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

BÁO CÁO

Bài 13: Đảm bảo an toàn với mã hóa

Giảng viên hướng dẫn: Vũ Minh Mạnh

Sinh viên thực hiện: Nguyễn Quốc Vượng

Mã sinh viên: B21DCAT227

Lớp: D21CQAT03-B

Hà Nội, 2023

Môn học Thực tập cơ sở

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

❖ TrueCrypt là một công cụ mã hóa dữ liệu mã nguồn mở, được sử dụng để tạo ra các ổ đĩa ảo được mã hóa và/hoặc mã hóa các phân vùng hoặc ổ đĩa thực. Dưới đây là mô tả ngắn về lý thuyết và cách thức hoạt động của TrueCrypt:

Lý thuyết về TrueCrypt:

- **Mã hóa đối xứng**: TrueCrypt sử dụng mã hóa đối xứng để bảo vệ dữ liệu. Điều này có nghĩa là cùng một khóa được sử dụng để mã hóa và giải mã dữ liệu. TrueCrypt hỗ trợ nhiều thuật toán mã hóa đối xứng như AES, Serpent và Twofish.
- **Mã hóa đa cấp**: TrueCrypt sử dụng một hệ thống mã hóa đa cấp, trong đó một khóa được tạo ra mỗi khi một thư mục hoặc ổ đĩa mới được tạo ra. Điều này giúp tăng cường bảo mật bằng cách ngăn chặn việc tấn công từ vị trí khóa duy nhất.
- **Hệ thống phức tạp**: TrueCrypt sử dụng một hệ thống phức tạp của các thùng chứa (container) và một cấu trúc khóa hỗn hợp để bảo vệ dữ liệu.

Cách thức hoặc phương pháp áp dụng TrueCrypt để mã hóa file hoặc thư mục:

1. **Tạo thùng chứa (container)**:
    - Sử dụng TrueCrypt để tạo một thùng chứa ảo, thường là một tệp hoặc một phân vùng trên ổ đĩa.
    - Chọn dung lượng và cài đặt mật khẩu cho thùng chứa. Mật khẩu này sẽ được sử dụng để mở thùng chứa sau này.
    - Lựa chọn thuật toán mã hóa và các cài đặt bổ sung nếu cần.
2. **Mở và sử dụng thùng chứa**:
    - Sử dụng TrueCrypt để mở thùng chứa đã tạo bằng cách nhập mật khẩu được thiết lập trước đó.
    - Một khi thùng chứa đã được mở, nó sẽ hiển thị như một ổ đĩa mới trong hệ thống tập tin của bạn.

- Bạn có thể lưu trữ, chỉnh sửa và di chuyển các tệp tin vào và ra khỏi thùng chứa này như bạn làm với bất kỳ ổ đĩa nào khác.

3. **Đóng thùng chứa**:
    - Khi bạn đã hoàn thành công việc của mình, hãy sử dụng TrueCrypt để đóng thùng chứa.
    - Việc này sẽ đảm bảo rằng dữ liệu trong thùng chứa được mã hóa lại và trở nên không thể truy cập được nếu không có mật khẩu.

TrueCrypt cung cấp một phương pháp hiệu quả và linh hoạt để bảo vệ dữ liệu của bạn, đặc biệt là khi cần chuyển tải dữ liệu một cách an toàn hoặc lưu trữ dữ liệu quan trọng một cách bảo mật.

