

Dom Moore  
OpenSSL / GnuPG

## Overview

Encryption is a key component of data security

### Problem Area:

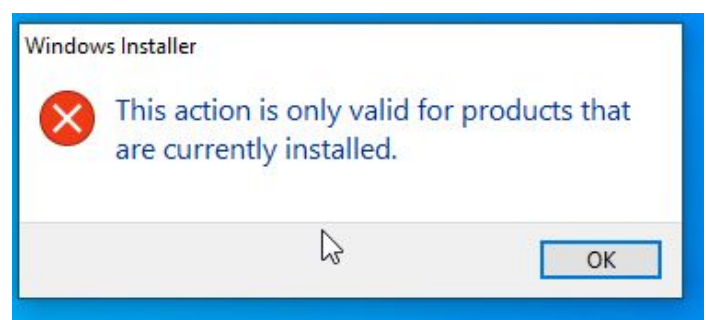
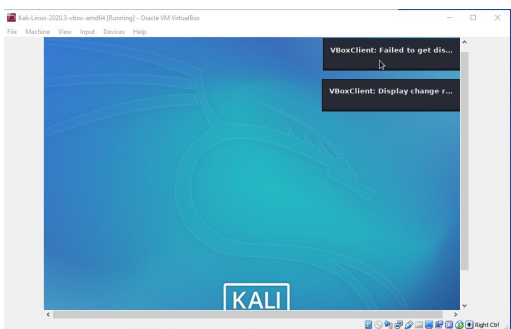
During the install of Docker, it required adjusting of the internal system of the pc and those adjustments affected the virtualization of the other programs within VirtualBox, and to begin this project I was not able to access the Windows 10 nor the Kali Linux virtual machines.

### Solution:

The solution required implementing several steps to be able to establish a connection with the virtual machines within VirtualBox.

- Step 1 - Uninstall Docker / Wsl package
- Step 2 - Navigate to windows features (Turn Windows features on / off)
- Step 3 - Toggle of Hyper- V and subsystems Linux
- Step 4 - Navigate to PowerShell( Administrator)
- Step 5 - Run PowerShell cmdlet bcdedit /set hypervisorlaunchtype off
- Step 6 - Restart PC

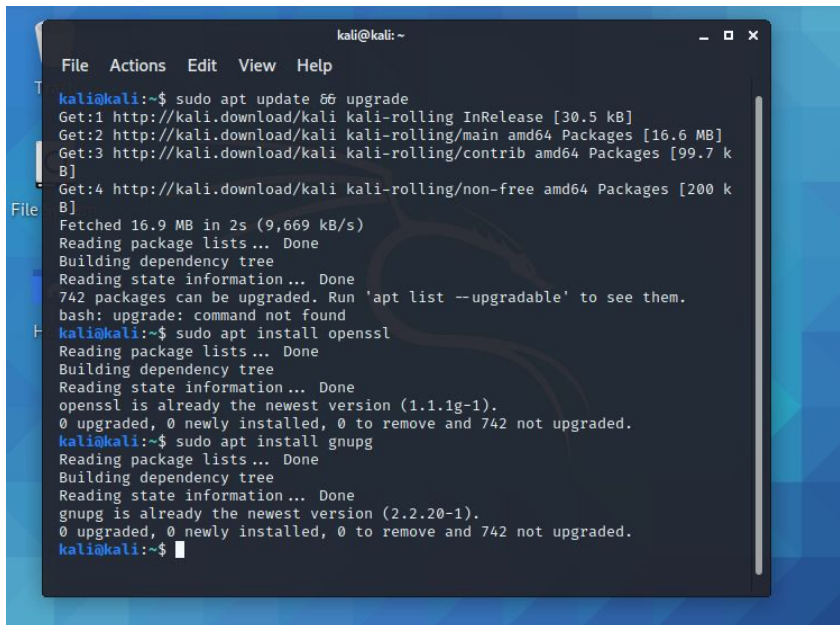
### Images of the virtual machine error



## Part 1: Staging Windows 10

- Install a Windows 10 VM on Virtualbox.
- Install 7-Zip on the new Windows 10 VM.
- Install GNU Privacy Guard on your Linux system.
- Install OpenSSL on your Linux system.

