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:

B22DCAT199 Đỗ Duy Nam

Giảng viên hướng dẫn: TS.Đinh Trường 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 Các công cụ TrueCrypt

TrueCrypt là một phần mềm mã nguồn mở (open-source) dùng để mã hóa dữ liệu, được phát triển từ năm 2004 và ngừng cập nhật vào năm 2014. Nó cho phép người dùng tạo các ổ đĩa ảo được mã hóa (encrypted virtual disks) hoặc mã hóa toàn bộ phân vùng/ổ cứng để bảo vệ dữ liệu nhạy cảm.

a) Nguyên lý hoạt động

- Mã hóa thời gian thực (On-the-fly Encryption): TrueCrypt mã hóa và giải mã dữ liệu ngay khi dữ liệu được ghi hoặc đọc, mà không cần người dùng can thiệp thủ công. Điều này đảm bảo tính minh bạch và tiện lợi.
- Container mã hóa: TrueCrypt tạo ra các "tập tin container" (file container) hoạt động như ổ đĩa ảo. Khi được "mount" (gắn kết) với mật khẩu đúng, container này xuất hiện như một ổ đĩa thông thường.
- Mã hóa toàn bộ hệ thống: Có thể mã hóa toàn bộ ổ cứng, bao gồm cả hệ điều hành, để bảo vệ dữ liệu ngay từ khi khởi động.

b) Các công cụ chính

- Tạo ổ đĩa ảo (Volume Creation): Người dùng có thể tạo một tập tin container (encrypted volume) với dung lượng tùy chọn, sử dụng các thuật toán mã hóa như AES, Serpent, hoặc Twofish.
- Mã hóa phân vùng/ổ cứng: Cho phép mã hóa toàn bộ phân vùng hoặc thiết bị lưu trữ (USB, HDD), với tùy chọn mã hóa hệ thống (system partition).
- Hidden Volume (Ổ đĩa ẩn): TrueCrypt hỗ trợ tạo ổ đĩa ẩn bên trong một container mã hóa khác, giúp bảo vệ dữ liệu nhạy cảm ngay cả khi bị ép buộc tiết lộ mật khẩu chính (plausible deniability).
- Keyfiles: Ngoài mật khẩu, TrueCrypt cho phép sử dụng tệp khóa (keyfile) để tăng cường bảo mật.
- Mount/Dismount: Công cụ gắn kết (mount) và tháo gỡ (dismount) các volume mã hóa, yêu cầu nhập mật khẩu hoặc keyfile để truy cập.

c) Thuật toán mã hóa

- TrueCrypt hỗ trợ nhiều thuật toán mã hóa mạnh mẽ:
    - AES (Advanced Encryption Standard): Chuẩn mã hóa 256-bit phổ biến nhất.
    - Serpent và Twofish: Các thuật toán thay thế với độ bảo mật cao.
    - Kết hợp (Cascade Encryption): Có thể dùng nhiều thuật toán cùng lúc (ví dụ: AES-Twofish-Serpent) để tăng cường bảo mật.
- Hàm băm (hash): SHA-512, RIPEMD-160, Whirlpool để tạo khóa mã hóa từ mật khẩu.

d) Tính năng bảo mật

- Plausible Deniability: Ổ đĩa ẩn và thiết kế không để lại dấu vết rõ ràng về sự tồn tại của dữ liệu mã hóa.
- Không lưu trữ dữ liệu chưa mã hóa: Dữ liệu chỉ tồn tại dưới dạng mã hóa trên ổ đĩa, ngay cả trong RAM cũng được bảo vệ (trừ khi đang truy cập).

e) Hạn chế và di sản

- TrueCrypt ngừng phát triển vào năm 2014 với thông báo gây tranh cãi rằng nó "không còn an toàn". Tuy nhiên, mã nguồn đã được kiểm tra (audit) vào năm 2015 và không tìm thấy lỗ hổng nghiêm trọng.
- Các dự án kế thừa như VeraCrypt (cải tiến từ TrueCrypt) đã khắc phục một số hạn chế và tiếp tục phát triển.

1.2.2 Cách thức hoặc phương pháp công cụ TrueCrypt áp dụng để mã hóa file hoặc thư mục

TrueCrypt sử dụng một quy trình mã hóa mạnh mẽ và linh hoạt để bảo vệ file hoặc thư mục thông qua việc tạo ra các volume mã hóa (encrypted volumes).

❖ Khái niệm cơ bản

TrueCrypt không mã hóa trực tiếp từng file hoặc thư mục riêng lẻ như một số phần mềm nén/mã hóa (ví dụ: WinRAR). Thay vào đó, nó tạo ra một container mã hóa (file container) hoặc mã hóa toàn bộ phân vùng, nơi người dùng có thể lưu trữ file/thư mục. Container này hoạt động như một ổ đĩa ảo được mã hóa, chỉ có thể truy cập khi được "mount" (gắn kết) với mật khẩu đúng.

❖ Quy trình mã hóa file hoặc thư mục

Bước 1: Tạo volume mã hóa

- Người dùng sử dụng TrueCrypt Volume Creation Wizard để tạo một tập tin container (ví dụ: mydata.tc) với dung lượng cố định hoặc động (dynamic).
- Container này là một tệp đơn, nhưng bên trong nó hoạt động như một hệ thống tệp (file system) độc lập (hỗ trợ FAT hoặc NTFS).

Bước 2: Chọn thuật toán mã hóa

- TrueCrypt cho phép chọn một hoặc nhiều thuật toán mã hóa đối xứng:
    - AES: Chuẩn mã hóa 256-bit, nhanh và được sử dụng rộng rãi.
    - Serpent: Độ bảo mật cao, chậm hơn AES.
    - Twofish: Linh hoạt và an toàn.
    - Có thể kết hợp nhiều thuật toán (cascade encryption), ví dụ: AES-Twofish hoặc AES-Twofish-Serpent, để tăng cường bảo mật.
- Hàm băm (hash function) như SHA-512 hoặc RIPEMD-160 được dùng để tạo khóa mã hóa từ mật khẩu người dùng.

Bước 3: Tạo khóa mã hóa

- TrueCrypt kết hợp mật khẩu người dùng (và keyfile nếu có) với một giá trị ngẫu nhiên gọi là salt (muối), sau đó sử dụng hàm băm để sinh ra khóa mã hóa chính (master key).
- Master key này được lưu trong header của volume (được mã hóa riêng) và không bao giờ lưu dưới dạng plaintext.

Bước 4: Mã hóa dữ liệu

- On-the-fly Encryption (OTFE): Dữ liệu được mã hóa ngay khi ghi vào volume và giải mã khi đọc ra, tất cả diễn ra trong thời gian thực.
- TrueCrypt chia volume thành các khối (block) nhỏ, mỗi khối được mã hóa bằng master key sử dụng chế độ mã hóa khối (block cipher mode):
    - XTS (XEX-based Tweaked-codebook mode with ciphertext Stealing): Là chế độ mặc định trong TrueCrypt, đảm bảo tính ngẫu nhiên và bảo mật cao, phù hợp cho mã hóa ổ đĩa.
- Toàn bộ dữ liệu trong volume, bao gồm metadata của hệ thống tệp, đều được mã hóa.

Bước 5: Lưu trữ và truy cập

- Sau khi container được tạo, người dùng "mount" nó bằng TrueCrypt, nhập mật khẩu (và keyfile nếu có). Container xuất hiện như một ổ đĩa (ví dụ: ổ Z: trên Windows).
- File/thư mục được sao chép vào ổ đĩa này sẽ tự động mã hóa. Khi "dismount" (tháo gỡ), dữ liệu trở lại trạng thái mã hóa hoàn toàn và không thể truy cập mà không có mật khẩu.

❖ Phương pháp cụ thể

- Mã hóa toàn bộ volume: Thay vì mã hóa từng file riêng lẻ, TrueCrypt mã hóa toàn bộ không gian của container hoặc phân vùng, kể cả phần không sử dụng (free space), để không để lại dấu vết về cấu trúc dữ liệu.

- Hidden Volume: TrueCrypt hỗ trợ tạo volume ẩn bên trong volume chính:
    - Volume chính (outer volume) và volume ẩn (hidden volume) dùng các mật khẩu khác nhau.
    - Nếu bị ép buộc tiết lộ mật khẩu, người dùng có thể cung cấp mật khẩu của volume chính mà không để lộ volume ẩn, tăng tính "plausible deniability".
- Header mã hóa: Mỗi volume có một header (thường 512 byte) chứa thông tin khóa và cấu hình, được mã hóa bằng mật khẩu người dùng. Nếu header bị hỏng, dữ liệu trong volume không thể giải mã.

❖ Cơ chế bảo vệ bổ sung

- Salt và Iteration: TrueCrypt sử dụng hàng nghìn vòng lặp (iteration) trong hàm băm (PBKDF2) để tăng độ khó cho các cuộc tấn công brute-force.
- Keyfile: Người dùng có thể thêm tệp khóa (keyfile) để làm phức tạp hơn quá trình giải mã, vì kẻ tấn công cần cả mật khẩu lẫn keyfile.
- Không lưu plaintext: Dữ liệu chưa mã hóa chỉ tồn tại tạm thời trong RAM khi volume được mount, và TrueCrypt có cơ chế xóa bộ nhớ cache để giảm nguy cơ rò rỉ.

1.3 Kết luận

Ở chương này đã mô tả về các công cụ TrueCrypt và cách thức, phương pháp công cụ TrueCrypt để áp dụng mã hóa file hoặc thư mục.

