**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:

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 |
|---|---|---|
| AES | Advanced Encryption Standard | Tiêu chuẩn mã hóa tiên tiến |
| ECC | Elliptic Curve Cryptography | Mật mã đường cong elliptic |
| SHA | Secure Hash Algorithm | Thuật toán băm an toàn |
| SSL | Secure Sockets Layer | Lớp bảo mật cho truyền thông Internet |
| TLS | Transport Layer Security | Bảo mật tầng truyền tải |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

## 1.1 Mục đích

Mục đích của bài thực hành "2.4: Đảm bảo an toàn thông tin dựa trên mã hóa" là 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*

TrueCrypt là một công cụ mã hóa dữ liệu mã nguồn mở và miễn phí, cho phép người dùng tạo ra các ổ đĩa ảo được mã hóa để lưu trữ dữ liệu một cách an toàn. Nó cung cấp khả năng mã hóa đủ mạnh mẽ để bảo vệ dữ liệu cá nhân hoặc nhạy cảm của bạn khỏi việc truy cập trái phép.

Cơ chế thiết lập và quản lý của TrueCrypt là mã hóa ổ đĩa trên đường đi (on-the-fly encryption). Nghĩa là dữ liệu tự động được mã hóa hoặc giải mã ngay khi được ghi xuống đĩa cứng hoặc ngay khi dữ liệu được nạp lên mà không có bất kỳ sự can thiệp nào của người dùng. Dữ liệu được lưu trữ trên một ổ đĩa đã được mã hóa (encryption volume) không thể đọc được nếu người dùng không cung cấp đúng khóa mã hóa bằng một trong ba hình thức là mật khẩu (password) hoặc tập tin có chứa khóa (keyfile) hoặc khóa mã hóa (encryption key). Toàn bộ dữ liệu trên ổ đĩa mã hóa đều được mã hóa (ví dụ như tên file, tên folder, nội dung của từng file, dung lượng còn trống, siêu dữ liệu...). Dữ liệu có thể được copy từ một ổ đĩa mã hóa của TrueCrypt sang một ổ đĩa bình thường không mã hóa trên Windows (và ngược lại) một cách bình thường mà không có sự khác biệt nào cả, kể cả các thao tác kéo-thả.

Ưu điểm của TrueCrypt:

- *Miễn phí và mã nguồn mở*: TrueCrypt là một phần mềm mã nguồn mở, điều này có nghĩa là mã nguồn của nó có thể được kiểm tra và xác minh bởi cộng đồng người dùng.
- *Mã hóa mạnh mẽ*: TrueCrypt sử dụng các thuật toán mã hóa tiên tiến như AES, Serpent và Twofish để bảo vệ dữ liệu của bạn.
- *Hỗ trợ nhiều nền tảng*: TrueCrypt có sẵn cho nhiều hệ điều hành như Windows, macOS và Linux, giúp bạn có thể sử dụng trên nhiều thiết bị.

Hạn chế của TrueCrypt:

- *Ngừng phát triển*: TrueCrypt đã ngừng phát triển từ năm 2014 và đã được khuyến nghị bởi các chuyên gia an ninh thông tin để ngừng sử dụng vì lỗ hổng bảo mật có thể tồn tại mà không được vá.
- *Không được hỗ trợ chính thức*: Vì không còn phát triển chính thức, không có sự hỗ trợ chính thức từ nhà sản xuất hoặc cộng đồng người dùng, điều này có thể khiến việc giải quyết vấn đề hoặc hỏi đáp về vấn đề kỹ thuật trở nên khó khăn.

- *Không có cơ chế cập nhật*: Với sự ngừng phát triển, TrueCrypt không cung cấp cơ chế tự động cập nhật, điều này có thể dẫn đến việc sử dụng phiên bản cũ với các lỗ hổng bảo mật không được vá.

Do các vấn đề bảo mật và ngừng phát triển, nhiều người dùng đã chuyển sang sử dụng các giải pháp mã hóa dữ liệu khác như VeraCrypt, một dự án phát triển từ TrueCrypt và cung cấp sự tiếp tục phát triển và hỗ trợ.

### *1.2.2 Cách thức TrueCrypt mã hóa file hoặc thư mục*

#### *1.2.2.1 Các thuật toán mã hóa mà TrueCrypt sử dụng*

TrueCrypt sử dụng một số thuật toán mã hóa mạnh mẽ để bảo vệ dữ liệu, bao gồm:

- *AES (Advanced Encryption Standard)*: AES là một trong những thuật toán mã hóa simétric phổ biến nhất. TrueCrypt hỗ trợ các khóa 128-bit, 192-bit và 256 bit cho việc mã hóa dữ liệu.
- *Serpent*: Serpent là một thuật toán mã hóa simétric được thiết kế để cung cấp mức độ bảo mật cao. TrueCrypt sử dụng Serpent với các khóa 128-bit, 192-bit và 256-bit.
- *Twofish*: Twofish cũng là một thuật toán mã hóa simétric, được thiết kế để cung cấp hiệu suất cao và bảo mật. TrueCrypt hỗ trợ Twofish với các khóa 128 bit, 192-bit và 256-bit. Các thuật toán này được sử dụng bởi TrueCrypt để mã hóa dữ liệu trên các ổ đĩa ảo hoặc phân vùng được tạo ra bởi phần mềm, cung cấp một lớp bảo vệ mạnh mẽ chống lại việc truy cập trái phép.

#### *1.2.2.2 Các hình thức khóa TrueCrypt hỗ trợ để mã hóa/ giải mã dữ liệu*

TrueCrypt hỗ trợ một số hình thức khóa để mã hóa dữ liệu, bao gồm:

- *Khóa mật khẩu (Password)*: Đây là phương thức phổ biến nhất, người dùng nhập mật khẩu để mở khóa tệp hoặc thiết bị. Mật khẩu có thể được tạo ra từ các ký tự ASCII, bao gồm chữ cái, chữ số và ký tự đặc biệt.
- *Khóa file (Keyfile)*: Bạn có thể sử dụng một tập tin nhất định như một phần của khóa. Thông thường, file này được tạo ra bằng cách chọn một file bất kỳ trên máy tính của bạn.
- *Khóa không gian (Keyfile and Password)*: Kết hợp cả hai, yêu cầu cả một mật khẩu và một keyfile để mở khóa. Mỗi phương thức có ưu và nhược điểm riêng, và việc lựa chọn loại khóa thích hợp phụ thuộc vào yêu cầu cụ thể của bạn về bảo mật và tiện ích.

#### *1.2.2.3 Cách thức mã hóa của công cụ TrueCrypt*

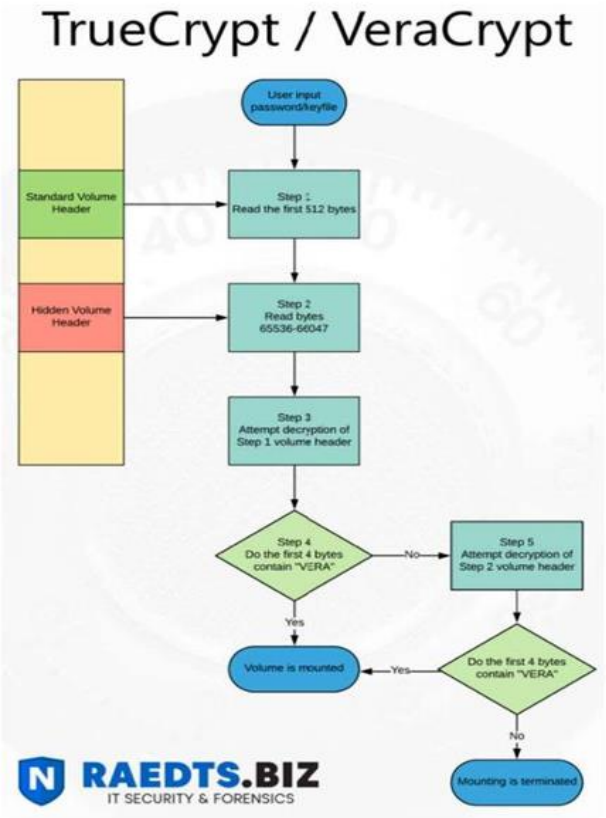
Bước 1: 512 byte đầu tiên của volume được đọc thành RAM, trong đó 64 byte đầu tiên là salt. Đối với mã hóa hệ thống, 512 byte cuối cùng của rãnh ổ đĩa logic đầu tiên được đọc vào RAM.

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*

*1.2.2.4 Quá trình tạo ổ đĩa ảo được mã hóa để bảo vệ tài liệu nhạy cảm*

Khi người dùng tạo một ổ đĩa ảo được mã hóa với TrueCrypt, thực tế là họ đã tạo một vùng duy nhất để chứa các tập tin được gọi là *File container*, mà chỉ có thể mở hoặc giải mã với mật khẩu được chọn.

Cũng như các tập tin bình thường khác, file trong ổ đĩa ảo này có thể được xóa, di chuyển hoặc sao chép. Chỉ khác ở chỗ người dùng chỉ có thể truy cập vào chúng để làm việc này khi có mật khẩu chính xác. Sau đó khởi động ứng dụng, thực hiện theo các bước dưới đây để tạo *File container* mã hóa:

1. Kích **Create Volume** để bắt đầu.

2. Chọn **Create an encrypted file container** và kích **Next**.

3. Chọn **Standard TrueCrypt volume** sau đó nhấn **Next**.

4. Kích **Select File**, điều hướng đến nơi bạn muốn đặt file container mã hóa, đặt tên cho nó và nhấn **Save**. Cuối cùng nhấn **Next**.

5. Trừ khi có lý do đặc biệt nào đó, nếu không hãy chấp nhận các tùy chọn mã hóa mặc định và kích **Next**.

6. Chỉ định kích thước muốn cung cấp cho file container. Đảm bảo cho nó đủ lớn để lưu trữ các tập tin tài liệu quan trọng. Nhấn **Next**.

7. Nhập vào mật khẩu để mã hóa/giải mã và nhấn **Next**.

8. Giữ nguyên thiết lập định dạng volume mặc định, nhưng hãy di chuyển con trỏ chuột xung quanh một cách ngẫu nhiên để tăng sức mạnh và độ an toàn cho mật khẩu. Sau đó kích **Format** để khởi tạo file container.

Để sử dụng file container mã hóa này người dùng cần kết nối (mount) nó như một ổ đĩa. Cách cơ bản nhất để làm điều này là kích vào ổ đĩa mong muốn trên cửa sổ chính của TrueCrypt, chọn **Select File** và tìm đến file container, nhấn **Mount**. Người dùng sẽ được nhắc nhở về mật khẩu mã hóa đã thiết lập khi tạo file container, nhập vào và kích **OK**. Sau đó là truy cập vào các file trong cửa sổ bằng cách sử dụng Computer (hoặc My Computer). Cũng như các ổ đĩa khác, người dùng có thể xem, truy cập từ các hộp thoại open/save trong Windows và các chương trình khác. Nếu người dùng muốn file container tự động gắn kết khi đăng nhập vào Windows, có thể thêm nó vào Favorites của mình.

# CHƯƠNG 2. NỘI DUNG THỰC HÀNH

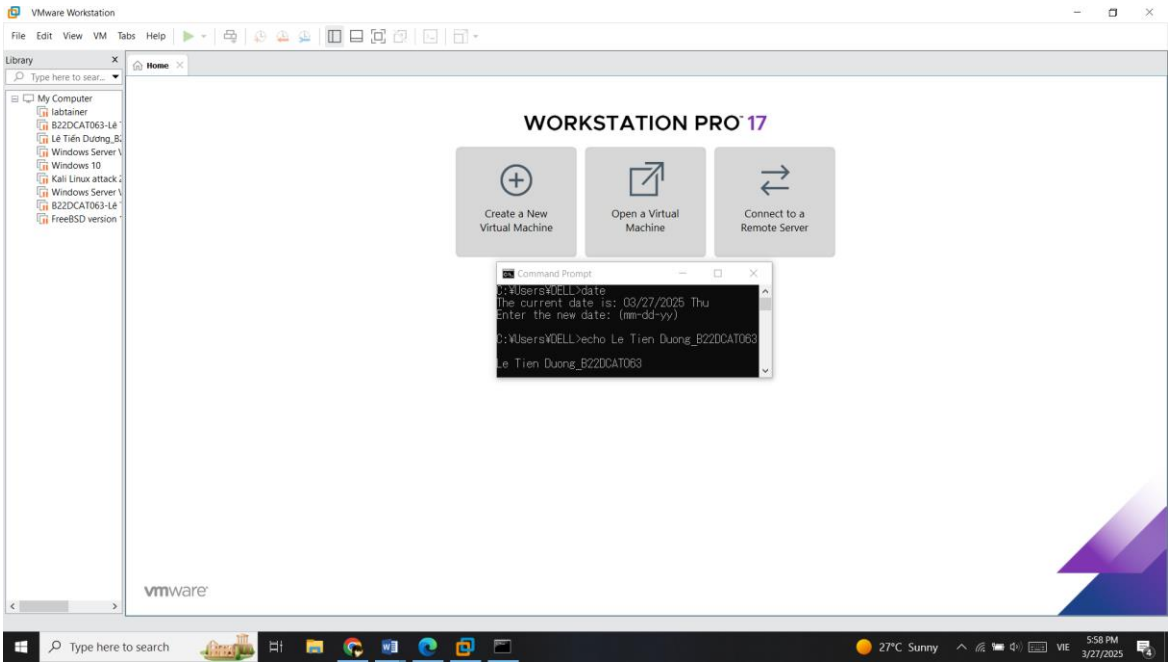
## 2.1 Chuẩn bị môi trường

- Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm ảo hóa khác.
- Công cụ TrueCrypt.

