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:

B22DCAT034 Trương Quốc Bảo

Giảng viên hướng dẫn: TS. Đinh Trường Duy

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**
OTFE	On-The-Fly Encryption	Mã hóa tức thời
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
KDF	Key Derivation Function	Hàm dẫn xuất khóa

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 Công cụ TrueCrypt

1.2.1.1 Giới thiệu

TrueCrypt là một phần mềm mã hóa dữ liệu mạnh mẽ, miễn phí và mã nguồn mở (source-available) được thiết kế để bảo vệ thông tin nhạy cảm thông qua mã hóa tức thời (on-the-fly encryption - OTFE). Nó cho phép người dùng tạo các đĩa ảo mã hóa (encrypted virtual disks) trong một tệp duy nhất, mã hóa toàn bộ phân vùng đĩa (partition) hoặc mã hóa toàn bộ thiết bị lưu trữ như USB hay ổ cứng, với tùy chọn yêu cầu xác thực trước khi khởi động hệ điều hành (pre-boot authentication). TrueCrypt được phát triển bởi một nhóm ẩn danh có tên "TrueCrypt Team", ra mắt lần đầu vào tháng 2 năm 2004, dựa trên mã nguồn của phần mềm E4M (Encryption for the Masses). Phần mềm này tương thích với nhiều hệ điều hành, bao gồm Windows, macOS và Linux, và được cộng đồng đánh giá cao nhờ tính linh hoạt, hiệu suất và khả năng bảo mật. Tuy nhiên, TrueCrypt đã chính thức ngừng phát triển vào ngày 28 tháng 5 năm 2014, sau khi nhóm phát triển tuyên bố phần mềm "không còn an toàn" vì các lỗ hổng tiềm ẩn không được vá (dù không có bằng chứng cụ thể về lỗ hổng nghiêm trọng tại thời điểm đó). Sau khi ngừng phát triển, các dự án kế thừa như VeraCrypt đã tiếp tục cải tiến và duy trì các tính năng của TrueCrypt.

TrueCrypt không chỉ đơn thuần là công cụ mã hóa mà còn nổi bật với tính năng "plausible deniability" (từ chối hợp lý), cho phép người dùng che giấu sự tồn tại của dữ liệu mã hóa thông qua các ổ đĩa ẩn (hidden volumes). Điều này đặc biệt hữu ích trong các tình huống pháp lý hoặc bị ép buộc tiết lộ mật khẩu, vì không thể chứng minh được sự tồn tại của dữ liệu ẩn mà không có mật khẩu riêng biệt.

1.2.1.2 Tính năng của TrueCrypt

TrueCrypt sử dụng một quy trình mã hóa phức tạp và hiệu quả để bảo vệ tệp hoặc thư mục, dựa trên các thuật toán mã hóa tiêu chuẩn công nghiệp và cơ chế hoạt động linh hoạt. Dưới đây là một số tính năng quan trọng:

- Tạo ổ đĩa mã hóa (Encrypted Volume):

TrueCrypt cho phép người dùng tạo một "ổ đĩa ảo" (virtual volume) dưới dạng tệp chứa (container file), ví dụ: mydata.tc, hoặc mã hóa trực tiếp một phân vùng/thiết bị. Khi tạo ổ đĩa, người dùng chọn kích thước (ví dụ: 10MB, 1GB), hệ thống tệp (FAT, NTFS, ext2/ext3), và thuật toán mã hóa.

Các thuật toán mã hóa được hỗ trợ bao gồm AES (chuẩn mã hóa tiên tiến với khóa 256-bit), Serpent, Twofish, hoặc kết hợp chúng theo dạng xếp chồng (cascade) như AES-Twofish hoặc AES-Twofish-Serpent để tăng cường bảo mật. Khóa mã hóa được tạo từ mật khẩu người dùng kết hợp với một giá trị salt ngẫu nhiên, sử dụng hàm băm như SHA-512, RIPEMD-160 hoặc Whirlpool để đảm bảo tính duy nhất và độ phức tạp của khóa.

- Gắn ổ đĩa (Mounting):

Sau khi tạo, ổ đĩa mã hóa được gắn (mounted) như một ổ đĩa ảo trong hệ thống (ví dụ: ổ D: trên Windows). Để gắn, người dùng phải nhập mật khẩu chính xác hoặc cung cấp tệp khóa (keyfile). Nếu xác thực thành công, TrueCrypt giải mã tiêu đề ổ đĩa (volume header) chứa thông tin cấu hình và khóa chính (master key), sau đó sử dụng khóa này để mã hóa/giải mã dữ liệu.

- Mã hóa tức thời (On-the-Fly Encryption - OTFE):

TrueCrypt mã hóa và giải mã dữ liệu trong thời gian thực. Khi người dùng ghi dữ liệu vào ổ đĩa ảo (ví dụ: sao chép tệp vào ổ D:), dữ liệu được mã hóa trước khi lưu vào ổ đĩa. Ngược lại, khi đọc dữ liệu, TrueCrypt giải mã dữ liệu ngay lập tức để hiển thị dưới dạng không mã hóa cho người dùng. Quá trình này diễn ra trong bộ nhớ (RAM) và không lưu trữ dữ liệu giải mã trên đĩa, đảm bảo tính bảo mật.

- Cơ chế bảo vệ khóa:

Khóa mã hóa chính (master key) được lưu trong tiêu đề ổ đĩa (volume header), vốn cũng được mã hóa bằng mật khẩu người dùng. TrueCrypt sử dụng hàm tạo khóa (key derivation function - KDF) như PBKDF2 với hàng nghìn lần lặp (iteration) để tăng độ khó cho các cuộc tấn công vét cạn (brute-force). Người dùng có thể sao lưu tiêu đề ổ đĩa để khôi phục dữ liệu nếu mật khẩu bị quên hoặc tiêu đề bị hỏng.

- Tính năng ổ đĩa ẩn (Hidden Volume):

TrueCrypt hỗ trợ tạo ổ đĩa ẩn bên trong ổ đĩa chính. Khi tạo, người dùng chỉ định hai mật khẩu: một cho ổ đĩa "bên ngoài" (outer volume) và một cho ổ đĩa "ẩn" (hidden volume). Ổ đĩa ẩn nằm trong không gian trống của ổ đĩa bên ngoài và không thể phát hiện nếu chỉ biết mật khẩu của ổ đĩa bên ngoài. Điều này cung cấp "plausible deniability": nếu bị ép buộc, người dùng có thể tiết lộ mật khẩu ổ đĩa bên ngoài mà không làm lộ dữ liệu nhạy cảm trong ổ đĩa ẩn.

1.2.1.3 Cách thức mã hóa

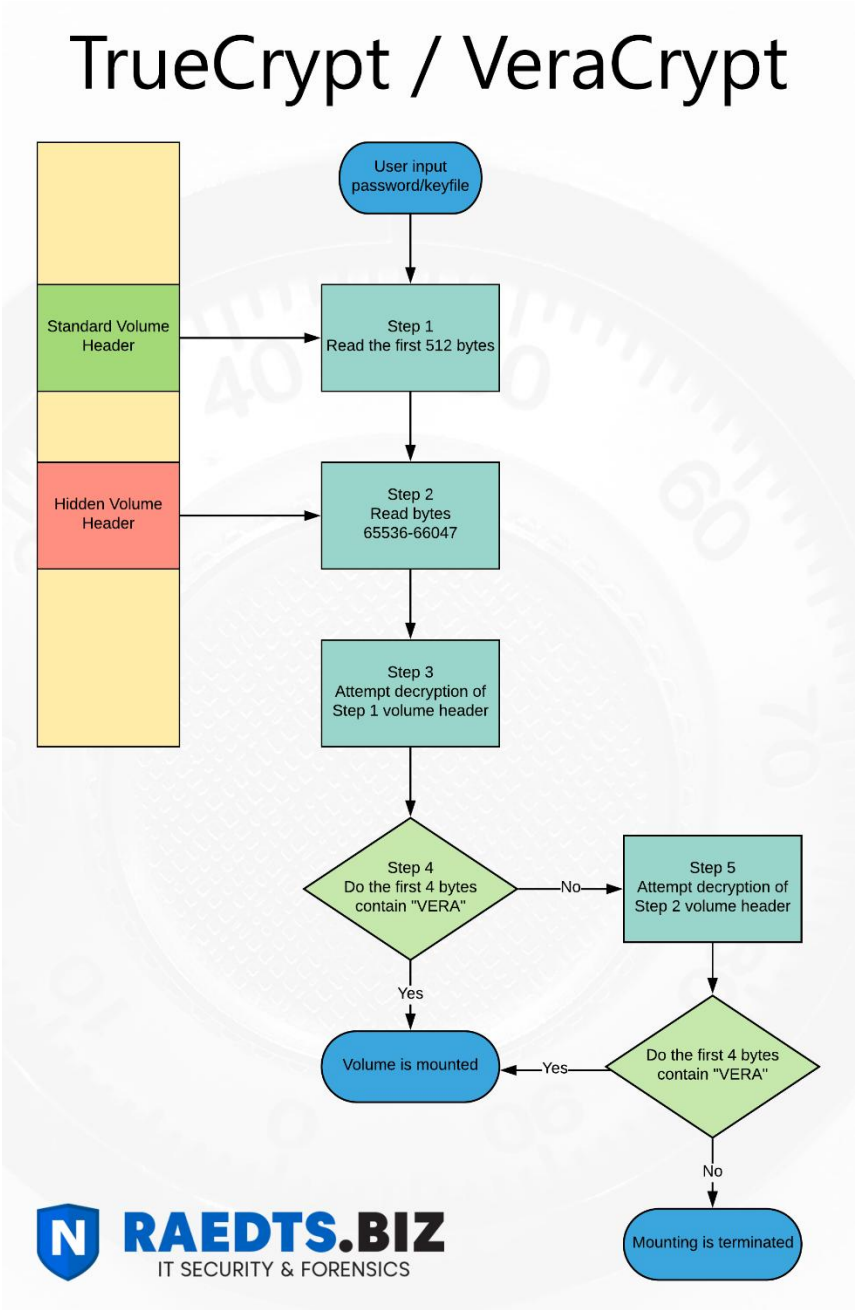
Bước 1: 512 byte đầu tiên của volume được đọc thành RAM, trong đó 64 byte đầu tiên là salt. Đối với mã hóa hệ thống, 512 byte cuối cùng của rãnh ổ đĩa logic đầu tiên được đọc vào RAM.

Bước 2: Các byte 65536->66047 của volume được đọc thành RAM. Đối với mã hóa hệ thống, byte 65536->66047 của phân vùng đầu tiên nằm phía sau phân vùng hoạt động được đọc.

