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 2.4
ĐẢM BẢO AN TOÀN THÔNG TIN DỰA TRÊN MÃ HÓA

Sinh viên thực hiện:

B22DCAT251 Đặng Đức Tài

Giảng viên hướng dẫn: TS. Phạm Hoàng Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

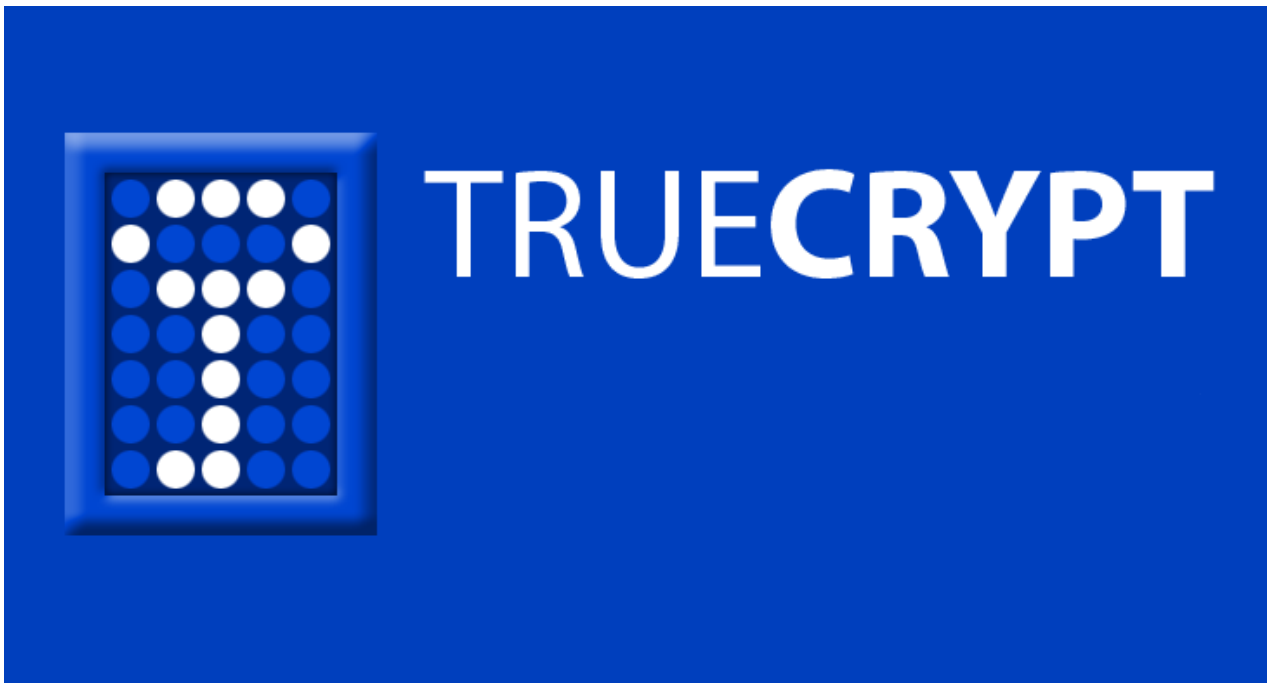
1.1 Mục đích

- Hiểu được nguyên tắc hoạt động của các kỹ thuật mã hóa.
- Hiểu được cách thức hoạt động của một số công cụ mã hóa dữ liệu
- Biết sử dụng các công cụ mã hóa để đảm bảo an toàn dữ liệu.

1.2 Tìm hiểu lý thuyết

1.2.1 Tổng quan về TrueCrypt

- TrueCrypt là một phần mềm mã hóa miễn phí và mã nguồn mở, được thiết kế để bảo vệ dữ liệu thông qua cơ chế tạo ổ đĩa mã hóa ảo. Người dùng có thể sử dụng TrueCrypt để mã hóa một tệp tin (container), một phân vùng hoặc thậm chí toàn bộ ổ đĩa. Mặc dù dự án TrueCrypt đã ngừng phát triển từ năm 2014, nhưng nhiều người vẫn tin tưởng và sử dụng nó nhờ vào tính bảo mật mạnh mẽ và sự linh hoạt trong quá trình mã hóa dữ liệu.
- Một trong những điểm mạnh của TrueCrypt là khả năng tạo ổ đĩa ảo mã hóa, giúp người dùng có thể lưu trữ dữ liệu một cách an toàn mà không ảnh hưởng đến hệ thống. Khi ổ đĩa này được gắn kết (mount), nó hoạt động như một ổ đĩa thông thường, cho phép đọc và ghi dữ liệu một cách dễ dàng. Tuy nhiên, ngay khi ổ bị tháo gỡ (dismount), toàn bộ dữ liệu bên trong sẽ được mã hóa và trở nên không thể truy cập nếu không có mật khẩu hoặc khóa giải mã.
- TrueCrypt hỗ trợ nhiều thuật toán mã hóa tiên tiến như AES-256 (Advanced Encryption Standard), Serpent và Twofish. Người dùng có thể lựa chọn một thuật toán duy nhất hoặc kết hợp nhiều thuật toán để tăng cường bảo mật. Khi dữ liệu được mã hóa, TrueCrypt đảm bảo rằng chỉ những ai có mật khẩu hợp lệ mới có thể truy cập vào nội dung bên trong.
- Ngoài ra, phần mềm này còn cung cấp cơ chế bảo mật nâng cao như Hidden Volume (ổ đĩa ẩn). Với tính năng này, người dùng có thể tạo một ổ đĩa mã hóa bên trong một ổ đĩa khác, giúp bảo vệ dữ liệu quan trọng khỏi những người cố tình truy cập trái phép. Điều này đặc biệt hữu ích trong trường hợp người dùng bị ép buộc cung cấp mật khẩu, vì họ có thể nhập mật khẩu của ổ mã hóa "bên ngoài" trong khi dữ liệu quan trọng vẫn được bảo vệ bên trong ổ ẩn.
- Nhờ vào cơ chế mã hóa mạnh mẽ, khả năng che giấu dữ liệu và tính linh hoạt trong sử dụng, TrueCrypt đã trở thành một công cụ hữu ích dành cho những ai muốn bảo vệ dữ liệu cá nhân khỏi truy cập trái phép.



Hình 1 Phần mềm TrueCrypt

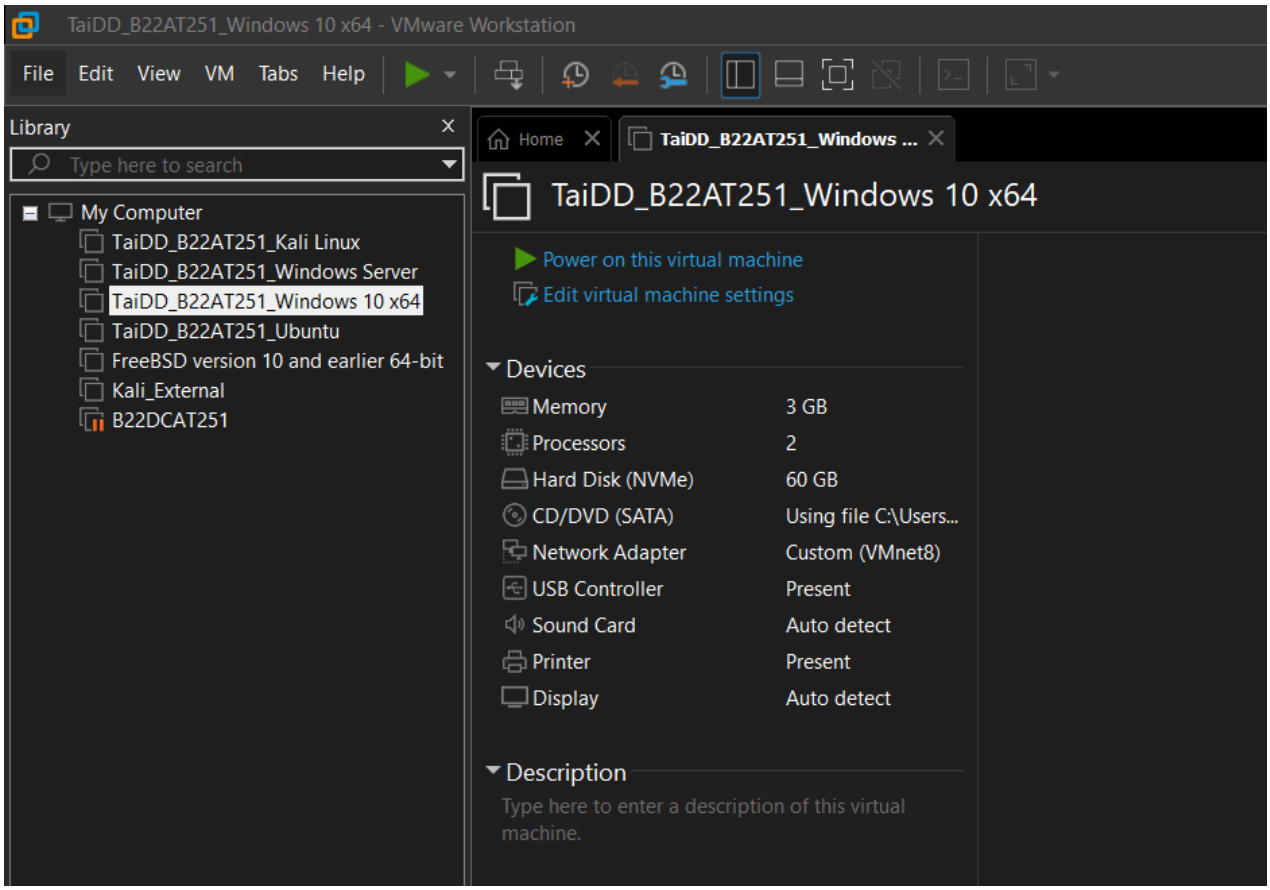
1.2.2 Phương pháp công cụ TrueCrypt áp dụng để mã hóa file hoặc thư mục

- TrueCrypt áp dụng phương pháp mã hóa bằng cách tạo một container mã hóa (file container) hoặc mã hóa trực tiếp phân vùng/thư mục trên ổ đĩa. Khi mã hóa file hoặc thư mục, quá trình bắt đầu bằng việc tạo một container, thực chất là một tệp đơn chứa dữ liệu được mã hóa. Người dùng chỉ định kích thước của container và chọn thuật toán mã hóa (thường là AES-256) cùng với một mật khẩu. Dữ liệu bên trong container được mã hóa tức thời khi ghi vào và giải mã khi đọc ra, với toàn bộ quá trình diễn ra trong bộ nhớ RAM mà không lưu trữ dữ liệu đã giải mã lên ổ đĩa. Để truy cập, container được gắn (mounted) dưới dạng một ổ đĩa ảo, cho phép người dùng thao tác với file và thư mục như trên ổ đĩa thông thường. Sau khi sử dụng, container được tháo (dismounted), khiến dữ liệu trở lại trạng thái mã hóa và không thể truy cập nếu không có mật khẩu đúng. Phương pháp này đảm bảo rằng chỉ những người sở hữu khóa giải mã mới có thể truy cập nội dung, đồng thời dữ liệu luôn được bảo vệ ngay cả khi thiết bị bị mất hoặc bị truy cập trái phép. Đối với mã hóa thư mục, TrueCrypt không mã hóa trực tiếp thư mục mà yêu cầu di chuyển dữ liệu vào container hoặc phân vùng đã mã hóa để thực hiện bảo vệ.
- Phương pháp này kết hợp tính linh hoạt và hiệu quả, tận dụng các thuật toán mã hóa tiên tiến để đảm bảo an toàn dữ liệu trong nhiều tình huống sử dụng khác nhau. TrueCrypt cũng hỗ trợ song song hóa (parallelization) và xử lý đường ống (pipelining) để tối ưu hóa hiệu suất trên các hệ thống đa lõi, giảm thiểu tác động của mã hóa lên tốc độ truy cập dữ liệu.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

