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

Tên sinh viên: Nguyễn Văn Hùng

Mã sinh viên: B22DCAT136

Nhóm lớp: 09

Giảng viên: Quản Trọng Thế

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC 1
DANH MỤC CÁC HÌNH VẼ 2
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH 3
1.1 Mục đích 3
1.2 Tìm hiểu lý thuyết 3
1.2.1 Giới thiệu 3
1.2.2 Phương pháp TruyCrypt mã hóa 3
1.3 Kết luận 3
CHƯƠNG 2. NỘI DUNG THỰC HÀNH 4
2.1 Chuẩn bị môi trường 4
2.2 Các bước thực hiện 4
2.2.1 Cài đặt TrueCrypt 4
2.2.2 Sử dụng công cụ TrueCrypt để mã hóa file 5
2.2.2.1 Tạo volume mã hóa 5
2.2.2.2 Mount volume và thêm file vào 9
2.2.3 Sử dụng công cụ TrueCrypt để mã hóa thư mục 10
2.2.4 Sao lưu khóa mã hóa của công cụ TrueCrypt 11
2.2.5 Sử dụng công cụ TrueCrypt để khôi phục file và thư mục mã hóa 13
TÀI LIỆU THAM KHẢO 15

DANH MỤC CÁC HÌNH VẼ

Hình 1 . Tải và cài đặt TrueCrypt 4
Hình 2 . Giao diện TruyCrypt 5
Hình 3 . Lựa chọn tạo Volume 6
Hình 4 . Chọn Volume Type 7
Hình 5 . Chọn Volume Location 7
Hình 6 . Tiếp tục lựa chọn cấu hình 8
Hình 7 . Tạo Volume thành công 8
Hình 8 . Mount Volume 9
Hình 9 . Mở ổ đĩa trong File Explorer 10
Hình 10 . Copy các file vào ổ đĩa mã hóa 10
Hình 11 . Dismount Volume 10
Hình 12 . Chọn Volume Location 11
Hình 13 . Copy thư mục 11
Hình 14 . Chọn Backup Volume Header 12
Hình 15 . Các lựa chọn để sao lưu 12
Hình 16 . Đặt tên file và cửa sổ Random Pool Enrichment 13
Hình 17 . Cửa sổ thông báo sao lưu thành công 13
Hình 18 . Khôi phục file và thư mục mã hóa 14

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 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.

1.2 Tìm hiểu lý thuyết

1.2.1 Giới thiệu

TrueCrypt là một phần mềm mã hóa dữ liệu mã nguồn mở được sử dụng để tạo và quản lý các ổ đĩa ảo và thư mục mã hóa trên hệ điều hành Windows, macOS và Linux.

Công cụ này cho phép người dùng:

- Tạo một volume mã hóa (ổ đĩa ảo) có thể gắn vào hệ thống như một ổ đĩa thật.
- Mã hóa toàn bộ phân vùng ổ cứng hoặc thiết bị lưu trữ ngoài như USB.
- Hỗ trợ tạo Hidden Volume (ổ ẩn) để bảo vệ dữ liệu trong trường hợp bị ép buộc phải tiết lộ mật khẩu.
- Mã hóa theo thời gian thực: dữ liệu được mã hóa tự động khi ghi và giải mã khi đọc mà người dùng không cần thao tác gì thêm.

1.2.2 Phương pháp TruyCrypt mã hóa

TrueCrypt tạo ra một đĩa mã hóa ảo (encryption volume), gắn trên ổ cứng giống như một đĩa thật. Nghĩa là dữ liệu tự động được mã hóa ngay khi được ghi xuống đĩa cứng hoặc ngay khi dữ liệu được nạp lên (on-the-fly encryption). Toàn bộ dữ liệu này đều không thể tiếp cận được nếu bạn không cung cấp đúng mã khóa mà mình đã chọn, có ba hình thức là mật khẩu (password), tập tin có chứa khóa (keyfile) và khóa mã hóa (encryption key).

Dữ liệu có thể được copy, xóa hay di chuyển từ một ổ đĩa mã hóa của TrueCrypt sang một ổ đĩa bình thường bất kỳ trên Windows (và ngược lại), nhưng bạn chỉ có thể truy cập vào chúng khi có mật khẩu mở mã hóa chính xác.

TrueCrypt áp dụng các thuật toán mã hóa mạnh để đảm bảo tính bảo mật cao cho dữ liệu: AES (Advanced Encryption Standard), Serpent, Twofish

Ngoài ra, TrueCrypt còn hỗ trợ kết hợp nhiều thuật toán theo chuỗi để tăng cường độ an toàn (ví dụ: AES–Twofish–Serpent).

1.3 Kết luận

TrueCrypt là phần mềm cung cấp giải pháp mã hóa mạnh mẽ với khả năng kiểm soát hoàn toàn của người dùng, phù hợp với việc bảo vệ các file và thư mục quan trọng.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