Bước 3: TrueCrypt cố gắng giải mã tiêu đề tiêu chuẩn của volume trong Bước 1. Tất cả dữ liệu được sử dụng và tạo trong quá trình giải mã được giữ trong RAM. Do volume không chứa bất kỳ thông tin nào về các tham số đã sử dụng khi volume được tạo, các tham số phải được xác định thông qua quá trình thử nghiệm và sửa lỗi.

Bước 4: Nhập mật khẩu Mật khẩu được nhập bởi người dùng và salt được đọc trong bước 1 được chuyển đến hàm dẫn xuất khóa tiêu đề, tạo ra một chuỗi các giá trị mà từ đó khóa mã hóa tiêu đề và khóa tiêu đề thứ cấp (chế độ XTS) được hình thành. Các khóa này được sử dụng để giải mã tiêu đề volume.

Bước 5: Giải mã, TrueCrypt giải mã theo sơ đồ sau:



Hình 1 Sơ đồ giải mã của TrueCrypt

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

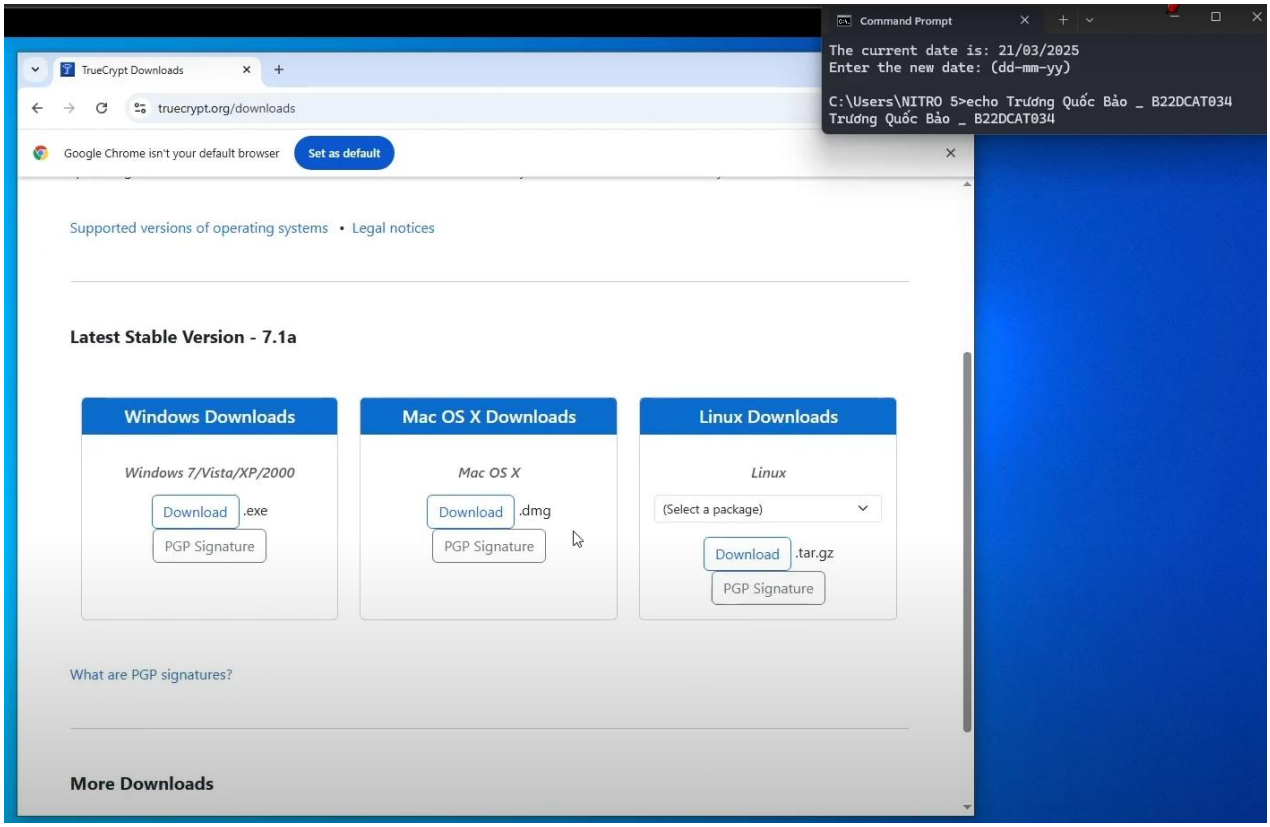
- Cài đặt công cụ ảo hóa.
- Cài đặt máy ảo chạy hệ điều hành Windows.
- Cài đặt TrueCrypt trên hệ điều hành windows

2.2 Các bước thực hiện

2.2.1 Chuẩn bị môi trường

Đảm bảo máy Windows có kết nối mạng LAN.

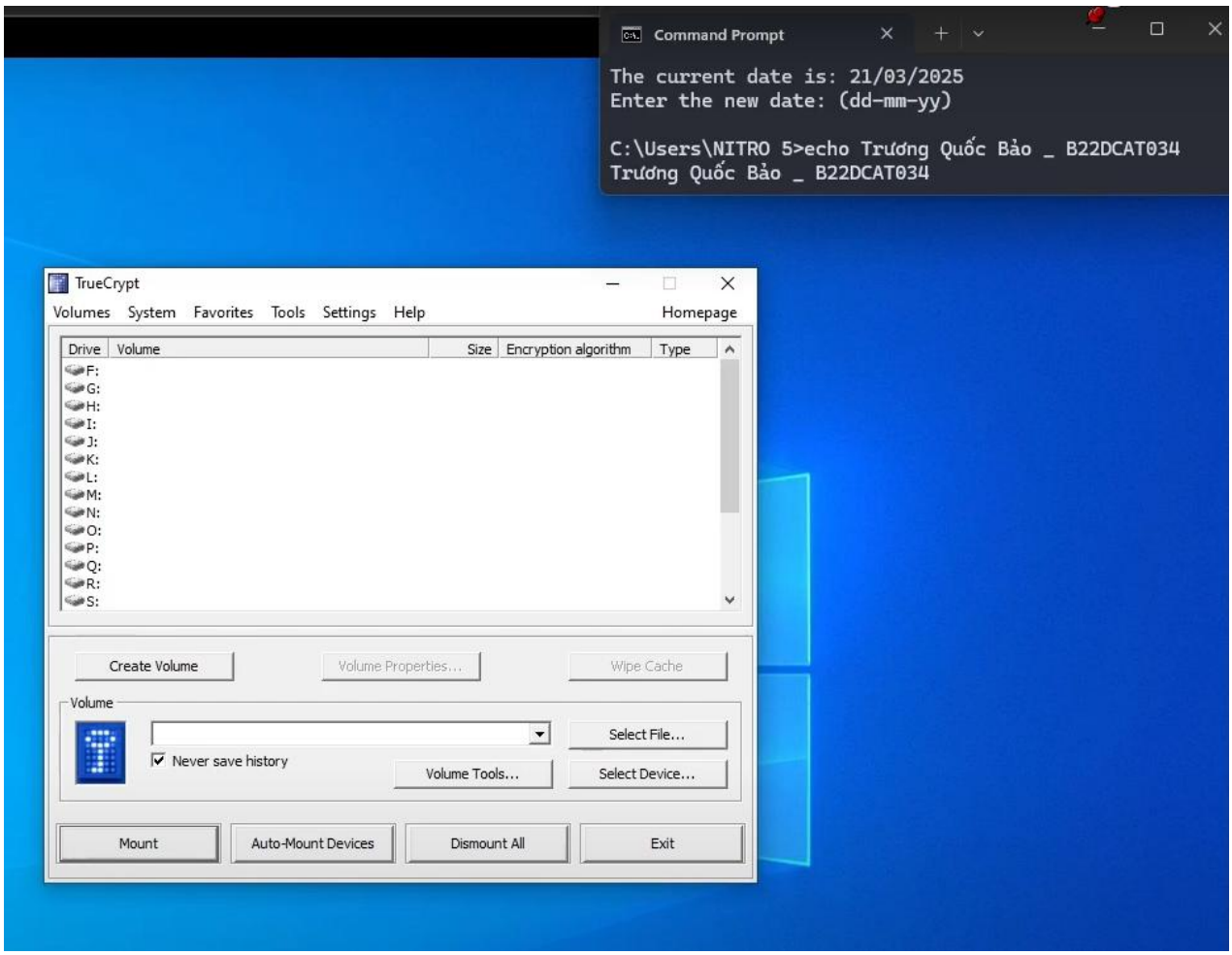
Truy cập trình duyệt để tìm kiếm công cụ TrueCrypt, tải xuống phiên bản dành cho Windows. Vì đã ngừng hỗ trợ nên phiên bản mới nhất là dành cho Windows 7.



Hình 2 Cài đặt TrueCrypt

Tải xuống và tiến hành cài đặt công cụ.

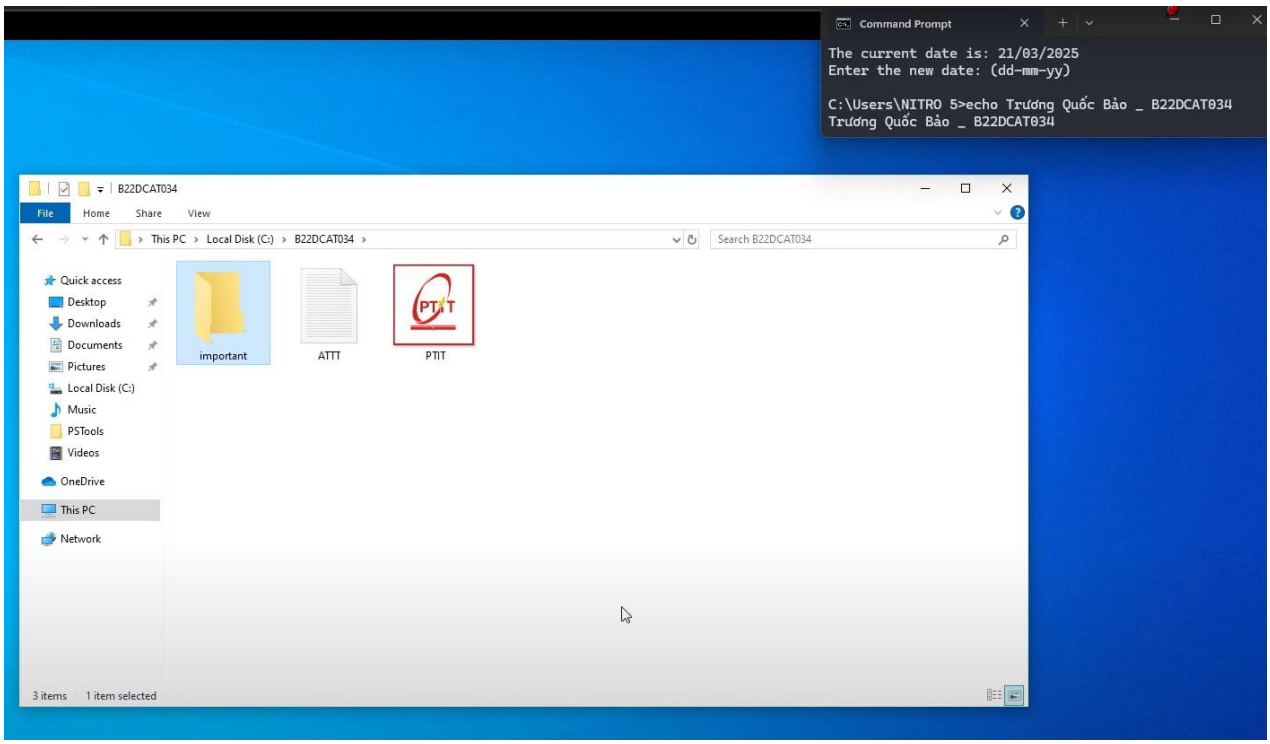
Khi chạy, giao diện làm việc sẽ như hình bên dưới.