OpenSSL Install /GNUPG Install

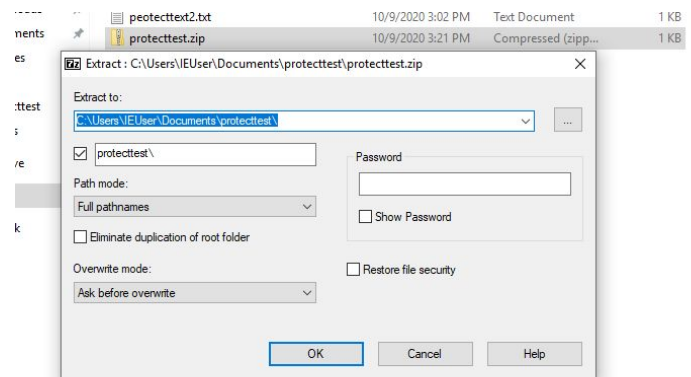
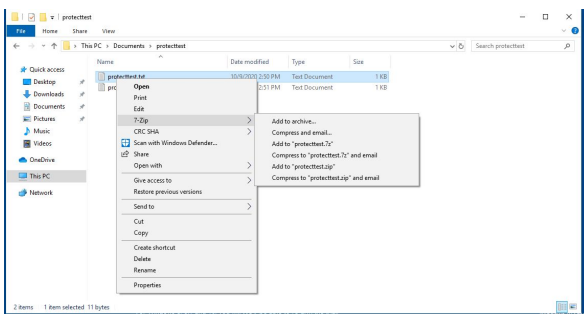
A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help) and a scrollbar on the right. The terminal output shows the following commands and their results:

```
kali@kali:~$ sudo apt update && upgrade
Get:1 http://kali.download/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [16.6 MB]
Get:3 http://kali.download/kali kali-rolling/contrib amd64 Packages [99.7 kB]
Get:4 http://kali.download/kali kali-rolling/non-free amd64 Packages [200 kB]
Fetched 16.9 MB in 2s (9,669 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
742 packages can be upgraded. Run 'apt list --upgradable' to see them.
bash: upgrade: command not found
kali@kali:~$ sudo apt install openssl
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssl is already the newest version (1.1.1g-1).
0 upgraded, 0 newly installed, 0 to remove and 742 not upgraded.
kali@kali:~$ sudo apt install gnupg
Reading package lists... Done
Building dependency tree
Reading state information... Done
gnupg is already the newest version (2.2.20-1).
0 upgraded, 0 newly installed, 0 to remove and 742 not upgraded.
kali@kali:~$
```

## Part 2: Data Encryption with 7-Zip in Windows

- Encrypt a single file with 7-Zip in the Windows GUI.
- Validate the encryption succeeded by decrypting and uncompressing the archive contents to your desktop.
- Document the steps are taken and include screenshots.
- use 7-Zip to obfuscate the contents of an archive.
- Encrypt a folder containing multiple files with 7-Zip in the Windows GUI. This time, encrypt the file names.
- Include screenshots of encrypted files in your submission. Explain the steps taken and what changed when you encrypted file names.