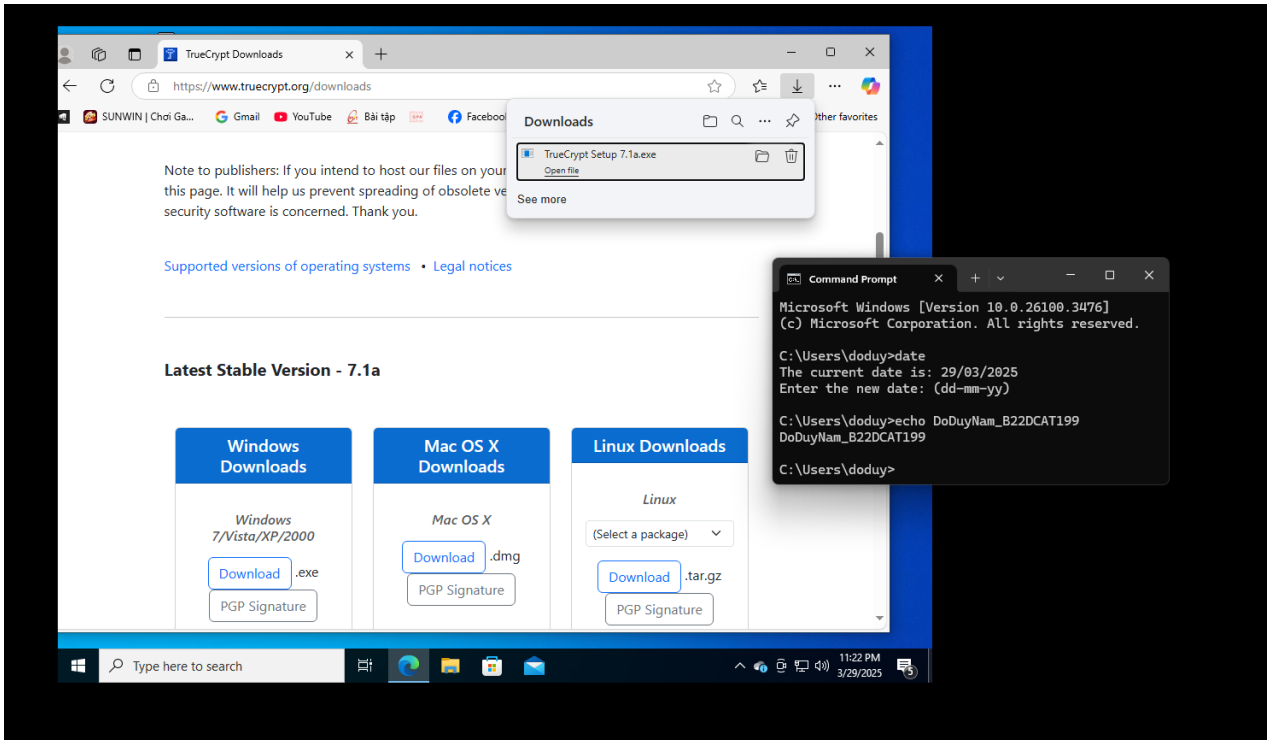
CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

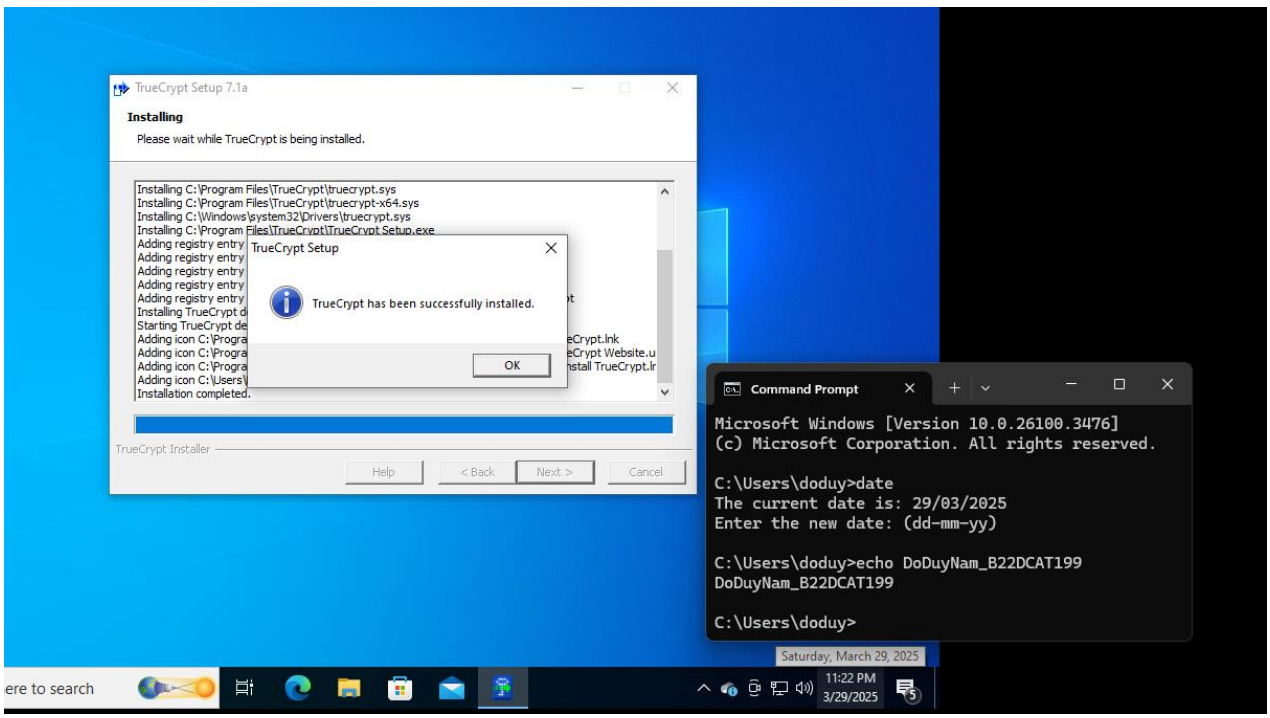
- Máy Windows để càu TrueCrypt.