Hình 3 Giao diện làm việc của TrueCrypt

2.2.2 Tạo ổ đĩa lưu trữ

Ta tạo một số file dữ liệu ở trong một thư mục bất kì trên máy Windows, có thể lưu ở ổ nào tùy thích.

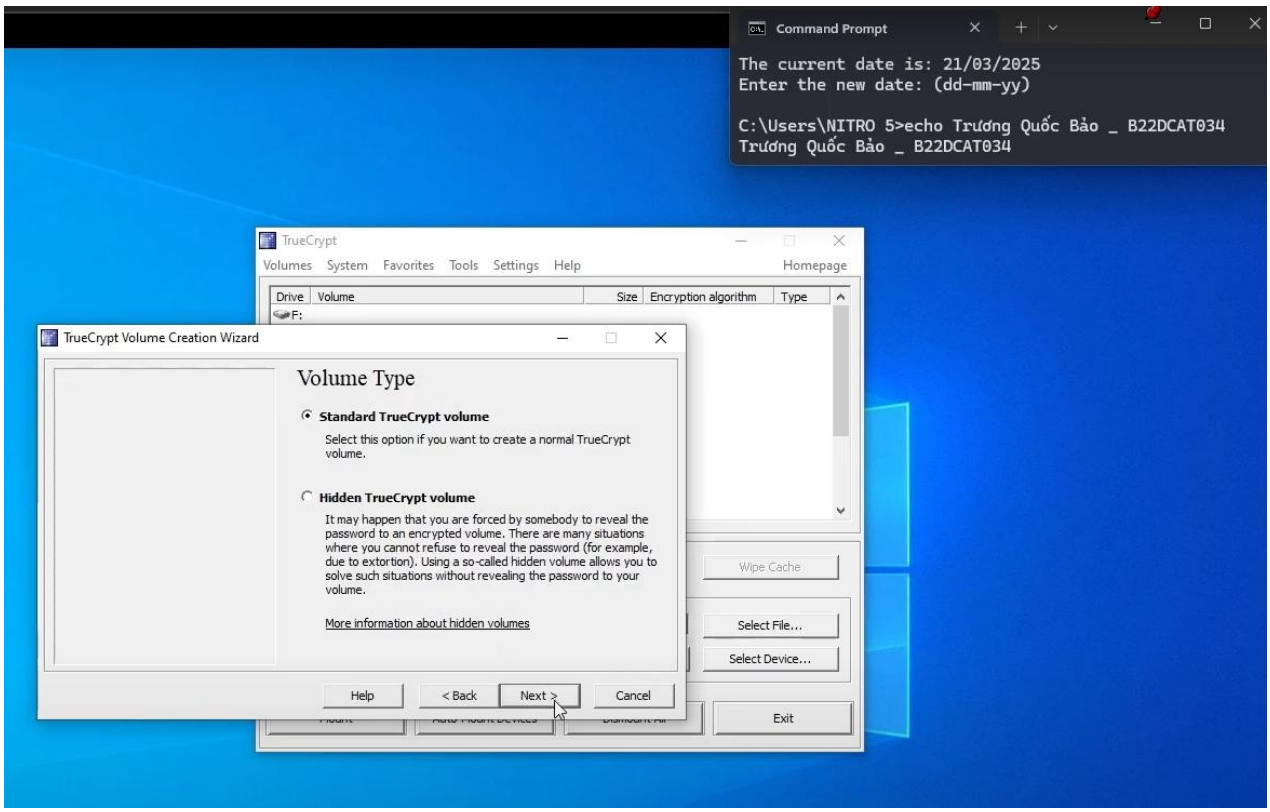


Hình 4 Tạo thư mục chứa các file dữ liệu

Mở công cụ TrueCrypt để tiến hành tạo ổ đĩa mã hóa.

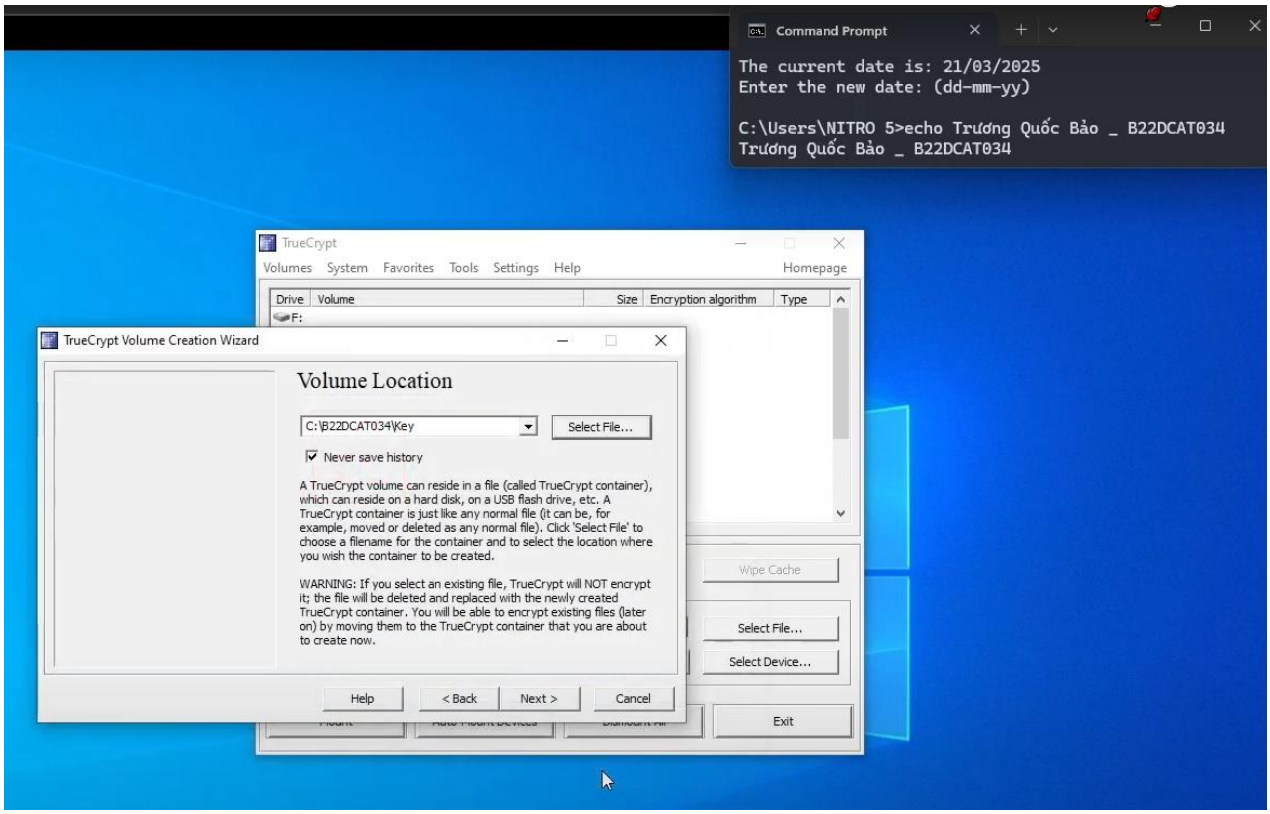
Từ giao diện làm việc chính, chọn tên ổ đĩa muốn đặt và chọn “Create Volume”

Chọn volume tiêu chuẩn (Standard) và nhấn “Next”



Hình 5 Chọn kiểu mã hóa ổ đĩa

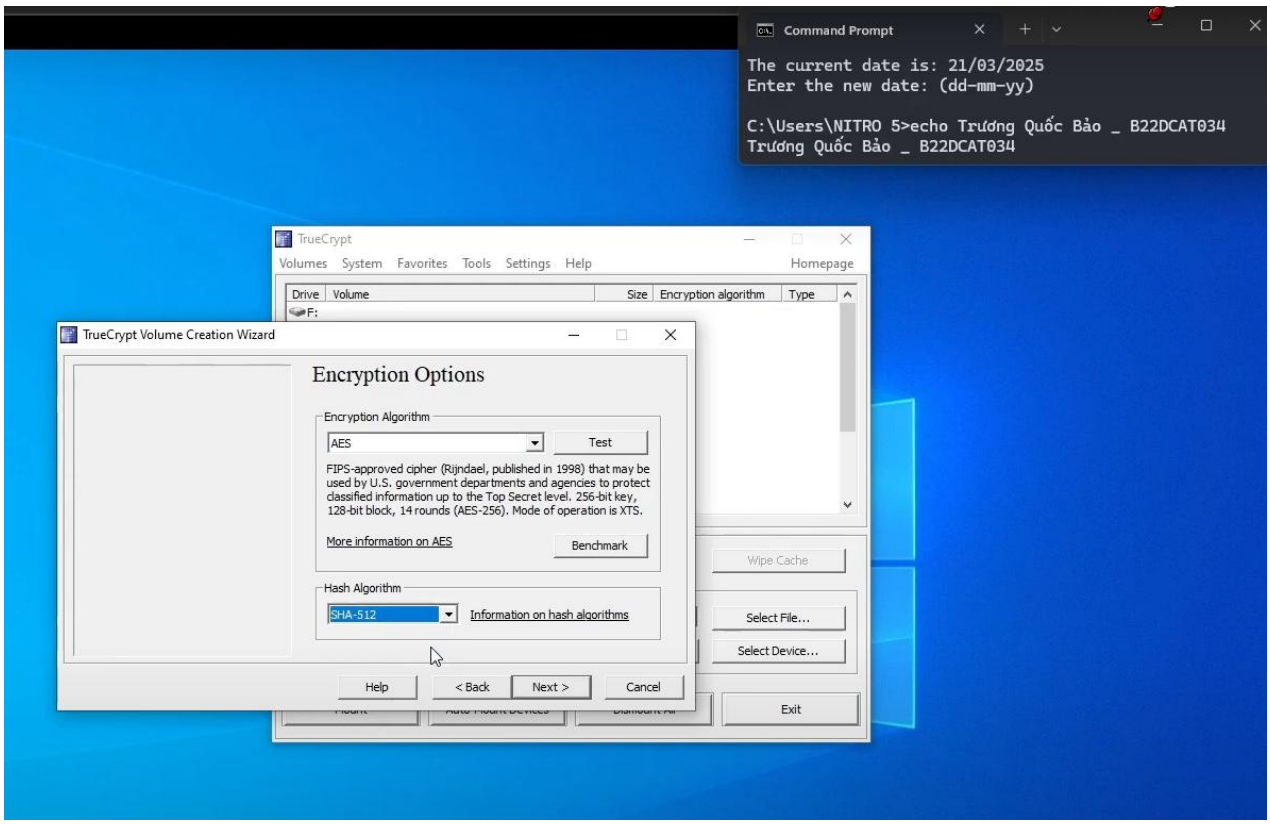
Ta chọn vị trí lưu file mã hóa, file này sẽ chứa dữ liệu của ổ đĩa mã hóa. Tuy nhiên ta sẽ không thể đọc được file này.