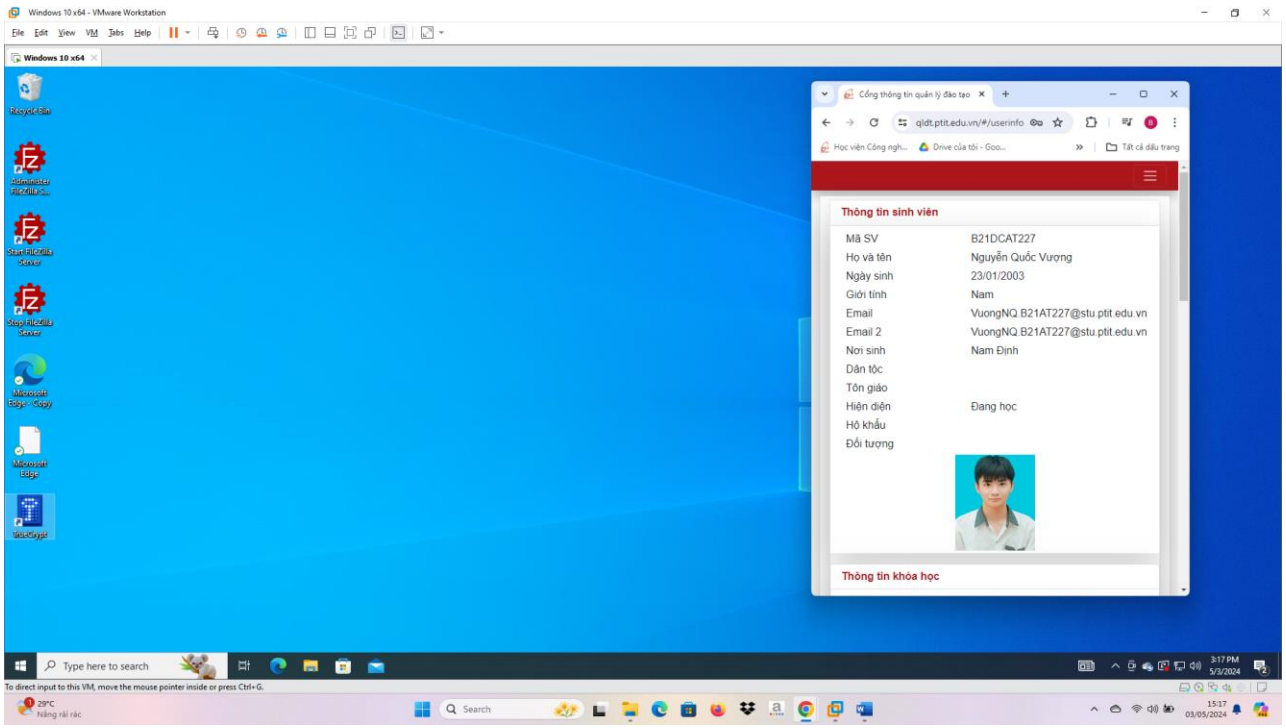
2.2. Chuẩn bị môi trường

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

2.3. Các bước thực hiện

