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:

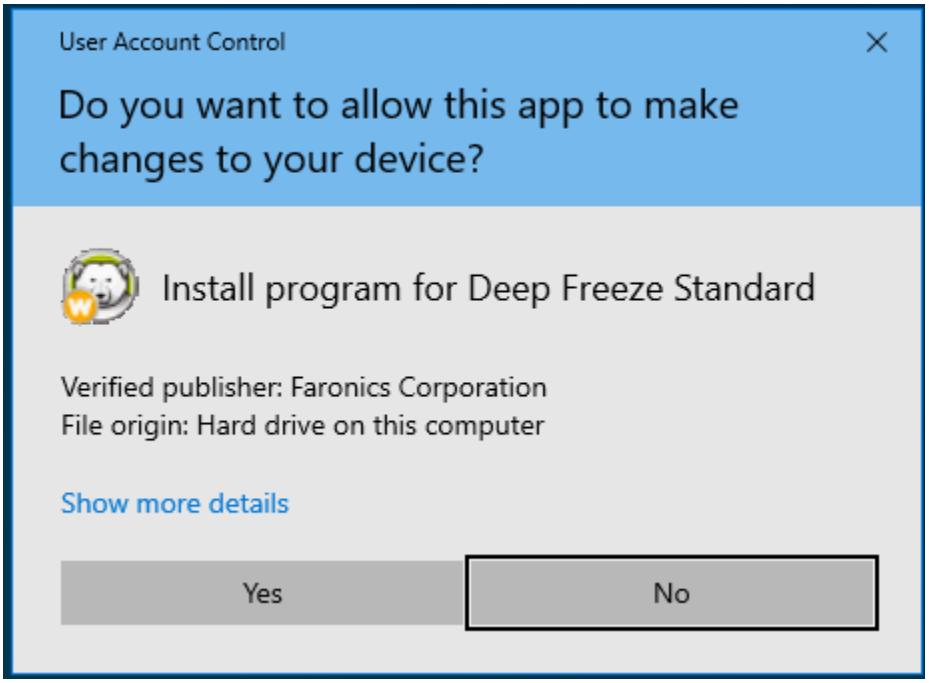
- Windows 7 (32 and 64-bit)
- Windows 8.1 (32 and 64-bit)
- Windows 10 up to version 22H2 (32 and 64-bit)
- Windows 11 up to version 23H2 (64-bit)

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

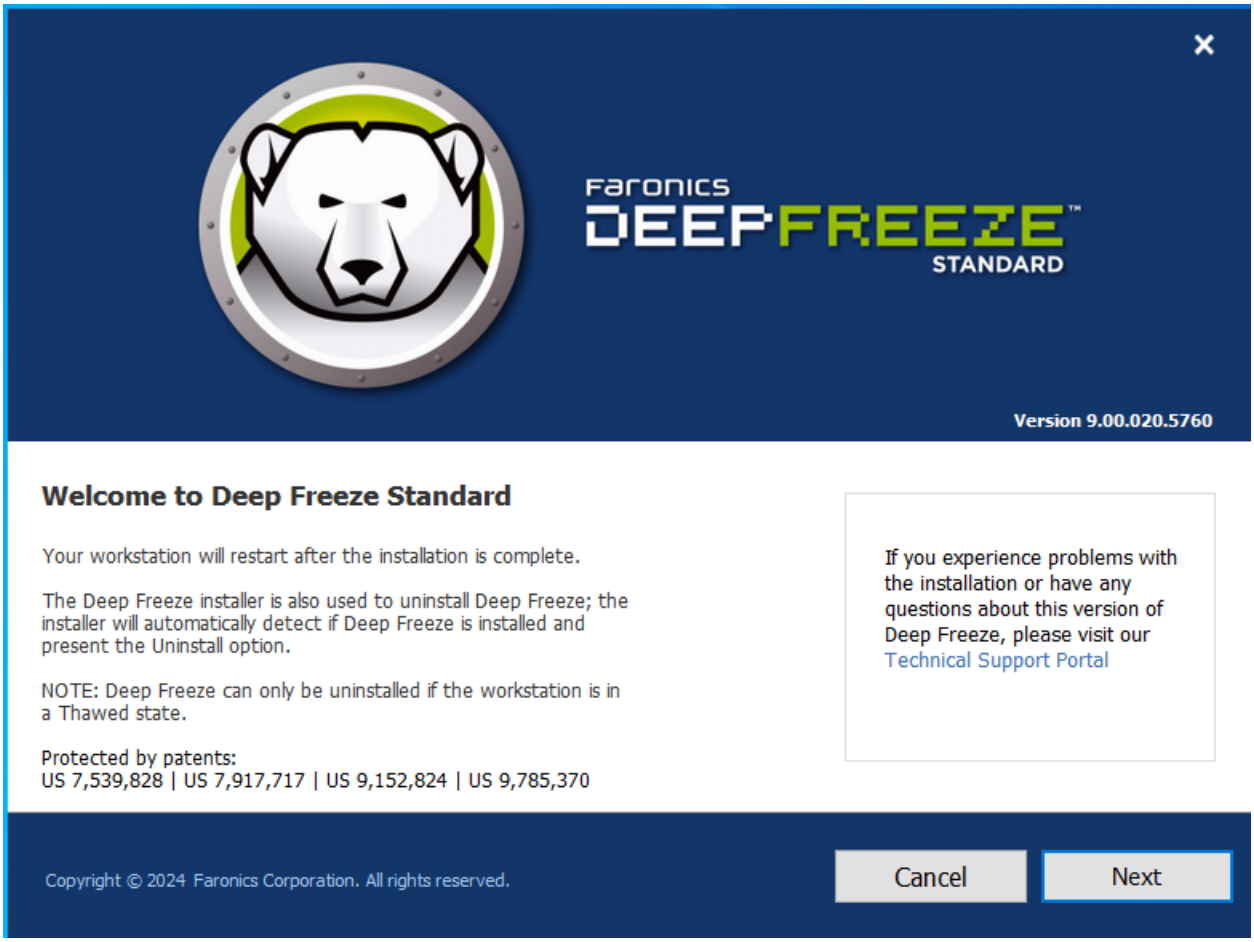
In this LAB lesson, we will install Deep Freeze on Windows 10. We go to the following link to download:

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:

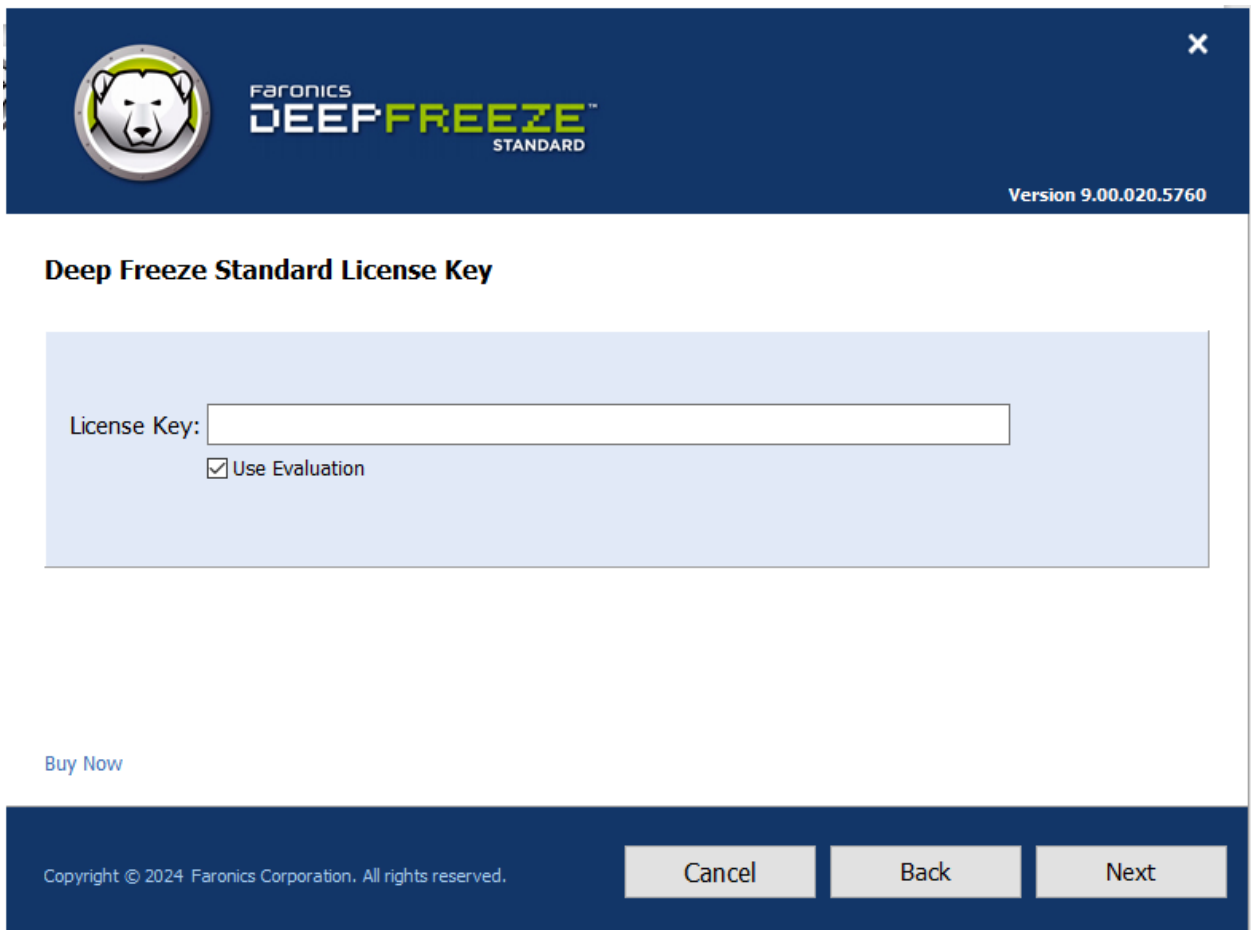

User Account Control
Do you want to allow this app to make changes to your device?
Install program for Deep Freeze Standard
Verified publisher: Faronics Corporation
File origin: Hard drive on this computer
Show more details
Yes
No

