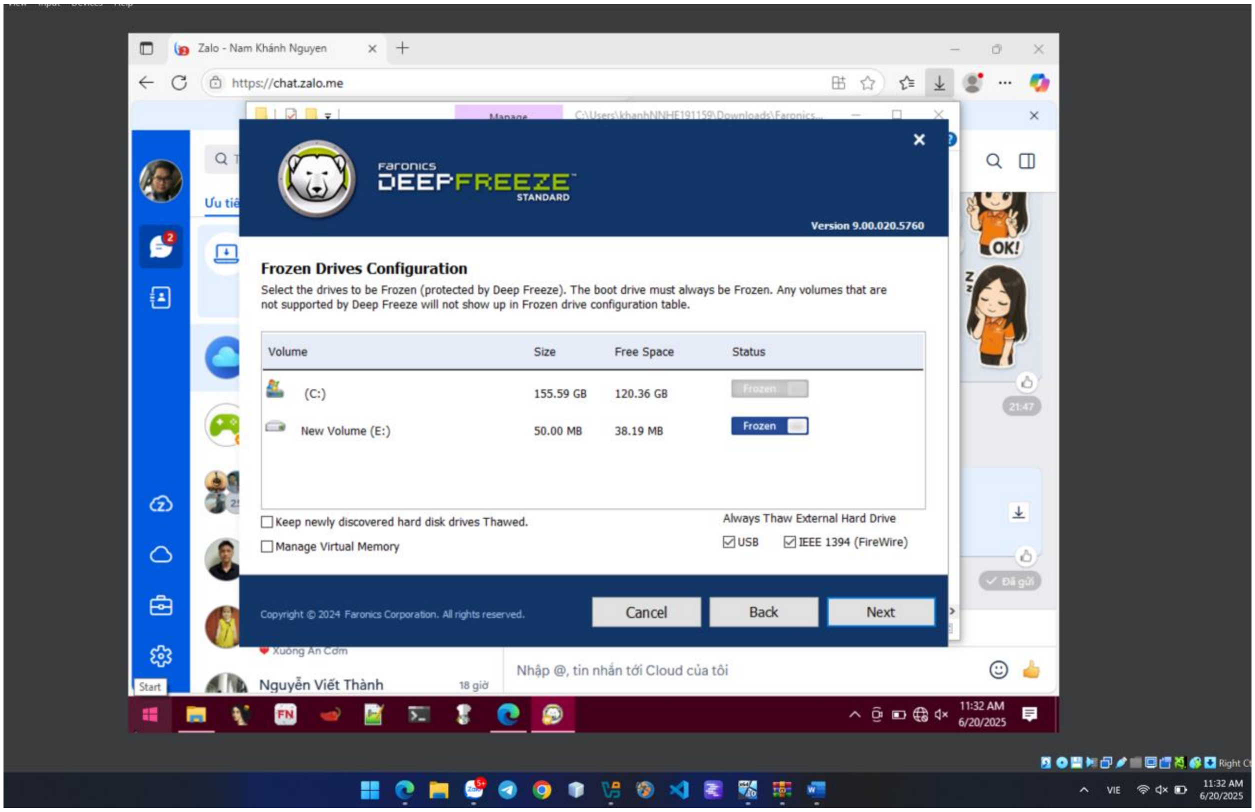
KHANHNNHE191159

NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

LAB 10: Install Deep Freeze

Frozen Drives Configuration



Frozen Drives Configuration

Select the drives to be Frozen (protected by Deep Freeze). The boot drive must always be Frozen. Any volumes that are not supported by Deep Freeze will not show up in Frozen drive configuration table.

Volume	Size	Free Space	Status
(C:)	155.59 GB	120.36 GB	Frozen
New Volume (E:)	50.00 MB	38.19 MB	Frozen

□ Keep newly discovered hard disk drives Thawed.

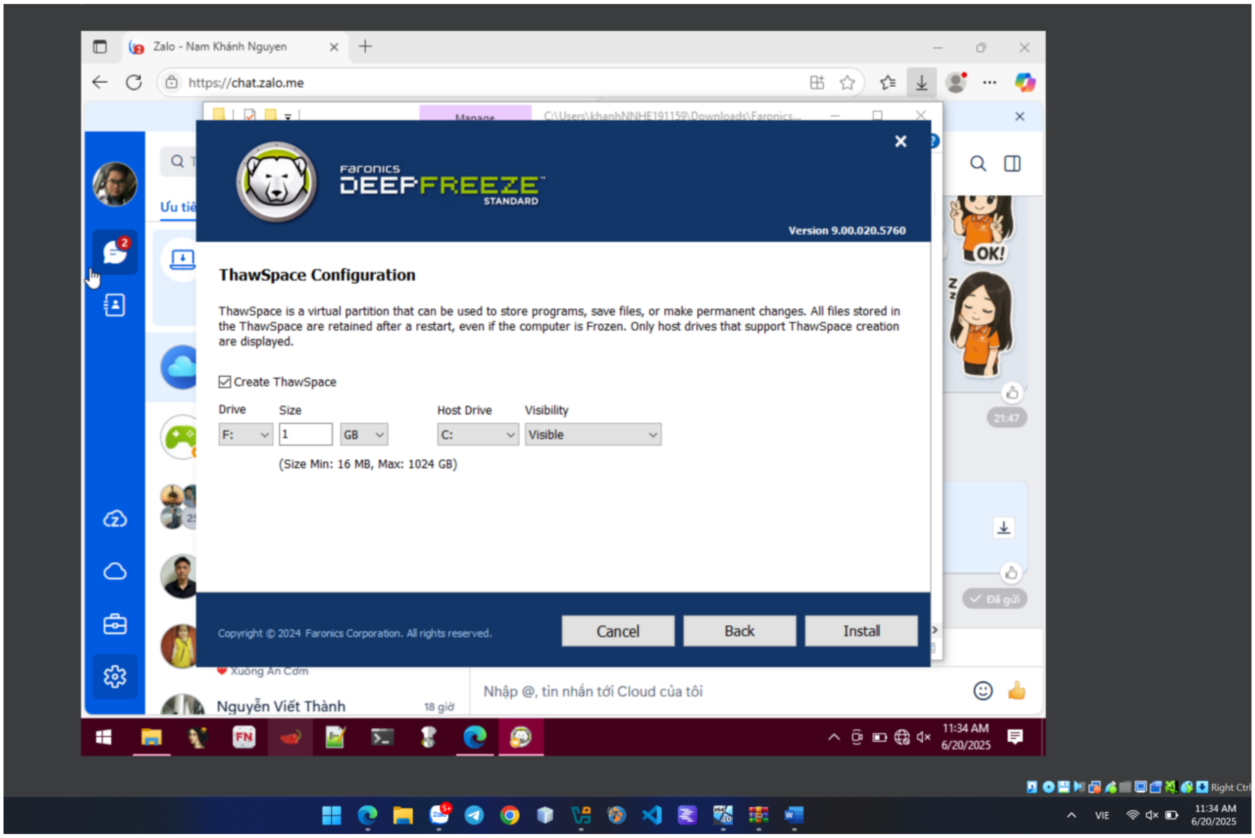
□ Manage Virtual Memory

Always Thaw External Hard Drive

☑ USB ☑ IEEE 1394 (FireWire)

Copyright © 2024 Faronics Corporation. All rights reserved.

ThawnSpace Configuration



ThawSpace Configuration

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. Only host drives that support ThawSpace creation are displayed.

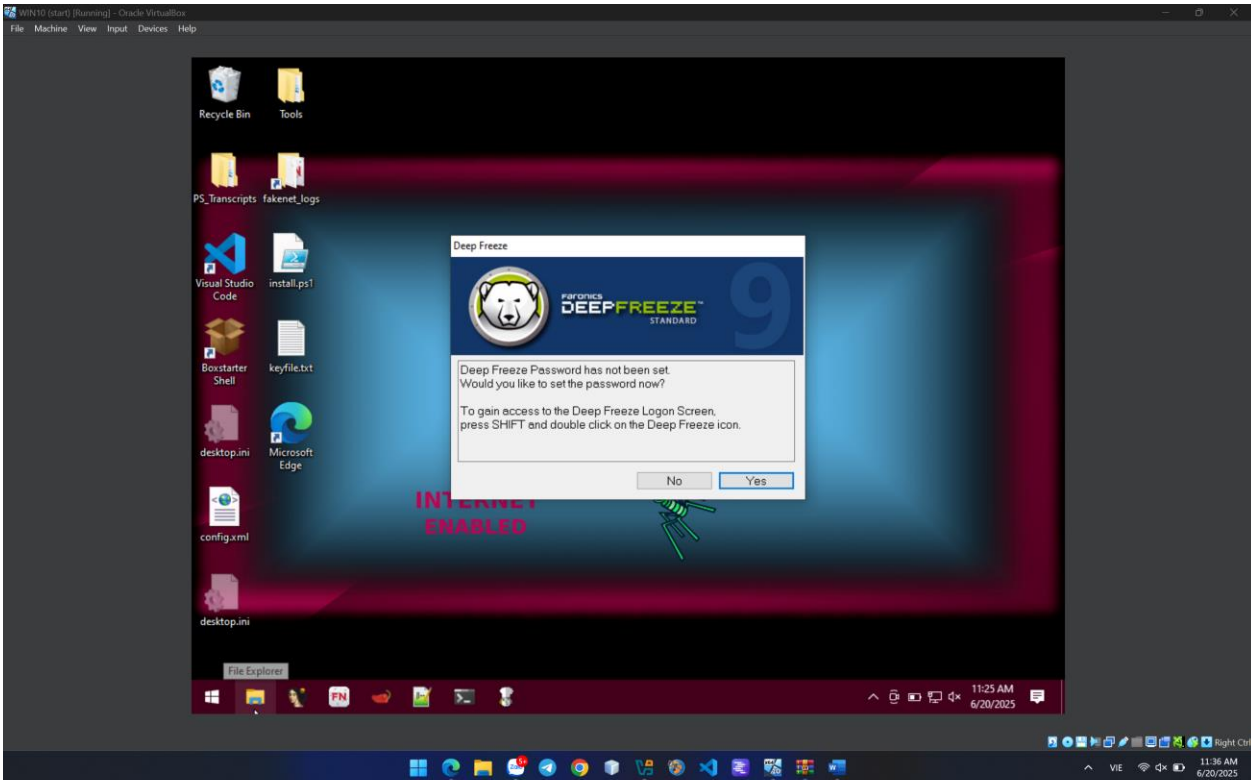
☑ Create ThawSpace

Drive	Size		Host Drive	Visibility
F:	1	GB	C:	Visible

(Size Min: 16 MB, Max: 1024 GB)

Copyright © 2024 Faronics Corporation. All rights reserved.

