Báo cáo bài thực hành số 13

Môn học

**Thực tập cơ sở**

Giảng viên : Hoàng Xuân Dậu

Họ tên : Nguyễn Minh Phương

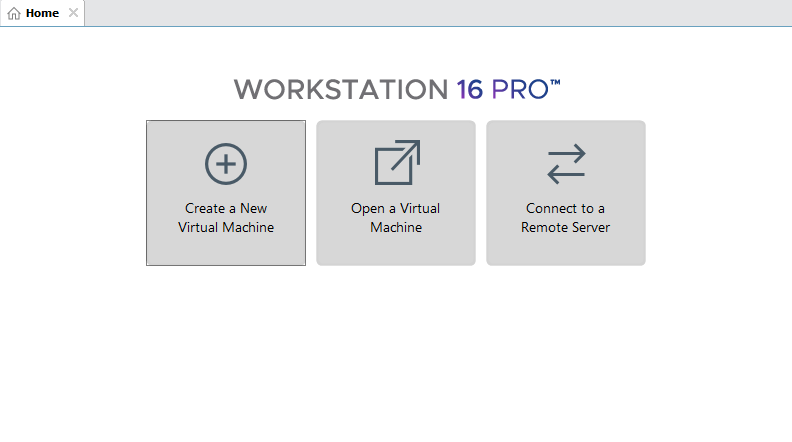
Mã SV: B19DCAT141

**1 Lý thuyết**

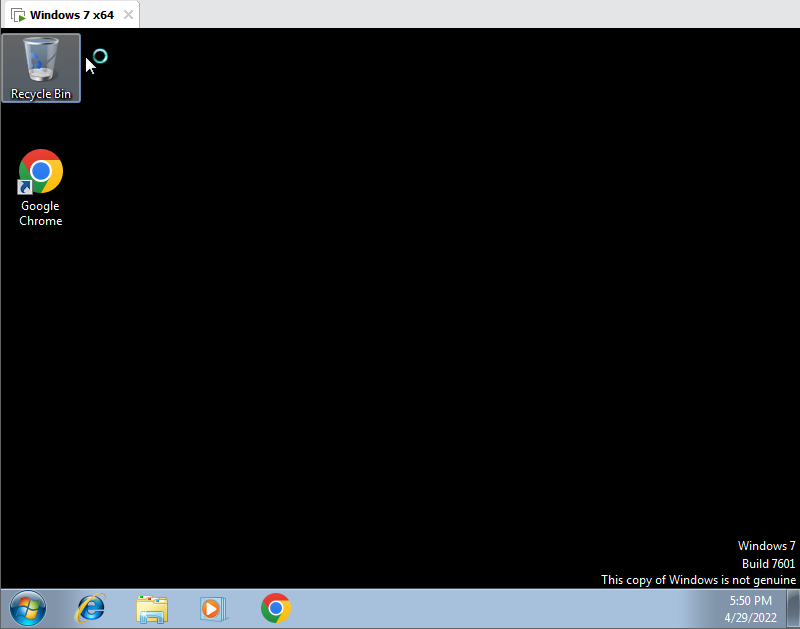
* Công cụ TrueCrypt:
  + TrueCrypt bảo vệ dữ liệu khỏi những truy cập không mong muốn bằng cách khóa chúng bằng một mật khẩu tạo ra.
  + TrueCrypt sử dụng việc mã hóa để bảo vệ thông tin.
  + Không chỉ mã hóa một số tệp riêng biệt, TrueCrypt tạo ra một vùng bảo vệ, gọi là vùng mã hóa, trên máy tính, có thể lưu trữ các tệp của mình một cách an toàn bên trong vùng mã hóa này.
  + TrueCrypt cung cấp tính năng tạo vùng mã hóa chuẩn và vùng mã hóa ẩn.
  + Trong trường hợp bị bắt buộc phải mở vùng mã hóa TrueCrypt, vùng mã hóa ẩn sẽ là cứu cánh cho 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 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 bằng một trong ba hình thức là mật khẩu (password) 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.