Hình 6 Chọn vị trí mã hóa

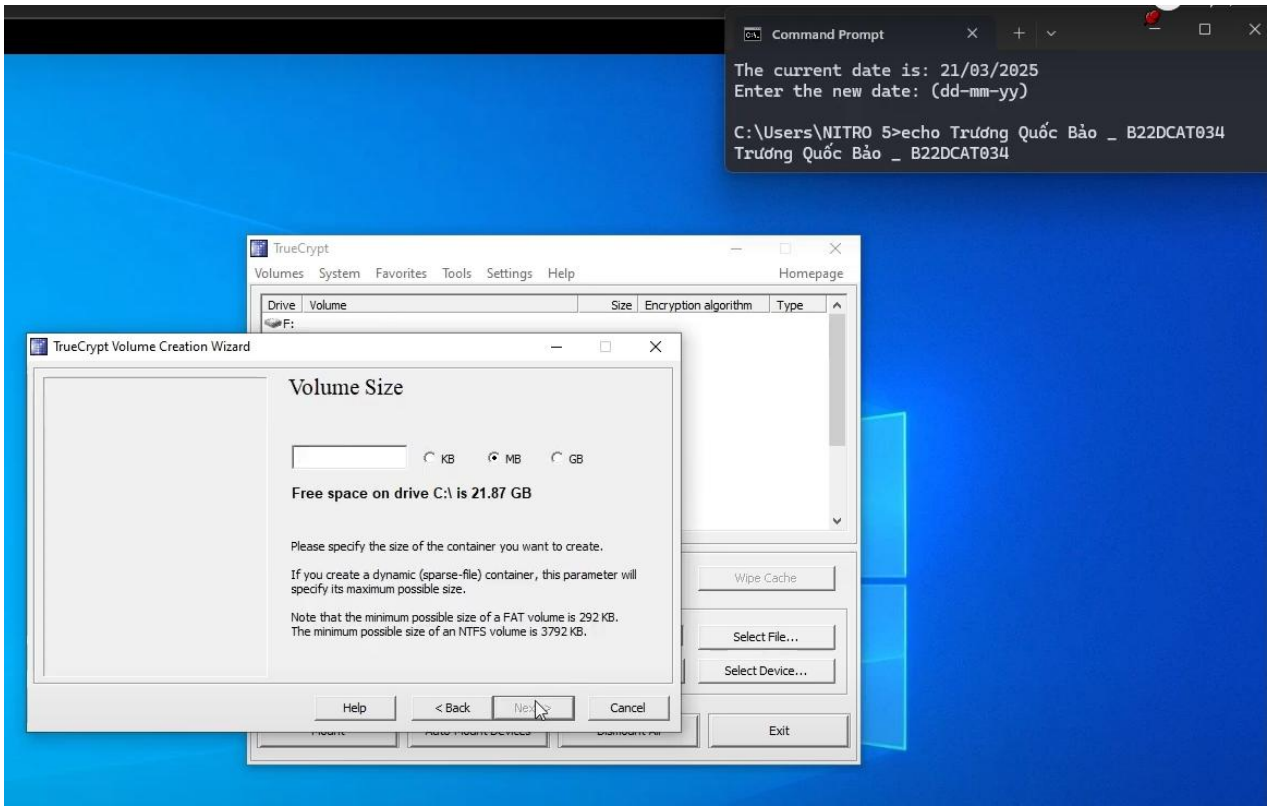
Chọn thuật toán mã hóa. TrueCrypt hỗ trợ nhiều thuật toán như AES, Serpent, Twofish, … và các thuật toán mã hóa hàm băm như SHA-512, Whirlpool, …

Có thể chọn “Test” để thử hoặc “Bechmark” để chấm điểm độ an toàn cho loại mã hóa này



Hình 7 Chọn thuật toán mã hóa

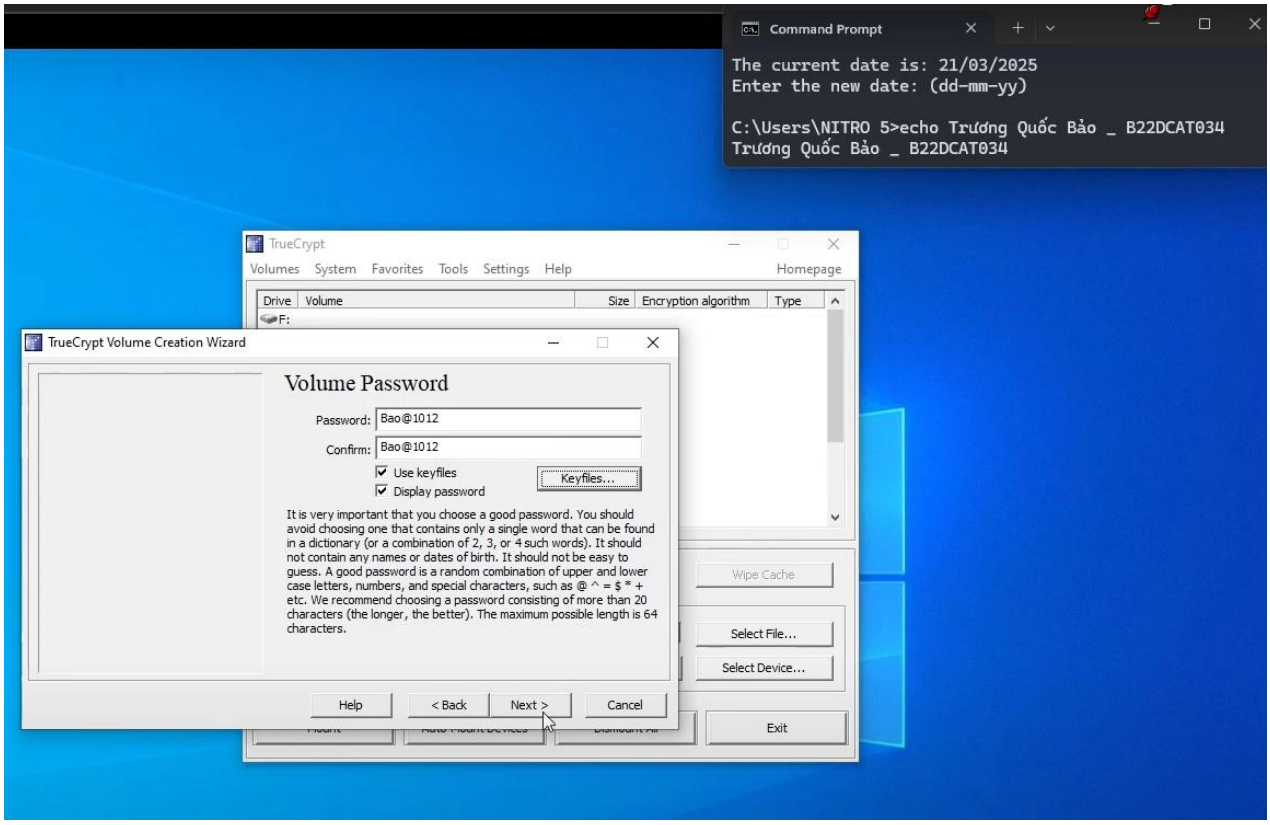
Chọn dung lượng để mã hóa ổ đĩa. Tùy thuộc vào nhu cầu lưu trữ dữ liệu, có thể chọn KB, MB, GB.



Hình 8 Chọn kích thước mã hóa

Đặt mật khẩu cho ổ đĩa. Mật khẩu sẽ được yêu cầu khi ta muốn Mount hoặc Dismount ổ đĩa mã hóa.

Có thể chọn “Use keyfiles” nếu đã có file chứa khóa.

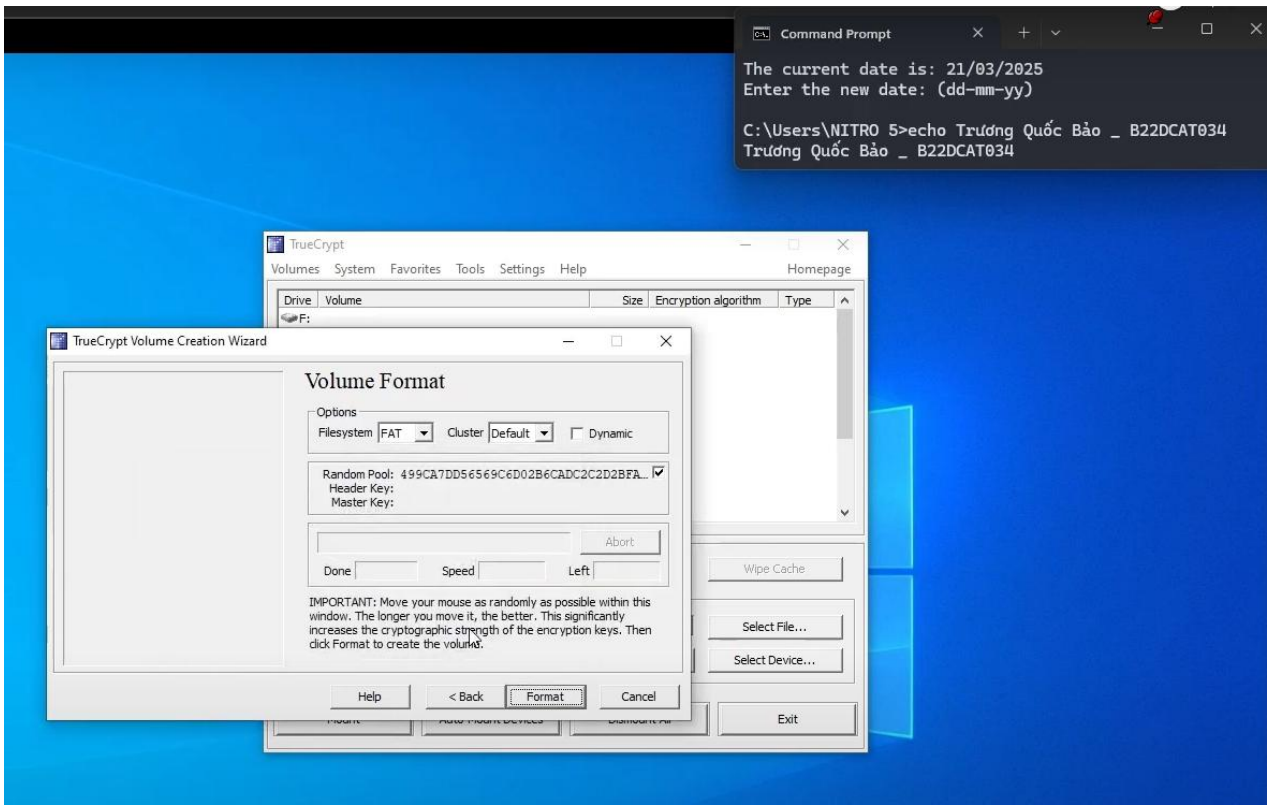


Hình 9 Đặt mật khẩu mã hóa

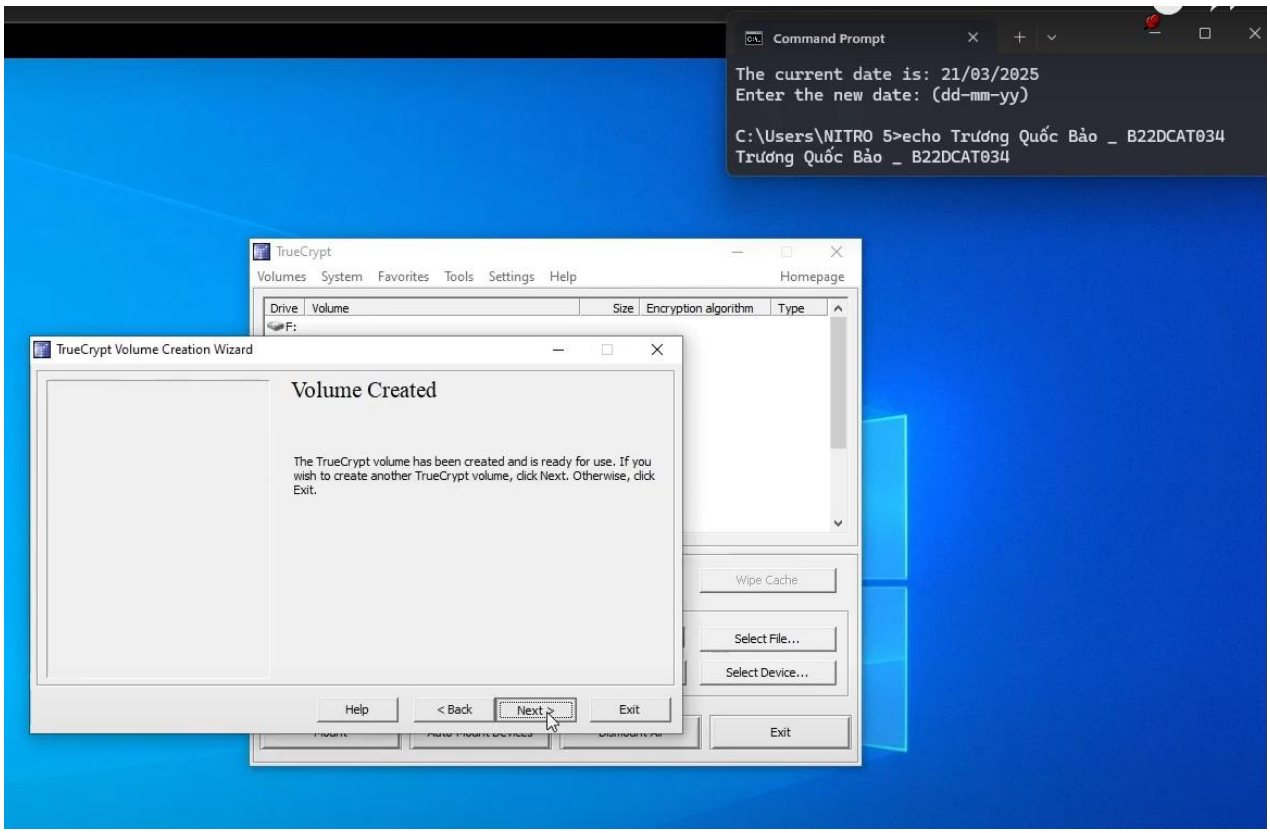
Chọn hệ thống lưu trữ cho ổ đĩa.

Công cụ sẽ tự động mã hóa đĩa và hiện khóa tương ứng.

Nhấn “Format” để hoàn thành tạo ổ đĩa.

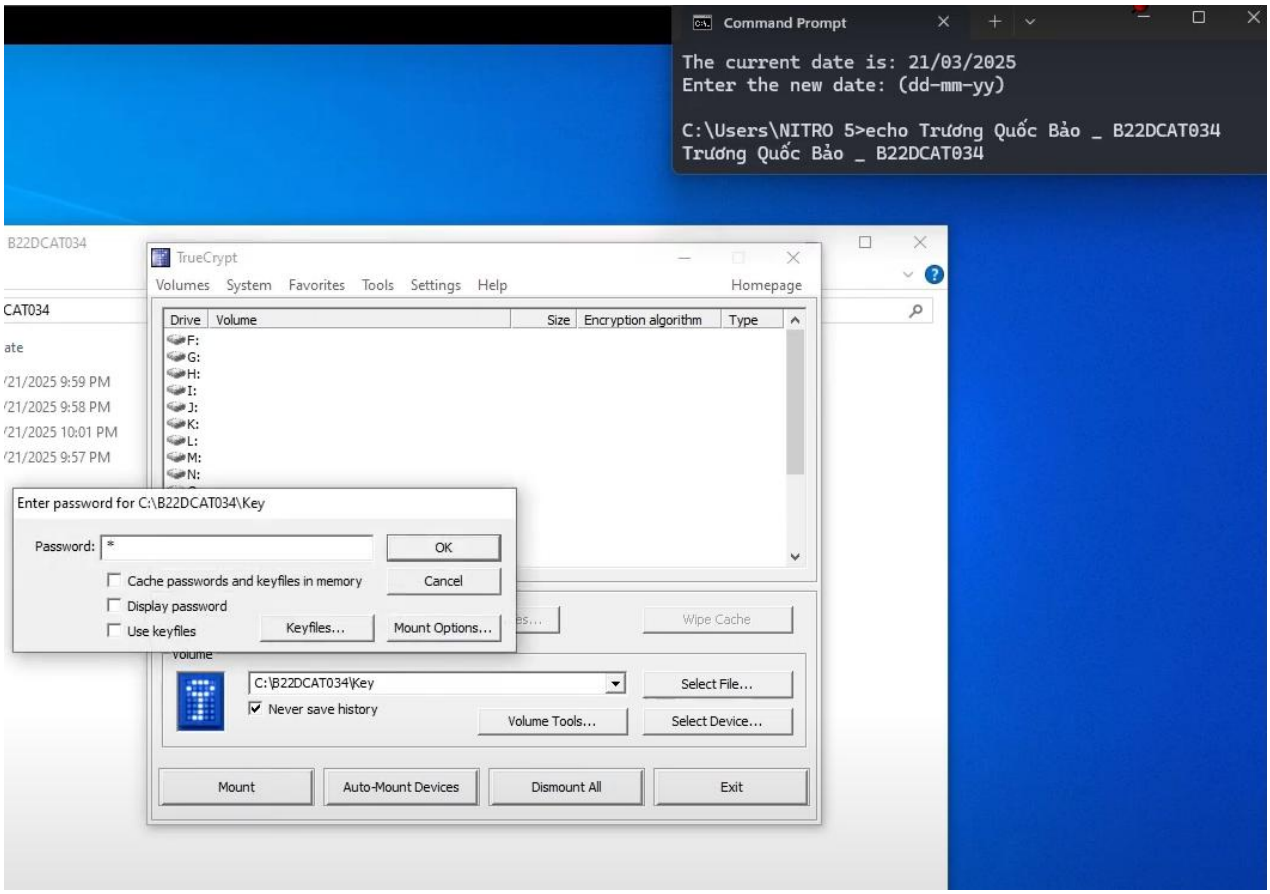


Hình 10 Chọn format cho ổ đĩa



Hình 11 Tạo ổ đĩa thành công

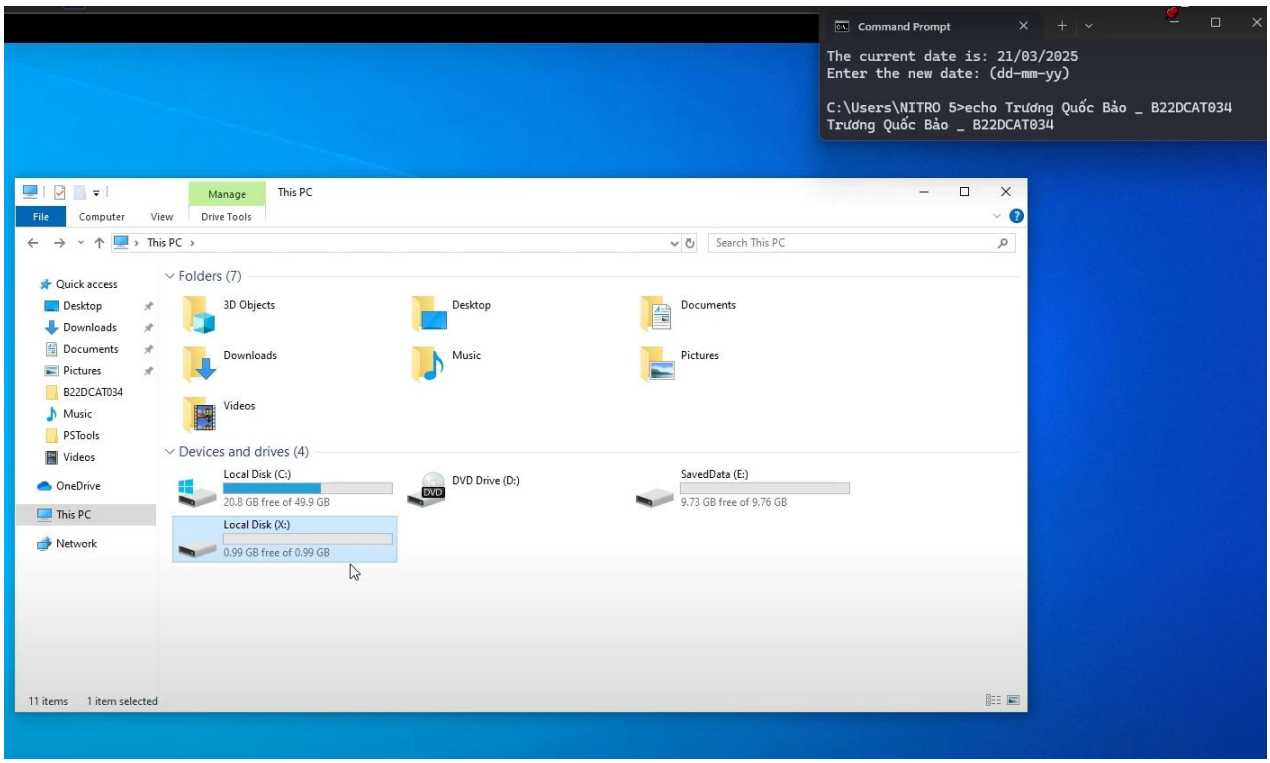
Để hiện ổ đĩa, ta chọn Select File, đường dẫn sẽ chỉ tới vị trí ta đã lưu file mã hóa ổ đĩa trước đó. Nhập mật khẩu hoặc sử dụng file khóa và nhấn Mount.



Hình 12 Nhập mật khẩu để mount ổ đĩa

Giao diện ở File Explorer đã hiện ổ đĩa mã hóa ta tạo trước đó.

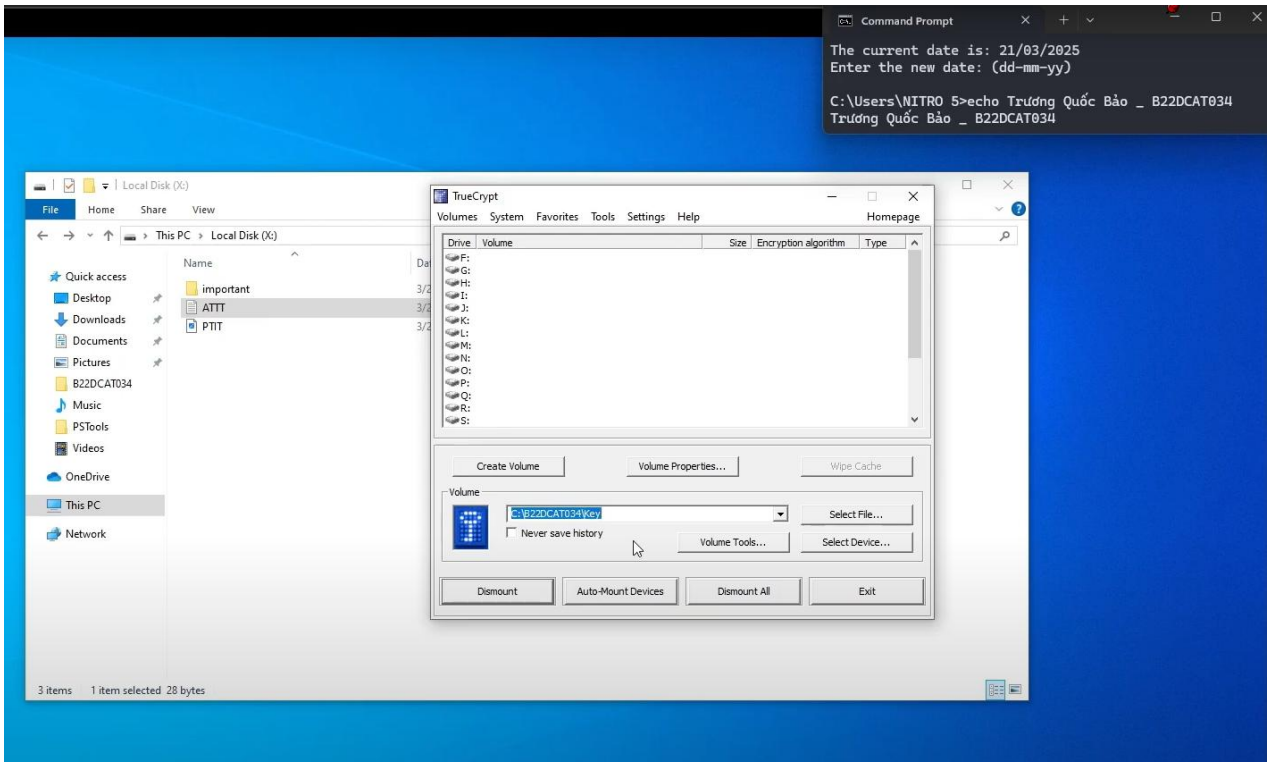
Có thể truy cập tùy ý, và lưu trữ dữ liệu trong này.



Hình 13 Ổ đĩa mã hóa xuất hiện

Ta di chuyển một số file cần lưu trữ vào ổ đĩa mã hóa.

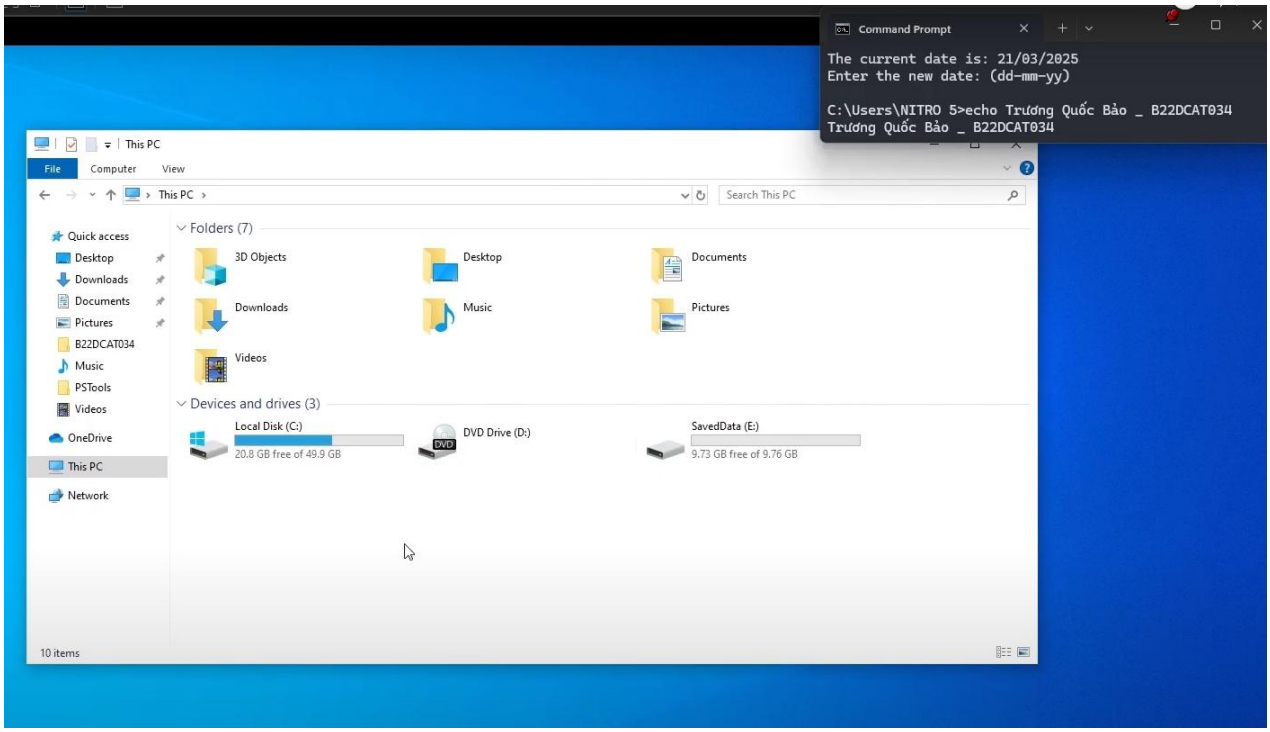
Chọn Dismount để khóa ổ đĩa.



Hình 14 Dismount ổ đĩa mã hóa

Ổ đĩa đã khóa, biến mất khỏi File Explorer.

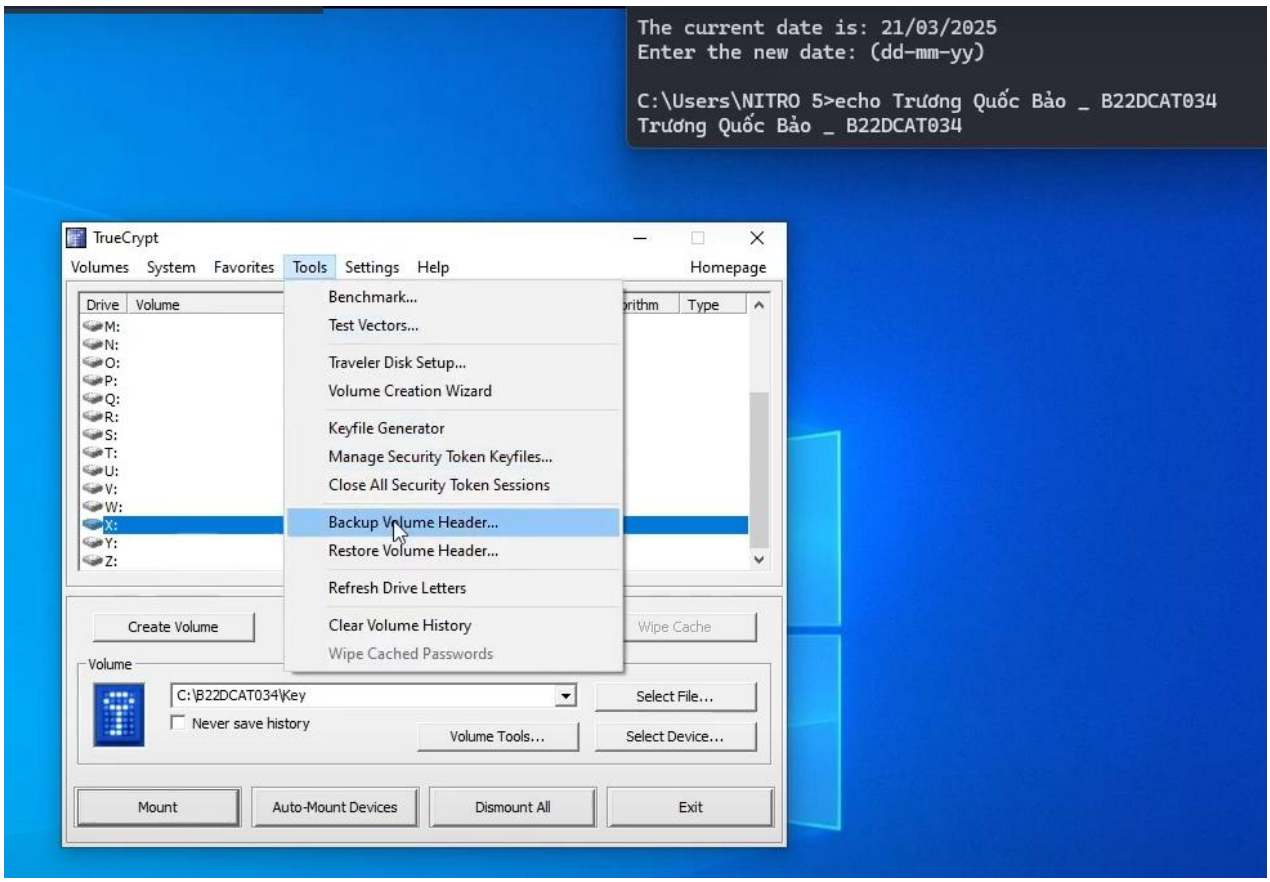
Khi cần mở lại, ta chỉ cần chọn lại vị trí lưu file mã hóa và Mount.



Hình 15 Ổ đĩa mã hóa biến mất

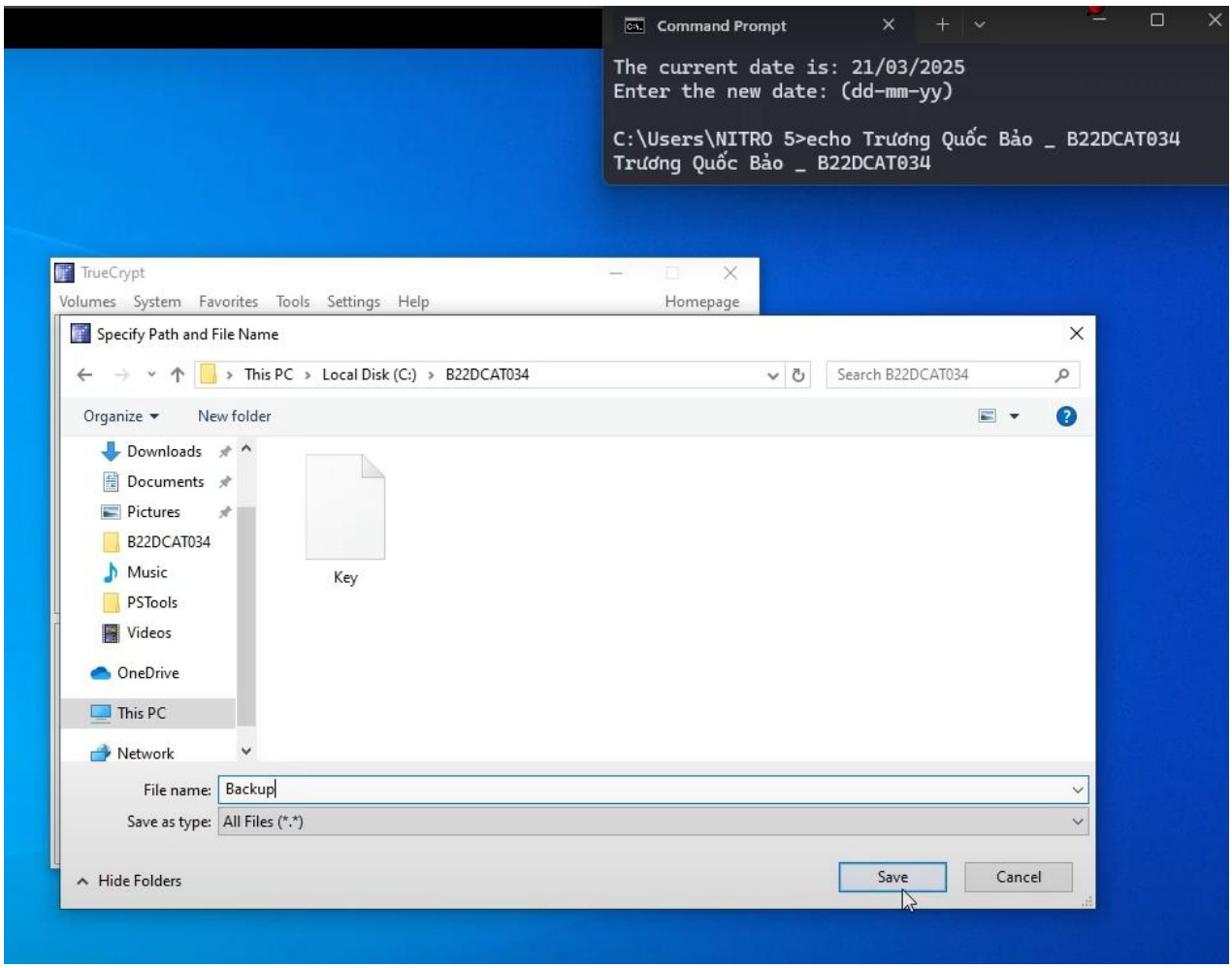
2.2.3 Sao lưu ổ đĩa

Để tạo ổ đĩa sao lưu. Trên thanh làm việc, chọn Tools, chọn Backup Volume Header.

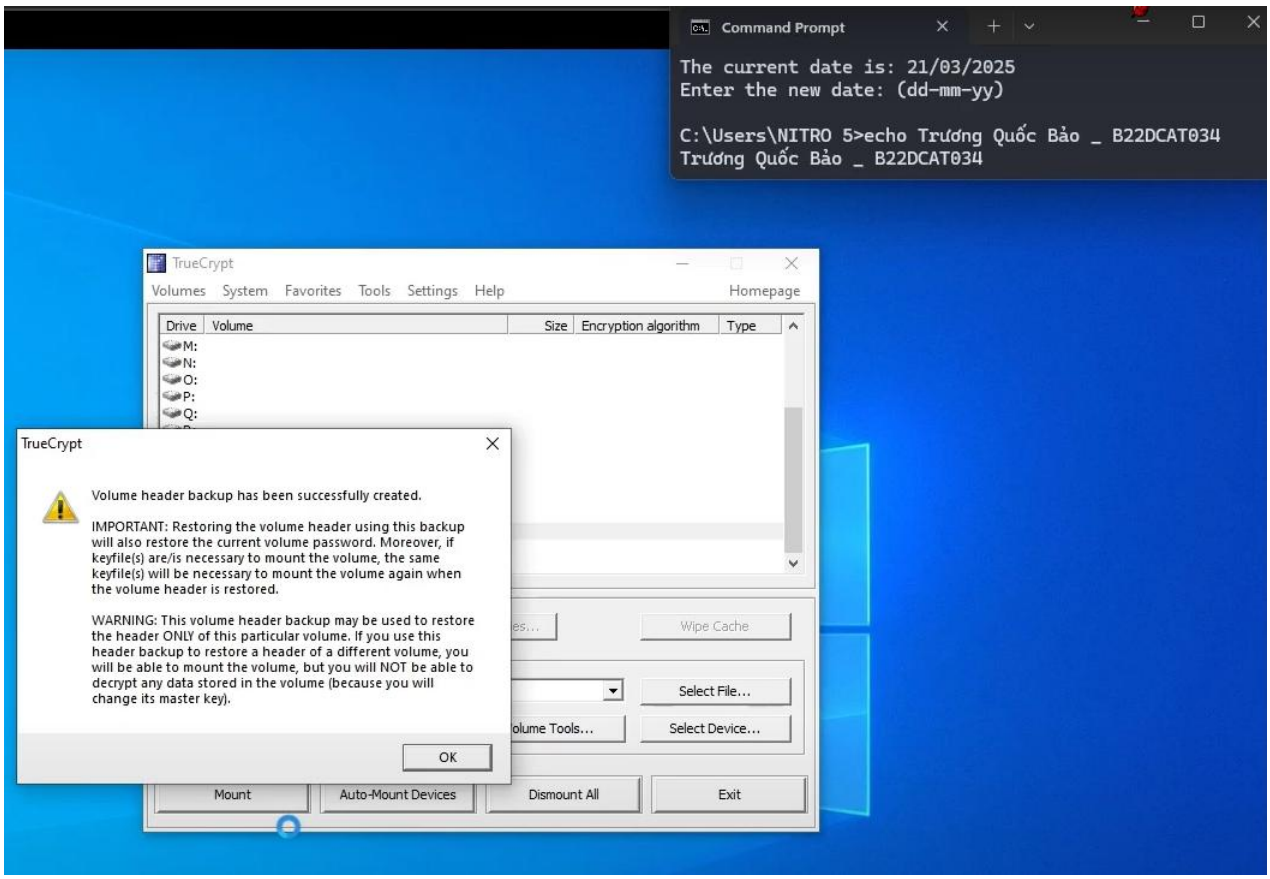


Hình 16 Tạo sao lưu cho ổ đĩa

Công cụ sẽ tạo ra một file dữ liệu backup cho file mã hóa ổ đĩa ta tạo trước đó. Chọn vị trí để lưu trữ.



