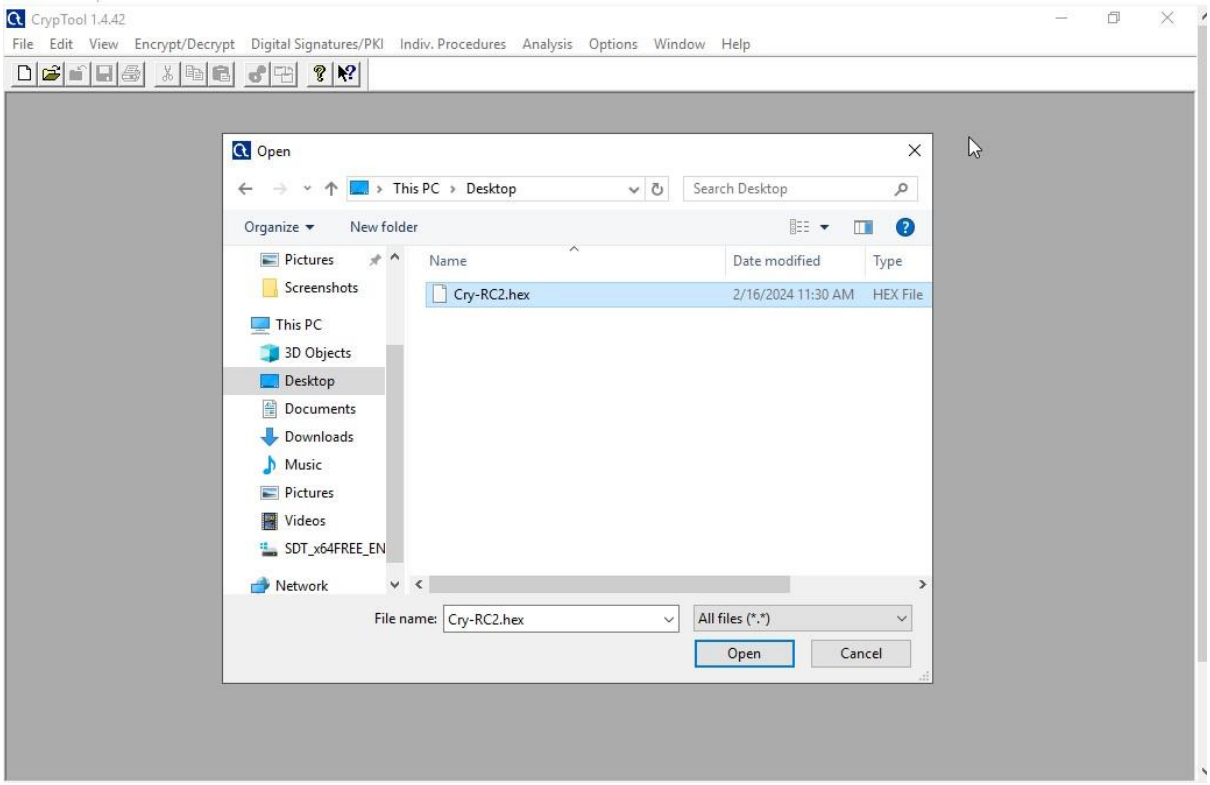
-

- **Switch to windows server 2019, navigate through the CrytpTool**

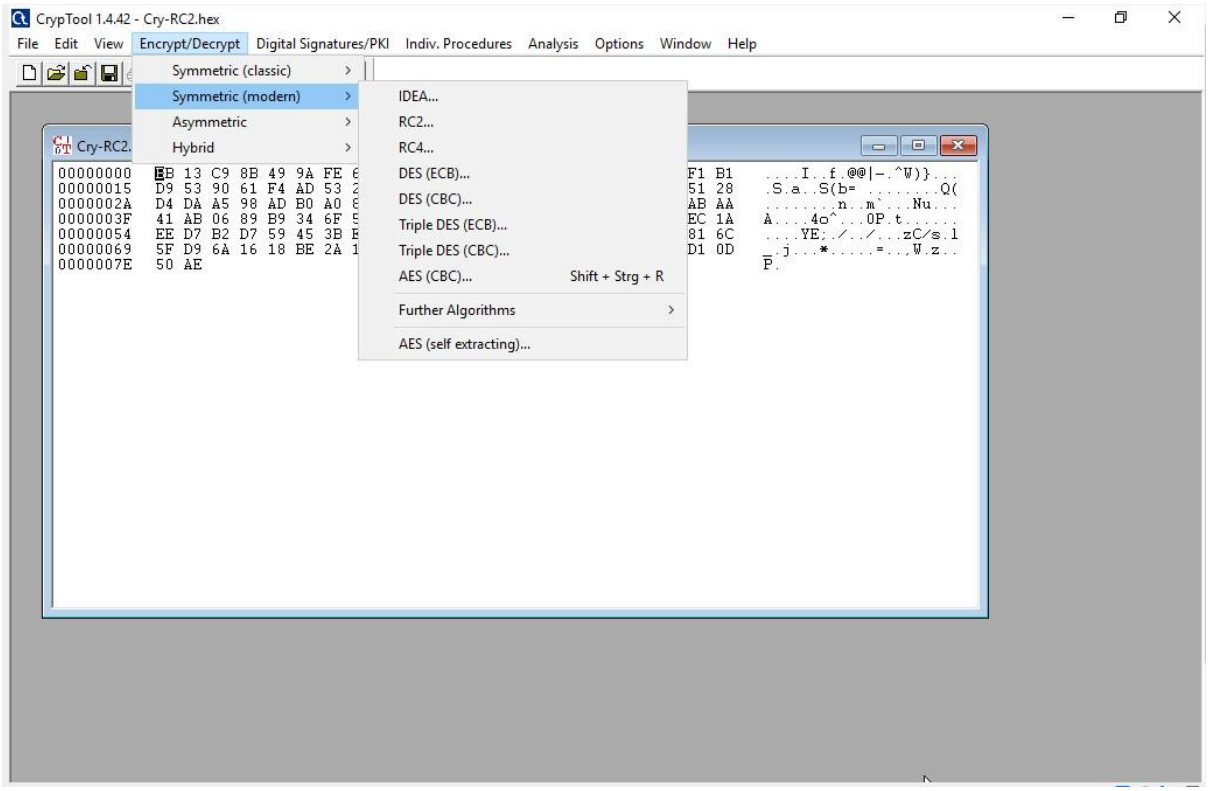


- **In the cryptool window, click file tab and select open**

- **Navigate to the file location of the encrypted file (Desktop) and click okay.**