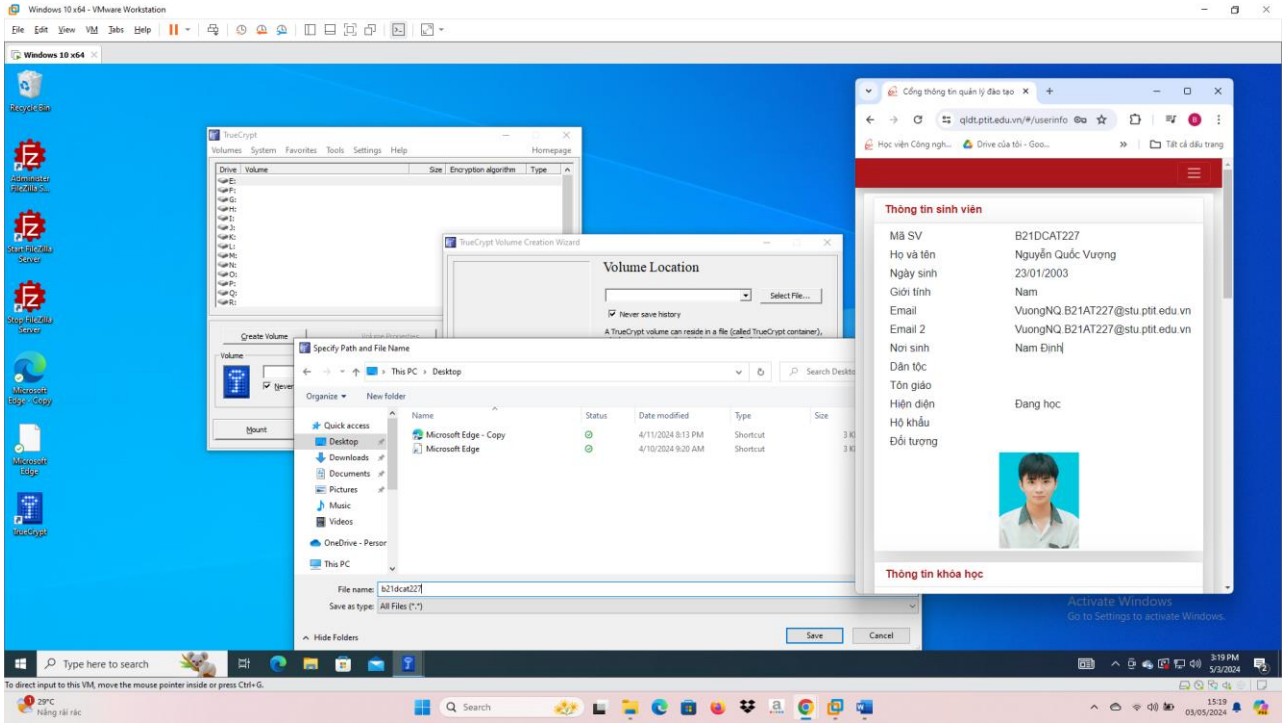
2.3.1. Chuẩn bị môi trường

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

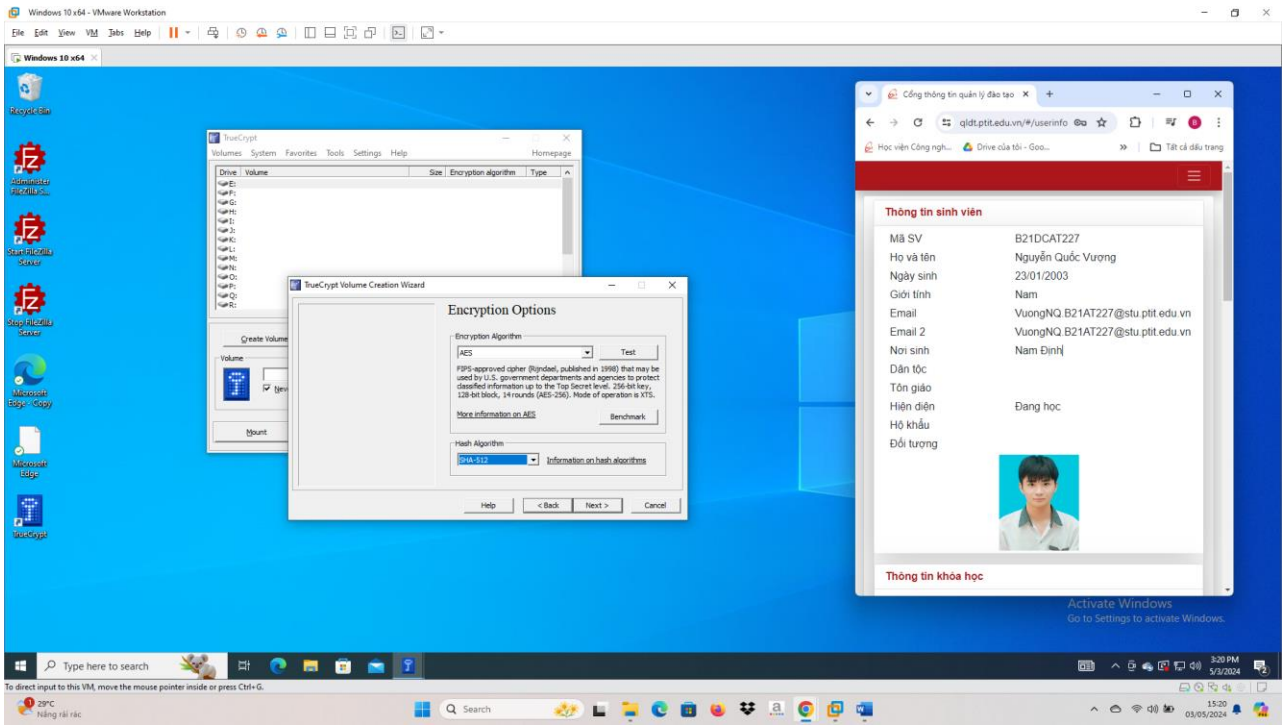