Click Yes

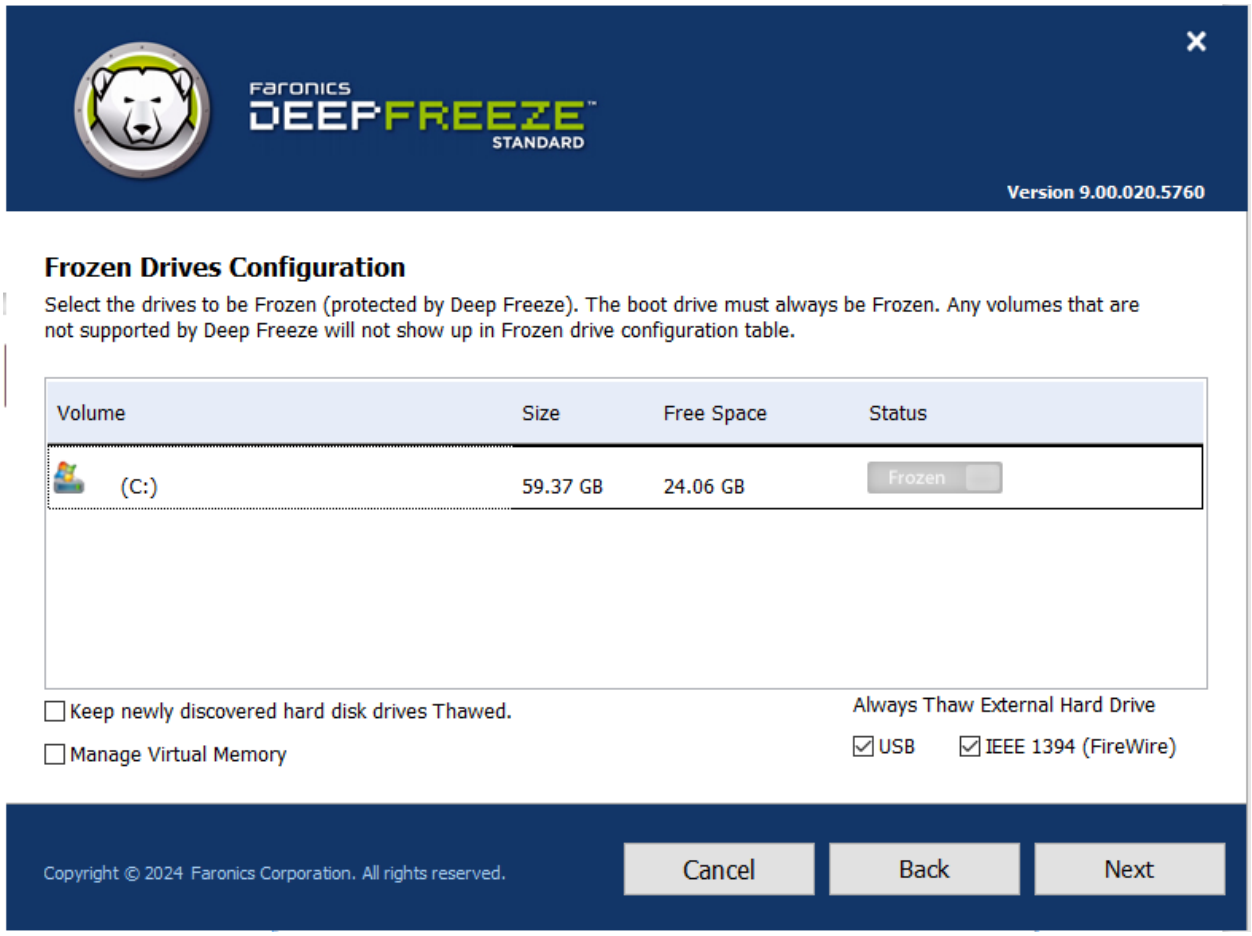

Faronics
DEEP FREEZE
STANDARD
Version 9.00.020.5760
Welcome to Deep Freeze Standard
Your workstation will restart after the installation is complete.
The Deep Freeze installer is also used to uninstall Deep Freeze; the installer will automatically detect if Deep Freeze is installed and present the Uninstall 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

