HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOAN AN TOÀN THÔNG TIN

BÁO CÁO THỰC HÀNH

Bài 13: Đảm bảo an toàn với mã hóa

Họ và tên: VũThành Long

Mã sinh viên: B21DCAT012

Nhóm: 06

Môn học: Thực tập cơ sở

Giảng viên giảng dạy: Nguyễn Hoa Cương

Hà Nội, 2024

Mục lục

I. Tìm hiểu lý thuyết:

1. TrueCrypt:

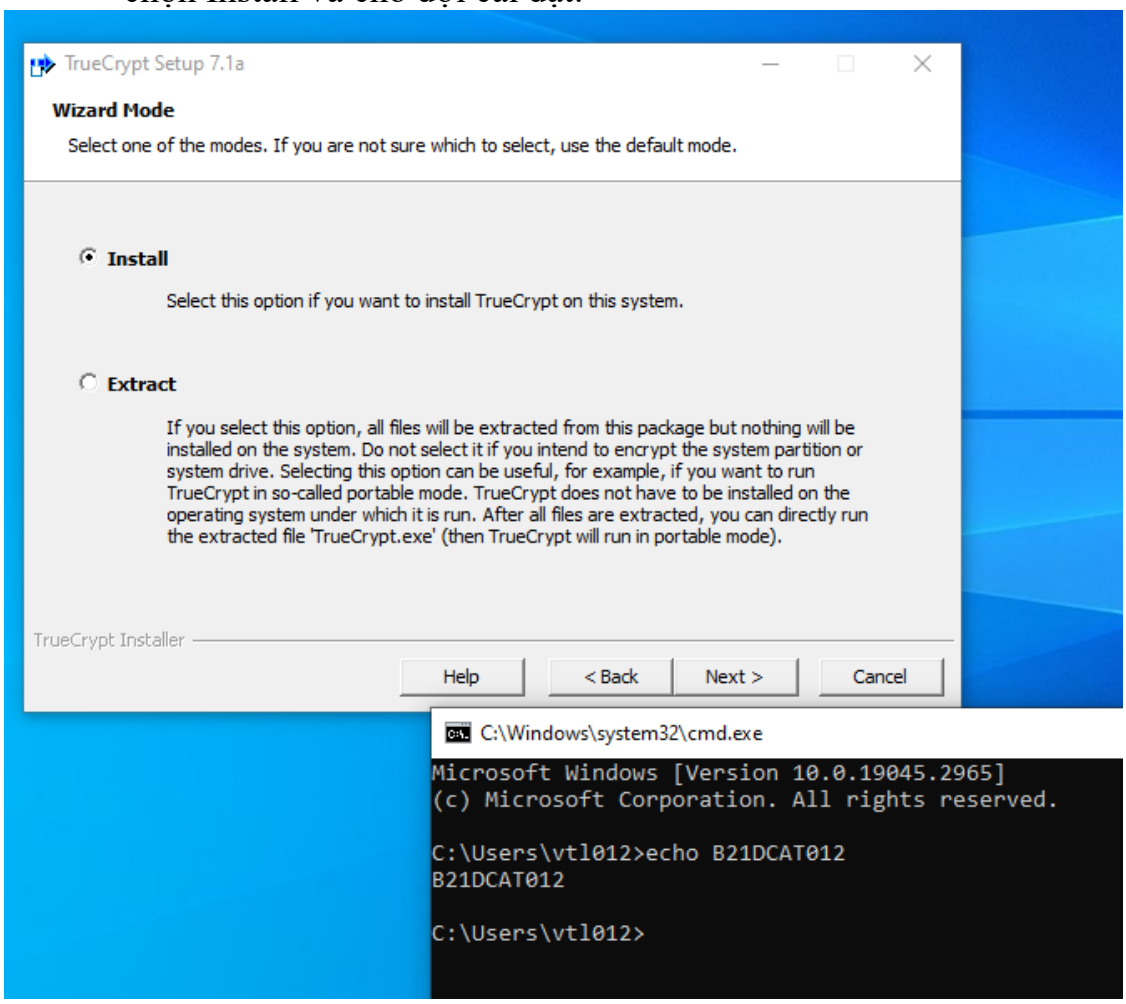
- TrueCrypt là công cụ miễn phí, mã nguồn mở để mã hoá dữ liệu trên ổ đĩa cứng.
- TrueCrypt có thể tạo một đĩa ảo được mã hóa trong một tệp, hoặc mã hóa một phân vùng hoặc toàn bộ thiết bị lưu trữ.
- TrueCrypt có mặt trên hệ điều hành Windows, MacOS và Linux 32-bit và 64-bit.
- Các thuật toán mã hoá mà TrueCrypt hỗ trợ là AES, Serpent và Twofish. Ngoài ra, có sẵn năm tổ hợp thuật toán xếp tầng khác nhau: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES và Twofish-Serpent. TrueCrypt hỗ trợ các hàm băm RIPEMD-160, SHA-512 và Whirlpool.
- Tháng 5 năm 2014, đội ngũ phát triển TrueCrypt tuyên bố dừng bảo trì phần mềm này. Tính đến thời điểm làm báo cáo này, một bản fork của TrueCrypt là VeraCrypt vẫn được phát triển. Người dùng nên chuyển sang sử dụng VeraCrypt.

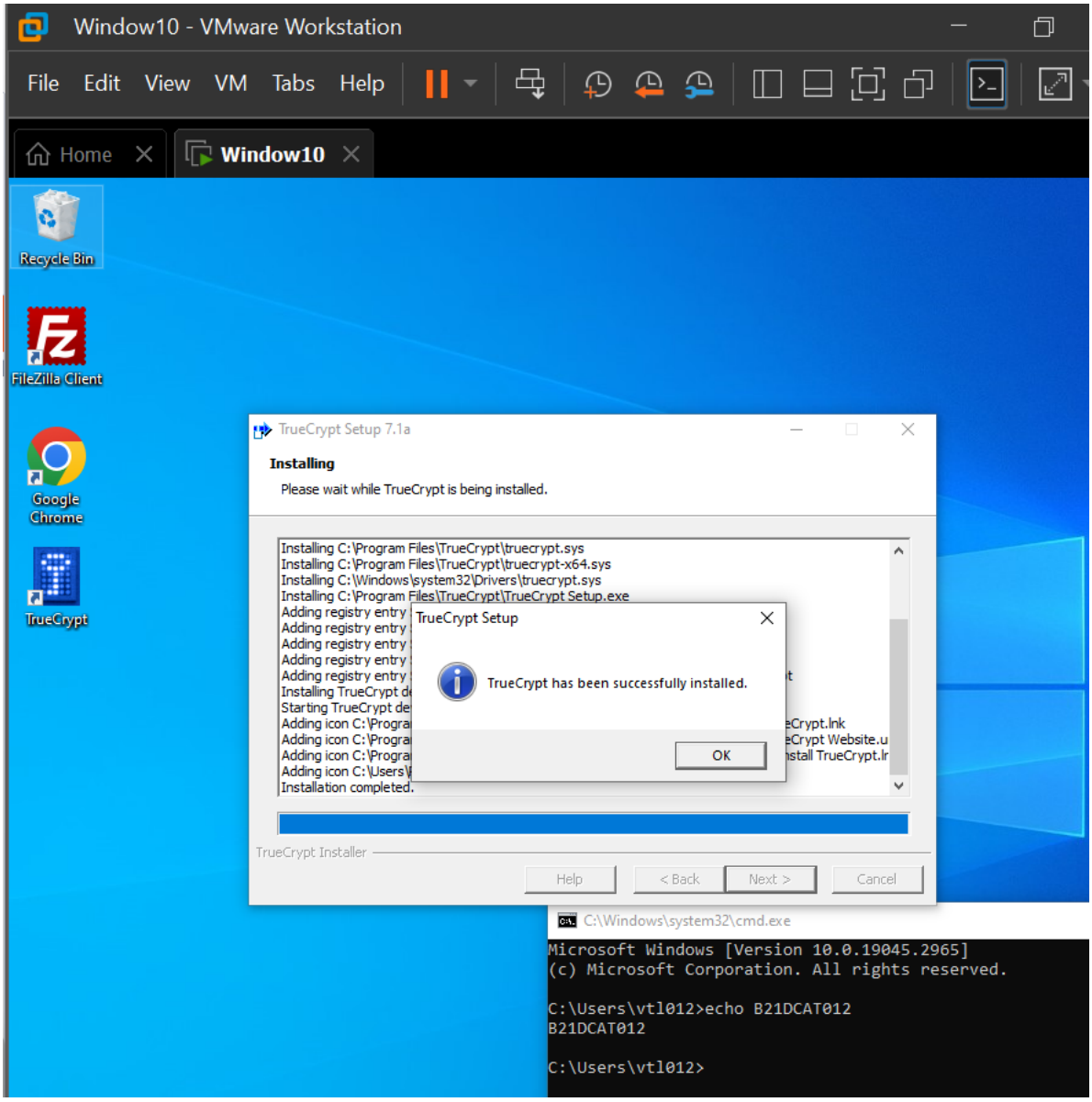
2. Phương thức hoạt động:

- Để mã hoá một tệp hoặc thư mục, trước hết TrueCrypt tạo một tệp tin mã hoá gọi là container. Kích cỡ của container sẽ do người dùng đặt. Sau khi tạo container, người dùng sẽ nạp (mount) container như khi nạp một ổ cứng thật. Sau khi nạp, người dùng có thể chuyển các tệp và thư mục vào container.
- Dữ liệu trong container được bảo vệ bằng cách sử dụng mã hoá khoá đối xứng với khóa được tạo ngẫu nhiên khi container được thiết lập lần đầu tiên. Sau đó, để truy cập dữ liệu của container, người dùng phải điền mật khẩu để cung cấp khóa cho phần mềm.

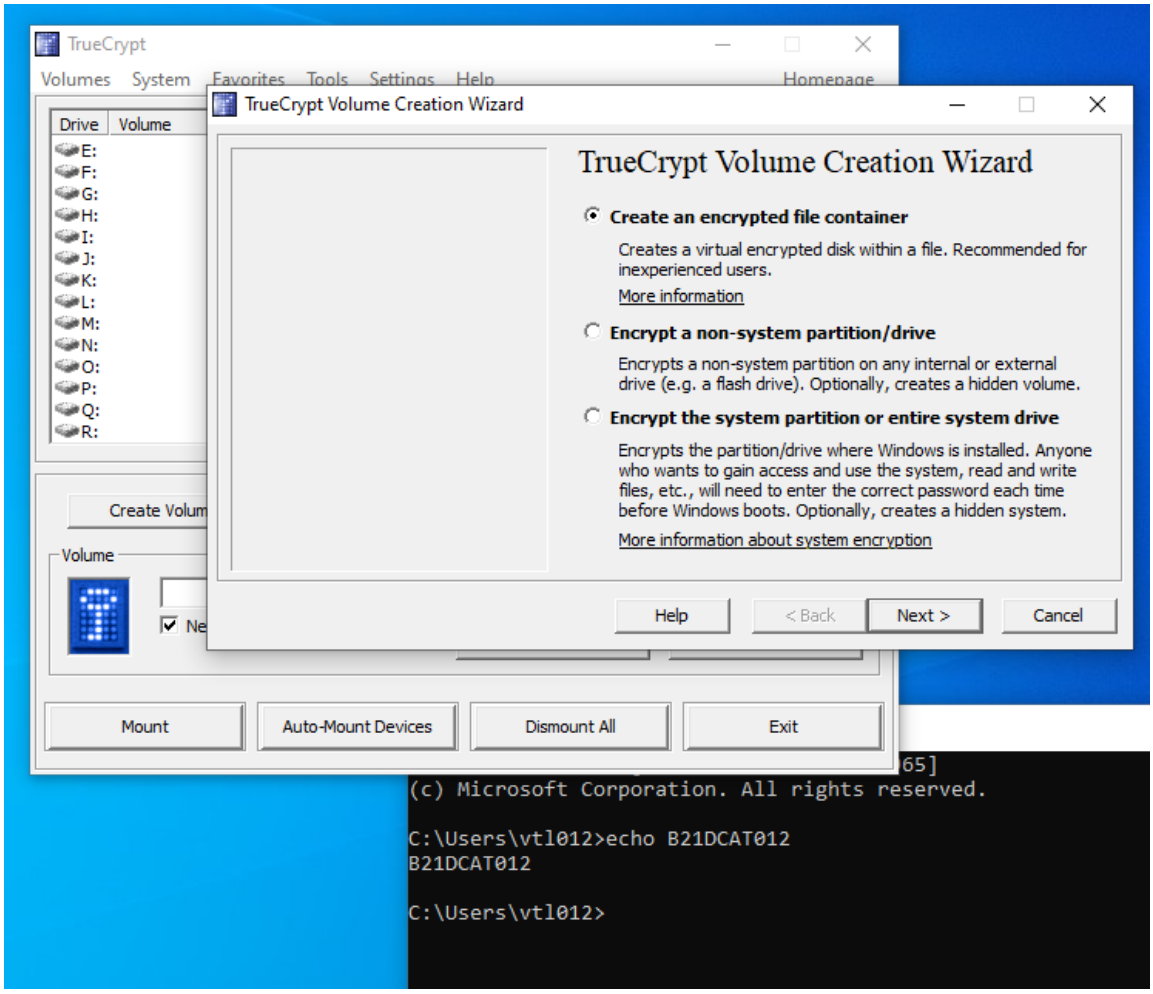
II. Mô tả cài đặt & kết quả:

– Thực hiện cài đặt TrueCrypt. Chạy chương trình cài đặt TrueCrypt, chọn Install và chờ đợi cài đặt.

