LAB 10: Install Deep Freeze

Faronics Deep Freeze helps eliminate computer damage and downtime by making computer configurations indestructible. Once Deep Freeze is installed on a computer, any changes made to the computer—regardless of whether they are accidental or malicious—are never permanent. Deep Freeze provides immediate immunity from many of the problems that plague computers today—inevitable configuration drift, accidental system misconfiguration, malicious software activity, and incidental system degradation\

System Requirements:

Deep Freeze is supported on:

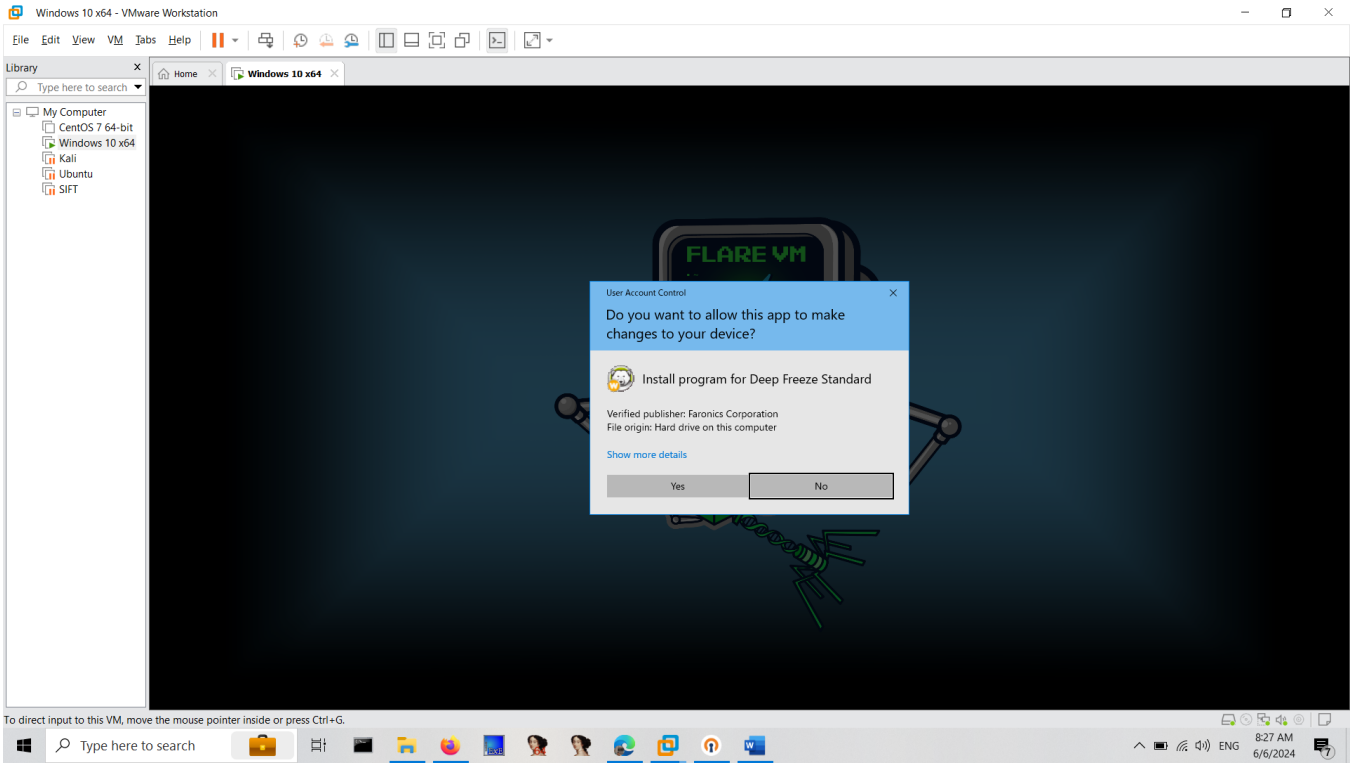
- Windows 7 (32 and 64-bit)
- Windows 8.1 (32 and 64-bit)
- Windows 10 up to version 22H2 (32 and 64-bit)
- Windows 11 up to version 23H2 (64-bit)

Deep Freeze requires 10% free hard drive space. The hardware requirements are the same as the recommended hardware requirements for the host operating system.

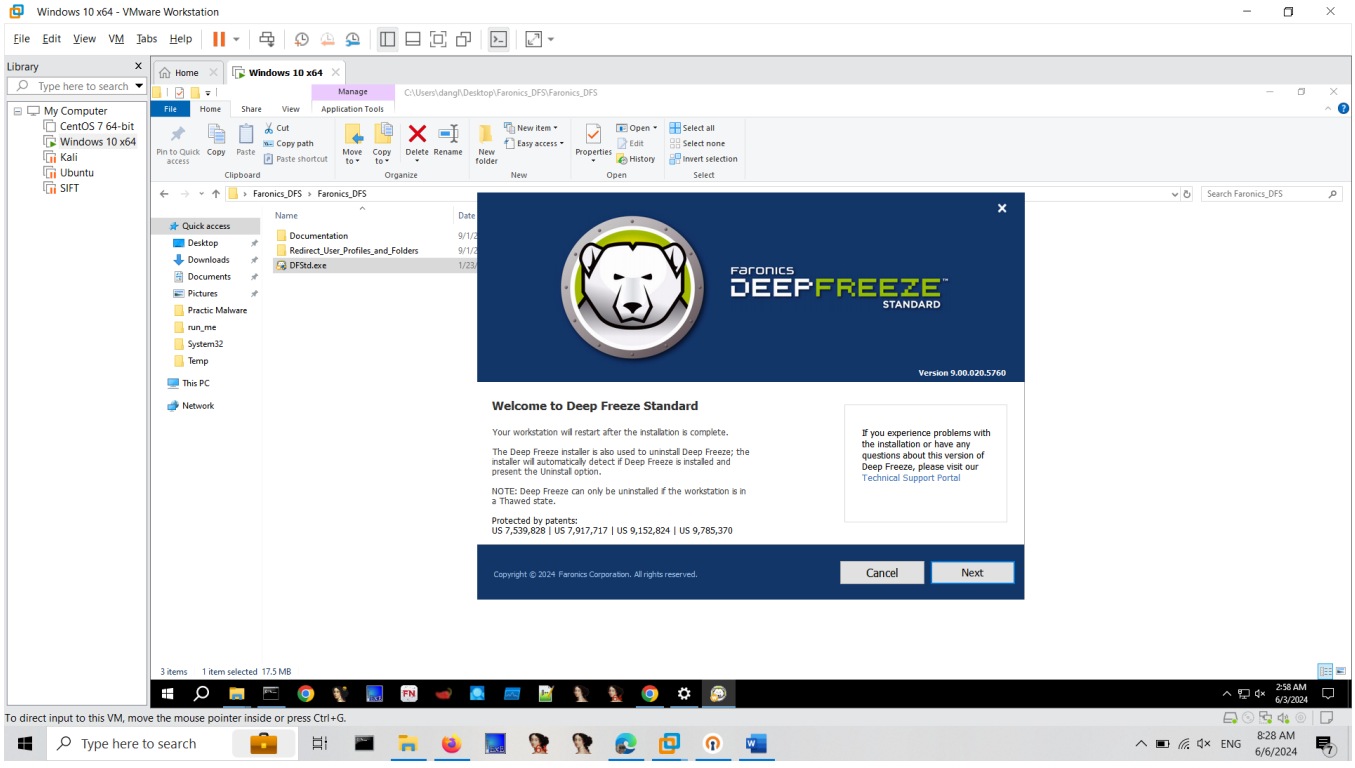
In this LAB lesson, we will install Deep Freeze on Windows 10. We go to the following link to download:

https://www.faronics.com/en-uk/downloads_en-uk/download-files_en-uk?product=DFS&CC=DDE0000&verify=WbYPor6FjX3YbXT21RKmVXmfx&DLCode=

