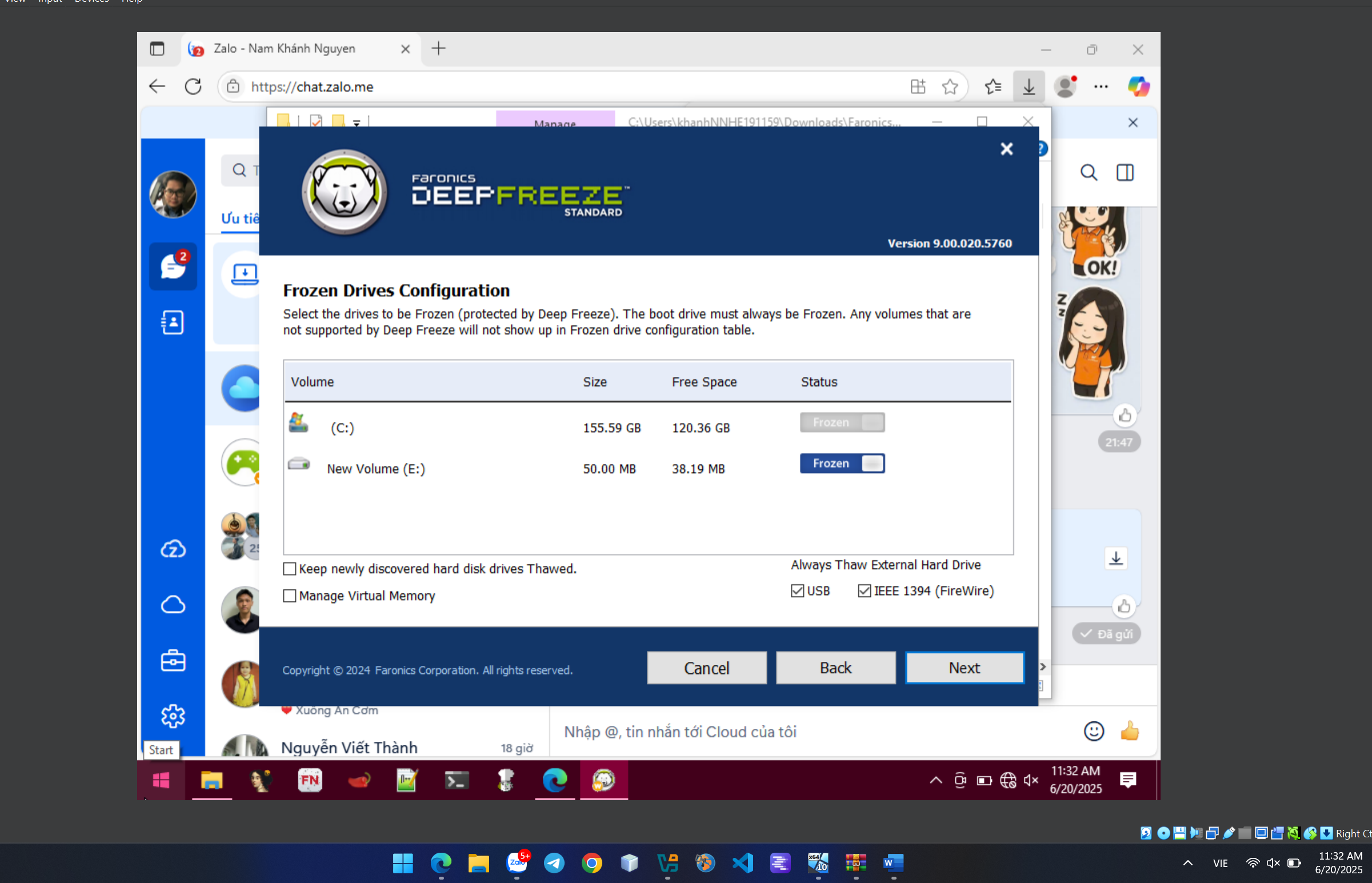
**KHANHNNHE191159**

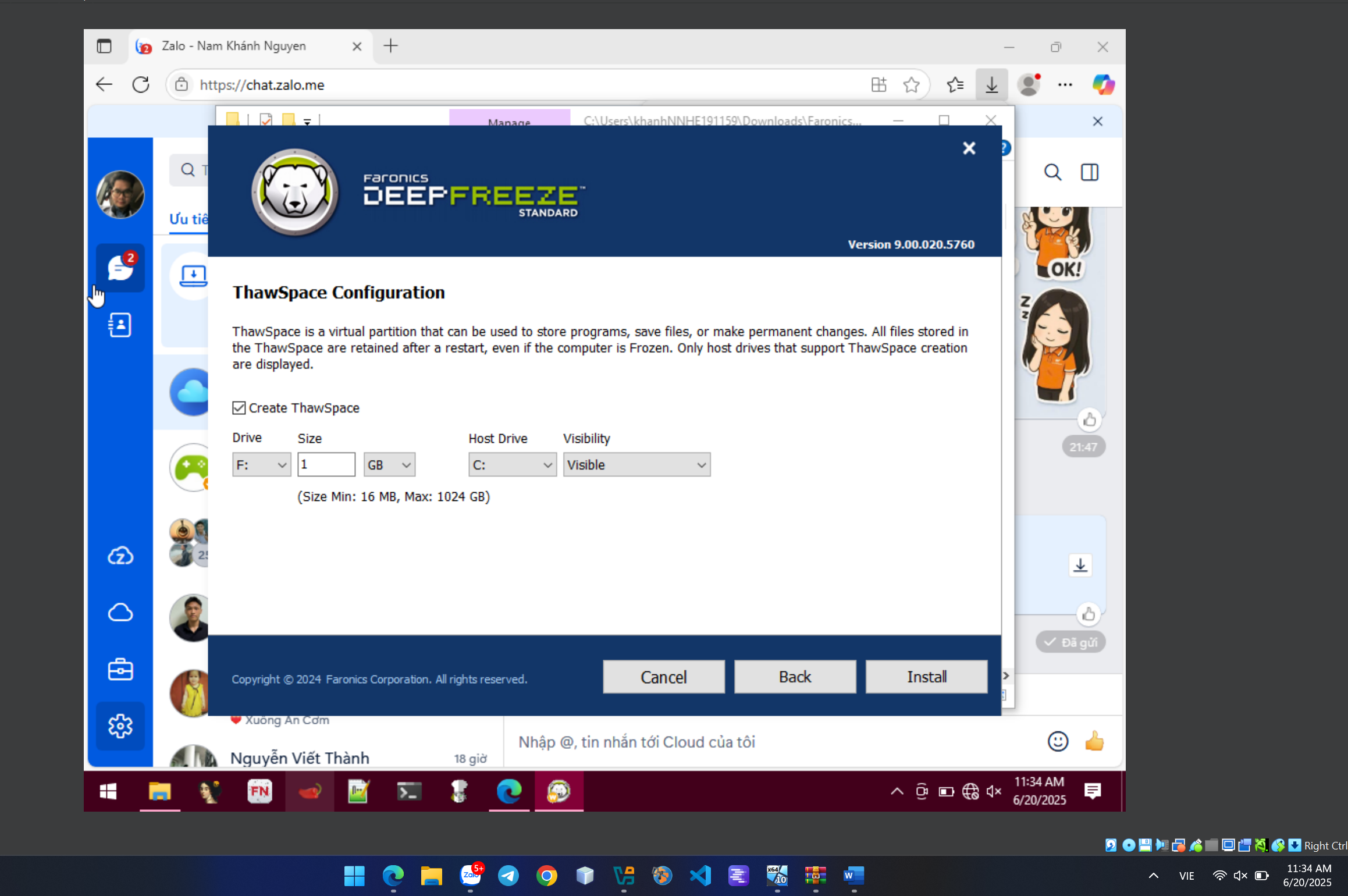
**NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302**

