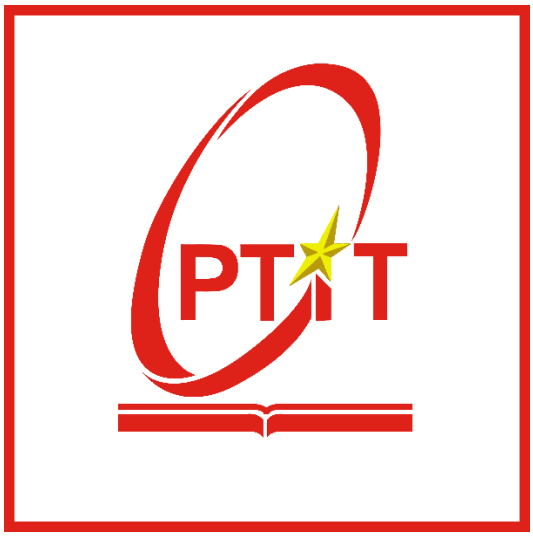
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



Môn học: **THỰC TẬP CƠ SỞ**

BÁO CÁO BÀI THỰC HÀNH SỐ 13

ĐẢM BẢO AN TOÀN VỚI MÃ HÓA

Sinh viên thực hiện: Lê Anh Tuấn

Mã sinh viên: B21DCAT205

Giảng viên: Ninh Thị Thu Trang

~ Hà Nội, tháng 5/2024 ~

Mục Lục

Bài 13: Đảm bảo an toàn với mã hóa

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 công cụ TrueCrypt

TrueCrypt là một tiện ích phần mềm miễn phí mã nguồn mở được sử dụng để mã hóa tập tin, TrueCrypt hỗ trợ nhiều hệ điều hành, bao gồm Windows, macOS và Linux, làm cho nó trở thành một công cụ đa nền tảng linh hoạt. Người dùng có thể tạo ra các ổ đĩa ảo, hay còn gọi là "container," và sau đó mã hóa chúng với các thuật toán mạnh mẽ như AES hay Serpent. Sự linh hoạt này giúp TrueCrypt trở thành một lựa chọn phổ biến cho người dùng có nhu cầu bảo vệ dữ liệu trên nhiều thiết bị và hệ điều hành. 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 giảimã 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 hóađa luồng các hệ thống đa lõi. Trên các bộ xử lý mới hơn hỗ trợ AES-NI, TrueCrypthỗ 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 thườngsử dụng truy cập bộ nhớ trực tiếp (DMA), vì Tất cả dữ liệu phải truyền qua CPUđể 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 kể từ 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.

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:

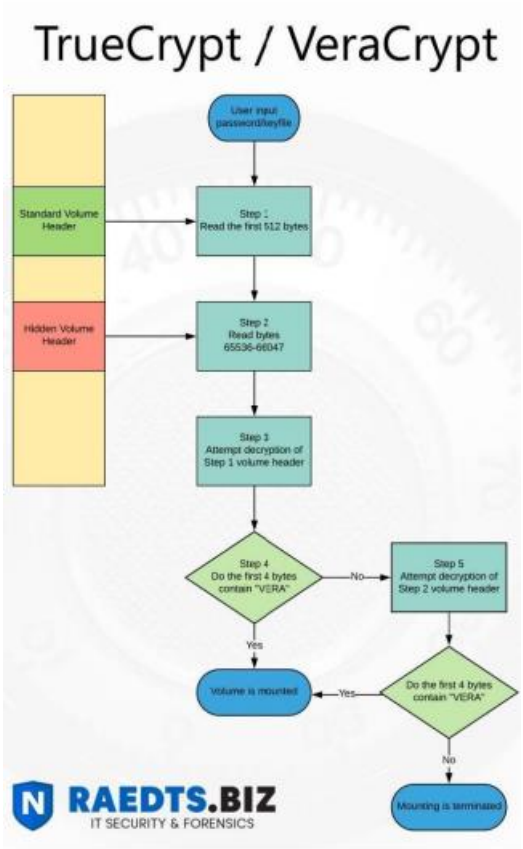
Bước 1: 512 byte đầu tiên của volume được đọc thành RAM, trong đó 64 byte đầu tiên là salt. Đối với mã hóa hệ thống, 512 byte cuối cùng của rãnh ổ đĩa logic đầu tiên được đọc vào RAM.

Bước 2: Các byte 65536->66047 của volume được đọc thành RAM. Đối với mã hóa hệ thống, byte 65536->66047 của phân vùng đầu tiên nằm phía sau phân vùng hoạt động được 1 đọc.

Bước 3: TrueCrypt cố gắng giải mã tiêu đề tiêu chuẩn của volume trong Bước 1. Tất cả dữ liệu được sử dụng và tạo trong quá trình giải mã được giữ trong RAM. Do volume không chứa bất kỳ thông tin nào về các tham số đã sử dụng khi volume được tạo, các tham số phải được xác định thông qua quá trình thử nghiệmvà sửa lỗi.

Bước 4: Nhập mật khẩu Mật khẩu được nhập bởi người dùng và salt được đọc trong bước 1 được chuyển đến hàm dẫn xuất khóa tiêu đề, tạo ra một chuỗi các giá trị mà từ đó khóa mã hóa tiêu đề và khóa tiêu đề thứ cấp (chế độ XTS) được hình thành. Các khóa này được sử dụng để giải mã tiêu đề volume.

Bước 5: Giải mã, TrueCrypt giải mã theo sơ đồ sau:



Hình 1: Sơ đồ giải mã TrueCrypt

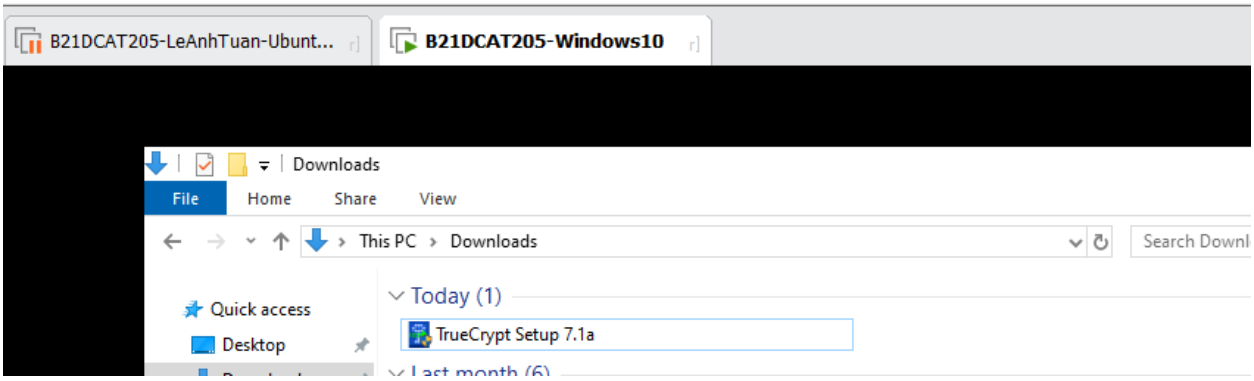
Mặc dù TrueCrypt từng là công cụ phổ biến, nhưng vào năm 2014, nhóm phát triển bất ngờ tuyên bố ngừng phát triển và khuyến cáo người dùng chuyển sang các giải pháp thay thế. Sự kiện này đã tạo ra nhiều tranh cãi và tin đồn, với nhiều người chỉ trích quyết định này và đặt ra nhiều câu hỏi về an ninh và quản lý dự án mã nguồn mở.

Trong những năm sau đó, nhiều dự án phát triển tiếp theo TrueCrypt đã xuất hiện, như VeraCrypt, có nhiệm vụ duy trì và phát triển các tính năng mà TrueCrypt đã để lại. VeraCrypt đã giữ lại nhiều ưu điểm của TrueCrypt và cải tiến với những tính năng mới, đồng thời duy trì cam kết về mã nguồn mở và an toàn.

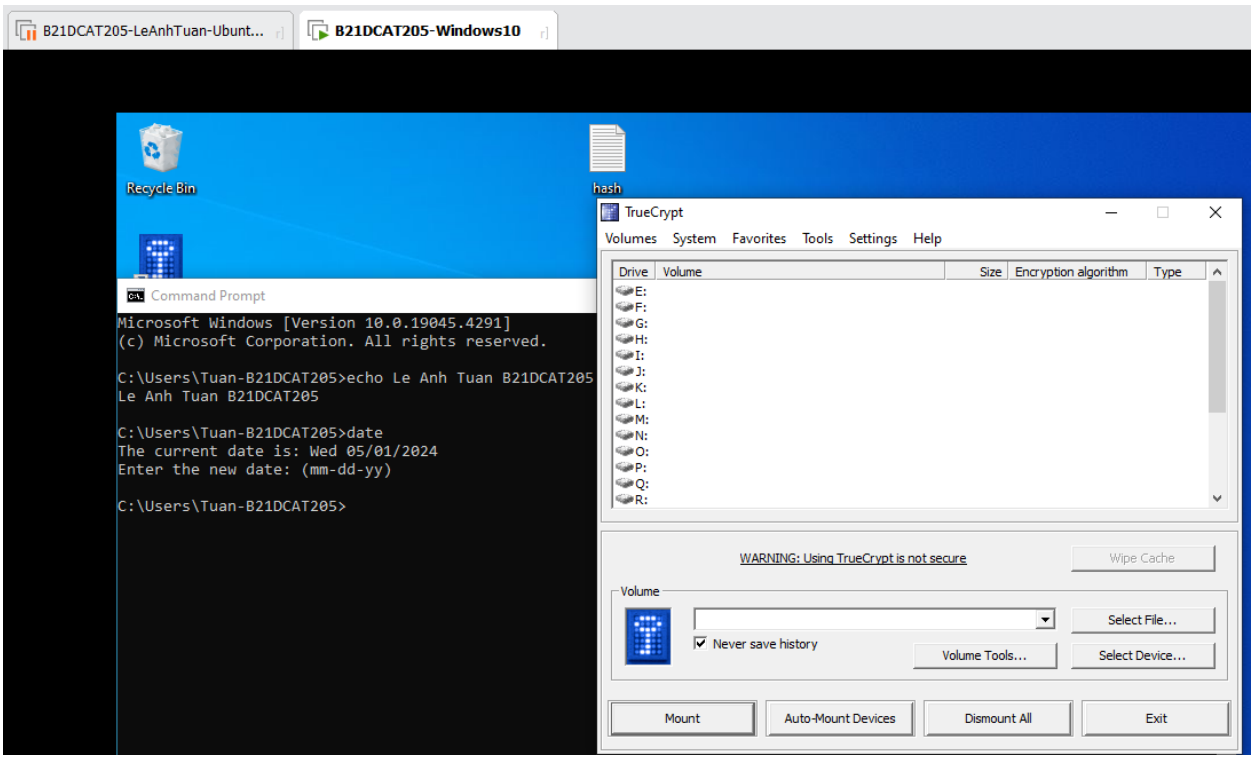
2.2 Nội dung thực hành.

2.2.1 Chuẩn bị môi trường

Khuyến nghị cài đặt phiên bản 7.1a để không bị lỗi



Hình 2: Cài đặt phiên bản 7.1a của TrueCrypt

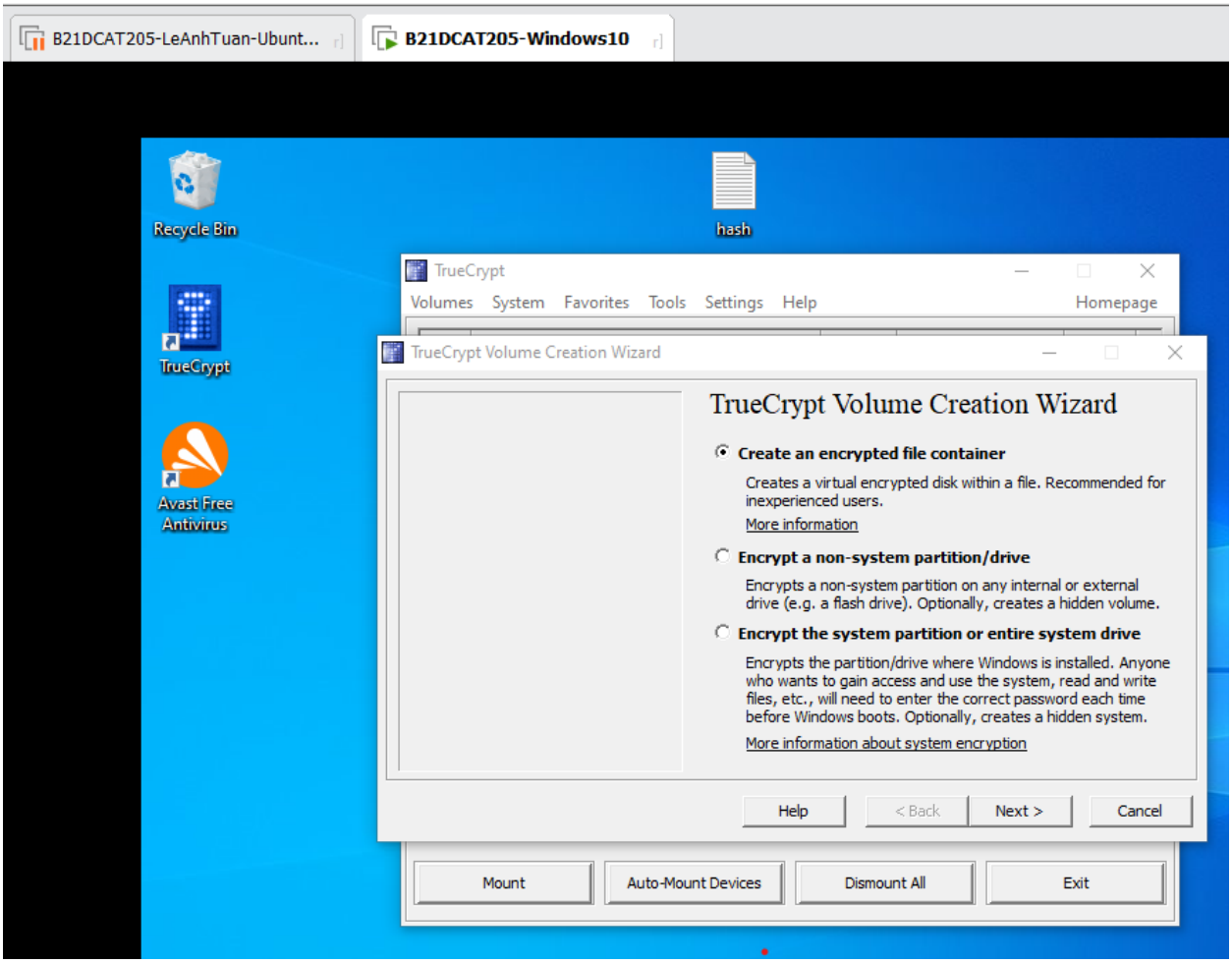


Hình 3: Giao diện TrueCrypt sau khi cài đặt thành công

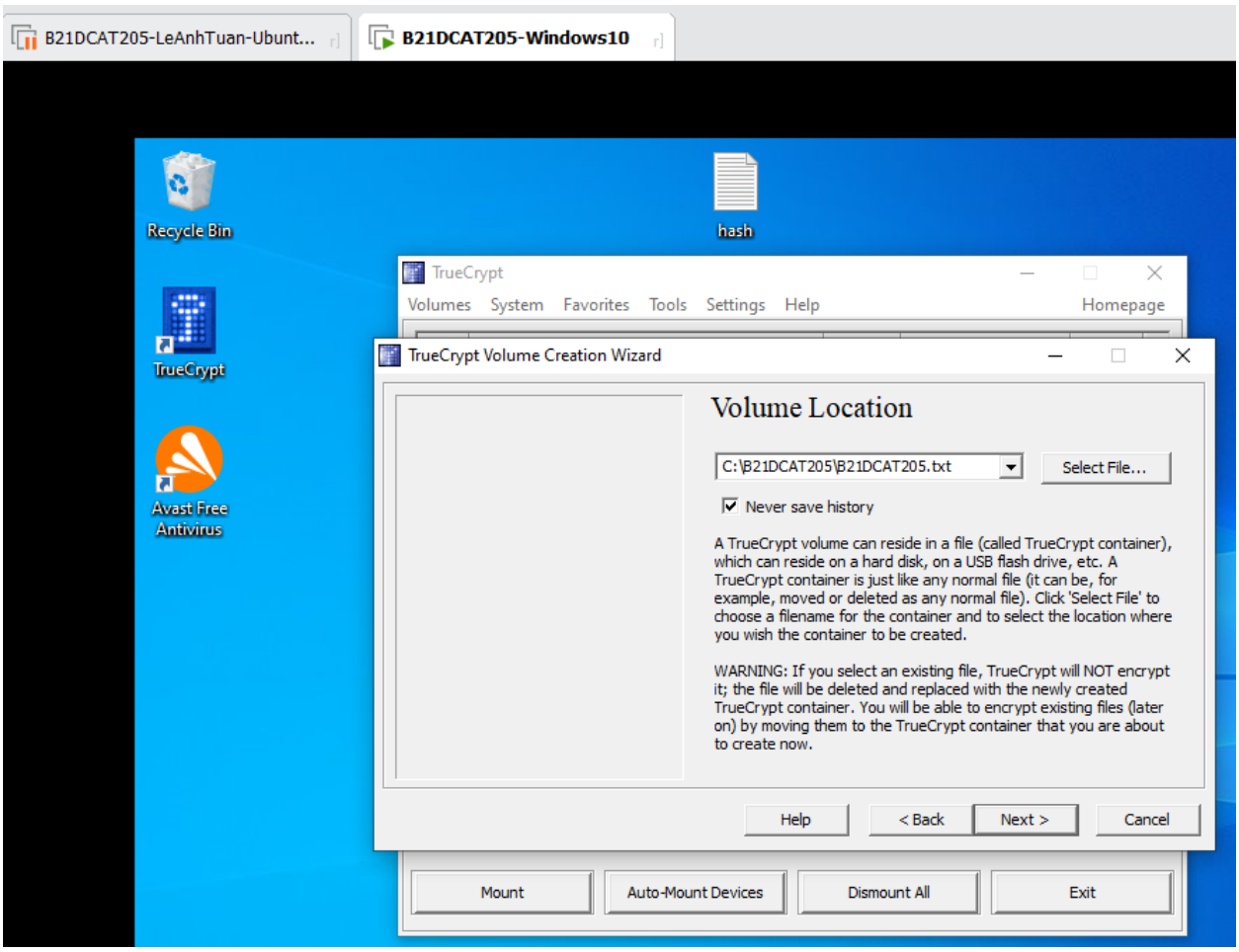
2.2.2 Thực hành

2.2.2.1 Khởi chạy và cấu hình TrueCrypt

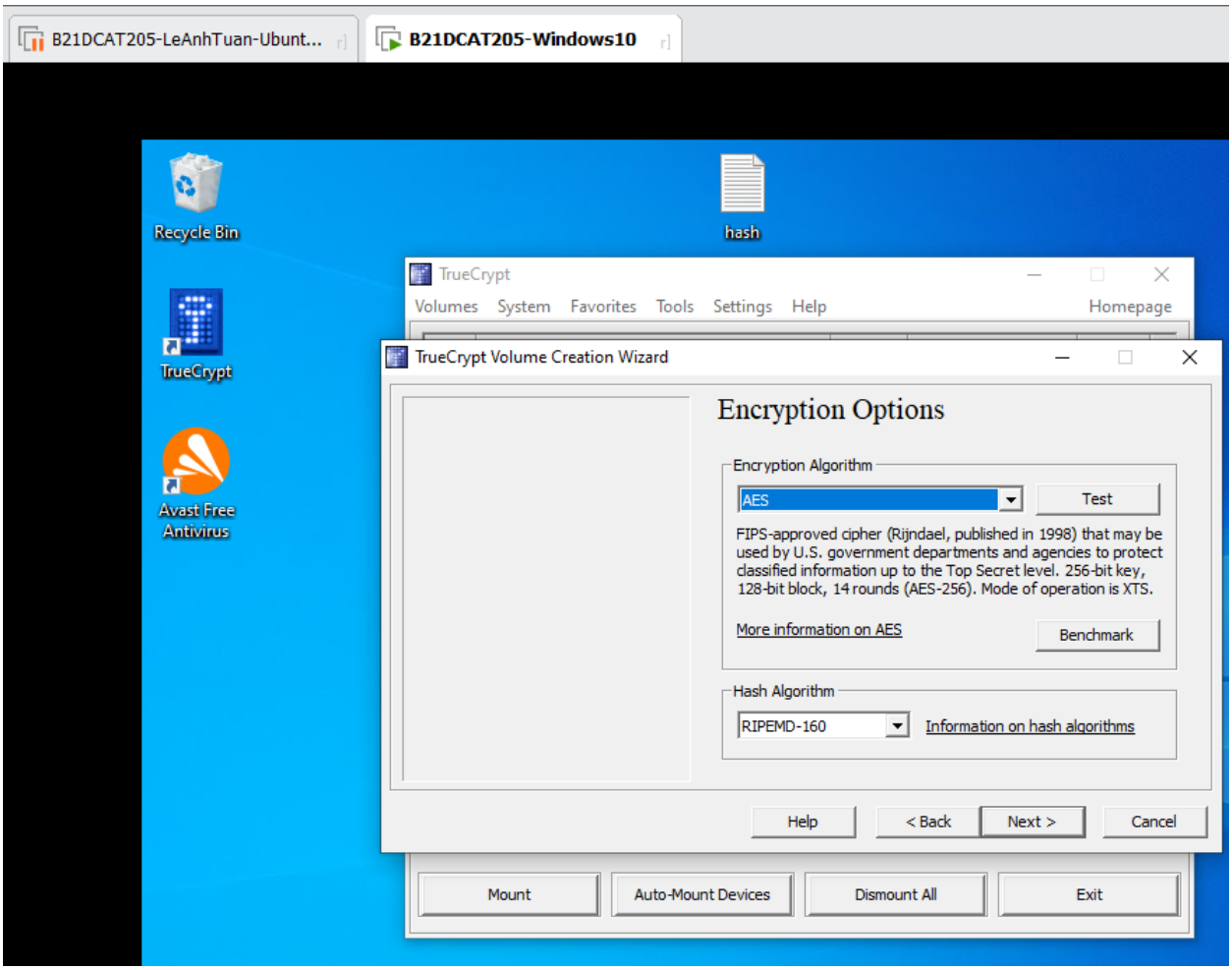
Tạo vùng khóa chuẩn:



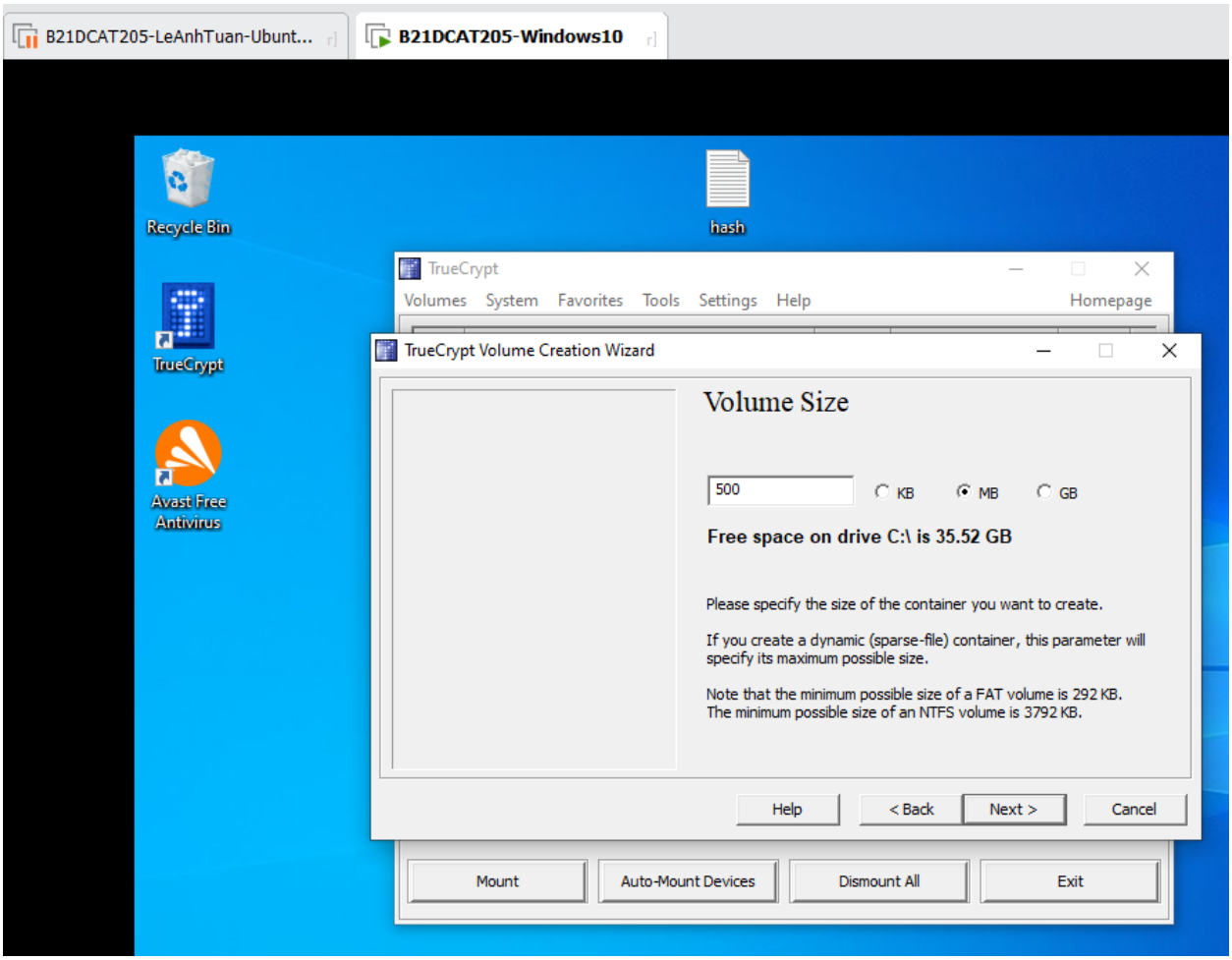
Hình 4: Bấm Create Volume và chọn next



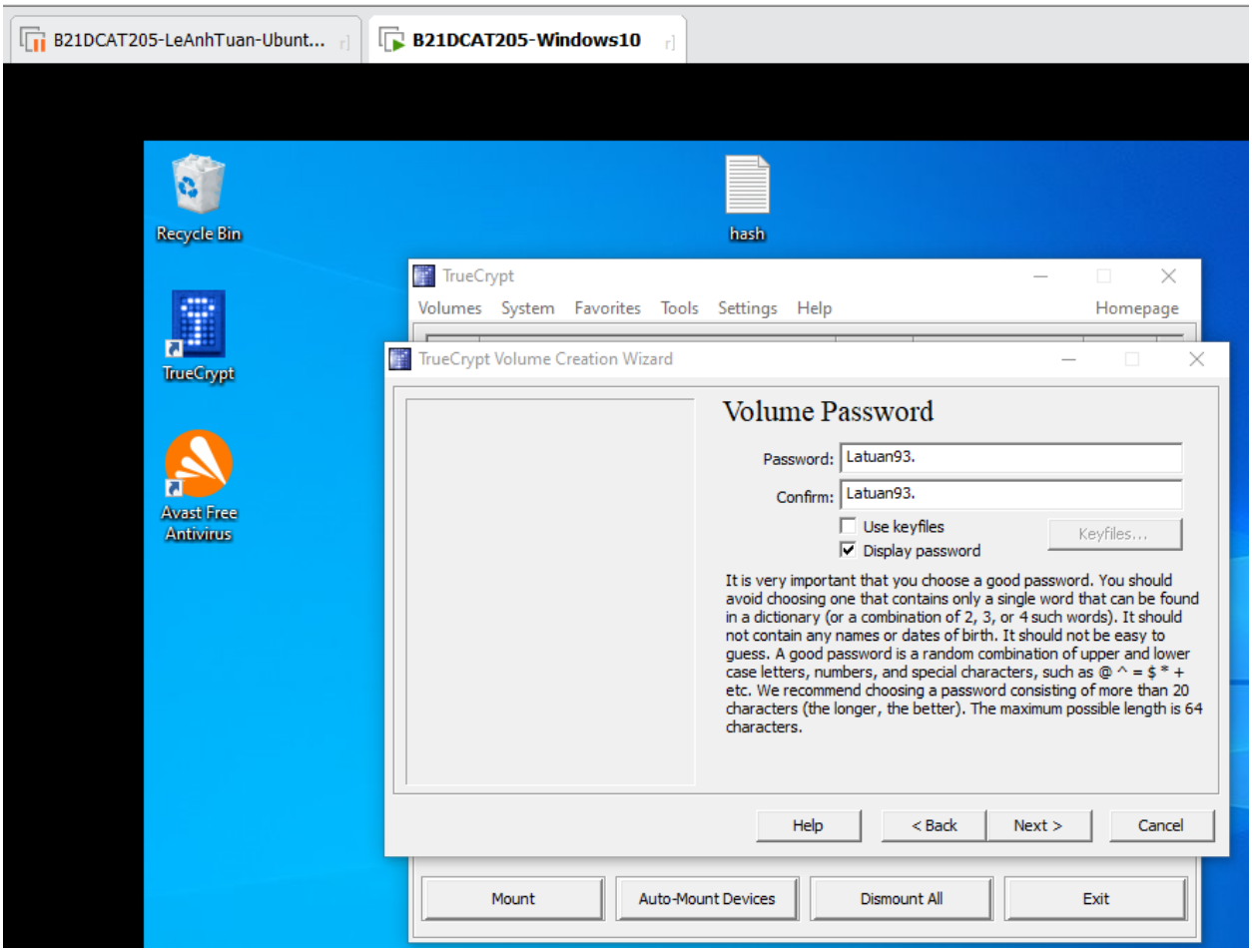
Hình 5:Select file và Chọn next



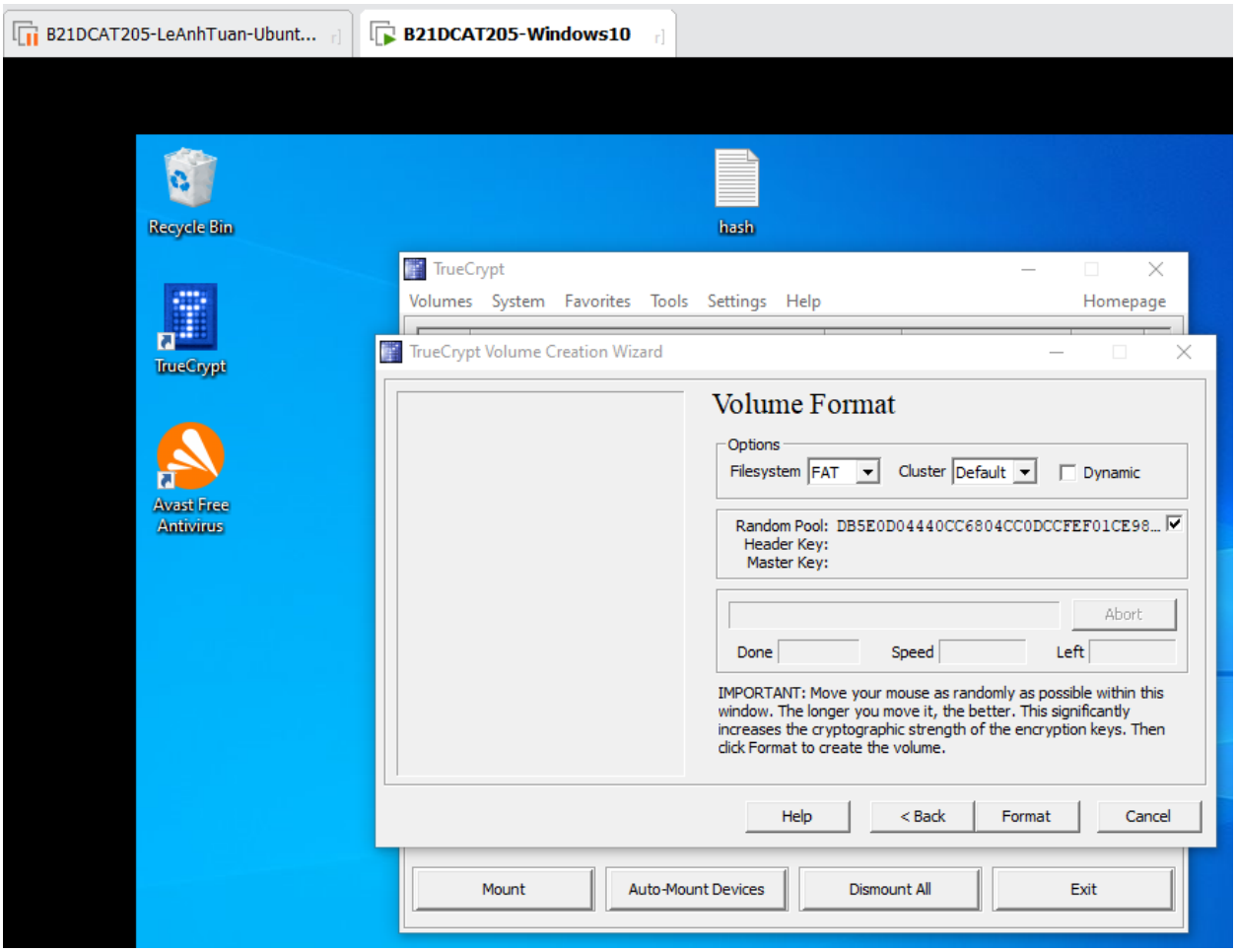
Hình 6: Chọn thuật toán mã hóa AES và hàm băm RIPEMD-160



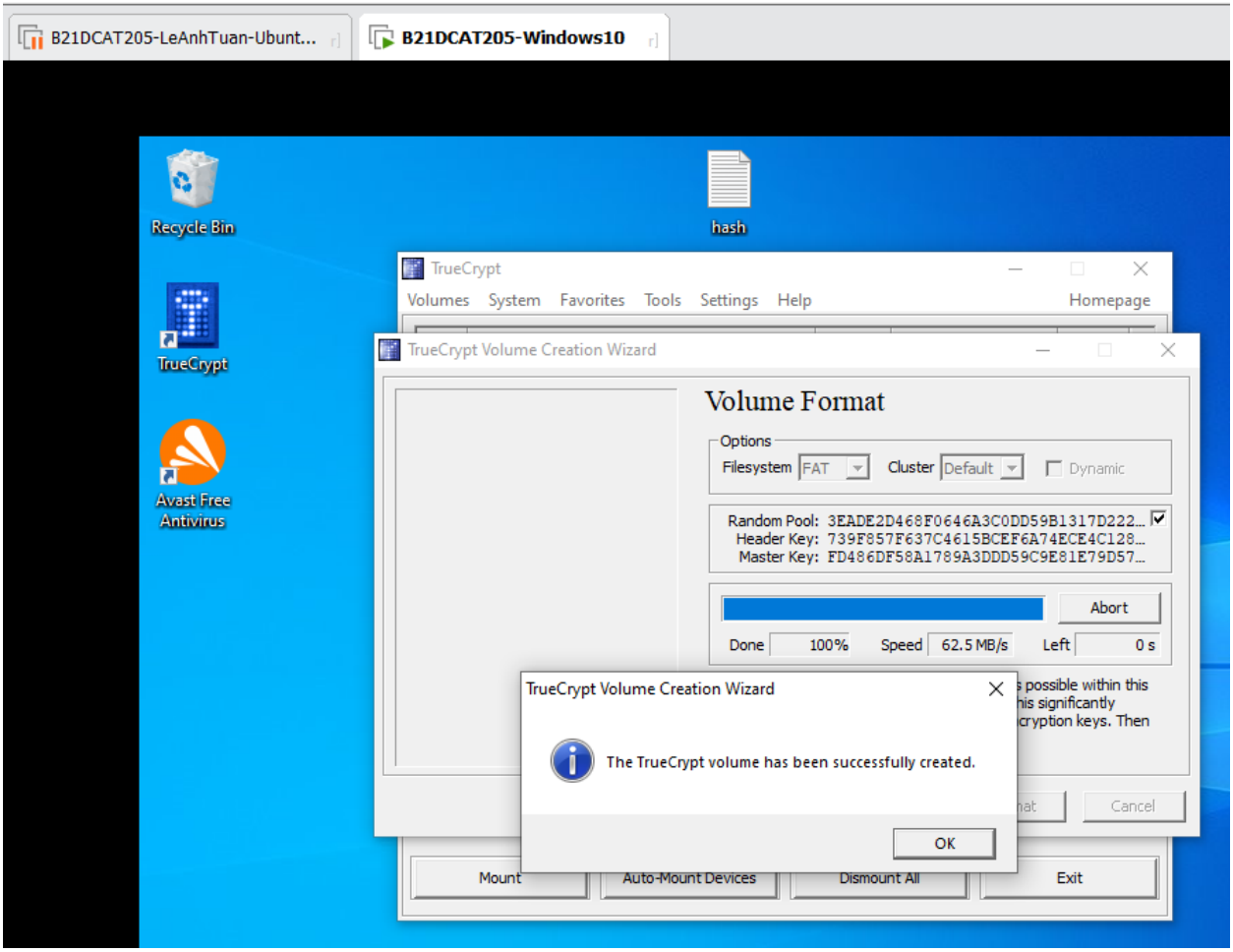
Hình 7: Điều chỉnh kích thước tối đa cho ổ đĩa



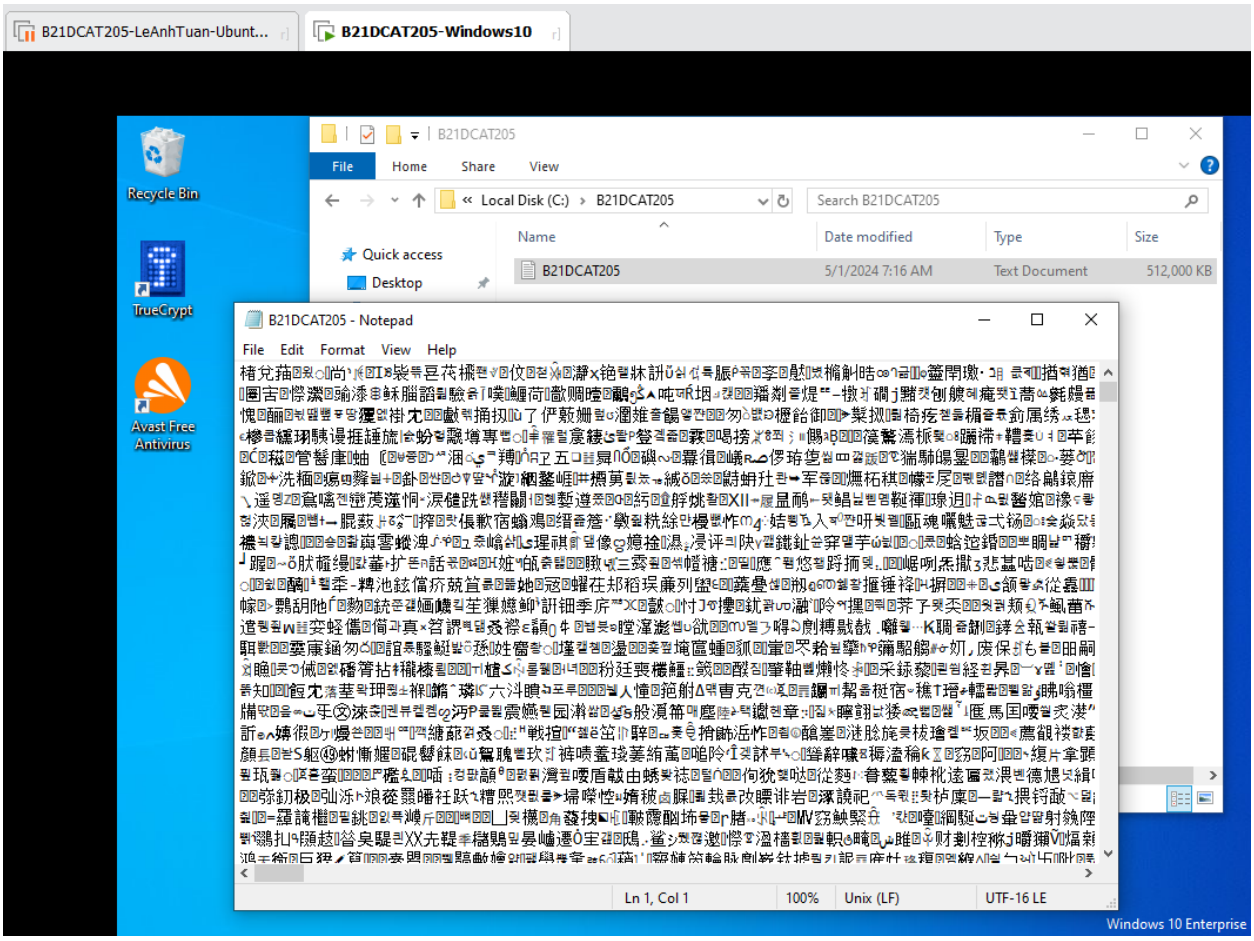
Hình 8: Cài đặt mật khẩu



Hình 9: Chọn format để tạo ổ đĩa

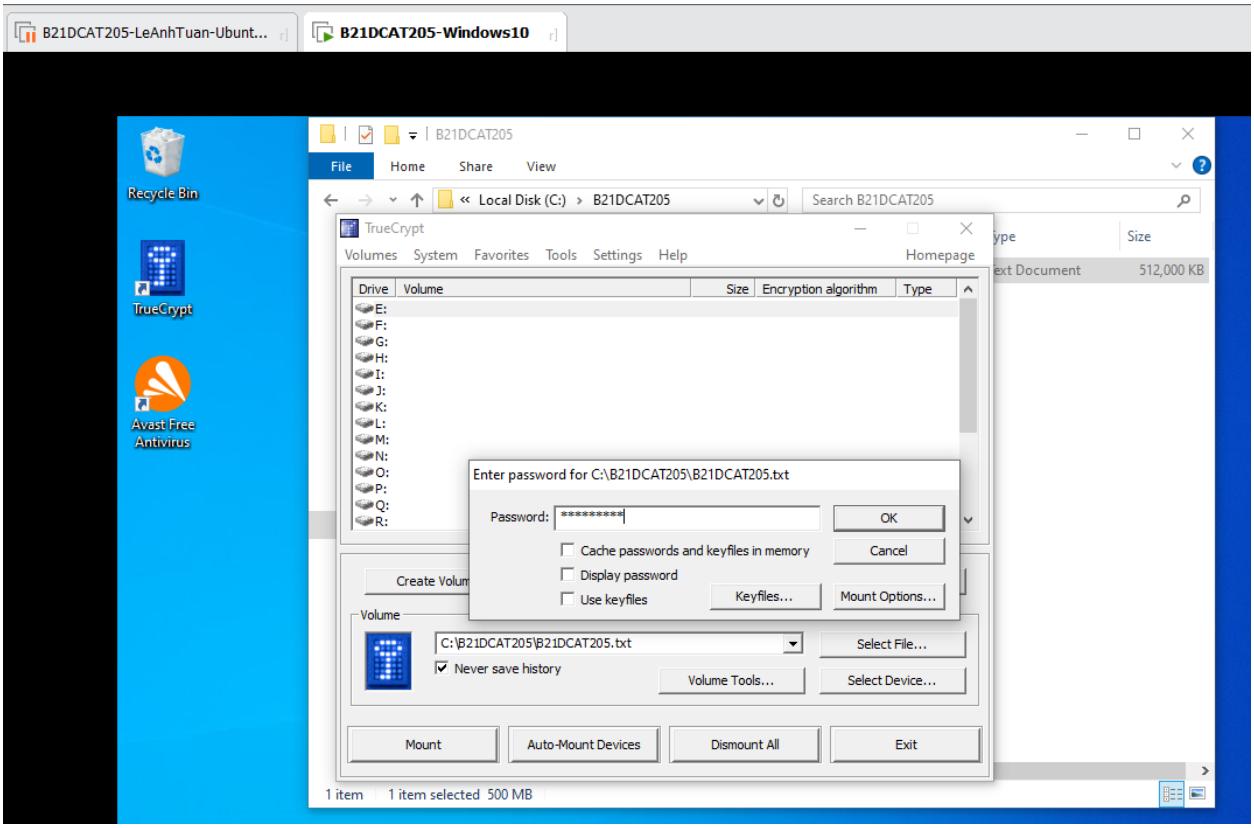


Hình 10: Ổ đĩa TrueCrypt được tạo thành công

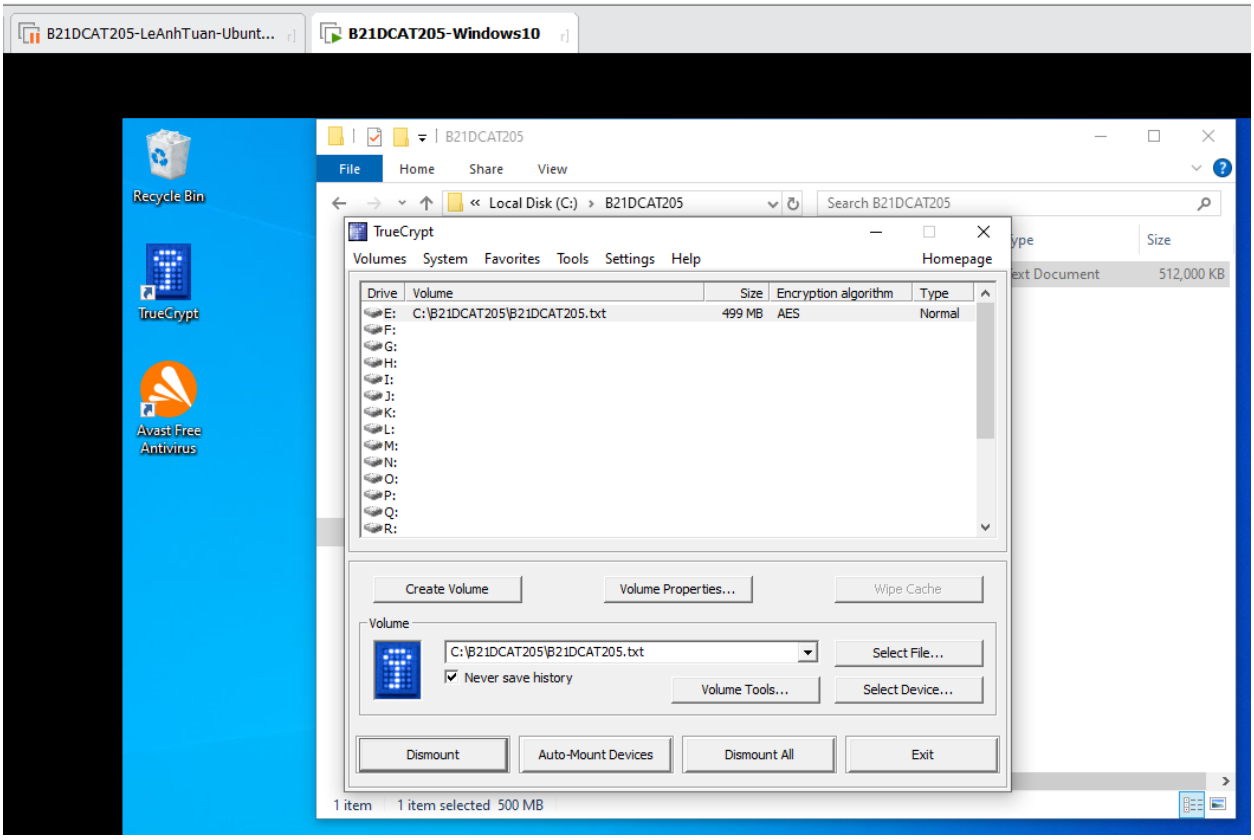


Hình 11: Mã hóa thông tin đối với ổ đĩa TrueCrypt

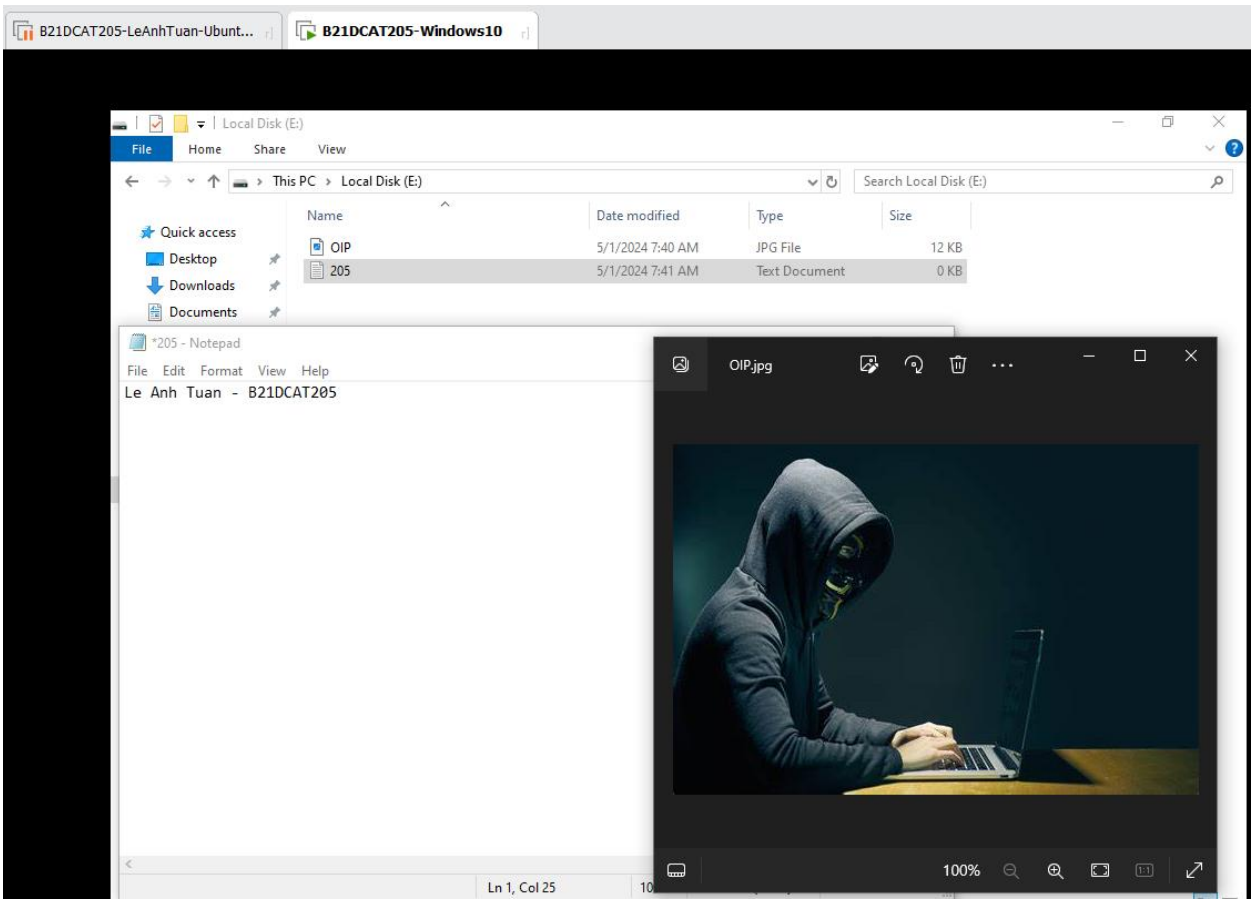
2.2.2.2 Gắn vùng mã hóa chuẩn



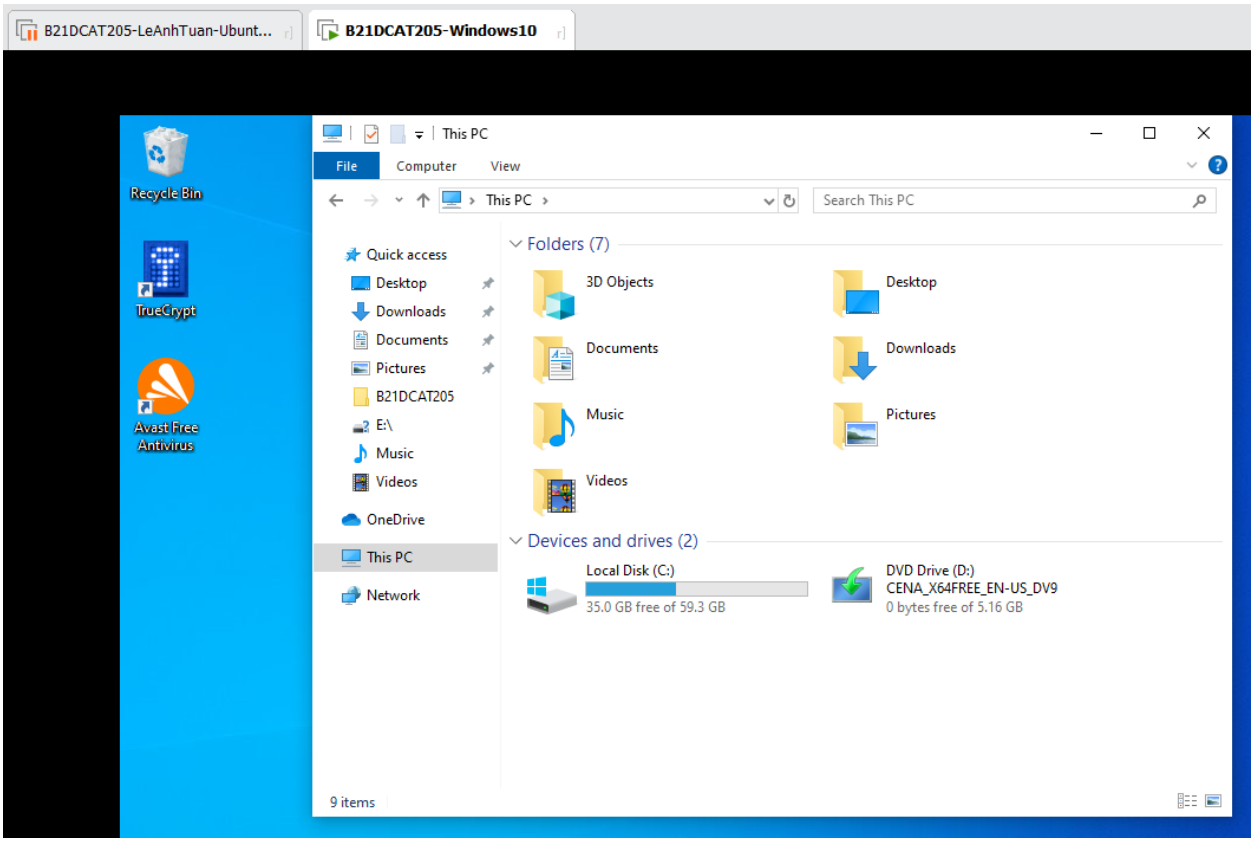
Hình 12: Chọn 1 ổ đĩa và nhập mật khẩu đã tạo



Hình 13: Mở vùng mã hóa thành công



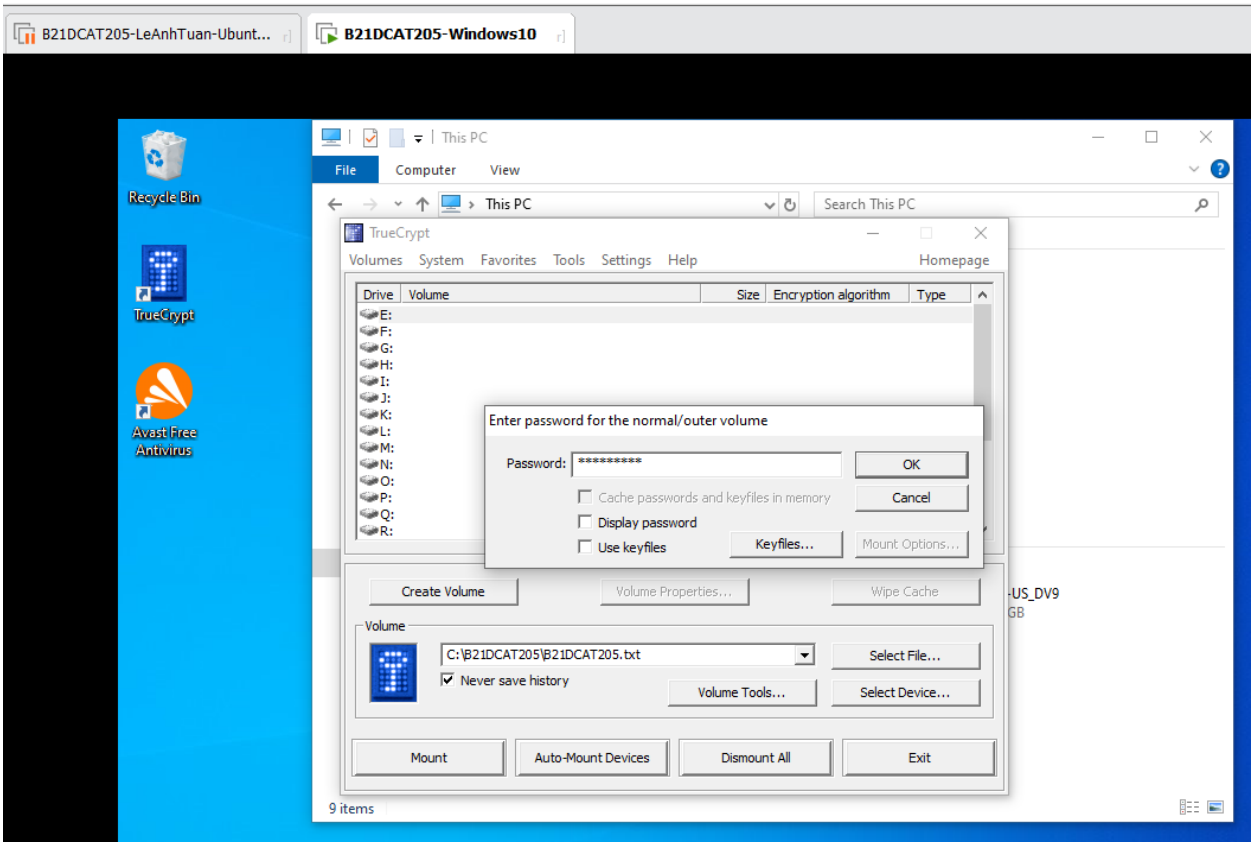
Hình 14: Di chuyển 2 file và tập tin cần mã hóa vào trong ổ E



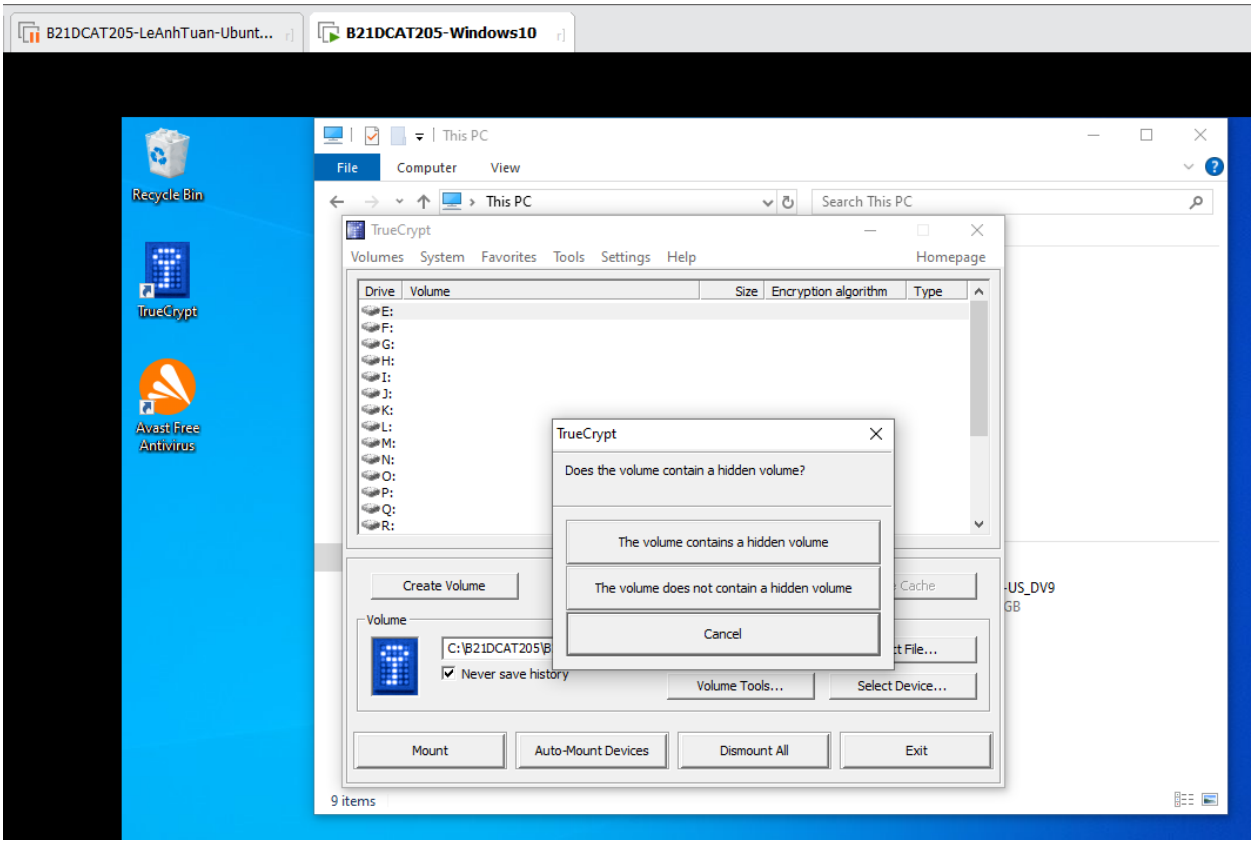
Hình 15: Chọn dismount, vùng mã hóa đóng lại ta thấy không còn ổ E

2.2.2.3 Sao lưu khóa

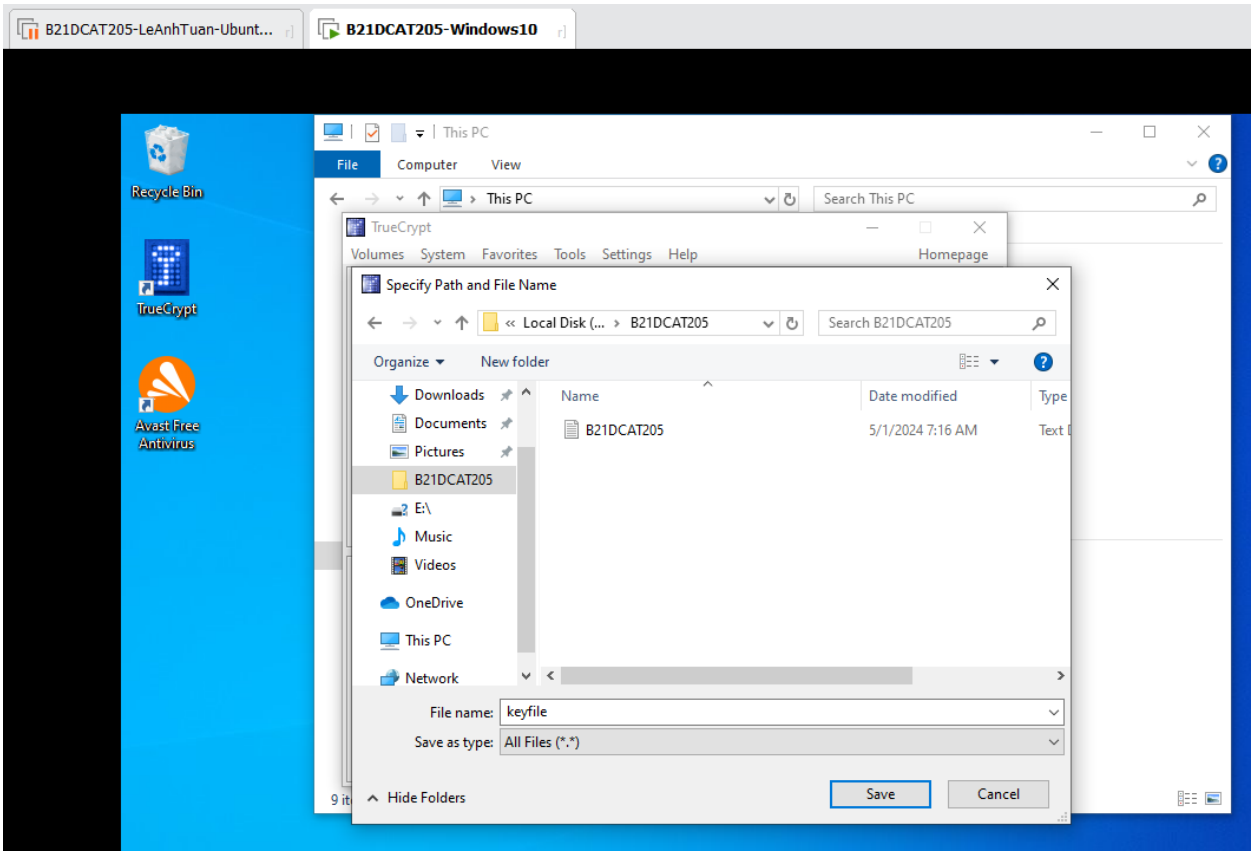
Nhấn select file chọn file để sao lưu và nhấn vào Volume tools chọn backup volume header



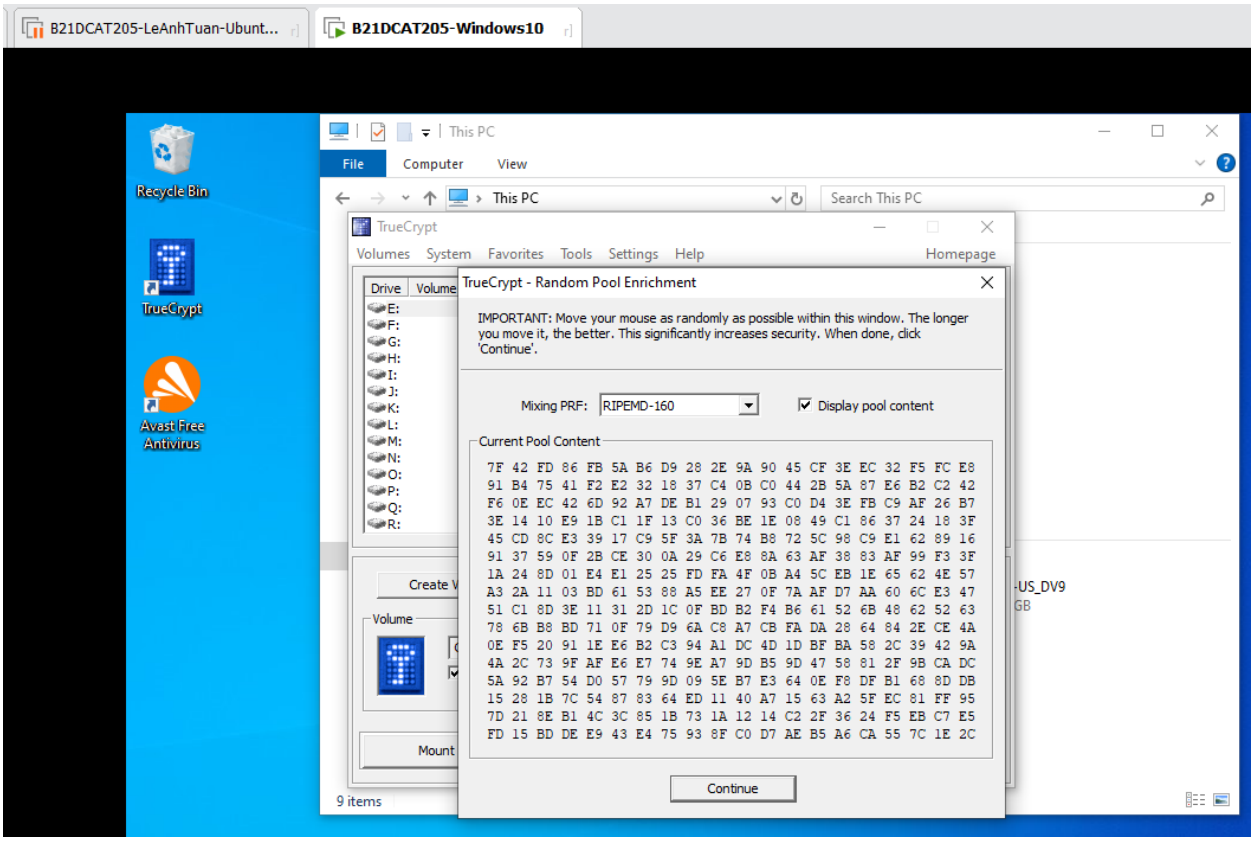
Hình 16: Chọn backup volume header và nhập mật khẩu



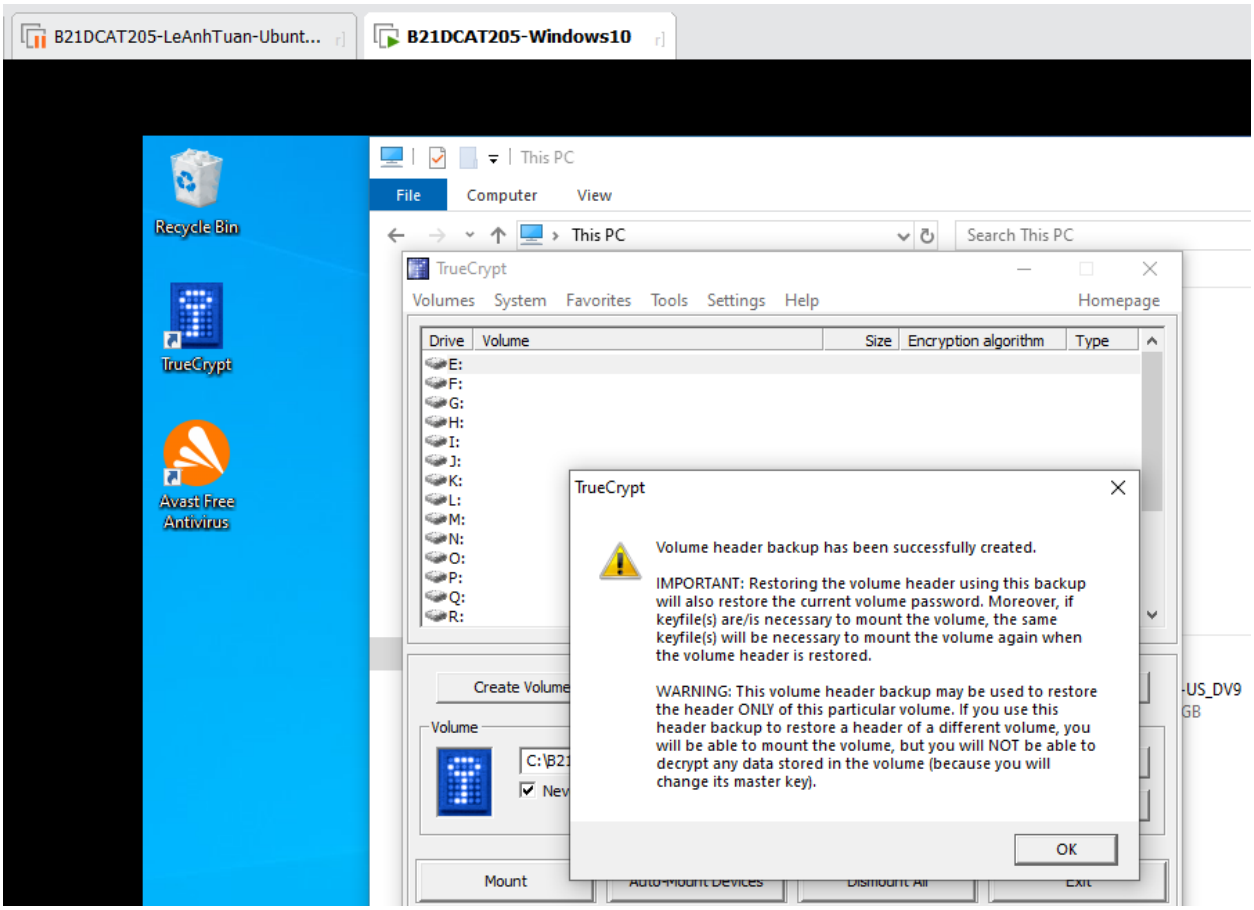
Hình 17: The volume does not contain a hidden volume



Hình 18: Đặt tên file lưu khóa và keyfile và lưu.

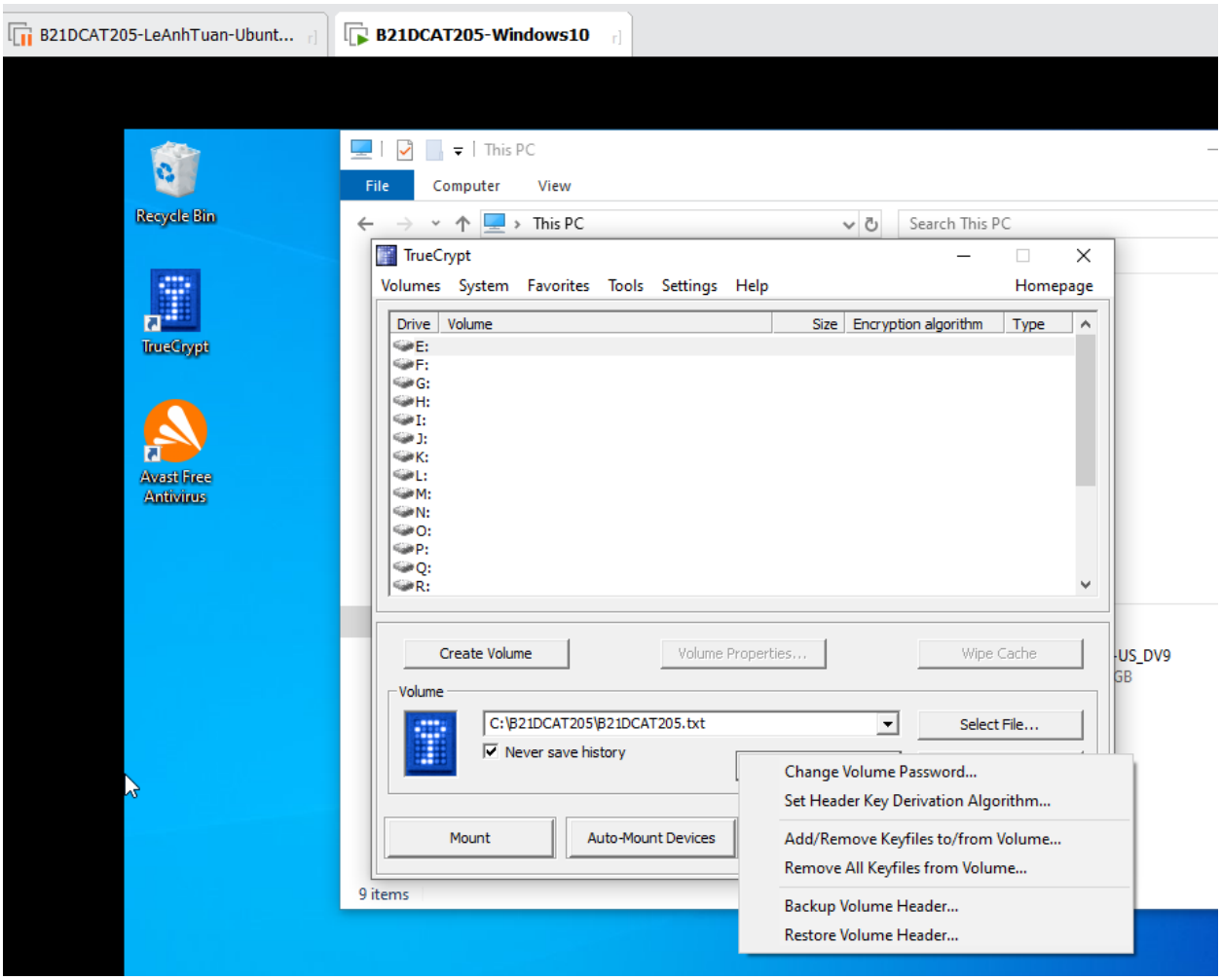


Hình 19: Mã băm RIPEMD-160 sử dụng cho keyfile



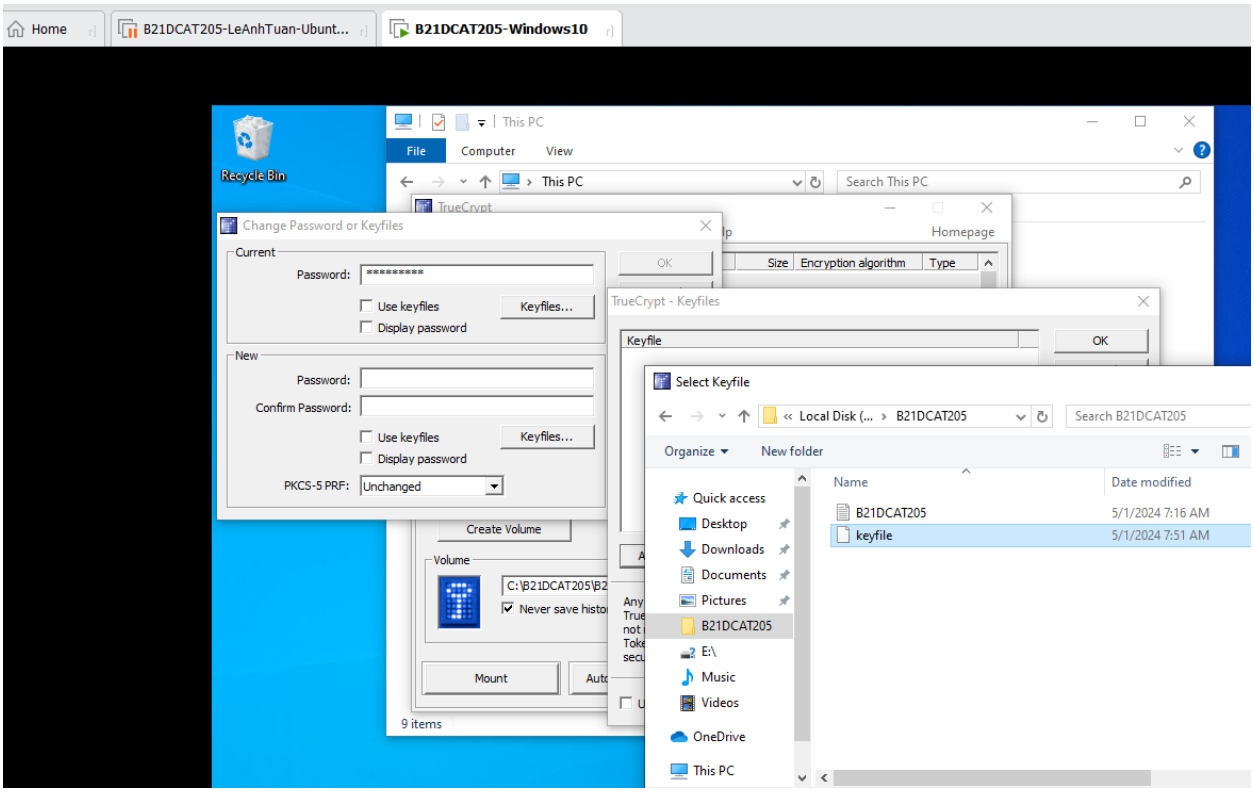
Hình 20: Volume header backup được tạo thành công

Tiếp đó, ta phải add keyfile này vào thư mục muốn mã hoá, để keyfile này hoạt động như một mật khẩu (trong Trường hợp ta quên mật khẩu chính)

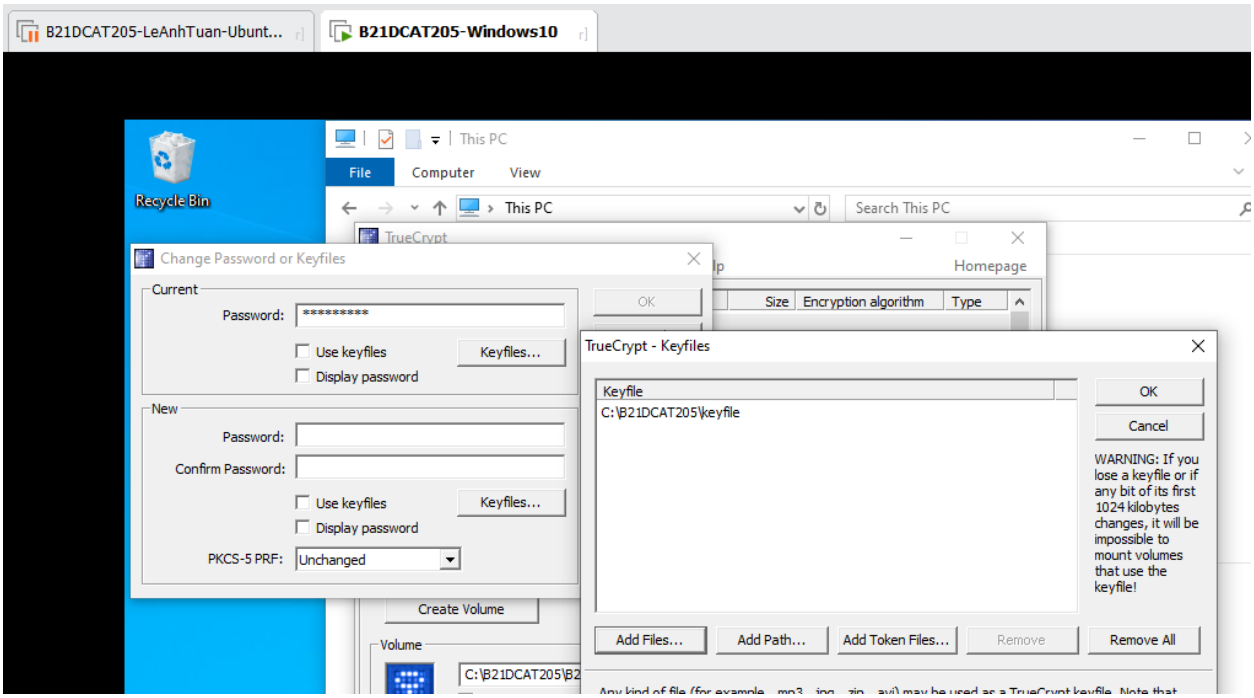


Hình 21: Chọn Change Volume Password

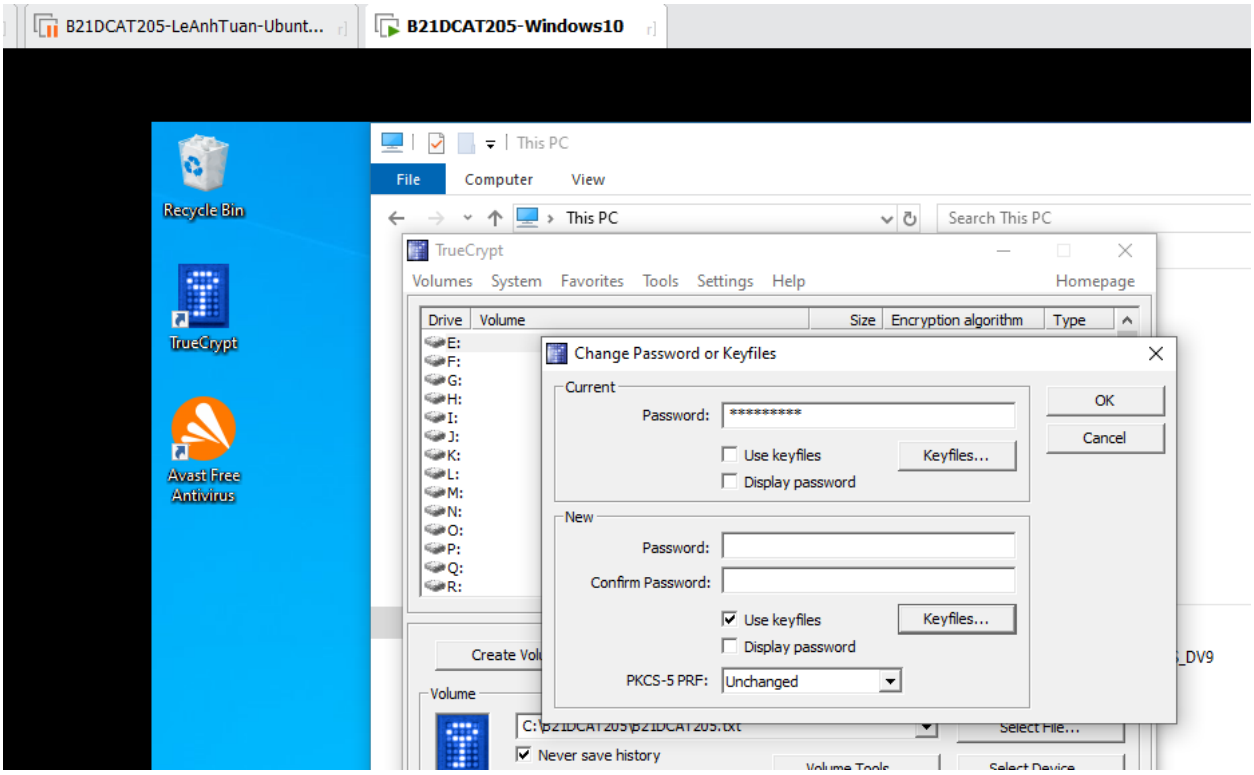
Chọn ô **Use keyfile** ở mục **New** -> click **Keyfile...** -> **Add Files Add keyfile** đã tạo ở bước trên



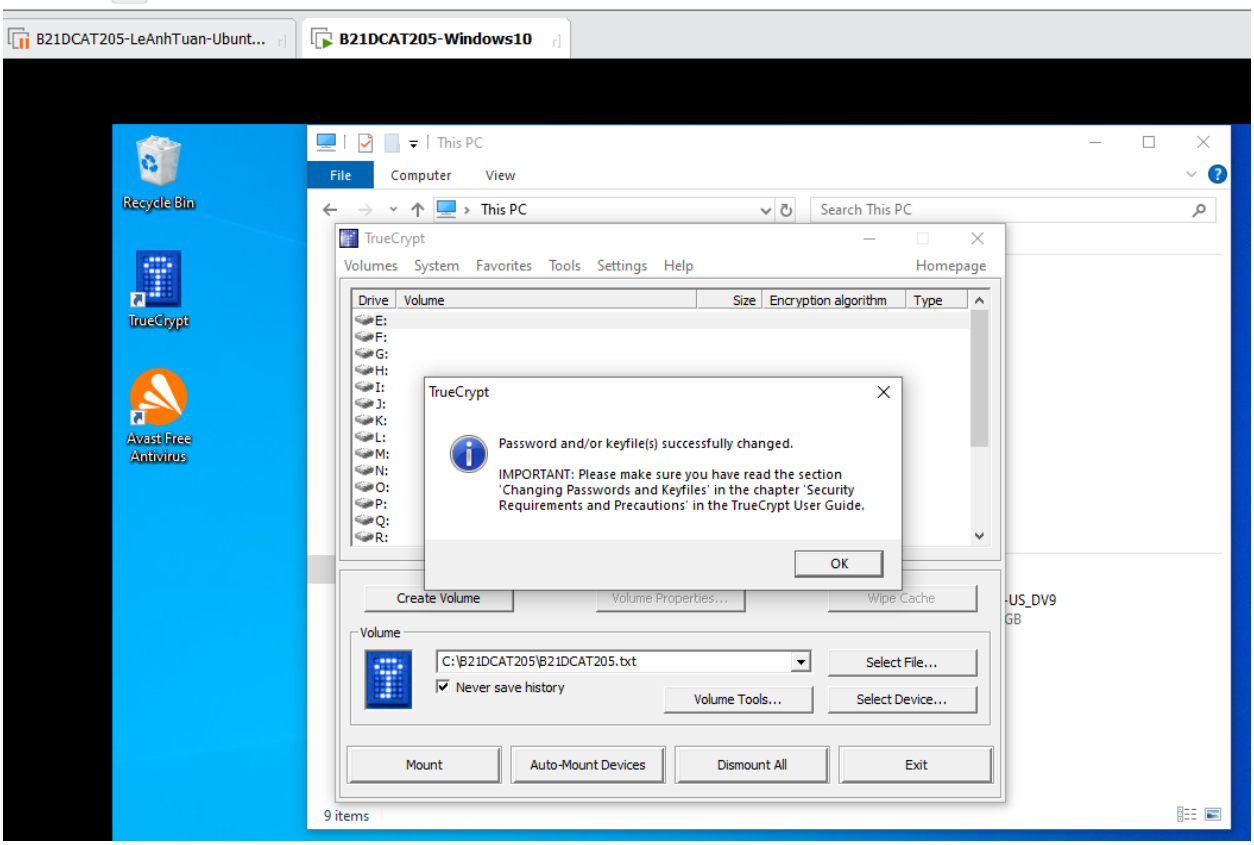
Hình 22: Chọn keyfile đã tạo



Hình 23: Ấn ok

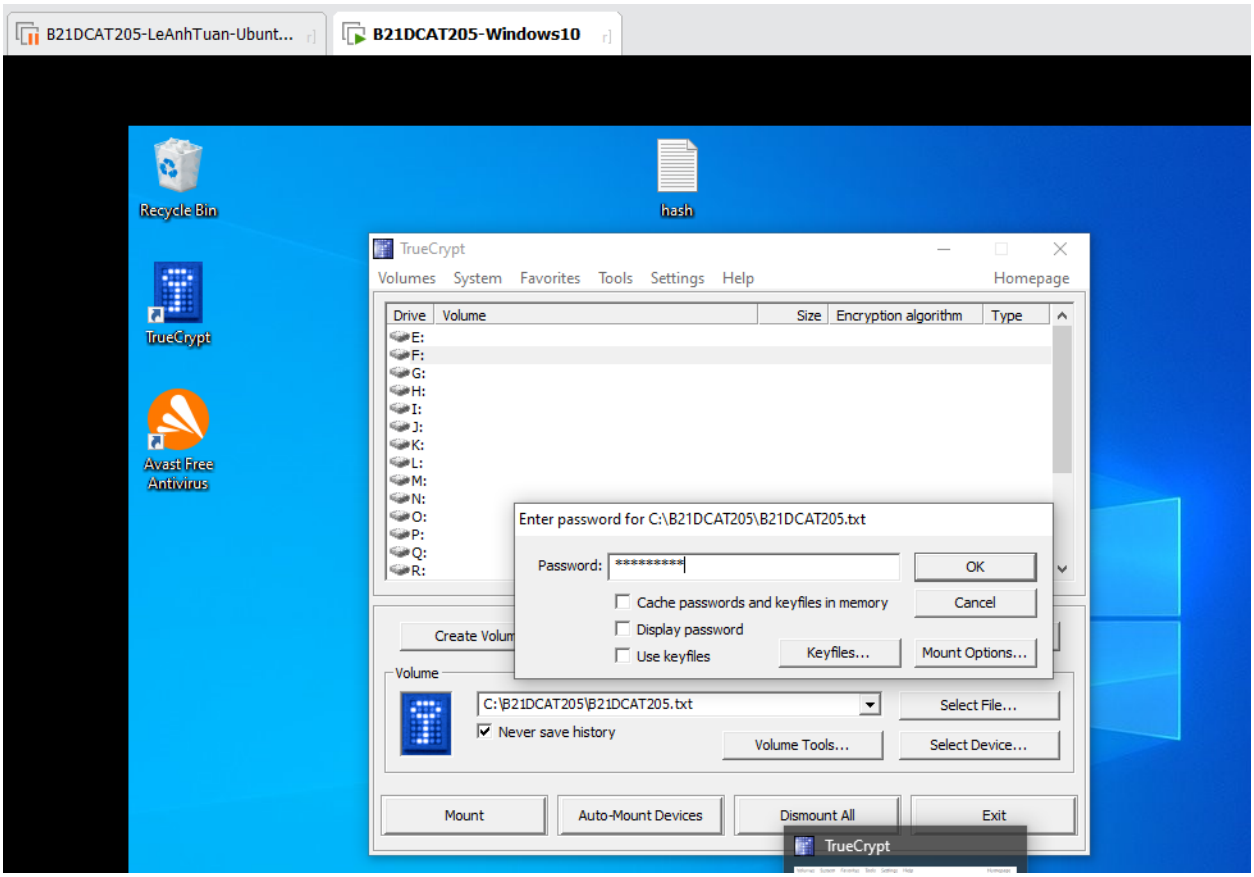


Hình 24: Ấn ok



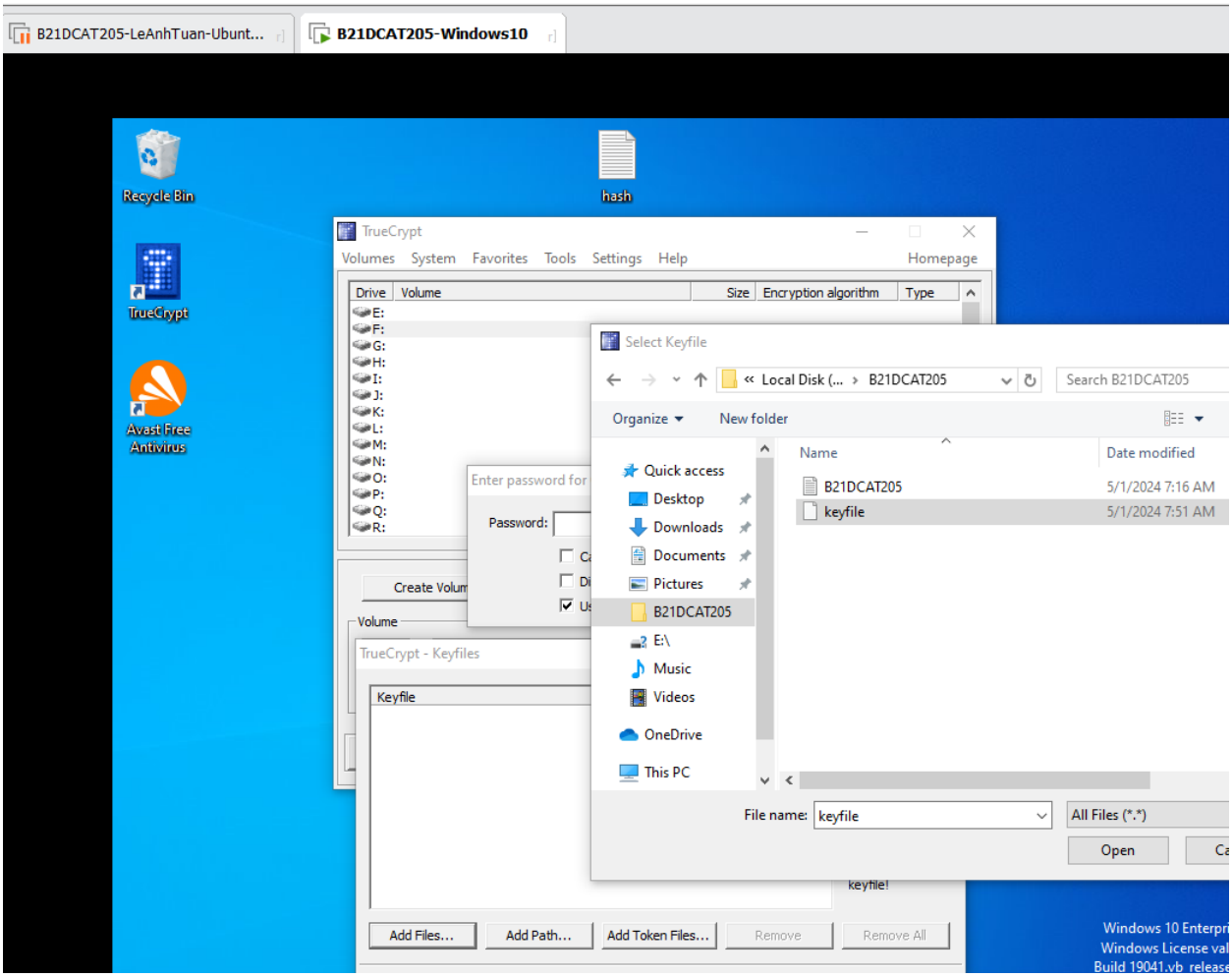
Hình 25: Sao lưu khóa vào keyfile thành công

2.2.2.4 Sử dụng TrueCrypt để khôi phục các file và thư mục đã mã hóa

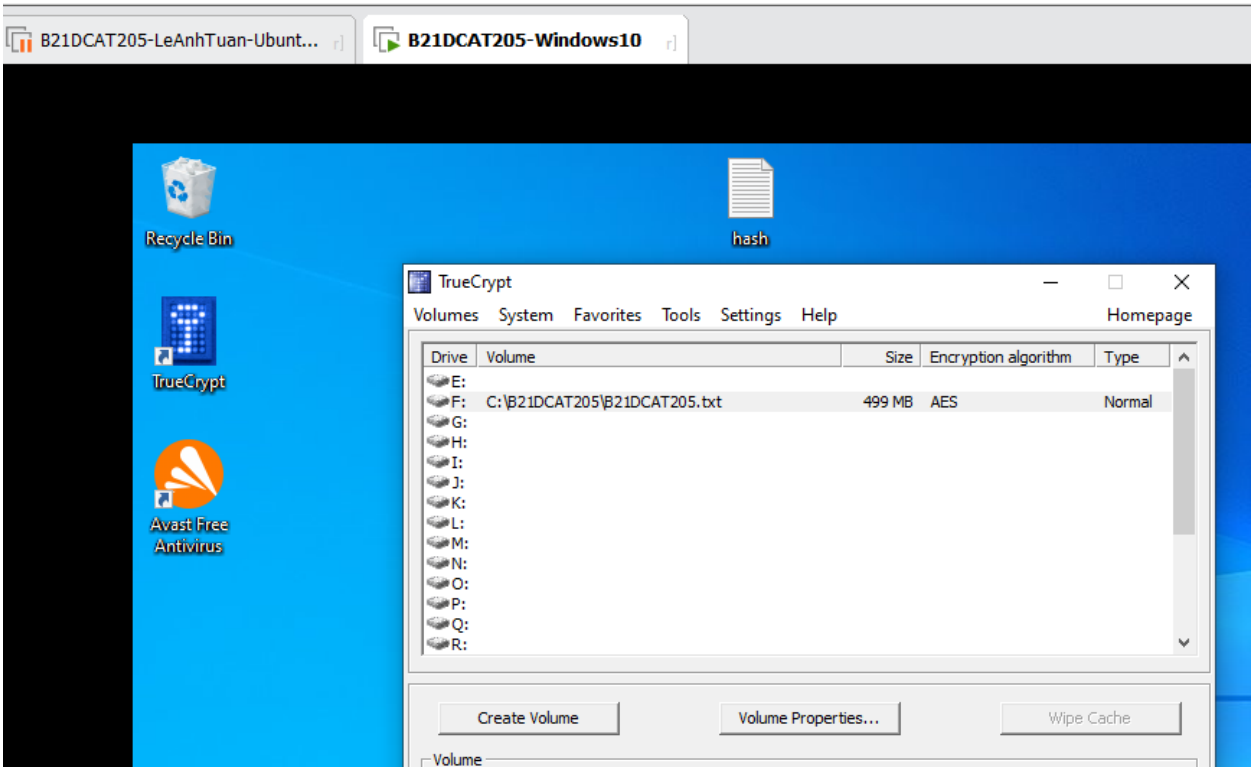


Hình 26: Sử dụng mật khẩu

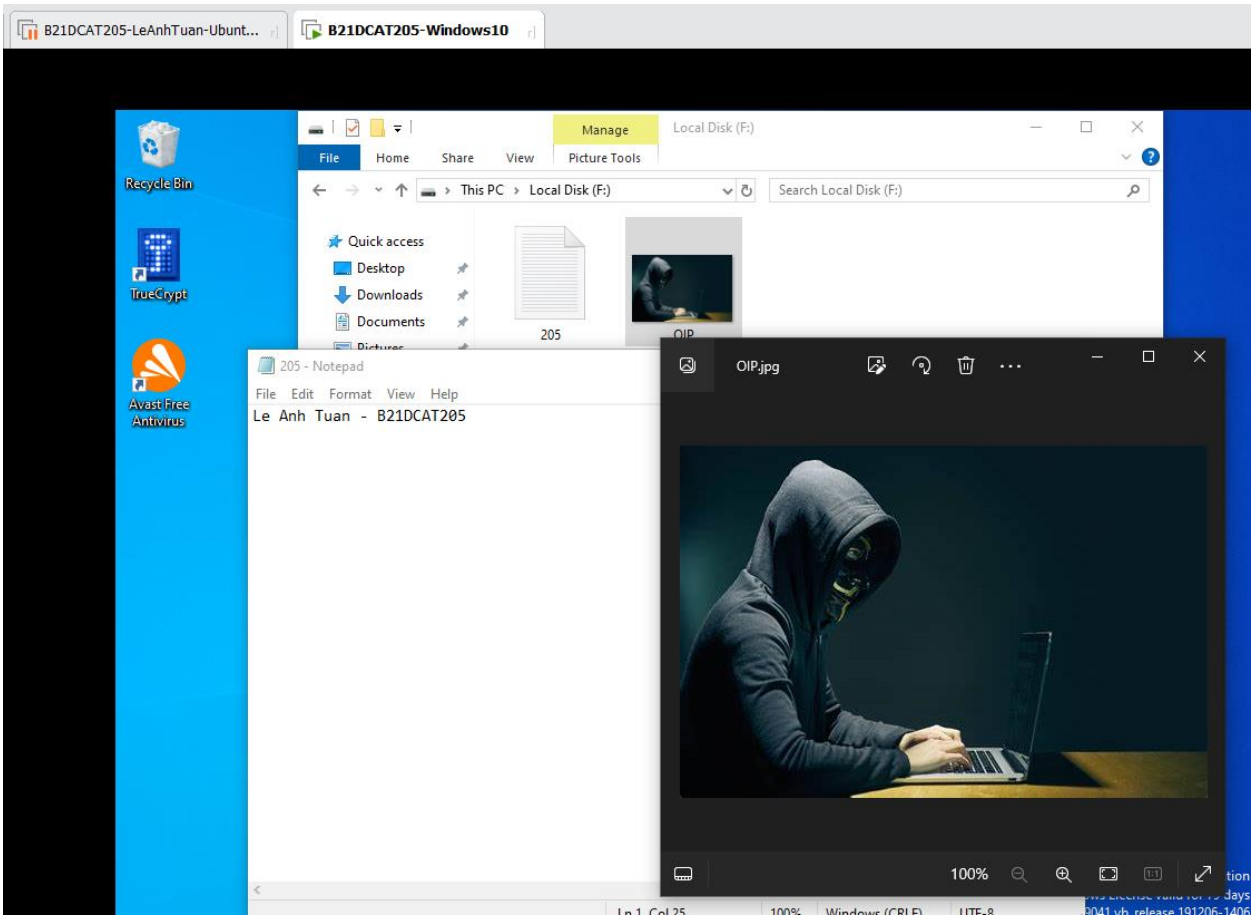
Nếu quên mật khẩu, ta có thể sử dụng keyfile để khôi phục file đã mã hoá Thay vì nhập mật khẩu, chọn Use keyfiles -> Add Files



Hình 27: Sử dụng keyfile



Hình 28: Mout ổ F



Hình 29: Khôi phục dữ liệu thành công

3 Kết luận

- Qua bản báo cáo trên ta đã đi tìm hiểu về cách mã hóa file bằng các công cụ. cách sử dụng chúng và các lý thuyết về mã hóa. Kết quả của bài này ta đã đạt được các mục đích mà bài đề ra.

4 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