LAB 3

Fuzzing - Reverse Engineering – Cryptography

Link youtube: https://youtu.be/cSy98cjPPqU

Họ tên và MSSV: Lý Gia Hưng – 1050080053

Học phần: Bảo mật mạng máy tính và hệ thống

- Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho TẤT CẢ các bài thực hành của

môn này.

- Bài nộp phải ở dạng docx, hình minh họa phải rõ ràng chi tiết. Hình minh hoạ chỉ cần chụp ở nội

dung thực hiện, không chụp toàn màn hình.

- Trình bày chi tiết từng bước 1

- Quay lại quá trình làm bài, quay luôn faces của mình đưa video vào

youtube và add link youtube vào trong file word, không gửi qua

google drive, sv không có video sẽ không được chấm bài.

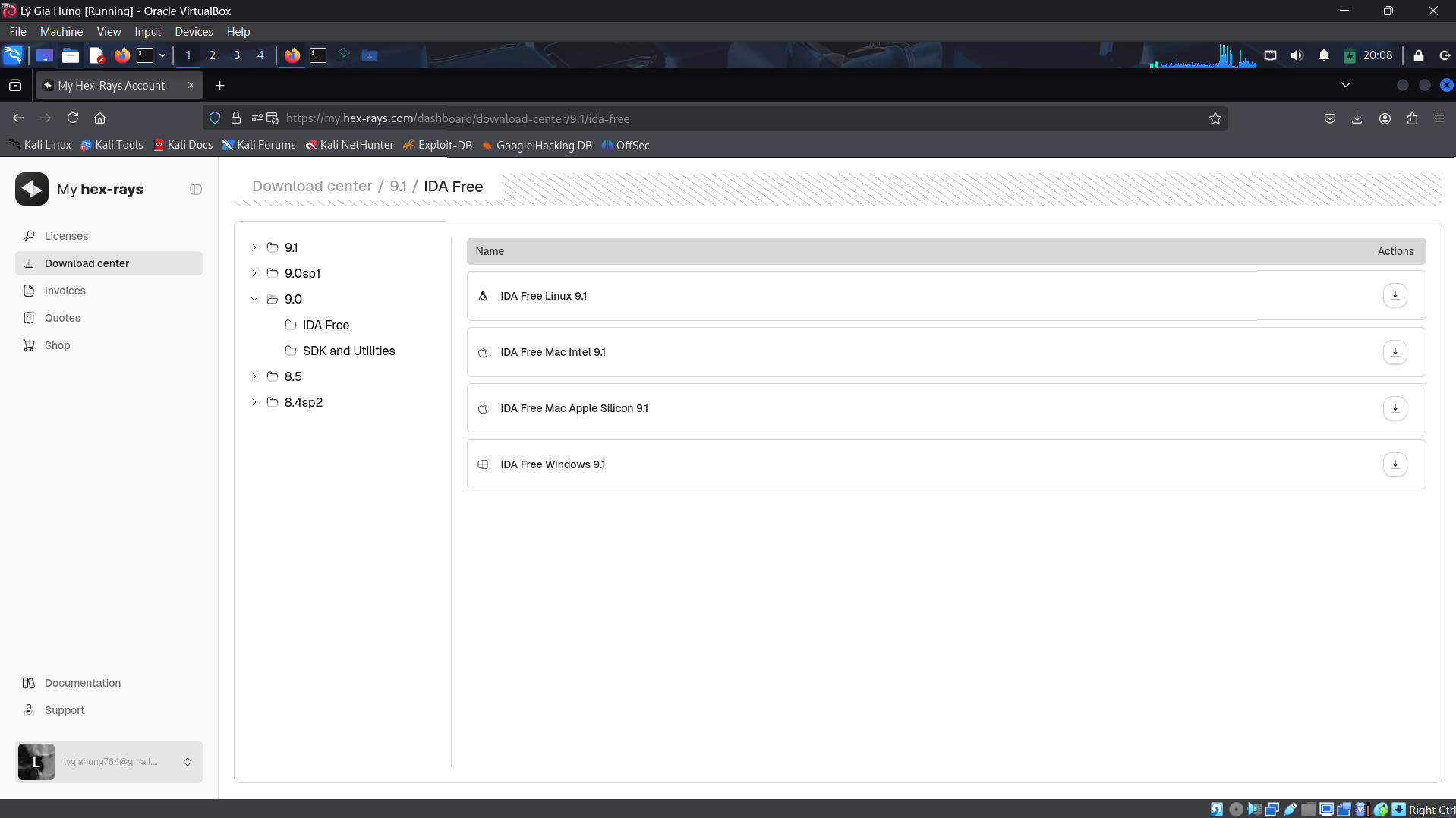
Lưu ý: sử dụng tài khoản là mã số sinh viên (đã tạo ở Câu 1.4 - Lab01) để thực hiện tất cả các câu trong

bài thực hành. Tất cả các câu trong bài thực hành này được thực hiện trên Kali Linux

Câu 1: Thực hiện kỹ thuật Reverse Engineering với công cụ IDA Free

1.1. Cài đặt IDA Free vào Kali Linux. Tải file cài đặt (ví dụ: idafree83\_linux.run):

- Nếu không cài được vào trang web IDA Free đăng ký tải khoản tải về

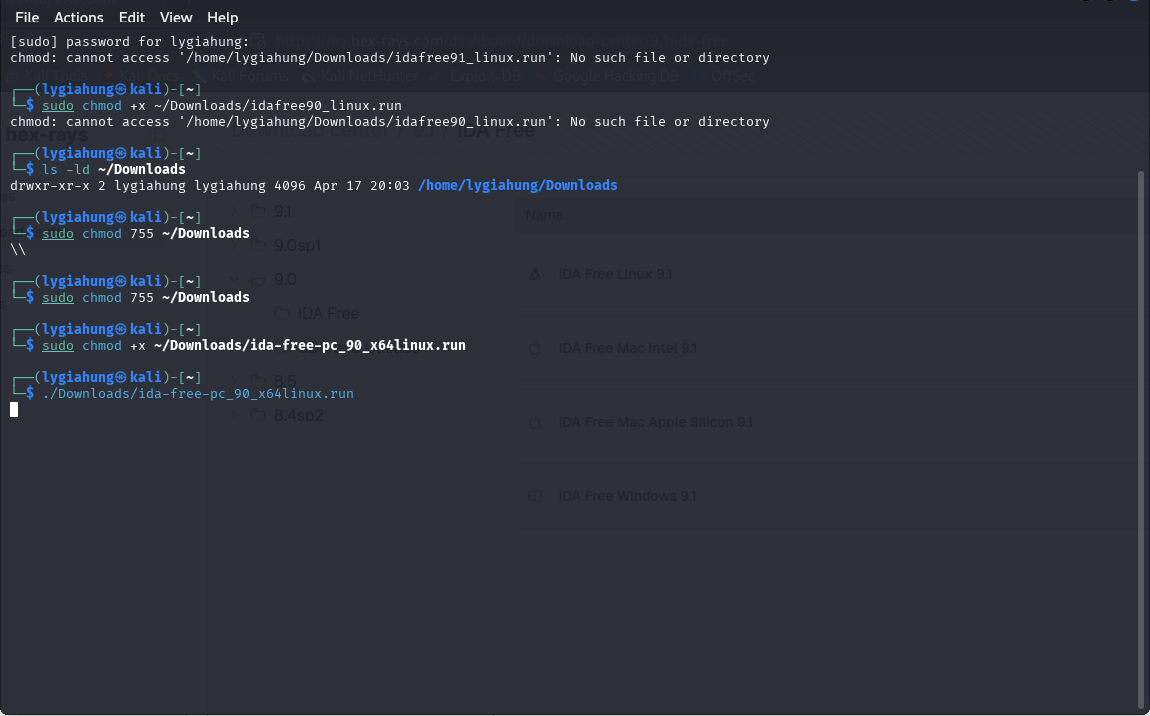


- Sau đó chạy lệnh bên dưới sửa lại tên theo phiên bản đã tải

$sudo chmod +x ~/Downloads/tên phiên bản.run

$~/Downloads/tên phiên bản.run

➢ Tài và cài đạt IDA



- Xong ta sẽ thấy giao diện cài đặt



➢ Thực hiện các bước theo yêu cầu. IDA Free sẽ được cài đặt ở thư mục cá nhân của người

dùng.

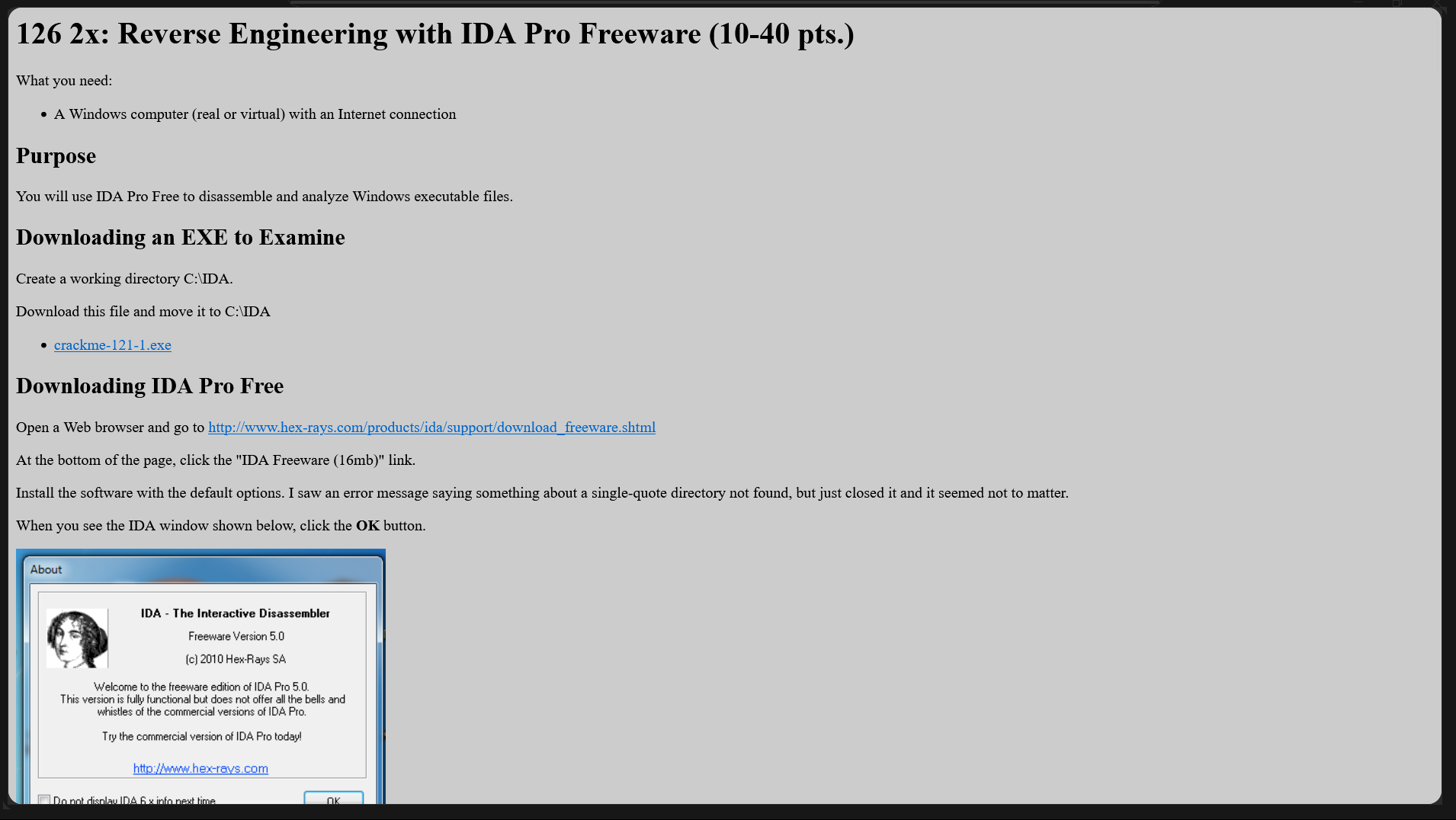
1.2. Nhấp vào link này 126 Proj 2x: Reverse Engineering with IDA Pro Freeware (10-40 pts.) tải các file(nếu làm trên window)

về tạo file Lab03.zip.

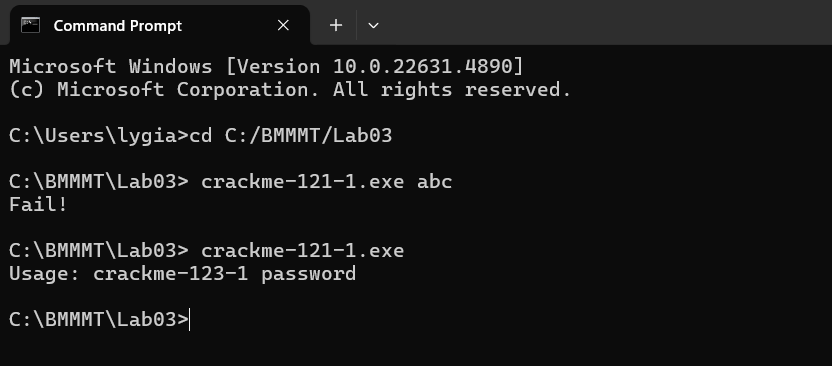
- Nếu thiếu file dll thì vào link này tải https://www.dll-files.com/download/440e9fd9824b8e97d3ca2f34bd1bfbd1/msvcr100d.dll.html?c=VlVESnZCdkhpamd1ODZnbGhZTzN3UT09

Trên máy Windows, tải file Lab03.zip. Giải nén sẽ được thư mục crackme chứa 02 file crackme.exe và

msvcr100d.dll. Chạy file crackme.exe ở môi trường CMD với vài giá trị đầu vào khác nhau và xem kếtquả.



- Tải file .exe sau đó nén lại thành file Lab03.zip và chạy trong cmd

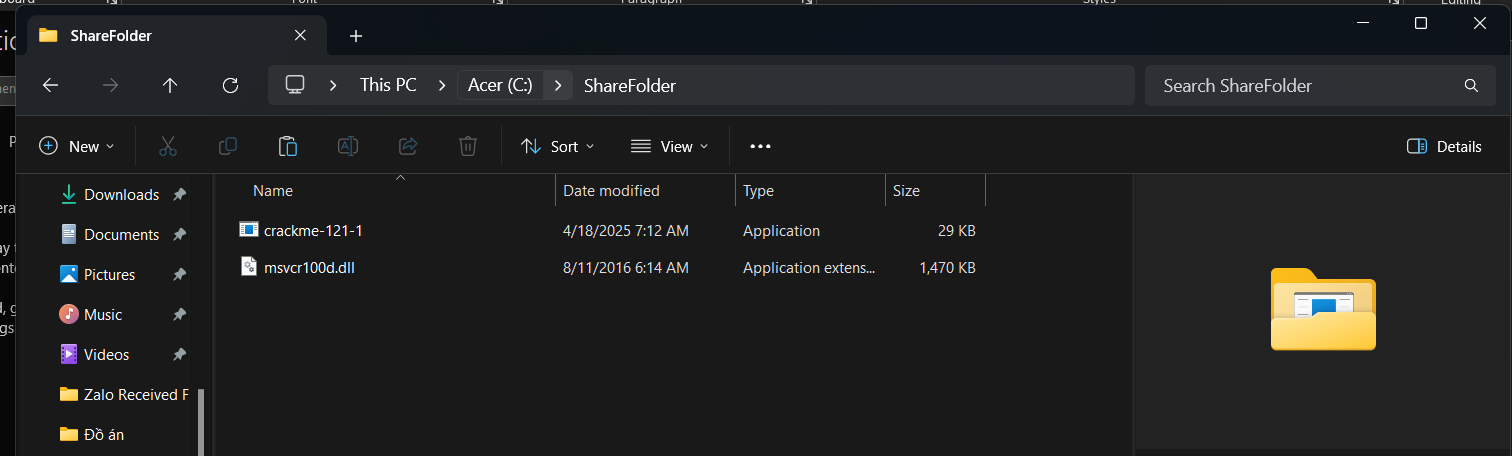


1.3. Di chuyển file crackme.exe vào máy ảo Kali Linux (sử dụng chức năng Shared Folders hoặc Drag

and Drop). Chạy IDA Free và mở file crackme.exe trên môi trường IDA Free.

➢ Dùng lệnh để copy file: $sudo cp share/crackme/crackme.exe .

- Tạo thư mục share trên window C:\SharedFolder và copy hết file từ Lab3 qua



- Bật chia sẻ file trong virtual box

 Tắt Kali VM nếu đang bật.

 Trong VirtualBox, chọn máy ảo Kali → **Settings** → **Shared Folders**

 Click icon + → chọn:

* **Folder Path**: C:\SharedFolder
* **Folder Name**: share
* **Mount automatically**: ✅
* **Make Permanent**: ✅

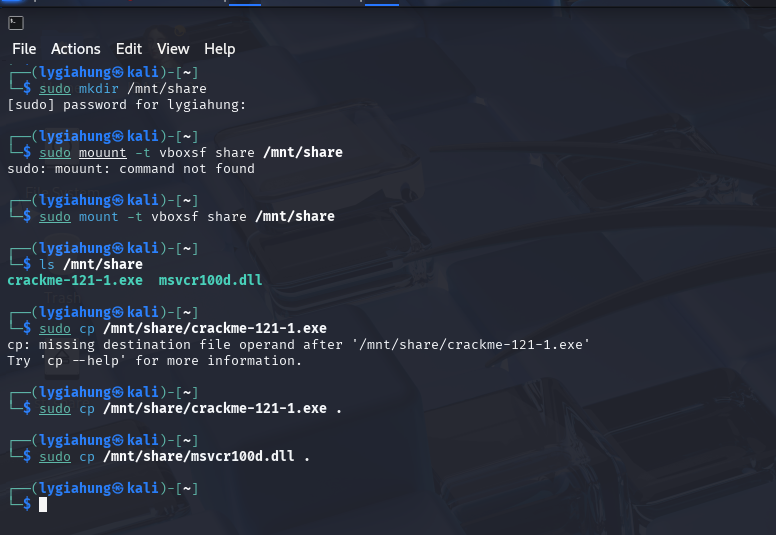
- Mount thư mục share trên kali

sudo mkdir /mnt/share

sudo mount -t vboxsf share /mnt/share

- Kiểm tra ls /mnt/share

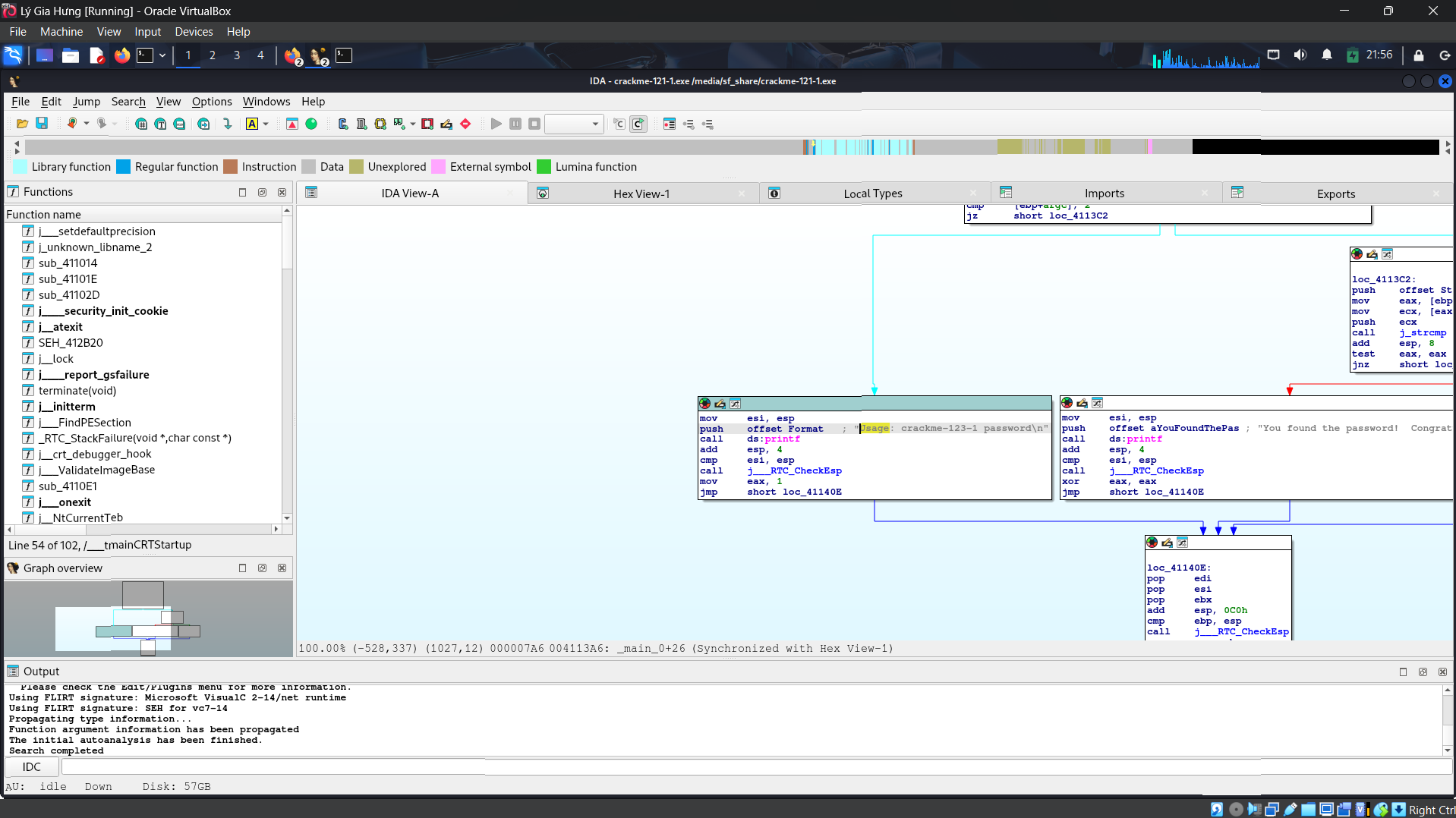
- copy sudo cp /mnt/share/crackme-121-1.exe .



1.4. Trên thanh menu, sử dụng chức năng “Search, Text” tìm kiếm với từ khóa “usage”. Trên cửa sổ

“IDA - View A” chọn “Fit window”. Chọn “Text view” hoặc “Graph view” để xem mã Assembly của

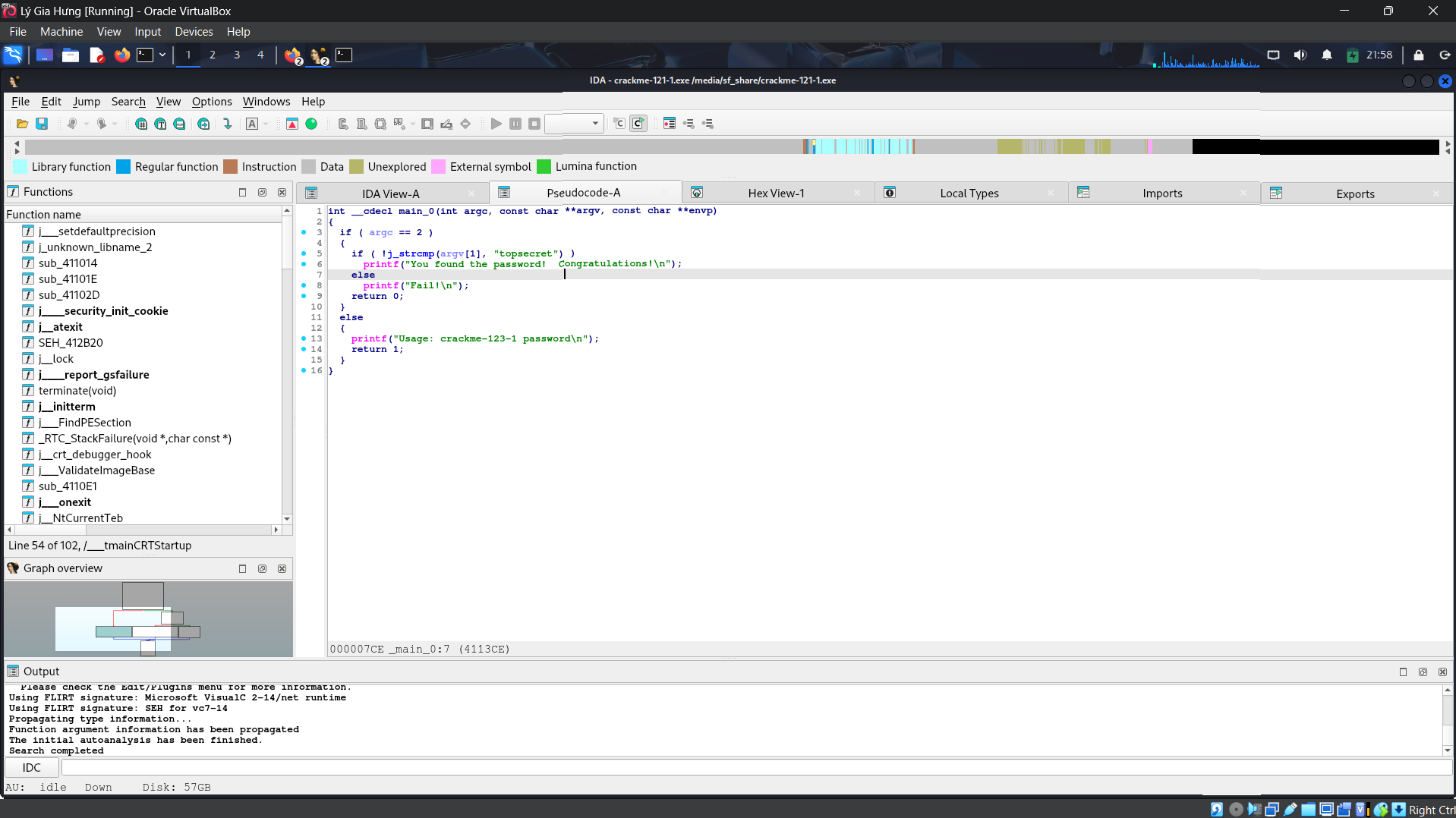
chương trình.

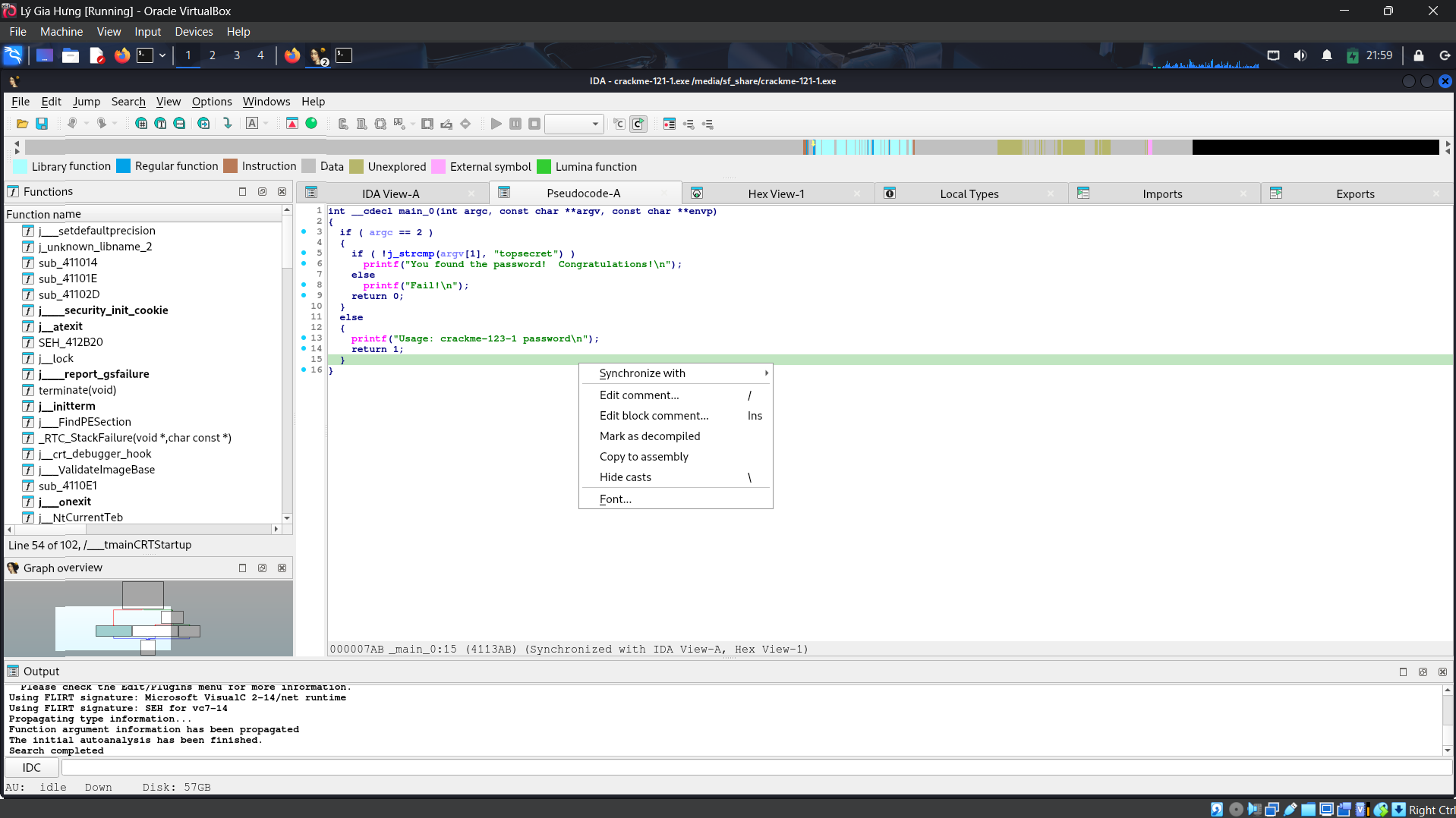


1.5 Trên thanh menu, sử dụng chức năng “View, Sub view, Generate pseudo code” (F5) để sinh mã giả của

crackme.exe. Trên cửa sổ “Pseudocode - A”, sử dụng chức năng “Synchronize with” để đồng bộ với “IDA

- View A” và “Hex - View 1”.

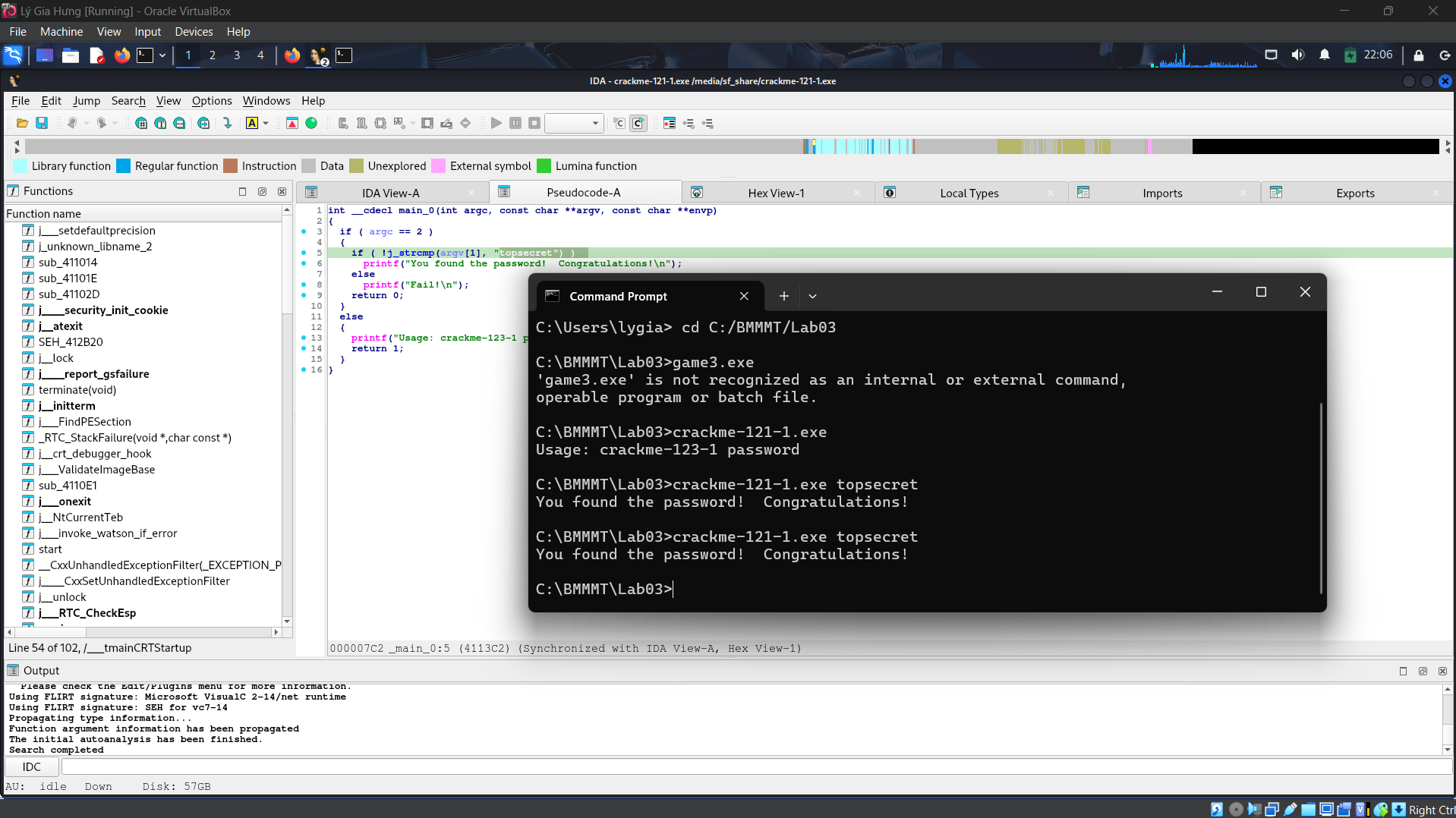




1.6 Phân tích mã giả của crackme.exe để có thể chạy chương trình in ra thông báo "Congratulations! You

solved the crackme puzzle!”. Chạy file crackme.exe ở môi trường CMD của máy Windows in ra thông báo

trên.



1.7. Cài đặt công cụ Bless hex editor vào Kali Linux:

➢ Cài đặt Bless

$ sudo apt update && sudo apt install bless –y

Nếu trong quá trình cài đặt bless xảy ra lỗi như hình bên dưới thì làm như sau

➢ Cách xử lý lỗi khi cài bless

✓ B1: $sudo nano /etc/apt/sources.list

✓ B2: Xoá toàn bộ dữ liệu trong file

✓ B3: Copy đoạn mã bên dưới dán vào file -> Lưu lại

deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware

deb http://http.kali.org/kali kali-last-snapshot main contrib non-free non-free-

firmware

deb http://http.kali.org/kali kali-experimental main contrib non-free non-free-

firmware

deb http://http.kali.org/kali kali-bleeding-edge main contrib non-free non-free-

firmware

deb-src http://http.kali.org/kali kali-rolling main contrib non-free non-free-

firmware

✓ B4: $sudo apt-get upgrade

✓ B5: $sudo apt-get update

✓ B6: $sudo apt-get install checkinstall

✓ B7: $sudo apt install bless –y

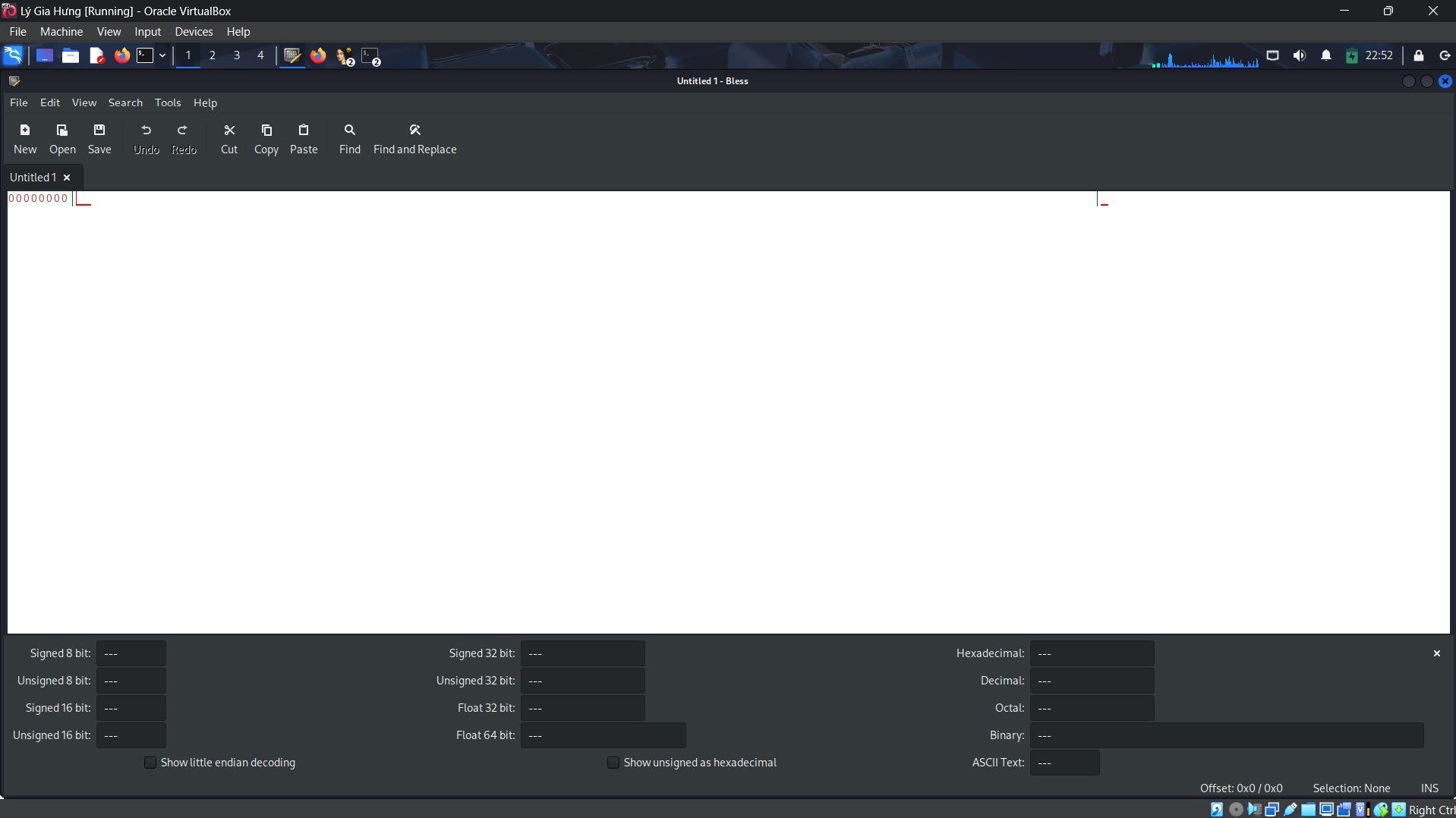
✓ B8: Sừ dụng lệnh $bless để kiểm tra cài đặt thành công chưa ?

- Nếu vẫn không cài được thì cài flatpak

$ sudo apt install flatpak -y

$ sudo flatpak install com.github.afrantzis.Bless -y

flatpak run com.github.afrantzis.Bless



1.8. Sử dụng công cụ Bless hex editor để thay đổi giá trị password cần nhập cho crackme.exe thành

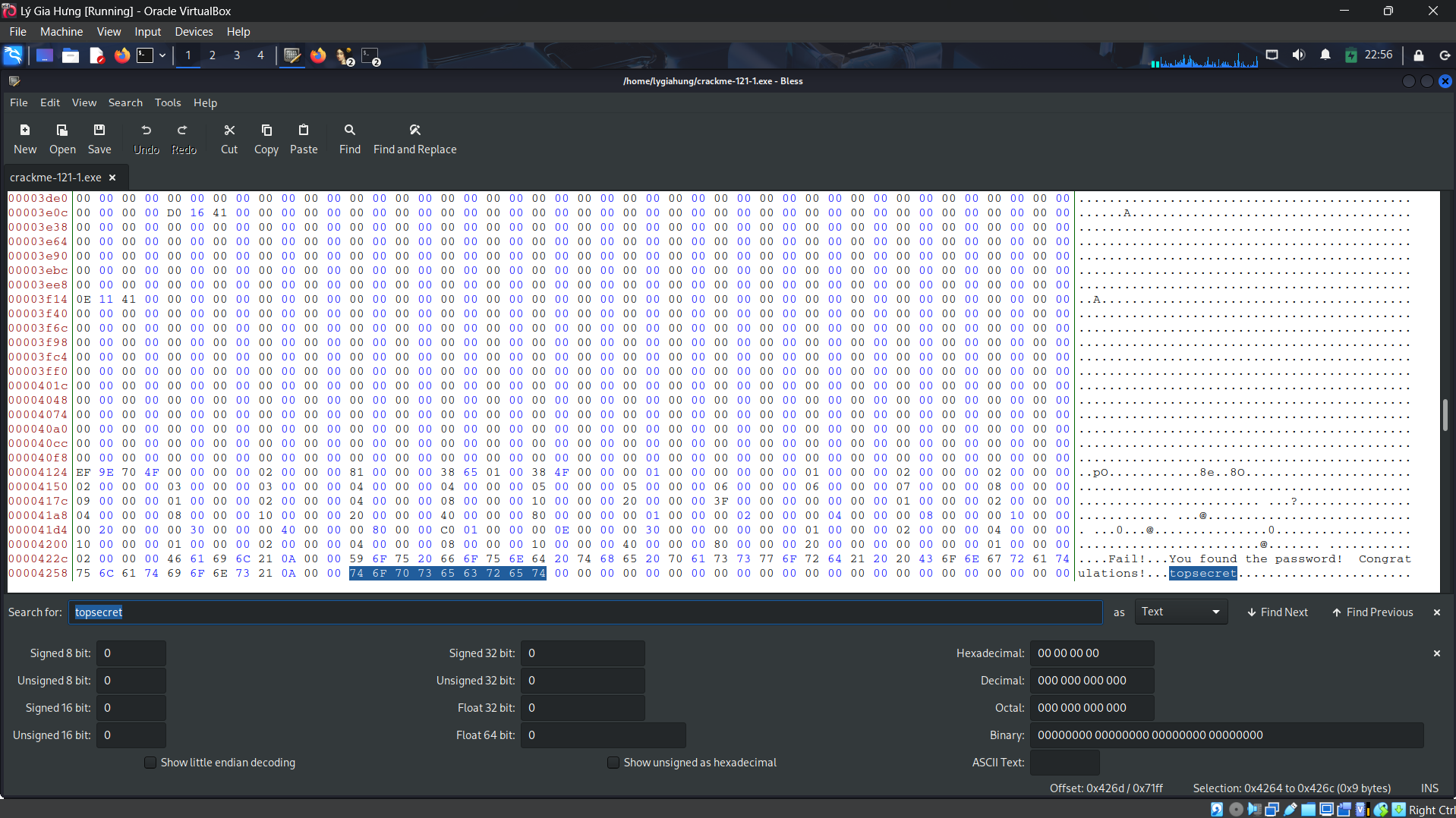
“aaaaaaaaa”. Di chuyển file crackme.exe từ Kali Linux qua máy Windows. Chạy file crackme.exe ở môi

trường CMD của máy Windows in ra thông báo trên "Congratulations! You solved the crackme puzzle!”

➢ Gõ lệnh: $bless để mở công cụ chỉnh sửa

➢ Tiếp theo vào Open mở file crackme

➢ Search -> Find ->tìm kiếm từ dromedary chọn as Text



➢ Thay đổi đổi mật khẩu từ dromedary bằng aaaaaaaaa -> Save - > tắt công cụ bless  
➢ Sao chép di chuyển tập tin crackme vào máy Windows thông qua thư mục share

➢ Vào thư mục crackme trong máy Windows xoá file game3 cũ

➢ Copy file crackme vào thư mục crackme và đổi tên thành game3

➢ Mở CMD của Windows và thực thi file game3.exe với mật khẩu là aaaaaaaaa