## 2.2 Các bước thực hiện

### *2.2.1 Chuẩn bị môi trường*

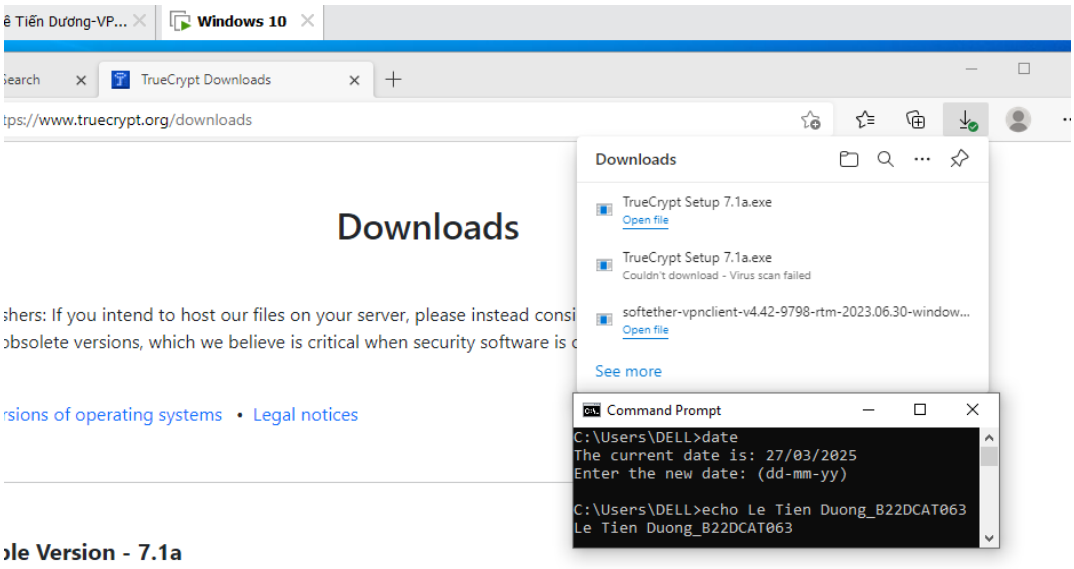
Cài đặt công cụ ảo hóa.




*Hình 2 – Công cụ ảo hóa VMWare*

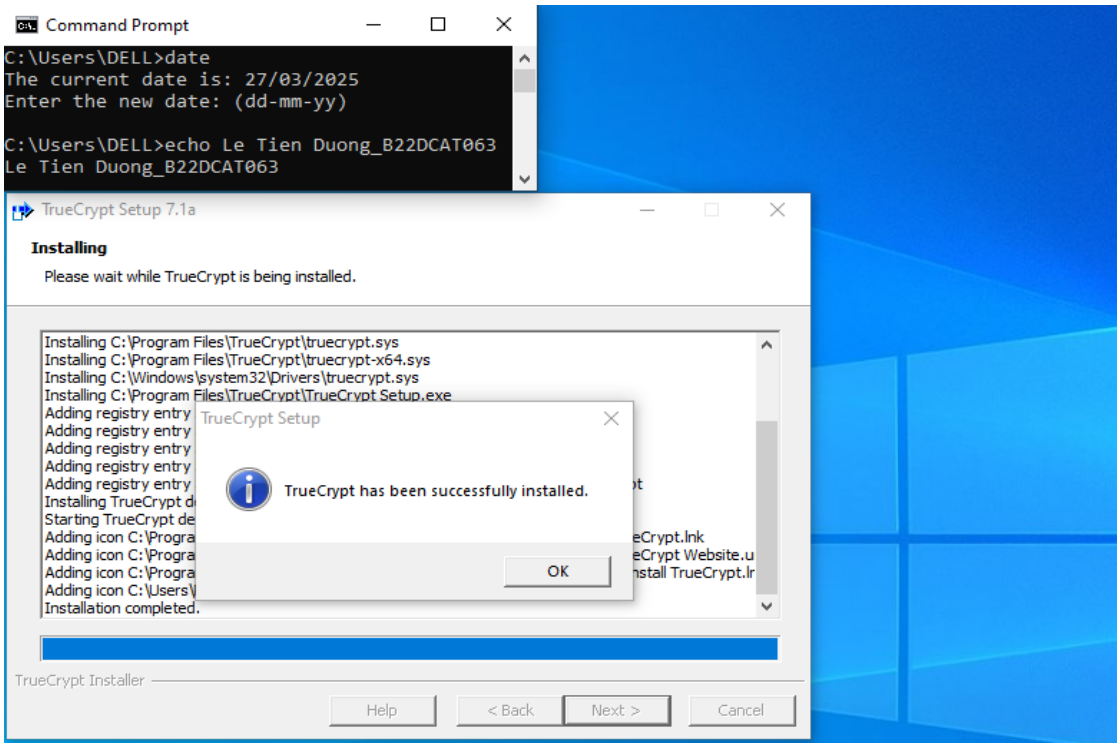
Cài đặt máy ảo chạy hệ điều hành Windows.

Cài đặt TrueCrypt trên hệ điều hành Windows.

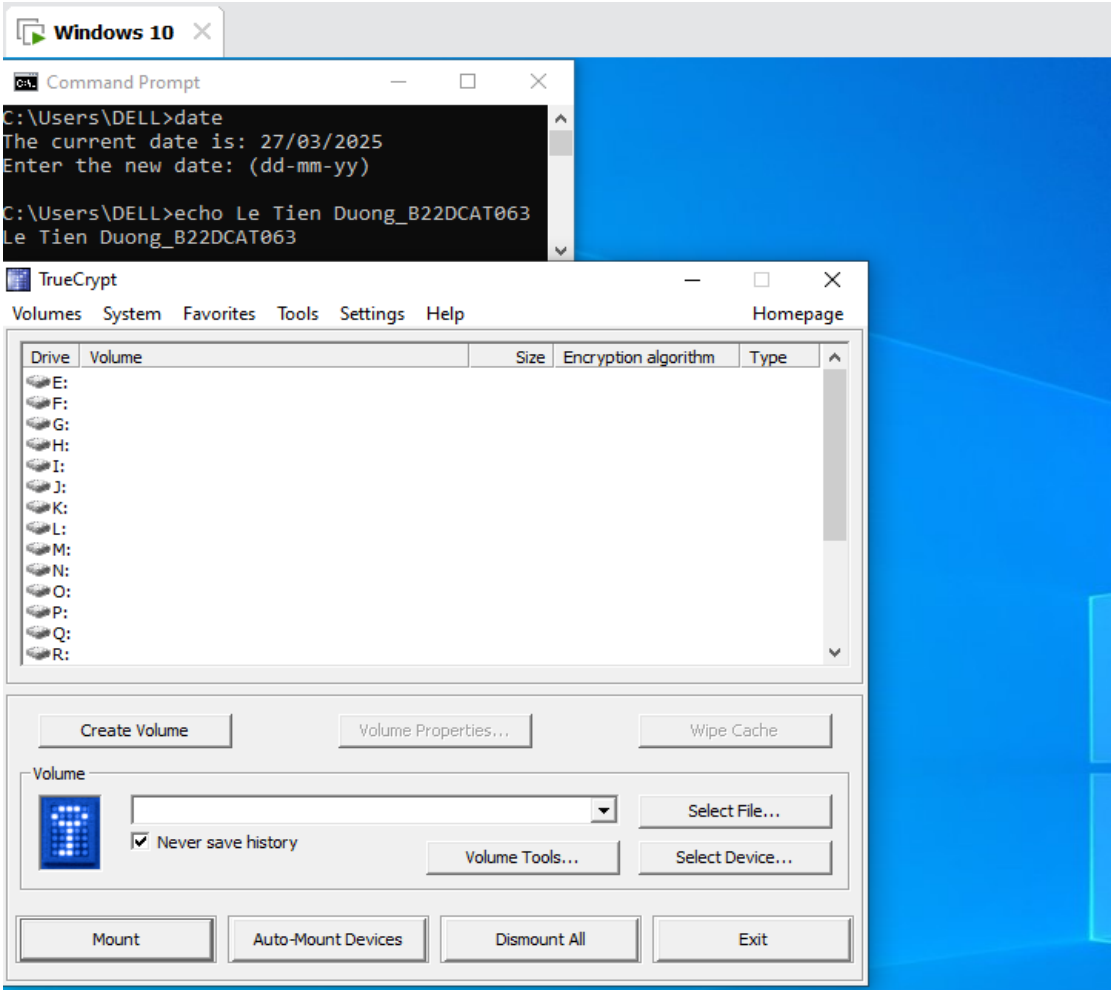



*Hình 3 – Cài đặt máy ảo Windows 10 và tải TrueCrypt*

Cài đặt công cụ TrueCrypt.