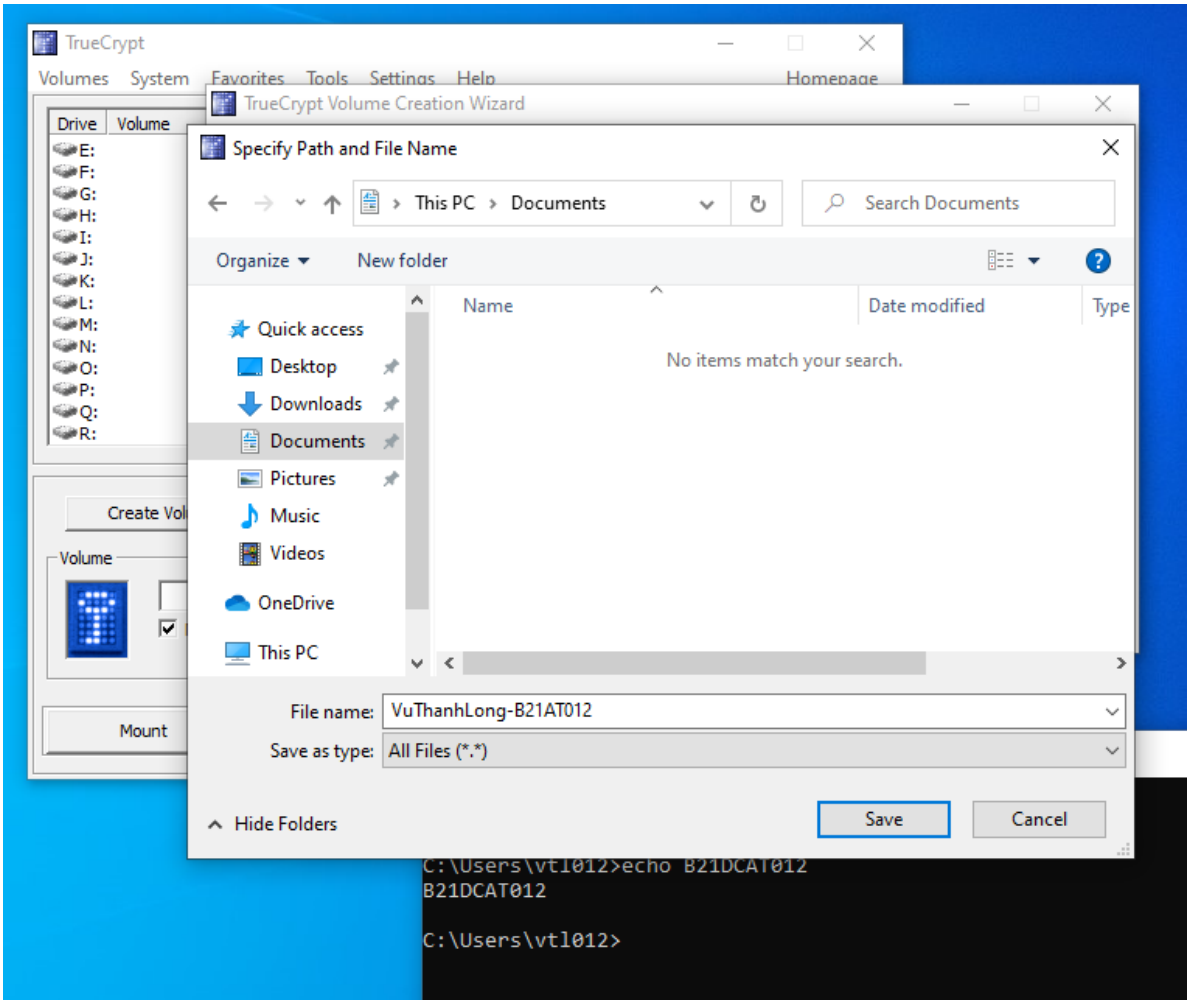




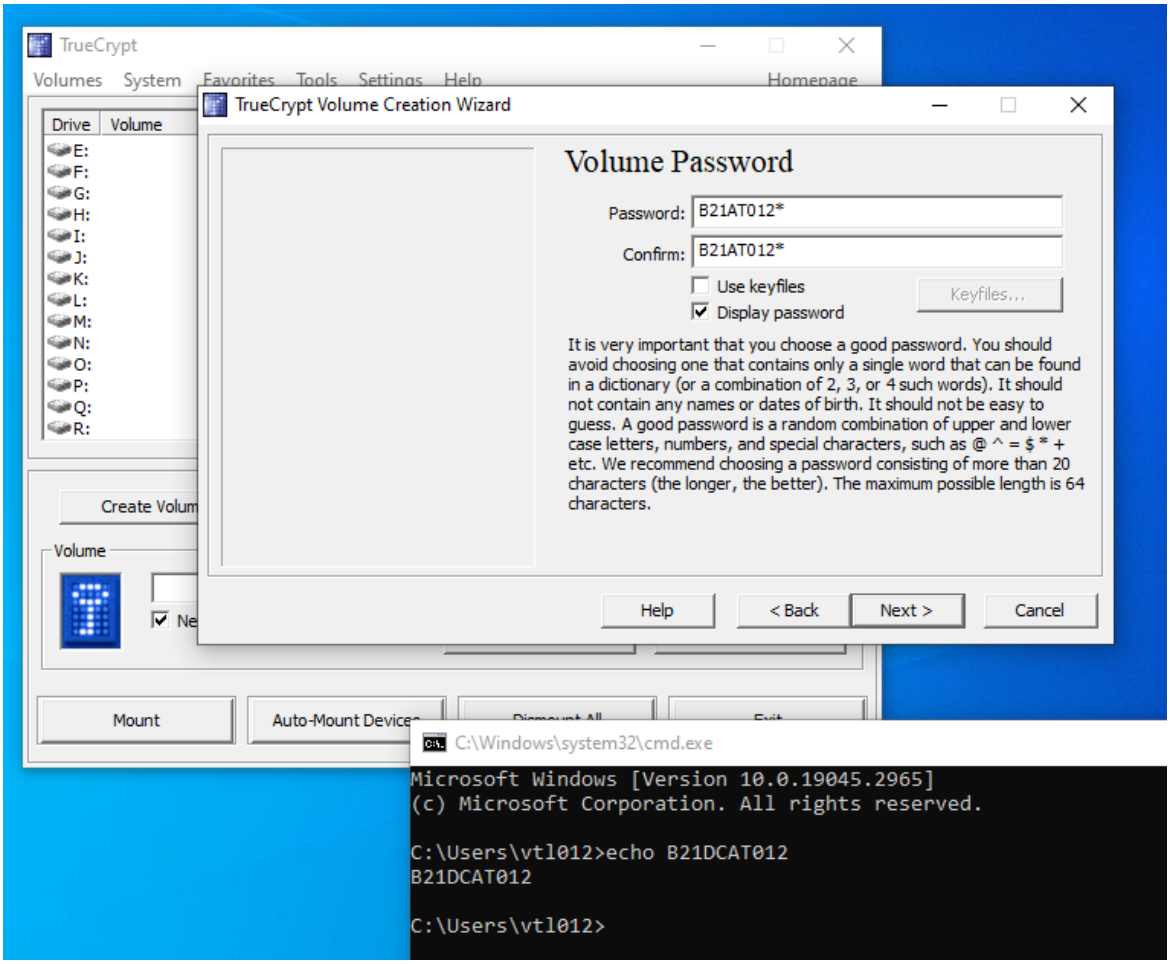
– Khởi động giao diện TrueCrypt. Trước hết, cần phải tạo một "container" mã hoá. Bấm Create Volume rồi chọn Create an encrypted file container.



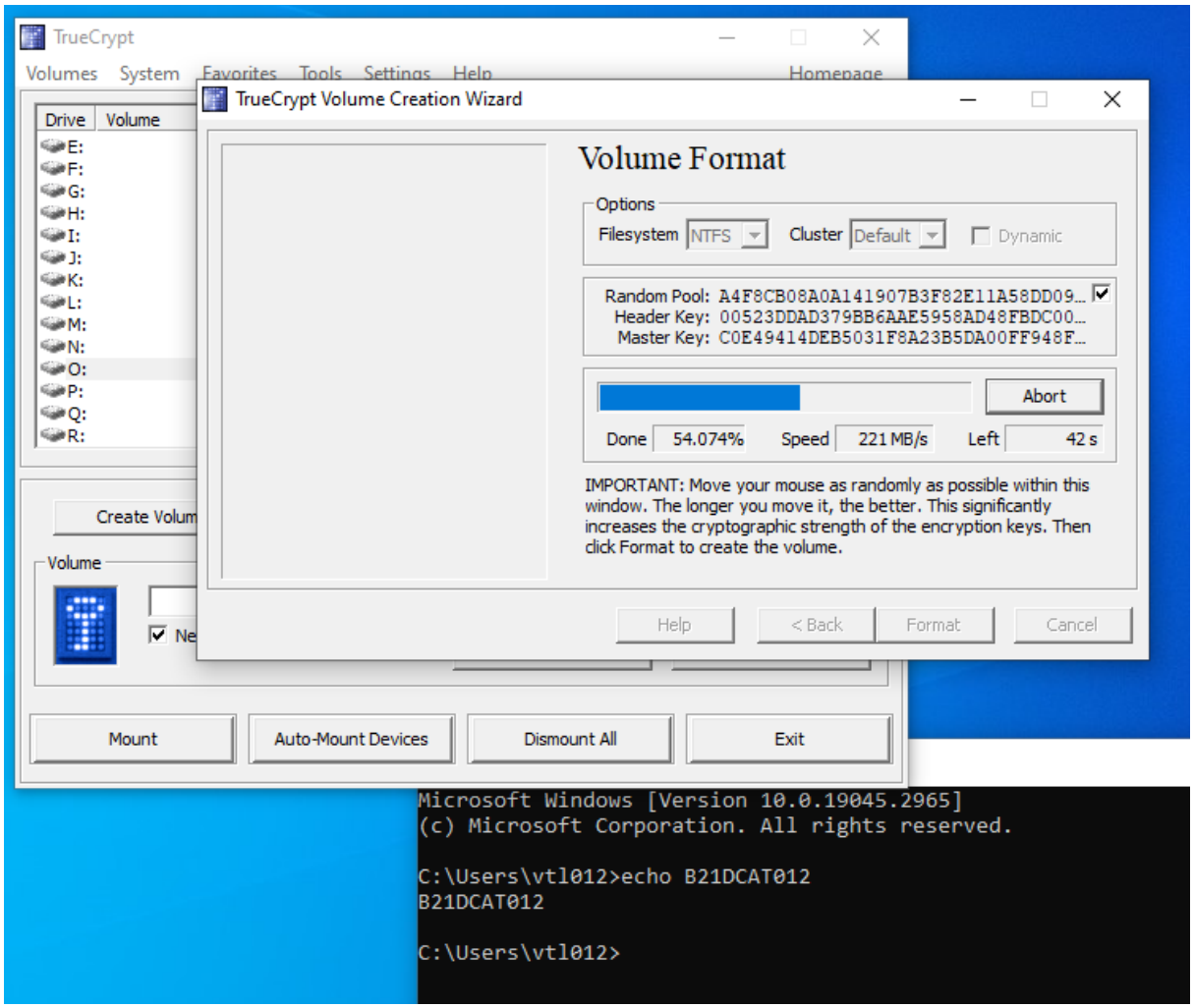
– Chọn địa chỉ và tên của container.