2.2 Các bước thực hiện

- Tải phần mềm TrueCrypt về máy

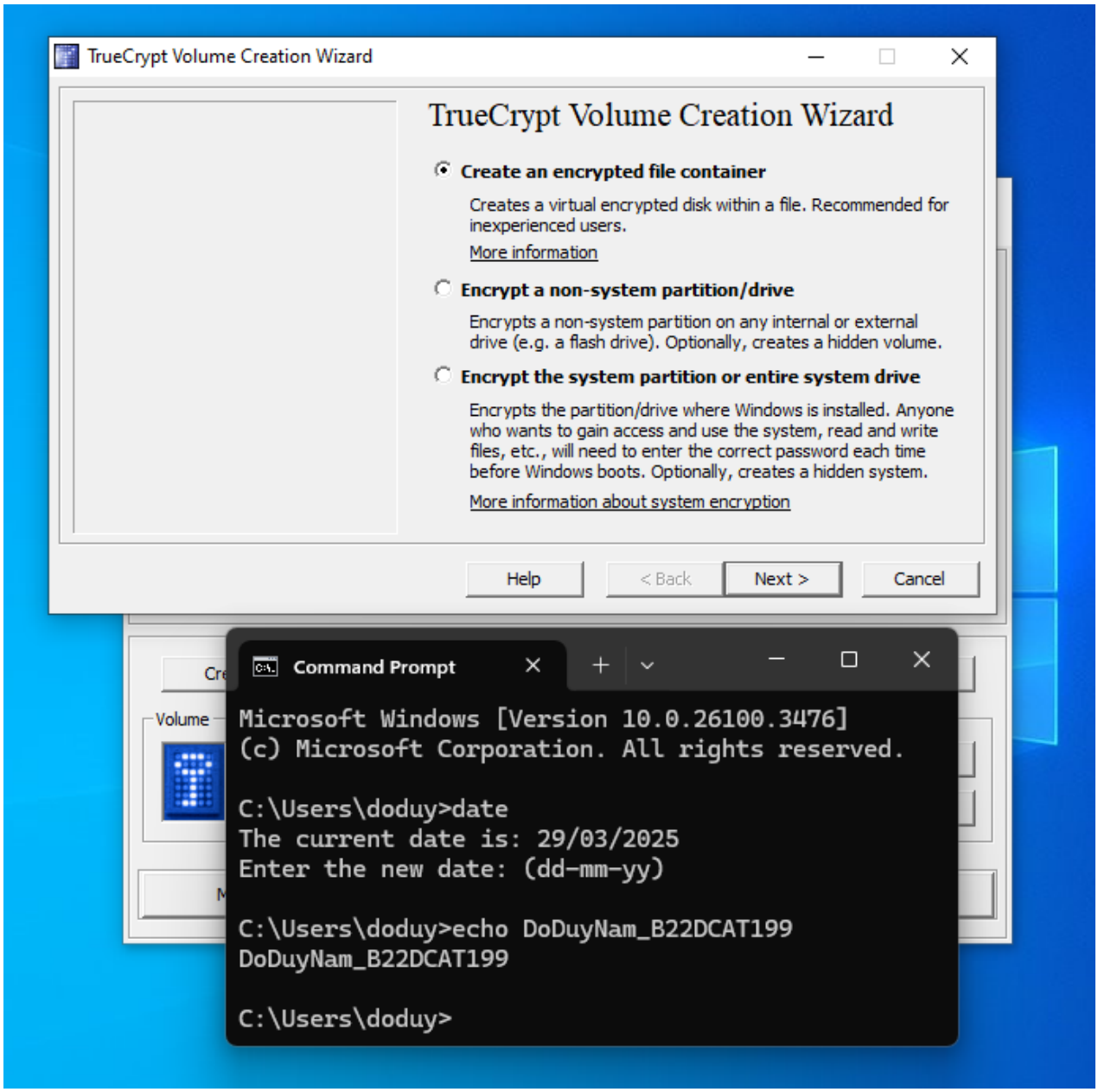


Hình 1 Tải TrueCrypt về máy Windows

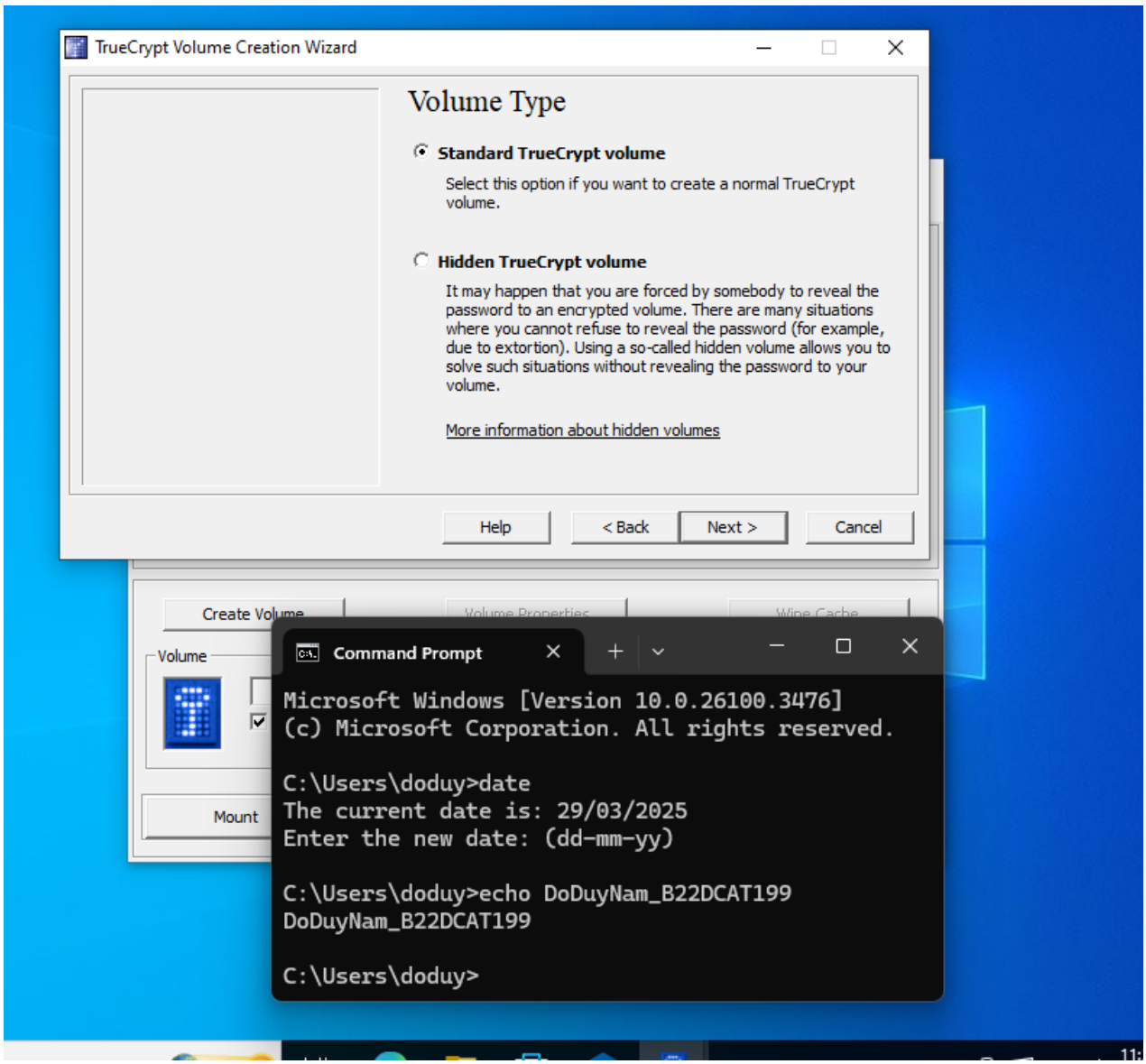


Hình 2 Cài đặt thành công phần mềm TrueCrypt trên máy Windows

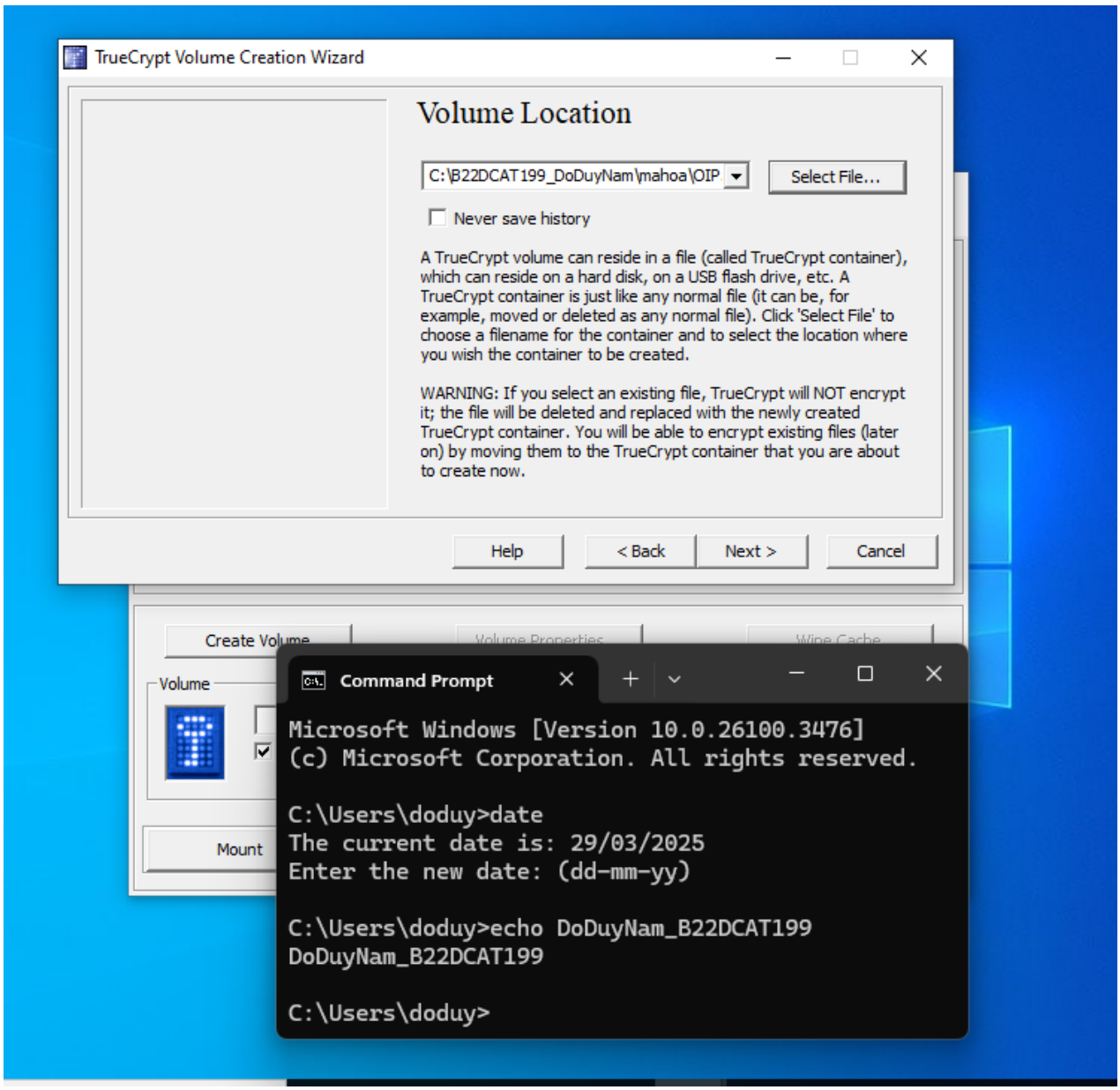
- Tạo 1 volume để mã hóa: Create Volume -> Create an encrypted file container



