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

Môn: Thực tập cơ sở

BÀI BÁO THỰC TẬP CƠ SỞ

Bài 13: Đảm bảo an toàn với mã hóa

Họ và tên giảng viên:	TS.Đinh Trường Duy
Họ và tên:	Nguyễn Quốc Khánh
Mã sinh viên:	B20DCAT103
Lớp:	D20CQAT03-B
Số điện thoại:	0964137761

Hà Nội 2023

I. Nội dung lý thuyết

1. Lý thuyết

TrueCrypt là một phần mềm mã hóa đĩa cứng miễn phí và mã nguồn mở. Nó cho phép người dùng tạo các tập tin ảo được mã hóa trên đĩa cứng hoặc các thiết bị lưu trữ khác, và truy cập chúng như các ổ đĩa bình thường. TrueCrypt cũng hỗ trợ tạo các ổ đĩa ẩn trong các tập tin ảo, để che giấu sự tồn tại của dữ liệu bí mật. Mục đích của TrueCrypt là bảo vệ dữ liệu cá nhân hoặc doanh nghiệp khỏi việc bị đánh cắp, mất mát hoặc xâm nhập bởi kẻ xấu. TrueCrypt sử dụng các thuật toán mã hóa mạnh như AES, Serpent và Twofish, và cho phép người dùng kết hợp chúng để tăng cường độ bảo mật. TrueCrypt cũng có khả năng mã hóa toàn bộ hệ thống, bao gồm cả phân vùng khởi động và hệ điều hành.

TrueCrypt là một phần mềm mã hóa dữ liệu miễn phí và mã nguồn mở được phát triển bởi TrueCrypt Foundation. Nó cho phép người dùng tạo ra các ổ đĩa ảo được mã hóa để bảo vệ dữ liệu của họ khỏi sự truy cập trái phép.

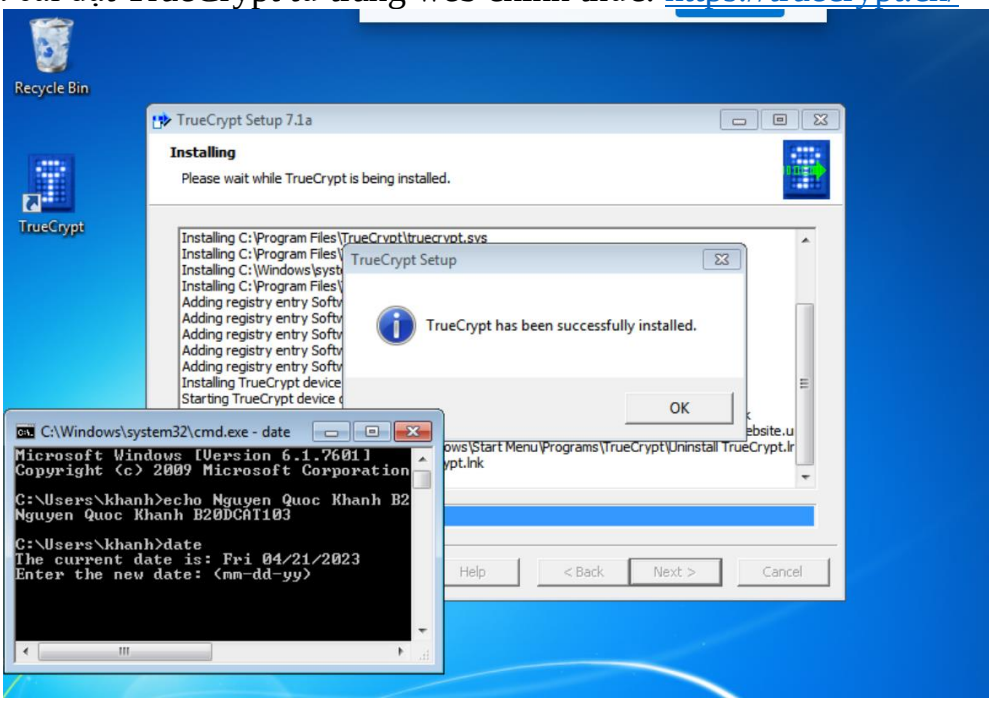
Công cụ TrueCrypt sử dụng các thuật toán mã hóa mạnh như AES, Serpent và Twofish để bảo vệ dữ liệu. Nó cũng cung cấp khả năng ẩn các thông tin nhạy cảm, giúp người dùng bảo vệ dữ liệu quan trọng khỏi sự truy cập trái phép. TrueCrypt cũng có thể được sử dụng để mã hóa toàn bộ ổ đĩa, bao gồm cả hệ thống tệp của bạn.