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

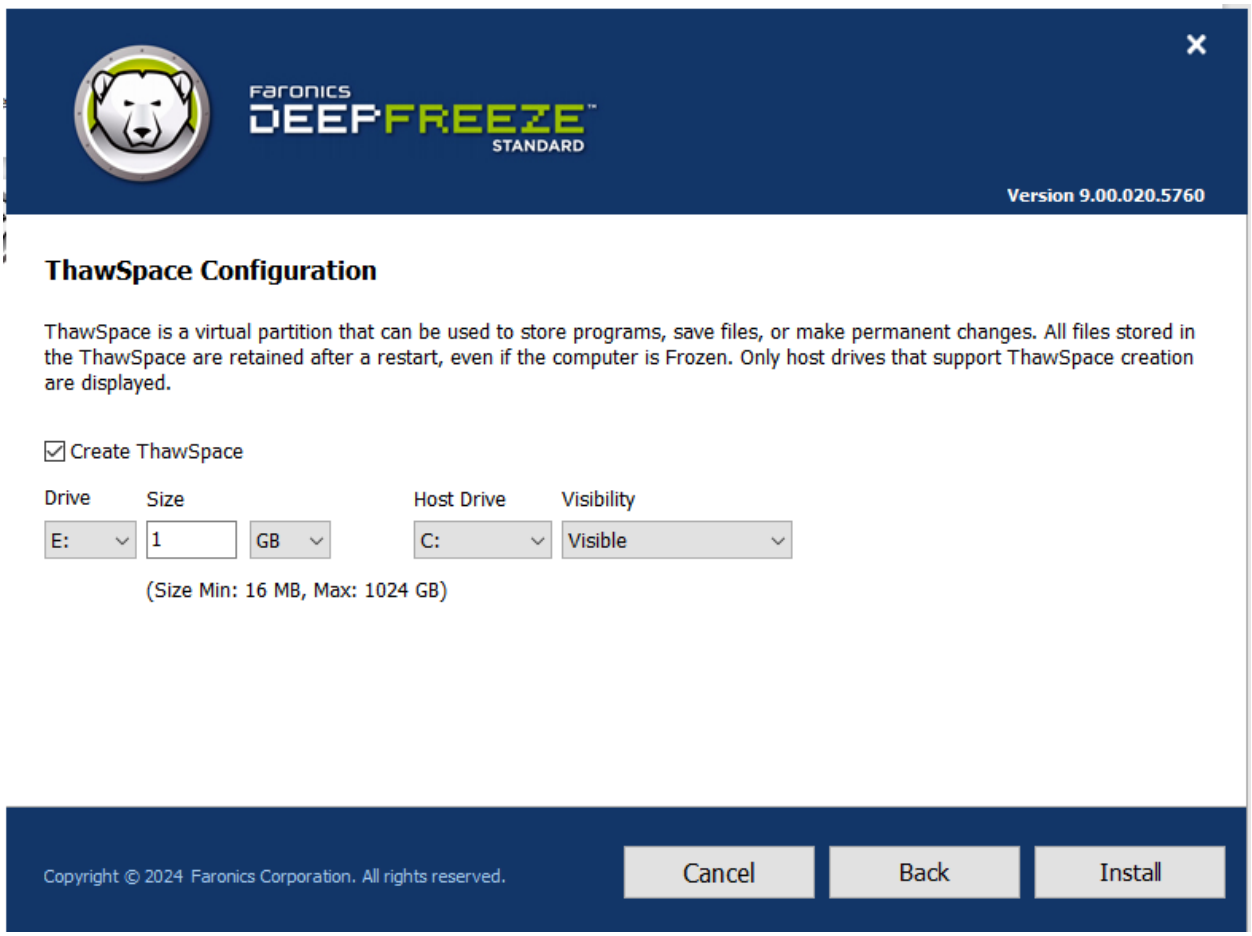


> Keep newly discovered hard disk drives Thawed — select this option if you want to keep the newly discovered hard disk drives in a Thawed state. Changes made on the newly discovered hard disk drives will be retained.

> 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.

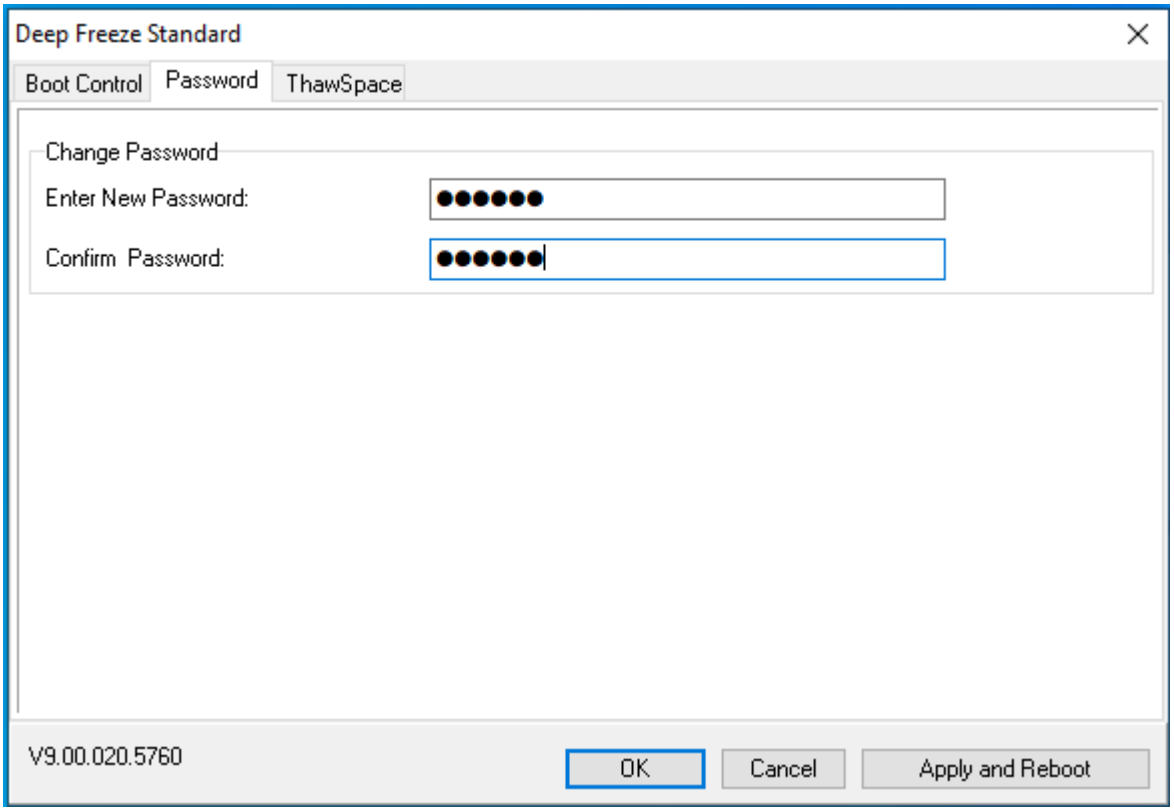
> If you select Hidden, the drive will not be visible in Windows Explorer.