### Encrypt File

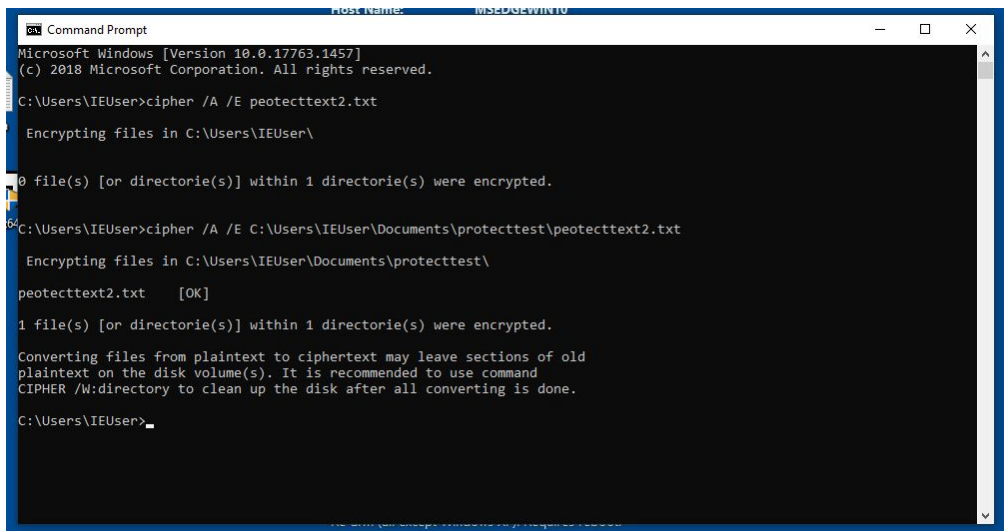


### To encrypted file:

- Step 1 - Navigate to file
- Step 2 - Right-click file wanting to encrypt
- Step 3 - Click add to the archive
- Step 4 - Select file format
- Step 5 - Select encrypt and set the password
- Step 7 - Save changes

## Part 3: Data Encryption with EFS in Windows

- Encrypt a single file using Powershell in Windows 10
- Decrypt the file using Powershell in Windows 10
- Encrypt a single file in Windows 10 CLI.
- Decrypt that same file in Windows 10 CLI.
- Include screenshots of encrypted files in your submission. Explain the steps taken.



```
Command Prompt
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>cipher /A /E peotecttext2.txt

Encrypting files in C:\Users\IEUser\

0 file(s) [or directorie(s)] within 1 directorie(s) were encrypted.

C:\Users\IEUser>cipher /A /E C:\Users\IEUser\Documents\protecttest\peotecttext2.txt

Encrypting files in C:\Users\IEUser\Documents\protecttest\
peotecttext2.txt [OK]

1 file(s) [or directorie(s)] within 1 directorie(s) were encrypted.

Converting files from plaintext to ciphertext may leave sections of old
plaintext on the disk volume(s). It is recommended to use command
CIPHER /W:directory to clean up the disk after all converting is done.

C:\Users\IEUser>
```

## Part 4: Secret Messages with Powershell Hash Generation

- Use Powershell to generate the hash value of a short sentence in SHA256 algorithm.
- Post your hash value to Slack class channel for others to decrypt. Something like “My secret message:  
64EC88CA00B268E5BA1A35678A1B5316D212F4F366B2477232534A8AECA37F3C”  
will do!
- Once a classmate has posted a hash value, decrypt it and add it to your submission alongside the original hash value.