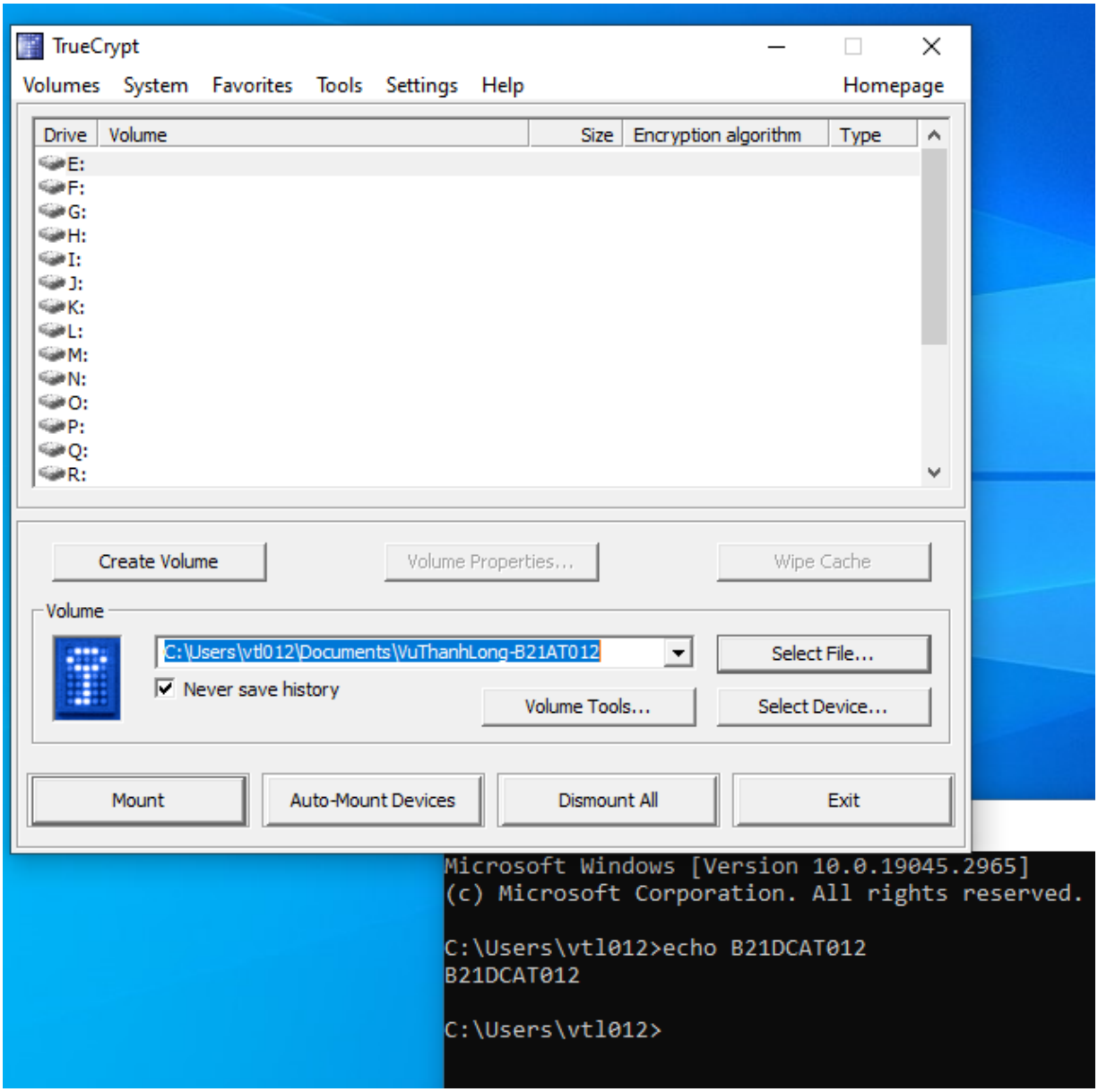
– Đến đây người dùng sẽ có các lựa chọn sau:
  - Mã hoá chỉ sử dụng mật khẩu (password).
  - Mã hoá chỉ sử dụng tệp tin khoá (keyfile).
  - Mã hoá sử dụng cả mật khẩu và tệp tin khoá.
– Sinh viên lựa chọn mã hoá bằng cả mật khẩu và tệp tin khoá, nhưng tạm thời chỉ đặt mật khẩu, sẽ thêm tệp tin khoá sau.



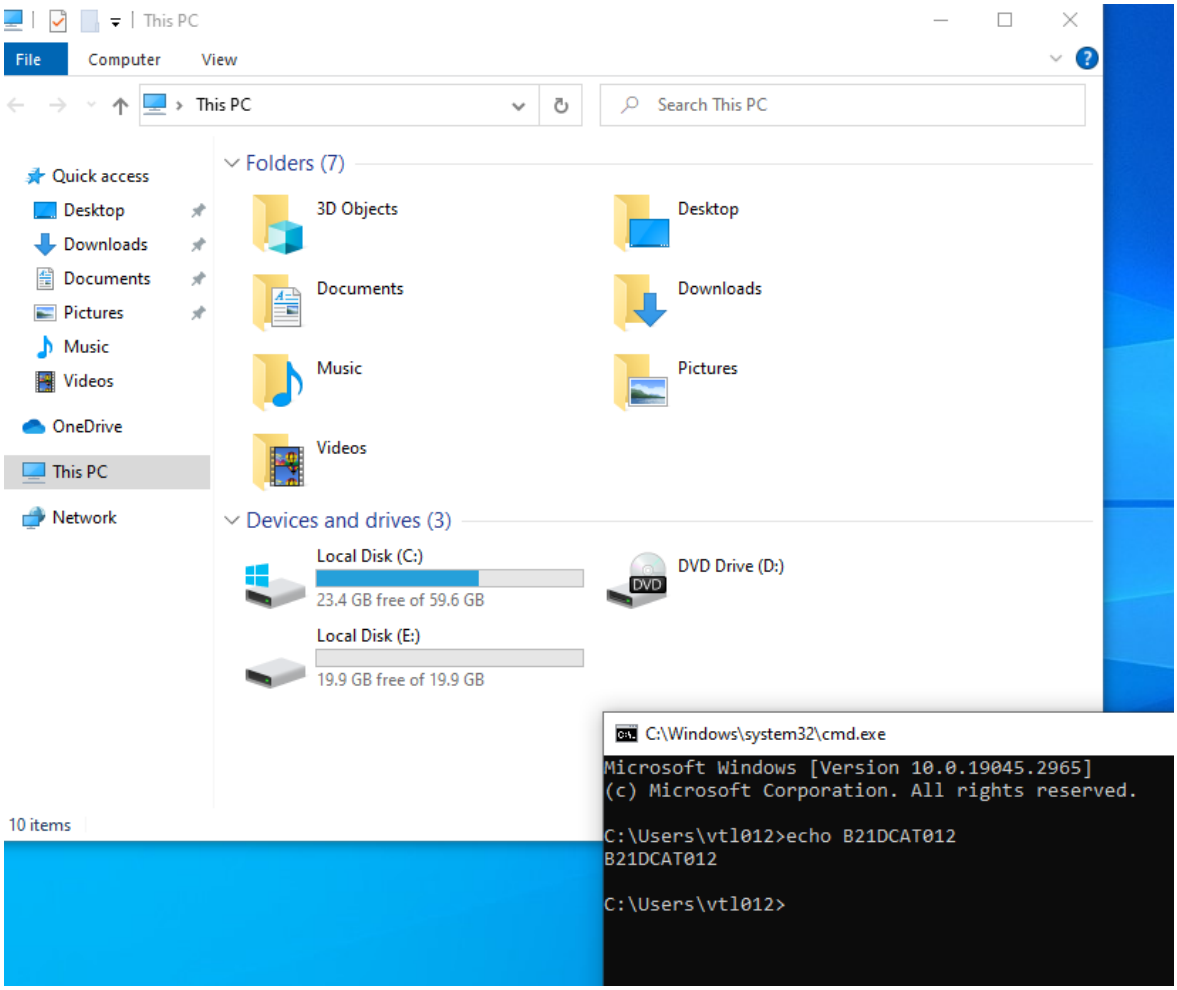
– Di chuột một cách ngẫu nhiên để tăng tính ngẫu nhiên của khoá rồi bấm Format.



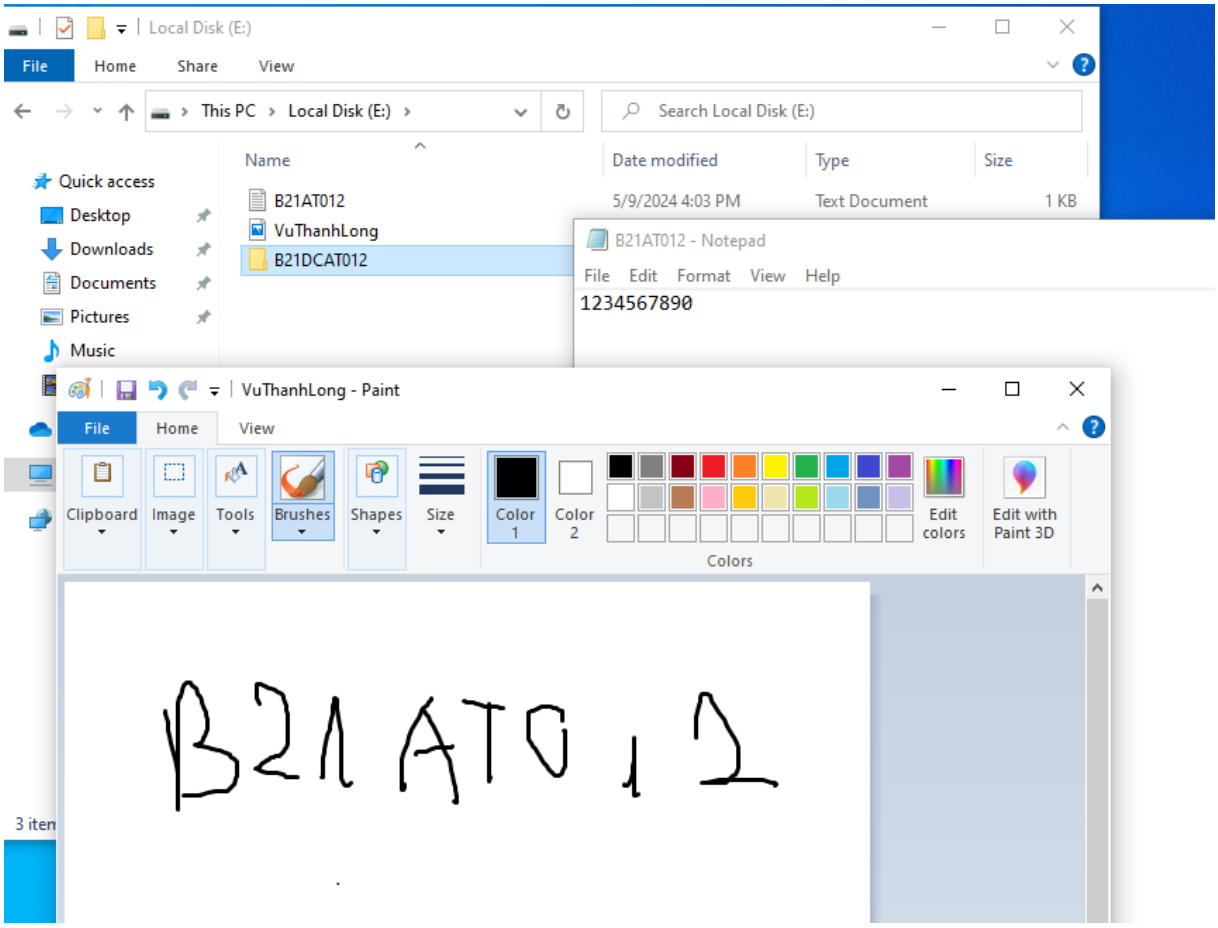
– Sau khi tạo container thành công, cần phải mount nó như một ổ đĩa. Mở lại giao diện TrueCrypt, chọn Select File, chọn container. Chọn một kí tự ổ cứng (trong trường hợp này là E) rồi bấm Mount.



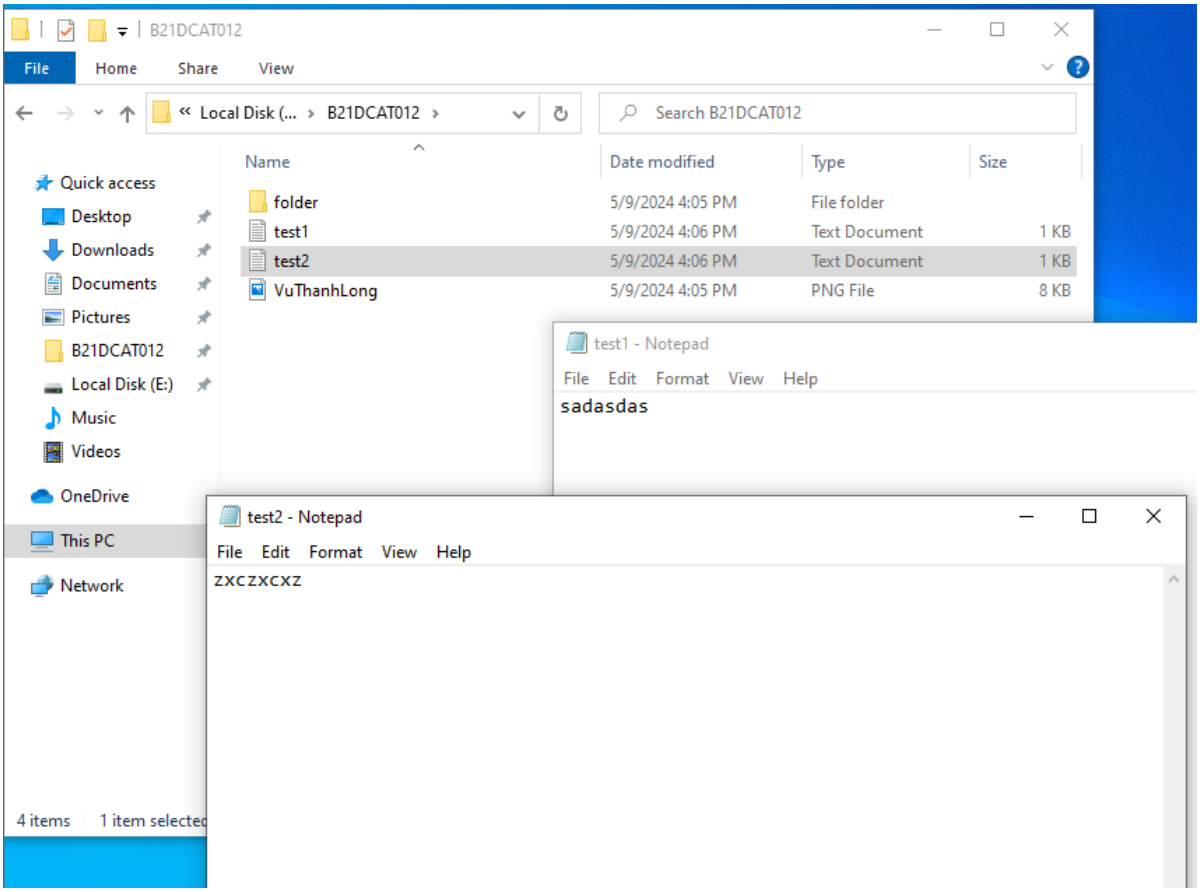
– Mở File Explorer để thấy ổ mới.



