**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN 1**

****

**Môn: THỰC TẬP CƠ SỞ**

**BÁO CÁO BÀI THỰC HÀNH SỐ 13**

**Họ và tên sinh viên:**

**Đỗ Tiến Sĩ**

**Mã số sinh viên:**

**B20DCAT153**

**Bài 13: Đảm bảo an toàn mã hóa.**

**Họ và tên giảng viên:**

**Thầy :Đỗ Xuân Chợ**

**Hà Nội 3/2023 (tháng/năm)**

**Đảm bảo an toàn với mã hóa**

**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

**2. Nội dung thực hành**

**2.1 Tìm hiểu lý thuyết**

**2.1.1 Mô tả ngắn gọn lý thuyết về công cụ TrueCrypt**

- TrueCrypt là một chương trình phần mềm dành cho hệ điều hành Windows, nó cho phép người dùng tạo một hoặc nhiều ổ đĩa ảo trên máy tính nhằm giúp người dùng ghi các dữ liệu như video, game, nhạc, chương trình ứng dụng lên đó mà không phải tốn quá nhiều thời gian, công sức cũng như tiền bạc. TrueCrypt tạo nên một vùng ổ đĩa ảo trong đó bạn có thể lưu, xóa hoặc mở các tập tin khi mà người khác không thể. Đây là biện pháp bảo vệ an toàn cho bạn trong trường hợp ổ đĩa cứng của bạn gặp vấn đề khiến các file dữ liệu trên máy tính có nguy cơ bị mất, hoặc sự tấn công nhằm ăn cắp các tài khoản cá nhân quan trọng của bạn từ các hacker máy tính

- Cơ chế thiết lập và quản lý của TrueCrypt là mã hóa ổ đĩa trên đường đi (on-

the-fly encrytion). 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 (encrytion volume) không thể đọc được nếu người dùng không cung cấp đúng khóa mã hóa bằng một trong 3 hình thức như: mật khẩu (password), 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 ...)

**2.1.2 Mô tả cách thức hoặc phương pháp công cụ TrueCrypt áp dụng để mã hóa file hoặc thư mục**

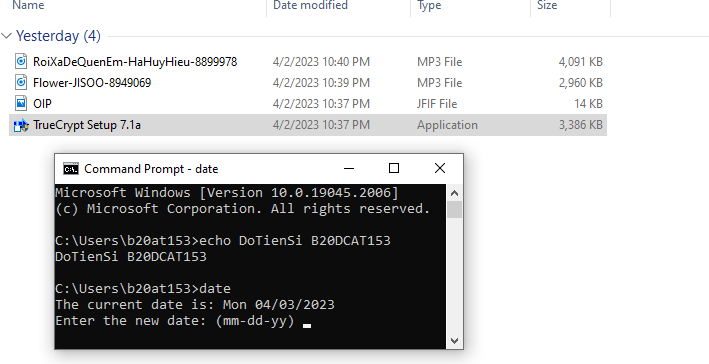
- Các tệp có thể được sao chép vào và từ một ổ đĩa TrueCrypt được gắn kết giống như chúng được sao chép vào từ bất kỳ đĩa thông thường nào (ví dụ: bằng các thao tác kéo thả đơn giản). các tệp sẽ tự động được giải mã một cách nhanh chóng(trong bộ nhớ/ RAM) khi chúng đang được đọc hoặc sao chéptừ một ổ đĩa TrueCrypt được mã hóa. Tương tụ, các tệp đang được ghi hoặc sao chép vào ổ đĩa TrueCrypt sẽ tự động được mã hóa ngay lập tức (ngay trước khi chúng được ghi vào đĩa) trong RAM. Lưu ý rằng điều này không có nghĩa là toàn bộ tệp tin sẽ được mã hóa/ giải mã phải được lưu trữ trong RAM trước khi nó có thể được mã hóa/ giải mã. TrueCrypt không bao giờ lưu dữ liệu chưa được mã hóa vào ổ đĩa, dữ liệu được mã hóa luôn được lưu trong RAM. Đây là một phương án rất an toàn ngăn chặn việc vô tình truy cập vào các tệp của người dùng.