- Phần mềm VMWare Workstation
- Máy ảo Windows 10
- Công cụ TrueCrypt

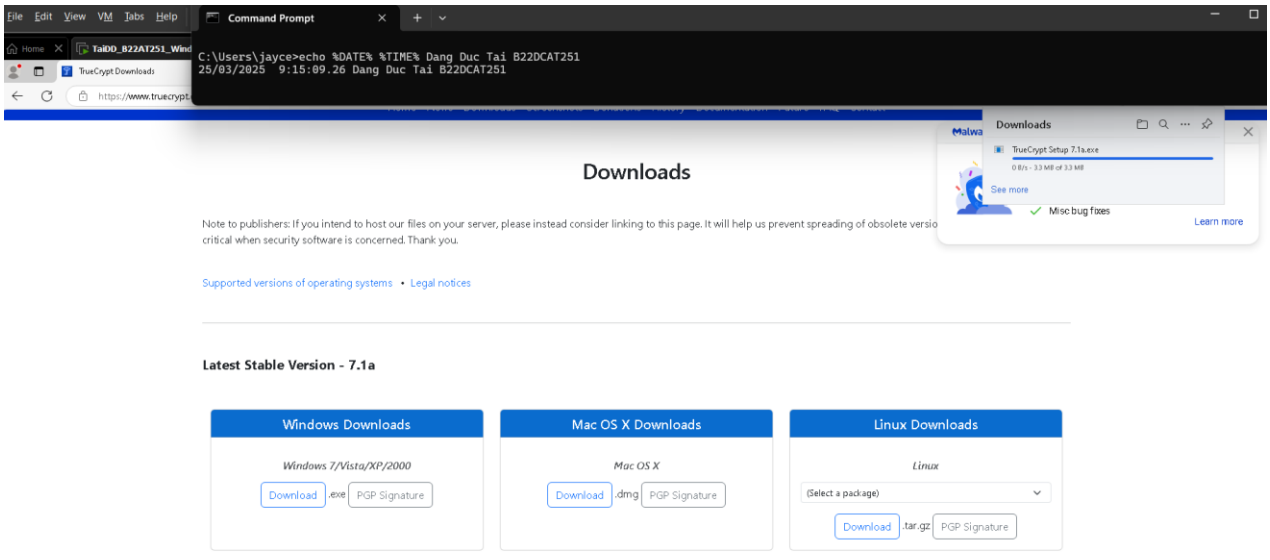


Hình 2 Chuẩn bị môi trường

2.2 Các bước thực hiện

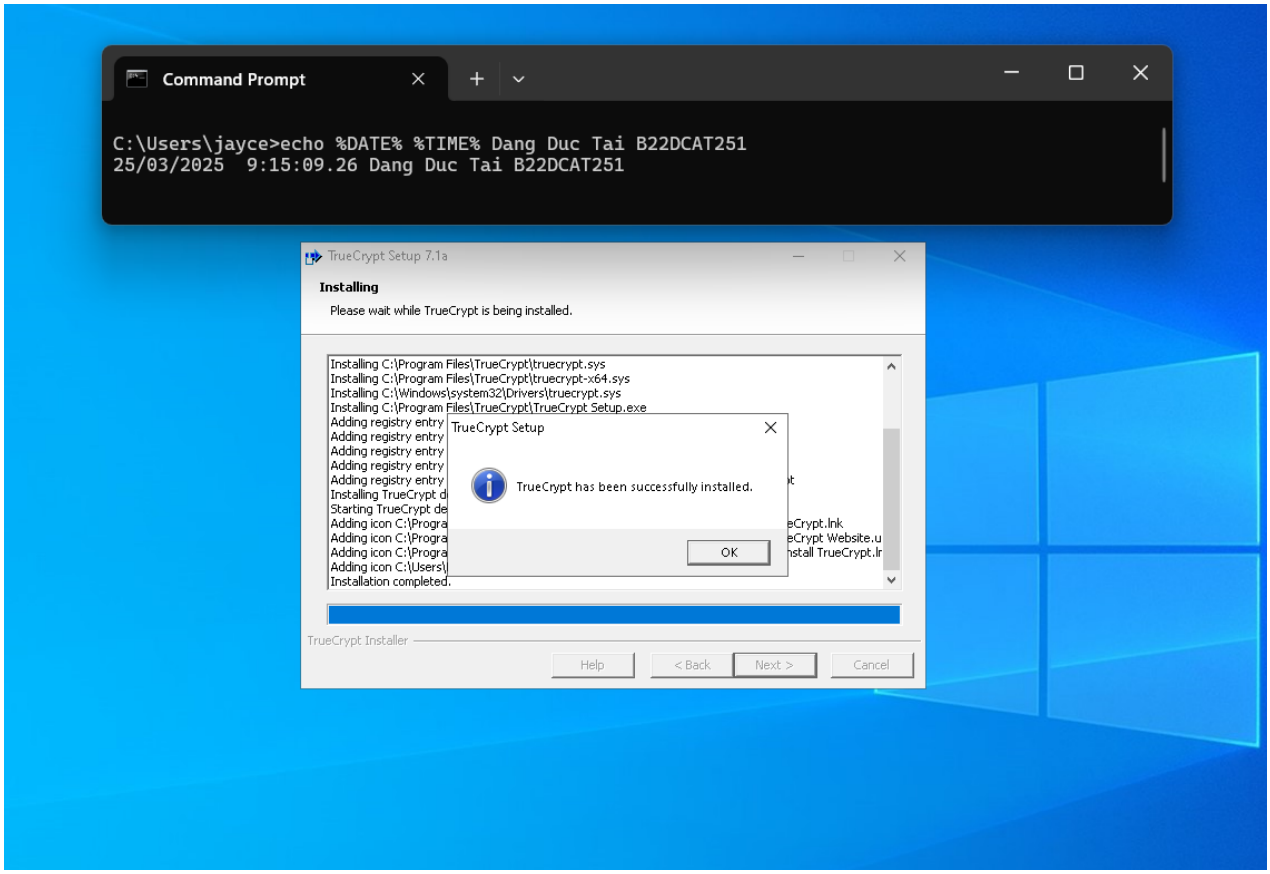
2.2.1 Cài đặt phần mềm TrueCrypt

- Tải phần mềm TrueCrypt tại đường dẫn https://www.truecrypt.org/downloads



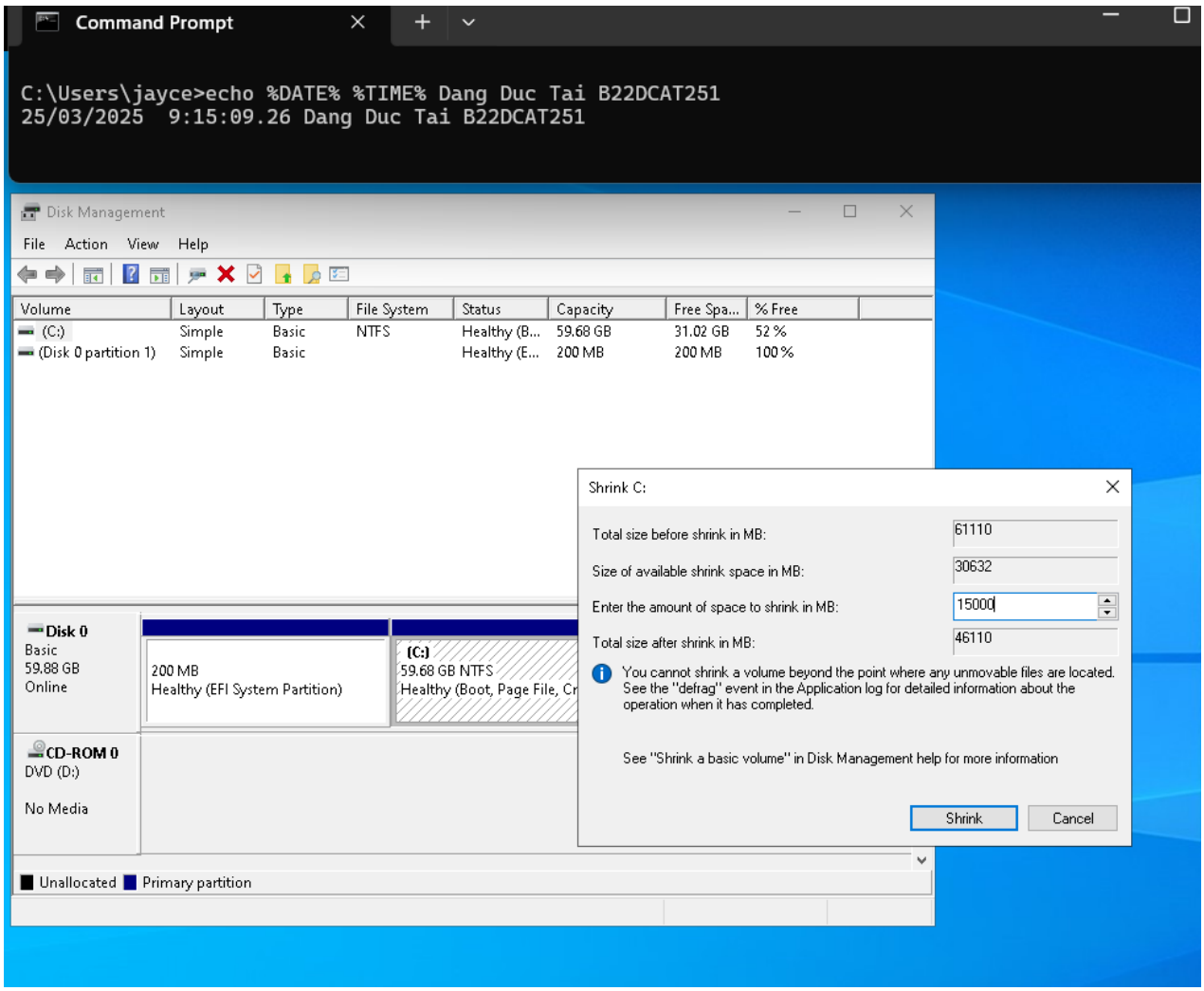
Hình 3 Tải phần mềm TrueCrypt

- Cài đặt thành công, giao diện của phần mềm TrueCrypt



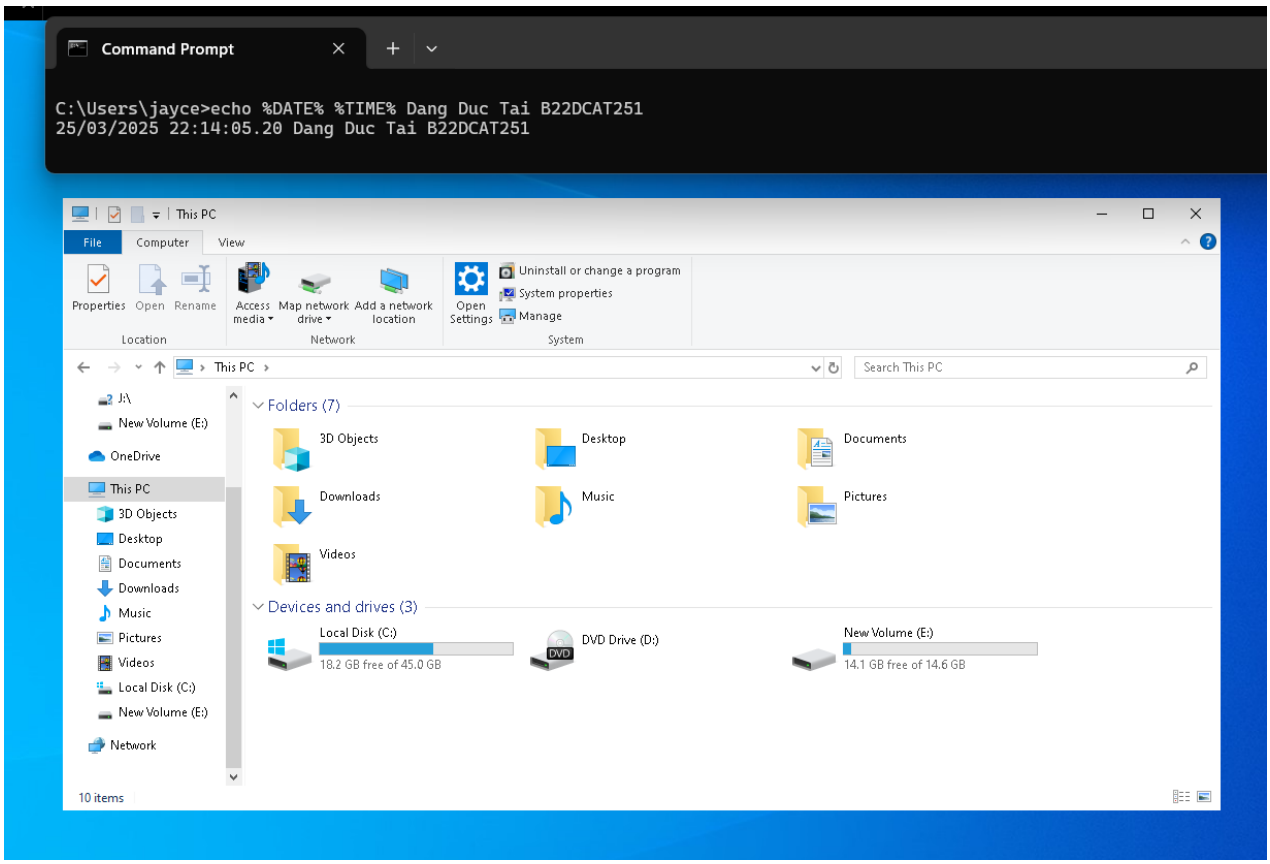
Hình 4 Cài đặt thành công phần mềm TrueCrypt