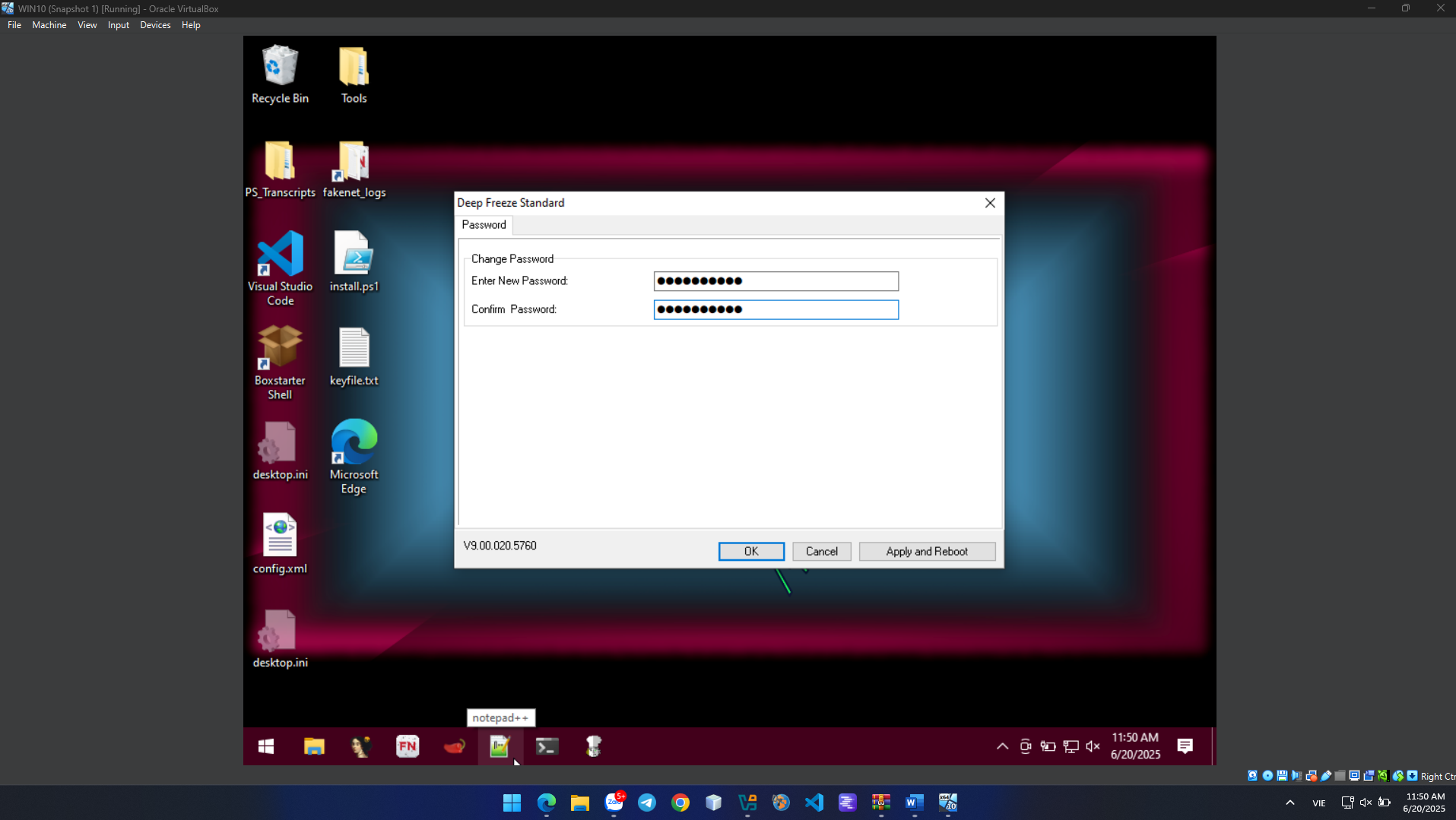
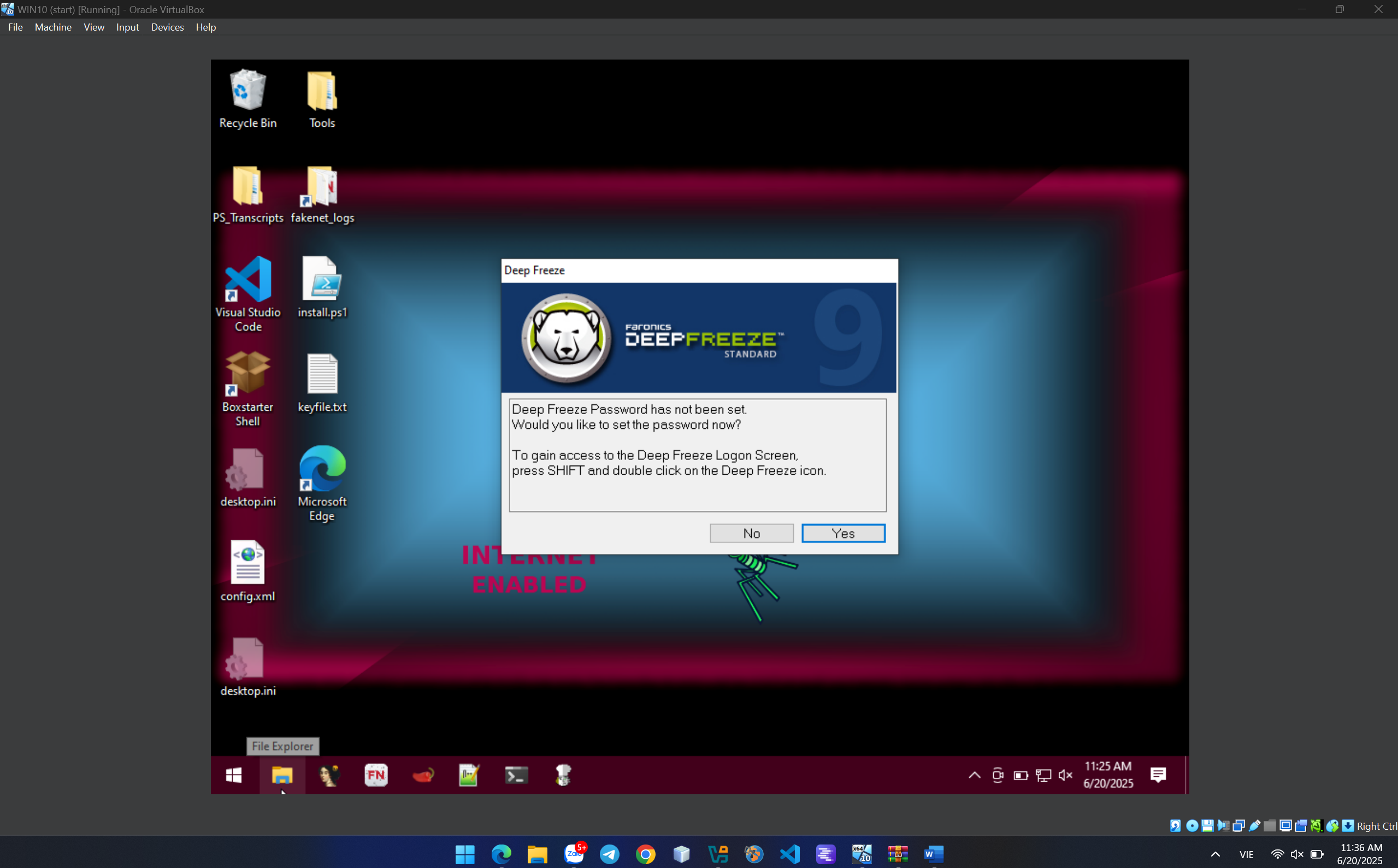
**LAB 10: Install Deep Freeze**

Frozen Drives Configuration



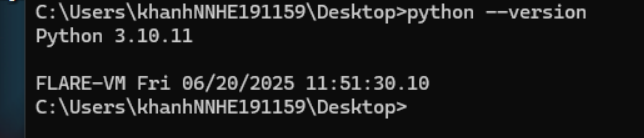
ThawnSpace Configuration

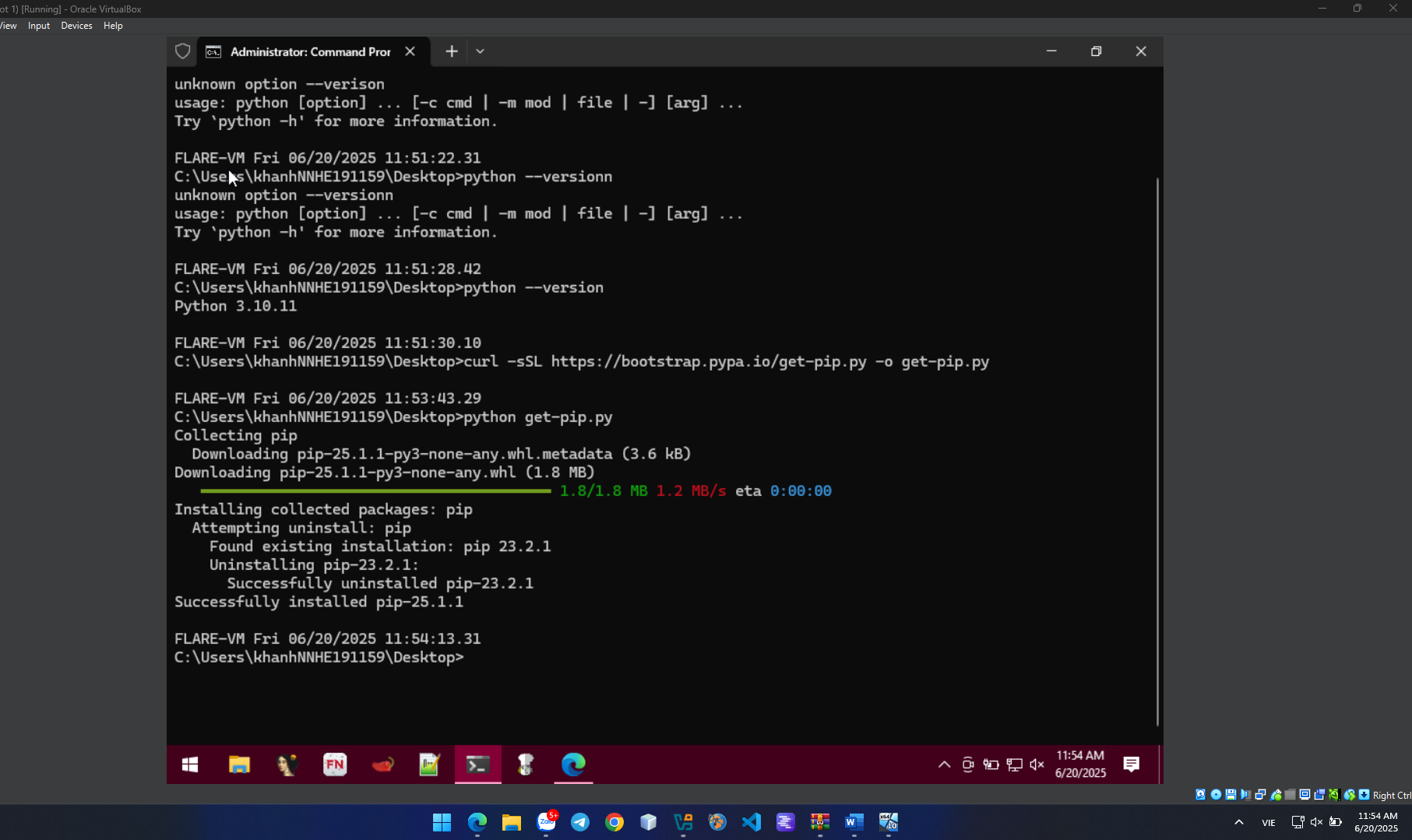
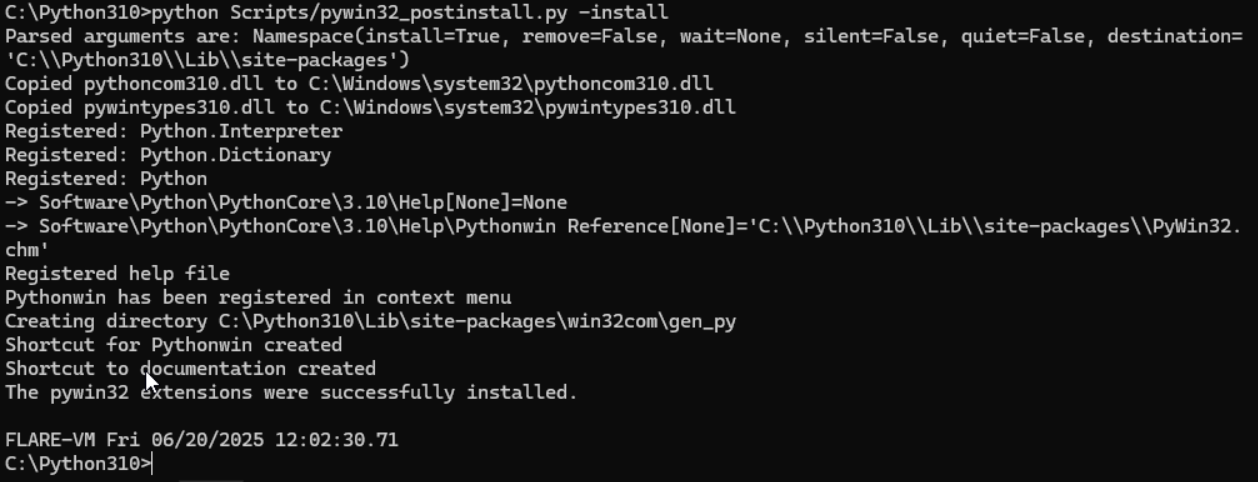
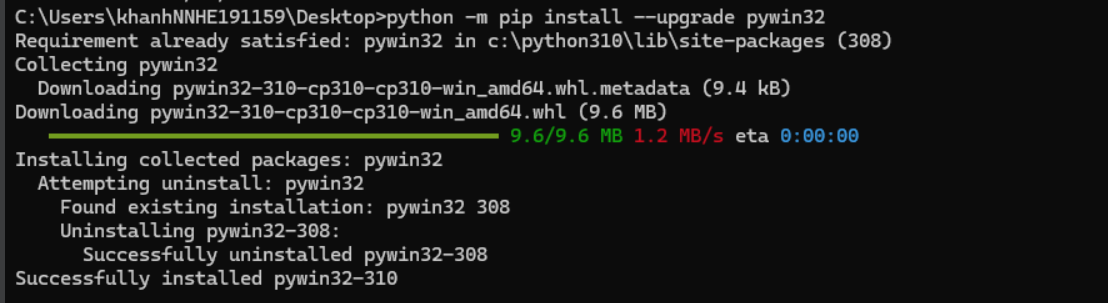
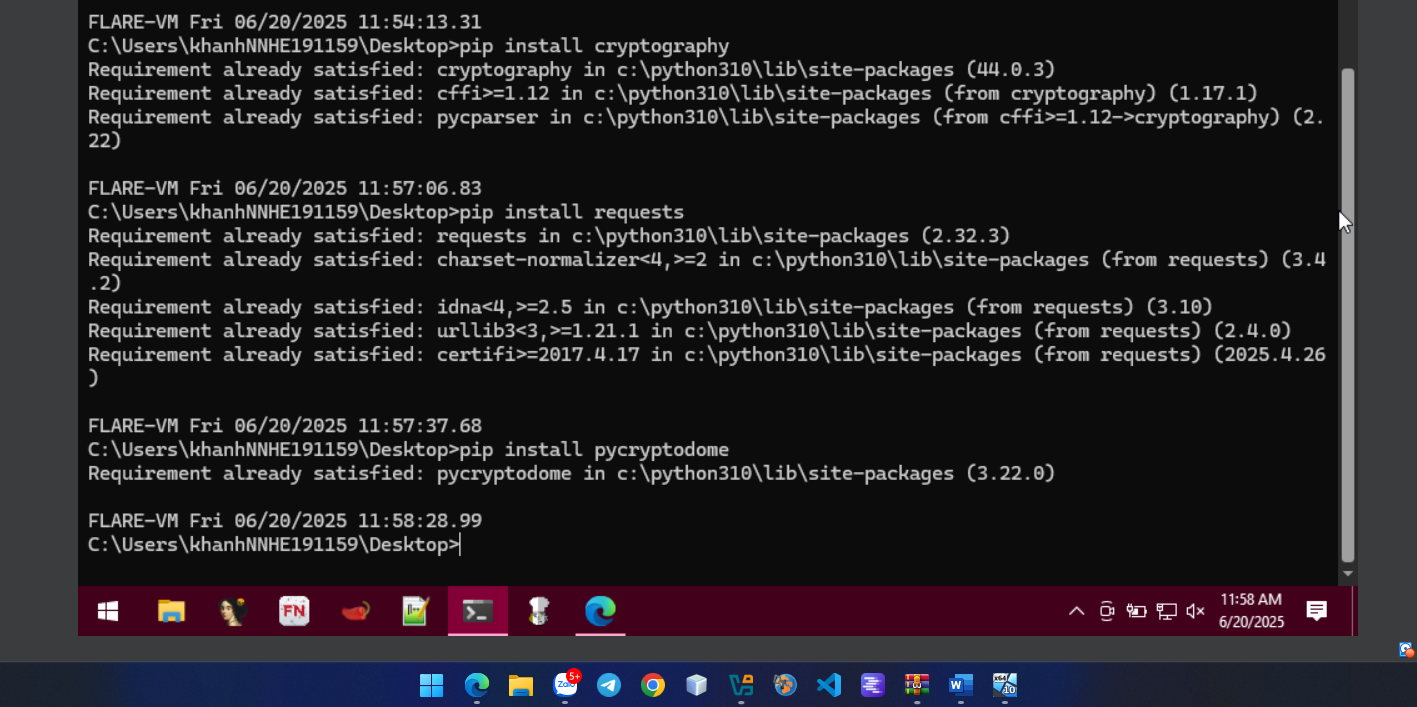


