

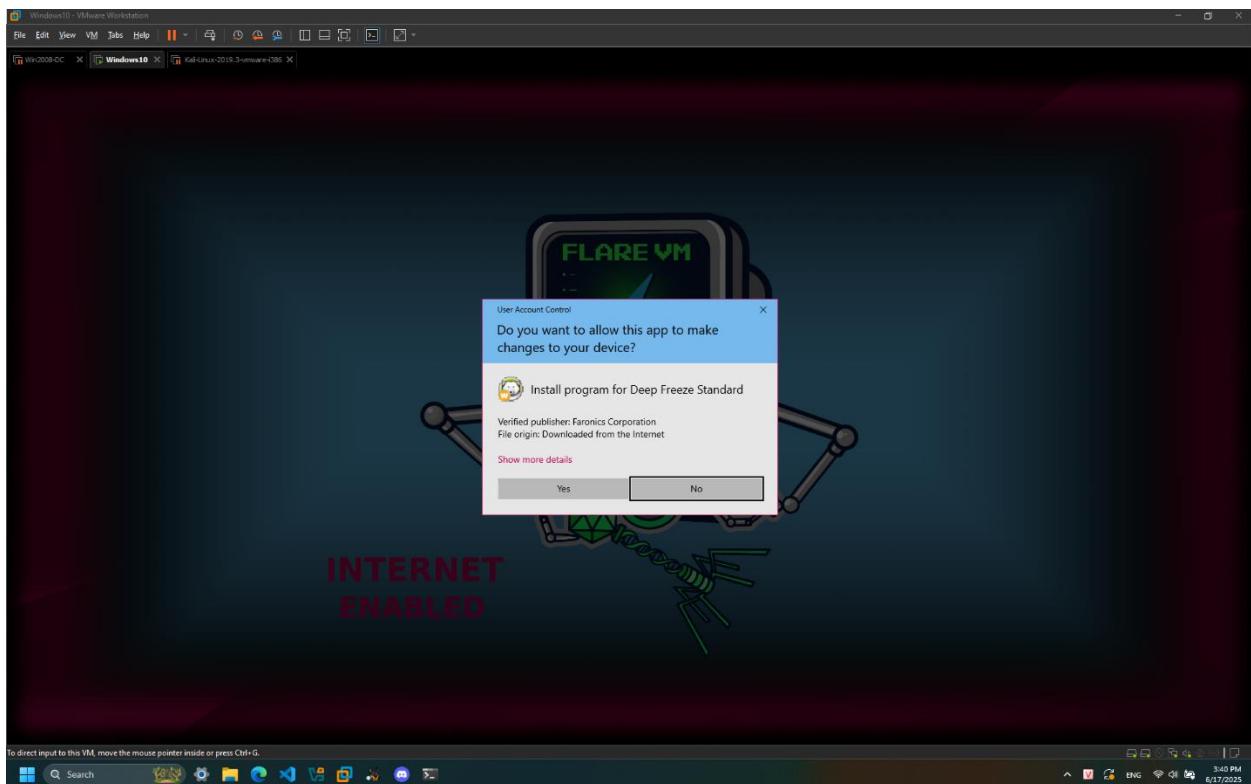
Họ và tên: Trần Trí Dũng

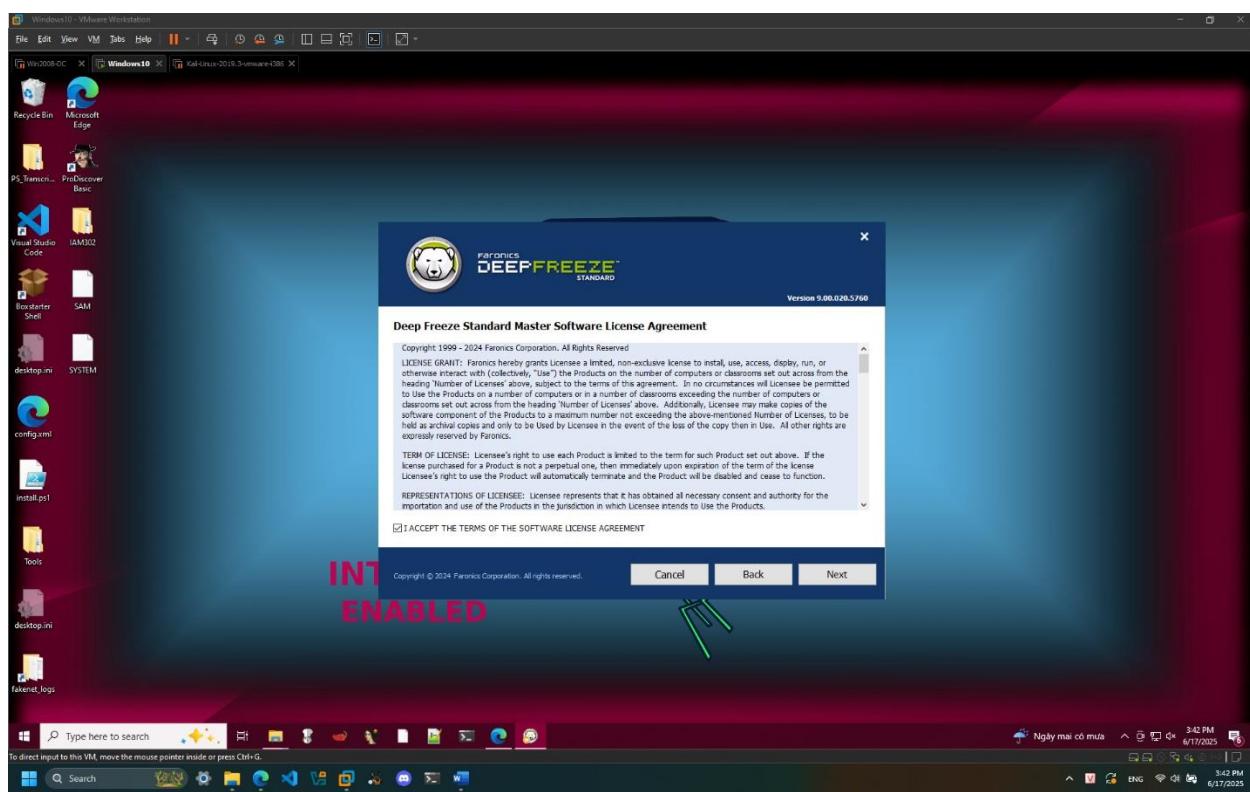
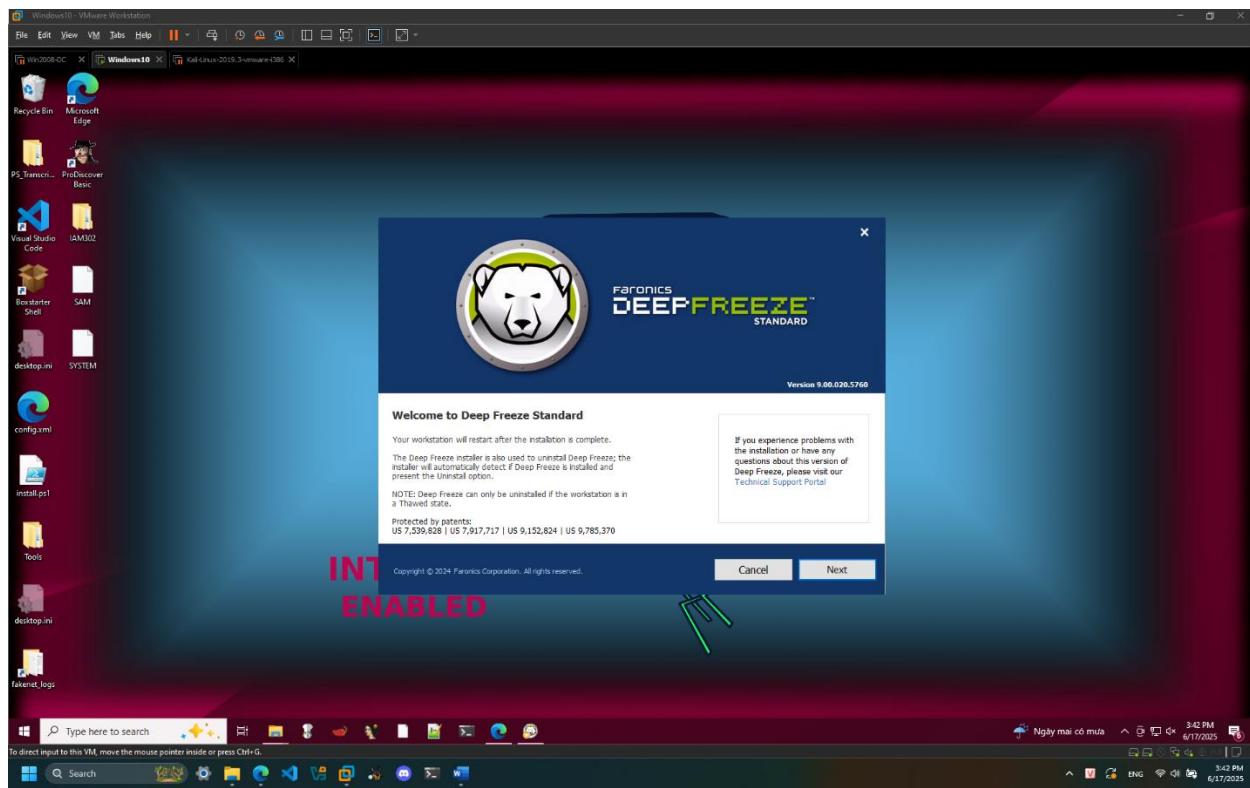
Mã số sinh viên: HE190680