**2 Thực hiện**

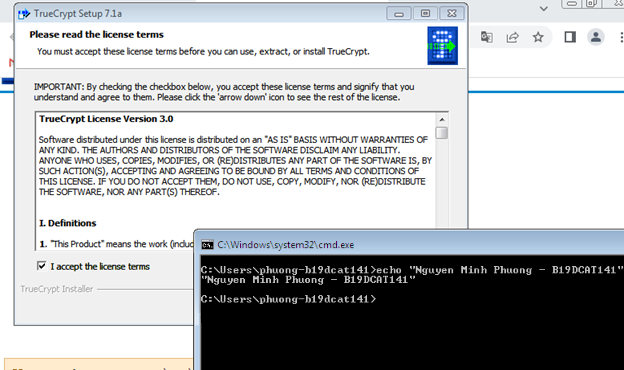
Cài đặt công cụ ảo hóa

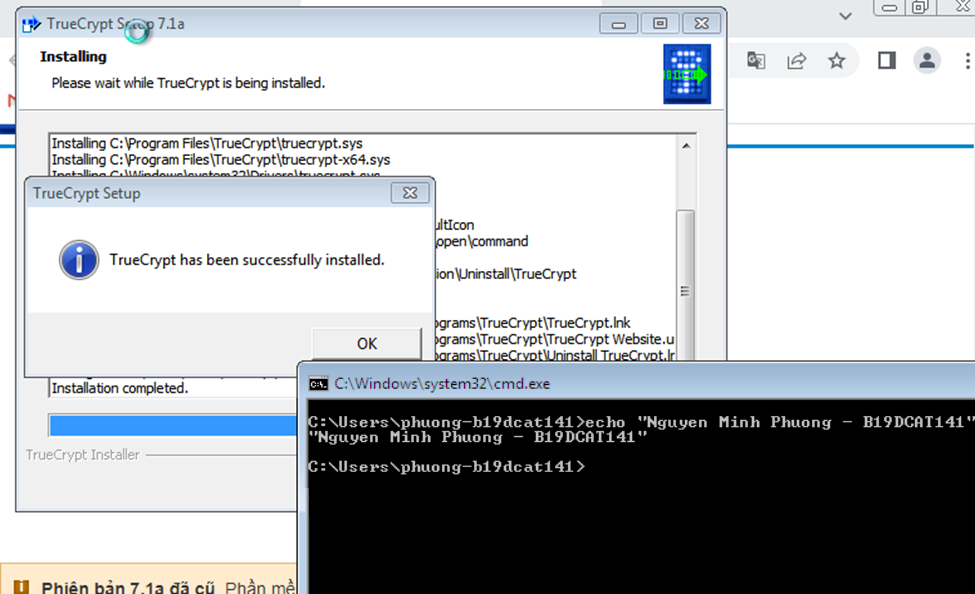


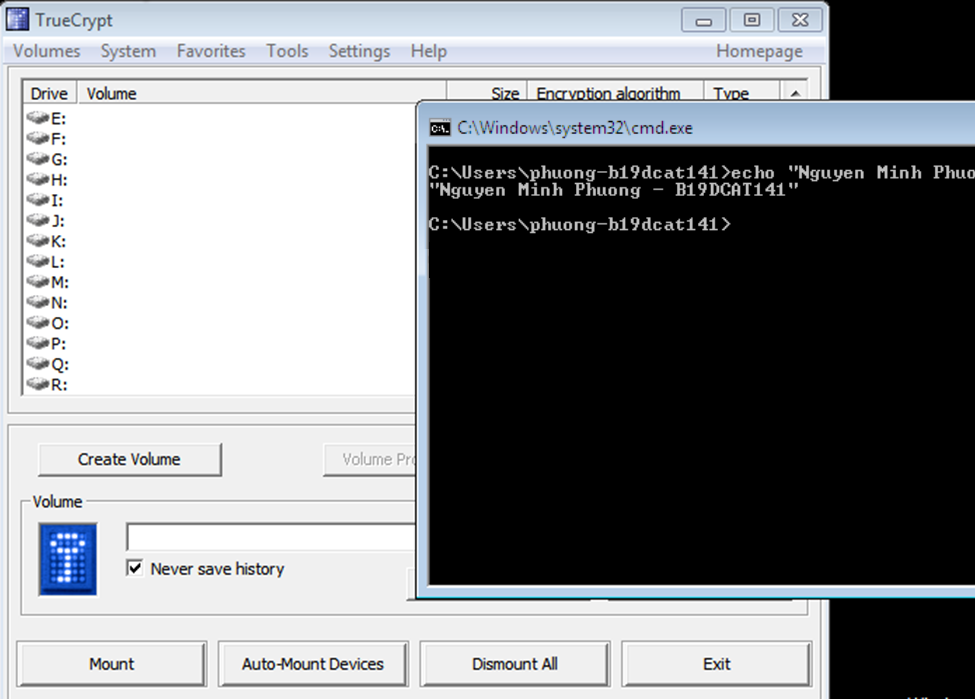
Cài đặt máy ảo chạy hệ điều hành Windows