Setting Password

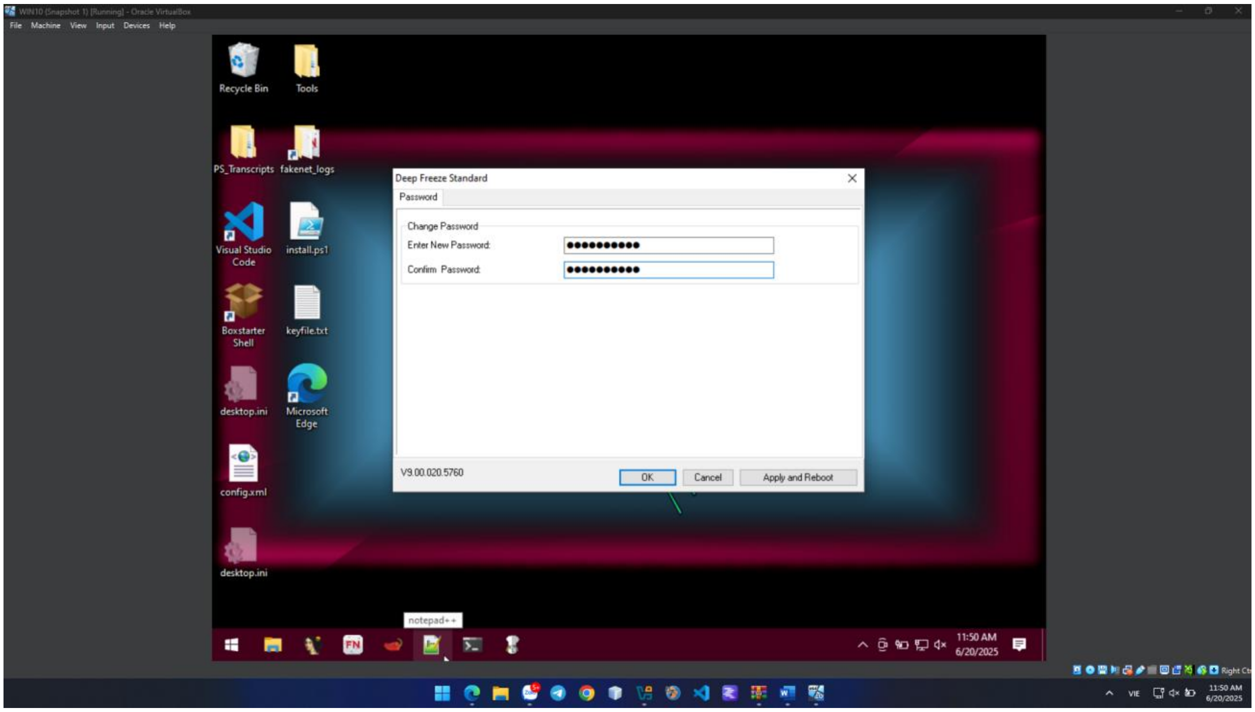


Deep Freeze

Deep Freeze Password has not been set.
Would you like to set the password now?

To gain access to the Deep Freeze Logon Screen, press SHIFT and double click on the Deep Freeze icon.

No Yes



Deep Freeze Standard

Password

Change Password

Enter New Password: ●●●●●●●●●●●

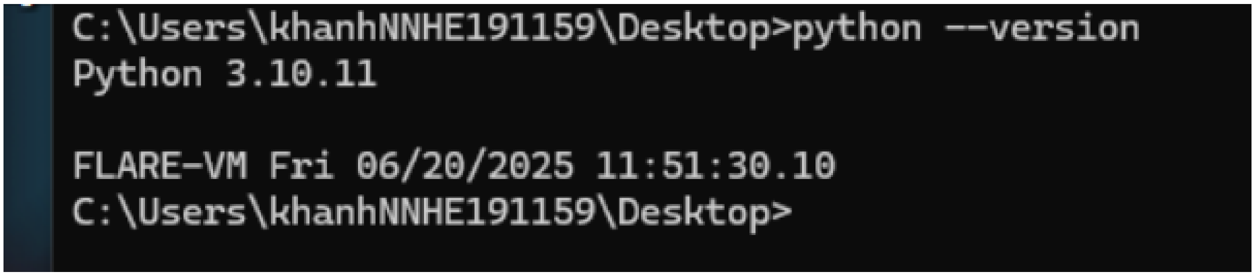
Confirm Password: ●●●●●●●●●●●

V9.00.020.5760

OK Cancel Apply and Reboot

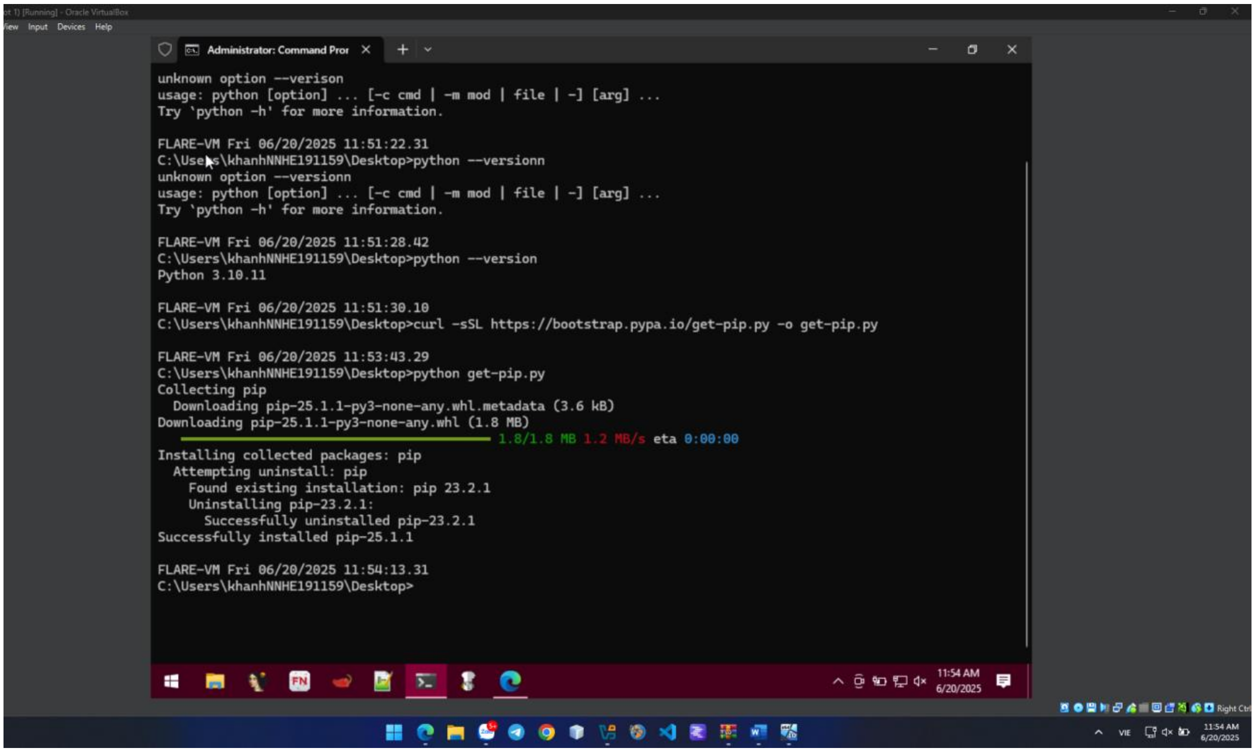
Prepare for Ransomware analysis.

Install python 3.10



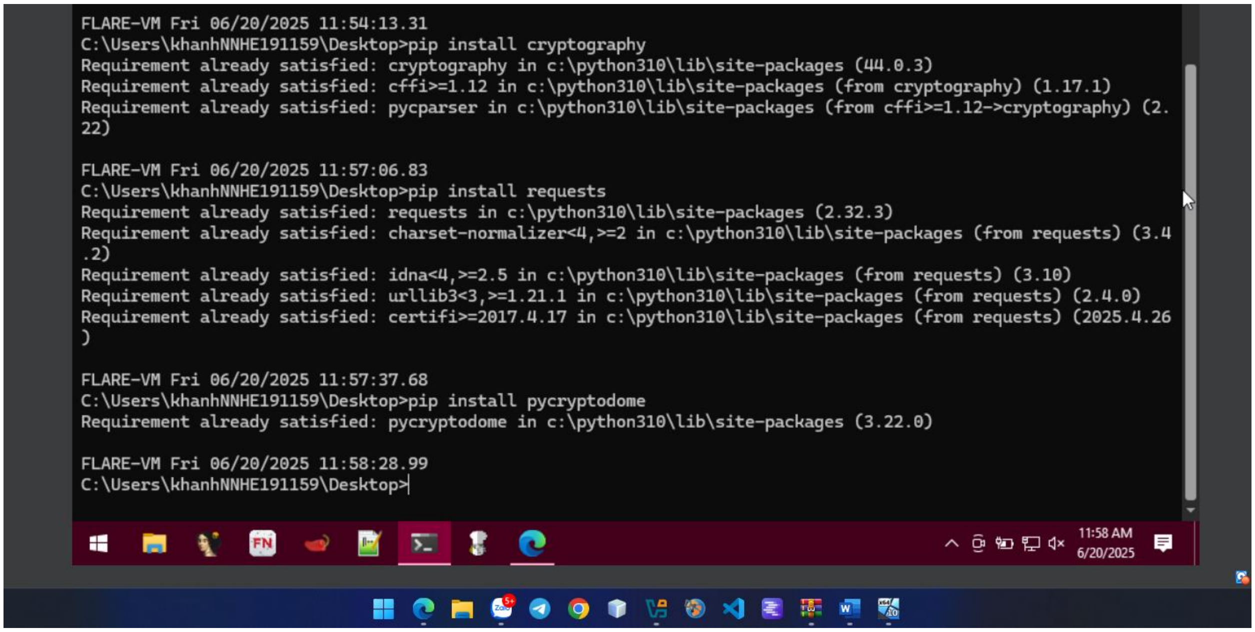
```
C:\Users\khanhNNHE191159\Desktop>python --version
Python 3.10.11

FLARE-VM Fri 06/20/2025 11:51:30.10
C:\Users\khanhNNHE191159\Desktop>
```

