HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BỘ MÔN THỰC TẬP CƠ SỞ

BÀI 13:
ĐẢM BẢO AN TOÀN VỚI MÃ HÓA

Giảng viên : Nguyễn Ngọc Điệp
Sinh viên : Nguyễn Đức Anh
Mã sinh viên : B21DCAT031
Hệ : Đại học chính quy

Hà Nội, 3/2024

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

a. 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.

b. Cách 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.

c. 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.

2.2 Tài liệu tham khảo

- 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.

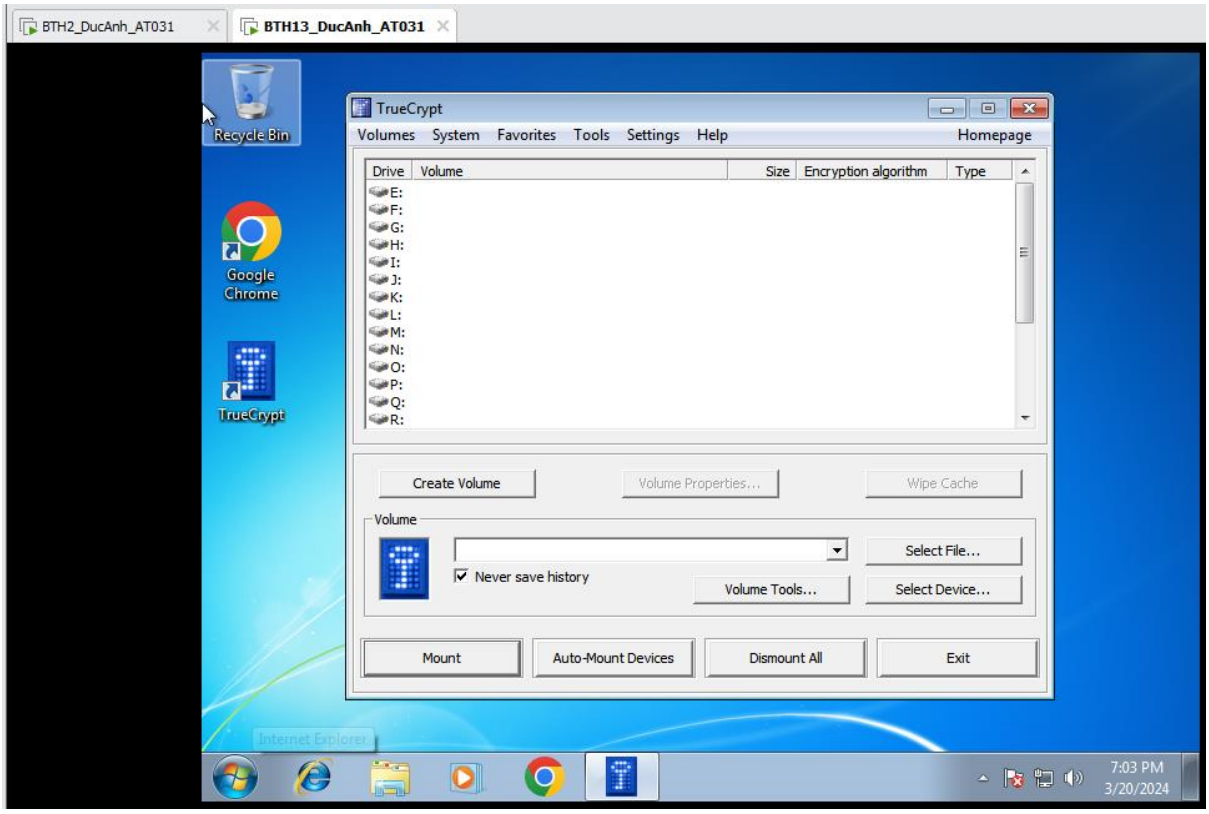
2.3 Chuẩn bị môi trường

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

2.4 Các bước thực hiện

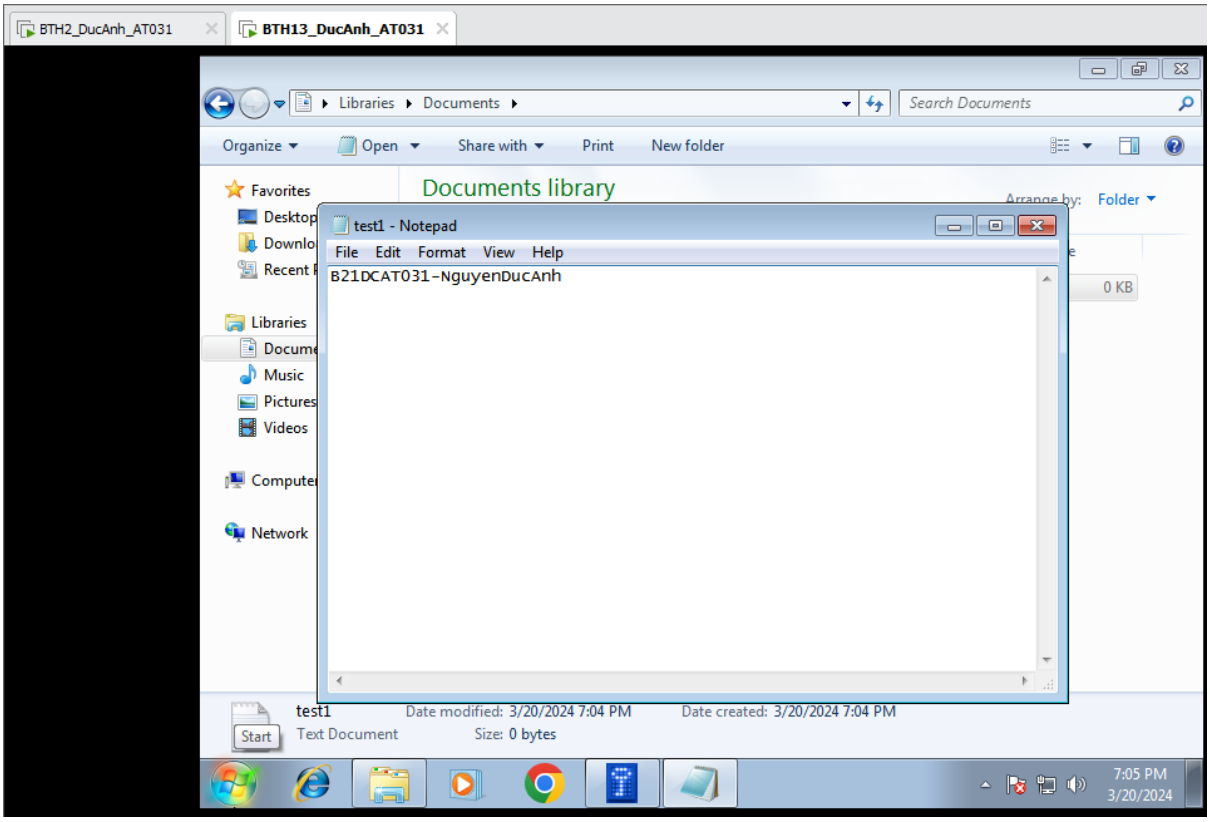
Bước 1: Chuẩn bị máy ảo Windows

Bước 2: Cài đặt TrueCrypt trên máy ảo.



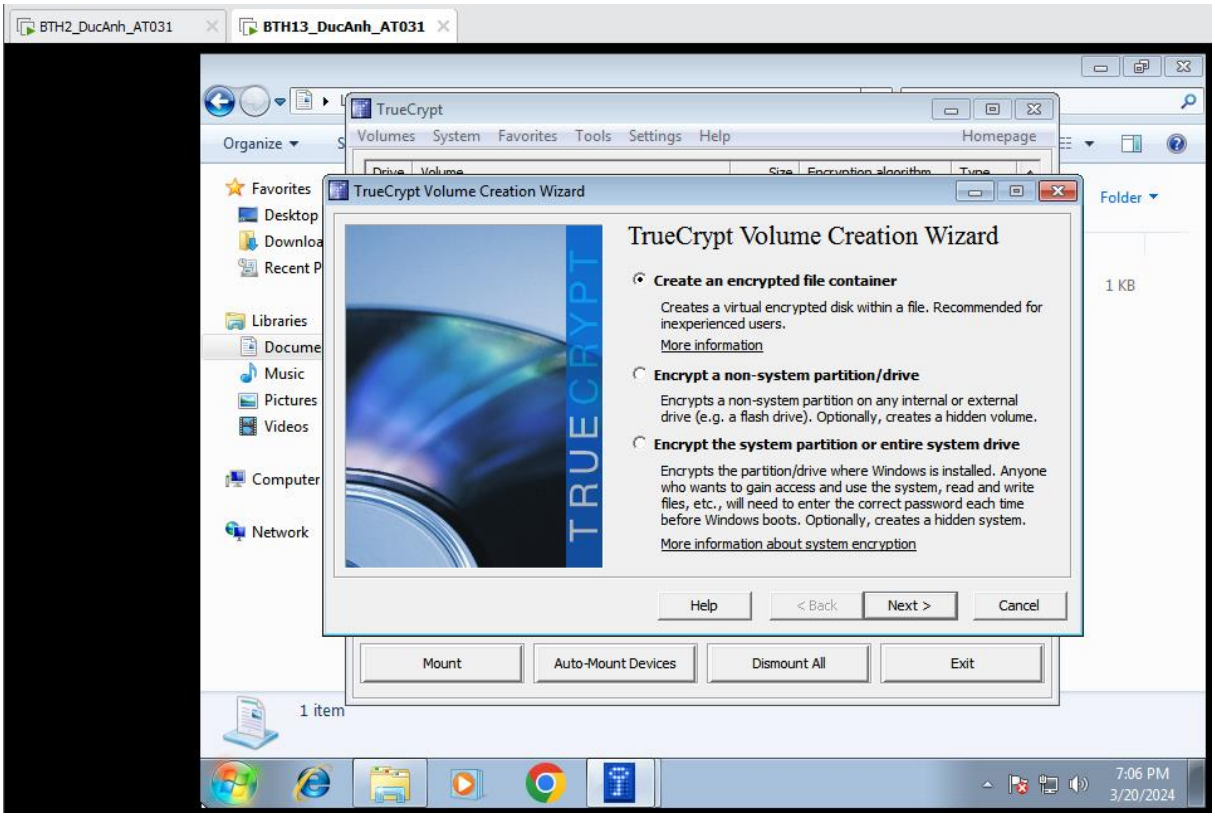
Bước 3: Mã hóa file văn bản

Tạo file văn bản, nội dung file như sau:

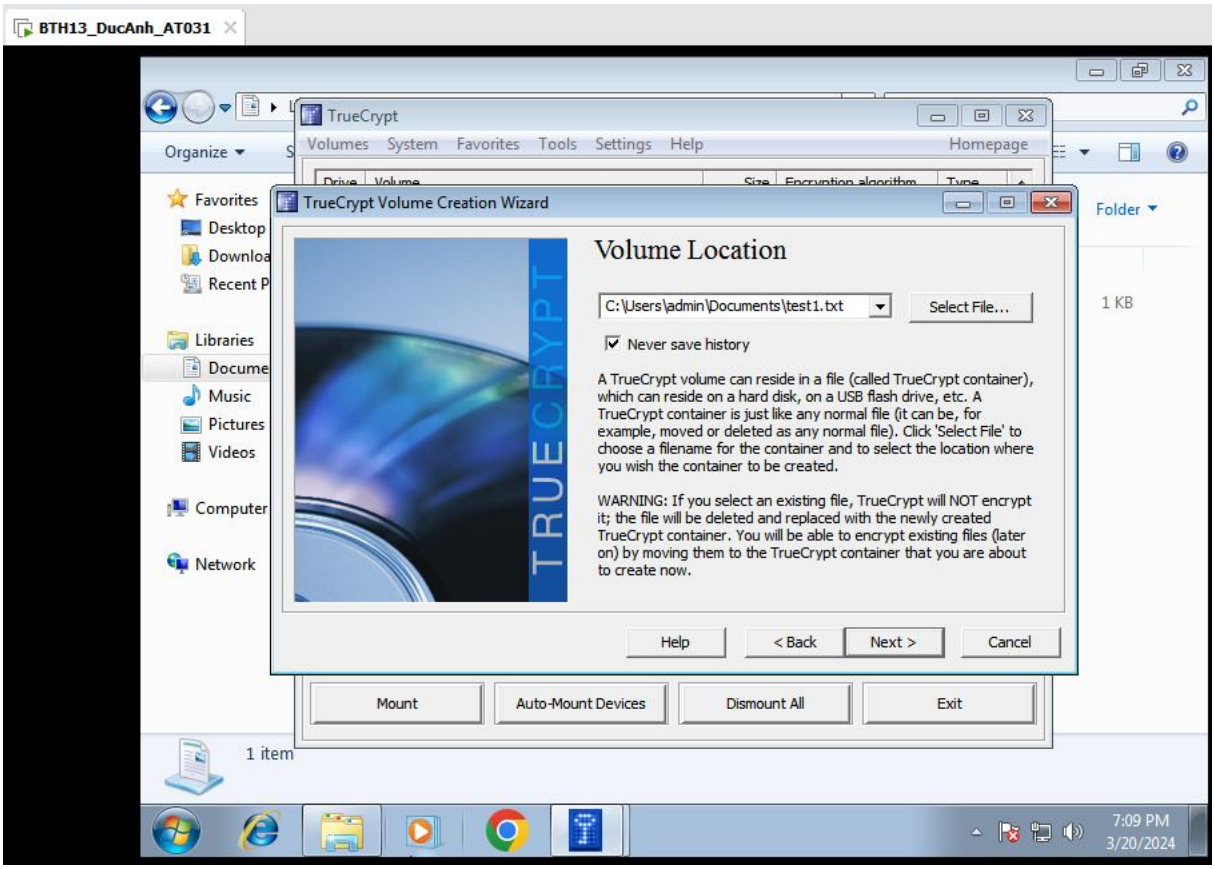


Tạo một ổ đĩa ảo để đưa file văn bản trên vào đó:

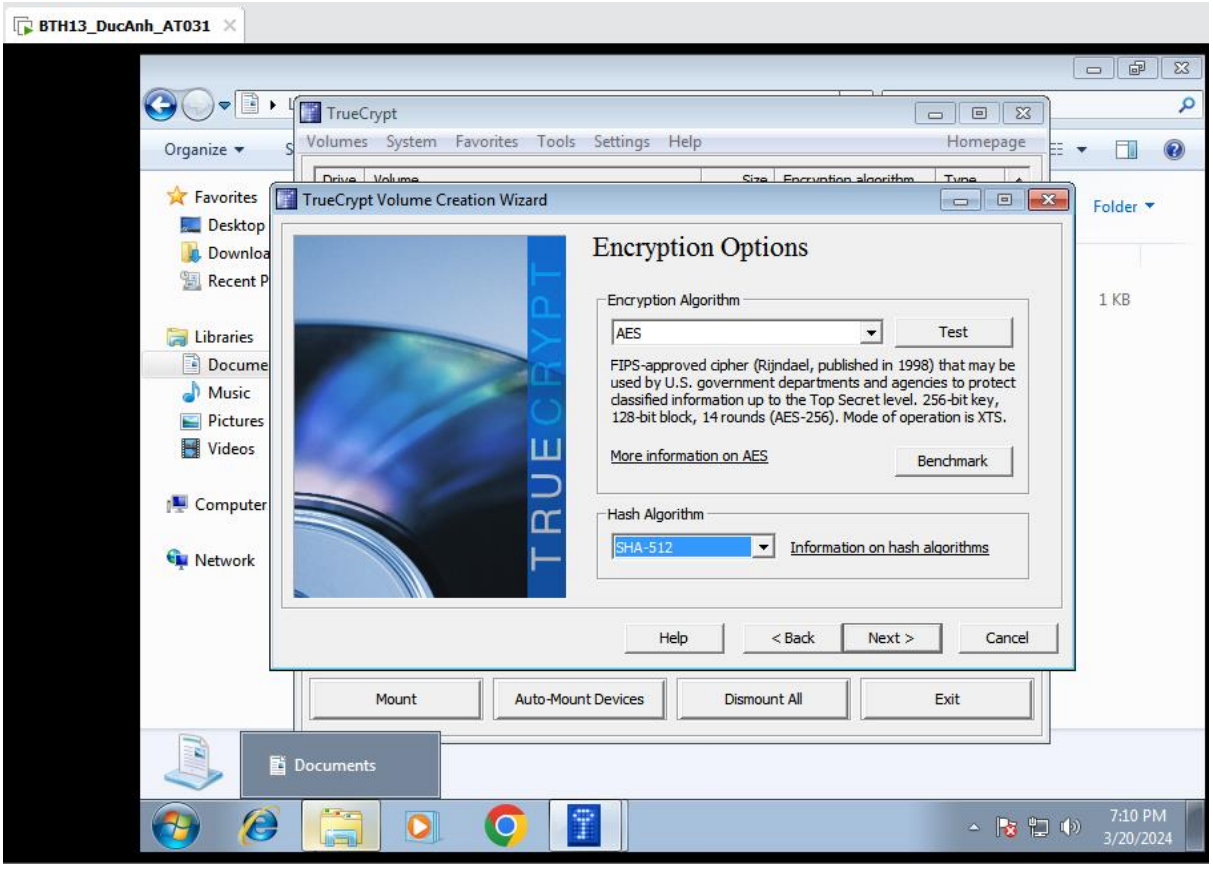
Chọn nút Create Volume.



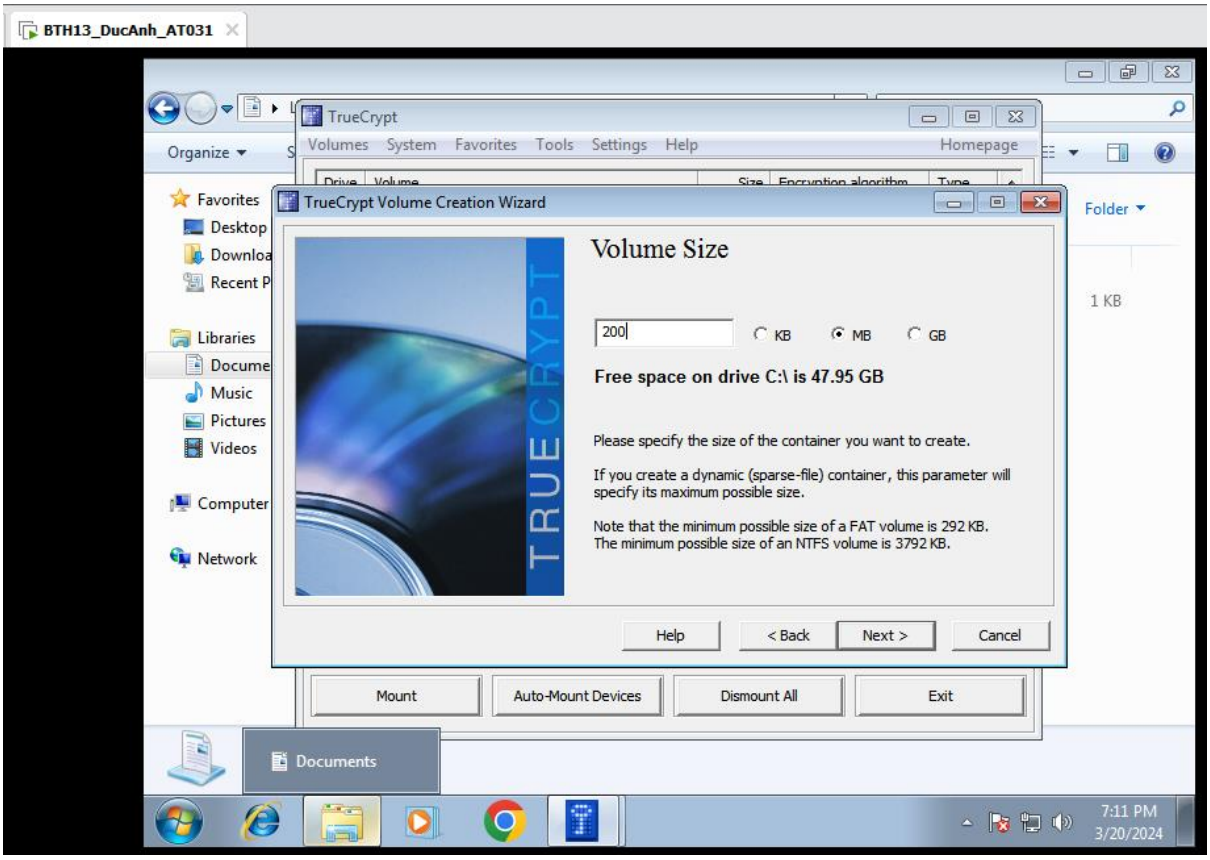
Bấm Next đến khi màn hình có yêu cầu nhập đường dẫn.



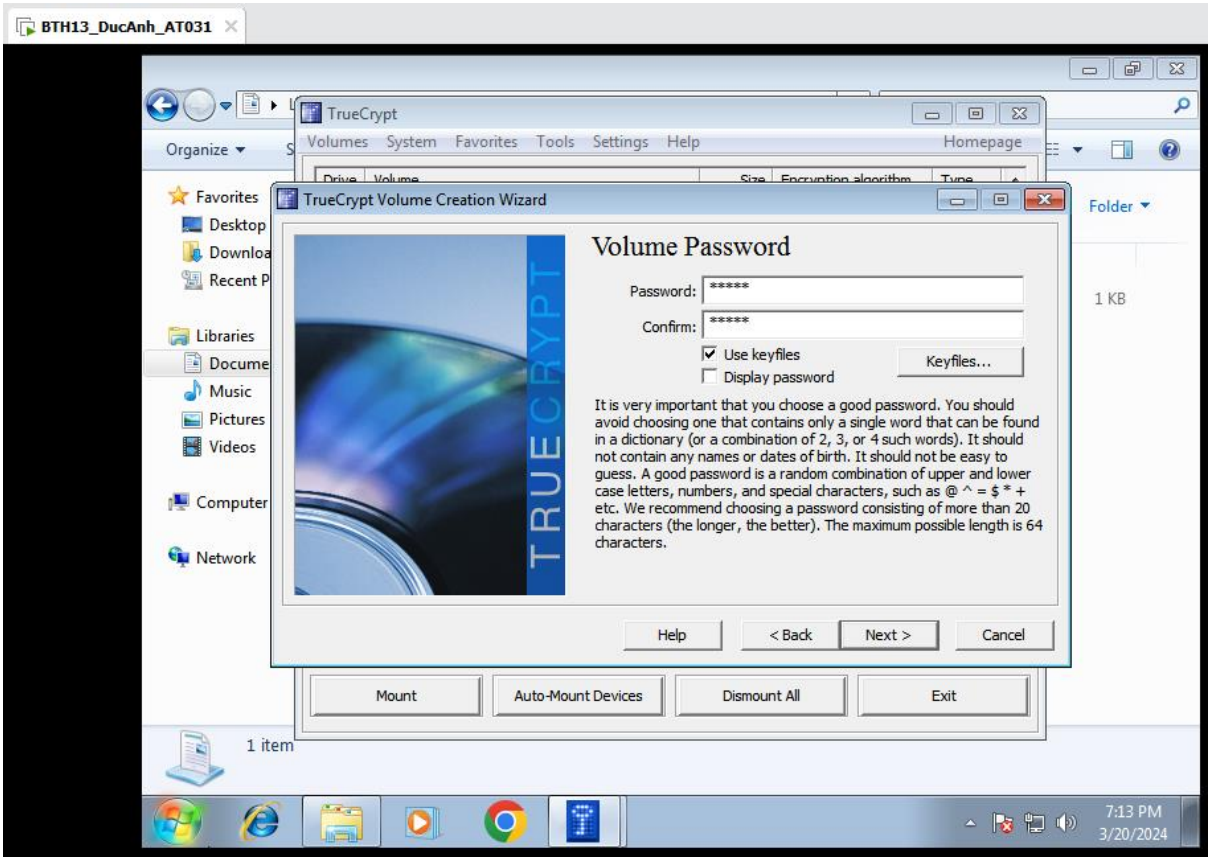
Ở phần tiếp theo, chọn thuật toán mã hóa là AES và thuật toán băm là SHA-512



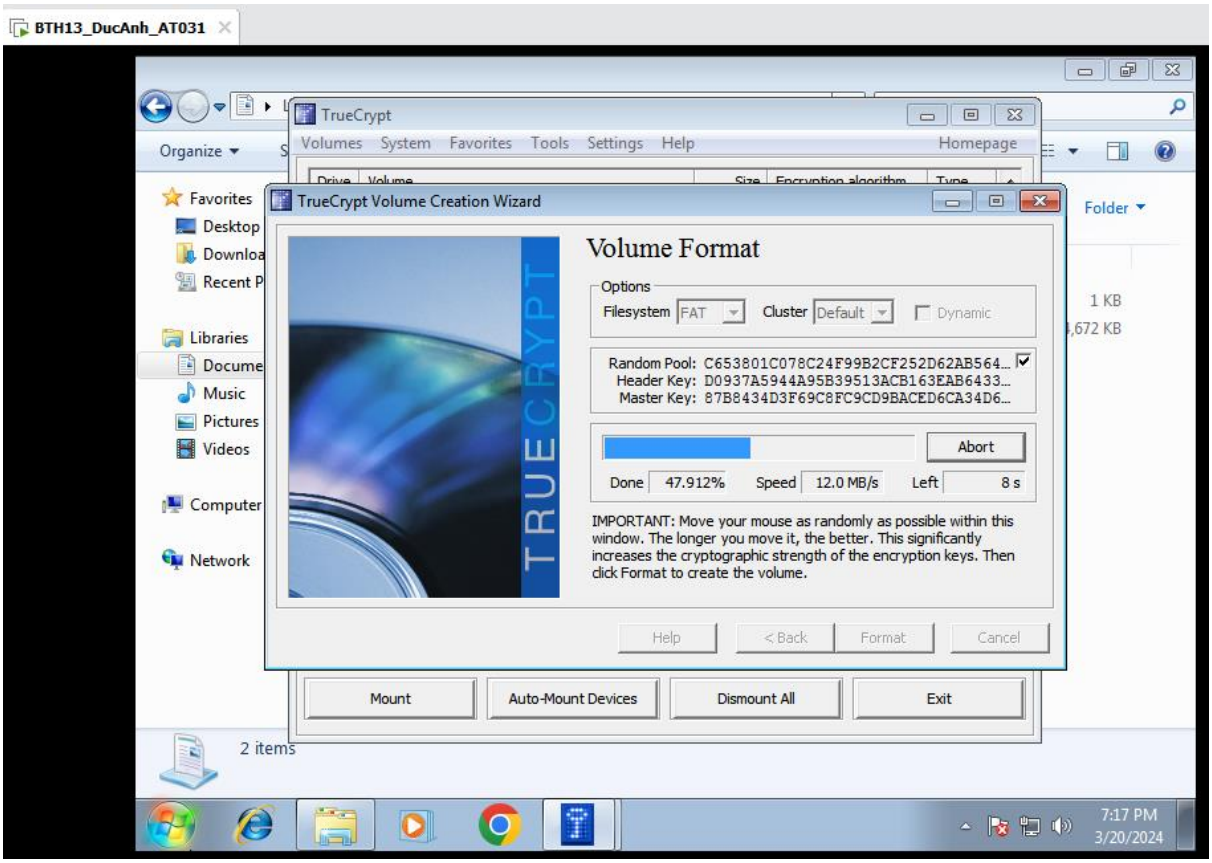
Để kích thước ổ đĩa ảo là 200MB

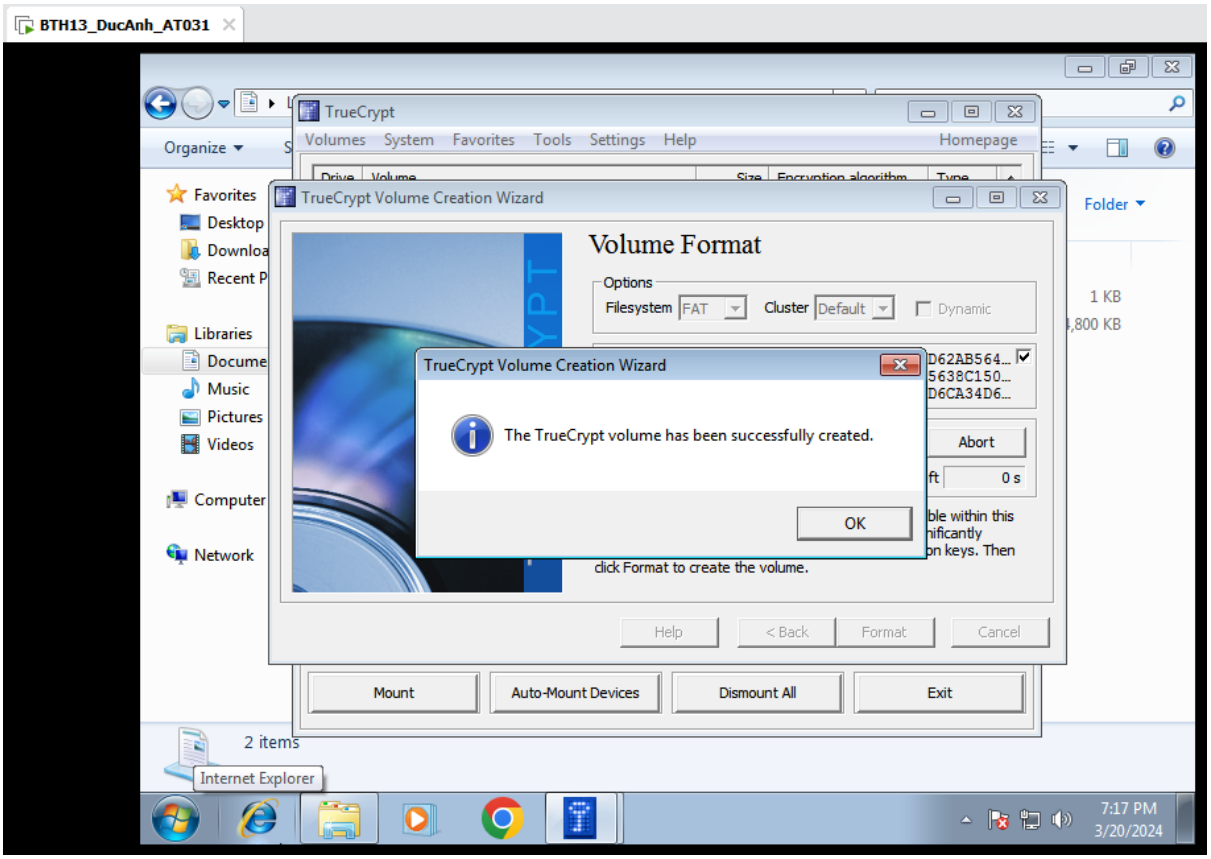


Thêm mật khẩu và keyfile (có thể sử dụng tính năng tạo keyfile ngẫu nhiên của TrueCrypt)



Chọn nút Format để bắt đầu tạo ổ đĩa ảo.

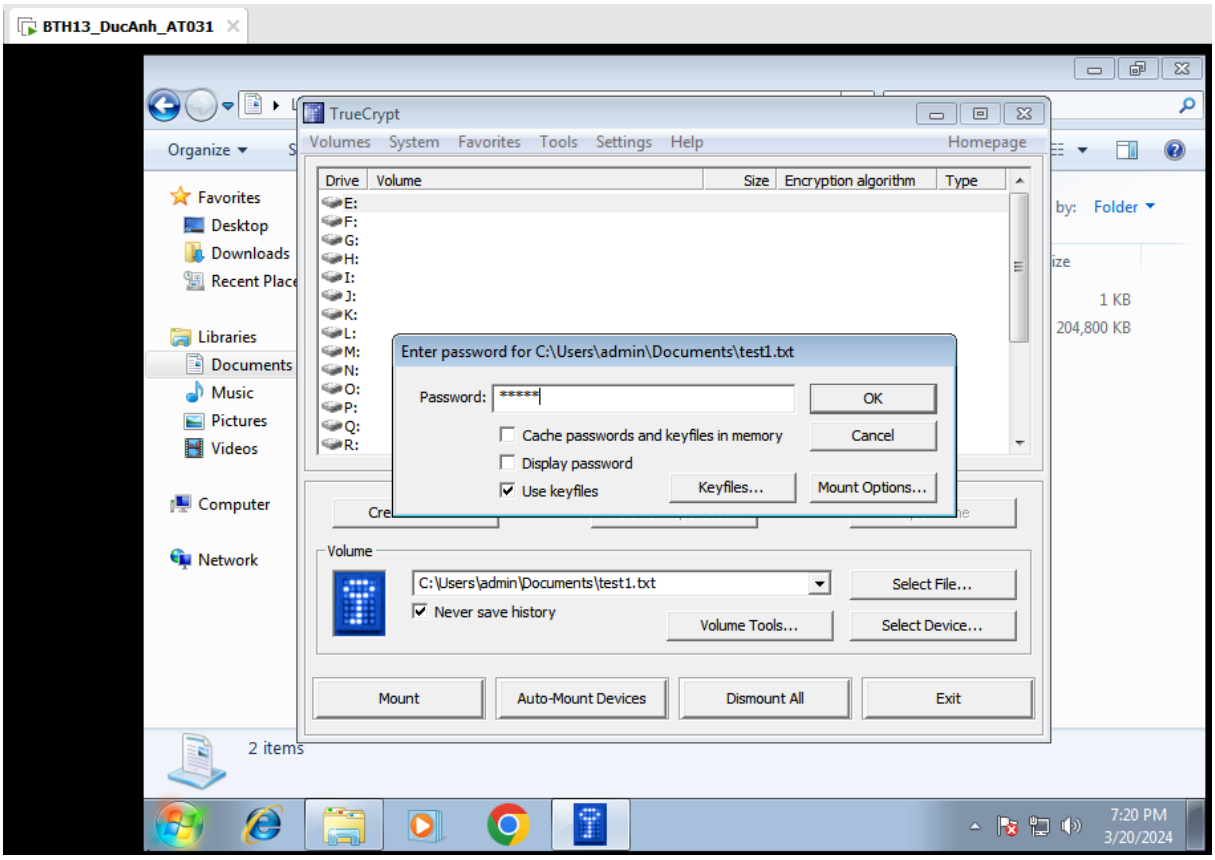




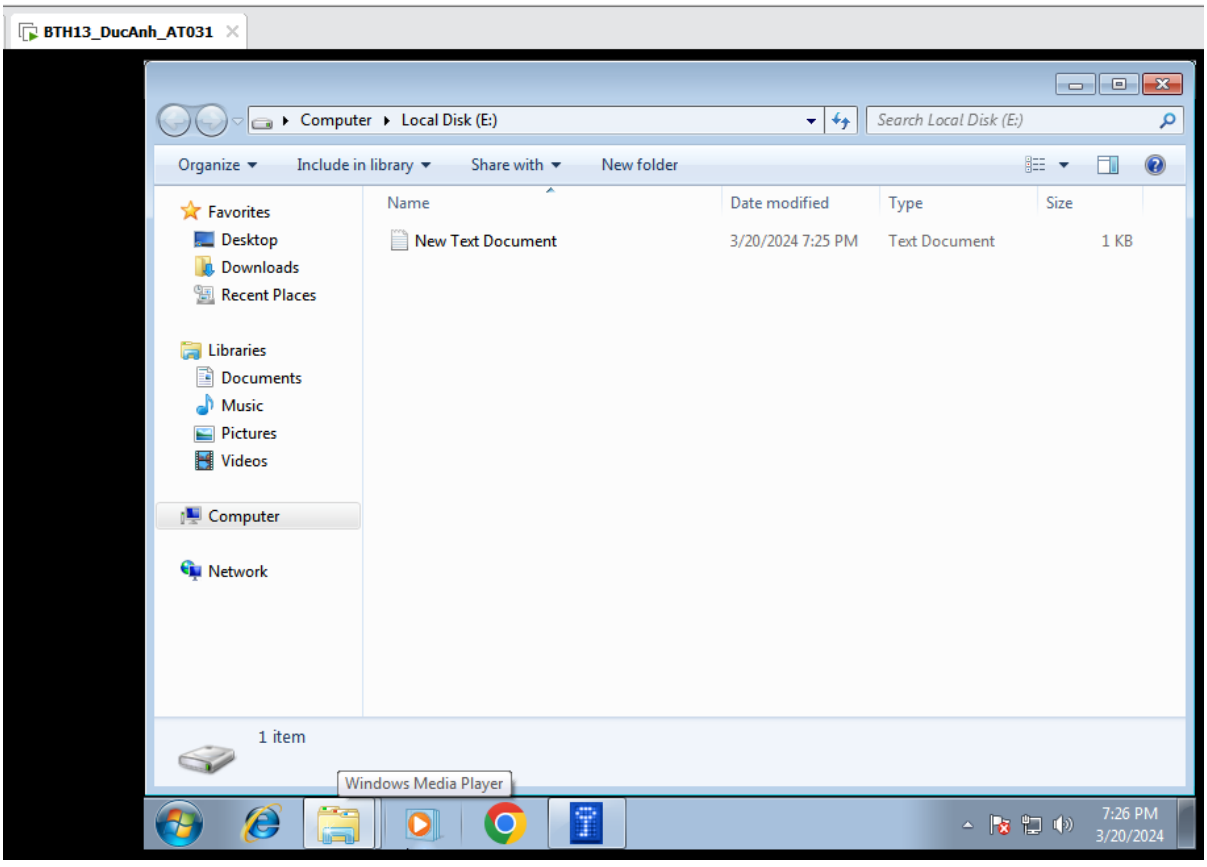
Tạo ổ đĩa ảo thành công.

Để mã hóa file, chọn một ổ đĩa ảo (ví dụ ổ E:) => Mount.

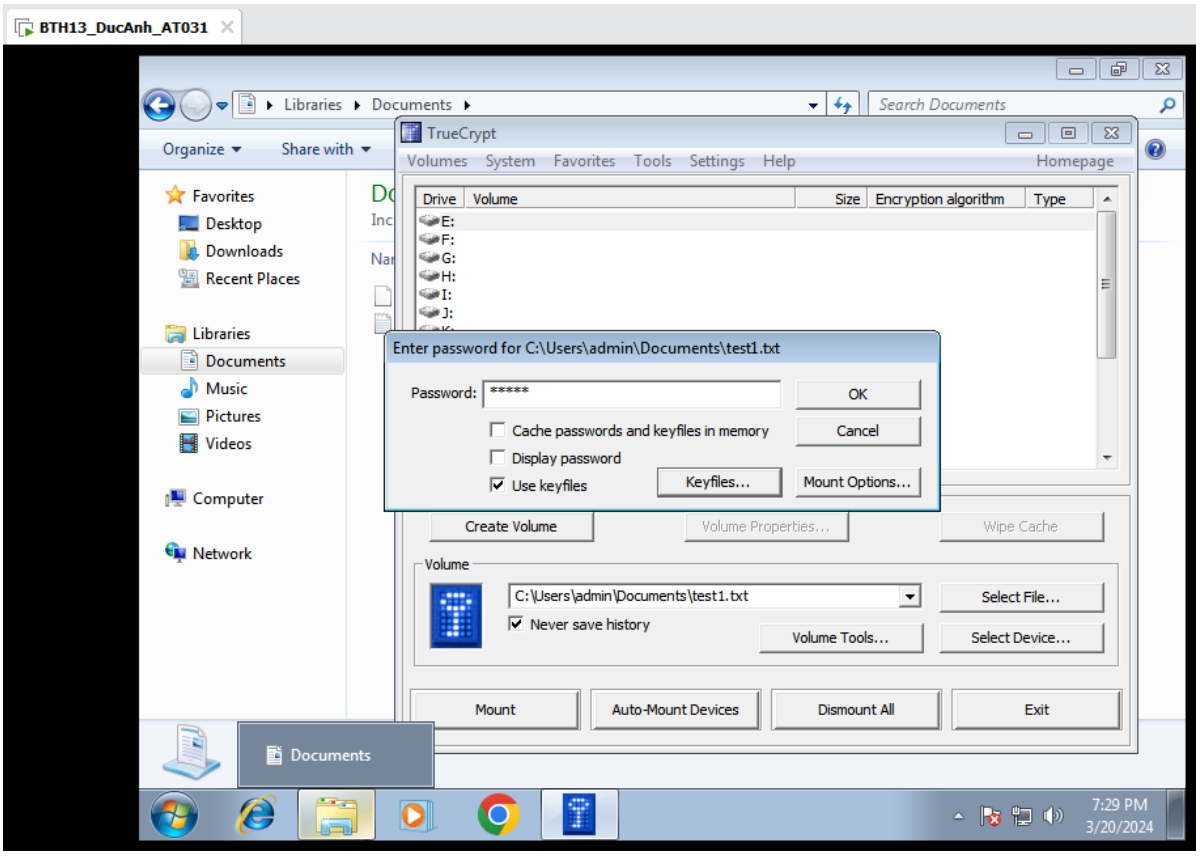
Nhập mật khẩu của ổ đĩa ảo vừa tạo và thêm keyfile tương ứng.

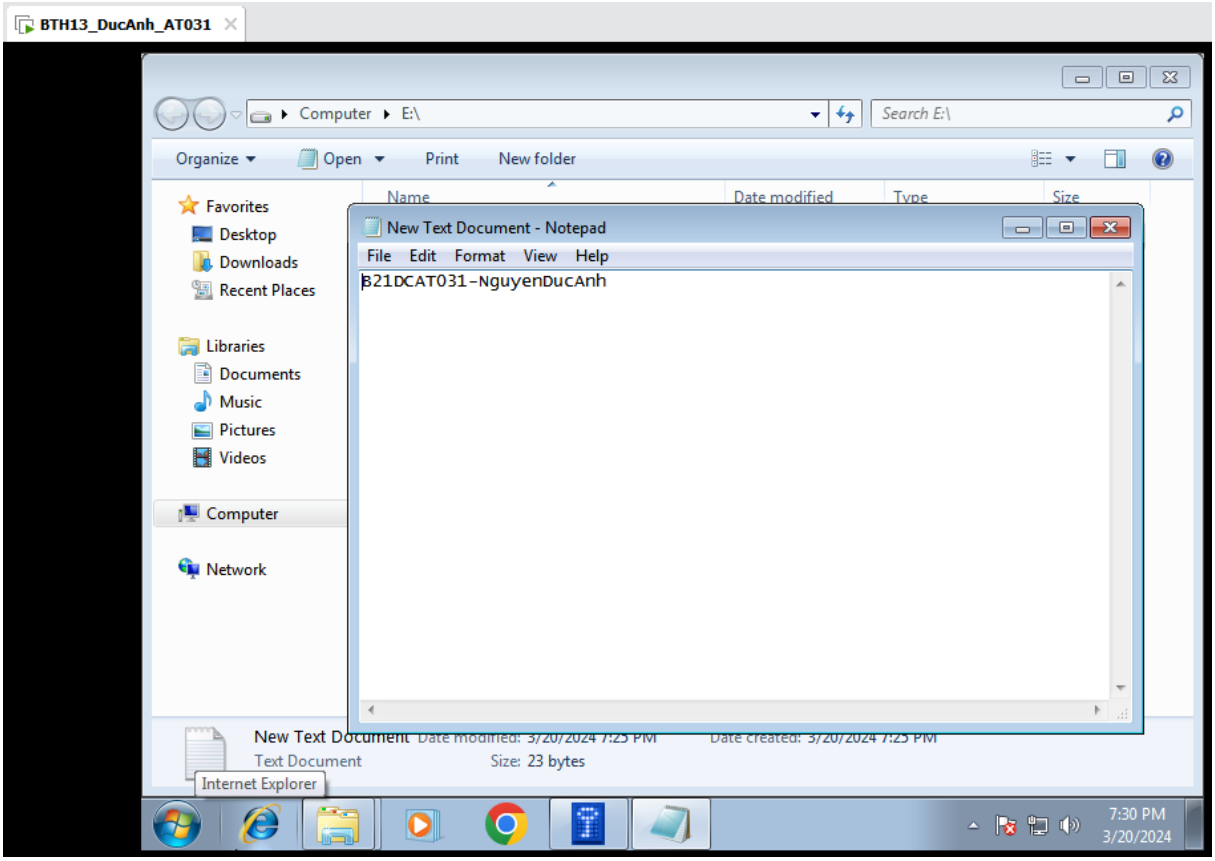


Đưa file cần mã hóa vào ổ, sau đó chọn Dismount.



Khi cần xem file đã mã hóa, chỉ cần Mount lại ổ đĩa là có thể xem được.