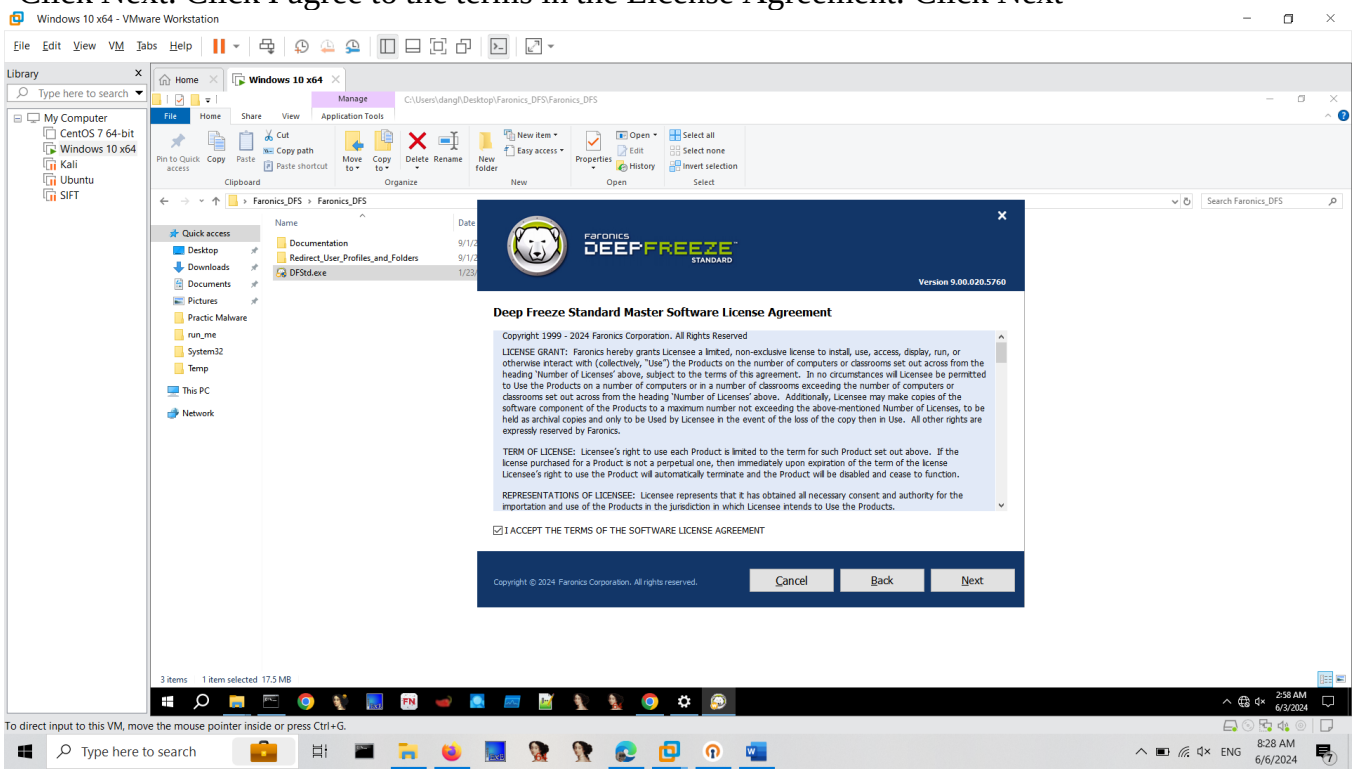
1. Double-click DFStd.exe to begin the installation process. The following screen appears:


Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
CentOS 7 64-bit
Windows 10 x64
Kali
Ubuntu
SIFT
Home
Windows 10 x64
FLARE VM
User Account Control
Do you want to allow this app to make changes to your device?
Install program for Deep Freeze Standard
Verified publisher: Faronics Corporation
File origin: Hard drive on this computer
Show more details
Yes
No
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
8:27 AM
6/6/2024

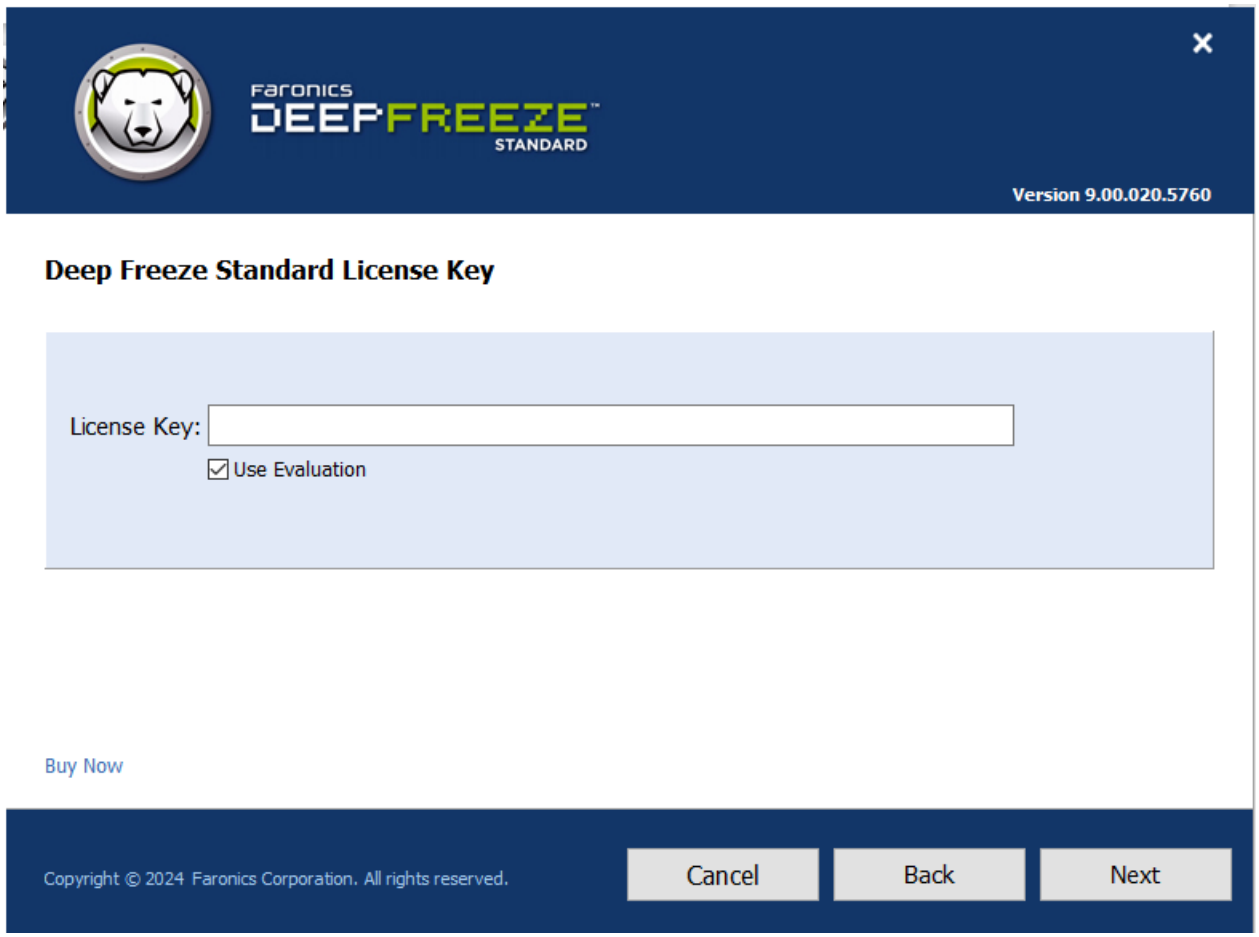
Click Yes


Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
CentOS 7 64-bit
Windows 10 x64
Kali
Ubuntu
SIFT
Home
Windows 10 x64
Faronics_DFS
Documentation
Redirect_User_Profiles_and_Folders
DFStd.exe
Faronics DEEP FREEZE STANDARD
Version 9.00.020.5760
Welcome to Deep Freeze Standard
Your workstation will restart after the installation is complete.
The Deep Freeze installer is also used to uninstall Deep Freeze; the installer will automatically detect if Deep Freeze is installed and present the Uninstall option.
NOTE: Deep Freeze can only be uninstalled if the workstation is in a Thawed state.
Protected by patents:
US 7,539,828 | US 7,917,717 | US 9,152,824 | US 9,785,370
If you experience problems with the installation or have any questions about this version of Deep Freeze, please visit our Technical Support Portal
Copyright © 2024 Faronics Corporation. All rights reserved.
Cancel
Next
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
8:28 AM
6/6/2024

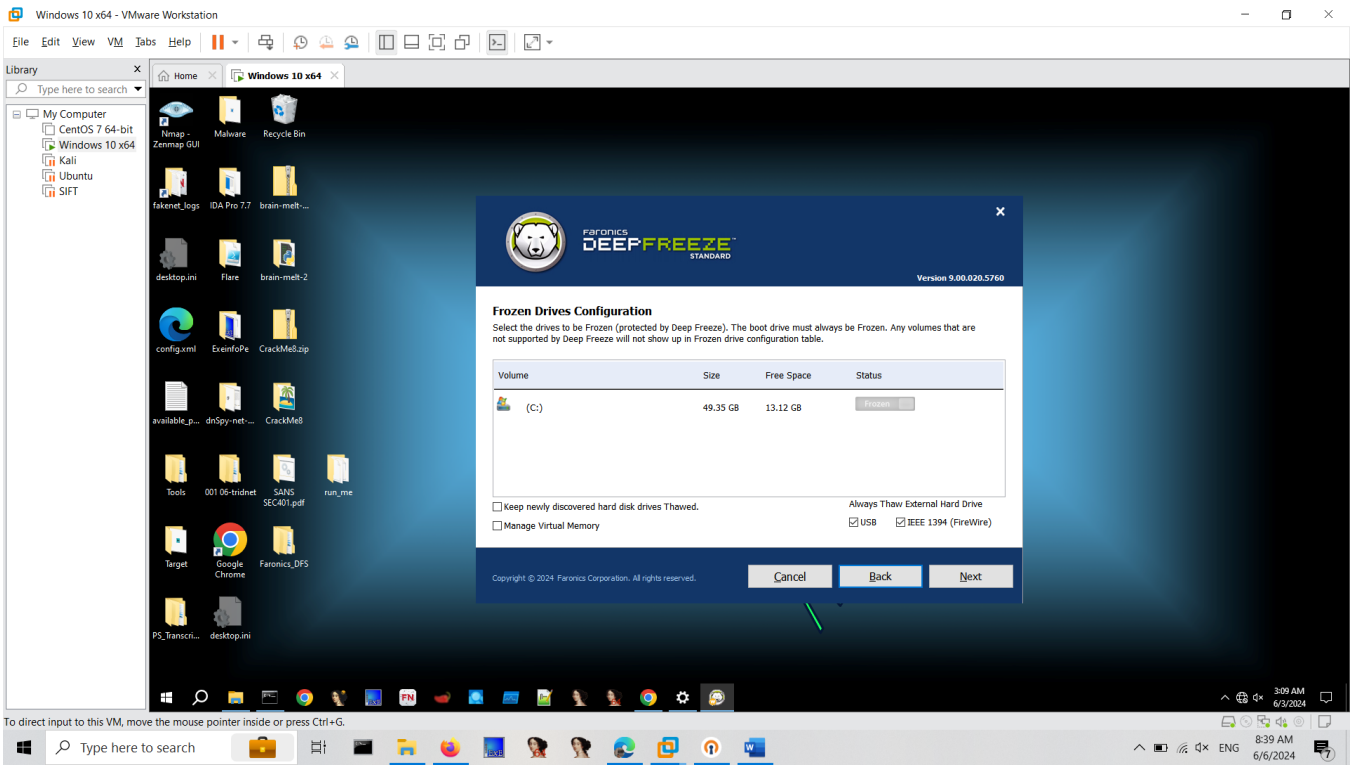
Click Next. Click I agree to the terms in the License Agreement. Click Next