Install pip

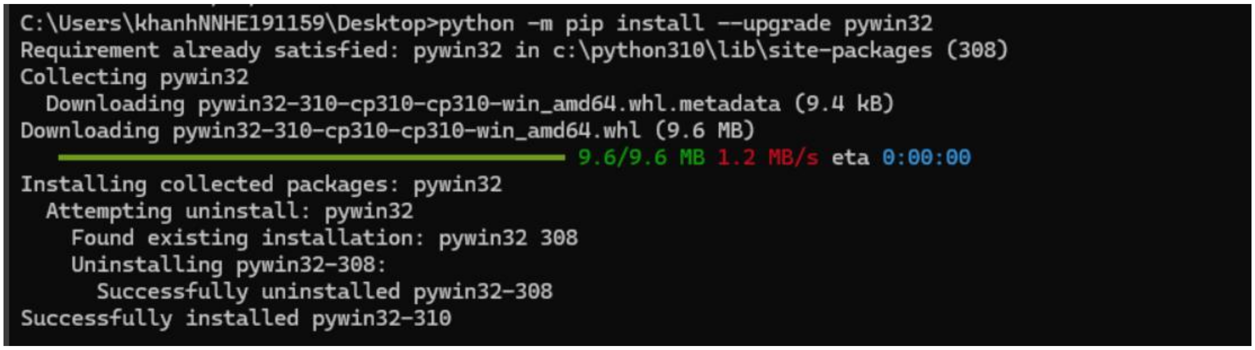


```
unknown option --verison
usage: python [option] ... [-c cmd | -m mod | file | -] [arg] ...
Try `python -h' for more information.

FLARE-VM Fri 06/20/2025 11:51:22.31
C:\Users\khanhNNHE191159\Desktop>python --versionn
unknown option --versionn
usage: python [option] ... [-c cmd | -m mod | file | -] [arg] ...
Try `python -h' for more information.

FLARE-VM Fri 06/20/2025 11:51:28.42
C:\Users\khanhNNHE191159\Desktop>python --version
Python 3.10.11

FLARE-VM Fri 06/20/2025 11:51:30.10
C:\Users\khanhNNHE191159\Desktop>curl -sSL https://bootstrap.pypa.io/get-pip.py -o get-pip.py

FLARE-VM Fri 06/20/2025 11:53:43.29
C:\Users\khanhNNHE191159\Desktop>python get-pip.py
Collecting pip
  Downloading pip-25.1.1-py3-none-any.whl.metadata (3.6 kB)
Downloading pip-25.1.1-py3-none-any.whl (1.8 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.8/1.8 MB 1.2 MB/s eta 0:00:00
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 23.2.1
    Uninstalling pip-23.2.1:
      Successfully uninstalled pip-23.2.1
Successfully installed pip-25.1.1

FLARE-VM Fri 06/20/2025 11:54:13.31
C:\Users\khanhNNHE191159\Desktop>
```

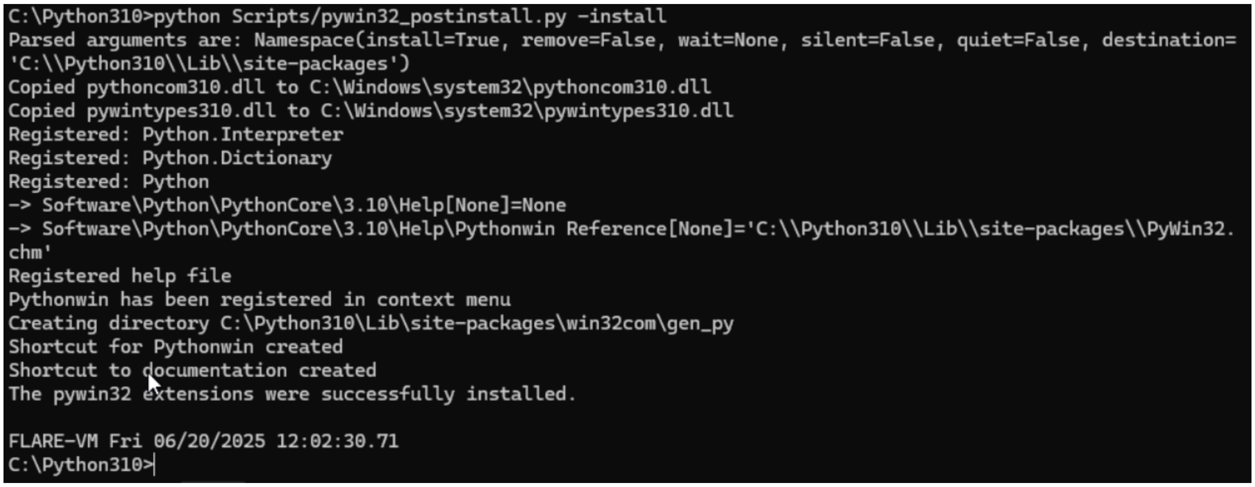
Install support library packages: cryptography, win32gui, requests, pycryptodome.



```
FLARE-VM Fri 06/20/2025 11:54:13.31
C:\Users\khanhNNHE191159\Desktop>pip install cryptography
Requirement already satisfied: cryptography in c:\python310\lib\site-packages (44.0.3)
Requirement already satisfied: cffi>=1.12 in c:\python310\lib\site-packages (from cryptography) (1.17.1)
Requirement already satisfied: pycparser in c:\python310\lib\site-packages (from cffi>=1.12->cryptography) (2.
22)

FLARE-VM Fri 06/20/2025 11:57:06.83
C:\Users\khanhNNHE191159\Desktop>pip install requests
Requirement already satisfied: requests in c:\python310\lib\site-packages (2.32.3)
Requirement already satisfied: charset-normalizer<4,>=2 in c:\python310\lib\site-packages (from requests) (3.4
.2)
Requirement already satisfied: idna<4,>=2.5 in c:\python310\lib\site-packages (from requests) (3.10)
Requirement already satisfied: urllib3<3,>=1.21.1 in c:\python310\lib\site-packages (from requests) (2.4.0)
Requirement already satisfied: certifi>=2017.4.17 in c:\python310\lib\site-packages (from requests) (2025.4.26
)

FLARE-VM Fri 06/20/2025 11:57:37.68
C:\Users\khanhNNHE191159\Desktop>pip install pycryptodome
Requirement already satisfied: pycryptodome in c:\python310\lib\site-packages (3.22.0)

FLARE-VM Fri 06/20/2025 11:58:28.99
C:\Users\khanhNNHE191159\Desktop>
```



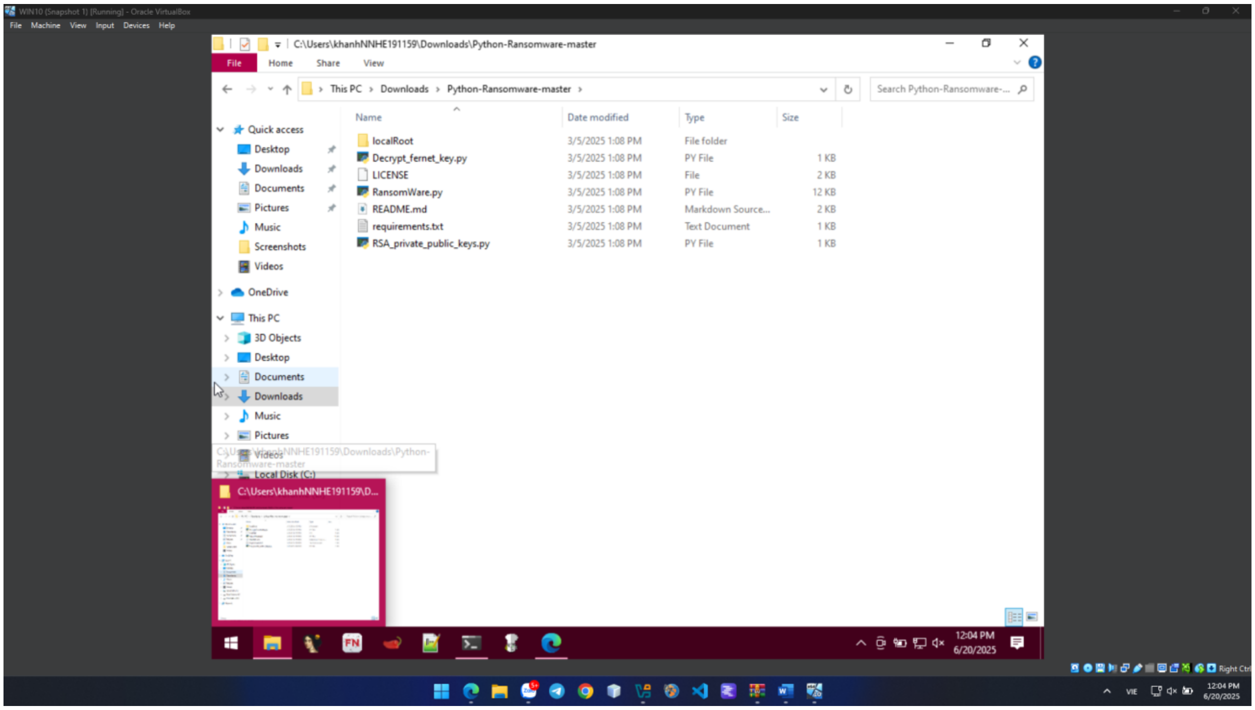
```
C:\Users\khanhNNHE191159\Desktop>python -m pip install --upgrade pywin32
Requirement already satisfied: pywin32 in c:\python310\lib\site-packages (308)
Collecting pywin32
  Downloading pywin32-310-cp310-cp310-win_amd64.whl.metadata (9.4 kB)
Downloading pywin32-310-cp310-cp310-win_amd64.whl (9.6 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 9.6/9.6 MB 1.2 MB/s eta 0:00:00
Installing collected packages: pywin32
  Attempting uninstall: pywin32
    Found existing installation: pywin32 308
    Uninstalling pywin32-308:
      Successfully uninstalled pywin32-308
Successfully installed pywin32-310
```



```
C:\Python310>python Scripts/pywin32_postinstall.py -install
Parsed arguments are: Namespace(install=True, remove=False, wait=None, silent=False, quiet=False, destination=
'C:\\Python310\\Lib\\site-packages')
Copied pythoncom310.dll to C:\Windows\system32\pythoncom310.dll
Copied pywintypes310.dll to C:\Windows\system32\pywintypes310.dll
Registered: Python.Interpreter
Registered: Python.Dictionary
Registered: Python
-> Software\Python\PythonCore\3.10\Help[None]=None
-> Software\Python\PythonCore\3.10\Help\Pythonwin Reference[None]='C:\\Python310\\Lib\\site-packages\\PyWin32.
chm'
Registered help file
Pythonwin has been registered in context menu
Creating directory C:\Python310\Lib\site-packages\win32com\gen_py
Shortcut for Pythonwin created
Shortcut to documentation created
The pywin32 extensions were successfully installed.

FLARE-VM Fri 06/20/2025 12:02:30.71
C:\Python310>
```

Because I installed recently so let move to next stage.