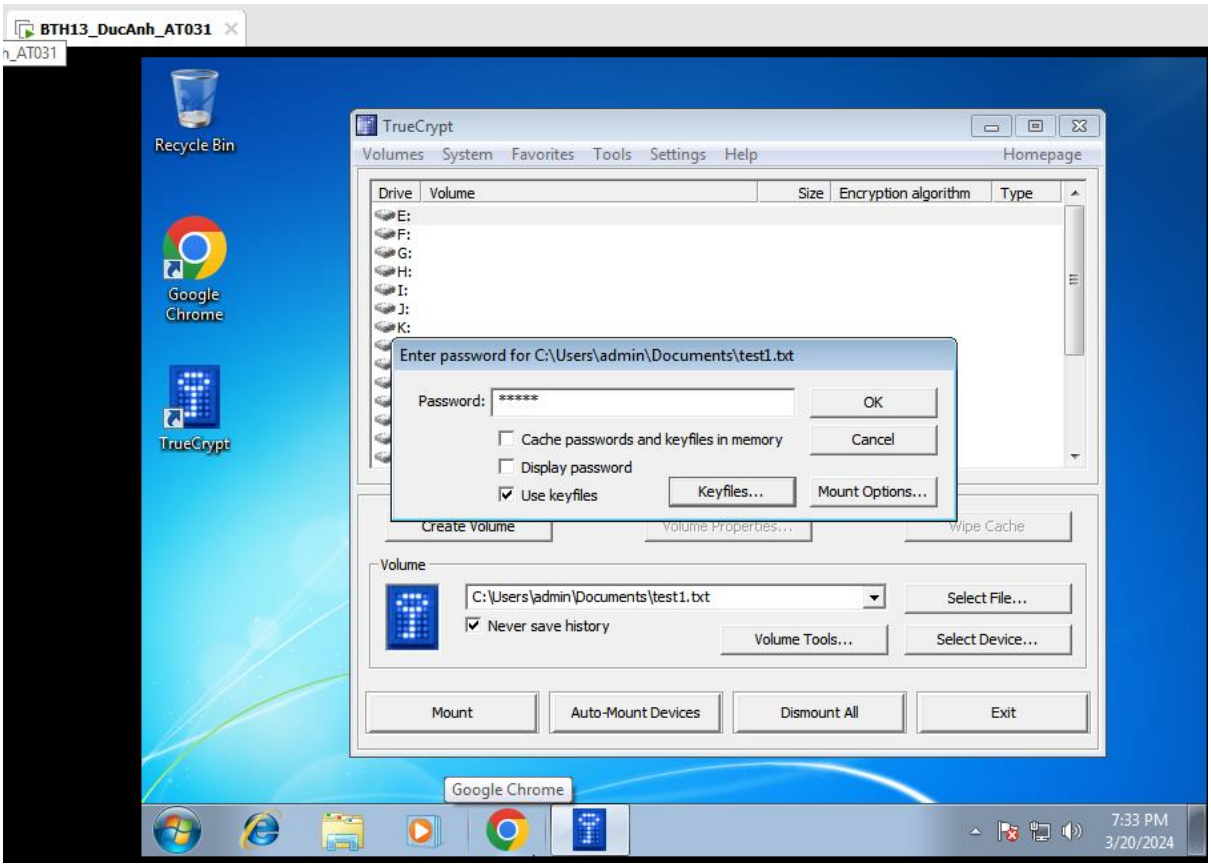


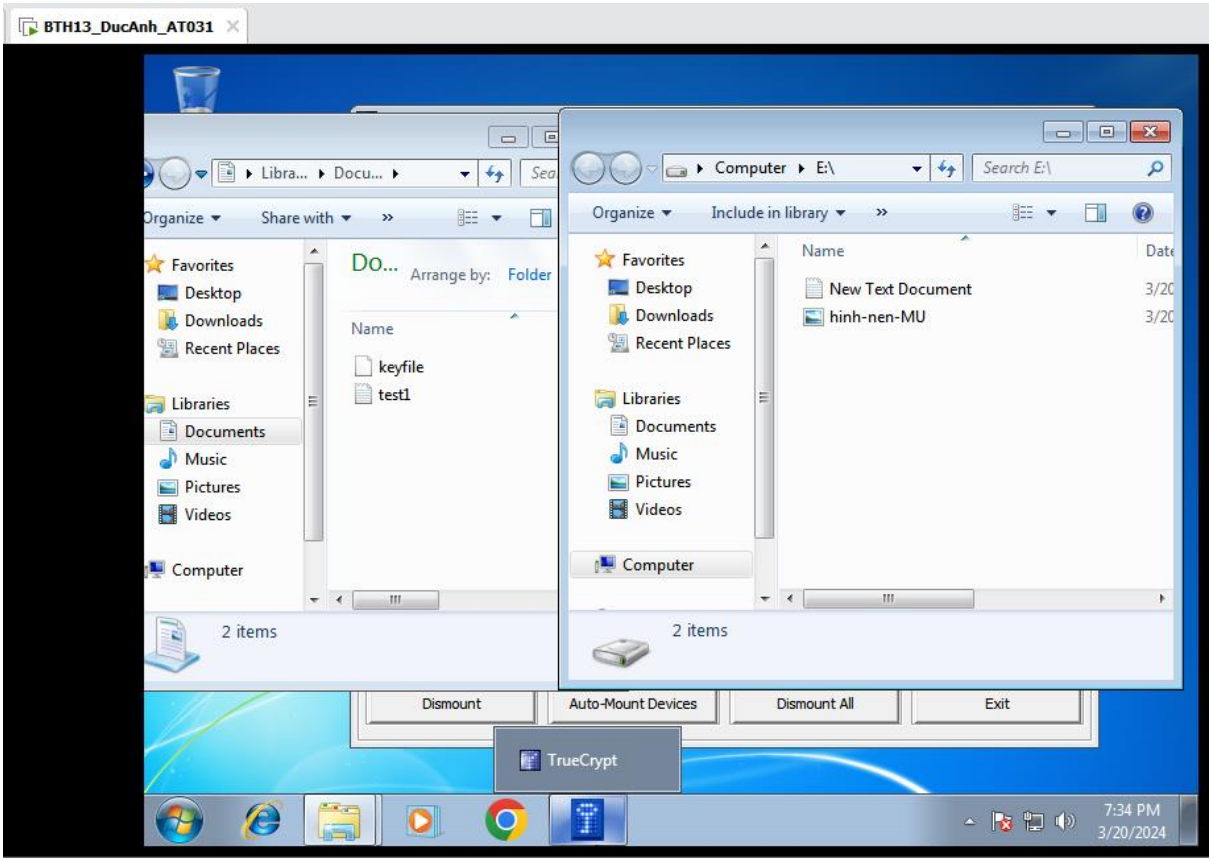


Bước 4: Mã hóa file ảnh

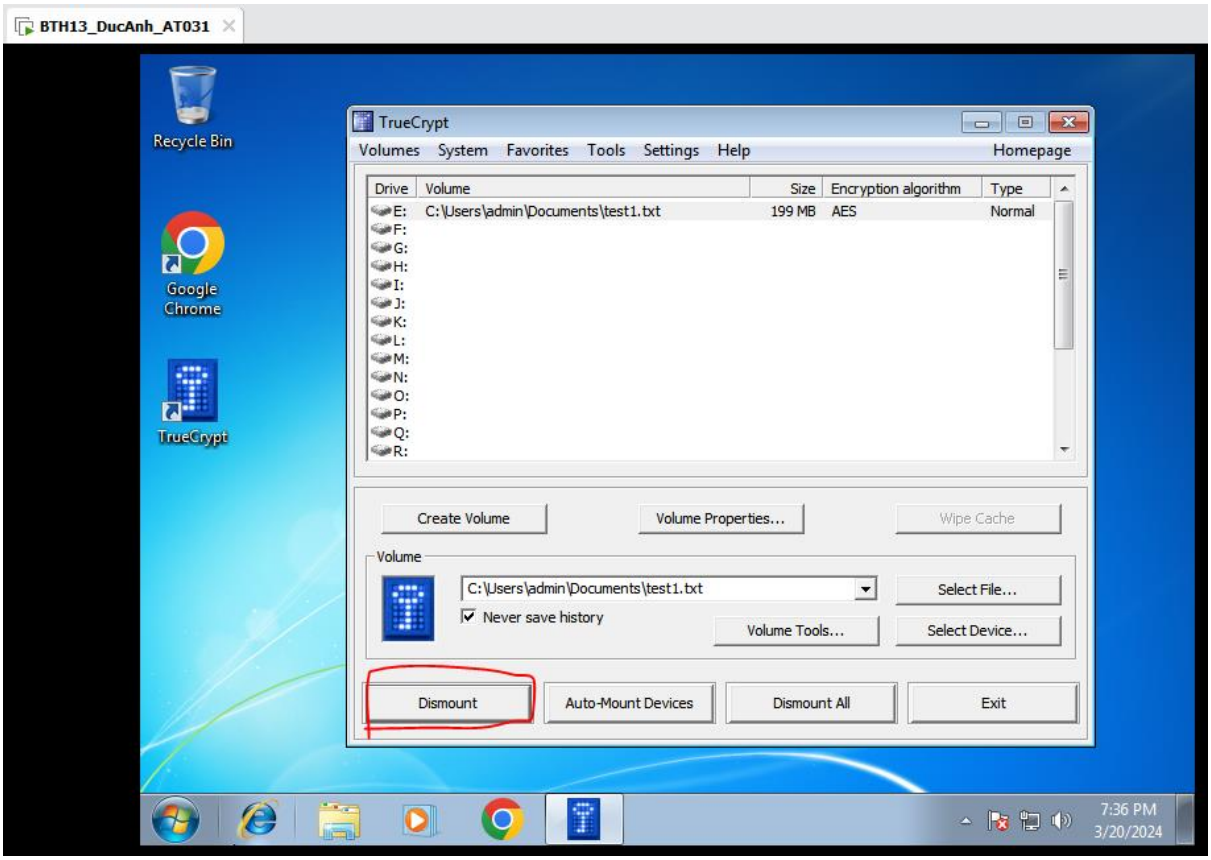
Trước hết ta phải tạo ổ đĩa ảo để mã hóa file ảnh, ở đây ta có thể dùng lại ổ đĩa dùng để mã hóa file văn bản phía trên.

Tiến hành đưa file ảnh vào trong ổ đĩa.

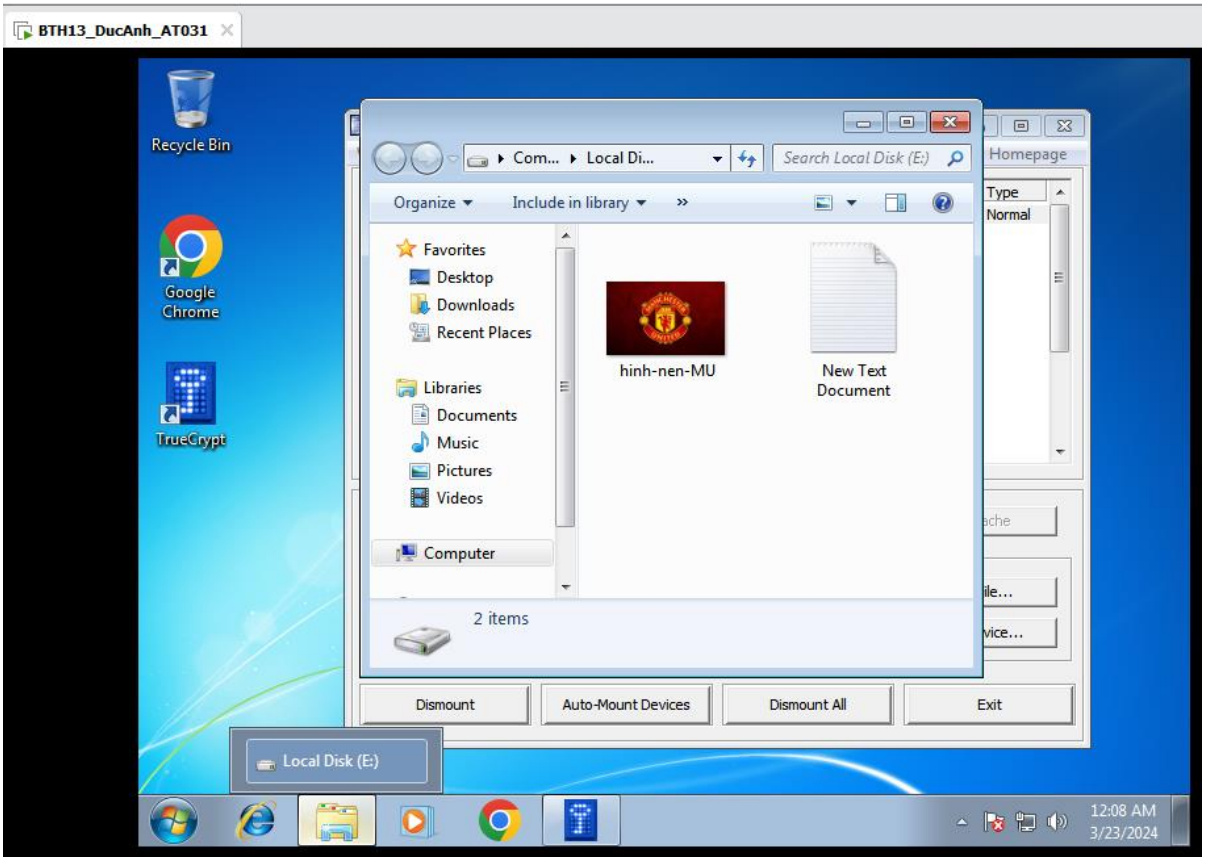




Dismount ổ đĩa để mã hóa file ảnh.