- Tiến hành phân vùng ổ đĩa để tạo không gian lưu file mã hóa



Hình 5 Phân vùng ổ đĩa

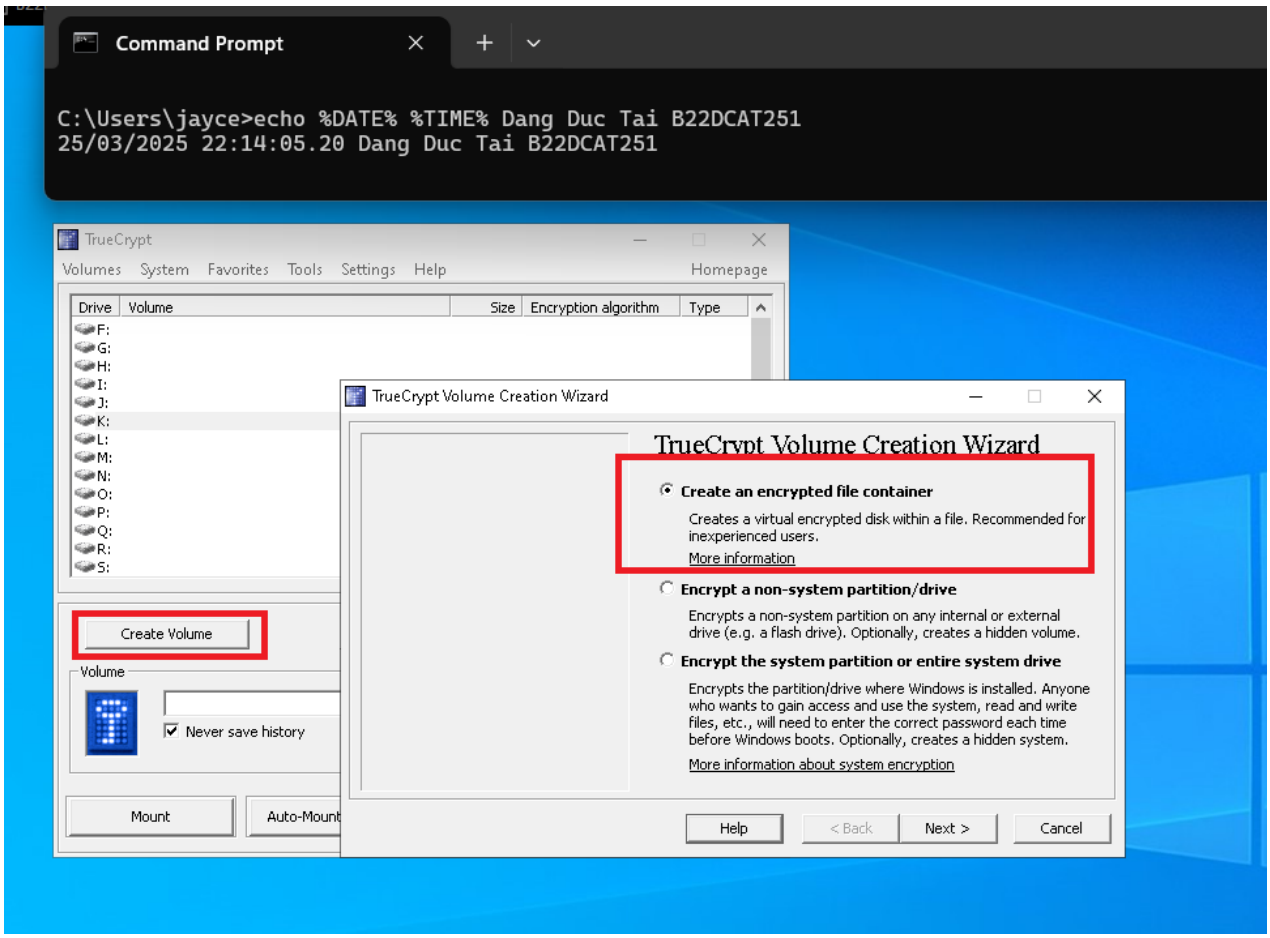
- Ổ đĩa mới (E:\) sau khi phân vùng



Hình 6 Ổ đĩa mới sau khi phân vùng

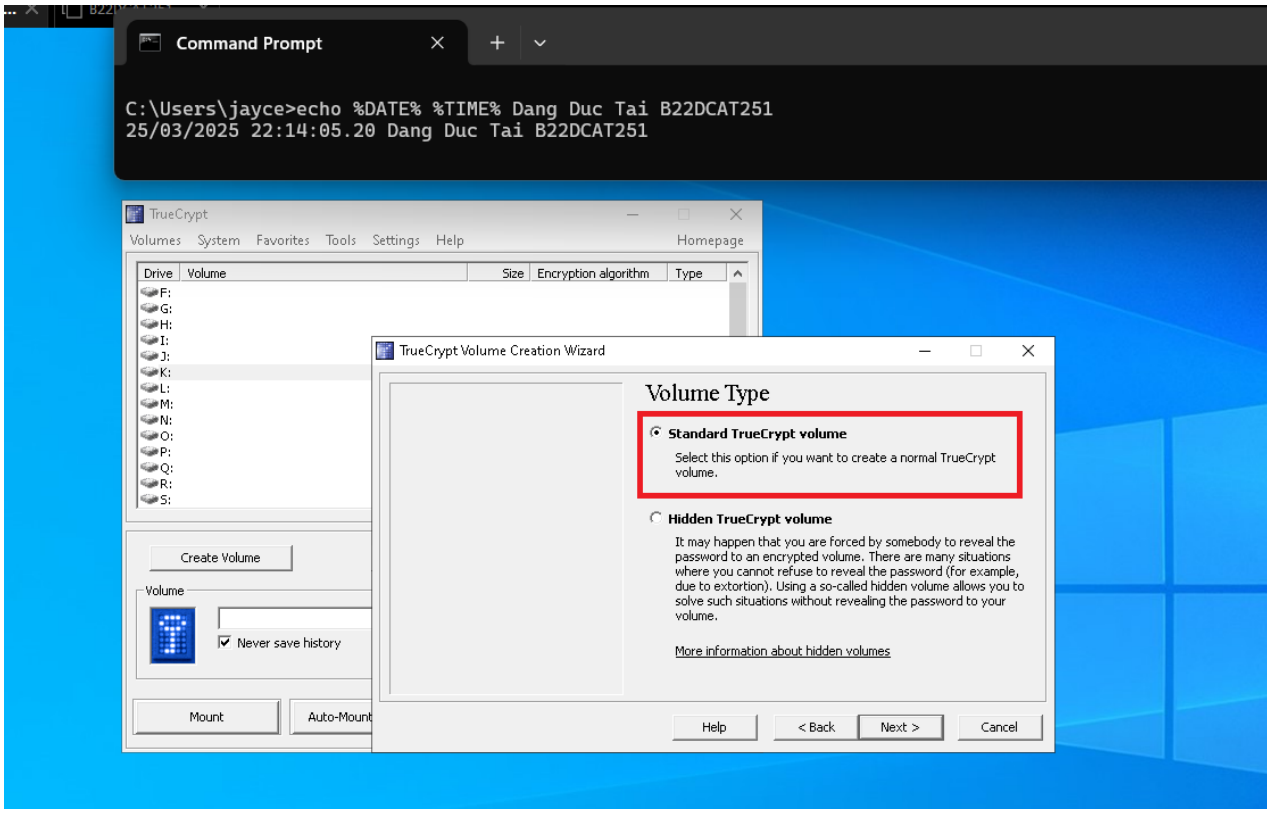
2.2.2 Sử dụng TrueCrypt cho mã hóa file

- Tạo Volume chứa dữ liệu được mã hóa
  Create Volume → Create an encrypted file container



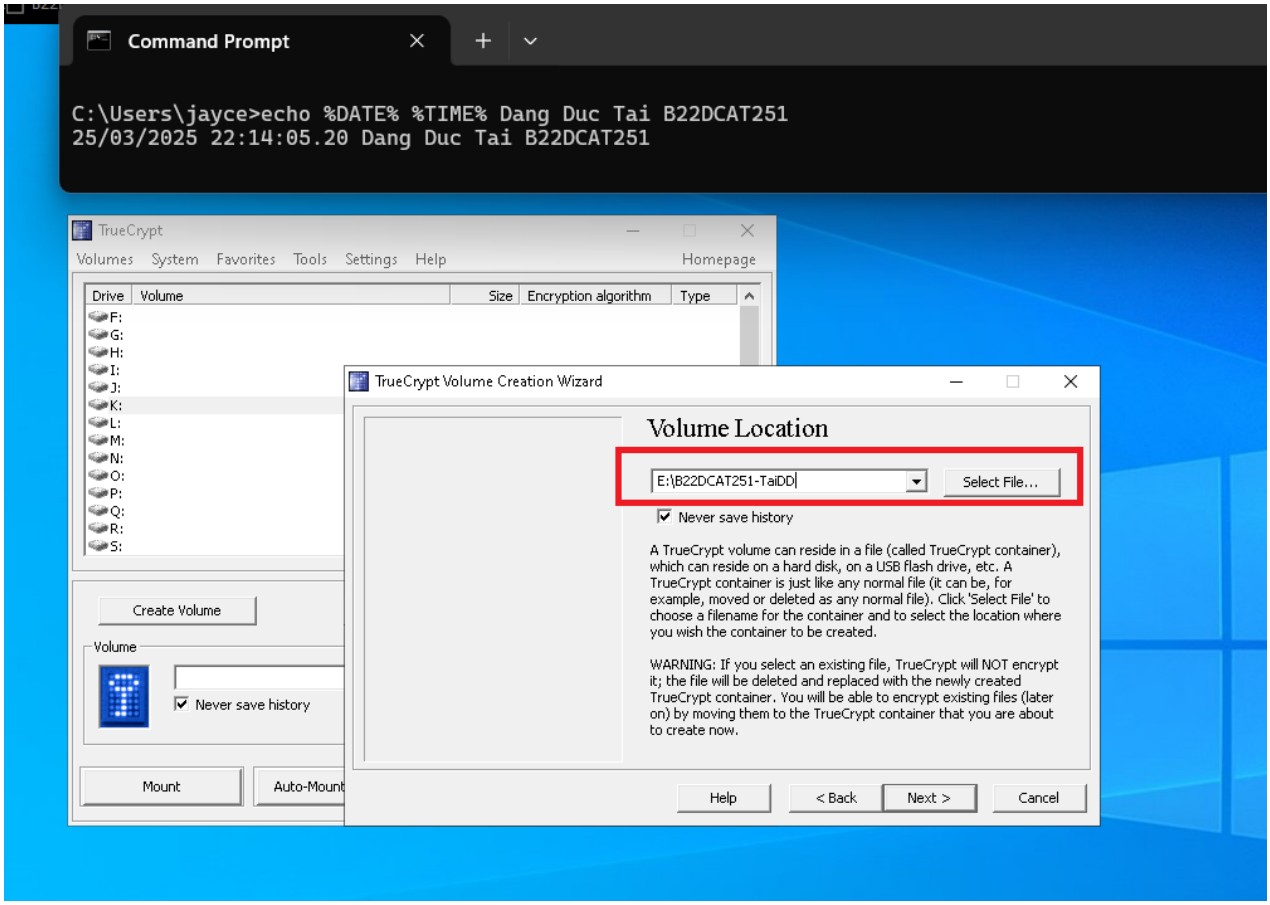
Hình 7 Tạo Volume chứa dữ liệu mã hóa

- Chọn tạo ổ đĩa TrueCrypt bình thường (Standard)