Enter the License Key or select the Use Evaluation checkbox to install Deep Freeze in Evaluation mode. The Evaluation period ends 30 days after installation. Contact Faronics to purchase a License Key. Click Next



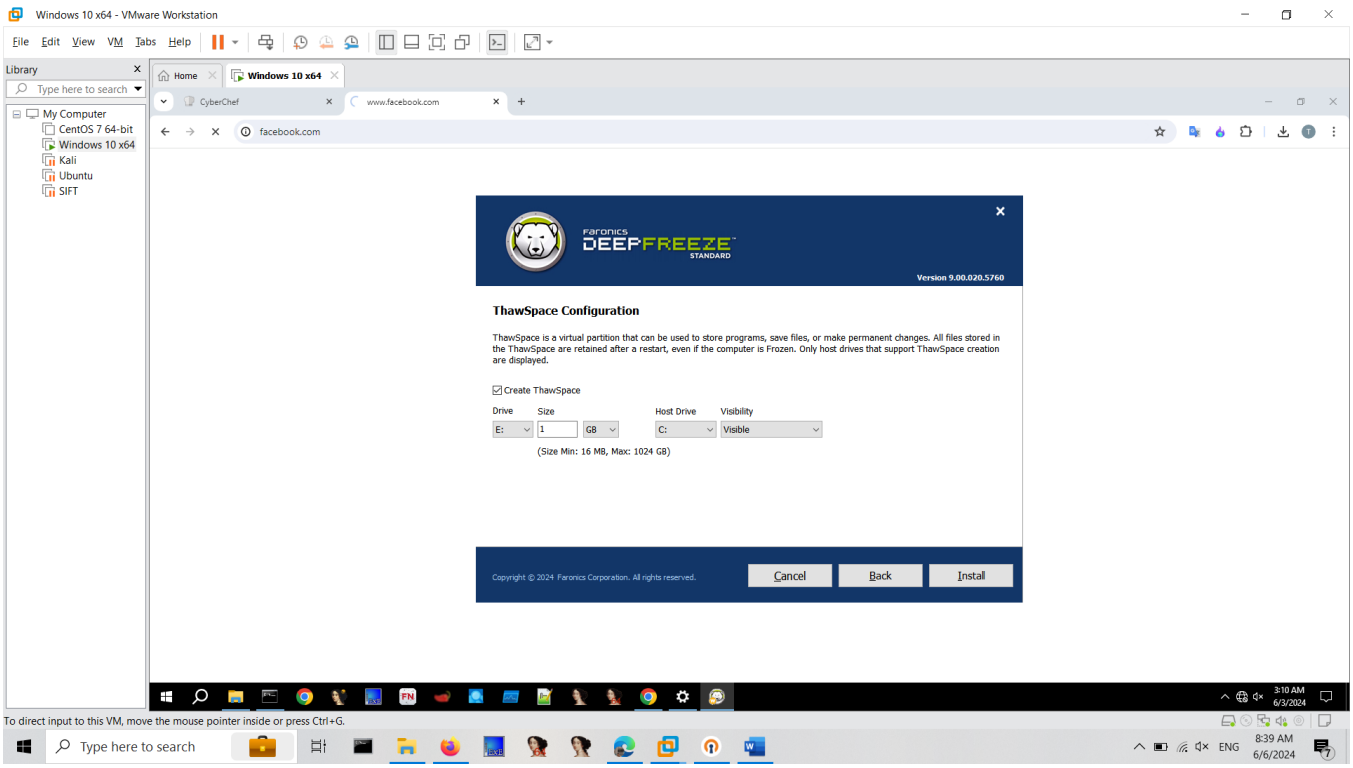
Choose the drives to Freeze from the displayed list. Click Next



> Keep newly discovered hard disk drives Thawed — select this option if you want to keep the newly discovered hard disk drives in a Thawed state. Changes made on the newly discovered hard disk drives will be retained.

> Always Thaw External Hard Drives — this option has two checkboxes, USB and IEEE 1394 (FireWire) and both checkboxes are selected by default. This ensures that the USB or IEEE 1394 (FireWire) hard drives are always Thawed. If the USB and/or IEEE 1394 (FireWire) external hard drives checkboxes are cleared, the drive is Frozen or Thawed according to the letter each drive mounts to in the Frozen Drives screen. Network drives and removable media drives (floppy, memory keys, CD-RW, etc.) are not affected by Deep Freeze and therefore cannot be Frozen

ThawSpace is a virtual partition that can be used to store programs, save files, or make permanent changes. All files stored in the ThawSpace are retained after a restart, even



if the computer is Frozen. A ThawSpace can be created on a drive that is configured to be Frozen or Thawed. Select the Create ThawSpace checkbox.

To create a ThawSpace or multiple ThawSpaces, complete the following steps:

• Select the Drive Letter. The next available letter is automatically used if the selected drive letter already exists on a computer when Deep Freeze is installed.

> The Drive Letter cannot be same as the Host Drive.

• Enter the Size. This is the size of the ThawSpace. The maximum size is 1024 GB and the minimum size is 16 MB.

> If you select the Size less than 16 MB, the ThawSpace is set to 16 MB.

> If you select the Size more than 1024 GB (1 TB), the ThawSpace is set to 1024GB (1 TB).

• Select the ThawSpace storage unit in MB or GB.

• Select the Host Drive.

> The Host Drive is the drive where the ThawSpace is created.

> The storage required for the ThawSpace is used from the total storage available on the Host Drive.

• Select Visible or Hidden from the Visibility drop-down.

> If you select Visible, the drive will be visible in Windows Explorer.

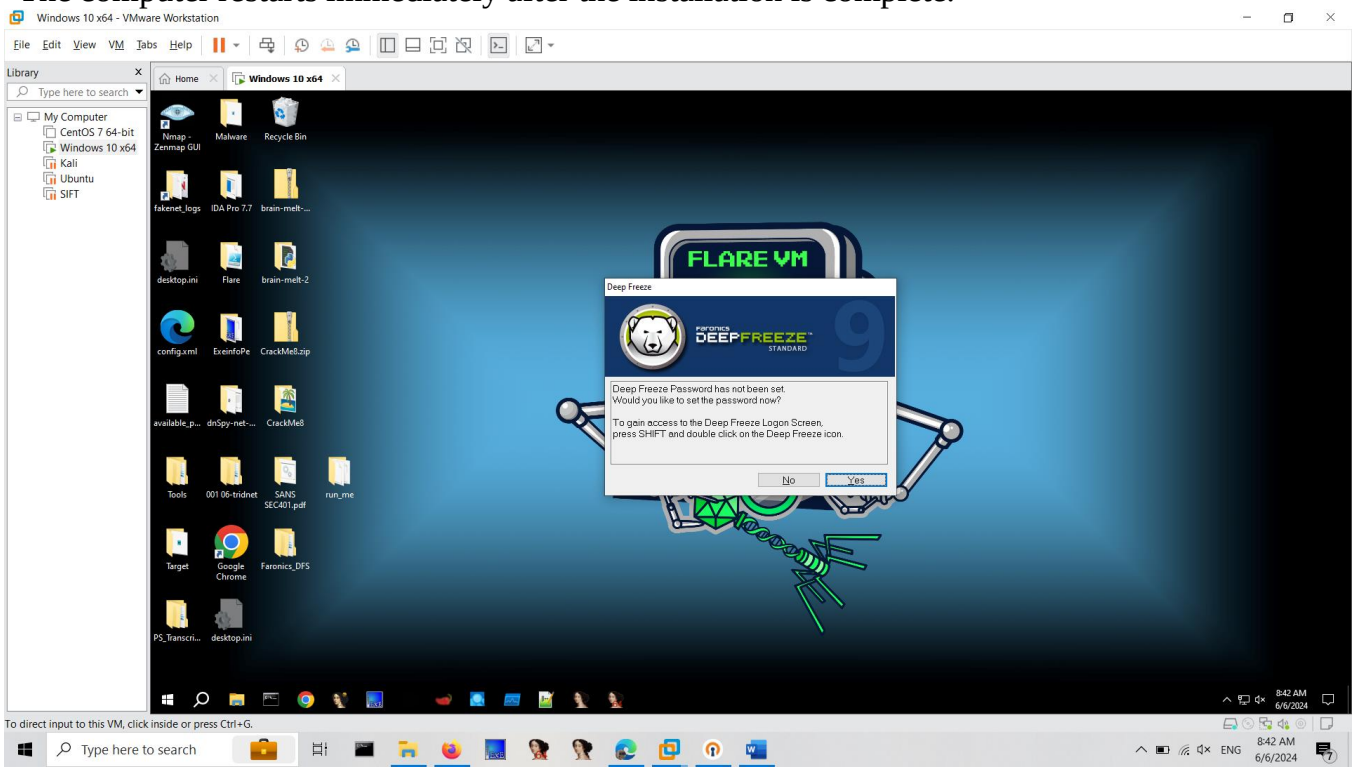
> If you select Hidden, the drive will not be visible in Windows Explorer.