Setting Password

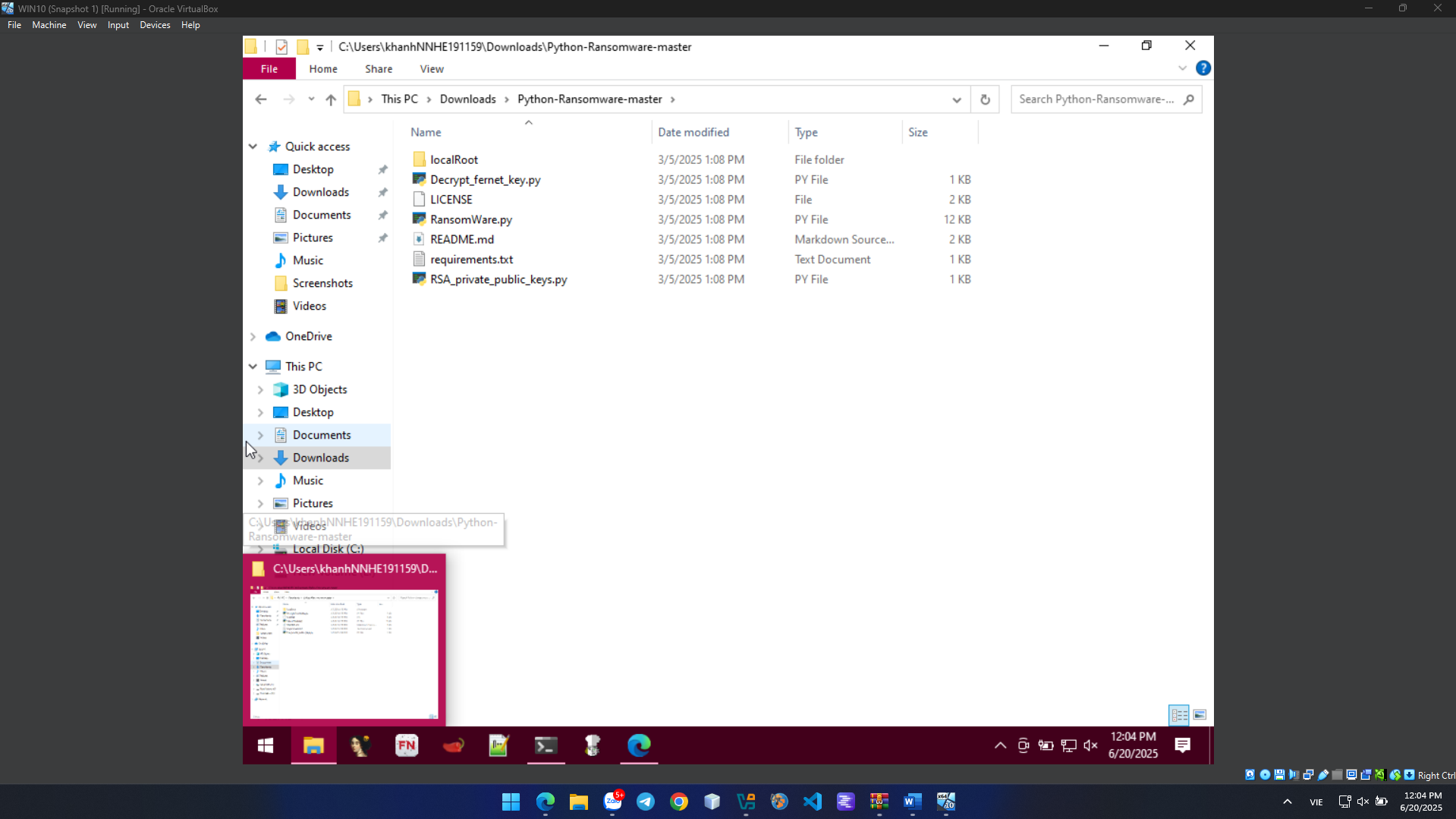
Prepare for Ransomware analysis.