Cài đặt TrueCrypt trên hệ điều hành windows





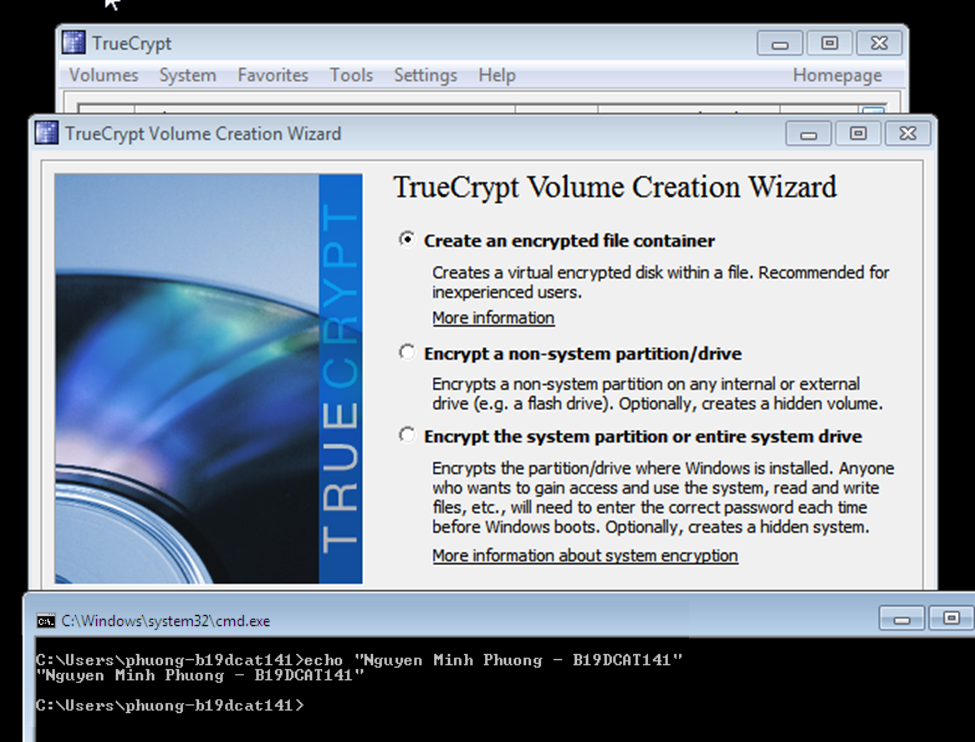


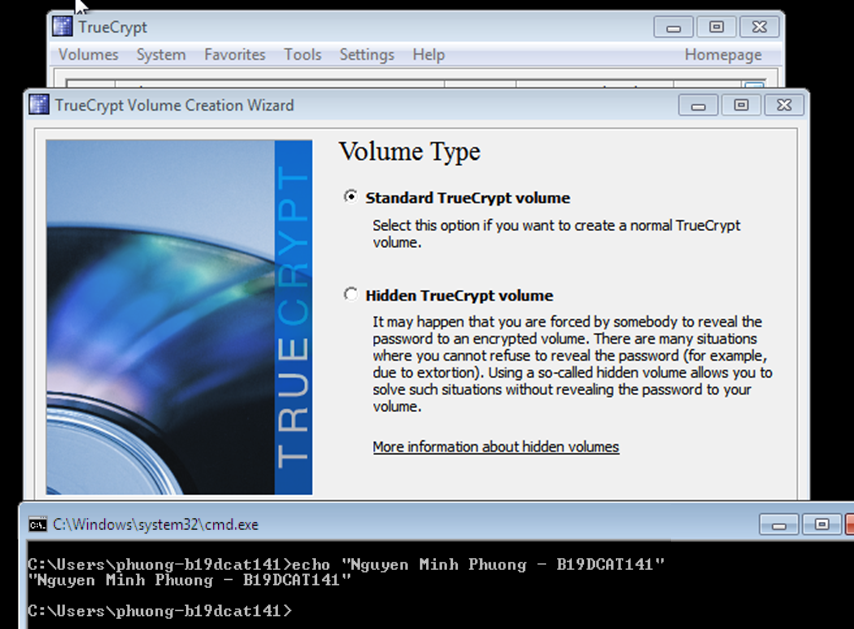
**2.2.2 Nội dung thử nghiệm**

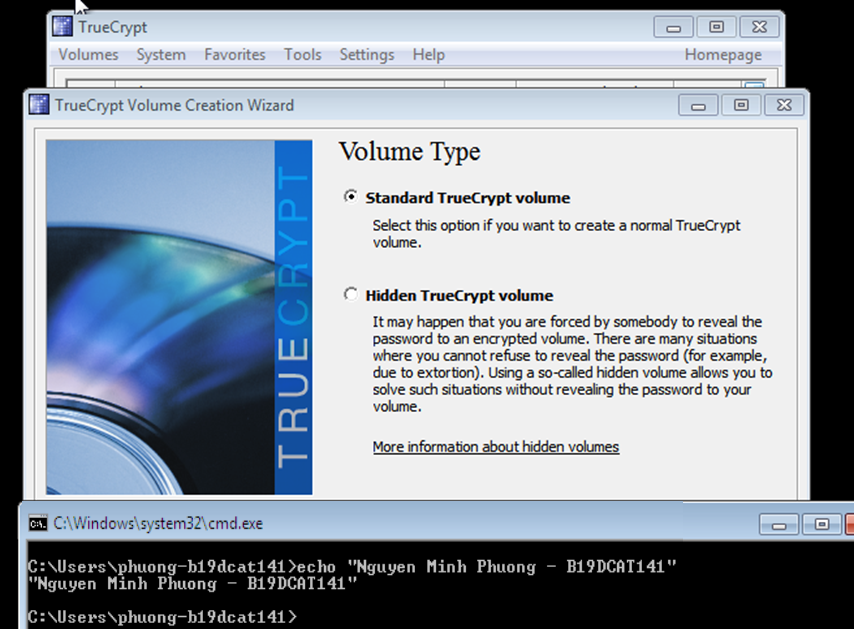