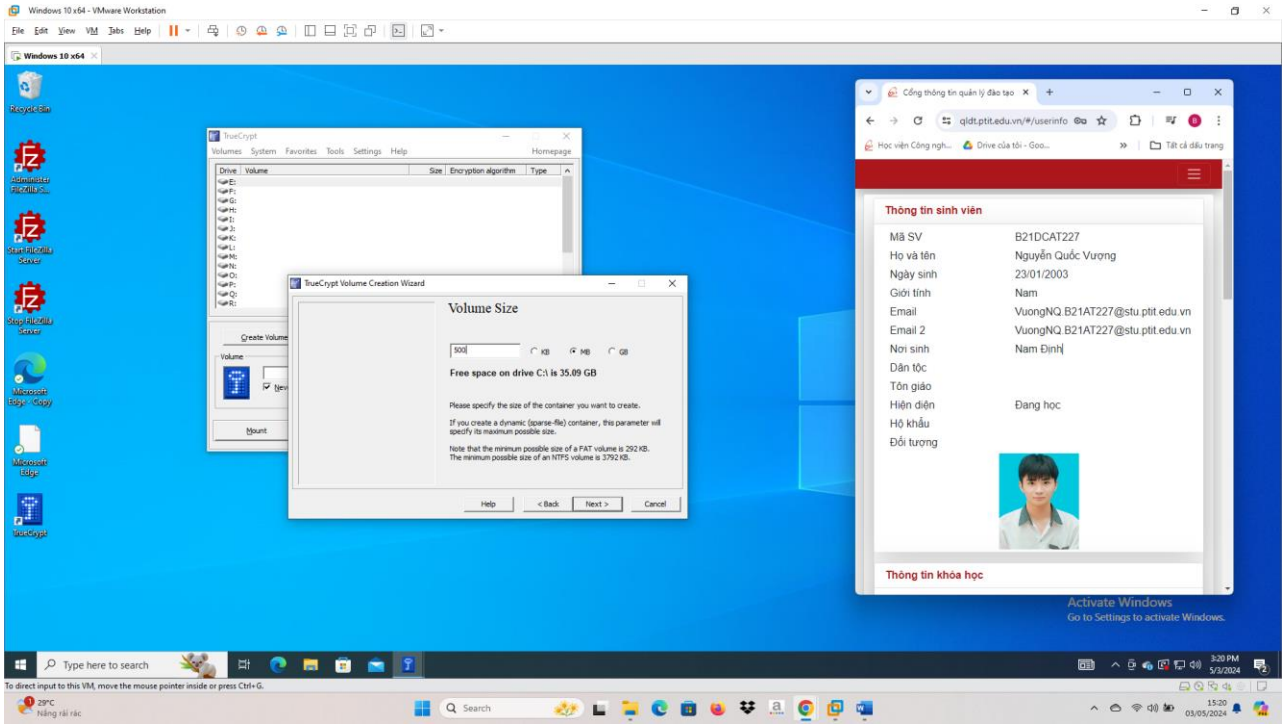
2.3.2. *Nội dung thử nghiệm*

Tạo volume mới:

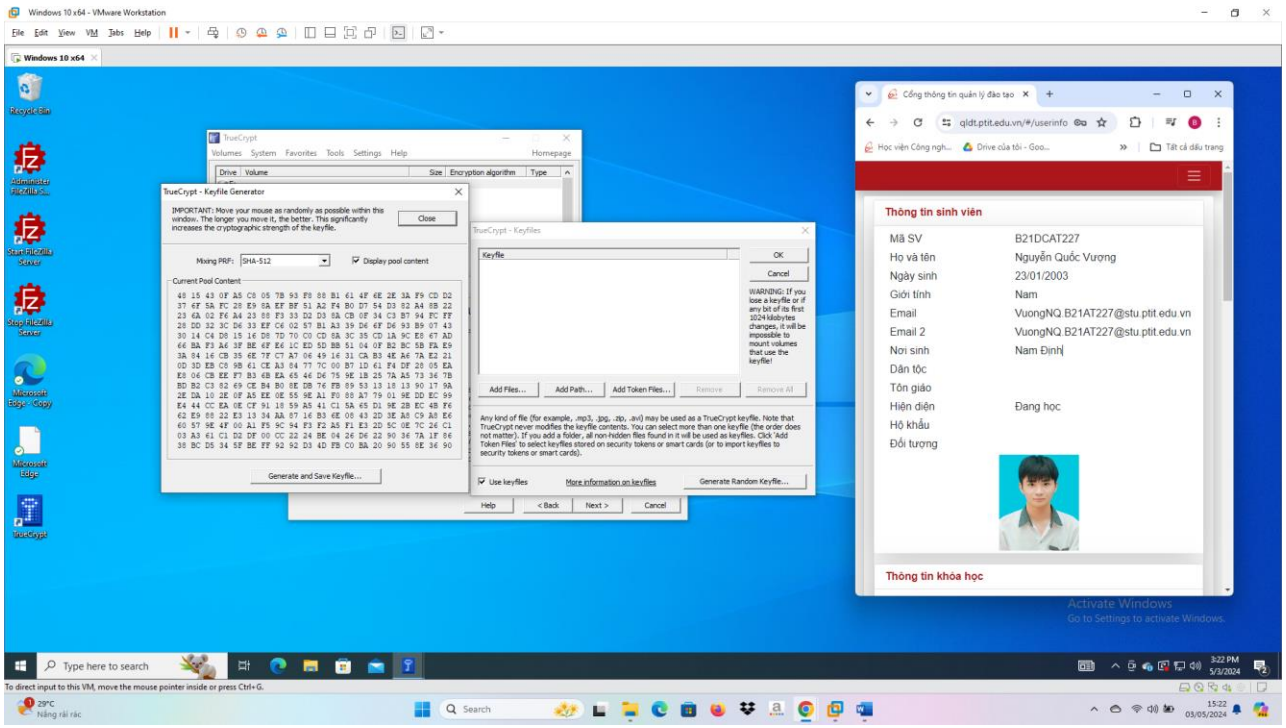


Chọn thuật toán mã hóa:



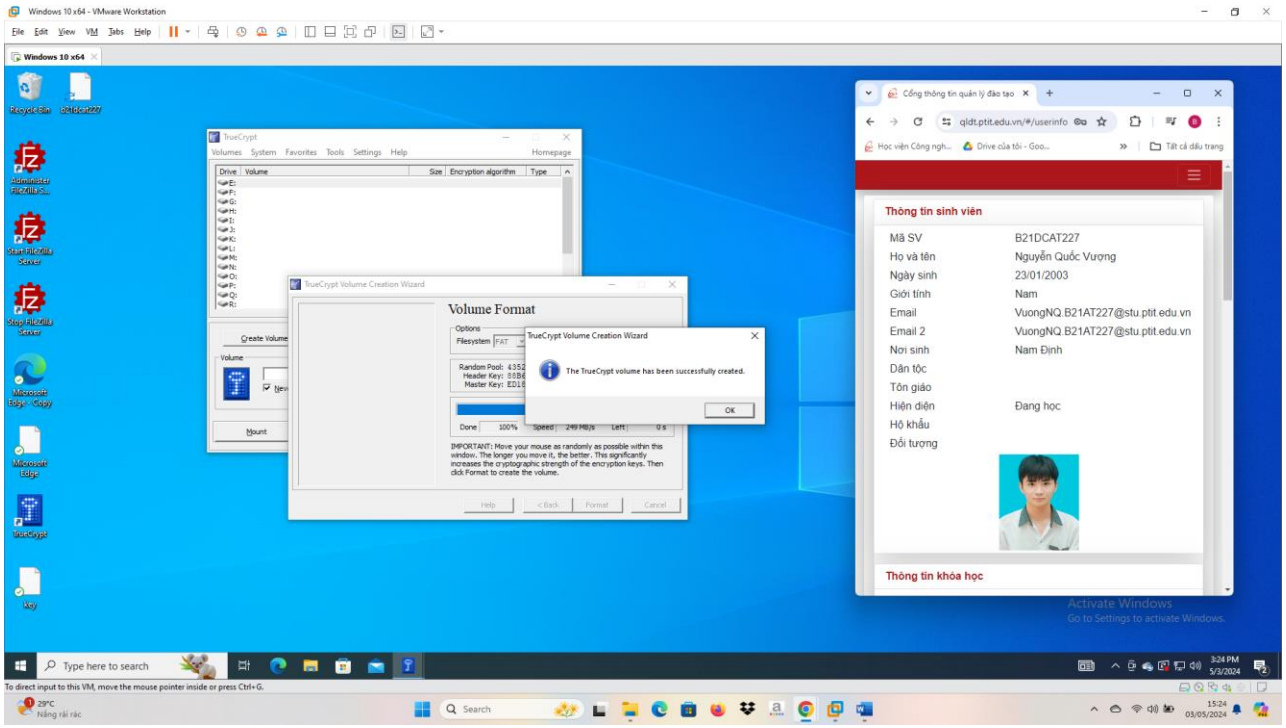


Tạo key: (chọn generate random keyfile => generate and save keyfile)



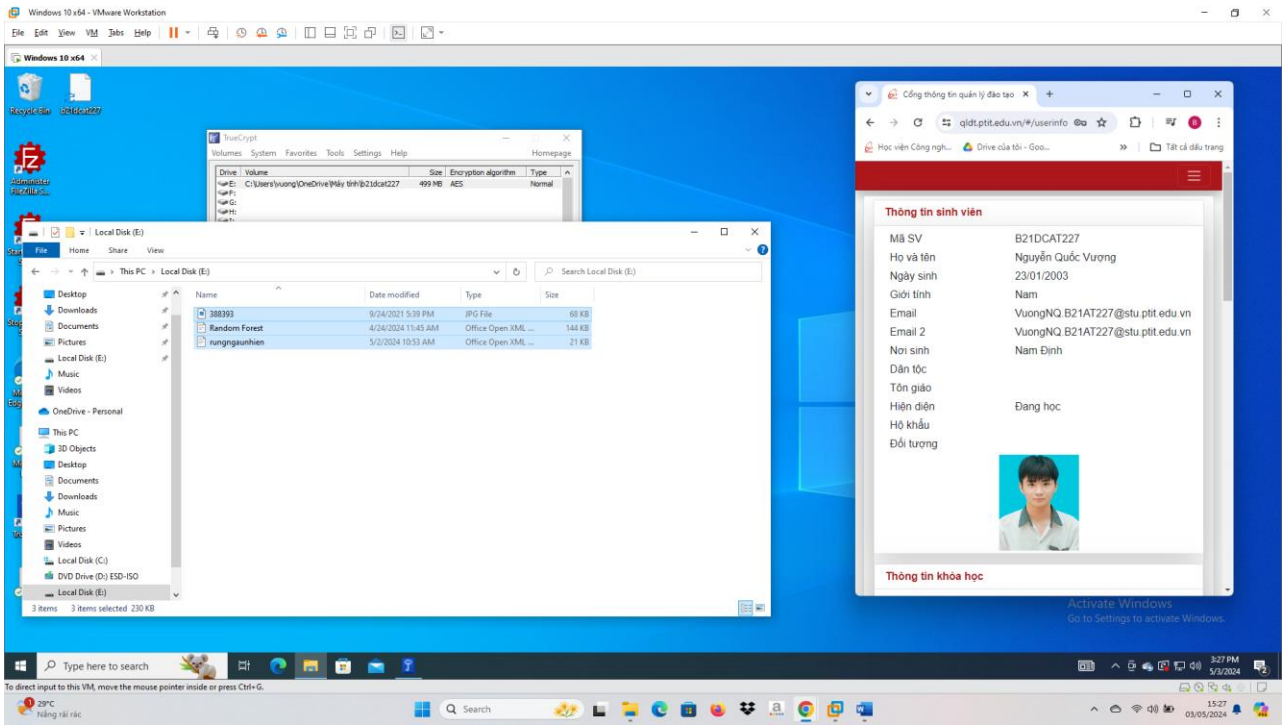
Thêm key vào volume đang tạo(add files)