Công cụ TrueCrypt cho phép người dùng chọn nhiều loại chế độ mã hóa, bao gồm các chế độ ổ đĩa độc lập và các chế độ phân vùng. Nó cũng cho phép người dùng tạo các ổ đĩa ảo được mã hóa và lưu trữ các tập tin dữ liệu trên chúng.

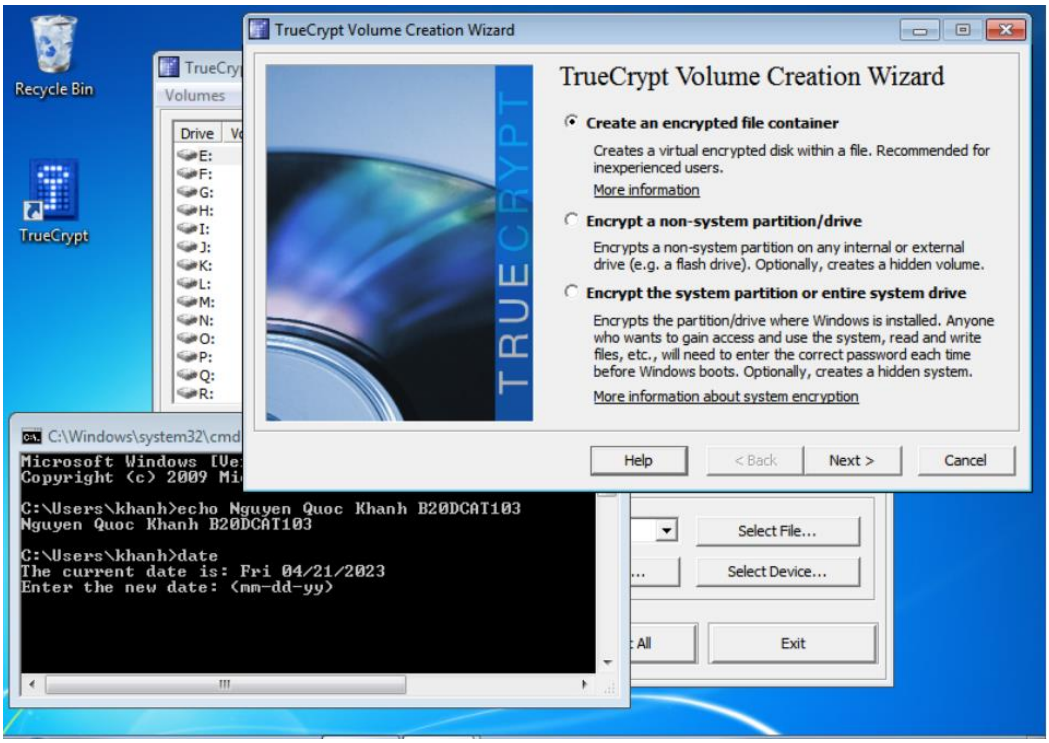
Về thuật toán mã hóa, các thuật toán mã hóa được hỗ trợ bởi TrueCrypt là AES, Serpent và Twofish. Ngoài ra, có 5 tổ hợp phương thức mã hóa chồng là: AES-Twofish, Aes-Twofish-Serpent, Serpent-Aes, Serpent-Twofish-AES và Twofish-Serpent. Các hàm băm có sẵn để sử dụng trong TrueCrypt là RIPEMD-160, SHA-512 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.