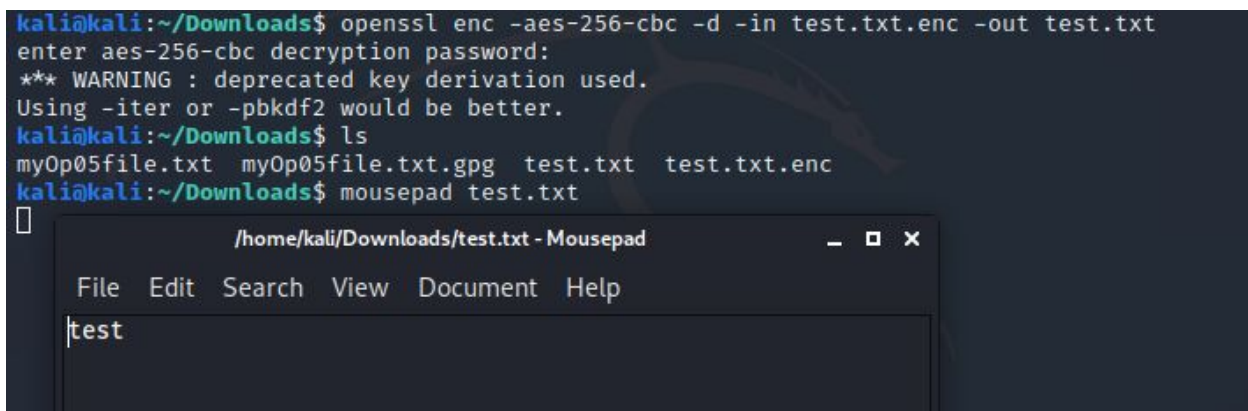
```
PS C:\Users\IEUser\Documents> Get-FileHash Op05File.txt | Format-List

Algorithm : SHA256
Hash      : 0F97C43923C3F939EA2EE2183E704F2D21D87E46441CDE33CC64ABFC329096D3
Path      : C:\Users\IEUser\Documents\Op05File.txt
```

## Part 5: Hash Validation

- Use Powershell to generate the hash value of a small file
- Share the file with a, along with the hash value.
- Have your teammate generate the hash value of the downloaded file and compare it to the value you provided.

```
kali@kali:~/Downloads$ openssl enc -aes-256-cbc -d -in test.txt.enc -out test.txt
enter aes-256-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
kali@kali:~/Downloads$ ls
myOp05file.txt  myOp05file.txt.gpg  test.txt  test.txt.enc
kali@kali:~/Downloads$ mousepad test.txt
```



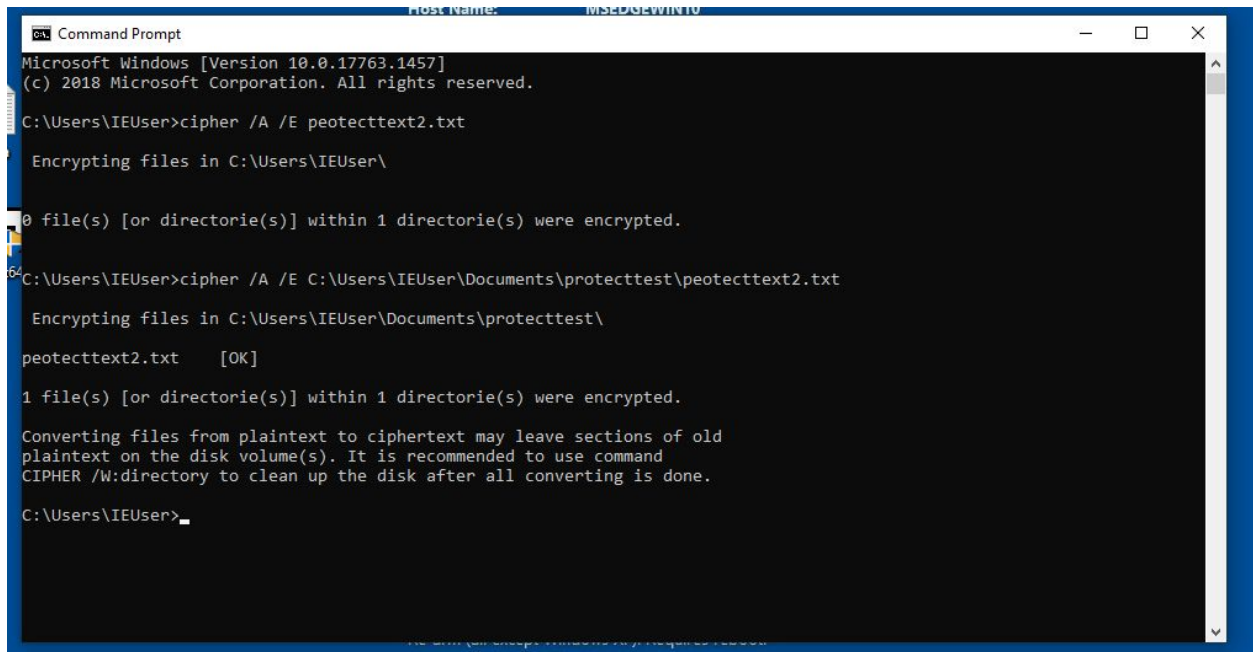
The screenshot shows a terminal window with the following commands and output:

```
kali@kali:~/Downloads$ openssl enc -aes-256-cbc -d -in test.txt.enc -out test.txt
enter aes-256-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
kali@kali:~/Downloads$ ls
myOp05file.txt  myOp05file.txt.gpg  test.txt  test.txt.enc
kali@kali:~/Downloads$ mousepad test.txt
```

Below the terminal, a window titled "/home/kali/Downloads/test.txt - Mousepad" is open. It has a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". The text area contains the word "test".

## Part 6: Data File Encryption with GNU Privacy Guard (GnuPG) in Linux

- Generate a key.
- Compose a .txt file in Linux and write a short sentence
- Encrypt the .txt file with GnuPG.
- When you have received the GPG-encrypted file, decrypt it.



```
Command Prompt
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>cipher /A /E peotecttext2.txt

Encrypting files in C:\Users\IEUser\

0 file(s) [or directorie(s)] within 1 directorie(s) were encrypted.

C:\Users\IEUser>cipher /A /E C:\Users\IEUser\Documents\protecttest\peotecttext2.txt

Encrypting files in C:\Users\IEUser\Documents\protecttest\
peotecttext2.txt [OK]

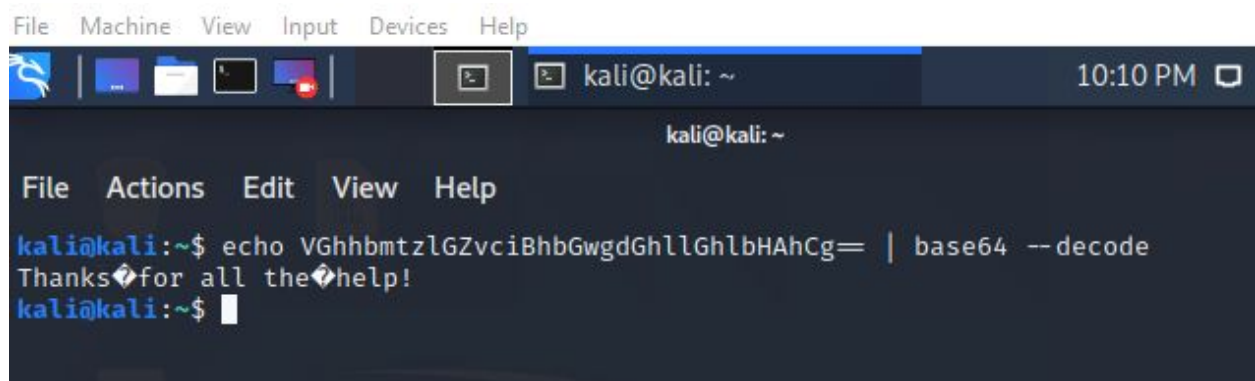
1 file(s) [or directorie(s)] within 1 directorie(s) were encrypted.

Converting files from plaintext to ciphertext may leave sections of old
plaintext on the disk volume(s). It is recommended to use command
CIPHER /W:directory to clean up the disk after all converting is done.

C:\Users\IEUser>
```

## Part 7: Data File Encryption and Secret Messages with OpenSSL in Linux

- Compose a .txt file in Linux and write a short sentence in it
- Encrypt the .txt file with OpenSSL.
- Contact a teammate and ask them if it's OK to send an OpenSSL-encrypted file over. Transmit once they've responded.
- When you have received the OpenSSL-encrypted file from your classmate, decrypt it.
- Use OpenSSL to generate base64 ciphertext from a cleartext string sentence.
- Post your ciphertext to the Slack class channel for others to decrypt. Don't indicate this is Part 7; keep your classmates guessing!
- Once a classmate has posted a base64 ciphertext string, decrypt it and add it to your submission alongside the original hash value.