*Hình 4 – Cài đặt thành công công cụ TrueCrypt*

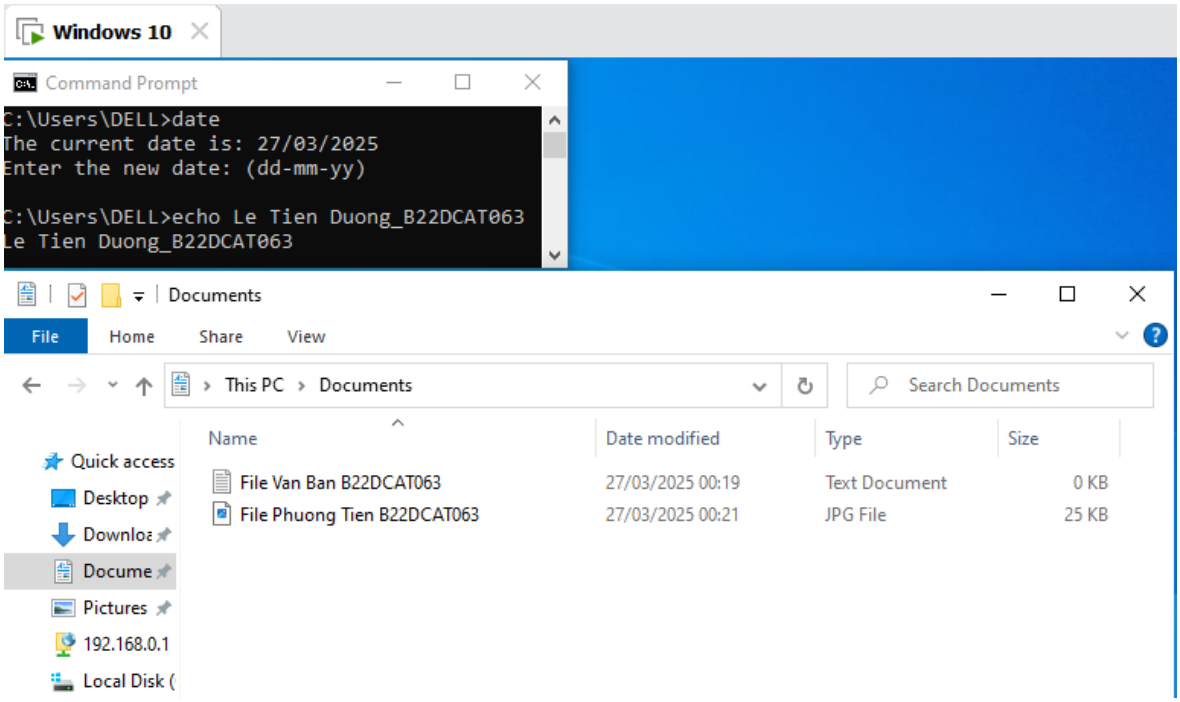



*Hình 5 – Giao diện TrueCrypt trên hệ điều hành Windows*

### *2.2.2 Nội dung thử nghiệm*

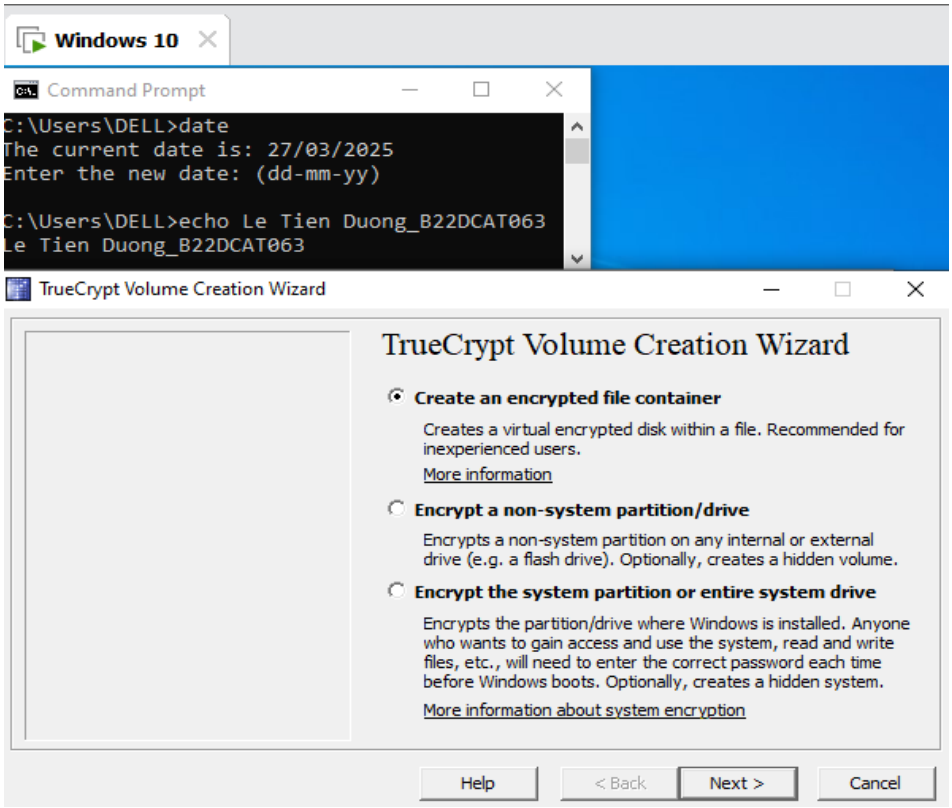
*2.2.2.1 Sử dụng công cụ TrueCrypt để hóa mã file. Yêu cầu thực hiện trên ít nhất 2 loại file bao gồm: file văn bản và file đa phương tiện (định dạng ảnh, video, hoặc âm thanh)*

Tạo 2 file như yêu cầu.



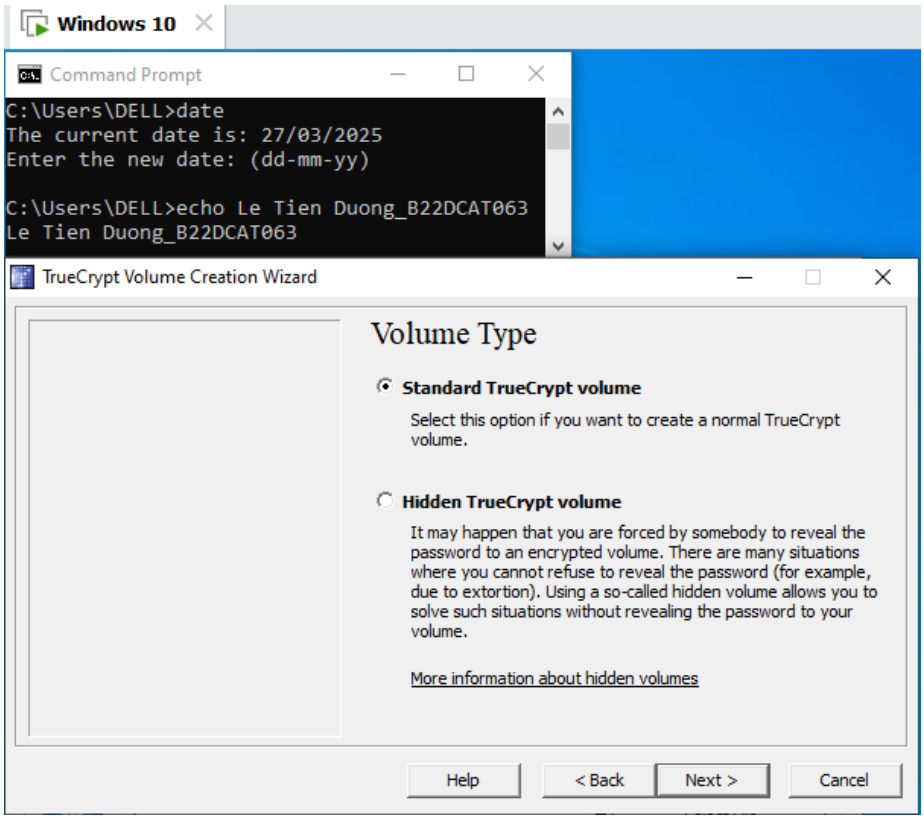

*Hình 6 – Tạo 2 file theo yêu cầu*

Tạo 1 volume để mã hóa.



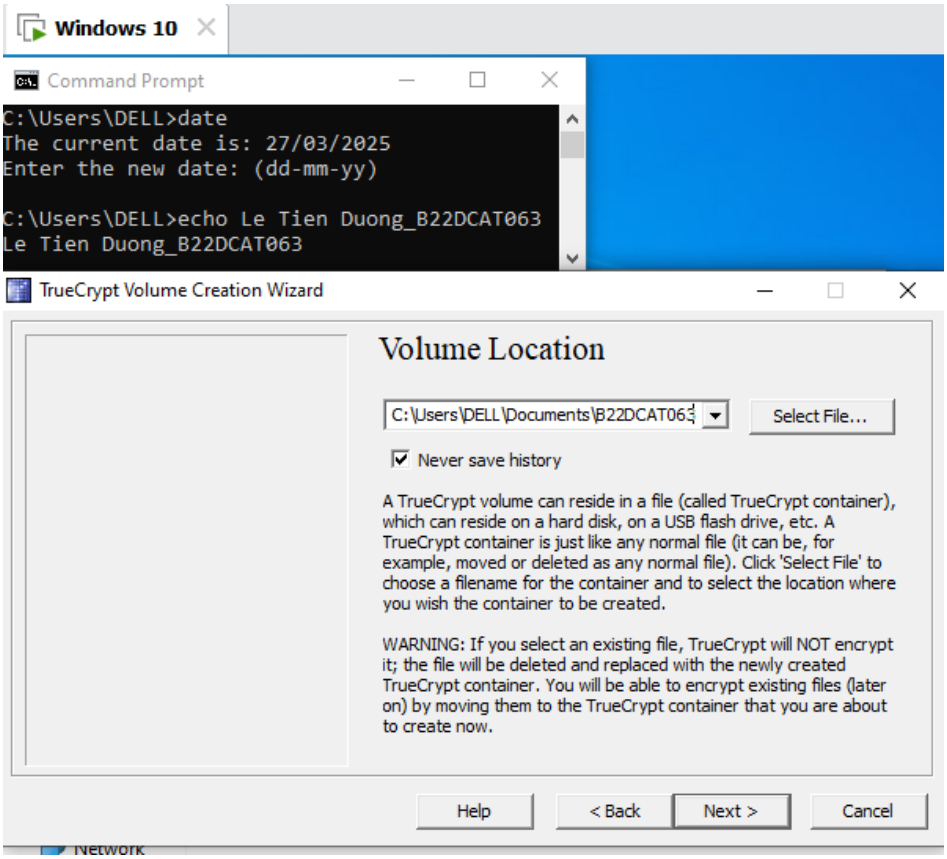

*Hình 7 – Tạo 1 volume để mã hóa*

Sau đó lựa chọn tạo một ổ đĩa bình thường.



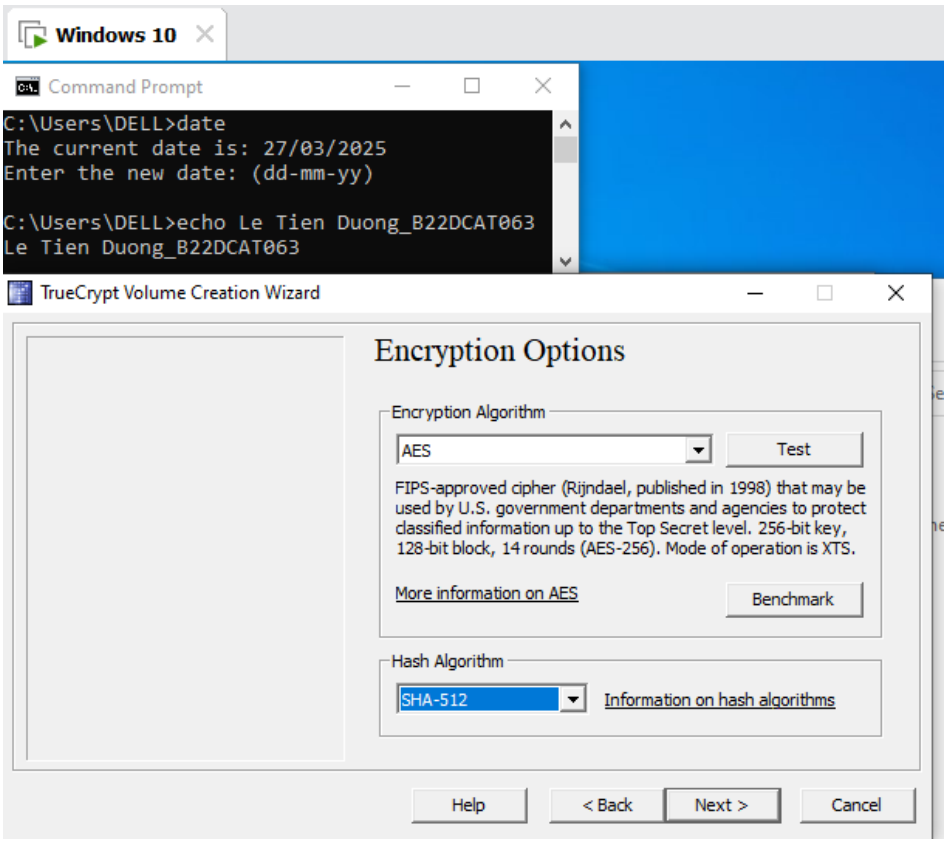

*Hình 8 – Chọn loại Volume*

Chọn vị trí ổ đĩa mã hóa.



