HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BÀI BÁO CÁO THỰC HÀNH SỐ 13

MÔN THỰC TẬP CƠ SỞ

ĐẢM BẢO AN TOÀN VỚI MÃ HÓA

Tên sinh viên: Ninh Chí Hướng

Mã sinh viên: B20DCAT094

Số điện thoại: 0353770347

Giảng viên hướng dẫn : Th.s Ninh Thị Thu Trang

HÀ NỘI, THÁNG 5/2023

Contents

I. Tìm hiểu lý thuyết

1. Tìm hiểu về Truecrypt

1.1 Cách hoạt động :

TrueCrypt là một phần mềm mã hóa dữ liệu mã nguồn mở, được sử dụng để tạo ra các file ảo hoặc các phân vùng ổ đĩa ảo được mã hóa, nhằm bảo vệ dữ liệu trước khi lưu trữ hoặc truyền tải trên Internet.

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. Dữ liệu được lưu trữ trên một ổ đĩa đã được mã hóa (encryption volume) không thể đọc được nếu người dùng không cung cấp đúng khóa mã hóa bằng một trong ba hình thức là mật khẩu (password) hoặc 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...). Dữ liệu có thể được copy từ một ổ đĩa mã hóa của TrueCrypt sang một ổ đĩa bình thường không mã hóa trên Windows (và ngược lại) một cách bình thường mà không có sự khác biệt nào cả, kể cả các thao tác kéo-thả.

Khi sử dụng TrueCrypt, người dùng cần chọn một vùng dữ liệu (ổ đĩa hoặc phân vùng) để mã hóa. Sau đó, phần mềm sẽ sử dụng các thuật toán mã hóa như AES, Serpent hoặc Twofish để mã hóa dữ liệu. Người dùng cần cung cấp mật khẩu để truy cập vào vùng dữ liệu đã mã hóa, nếu không, dữ liệu sẽ không thể đọc được.

Khi người dùng muốn truy cập vào dữ liệu đã mã hóa, phần mềm sẽ yêu cầu mật khẩu và sử dụng nó để giải mã dữ liệu. Sau đó, dữ liệu được hiển thị như bình thường trên máy tính của người dùng.

TrueCrypt cũng hỗ trợ việc tạo ra các file ảo chứa dữ liệu mã hóa. Người dùng có thể tạo ra một file ảo, chọn mật khẩu để mã hóa nó và sau đó lưu trữ file ảo này trên ổ đĩa hoặc trên các thiết bị lưu trữ khác. Khi muốn truy cập vào dữ liệu trong file ảo, người dùng chỉ cần mở file ảo và nhập mật khẩu để giải mã dữ liệu.

1.2 Mã hóa một file với TrueCrypt

Để mã hóa một file với TrueCrypt, bạn cần thực hiện các bước sau:

1. Tải và cài đặt phần mềm TrueCrypt trên máy tính của bạn.
2. Mở phần mềm TrueCrypt và chọn "Create Volume".
3. Trong hộp thoại "TrueCrypt Volume Creation Wizard", chọn "Create a file container". Điều này sẽ cho phép bạn tạo ra một file ảo để lưu trữ dữ liệu mã hóa.
4. Chọn nơi lưu trữ file ảo và đặt tên cho file ảo đó.

5. Chọn loại mã hóa mà bạn muốn sử dụng để bảo vệ file ảo. TrueCrypt hỗ trợ nhiều loại mã hóa, bao gồm AES, Serpent và Twofish.
6. Thiết lập kích thước của file ảo và cung cấp mật khẩu để truy cập vào file ảo.
7. Sau khi hoàn thành các thiết lập, chọn "Format" để tạo ra file ảo.
8. Khi file ảo đã được tạo, bạn có thể mở file ảo và chọn "Mount" để kết nối file ảo với một ổ đĩa ảo trên máy tính. Bạn sẽ được yêu cầu nhập mật khẩu để truy cập vào dữ liệu được lưu trữ trong file ảo.
9. Sau khi ổ đĩa ảo đã được kết nối, bạn có thể sao chép các file cần mã hóa vào ổ đĩa ảo này.
10. Khi hoàn tất, bạn có thể tháo ổ đĩa ảo bằng cách chọn "Dismount" trong phần mềm TrueCrypt. Các file văn bản bên trong file ảo sẽ được tự động mã hóa khi ổ đĩa ảo bị tháo ra.

1.3 Sao lưu khóa mã hóa

TrueCrypt cung cấp cho người dùng khả năng sao lưu khóa mã hóa (recovery key), cho phép bạn khôi phục lại dữ liệu của mình trong trường hợp bạn quên mật khẩu hoặc không thể truy cập vào tệp tin mã hóa. Sau đây là các bước để sao lưu khóa mã hóa bằng TrueCrypt:
1. Mở phần mềm TrueCrypt trên máy tính của bạn.
2. Nhấn vào nút "Volumes" trên giao diện chính của TrueCrypt, sau đó chọn "Create Volume" để tạo một ổ đĩa mã hóa mới.
3. Trong cửa sổ "TrueCrypt Volume Creation Wizard", chọn "Create an encrypted file container" và chọn nơi lưu trữ tệp tin container của bạn.
4. Đặt tên cho tệp tin container và chọn loại mã hóa bạn muốn sử dụng.
5. Đặt kích thước tối đa của tệp tin container và nhập mật khẩu để truy cập vào nó.
6. Nhấn vào nút "Next" và chọn "Create keyfile in order to enable plausible deniability." (Tạo khóa mã hóa để bảo vệ tính năng chối bỏ được.)
7. Chọn loại khóa mã hóa mà bạn muốn sử dụng và tiếp tục theo hướng dẫn trên màn hình.
8. Sử dụng các tùy chọn khác để tùy chỉnh các thiết lập thông tin cho tệp tin container của bạn.
9. Nhấn vào nút "Next" và kiểm tra lại các thiết lập của bạn. Nếu mọi thứ đều chính xác, nhấn vào nút "Create" để tạo tệp tin container.
10. Sau khi tạo tệp tin container, chọn tệp tin đó trong phần mềm TrueCrypt và nhấn vào nút "Volumes" trên giao diện chính. Chọn "Backup Volume Header" để sao lưu khóa mã hóa của bạn.
11. Chọn nơi lưu trữ khóa mã hóa của bạn và nhập mật khẩu để xác nhận tài khoản của bạn.
12. Khi hoàn tất, sao lưu file khóa mã hóa của bạn ở một địa điểm an toàn và không bị mất hoặc hư hỏng.

Lưu ý rằng việc sao lưu khóa mã hóa là rất quan trọng để đảm bảo tính bảo mật của dữ liệu của bạn. Nếu bạn không sao lưu khóa mã hóa và quên mật khẩu hoặc

không thể truy cập vào tệp tin mã hóa, bạn có thể không thể khôi phục lại dữ liệu của mình.