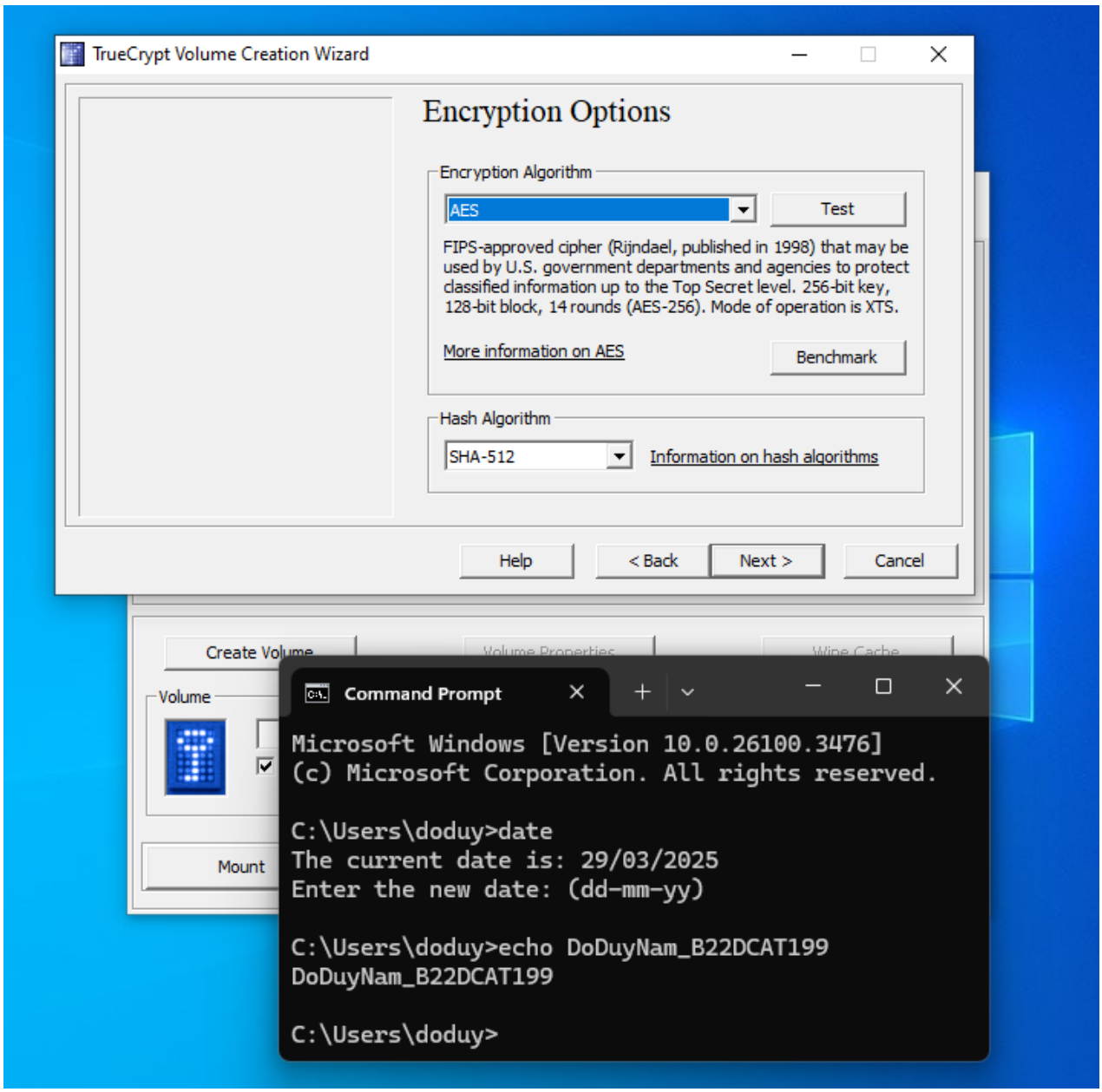
Hình 3 Tạo volume để mã hóa



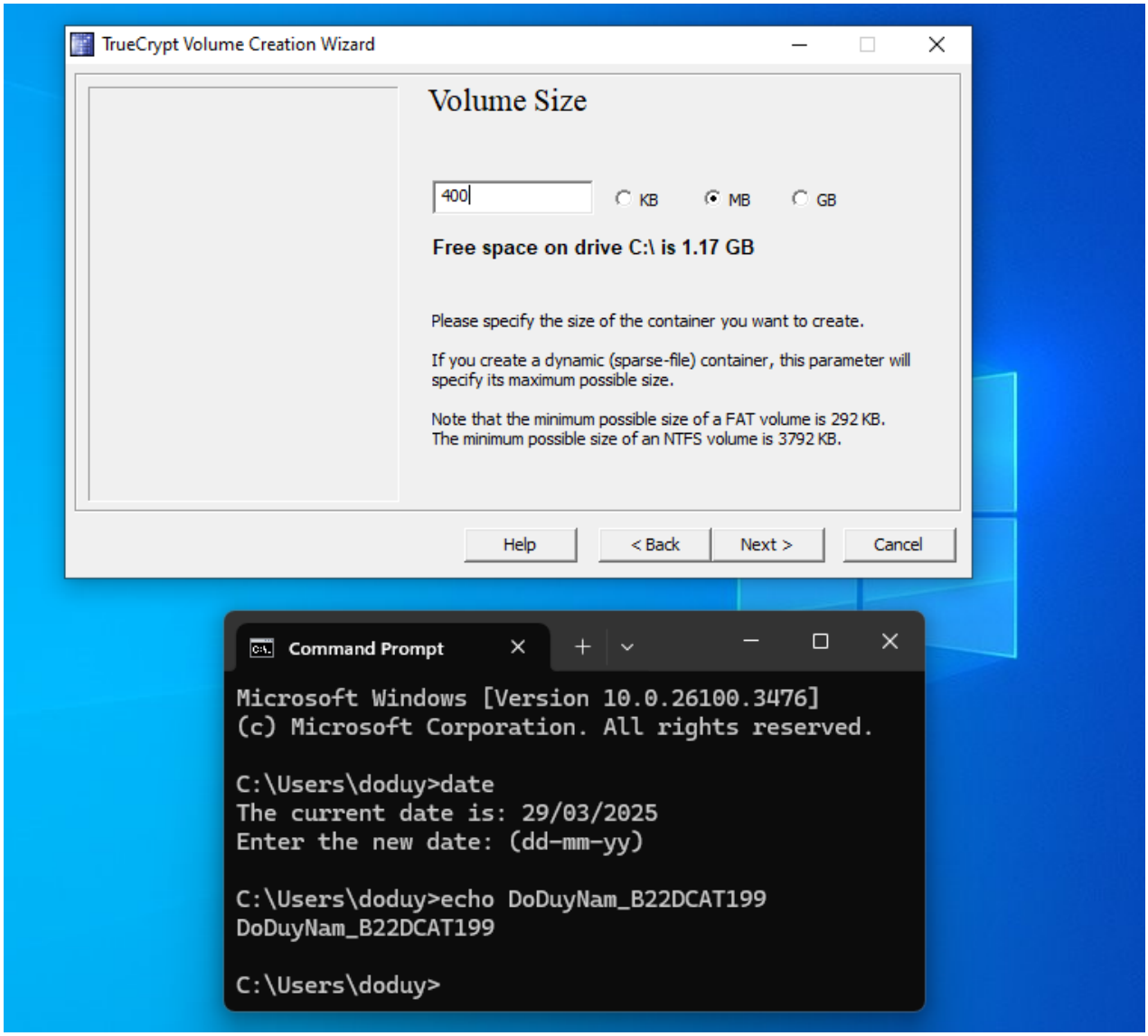
Hình 4 Chọn loại Volume



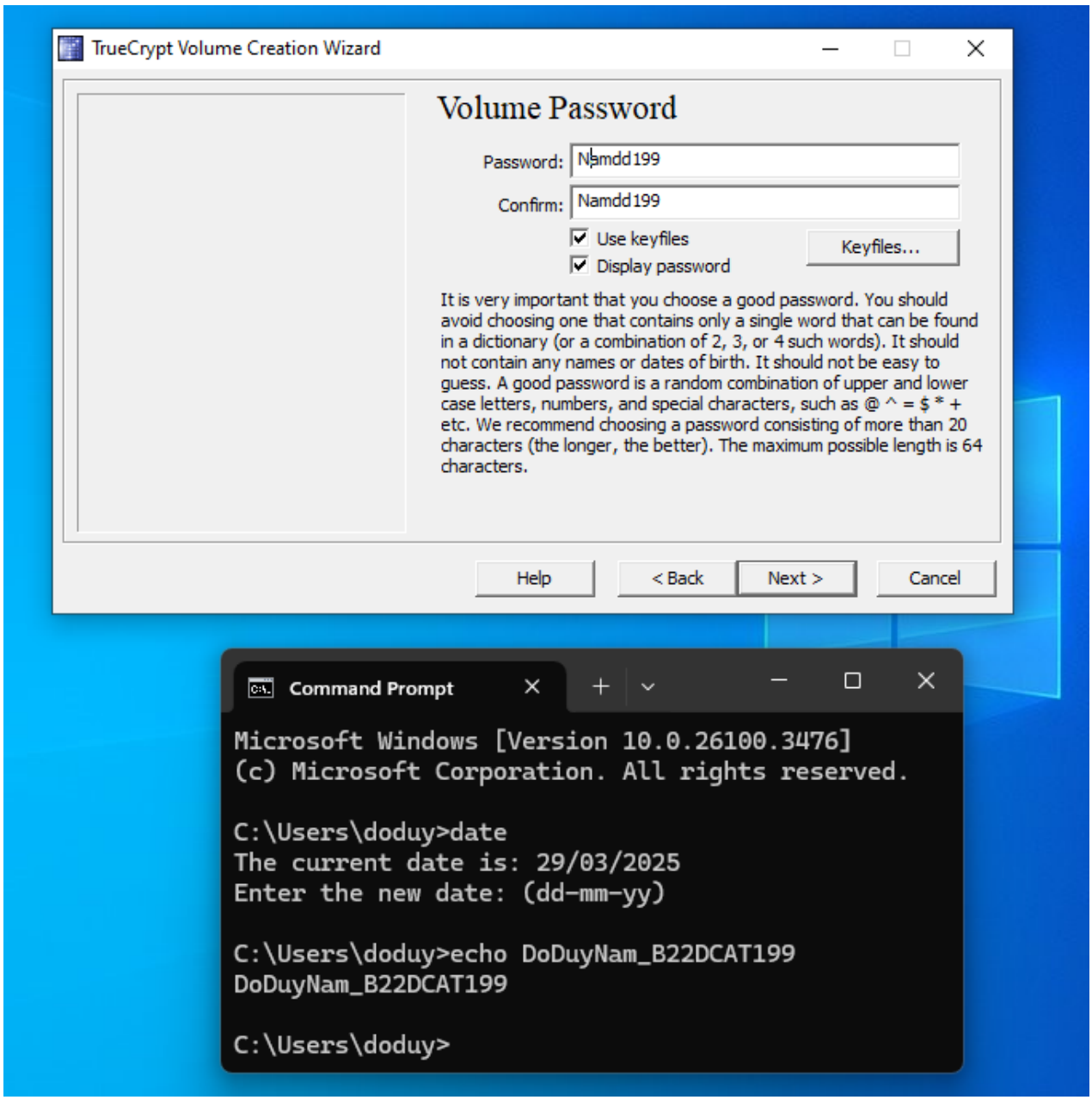
Hình 5 Chọn vị trí volume



Hình 6 Chọn thuật toán mã hóa