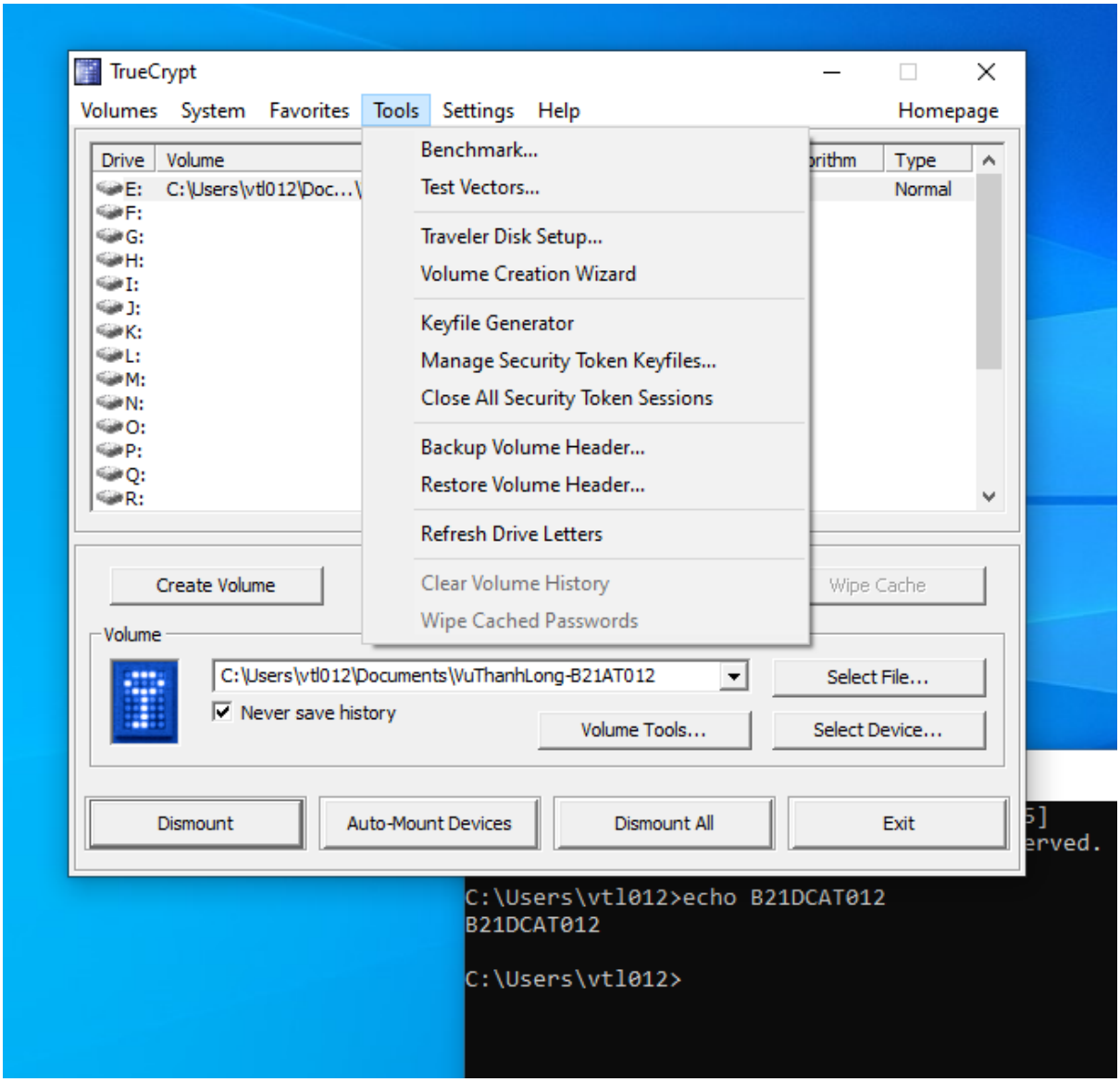
– Tại đây, sinh viên thêm vào một tệp văn bản .txt và một ảnh .png với nội dung như hình dưới. Đồng thời, sinh viên cũng tạo một thư mục tên B21DCAT012.



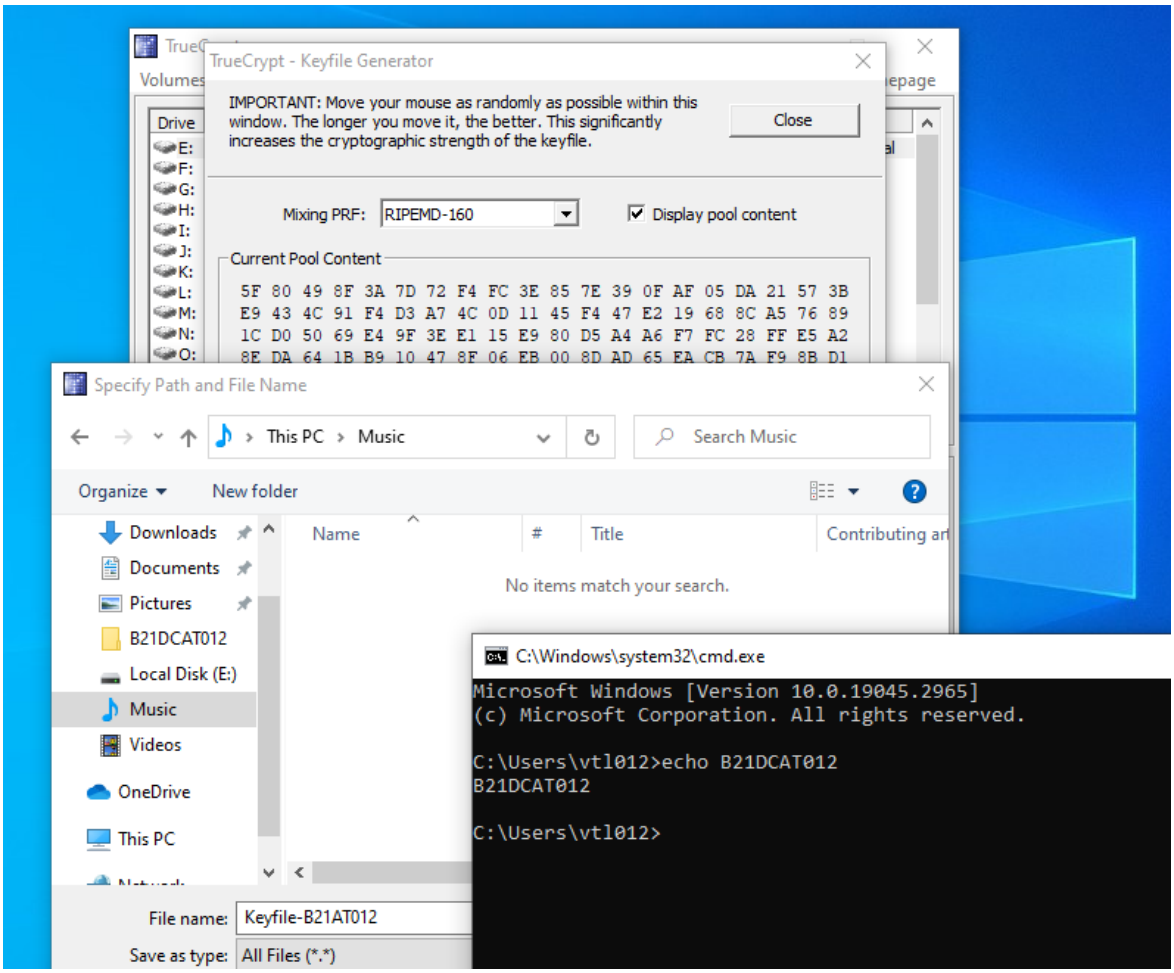
– Trong thư mục B21DCAT012, sinh viên tạo hai tệp văn bản, một tệp ảnh và một thư mục con với tên và nội dung như hình dưới.