II. Tiến hành thực hành

2.1. Chuẩn bị môi trường

• Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm ảo hóa khác.
• Công cụ TrueCrypt

2.2. Các bước thực hiện

2.2.1. Chuẩn bị môi trường

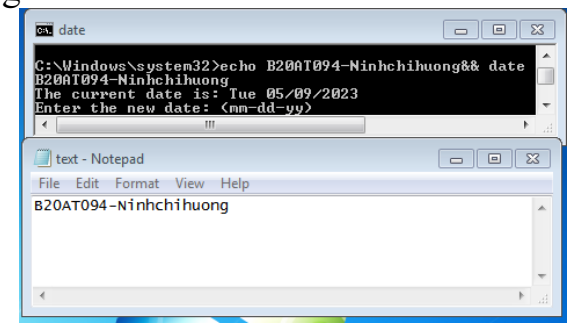
• Cài đặt công cụ ảo hóa.
• Cài đặt máy ảo chạy hệ điều hành Windows.
• Cài đặt TrueCrypt trên hệ điều hành windows.

2.2.2. Nội dung thử nghiệm

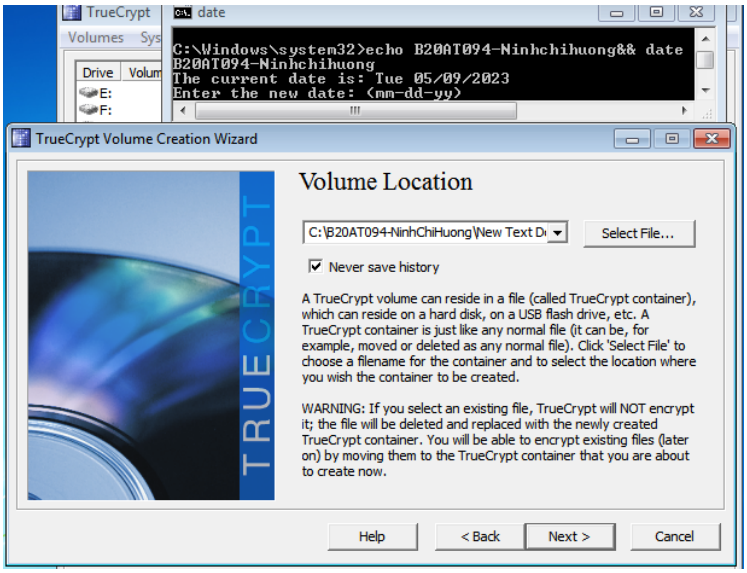
- Sử dụng công cụ TrueCrypt để hóa mã file. Yêu cầu thực hiện trên ít nhất 2 loại file bao gồm: file văn bản và file đa phương tiện (định dạng ảnh, video, hoặc âm thanh).

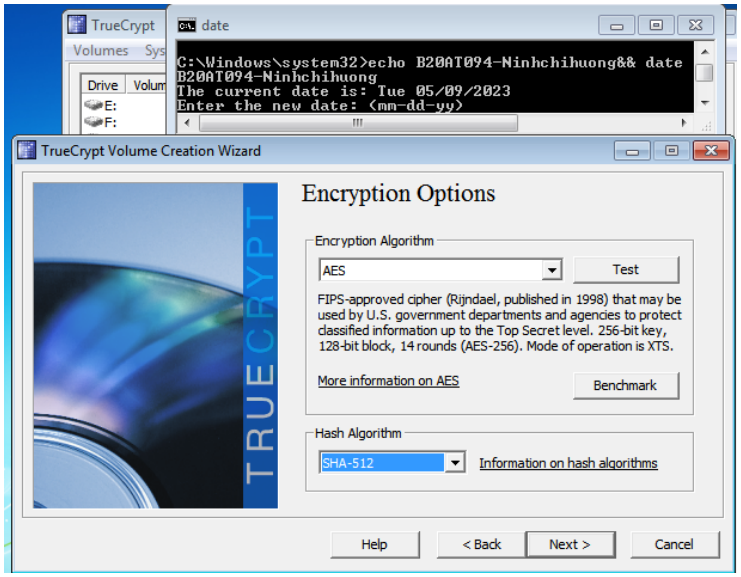
2.2.2.1 Mã hóa file văn bản

Tạo file văn bản, nội dung file như sau:

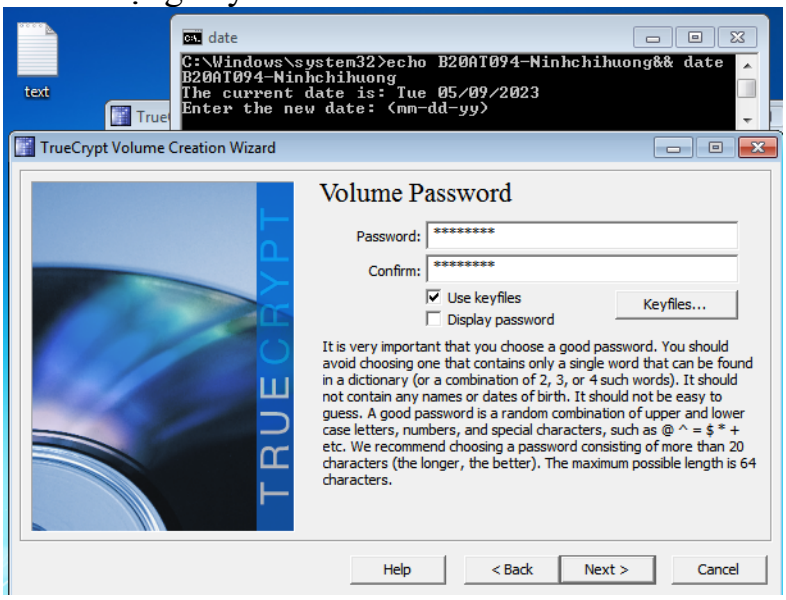


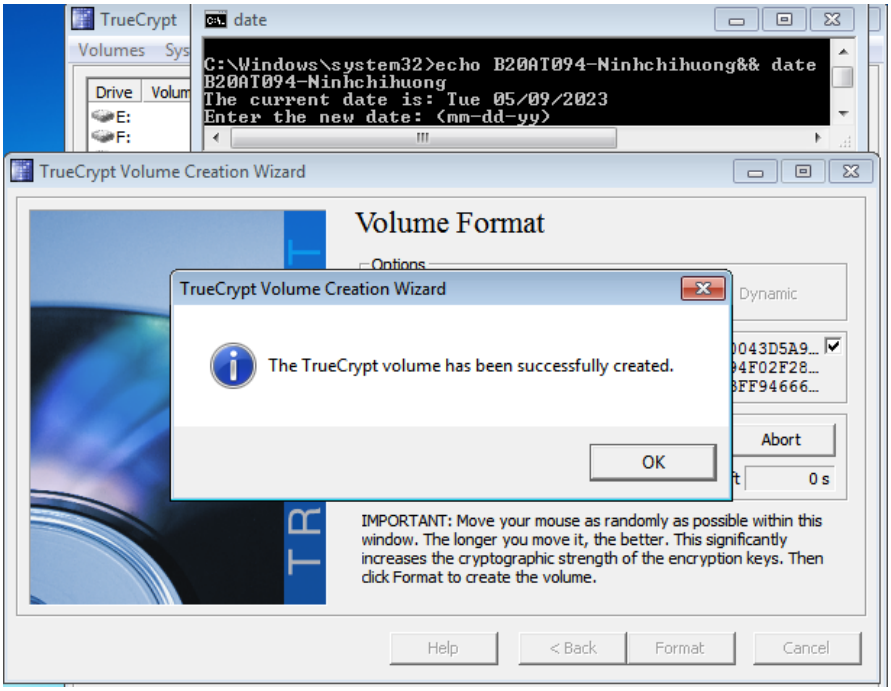
Tạo một ổ đĩa ảo để đưa file văn bản trên vào đó :