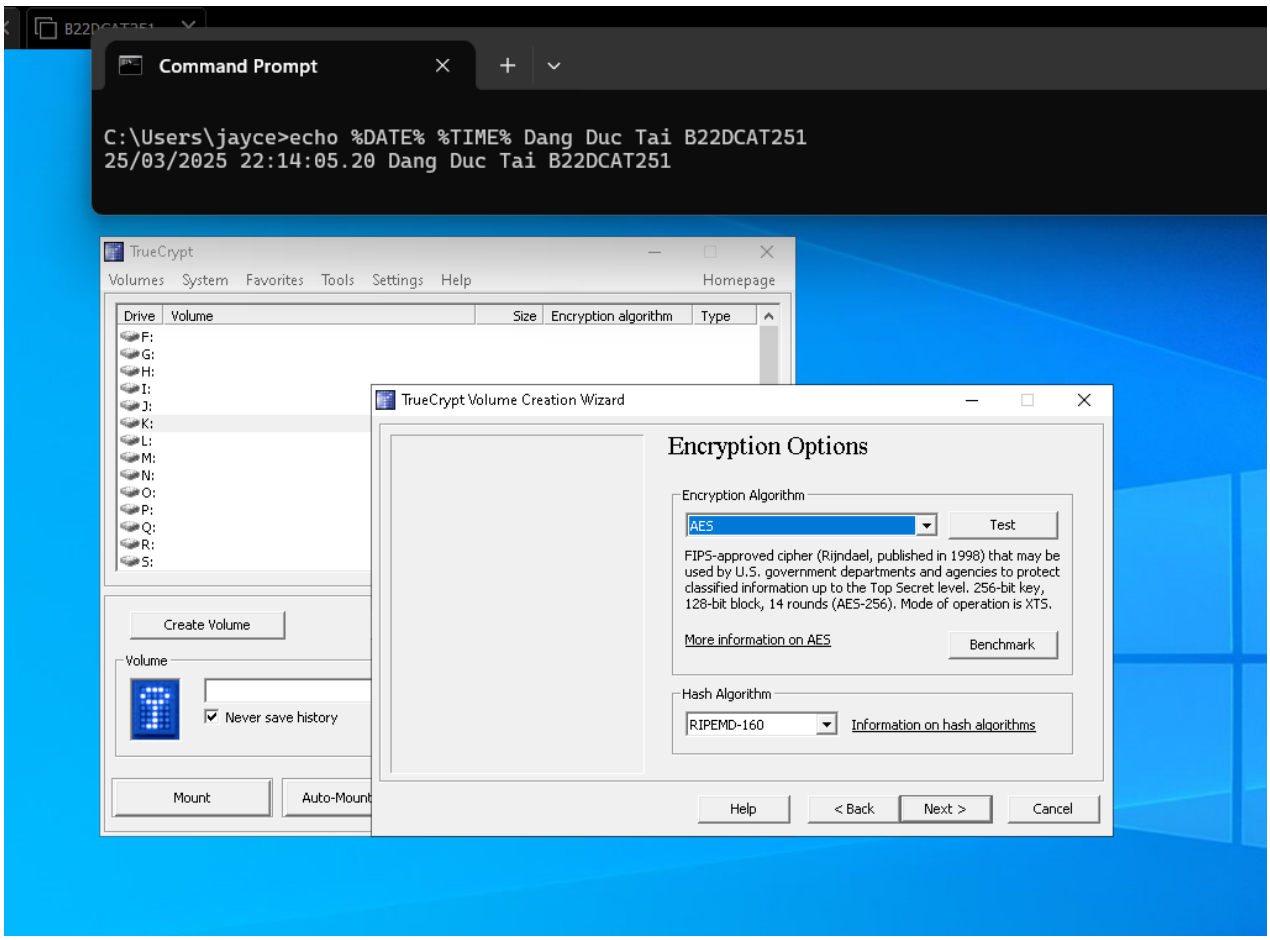
Hình 8 Chọn loại Volume

- Chọn vị trí ổ đĩa mã hóa
- Nên sử dụng ổ đĩa khác ổ C để lưu trữ file mã hóa. Trong bài này sử dụng luôn ổ đĩa E:\ mới được tạo



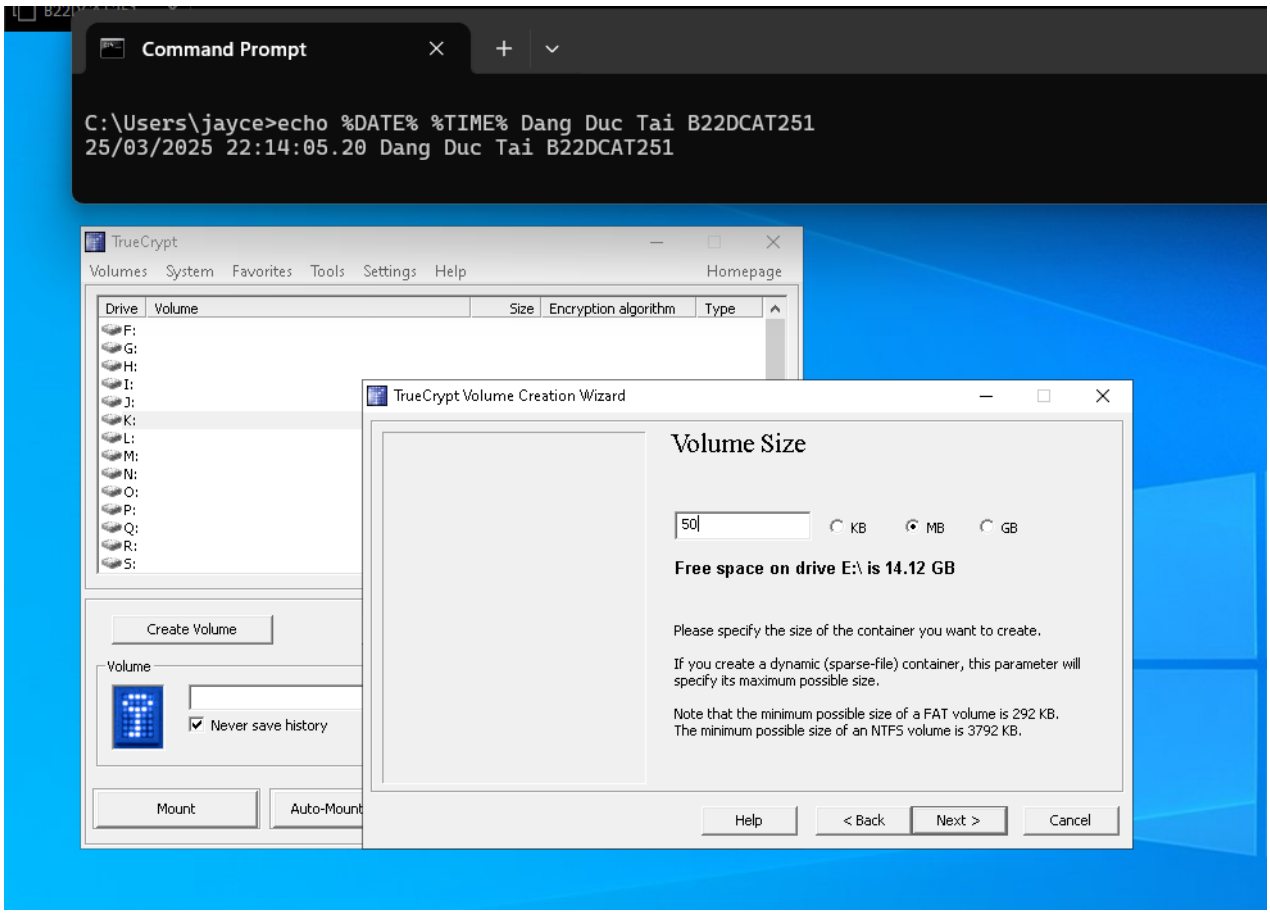
Hình 9 Chọn vị trí ổ đĩa mã hóa

- Chọn thuật toán mã hóa (Mặc định sẽ là AES)



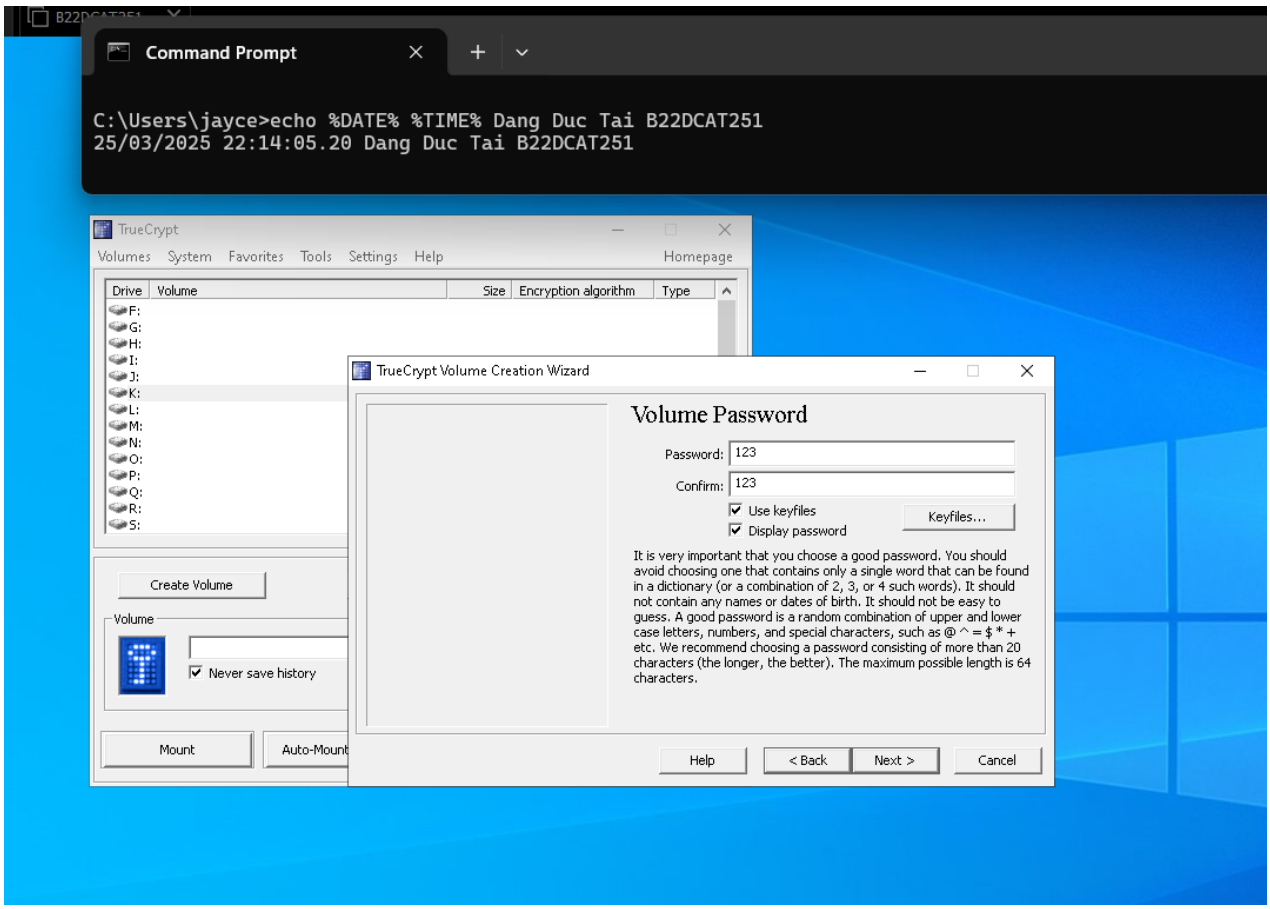
Hình 10 Chọn thuật toán mã hóa

- Chọn kích thước Volume



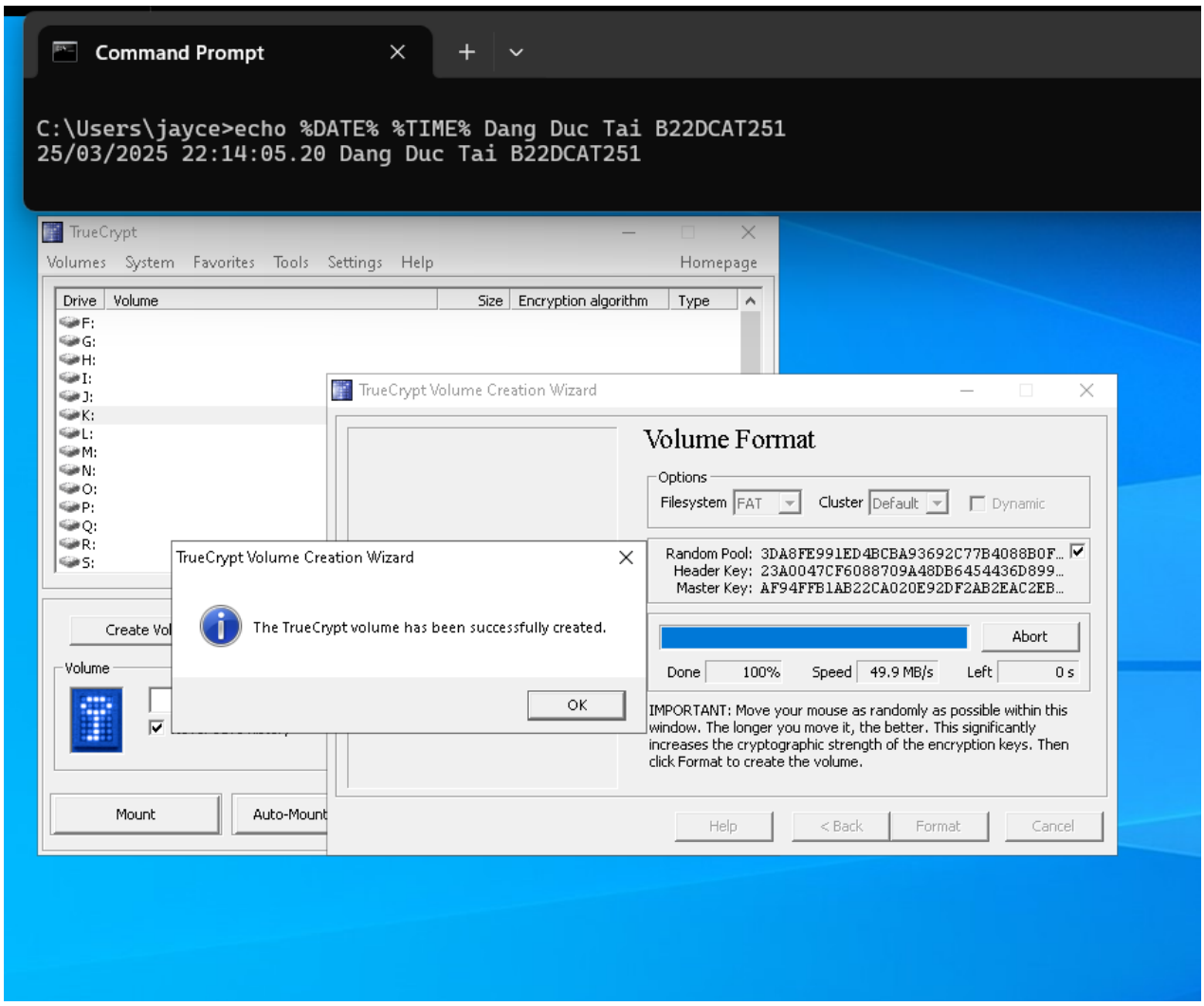
Hình 11 Chọn kích thước Volume

- Chọn mật khẩu cho Volume
- Có thể sử dụng keyfile để tăng cường mức bảo mật cho Volume



