BỘ THÔNG TIN VÀ TRUYỀN THÔNG

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

MÔN HỌC: THỰC TẬP CƠ SỞ

BÁO CÁO BÀI THỰC HÀNH SỐ 13

Giảng viên hướng dẫn : PGS.TS Hoàng Xuân Dậu
Sinh viên thực hiện : Nguyễn Nhật Minh
Mã sinh viên : B21DCAT132

Hà Nội, tháng 3 năm 2024

Môn học: Thực tập cơ sở
Bài 13: Đảm bảo an toàn với mã hóa

1. Mục đích

- Hiểu được nguyên tăc hoạt động của các ký thuật mã hóa
- Hiểu được cách thức hoạt động của một sô công cụ mã hóa dữ liệu
- Biết sử dụng các công cụ mã hóa để đảm bảo an toàn dữ liệu

2. Tìm hiểu lí thuyết

Trong thời buổi mà phần mềm gián điệp (spyware) tung hoành thì không có gì đảm bảo các file dữ liệu sẽ bị rò rỉ. Vì vậy trên máy tính nên có 1 cái két dữ liệu giống như ngoài. Khác với két sắt, két dữ liệu có hai lớp bảo vệ: phải mở két bằng mật khẩu mới truy cập được các file ở bên trong, nội dung các file đó lại được mã hoá bằng mật khẩu, phải qua quá trình giải mã mới đọc được. Một trong những phần mềm tốt nhất để tạo một két như thế là TrueCrypt

2.1. 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 dụngtruy 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 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

2.2. 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, 192-bit 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 sau được thực hiện:

1. 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.

2. 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.

3. 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.

4. 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.

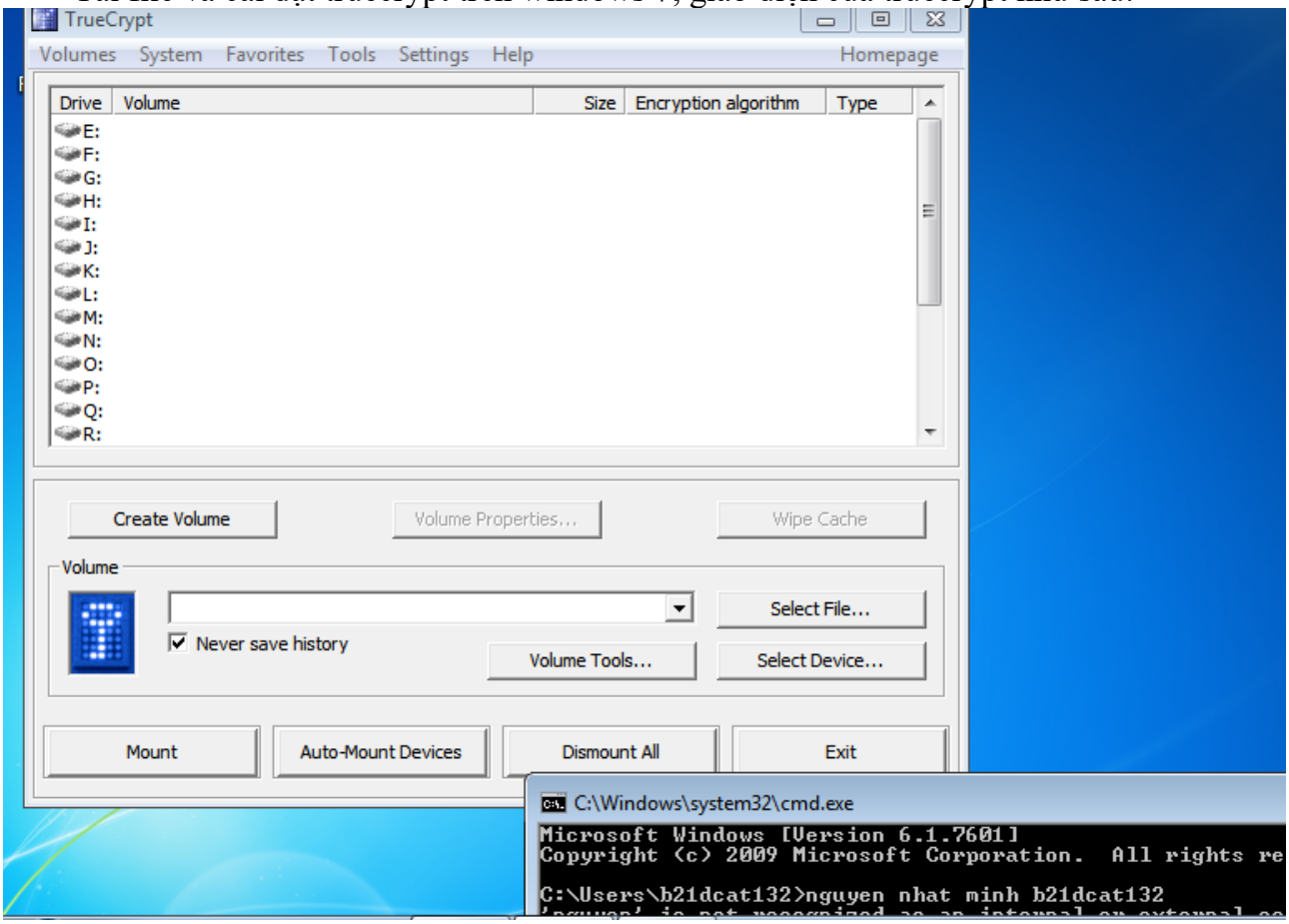
3. Chuẩn bị môi trường

- Máy ảo windows7 và cài đặt truecrypt

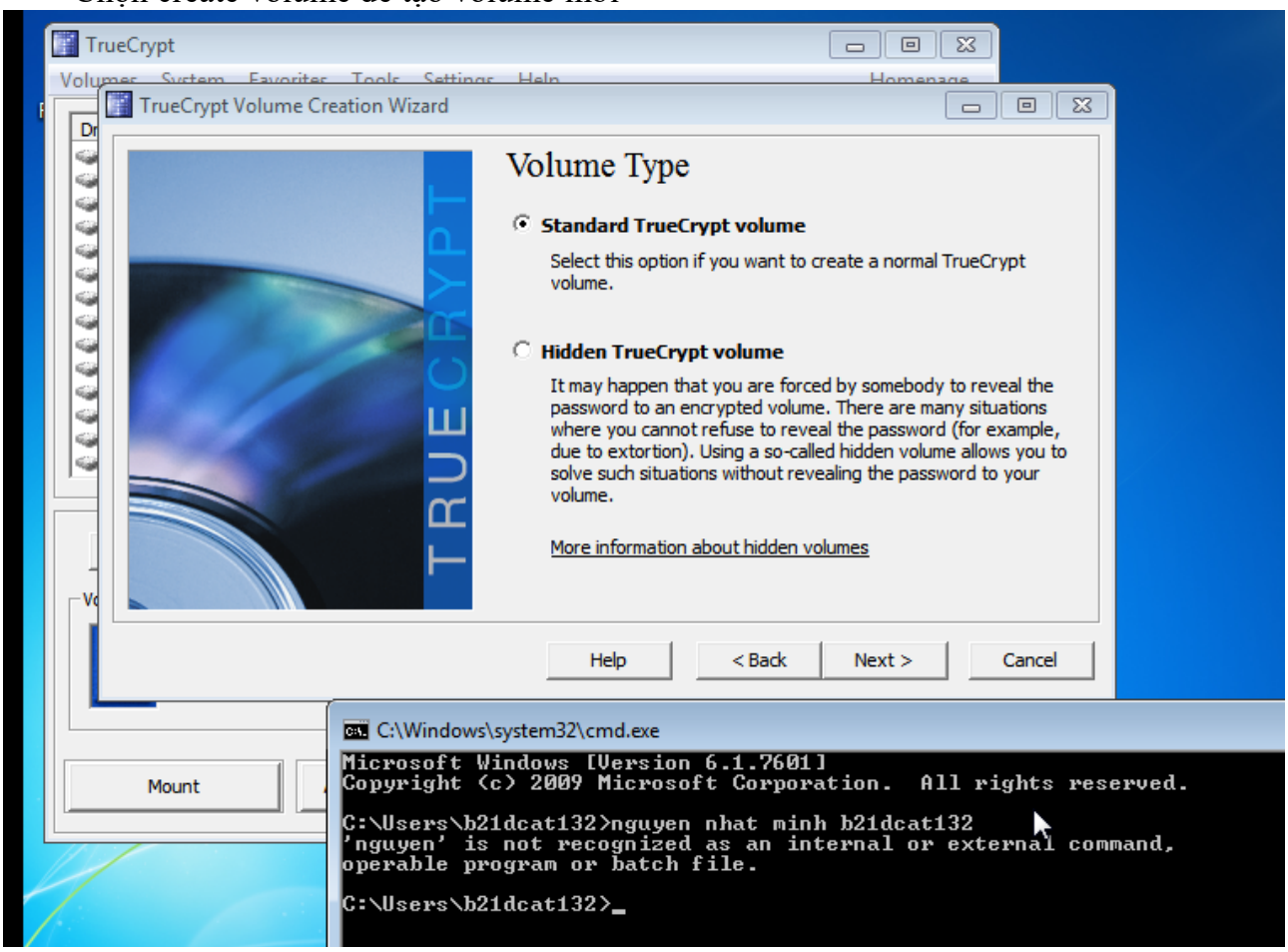
4. Thực hành

4.1. Cài đặt truecrypt và tạo volume

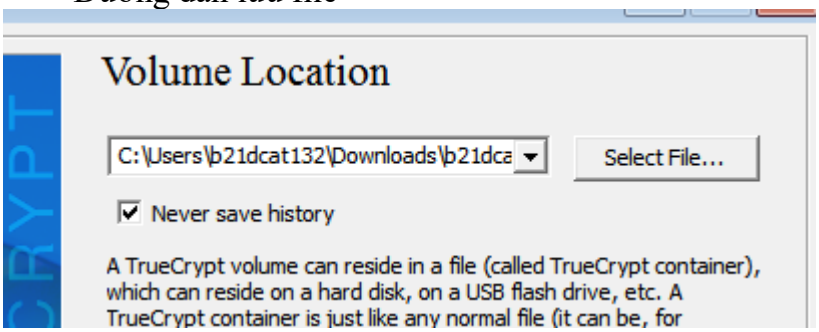
- Tải file và cài đặt truecrypt trên windows 7, giao diện của truecrypt như sau:



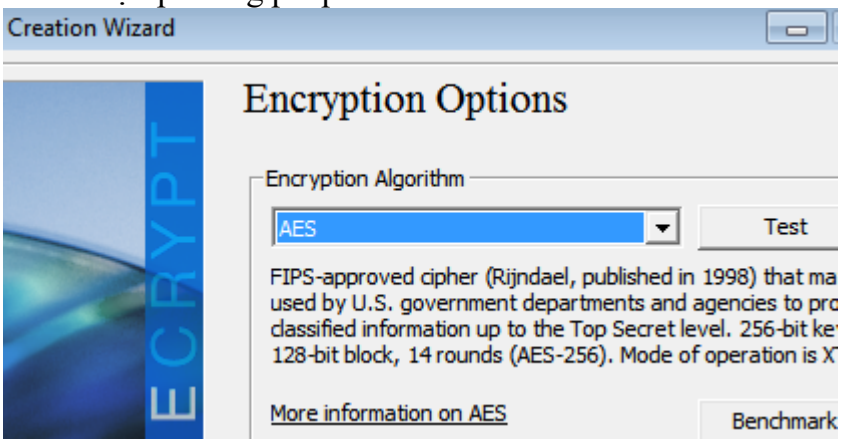
- Chọn create volume để tạo volume mới



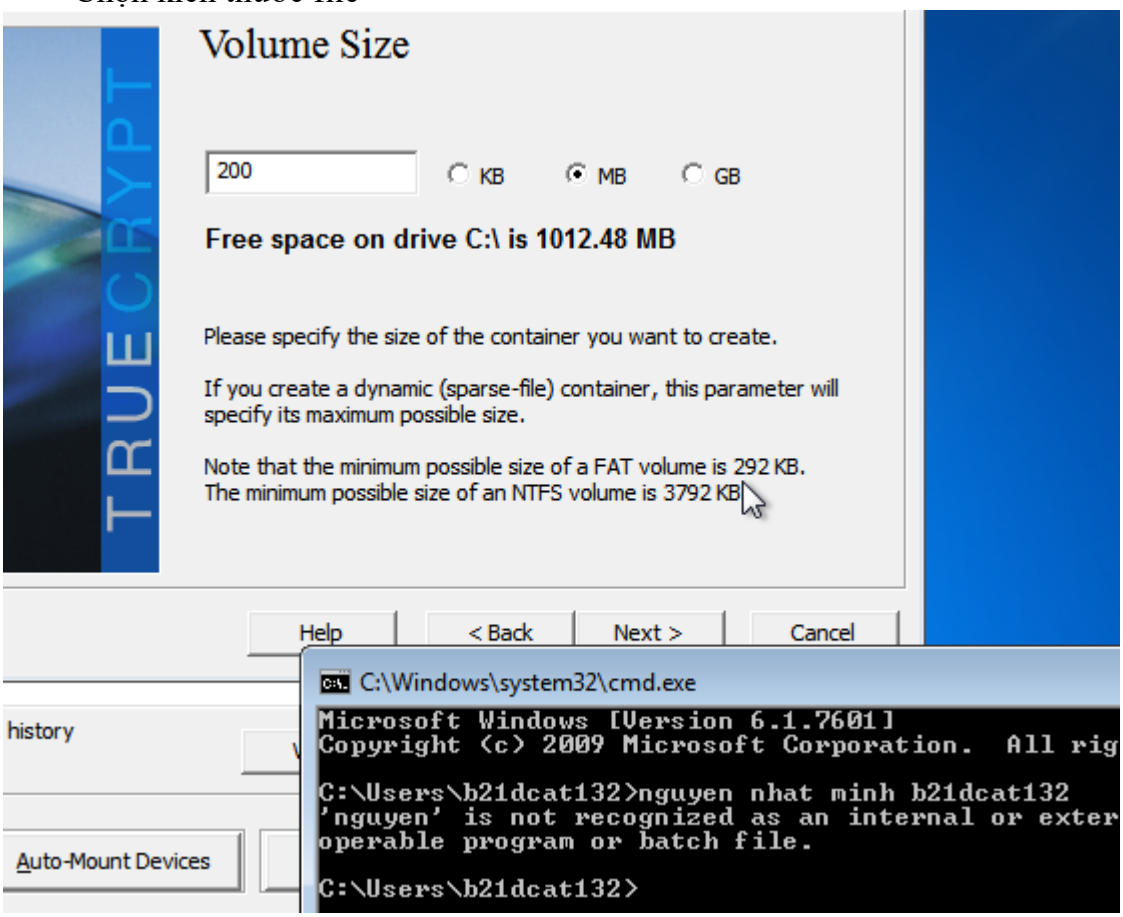
- Đường dẫn lưu file



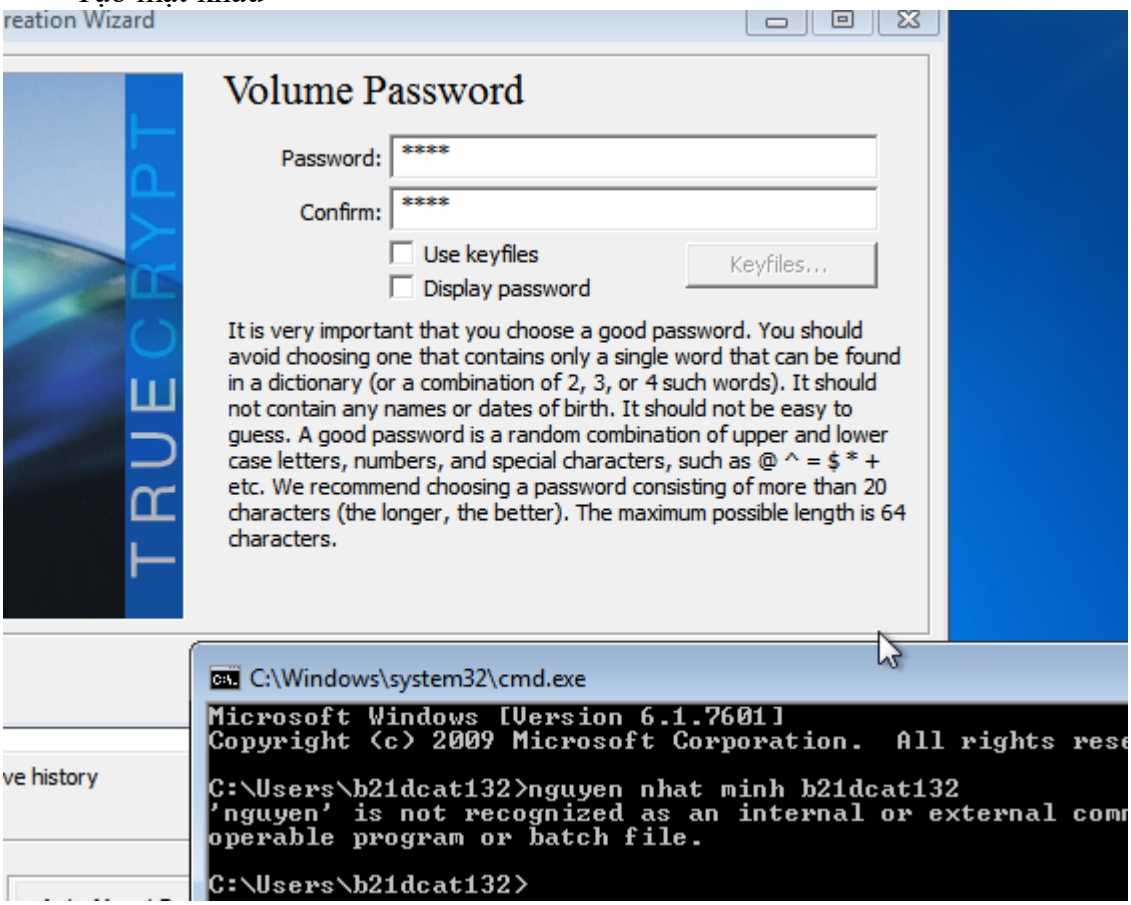
- Chọn phương pháp mã hóa



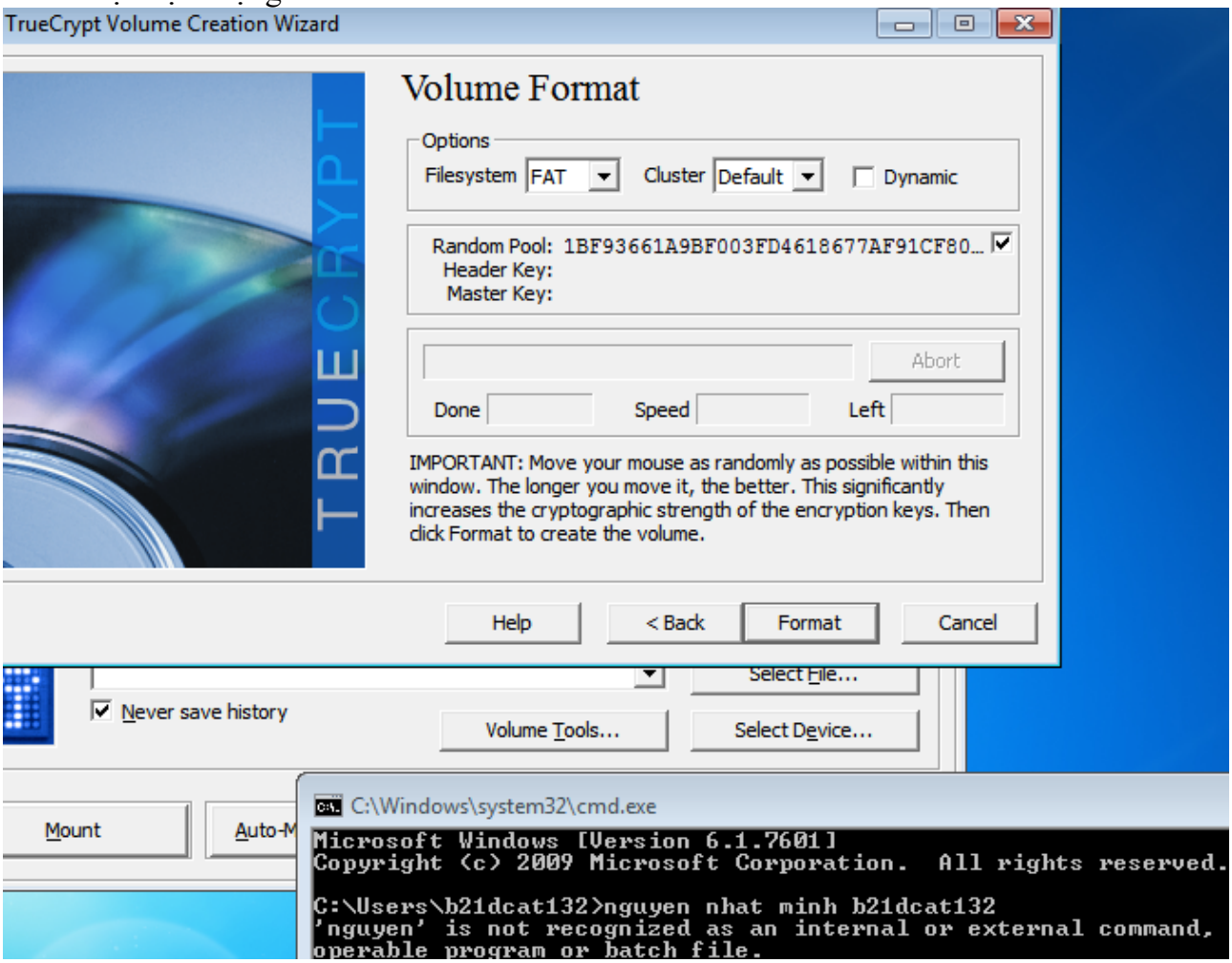
- Chọn kích thước file



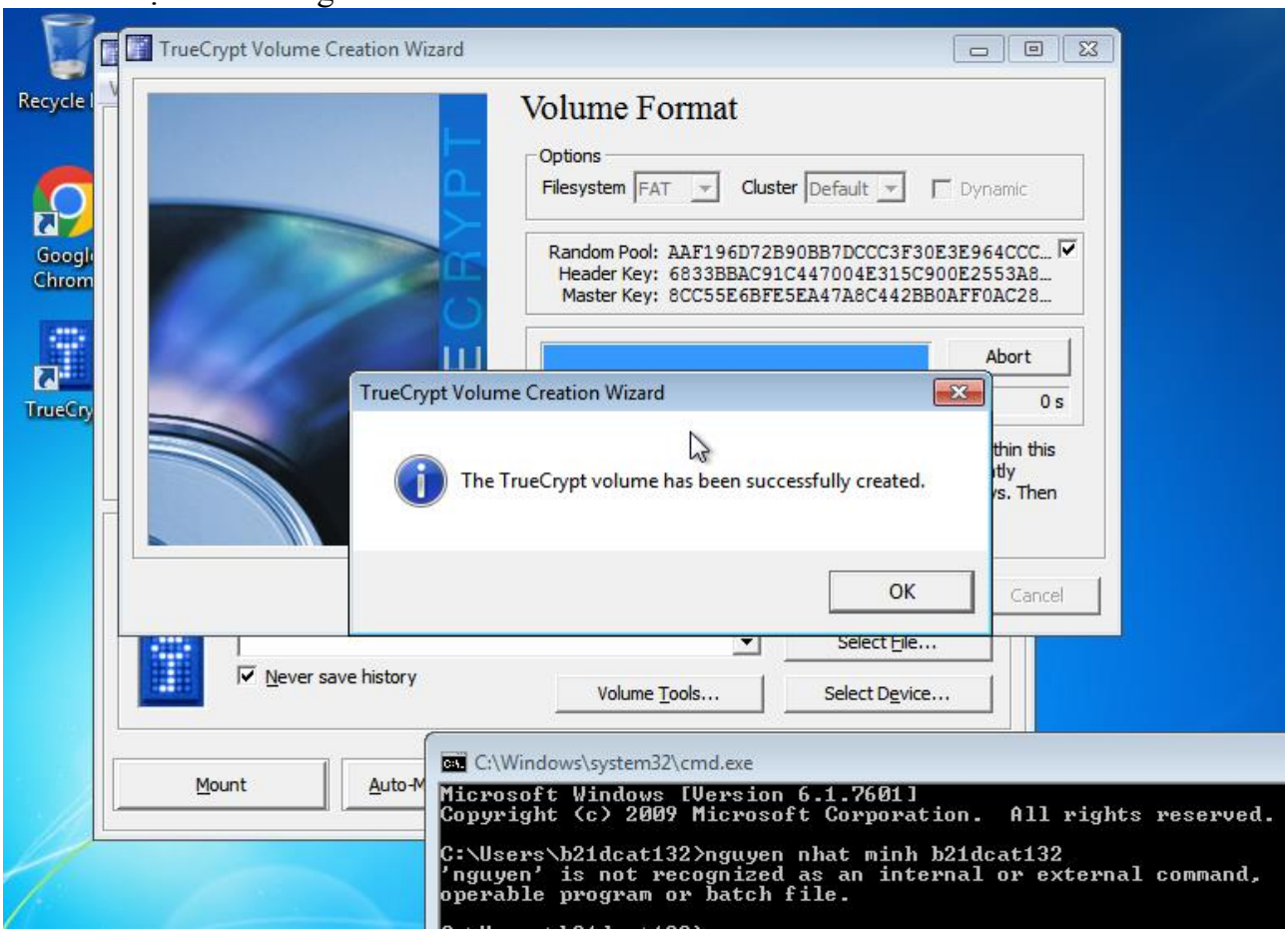
- Tạo mật khẩu


reation Wizard
Volume Password
Password:
****
Confirm:
****
Use keyfiles
Keyfiles...
Display password
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.
TRUECRYPT
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights rese
C:\Users\b21dcat132>nguyen nhat minh b21dcat132
'nguyen' is not recognized as an internal or external comm
operable program or batch file.
C:\Users\b21dcat132>
ve history

- Chọn định dạng của volume

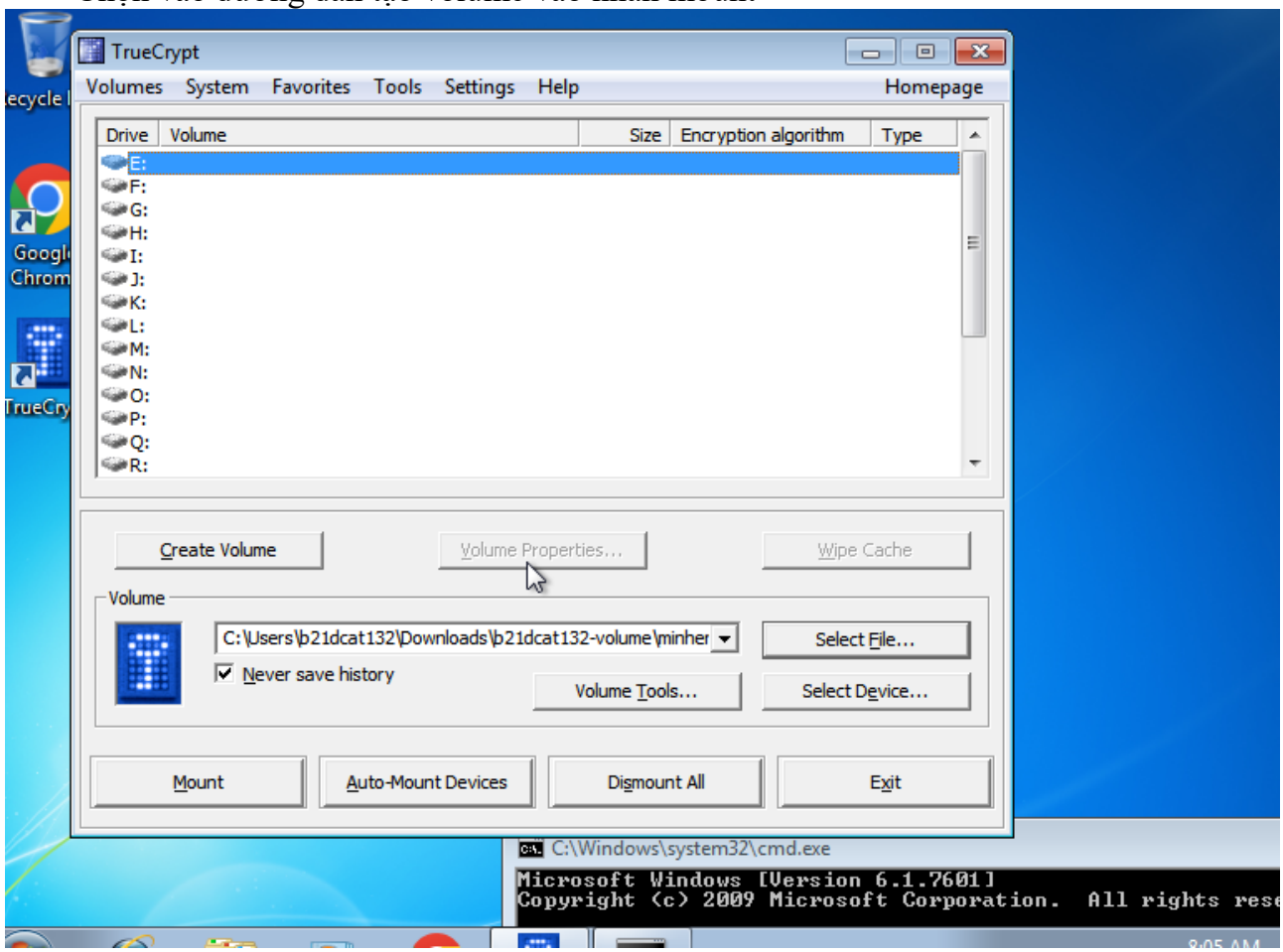


- Cài đặt thành công

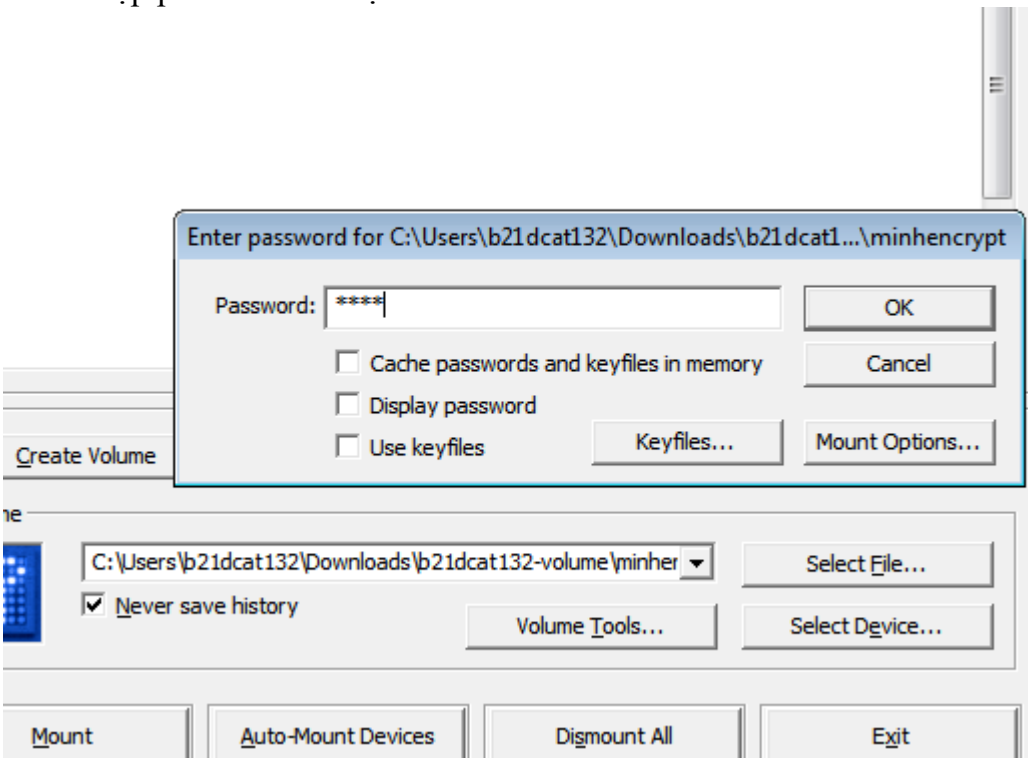


4.2. Gắn vùng mã hóa chuẩn

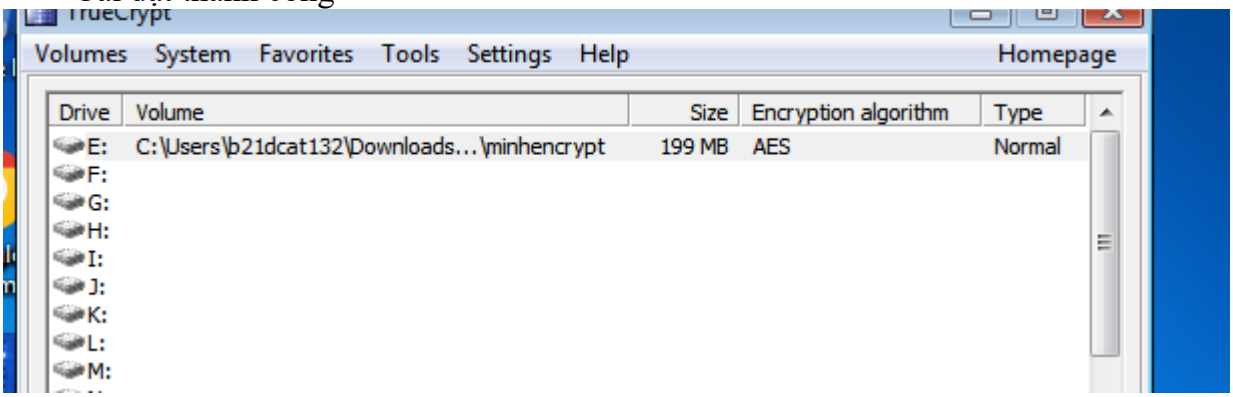
- Tiếp theo ta cần gắn vùng mã hóa chuẩn
- Chọn vào đường dẫn tạo volume vào nhấn mount



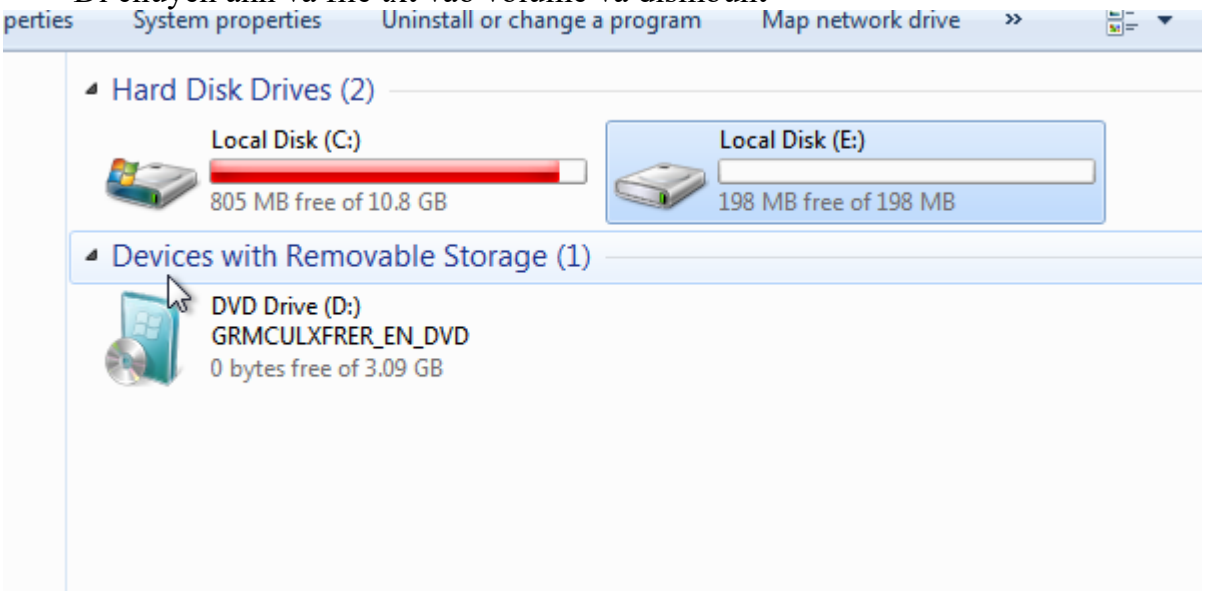
- Nhập password vừa tạo

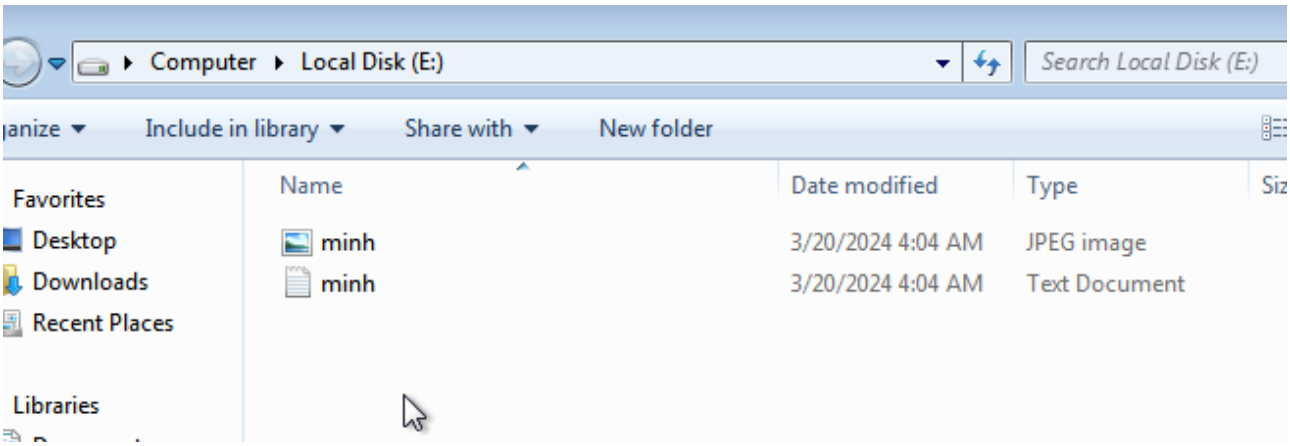


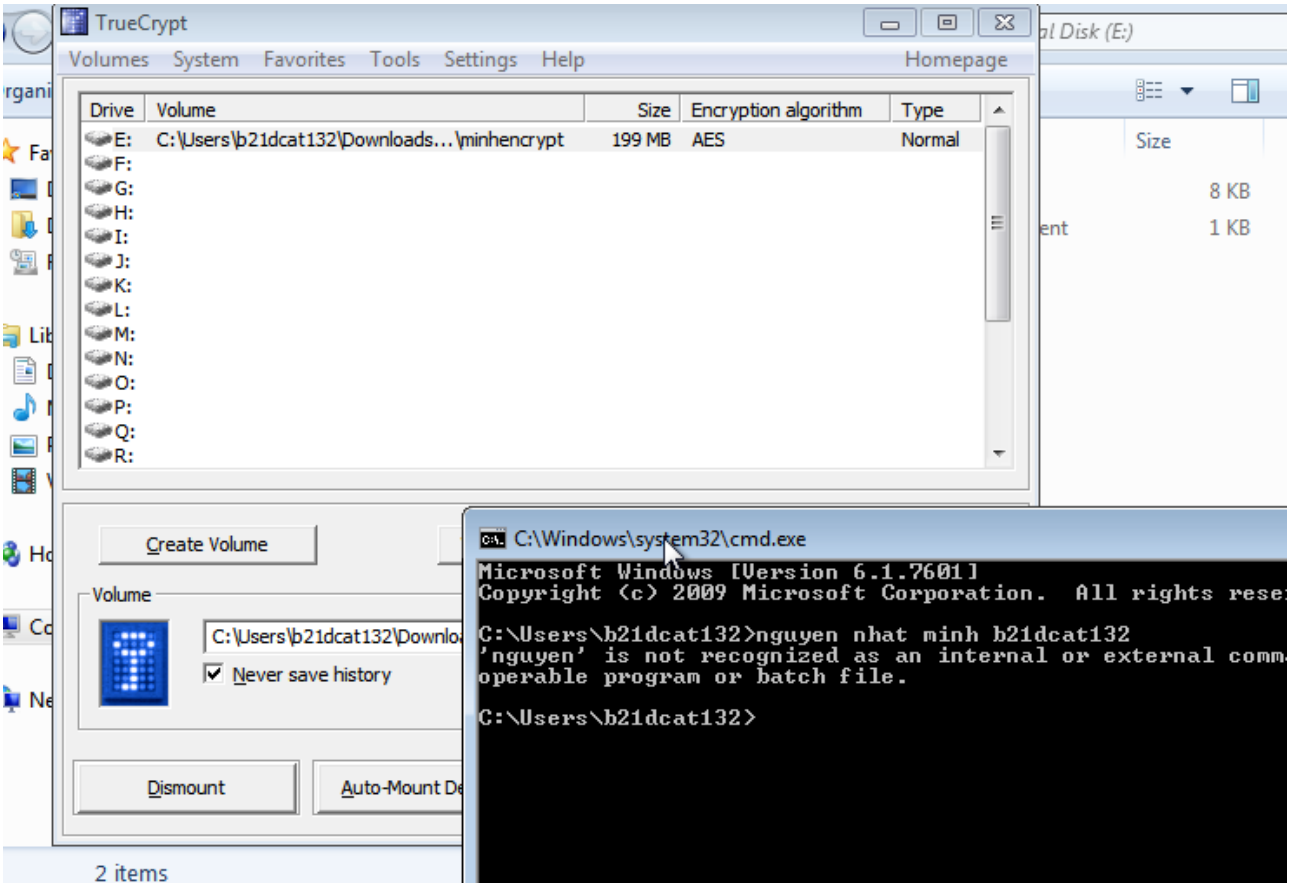
- Cài đặt thành công



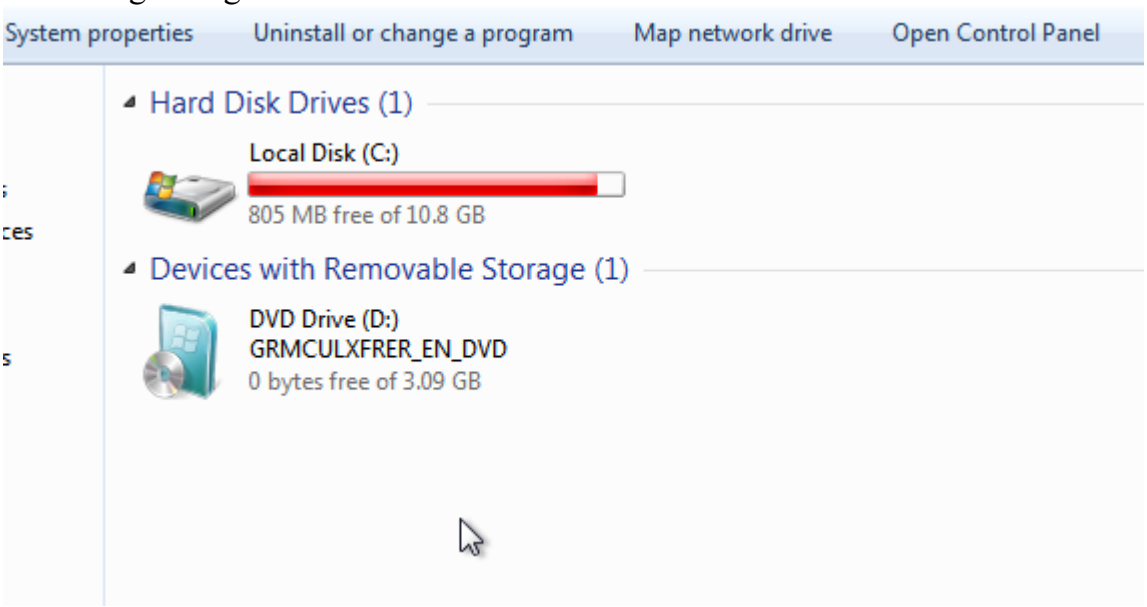
- Di chuyển ảnh và file txt vào volume và dismount





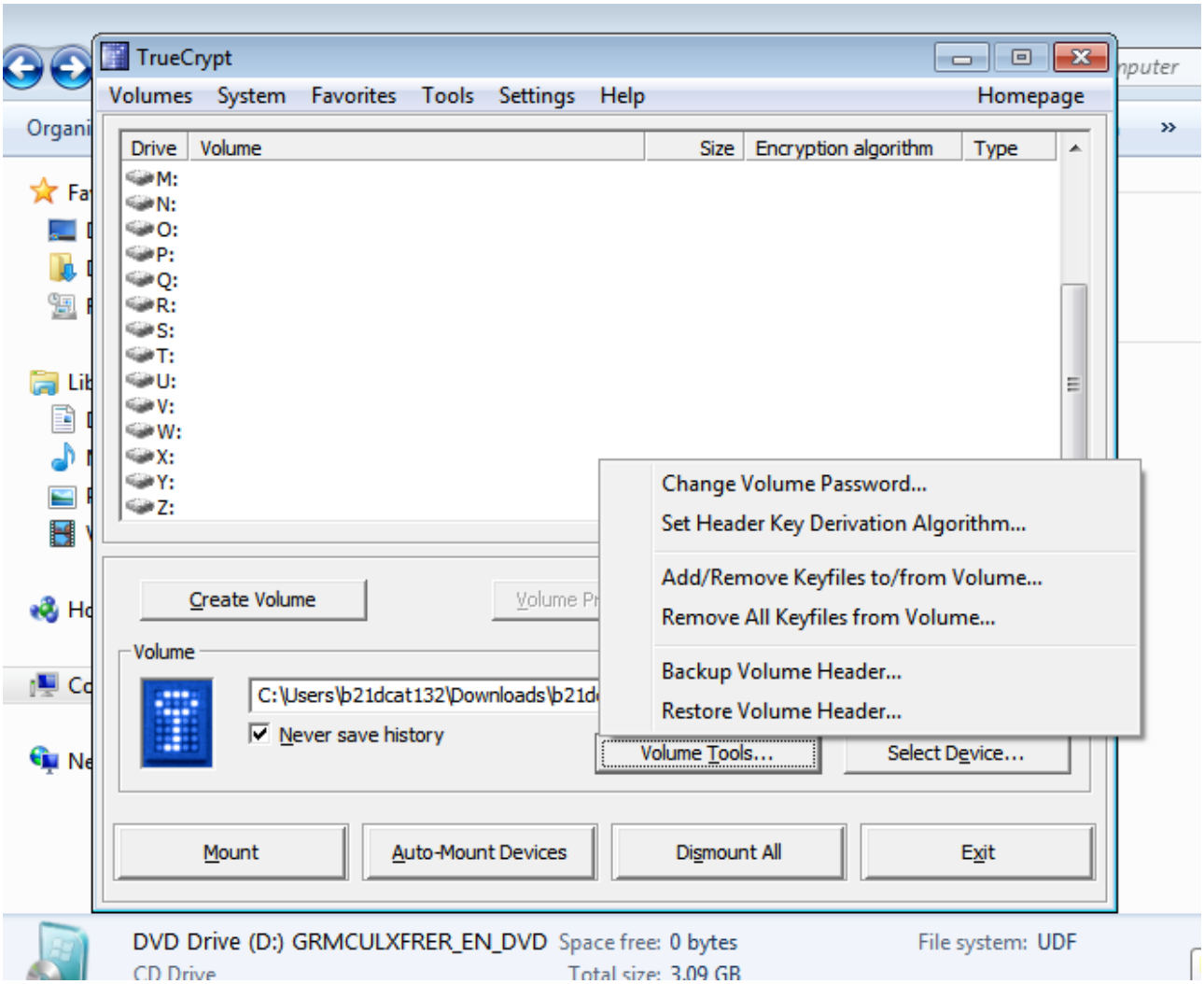


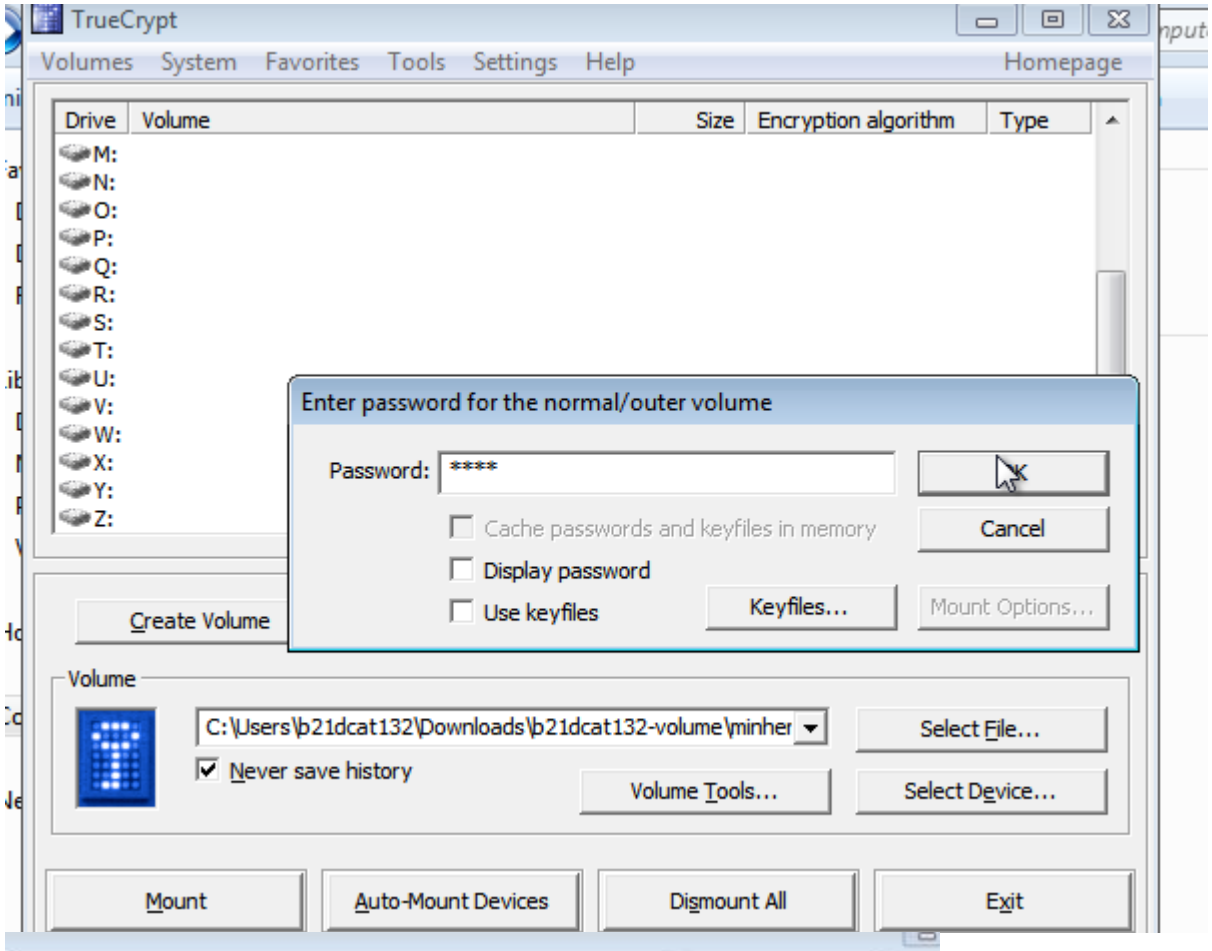
- Sau khi dismount, khi truy cập từ bên ngoài, người dùng không thể xem nội dung file
- Bằng chứng là ổ đĩa E đã biến mất

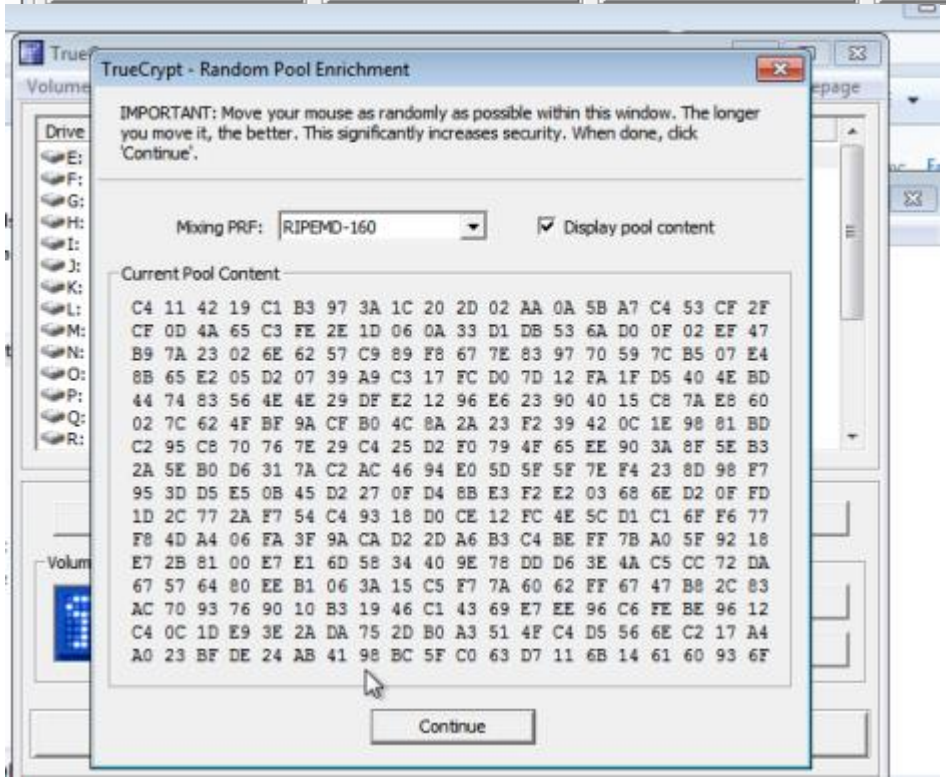


4.3. Sao lưu mã hóa

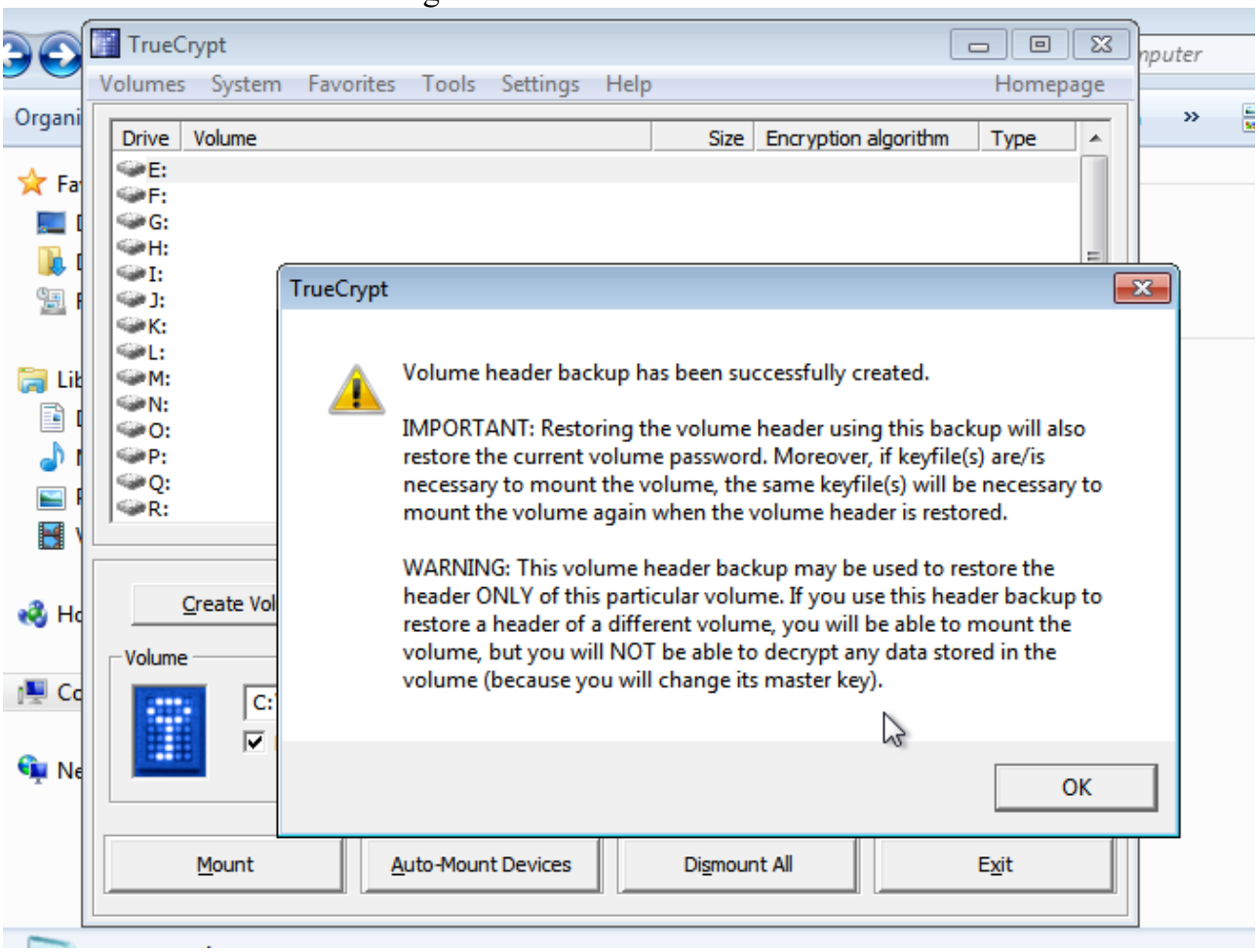
- Chọn vào vùng mã hóa, chọn volume tools, chọn backup volume header.
- Header là nơi lưu trữ mã hóa




TrueCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption algorithm Type
M:
N:
O:
P:
Q:
R:
S:
T:
U:
V:
W:
X:
Y:
Z:
Enter password for the normal/outer volume
Password: ****
OK
Cancel
Cache passwords and keyfiles in memory
Display password
Use keyfiles
Keyfiles...
Mount Options...
Create Volume
Volume
C:\Users\b21dcat132\Downloads\b21dcat132-volume\minher
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