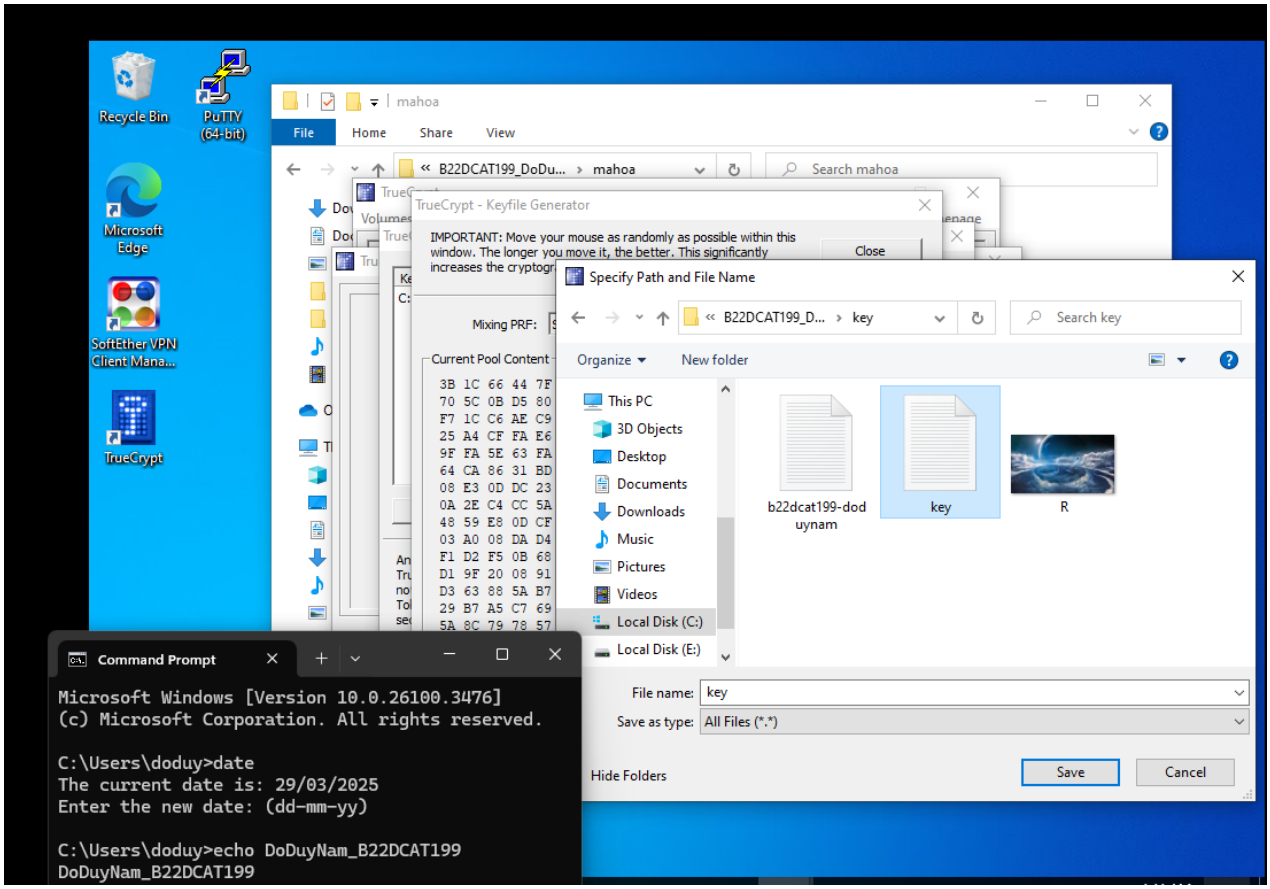


Hình 7 Chọn kích thước cấp cho Volume

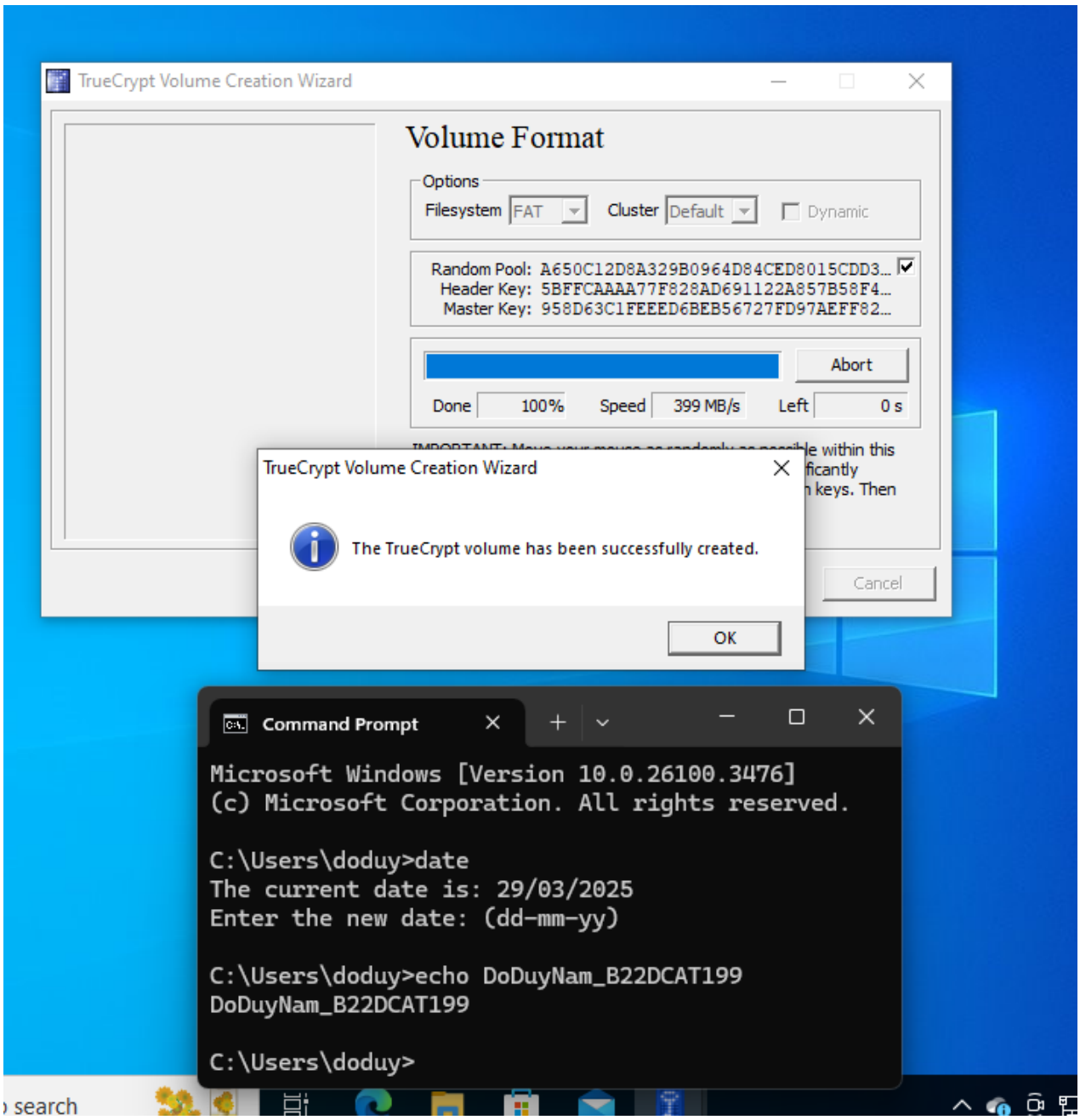


Hình 8 Nhập mật khẩu để mã hóa Volume

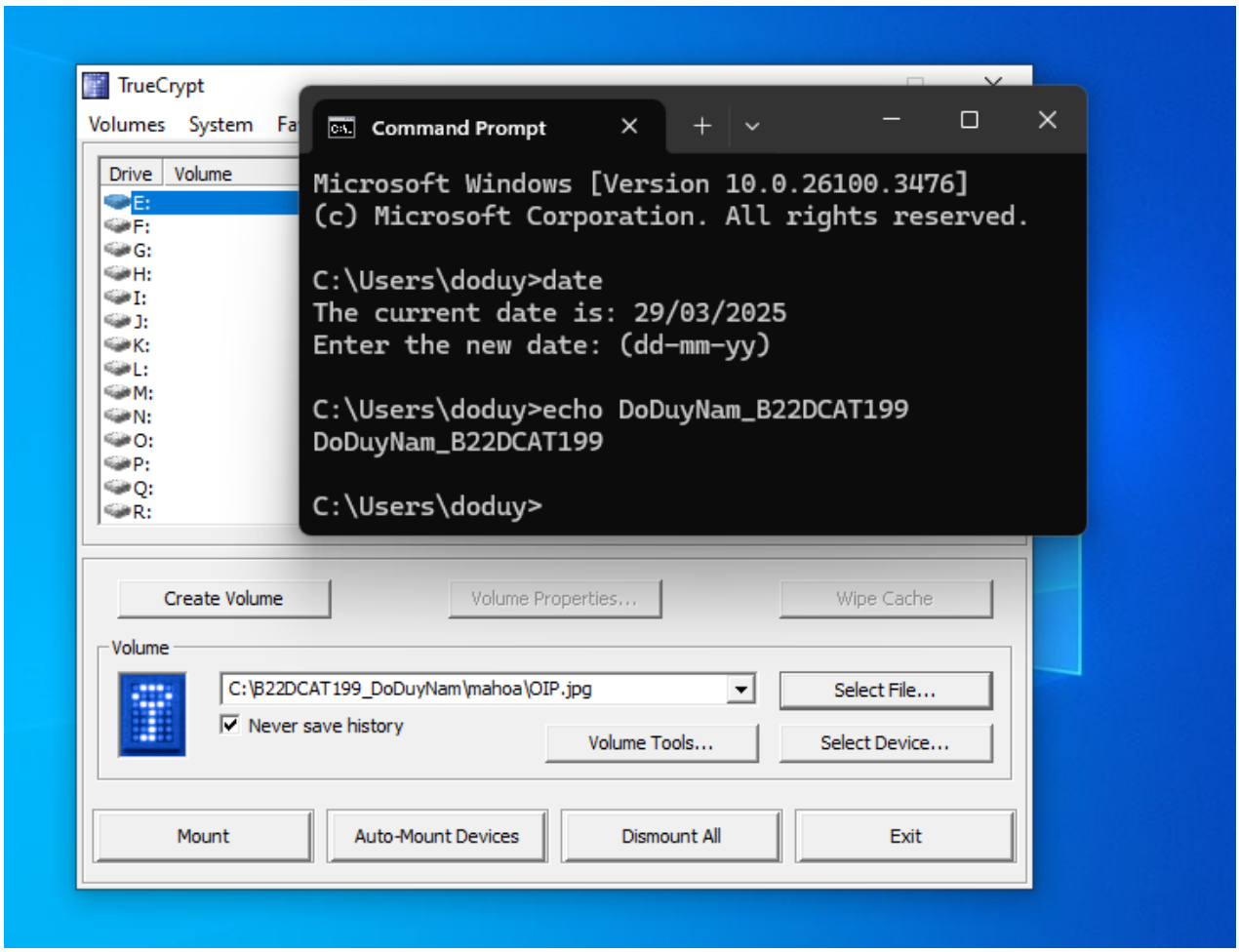
- Sao lưu khóa mã hóa của công cụ TrueCrypt.