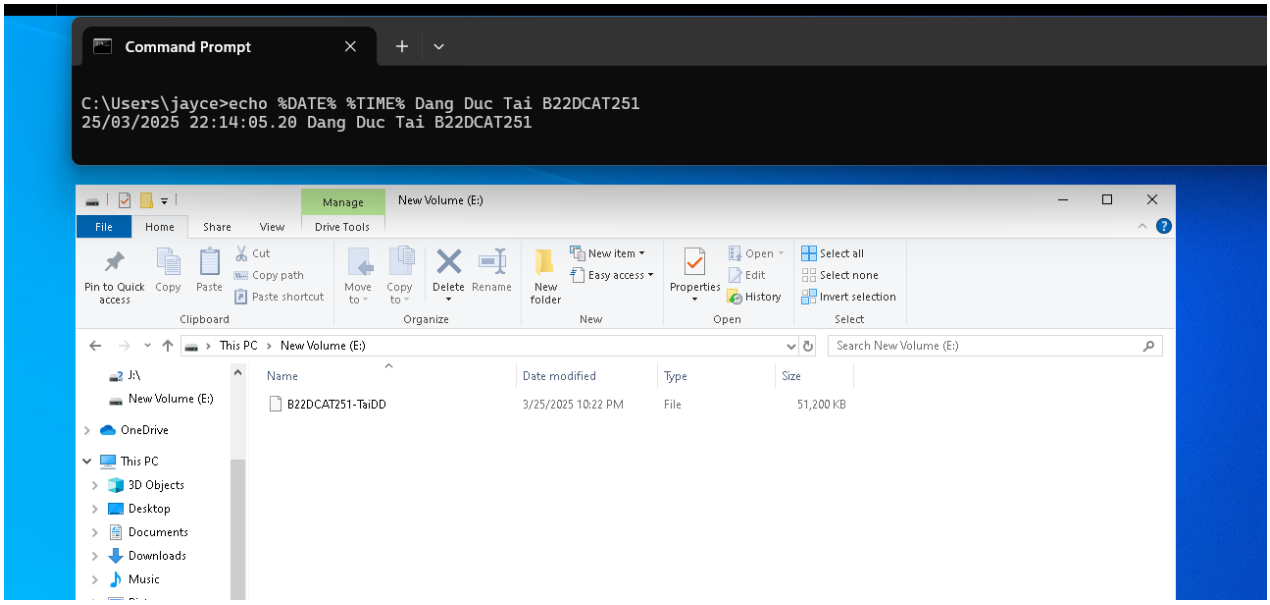
Hình 12 Chọn mật khẩu cho Volume

- Chọn định dạng Volume



Hình 13 Chọn định dạng Volume

- Kiểm tra file chứa Volume đã được tạo

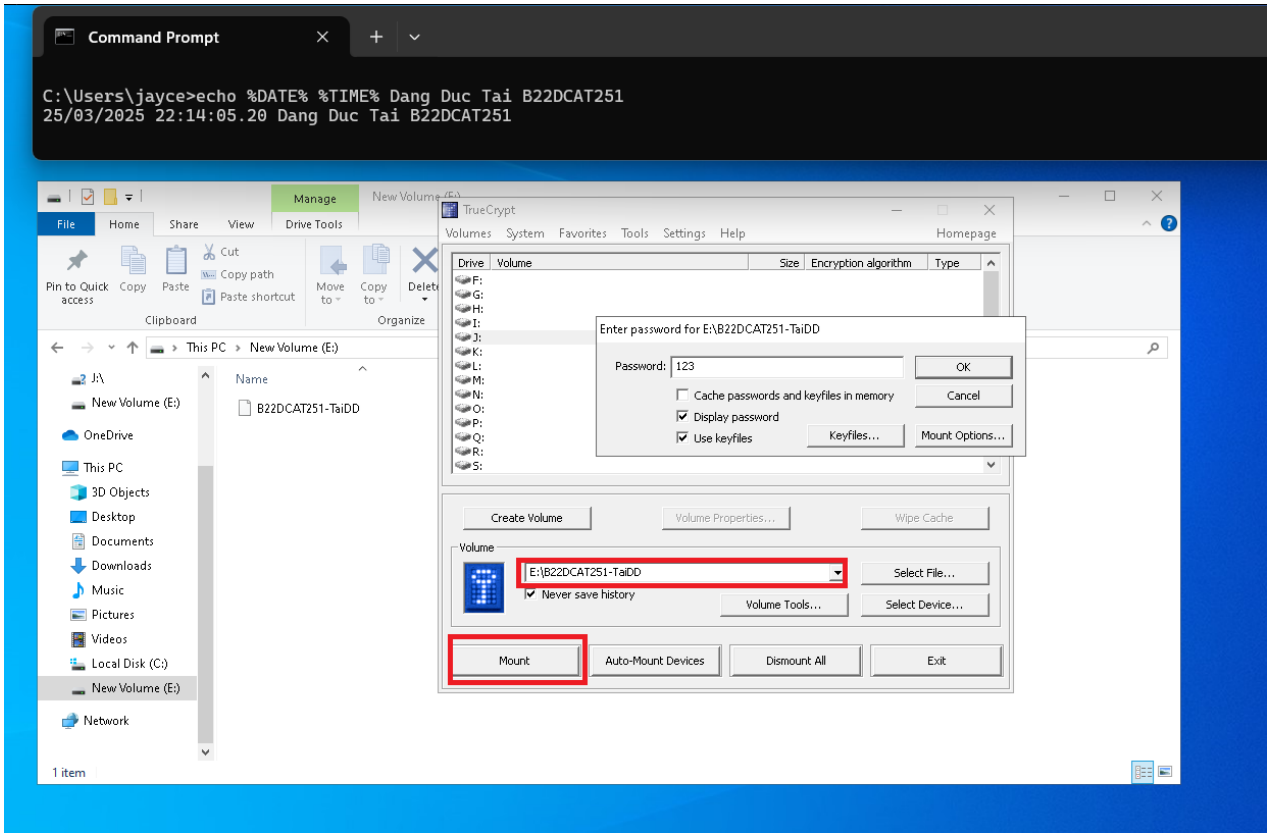


Hình 14 Kiểm tra file Volume

- Thực hiện mount Volume

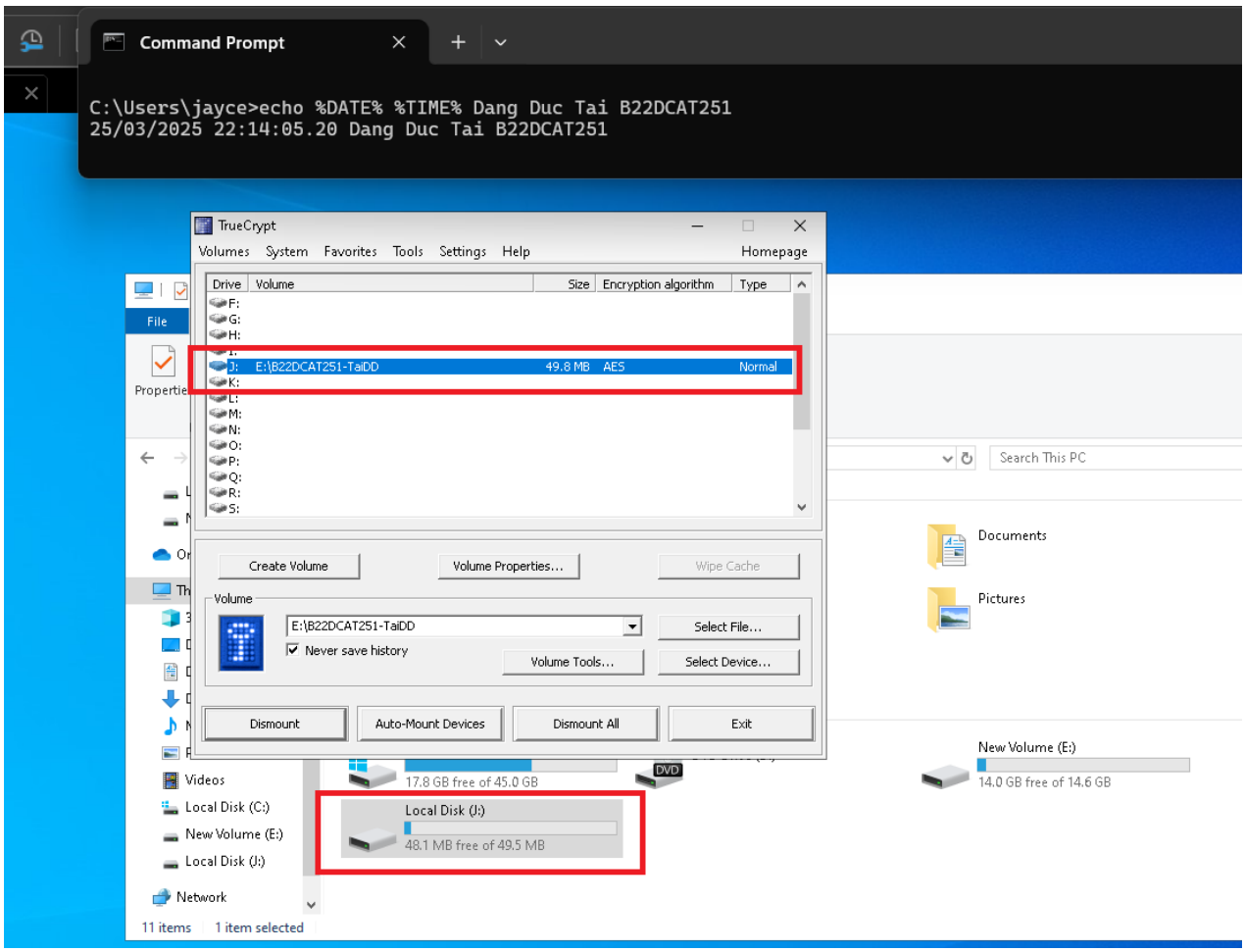
- Chọn đường dẫn chứa file Volume
- Chọn Drive lưu trữ các file mã hóa J: (*)
- Nhập mật khẩu để thực hiện mount

→ Dữ liệu sẽ được lưu tại một ổ mới (đã chọn ở bước (*))