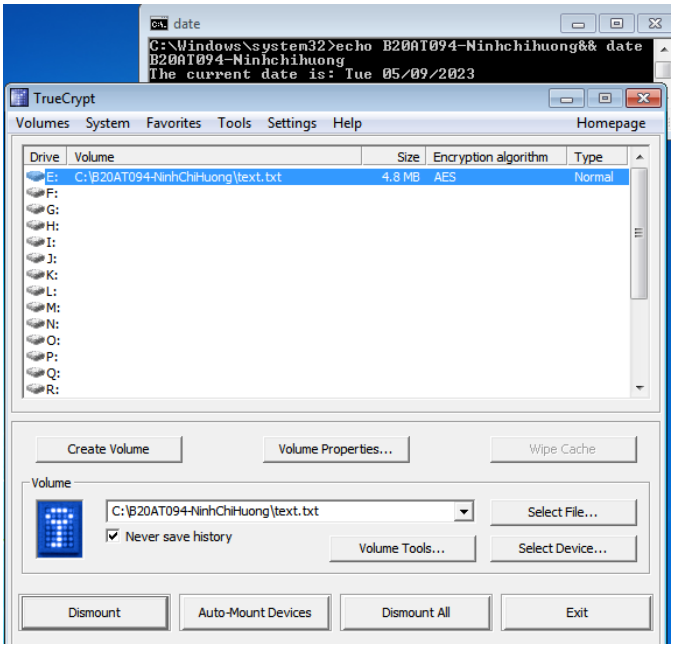


Nhập password và sử dụng keyfile

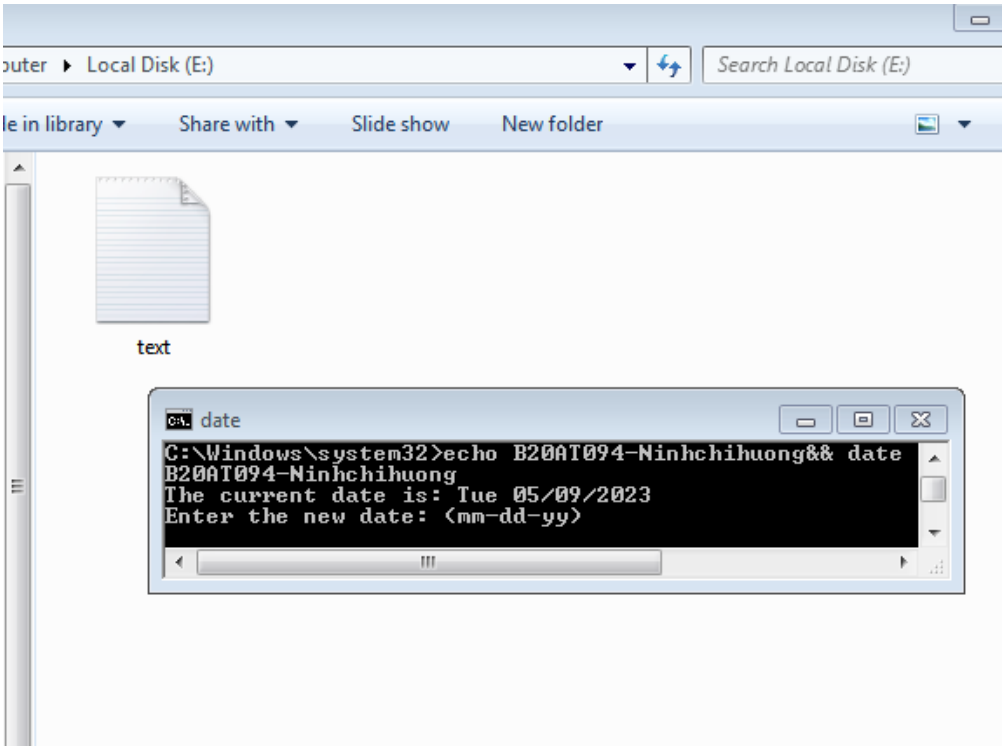




Tạo ổ đĩa ảo để mã hóa file văn bản thành công



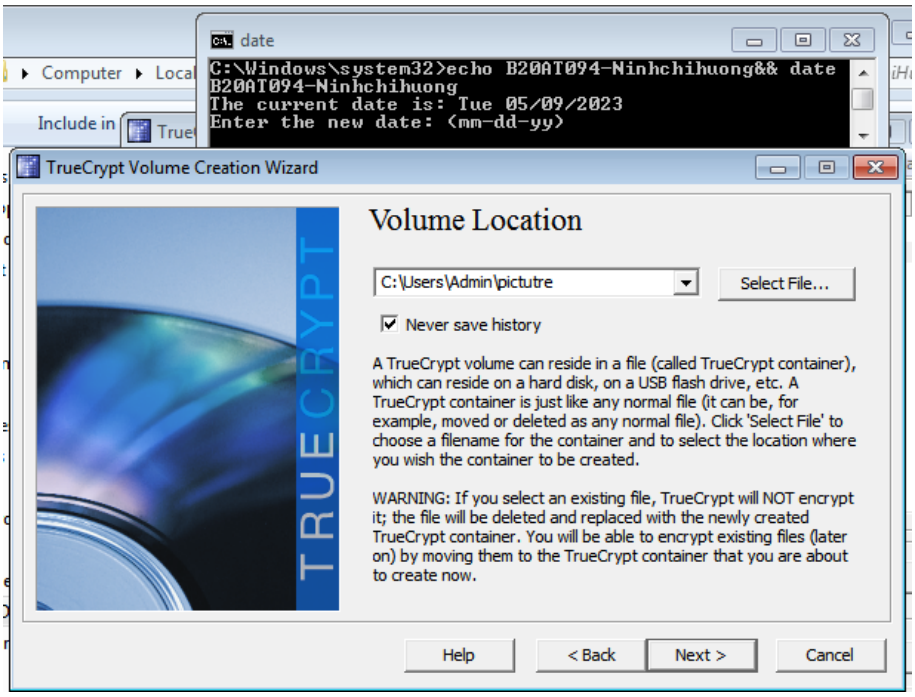
Tiến hành nhập password và mount ổ đĩa vào máy