II. Các bước thực hành

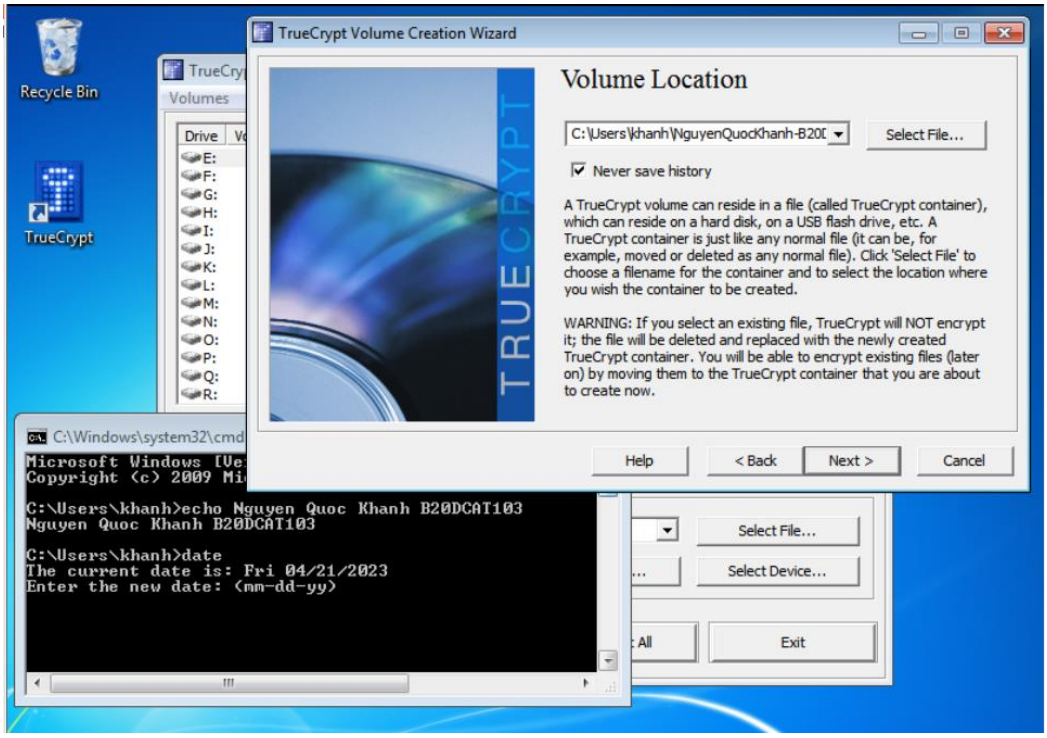
- Tải và cài đặt TrueCrypt từ trang web chính thức: https://truecrypt.ch/



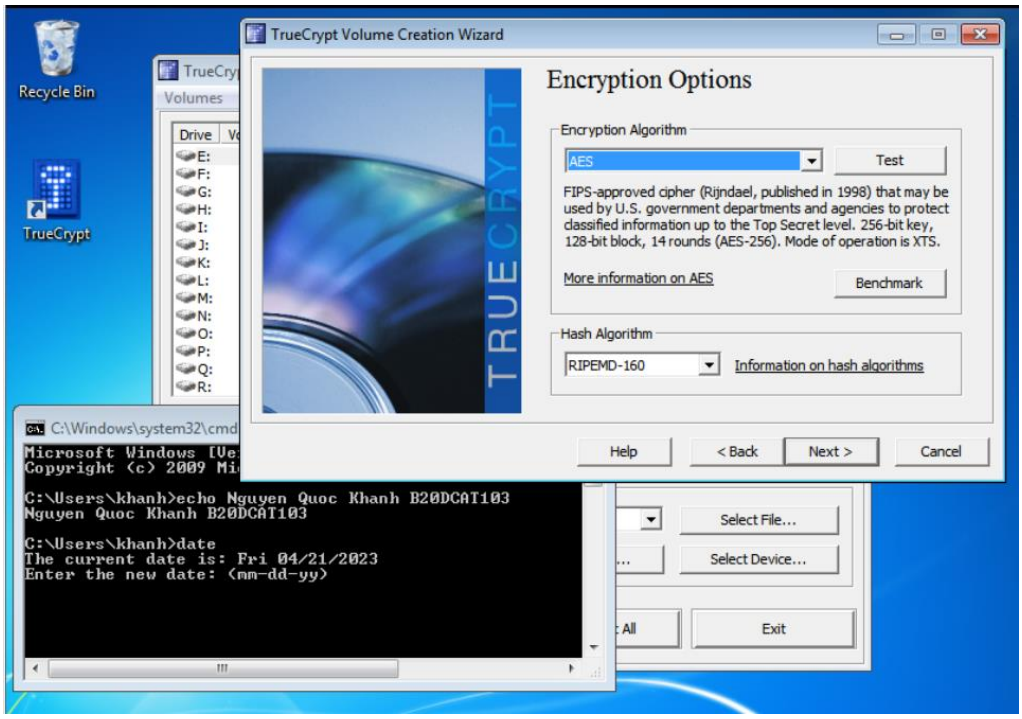
- Chọn Create an encrypted file container (Tạo một tập tin chứa được mã hoá) và nhấn Next (Tiếp tục).