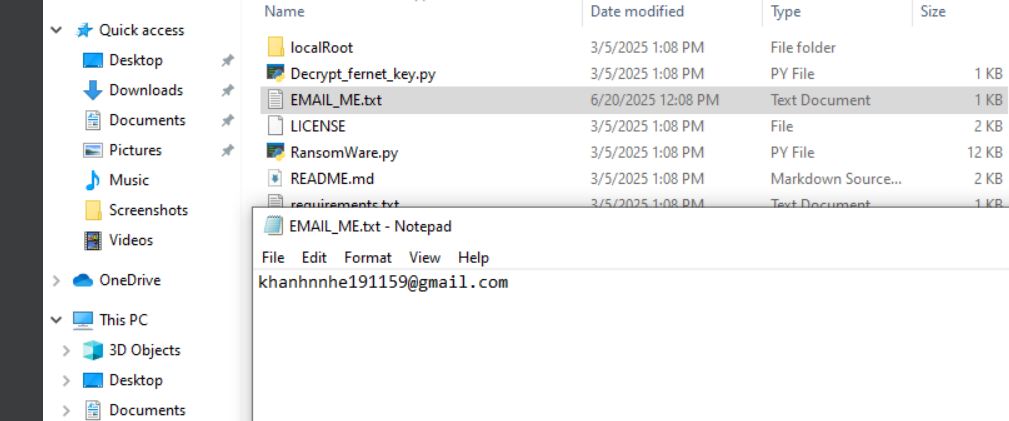
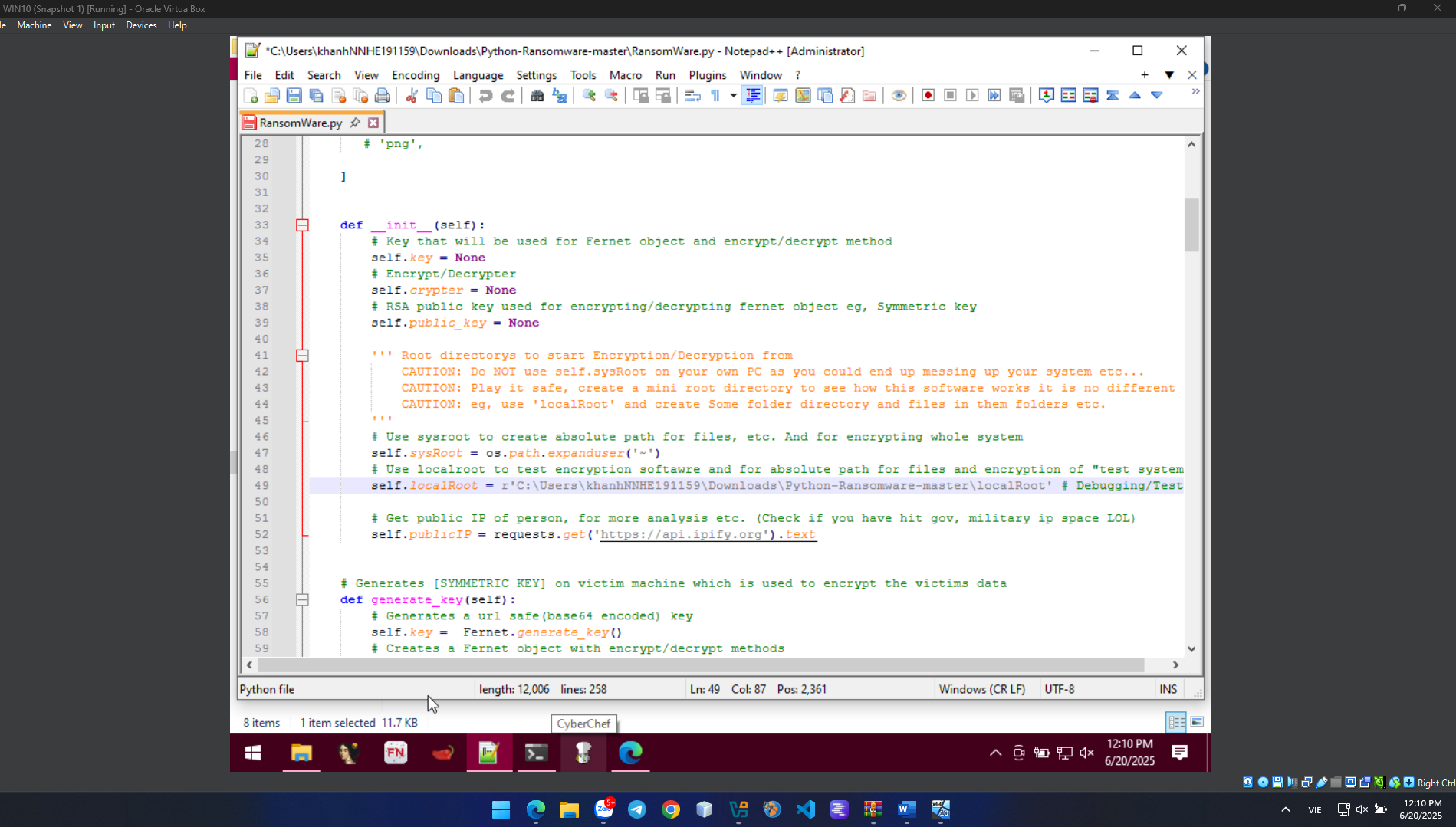
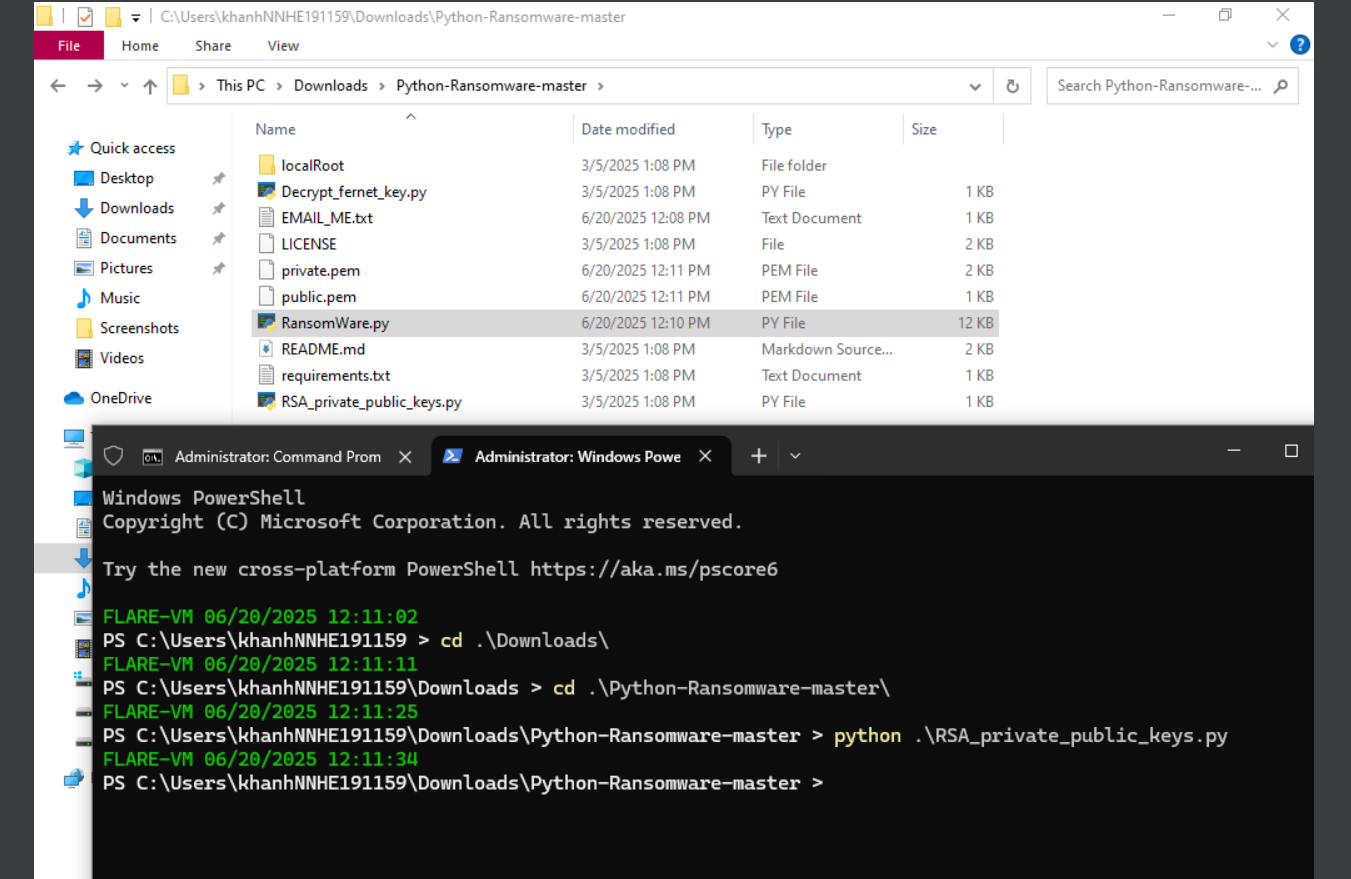
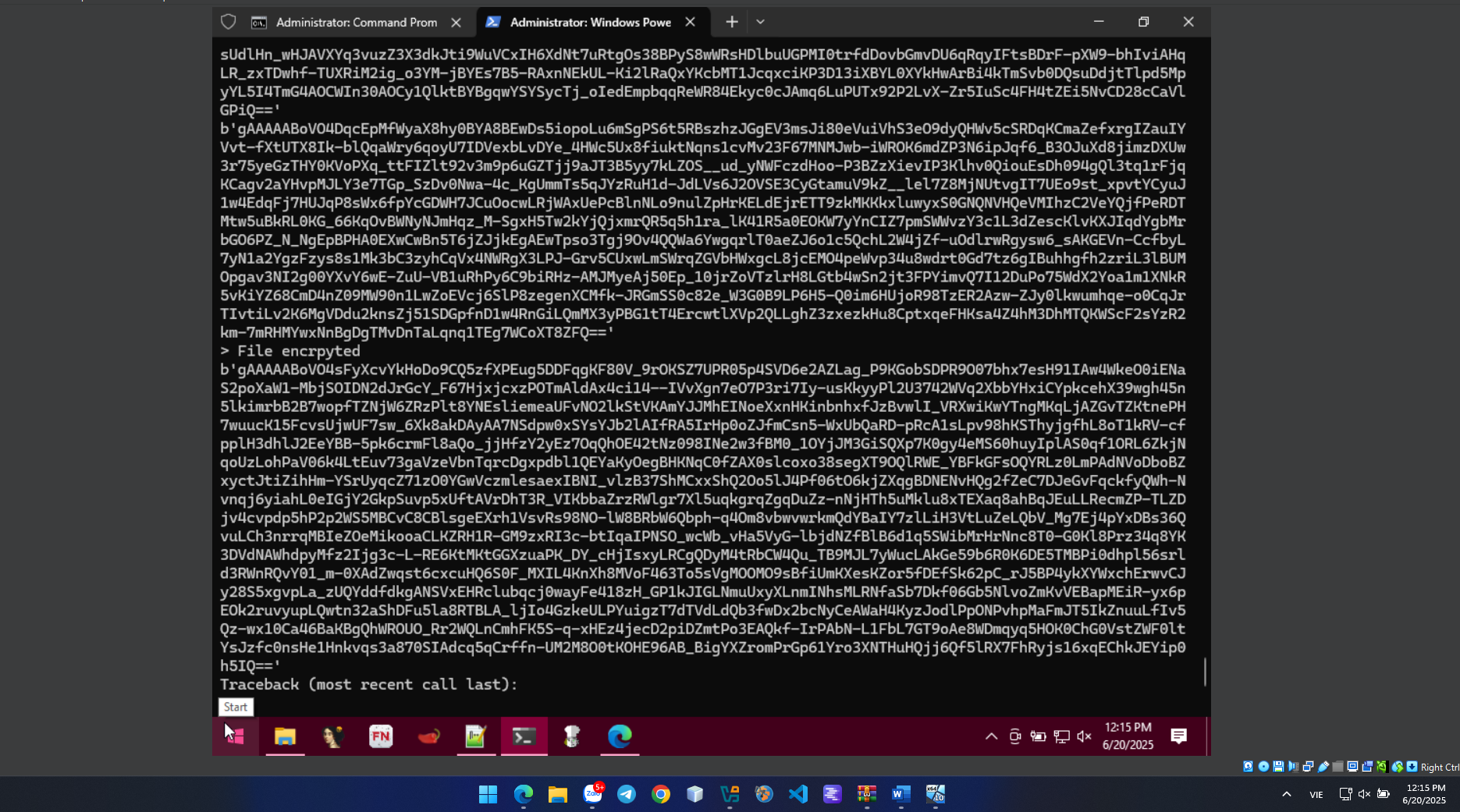
Install python 3.10