Tạo thành công volume:



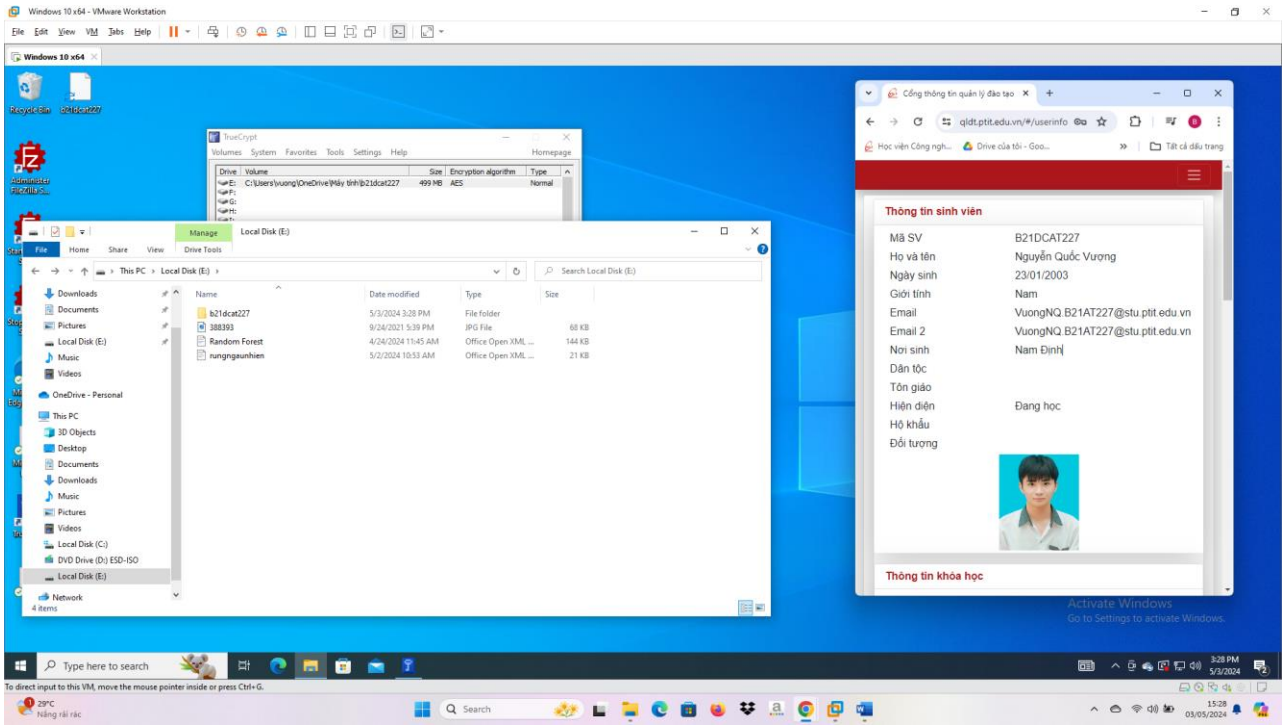
- Sử dụng công cụ TrueCrypt để hóa mã file.