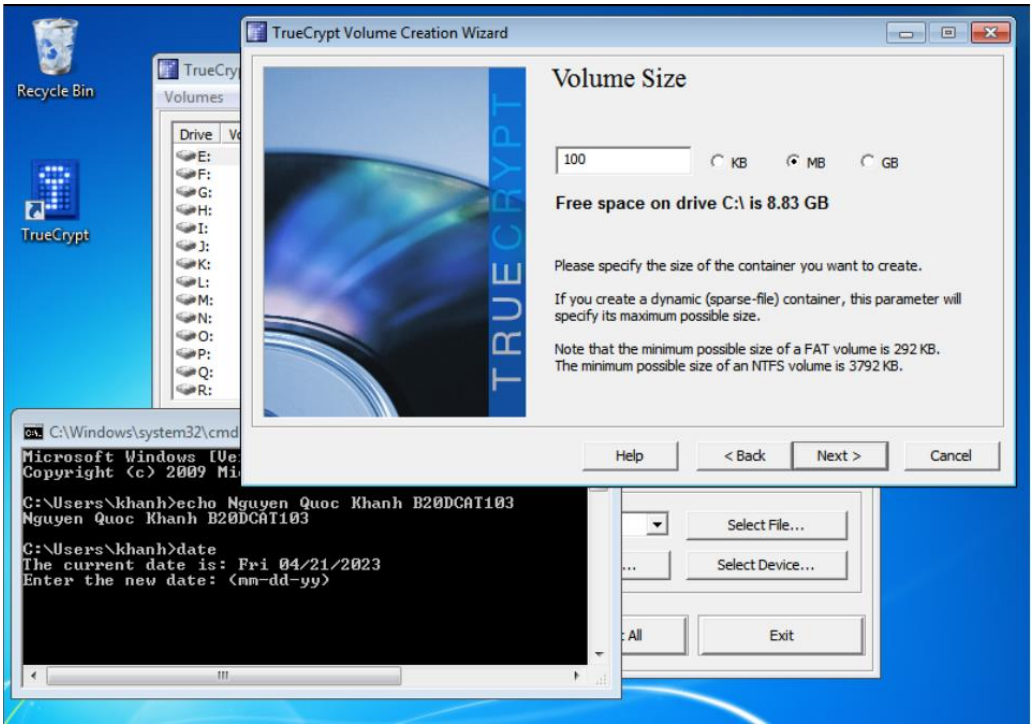
- Chọn nơi lưu trữ tập tin ảo được mã hoá bằng cách nhấn Select File (Chọn tập tin) và nhập tên cho nó. Nhấn Next (Tiếp tục).



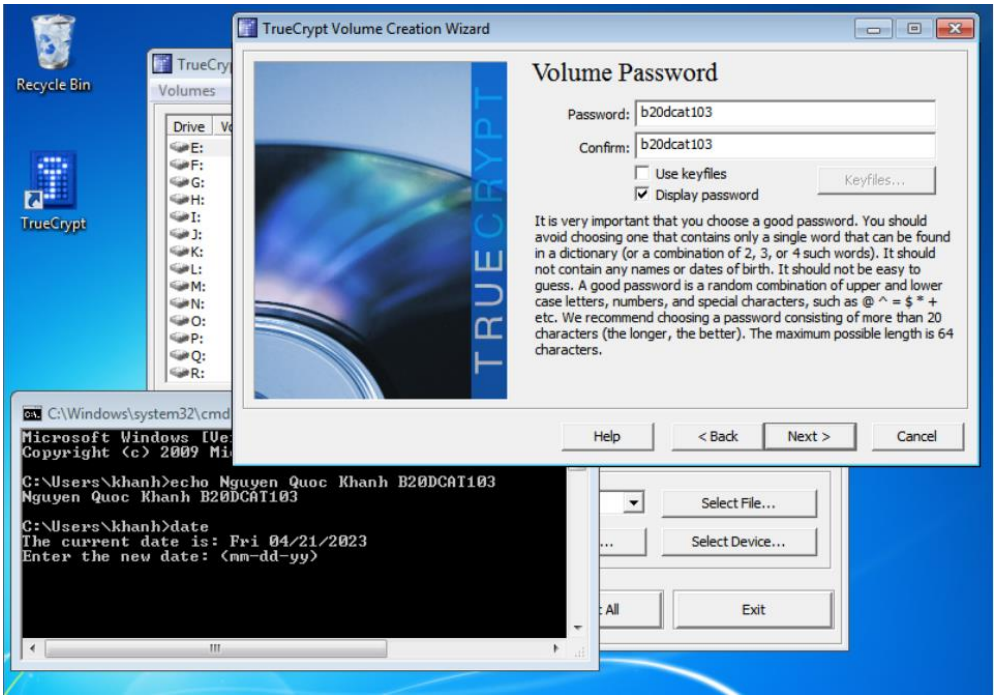
- Chọn thuật toán mã hoá và thuật toán băm cho ổ đĩa TrueCrypt, có thể để mặc định là AES và SHA-512 hoặc chọn các thuật toán khác theo ý thích. Nhấn Next (Tiếp tục).



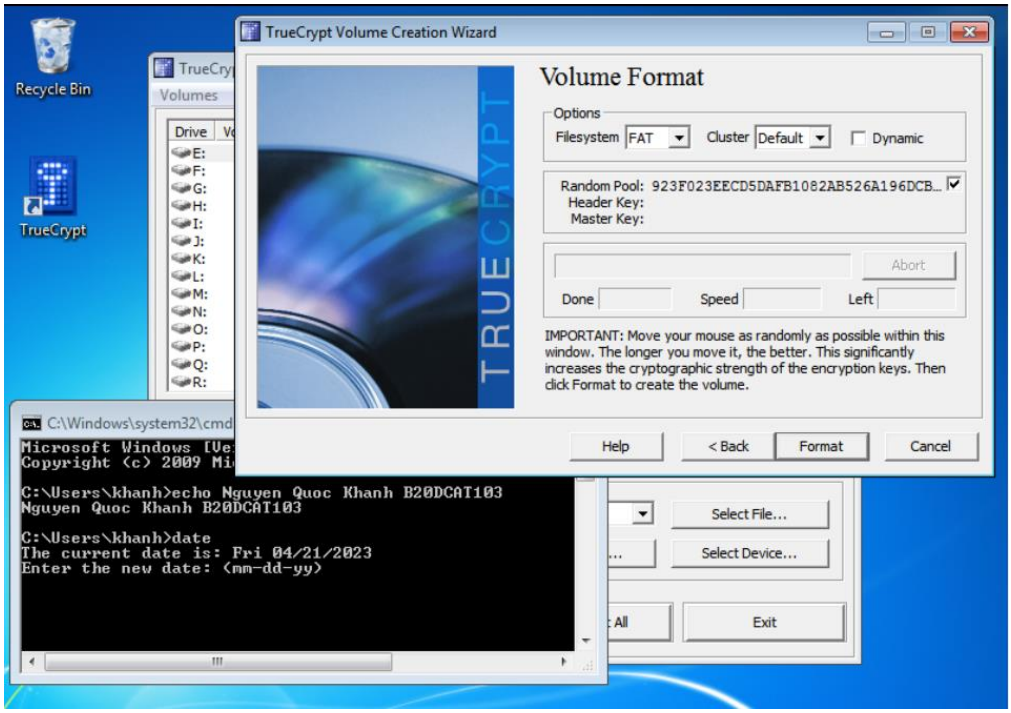
- Nhập dung lượng cho ổ đĩa TrueCrypt chọn một dung lượng lớn hơn kích thước của file bạn muốn mã hoá. Nhấn Next (Tiếp tục).



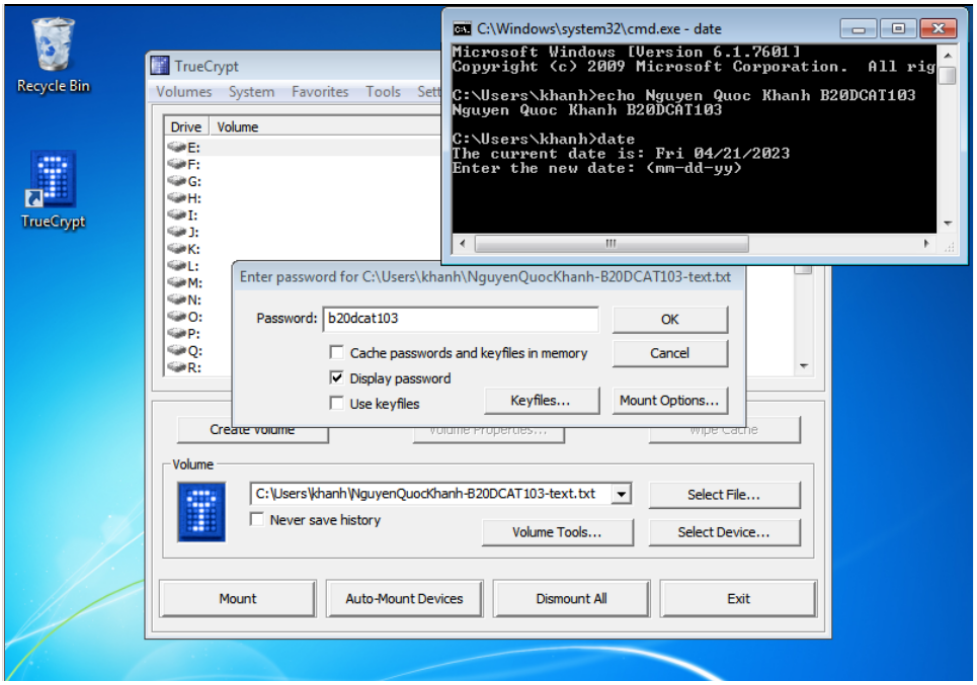
- Nhập mật khẩu cho ổ đĩa TrueCrypt của bạn. Nên chọn một mật khẩu mạnh, bao gồm cả chữ hoa, chữ thường, số và ký tự đặc biệt. Nhấn Next (Tiếp tục).