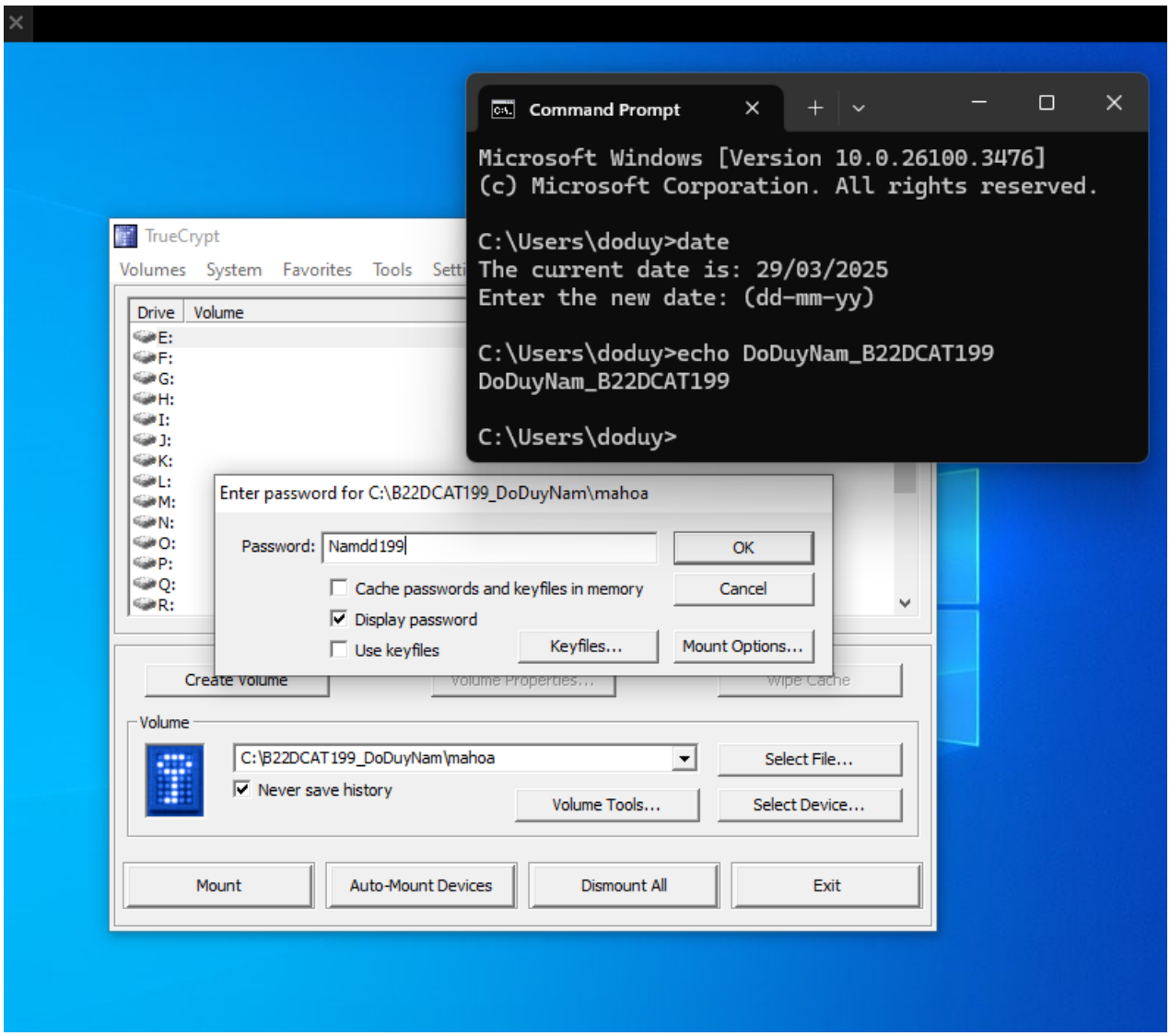
Hình 9 Tạo vào lưu file key



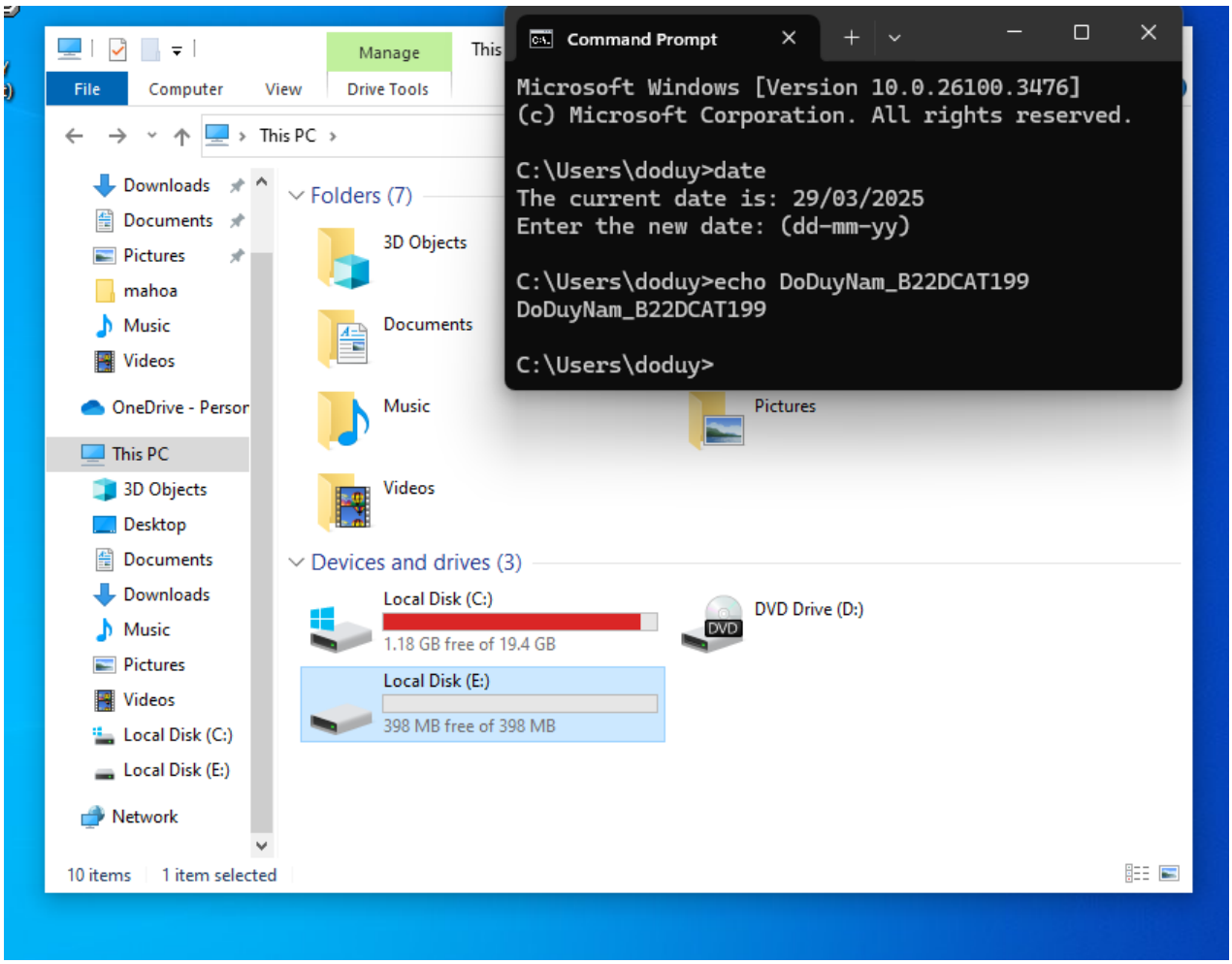
Hình 10 Tạo thành công Volume



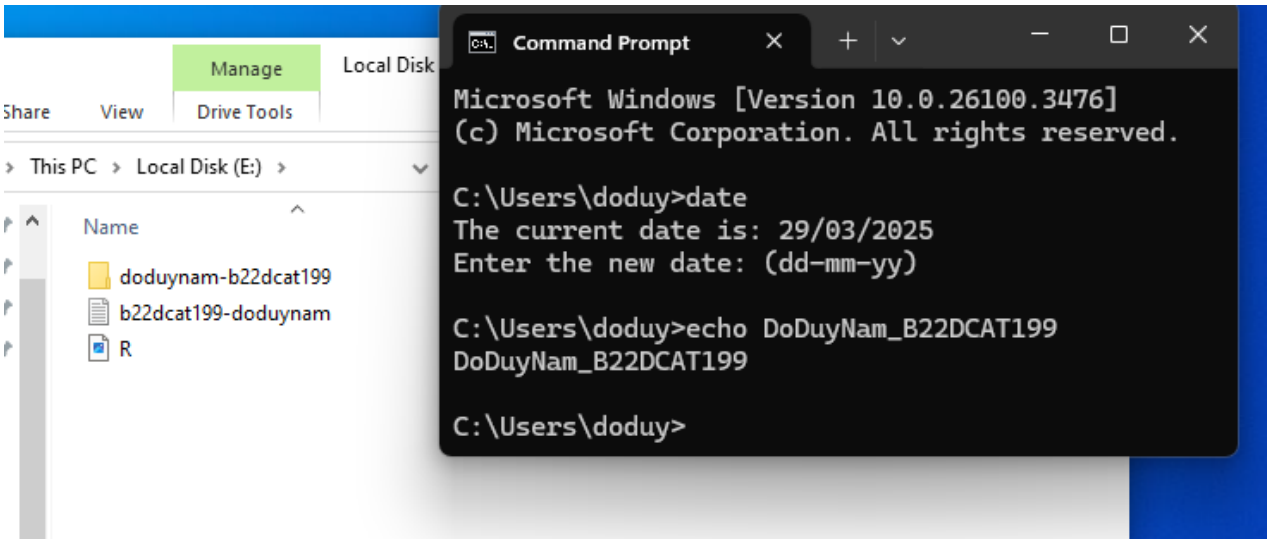
Hình 11 Chọn Volume mới được tạo



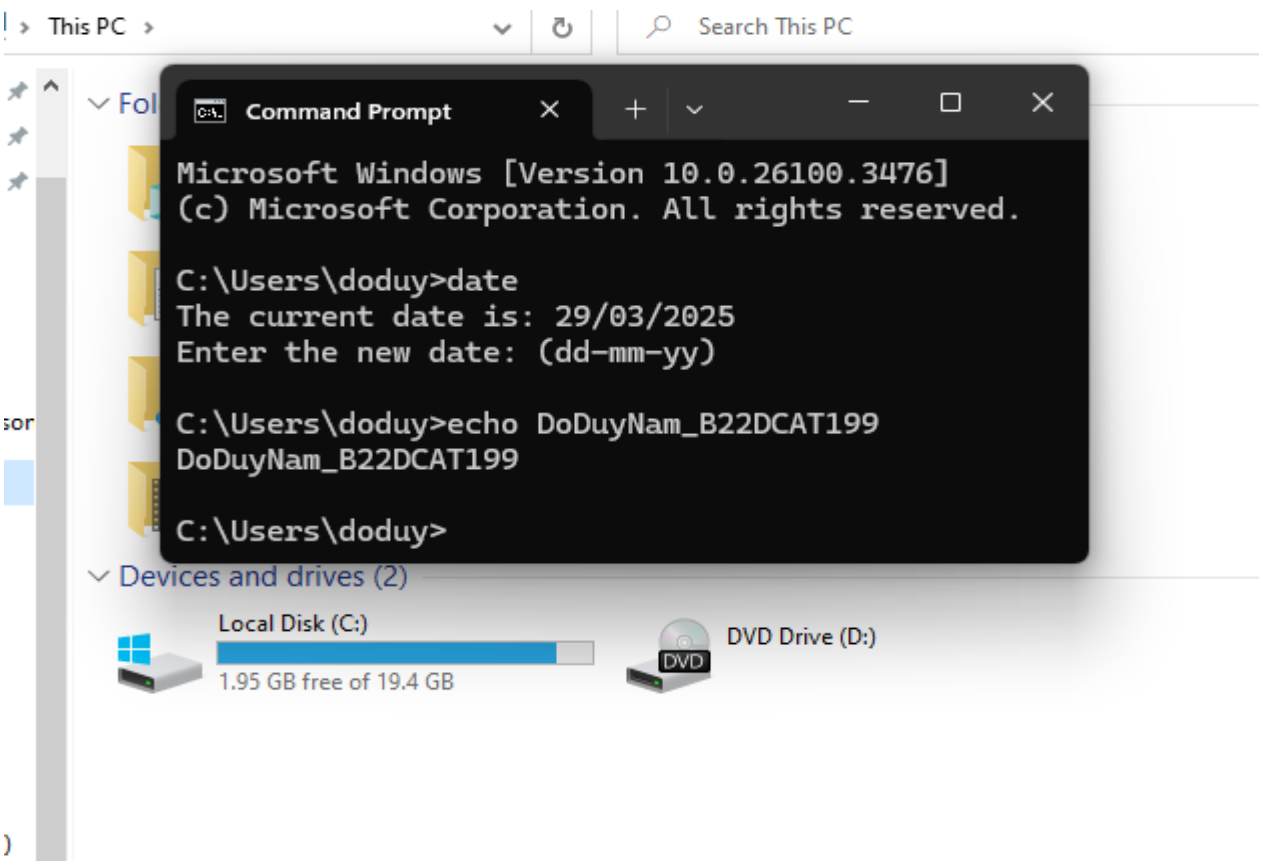
Hình 12 Nhập mật khẩu của Volume



Hình 13 Tạo thành công 1 ổ đĩa mã hóa để lưu trữ các định dạng file, thư mục

