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

BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147

BÀI THỰC HÀNH 2.4

ĐẢM BẢO AN TOÀN THÔNG TIN DỰA TRÊN MÃ HÓA

Sinh viên thực hiện: B22DCAT176 Nguyễn Thị Thùy Linh

Giảng viên hướng dẫn: PGS.TS Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC HÌNH ẢNH

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
ARM	Advanced RISC Machine	Kiến trúc bộ xử lý dựa trên RISC
SSH	Secure Shell	Giao thức thiết lập kết nối an toàn giữa hai hệ thống
GUI	Graphical User Interface	Giao diện đồ họa
ICMP	Internet Control Message Protocol	Thông báo các lỗi xảy ra trong quá trình truyền các gói dữ liệu của mạng.
LAN	Local Area Network	Mạng nội bộ

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

I. 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 dảm bảo an toàn dữ liệu.

II. Tìm hiểu lý thuyết

1.Tìm hiểu về TrueCrypt

1.1 Cách hoạt động

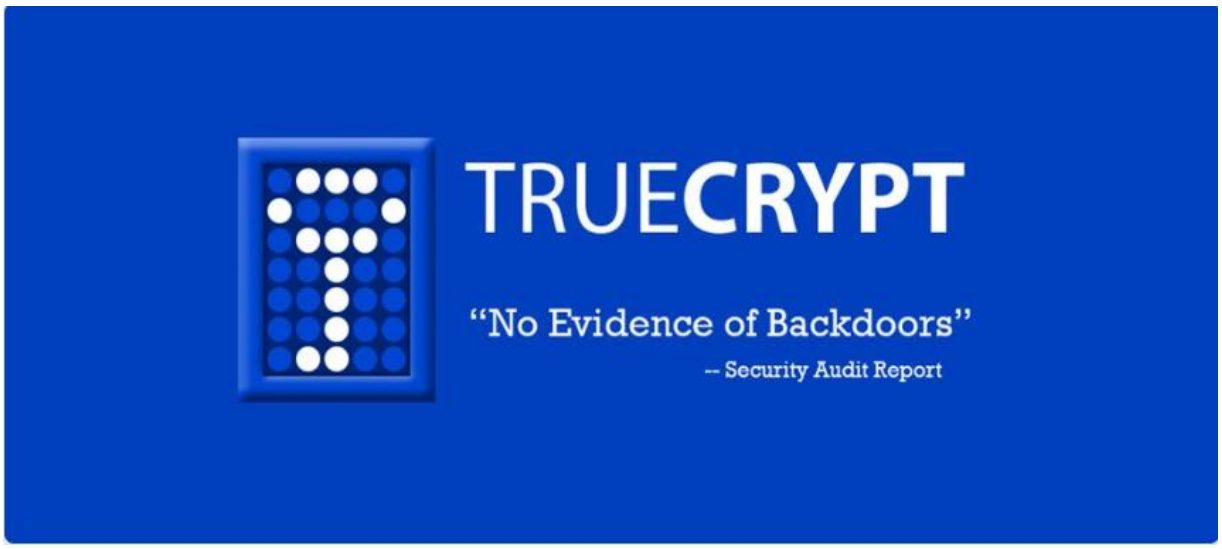
TrueCrypt là một phần mềm mã hóa dữ liệu mã nguồn mở, được sử dụng để tạo ra các file ảo hoặc các phân vùng ổ đĩa ảo được mã hóa, nhằm bảo vệ dữ liệu trước khi lưu trữ hoặc truyền tải trên Internet.

Cơ chế thiết lập và quản lý của TrueCrypt là mã hóa ổ đĩa trên đường đi (*in-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 bằn một trong ba hình thức là mật khẩu 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 thưởng trên máy tính của người dùng.

TrueCrypt cũng hỗ tợ việc tạo ra các file ảo chứa dữ liệu mã hóa. Người dùng có thể tạo ra một file ảo, chọn mât 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.



Hình ảnh 1 : Phần mềm TrueCrypt.

1.2 Cách mã hóa một file với TrueCrypt

Để mã hóa một file với TrueCrypt, bạn cần thực hiên 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 TrueCrpyt, sau đó chọn "*Create Volume*" để tạp một ổ đĩa mã hóa mới.

3. Trong cửa sổ “*TrueCrypt Volume Creation Wizard*”, chọn “*Creare 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

CHƯƠNG 2 : NỘI DUNG THỰC HÀNH

I. Chuẩn bị môi trường

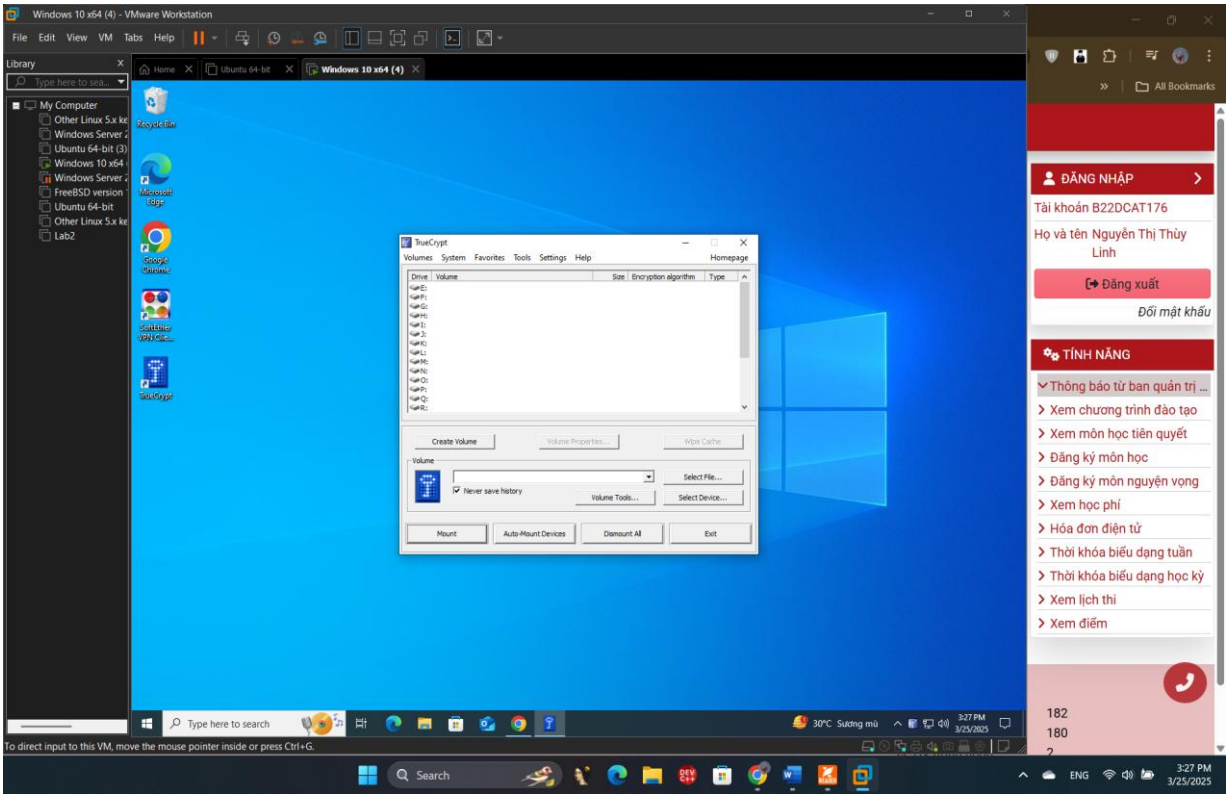
- Phần mềm ảo hóa Vmware.
- Máy ảo Windows.
- Công cụ TrueCrypt.

II. Các bước thực hiện

1.1 Chuẩn bị máy ảo Windows.

1.2 Cài đặt TrueCrypt trên máy ảo.

- Vào trang chủ *truecrypt.org* để tải và cài đặt TrueCrypt.

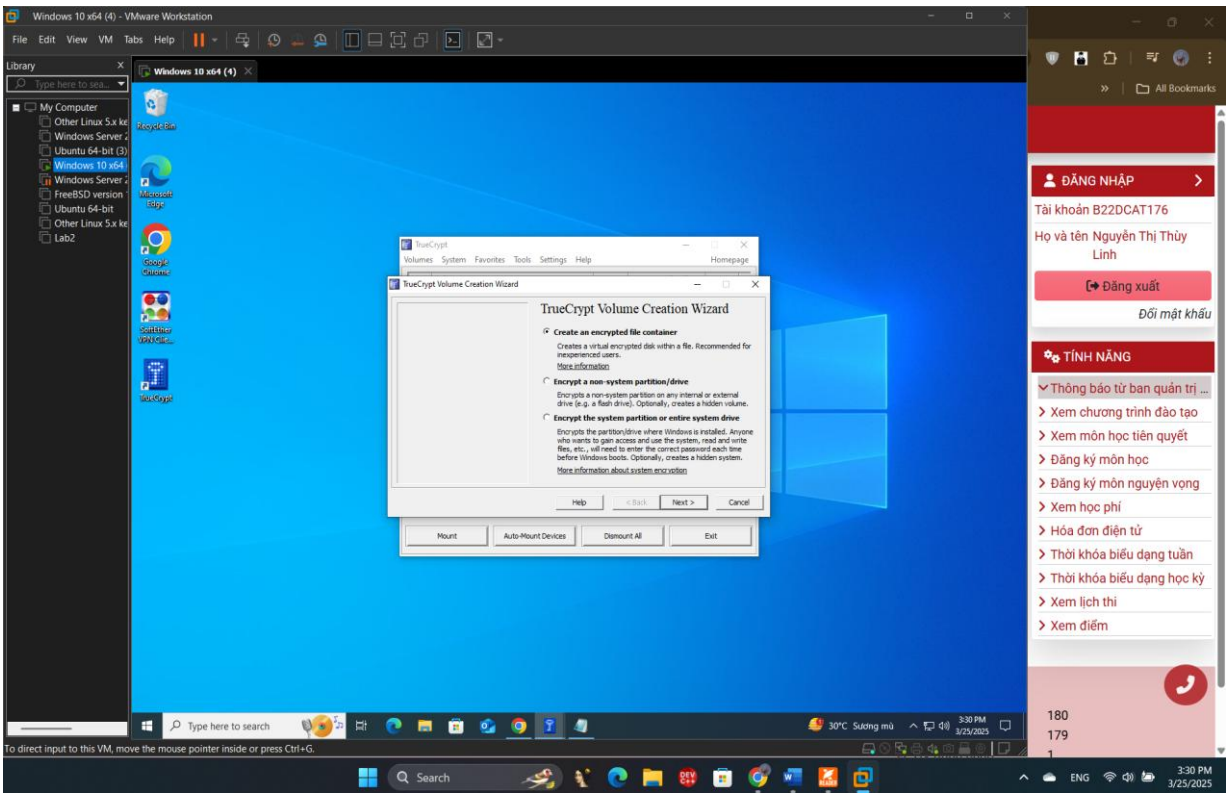


Hình ảnh 2: Phần mềm TrueCrypt sau khi đã cài đặt xong.

1.3 Mã hóa file văn bản:

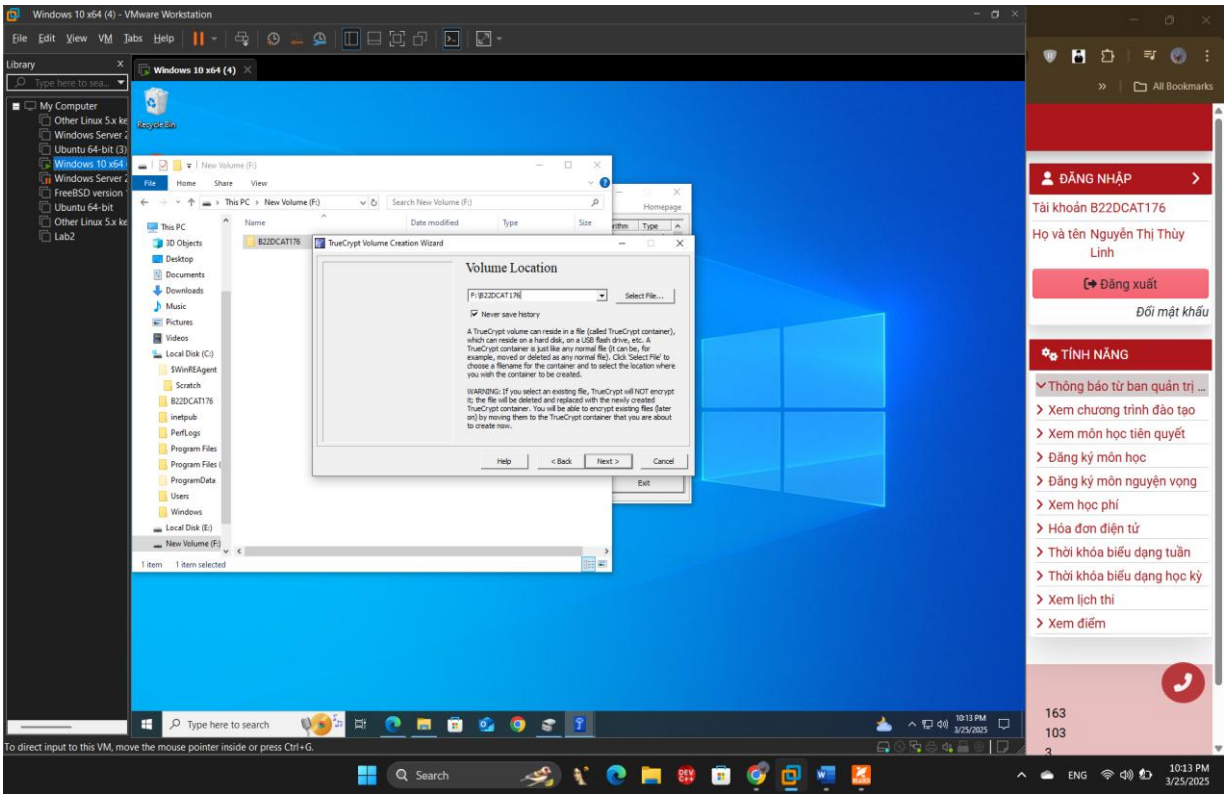
- Tạo một ổ đĩa ảo để đưa file văn bản vào trong đó:

Chọn nút *Create Volume*.



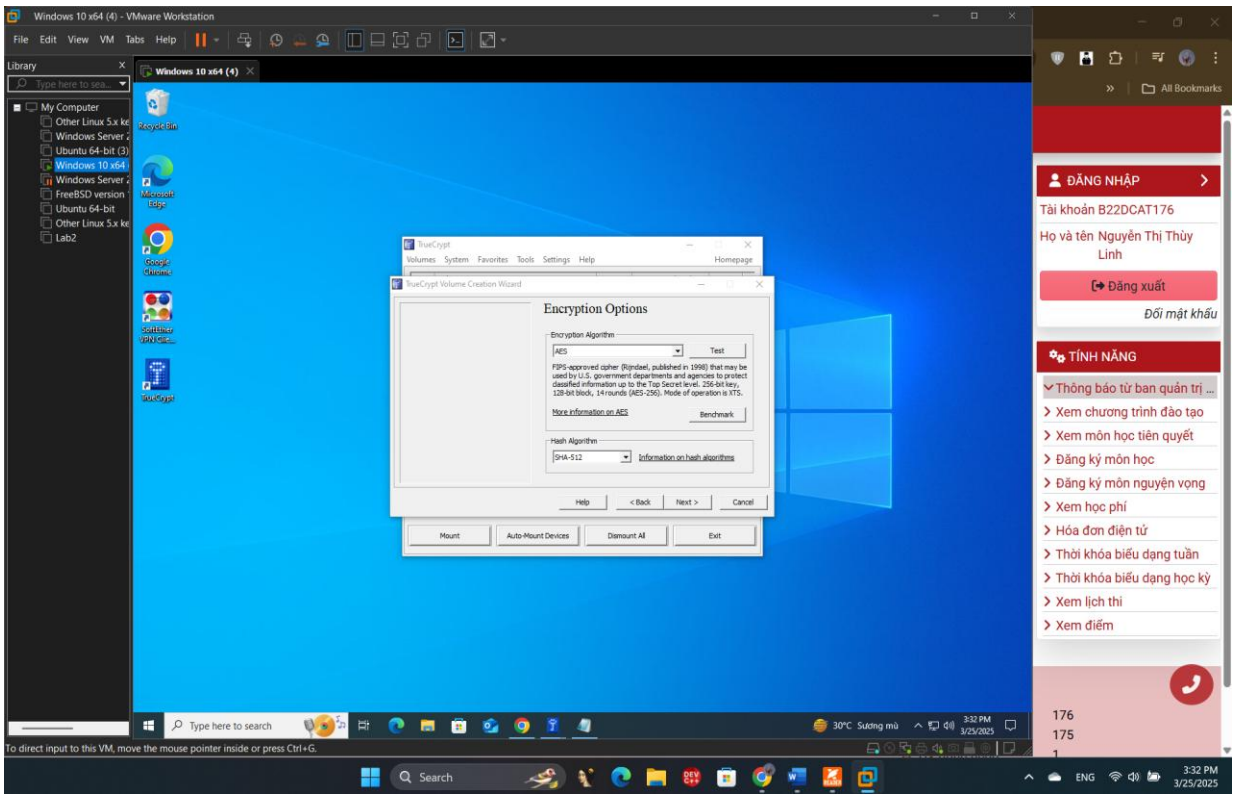
Hình ảnh 3: Create Volume.

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



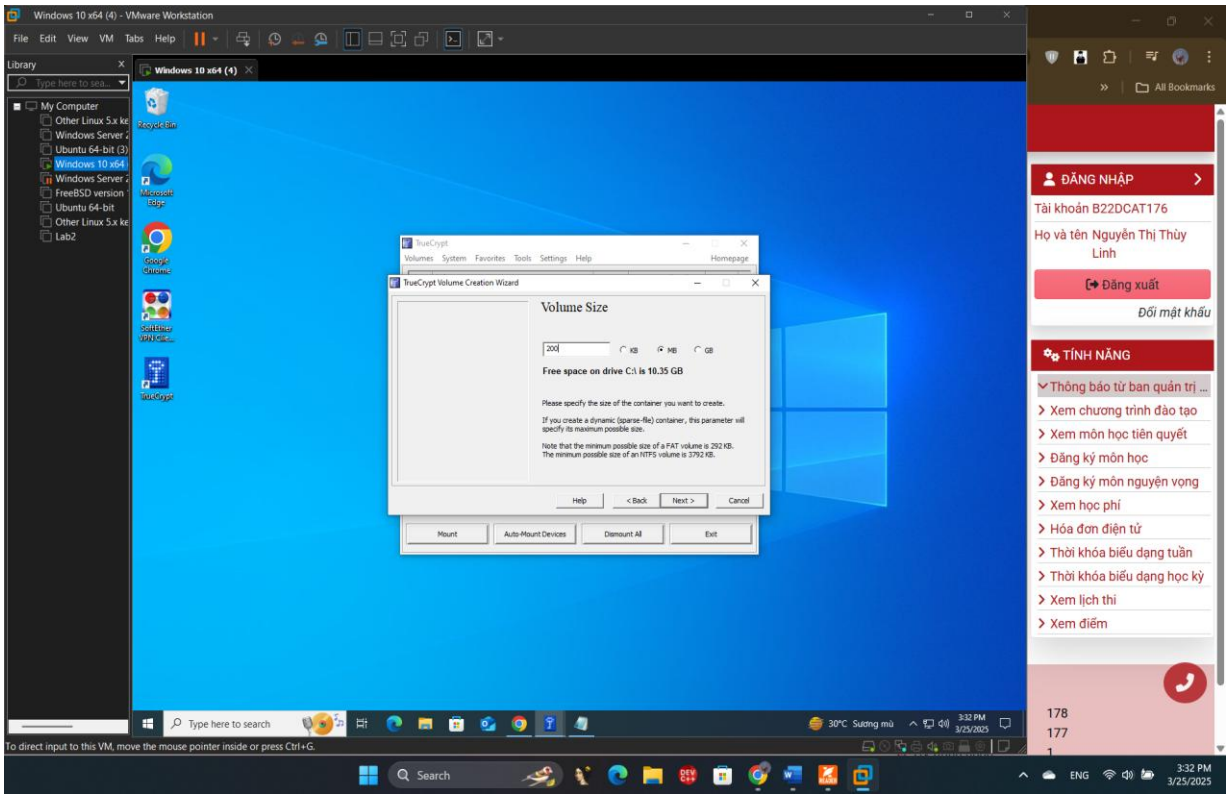
Hình ảnh 4: Nhập đường dẫn mà bạn muốn tạo folder.

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



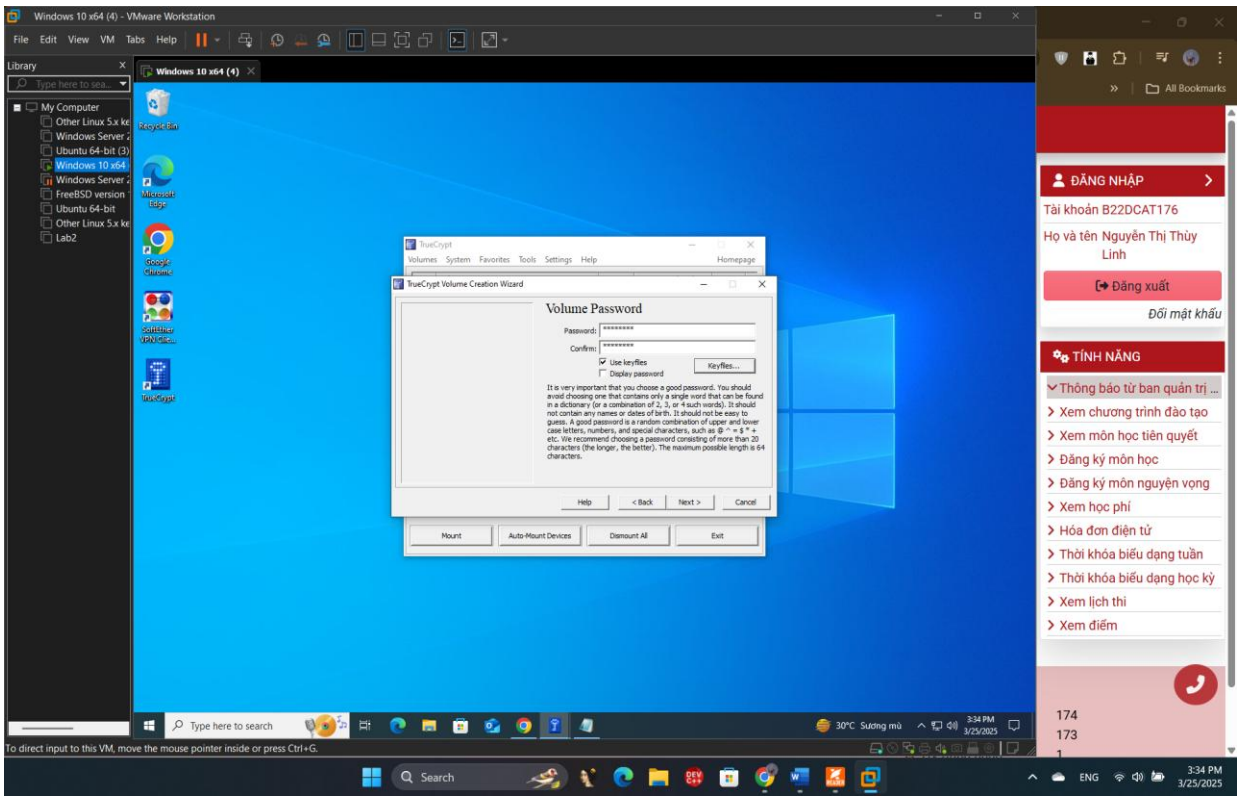
Hình ảnh 5: Chọn thuật toán mã hóa và thuật toán băm.

Để kích thước ổ đĩa ảo là 200MB.



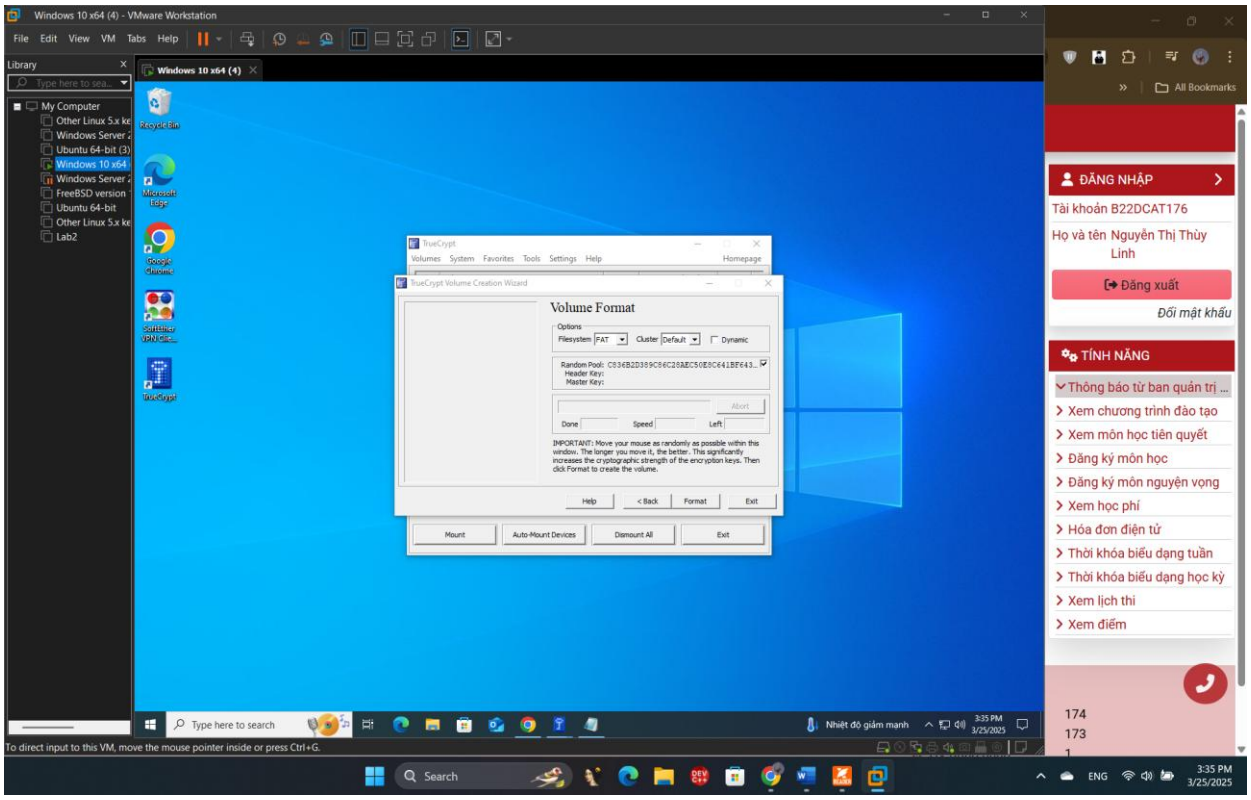
Hình ảnh 6 : Đặt kích thước ổ đĩa ảo.

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



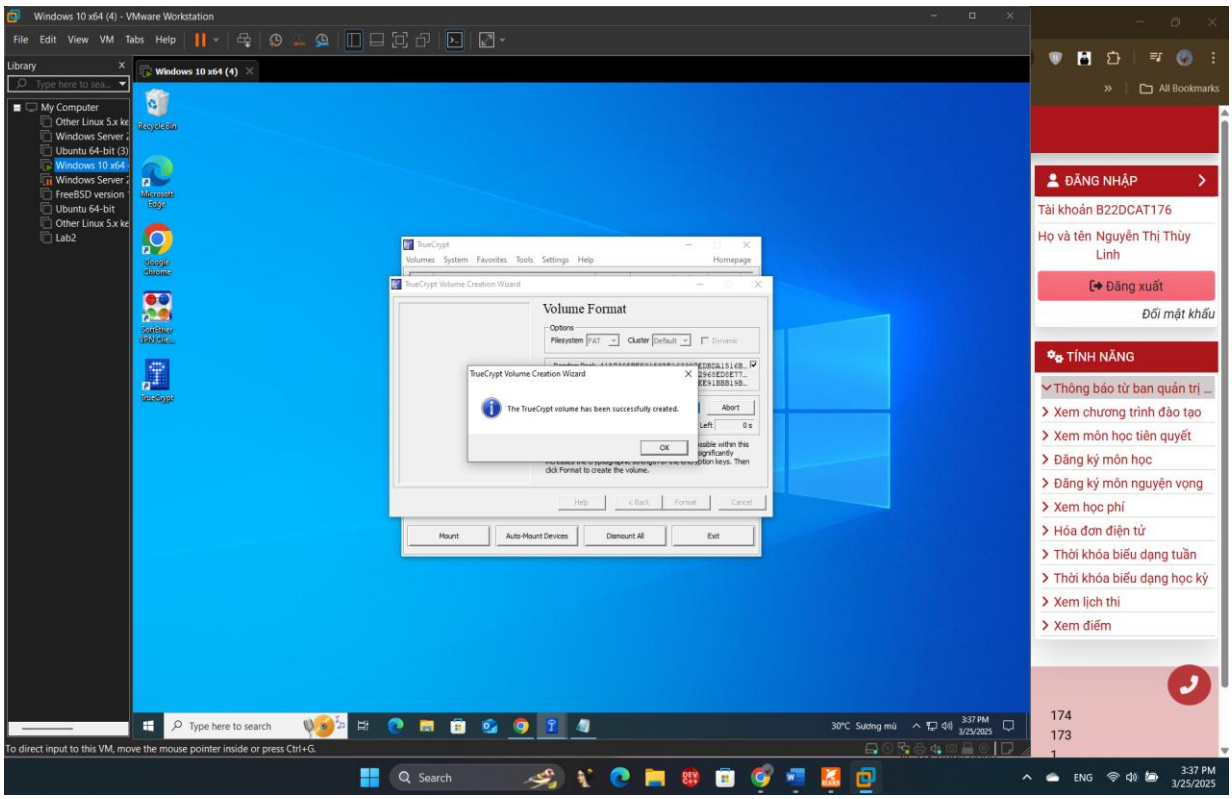
Hình ảnh 7 : Thêm mật khẩu và keyfile.

Chọn nút *Format* để bắt đầu tạo ổ đĩa ảo.



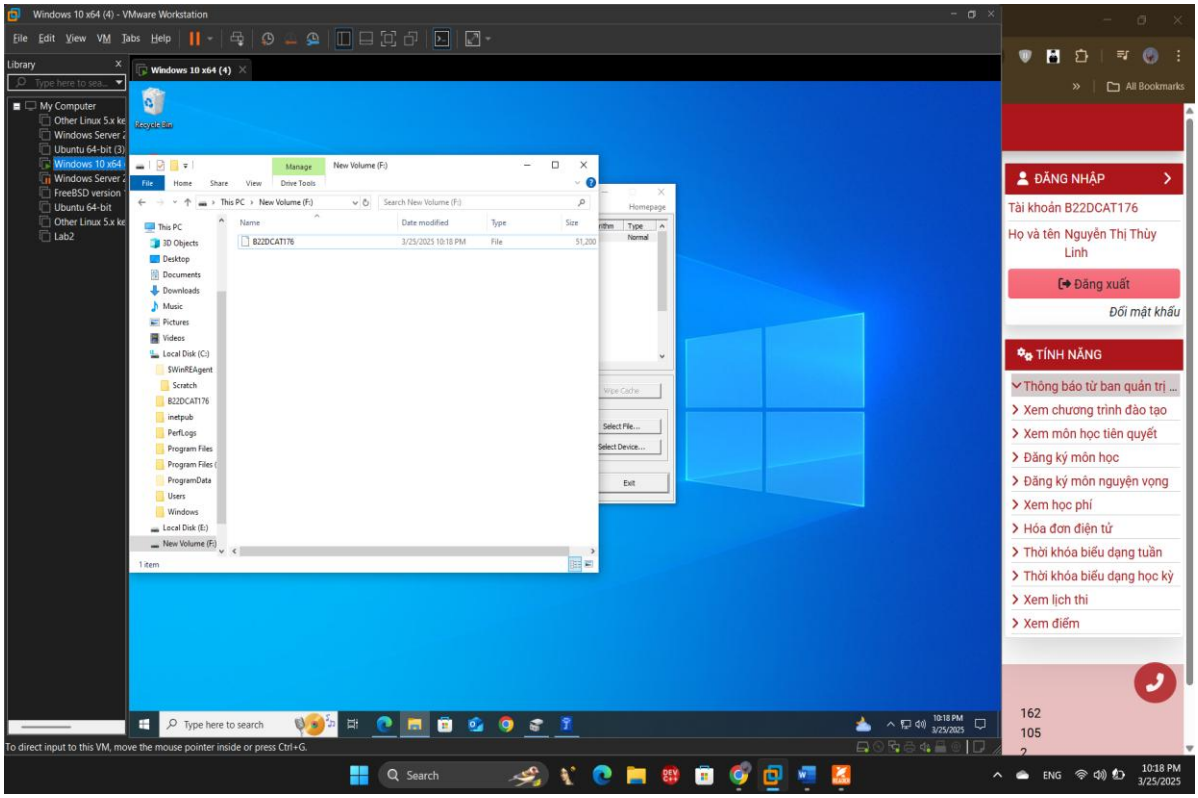
Hình ảnh 8 : Bắt đầu tạo ổ đĩa ảo.

Hiện thông báo tạo ổ đĩa ảo thành công.



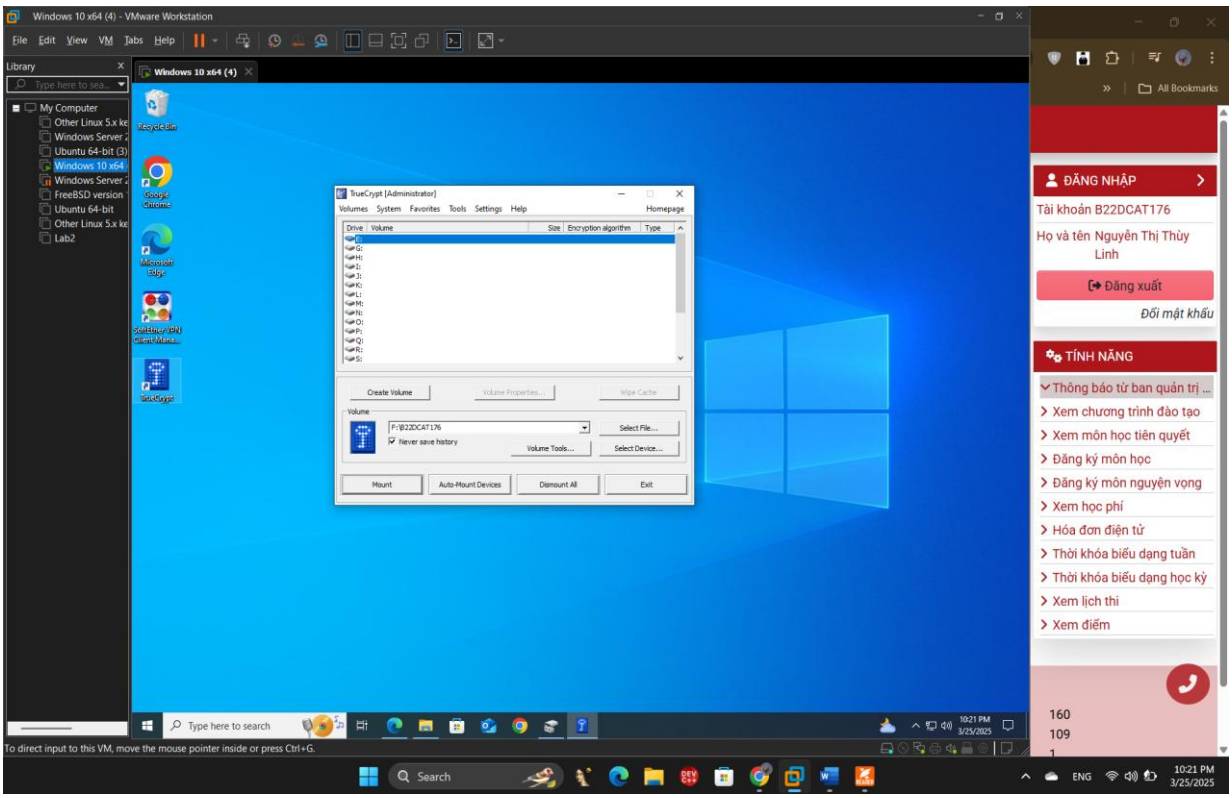
Hình ảnh 9: Tạo ổ đĩa ảo thành công.

Sau khi tạo ổ đĩa ảo thành công, xuất hiện 1 file *B22DCAT176* trong ổ đĩa F (như những gì đã nhập đường dẫn để cài đặt).



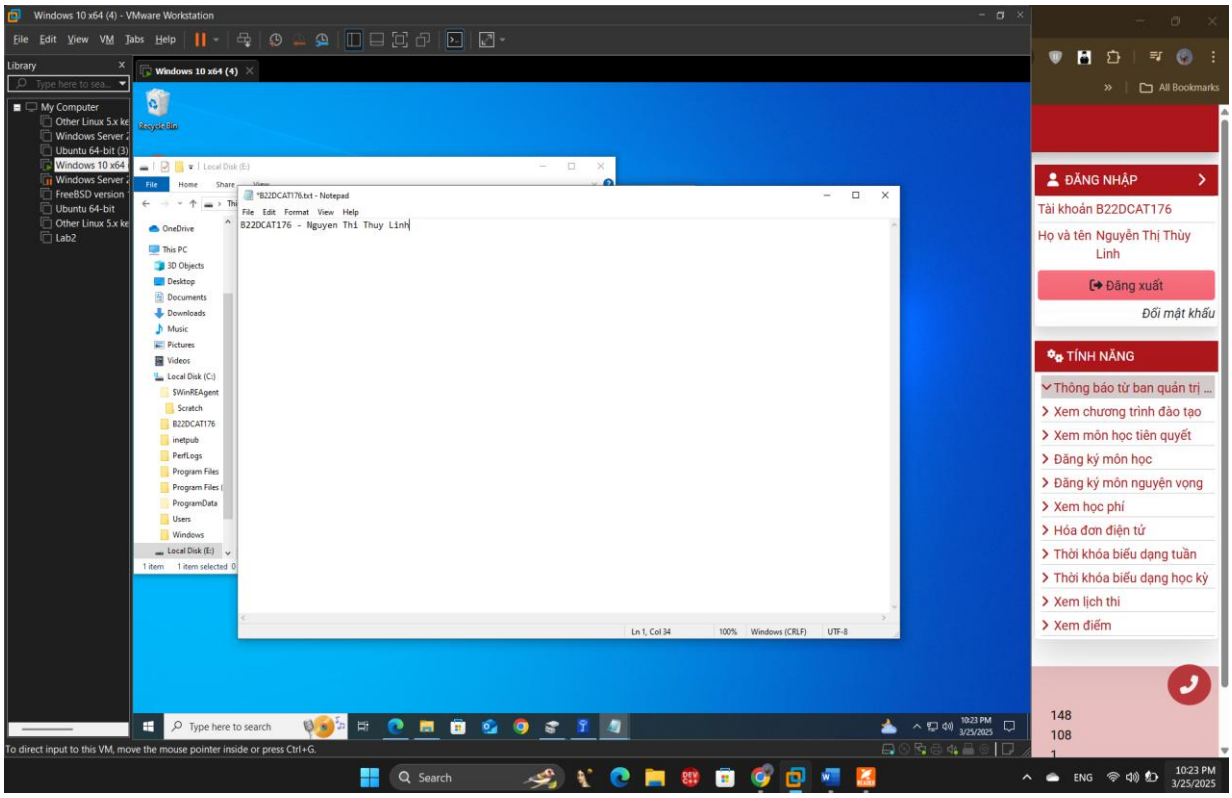
Hình ảnh 10: Xuất hiện file như đường dẫn đã nhập.

Để mã hóa file như đề bài, chọn 1 ổ đĩa ảo (ví dụ ổ E) => *Mount* và tiến hành nhập password và keyfile.



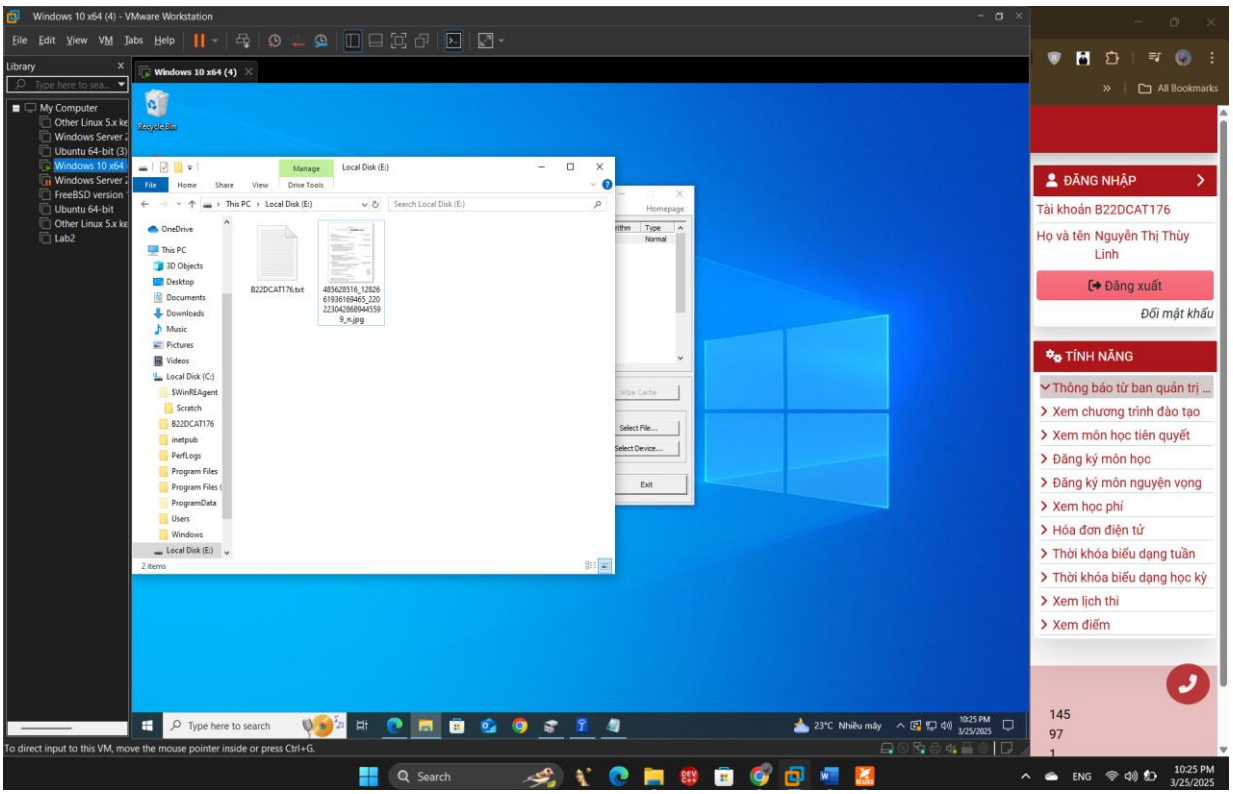
Hình ảnh 11: Chọn ổ đĩa ảo để thực hiện mã hóa file.

Ở ổ E, tạo 1 file txt có dạng B22DCAT176.txt và them nội dung "*B22DCAT176 – Nguyen Thi Thuy Linh*" vào file B22DCAT176.txt



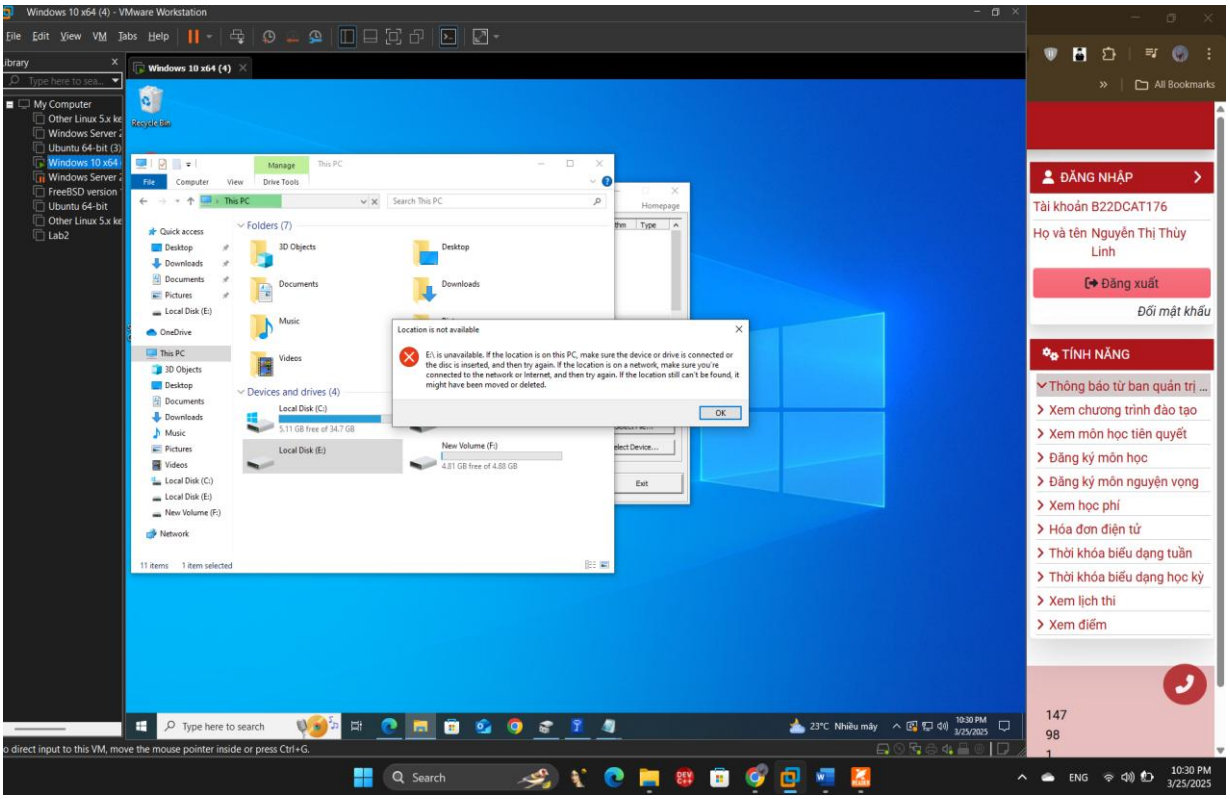
Hình ảnh 12: Tạo file và thêm nội dung vào file B22DCAT176.txt

- Theo như yêu cầu của đề bài, them 1 file hình ảnh vào ổ E, lúc này đã có 2 file và sau đó Dismount.



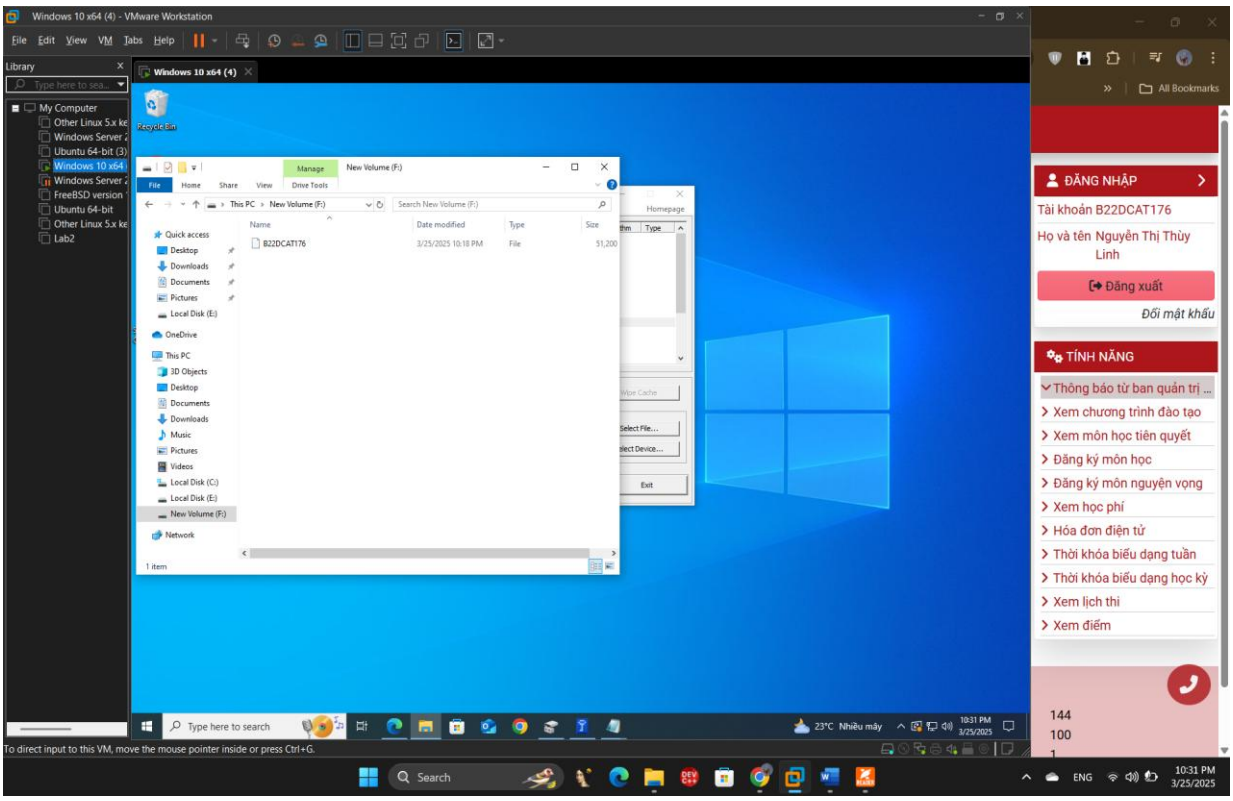
Hình ảnh 13 : Thêm 1 file hình ảnh vào theo yêu cầu.

Lúc này, ta mở lại This PC và thấy ở E đã không còn tồn tại, còn mỗi ổ F tồn tại file B22DCAT176.



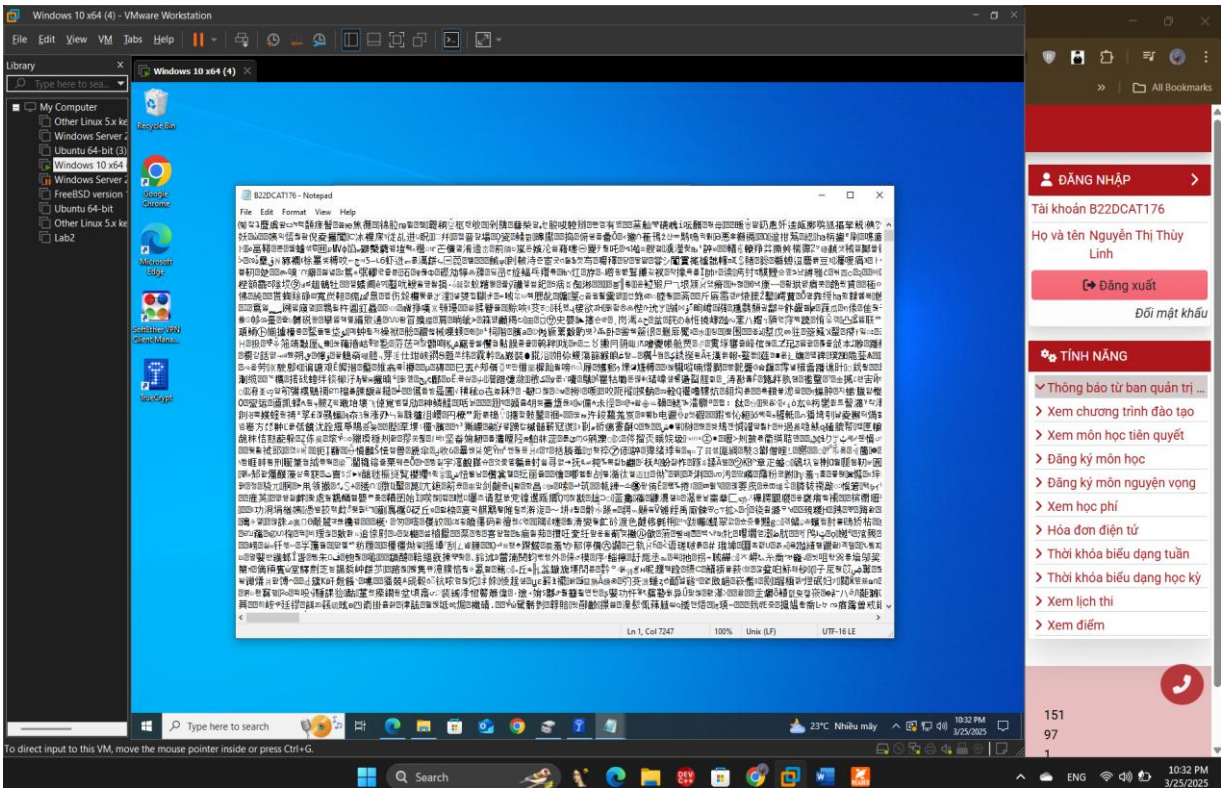
Hình ảnh 14: Kết quả sau khi Dismount.

-Trong ổ F lúc này có file:



Hình ảnh 15 : Kết quả sau khi Dismount.

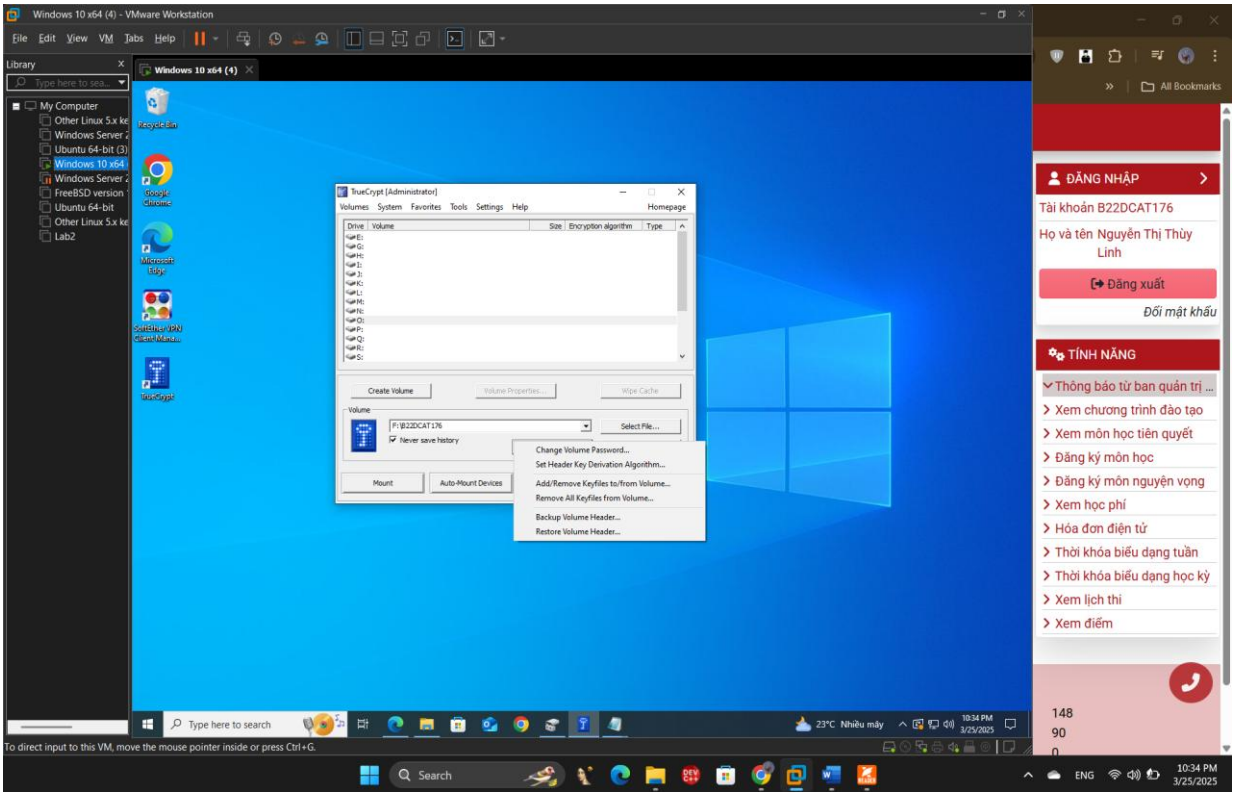
- Xem nội dung file B22DCAT176 thì thấy nội dung lúc này đã được mã hóa.



Hình ảnh 16: Nội dung file B22DCAT176 đã được mã hóa..

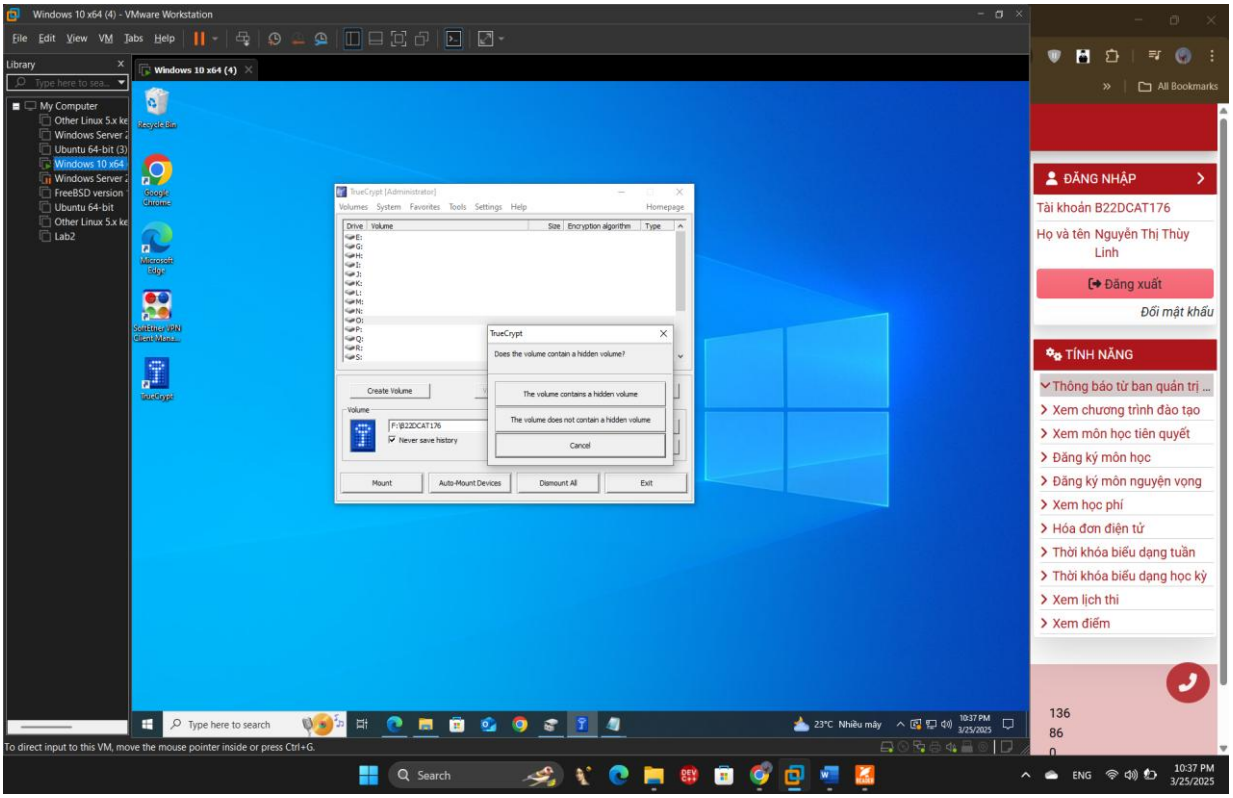
1.4 Sao lưu ổ đĩa

Chọn tệp tin đó trong phần mềm TrueCrypt và nhấn nút "*Volumes*" trên giao diện chính. Chọn "*Backup Volume Header*" để sao lưu khóa mã hóa của bạn và nhập password.



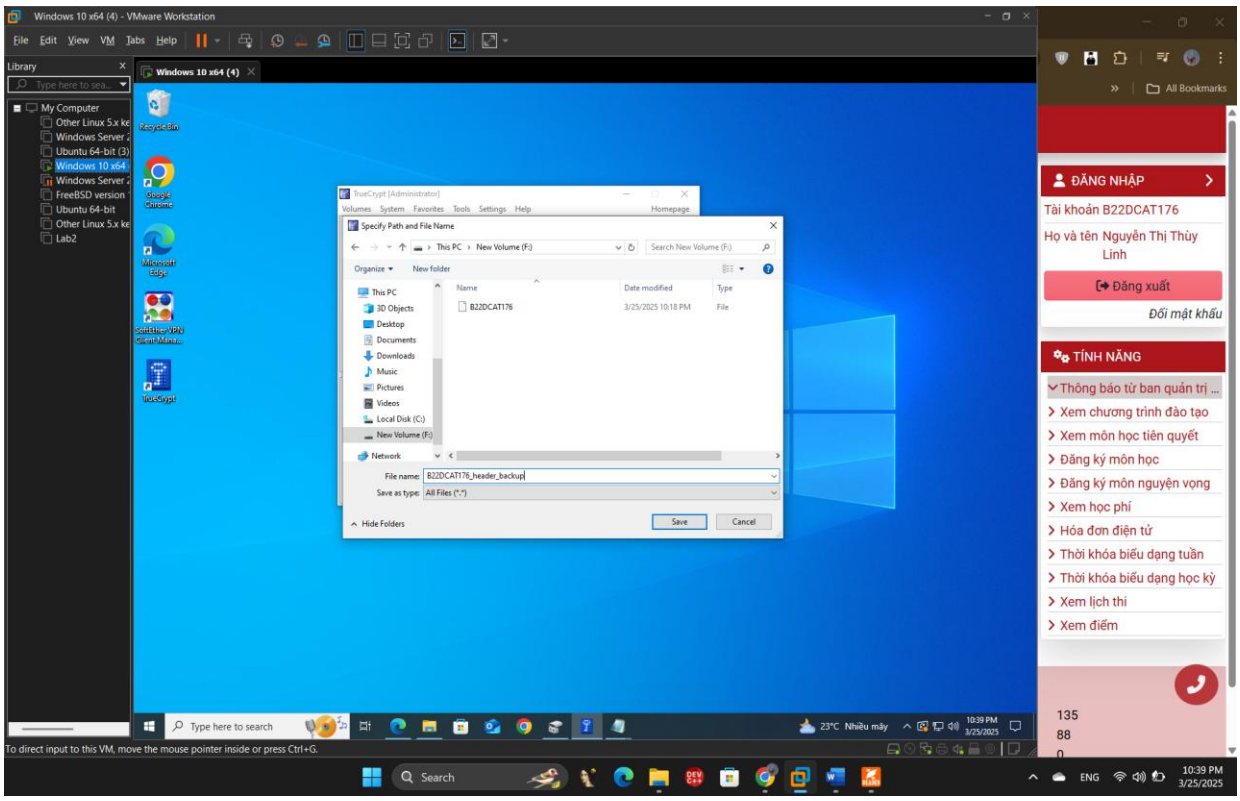
Hình ảnh 17 : Chọn Backup Volume Header.

Chọn tùy chọn thứ 2 "*The volume does not contain a hidden volume*" và chọn *Yes*.



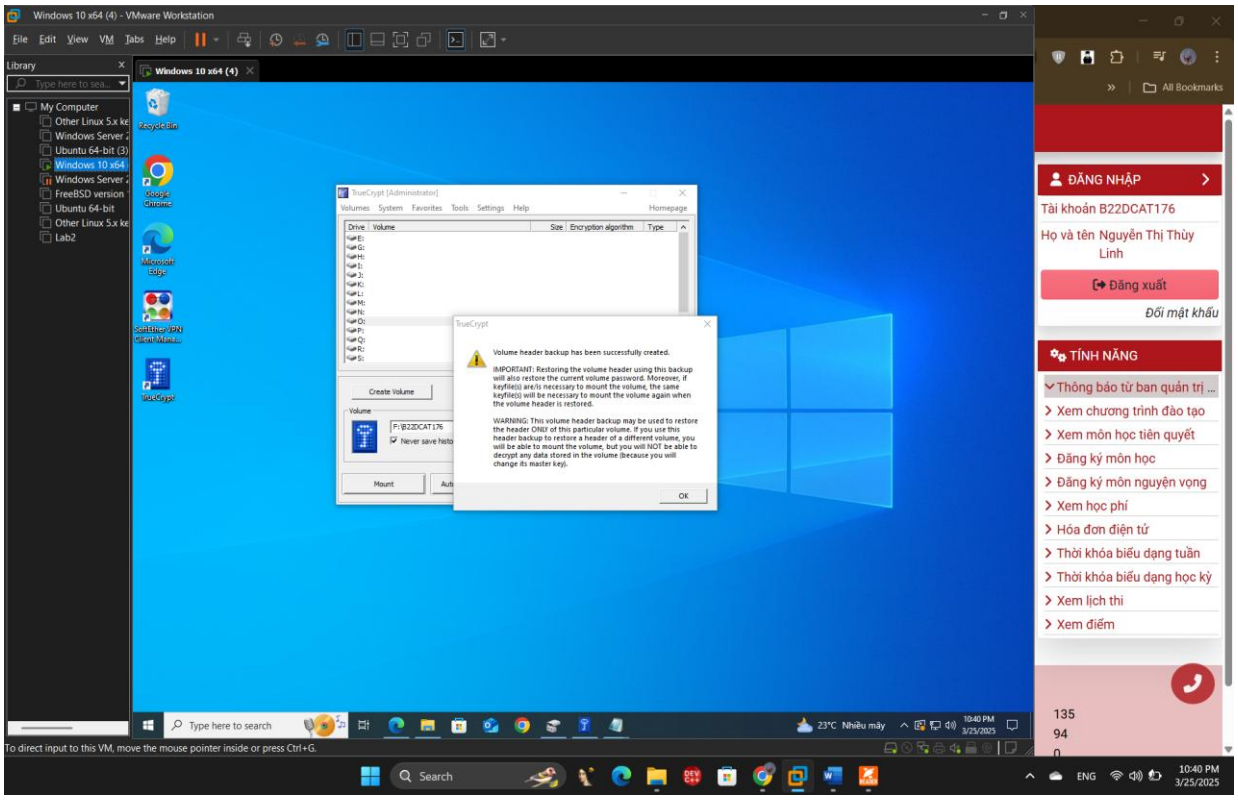
Hình ảnh 18: Chọn tùy chon thứ 2.

- Sau đó chọn file đã bị mã hóa.



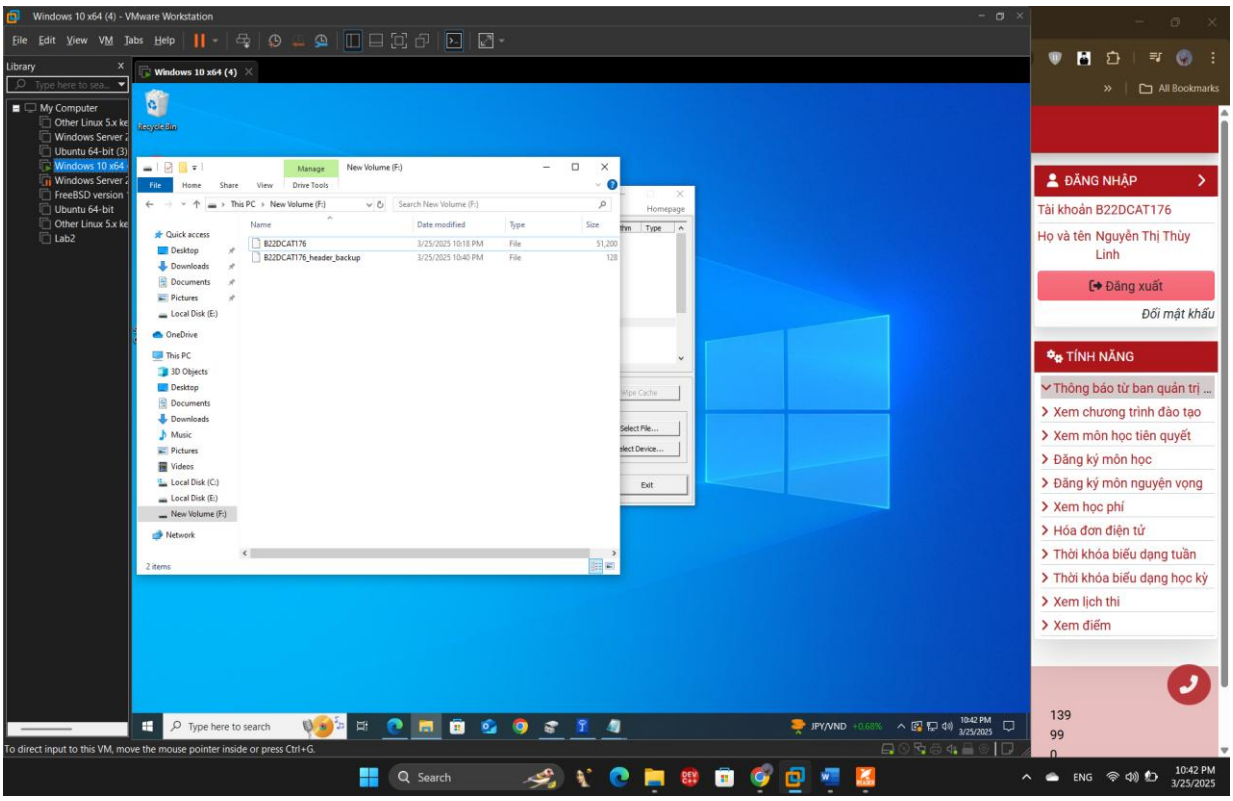
Hình ảnh 19 : Chọn file để backup.

- Hiện thông báo sao lưu back up thành công:



Hình ảnh 20 : Quá trình backup header thành công.

Lúc này ở trong ổ F đã có 2 file, 1 file bị mã hóa ban đầu và 1 file backup.

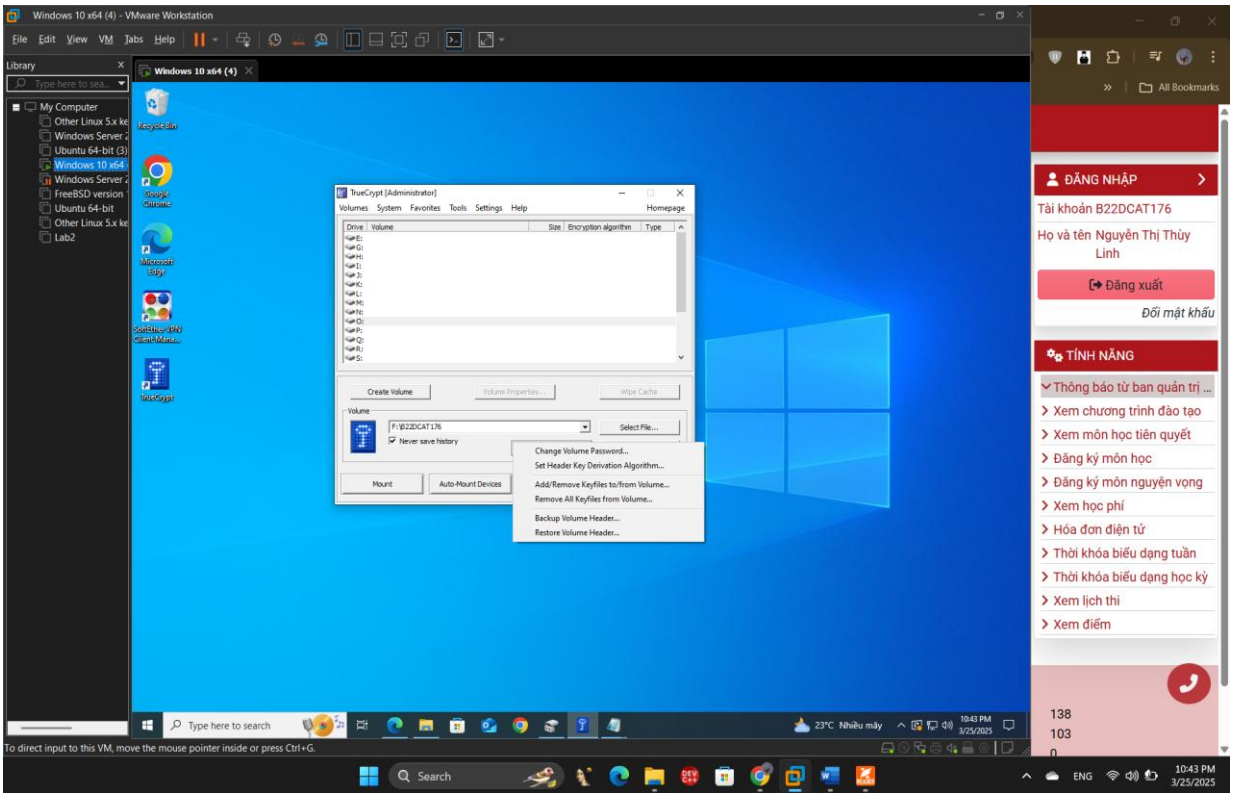


Hình ảnh 21: Kiểm tra lại file đã backup thành công.

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.

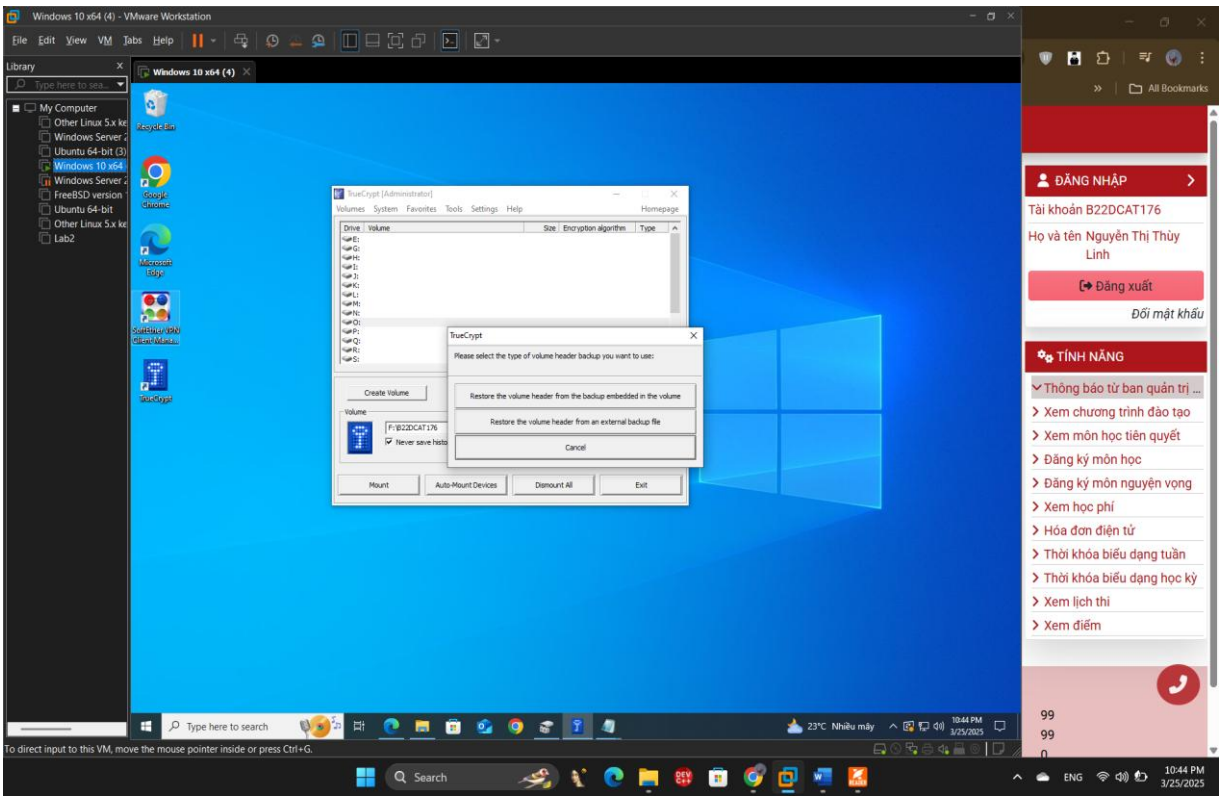
1.5 Tiến hành khôi phục lại

Chọn "*Volume Tools*", chọn "*Restore Volume Header*" để tiến hành khôi phục lại.



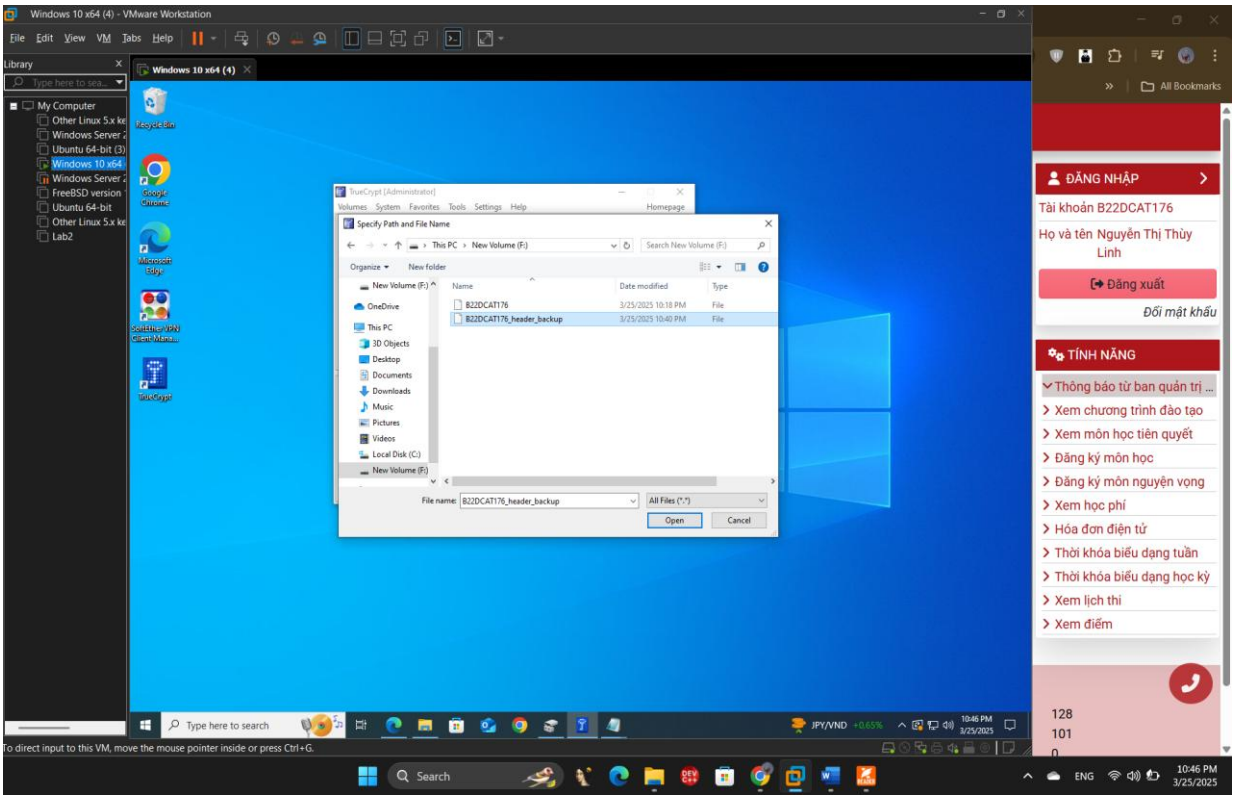
Hình ảnh 22: Chọn "Restore Volume Header".

Chọn lựa chọn thứ 2 "*Restore the volume header from an external backup file*". Sau đó chọn *Yes*.



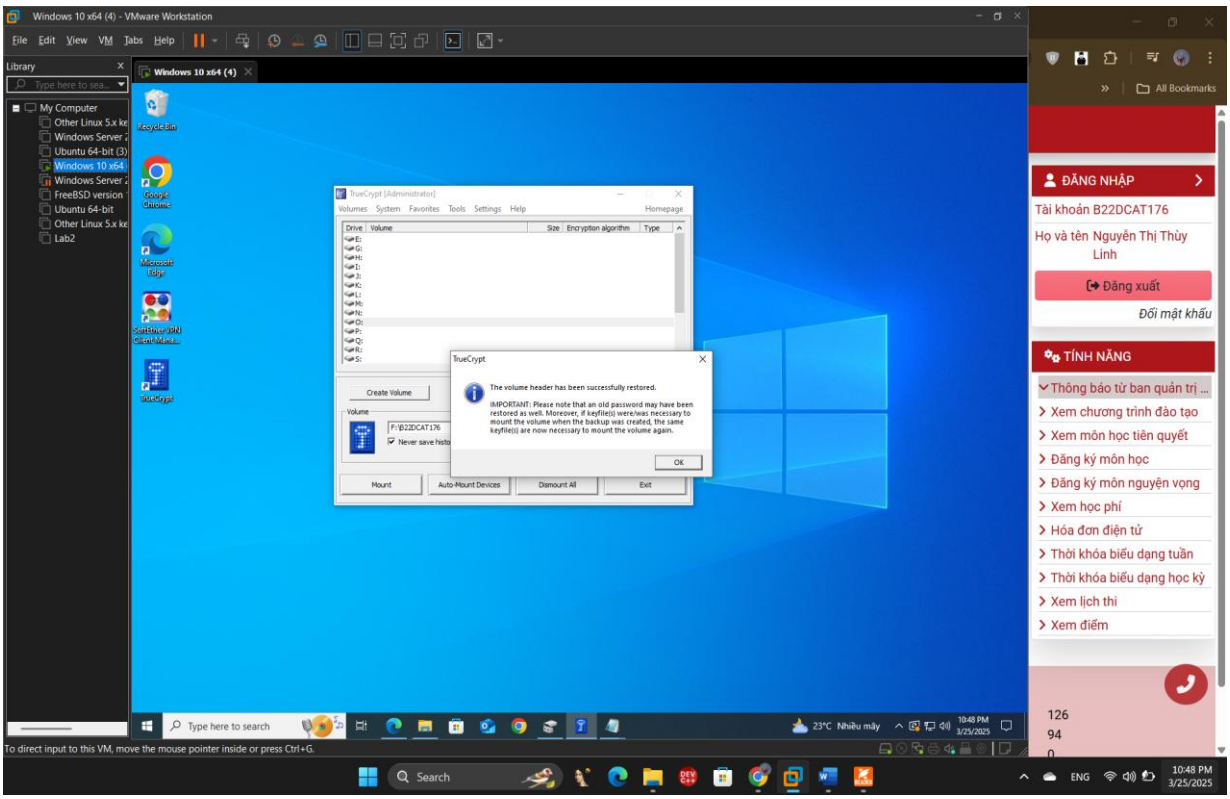
Hình ảnh 23: Chọn tùy chọn thứ 2

- Chọn file sau khi đã được backup lưu ở ổ F:



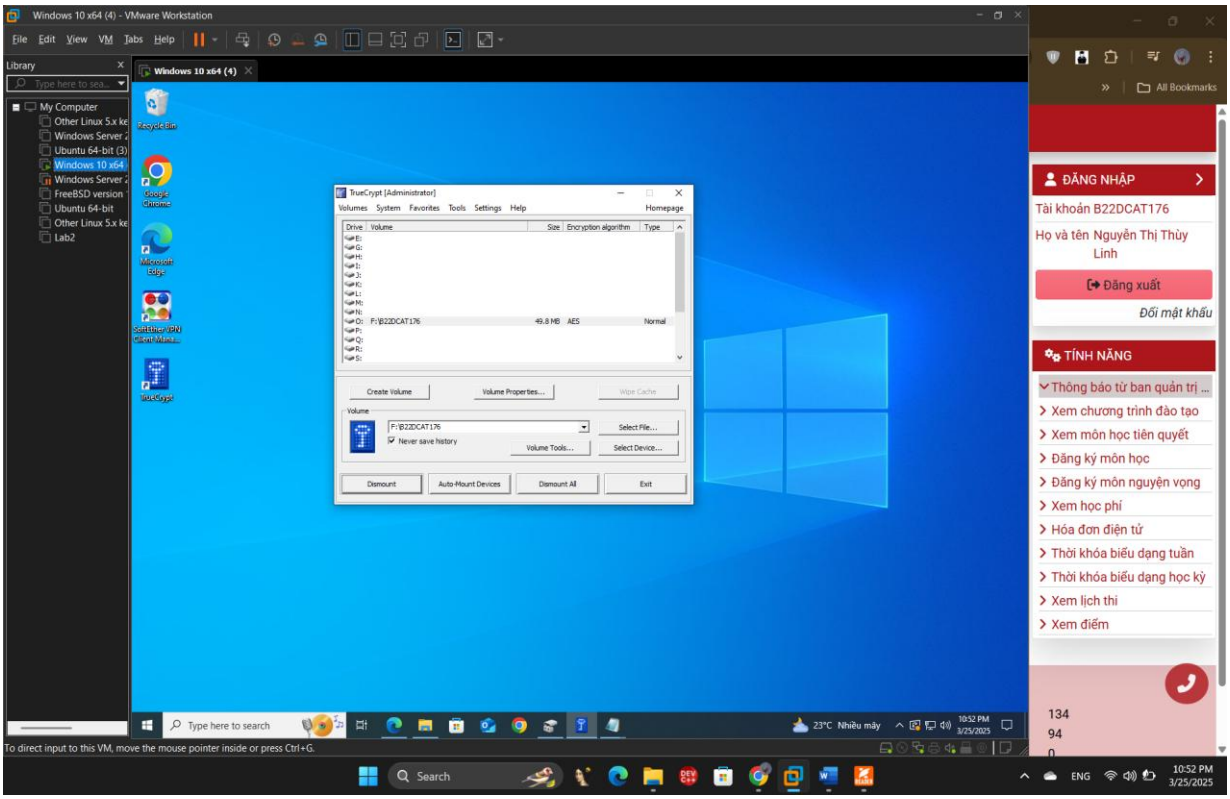
Hình ảnh 24: Chọn file sau khi đã được backup.

Thông báo *Recover* thành công.



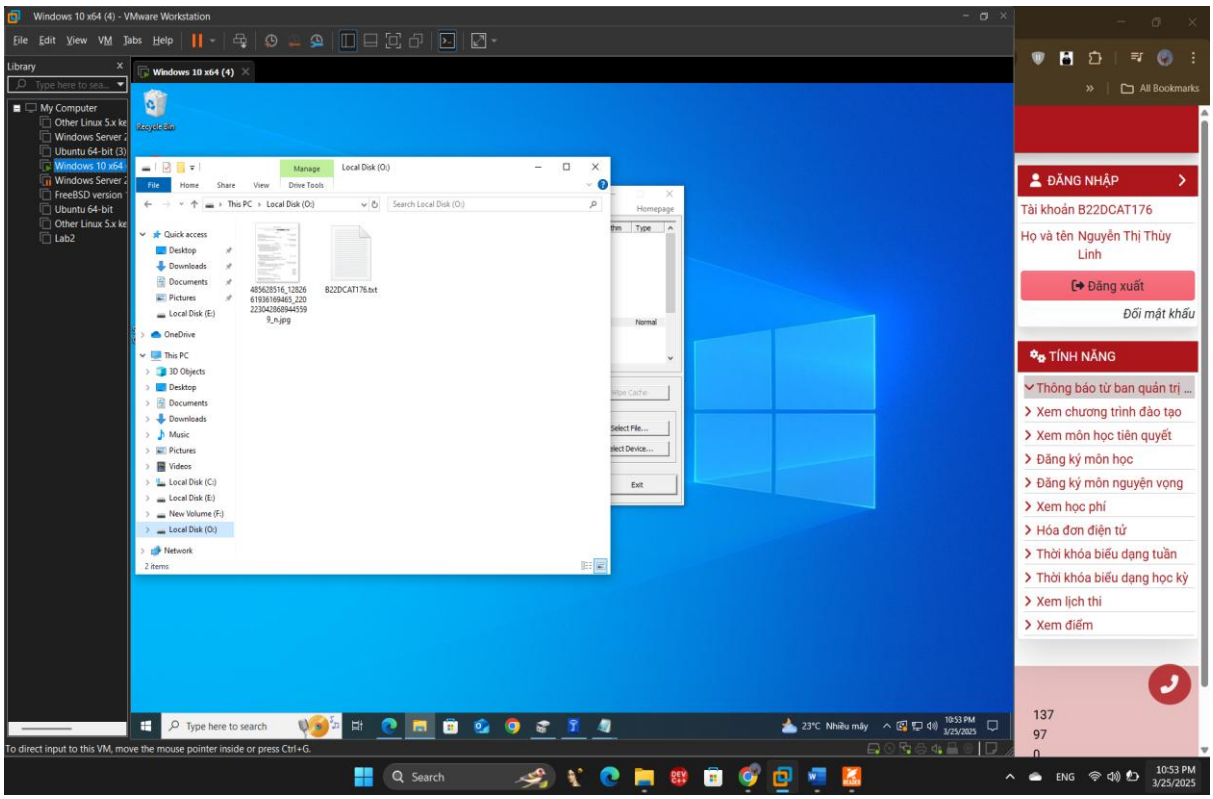
Hình ảnh 25: Restore thành công.

TrueCrypt thông báo file Restore ở thư mục O:



Hình ảnh 26: Thông báo ổ chứa file Restore.

Vào ổ O xem và đã thấy dữ liệu được Restore thành công.



Hình ảnh 27: Kiểm tra Restore thành công.

TÀI LIỆU THAM KHẢO

[1] Đinh Trường Duy, Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2022.
[2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.
[3] Giáo trình Hệ điều hành