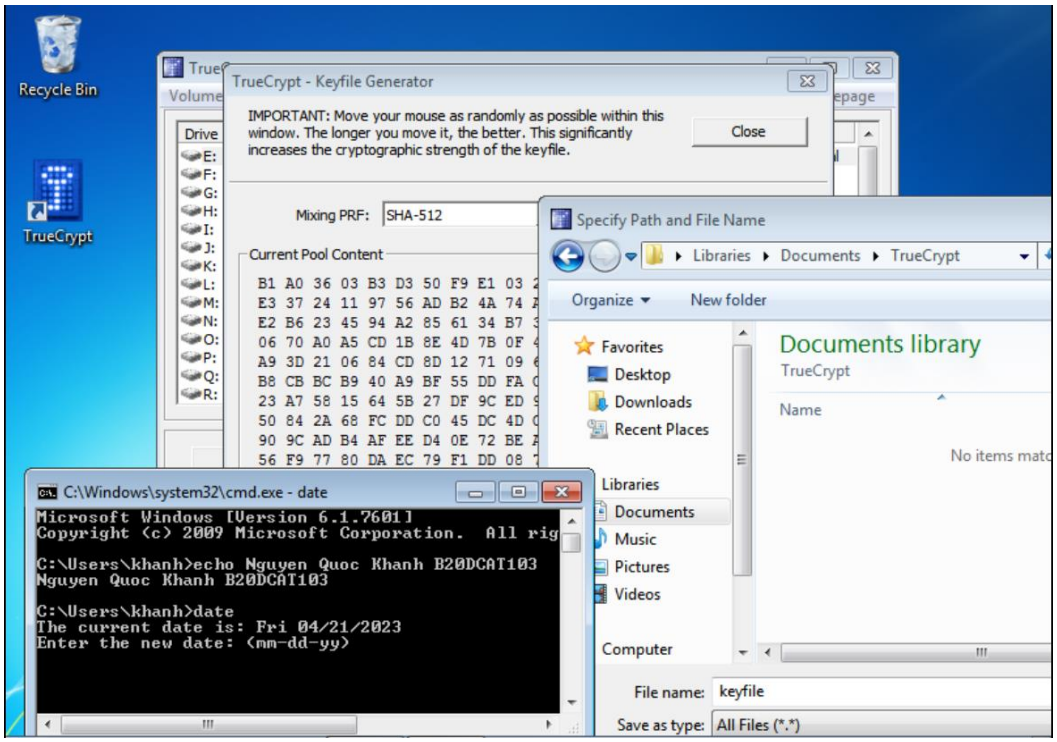


- Di chuyển chuột ngẫu nhiên trên cửa sổ để tạo ra các số ngẫu nhiên cho khóa mã hoá. Nhấn Format (Định dạng) để bắt đầu quá trình tạo ổ đĩa TrueCrypt.

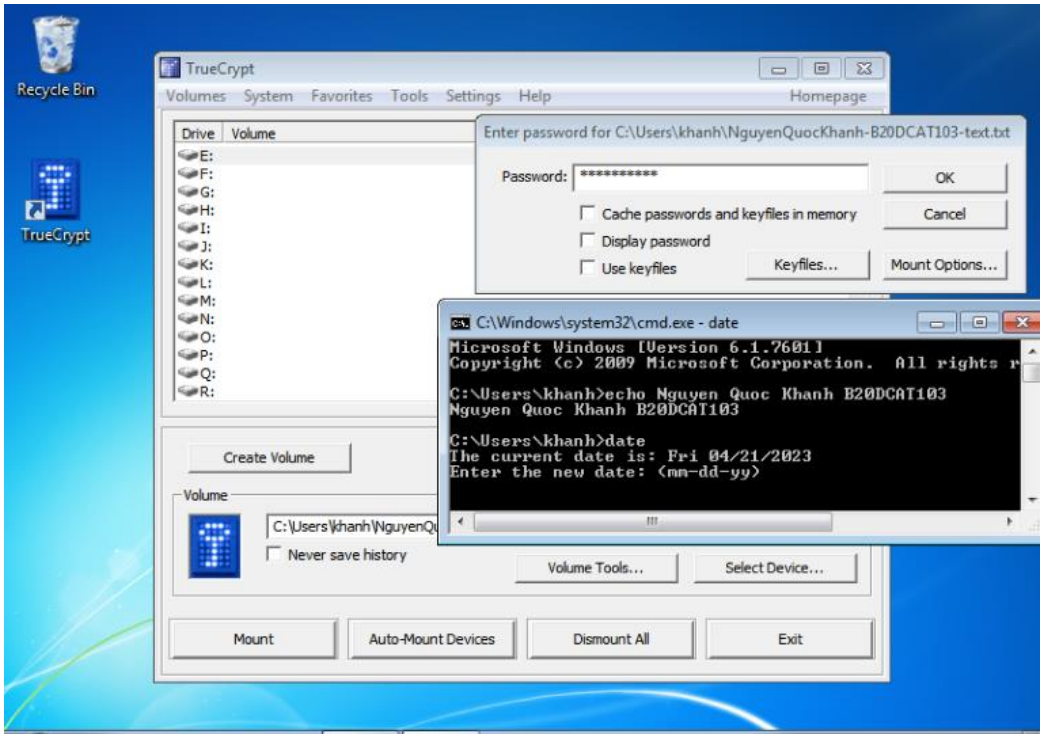


- Sau khi quá trình tạo ổ đĩa TrueCrypt hoàn tất, bạn có thể gắn kết ổ đĩa TrueCrypt bằng cách chọn nó trong danh sách Available Devices (Thiết bị có sẵn) và nhấn Mount (Gắn kết) sẽ được yêu cầu nhập mật khẩu để mở khóa ổ đĩa TrueCrypt.