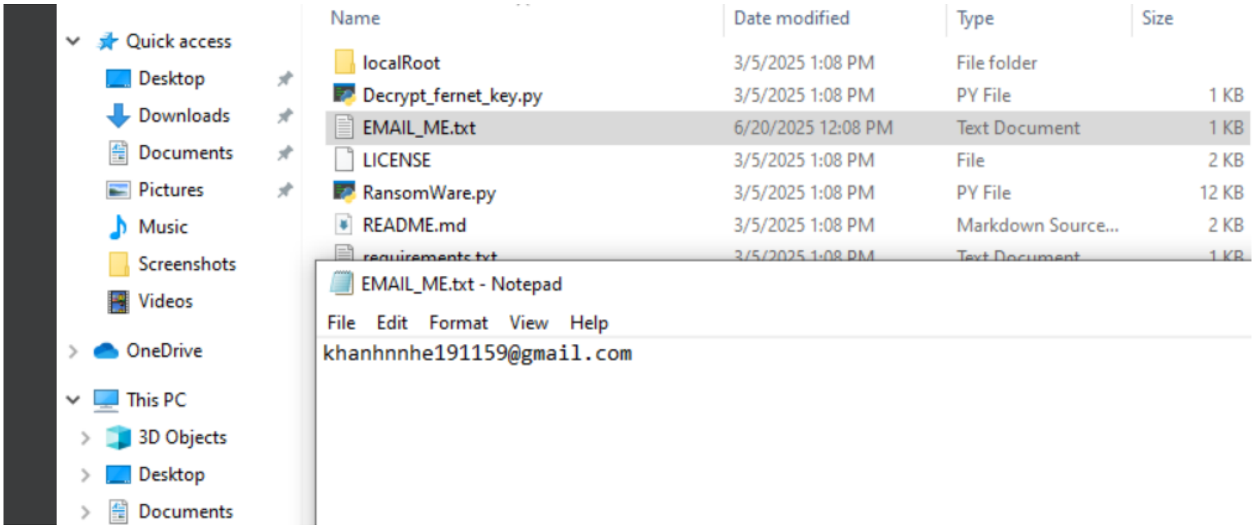
Download Source Ransomware here: https://github.com/ncorbuk/Python-Ransomware/
After unpacking, we have the following files:



C:\Users\khanhNNHE191159\Downloads\Python-Ransomware-master

Name	Date modified	Type	Size
localRoot	3/5/2025 1:08 PM	File folder	
Decrypt_fernet_key.py	3/5/2025 1:08 PM	PY File	1 KB
LICENSE	3/5/2025 1:08 PM	File	2 KB
RansomWare.py	3/5/2025 1:08 PM	PY File	12 KB
README.md	3/5/2025 1:08 PM	Markdown Source...	2 KB
requirements.txt	3/5/2025 1:08 PM	Text Document	1 KB
RSA_private_public_keys.py	3/5/2025 1:08 PM	PY File	1 KB

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

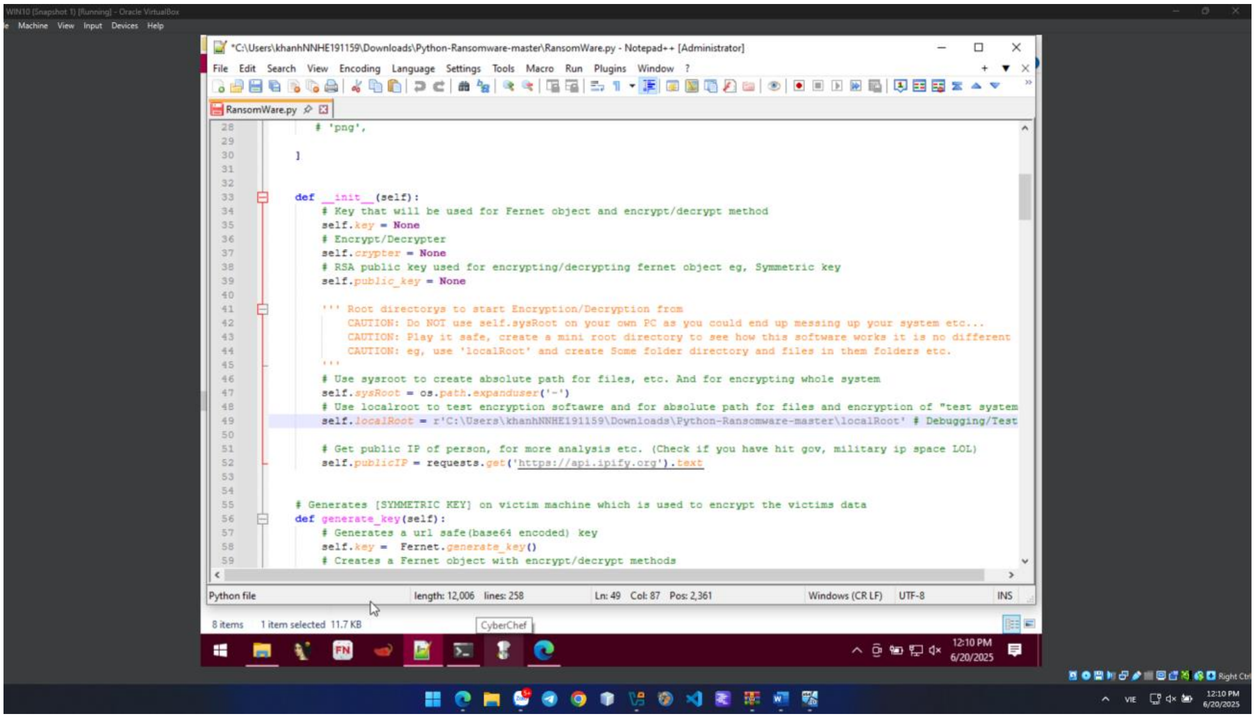


Name	Date modified	Type	Size
localRoot	3/5/2025 1:08 PM	File folder	
Decrypt_fernet_key.py	3/5/2025 1:08 PM	PY File	1 KB
EMAIL_ME.txt	6/20/2025 12:08 PM	Text Document	1 KB
LICENSE	3/5/2025 1:08 PM	File	2 KB
RansomWare.py	3/5/2025 1:08 PM	PY File	12 KB
README.md	3/5/2025 1:08 PM	Markdown Source...	2 KB
requirements.txt	3/5/2025 1:08 PM	Text Document	1 KB

EMAIL_ME.txt - Notepad

```
khanhnnhe191159@gmail.com
```

edit some content in the RansomWare.py file

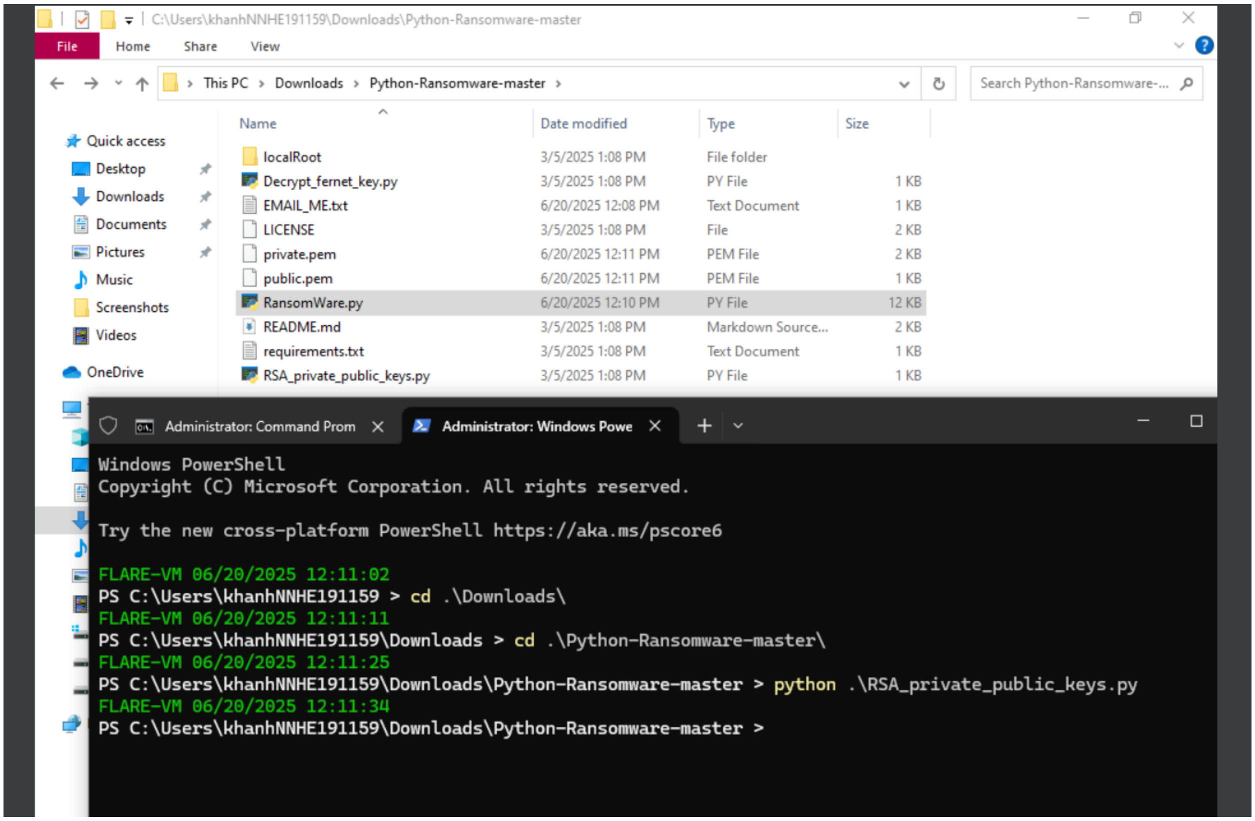


*C:\Users\khanhNNHE191159\Downloads\Python-Ransomware-master\RansomWare.py - Notepad++ [Administrator]

```python
            # 'png',

        ]


    def __init__(self):
        # Key that will be used for Fernet object and encrypt/decrypt method
        self.key = None
        # Encrypt/Decrypter
        self.crypter = None
        # RSA public key used for encrypting/decrypting fernet object eg, Symmetric key
        self.public_key = None

        ''' 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\khanhNNHE191159\Downloads\Python-Ransomware-master\localRoot' # Debugging/Test

        # 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


    # Generates [SYMMETRIC KEY] on victim machine which is used to encrypt the victims data
    def generate_key(self):
        # Generates a url safe(base64 encoded) key
        self.key =  Fernet.generate_key()
        # Creates a Fernet object with encrypt/decrypt methods
```

Python file
length: 12,006 lines: 258
Ln: 49 Col: 87 Pos: 2,361
Windows (CR LF)
UTF-8
INS
8 items 1 item selected 11.7 KB
CyberChef
12:10 PM
6/20/2025