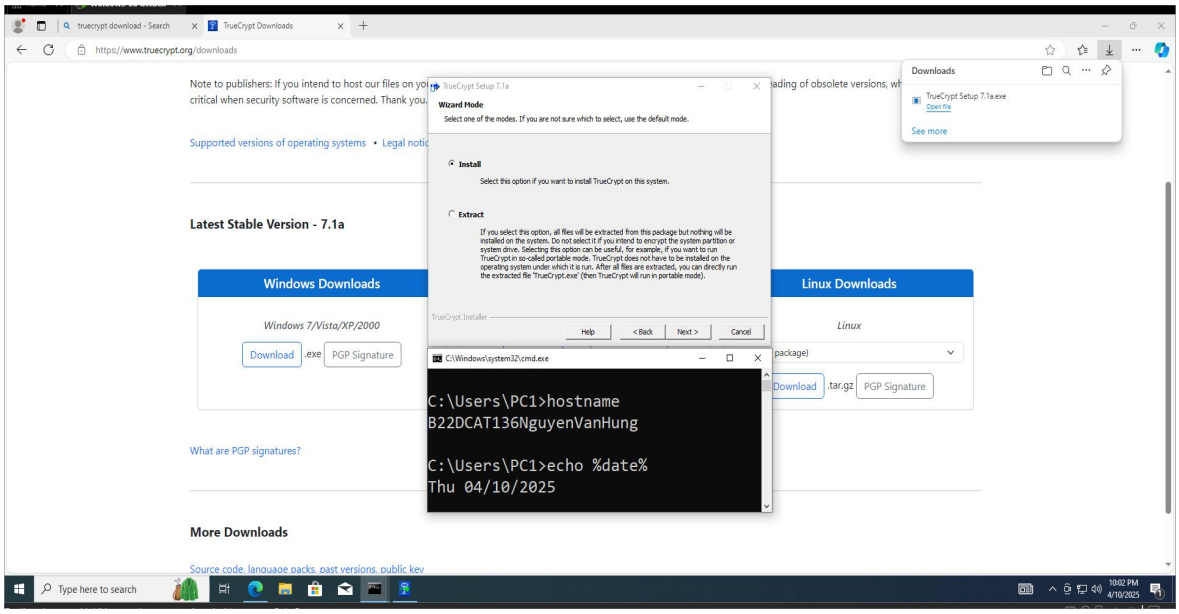
2.1 Chuẩn bị môi trường

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

2.2 Các bước thực hiện

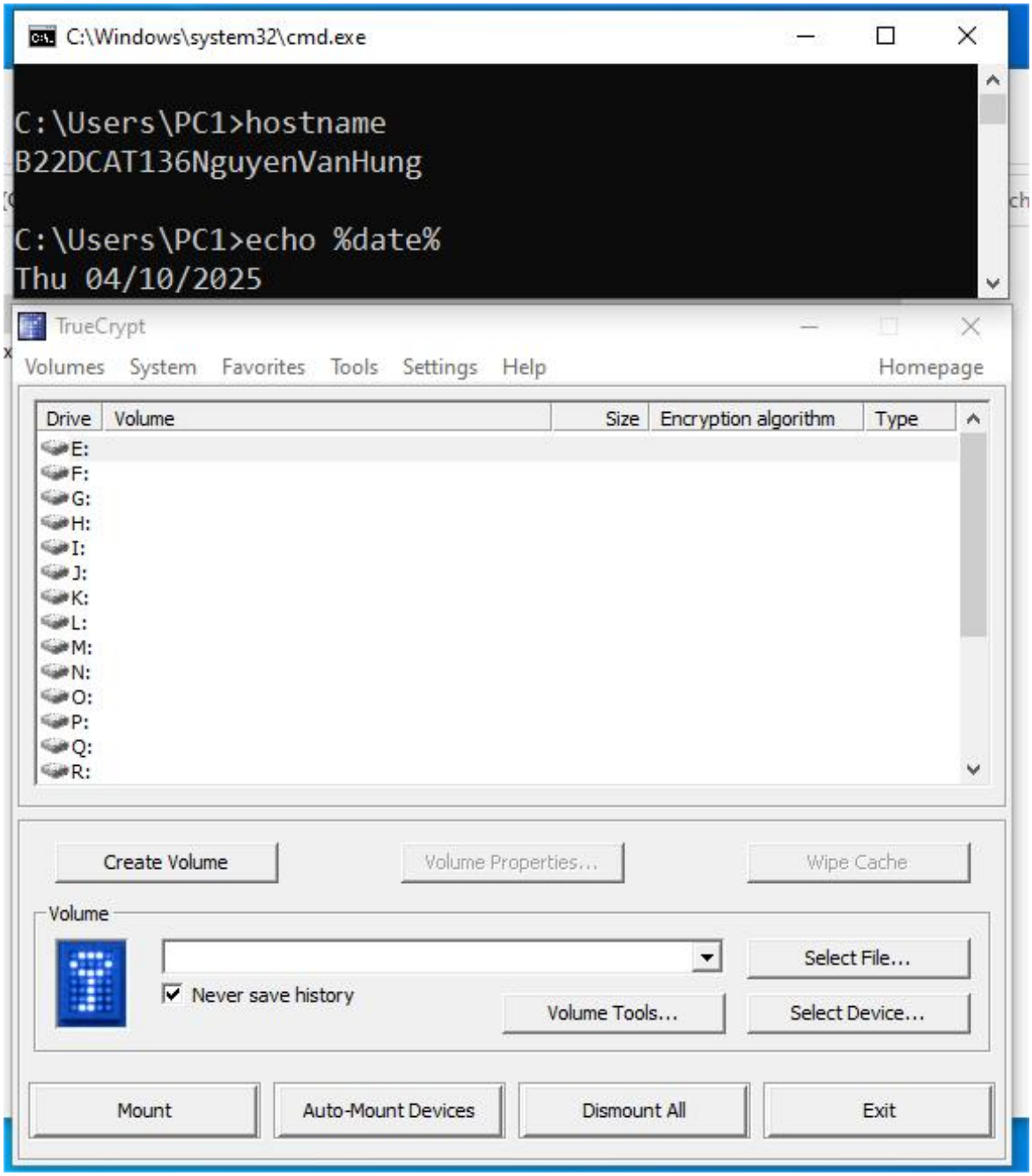
2.2.1 Cài đặt TrueCrypt

- Tải và cài đặt TrueCrypt:



Hình 1. Tải và cài đặt TrueCrypt

- Giao diện công cụ TrueCrypt:



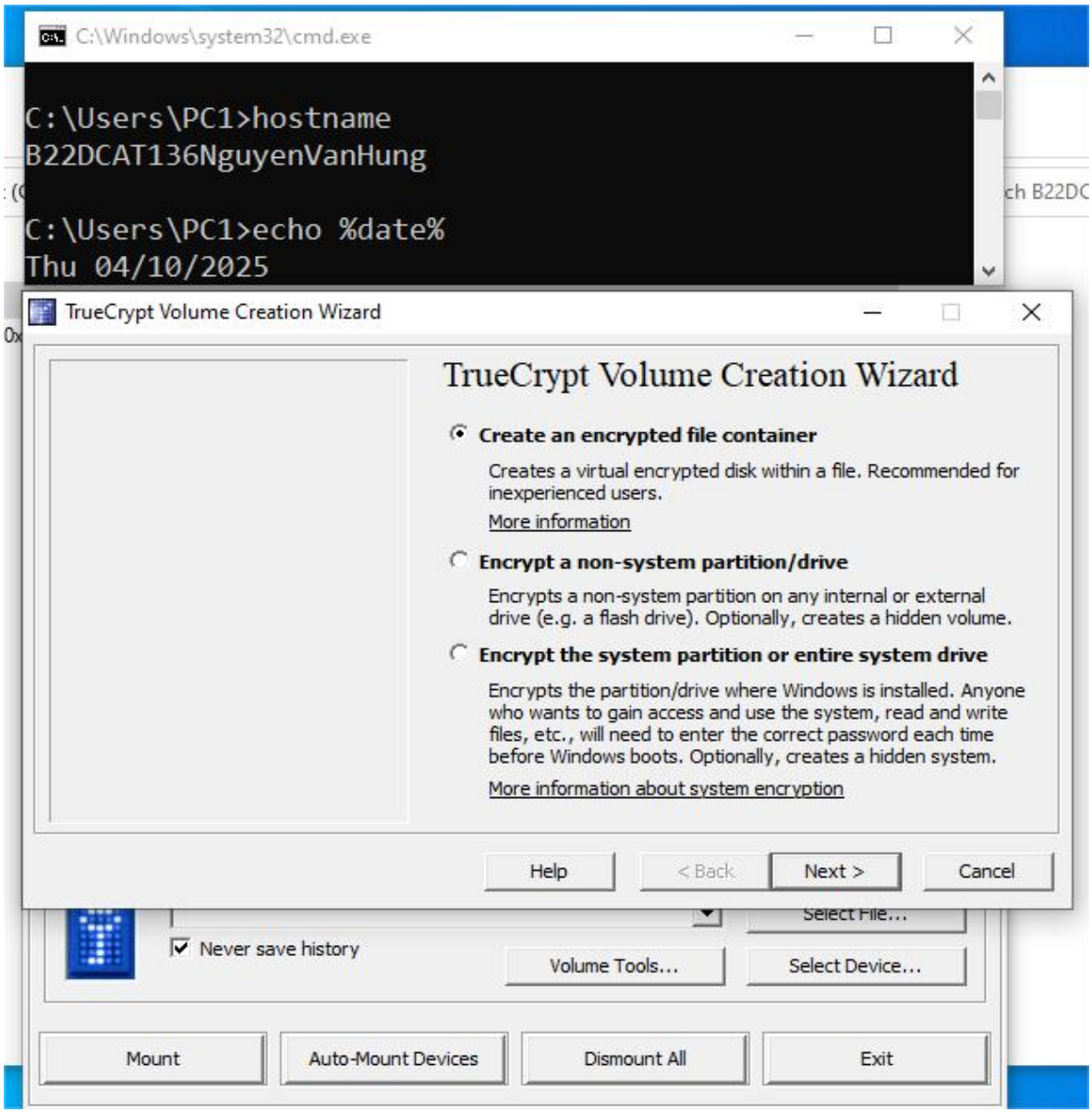
Hình 2. Giao diện TruyCrypt

2.2.2 Sử dụng công cụ TrueCrypt để mã hóa file

2.2.2.1 Tạo volume mã hóa

- Chạy TrueCrypt dưới quyền Administrator, chọn **Create Volume**, xuất hiện 3 lựa chọn chính khi tạo volume:
    - Create an encrypted file container: Tạo mọt file mã hóa giống như một ổ đĩa ảo, chứa các file/thư mục bên trong.
    - Encrypt a non-system partition/drive: Mã hóa nguyên phân vùng ổ đĩa thật.