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

Windows Explorer or Windows Command Line interface.

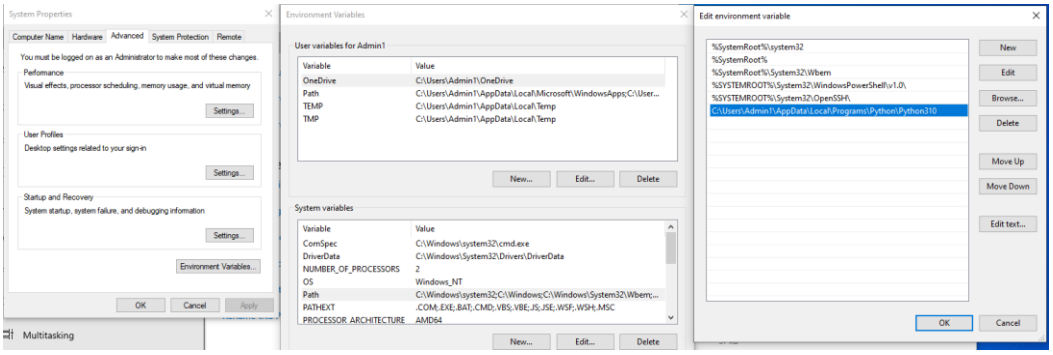
Click Install to begin the installation.

The computer restarts immediately after the installation is complete.



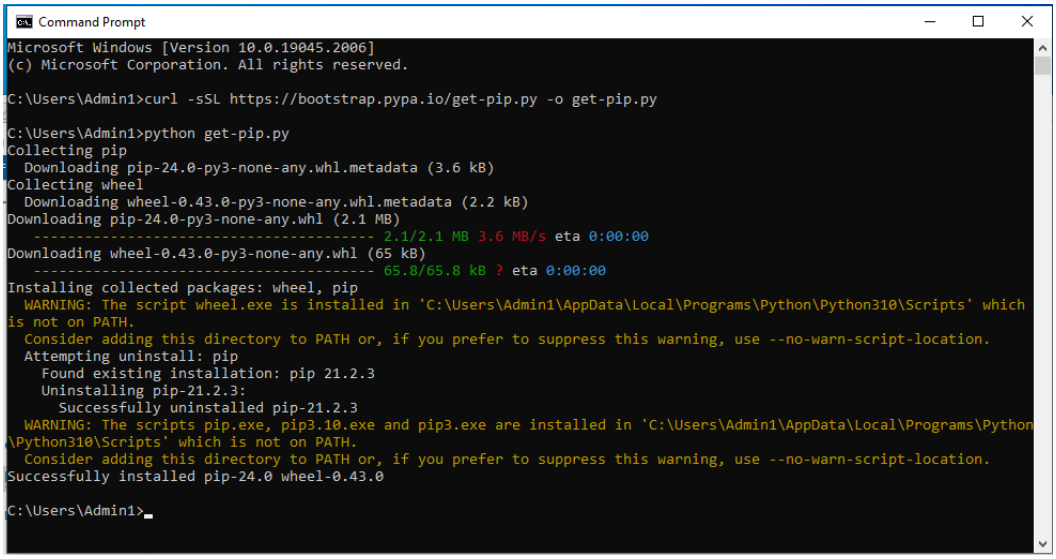
- Prepare for Ransomware analysis.

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:

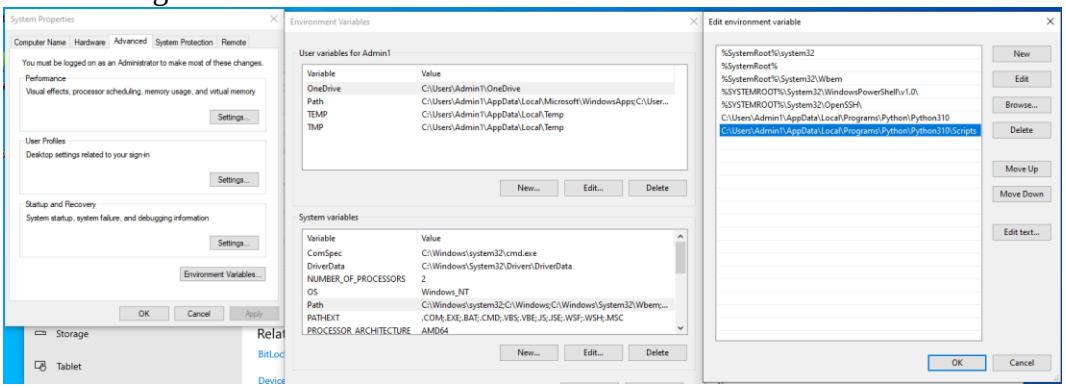


Install pip using the following command (https://github.com/pypa/get-pip)

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



need to assign environment variables as shown:



Install support library packages:

- cryptography
- pycryptodome
- requests
- win32gui

Command Prompt

```
C:\Users\Admin1>pip install cryptography
Collecting cryptography
  Downloading cryptography-42.0.5-cp39-abi3-win_amd64.whl.metadata (5.4 kB)
Collecting cffi>=1.12 (from cryptography)
  Downloading cffi-1.16.0-cp310-cp310-win_amd64.whl.metadata (1.5 kB)
Collecting pycparser (from cffi>=1.12->cryptography)
  Downloading pycparser-2.22-py3-none-any.whl.metadata (943 bytes)
Downloading cryptography-42.0.5-cp39-abi3-win_amd64.whl (2.9 MB)
   ---------------------------------------- 2.9/2.9 MB 2.4 MB/s eta 0:00:00
Downloading cffi-1.16.0-cp310-cp310-win_amd64.whl (181 kB)
   ---------------------------------------- 181.6/181.6 kB 5.4 MB/s eta 0:00:00
Downloading pycparser-2.22-py3-none-any.whl (117 kB)
   ---------------------------------------- 117.6/117.6 kB 2.3 MB/s eta 0:00:00
Installing collected packages: pycparser, cffi, cryptography
Successfully installed cffi-1.16.0 cryptography-42.0.5 pycparser-2.22

C:\Users\Admin1>pip install pycryptodome
Collecting pycryptodome
  Downloading pycryptodome-3.20.0-cp35-abi3-win_amd64.whl.metadata (3.4 kB)
Downloading pycryptodome-3.20.0-cp35-abi3-win_amd64.whl (1.8 MB)
   ---------------------------------------- 1.8/1.8 MB 1.5 MB/s eta 0:00:00
Installing collected packages: pycryptodome
Successfully installed pycryptodome-3.20.0

C:\Users\Admin1>
```

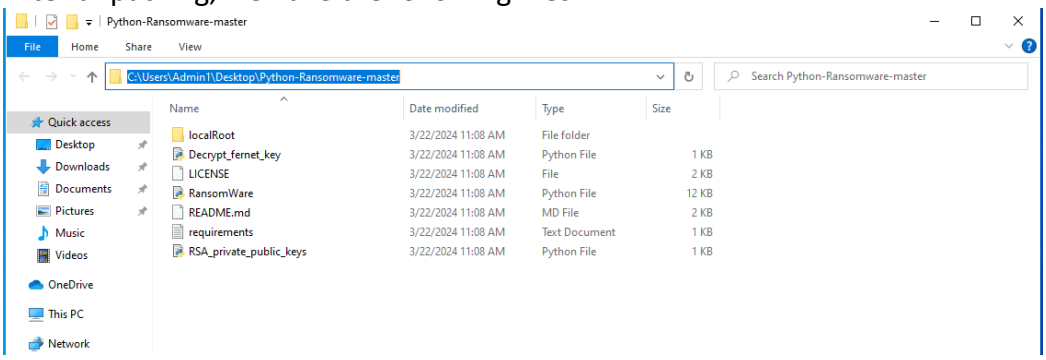
```
C:\Users\Admin1>pip install requests
Collecting requests
  Downloading requests-2.31.0-py3-none-any.whl.metadata (4.6 kB)
Collecting charset-normalizer<4,>=2 (from requests)
  Downloading charset_normalizer-3.3.2-cp310-cp310-win_amd64.whl.metadata (34 kB)
Collecting idna<4,>=2.5 (from requests)
  Downloading idna-3.7-py3-none-any.whl.metadata (9.9 kB)
Collecting urllib3<3,>=1.21.1 (from requests)
  Downloading urllib3-2.2.1-py3-none-any.whl.metadata (6.4 kB)
Collecting certifi>=2017.4.17 (from requests)
  Downloading certifi-2024.2.2-py3-none-any.whl.metadata (2.2 kB)
Downloading requests-2.31.0-py3-none-any.whl (62 kB)
   ---------------------------------------- 62.6/62.6 kB 222.7 kB/s eta 0:00:00
Downloading certifi-2024.2.2-py3-none-any.whl (163 kB)
   ---------------------------------------- 163.8/163.8 kB 68.2 kB/s eta 0:00:00
Downloading charset_normalizer-3.3.2-cp310-cp310-win_amd64.whl (100 kB)
   ---------------------------------------- 100.3/100.3 kB 71.2 kB/s eta 0:00:00
Downloading idna-3.7-py3-none-any.whl (66 kB)
   ---------------------------------------- 66.8/66.8 kB 134.1 kB/s eta 0:00:00
Downloading urllib3-2.2.1-py3-none-any.whl (121 kB)
   ---------------------------------------- 121.1/121.1 kB 129.0 kB/s eta 0:00:00
Installing collected packages: urllib3, idna, charset-normalizer, certifi, requests
Successfully installed certifi-2024.2.2 charset-normalizer-3.3.2 idna-3.7 requests-2.31.0 urllib3-2.2.1

C:\Users\Admin1>
```

```
C:\Users\Admin1>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 226.6 kB/s eta 0:00:00
Installing collected packages: pywin32
Successfully installed pywin32-306
```