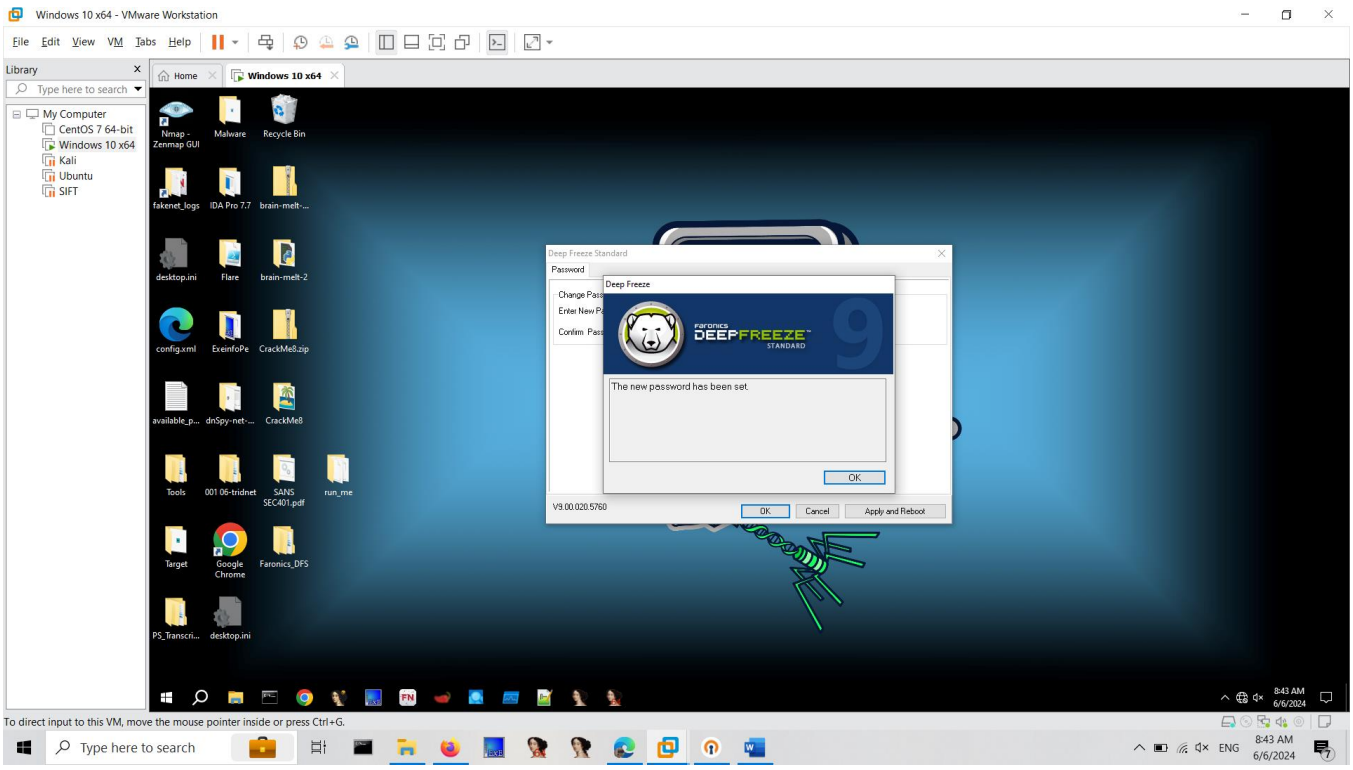
> However, the hidden drive can be accessed by typing the drive letter in Start > Run,

Windows Explorer or Windows Command Line interface.

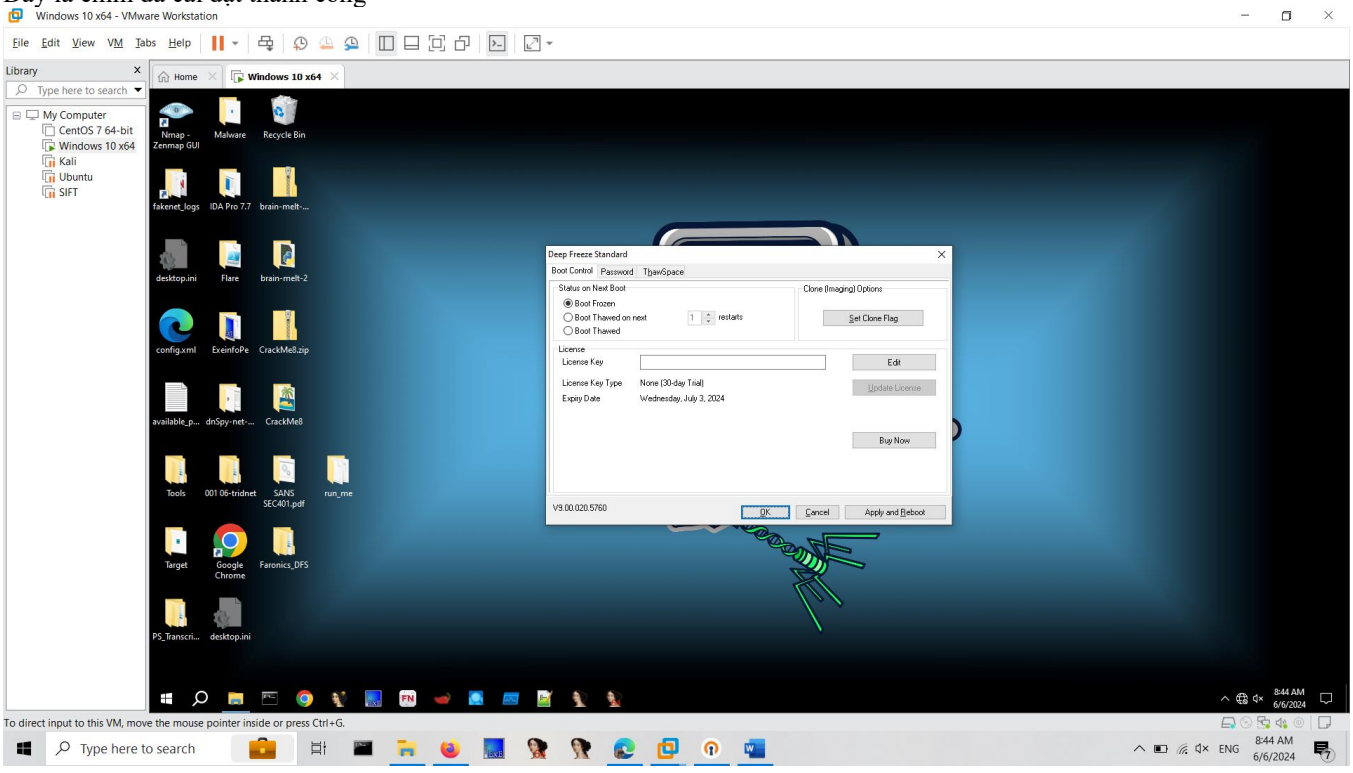
Click Install to begin the installation.

The computer restarts immediately after the installation is complete.



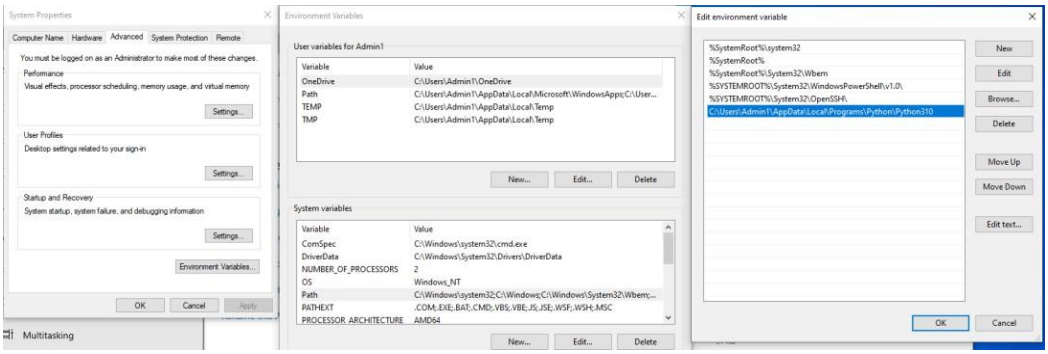


Đây là emm đã cài đặt thành công



- Prepare for Ransomware analysis.