- Khi gắn ổ đĩa TrueCrypt hoặc khi thực hiện xác thực trước khi khởi động, các bước sau được thực hiện.

* Bước 1: 512 bytes đầu tiên của ổ đĩa (tức là header ổ đĩa tiêu chuẩn) được đọc vào RAM, trong đó 64 bytes đầu tiên là salt (xem thông số kỹ thuật định dạng ổ đĩa TrueCrypt)
* Bước 2: Các byte 65536-66047 của ổ đĩa được đọc vào RAM. Nếu có một ổ ẩn trong ổ này (hoặc trong phân vùng phía sau phân vùng khởi động), nó đã đọc header của nó tại thời điểm này, nếu không, nó vừa đọc dữ liệu ngẫu nhiên (có hay không một tập đĩa ẩn bên trong nó phải được xác định bằng cách cố giải mã dữ liệu này)
* Bước 3: Bây giờ TrueCrypt cố gắng giải mã header ổ đĩa tiêu chuẩn được đọc trong bước. Tất cả dữ liệu được sử dụng vào tạo ra trong quá trình giải mã được lưu trong RAM (truecrypt không bao giờ lưu chúng vào đĩa). Các thông số sau là không xác định thông qua quá trình thử và sai.
* Bước 4: Giải mã được coi là thành công nếu 4 bytes đầu tiên của dữ liệu được giải mã chứa chuỗi ASCII “TRUE” và nếu tổng kiểm tra CRC-32 của 256 bytes cuối cùng của dữ liệu được giải mã (header tập) khớp với giá trị nằm ở byte#8 của dữ liệu được giải mã. Nếu các điều kiện này không được đáp ứng, quá trình lại tiếp tục từ (b3) nhưng lần này thay vì dữ liệu được đọc trong bước 1, dữ liệu được đọc trong bước 2 sẽ được sử dụng (tức là có thể có header tập đĩa ẩn). nếu các điều kiện không được đáp ứng một lần nữa, quá trình gắn kết sẽ bị chấm dứt (sai mật khẩu, ổ đĩa bị hỏng hoặc không phải là ổ đĩa TrueCrypt)
* Bước 5: Bây giờ chúng ta biết (hoặc giả sử với xác suất rất cao) rằng chúng ta có mật khẩu chính xác, thuật toán mã hóa chính xác, chế độ, kích thước khóa và thuật toán dẫn xuất khóa header chính xác. Nếu chúng giải mã thành công dữ liệu được đọc trong bước 2, chúng cũng biết rằng chúng tôi đang gắn một tập đĩa ẩn và kích thước của nó được truy xuất từ dữ liệu
* đọc trong bước 2 được giải mã trong bước 3
* Bước 6: Quy trình mã hóa được khời động lại bằng khóa chính và khóa chính phụ, được truy xuất từ header ổ đĩa được giải mã bất kỳ khu vực nào của ổ đĩa, ngoại trừ vùng header ổ đĩa (hoặc vùng dữ liệu khóa, để mã hóa hệ thống), đã được mã hóa bằng các khóa header. ổ đĩa được gắn kết