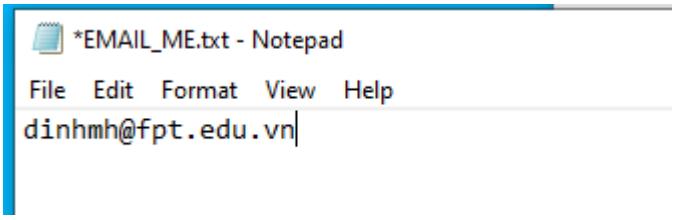
```
C:\Users\Admin1>cd C:\Users\Admin1\AppData\Local\Programs\Python\Python310

C:\Users\Admin1\AppData\Local\Programs\Python\Python310>python Scripts/pywin32_postinstall.py -install
Parsed arguments are: Namespace(install=True, remove=False, wait=None, silent=False, quiet=False, destination='C:\\Users
\\Admin1\\AppData\\Local\\Programs\\Python\\Python310\\Lib\\site-packages')
Copied pythoncom310.dll to C:\Users\Admin1\AppData\Local\Programs\Python\Python310\pythoncom310.dll
Copied pywintypes310.dll to C:\Users\Admin1\AppData\Local\Programs\Python\Python310\pywintypes310.dll
You do not have the permissions to install COM objects.
The sample COM objects were not registered.
-> Software\Python\PythonCore\3.10\Help[None]=None
-> Software\Python\PythonCore\3.10\Help\Pythonwin Reference[None]='C:\\Users\\Admin1\\AppData\\Local\\Programs\\Python\\
Python310\\Lib\\site-packages\\PyWin32.chm'
Registered help file
Pythonwin has been registered in context menu
Creating directory C:\Users\Admin1\AppData\Local\Programs\Python\Python310\Lib\site-packages\win32com\gen_py
Shortcut for Pythonwin created
Shortcut to documentation created
The pywin32 extensions were successfully installed.

C:\Users\Admin1\AppData\Local\Programs\Python\Python310>
```

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

After unpacking, we have the following files:



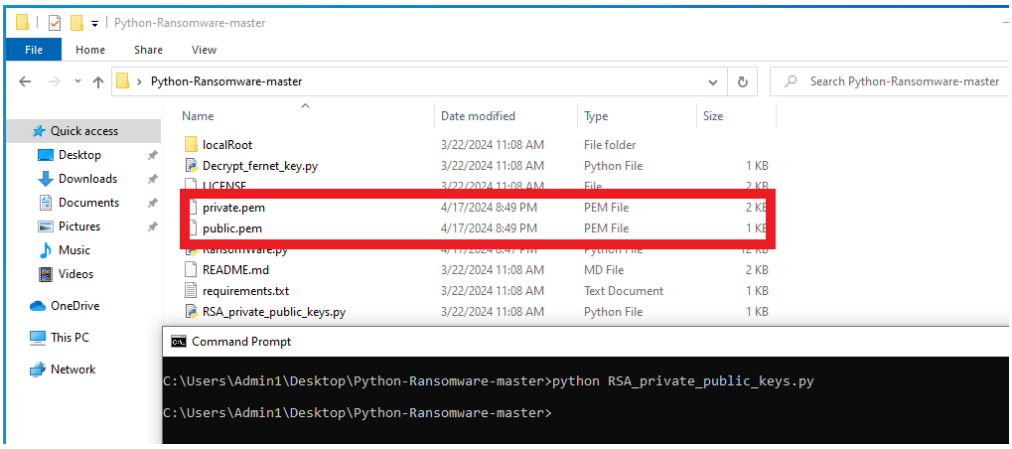
We need to create an EMAIL_ME.txt file with the Attacker's email address



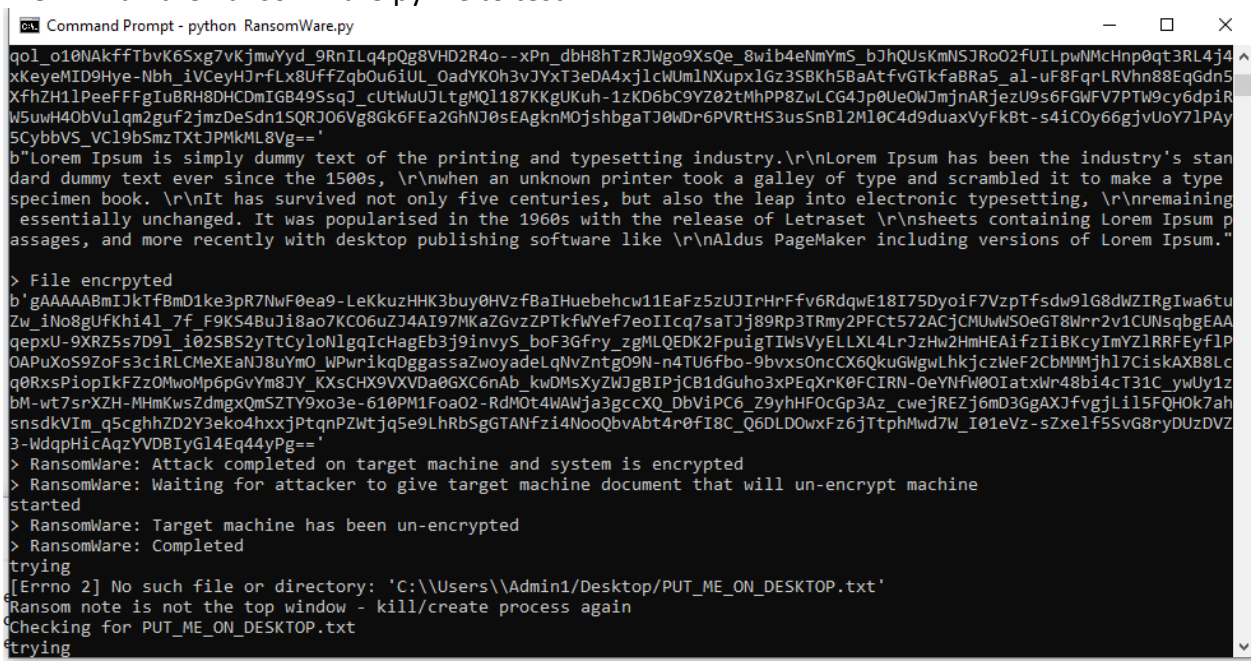
We need to edit some content in the RansomWare.py file as follows

```
''' Root directorys to start Encryption/Decryption from
    CAUTION: Do NOT use self.sysRoot on your own PC as you could end up messing up your system etc...
    CAUTION: Play it safe, create a mini root directory to see how this software works it is no different
    CAUTION: eg, use 'localRoot' and create Some folder directory and files in them folders etc.
'''
# Use sysroot to create absolute path for files, etc. And for encrypting whole system
self.sysRoot = os.path.expanduser('~')
# Use localroot to test encryption softawre and for absolute path for files and encryption of "test system
self.localRoot = r'C:\Users\Admin1\Desktop\Python-Ransomware-master\localRoot' # Debugging/Testing

# Get public IP of person, for more analysis etc. (Check if you have hit gov, military ip space LOL)
self.publicIP = requests.get('https://api.ipify.org').text
```