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

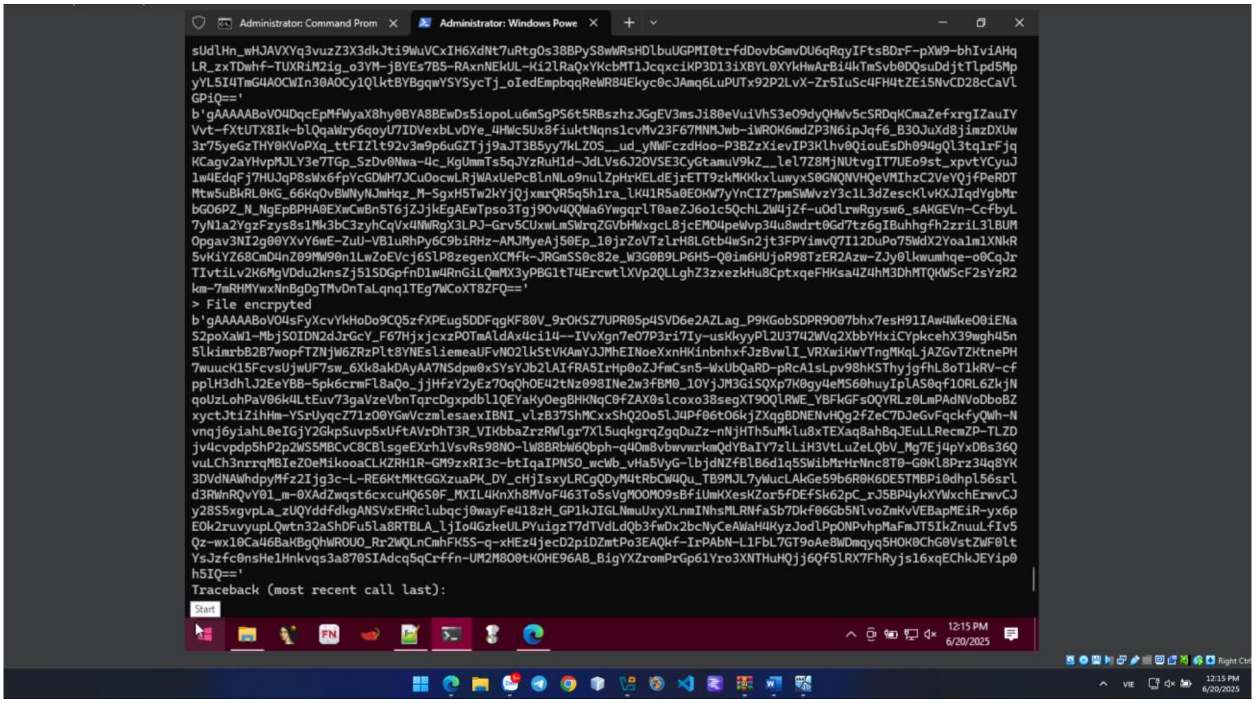


C:\Users\khanhNNHE191159\Downloads\Python-Ransomware-master

Name	Date modified	Type	Size
localRoot	3/5/2025 1:08 PM	File folder	
Decrypt_fernet_key.py	3/5/2025 1:08 PM	PY File	1 KB
EMAIL_ME.txt	6/20/2025 12:08 PM	Text Document	1 KB
LICENSE	3/5/2025 1:08 PM	File	2 KB
private.pem	6/20/2025 12:11 PM	PEM File	2 KB
public.pem	6/20/2025 12:11 PM	PEM File	1 KB
RansomWare.py	6/20/2025 12:10 PM	PY File	12 KB
README.md	3/5/2025 1:08 PM	Markdown Source...	2 KB
requirements.txt	3/5/2025 1:08 PM	Text Document	1 KB
RSA_private_public_keys.py	3/5/2025 1:08 PM	PY File	1 KB

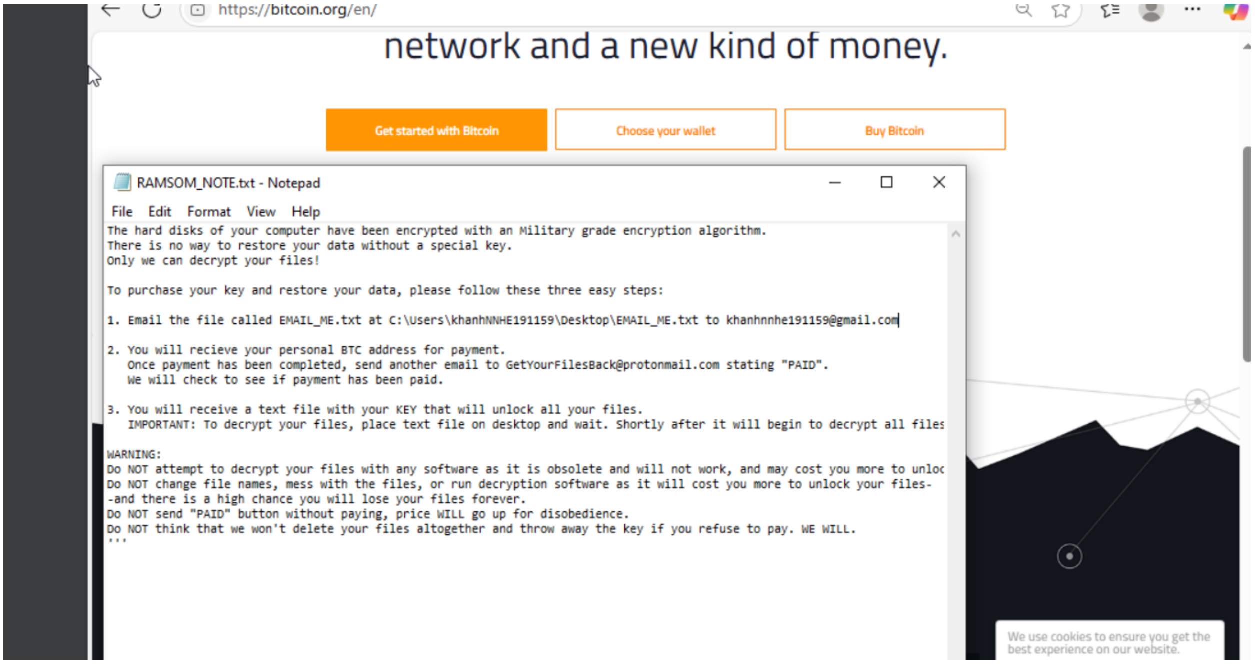
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

FLARE-VM 06/20/2025 12:11:02
PS C:\Users\khanhNNHE191159 > cd .\Downloads\
FLARE-VM 06/20/2025 12:11:11
PS C:\Users\khanhNNHE191159\Downloads > cd .\Python-Ransomware-master\
FLARE-VM 06/20/2025 12:11:25
PS C:\Users\khanhNNHE191159\Downloads\Python-Ransomware-master > python .\RSA_private_public_keys.py
FLARE-VM 06/20/2025 12:11:34
PS C:\Users\khanhNNHE191159\Downloads\Python-Ransomware-master >
```

We will run the RansomWare.py file to test:

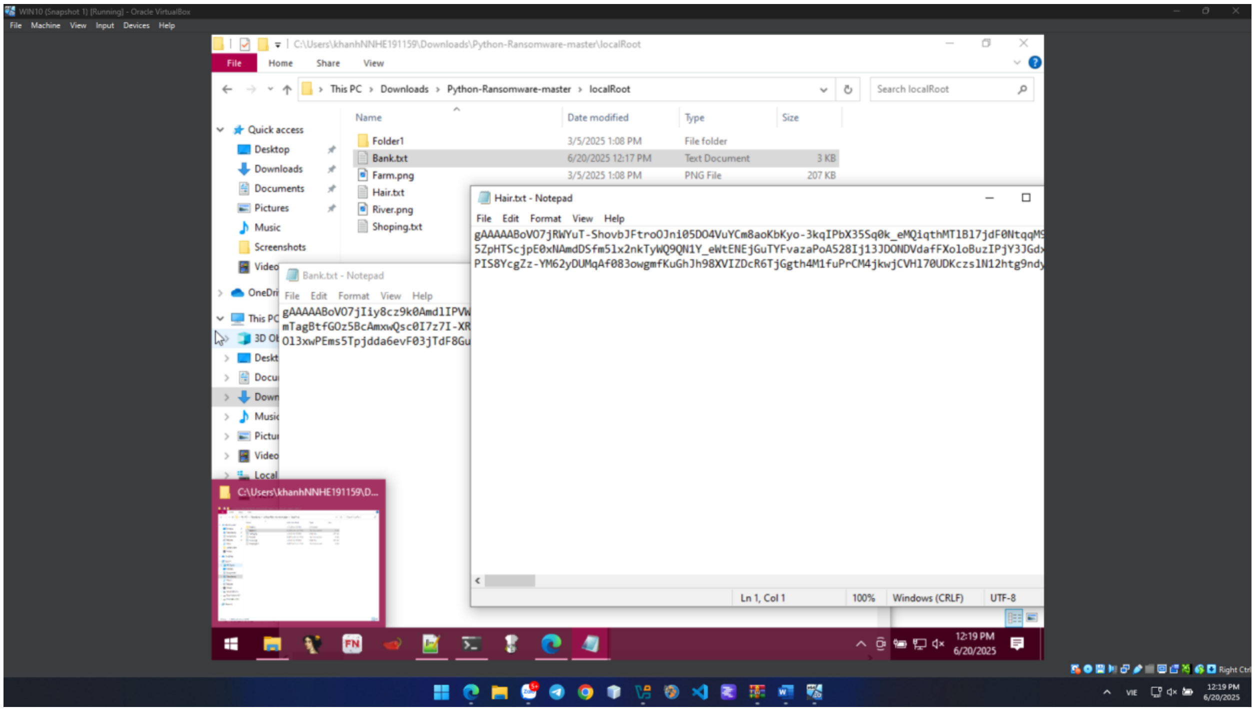