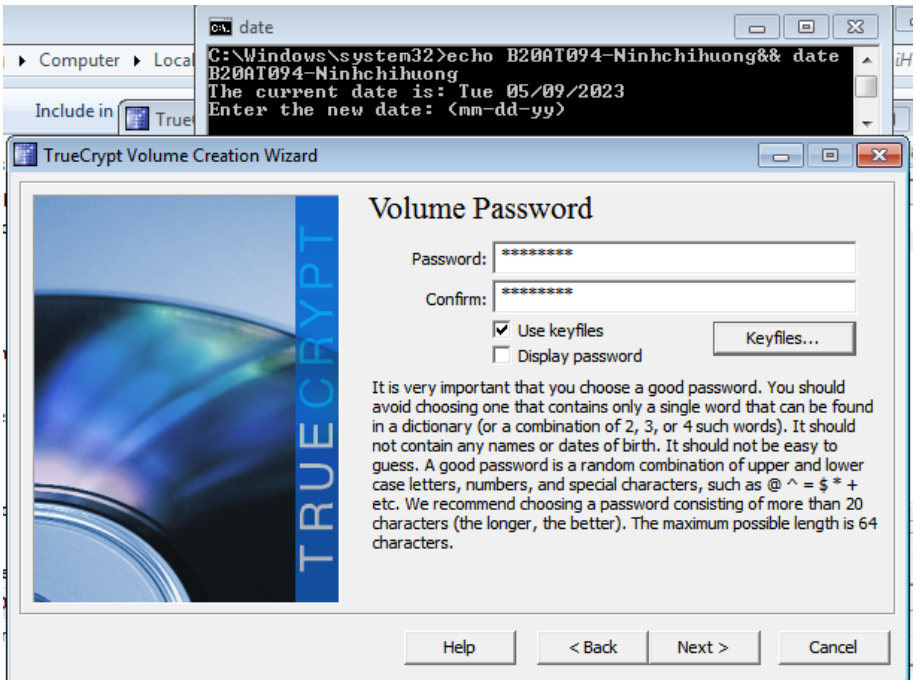


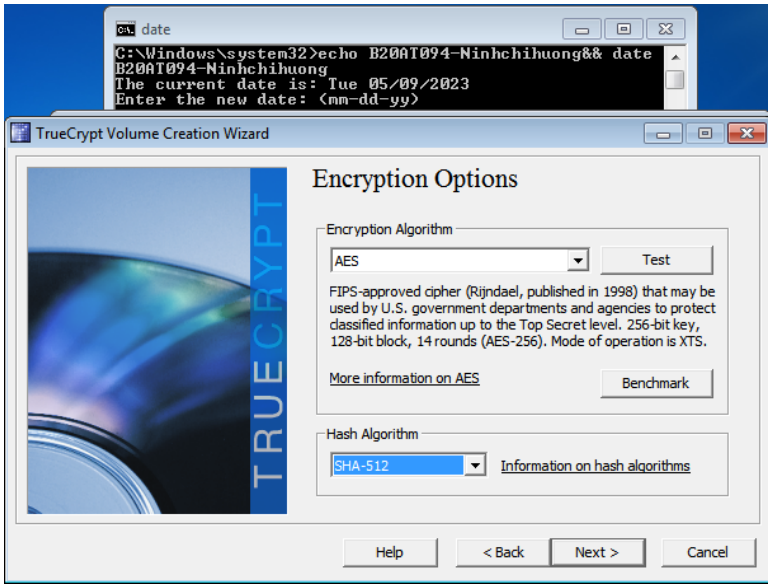
Đưa file văn bản đã tạo vào trong ổ đĩa ảo, sau đó dismount lại ổ đĩa, như vậy là file văn bản đã được mã hóa, khi cần xem lại thì mount và nhập mật khẩu để xem lại

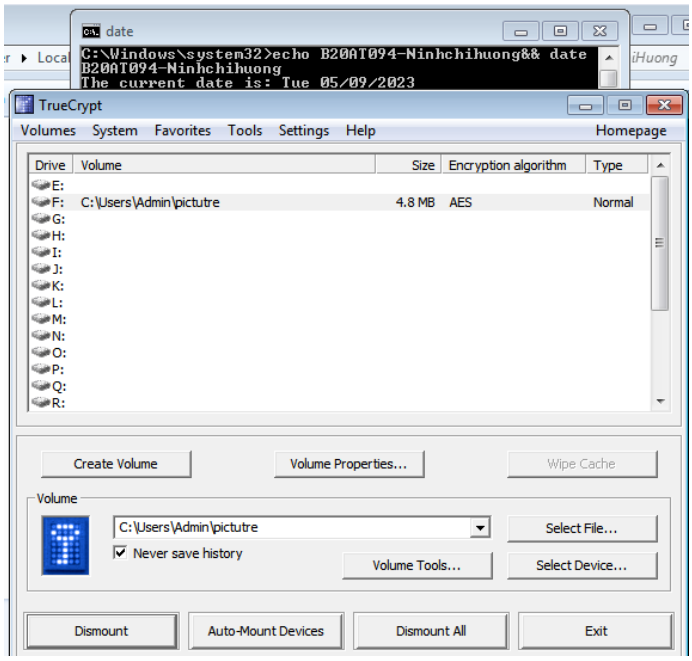
2.2.2.2 Mã hóa ảnh

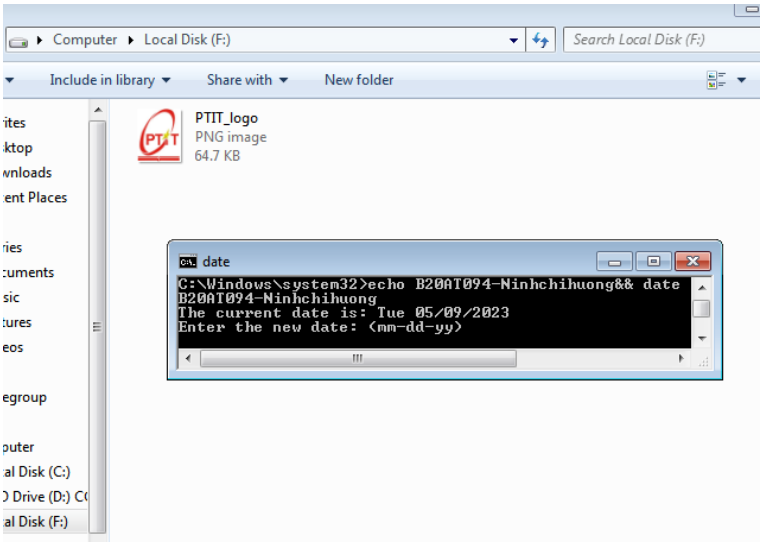
Tạo ổ đĩa ảo để sau đó đưa ảnh vào để mã hoá:







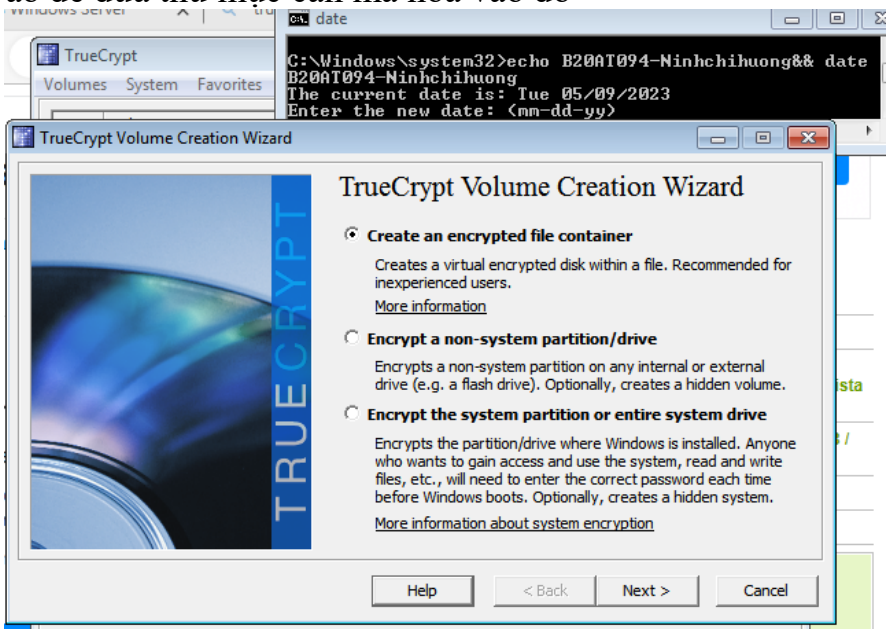


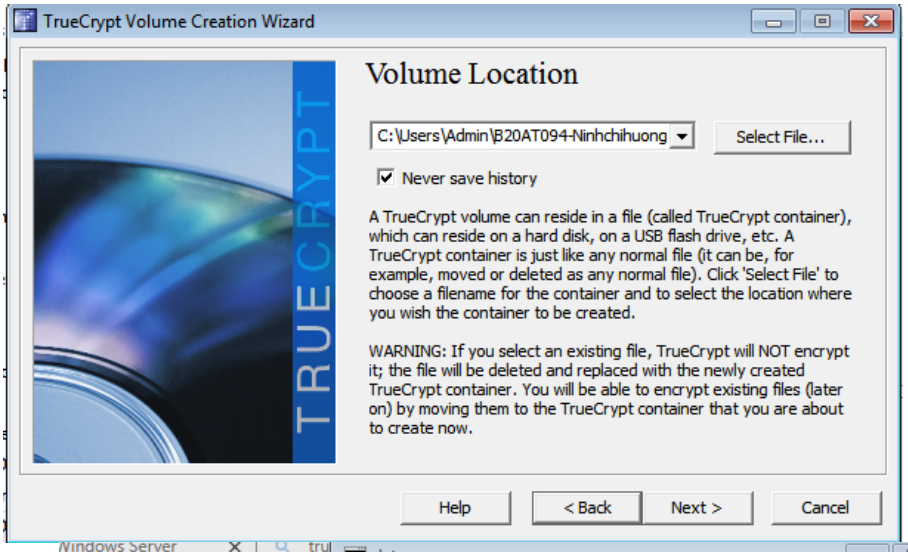


Ta đưa ảnh vào trong ổ đĩa, sau đó dismount là toàn bộ dữ liệu trong ổ đĩa sẽ được mã hóa.

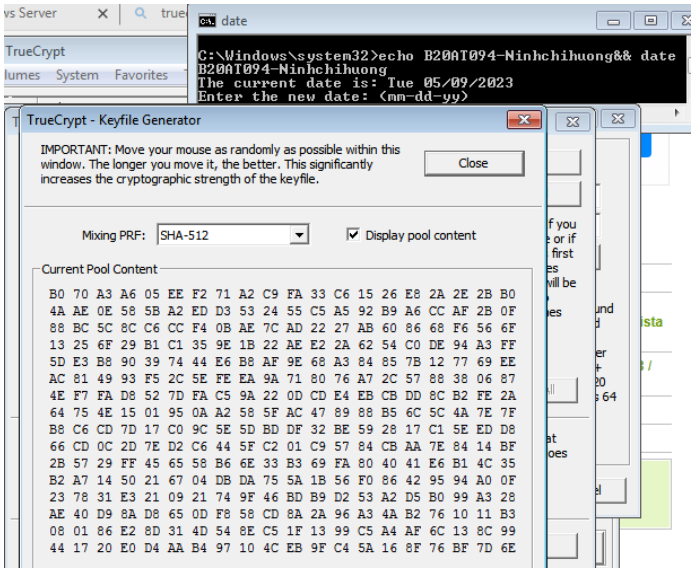
2.2.2.3 Mã hóa thư mục

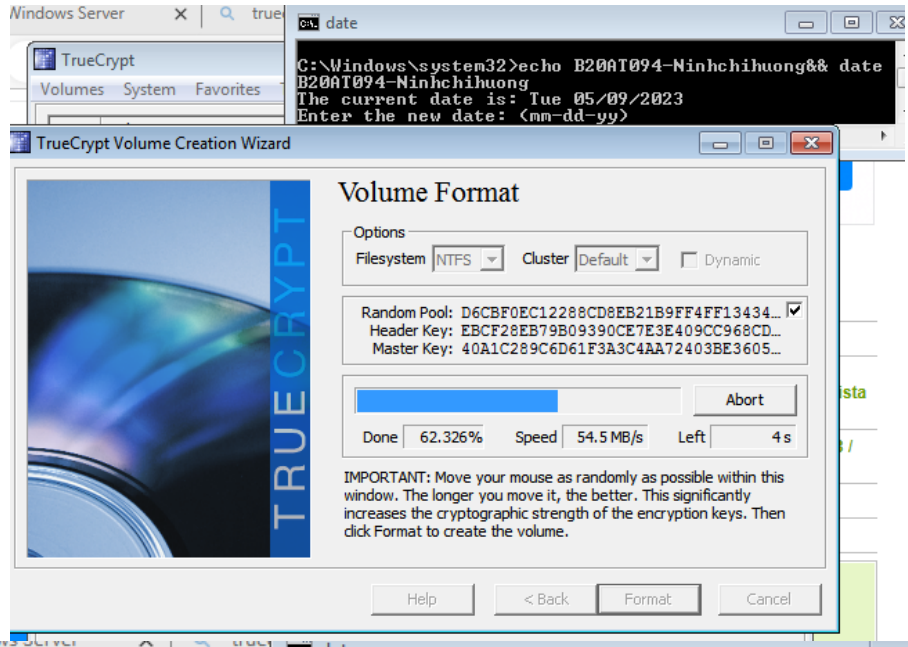
Tạo ổ đĩa ảo để đưa thư mục cần mã hóa vào đó