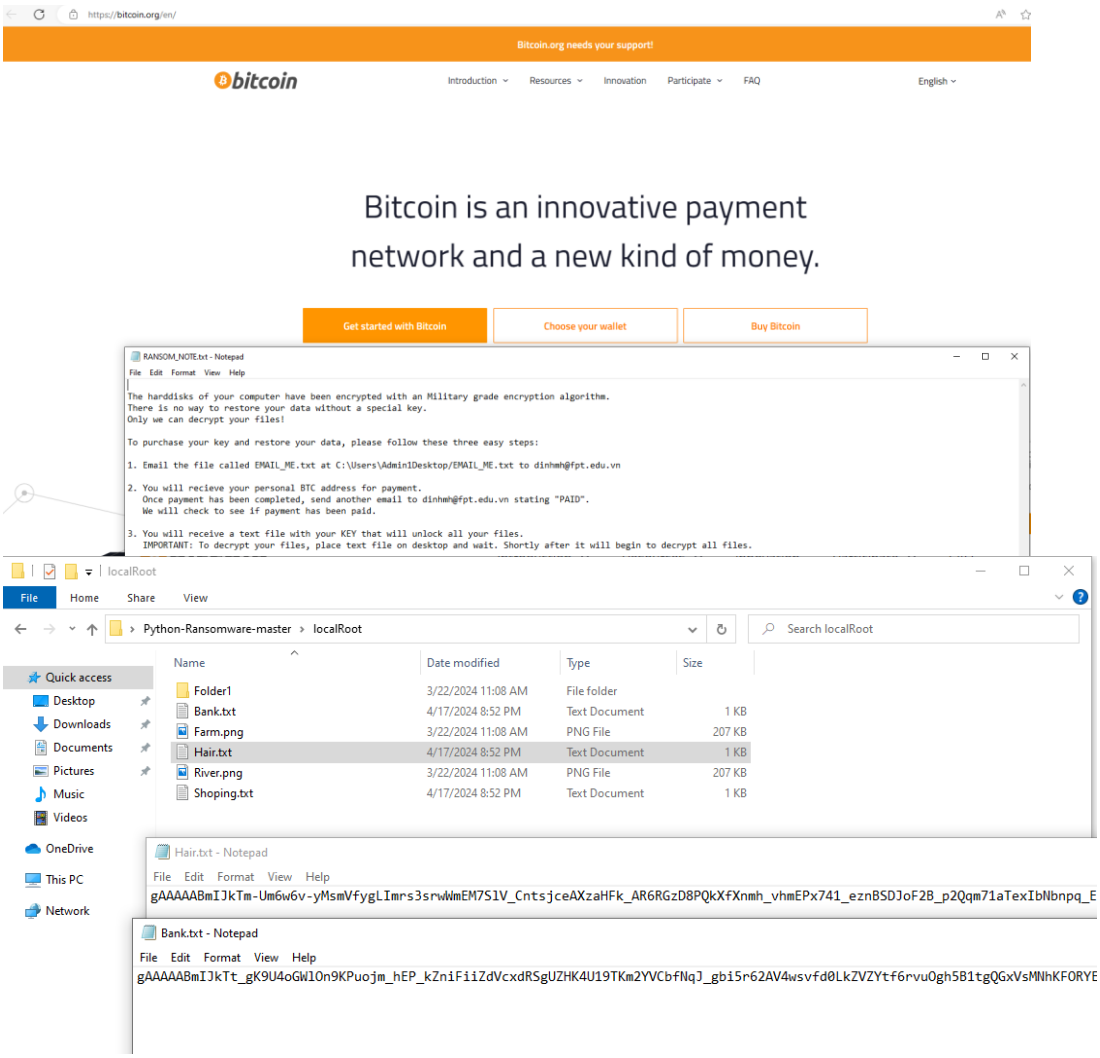
We will run the RSA_private_public_keys.py file to generate a key pair:



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.