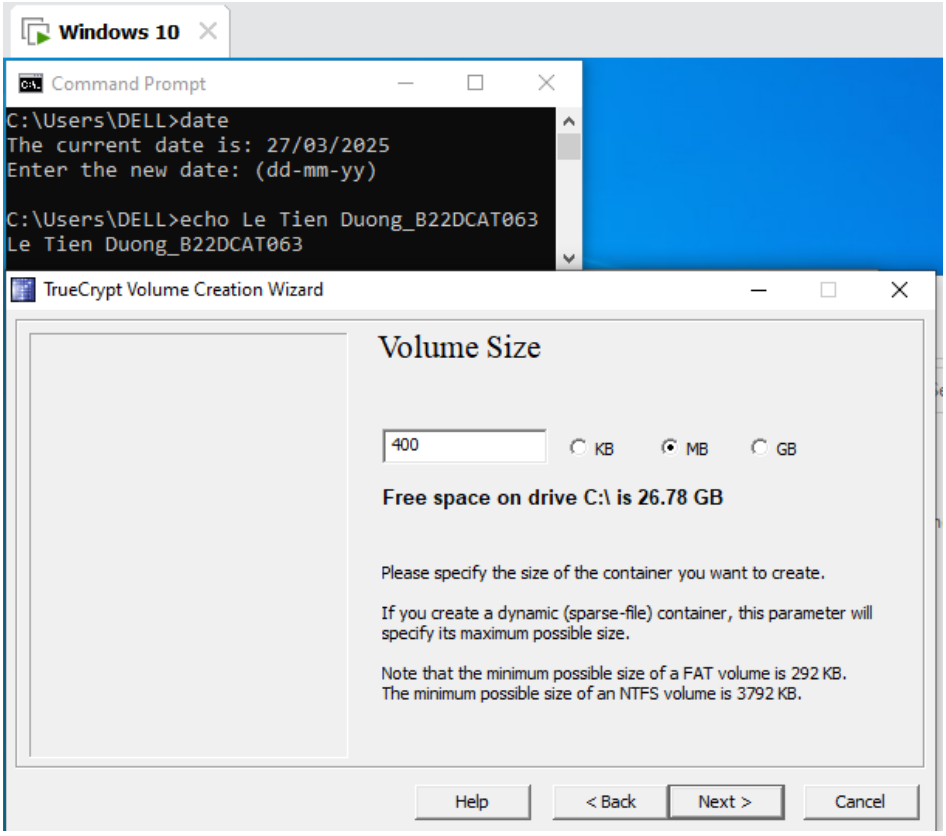

*Hình 9 – Chọn vị trí Volume*

Chọn thuật toán mã hóa.



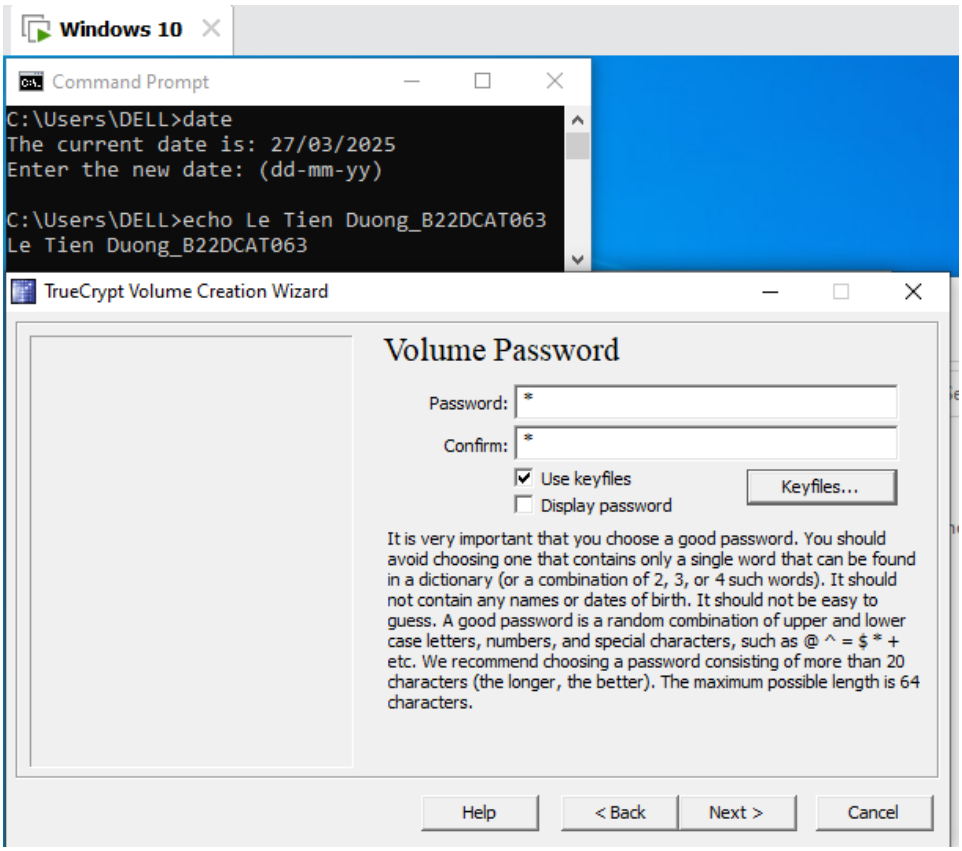

*Hình 10 – Chọn thuật toán mã hóa*

Chọn kích thước tối đa cho Volume.



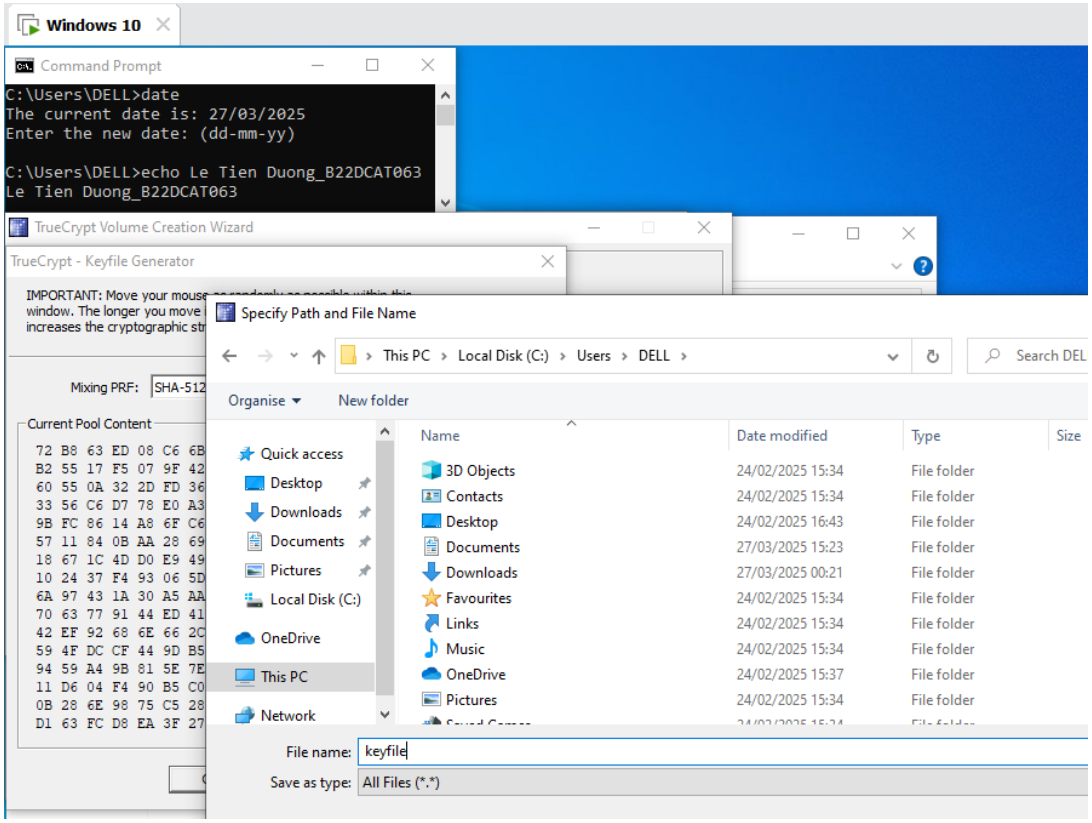

*Hình 11 – Chọn kích thước cấp cho Volume*

Chọn mật khẩu để mount Volume.

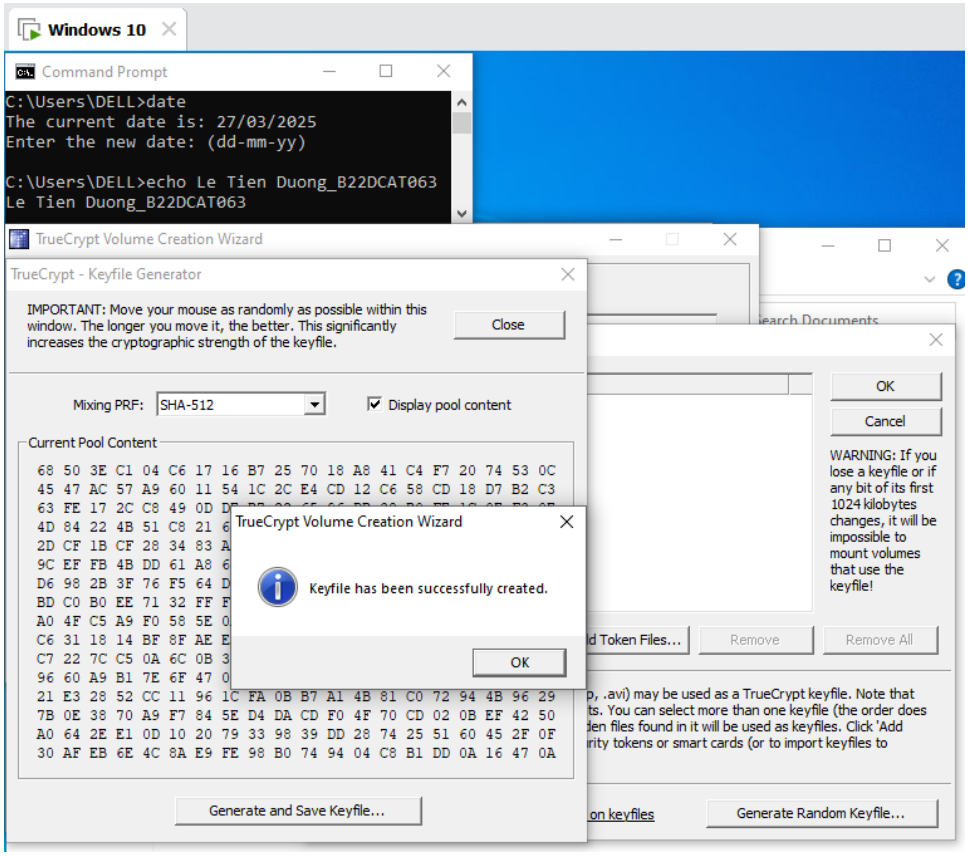



*Hình 12 – Nhập mật khẩu để mã hóa Volume*

Lưu trữ Keyfile.

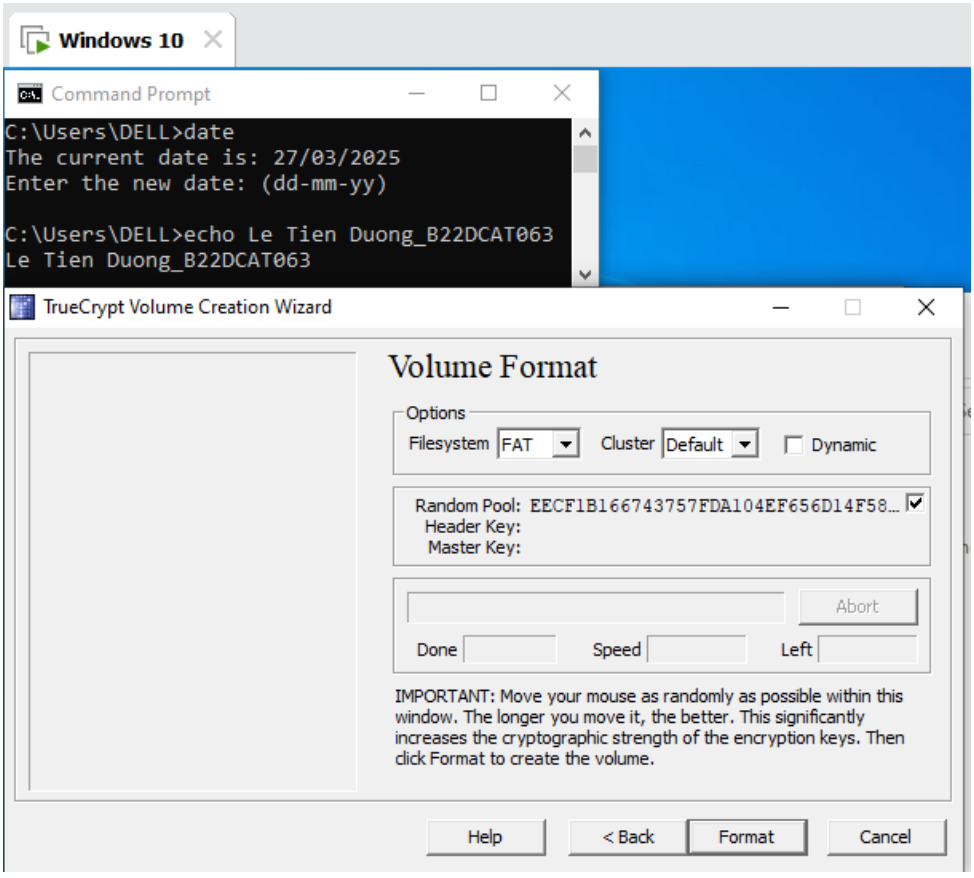



*Hình 13 – Lưu trữ Keyfile*



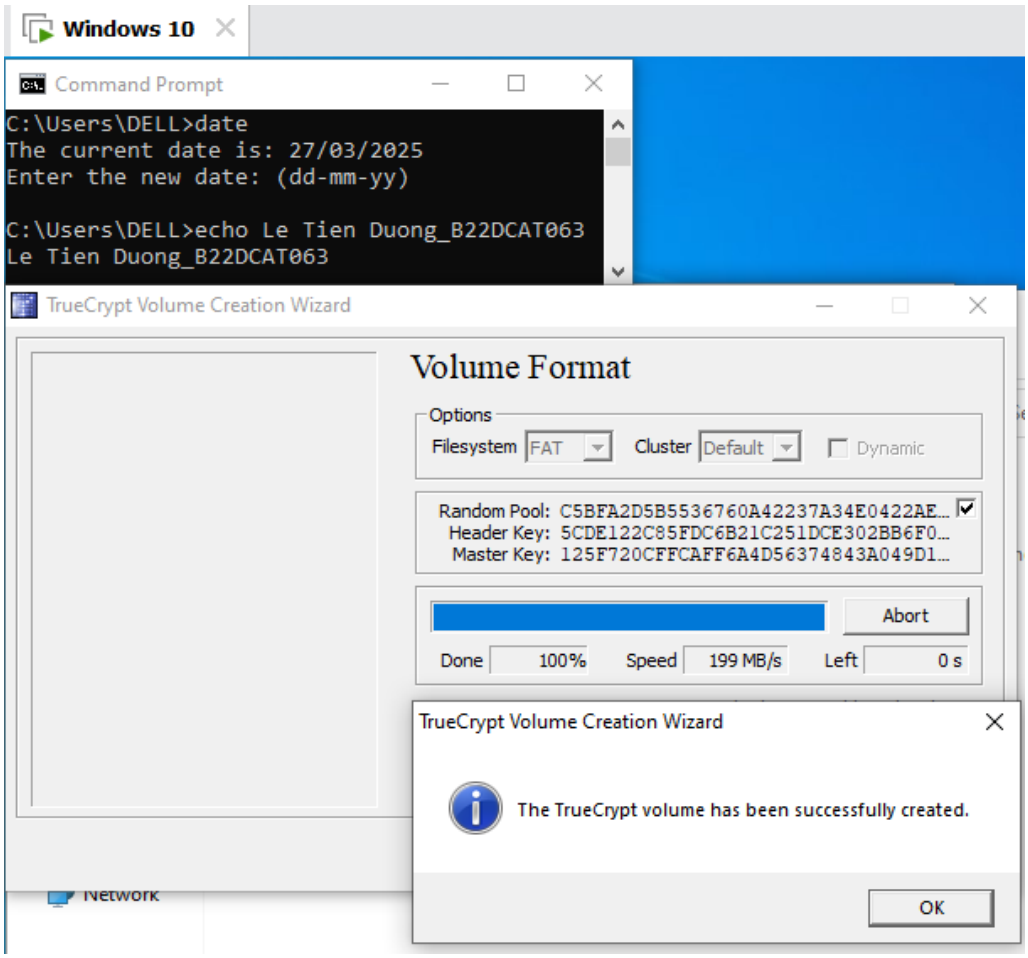

*Hình 14 – Tạo và lưu thành công*

Chọn định dạng của Volume.



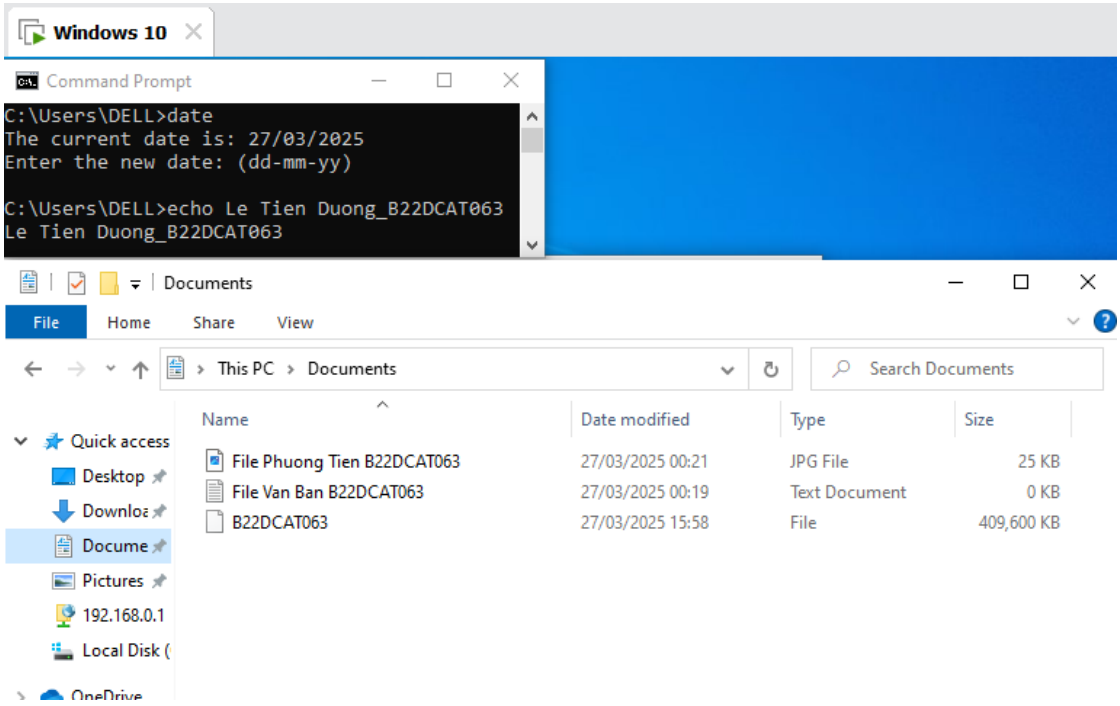

*Hình 15 – Chọn định dạng Volume*

Hoàn thành các bước trên là đã tạo thành công Volume.



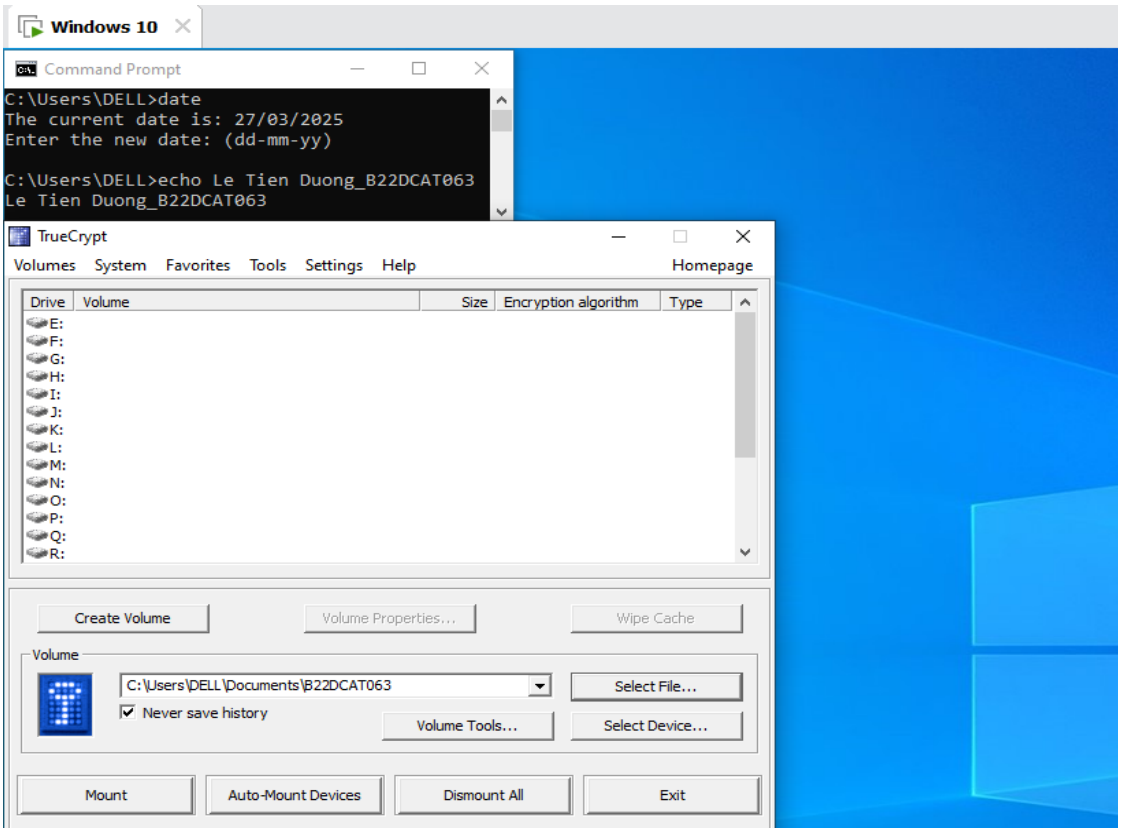

*Hình 16 – Tạo thành công Volume*

Thấy xuất hiện File B22DCAT063.



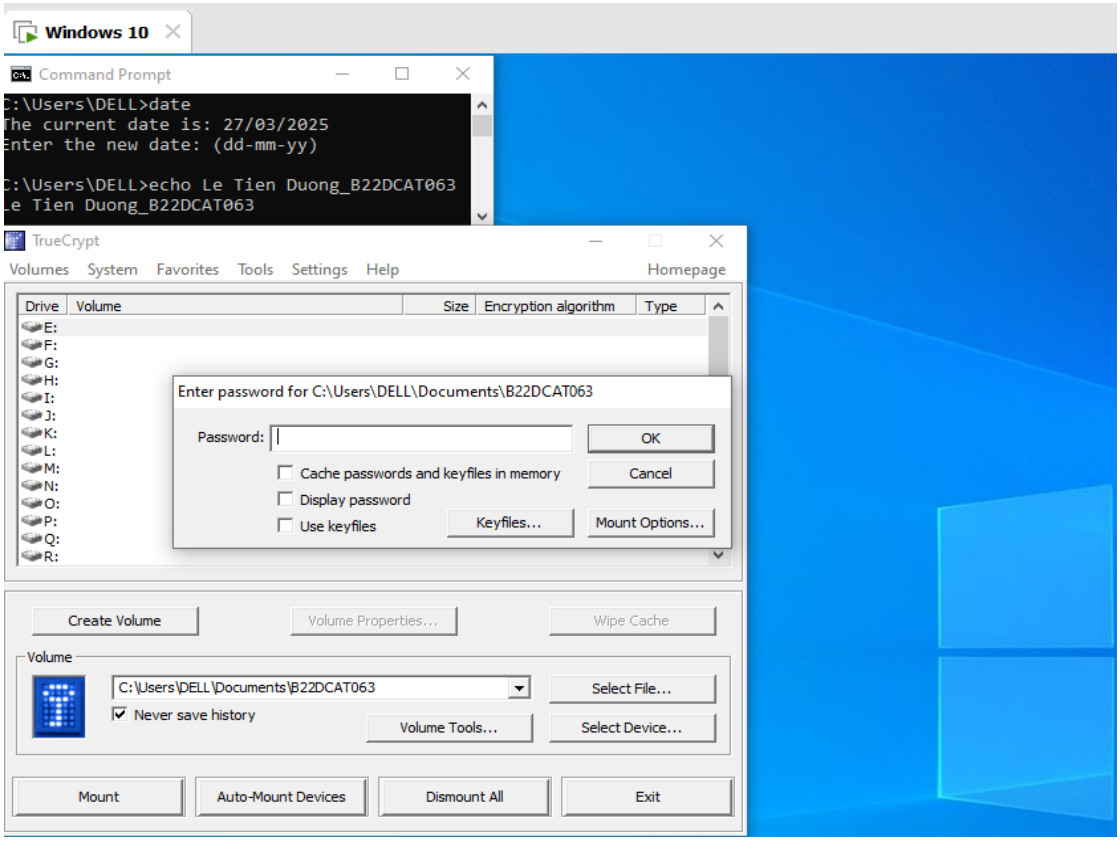

*Hình 17 – Xuất hiện File B22DCAT063*

Chọn Volume mới được tạo.



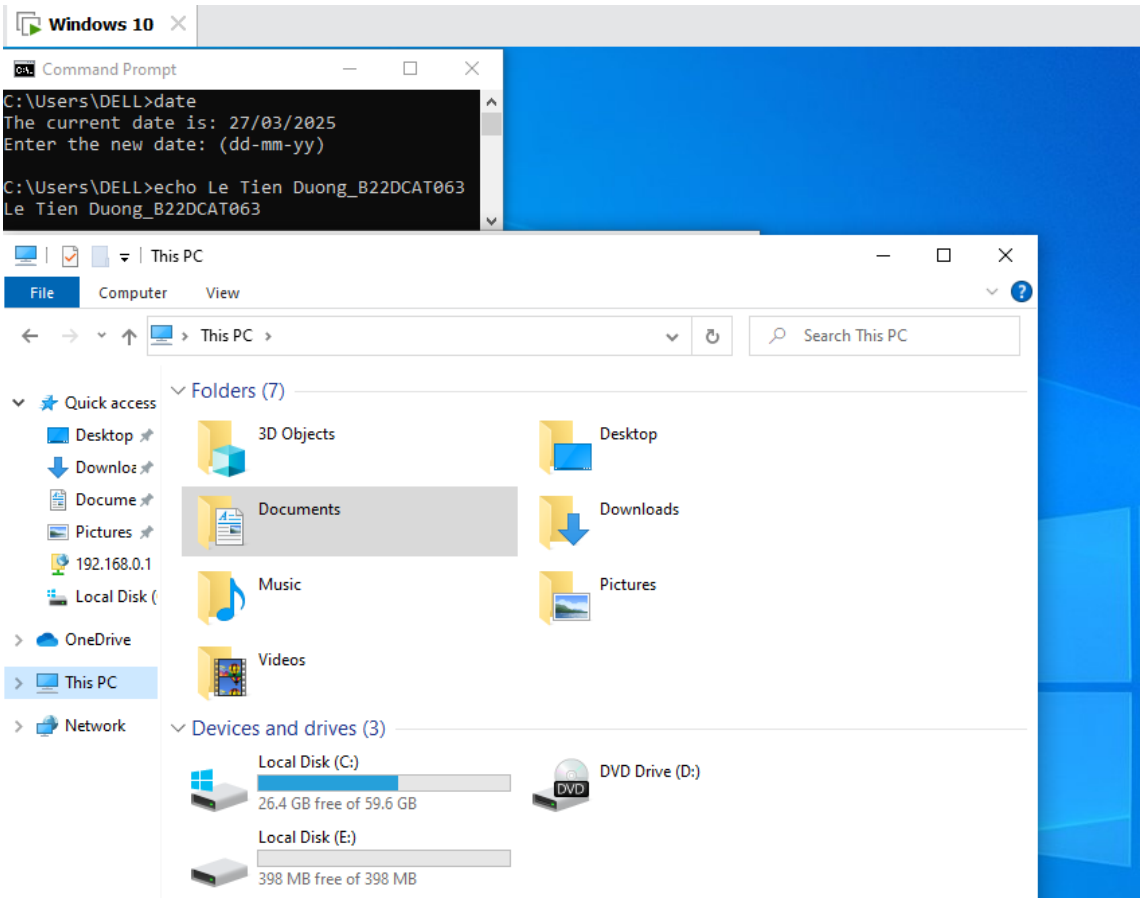

*Hình 18 – Chọn Volume vừa mới được tạo*

Nhập mật khẩu để mount Volume.



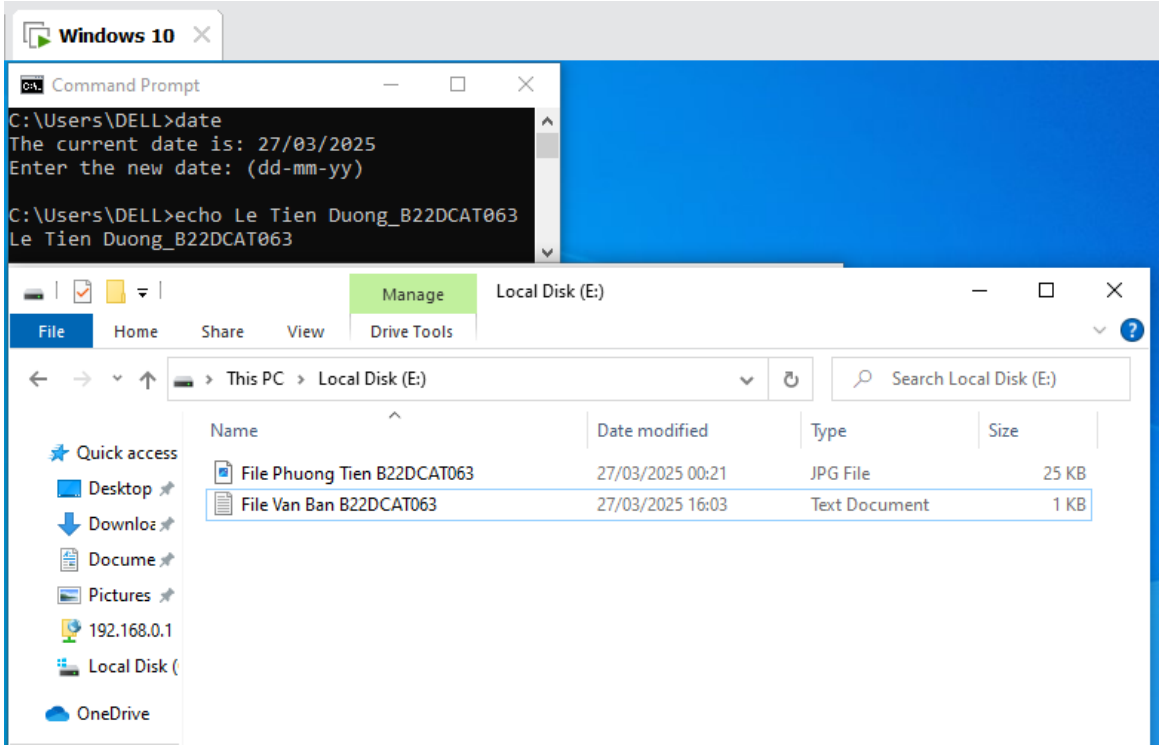

*Hình 19 – Nhập mật khẩu của Volume*

Sau đó một ổ đĩa mới sẽ được tạo ra.



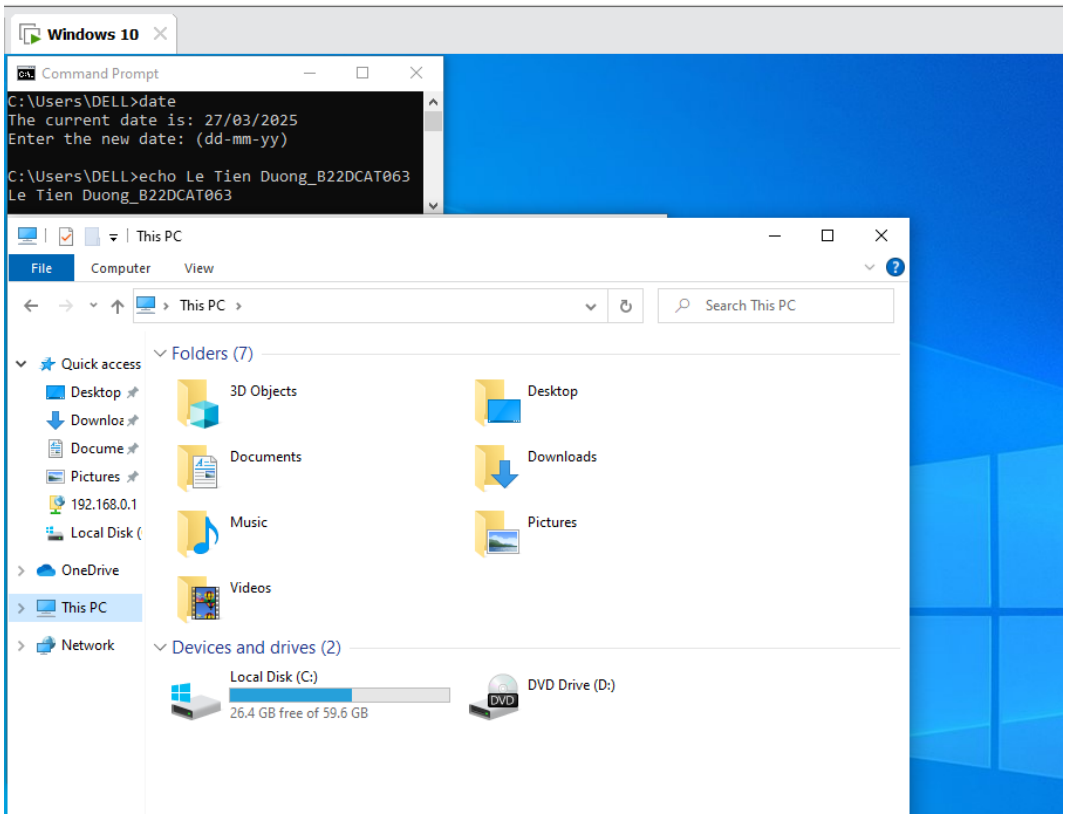

*Hình 20 – Tạo thành công một ổ đĩa mã hóa để lưu trữ các định dạng file, thư mục*

Di chuyển các file và tệp tin cần mã hóa vào trong Volume E.



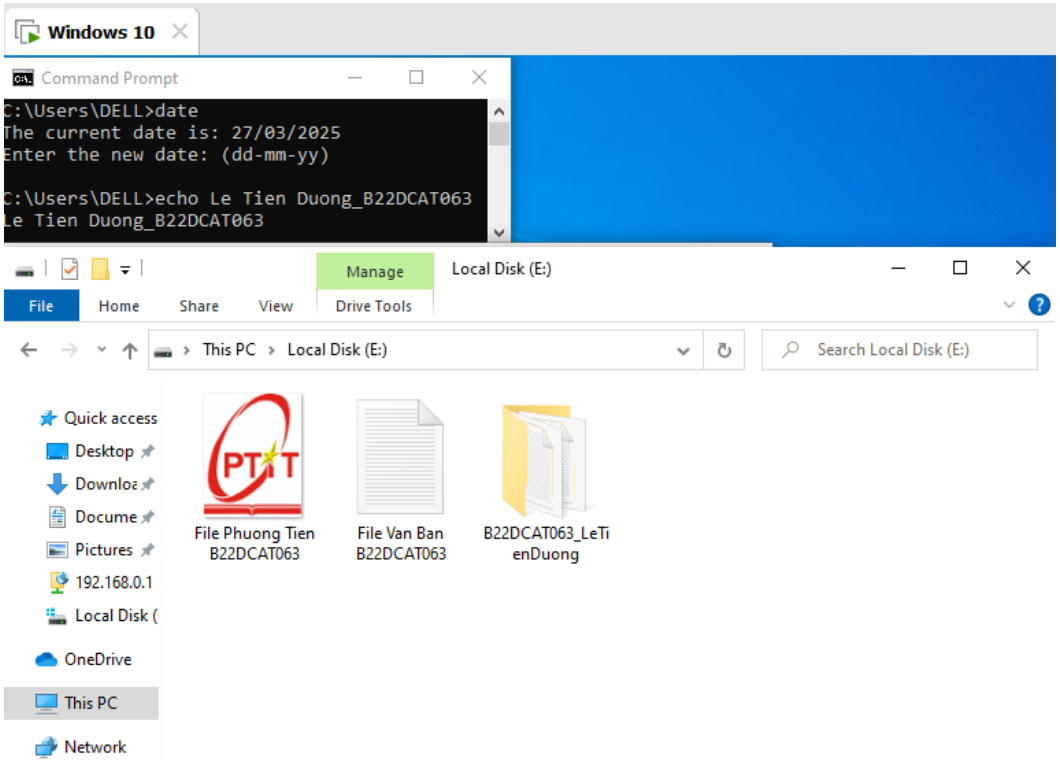

*Hình 21 – Đưa các file bài yêu cầu vào ổ đĩa mã hóa này*

Dismount ổ đĩa (đóng ổ đĩa) thì ta thấy ổ đĩa biến mất.



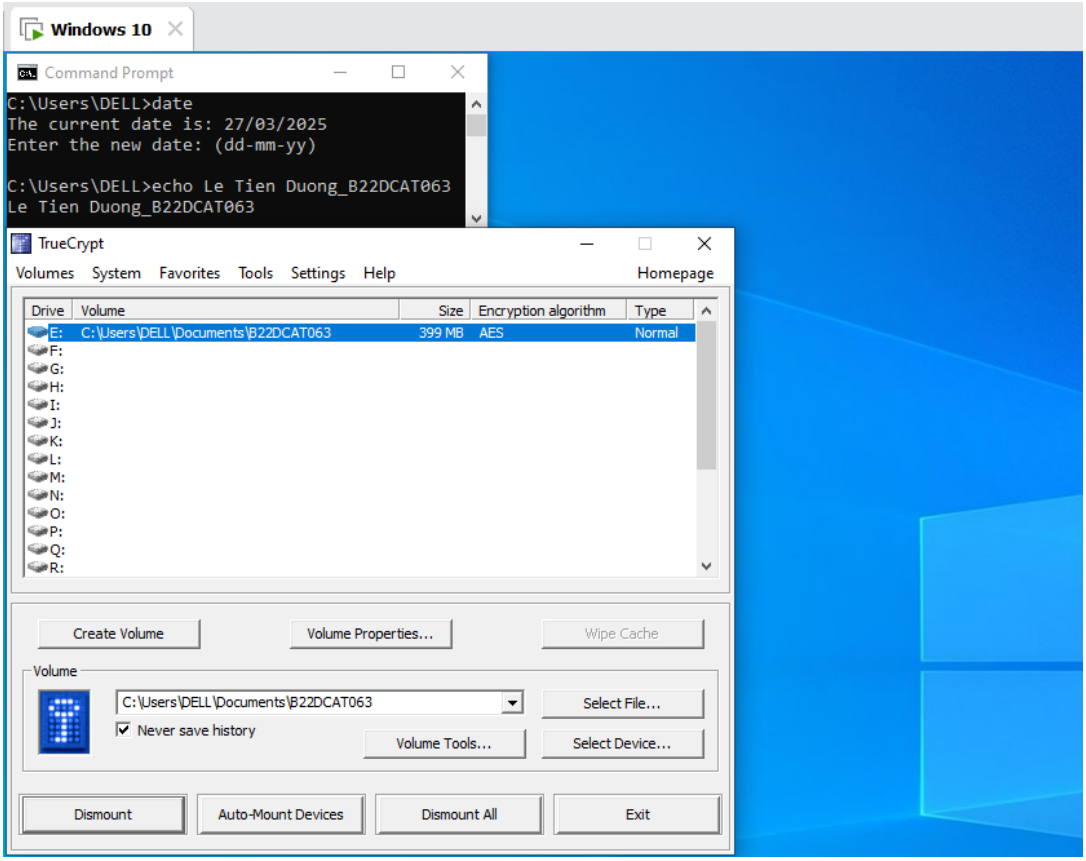

*Hình 22 – Dismount ổ đĩa (đóng ổ đĩa) để không ai có thể truy/xem/sửa được → ổ E biến mất*

*2.2.2.2 Sử dụng công cụ TrueCrypt để hóa thư mục. Đặt tên thư mục theo mã sinh viên và có chứa 1 số file khác nhau. Di chuyển thư mục cần mã hóa vào trong Volume E*



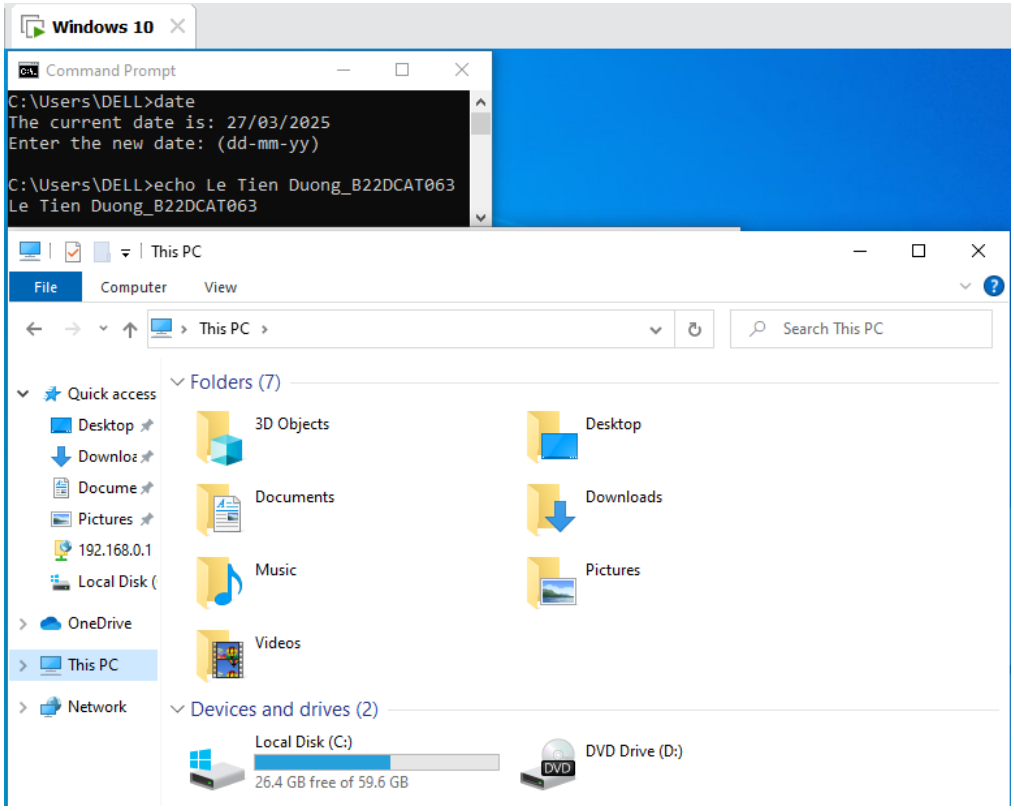

*Hình 23 – Di chuyển thư mục cần mã hóa vào ổ đĩa*

Chọn Volume đã tạo.




*Hình 24 – Chọn Volume đã tạo*

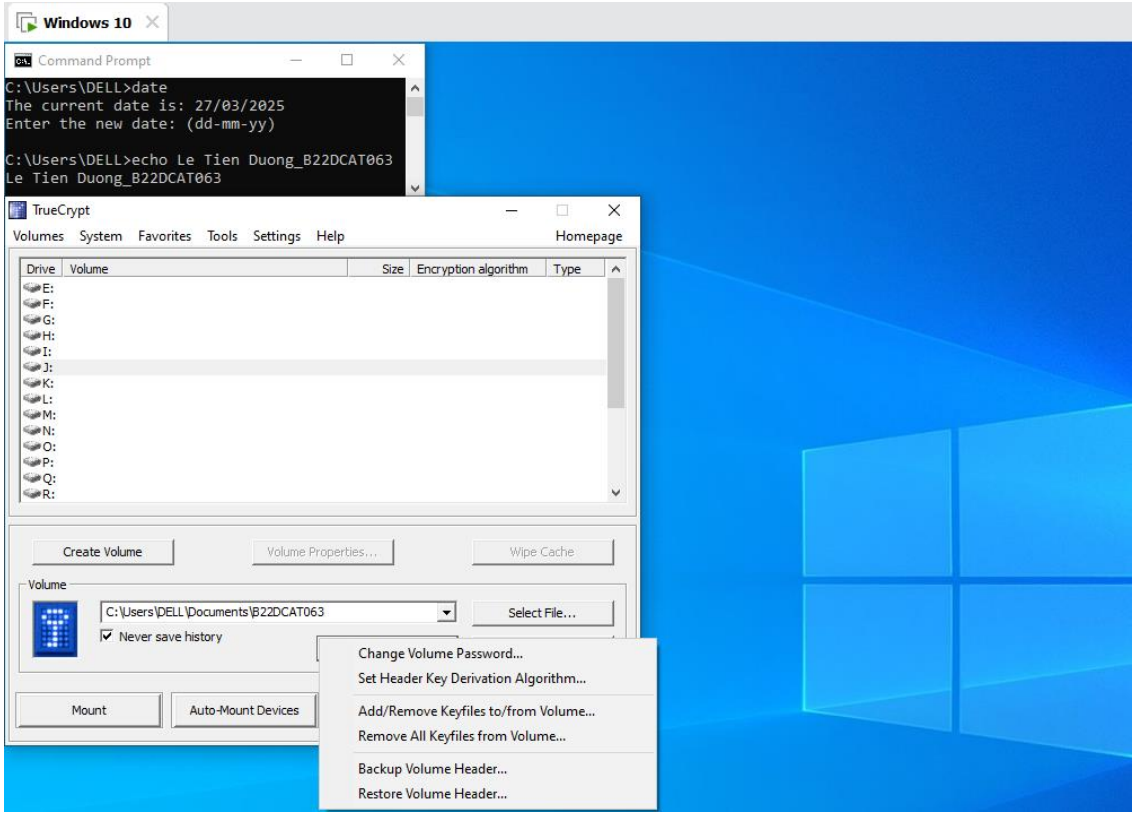
Dismount ổ đĩa (đóng ổ đĩa).




*Hình 25 – Đóng ổ đĩa -> Ổ đĩa biến mất*

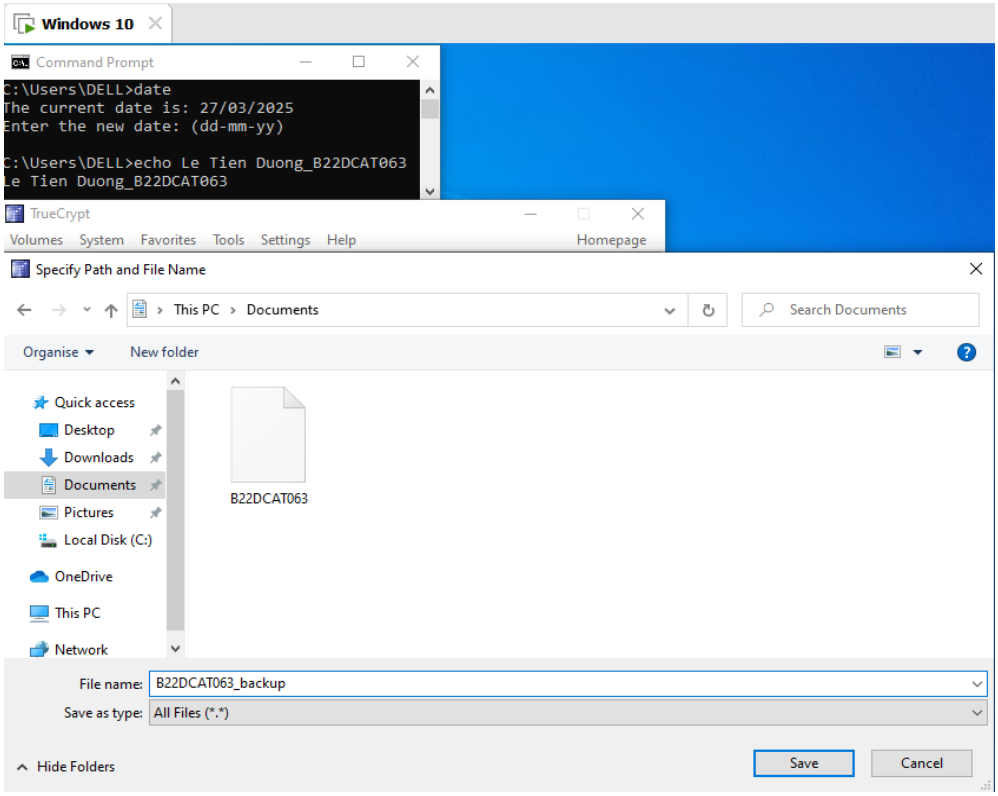
### *2.2.2.3 Sao lưu khóa mã hóa của công cụ TrueCrypt*