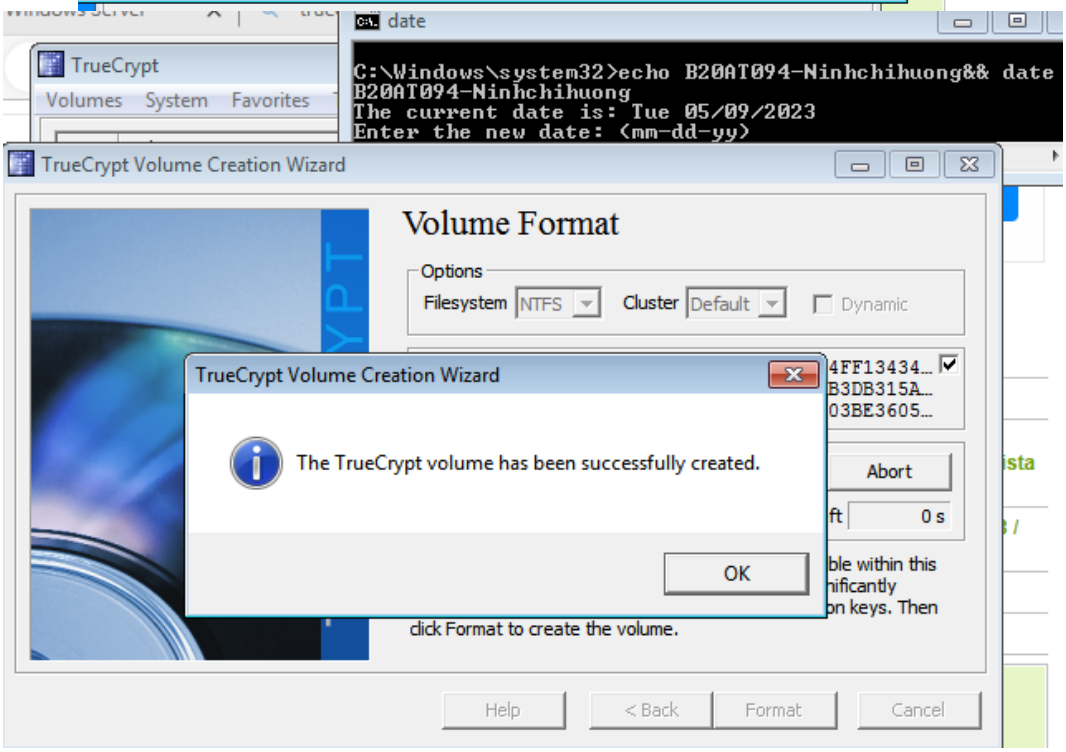




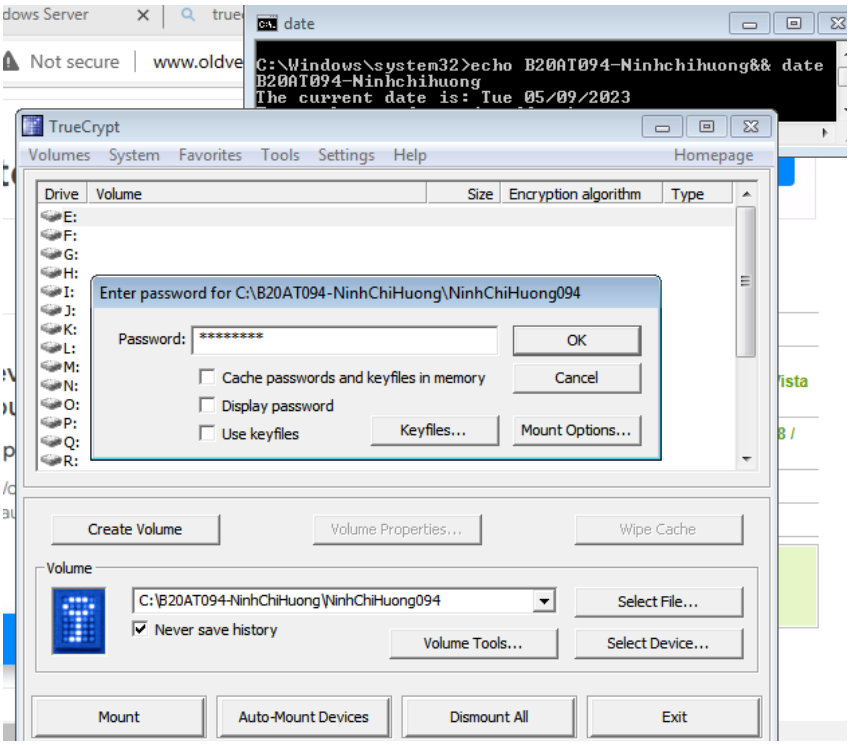
Tạo keyfile

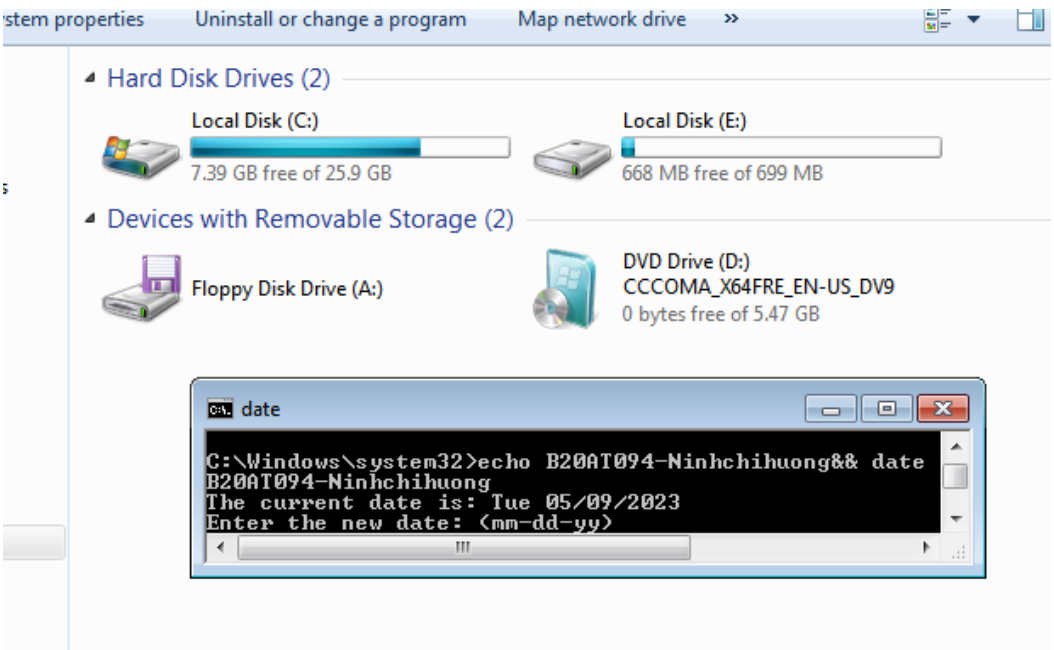

date
C:\Windows\system32>echo B20AT094-Ninhchihuong&& date
B20AT094-Ninhchihuong
The current date is: Tue 05/09/2023
Enter the new date: (mm-dd-yy)
TrueCrypt - Keyfile Generator
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the keyfile.
Close
Mixing PRF: SHA-512
Display pool content
Current Pool Content
B0 70 A3 A6 05 EE F2 71 A2 C9 FA 33 C6 15 26 E8 2A 2E 2B B0
4A AE 0E 58 5B A2 ED D3 53 24 55 C5 A5 92 B9 A6 CC AF 2B 0F
88 BC 5C 8C C6 CC F4 0B AE 7C AD 22 27 AB 60 86 68 F6 56 6F
13 25 6F 29 B1 C1 35 9E 1B 22 AE E2 2A 62 54 C0 DE 94 A3 FF
5D E3 B8 90 39 74 44 E6 B8 AF 9E 68 A3 84 85 7B 12 77 69 EE
AC 81 49 93 F5 2C 5E FE EA 9A 71 80 76 A7 2C 57 88 38 06 87
4E F7 FA D8 52 7D FA C5 9A 22 0D CD E4 EB CB DD 8C B2 FE 2A
64 75 4E 15 01 95 0A A2 58 5F AC 47 89 88 B5 6C 5C 4A 7E 7F
B8 C6 CD 7D 17 C0 9C 5E 5D BD DF 32 BE 59 28 17 C1 5E ED D8
66 CD 0C 2D 7E D2 C6 44 5F C2 01 C9 57 84 CB AA 7E 84 14 BF
2B 57 29 FF 45 65 58 B6 6E 33 B3 69 FA 80 40 41 E6 B1 4C 35
B2 A7 14 50 21 67 04 DB DA 75 5A 1B 56 F0 86 42 95 94 A0 0F
23 78 31 E3 21 09 21 74 9F 46 BD B9 D2 53 A2 D5 B0 99 A3 28
AE 40 D9 8A D8 65 0D F8 58 CD 8A 2A 96 A3 4A B2 76 10 11 B3
08 01 86 E2 8D 31 4D 54 8E C5 1F 13 99 C5 A4 AF 6C 13 8C 99
44 17 20 E0 D4 AA B4 97 10 4C EB 9F C4 5A 16 8F 76 BF 7D 6E