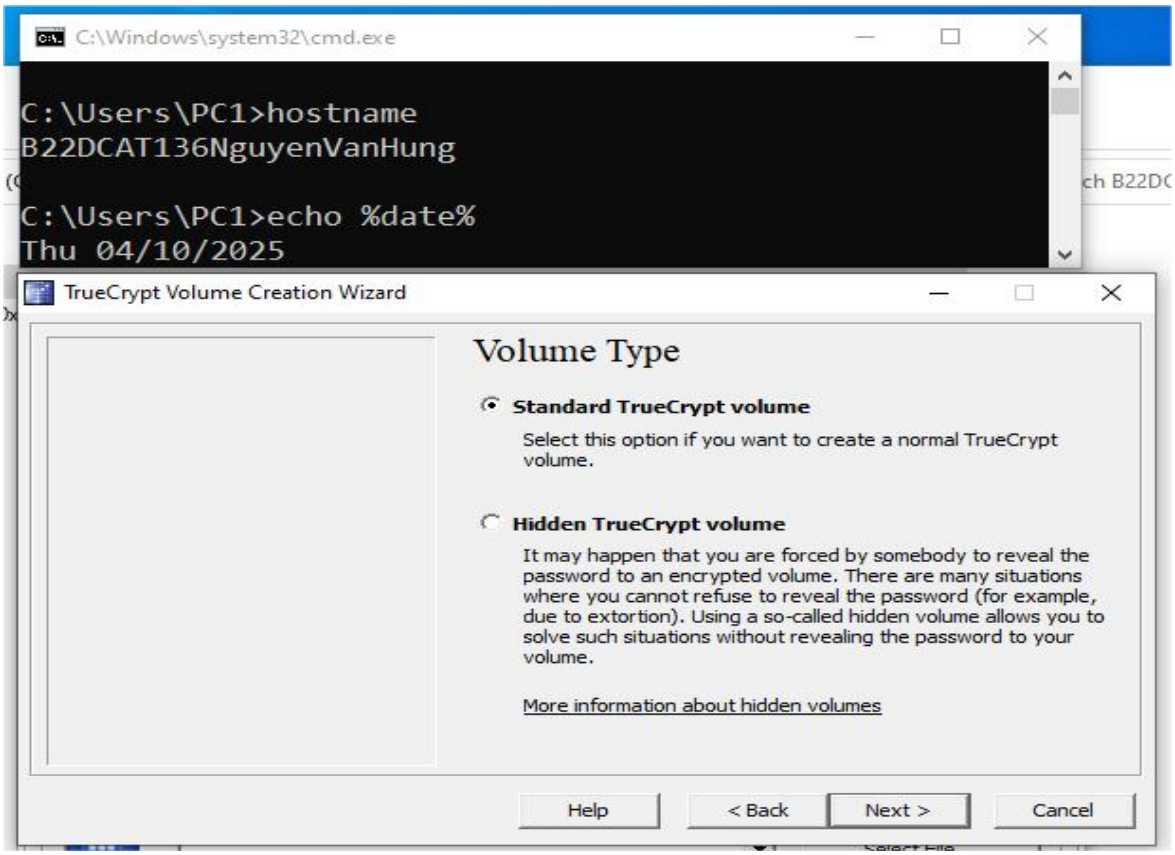
- Encrypt the system partition or entire system drive: Mã hóa toàn bộ ổ đĩa chạy hệ điều hành.
- Chọn: **Create an encrypted file container** phù hợp cho bài thực hành.



Hình 3. Lựa chọn tạo Volume

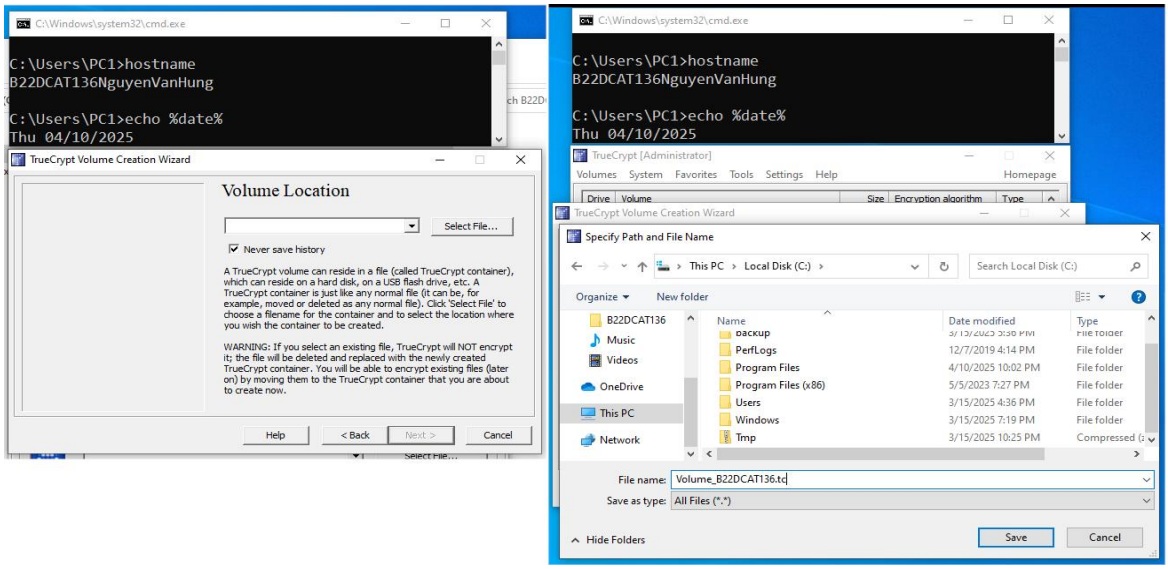
- Giao diện chọn **Volume Type**, có 2 lựa chọn:
- **Standard TrueCrypt Volume**: Phù hợp cho bài thực hành này.
  - Đây là volume bình thường.
  - Khi mount vào, nhập mật khẩu là mở ra toàn bộ nội dung.
- **Hidden TrueCrypt Volume**:
  - Đây là một volume "ẩn" nằm bên trong một volume khác (outer volume).
  - Dùng để che giấu thông tin cực kỳ nhạy cảm, người ngoài sẽ không biết có tồn tại volume ẩn nếu chỉ thấy outer volume.

- Khi mount: nếu bạn nhập mật khẩu của outer volume, nó mở outer (bình thường). Nếu bạn nhập mật khẩu khác (của volume ẩn), nó mở phần ẩn bên trong.



Hình 4. Chọn Volume Type

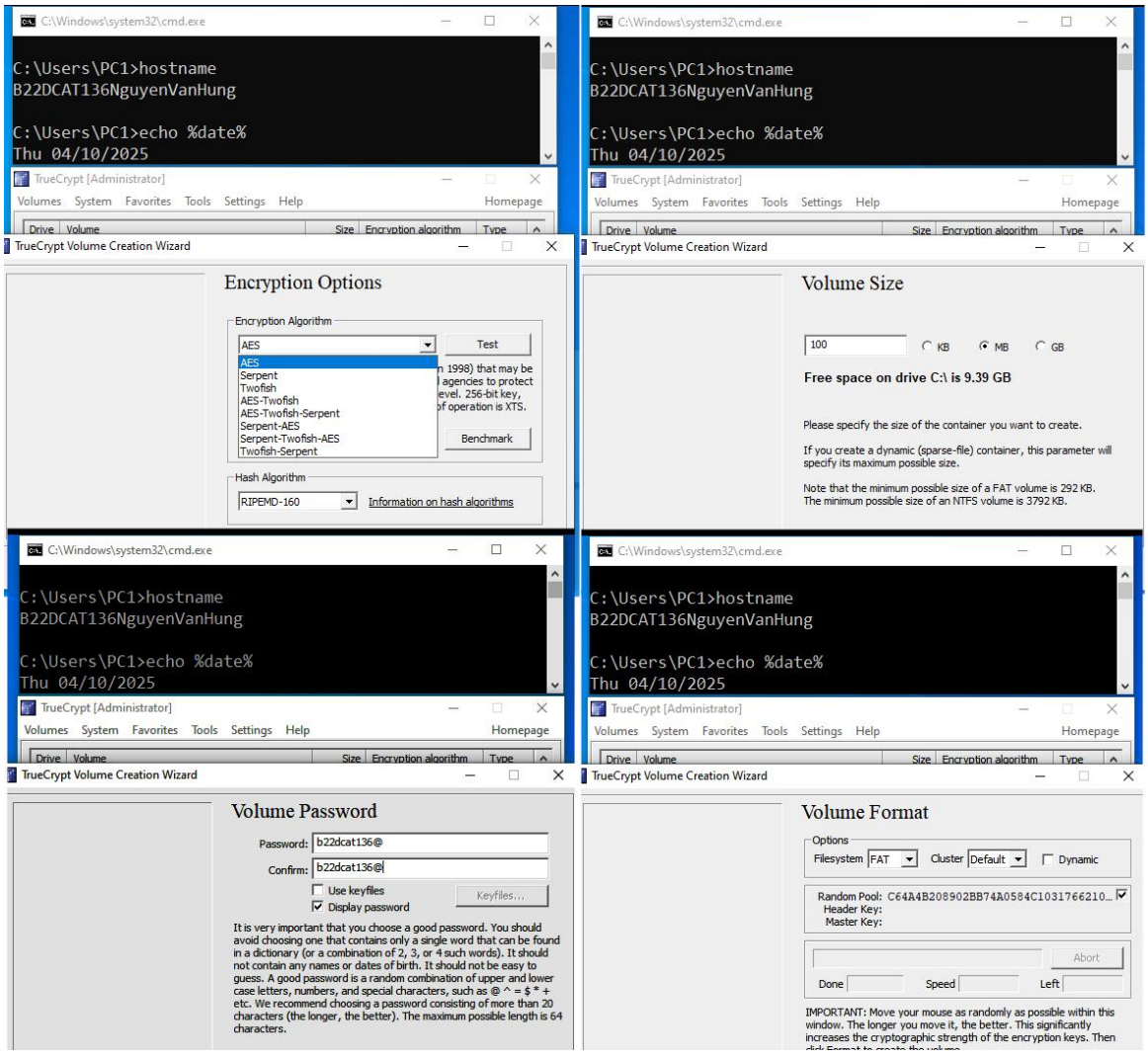
- Chọn nơi lưu volume: **Volume_B22DCAT136.tc**



Hình 5. Chọn Volume Location

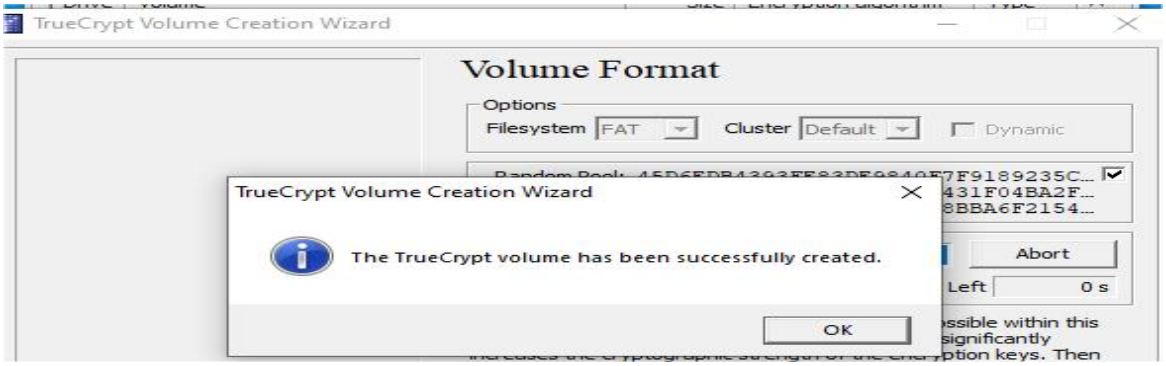
- Tiếp tục với các bước:
  - Chọn thuật toán: AES (mặc định)

- Dung lượng volume: 100 MB
- Nhập mật khẩu
- Chọn định dạng hệ thống file (FAT)
- Di chuyển chuột ngẫu nhiên để tạo entropy tăng tính bảo mật
- **Format**



Hình 6. Tiếp tục lựa chọn cấu hình

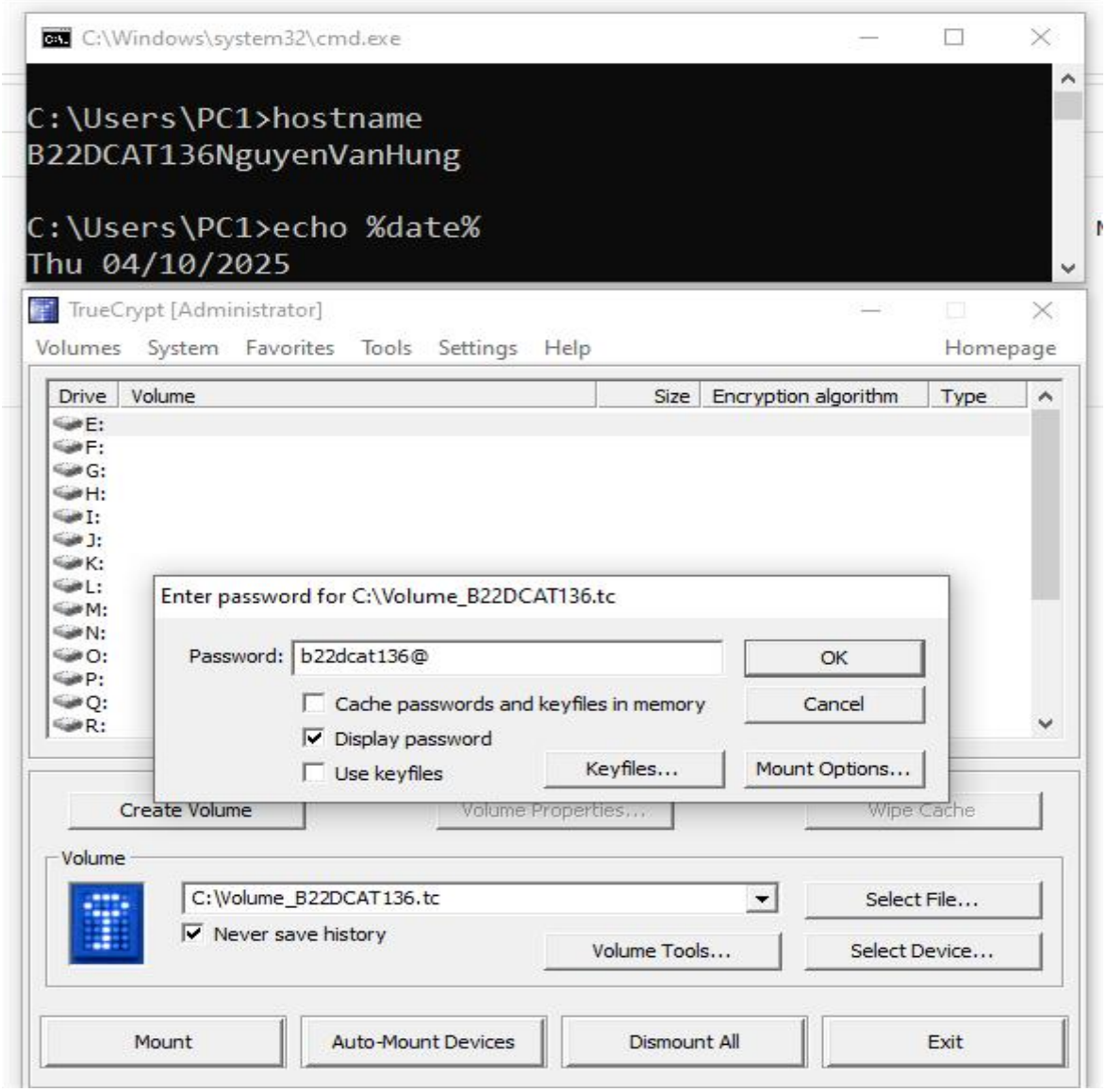
- Tạo volume thành công:



Hình 7. Tạo Volume thành công

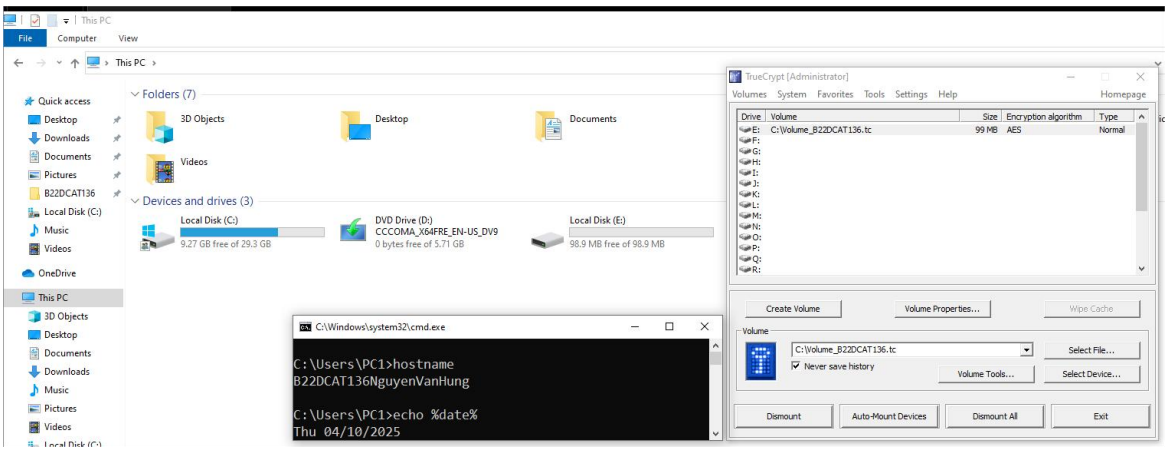
2.2.2.2 Mount volume và thêm file vào

- Trở về giao diện chính của TrueCrypt, chọn một ổ đĩa: E
- Chọn **Select File**, tìm đến volume vừa tạo: **Volume_B22DCAT136.tc**
- Chọn **Mount** và nhập mật khẩu:



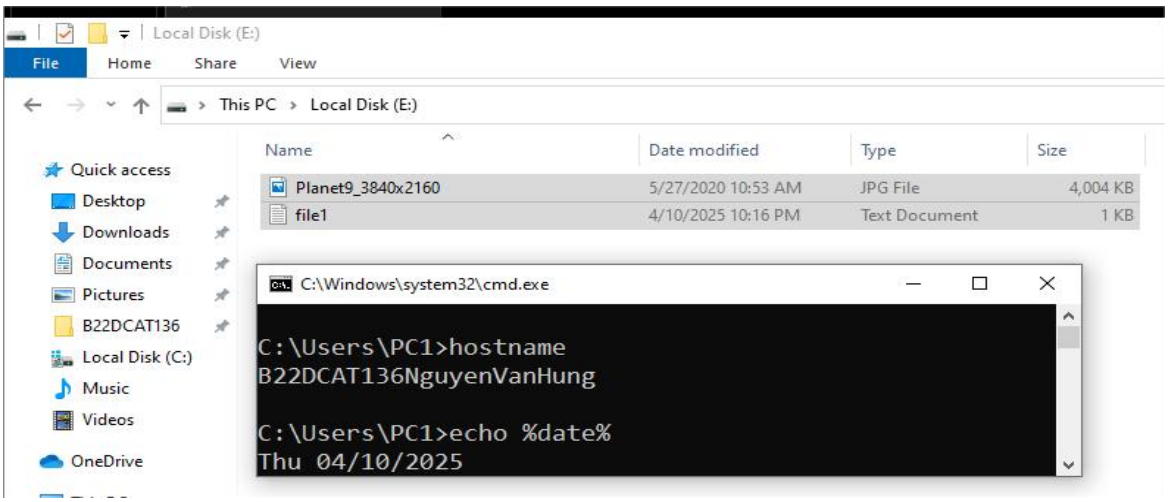
Hình 8. Mount Volume

- Mở File Explorer thấy được ổ đĩa E:



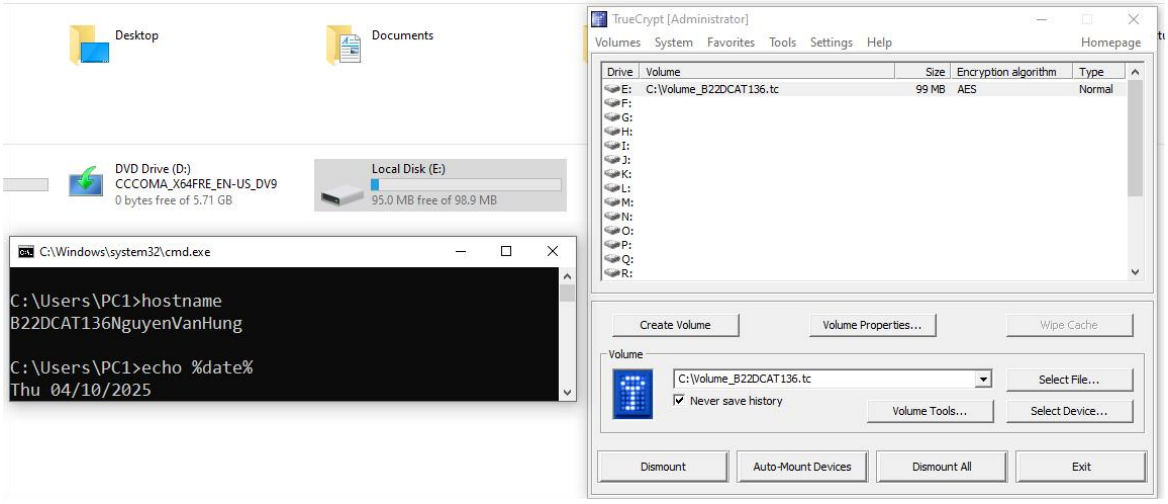
Hình 9. Mở ổ đĩa trong File Explorer

- Copy các file vào ổ đĩa E, các file đã nằm trong ổ đĩa mã hóa



Hình 10. Copy các file vào ổ đĩa mã hóa

- Trở lại giao diện TruyCrypt, chọn **Dismount**

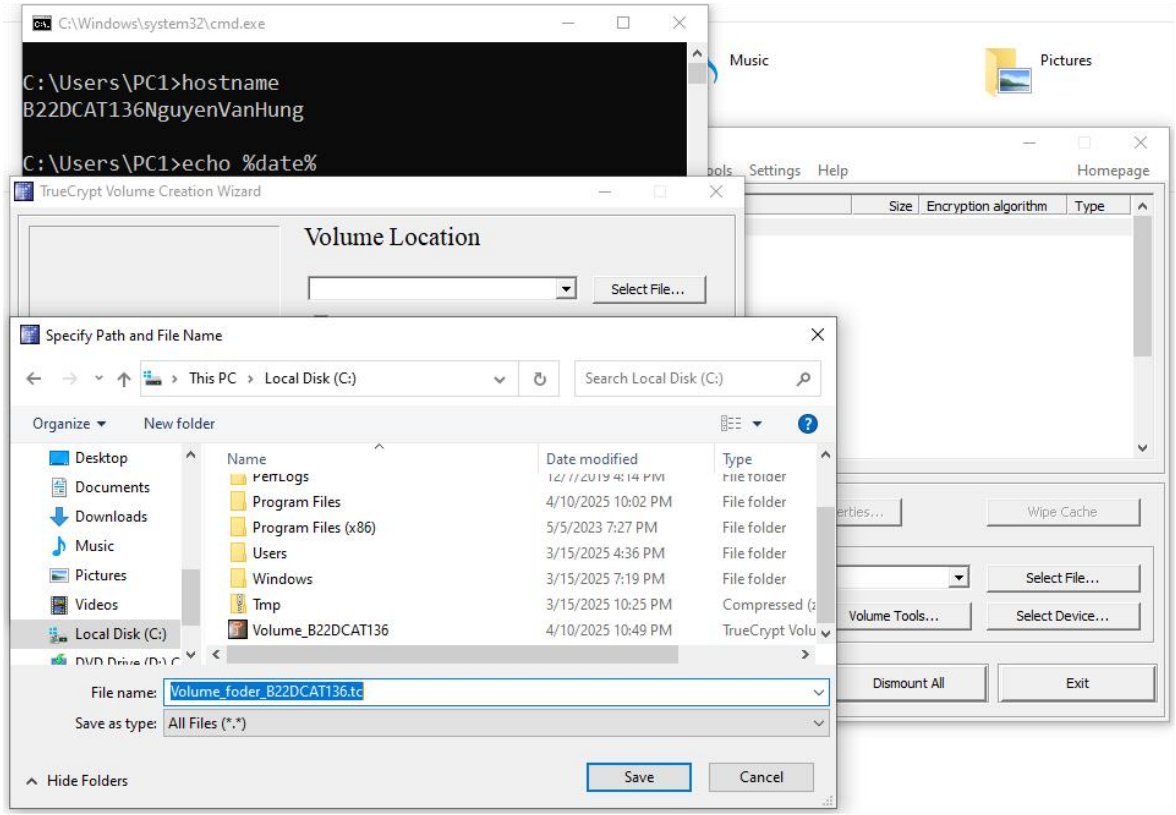


Hình 11. Dismount Volume

- Ta được kết quả thành công mã hóa file

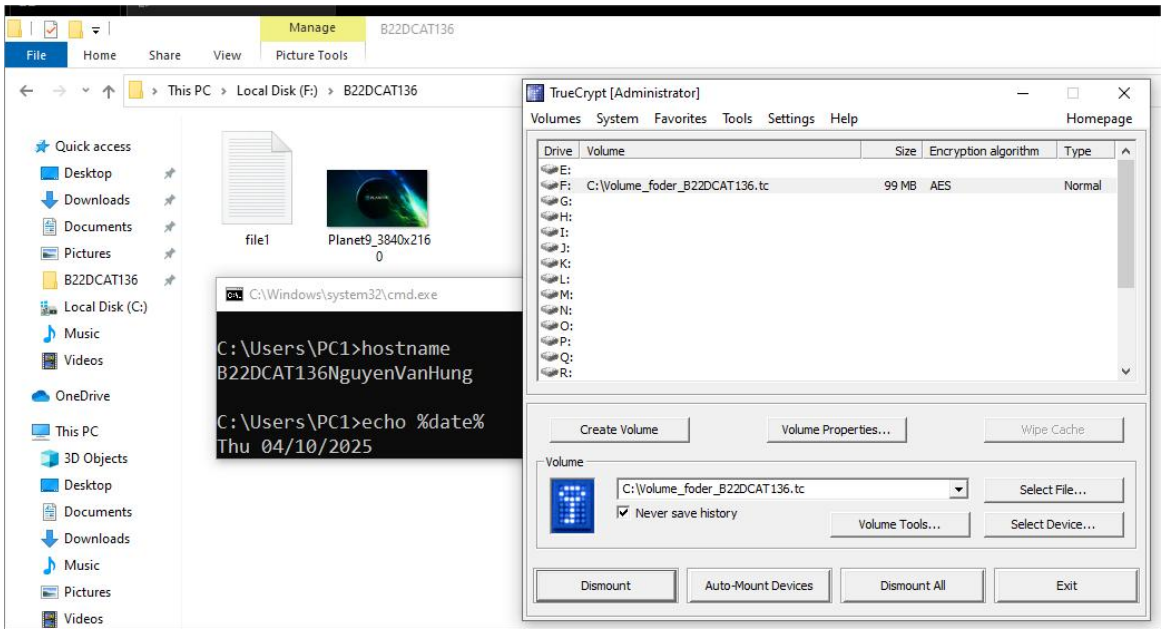
2.2.3 Sử dụng công cụ TrueCrypt để mã hóa thư mục

- Với mã hóa thư mục, làm tương tự như các bước mã hóa file ở trên tạo volume mới: **Volume_folder_B22DCAT136.ct**



Hình 12. Chọn Volume Location

- Mount và copy thư mục B22DCAT136 vào Volume_folder_B22DCAT136.tc, trong thư mục chứa các file khác nhau:

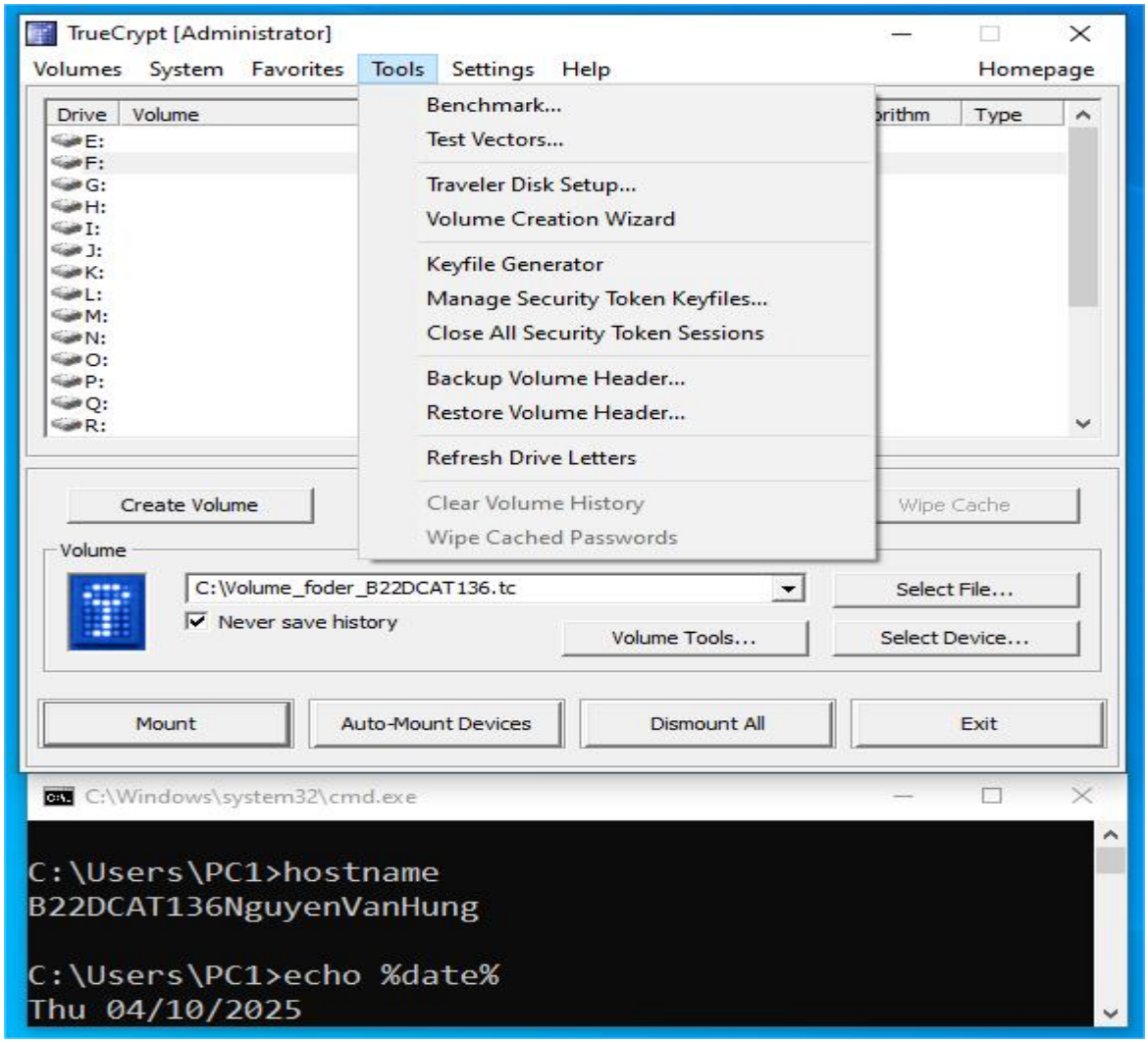


Hình 13. Copy thư mục

- Thành công mã hóa thư mục.

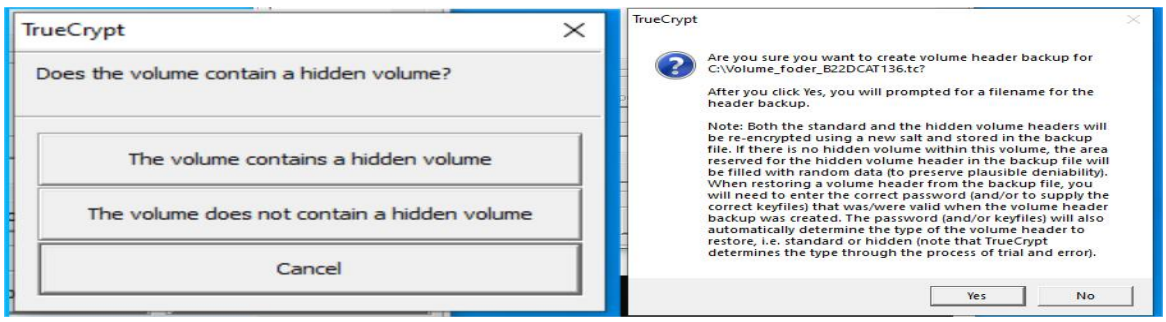
2.2.4 Sao lưu khóa mã hóa của công cụ TrueCrypt

- Mở TrueCrypt, chọn **Select File**: chọn Volume cần sao lưu khóa mã hóa
- chọn **Tools → Backup Volume Header**
    - Chỉ sao lưu phần đầu (header) của volume chứa thông tin mã hóa quan trọng: master key, salt, các thông số mã hóa
- Nhập mật khẩu của Volume đã chọn khi được yêu cầu



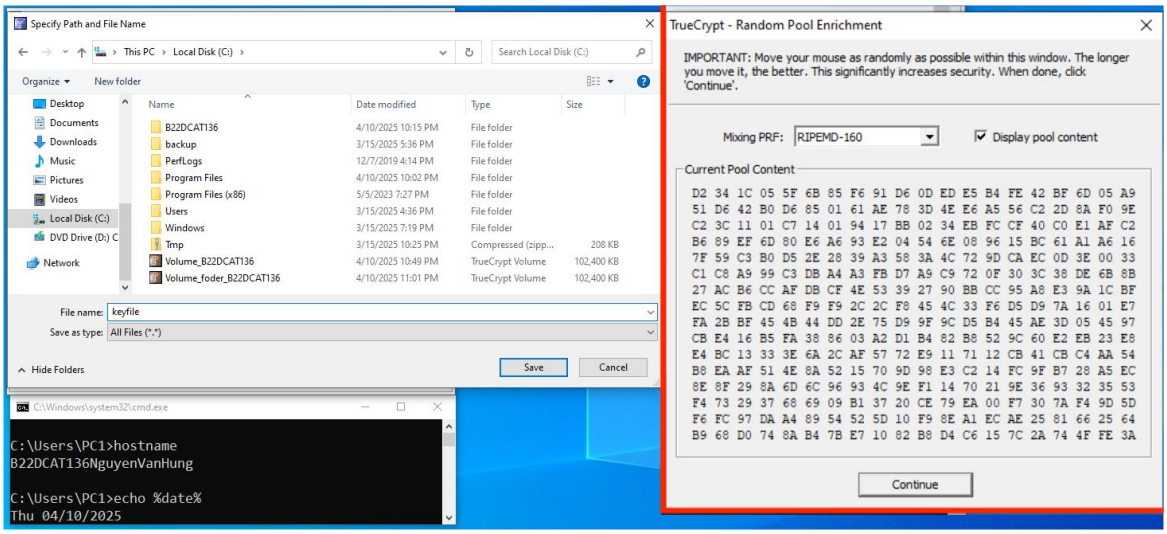
Hình 14. Chọn Backup Volume Header

- Chọn **The volume does not contain a hidden volume** phù hợp cho bài thực hành
- Chọn **Yes**