```
sUdlHn_wHJAVXYq3vuzZ3X3dkJti9WuVCxIH6XdNt7uRtgOs38BPyS8wWRsHDlbuUGPMI0trfdDovbGmvDU6qRqyIFtsBDrF-pXW9-bhIviAHq
LR_zxTDwhf-TUXRiM2ig_o3YM-jBYEs7B5-RAxnNEkUL-Ki2lRaQxYKcbMT1JcqxciKP3D13iXBYL0XYkHwArBi4kTmSvb0DQsuDdjtTlpd5Mp
yYL5I4TmG4AOCWIn30AOCy1QlktBYBgqwYSYSycTj_oIedEmpbqqReWR84Ekyc0cJAmq6LuPUTx92P2LvX-Zr5IuSc4FH4tZEi5NvCD28cCaVl
GPiQ=='
b'gAAAAABoVO4DqcEpMfWyaX8hy0BYA8BEwDs5iopoLu6mSgPS6t5RBszhzJGgEV3msJi80eVuiVhS3eO9dyQHWv5cSRDqKCmaZefxrgIZauIY
Vvt-fXtUTX8Ik-blQqaWry6qoyU7IDVexbLvDYe_4HWc5Ux8fiuktNqns1cvMv23F67MNMJwb-iWROK6mdZP3N6ipJqf6_B3OJuXd8jimzDXUw
3r75yeGzTHY0KVoPXq_ttFIZlt92v3m9p6uGZTjj9aJT3B5yy7kLZOS__ud_yNWFczdHoo-P3BZzXievIP3Klhv0QiouEsDh094gQl3tq1rFjq
KCagv2aYHvpMJLY3e7TGp_SzDv0Nwa-4c_KgUmmTs5qJYzRuH1d-JdLVs6J2OVSE3CyGtamuV9kZ__lel7Z8MjNUtvgIT7UEo9st_xpvtYCyuJ
1w4EdqFj7HUJqP8sWx6fpYcGDWH7JCuOocwLRjWAxUePcBlnNLo9nulZpHrKELdEjrETT9zkMKKkxluwyxS0GNQNVHQeVMIhzC2VeYQjfPeRDT
Mtw5uBkRL0KG_66KqOvBWNyNJmHqz_M-SgxH5Tw2kYjQjxmrQR5q5h1ra_lK41R5a0EOKW7yYnCIZ7pmSWWvzY3c1L3dZescKlvKXJIqdYgbMr
bGO6PZ_N_NgEpBPHA0EXwCwBn5T6jZJjkEgAEwTpso3Tgj9Ov4QQWa6YwgqrlT0aeZJ6o1c5QchL2W4jZf-uOdlrwRgysw6_sAKGEVn-CcfbyL
7yN1a2YgzFzys8s1Mk3bC3zyhCqVx4NWRgX3LPJ-Grv5CUxwLmSWrqZGVbHWxgcL8jcEMO4peWvp34u8wdrt0Gd7tz6gIBuhhgfh2zriL3lBUM
Opgav3NI2g00YXvY6wE-ZuU-VB1uRhPy6C9biRHz-AMJMyeAj50Ep_10jrZoVTzlrH8LGtb4wSn2jt3FPYimvQ7I12DuPo75WdX2Yoa1m1XNkR
5vKiYZ68CmD4nZ09MW90n1LwZoEVcj6SlP8zegenXCMfk-JRGmSS0c82e_W3G0B9LP6H5-Q0im6HUjoR98TzER2Azw-ZJy0lkwumhqe-o0CqJr
TIvtiLv2K6MgVDdu2knsZj51SDGpfnD1w4RnGiLQmMX3yPBG1tT4ErcwtlXVp2QLLghZ3zxezkHu8CptxqeFHKsa4Z4hM3DhMTQKWScF2sYzR2
km-7mRHMYwxNnBgDgTMvDnTaLqnq1TEg7WCoXT8ZFQ=='
> File encrpyted
b'gAAAAABoVO4sFyXcvYkHoDo9CQ5zfXPEug5DDFqgKF80V_9rOKSZ7UPR05p4SVD6e2AZLag_P9KGobSDPR9O07bhx7esH91IAw4WkeO0iENa
S2poXaW1-MbjSOIDN2dJrGcY_F67HjxjcxzPOTmAldAx4ci14--IVvXgn7eO7P3ri7Iy-usKkyyPl2U3742WVq2XbbYHxiCYpkcehX39wgh45n
5lkimrbB2B7wopfTZNjW6ZRzPlt8YNEsliemeaUFvNO2lkStVKAmYJJMhEINoeXxnHKinbnhxfJzBvwlI_VRXwiKwYTngMKqLjAZGvTZKtnePH
7wuucK15FcvsUjwUF7sw_6Xk8akDAyAA7NSdpw0xSYsYJb2lAIfRA5IrHp0oZJfmCsn5-WxUbQaRD-pRcA1sLpv98hKSThyjgfhL8oT1kRV-cf
pplH3dhlJ2EeYBB-5pk6crmFl8aQo_jjHfzY2yEz7OqQhOE42tNz098INe2w3fBM0_1OYjJM3GiSQXp7K0gy4eMS60huyIplAS0qf1ORL6ZkjN
qoUzLohPaV06k4LtEuv73gaVzeVbnTqrcDgxpdbl1QEYaKyOegBHKNqC0fZAX0slcoxo38segXT9OQlRWE_YBFkGFsOQYRLz0LmPAdNVoDboBZ
xyctJtiZihHm-YSrUyqcZ71zO0YGwVczmlesaexIBNI_vlzB37ShMCxxShQ2Oo5lJ4Pf06tO6kjZXqgBDNENvHQg2fZeC7DJeGvFqckfyQWh-N
vnqj6yiahL0eIGjY2GkpSuvp5xUftAVrDhT3R_VIKbbaZrzRWlgr7Xl5uqkgrqZgqDuZz-nNjHTh5uMklu8xTEXaq8ahBqJEuLLRecmZP-TLZD
jv4cvpdp5hP2p2WS5MBCvC8CBlsgeEXrh1VsvRs98NO-lW8BRbW6Qbph-q4Om8vbwvwrkmQdYBaIY7zlLiH3VtLuZeLQbV_Mg7Ej4pYxDBs36Q
vuLCh3nrrqMBIeZOeMikooaCLKZRH1R-GM9zxRI3c-btIqaIPNSO_wcWb_vHa5VyG-lbjdNZfBlB6d1q5SWibMrHrNnc8T0-G0Kl8Prz34q8YK
3DVdNAWhdpyMfz2Ijg3c-L-RE6KtMKtGGXzuaPK_DY_cHjIsxyLRCgQDyM4tRbCW4Qu_TB9MJL7yWucLAkGe59b6R0K6DE5TMBPi0dhpl56srl
d3RWnRQvY01_m-0XAdZwqst6cxcuHQ6S0F_MXIL4KnXh8MVoF463To5sVgMOOMO9sBfiUmKXesKZor5fDEfSk62pC_rJ5BP4ykXYWxchErwvCJ
y28S5xgvpLa_zUQYddfdkgANSVxEHRclubqcj0wayFe418zH_GP1kJIGLNmuUxyXLnmINhsMLRNfaSb7Dkf06Gb5NlvoZmKvVEBapMEiR-yx6p
EOk2ruvyupLQwtn32aShDFu5la8RTBLA_ljIo4GzkeULPYuigzT7dTVdLdQb3fwDx2bcNyCeAWaH4KyzJodlPpONPvhpMaFmJT5IkZnuuLfIv5
Qz-wx10Ca46BaKBgQhWROUO_Rr2WQLnCmhFK5S-q-xHEz4jecD2piDZmtPo3EAQkf-IrPAbN-L1FbL7GT9oAe8WDmqyq5HOK0ChG0VstZWF0lt
YsJzfc0nsHe1Hnkvqs3a870SIAdcq5qCrffn-UM2M8O0tKOHE96AB_BigYXZromPrGp61Yro3XNTHuHQjj6Qf5lRX7FhRyjs16xqEChkJEYip0
h5IQ=='
Traceback (most recent call last):
```

As a result, the Windows 10 machine has been encrypted


https://bitcoin.org/en/
network and a new kind of money.
Get started with Bitcoin
Choose your wallet
Buy Bitcoin
RAMSOM_NOTE.txt - Notepad
File Edit Format View Help
We use cookies to ensure you get the best experience on our website.

```
The hard disks of your computer have been encrypted with an Military grade encryption algorithm.
There is no way to restore your data without a special key.
Only we can decrypt your files!

To purchase your key and restore your data, please follow these three easy steps:

1. Email the file called EMAIL_ME.txt at C:\Users\khanhNNHE191159\Desktop\EMAIL_ME.txt to khanhnnhe191159@gmail.com

2. You will recieve your personal BTC address for payment.
   Once payment has been completed, send another email to GetYourFilesBack@protonmail.com stating "PAID".
   We will check to see if payment has been paid.

3. You will receive a text file with your KEY that will unlock all your files.
   IMPORTANT: To decrypt your files, place text file on desktop and wait. Shortly after it will begin to decrypt all files

WARNING:
Do NOT attempt to decrypt your files with any software as it is obsolete and will not work, and may cost you more to unloc
Do NOT change file names, mess with the files, or run decryption software as it will cost you more to unlock your files-
-and there is a high chance you will lose your files forever.
Do NOT send "PAID" button without paying, price WILL go up for disobedience.
Do NOT think that we won't delete your files altogether and throw away the key if you refuse to pay. WE WILL.
'''
```


WIN10 [Snapshot 1] [Running] - Oracle VirtualBox
File Machine View Input Devices Help
C:\Users\khanhNNHE191159\Downloads\Python-Ransomware-master\localRoot
File Home Share View
This PC › Downloads › Python-Ransomware-master › localRoot
Search localRoot
Quick access
Desktop
Downloads
Documents
Pictures
Music
Screenshots
Videos
OneDrive
This PC
Hair.txt - Notepad
Bank.txt - Notepad
File Edit Format View Help
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8
12:19 PM
6/20/2025

Name	Date modified	Type	Size
Folder1	3/5/2025 1:08 PM	File folder	
Bank.txt	6/20/2025 12:17 PM	Text Document	3 KB
Farm.png	3/5/2025 1:08 PM	PNG File	207 KB
Hair.txt			
River.png			
Shoping.txt			

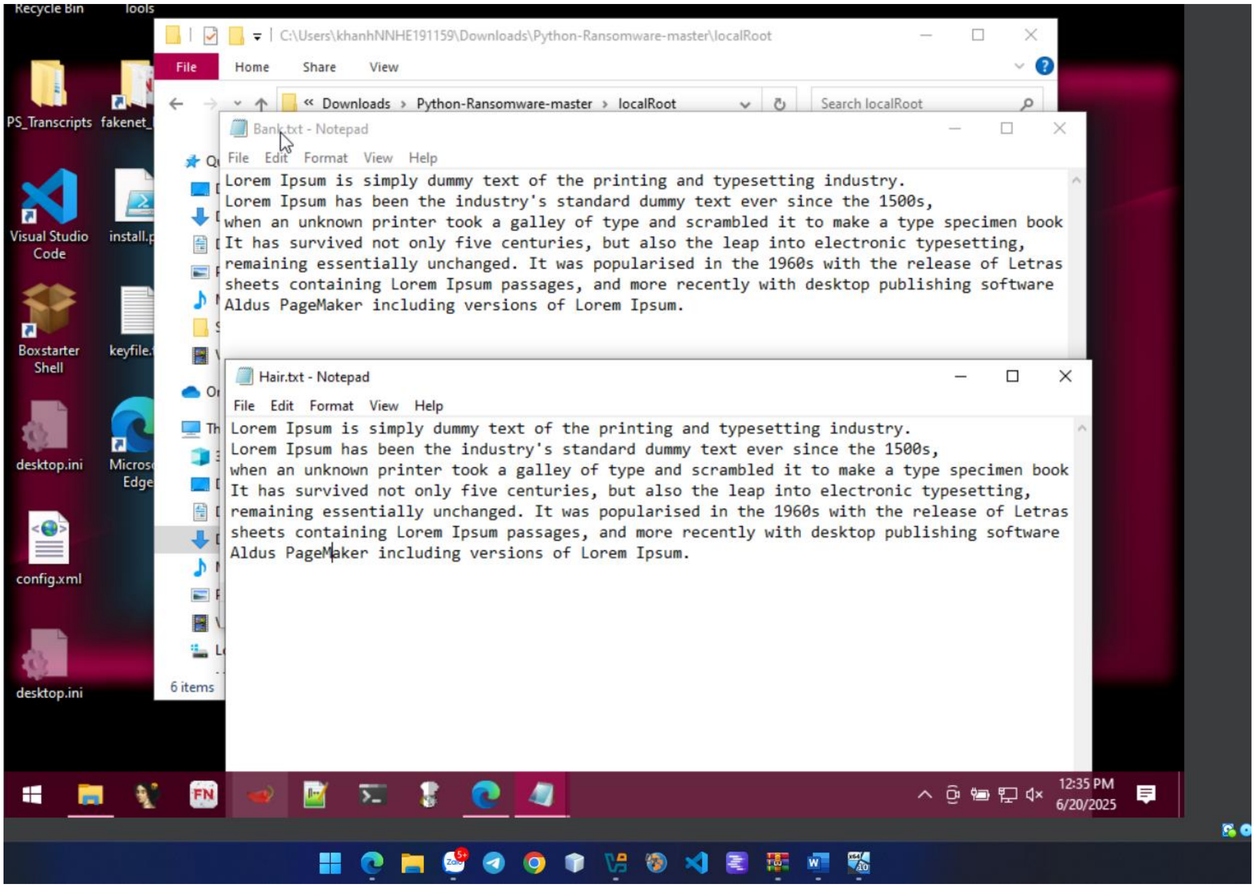
Hair.txt - Notepad