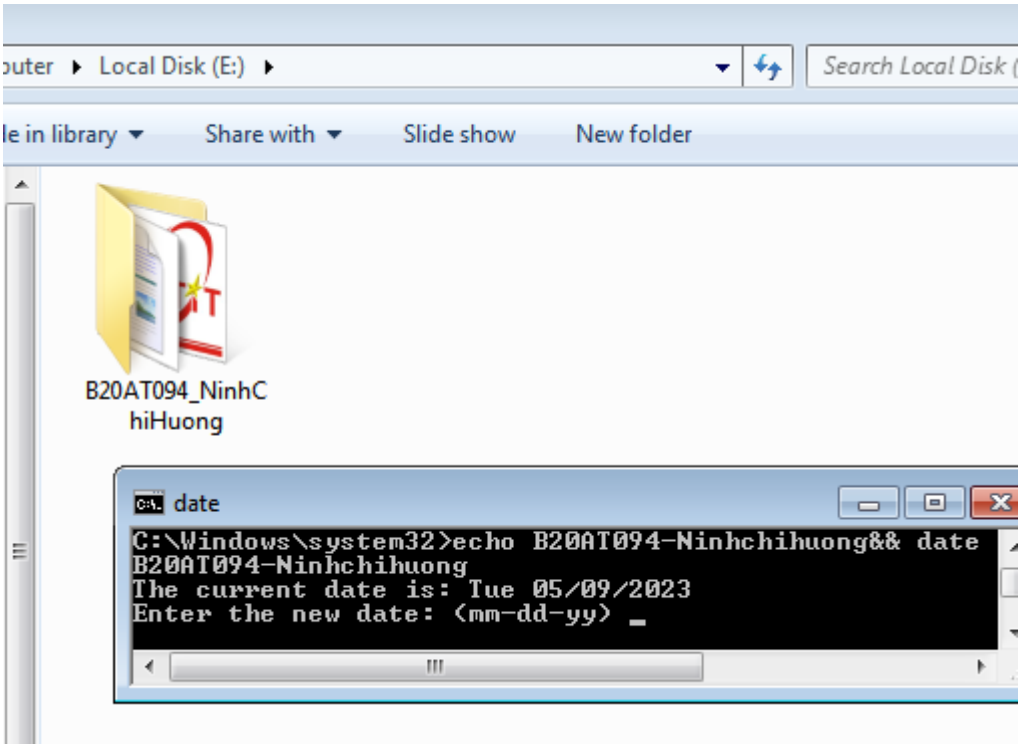

date
C:\Windows\system32>echo B20AT094-Ninhchihuong&& date
B20AT094-Ninhchihuong
The current date is: Tue 05/09/2023
Enter the new date: (mm-dd-yy)
TrueCrypt
Volumes System Favorites
TrueCrypt Volume Creation Wizard
Volume Format
Options
Filesystem NTFS Cluster Default Dynamic
Random Pool: D6CBF0EC12288CD8EB21B9FF4FF13434...
Header Key: EBCF28EB79B09390CE7E3E409CC968CD...
Master Key: 40A1C289C6D61F3A3C4AA72403BE3605...
Abort
Done 62.326% Speed 54.5 MB/s Left 4 s
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
Help < Back Format Cancel


date
C:\Windows\system32>echo B20AT094-Ninhchihuong&& date
B20AT094-Ninhchihuong
The current date is: Tue 05/09/2023
Enter the new date: (mm-dd-yy)
TrueCrypt
Volumes System Favorites
TrueCrypt Volume Creation Wizard
Volume Format
Options
Filesystem NTFS Cluster Default Dynamic
TrueCrypt Volume Creation Wizard
The TrueCrypt volume has been successfully created.
OK
Abort
0 s
click Format to create the volume.
Help < Back Format Cancel

Tiến hành mount ổ đĩa :