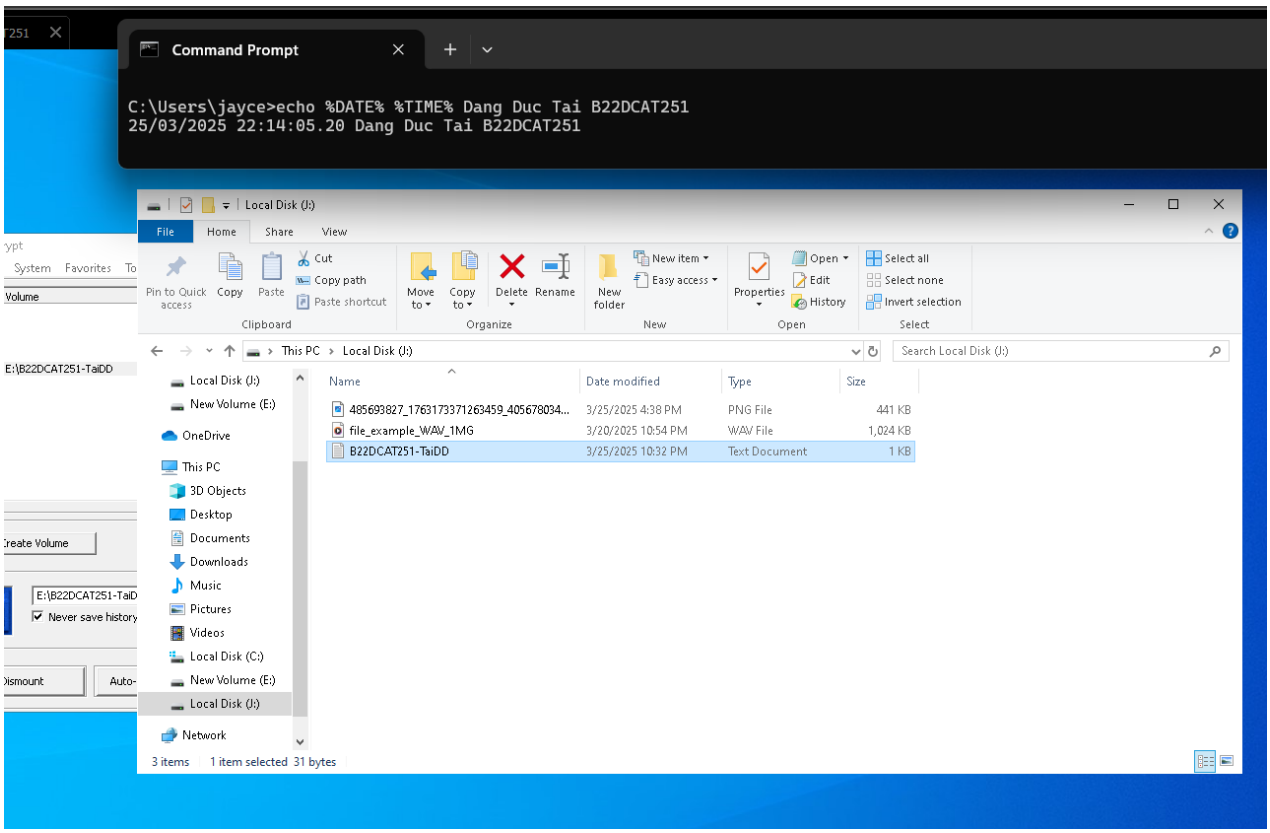
Hình 15 Mount Volume

- Kiểm tra drive mới được tạo



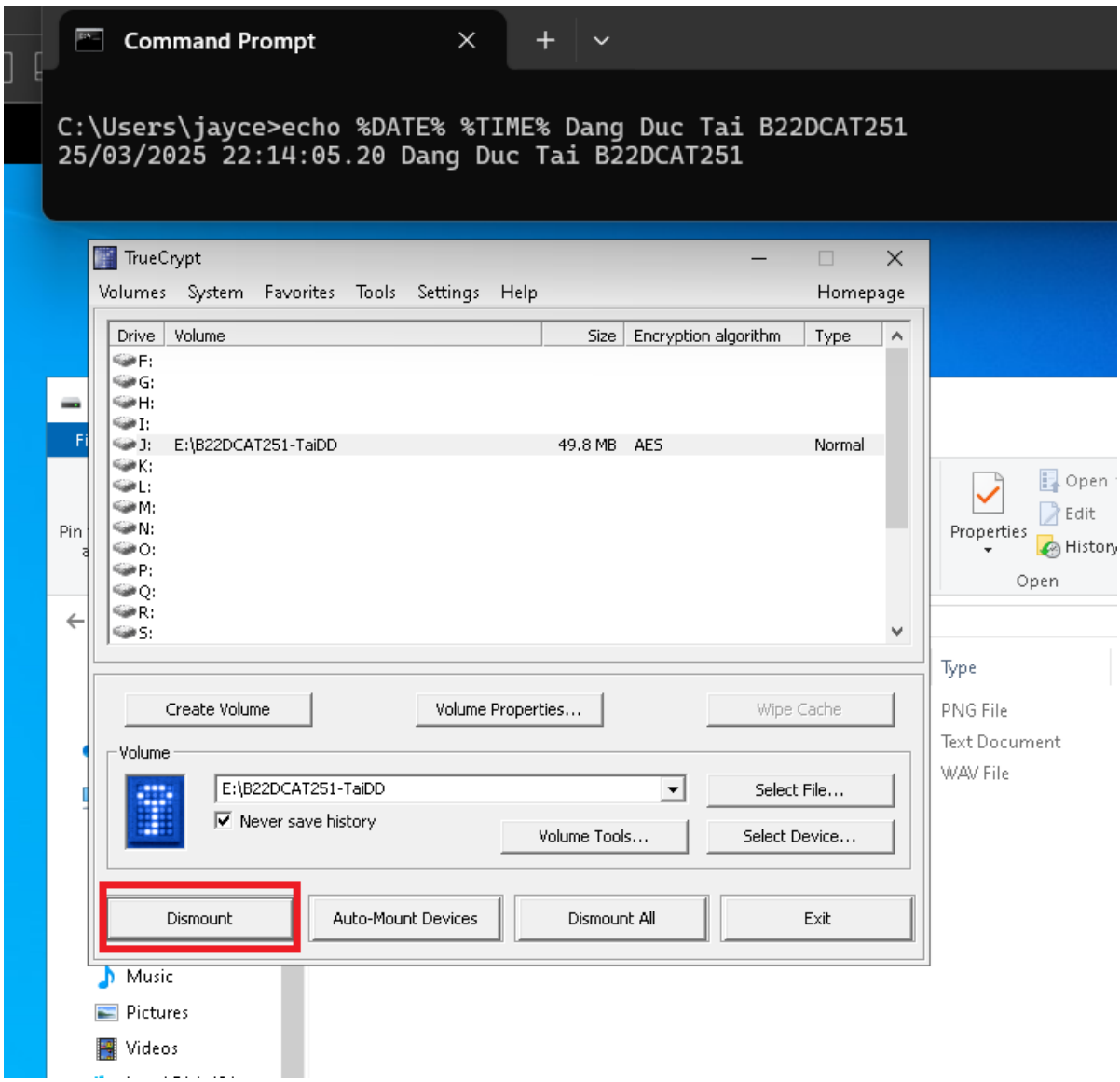
Hình 16 Kiểm tra ổ đĩa mới được tạo

- Di chuyển file cần mã hóa tới ổ đĩa Volume (J:)



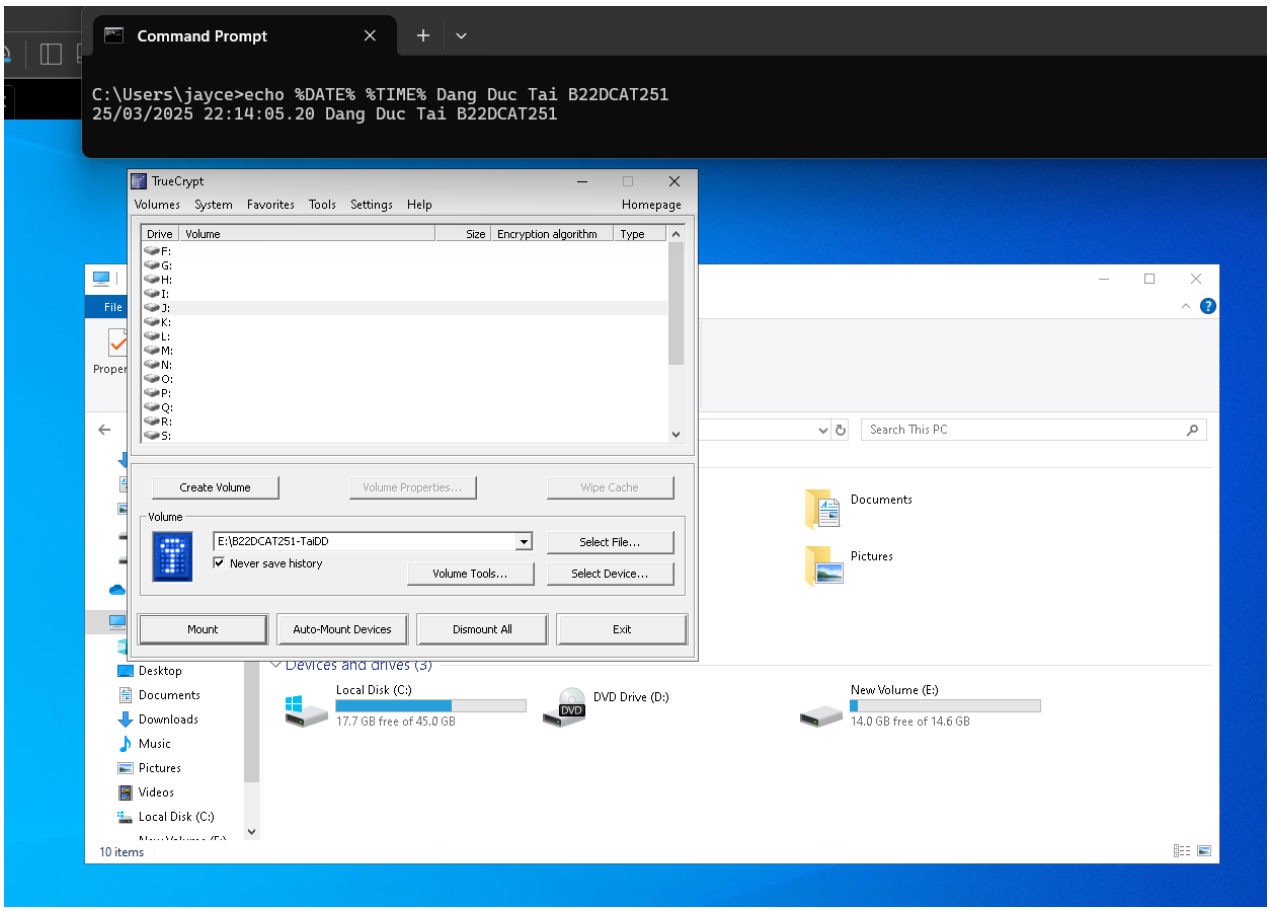
Hình 17 Di chuyển file cần mã hóa vào trong Volume

- Dismount Volume để ngắt kết nối ổ đĩa được gắn kết



Hình 18 Dismount ổ đĩa

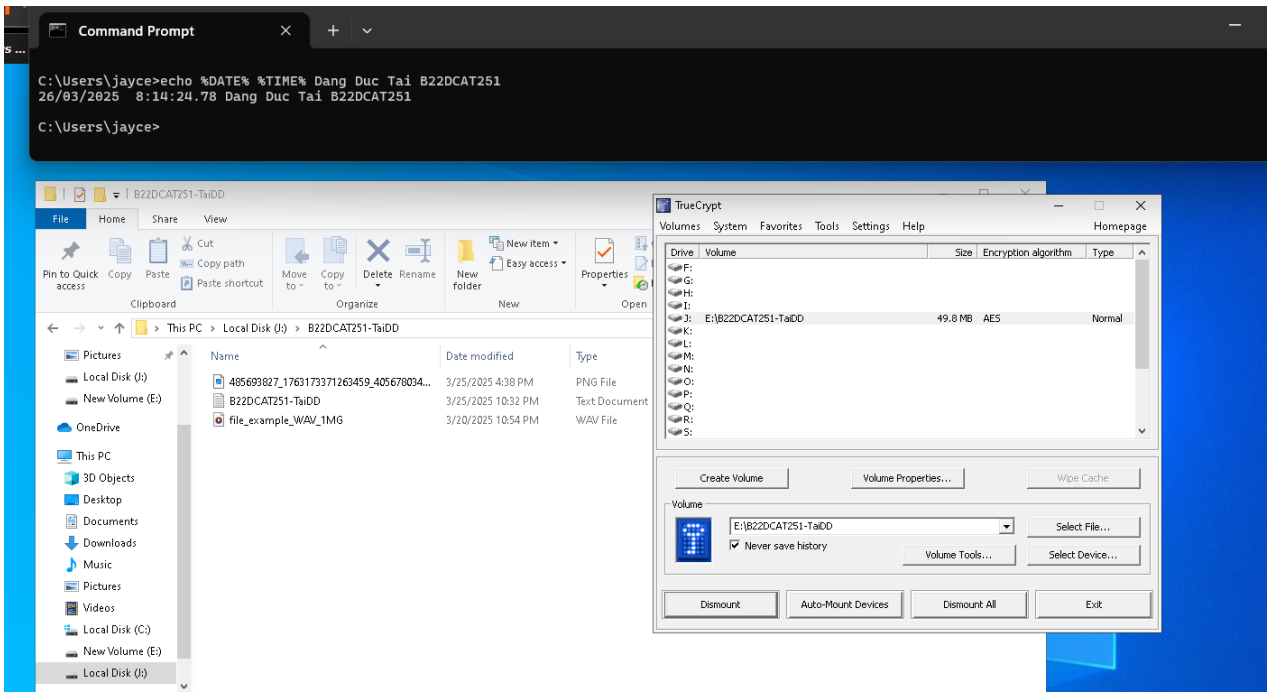
- Sau khi dismount, ổ đĩa J: sẽ biến mất