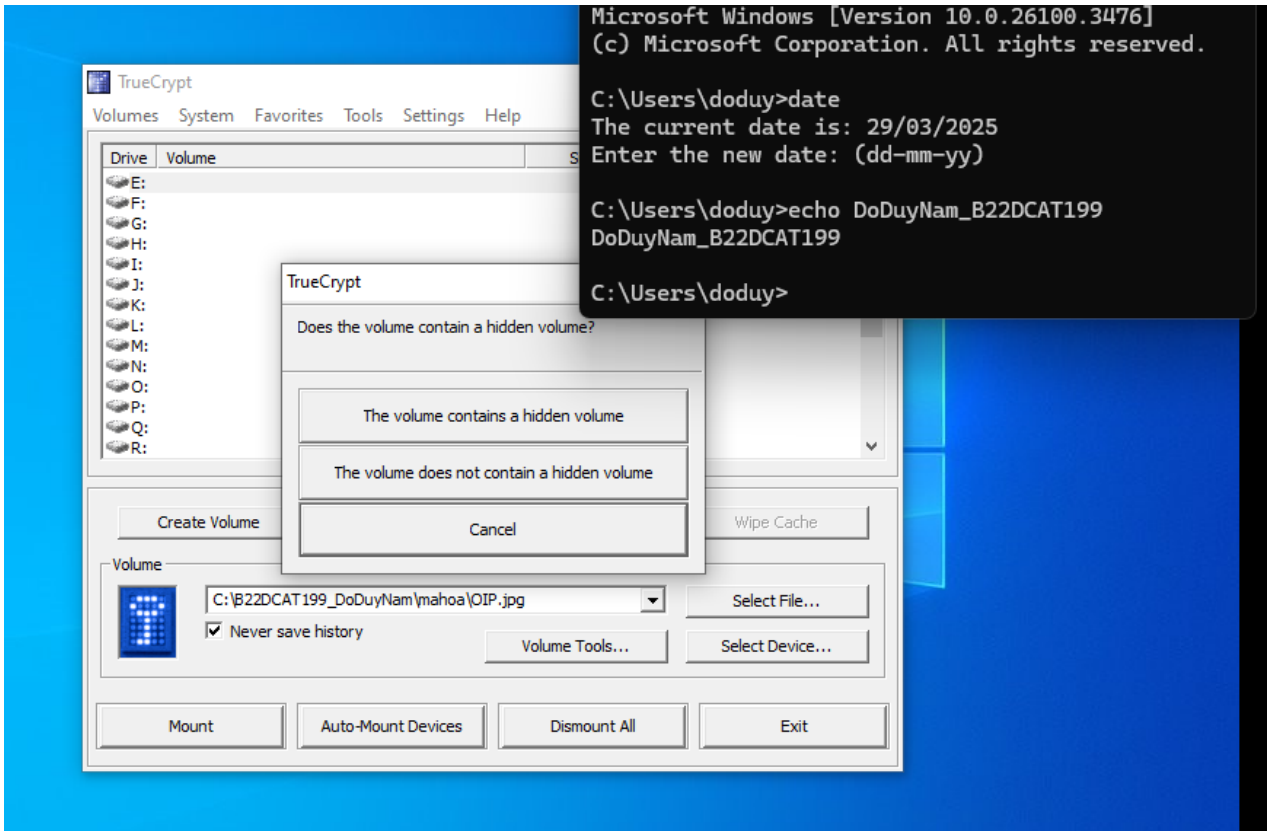


Hình 14 Đưa các file, thư mục vào ổ đĩa mã hóa vừa tạo

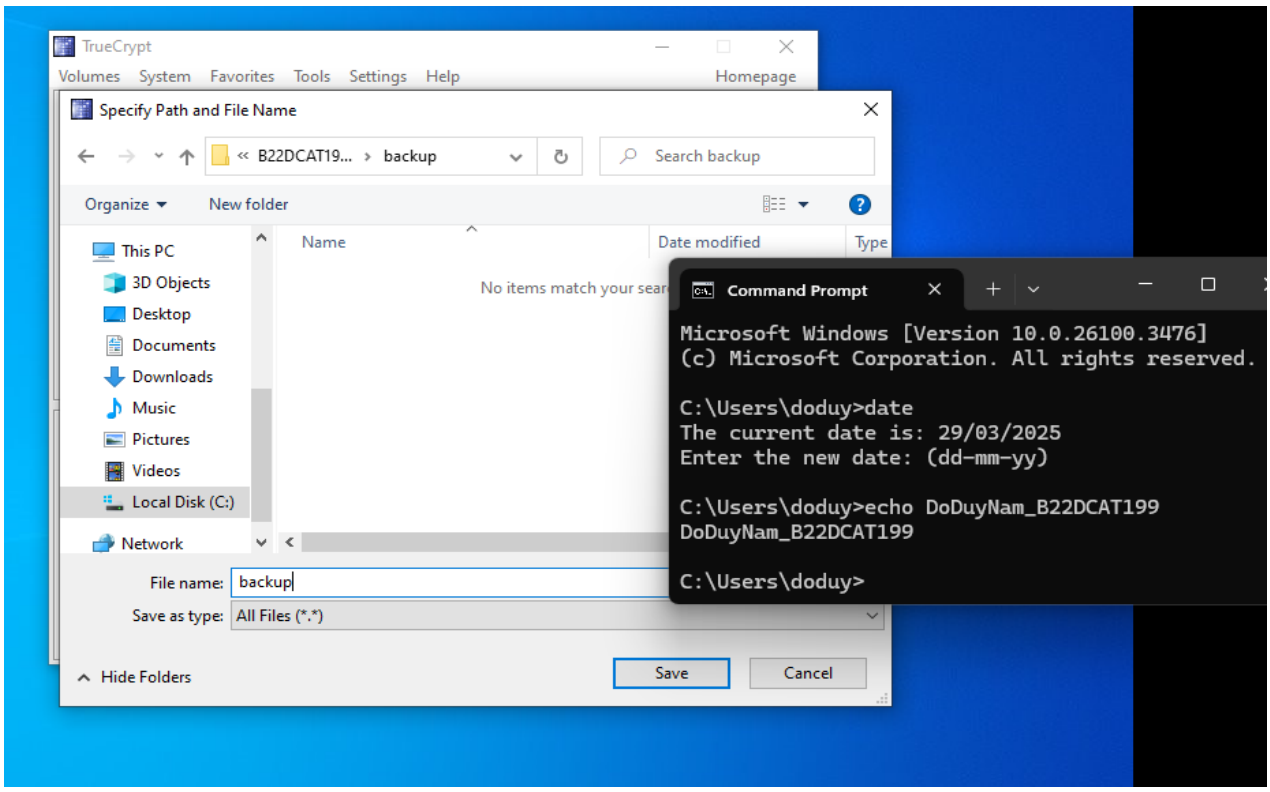


Hình 15 Dismount ổ đĩa để không ai có thể truy cập/xem/sử dụng được -> Ổ E biến mất

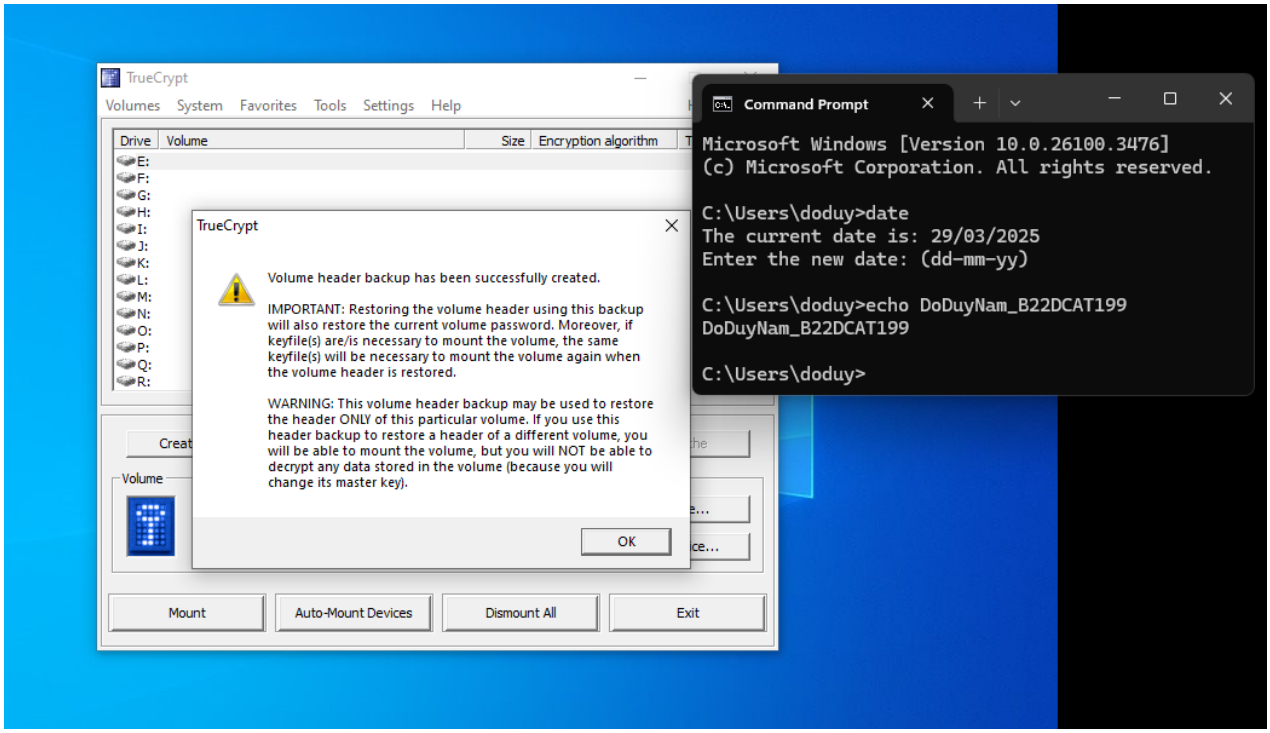
- Sử dụng công cụ TrueCrypt để khôi phục các file và thực mục mã hóa.