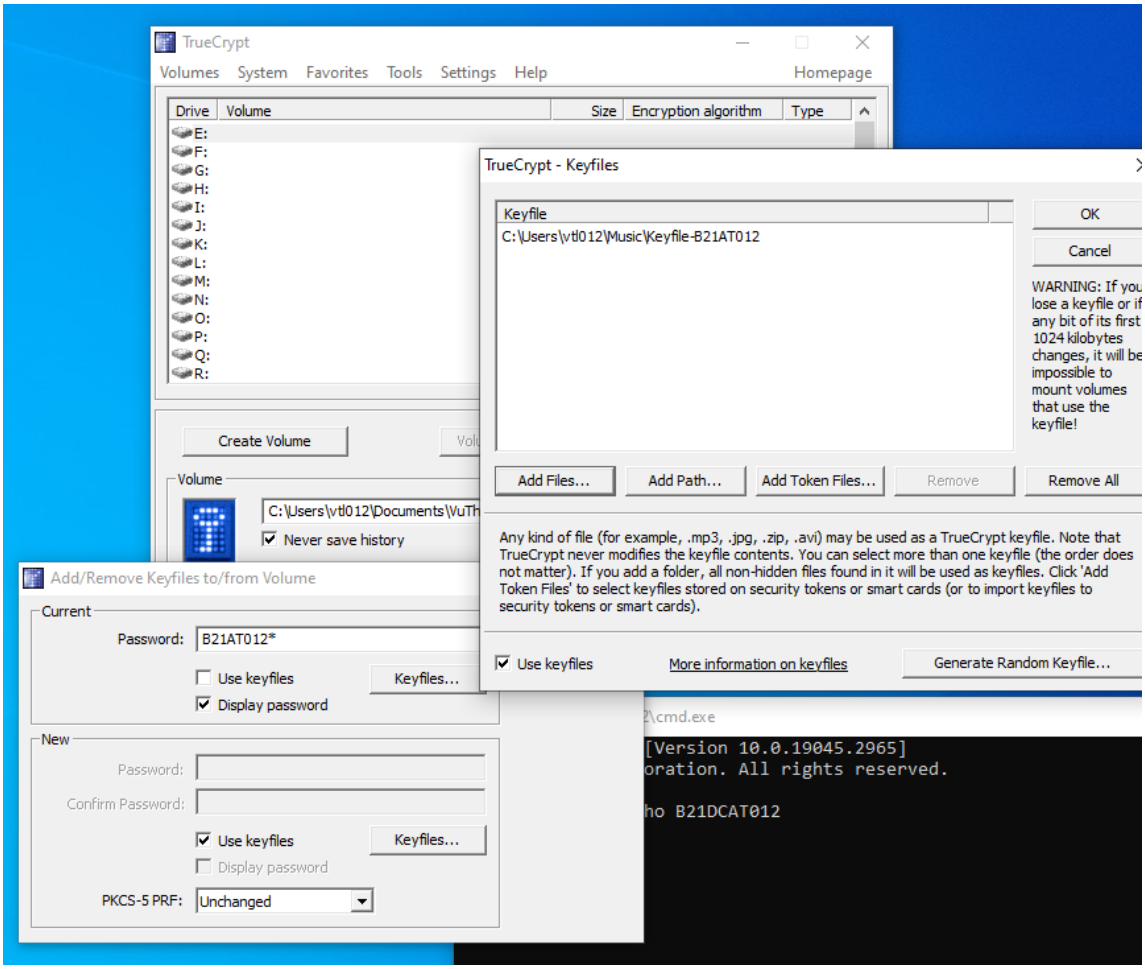
– Bây giờ sinh viên thực hiện thêm tệp tin khoá. Có thể sử dụng bất cứ tệp tin nào để làm tệp tin khoá, nhưng TrueCrypt cũng cung cấp tính năng tạo tệp tin khoá ngẫu nhiên. Trên giao diện TrueCrypt, chọn Tools -> Keyfile Generator.



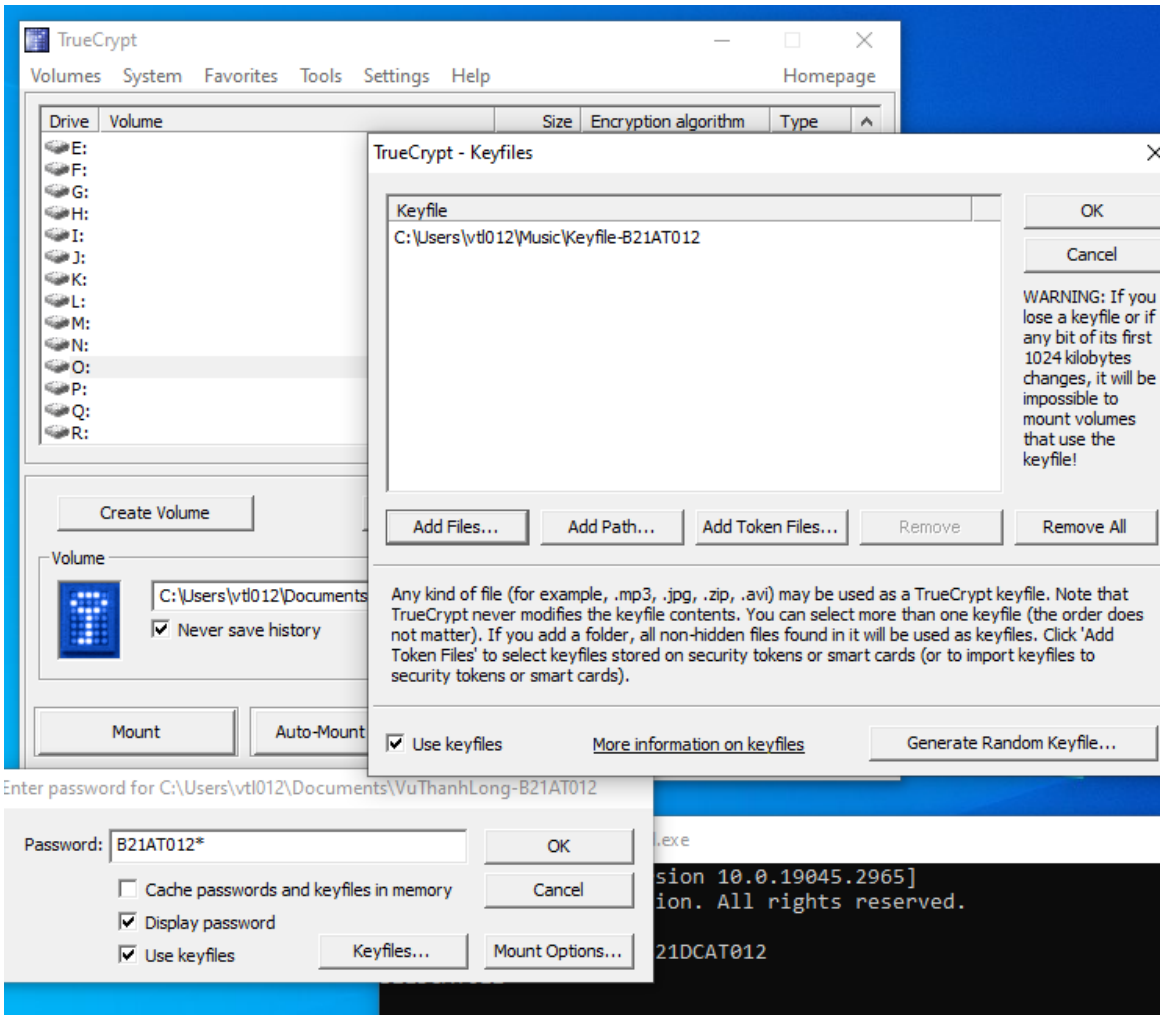
– Di chuột ngẫu nhiên để tạo khoá, chọn địa chỉ lưu tệp tin khoá. Quá trình tạo tệp tin khoá hoàn thành.