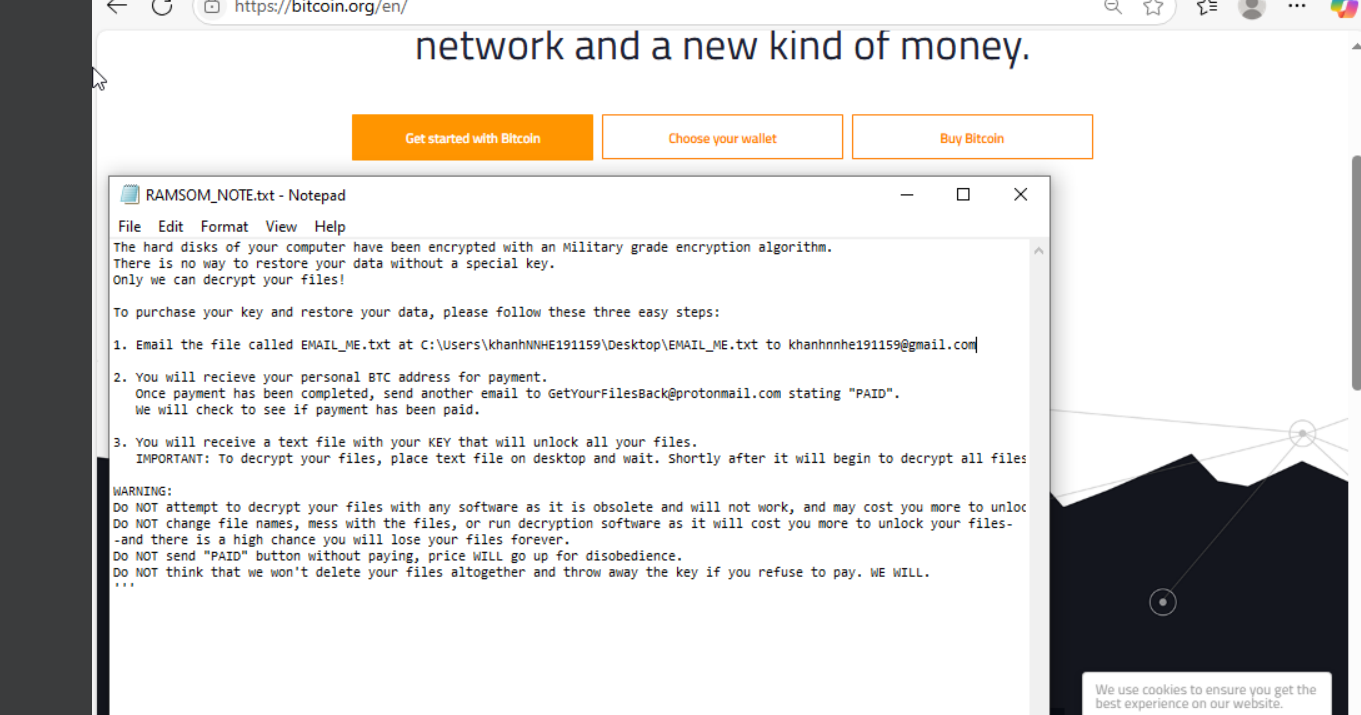
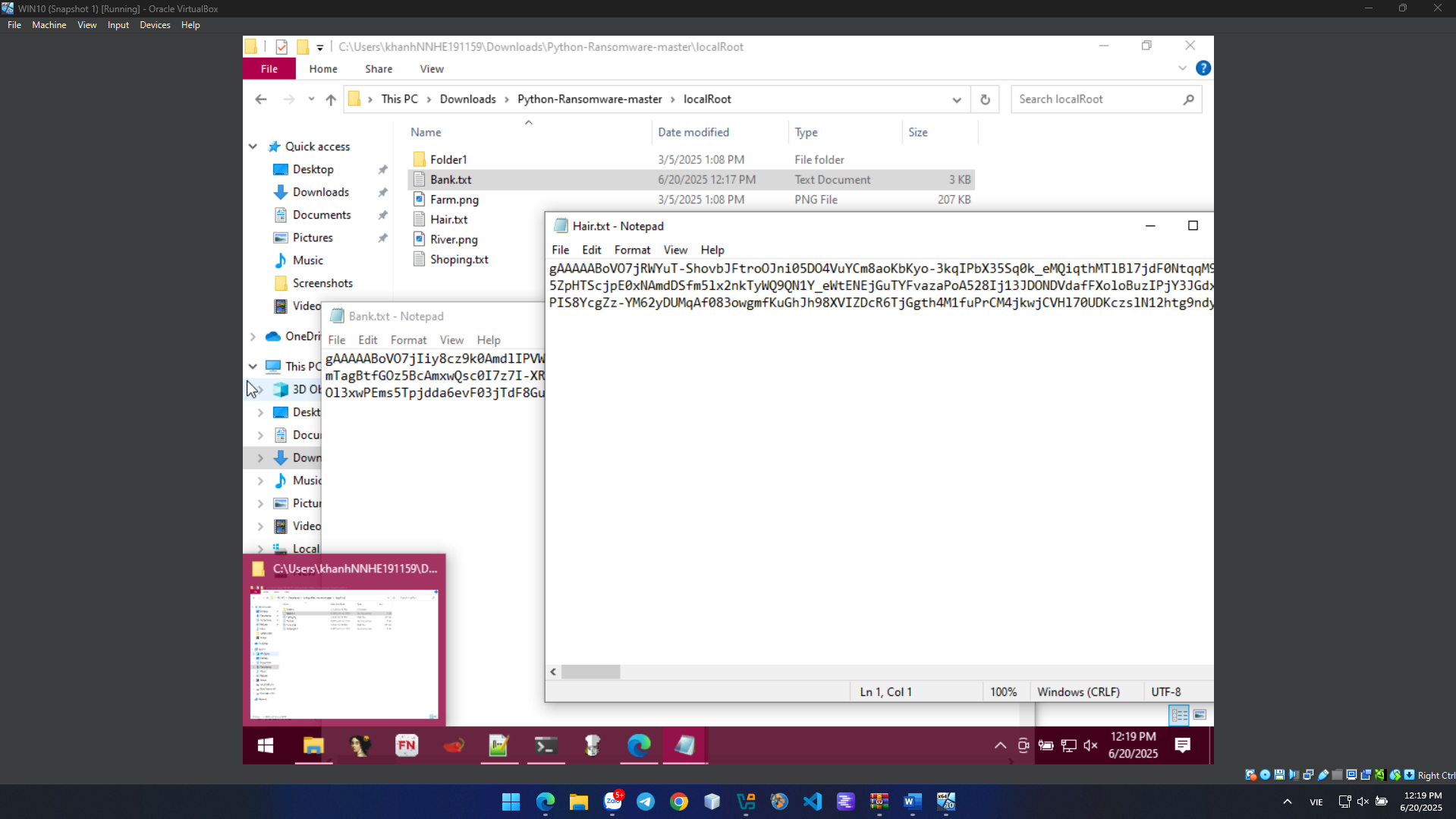
****