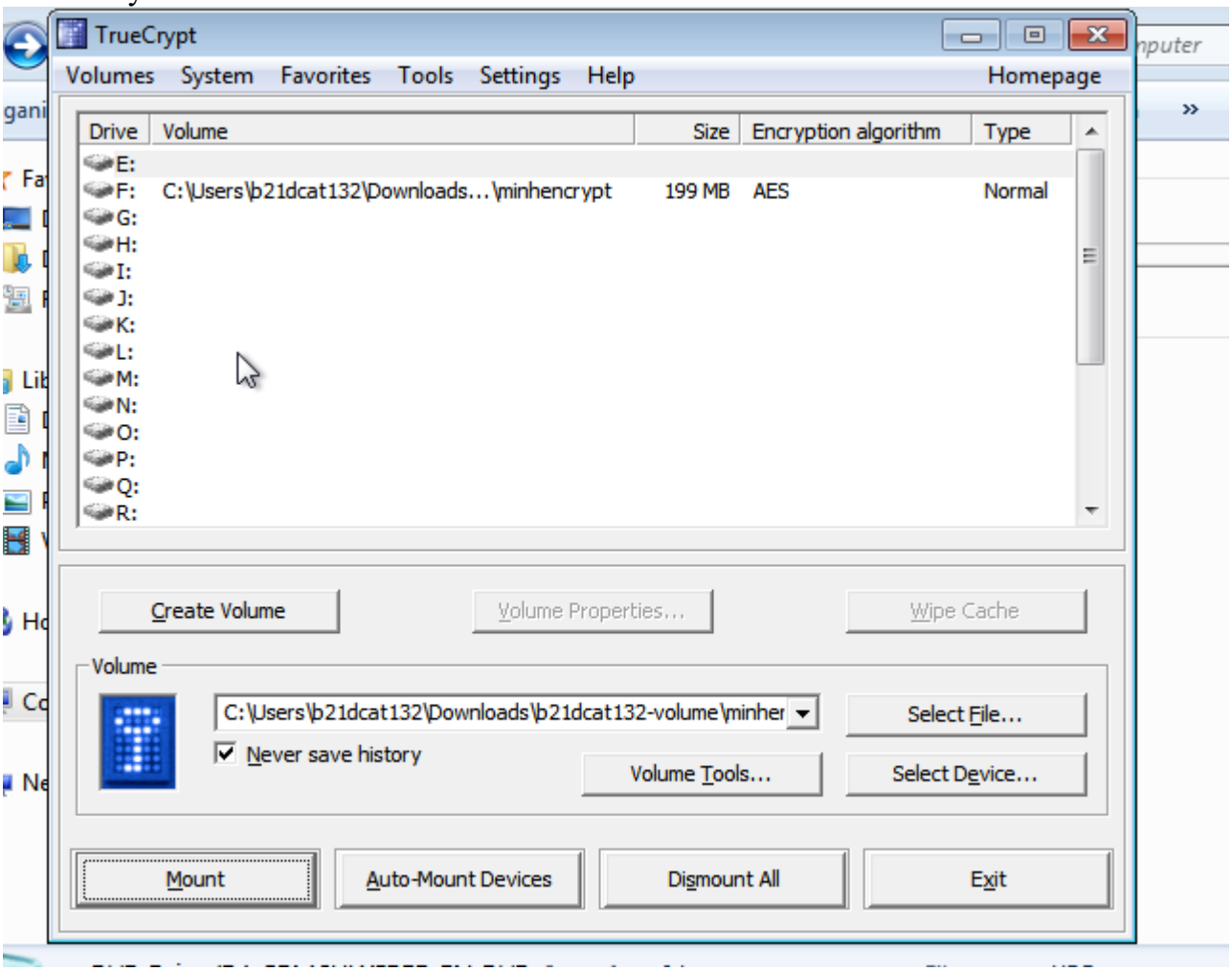

TrueCrypt - Random Pool Enrichment
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases security. When done, click 'Continue'.
Mixing PRF: RIPEMD-160
Display pool content
Current Pool Content
C4 11 42 19 C1 B3 97 3A 1C 20 2D 02 AA 0A 5B A7 C4 53 CF 2F
CF 0D 4A 65 C3 FE 2E 1D 06 0A 33 D1 DB 53 6A D0 0F 02 EF 47
B9 7A 23 02 6E 62 57 C9 89 F8 67 7E 83 97 70 59 7C B5 07 E4
8B 65 E2 05 D2 07 39 A9 C3 17 FC D0 7D 12 FA 1F D5 40 4E BD
44 74 83 56 4E 4E 29 DF E2 12 96 E6 23 90 40 15 C8 7A E8 60
02 7C 62 4F BF 9A CF B0 4C 8A 2A 23 F2 39 42 0C 1E 98 81 BD
C2 95 C8 70 76 7E 29 C4 25 D2 F0 79 4F 65 EE 90 3A 8F 5E B3
2A 5E B0 D6 31 7A C2 AC 46 94 E0 5D 5F 5F 7E F4 23 8D 98 F7
95 3D D5 E5 0B 45 D2 27 0F D4 8B E3 F2 E2 03 68 6E D2 0F FD
1D 2C 77 2A F7 54 C4 93 18 D0 CE 12 FC 4E 5C D1 C1 6F F6 77
F8 4D A4 06 FA 3F 9A CA D2 2D A6 B3 C4 BE FF 7B A0 5F 92 18
E7 2B 81 00 E7 E1 6D 58 34 40 9E 78 DD D6 3E 4A C5 CC 72 DA
67 57 64 80 EE B1 06 3A 15 C5 F7 7A 60 62 FF 67 47 B8 2C 83
AC 70 93 76 90 10 B3 19 46 C1 43 69 E7 EE 96 C6 FE BE 96 12
C4 0C 1D E9 3E 2A DA 75 2D B0 A3 51 4F C4 D5 56 6E C2 17 A4
A0 23 BF DE 24 AB 41 98 BC 5F C0 63 D7 11 6B 14 61 60 93 6F
Continue

- Sao lưu mã hóa thành công

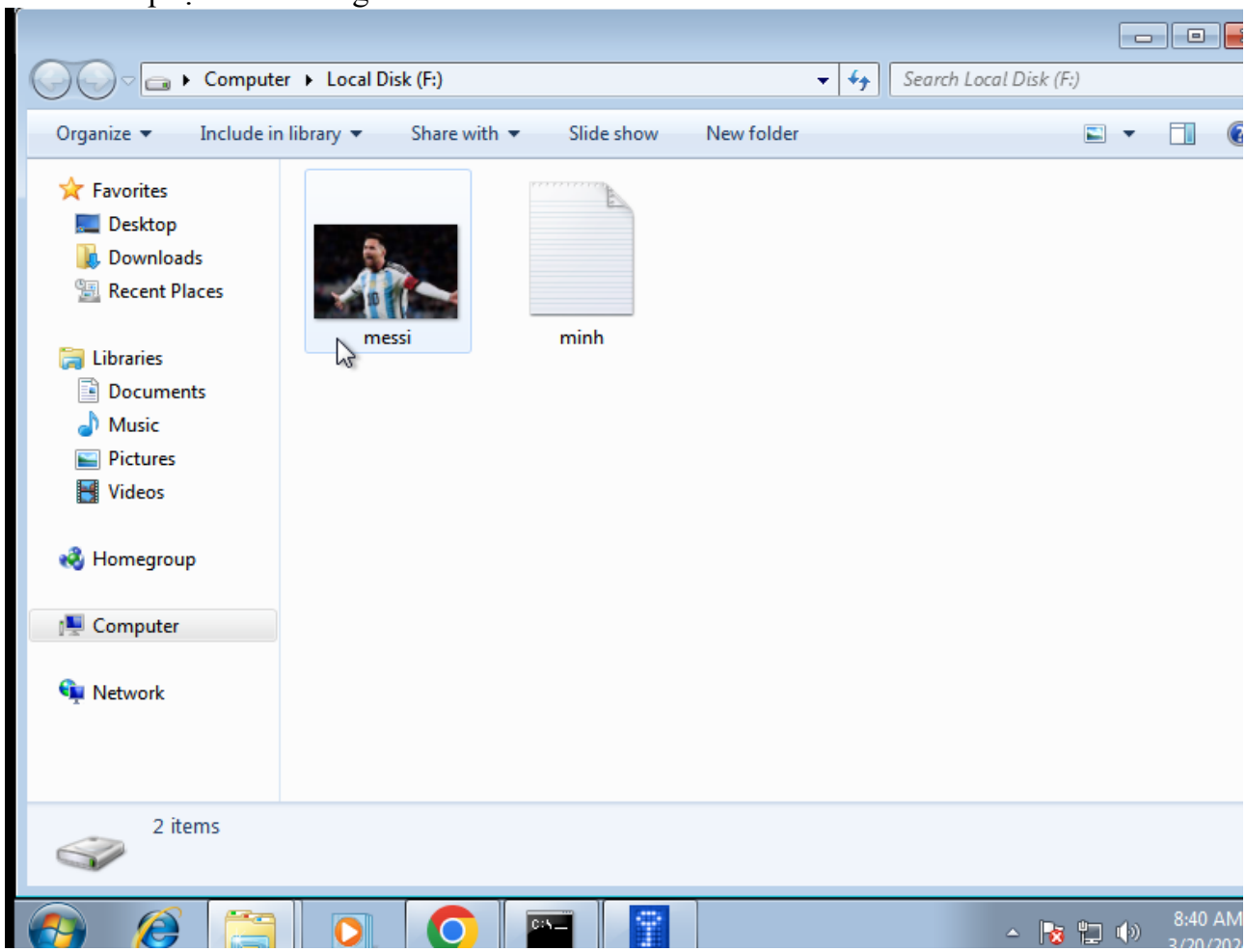


4.4. Khôi phục file và thư mục đã mã hóa

- Đơn giản là chỉ cần mount lại vào 1 volume là có thể khôi phục lại được file
- ở đây em mount vào ổ F



- Khôi phục thành công



5. Kết luận

- Bài thực hành hoàn thành vào ngày 20/03/2024