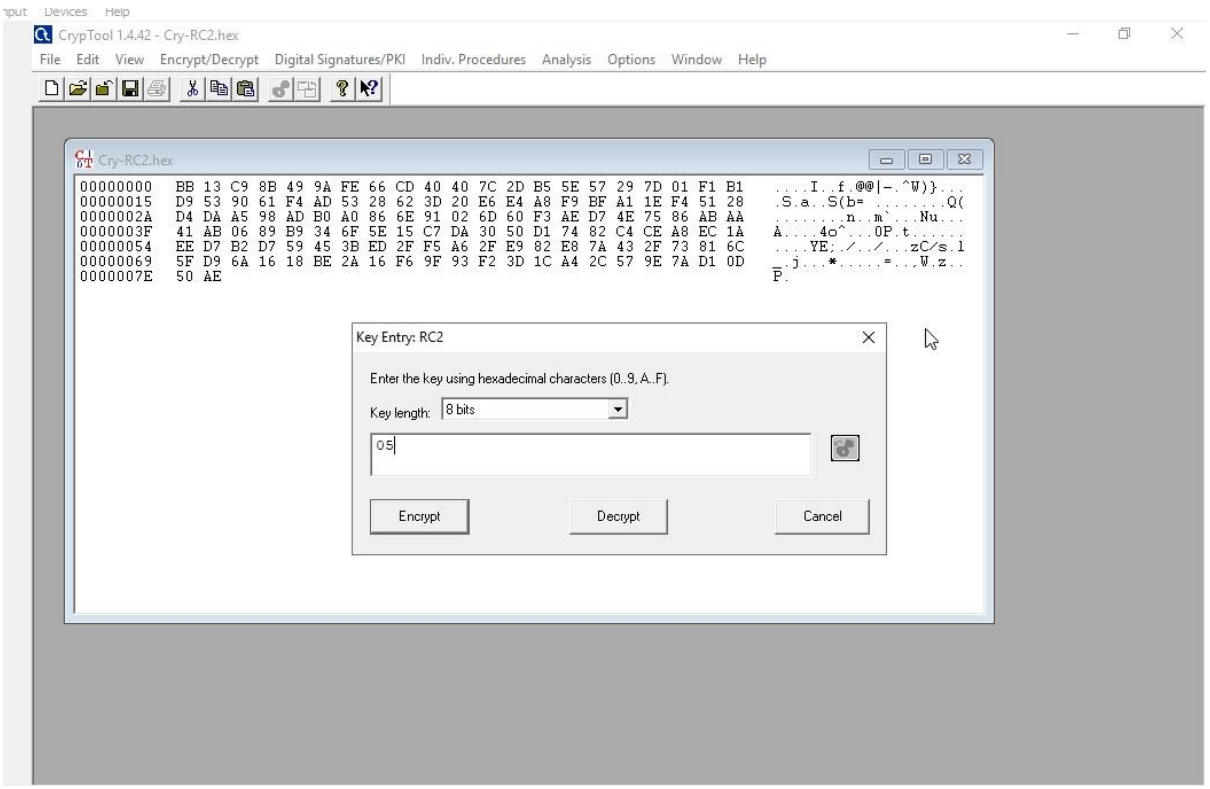


- **From the file bar select Encrypt/Decrypt and navigate to the symmetric(modern) RC2.**



The key entry:RC2 dialog box appears leave the key Lenth set do default, in the text field below, key Lenth enter04 as hexadecimal character and click decrypt.

-



The decrypted text appears