```
gAAAAABoVO7jRWYuT-ShovbJFtroOJni05DO4VuYCm8aoKbKyo-3kqIPbX35Sq0k_eMQiqthMT1B17jdF0NtqqM9
5ZpHTScjpE0xNAmdDSfm5lx2nkTyWQ9QN1Y_eWtENEjGuTYFvazaPoA528Ij13JDONDVdafFXoloBuzIPjY3JGdx
PIS8YcgZz-YM62yDUMqAf083owgmfKuGhJh98XVIZDcR6TjGgth4M1fuPrCM4jkwjCVHl70UDKczslN12htg9ndy
```

Bank.txt - Notepad

```
gAAAAABoVO7jIiy8cz9k0AmdlIPVW
mTagBtfGOz5BcAmxwQsc0I7z7I-XR
O13xwPEms5Tpjdda6evF03jTdF8Gu
```

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.


C:\Users\khanhNNHE191159\Downloads\Python-Ransomware-master\localRoot
Downloads > Python-Ransomware-master > localRoot
Search localRoot
6 items
Bank.txt - Notepad
Hair.txt - Notepad
File Edit Format View Help
12:35 PM
6/20/2025

```
Lorem Ipsum is simply dummy text of the printing and typesetting industry.
Lorem Ipsum has been the industry's standard dummy text ever since the 1500s,
when an unknown printer took a galley of type and scrambled it to make a type specimen book
It has survived not only five centuries, but also the leap into electronic typesetting,
remaining essentially unchanged. It was popularised in the 1960s with the release of Letras
sheets containing Lorem Ipsum passages, and more recently with desktop publishing software
Aldus PageMaker including versions of Lorem Ipsum.
```

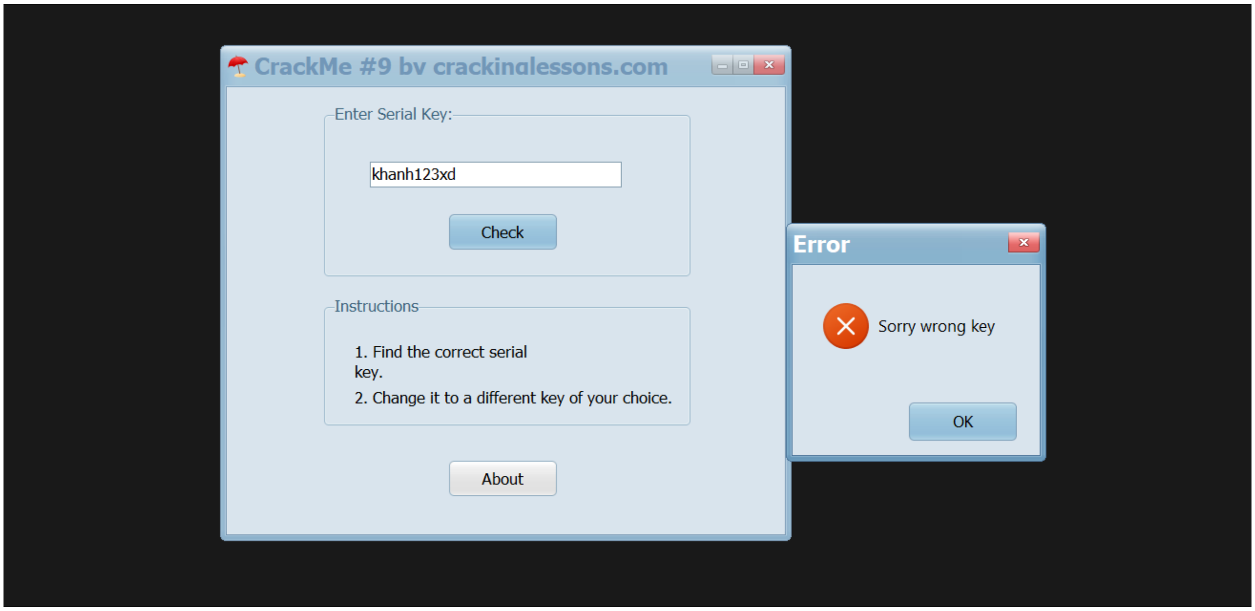
```
Lorem Ipsum is simply dummy text of the printing and typesetting industry.
Lorem Ipsum has been the industry's standard dummy text ever since the 1500s,
when an unknown printer took a galley of type and scrambled it to make a type specimen book
It has survived not only five centuries, but also the leap into electronic typesetting,
remaining essentially unchanged. It was popularised in the 1960s with the release of Letras
sheets containing Lorem Ipsum passages, and more recently with desktop publishing software
Aldus PageMaker including versions of Lorem Ipsum.
```

CRACK ME 9

To practice patching memory directly.

Objectives:

1. Find the correct serial key
2. Change it to a different key of your choice



CrackMe #9 by crackinglessons.com

Enter Serial Key: khanh123xd

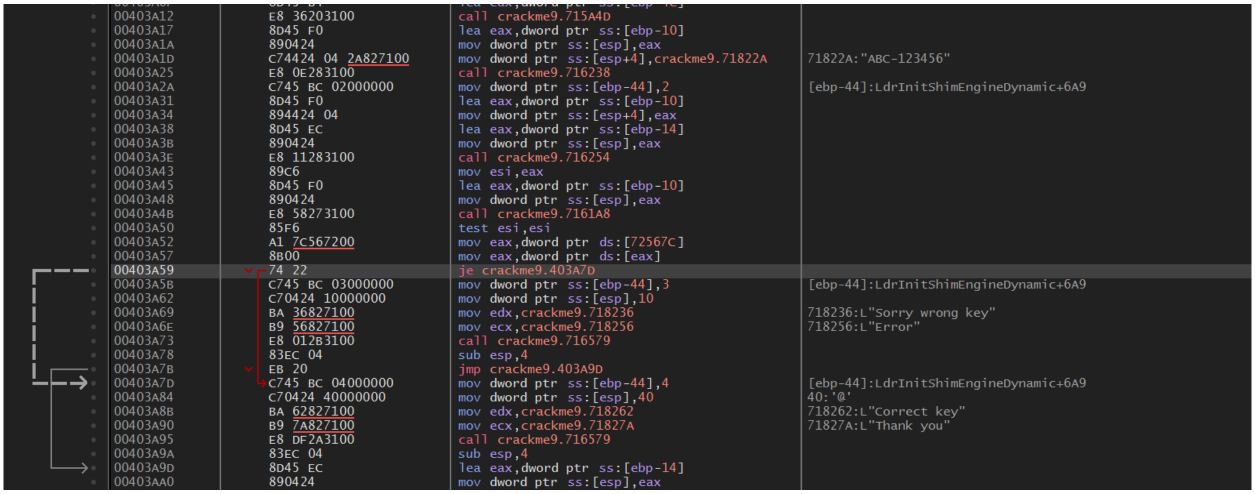
Instructions

1. Find the correct serial key.
2. Change it to a different key of your choice.

Error

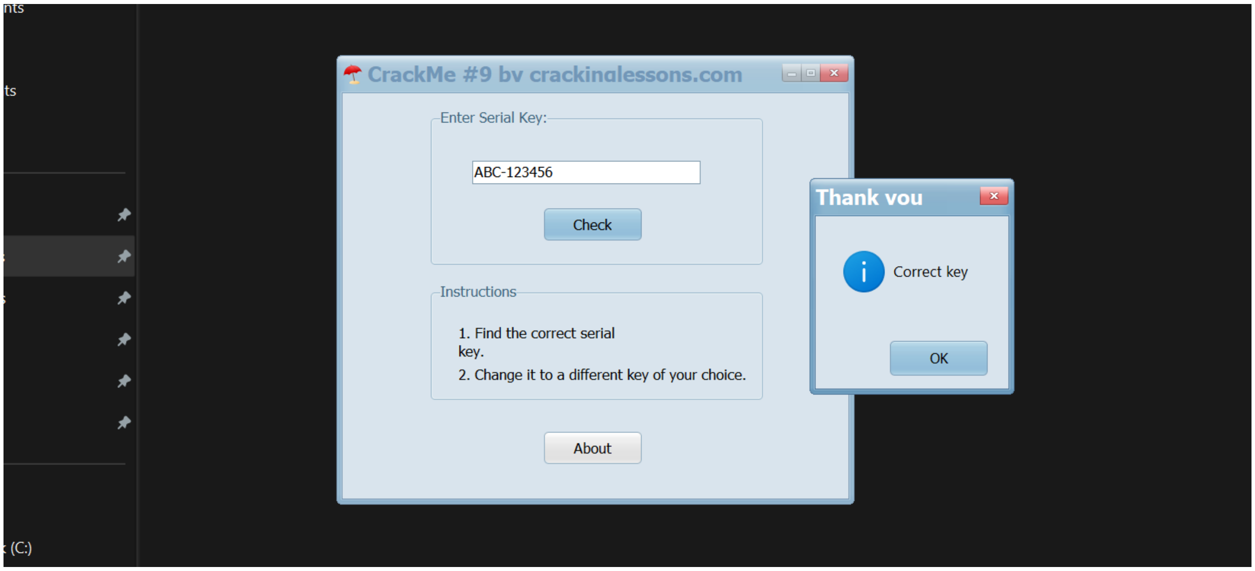
Sorry wrong key

First let move to to String reference to find the code corresponding.



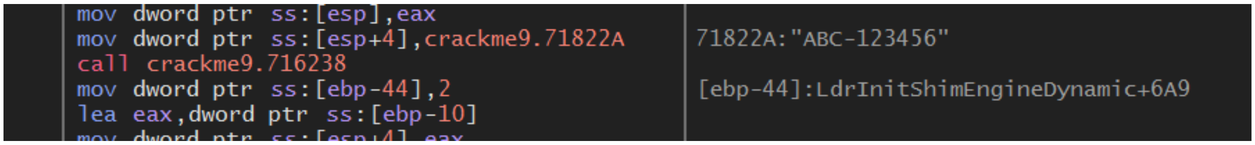
```
00403A12   E8 36203100         call crackme9.715A4D
00403A17   8D45 F0             lea eax,dword ptr ss:[ebp-10]
00403A1A   890424              mov dword ptr ss:[esp],eax
00403A1D   C74424 04 2A827100  mov dword ptr ss:[esp+4],crackme9.71822A     71822A:"ABC-123456"
00403A25   E8 0E283100         call crackme9.716238
00403A2A   C745 BC 02000000    mov dword ptr ss:[ebp-44],2                  [ebp-44]:LdrInitShimEngineDynamic+6A9
00403A31   8D45 F0             lea eax,dword ptr ss:[ebp-10]
00403A34   894424 04           mov dword ptr ss:[esp+4],eax
00403A38   8D45 EC             lea eax,dword ptr ss:[ebp-14]
00403A3B   890424              mov dword ptr ss:[esp],eax
00403A3E   E8 11283100         call crackme9.716254
00403A43   89C6                mov esi,eax
00403A45   8D45 F0             lea eax,dword ptr ss:[ebp-10]
00403A48   890424              mov dword ptr ss:[esp],eax
00403A4B   E8 58273100         call crackme9.7161A8
00403A50   85F6                test esi,esi
00403A52   A1 7C567200         mov eax,dword ptr ds:[72567C]
00403A57   8B00                mov eax,dword ptr ds:[eax]
00403A59   74 22               je crackme9.403A7D
00403A5B   C745 BC 03000000    mov dword ptr ss:[ebp-44],3                  [ebp-44]:LdrInitShimEngineDynamic+6A9
00403A62   C70424 10000000     mov dword ptr ss:[esp],10
00403A69   BA 36827100         mov edx,crackme9.718236                      718236:L"Sorry wrong key"
00403A6E   B9 56827100         mov ecx,crackme9.718256                      718256:L"Error"
00403A73   E8 012B3100         call crackme9.716579
00403A78   83EC 04             sub esp,4
00403A7B   EB 20               jmp crackme9.403A9D
00403A7D   C745 BC 04000000    mov dword ptr ss:[ebp-44],4                  [ebp-44]:LdrInitShimEngineDynamic+6A9
00403A84   C70424 40000000     mov dword ptr ss:[esp],40                    40:'@'
00403A8B   BA 62827100         mov edx,crackme9.718262                      718262:L"Correct key"
00403A90   B9 7A827100         mov ecx,crackme9.71827A                      71827A:L"Thank you"
00403A95   E8 DF2A3100         call crackme9.716579
00403A9A   83EC 04             sub esp,4
00403A9D   8D45 EC             lea eax,dword ptr ss:[ebp-14]
00403AA0   890424              mov dword ptr ss:[esp],eax
```

Notic string reference “ABC-123456”, it may be like the format of serial key, so I could insert this string again to verify and receice the true result.



CrackMe #9 by crackinglessons.com
Enter Serial Key:
ABC-123456
Check
Instructions
1. Find the correct serial key.
2. Change it to a different key of your choice.
About
Thank you
Correct key
OK

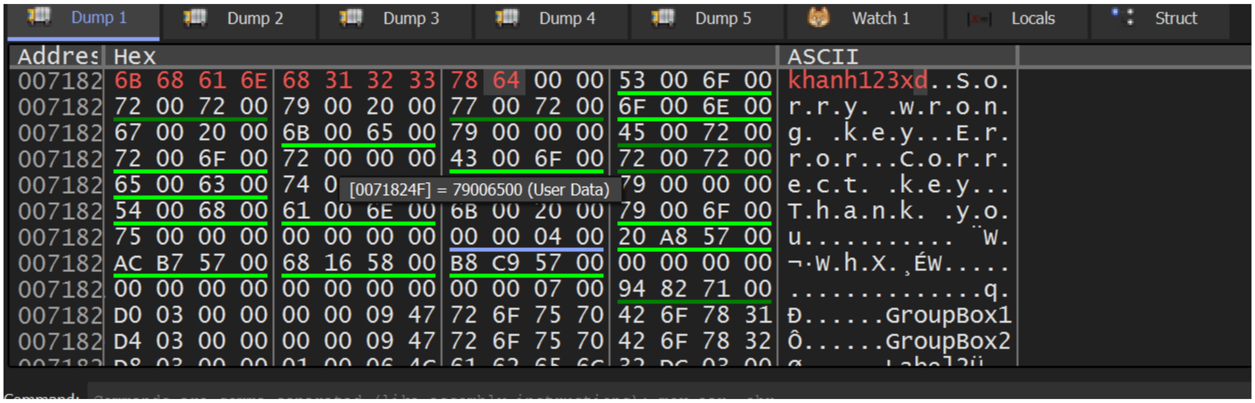
After successfully bypass serial key, we know that the line of code having string “ABC-123456” is assigning this value to the value for verify at the nex step.