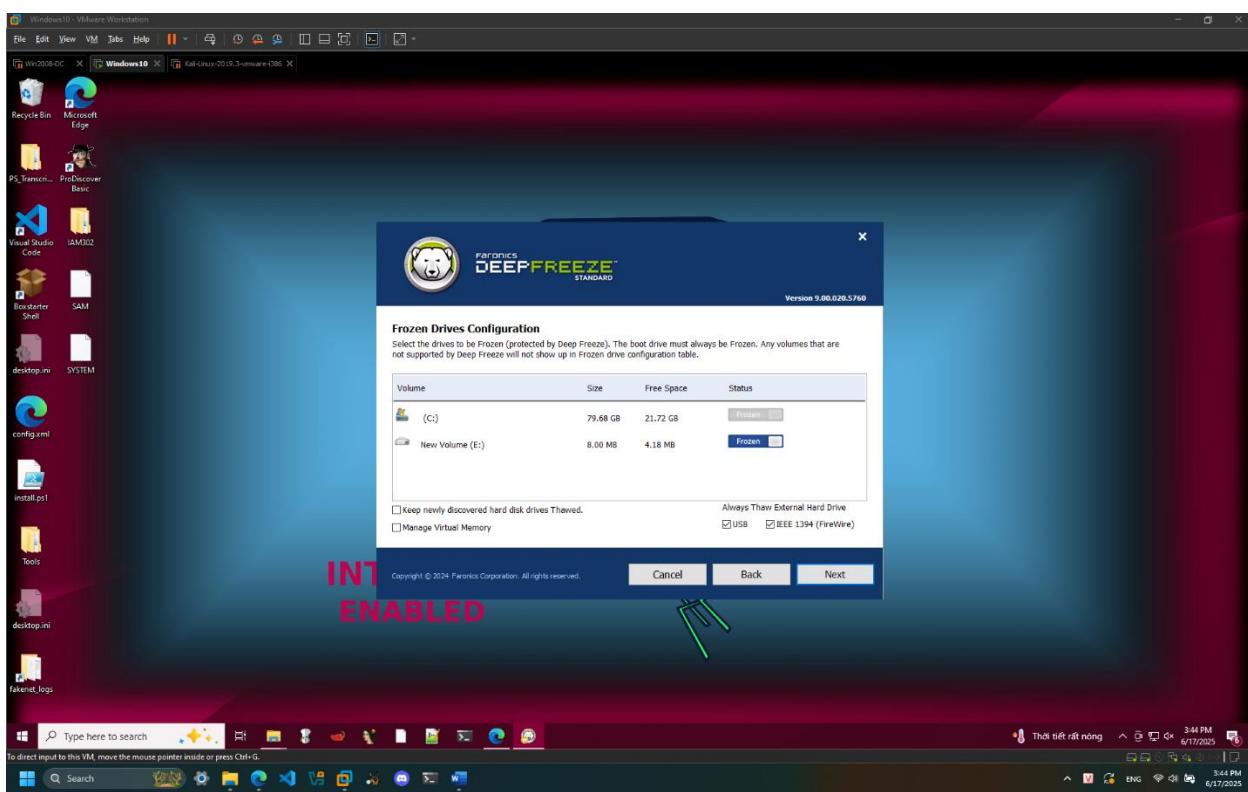
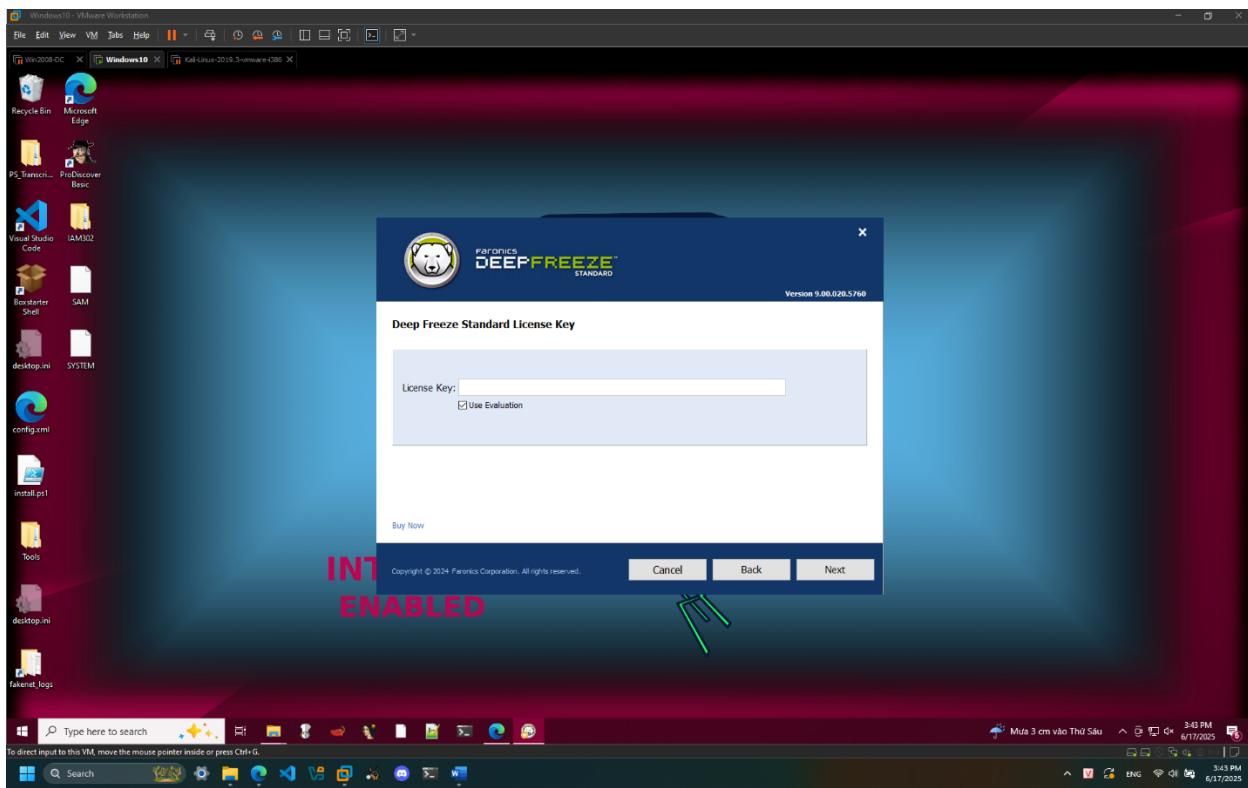
Lớp: IA1901

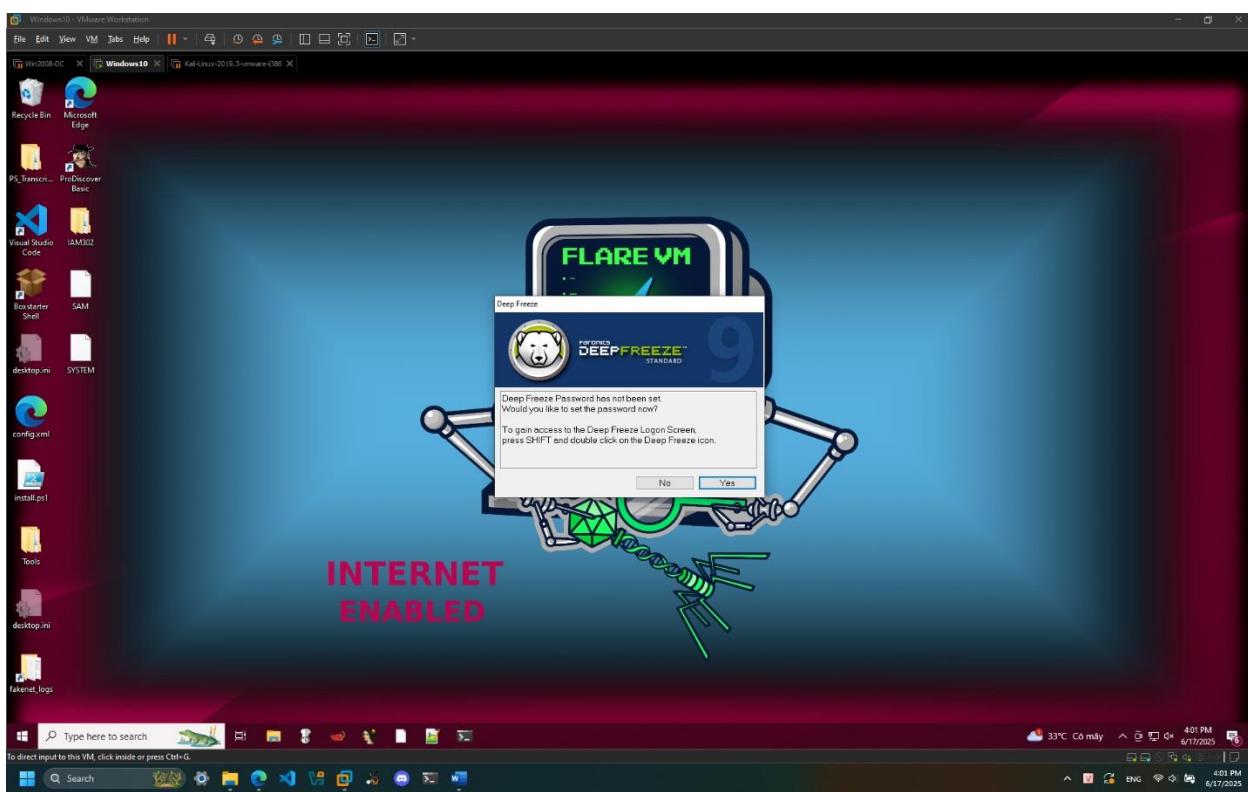
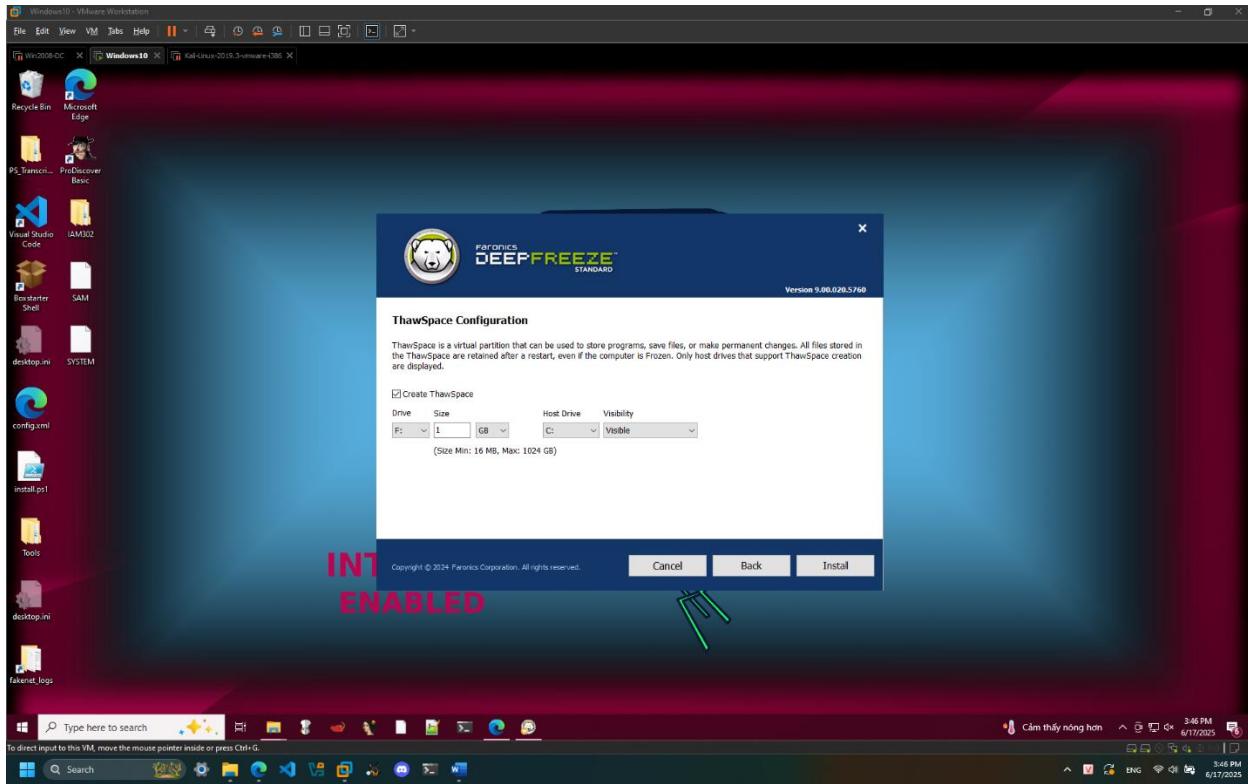
Lab 10