Thêm các file văn bản và phương tiện vào ổ đĩa đã mout:

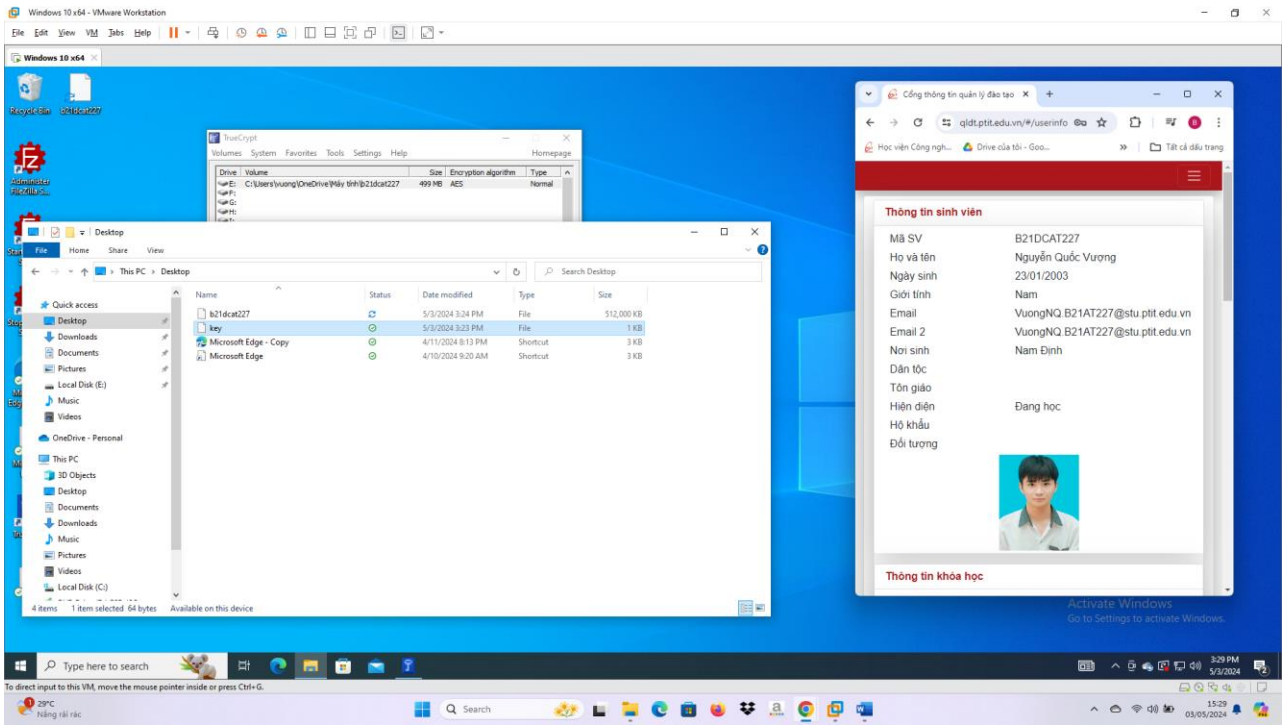


- Sử dụng công cụ TrueCrypt để hóa thư mục. Đặt tên thư mục theo mã sinh viên và có chứa 1 số file khác nhau.

Thêm thư mục vào ổ đĩa đã mount:

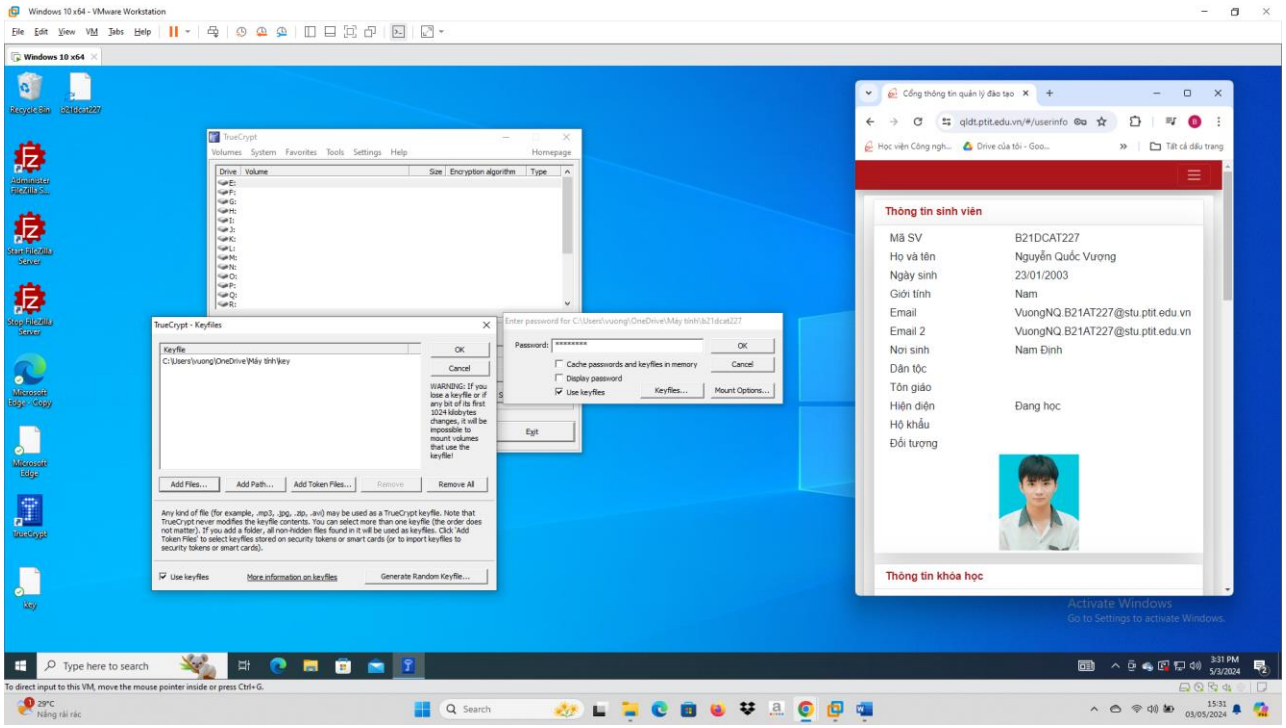


- Sao lưu khóa mã hóa của công cụ TrueCrypt.

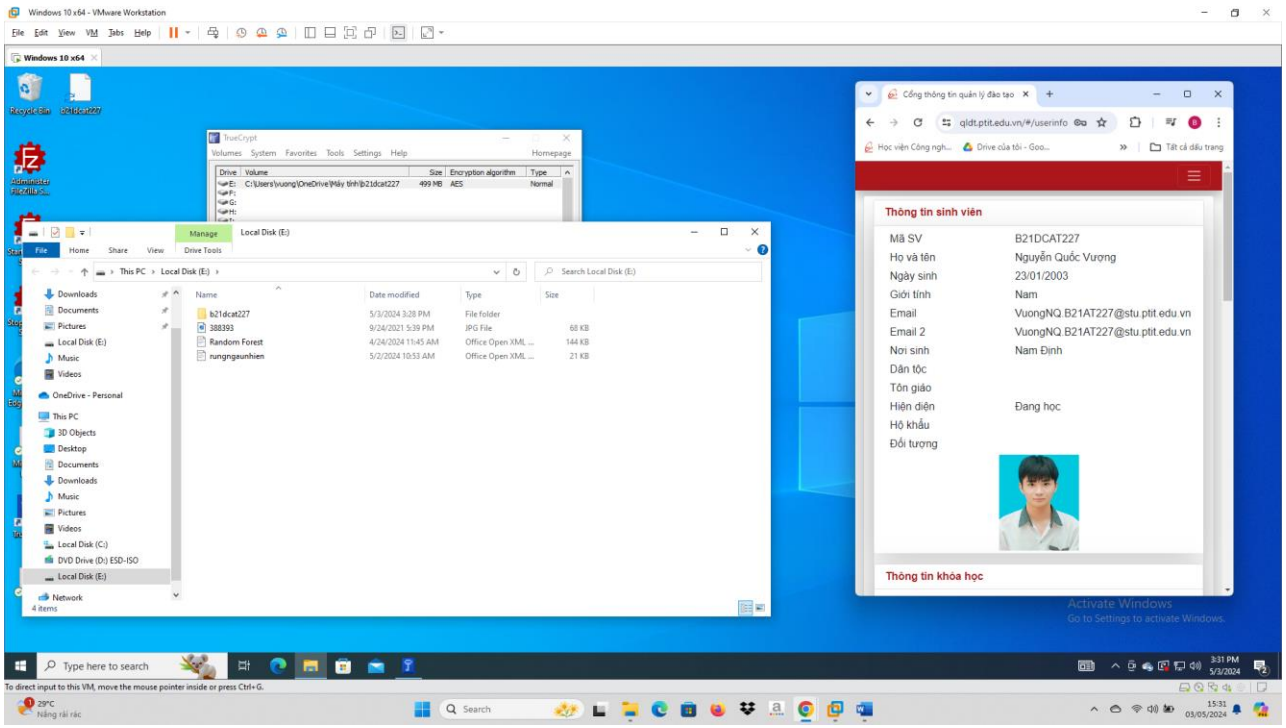


- Sử dụng công cụ TrueCrypt để khôi phục các file và thực mục mã hóa.

Thực hiện unmount và mount lại ổ đĩa để khôi phục bằng thư mục đã lưu với mật khẩu và file key đã lưu:



Khôi phục thành công:


Windows 10 x64 - VMware Workstation
Thông tin sinh viên
Mã SV B21DCAT227
Họ và tên Nguyễn Quốc Vượng
Ngày sinh 23/01/2003
Giới tính Nam
Email VuongNQ.B21AT227@stu.ptit.edu.vn
Email 2 VuongNQ.B21AT227@stu.ptit.edu.vn
Nơi sinh Nam Định
Dân tộc
Tôn giáo
Hiện diện Đang học
Hộ khẩu
Đối tượng
Thông tin khóa học
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.