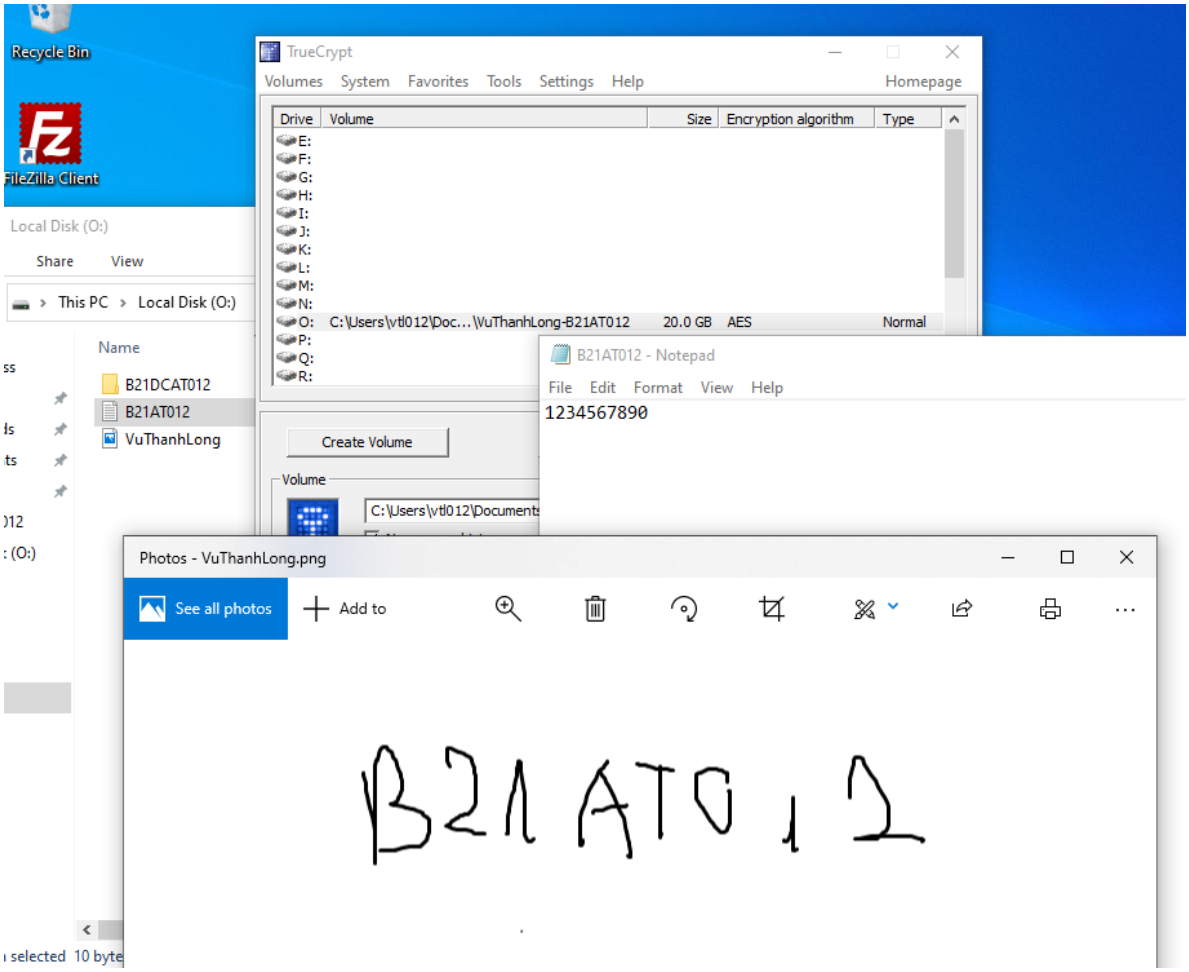
– Để cài đặt sao cho container VuThanhLong-B21AT012 sử dụng cả mật khẩu (password) và tệp tin khoá (keyfile) để xác minh, ta bấm Volume Tools -> Add/remove keyfile to/from volume.
– Trên cửa sổ mới hiển thị, ở mục Old điền mật khẩu cũ, ở mục New chọn Use keyfile rồi chọn tệp tin khoá đã tạo ở mục trước.

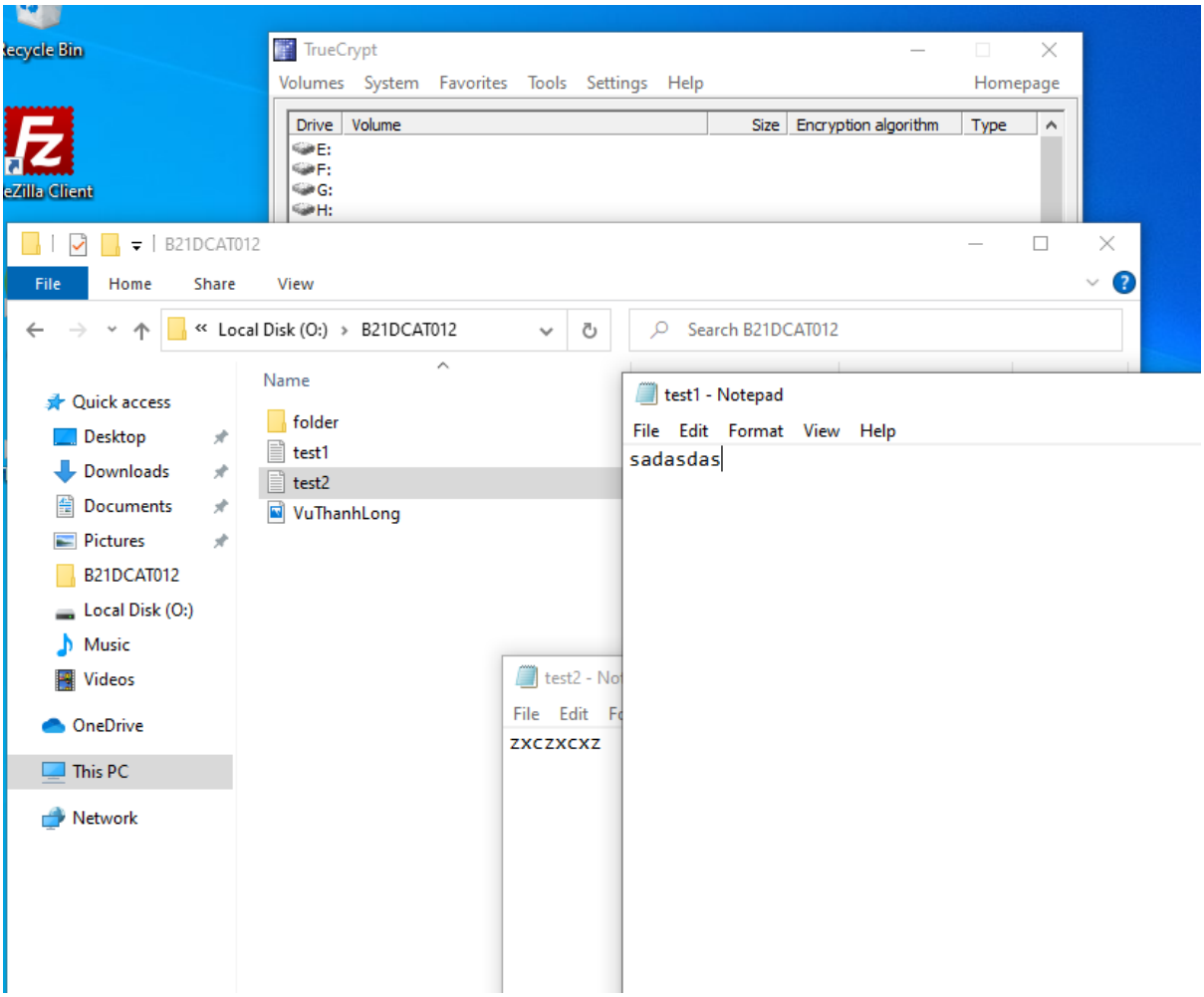


– Quá trình thêm tệp tin khoá thành công. Người dùng có thể sao lưu tệp tin khoá này sang ổ đĩa khác hoặc máy tính khác. Những lần sau, nếu muốn mở container này, người dùng cần làm những thao tác như sau:
– Mở giao diện TrueCrypt, nạp Container mã hoá và bấm Mount. Trên cửa sổ mới hiện lên, điền mật khẩu và chọn Use keyfile. Bấm nút Keyfile và chọn tệp tin khoá. Bấm OK rồi bấm Mount.



– Nếu mật khẩu và tệp tin khoá đúng, container sẽ được giải mã. Nội dung các tệp tin trong container không thay đổi.


Recycle Bin
FileZilla Client
TrueCrypt
Volumes System Favorites Tools Settings Help
Homepage
Drive Volume Size Encryption algorithm Type
O: C:\Users\vtl012\Doc...\VuThanhLong-B21AT012 20.0 GB AES Normal
Create Volume
Volume
B21AT012 - Notepad
File Edit Format View Help
1234567890
Local Disk (O:)
Share View
This PC > Local Disk (O:)
Name
B21DCAT012
B21AT012
VuThanhLong
Photos - VuThanhLong.png
See all photos
Add to
B21AT012
selected 10 byte


Recycle Bin
eZilla Client
TrueCrypt
Volumes System Favorites Tools Settings Help
Homepage
Drive Volume Size Encryption algorithm Type
E:
F:
G:
H:
B21DCAT012
File Home Share View
Local Disk (O:) › B21DCAT012
Search B21DCAT012
Quick access
Desktop
Downloads
Documents
Pictures
B21DCAT012
Local Disk (O:)
Music
Videos
OneDrive
This PC
Network
Name
folder
test1
test2
VuThanhLong
test1 - Notepad
File Edit Format View Help
sadasdas
test2 - No
File Edit
zxczxcxz