```
mov dword ptr ss:[esp],eax
mov dword ptr ss:[esp+4],crackme9.71822A          71822A:"ABC-123456"
call crackme9.716238
mov dword ptr ss:[ebp-44],2                       [ebp-44]:LdrInitShimEngineDynamic+6A9
lea eax,dword ptr ss:[ebp-10]
mov dword ptr ss:[esp+4],eax
```

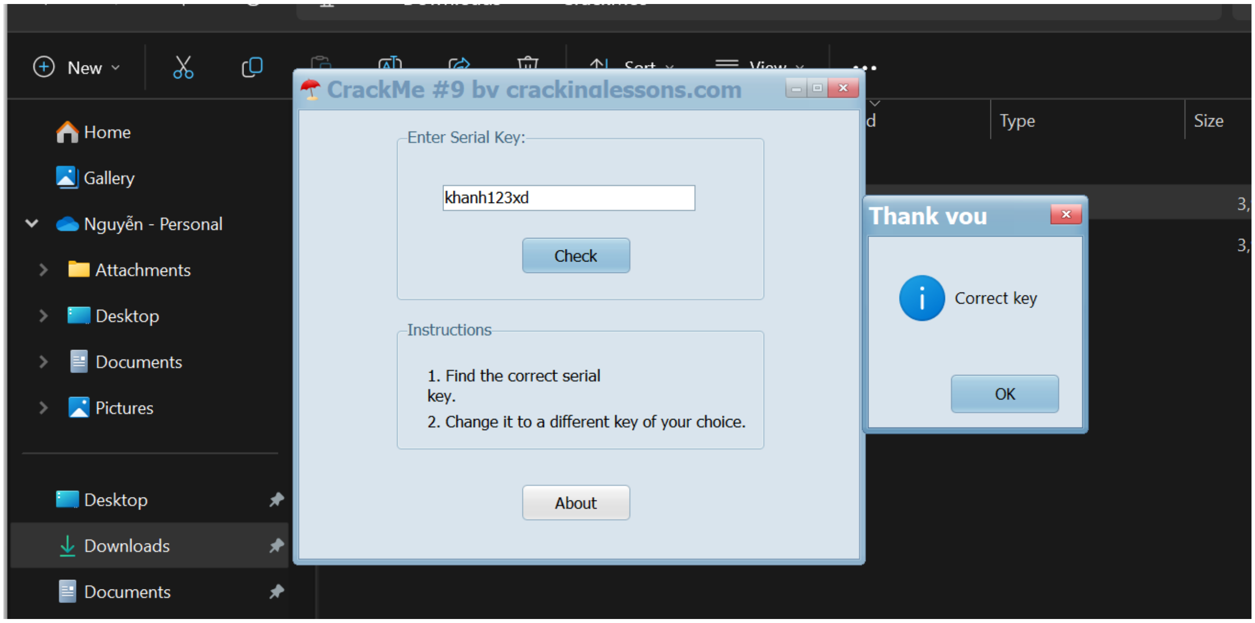
Address 0071822A contains the serial key, so i try to change the value of this address to change my own key.

ABC-123456 to khanh123xd



```
Addres Hex                                                  ASCII
007182 6B 68 61 6E 68 31 32 33 78 64 00 00 53 00 6F 00     khanh123xd..S.o.
007182 72 00 72 00 79 00 20 00 77 00 72 00 6F 00 6E 00     r.r.y. .w.r.o.n.
007182 67 00 20 00 6B 00 65 00 79 00 00 00 45 00 72 00     g. .k.e.y...E.r.
007182 72 00 6F 00 72 00 00 00 43 00 6F 00 72 00 72 00     r.o.r...C.o.r.r.
007182 65 00 63 00 74 0 [0071824F] = 79006500 (User Data) 79 00 00 00     e.c.t. .k.e.y...
007182 54 00 68 00 61 00 6E 00 6B 00 20 00 79 00 6F 00     T.h.a.n.k. .y.o.
007182 75 00 00 00 00 00 00 00 00 00 04 00 20 A8 57 00     u.......... ¨W.
007182 AC B7 57 00 68 16 58 00 B8 C9 57 00 00 00 00 00     ¬·W.h.X.¸ÉW.....
007182 00 00 00 00 00 00 00 00 00 00 07 00 94 82 71 00     ..............q.
007182 D0 03 00 00 00 00 09 47 72 6F 75 70 42 6F 78 31     Ð.......GroupBox1
007182 D4 03 00 00 00 00 09 47 72 6F 75 70 42 6F 78 32     Ô.......GroupBox2
```

Patch this file and verify again.



Enter Serial Key: khanh123xd

Instructions

1. Find the correct serial key.
2. Change it to a different key of your choice.

Correct key

DONE!!!