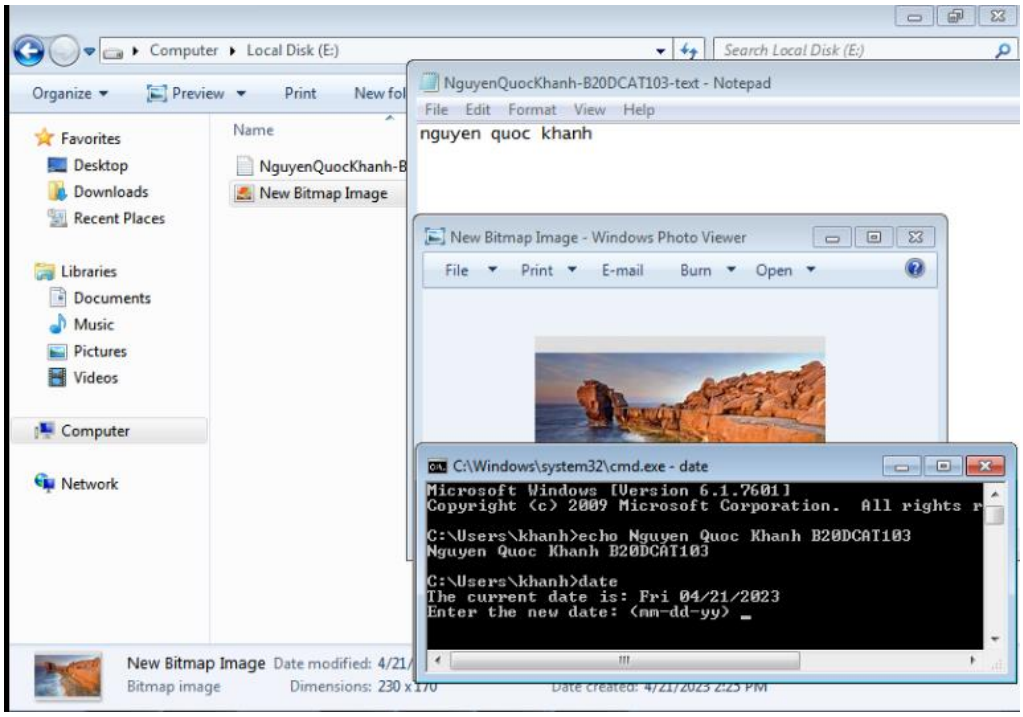




- Sau khi xong việc với file trong ổ đĩa TrueCrypt, nên hạ gắn kết ổ đĩa TrueCrypt bằng cách chọn nó trong danh sách Mounted Devices (Thiết bị đã gắn kết) và nhấn Dismount (Hạ gắn kết). Điều này sẽ bảo vệ file khỏi truy cập trái phép.



- Khôi phục file và thư mục thành công


Computer ▸ Local Disk (E:)
Search Local Disk (E:)
Organize
Preview
Print
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
NguyenQuocKhanh-B
New Bitmap Image
NguyenQuocKhanh-B20DCAT103-text - Notepad
File Edit Format View Help
nguyen quoc khanh
New Bitmap Image - Windows Photo Viewer
File Print E-mail Burn Open
C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights r
C:\Users\khanh>echo Nguyen Quoc Khanh B20DCAT103
Nguyen Quoc Khanh B20DCAT103
C:\Users\khanh>date
The current date is: Fri 04/21/2023
Enter the new date: (mm-dd-yy)
New Bitmap Image Date modified: 4/21/
Bitmap image
Dimensions: 230 x 170
Date created: 4/21/2023 2:25 PM