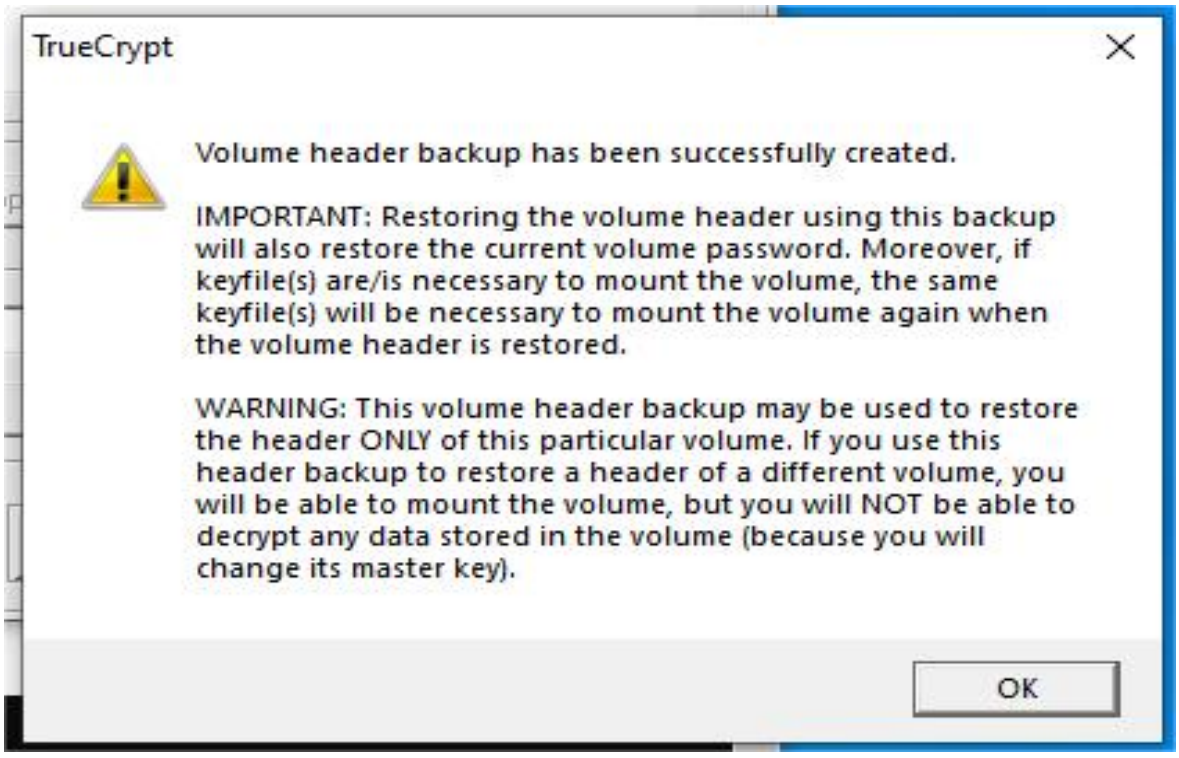
Hình 15. Các lựa chọn để sao lưu

- Đặt tên file: **keyfile**
- Cửa sổ Random Pool xuất hiện, di chuyển chuột ngẫu nhiên để tạo entropy mạnh hơn cho mã hóa, sau đó nhấn **Continue**



Hình 16. Đặt tên file và cửa sổ Random Pool Enrichment

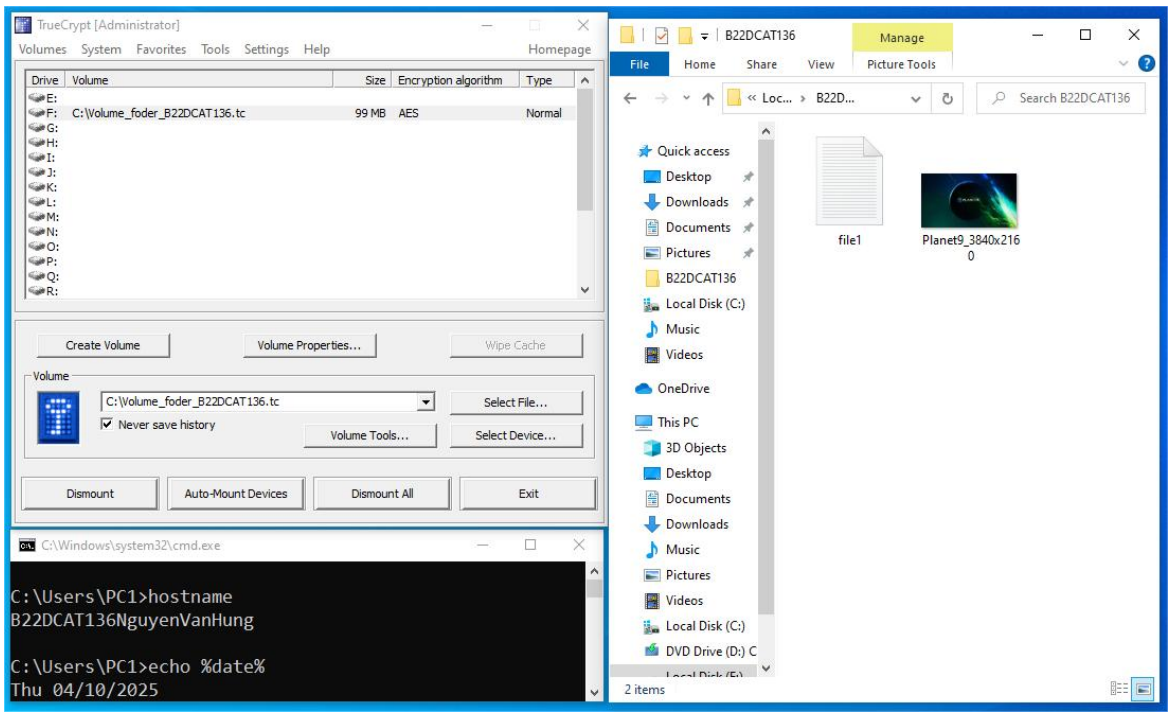
- Sao lưu thành công



Hình 17. Cửa sổ thông báo sao lưu thành công

2.2.5 Sử dụng công cụ TrueCrypt để khôi phục file và thư mục mã hóa

- Trong TrueCrypt, chọn ổ đĩa trống
- Chọn **Select File,** chọn volume: **Volume_folder_B22DCAT136.ct**
- Chọn **Mount** và nhập mật khẩu
- Truy cập ổ đĩa trong File Explorer để xem/copy các file đã mã hóa



Hình 18. Khôi phục file và thư mục mã hóa

TÀI LIỆU THAM KHẢO

[1] https://quantrimang.com/lang-cong-nghe/huong-dan-su-dung-truecrypt-de-ma-hoa-nhung-tai-lieu-nhay-cam-83755

[2] https://khophanmem.vn/truecrypt/#:~:text=TrueCrypt%20l%C3%A0%20m%E1%BB%99t%20c%C3%B4ng%20c%E1%BB%A5,d%E1%BB%AF%20li%E1%BB%87u%20%C4%91%C6%B0%E1%BB%A3c%20n%E1%BA%A1p%20l%C3%AAn.