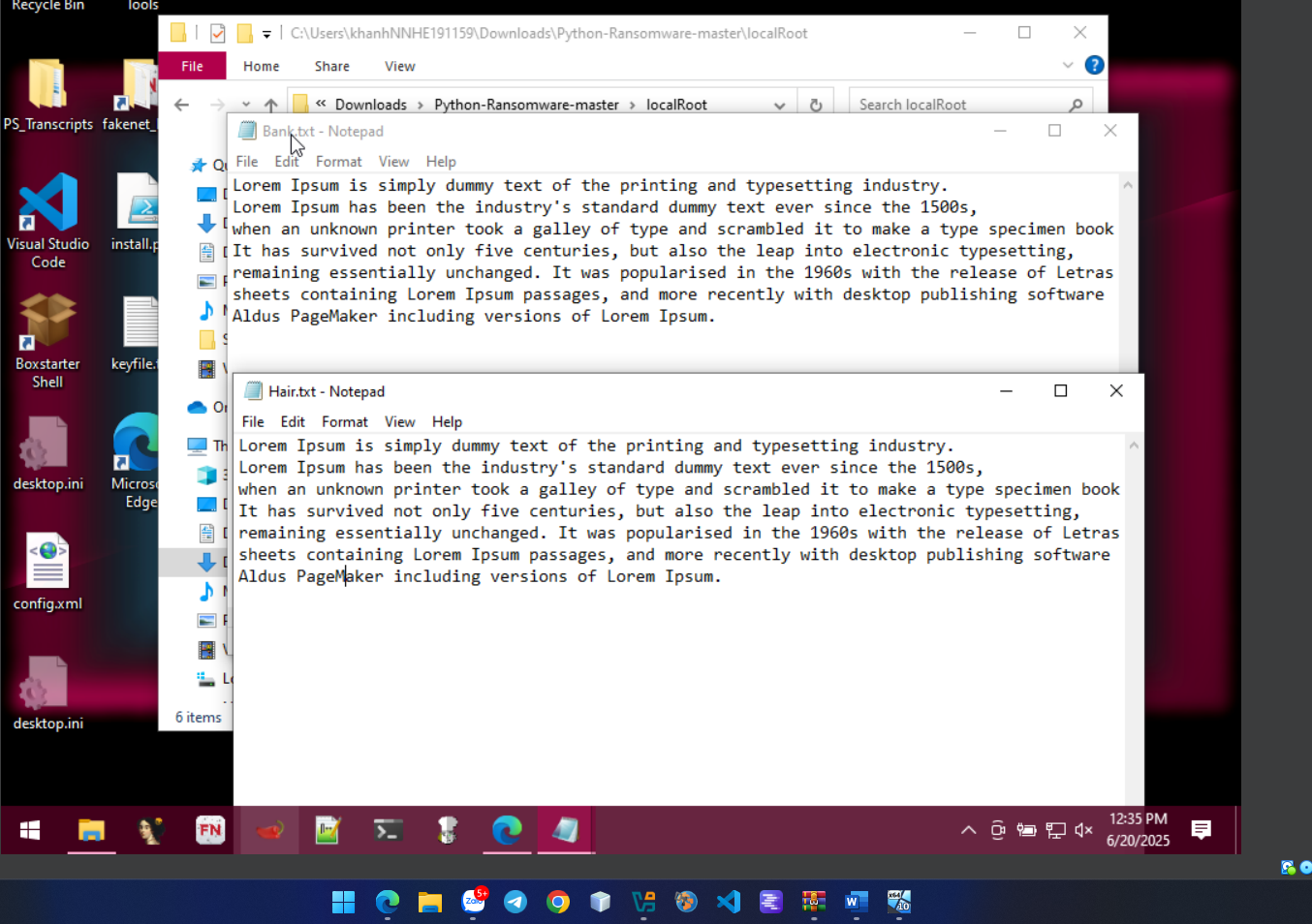
Install pip****Install support library packages: cryptography, win32gui, requests, pycryptodome.****

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: ****

We need to create an EMAIL\_ME.txt file with the Attacker's email address****edit some content in the RansomWare.py file**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****

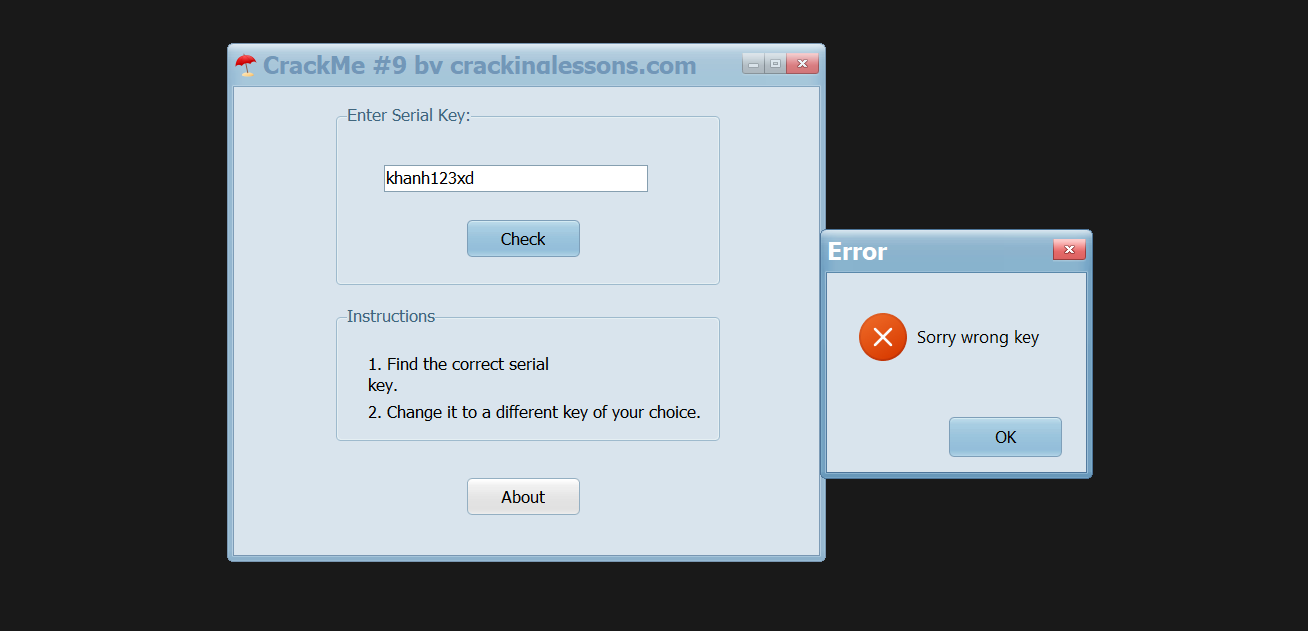
Because the machine preparing for analysis has Deep Freeze installed, we only need to restart the machine to return to the new state, in this case just like Snapshot. This is very useful in cases where we need physical systems to analyze specific malware. ****

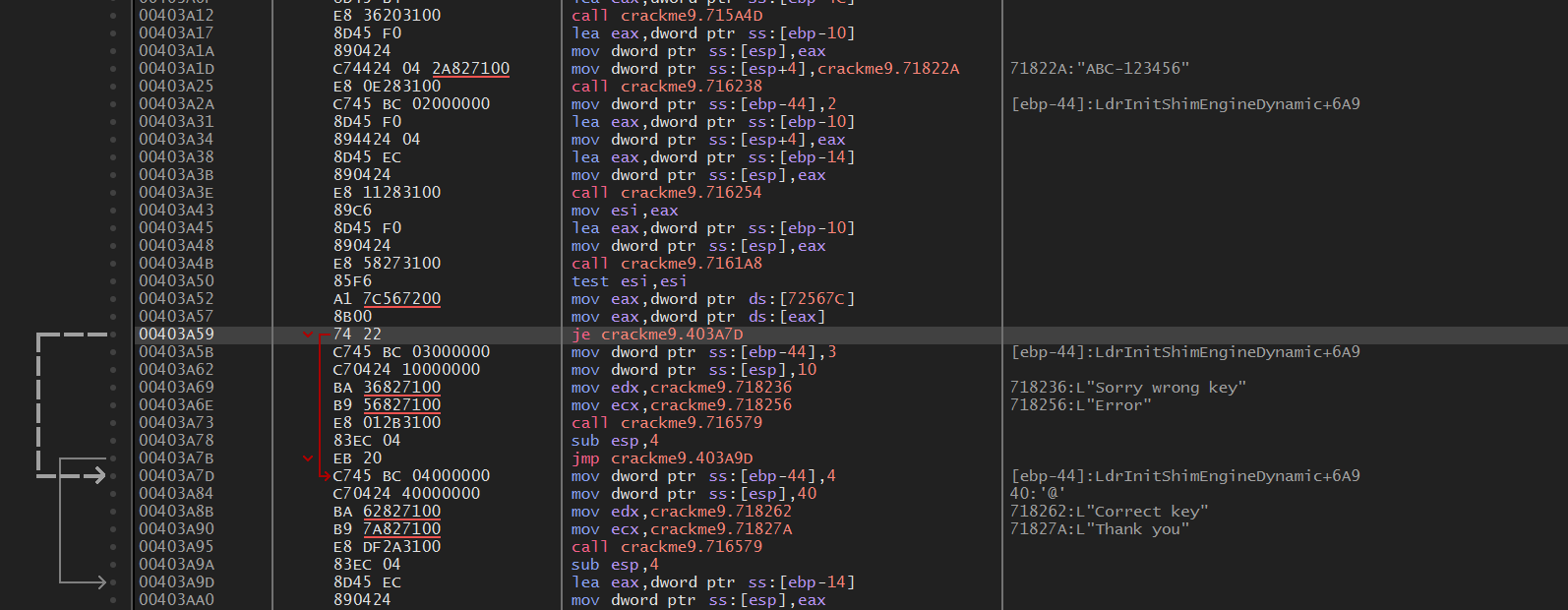
**CRACK ME 9**

To practice patching memory directly.

Objectives:

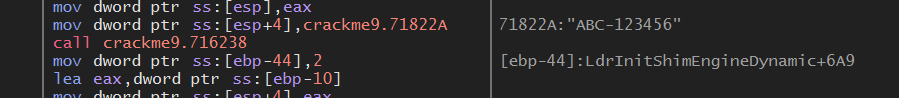
1. Find the correct serial key
2. Change it to a different key of your choice



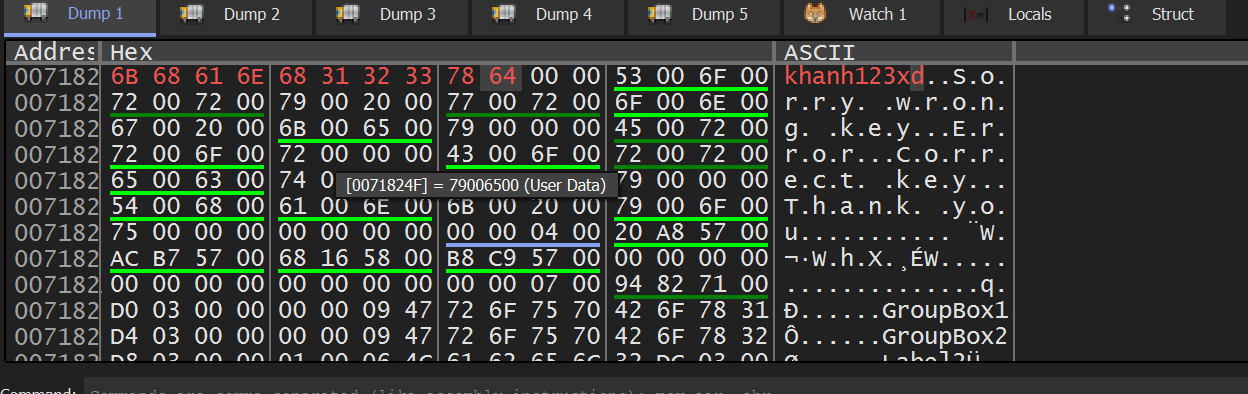
First let move to to String reference to find the code corresponding. 

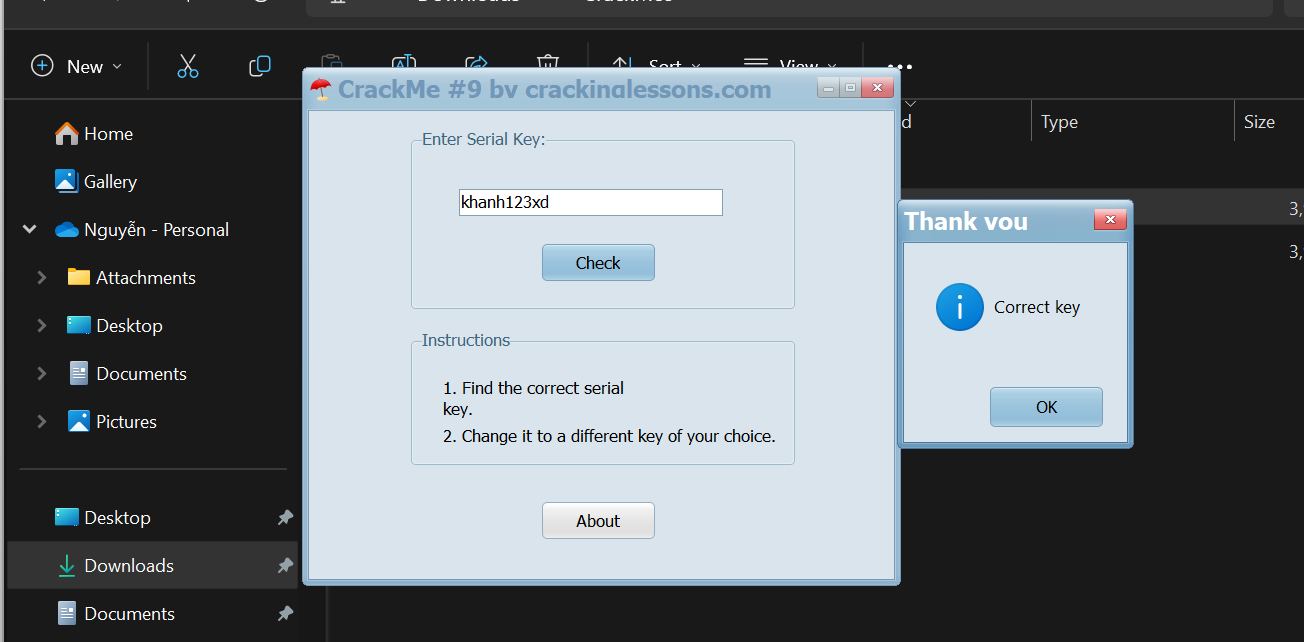
Notic string reference “ABC-123456”, it may be like the format of serial key, so I could insert this string again to verify and receice the true result.



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. 

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

Patch this file and verify again. 

DONE!!!