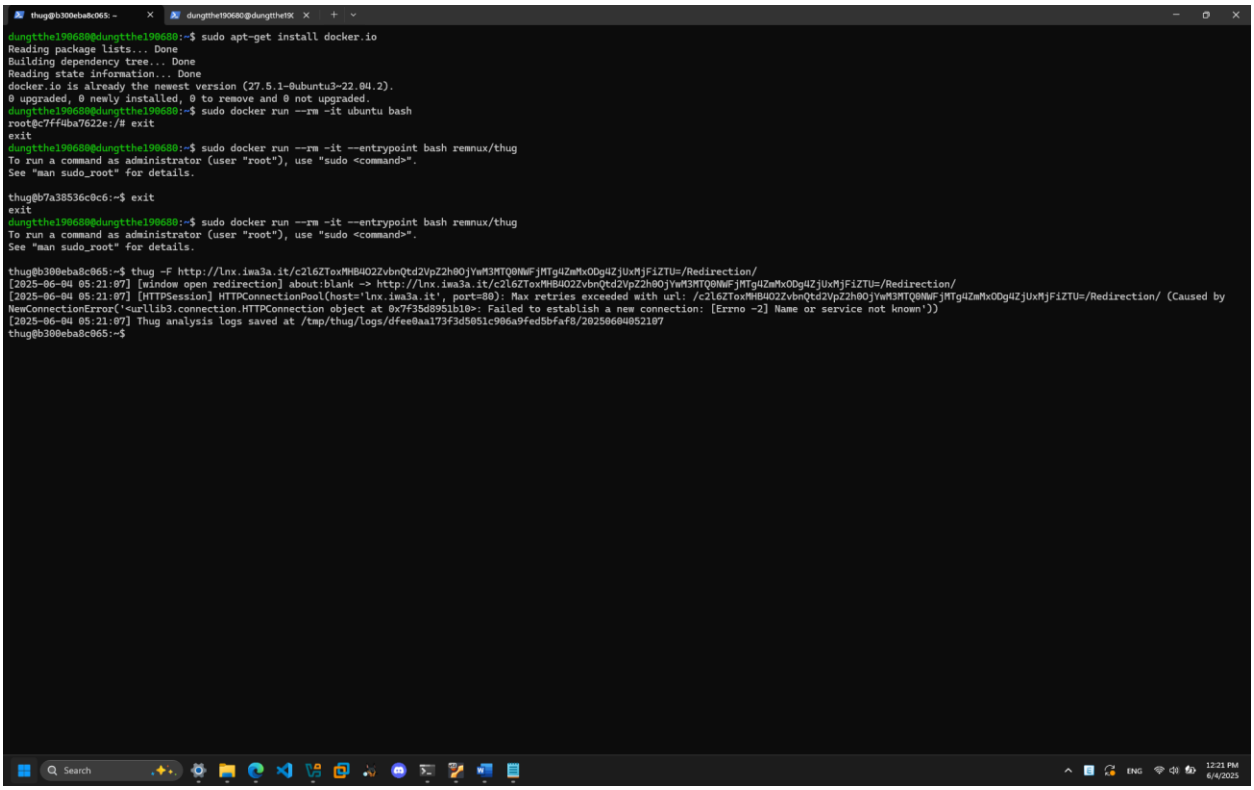
Họ và tên: Trần Trí Dũng

Mã số sinh viên: HE190680

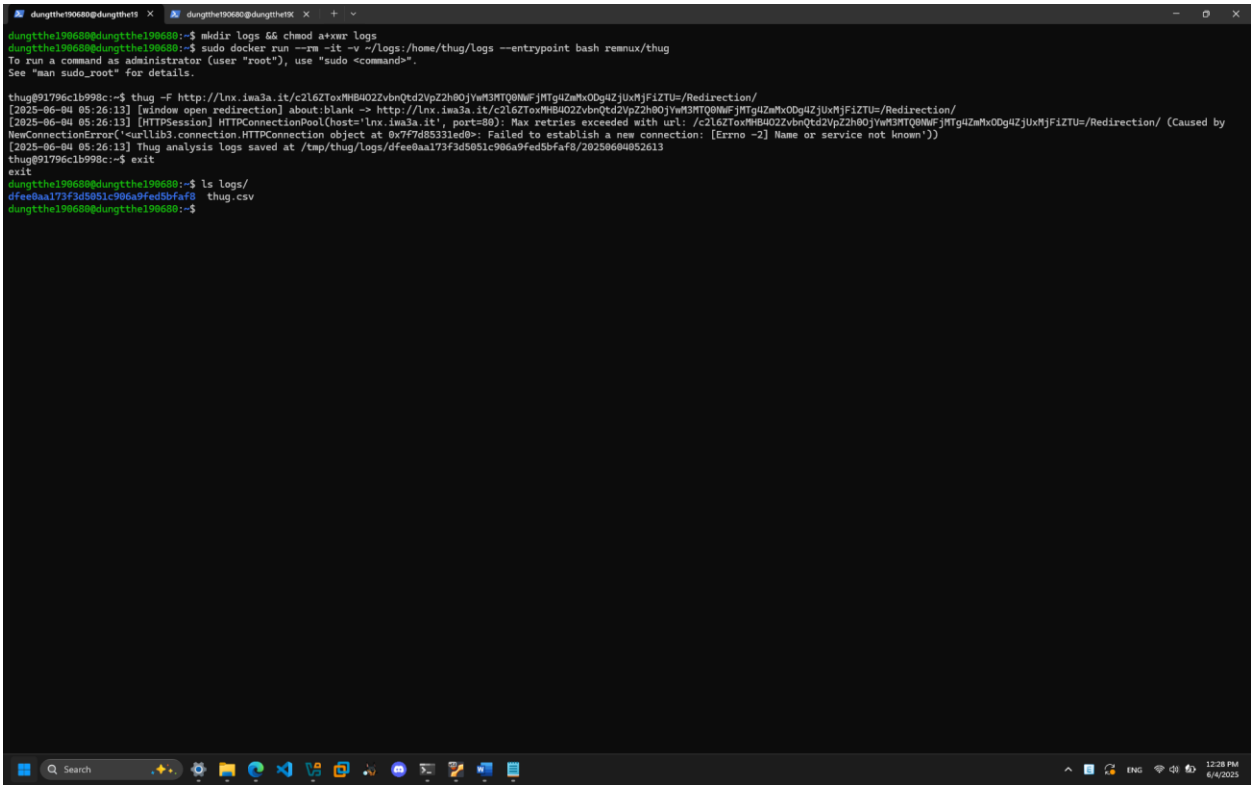
Lớp: IA1901

Lab 7:

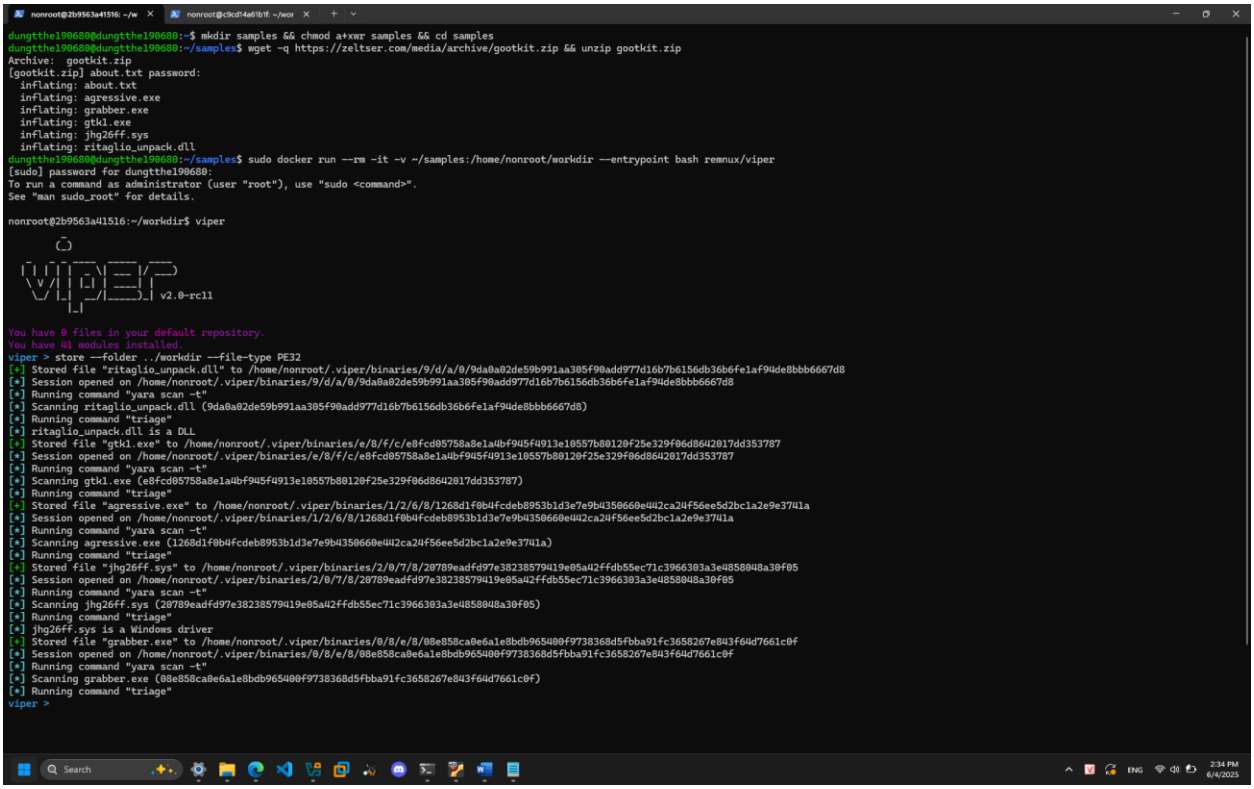
Install Docker.io -> Launch a transient instance of an Ubuntu container -> Launch the Thug honeyclient container:

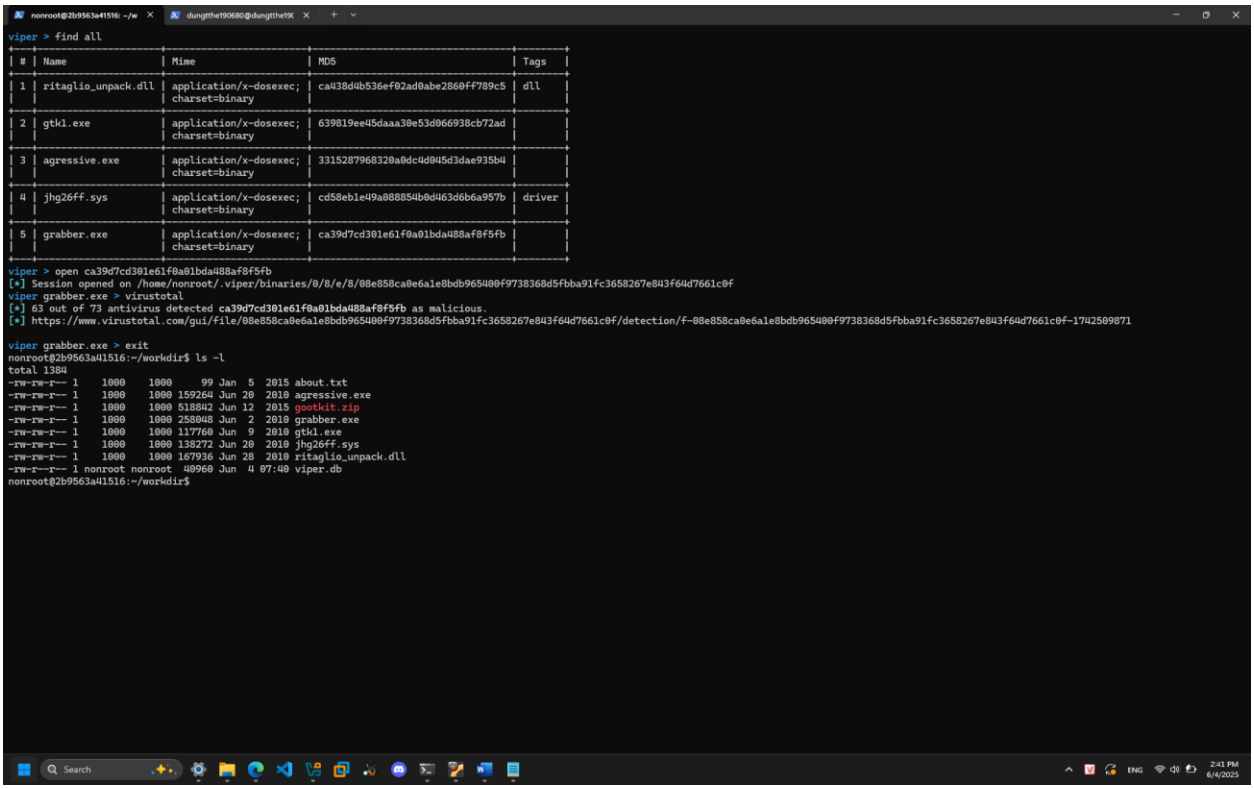


Create the directory on the underlying host and make it world-accessible -> Use “-v” to map the host’s directory into the container:

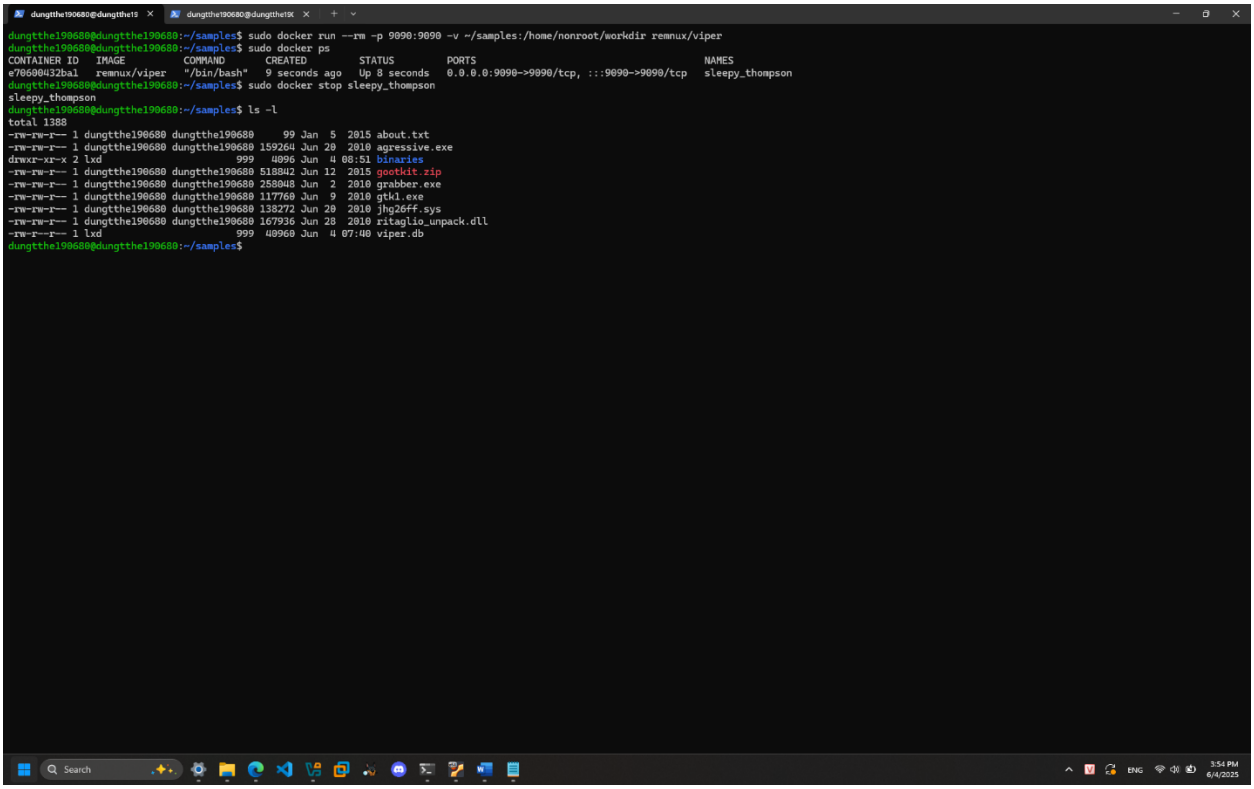


Store data on underlying host while running apps in transient environments:

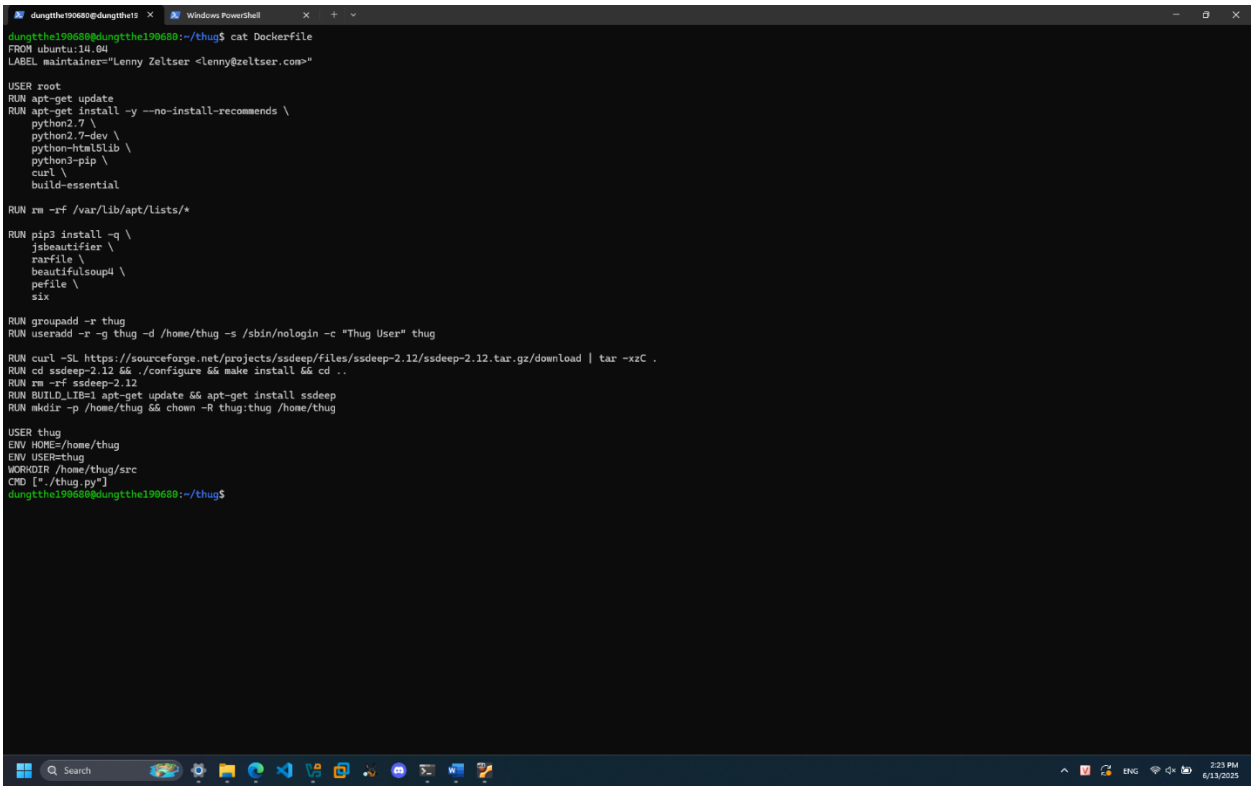




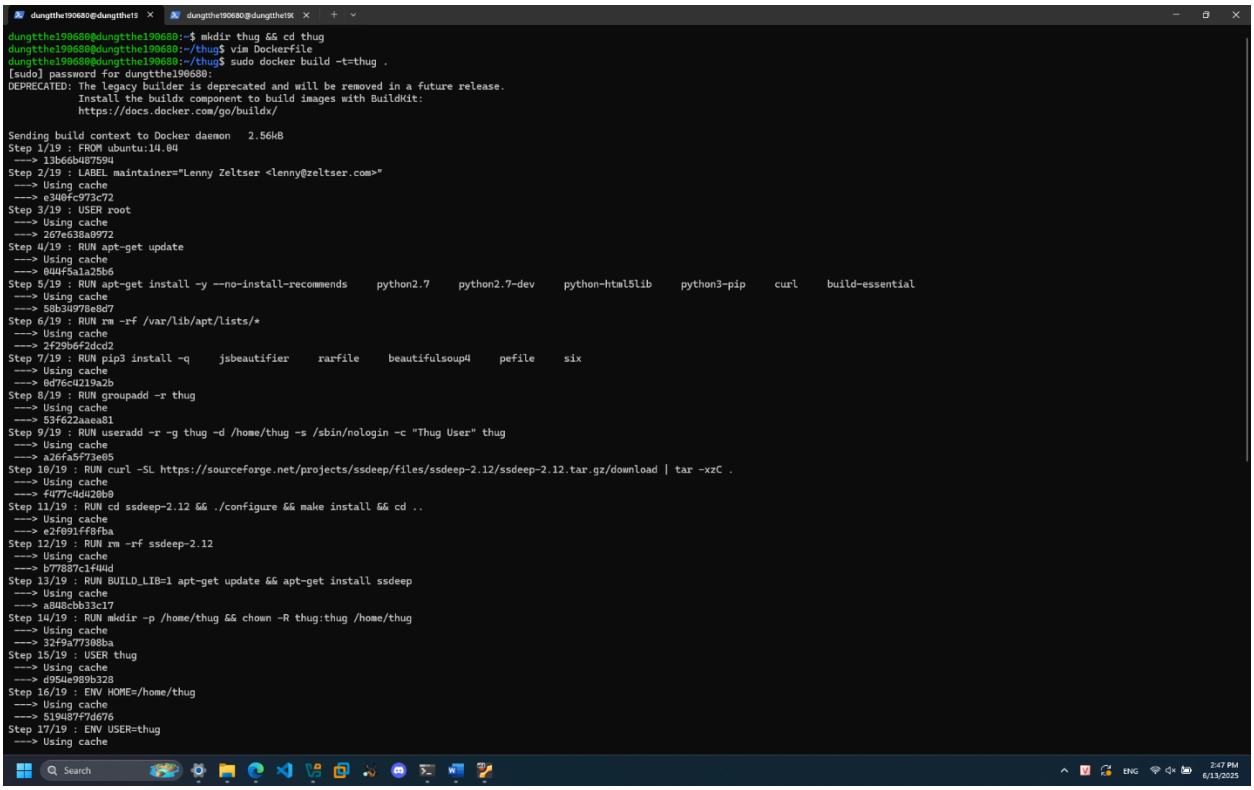
Expose container’s TCP port 9090 to interact with the application from localhost -> Use “-p” to access network ports within a container -> Use “ps” to show running containers and “stop” to stop them:



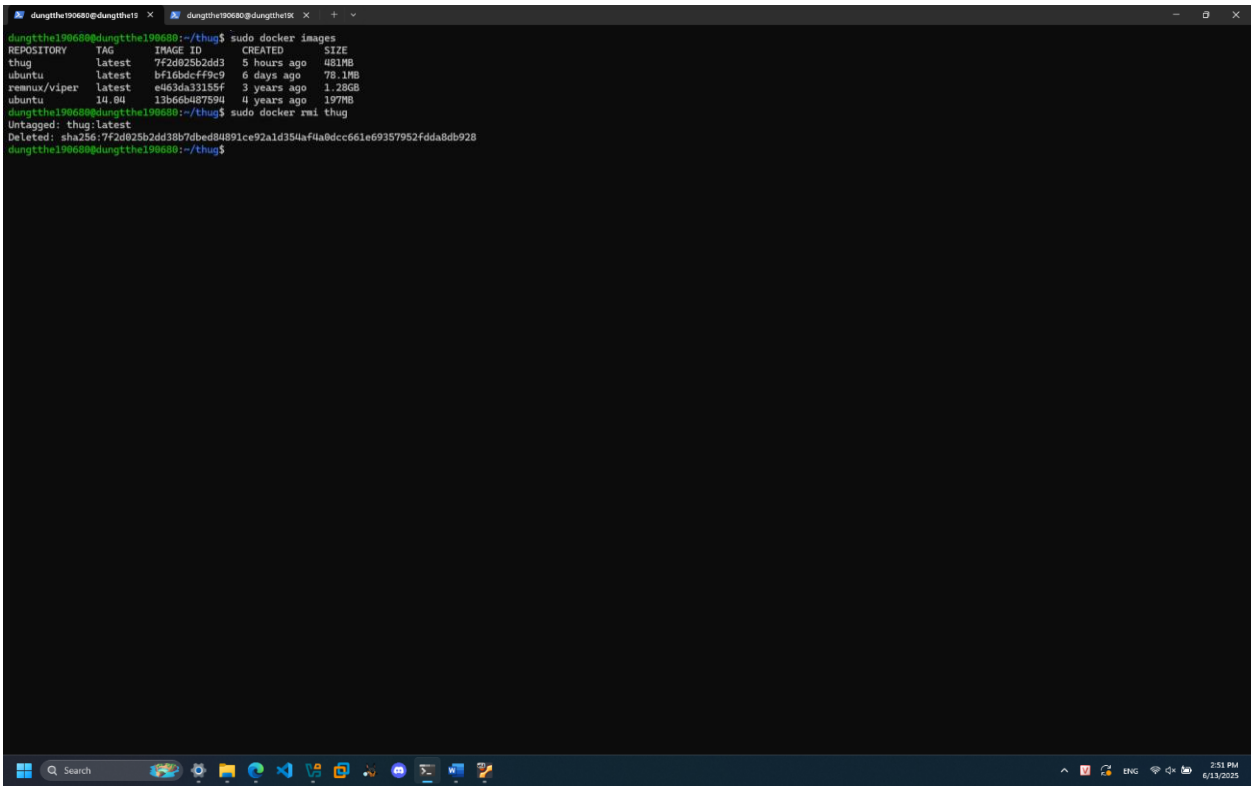
Create Dockerfile:



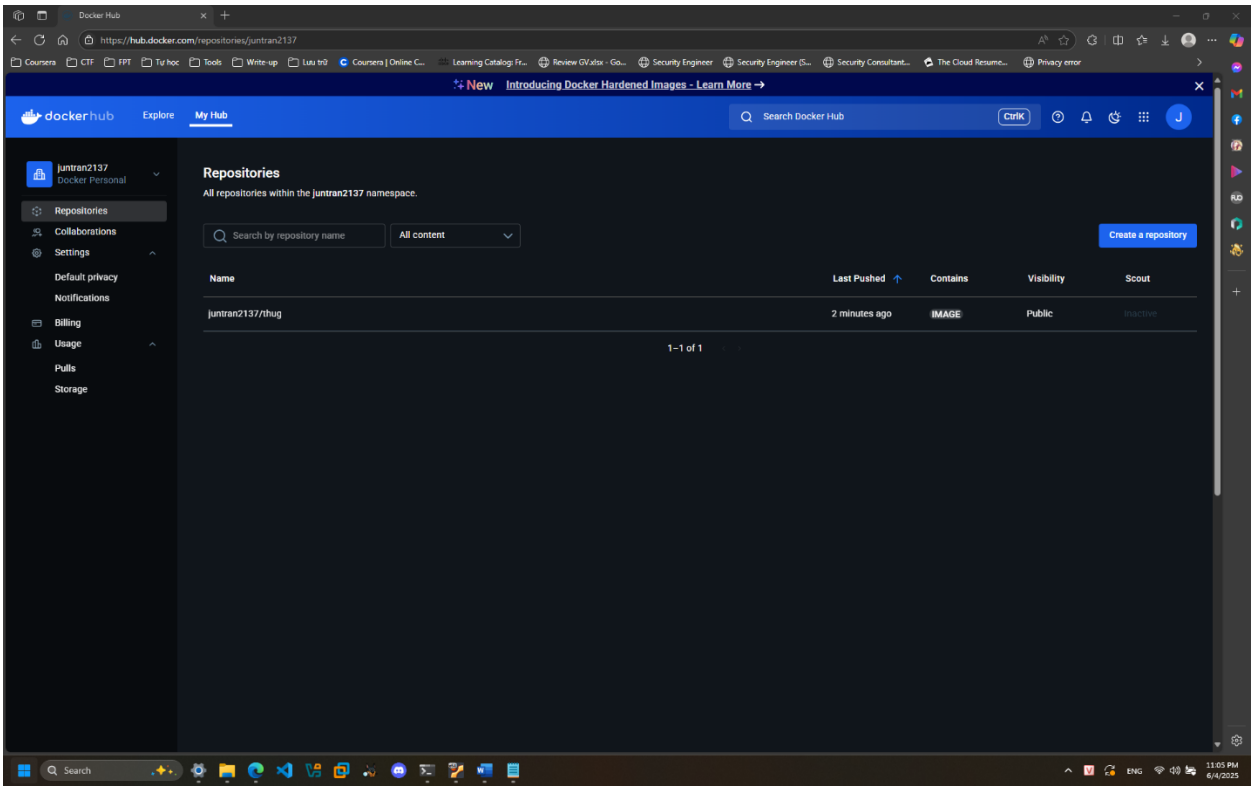
Use “docker build” to build the image out of the Dockerfile:



Use “docker images” and “docker rmi” to list and remove images:

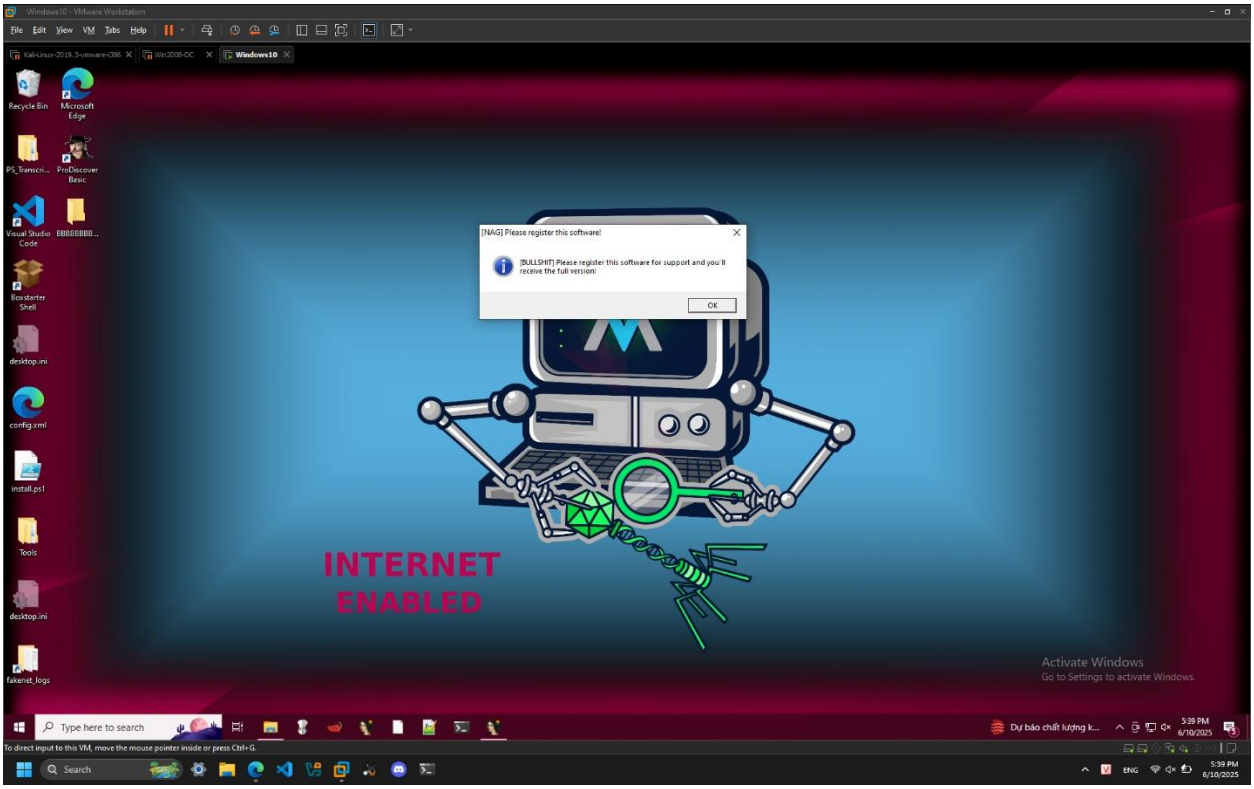


Share images via the public Docker Hub registry:

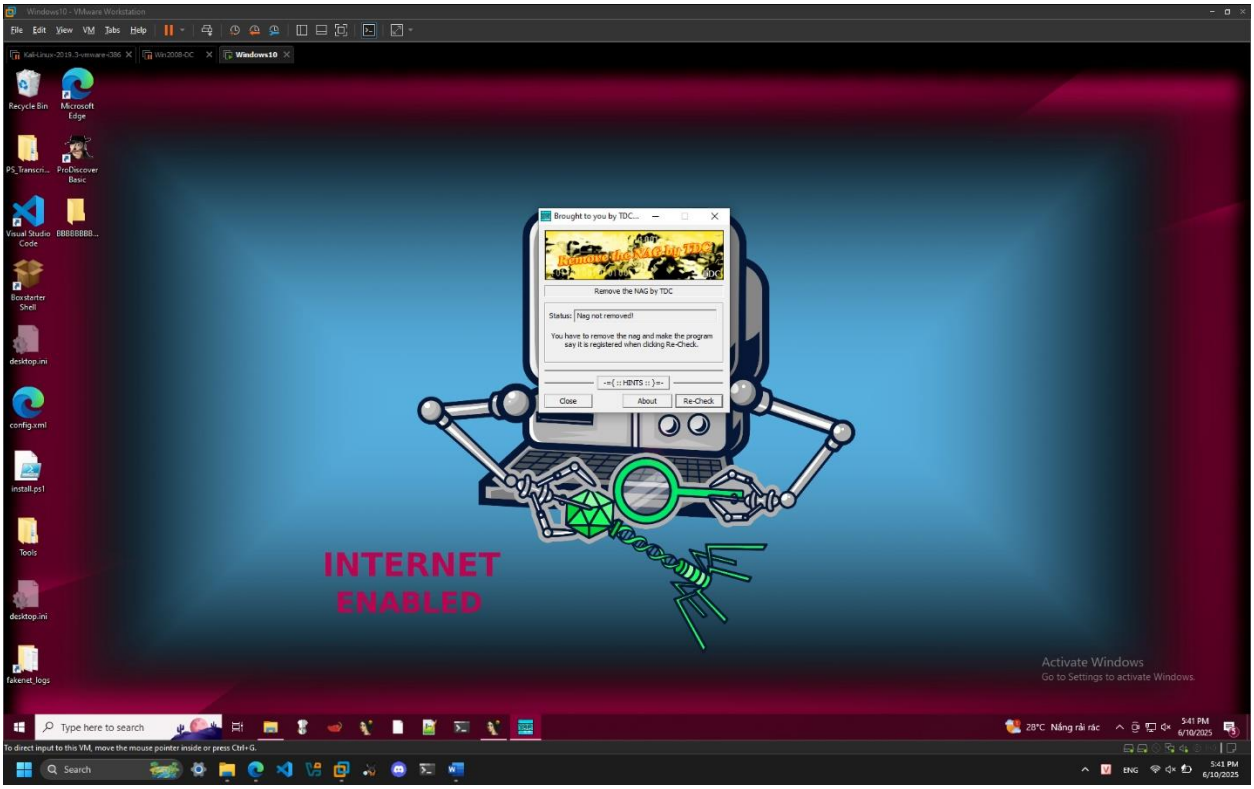


CrackMe #6

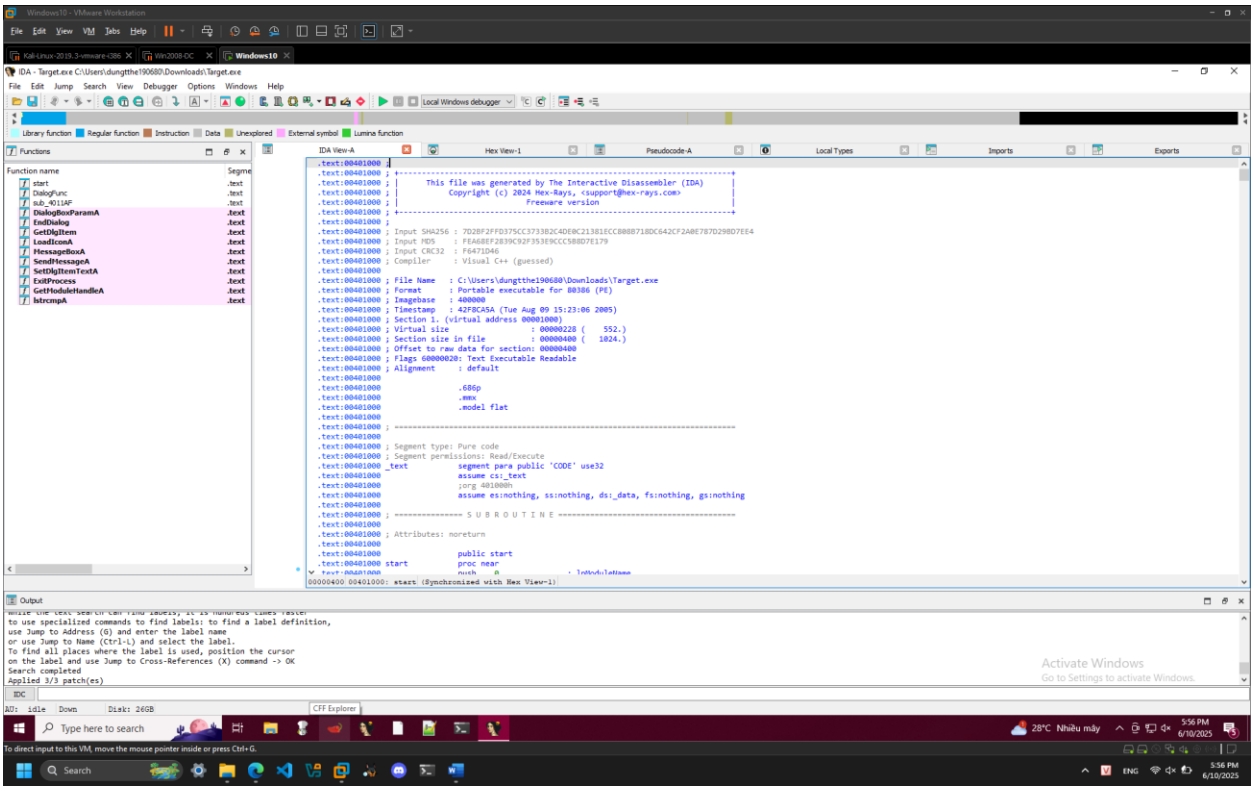
Đầu tiên em thử chạy chương trình và nhận được thông báo có từ khóa “BULLSHIT”:



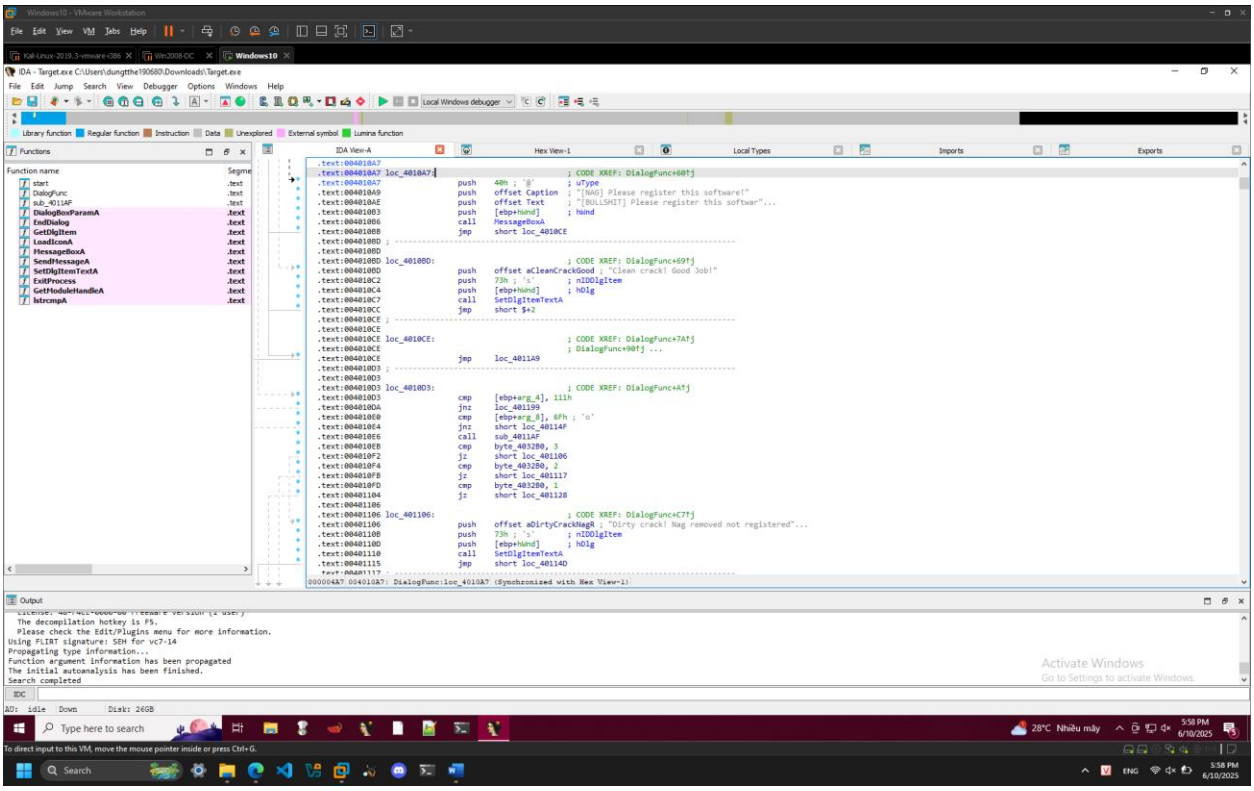
Sau khi tắt thông báo đầu tiên thì em nhận được thông báo khác là Nag chưa được loại bỏ:



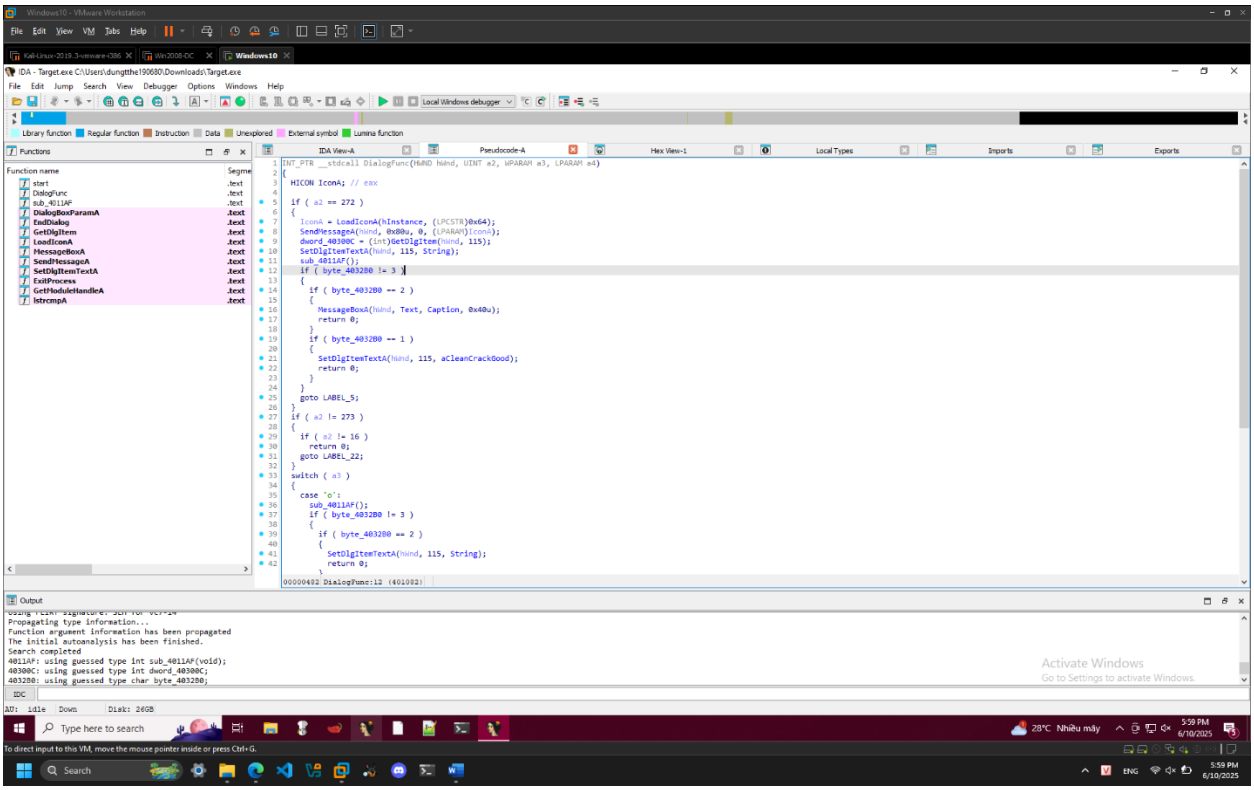
Em mở phần mềm IDA và tiến hành dịch ngược file:



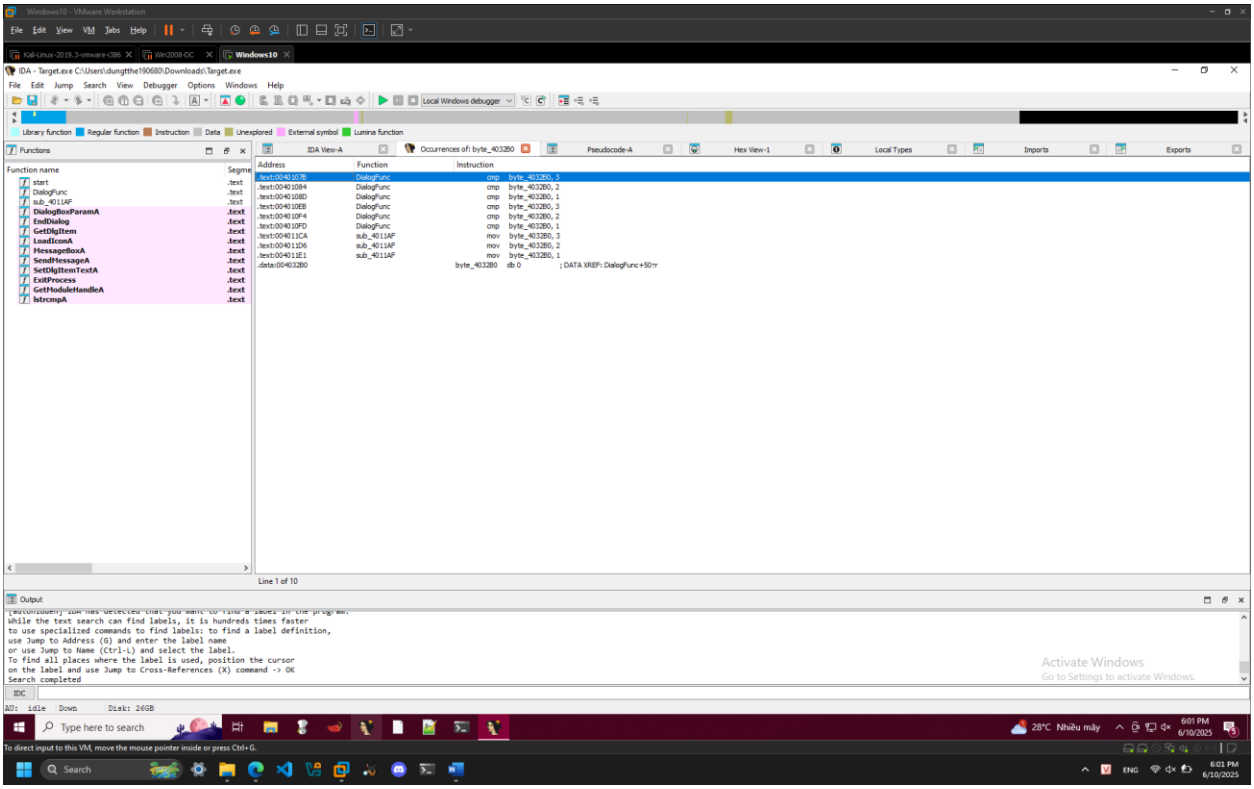
Em search từ khóa “BULLSHIT” và được điều hướng đến đoạn code này:



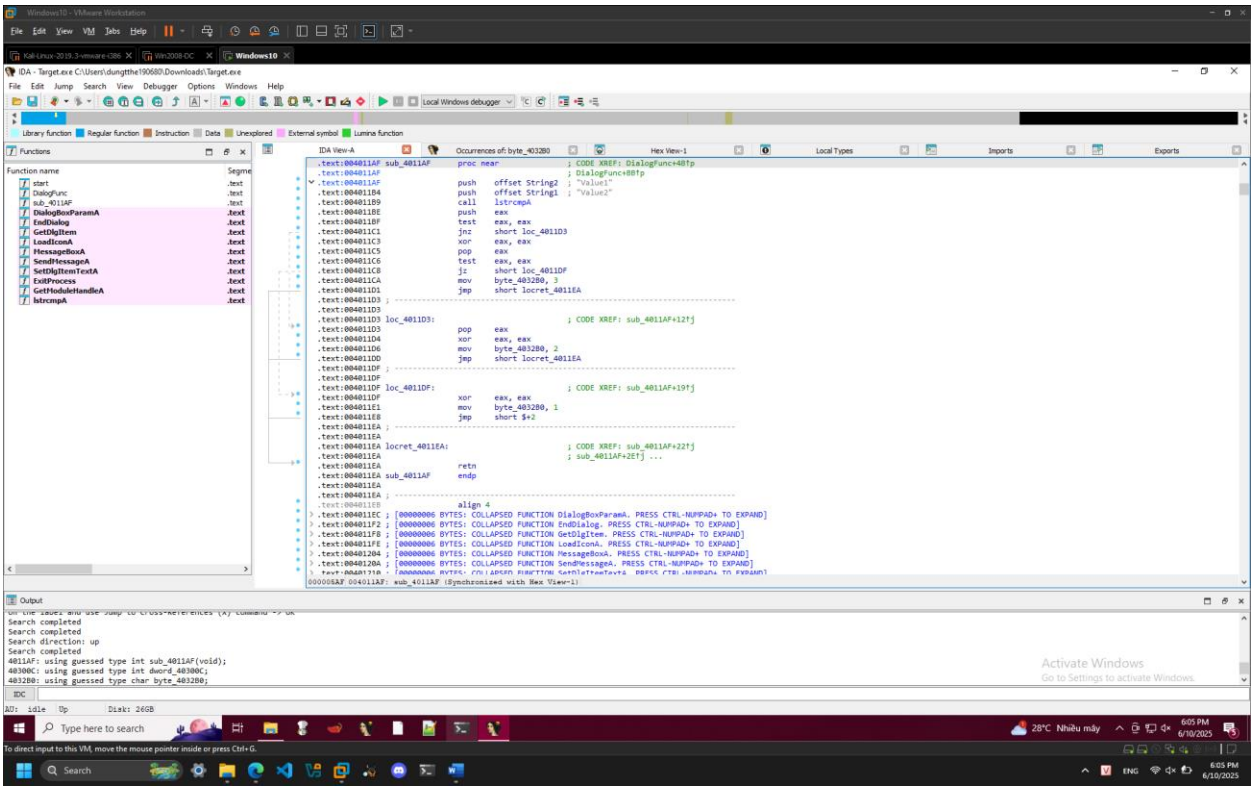
Em bôi đen đoạn code và decompile sang pseudocode thì nhận được đoạn code này:



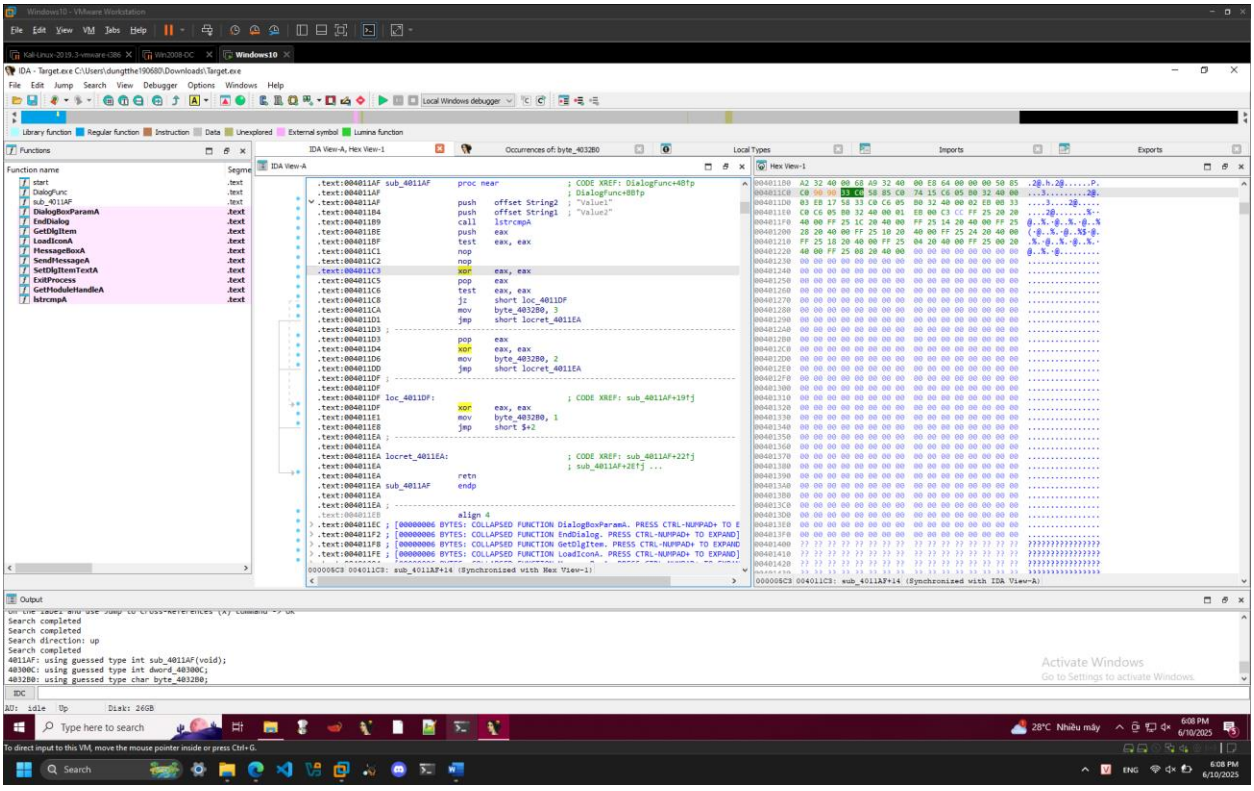
Có thể thấy thông báo được hiển thị phụ thuộc vào giá trị của biến byte_4032B0, Nag được loại bỏ hoàn toàn khi giá trị của biến bằng 1, vì vậy em search tiếp từ khóa “byte_4032B0”:



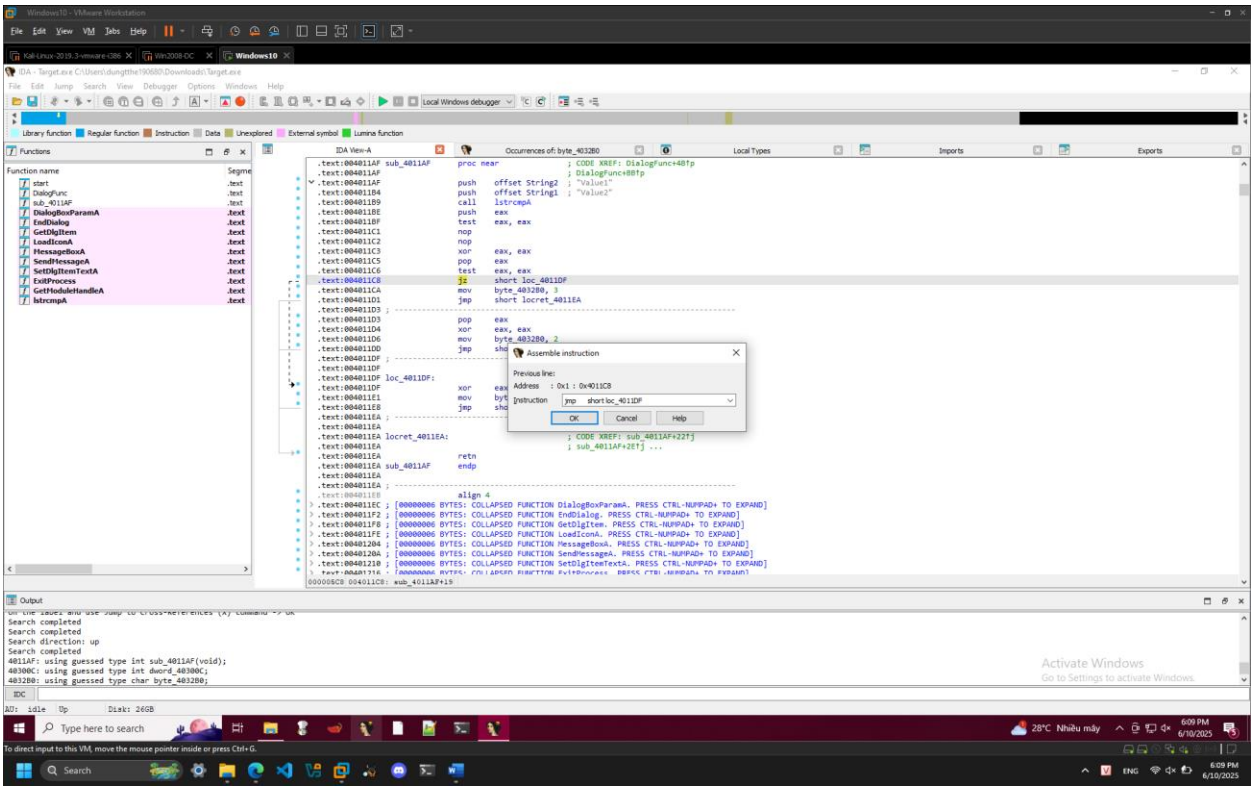
Em bấm vào lệnh gán giá trị cho biến và được điều hướng đến đoạn code này:



Để cố định giá trị biến bằng 1, đầu tiên em xóa lệnh nhảy đến lệnh gán giá trị biến bằng 2 bằng cách sửa mã hex thành 90 (nop):



Sau đó em sửa lệnh nhảy đến lệnh gán giá trị biến bằng 1 thành luôn xảy ra:



Lưu lại và chạy chương trình thì thấy Nag đã biến mất và nhận được thông báo đã loại bỏ Nag thành công: