HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147

BÀI THỰC HÀNH 1.1
CÀI ĐẶT HỆ ĐIỀU HÀNH MÁY TRẠM WINDOWS

Sinh viên thực hiện:

B22DCAT063 - Lê Tiến Dương

Giảng viên hướng dẫn: PGS. TS. Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
VM	Virtual Machine	Máy ảo

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

Mục đích của bài thực hành "1.1: Cài đặt hệ điều hành máy trạm Windows" là rèn luyện kỹ năng cài đặt và quản trị hệ điều hành máy trạm Windows cho người dùng với các dịch vụ cơ bản.

1.2 Tìm hiểu lý thuyết

1.2.1 Tìm hiểu về các phần mềm ảo hóa

1.2.1.1 VMWare Workstation

VMware Workstation là một phần mềm ảo hóa mạnh mẽ, cho phép người dùng tạo ra và quản lý nhiều máy tính ảo (virtual machine - VM) trên cùng một máy tính vật lý. Mỗi máy ảo hoạt động độc lập, có hệ điều hành riêng, phần cứng ảo riêng và các ứng dụng riêng, giống như một máy tính thực sự.

1.2.1.2 VirtualBox

VirtualBox là phần mềm tạo máy ảo miễn phí chuyên nghiệp. VirtualBox có sẵn để cài đặt trên Windows, Linux Ubuntu, Mac OS X và Solaris. Vì VirtualBox là một phần mềm ảo hóa các nền t*ảng, người dùng* có thể trải nghiệm những hệ điều hành mới, phần mềm mới một cách nhanh chóng và an toàn mà không lo bị nhiễm virus, không lo làm rác máy tính, không phải cài lại hệ điều hành,…

1.2.2 Tìm hiểu về hệ điều hành Windows

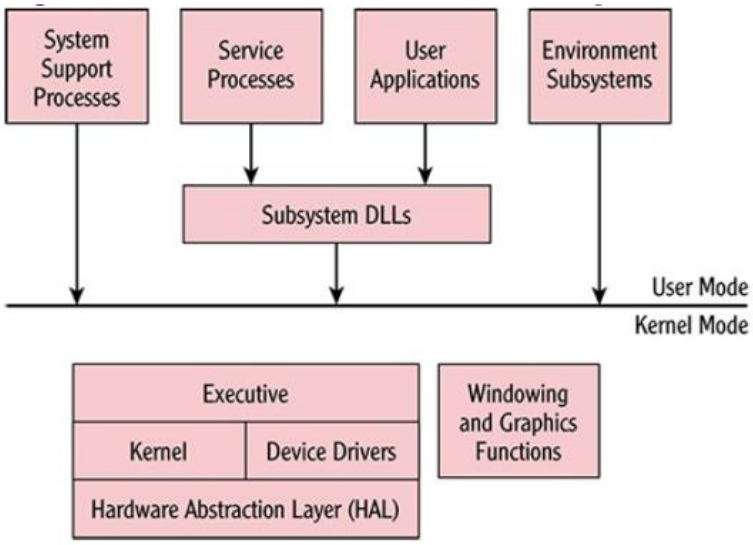
1.2.2.1 Lịch sử

Hệ điều hành Windows do Microsoft phát triển, ra mắt lần đầu vào năm 1985 và đã trải qua nhiều phiên bản nâng cấp quan trọng. Dưới đây là một số cột mốc chính:

- Windows 1.0 (1985): Giao diện đồ họa đầu tiên, chạy trên MS-DOS.
- Windows 3.0 & 3.1 (1990-1992): Cải tiến giao diện, hỗ trợ đa nhiệm tốt hơn.
- Windows 95 (1995): Giao diện Start Menu lần đầu xuất hiện, hỗ trợ 32 bit.
- Windows 98 (1998): Tích hợp tốt hơn với Internet và USB.
- Windows XP (2001): Ổn định, phổ biến nhất với giao diện cải tiến.
- Windows Vista (2006): Đồ họa đẹp nhưng hiệu suất không cao.
- Windows 7 (2009): Thành công lớn với hiệu suất tốt, bảo mật cao.
- Windows 8 & 8.1 (2012-2013): Thiết kế hướng đến màn hình cảm ứng, loại bỏ Start Menu.
- Windows 10 (2015): Start Menu trở lại, hỗ trợ đa nền tảng, cập nhật liên tục.
- Windows 11(2021): Giao diện hiện đại, tối ưu hiệu suất.

1.2.2.2 Kiến trúc

Kiến trúc của hệ điều hành Windows hiện thời dựa trên kiến trúc Windows NT.



Hình 1 – Kiến trúc của hệ điều hành Windows

Về cơ bản, kiến trúc này được chia thành hai lớp tương ứng với hai chế độ hoạt động: chế độ nhân và chế độ người dùng. Chế độ nhân dành cho hệ điều hành và các chương trình mức thấp khác hoạt động. Chế độ người dùng dành cho các ứng dụng như Word, Excel và các hệ thống con hoạt động.

1.2.2.3 Giao diện

- *Giao diện đồ họa GUI:* Giao diện người dùng đồ họa trong Windows bao gồm các cửa sổ, nút bấm, hộp văn bản và các phần tử định hướng khác. Phần tử quan trọng trong GUI chính là menu khởi động (*Start*) và thanh tác vụ (*Taskbar*). Phần quan trọng khác đó là màn hình làm việc (*desktop*). Đây là nơi chứa các biểu tượng các chương trình người dùng hay hệ thống hoặc các chương trình tiện ích.
- *Giao diện dòng lệnh:* Giao diện xưa nhất của Windows là dòng lệnh DOS. Trong môi trường Windows, nó không còn thực sự là DOS dù có nhiều câu lệnh DOS vẫn còn dùng được và được kích hoạt thông qua chương trình *cmd.exe.*
- *Giao diện PowerShell:* Giao diện dòng lệnh mới của Windows và là môi trường nên dùng cho các tác vụ quản trị. Thực tế, Microsoft hỗ trợ tập các lệnh trong môi trường PowerShell được gọi là *cmdlet* để thực hiện các tác vụ quản trị mong muốn.

1.2.2.4 Đặc điểm đặc trưng

- Giao diện đồ họa trực quan – Dễ sử dụng với Start Menu, Taskbar, File Explorer.
- Độ tương thích cao – Hỗ trợ nhiều phần cứng và phần mềm phổ biến.
- Hỗ trợ đa nhiệm – Cho phép chạy nhiều ứng dụng cùng lúc.
- Hệ sinh thái rộng lớn.
- Bảo mật và cập nhật – Windows Defender, tường lửa cập nhật thường xuyên.

- Dễ cài đặt và sử dụng – Phù hợp với cả người dùng cá nhân và doanh nghiệp.

1.2.3 Các phần mềm diệt Virus, phần mềm chống gián điệp, phần mềm cứu hộ

1.2.3.1 Phần mềm diệt Virus: AVG AntiVirus

- Phần mềm diệt virus là một chương trình bảo mật được thiết kế để phát hiện, ngăn chặn và loại bỏ virus, mã độc và các mối đe dọa trên máy tính hoặc thiết bị di động, giúp bảo vệ hệ thống, dữ liệu và thông tin cá nhân khỏi các cuộc tấn công mạng.
- AVG Antivirus là phần mềm bảo mật được phát triển bởi AVG Technologies (thuộc Avast), giúp phát hiện, ngăn chặn và loại bỏ virus, malware, spyware, ransomware và các mối đe dọa mạng.

1.2.3.2 Phần mềm chống gián điệp Spybot S&D (Spybot – Search & Destroy)

- Phần mềm gián điệp (Spyware) là một loại phần mềm độc hại được thiết kế để bí mật thu thập thông tin của người dùng mà không có sự cho phép. Nó có thể theo dõi hoạt động trực tuyến, đánh cắp thông tin cá nhân, tài khoản ngân hàng, mật khẩu hoặc ghi lại thao tác bàn phím (keylogger).
- SpyBot-S&D là phần mềm chống gián điệp dành cho hệ điều hành Windows. Chương trình này sẽ quét ổ cứng để xác định những phần mềm do thám hoặc những module phần mềm chuyên làm hiển thị các mục quảng cáo hoặc gửi thông tin từ máy của bạn về cho chủ của nó. Nếu tìm được những đối tượng này, Spybot Search and Destroy sẽ gỡ bỏ và thay thế chúng bằng những adware giả, trống rỗng, vì thông thường, phần mềm chủ của chúng vẫn sẽ hoạt động sau khi adware đã bị gỡ đi.

1.2.3.3 Phần mềm chống các phần mềm độc hại Malwarebytes Anti-Malware

- Phần mềm chống phần mềm độc hại (Anti-Malware Software) là chương trình bảo mật được thiết kế để phát hiện, ngăn chặn và loại bỏ các loại mã độc (malware) như virus, trojan, ransomware, spyware, adware, rootkit và các mối đe dọa khác nhằm bảo vệ hệ thống máy tính và dữ liệu người dùng.
- Tính năng chính của Malwarebytes Anti-Malware:
    - Quét và diệt malware nhanh chóng – Phát hiện và loại bỏ mã độc hiệu quả.
    - Bảo vệ thời gian thực (phiên bản trả phí) – Chặn các mối đe dọa trước khi gây hại.
    - Chống ransomware – Bảo vệ dữ liệu khỏi mã độc mã hóa tống tiền.
    - Bảo vệ trình duyệt – Ngăn chặn trang web độc hại, quảng cáo chứa mã độc.
    - Tường lửa chống tấn công mạng (trong phiên bản nâng cao).
    - Tự động cập nhật – Luôn cập nhật cơ sở dữ liệu malware mới nhất.
    - Tương thích với phần mềm diệt virus khác – Có thể dùng chung với các phần mềm bảo mật khác mà không gây xung đột.

1.2.3.4 Phần mềm cứu hộ Kaspersky Rescue Disk (KRD)

- Phần mềm cứu hộ (Rescue Software) là công cụ giúp khôi phục, sửa chữa và bảo vệ hệ thống máy tính khi gặp sự cố nghiêm trọng, chẳng hạn như hệ điều hành bị lỗi, nhiễm virus, mất dữ liệu hoặc không thể khởi động.
- Kaspersky Rescue Disk (KRD) là một phần mềm cứu hộ hệ thống miễn phí do Kaspersky Lab phát triển. Nó giúp diệt virus, sửa lỗi hệ thống và khôi phục dữ liệu khi máy tính bị nhiễm mã độc quá nặng và không thể khởi động hoặc sử dụng các phần mềm diệt virus thông thường.
- Chức năng chính của Kaspersky Rescue Disk:
    - Quét & loại bỏ virus, trojan, spyware, rootkit – Ngăn chặn mã độc gây hại cho hệ thống.
    - Quét hệ thống từ môi trường khởi động riêng biệt – Giúp diệt virus mà không cần vào Windows.

      Kiểm tra và sửa lỗi ổ cứng – Giúp phát hiện và sửa lỗi hệ thống tập tin.
    - Truy cập và sao lưu dữ liệu quan trọng – Dễ dàng lấy lại dữ liệu từ hệ thống bị lỗi.
    - Duyệt web an toàn – Có trình duyệt tích hợp để kiểm tra thông tin trực tuyến mà không ảnh hưởng đến hệ thống bị nhiễm.
    - Tự động cập nhật cơ sở dữ liệu virus – Đảm bảo nhận diện các mối đe dọa mới nhất.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

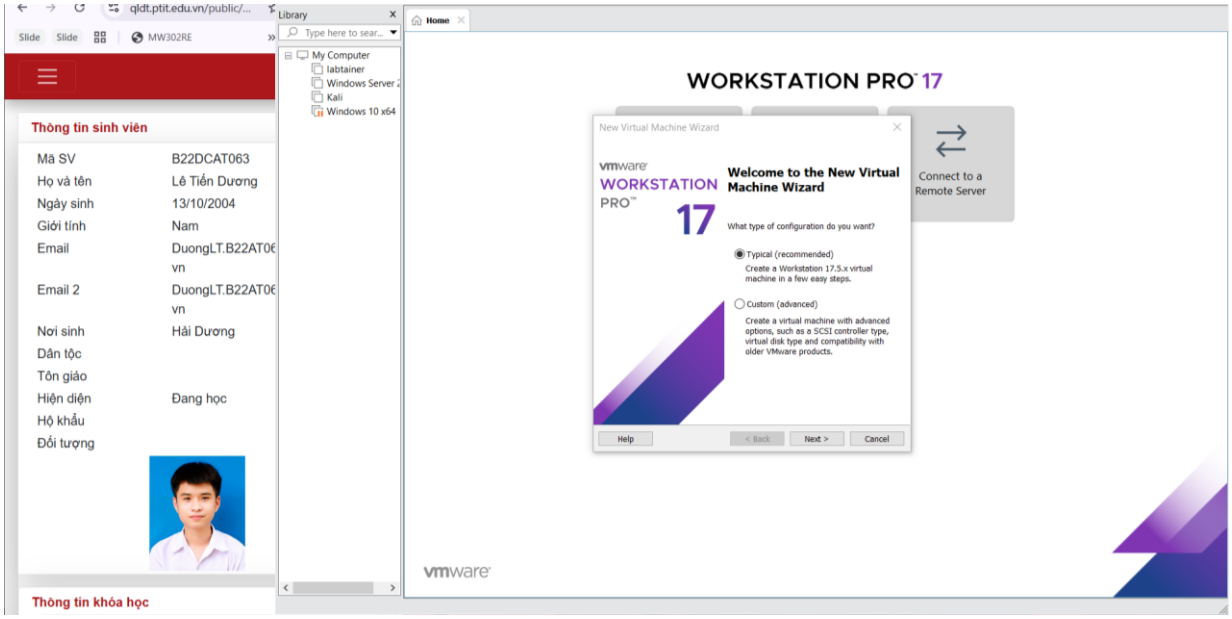
2.1 Chuẩn bị môi trường

- File cài đặt Windows 10 định dạng iso.
- Phần mềm ảo hóa VMWare Workstation.

2.2 Các bước thực hiện

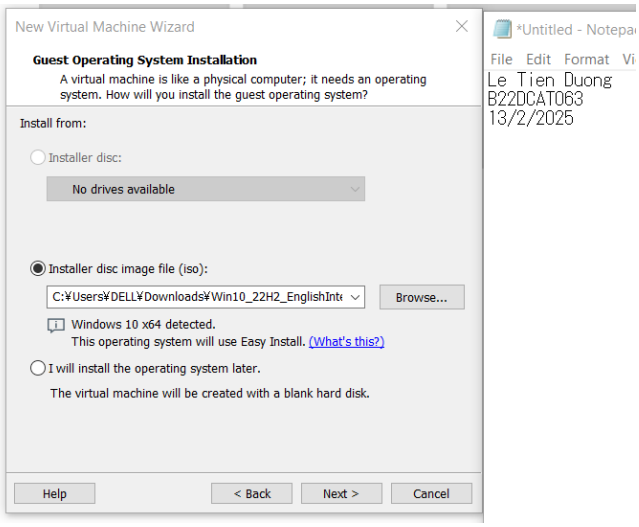
2.2.1 Cài đặt Windows

- Chọn File -> New Virtual Machine để mở cửa sổ New Virtual Wirzard -> Typical -> Next



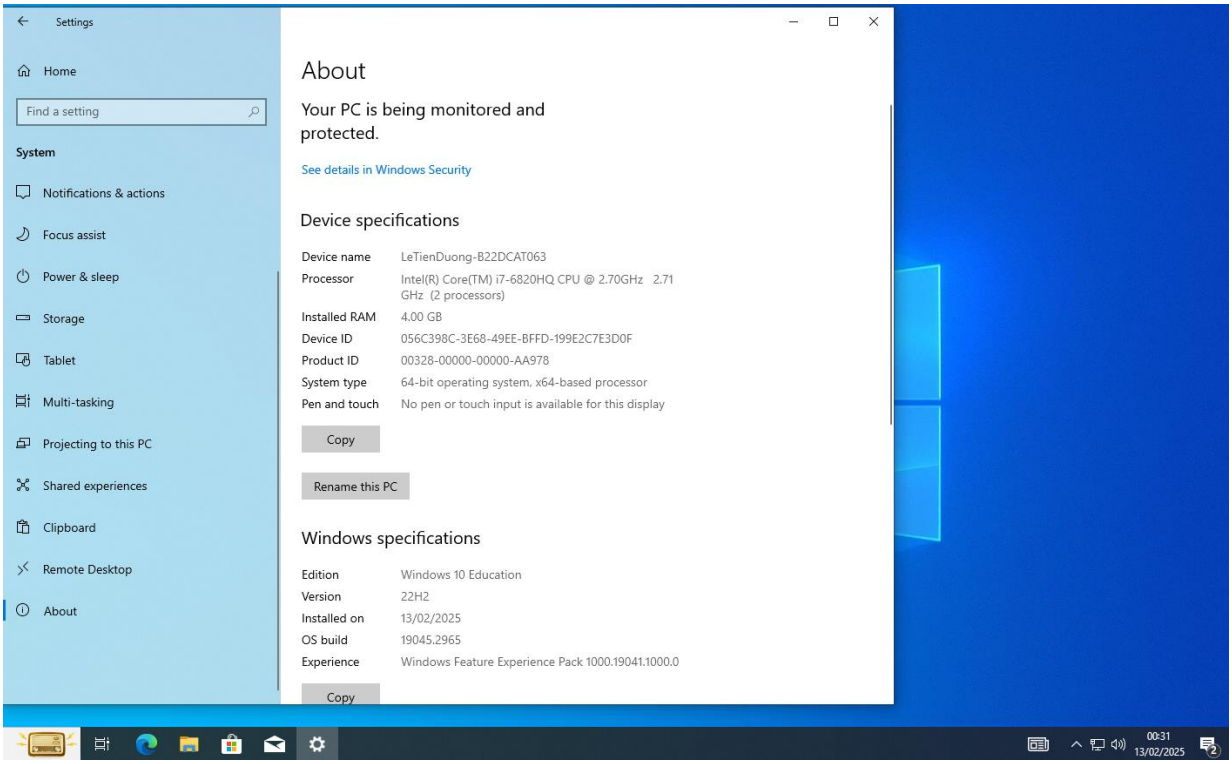
Hình 2 – Cửa sổ New Virtual Machine Wizard

- Chọn file iso Windows 10 đã tải về -> Next và tiến hành cài đặt.



Hình 3 – Chọn file iso

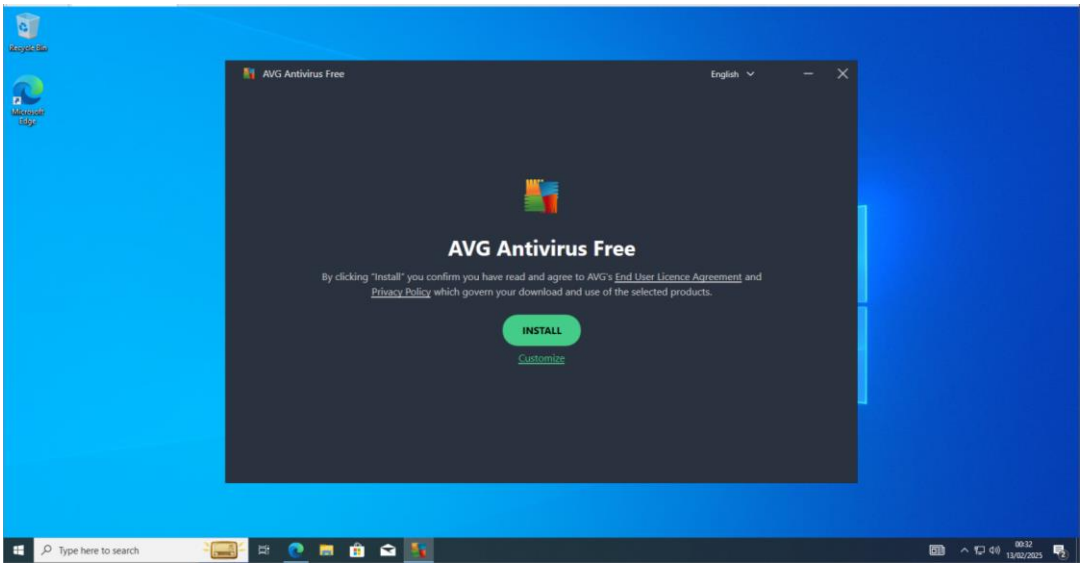
- Cài đặt thành công Windows 10 và đổi tên máy.



Hình 4 – Đổi tên máy Windows 10

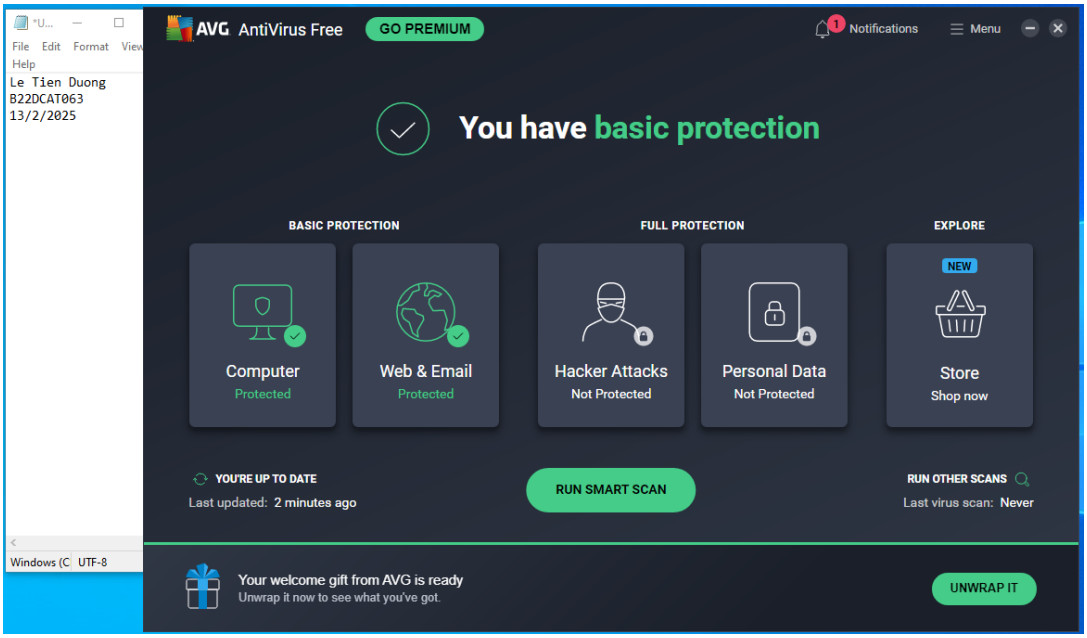
2.2.2 Cài đặt phần mềm diệt virus AVG AntiVirus

- Kích hoạt file vừa tải và tiến hành cài đặt.



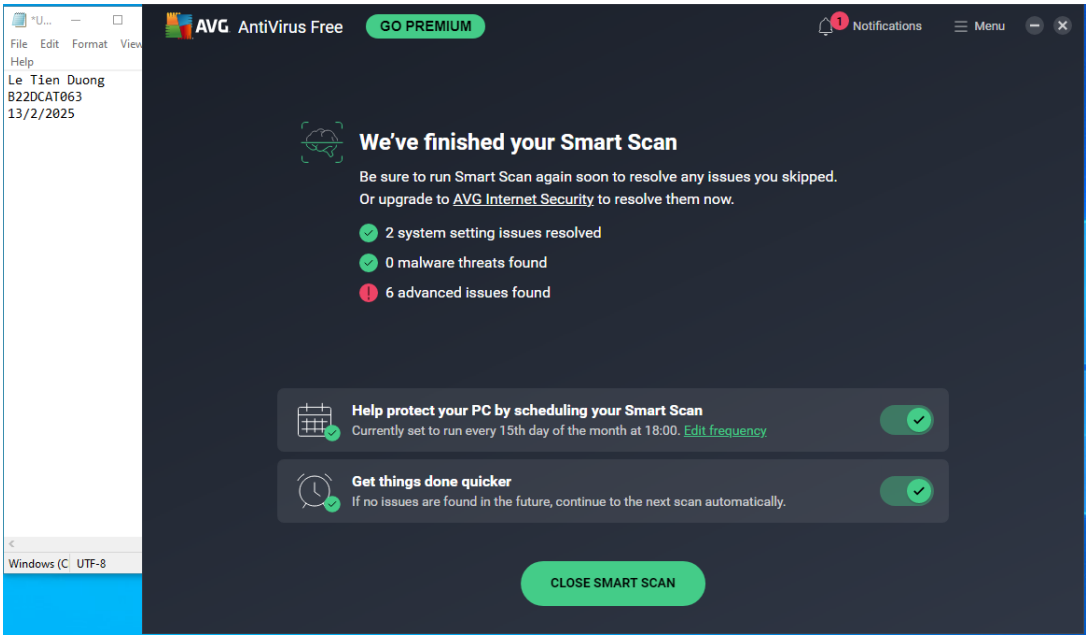
Hình 5 – Cài đặt phần mềm AVG AntiVirus

- Nhấn Install để cài đặt.



Hình 6 – Giao diện phần mềm AVG AntiVirus sau khi cài đặt thành công

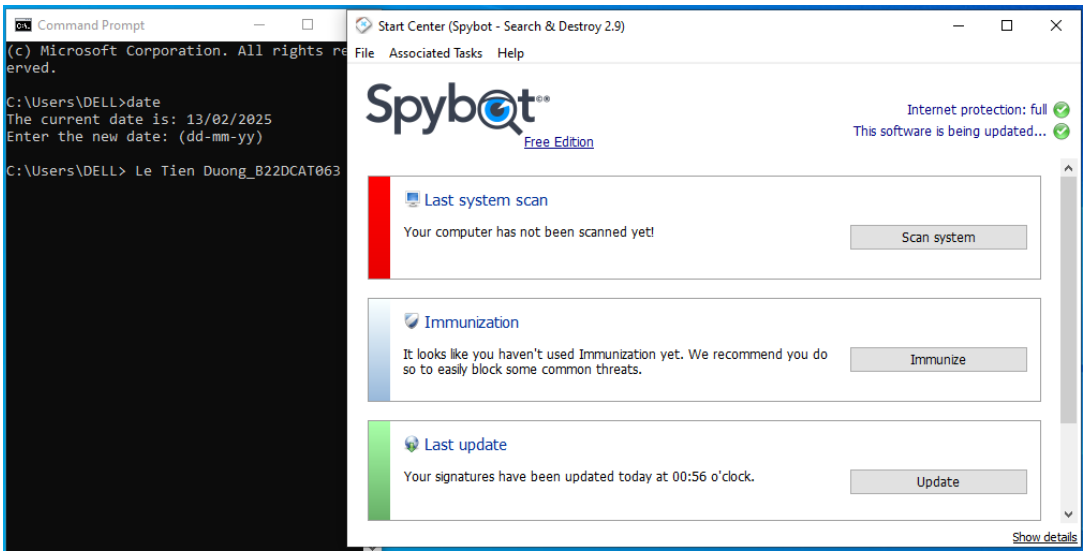
- Sử dụng phần mềm để quét.



Hình 7 – Chạy thử phần mềm

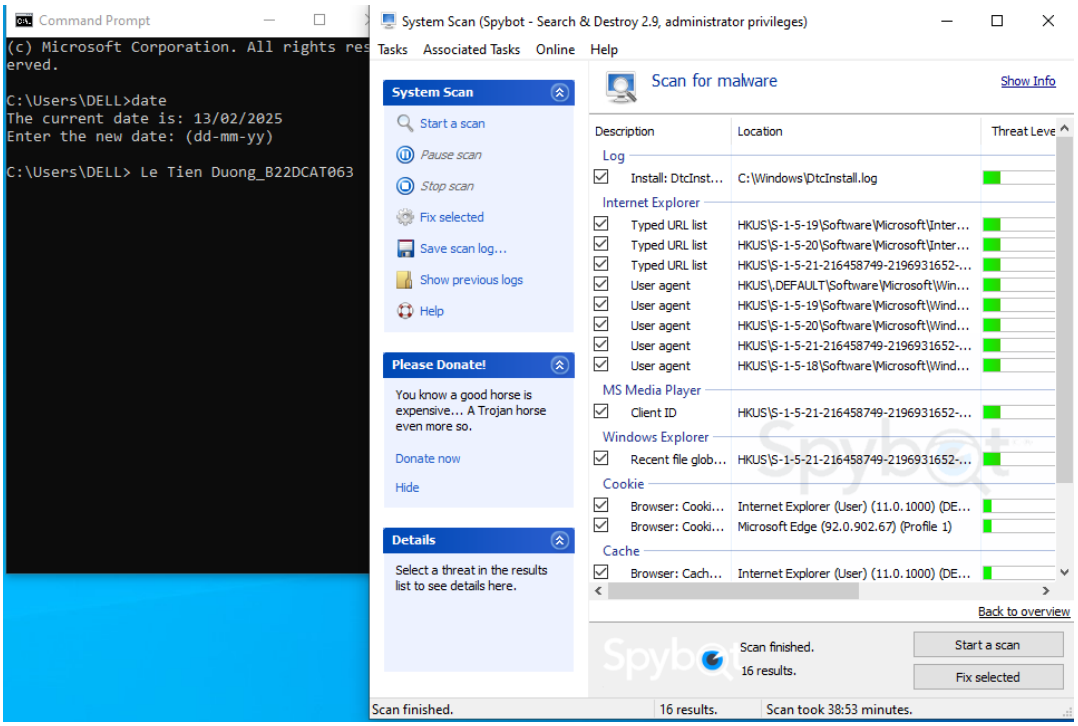
2.2.3 Cài đặt phần mềm Spybot S&D (Spybot – Search & Destroy)

- Khởi chạy file đã tải về và tiến hành cài đặt.



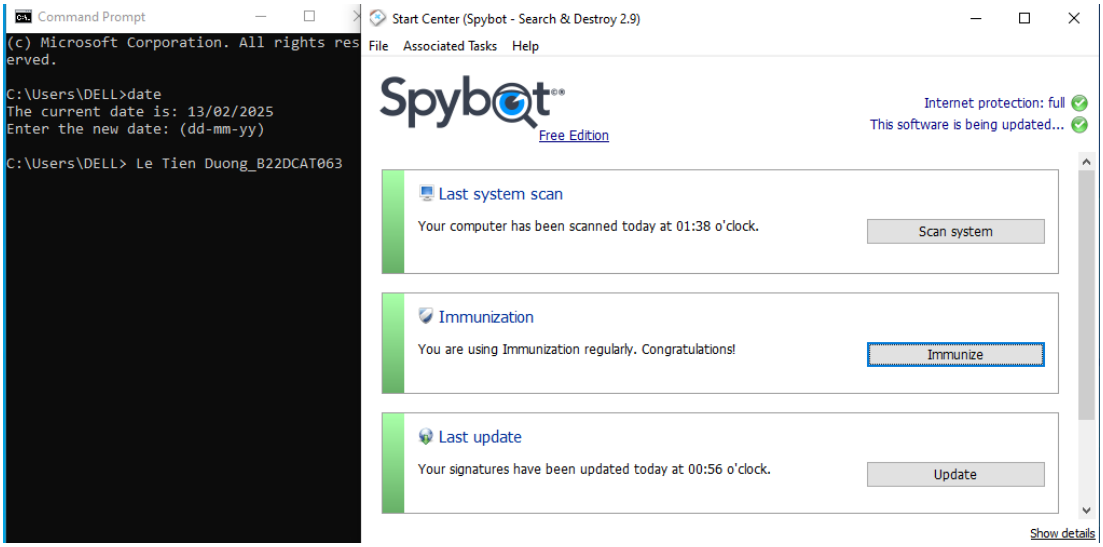
Hình 8 – Giao diện của Spybot S&D sau khi cài đặt thành công

- Chạy thử phần mềm.



Hình 9 – Kết quả sau khi scan system

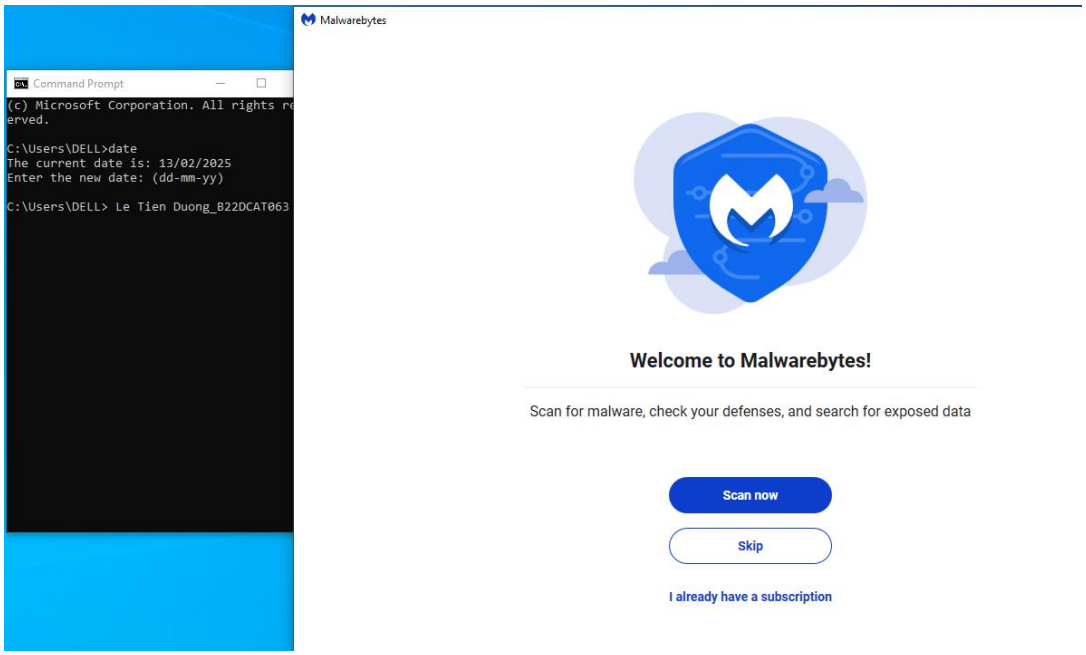
- Thực hiện Immunize.



Hình 10 – Kết quả sau khi Immunize

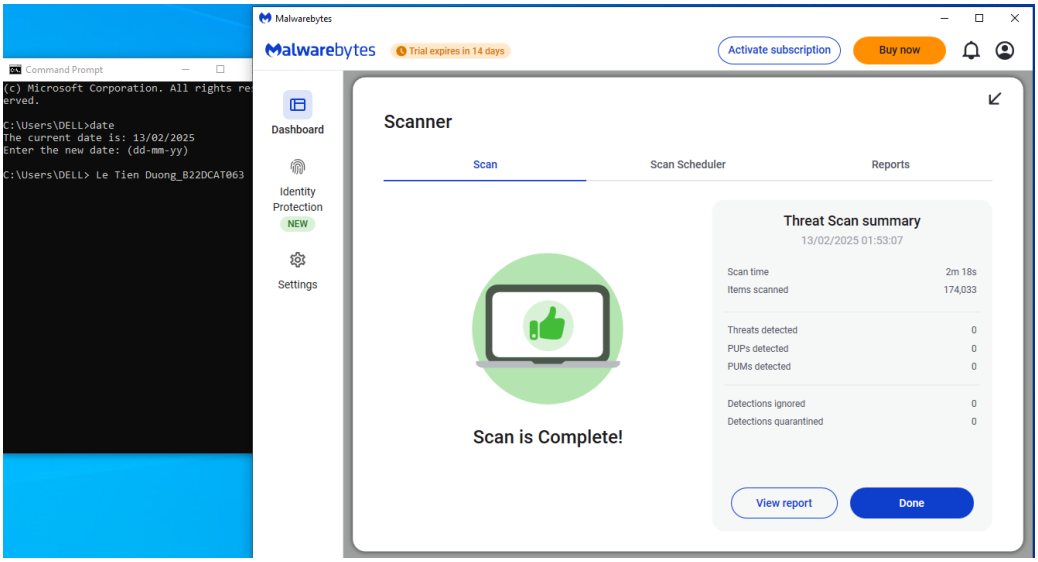
2.2.4 Cài đặt phần mềm Malwarebytes Anti-Malware

- Thực hiện cài đặt phần mềm từ file đã tải về.



Hình 11 – Phần mềm Malwarebytes Anti-Malware cài đặt thành công

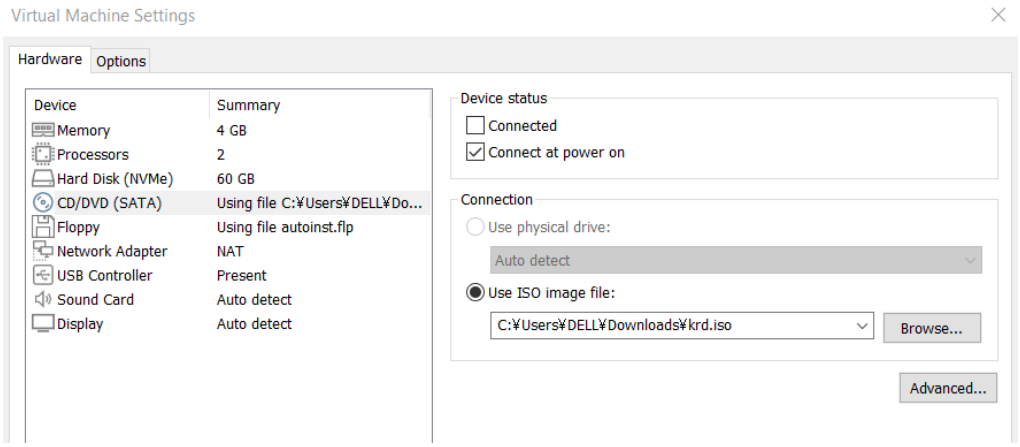
- Bắt đầu scan bằng phần mềm.



Hình 12 – Kết quả sau khi scan thành công

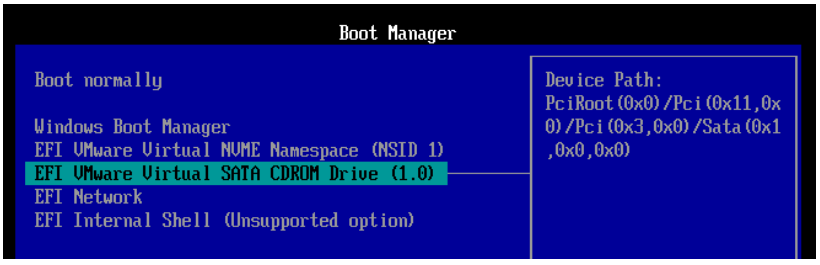
2.2.5 Cài đặt phần mềm cứu hộ Kaspersky Rescue Disk (KRD)

- Load file iso vào trong mục CD/DVD của máy trạm ảo.

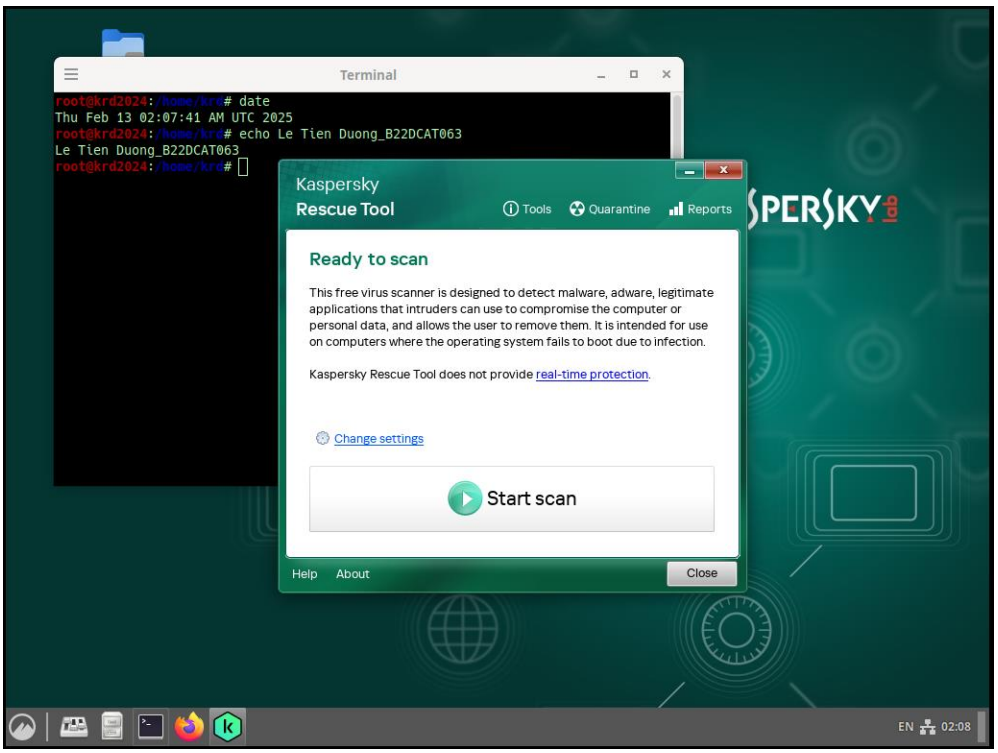


Hình 13 – Load file iso KRD vào mục CD/DVD của máy trạm ảo

- Chạy máy trạm ảo, sử dụng phím “esc” để chọn boot từ CD-ROM drive để cài đặt KRD.

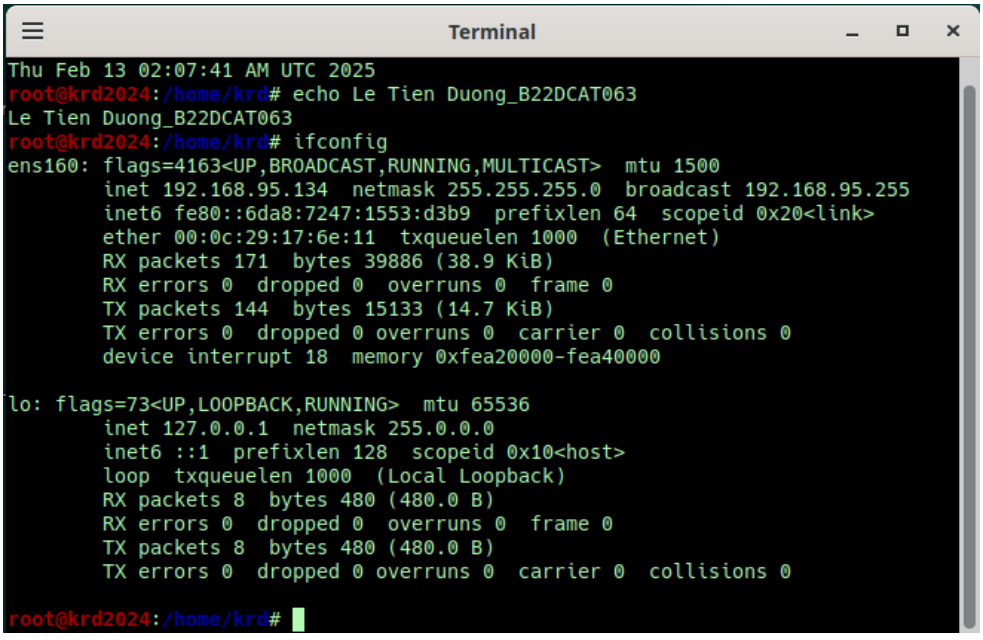


Hình 14 – Chạy phần mềm KRD



Hình 15 – Giao diện phần mềm cứu hộ Kaspersky

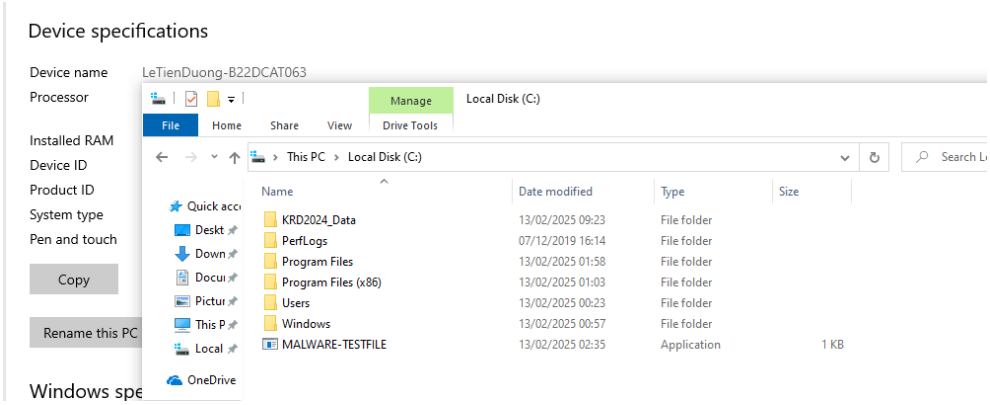
- Mở cmd để kiểm tra IP của máy trạm bằng câu lệnh : ifconfig



Hình 16 – Kiểm tra IP của máy trạm

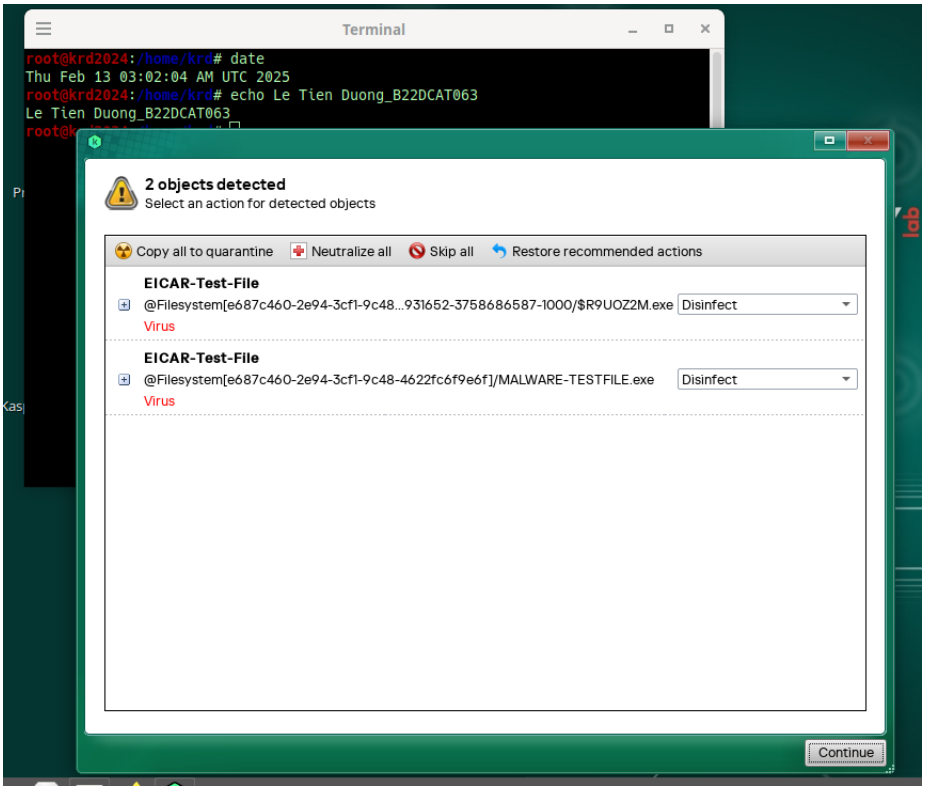
- Tải file mã độc từ đường link. Lưu file test mã độc vào ổ C của máy trạm

  http://www.computersecuritystudent.com/WINDOWS/W7/lesson7/MALWARE-TESTFILE.exe



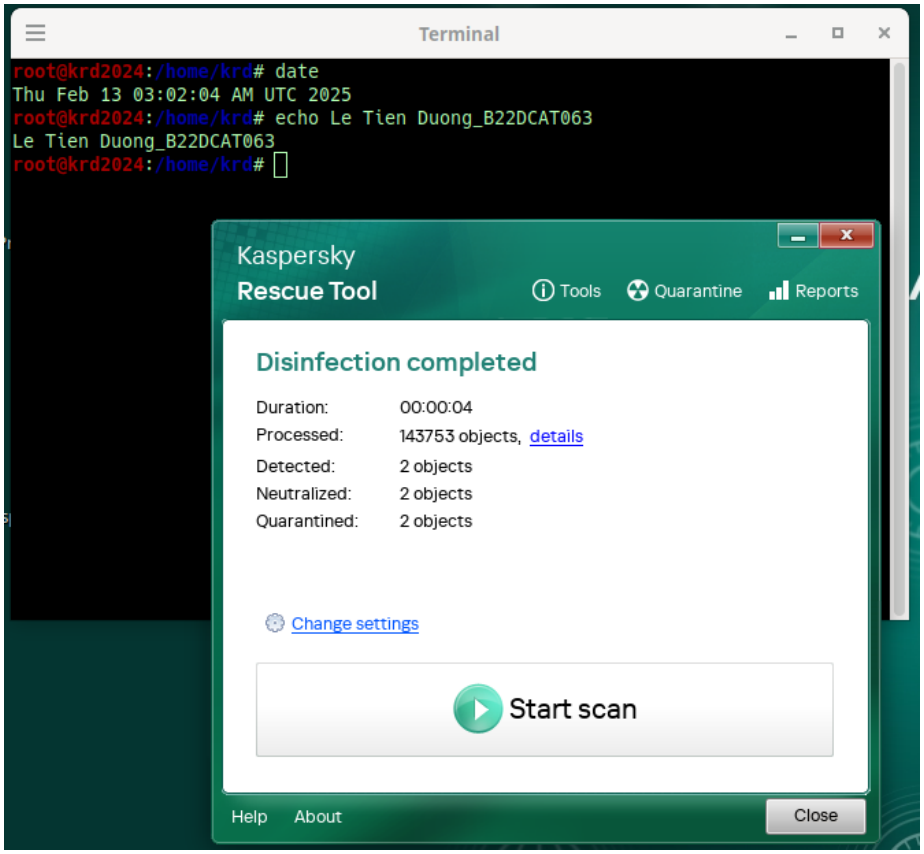
Hình 17 – Tải và lưu mã độc vào ổ C của máy trạm

- Sau đó chạy Kaspersky Rescue Tool, vào setting chọn quét tất cả các thư mục -> phát hiện ra file test mã độc và thực hiện xóa nó.



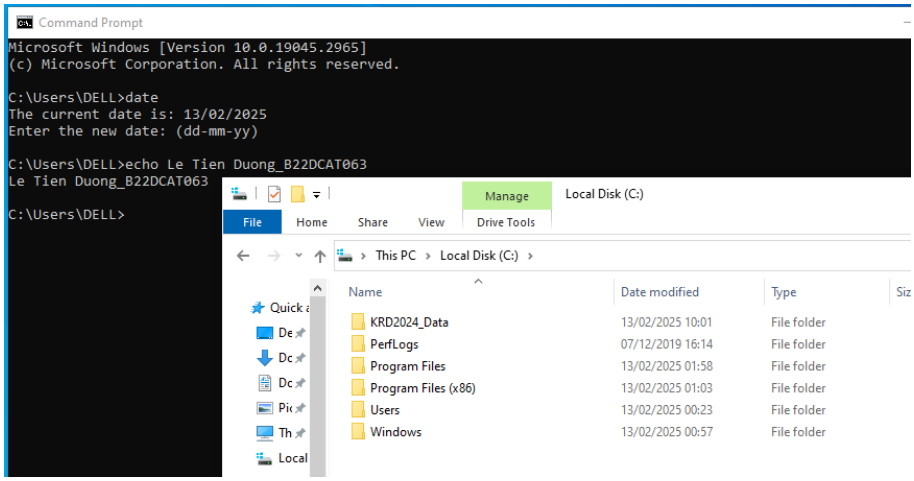
Hình 18 – Sử dụng KRD phát hiện file mã độc vừa tải

- Thực hiện xóa file mã độc.



Hình 19 – Thực hiện xóa file mã độc

- Quay lại máy Windows 10 kiểm tra -> file mã độc đã được xóa.



Hình 20 – File mã độc đã được xóa

TÀI LIỆU THAM KHẢO

[1] Đinh Trường Duy, Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2022.

[2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.