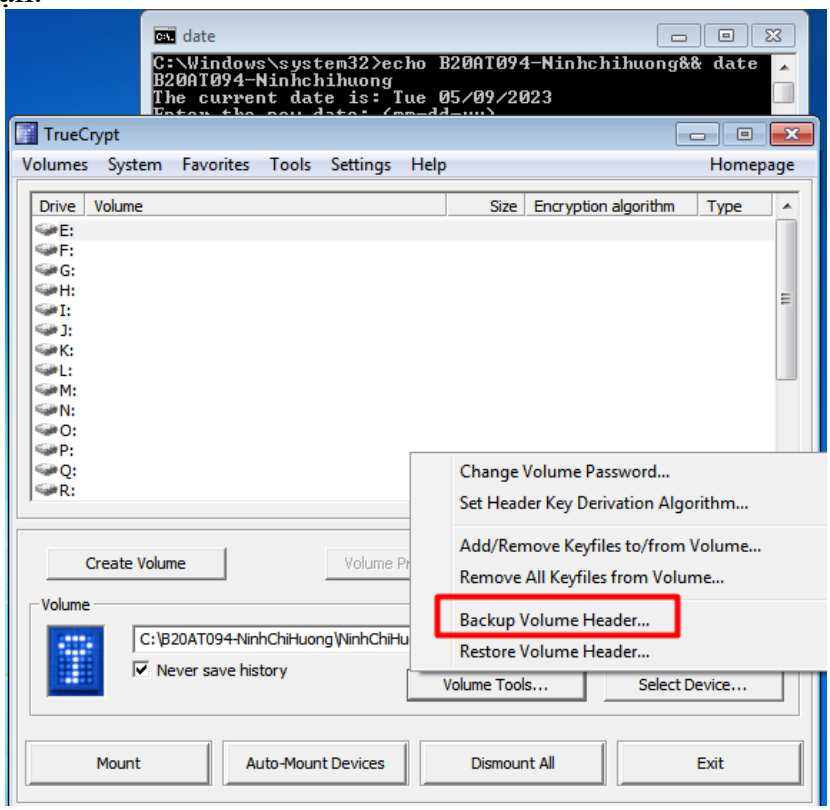


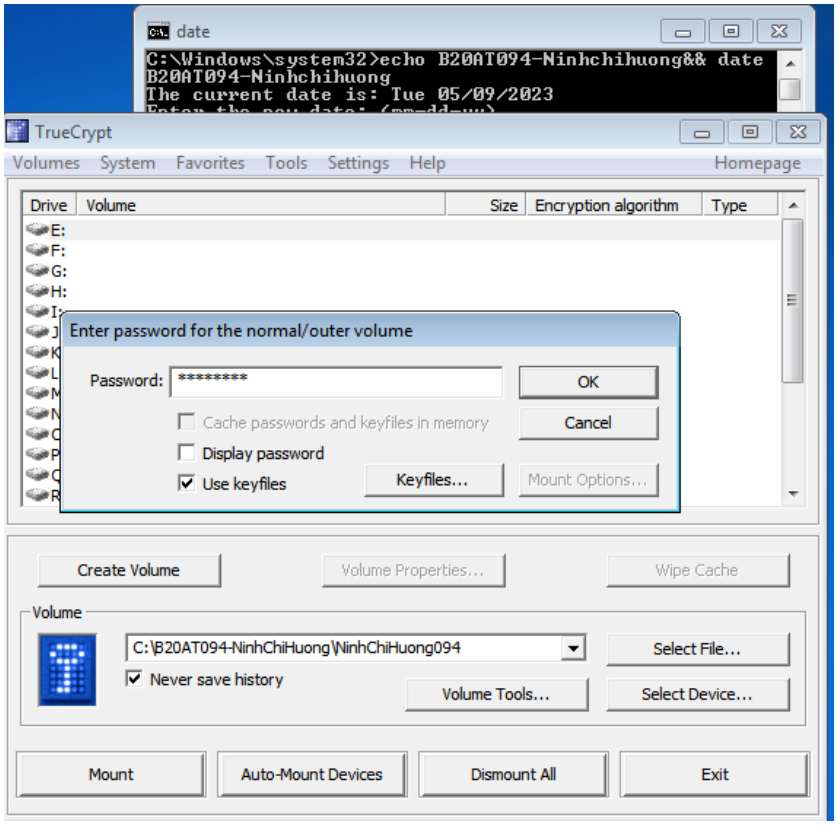


Ta đưa thư mục và trong ổ đĩa, sau đó dismount là toàn bộ dữ liệu trong ổ đĩa được mã hóa. Khi cần khôi phục thì ta cần mount và nhập lại mật khẩu và keyfile

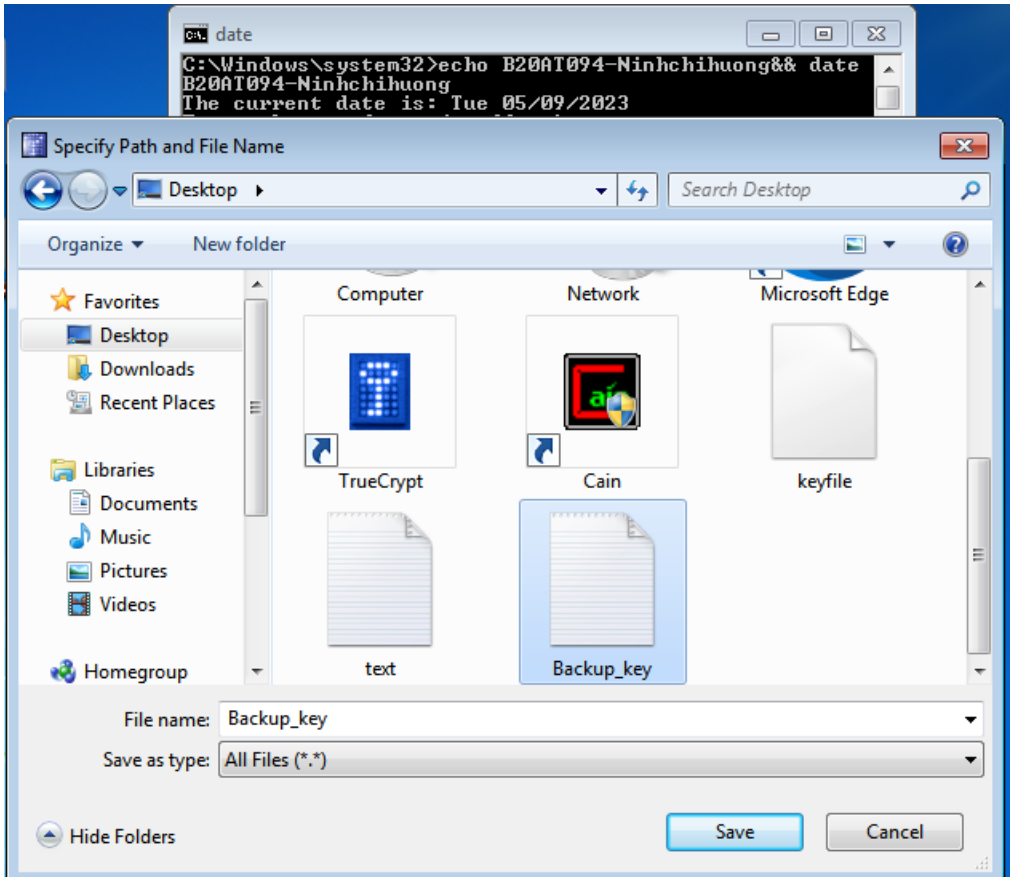
2.2.2.4 Sao lưu khóa mã hóa của công cụ TrueCrypt.

Sau khi tạo tệp tin container, chọn tệp tin đó trong phần mềm TrueCrypt và nhấn vào nút "Volumes" trên giao diện chính. Chọn "Backup Volume Header" để sao lưu khóa mã hóa của bạn.

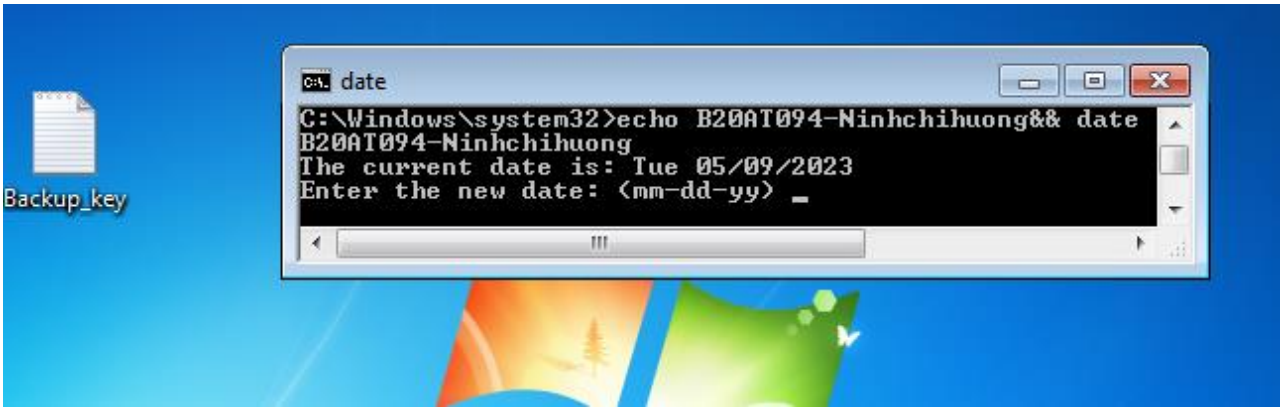




Chọn nơi lưu trữ khóa mã hóa của bạn và nhập mật khẩu để xác nhận tài khoản của bạn.



Khi hoàn tất, sao lưu file khóa mã hóa của bạn ở một địa điểm an toàn và không bị mất hoặc hư hỏng.



Lưu ý rằng việc sao lưu khóa mã hóa là rất quan trọng để đảm bảo tính bảo mật của dữ liệu của bạn. Nếu bạn không sao lưu khóa mã hóa và quên mật khẩu hoặc không thể truy cập vào tệp tin mã hóa, bạn có thể không thể khôi phục lại dữ liệu của mình.

III. Tài liệu tham khảo

https://quantrimang.com/lang-cong-nghe/huong-dan-su-dung-truecrypt-de-ma-hoa-nhung-tai-lieu-nhay-cam-83755

Đỗ Xuân Chợ, Bài giảng Mật mã học cơ sở, Học viện Công Nghệ Bưu Chính Viễn Thông, 2021.

Đỗ Xuân Chợ, Bài giảng Mật mã học nâng cao, Học viện Công Nghệ Bưu Chính Viễn Thông, 2021.