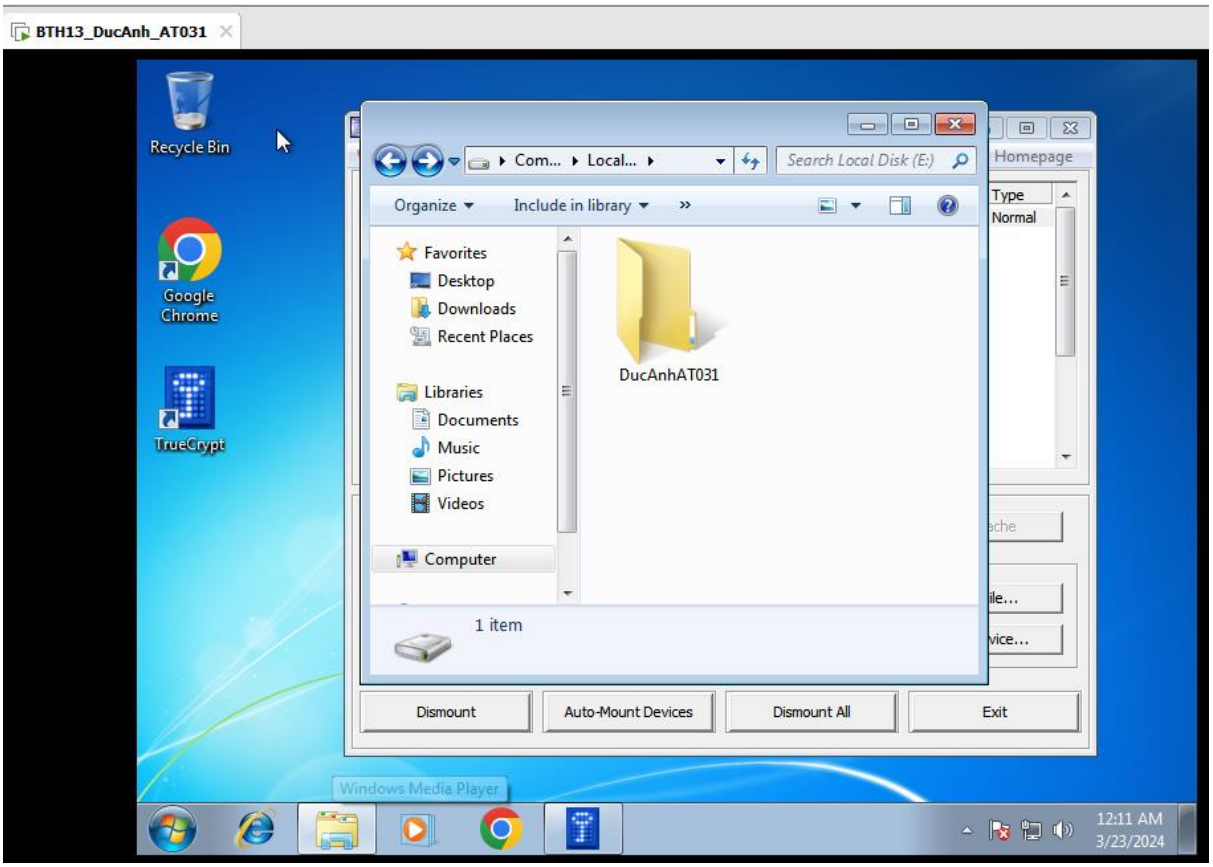


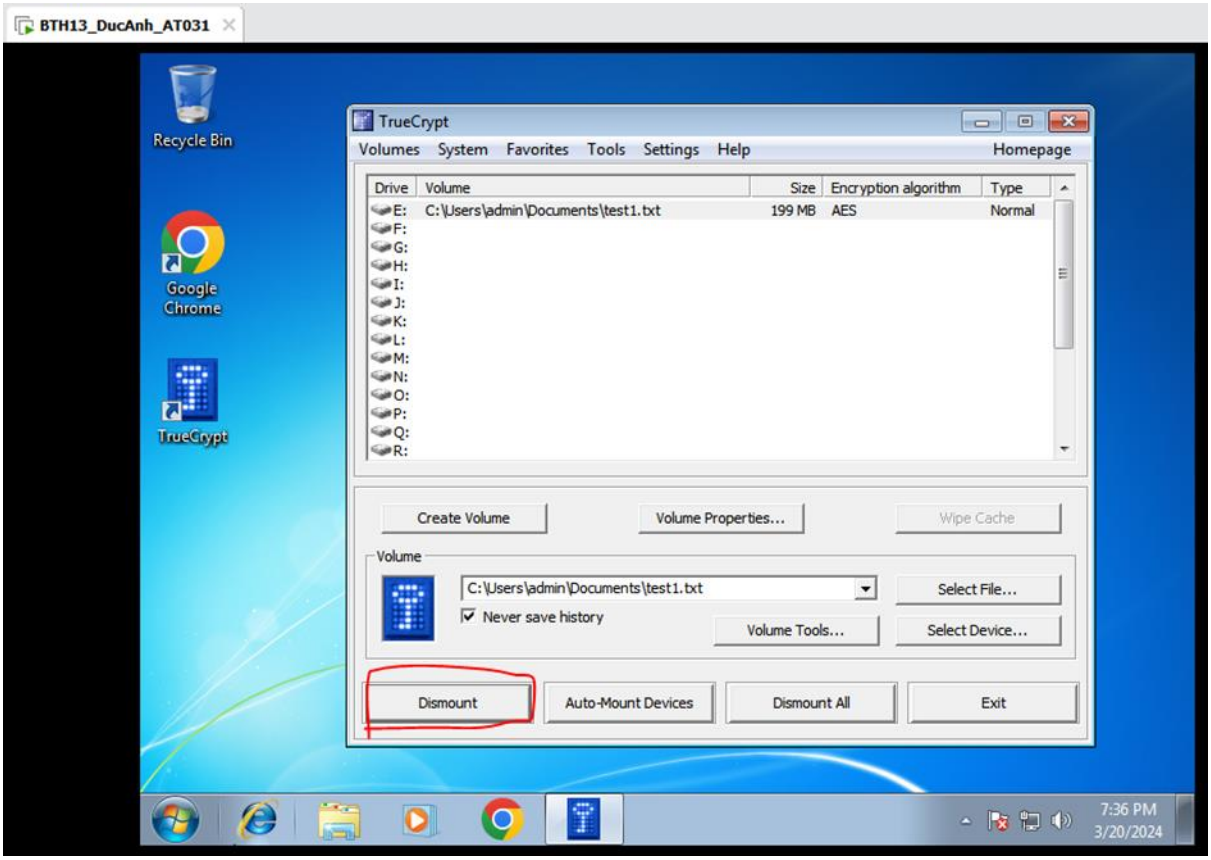
Khi cần xem lại file ảnh, chỉ cần Mount lại ổ đĩa ảo chứa file ảnh



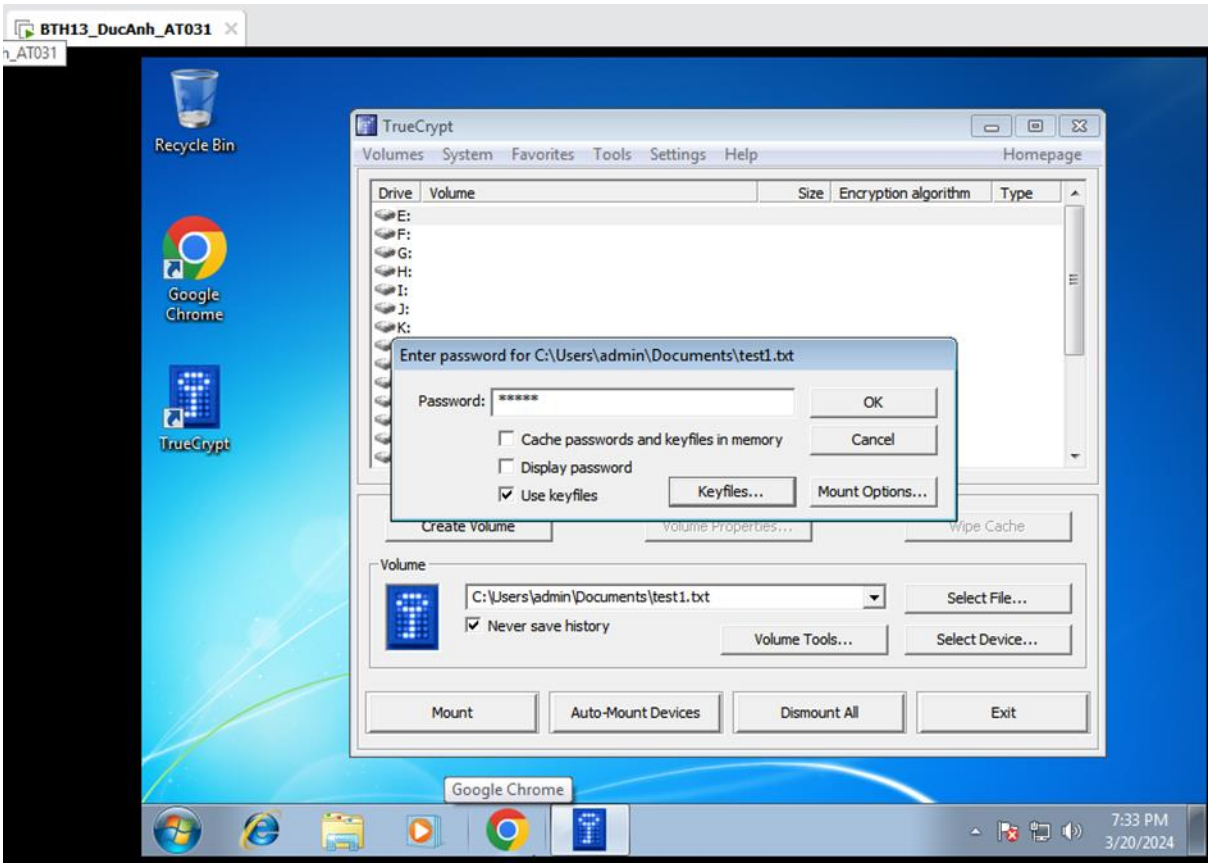
Bước 5: Mã hóa thư mục

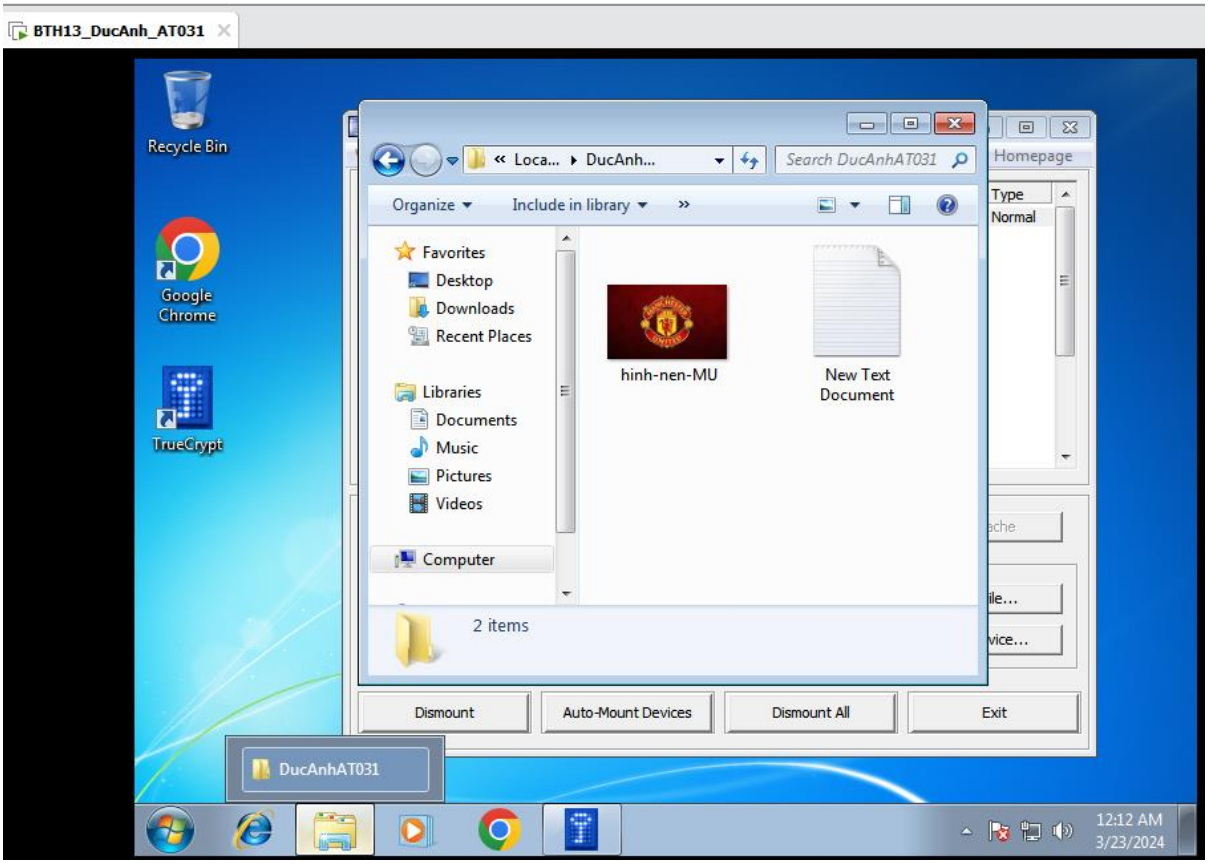
Tương tự với mã hóa file văn bản và file hình ảnh, ta cũng sẽ đưa thư mục cần mã hóa vào ổ đĩa ảo đã tạo, sau đó dismount.