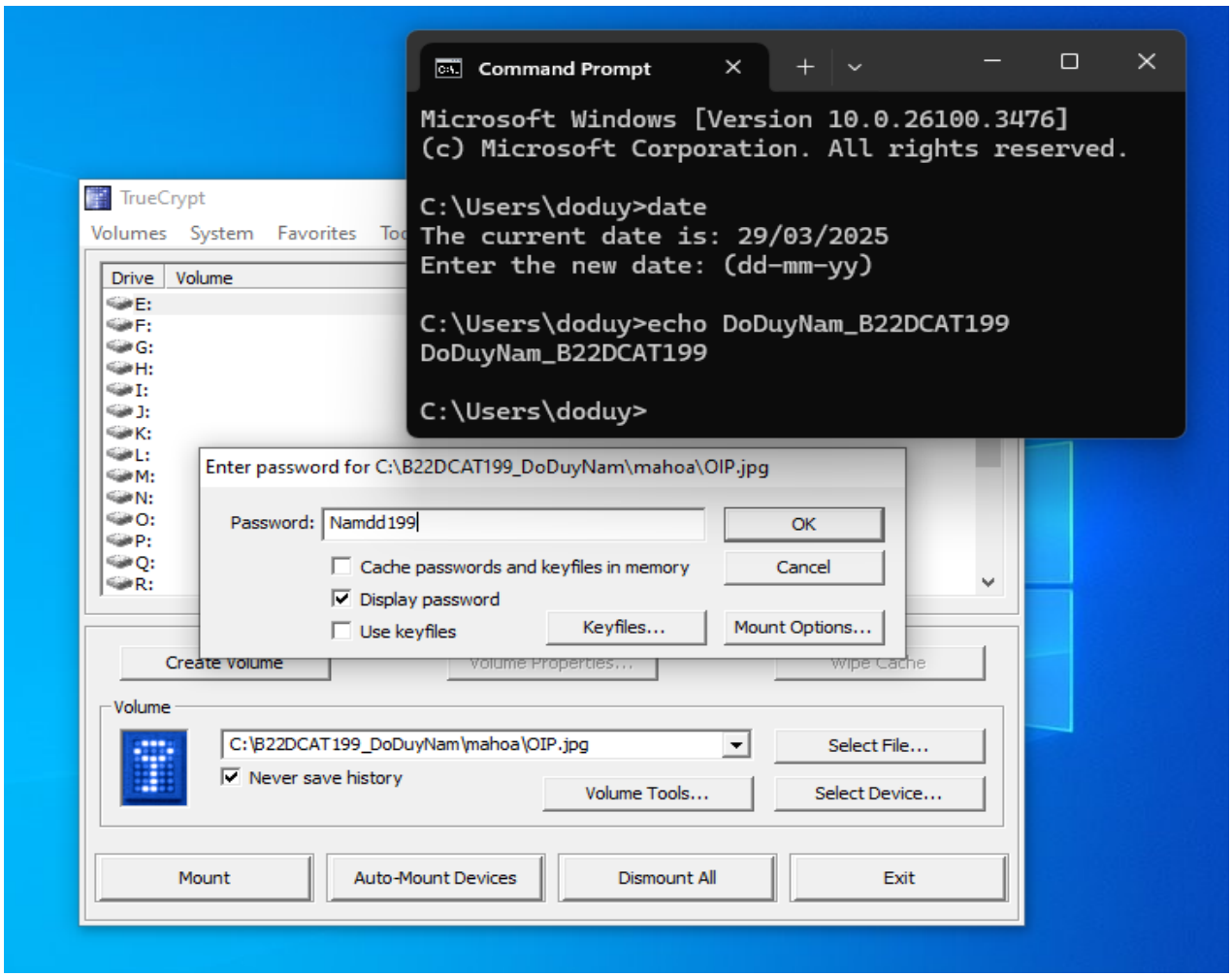
Hình 16 Tiến hành sao lưu file mã hóa



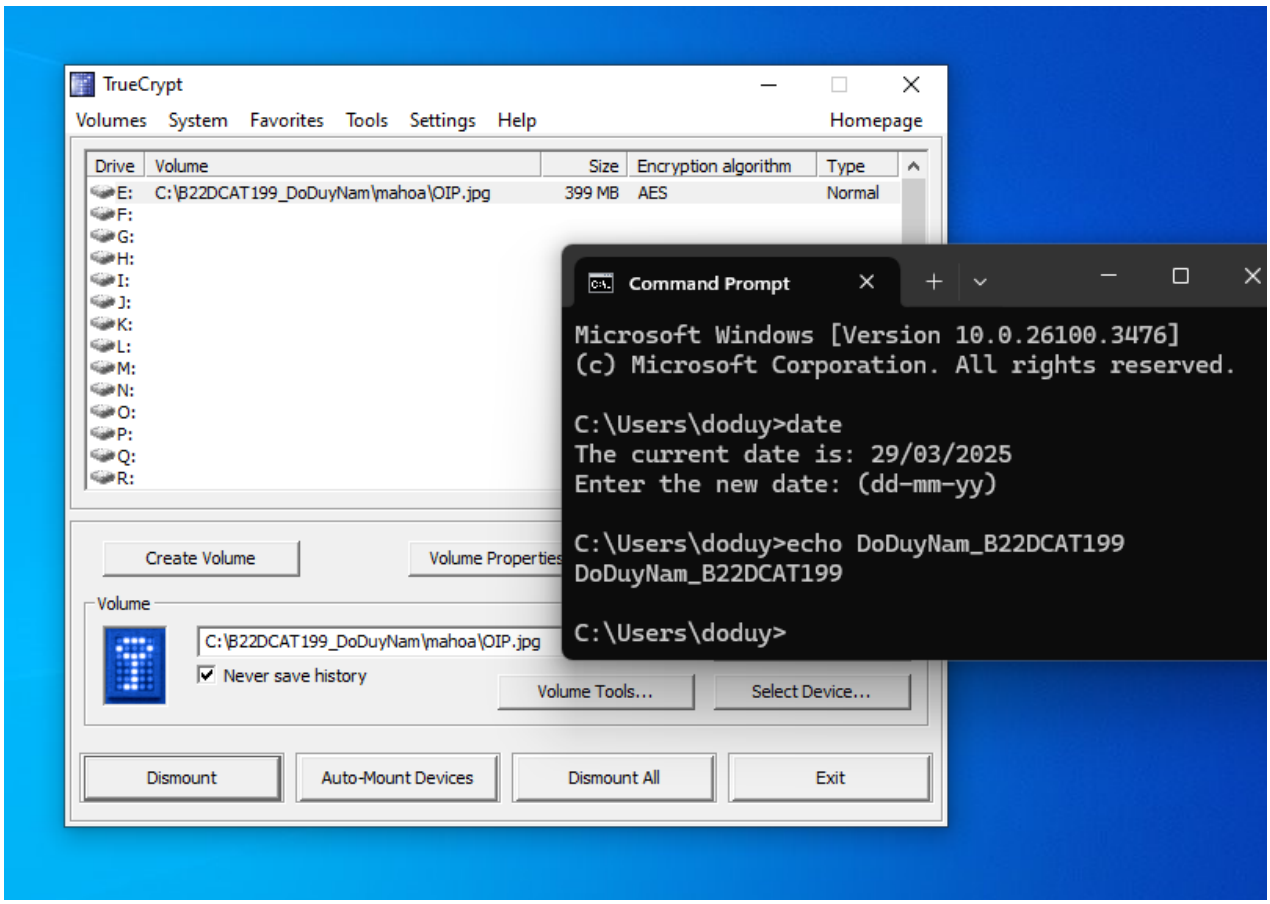
Hình 17 Lưu file mã hóa



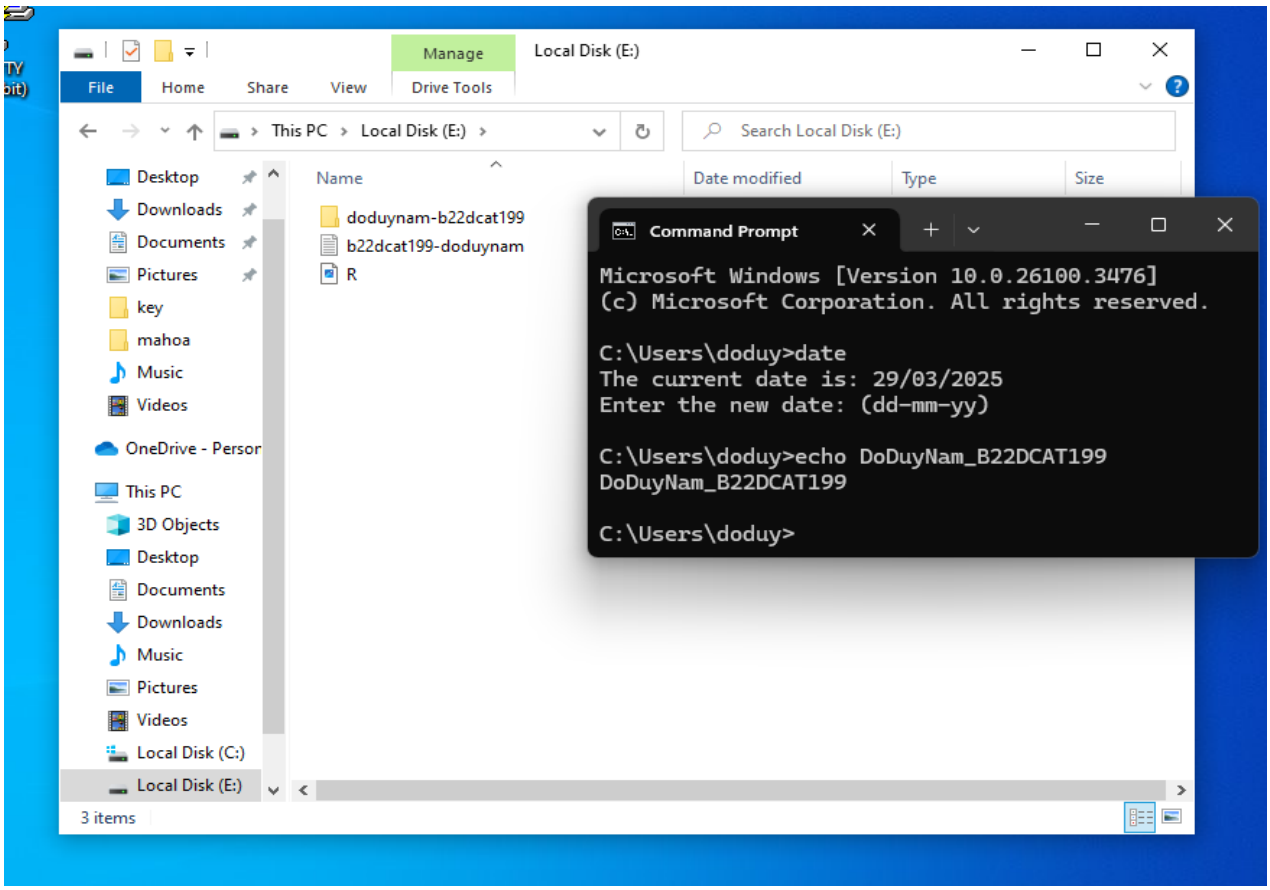
Hình 18 Thành công tạp file sao lưu



Hình 19 Chọn vào file chứa volume đã mã hóa -> Nhập mật khẩu



Hình 20 Chọn Mount để ổ đĩa hiện lên



Hình 21 Khôi phục thành công ổ đĩa

2.3 Kết luận

Ở chương này đã hướng dẫn thực hiện cài đặt TrueCrypt và sử dụng nó để mã hóa file, thư mục, sao lưu khóa mã hóa của công cụ TrueCrypt và đồng thời sử dụng để khôi phục các file và thư mục đã mã hóa

KẾT LUẬN

- Tìm hiểu về các công cụ của TrueCrypt.
- Tìm hiểu về cách thức hoặc phương pháp công cụ TrueCrypt áo dụng để mã hóa file hoặc thư mục.
- Cài đặt thành công công cụ TrueCrypt.
- Mã hóa thành công file, thư mục bằng TrueCrypt.
- Khôi phục thành công các file và thư mục đã bị mã hóa bởi TrueCrypt.

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.