2.2 Các bước thực hành – Kết quả

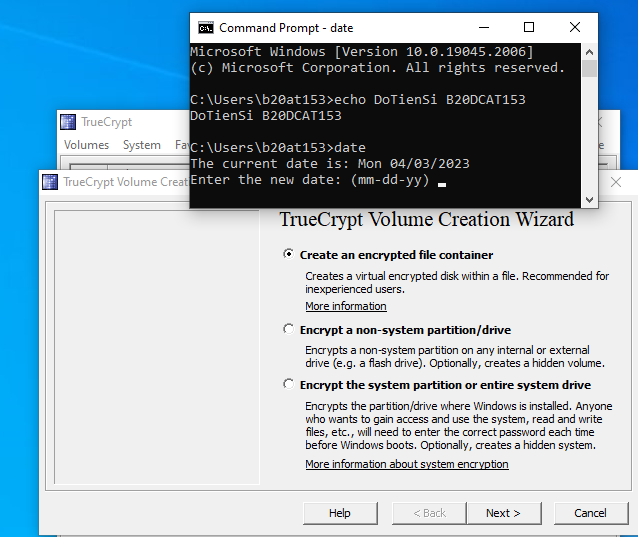
a. Cài đặt TrueCrypt

- Tải TrueCrypt

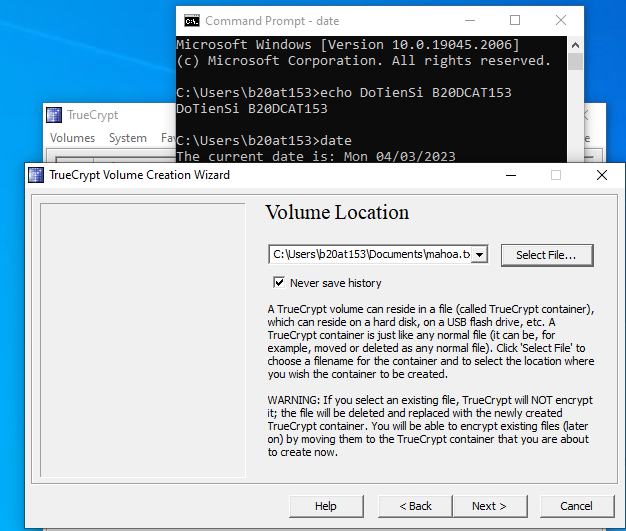
b. Sử dụng công cụ TrueCrypt để mã hóa file

- Tạo vùng khóa chuẩn

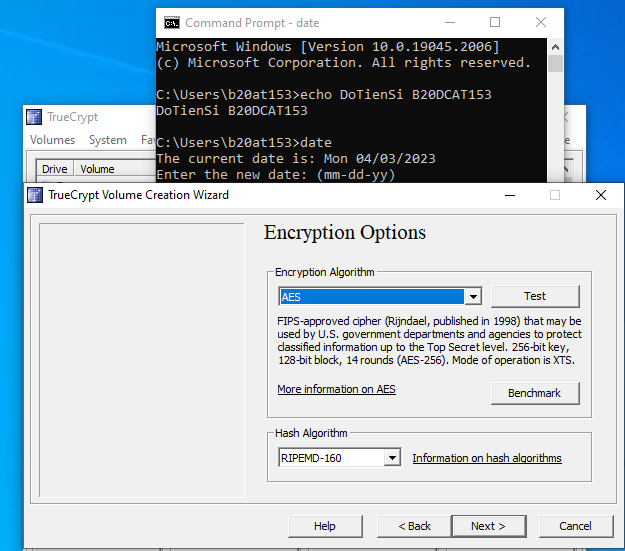
Bấm create volume



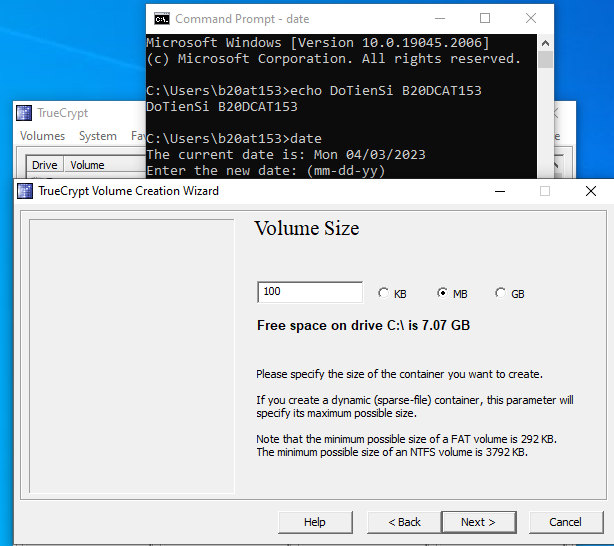
Chọn vị trí sao luu



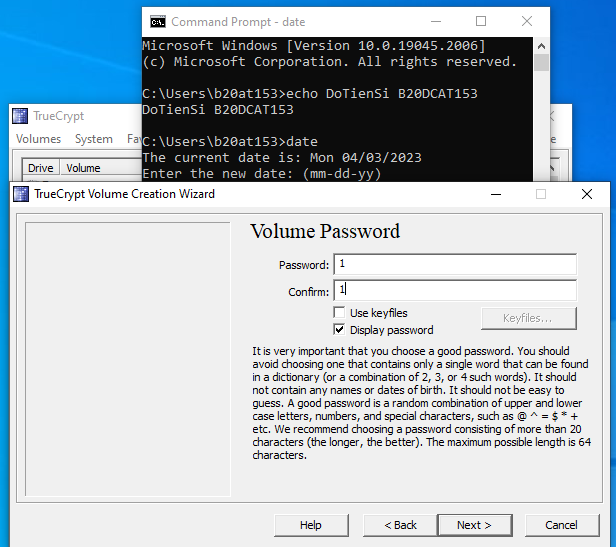
Chọn thuật toán mã hóa



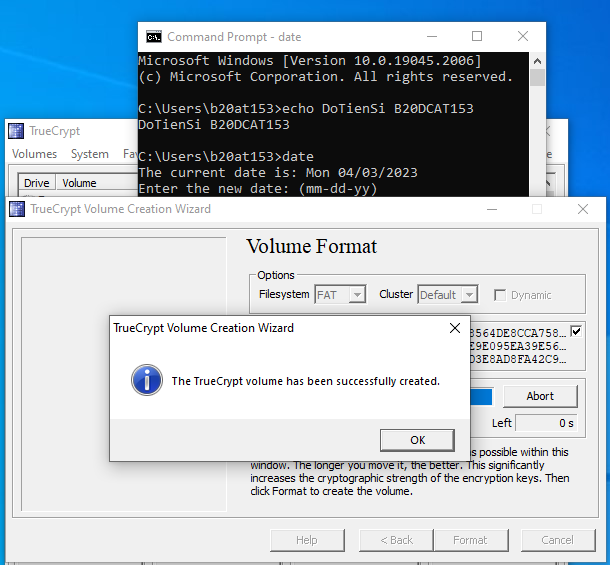
Chọn kích thước tối đa volume

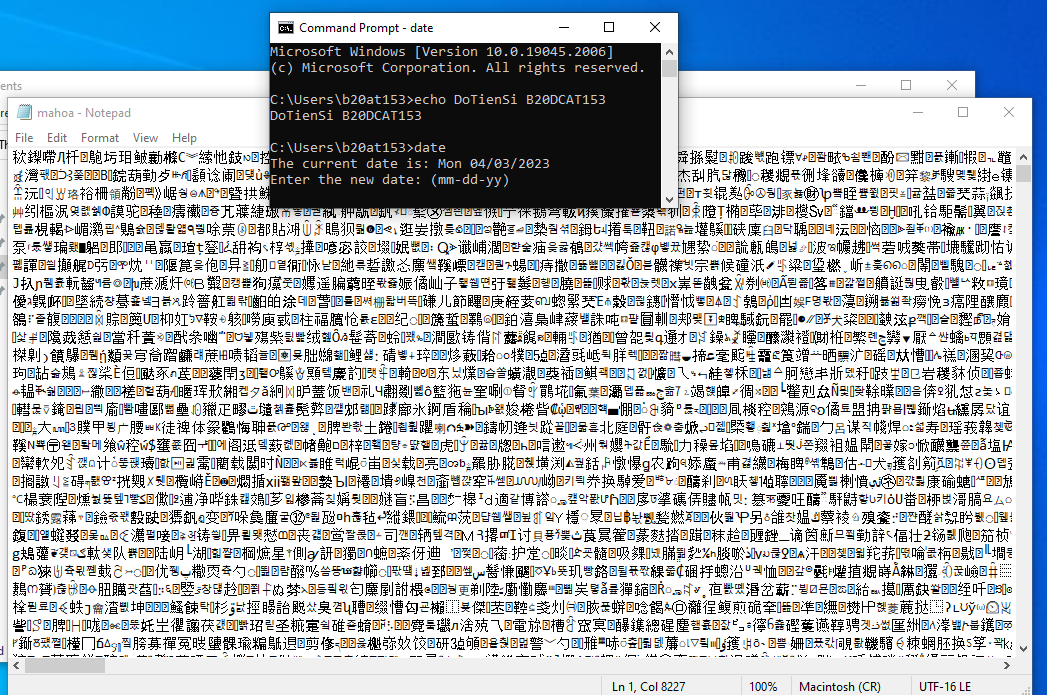


- Chọn mật khẩu để volume

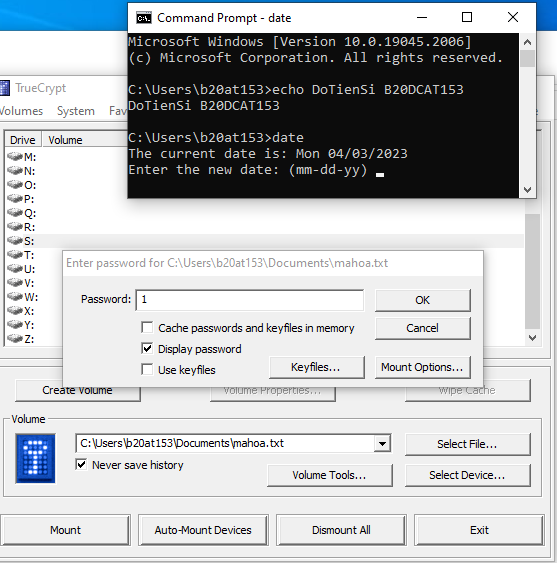


Tạo vùng mã hóa thành công

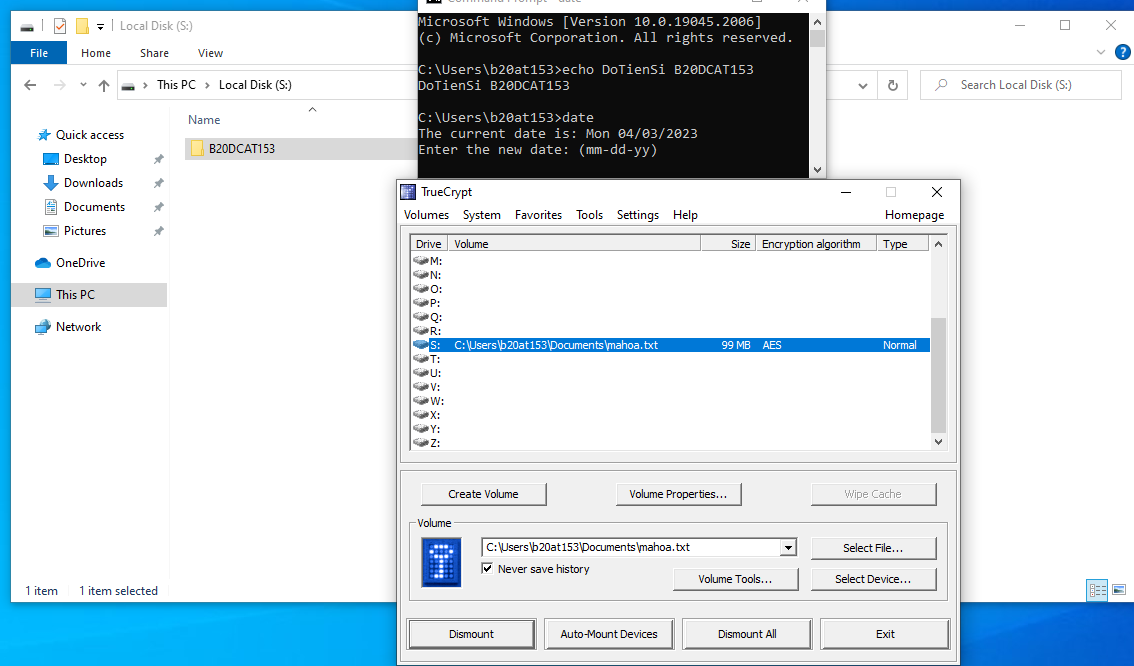


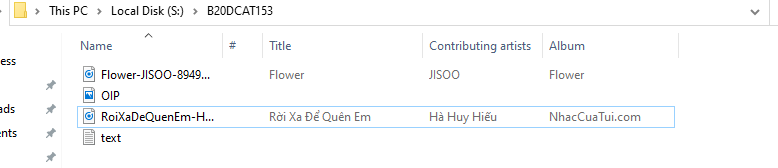


Gắn vùng mã hóa chuẩn

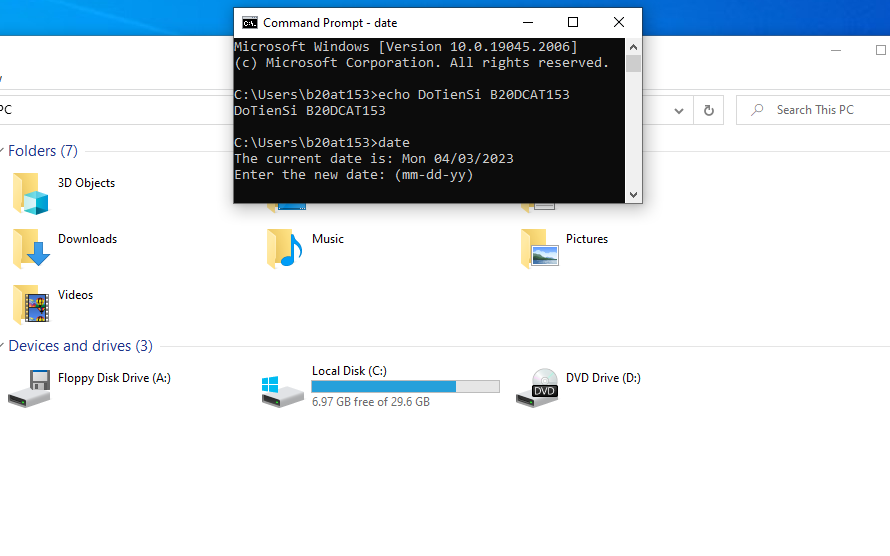


* Di chuyển thư mục có các tập tin ảnh ,text, mp3 cần mã hóa vào trong volume

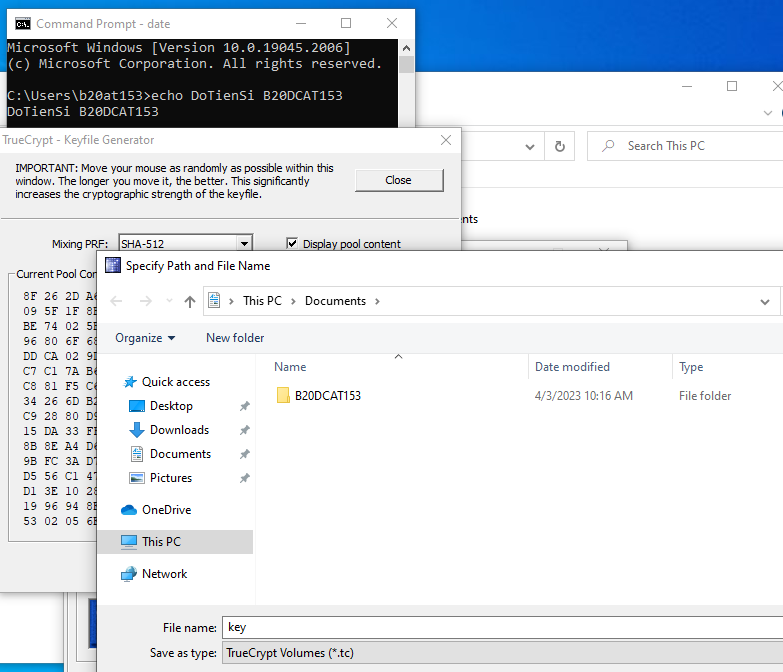




* Dismount



* Sao lưu khóa



* Khôi phục lại các file và thư mục đã mã hóa