Hình 19 Kiểm tra sau khi Dismount

2.2.3 Sử dụng công cụ TrueCrypt để mã hóa thư mục

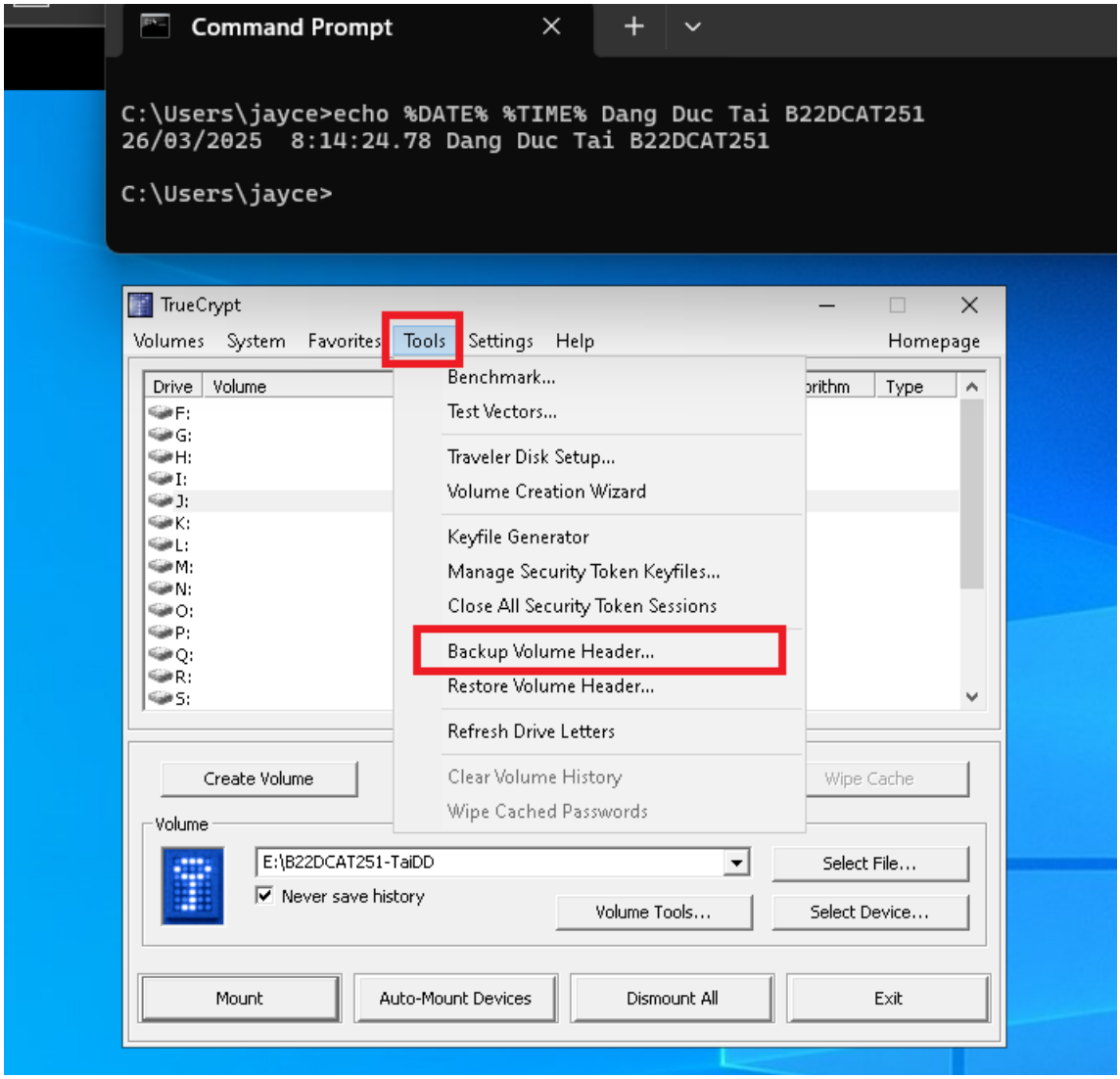
- Mã hóa thư mục tương tự như mã hóa file
  → Tạo, di chuyển thư mục cần mã hóa vào đường dẫn Volume → Chọn ổ lưu trữ dữ liệu J: → Dismount để ngắt kết nối Volume



Hình 20 Mã hóa thư mục bằng TruyCrypt

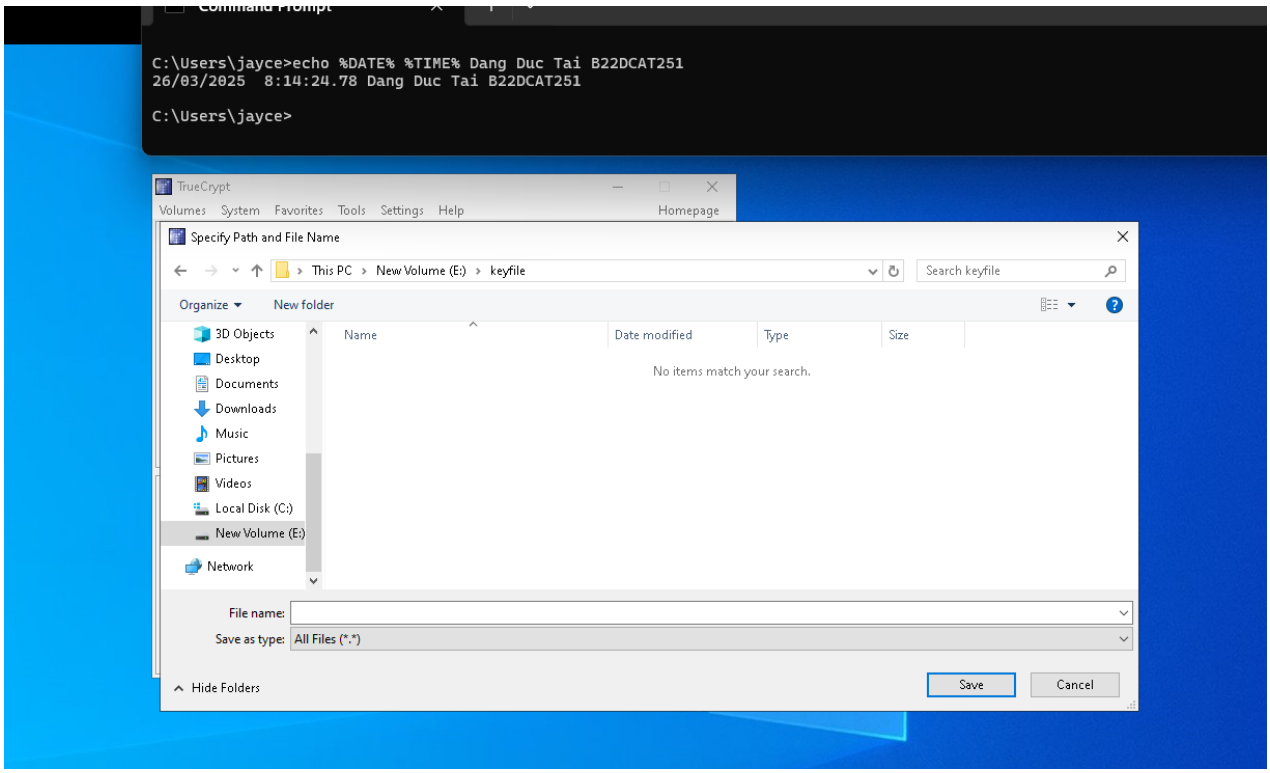
2.2.4 Sao lưu khóa mã hóa công cụ TrueCrypt