On a windows 10 machine, we need to install Python 3.10 and pip. After installing Python, we need to assign environment variables as shown:

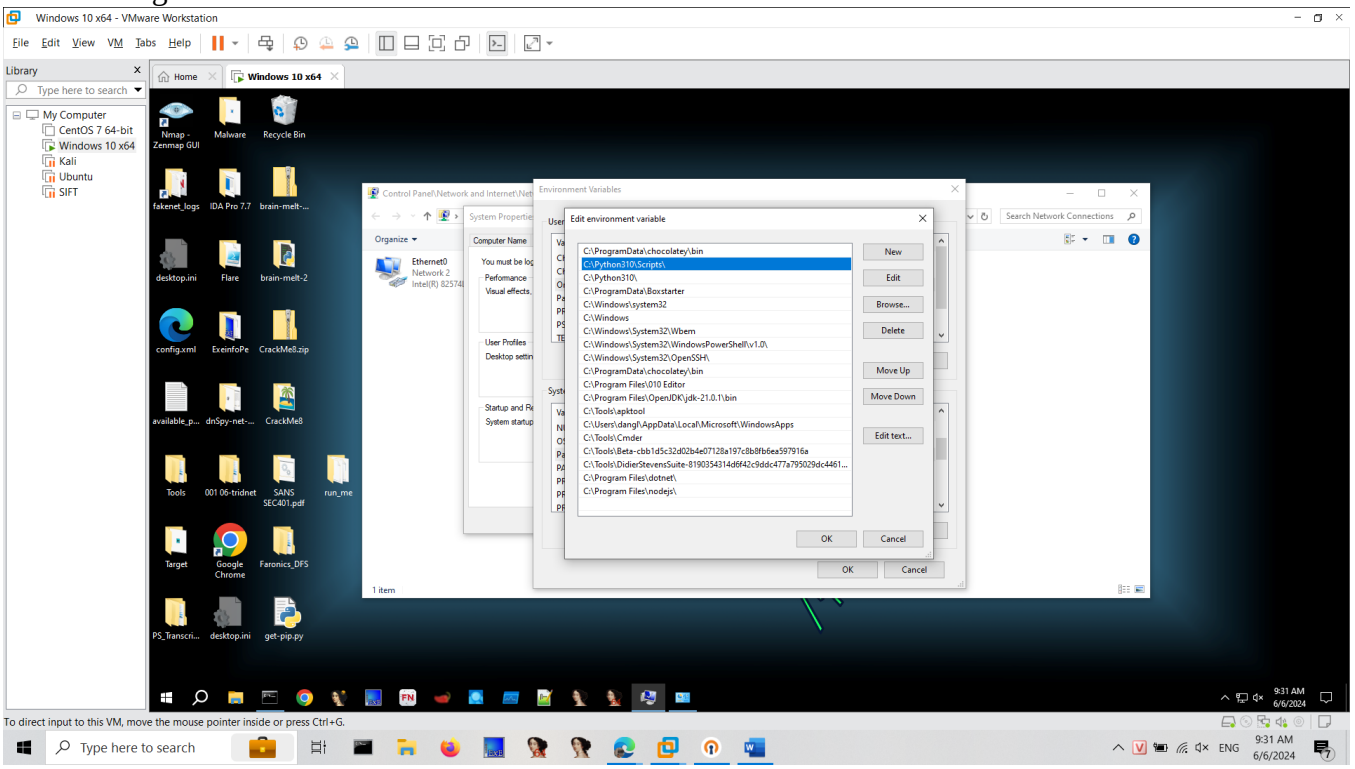


Install pip using the following command (https://github.com/pypa/get-pip)

- curl -sSL https://bootstrap.pypa.io/get-pip.py -o get-pip.py
- python get-pip.py

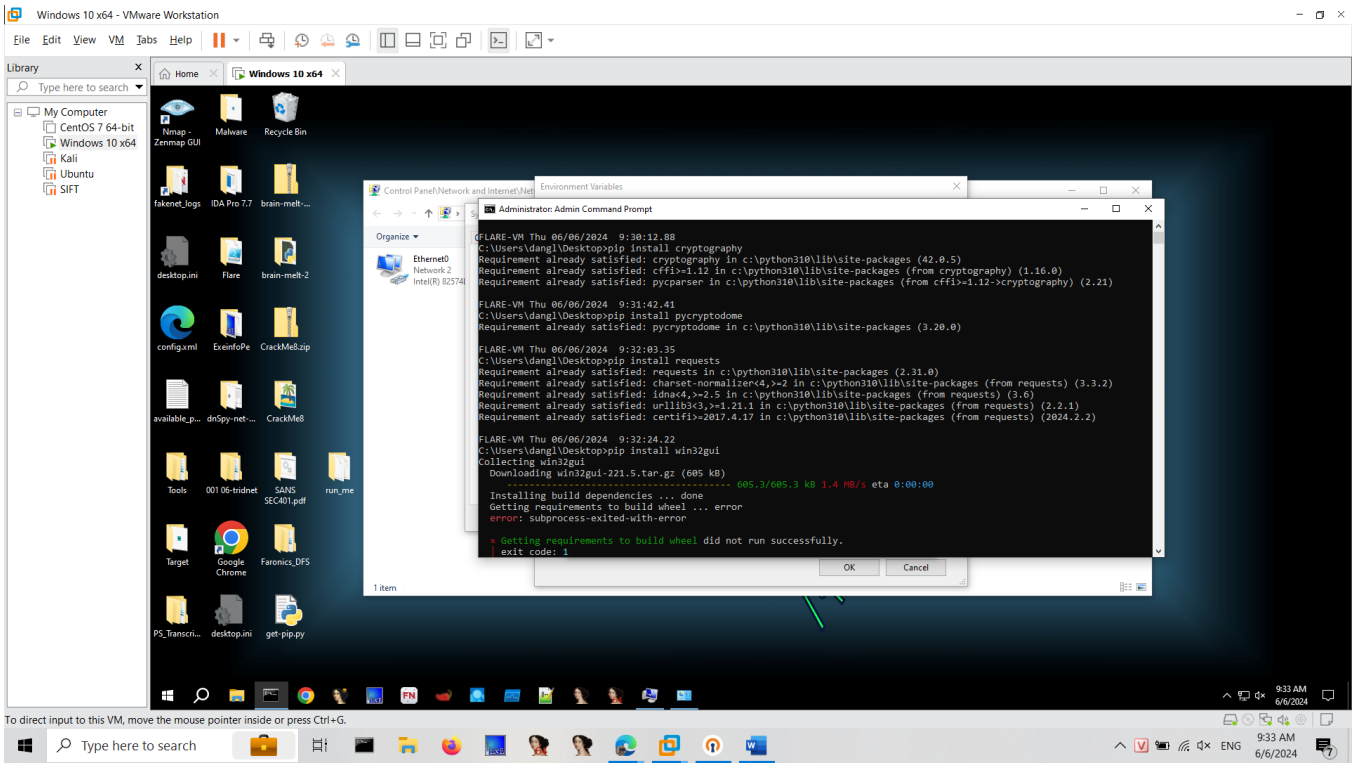
```
Command Prompt
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin1>curl -sSL https://bootstrap.pypa.io/get-pip.py -o get-pip.py

C:\Users\Admin1>python get-pip.py
Collecting pip
  Downloading pip-24.0-py3-none-any.whl.metadata (3.6 kB)
Collecting wheel
  Downloading wheel-0.43.0-py3-none-any.whl.metadata (2.2 kB)
Downloading pip-24.0-py3-none-any.whl (2.1 MB)
   ---------------------------------------- 2.1/2.1 MB 3.6 MB/s eta 0:00:00
Downloading wheel-0.43.0-py3-none-any.whl (65 kB)
   ---------------------------------------- 65.8/65.8 kB ? eta 0:00:00
Installing collected packages: wheel, pip
  WARNING: The script wheel.exe is installed in 'C:\Users\Admin1\AppData\Local\Programs\Python\Python310\Scripts' which
is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
  Attempting uninstall: pip
    Found existing installation: pip 21.2.3
    Uninstalling pip-21.2.3:
      Successfully uninstalled pip-21.2.3
  WARNING: The scripts pip.exe, pip3.10.exe and pip3.exe are installed in 'C:\Users\Admin1\AppData\Local\Programs\Python
\Python310\Scripts' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed pip-24.0 wheel-0.43.0

C:\Users\Admin1>_
```

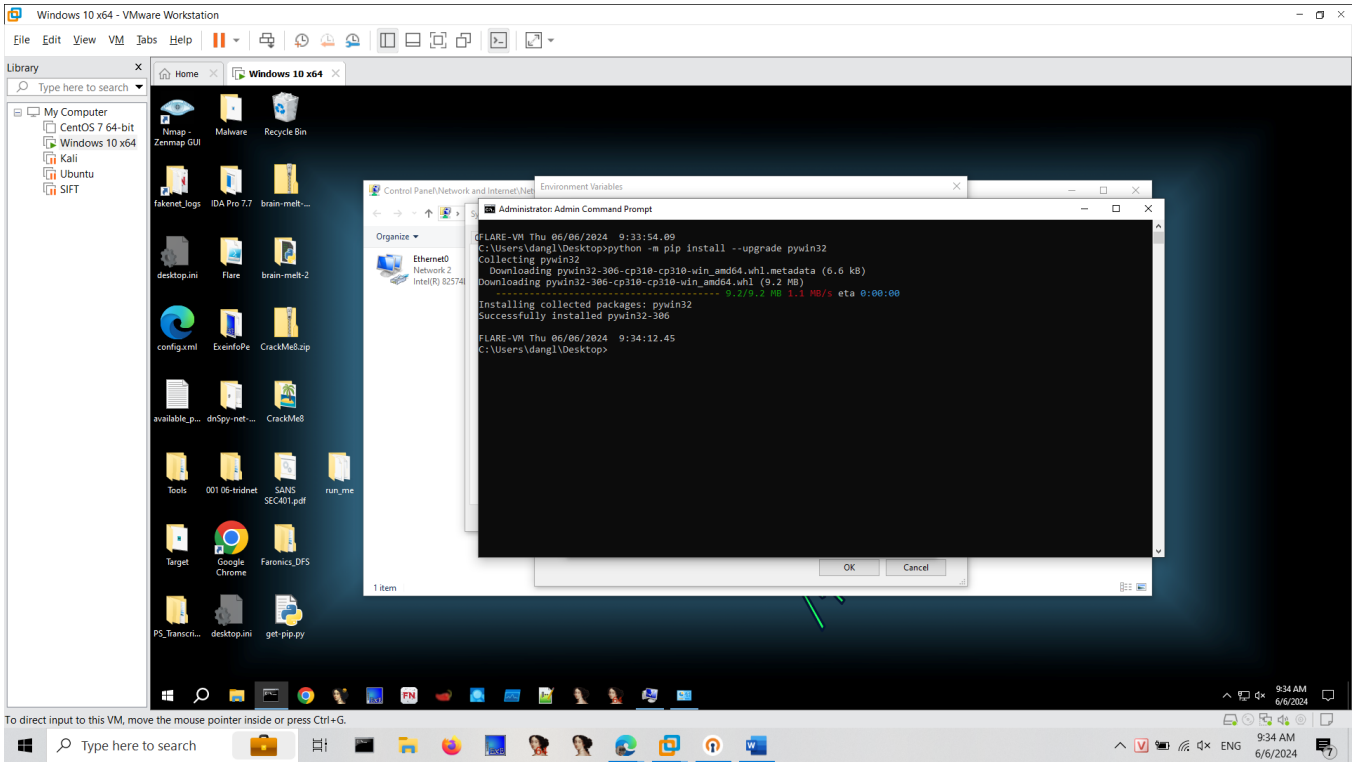
need to assign environment variables as shown:

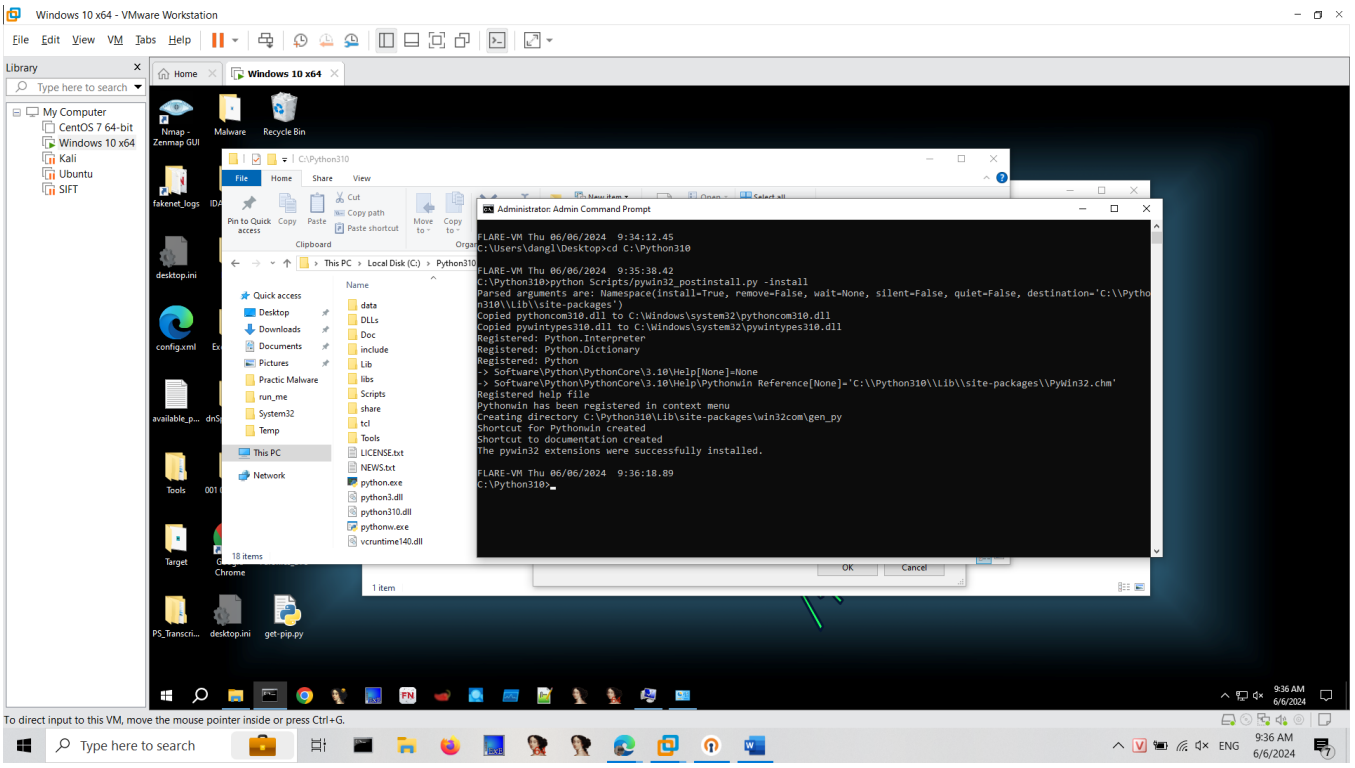


Install support library packages:

- cryptography
- pycryptodome
- requests
- win32gui

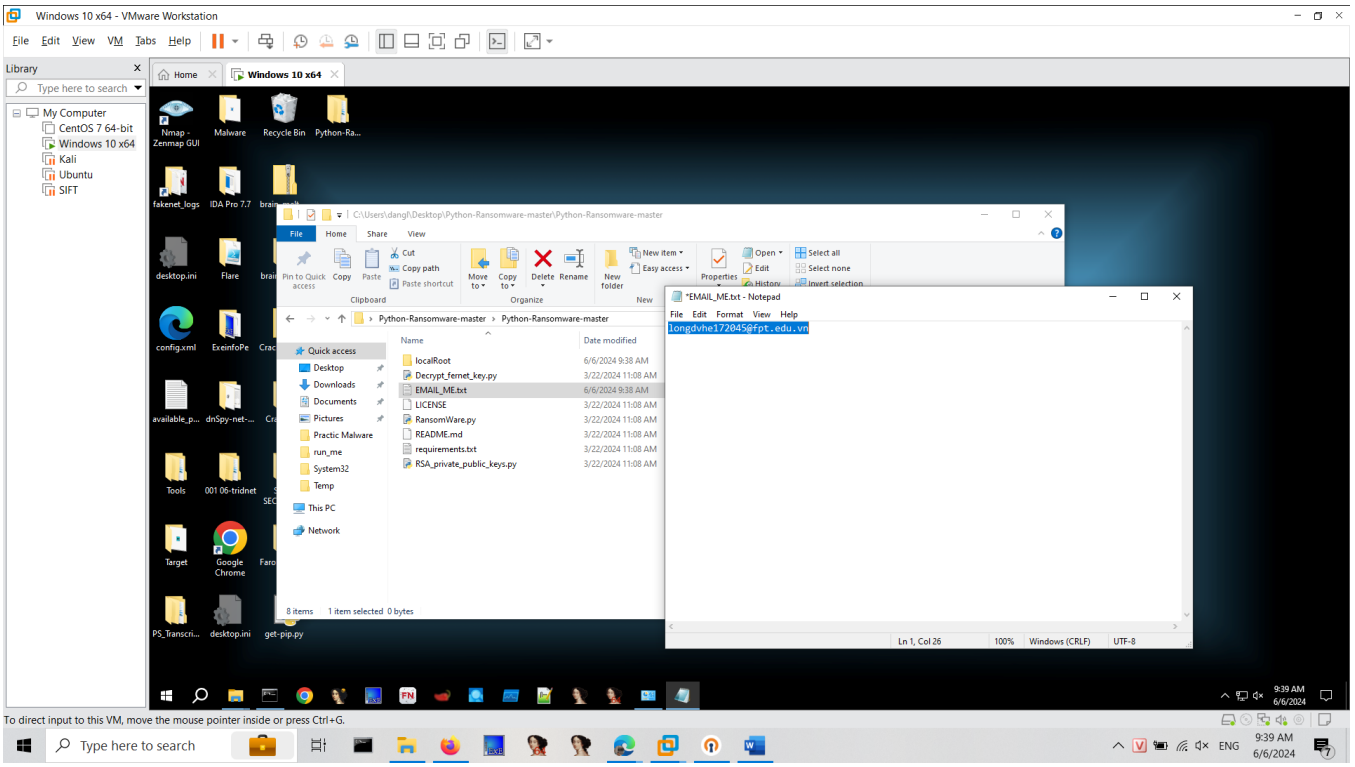

Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
CentOS 7 64-bit
Windows 10 x64
Kali
Ubuntu
SIFT
Home
Windows 10 x64
Nmap - Zenmap GUI
Malware
Recycle Bin
fakenet_logs
IDA Pro 7.7
brain-melt-...
desktop.ini
Flare
brain-melt-2
config.xml
ExeinfoPe
CrackMe8.zip
available_p...
dnSpy-net-...
CrackMe8
Tools
001 06-tridnet
SANS SEC401.pdf
run_me
Target
Google Chrome
Faronics_DFS
PS_Transcri...
desktop.ini
get-pip.py
Environment Variables
Administrator: Admin Command Prompt
FLARE-VM Thu 06/06/2024 9:30:12.88
C:\Users\dangl\Desktop>pip install cryptography
Requirement already satisfied: cryptography in c:\python310\lib\site-packages (42.0.5)
Requirement already satisfied: cffi>=1.12 in c:\python310\lib\site-packages (from cryptography) (1.16.0)
Requirement already satisfied: pycparser in c:\python310\lib\site-packages (from cffi>=1.12->cryptography) (2.21)
FLARE-VM Thu 06/06/2024 9:31:42.41
C:\Users\dangl\Desktop>pip install pycryptodome
Requirement already satisfied: pycryptodome in c:\python310\lib\site-packages (3.20.0)
FLARE-VM Thu 06/06/2024 9:32:03.35
C:\Users\dangl\Desktop>pip install requests
Requirement already satisfied: requests in c:\python310\lib\site-packages (2.31.0)
Requirement already satisfied: charset-normalizer<4,>=2 in c:\python310\lib\site-packages (from requests) (3.3.2)
Requirement already satisfied: idna<4,>=2.5 in c:\python310\lib\site-packages (from requests) (3.6)
Requirement already satisfied: urllib3<3,>=1.21.1 in c:\python310\lib\site-packages (from requests) (2.2.1)
Requirement already satisfied: certifi>=2017.4.17 in c:\python310\lib\site-packages (from requests) (2024.2.2)
FLARE-VM Thu 06/06/2024 9:32:24.22
C:\Users\dangl\Desktop>pip install win32gui
Collecting win32gui
Downloading win32gui-221.5.tar.gz (605 kB)
605.3/605.3 kB 1.4 MB/s eta 0:00:00
Installing build dependencies ... done
Getting requirements to build wheel ... error
error: subprocess-exited-with-error
× Getting requirements to build wheel did not run successfully.
exit code: 1
OK
Cancel
1 item
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
9:33 AM
6/6/2024


Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
CentOS 7 64-bit
Windows 10 x64
Kali
Ubuntu
SIFT
Home
Windows 10 x64
Nmap - Zenmap GUI
Malware
Recycle Bin
fakenet_logs
IDA Pro 7.7
brain-melt-...
desktop.ini
Flare
brain-melt-2
config.xml
ExeinfoPe
CrackMe8.zip
available_p...
dnSpy-net-...
CrackMe8
Tools
001 06-tridnet
SANS SEC401.pdf
run_me
Target
Google Chrome
Faronics_DFS
PS_Transcri...
desktop.ini
get-pip.py
Environment Variables
Administrator: Admin Command Prompt
FLARE-VM Thu 06/06/2024 9:33:54.09
C:\Users\dangl\Desktop>python -m pip install --upgrade pywin32
Collecting pywin32
Downloading pywin32-306-cp310-cp310-win_amd64.whl.metadata (6.6 kB)
Downloading pywin32-306-cp310-cp310-win_amd64.whl (9.2 MB)
9.2/9.2 MB 1.1 MB/s eta 0:00:00
Installing collected packages: pywin32
Successfully installed pywin32-306
FLARE-VM Thu 06/06/2024 9:34:12.45
C:\Users\dangl\Desktop>
OK
Cancel
1 item
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
9:34 AM
6/6/2024

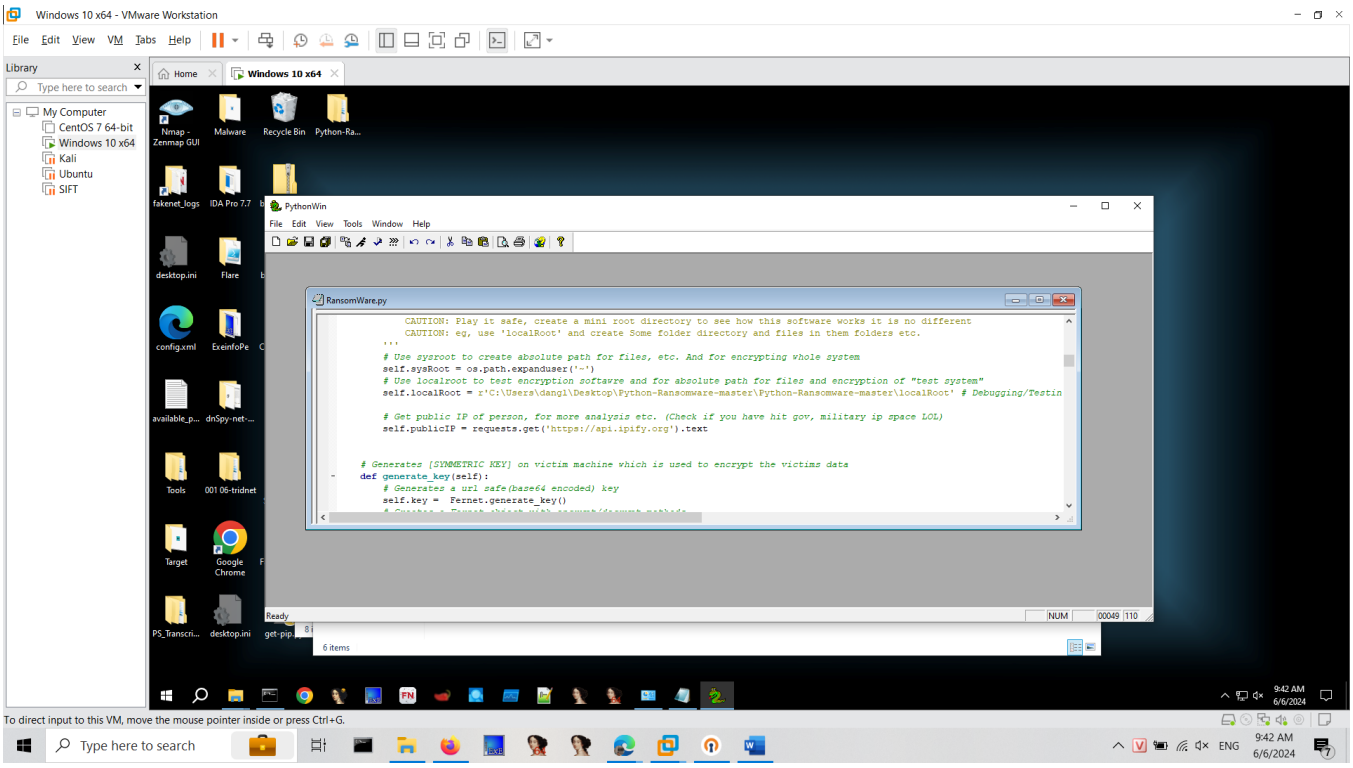


Download Source Ransomware here: https://github.com/ncorbuk/Python-Ransomware/

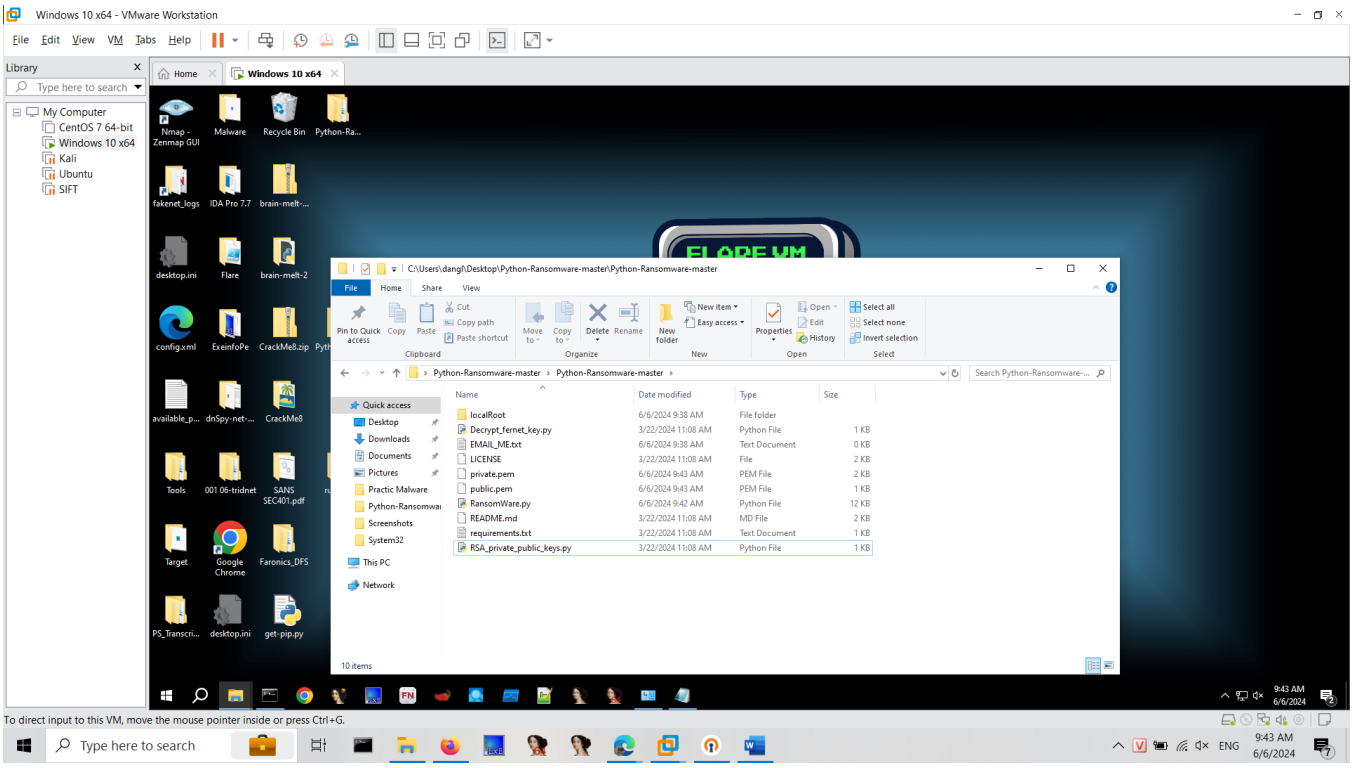
After unpacking, we have the following files and We need to create an EMAIL_ME.txt file with the Attacker's email address