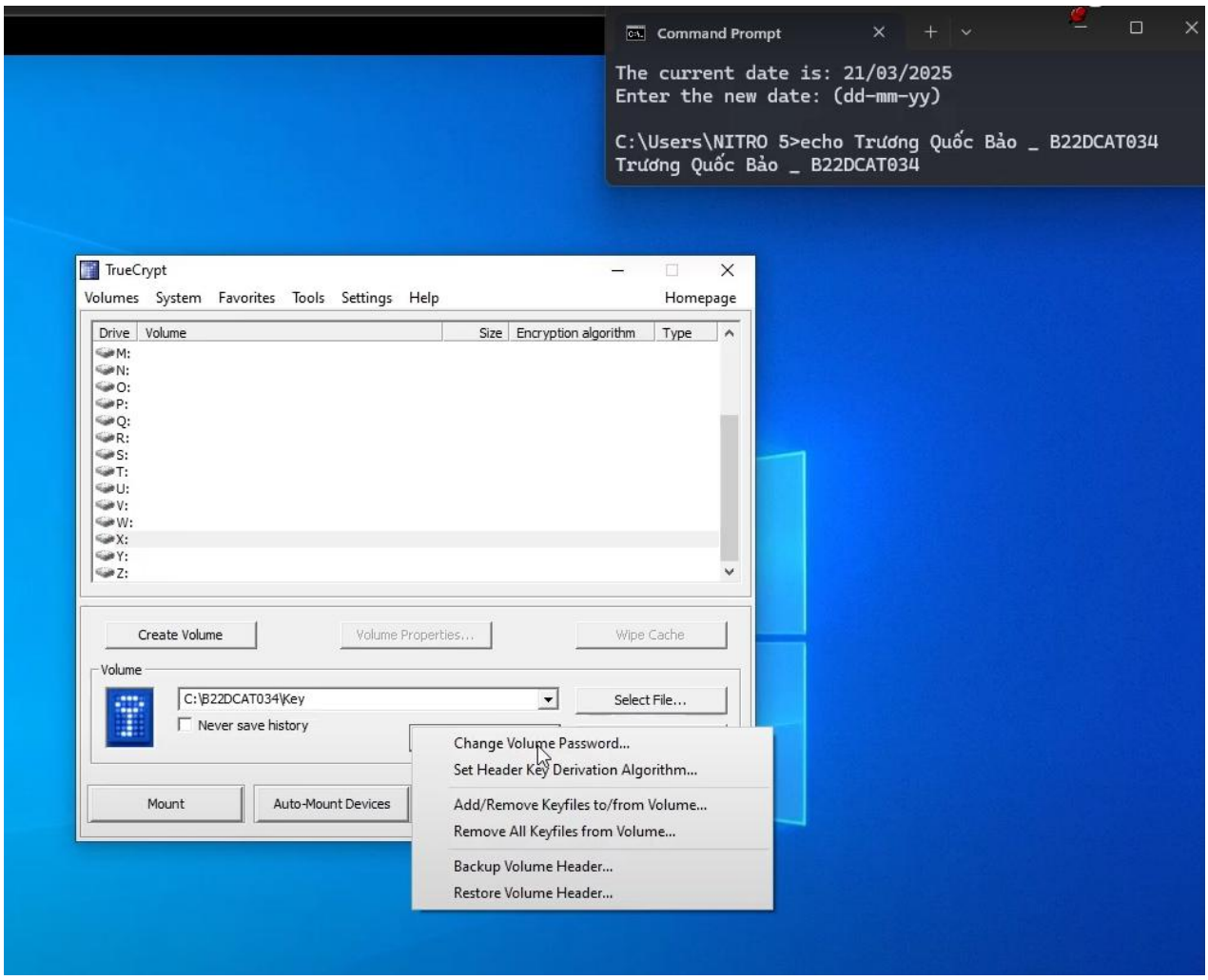
Hình 17 Chọn vị trí lưu sao lưu



Hình 18 Sao lưu thành công

Trong trường hợp file mã hóa gốc bị hỏng, mất hoặc không thể mở, ta có thể lựa chọn file backup này để sử dụng.

Chọn “Volume Tools”, chọn “Restore Volume Header” để tiến hành khôi phục lại.

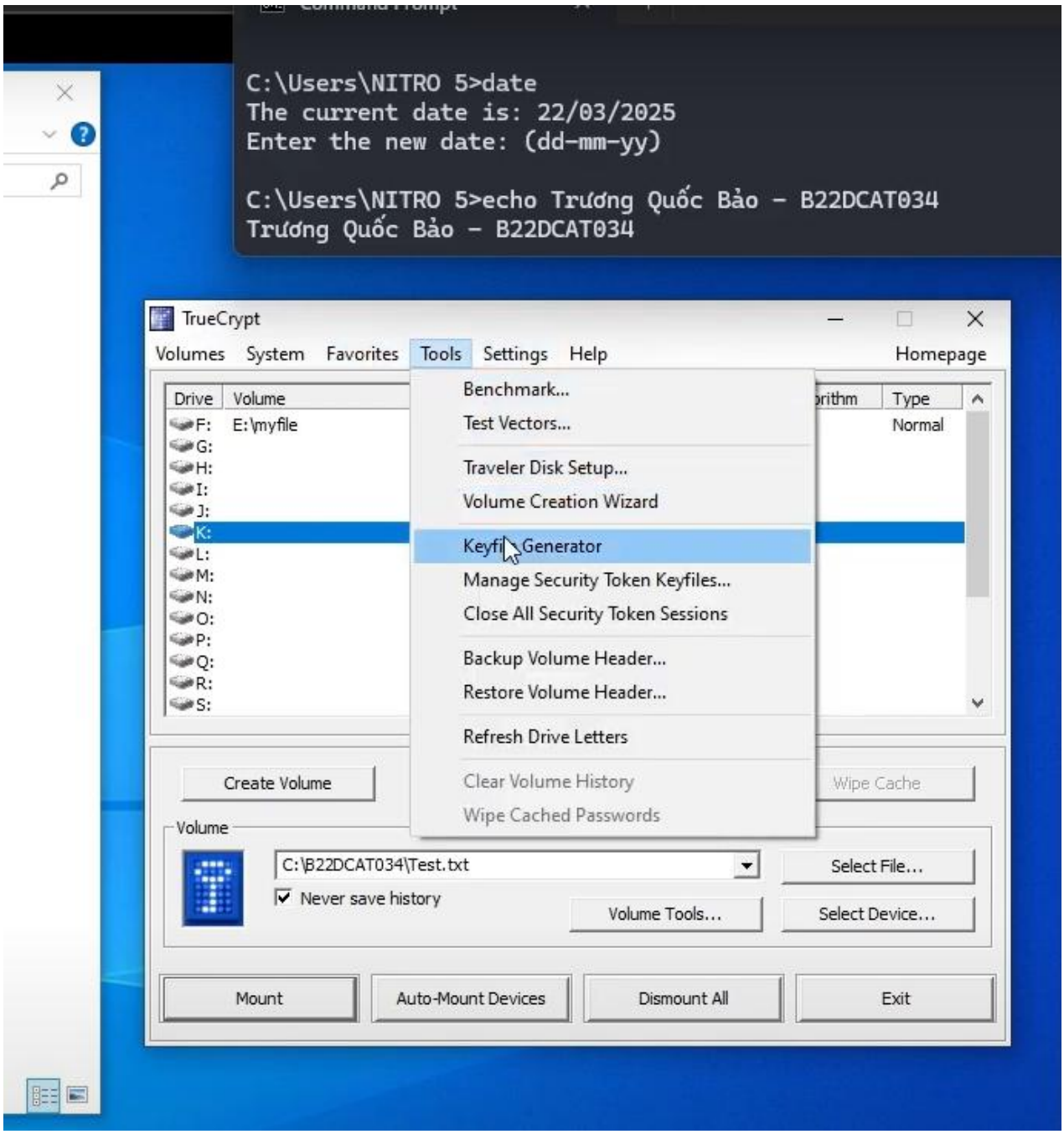


Hình 19 Khôi phục ổ đĩa nếu cần

2.2.4 Tạo khóa

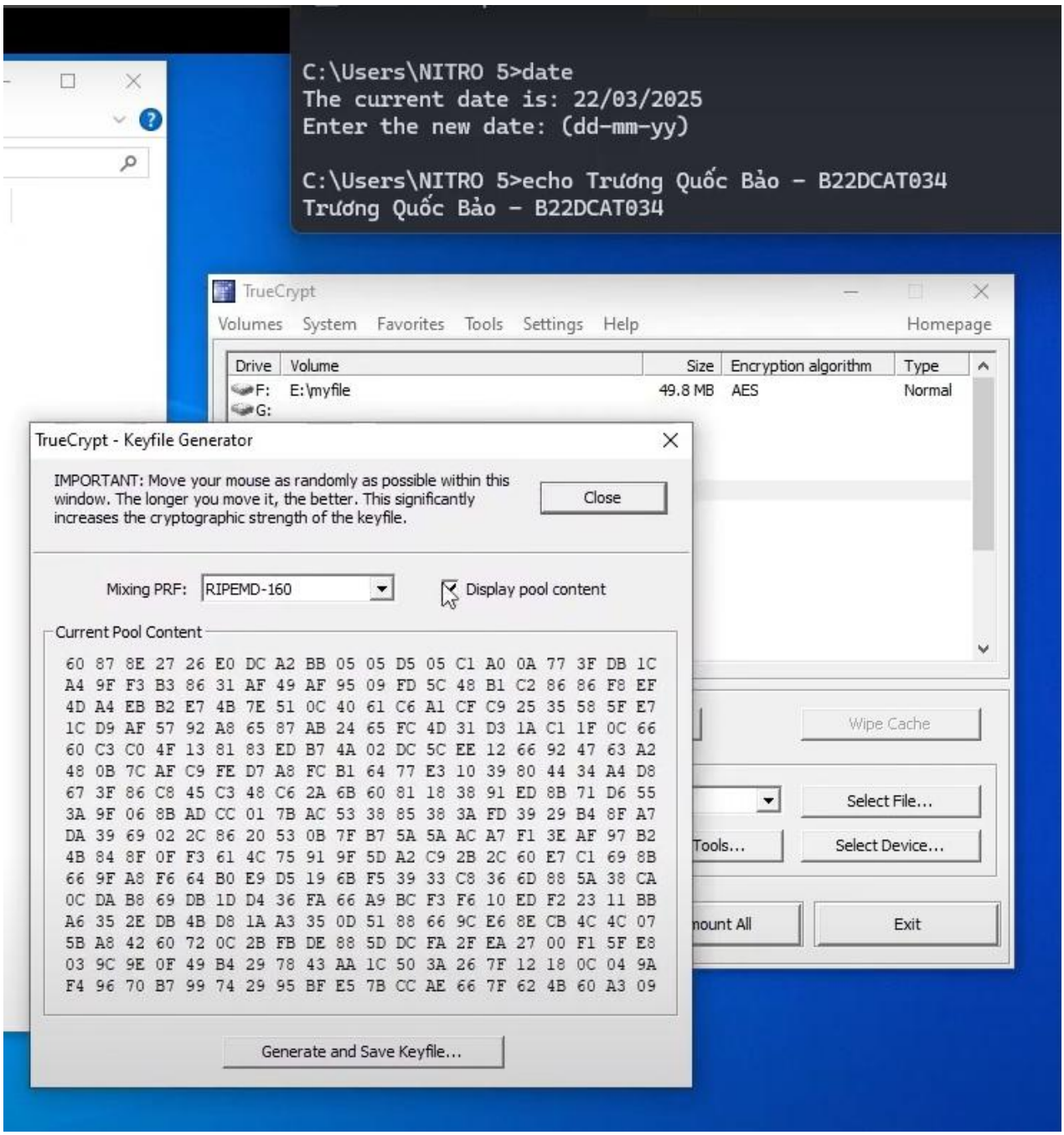
Để tạo file chứa khóa mã hóa, trên thanh làm việc, chọn Tools, chọn Keyfile Generator.

File khóa này sẽ được sử dụng thay thế mật khẩu, đảm bảo tránh việc bị tấn công dò quét mật khẩu (Brute-force).



Hình 20 Tạo file khóa

Chọn thuật toán mã hóa, vị trí lưu để hoàn tất việc tạo file khóa.



Hình 21 Tạo file khóa thành công

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.