Trong TrueCrypt, chọn Volume Tools -> Backup Volume Header



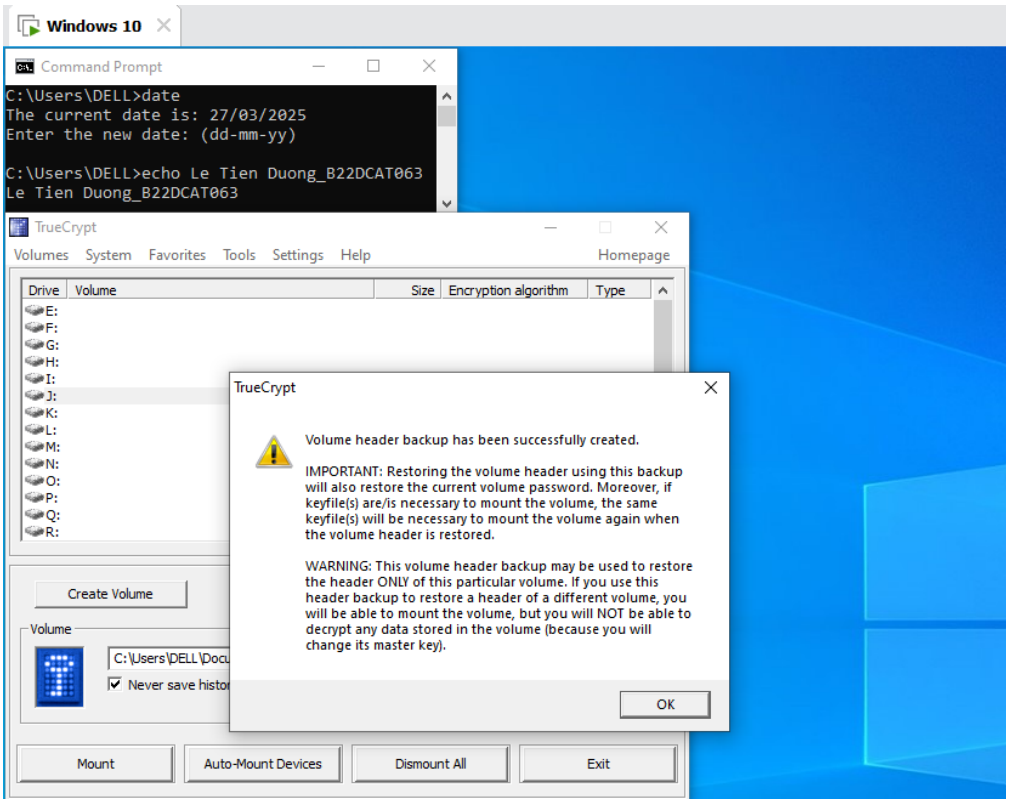

*Hình 26 – Chọn Backup Volume Header*

Đặt tên file.




*Hình 27 – Đặt tên file*

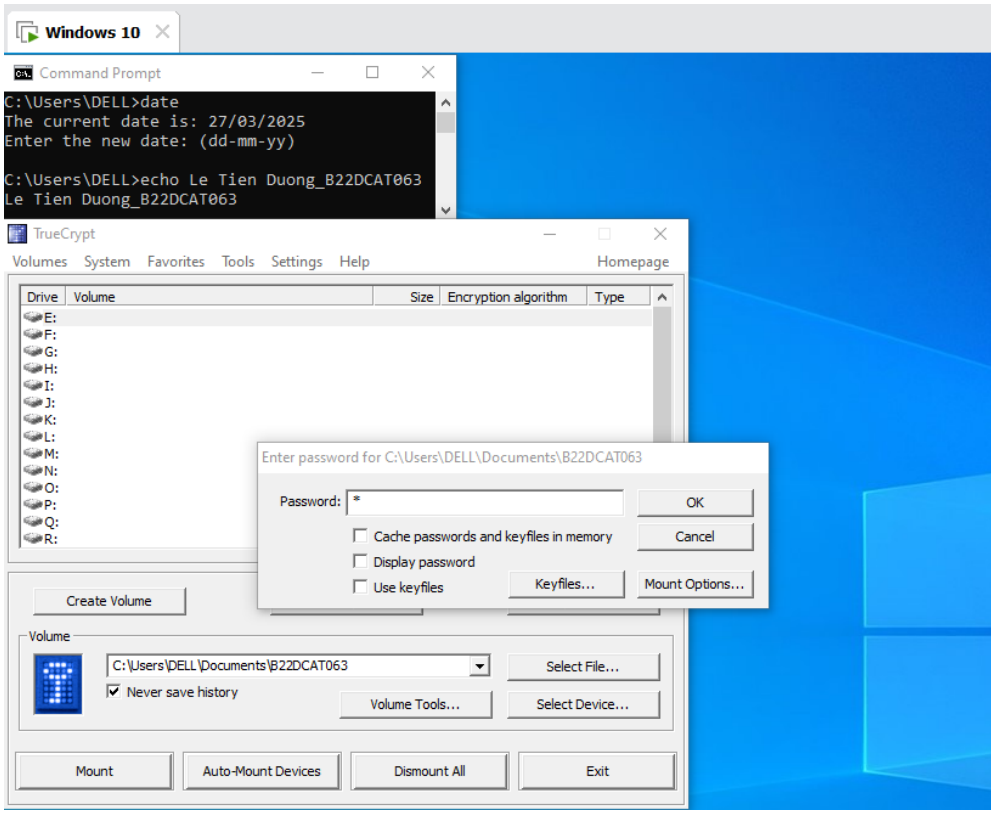
Tạo khóa mã hóa thành công



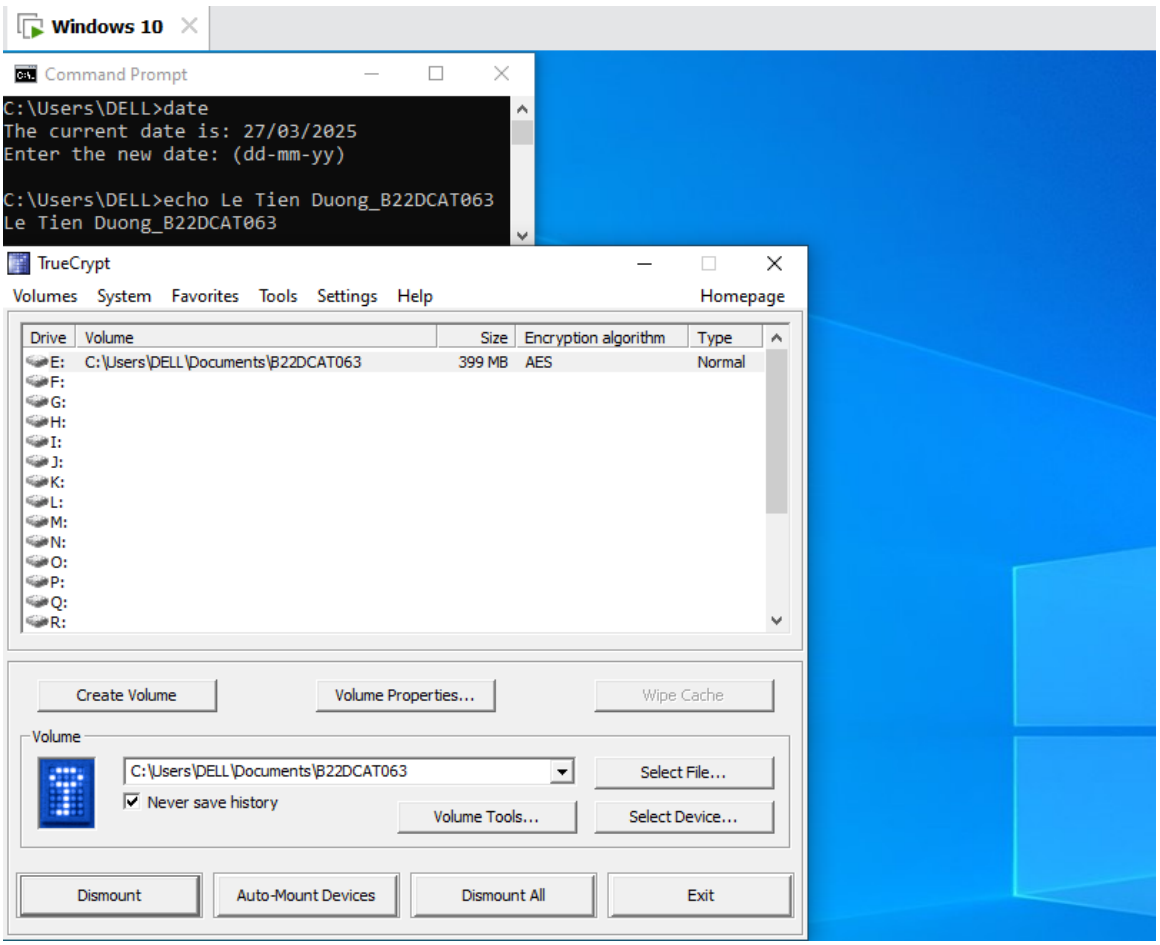

*Hình 28 – Tạo khóa mã hóa thành công*

*2.2.2.4 Sử dụng công cụ TrueCrypt để khôi phục các file và thư mục mã hóa*

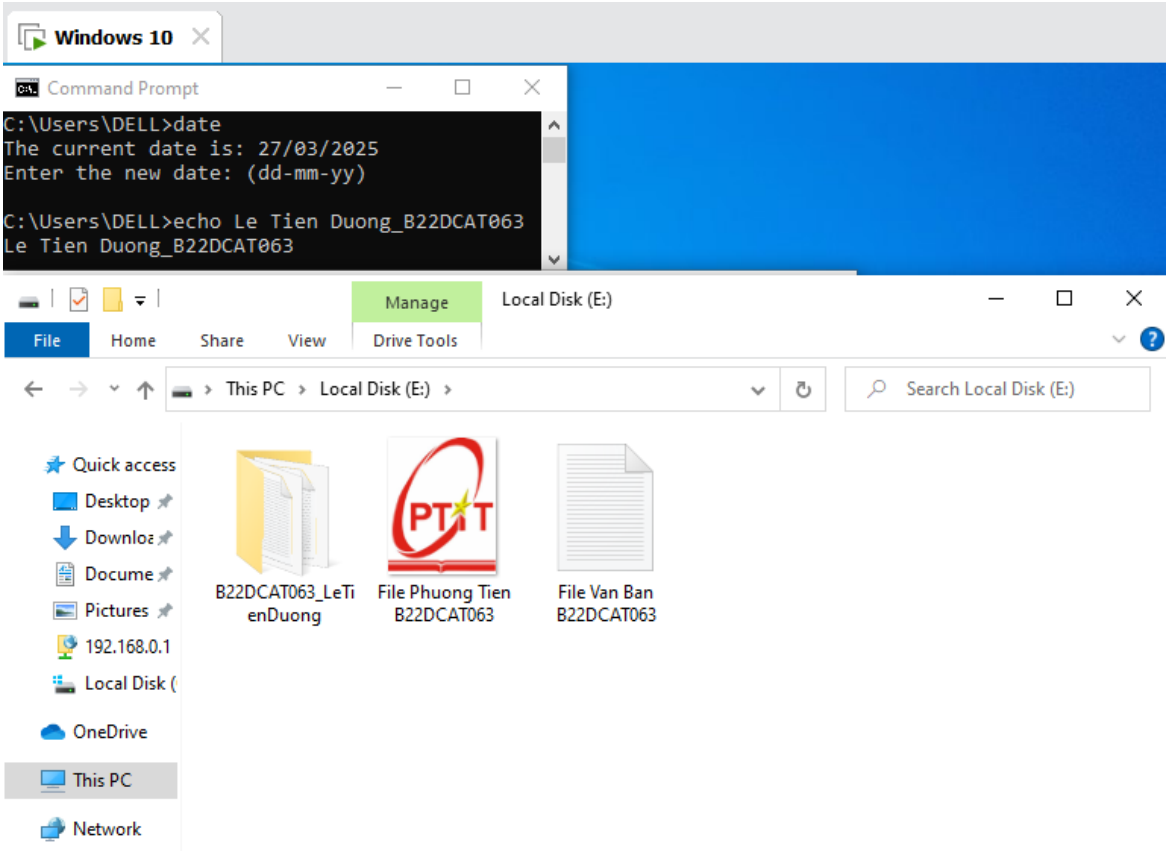
Ngưng mount Volume, nhập lại mật khẩu để khôi phục các file và thư mục mã hóa.




*Hình 29 – Nhập lại mật khẩu*




*Hình 30 – Xuất hiện ổ đĩa*




*Hình 31 – Các file và thư mục đã tạo được 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.