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


*Môn: Thực tập cơ sở*

*BÁO CÁO THỰC TẬP CƠ SỞ*

# Bài 8: Đảm bảo an toàn với mã hoá

| | |
|---|---|
| *Họ và tên giảng viên:* | *PGS.TS.Đỗ Xuân Chợ* |
| *Họ và tên:* | *Phạm Thanh Tùng* |
| *Mã sinh viên:* | *B20DCAT171* |
| *Lớp:* | *D20CQAT03-B* |
| *Số điện thoại:* | *0956915668* |

*Hà Nội 2023*

1. Nội dung lý thuyết

a. lý thuyết về công cụ TrueCrypt.

TrueCrypt là một tiện ích phần mềm miễn phí mã nguồn mở được sử dụng để mã hóa tập tin,hỗ trợ các hệ điều hành Windows, MacOS và Linux. Nó có thể tạo một đĩa được mã hóa ảo trong một tệp hoặc mã hóa một phân vùng hoặc toàn bộ thiết bị lưu trữ. 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. TrueCrypt hỗ trợ xử lý mã hóa đa luồng các hệ thống đa lõi. Trên các bộ xử lý mới hơn hỗ trợ AES-NI, TrueCrypt hỗ trợ tăng tốc phần cứng cho mã hóa AES để cải thiện hơn nữa hiệu suất. Tác động hiệu suất của mã hóa đĩa đặc biệt đáng chú ý đối với các hoạt động thường sử dụng truy cập bộ nhớ trực tiếp (DMA), vì Tất cả dữ liệu phải truyền qua CPU để giải mã, thay vì được sao chép trực tiếp từ đĩa sang RAM.

TrueCrypt ban đầu được phát hành dưới dạng phiên bản 1.0 vào tháng 2 năm 2004, dựa trên phần mềm E4M. Một số phiên bản và nhiều bản phát hành nhỏ bổ sung đã được thực hiện kể từ đó, với phiên bản mới nhất là 7.1a. Vào ngày 28 tháng 5 năm 2014, trang web TrueCrypt đã thông báo rằng dự án không còn được duy trì và người dùng khuyến nghị tìm thấy các giải pháp thay thế. Về thuật toán mã hóa, các thuật toán mã hóa được hỗ trợ bởi TrueCrypt là AES, Serpent và Twofish. Ngoài ra, có 5 tổ hợp phương thức mã hóa chồng là: AES-Twofish, Aes-Twofish-Serpent, Serpent-Aes, Serpent-Twofish-AES và Twofish-Serpent. Các hàm băm có sẵn để sử dụng trong TrueCrypt là RIPEMD-160, SHA-512 và Whirlpool. TrueCrypt hỗ trợ một khái niệm gọi là từ chối hợp lý, bằng cách cho phép một "volume ẩn" duy nhất được tạo trong một tập tập khác. Ngoài ra, các phiên bản Windows của TrueCrypt có khả năng tạo và chạy một hệ điều hành được mã hóa ẩn mà không bị phát hiện. Khi gắn một volume được mã hóa hoặc khi thực hiện xác thực trước khi khởi động hệ thống, các bước sau được thực hiện:

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

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.

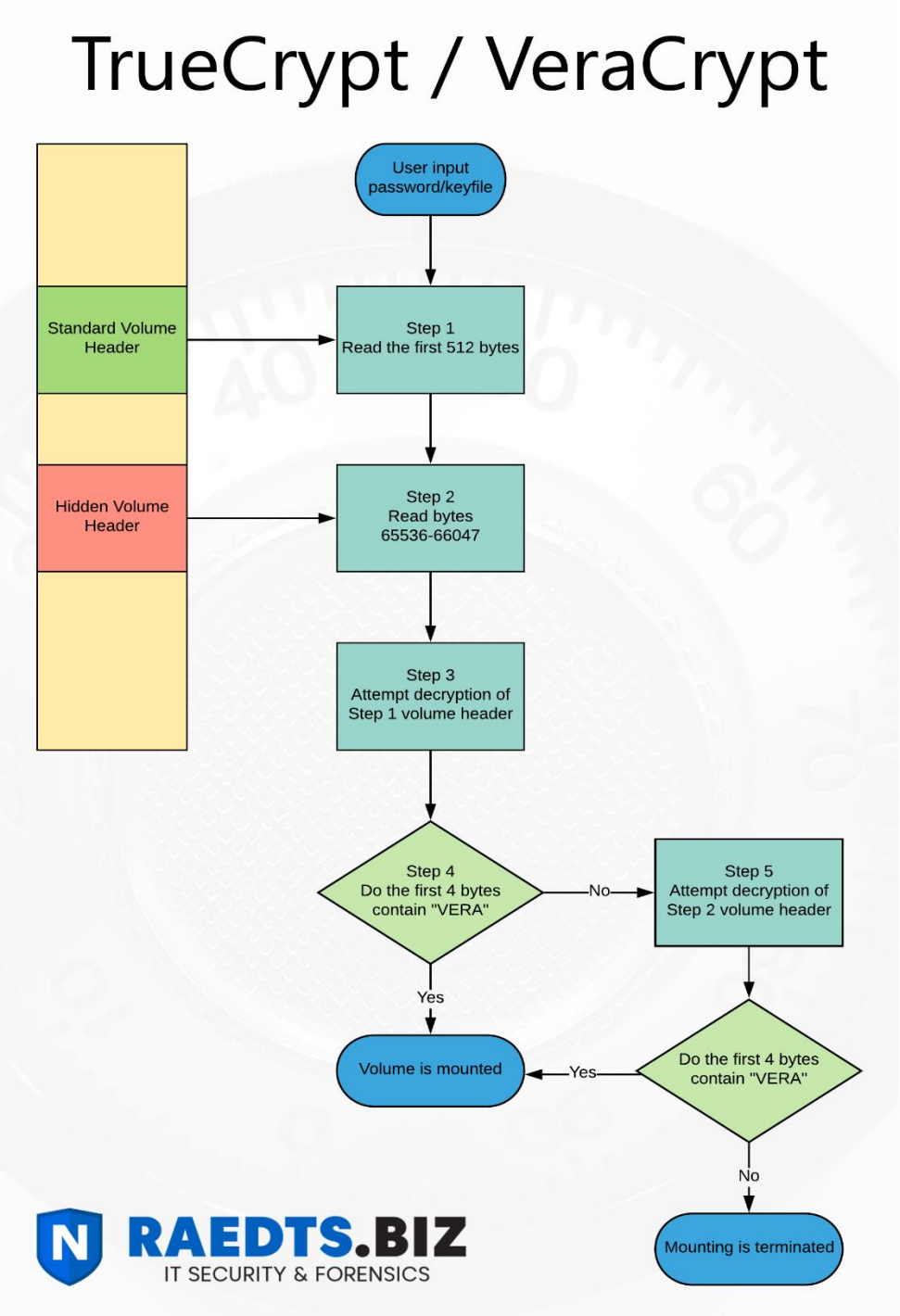
Bước 2: Các byte 65536->66047 của volume được đọc thành RAM. Đối với mã hóa hệ thống, byte 65536->66047 của phân vùng đầu tiên nằm phía sau phân vùng hoạt động được 1 đọc.

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.

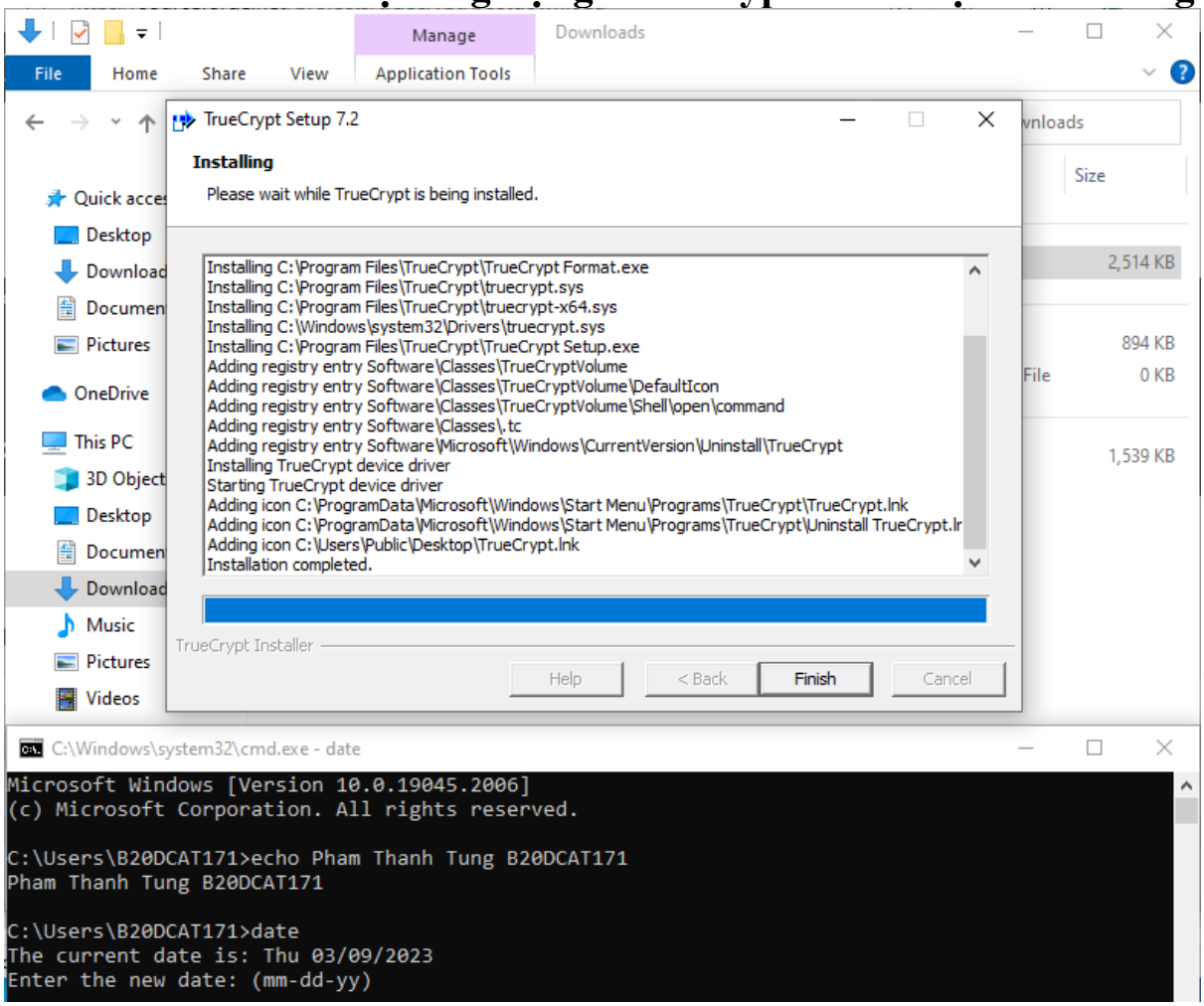
Bước 4: Nhập mật khẩu Mật khẩu được nhập bởi người dùng và salt được đọc trong bước 1 được chuyển đến hàm dẫn xuất khóa tiêu đề, tạo ra một chuỗi các giá trị mà từ đó khóa mã hóa tiêu đề và khóa tiêu đề thứ cấp (chế độ XTS) được hình thành. Các khóa này được sử dụng để giải mã tiêu đề volume.

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

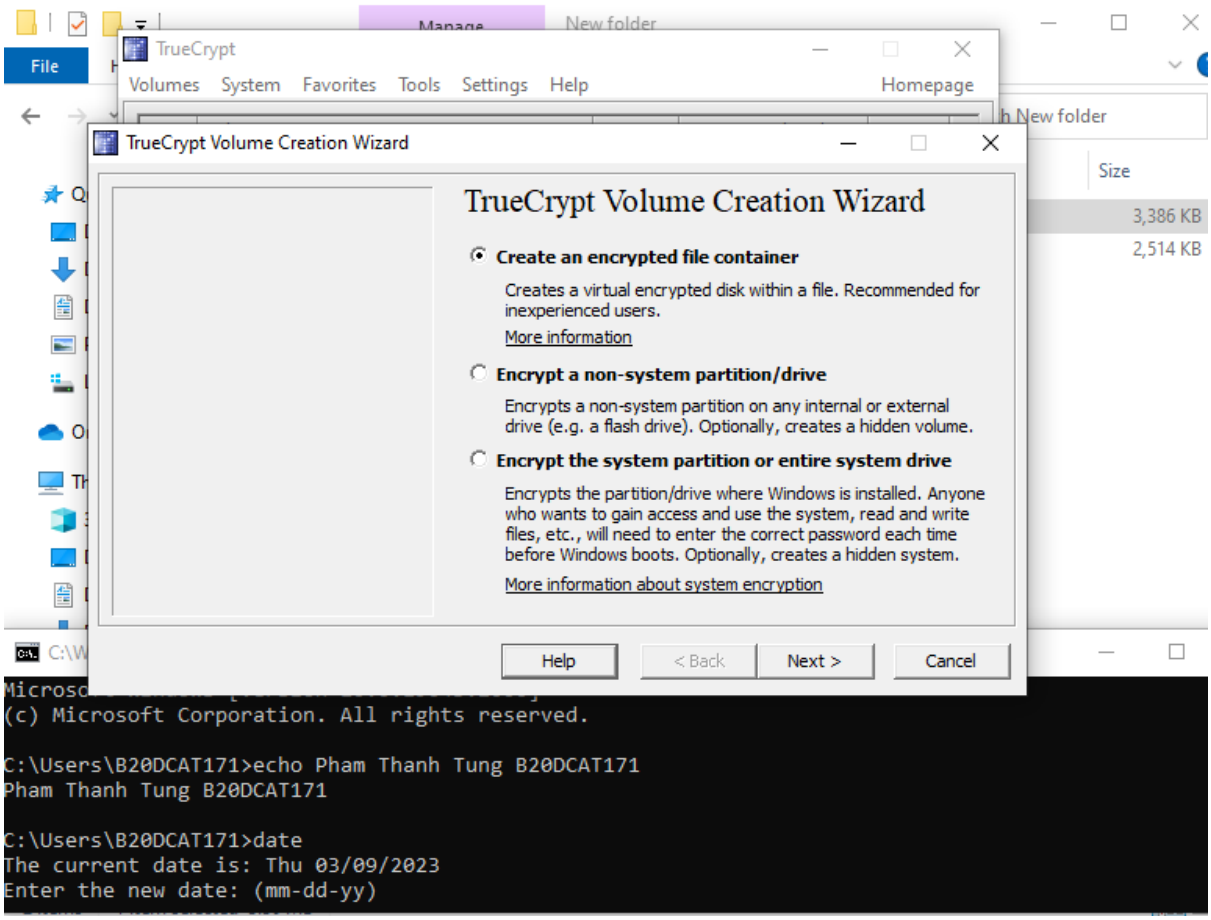


2. Nội dung thực hành

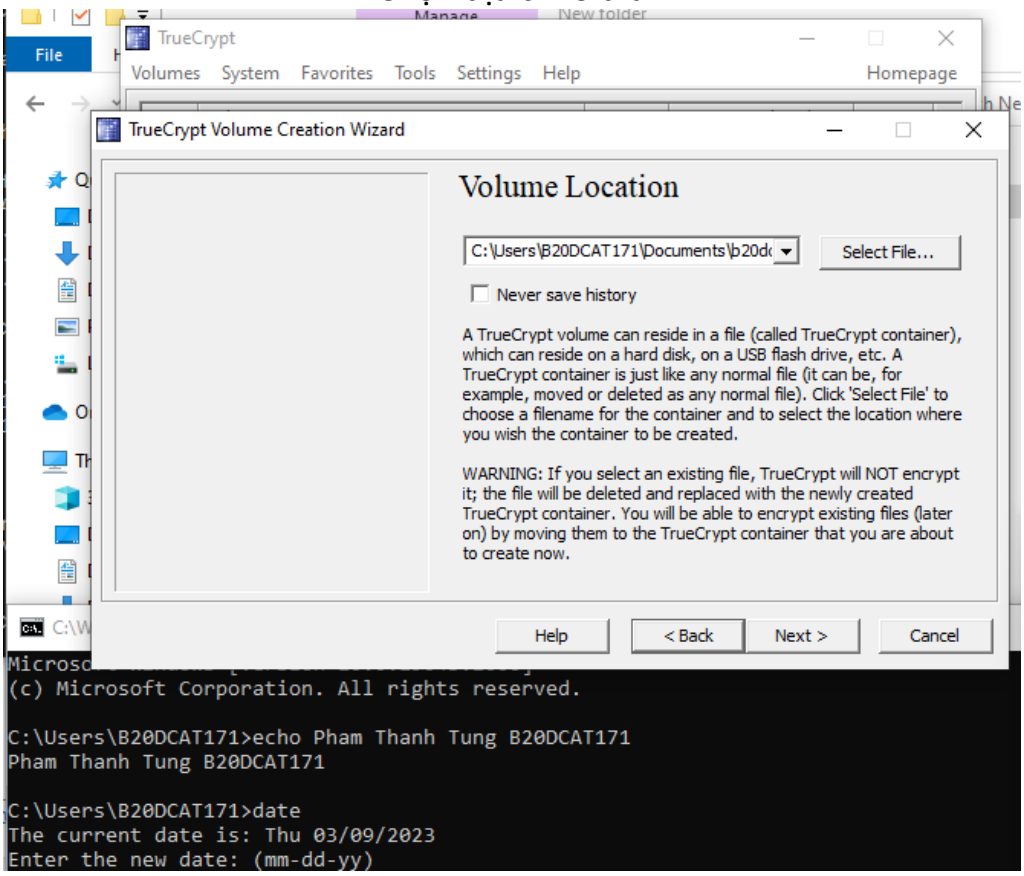
**Tải về file cài đặt ứng dụng TrueCrypt và cài đặt thành công**



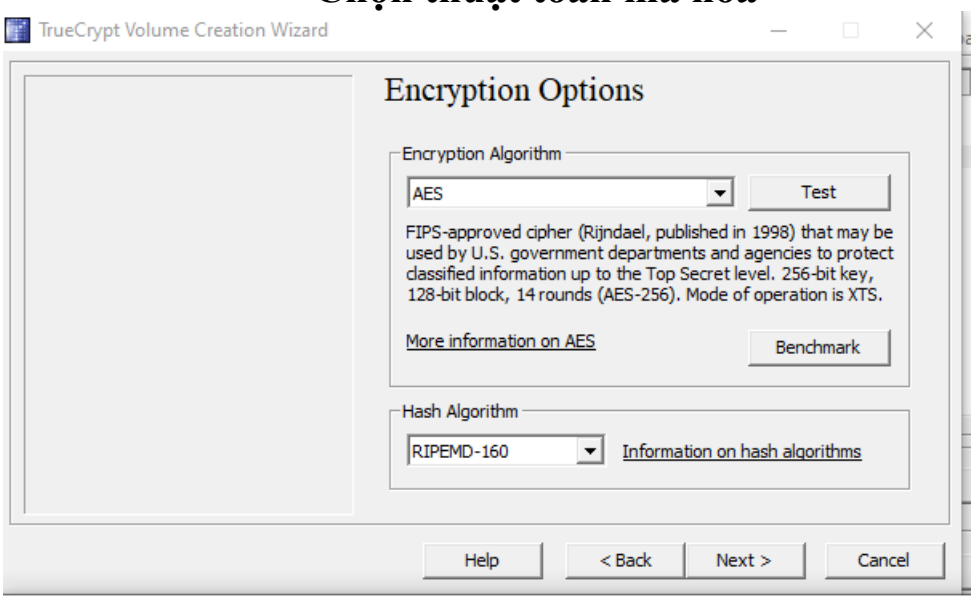

**Tạo volume chứa dữ liệu được mã hóa**

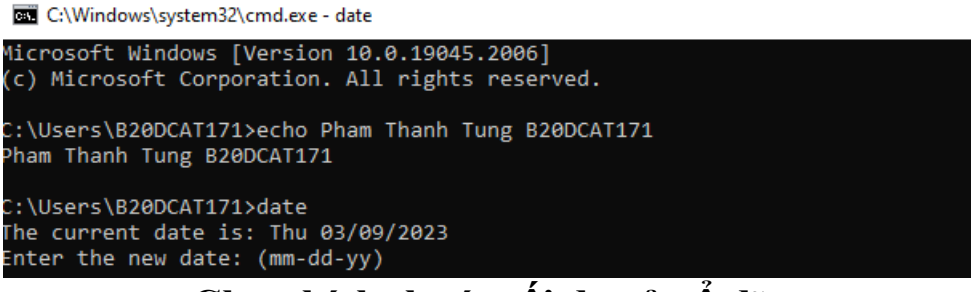



Chọn địa chỉ ổ đĩa

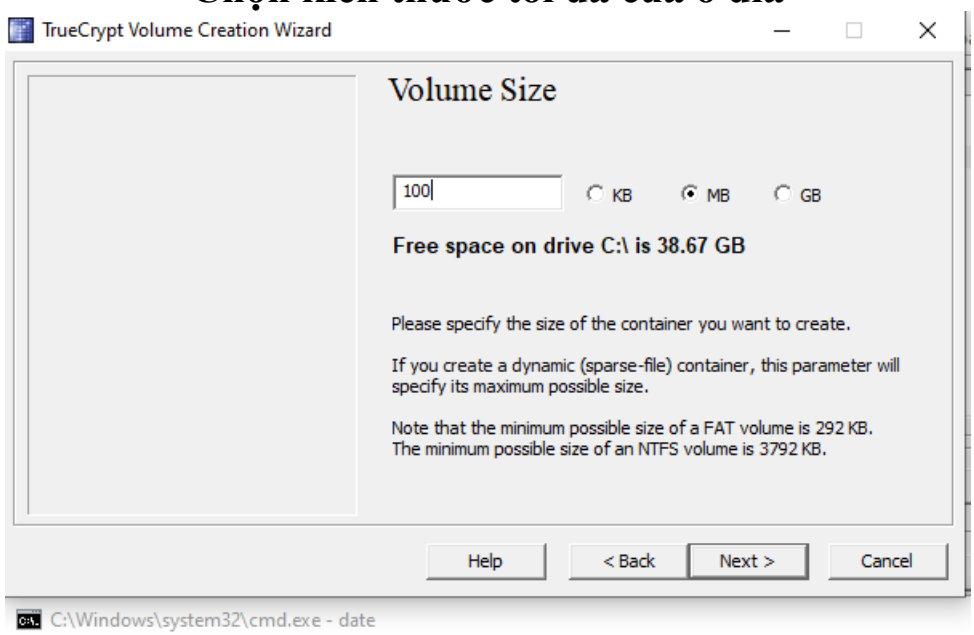


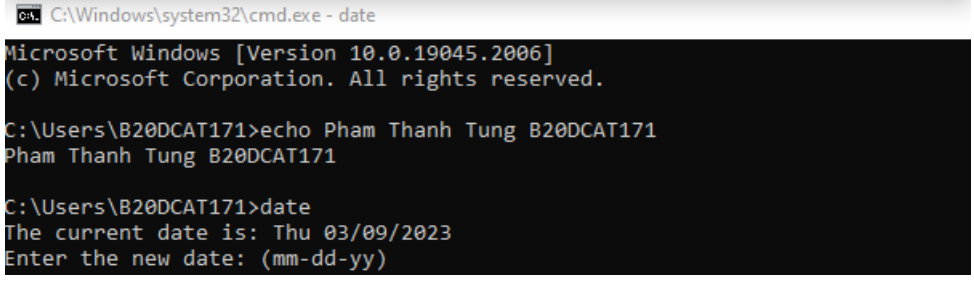
# Chọn thuật toán mã hóa



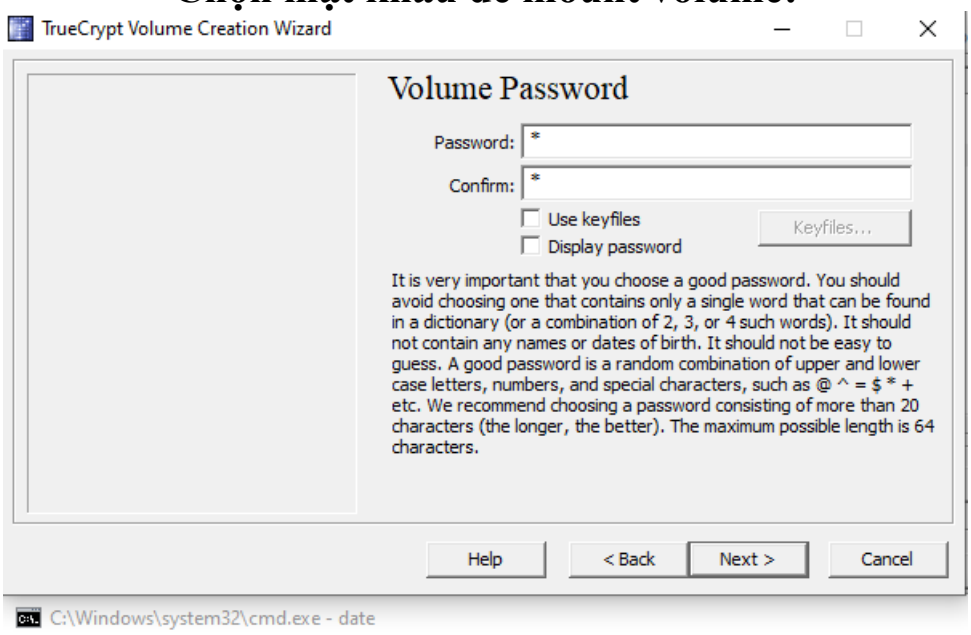



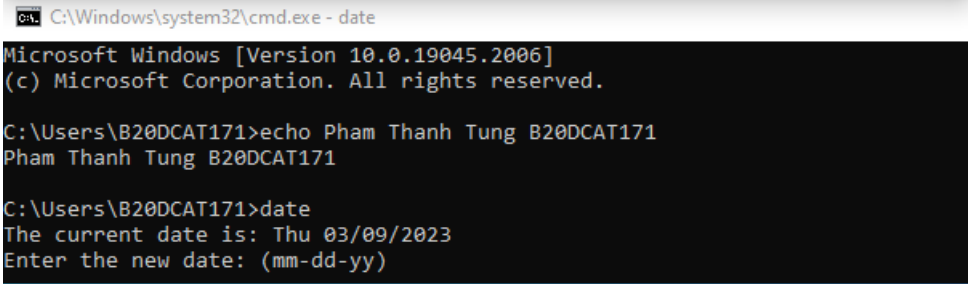

# Chọn kích thước tối đa của ổ đĩa



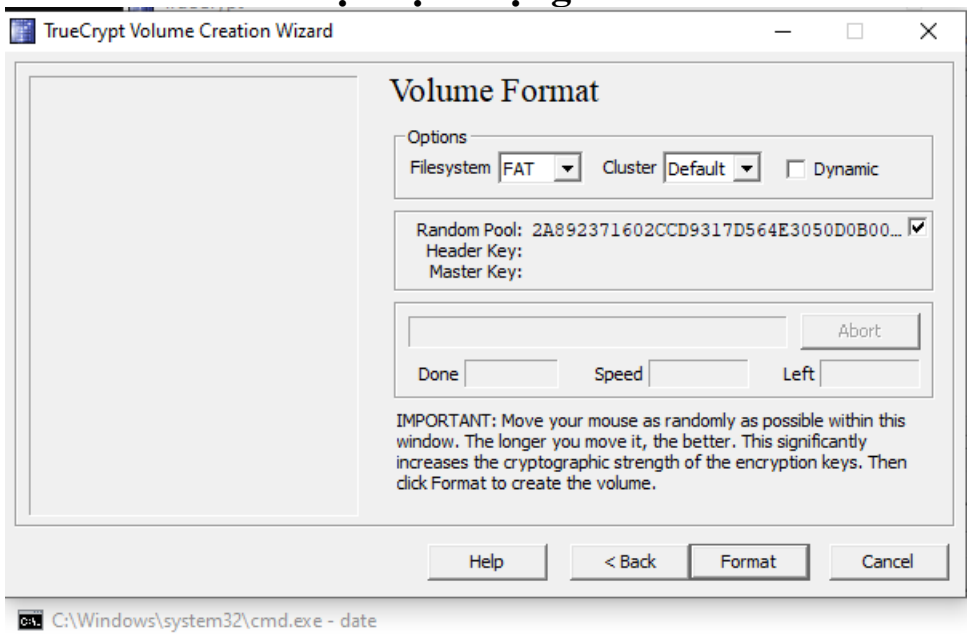



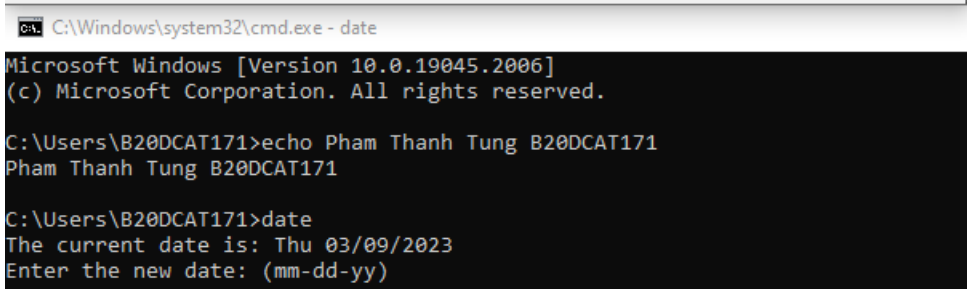
# Chọn mật khẩu để mount volume:



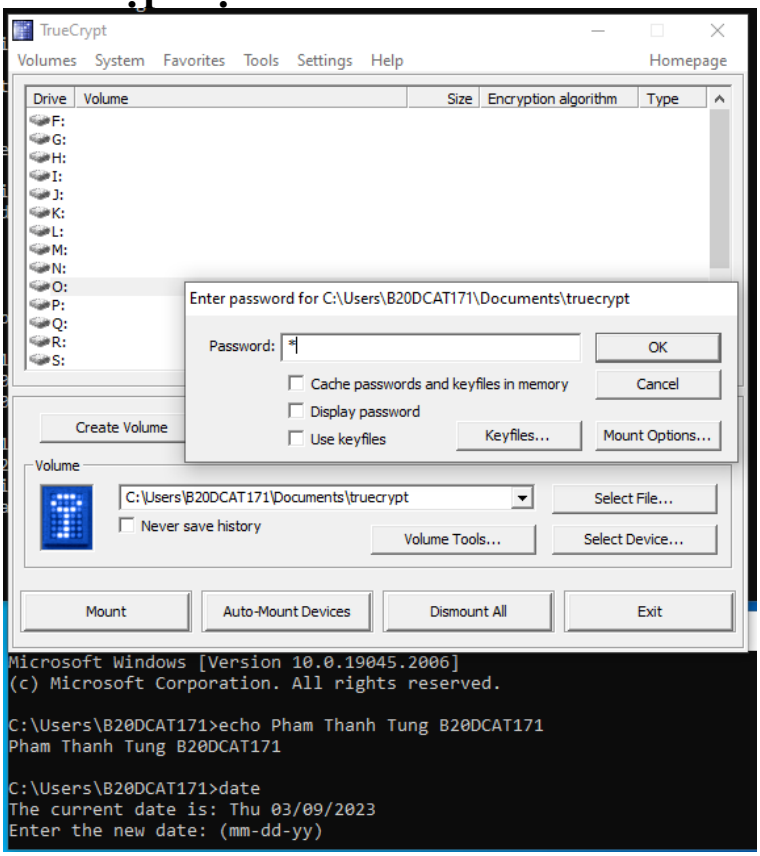




# Chọn định dạng của volume

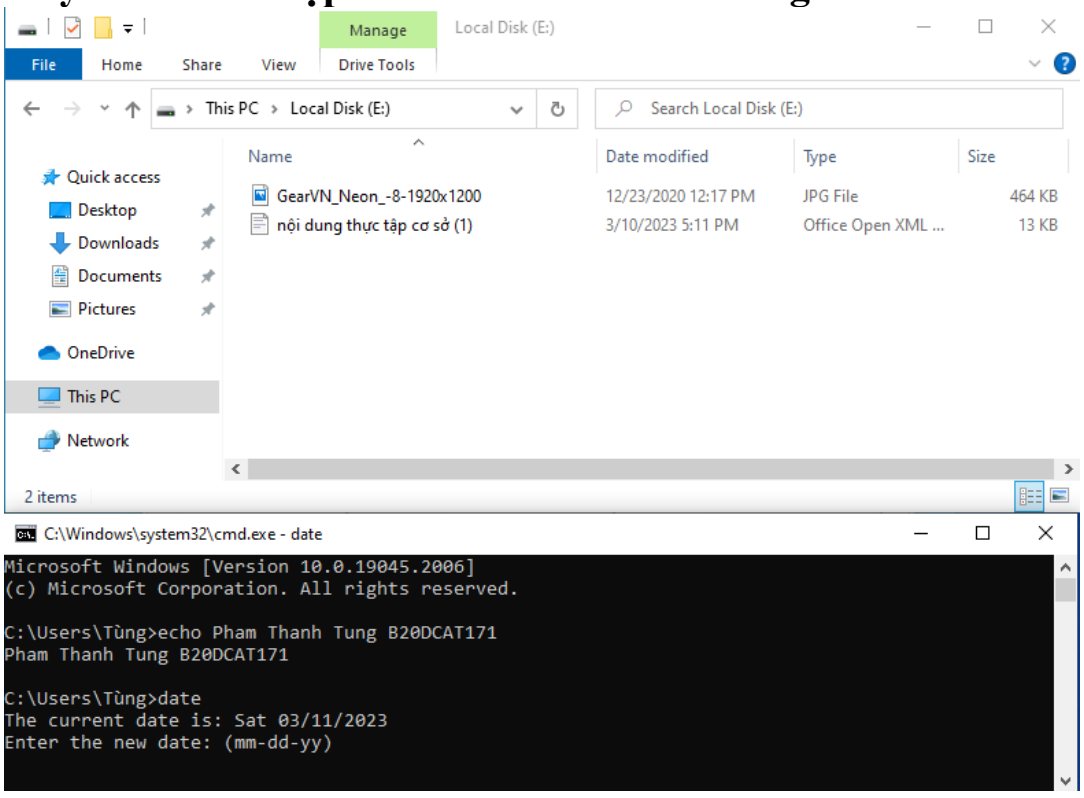


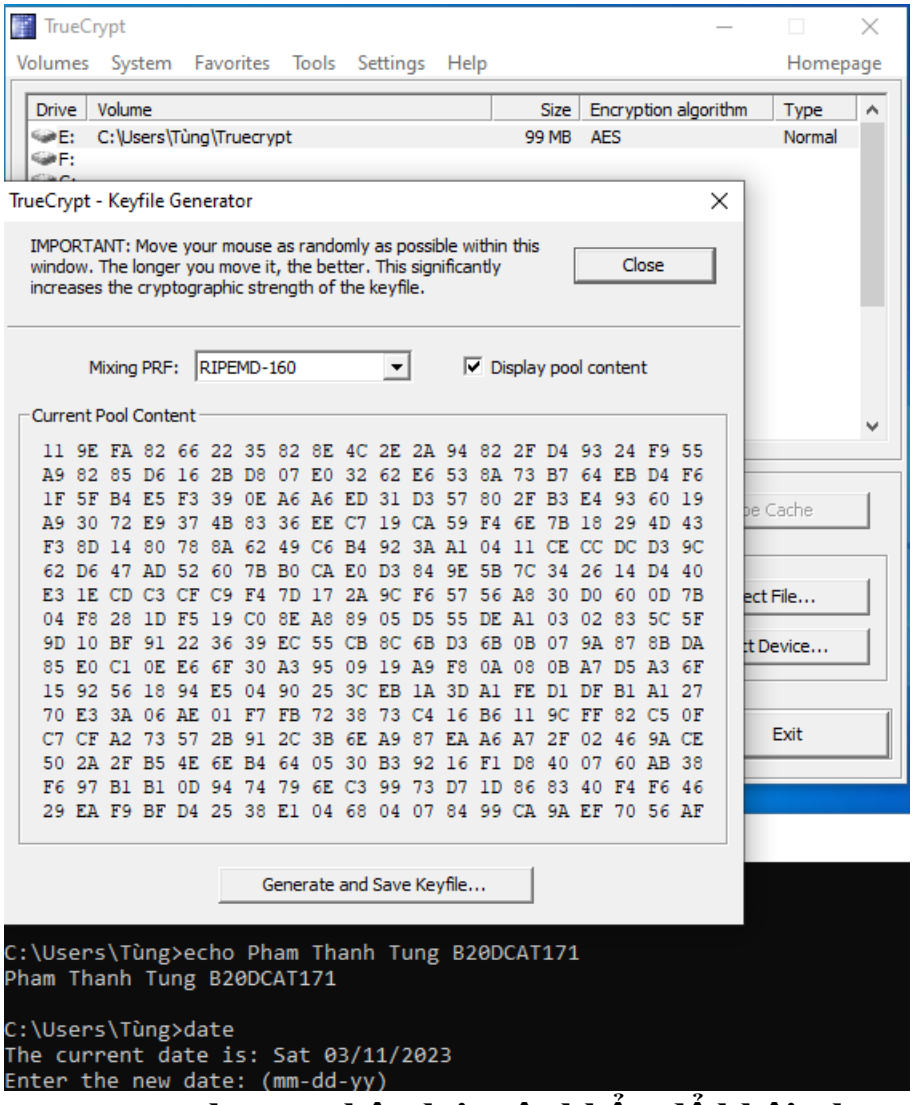
# Nhập mật khẩu để mount volume:



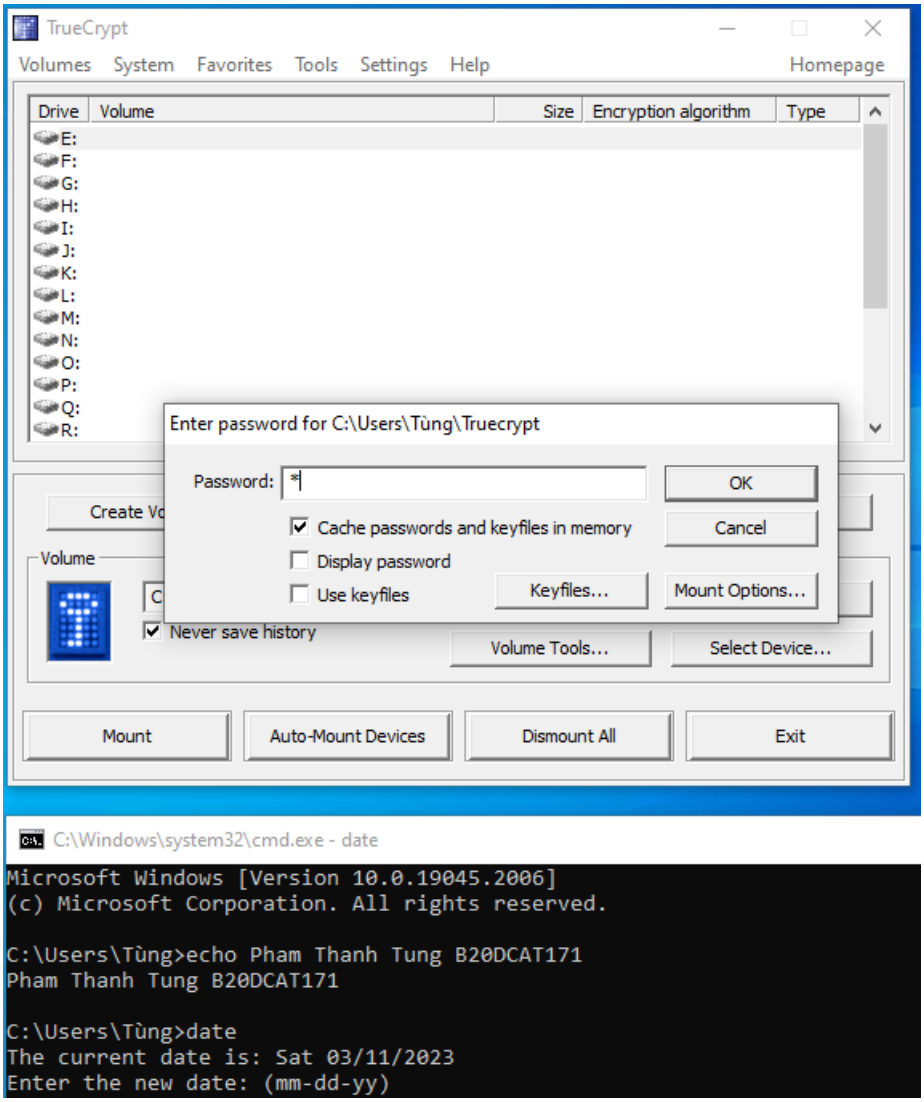

# Di chuyển 2 file và tập tin cần mã hóa vào trong volume:



**Sao lưu khóa mã hóa**




**Ngừng mount volume, nhập lại mật khẩu để khôi phục các file và thư mục mã hóa.**




# Khôi phục file và thư mục thành công