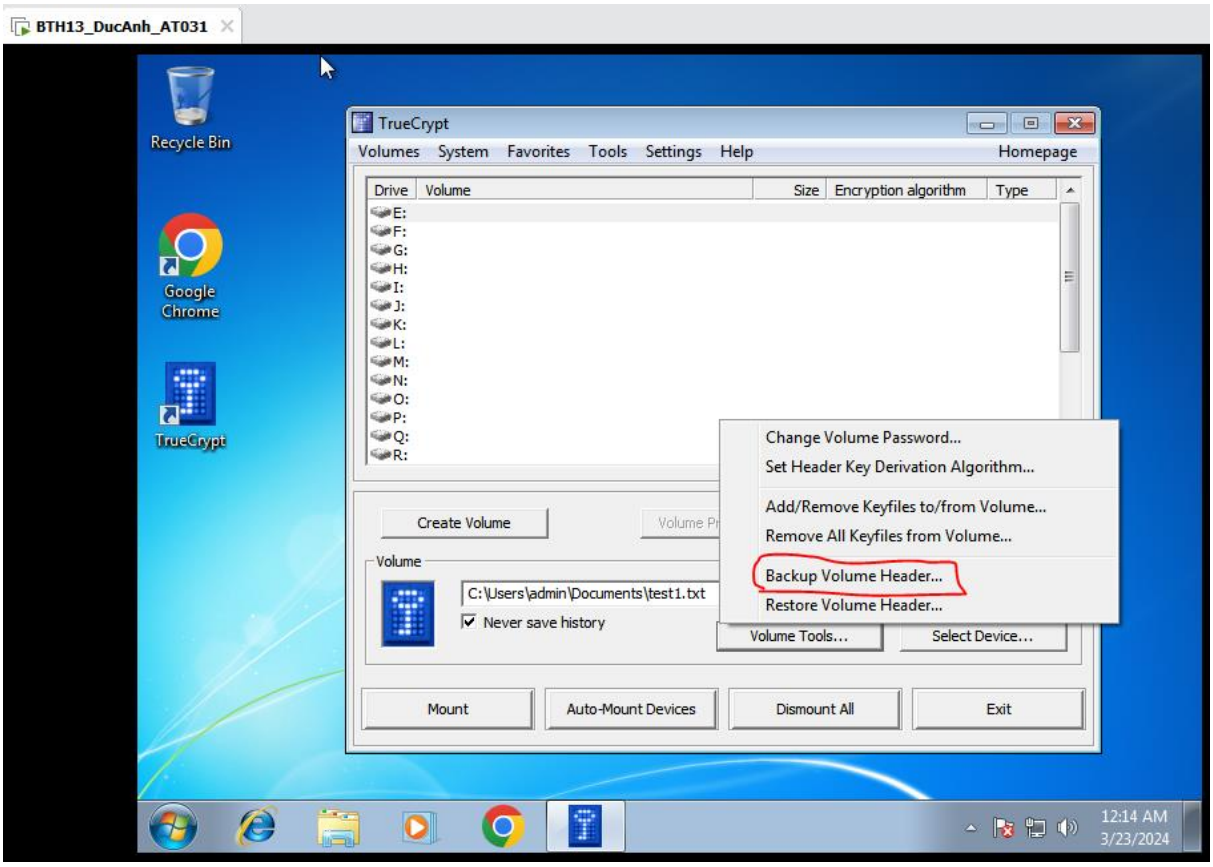
Để xem được thư mục đã mã hóa, ta chỉ cần Mount lại ổ đĩa với mật khẩu và keyfile tương ứng.



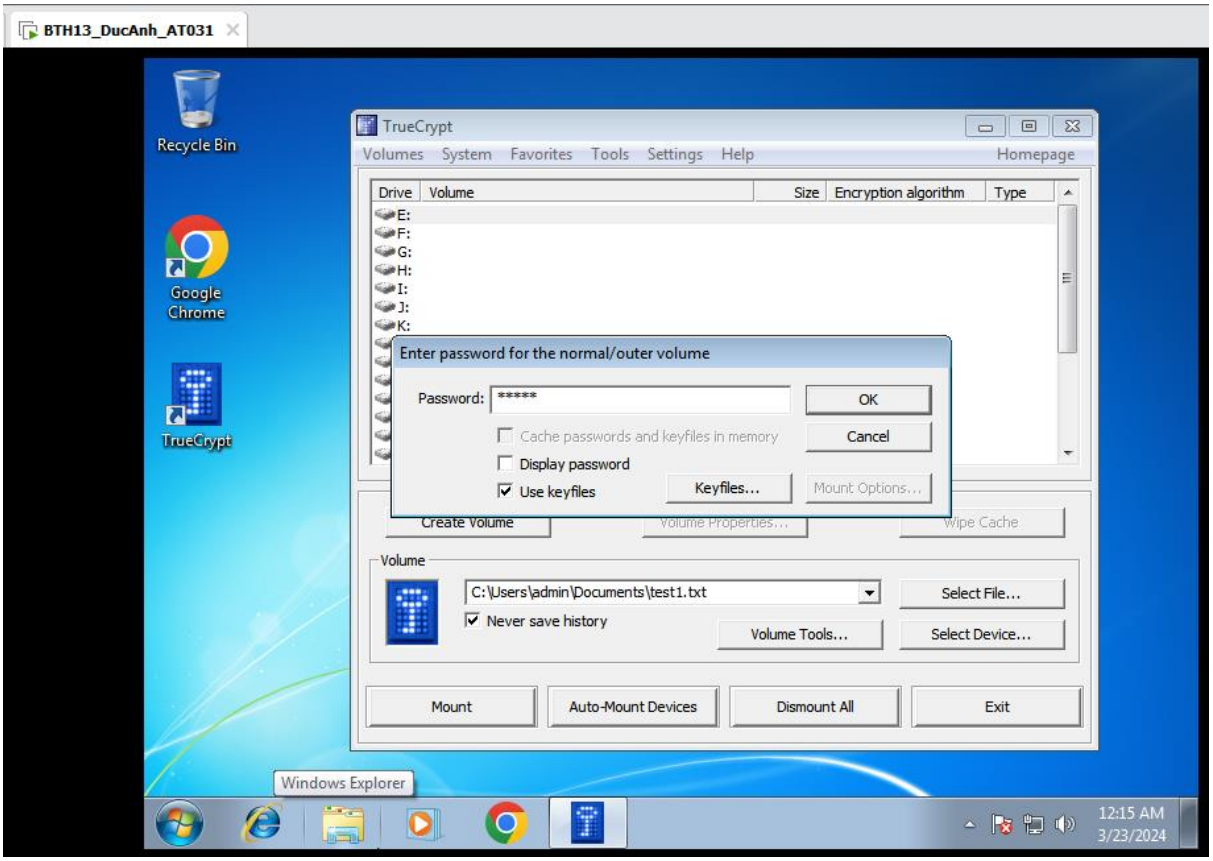


Bước 6: Sao lưu khóa mã hóa của TrueCrypt

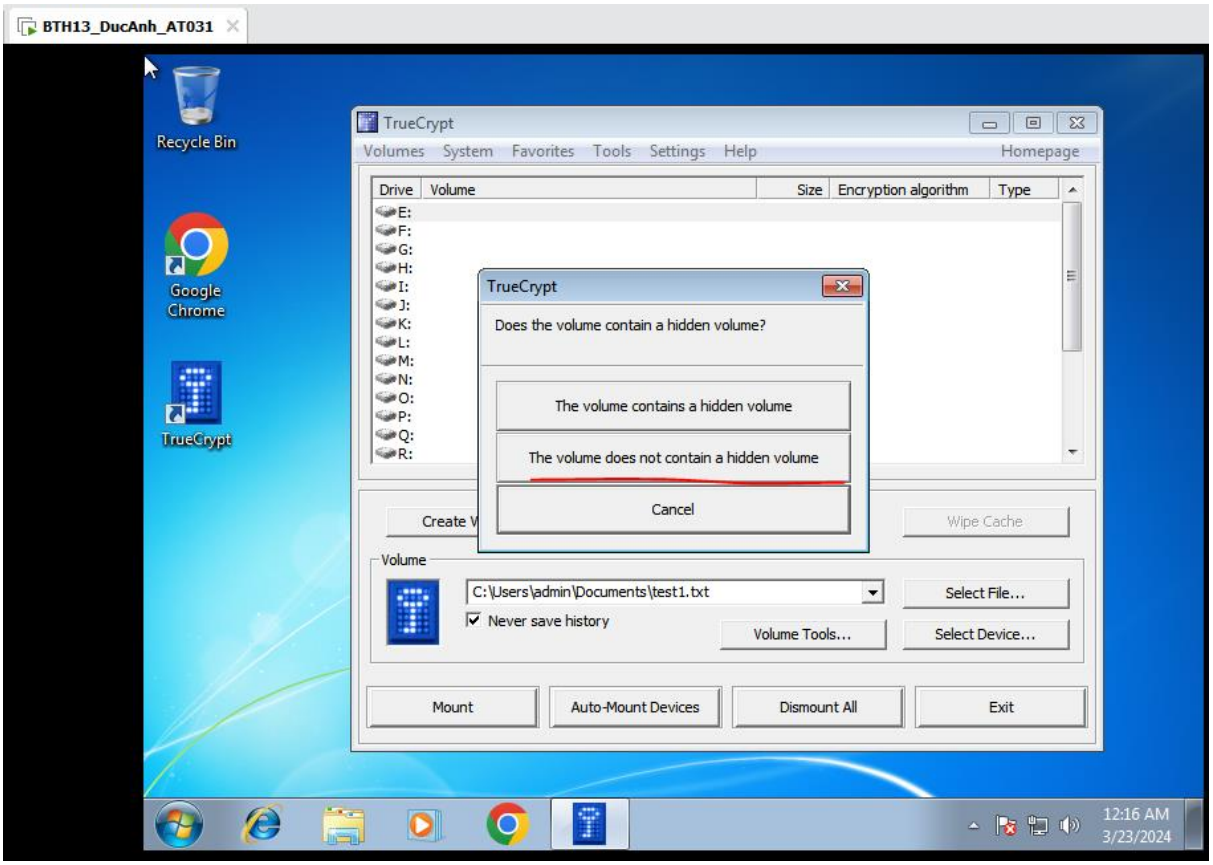
Sau khi tạo tệp tin container, chọn tệp tin đó trong phần mềm TrueCrypt và nhấn vào nút "Volumes" trên giao diện chính. Chọn "Backup Volume Header" để sao lưu khóa mã hóa của bạn.



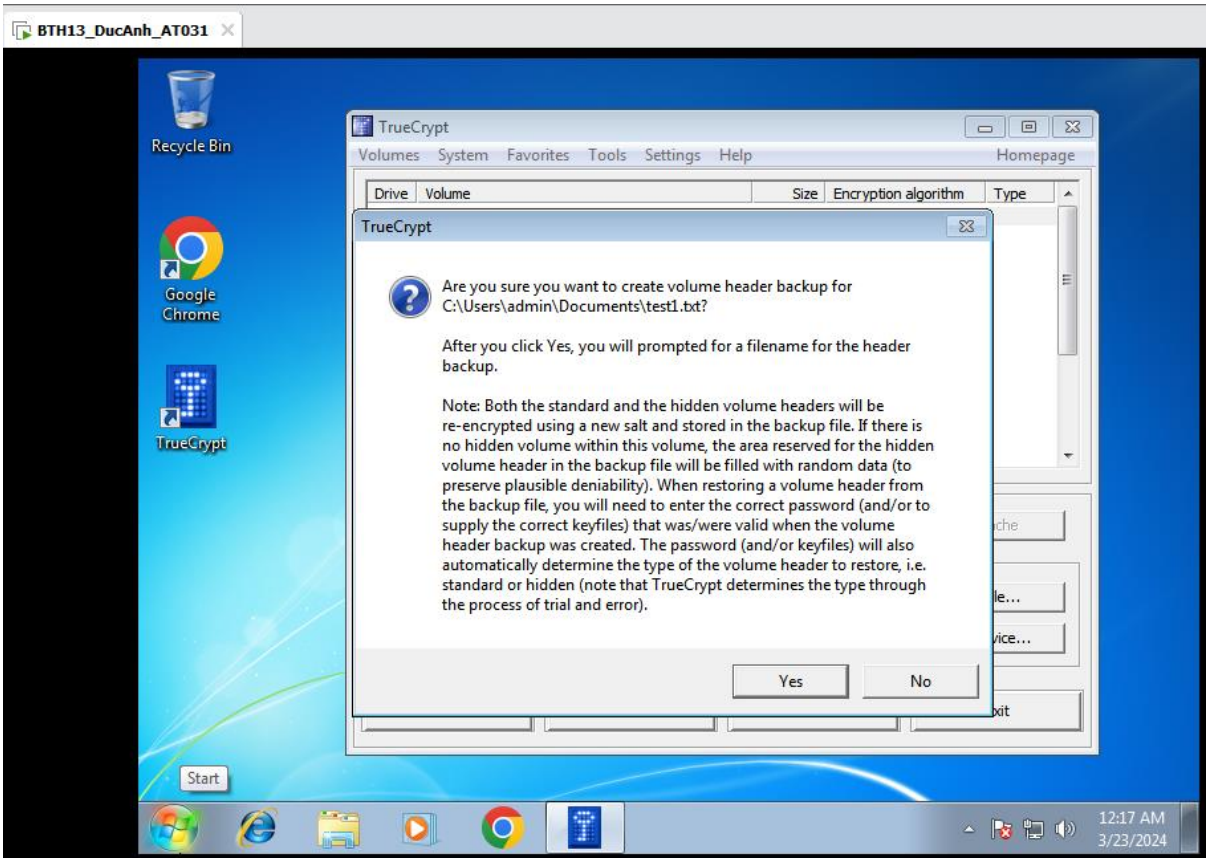
Nhập mật khẩu và keyfile

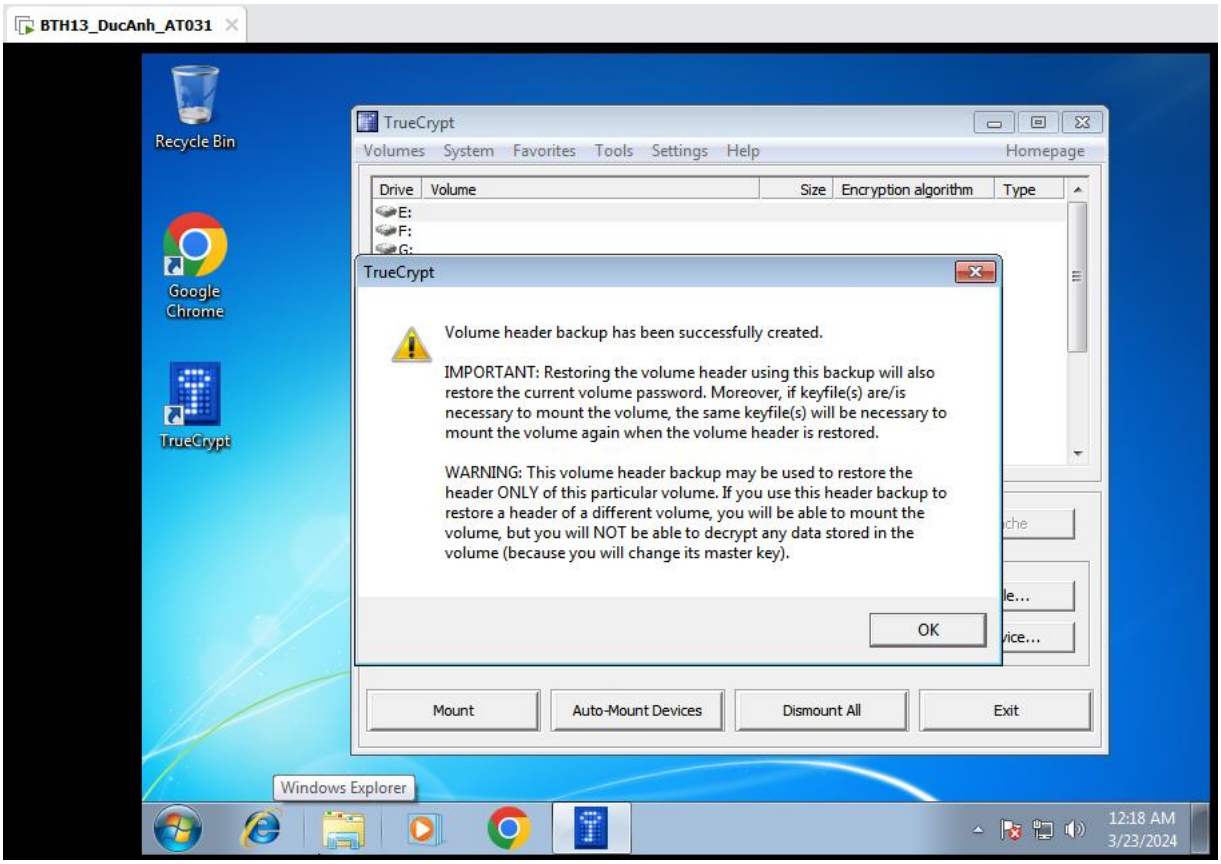


Chọn The Volume does not contain a hidden volume

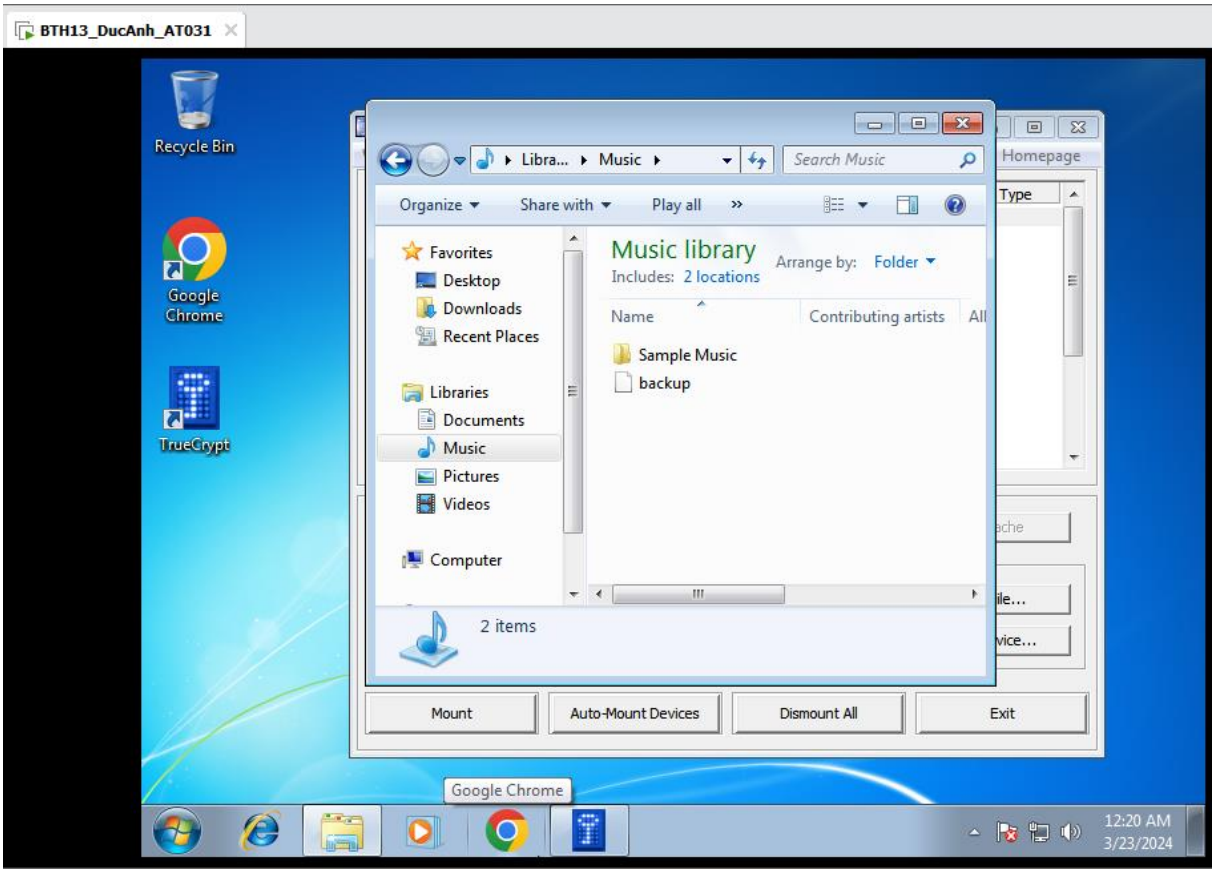

BTH13_DucAnh_AT031
Recycle Bin
Google Chrome
TrueCrypt
TrueCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption algorithm Type
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
O:
P:
Q:
R:
TrueCrypt
Does the volume contain a hidden volume?
The volume contains a hidden volume
The volume does not contain a hidden volume
Cancel
Create V
Wipe Cache
Volume
C:\Users\admin\Documents\test1.txt
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit
12:16 AM
3/23/2024

Chọn Yes


BTH13_DucAnh_AT031
Recycle Bin
Google Chrome
TrueCrypt
TrueCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption algorithm Type
TrueCrypt
Are you sure you want to create volume header backup for C:\Users\admin\Documents\test1.txt?
After you click Yes, you will prompted for a filename for the header backup.
Note: Both the standard and the hidden volume headers will be re-encrypted using a new salt and stored in the backup file. If there is no hidden volume within this volume, the area reserved for the hidden volume header in the backup file will be filled with random data (to preserve plausible deniability). When restoring a volume header from the backup file, you will need to enter the correct password (and/or to supply the correct keyfiles) that was/were valid when the volume header backup was created. The password (and/or keyfiles) will also automatically determine the type of the volume header to restore, i.e. standard or hidden (note that TrueCrypt determines the type through the process of trial and error).
Yes
No
Start
12:17 AM
3/23/2024



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.

3. Kết quả đạt được

- Cài đặt thành công phần mềm mã hóa TrueCrypt
- Mã hóa/giải mã được các file và thư mục sử dụng TrueCrypt
- Sao lưu thành công khóa mã hóa của TrueCrypt