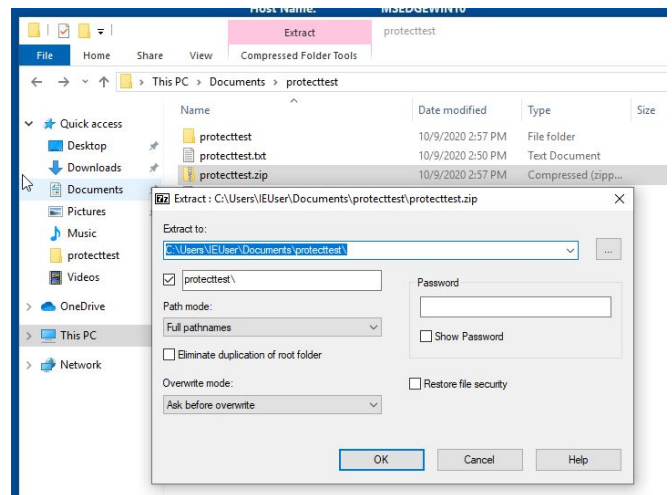
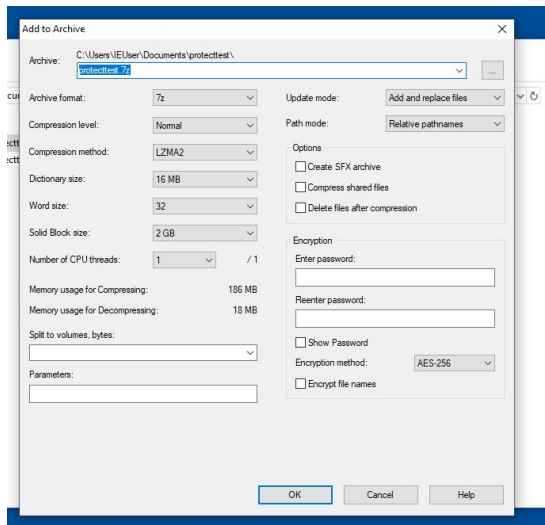


The image shows a terminal window from a Kali Linux machine. The window has a title bar with 'File', 'Machine', 'View', 'Input', 'Devices', and 'Help' menus. Below the title bar is a taskbar with several icons. The terminal itself has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is 'kali@kali: ~'. The command being executed is 'echo VGhhbmtzlgZvciBhbGwgdGhllGh1bHAhCg== | base64 --decode'. The output of the command is 'Thanks for all the help!'. The prompt is now 'kali@kali:~\$'.

```
File Machine View Input Devices Help
kali@kali: ~ 10:10 PM
kali@kali: ~
File Actions Edit View Help
kali@kali:~$ echo VGhhbmtzlgZvciBhbGwgdGhllGh1bHAhCg== | base64 --decode
Thanks for all the help!
kali@kali:~$
```



## Images Continued



```
C:\Users\IEUser>cipher /D C:\Users\IEUser\Documents\protecttest\protecttest2.txt  
Decrypting files in C:\Users\IEUser\Documents\protecttest\  
protecttest2.txt [OK]  
1 file(s) [or directorie(s)] within 1 directorie(s) were decrypted.  
C:\Users\IEUser>
```

```
kali@kali:~/Downloads$ openssl enc -aes-256-cbc -d -in test.txt.enc -out test.txt  
enter aes-256-cbc decryption password:  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
kali@kali:~/Downloads$ ls  
myOp05file.txt myOp05file.txt.gpg test.txt test.txt.enc  
kali@kali:~/Downloads$ mousepad test.txt
```