- Thực hiện các bước sau để sao lưu khóa mã
  → Tools → Backup Volume Header



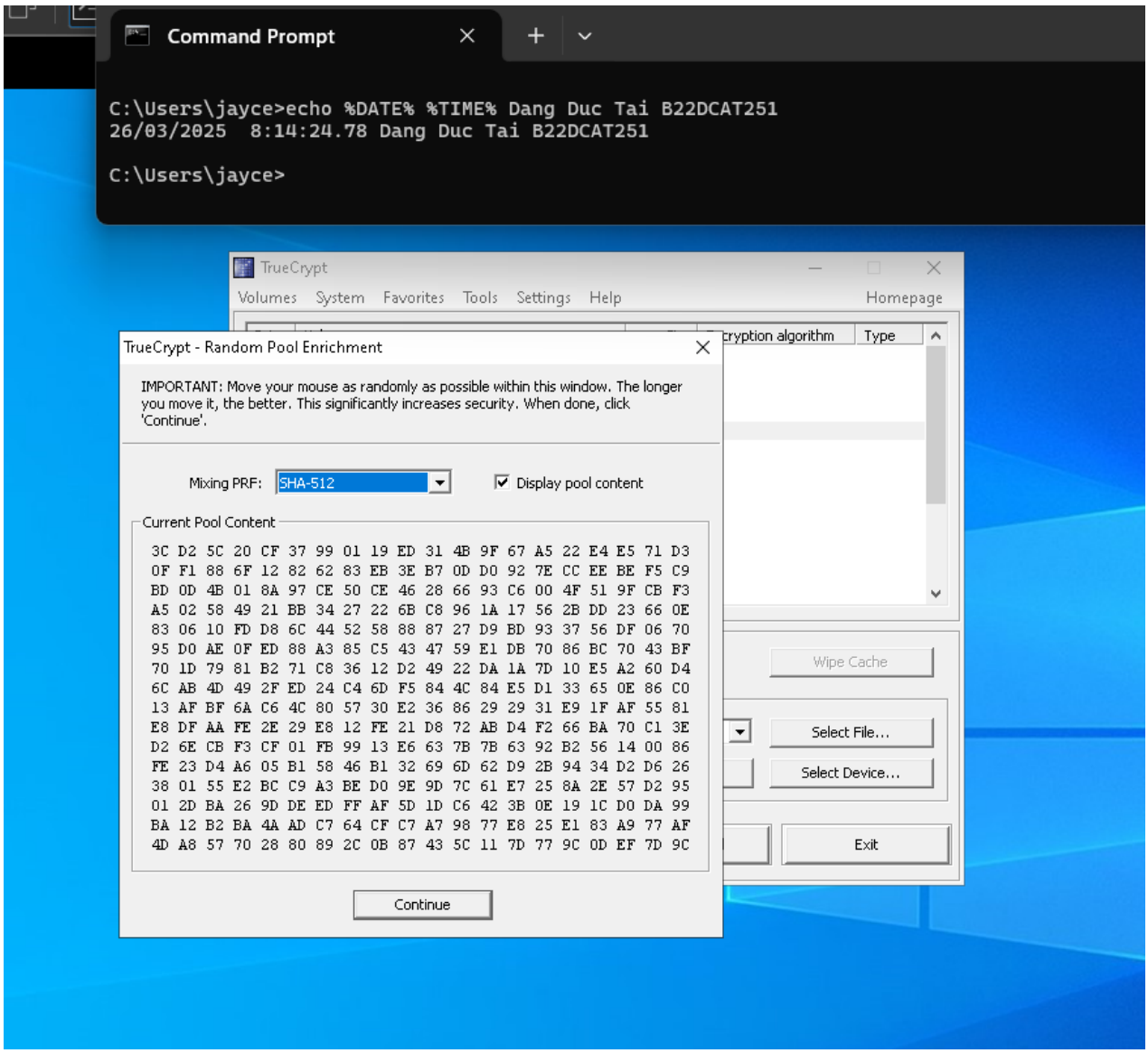
Hình 21 Thực hiện sao lưu khóa mã

- Chọn nơi lưu trữ file khóa mã



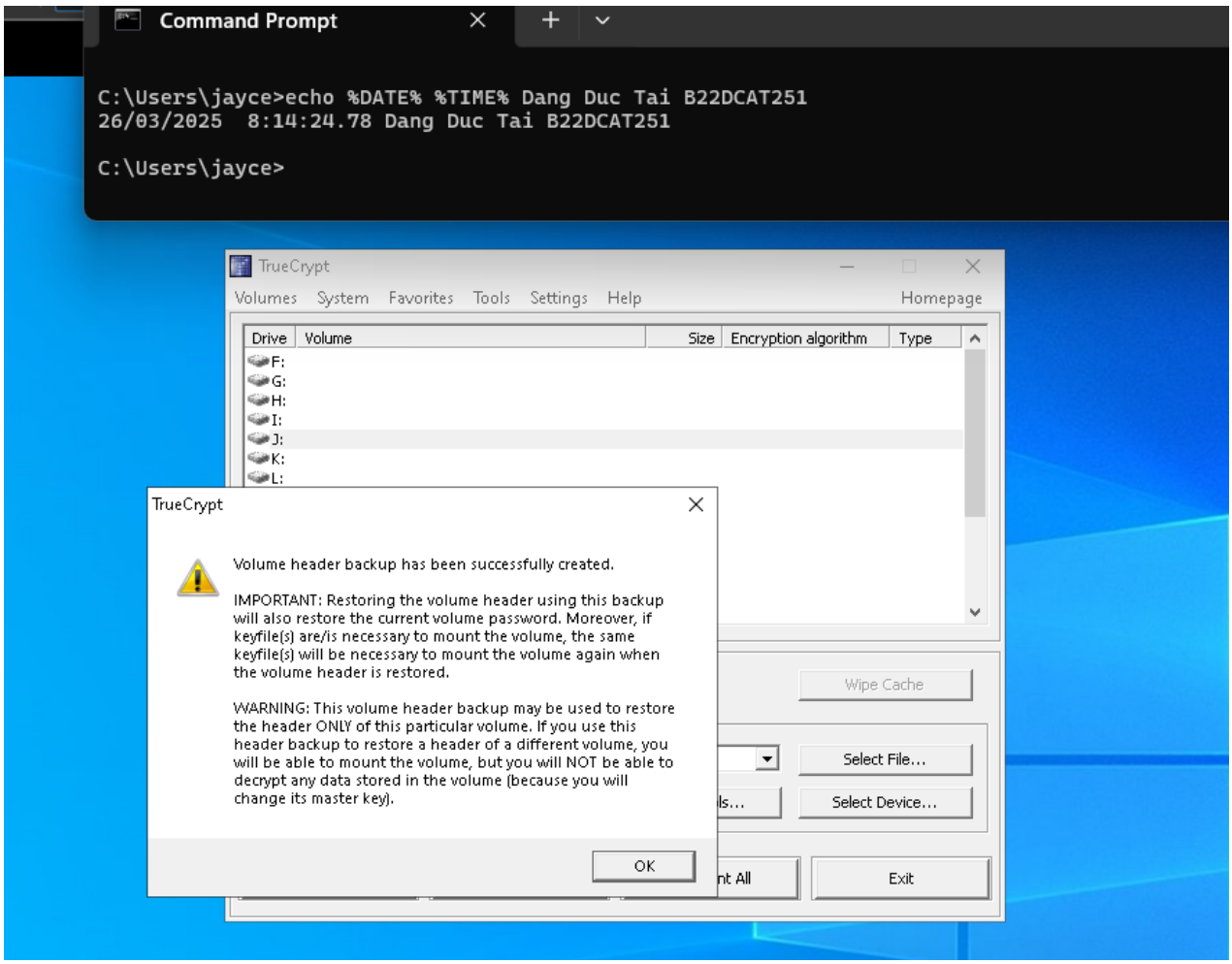
Hình 22 Chọn thư mục lưu trữ keyfile

- Quá trình mã hóa được thực hiện bằng cách tăng cường độ ngẫu nhiên (entropy) của dữ liệu, giúp khóa mã mạnh hơn
- Sử dụng thuật toán băm SHA512 để tạo khóa



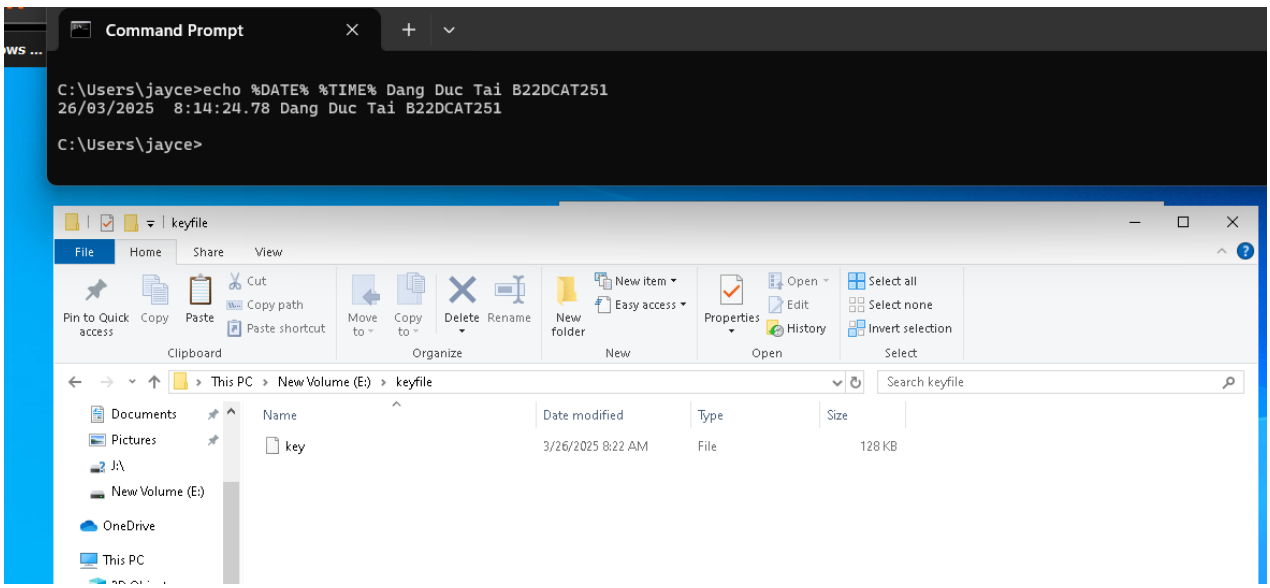
Hình 23 Quá trình tạo khóa

- Tạo khóa thành công



Hình 24 Tạo khóa thành công

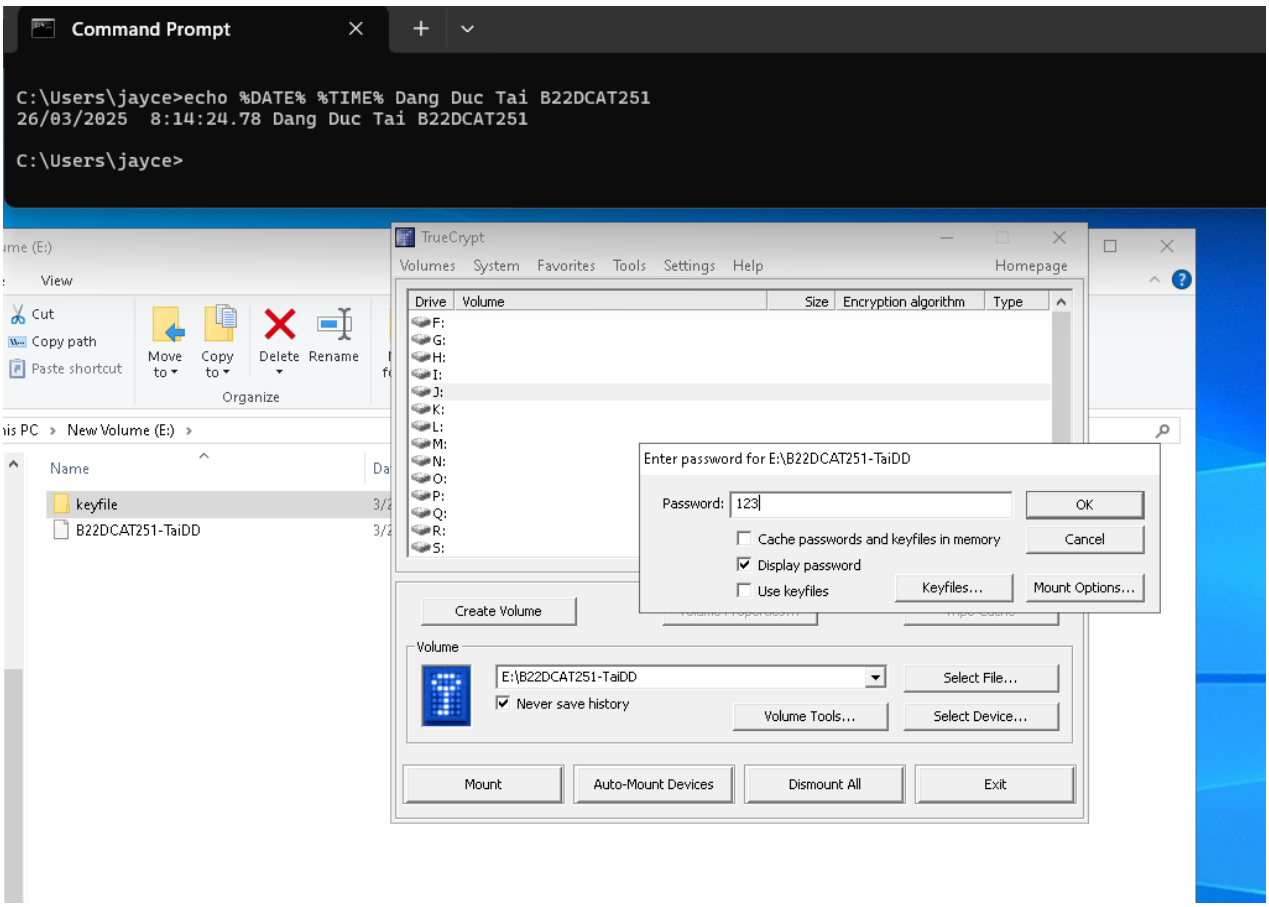
- Kiểm tra khóa sau khi tạo



Hình 25 Kiểm tra khóa sau khi tạo

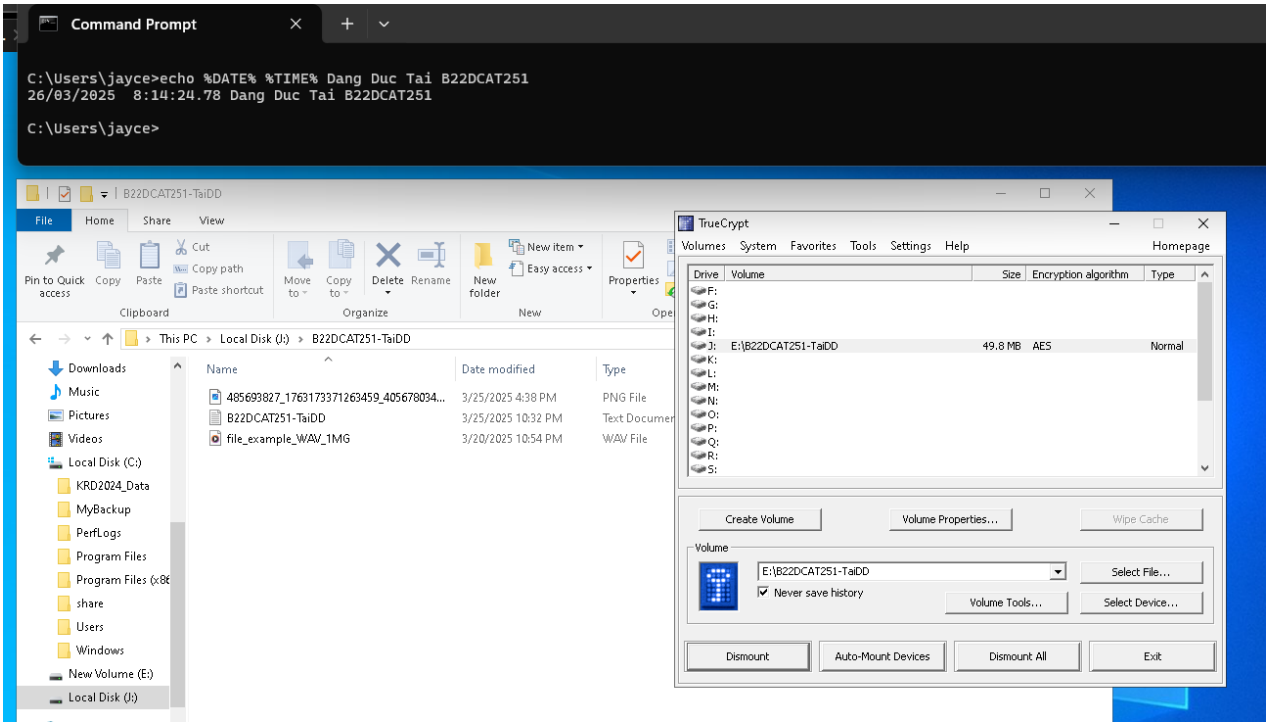
2.2.5 Sử dụng công cụ TruyCrypt để khôi phục các file và thư mục mã hóa

- Sử dụng mật khẩu để khôi phục các file và thư mục đã mã hóa



Hình 26 Khôi phục các file mã hóa

- Kiểm tra các file sau khi khôi phục



Hình 27 Kiểm tra các file sau khi khôi phục

TÀI LIỆU THAM KHẢO

[1] Đỗ Xuân Chợ, Bài giảng Mật mã học cơ sở, Học viện Công Nghệ Bưu Chính Viễn Thông, 2021.

[2] Đỗ Xuân Chợ, Bài giảng Mật mã học nâng cao, Học viện Công Nghệ Bưu Chính Viễn Thông, 2021.