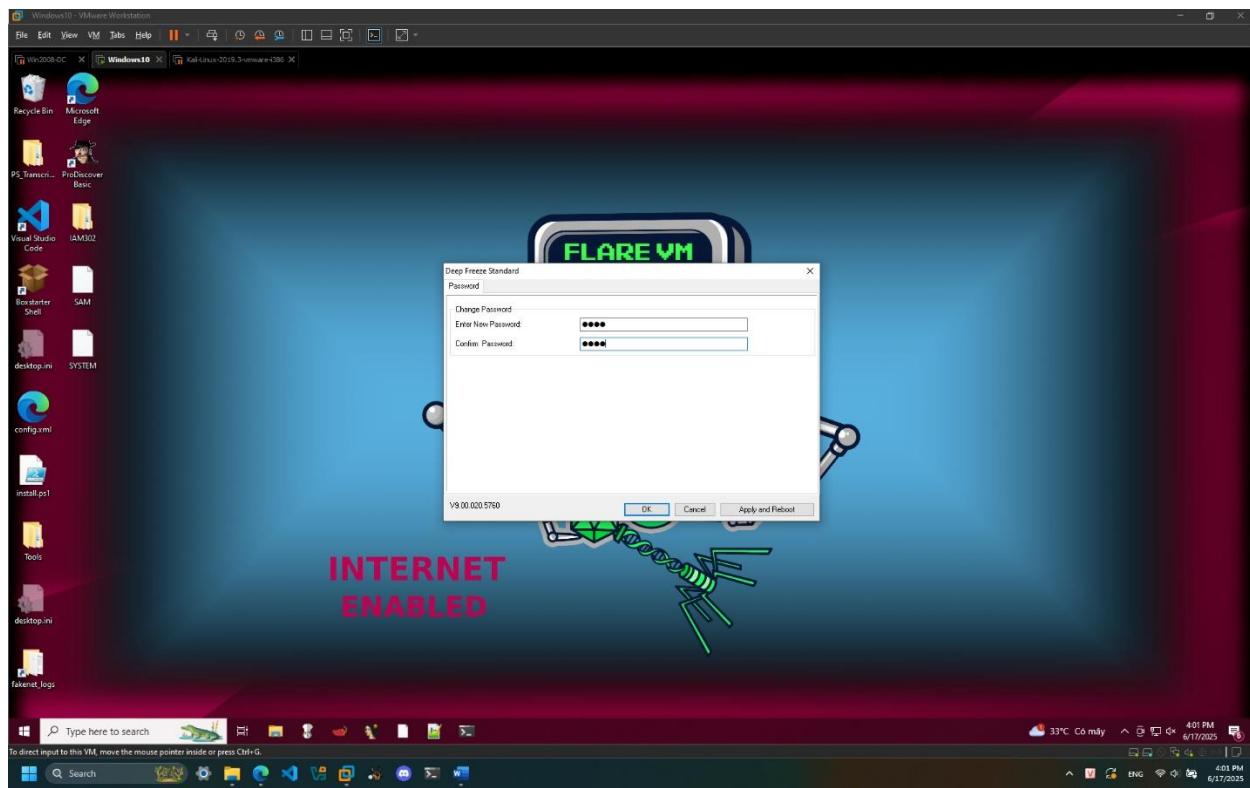
Install Deep Freeze:



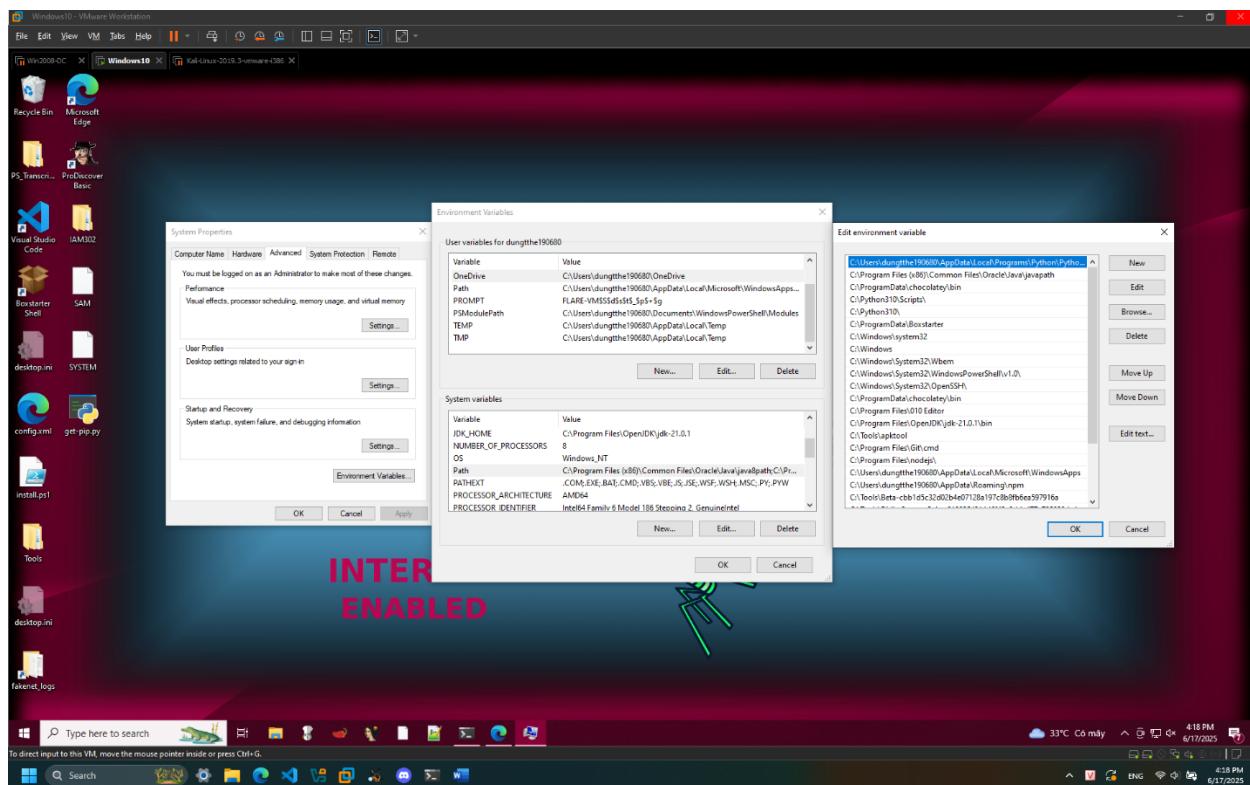




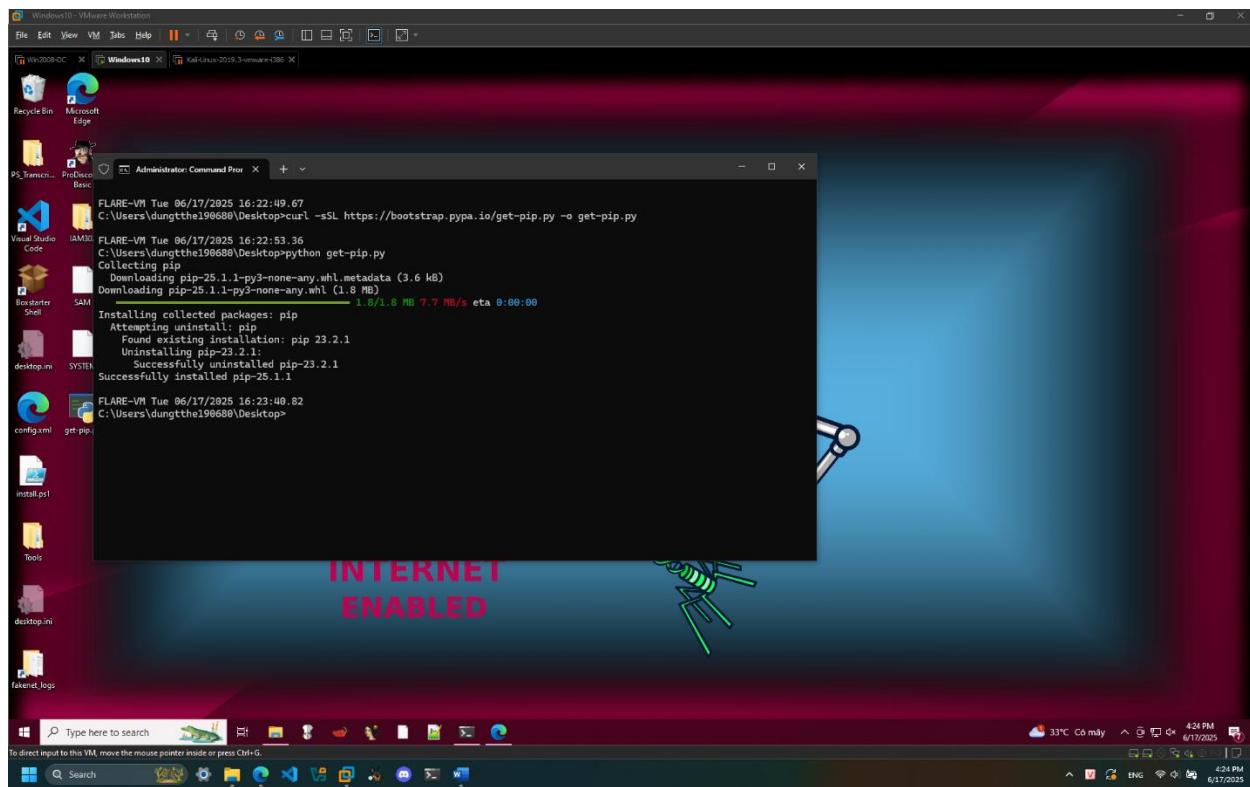




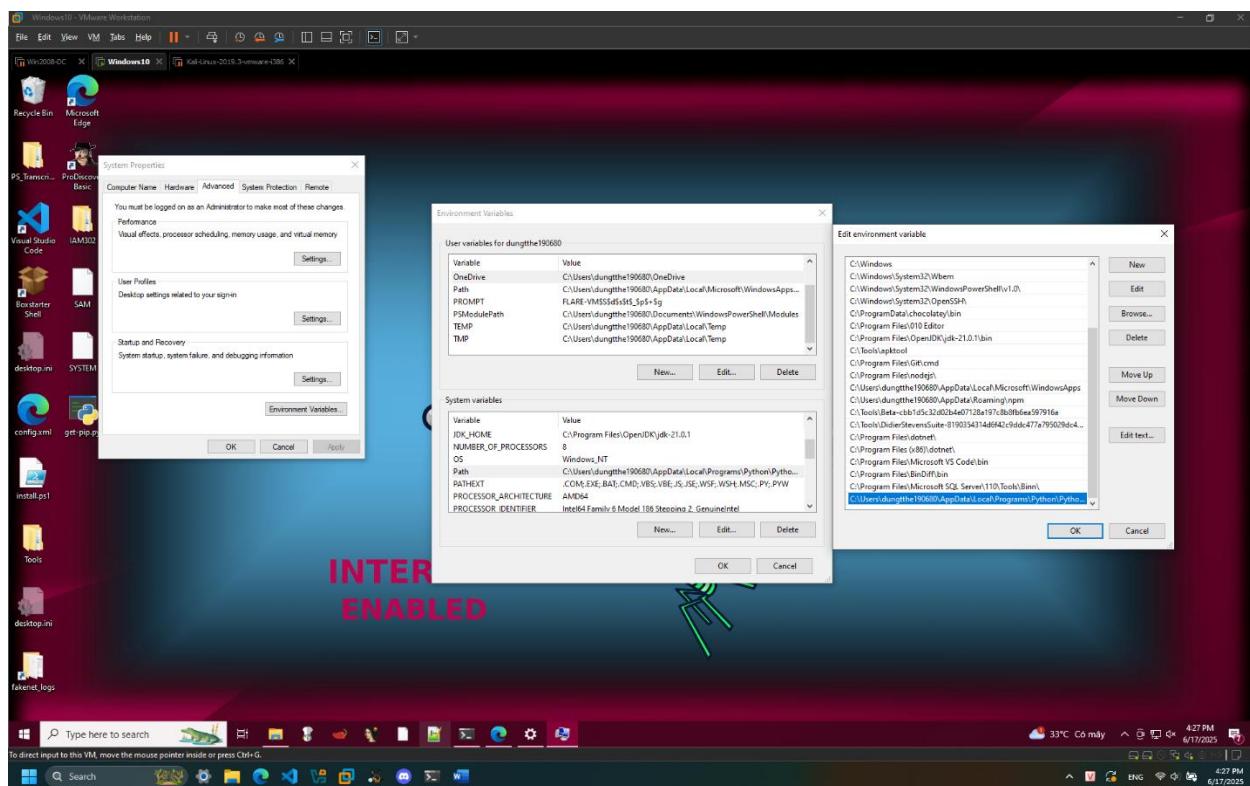
Assign environment variables after installing Python:



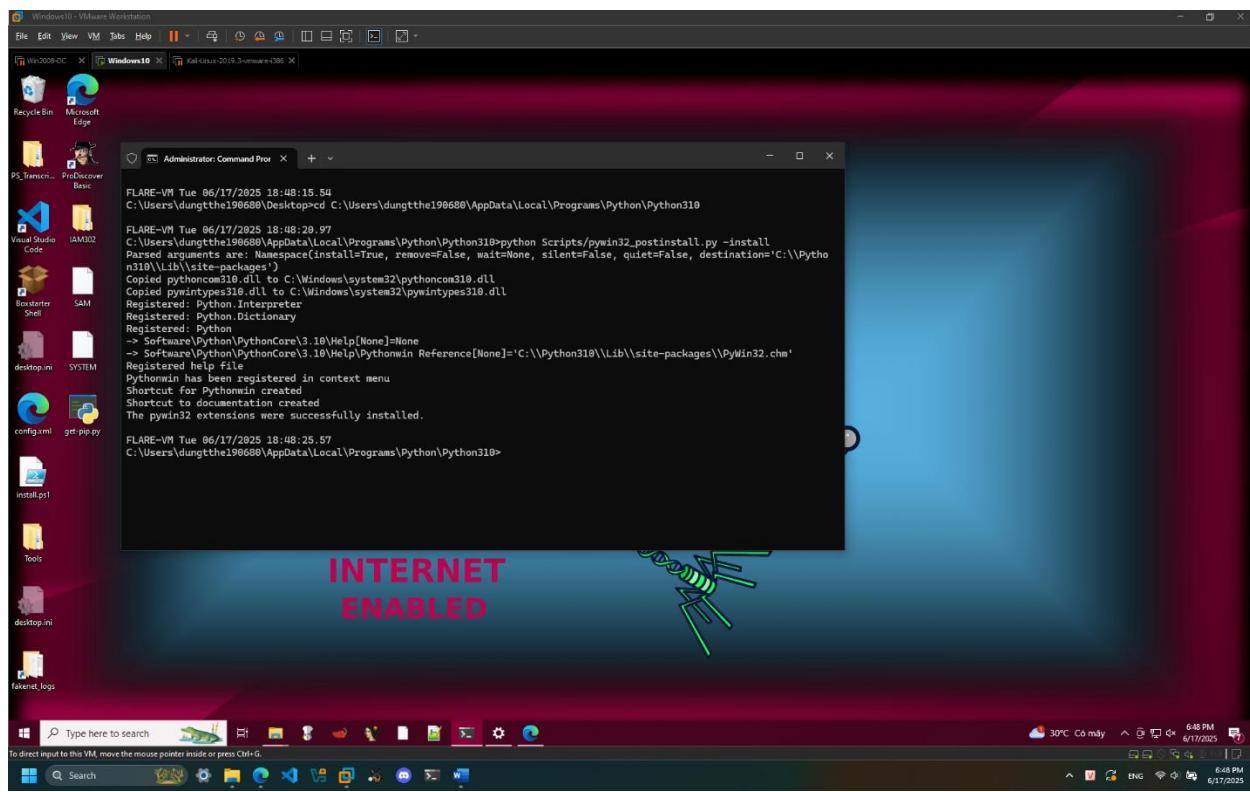
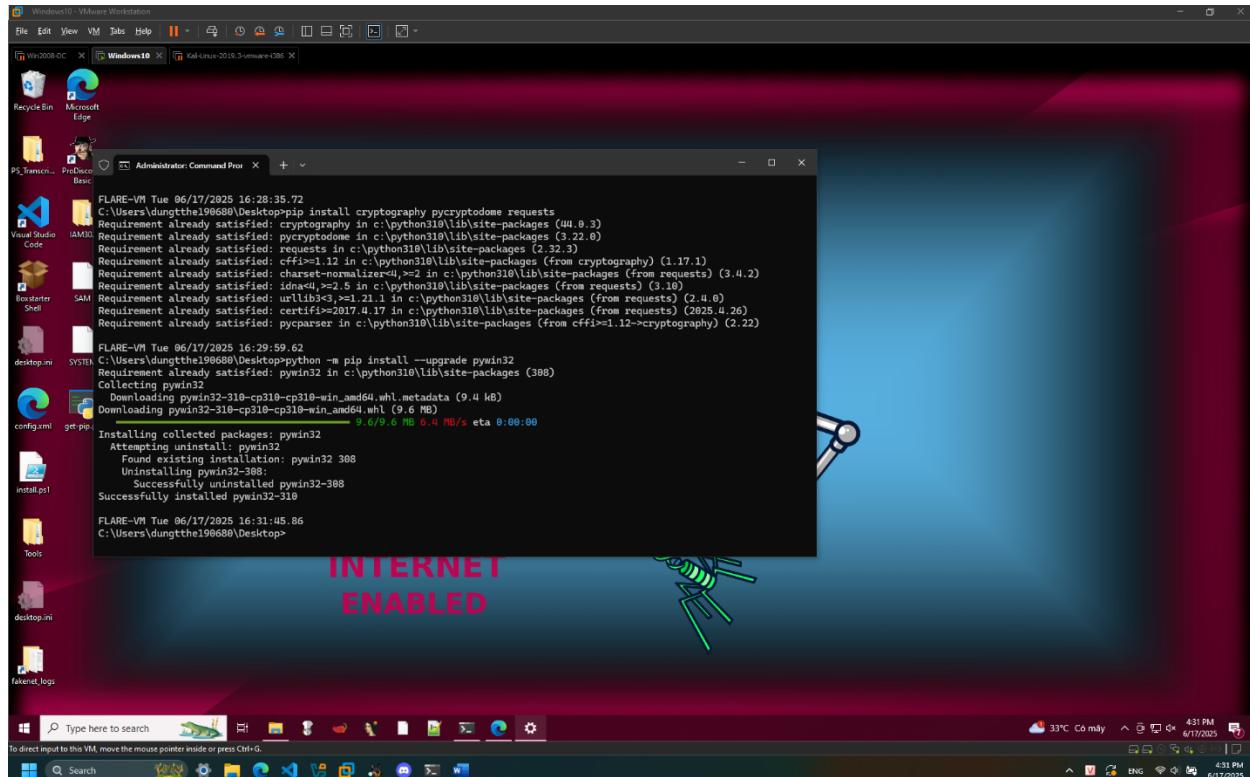
Install pip:



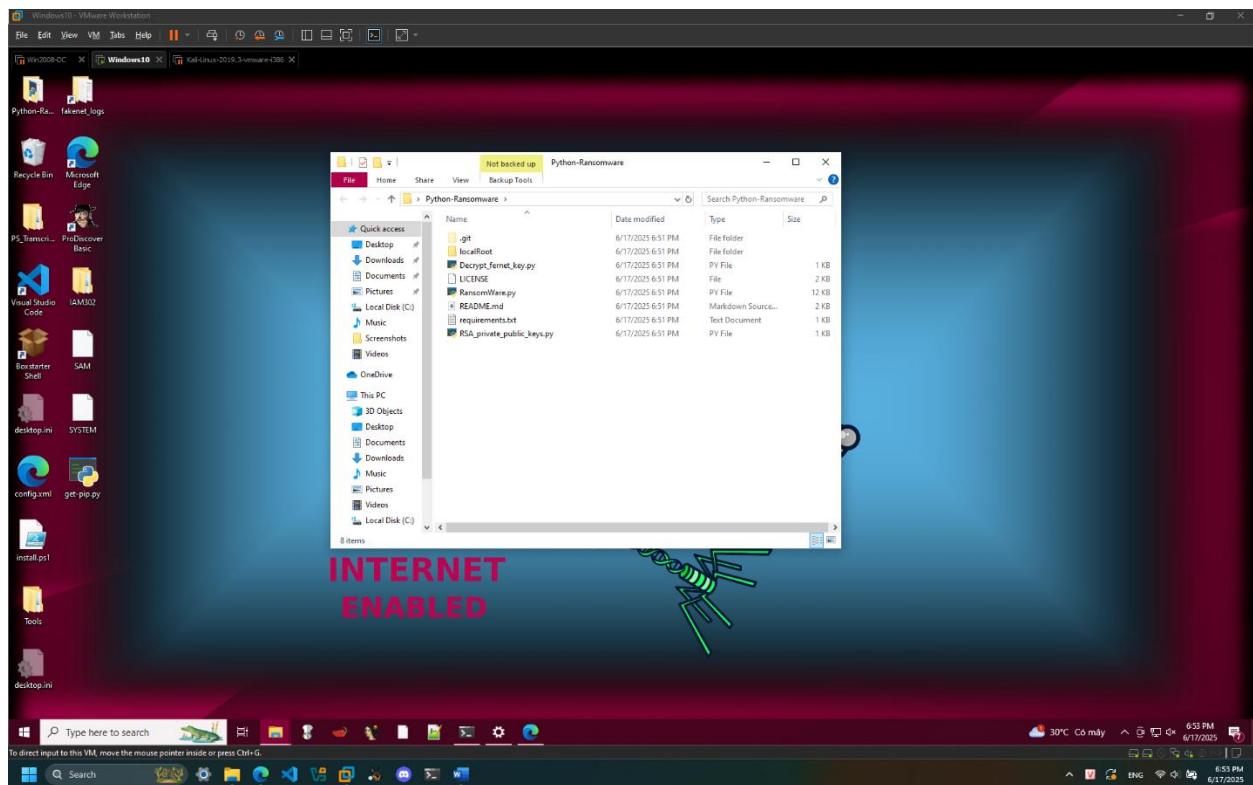
Assign environment variables:



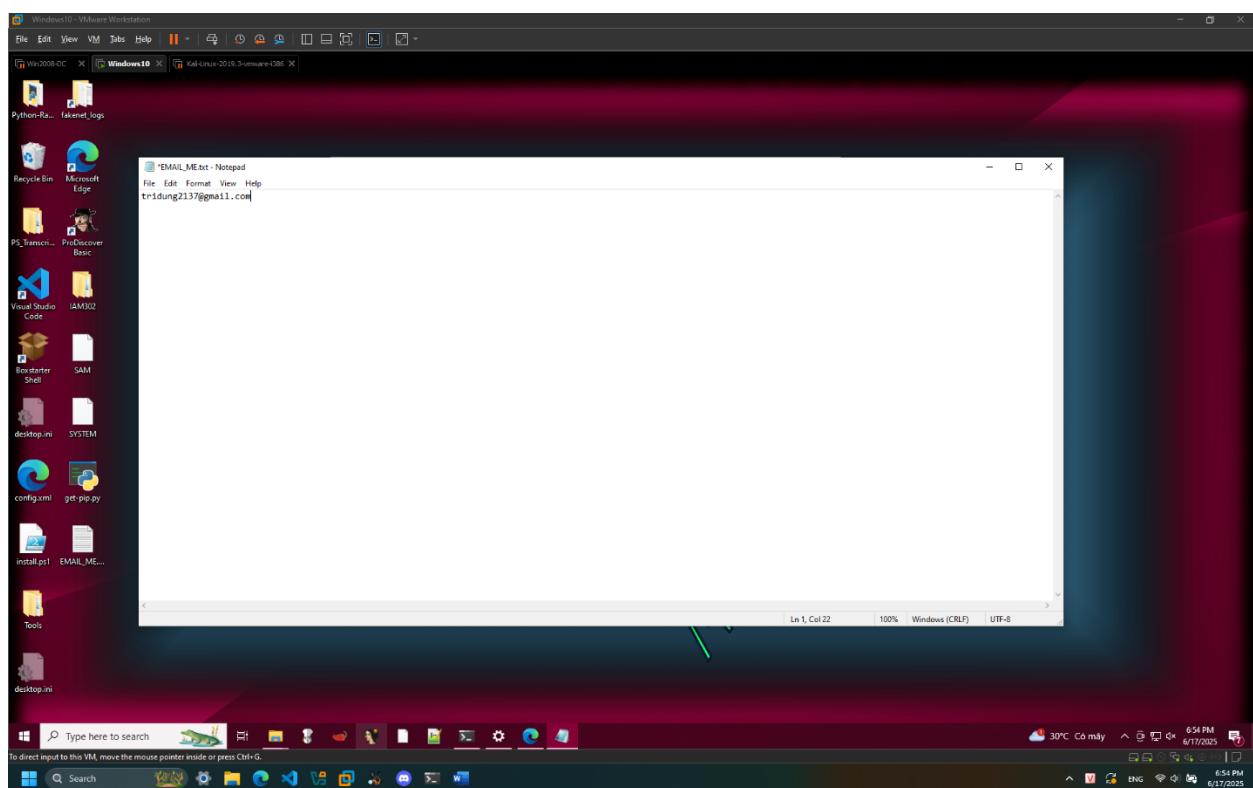
Install support library packages:



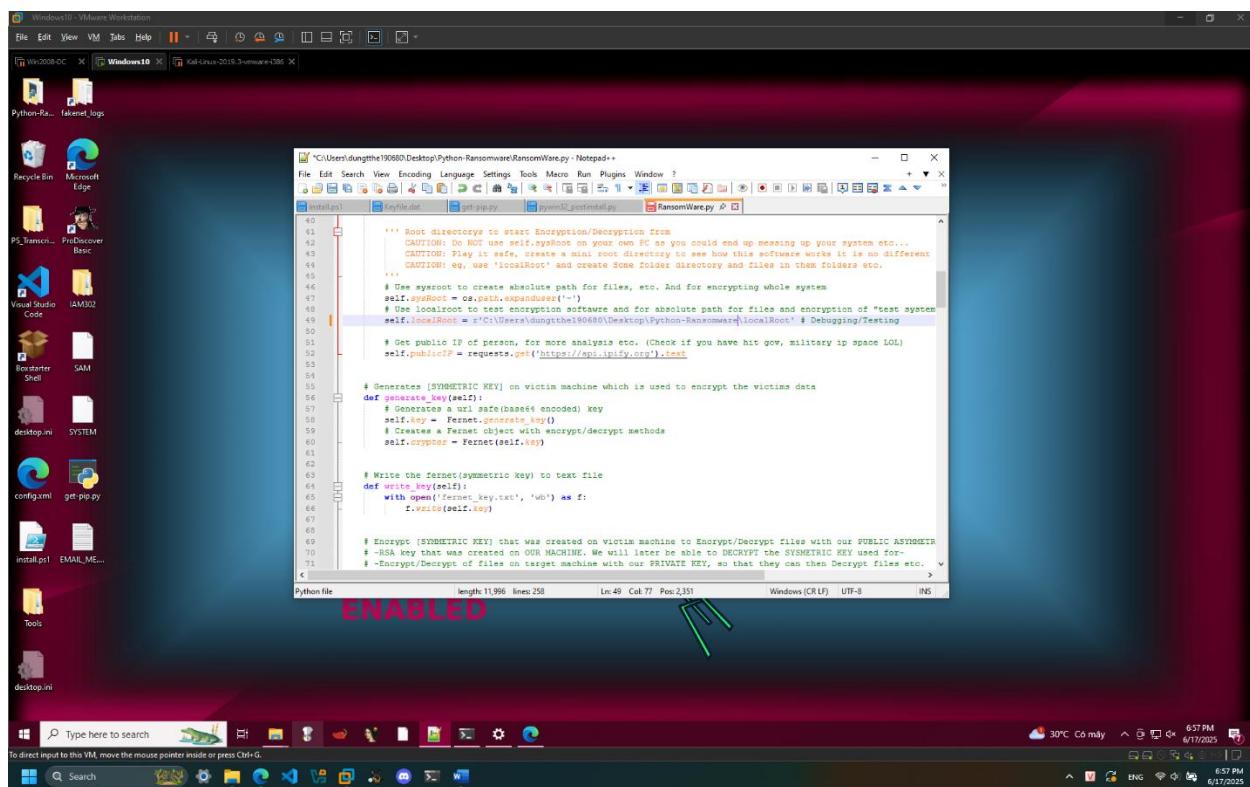
Download Source Ransomware and Unpack:



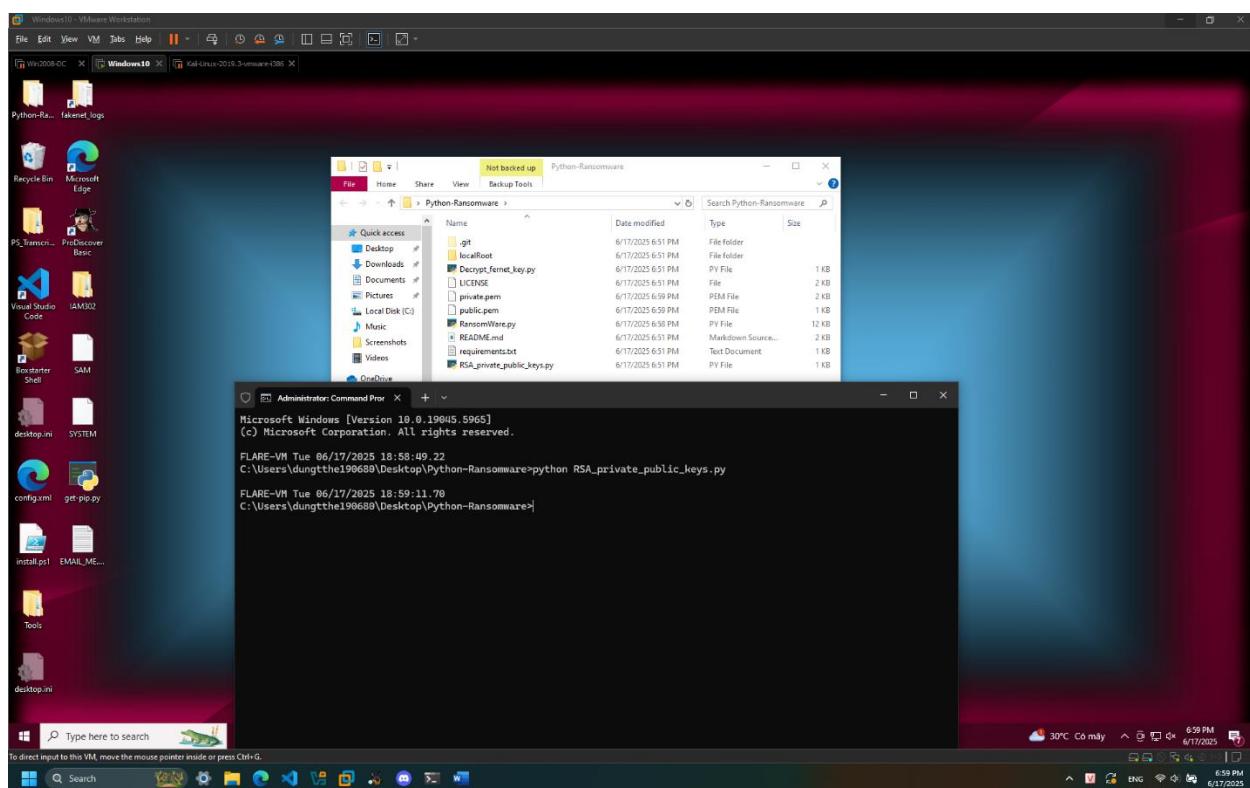
Create an EMAIL_ME.txt file with the Attacker's email address:



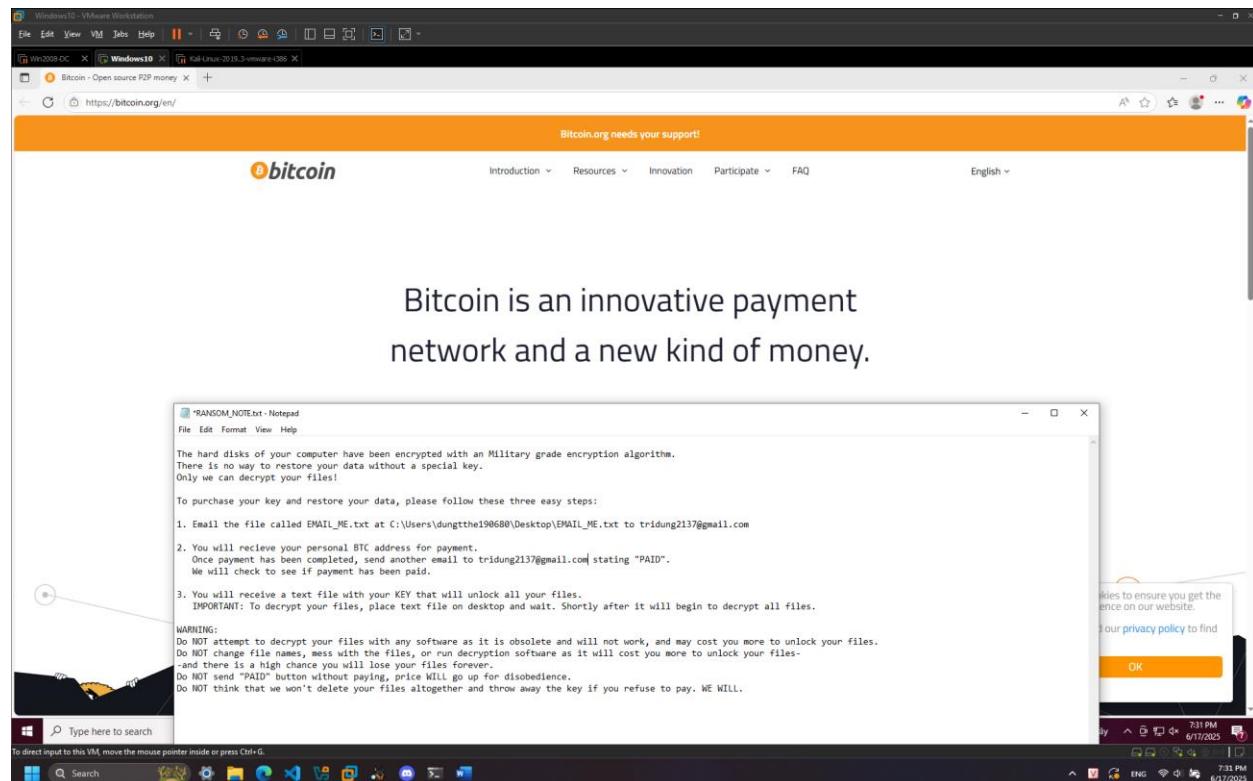
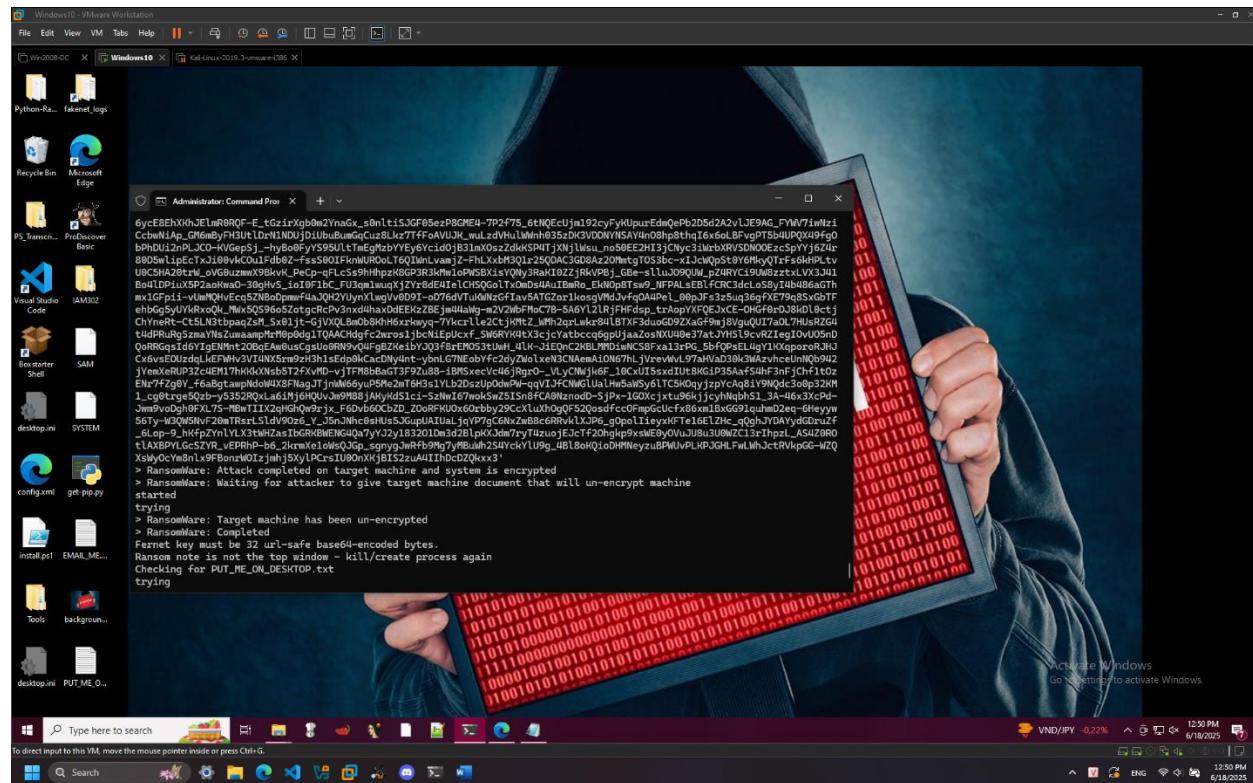
Edit some content in the RansomWare.py file:

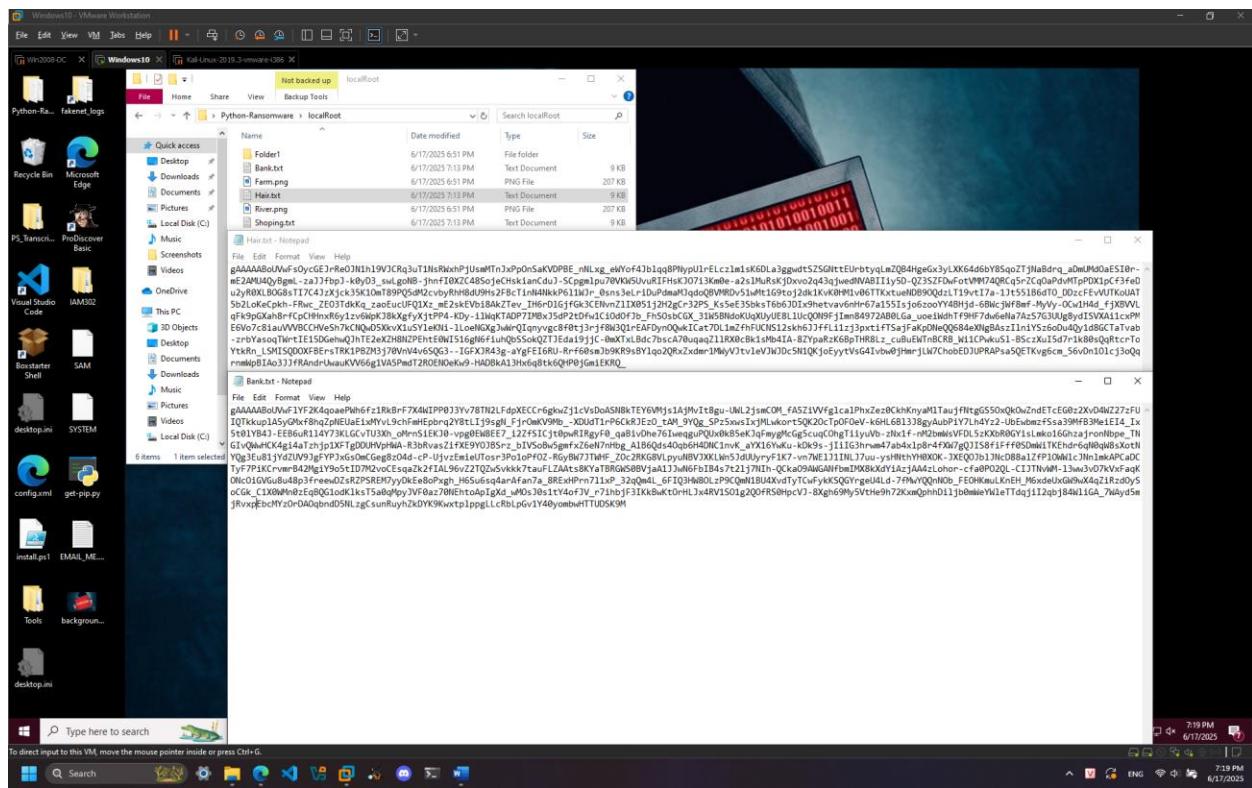


Run the RSA_private_public_keys.py file to generate a key pair:



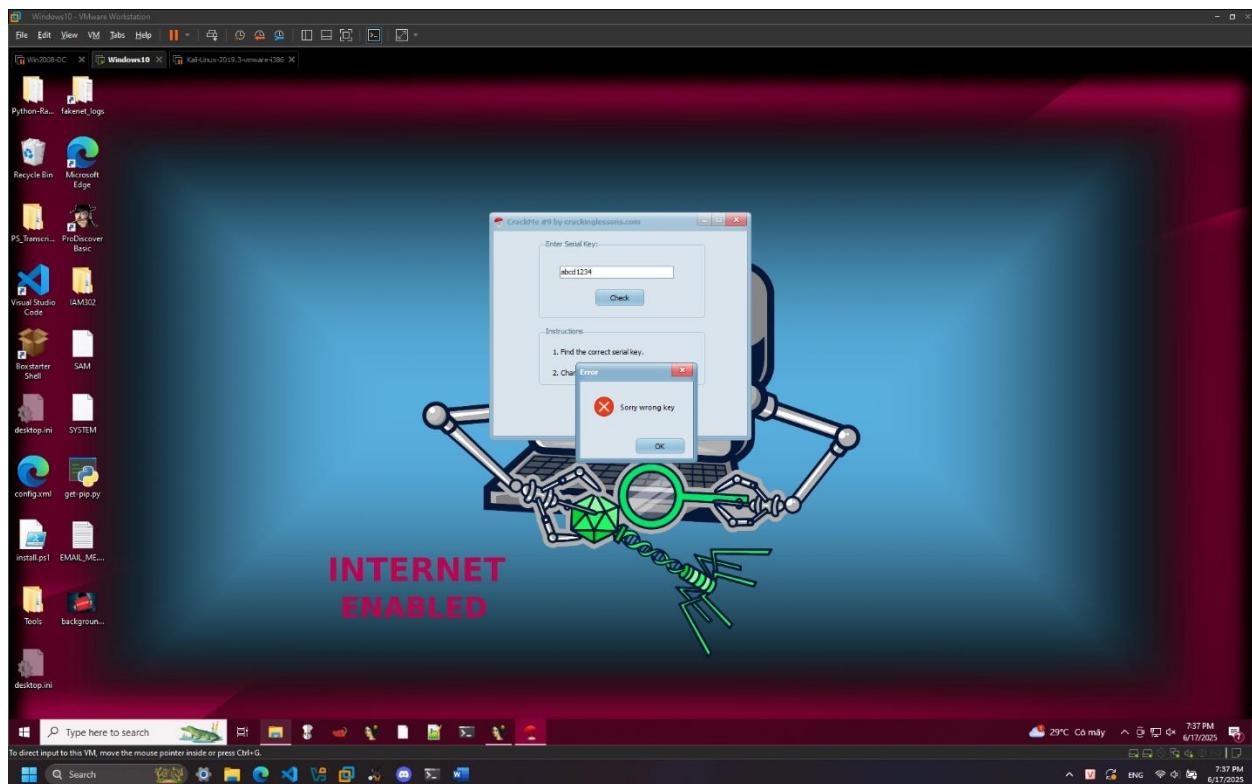
Run the RansomWare.py file to test:



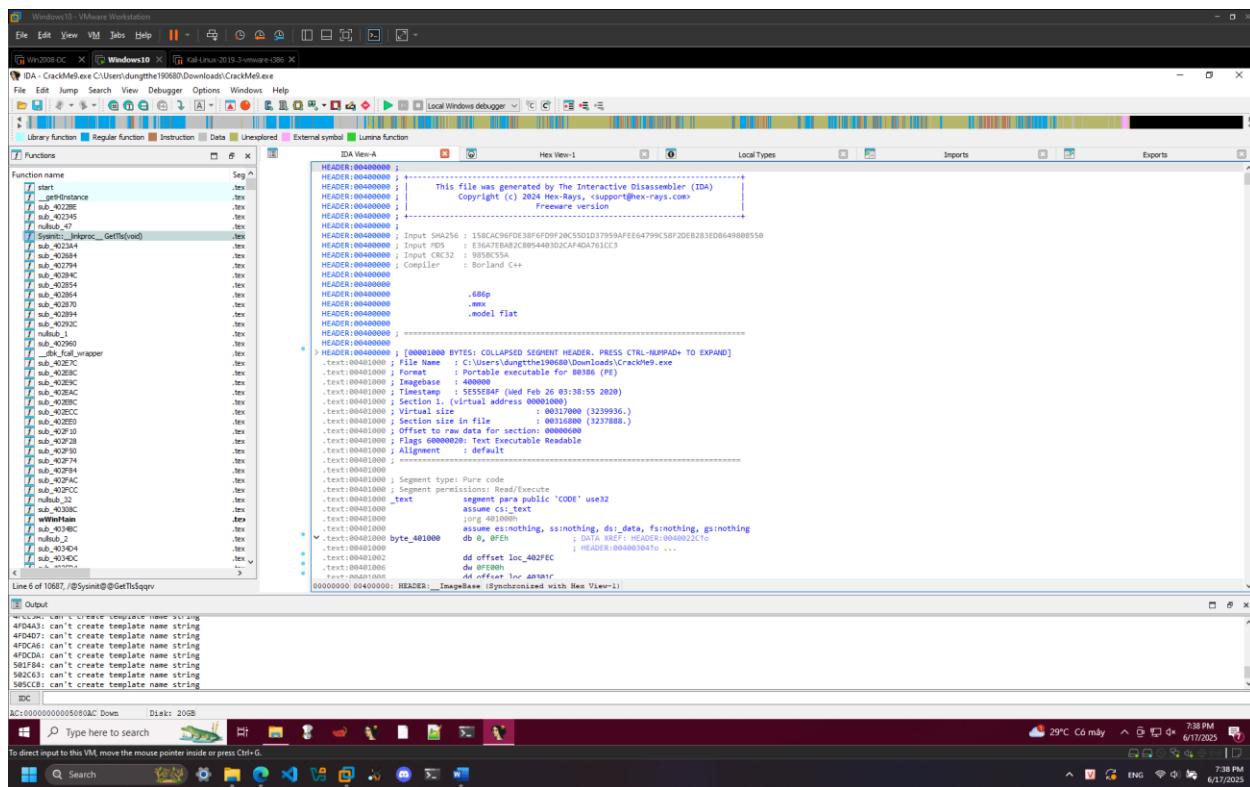


CrackMe #9

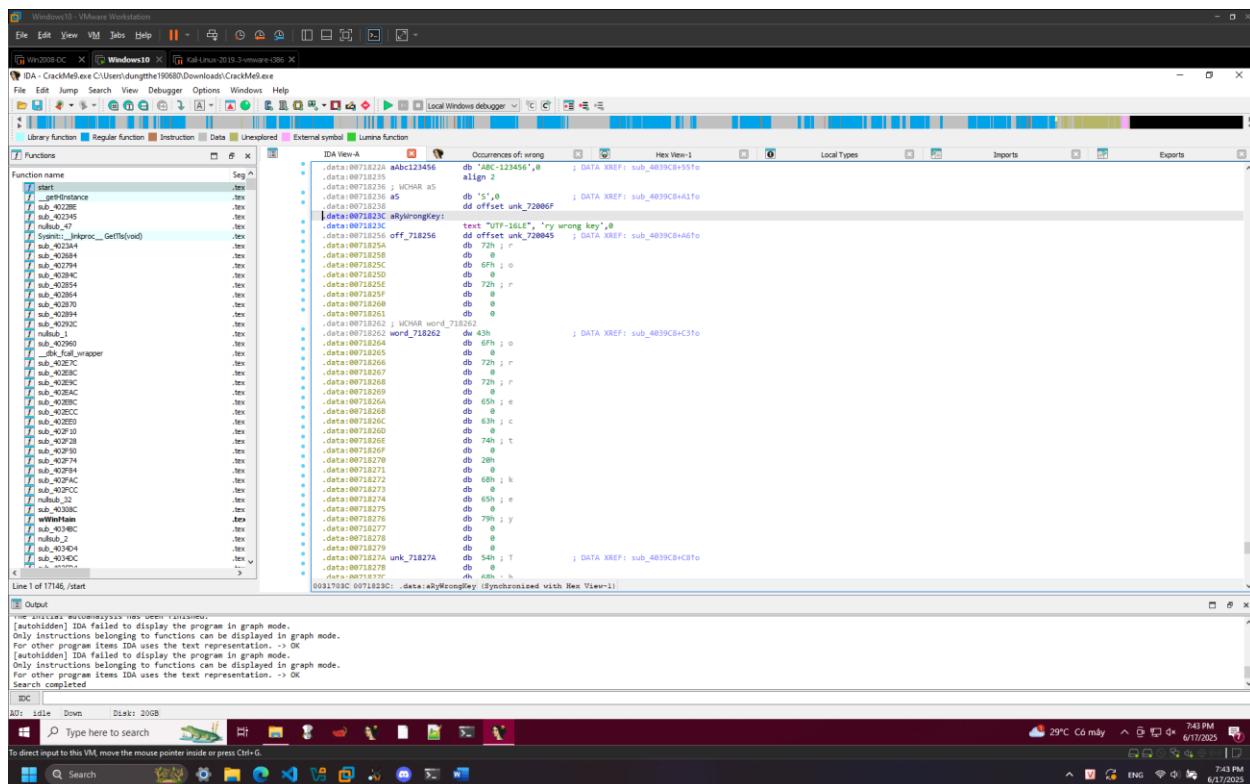
Đầu tiên em thử chạy chương trình và nhận được thông báo có từ khóa “wrong”:



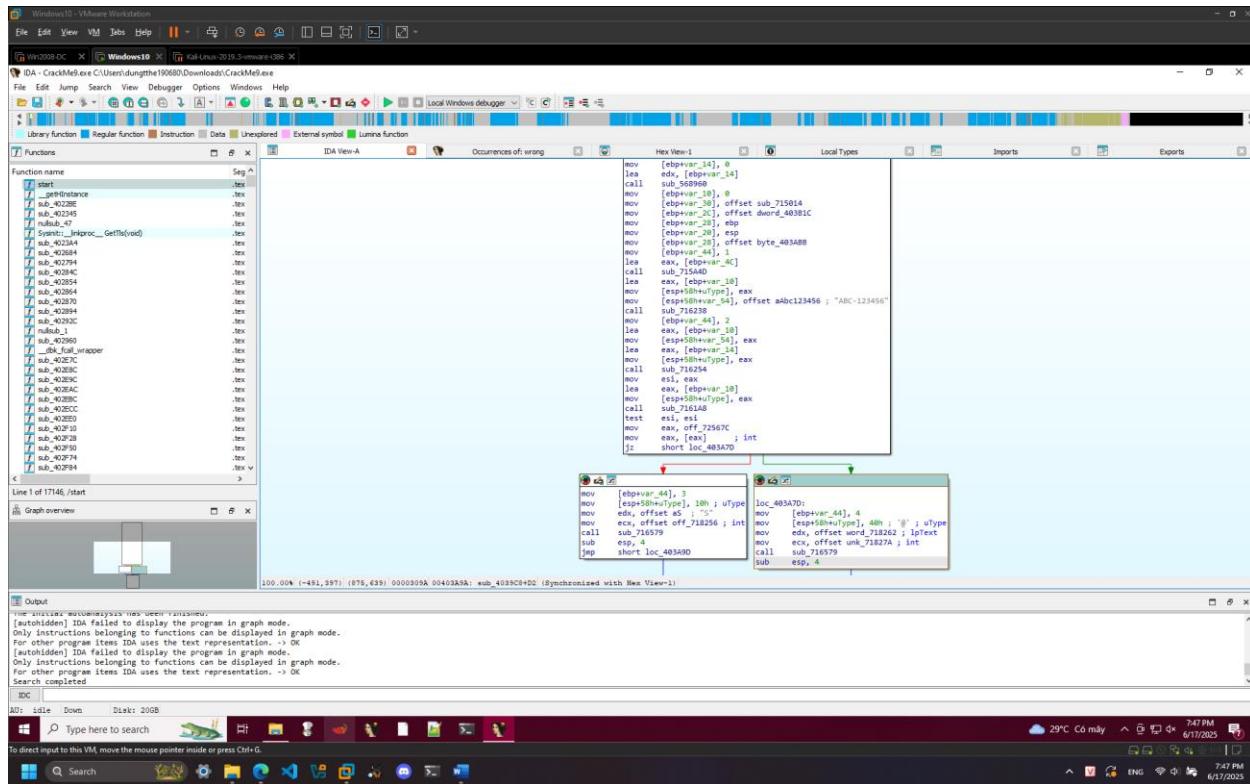
Sau đó em mở phần mềm IDA và tiến hành dịch ngược file:



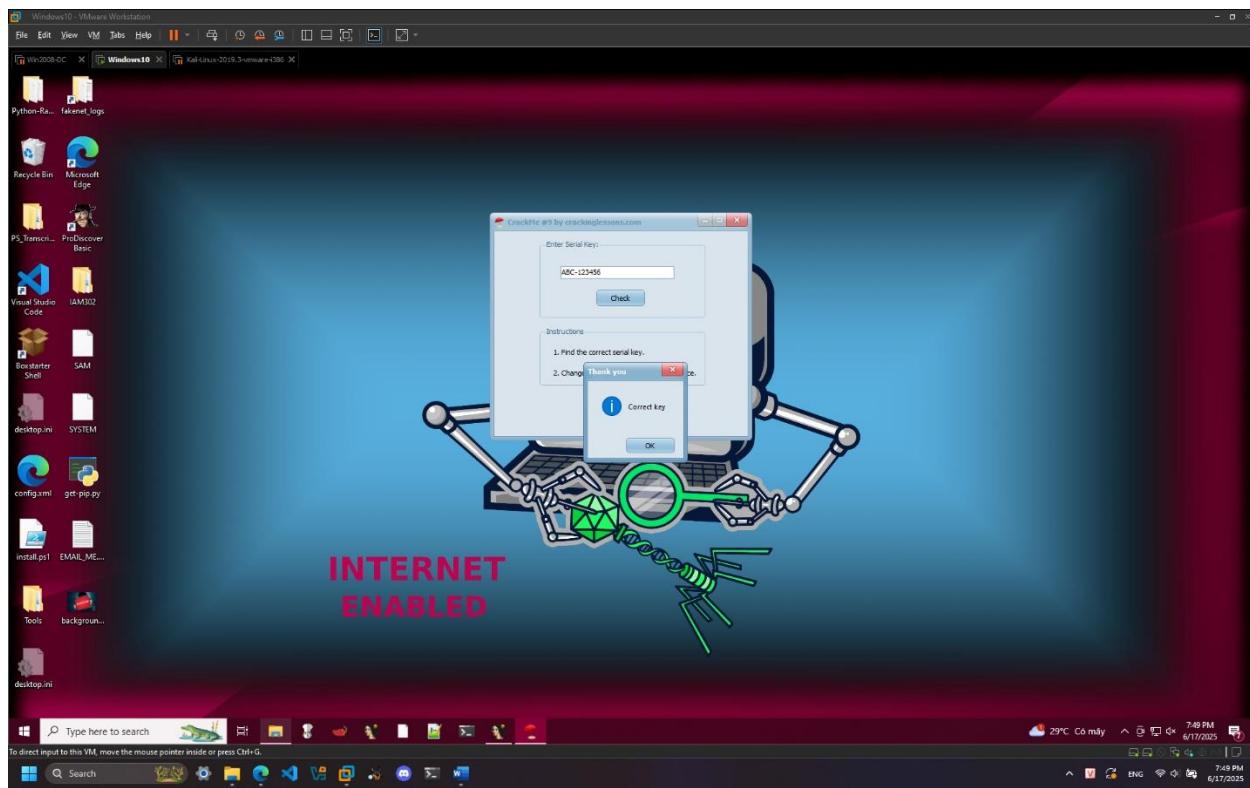
Em search từ khóa “wrong” và được điều hướng đến đoạn code này:



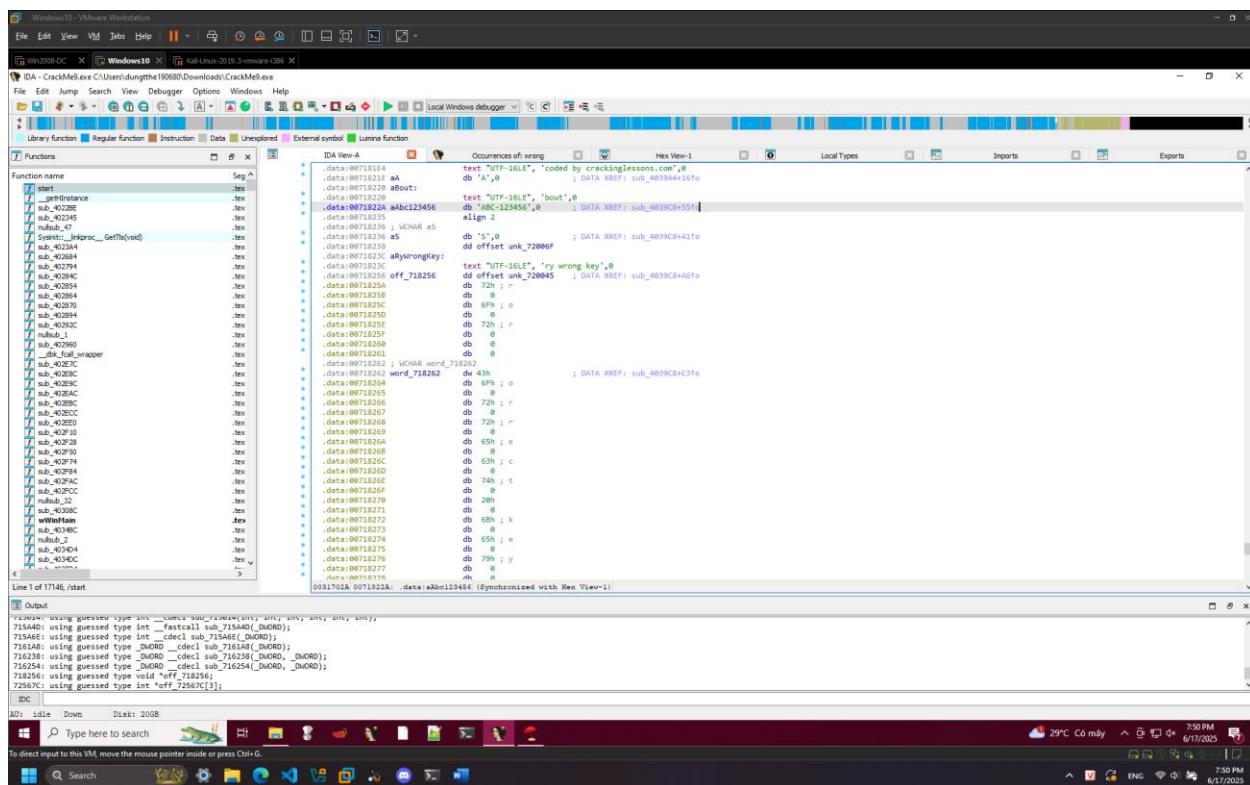
Có thể thấy thông báo mật khẩu chưa chính xác đã bị chia nhỏ thành nhiều phần khác nhau, em bấm vào phần đầu tiên của thông báo thì được điều hướng đến đoạn code này:



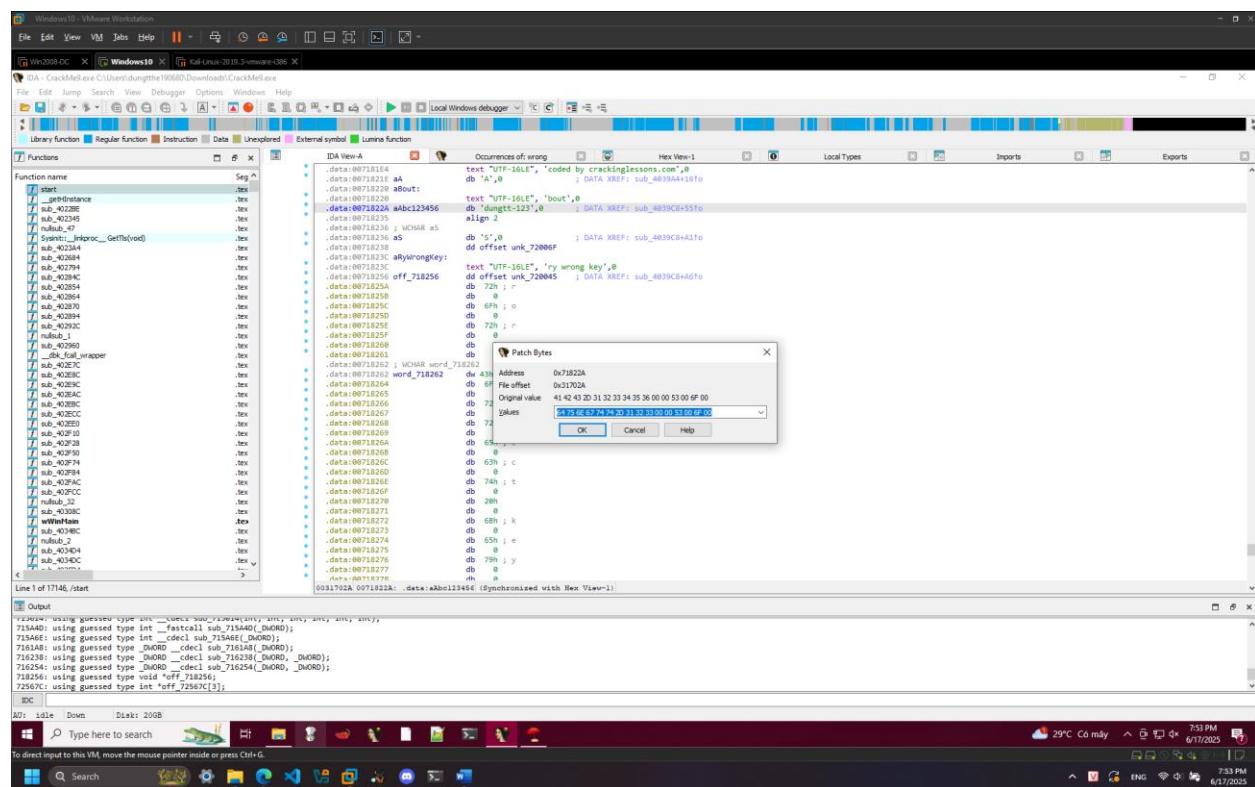
Từ đoạn code trên có thể suy ra mật khẩu chính xác là “ABC-123456”, được lưu trong biến “aAbc123456”. Chạy lại chương trình và nhập mật khẩu vừa tìm được, em nhận được thông báo mật khẩu chính xác:



Để thay đổi mật khẩu, em bấm vào biến “aAbc123456” và được điều hướng đến đoạn code này:



Em sửa mã hex của mật khẩu cũ để được mật khẩu mới là “dungtt-123”:



Lưu lại, chạy chương trình và nhập mật khẩu mới, em nhận được thông báo mật khẩu chính xác:

