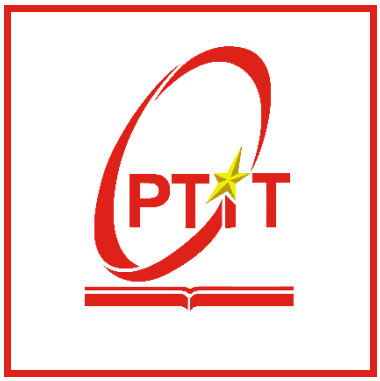
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



THỰC TẬP CƠ SỞ

Bài 13: Đảm bảo an toàn với mã hóa

Sinh viên	Nguyễn Duy Đạt
MSV	B21DCAT056
Giảng viên	Vũ Minh Mạnh

Hà Nội – 2024

Môn học Thực tập cơ sở

Bài 13: Đảm bảo an toàn với mã hóa

I. Lý thuyết

1. Giới thiệu 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 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 kểtừ 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

2. Thuật toán mã hóa

TrueCrypt sử dụng một số thuật toán mã hóa để bảo vệ dữ liệu của người dùng. Cụ thể, TrueCrypt đã tích hợp các thuật toán sau:

- AES (Advanced Encryption Standard): AES là một trong những thuật toán mã hóa phổ biến nhất và mạnh mẽ nhất hiện nay. TrueCrypt hỗ trợ AES với các khóa 128-bit, 192-bit và 256-bit.
- Twofish: Twofish là một thuật toán mã hóa đối xứng khá mạnh mẽ và đã được chứng minh tính bảo mật của nó. TrueCrypt hỗ trợ Twofish với các khóa 128-bit, 192-bit và 256-bit.
- Serpent: Serpent là một thuật toán mã hóa đối xứng mạnh mẽ khác, được thiết kế để cung cấp mức độ bảo mật cao. TrueCrypt hỗ trợ Serpent với các khóa 128-bit, 192bit và 256-bit.

Người dùng có thể lựa chọn và kết hợp các thuật toán này trong TrueCrypt để tăng cường bảo mật và đáp ứng nhu cầu cụ thể của họ. Trong quá trình tạo một phân vùng mã hóa hoặc ổ đĩa ảo, người dùng sẽ được yêu cầu chọn thuật toán và kích thước khóa cho mỗi phần của dữ liệu. Điều này giúp TrueCrypt linh hoạt và có thể tùy chỉnh theo nhu cầu bảo mật cụ thể của người dùng.

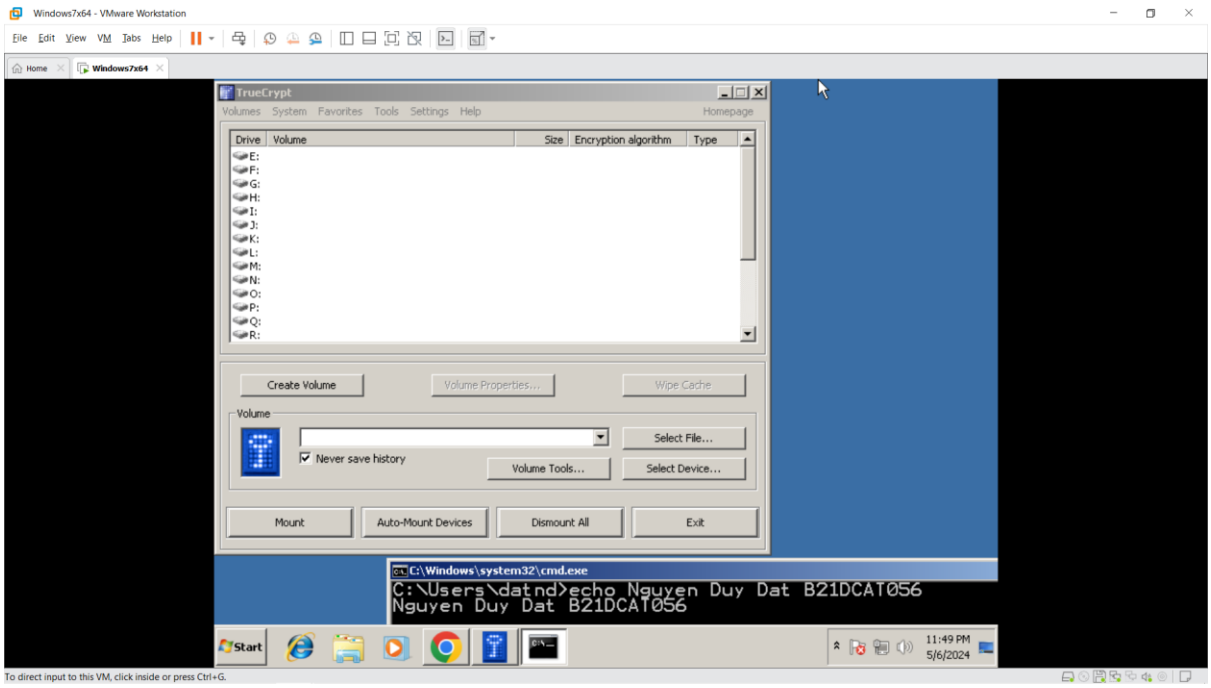
Ngoài ra, có 5 tổ hợp phương thức mã hóa chồng là: AES-Twofish, Aes-Twofish-Serpent, Serpent-Aes, Serpent-Twofish-AES và Twofish-Serpent. Các hàm băm có sẵn để sử dụng trong TrueCrypt là RIPEMD-160, SHA-512 và Whirlpool. TrueCrypt hỗ trợ một khái niệm gọi là từ chối hợp lý, bằng cách cho phép một "volume 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 bằng TrueCrypt, các bước thực hiện:

i. Nhập mật khẩu hoặc khóa: Người dùng được yêu cầu nhập mật khẩu hoặc khóa để mở khóa volume hoặc khóa hệ thống. Mật khẩu này có thể được yêu cầu trên giao diện người dùng của TrueCrypt hoặc trên giao diện xác thực trước khi khởi động hệ thống.
ii. Xác thực mật khẩu: TrueCrypt sẽ kiểm tra mật khẩu được nhập và so sánh với thông tin được lưu trữ để xác định xem mật khẩu có chính xác hay không. Nếu mật khẩu không khớp, TrueCrypt sẽ từ chối truy cập và yêu cầu người dùng nhập lại.
iii. Mở khóa volume hoặc khóa hệ thống: Nếu mật khẩu được nhập đúng, TrueCrypt sẽ sử dụng nó để mở khóa volume hoặc khóa hệ thống. Quá trình này bao gồm sử dụng mật khẩu hoặc khóa để giải mã dữ liệu được mã hóa.
iv. Truy cập dữ liệu: Khi volume được mã hóa được mở khóa thành công, người dùng có thể truy cập dữ liệu bên trong như bình thường. Đối với xác thực trước khi khởi động hệ thống, quá trình này sẽ cho phép hệ điều hành khởi động và truy cập các tệp hệ thống và ứng dụng một cách bình thường.

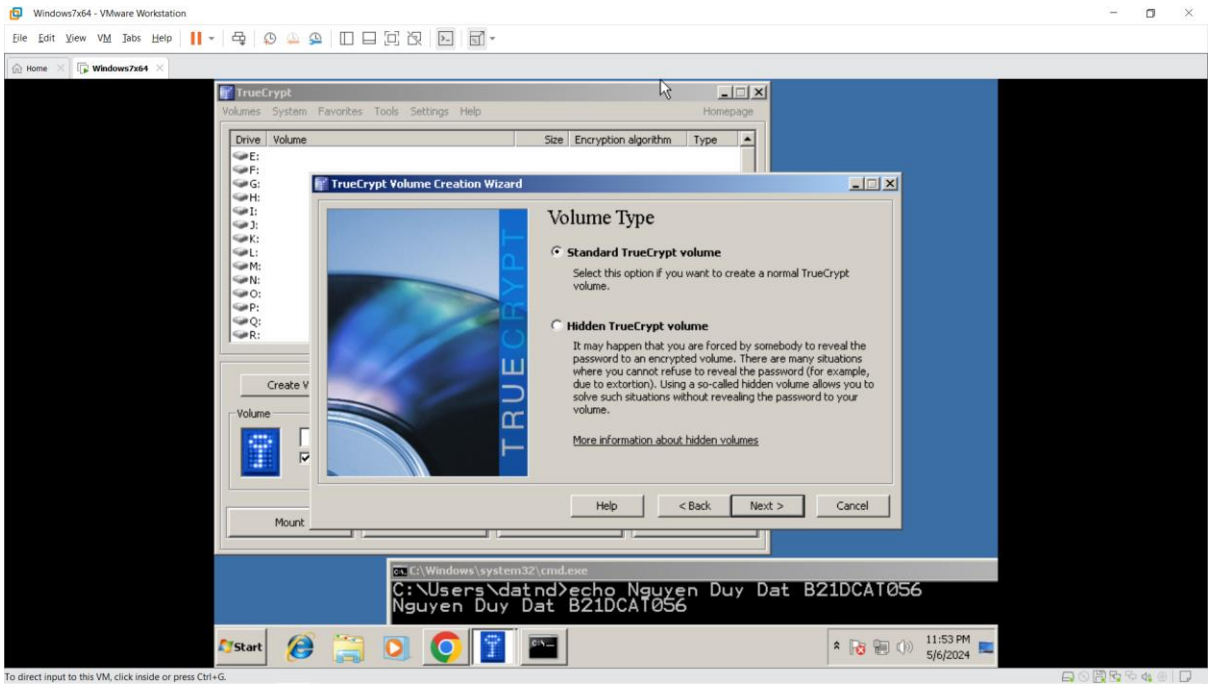
Quá trình này giúp bảo vệ dữ liệu được mã hóa bằng cách đảm bảo rằng chỉ những người có mật khẩu hoặc khóa chính xác mới có thể truy cập vào nó.

II. Thực hành

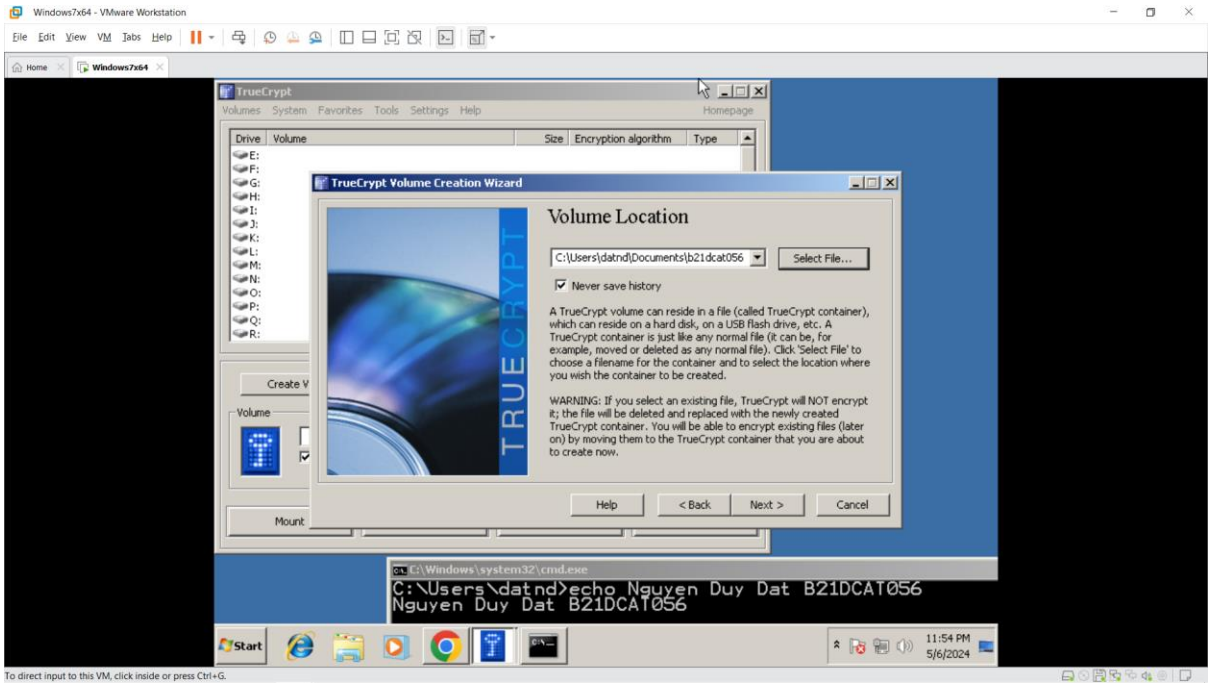
- Tải file và cài đặt truecrypt trên Windows 7, giao diện của truecrypt như sau:



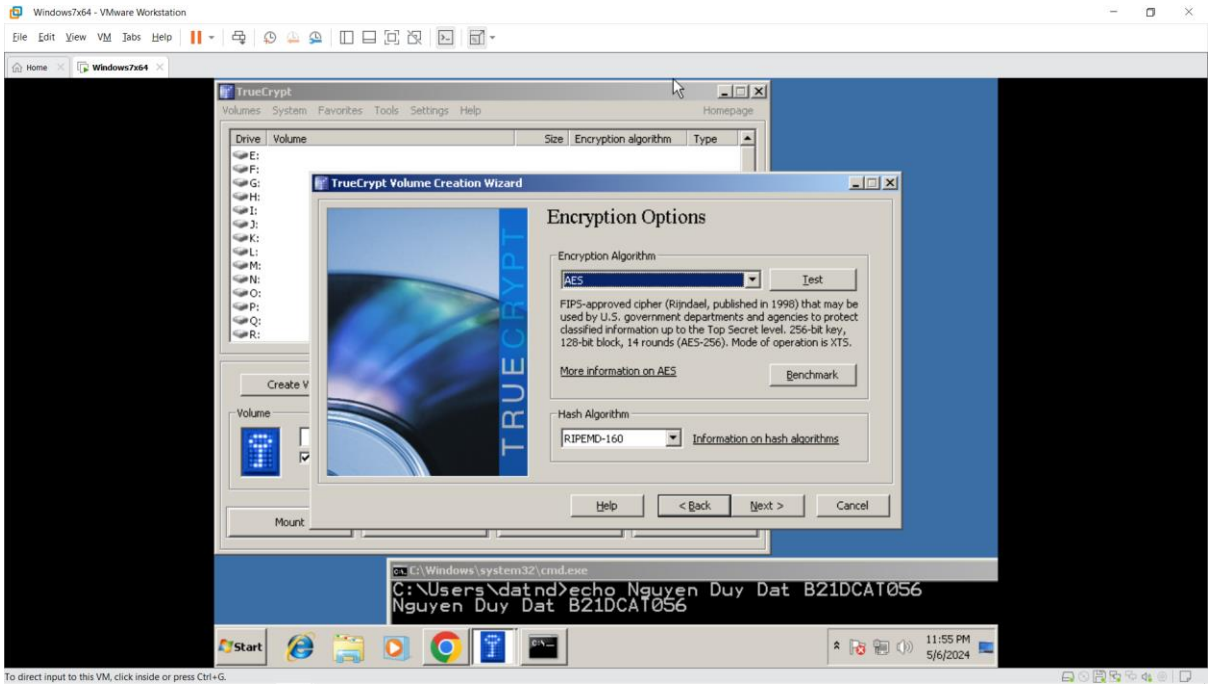
- Chọn create volume để tạo volume mới



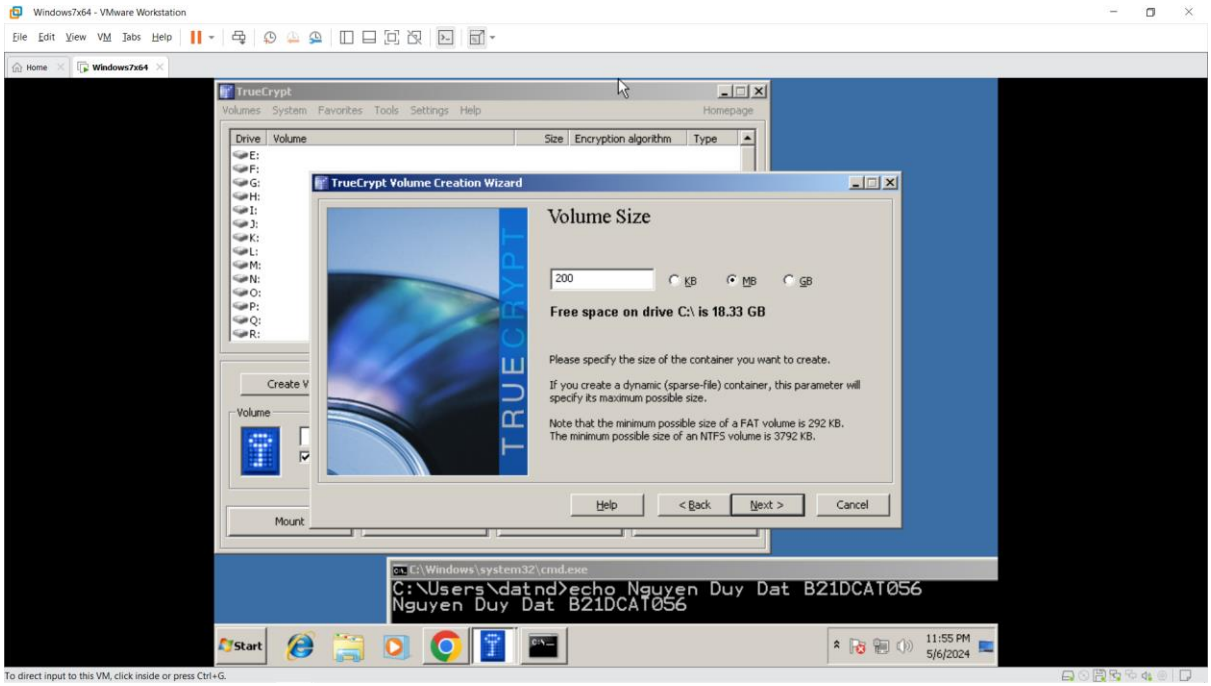
- Đường dẫn lưu file



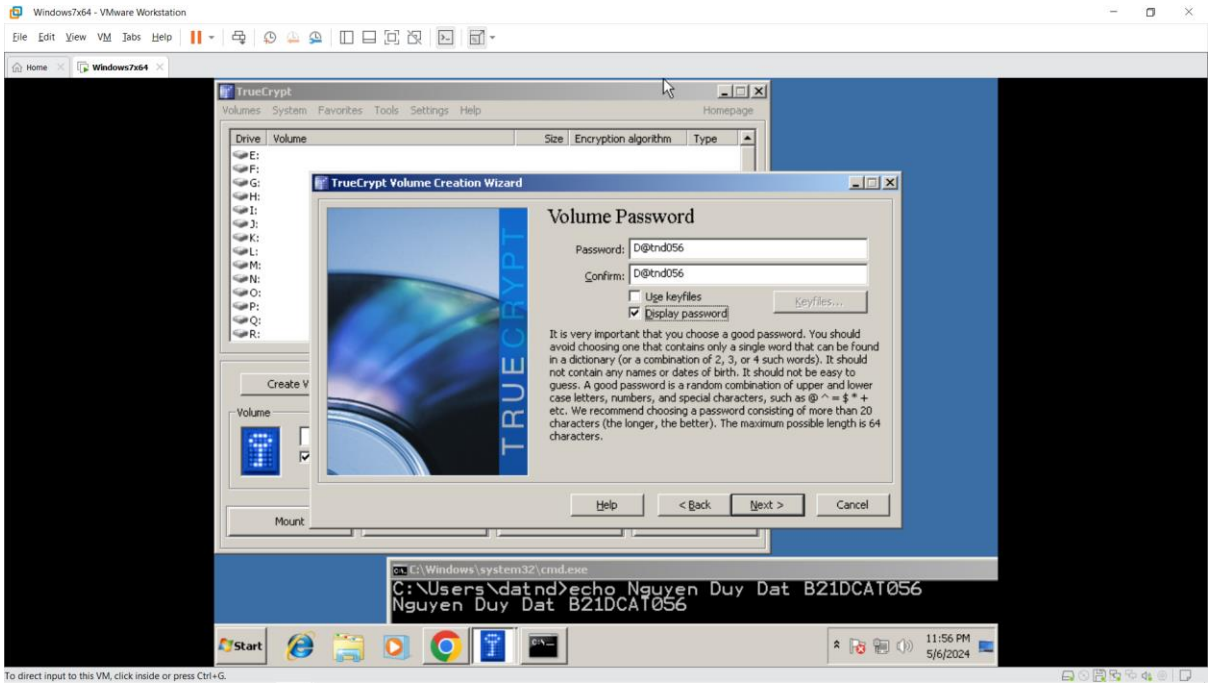
- Chọn phương pháp mã hóa



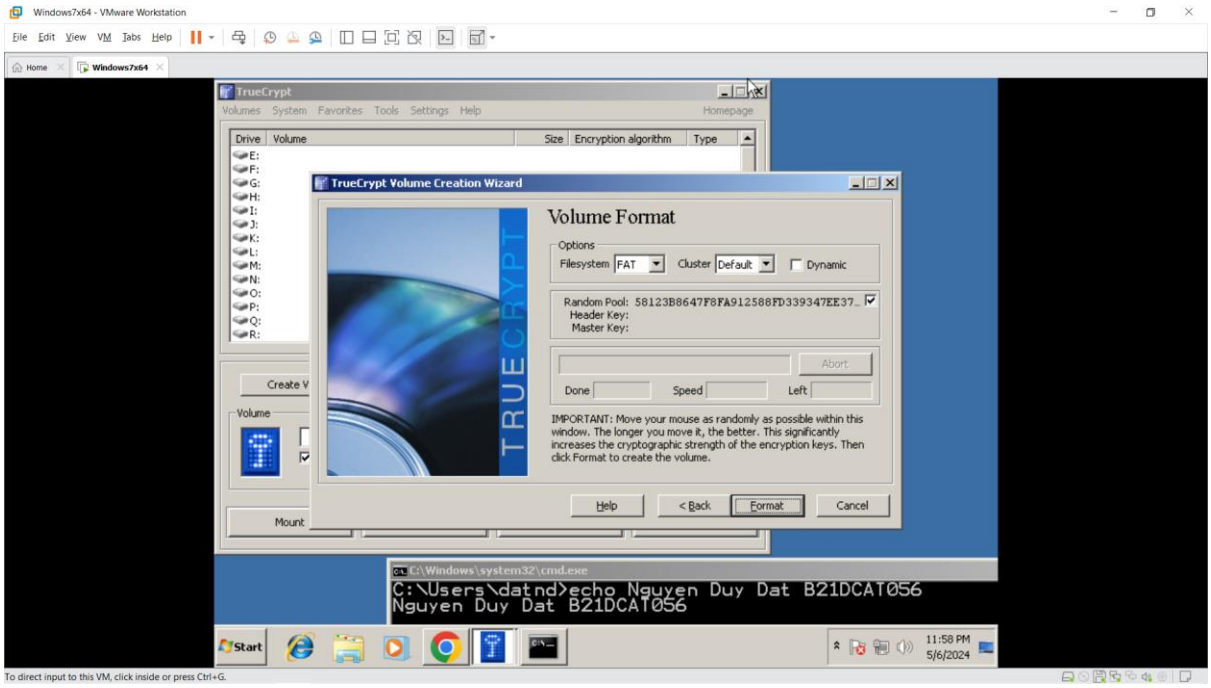
- Chọn kích thước file

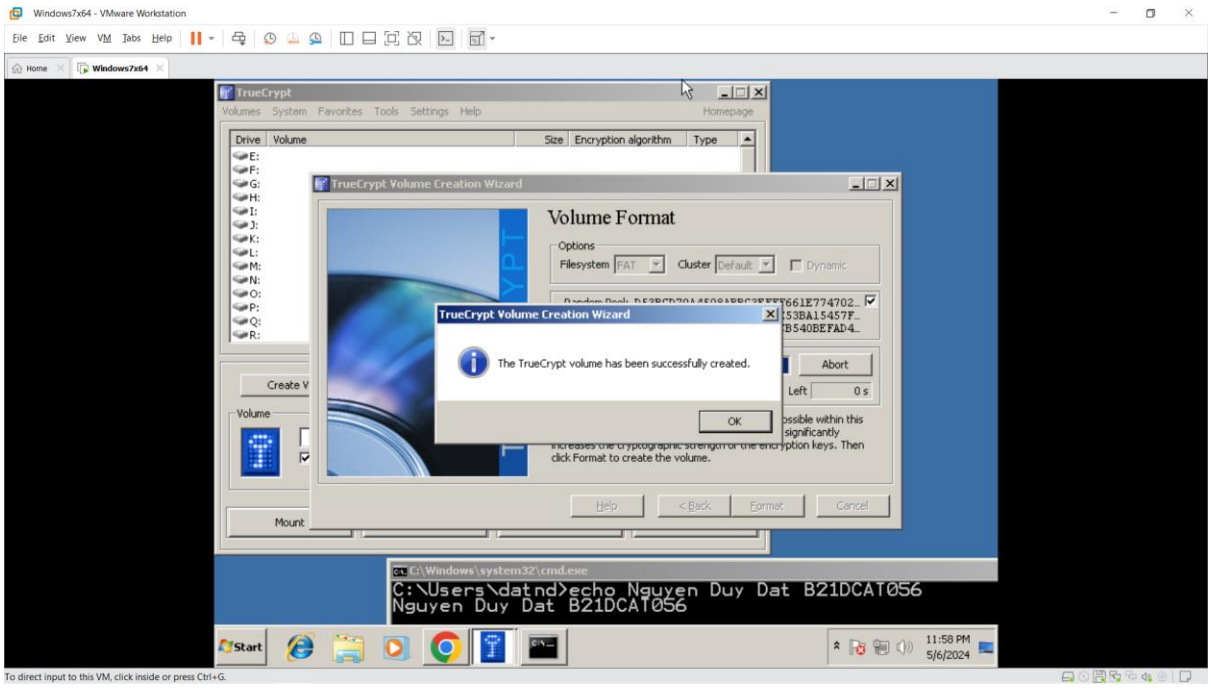


- Đến đây người dùng sẽ có các lựa chọn sau:
    - Mã hoá chỉ sử dụng mật khẩu (password).
    - Mã hoá chỉ sử dụng tệp tin khoá (keyfile).
    - Mã hoá sử dụng cả mật khẩu và tệp tin khoá.
- Tạm thời chỉ đặt mật khẩu, sẽ thêm tệp tin khoá sau.

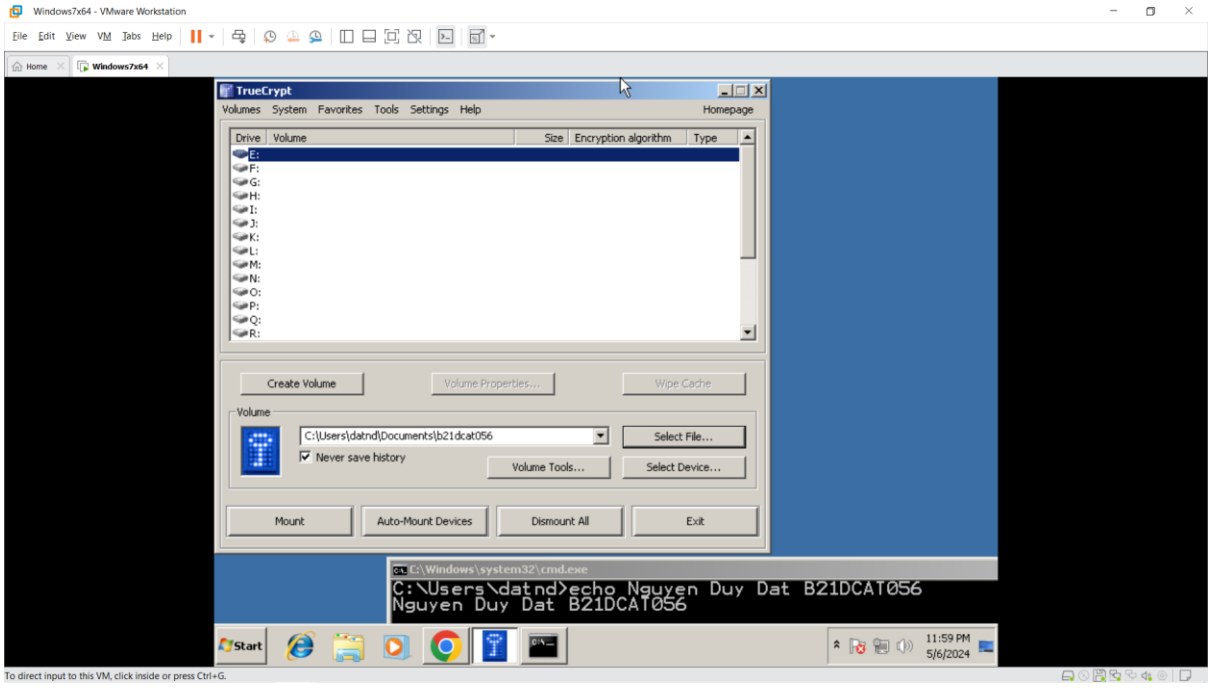


- Di chuột một cách ngẫu nhiên để tăng tính ngẫu nhiên của khoá rồi bấm Format

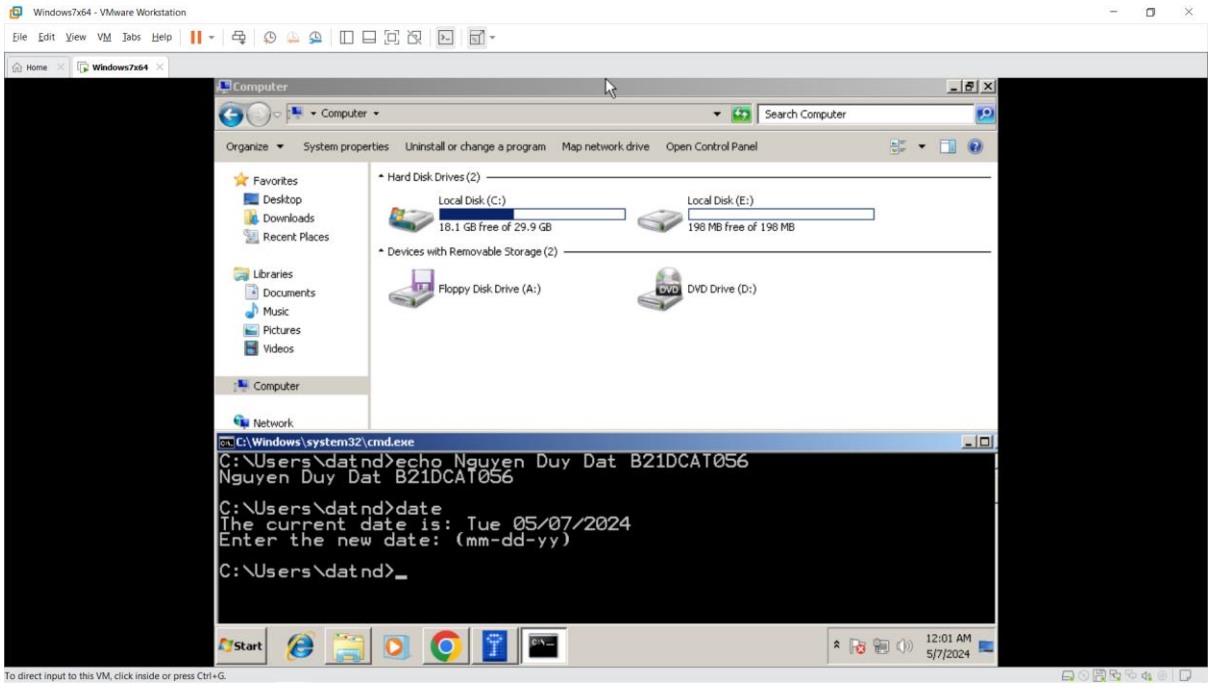




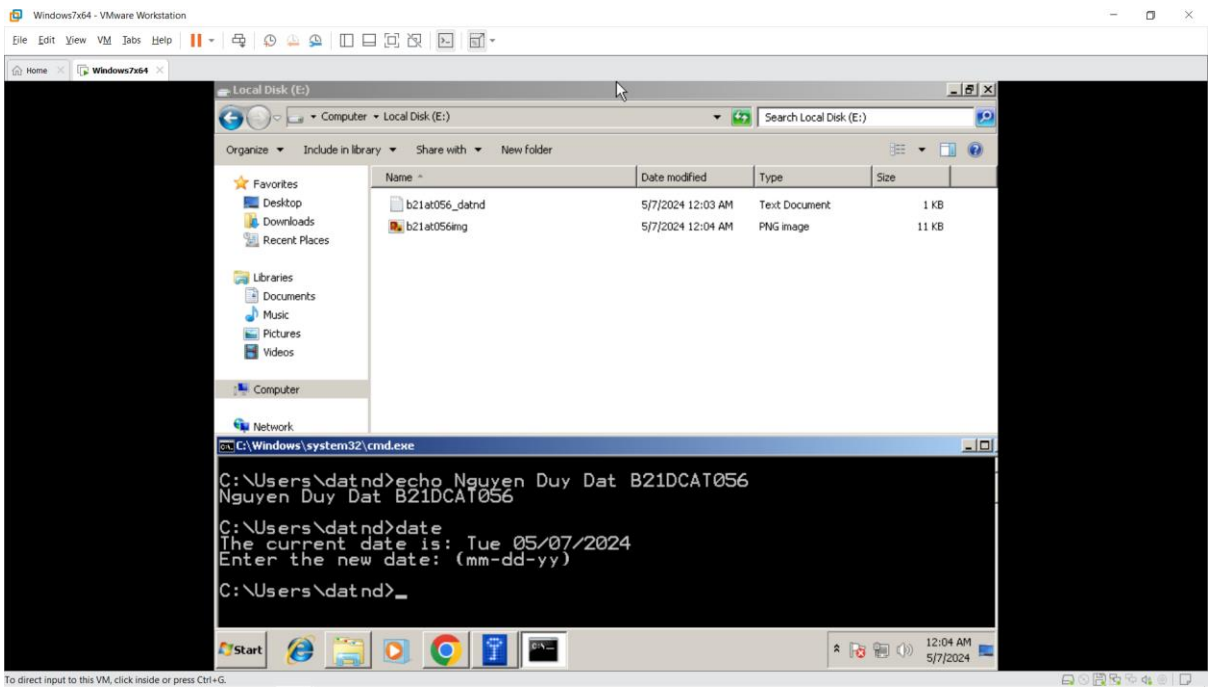
- Sau khi tạo container thành công, cần phải mount nó như một ổ đĩa. Mở lại giao diện TrueCrypt, chọn Select File, chọn container. Chọn một kí tự ổ cứng (trong trường hợp này là E) rồi bấm Mount.



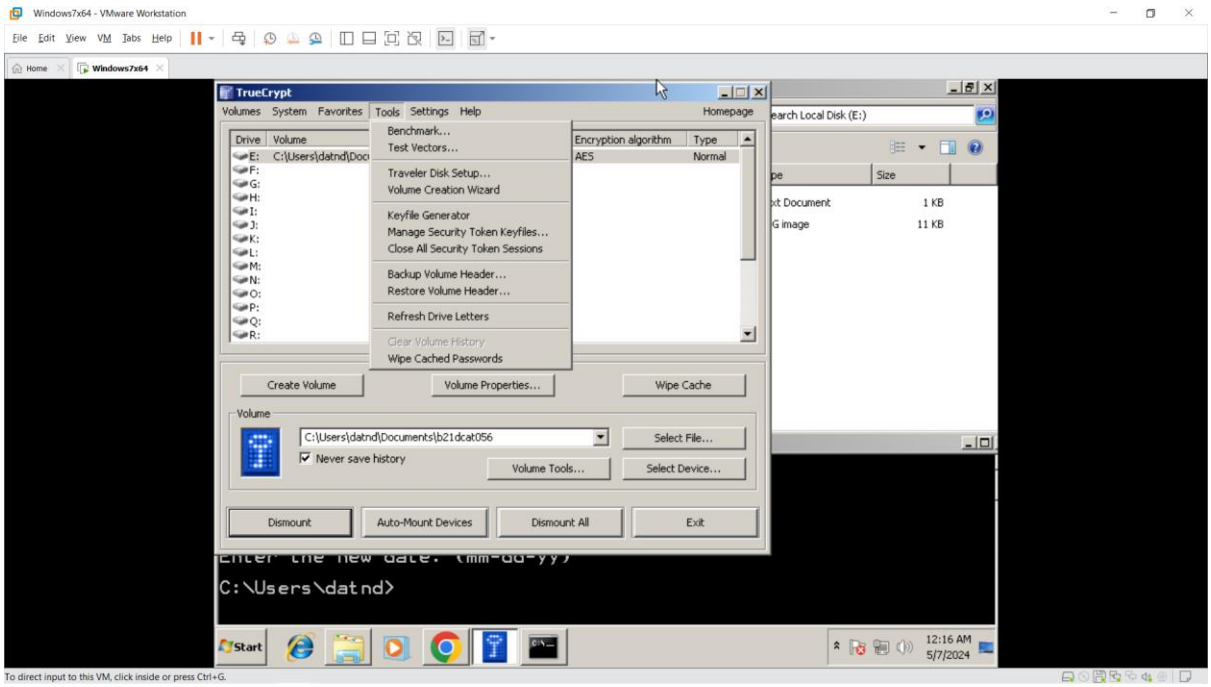
- Mở File Explorer để thấy ổ mới.

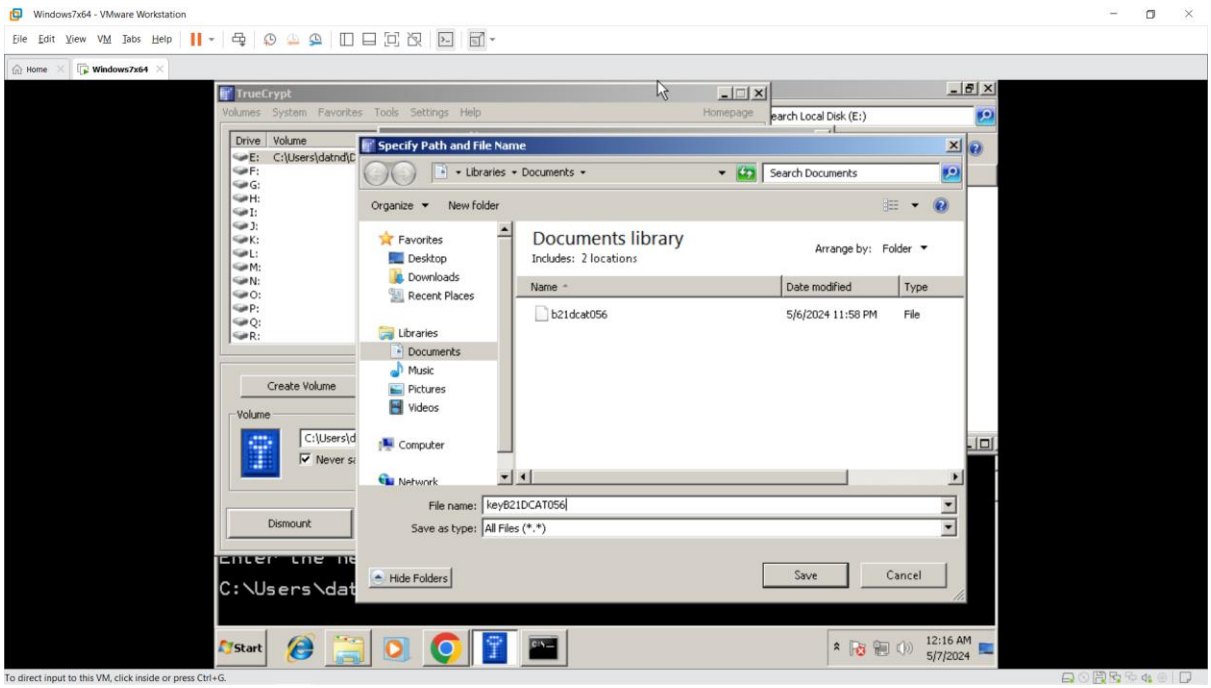


- Tại đây, thêm vào một tệp văn bản .txt và một ảnh .png với nội dung như hình dưới

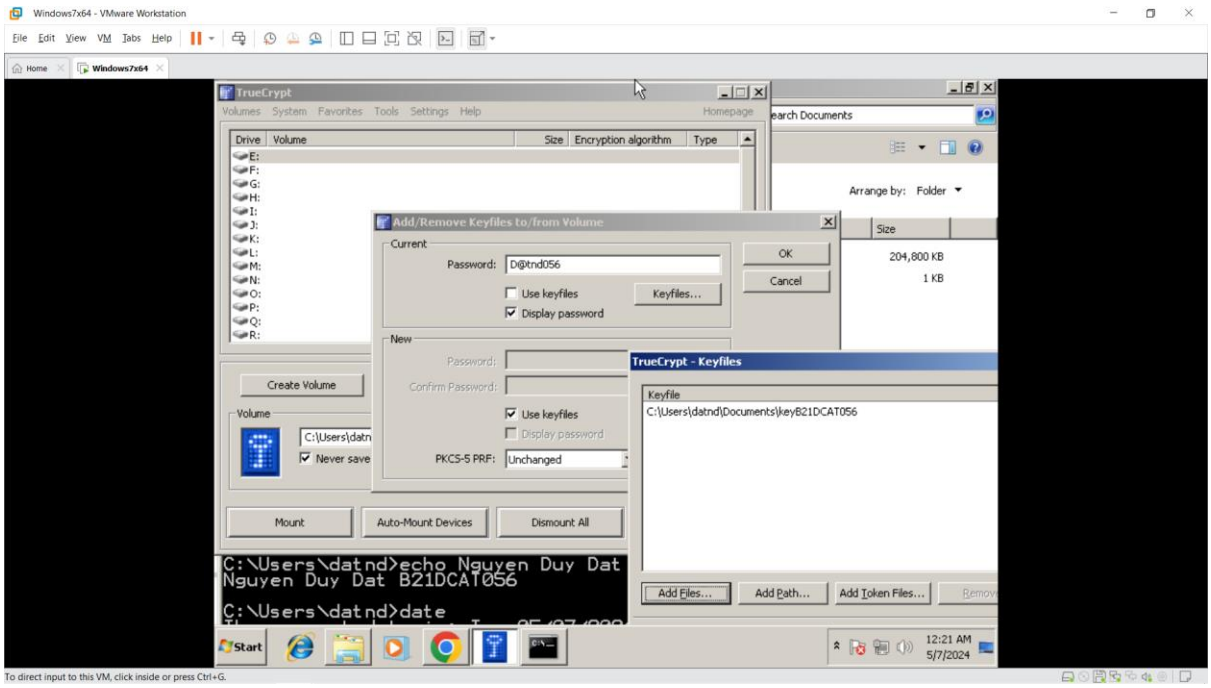


- Bây giờ thực hiện thêm tệp tin khoá. Có thể sử dụng bất cứ tệp tin nào để làm tệp tin khoá, nhưng TrueCrypt cũng cung cấp tính năng tạo tệp tin khoá ngẫu nhiên. Trên giao diện TrueCrypt, chọn Tools -> Keyfile Generator

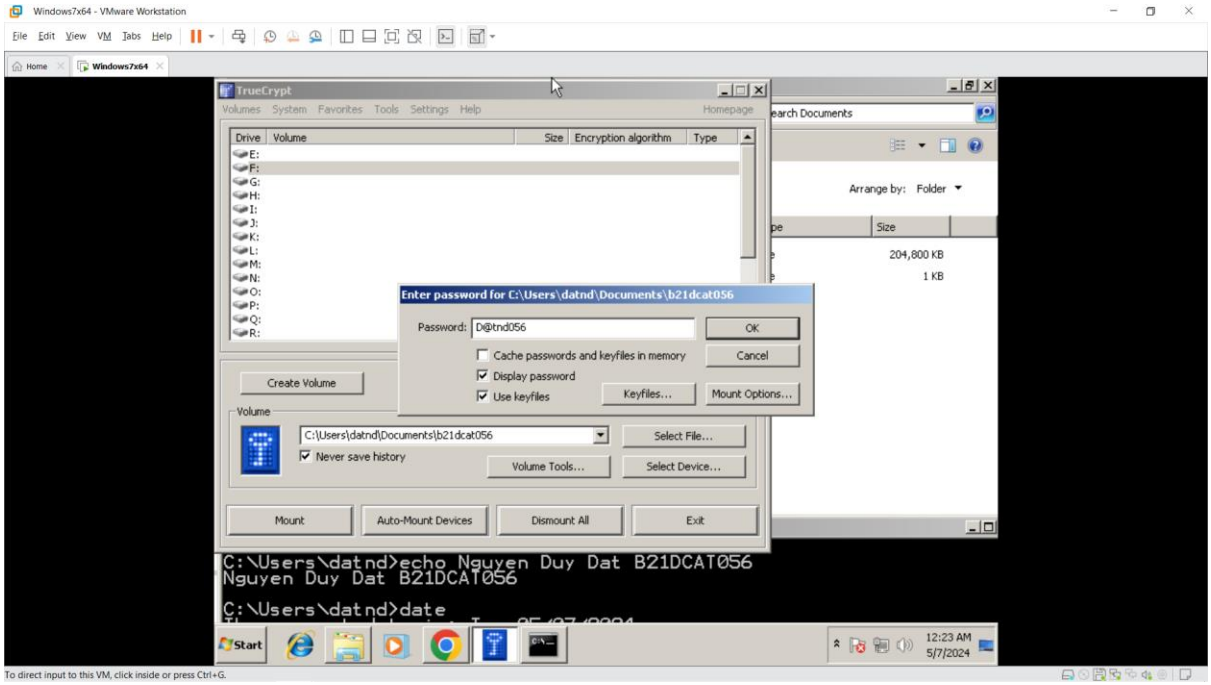




- Để cài đặt sao cho container sử dụng cả mật khẩu (password) và tệp tin khoá (keyfile) để xác minh, ta bấm Volume Tools -> Add/remove keyfile to/from volume.
- Trên cửa sổ mới hiển thị, ở mục Old điền mật khẩu cũ, ở mục New chọn Use keyfile rồi chọn tệp tin khoá đã tạo ở mục trước



- Quá trình thêm tệp tin khoá thành công. Người dùng có thể sao lưu tệp tin khoá này sang ổ đĩa khác hoặc máy tính khác. Những lần sau, nếu muốn mở container này, người dùng cần làm những thao tác như sau:
  Mở giao diện TrueCrypt, nạp Container mã hoá và bấm Mount. Trên cửa sổ mới hiện lên, điền mật khẩu và chọn Use keyfile. Bấm nút Keyfile và chọn tệp tin khoá. Bấm OK rồi bấm Mount.



- Nếu mật khẩu và tệp tin khoá đúng, container sẽ được giải mã. Nội dung các tệp tin trong container không thay đổi