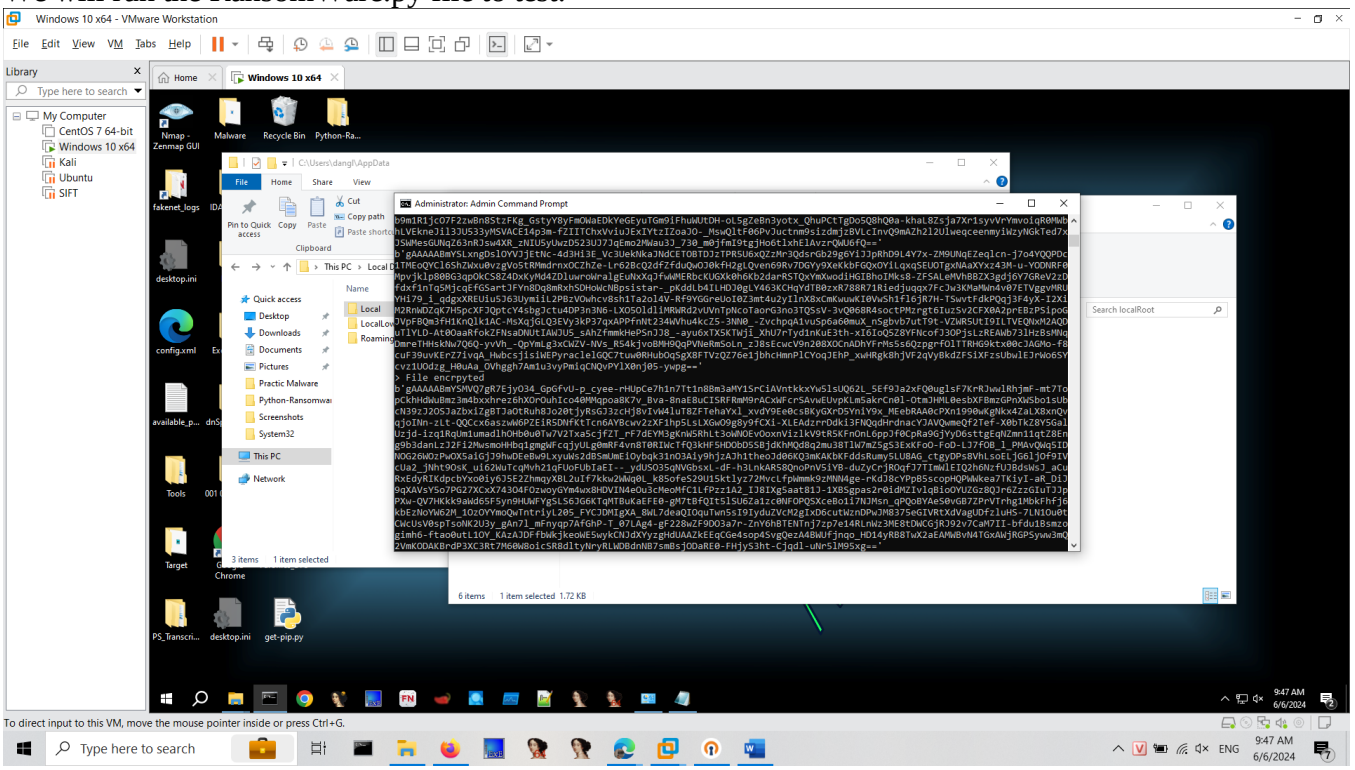
We need to edit some content in the RansomWare.py file as follows



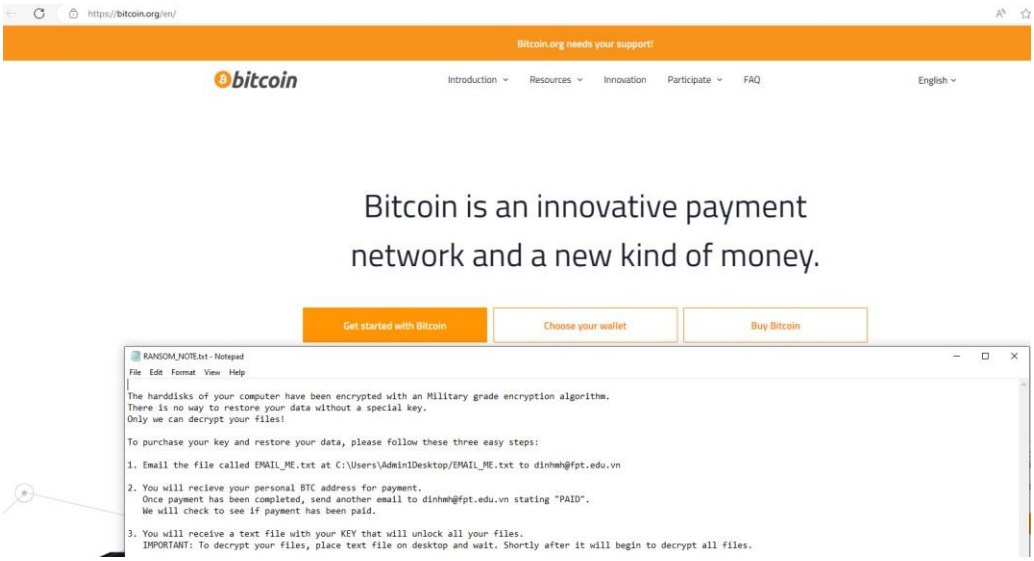
We will run the RSA_private_public_keys.py file to generate a key pair:

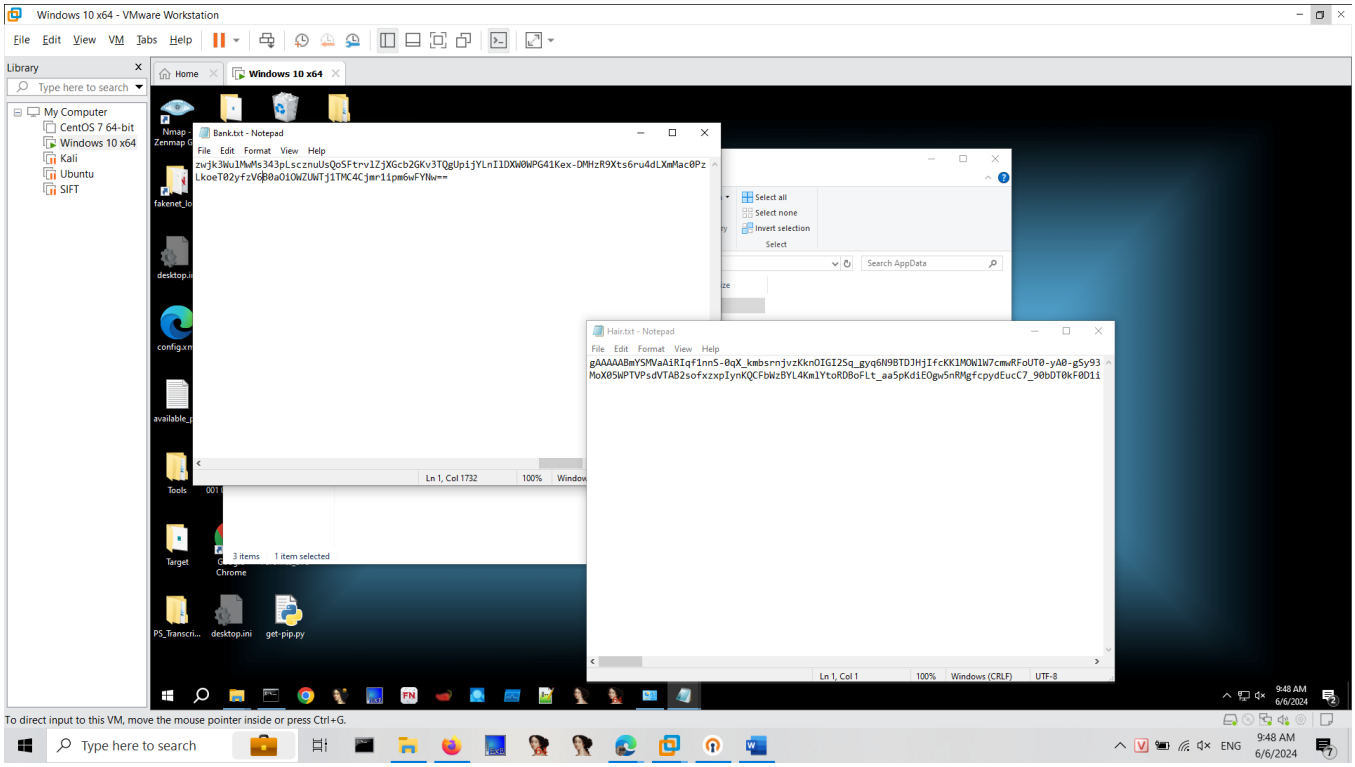


We will run the RansomWare.py file to test:



As a result, the Windows 10 machine has been encrypted





Because the machine preparing for analysis has Deep Freeze installed, we only need to restart the machine to return to the new state, in this case just like Snapshot. This is very useful in cases where we need physical systems to analyze specific malware.