Sử dụng công cụ TrueCrypt để hóa mã file. Yêu cầu thực hiện trên ít nhất 2 loại file bao gồm: file văn bản và file đa phương tiện (định dạng ảnh, video, hoặc âm thanh)

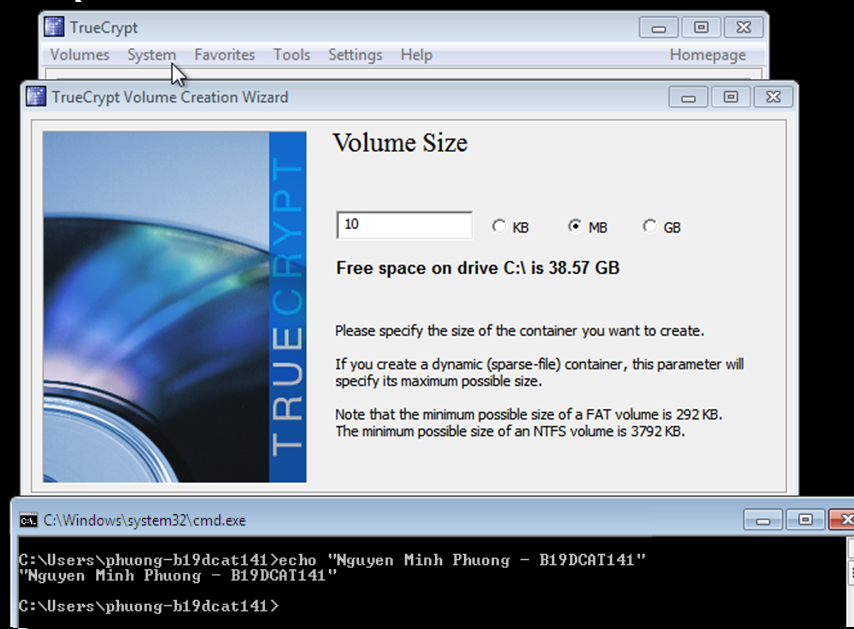
Tạo vùng mã hóa chuẩn

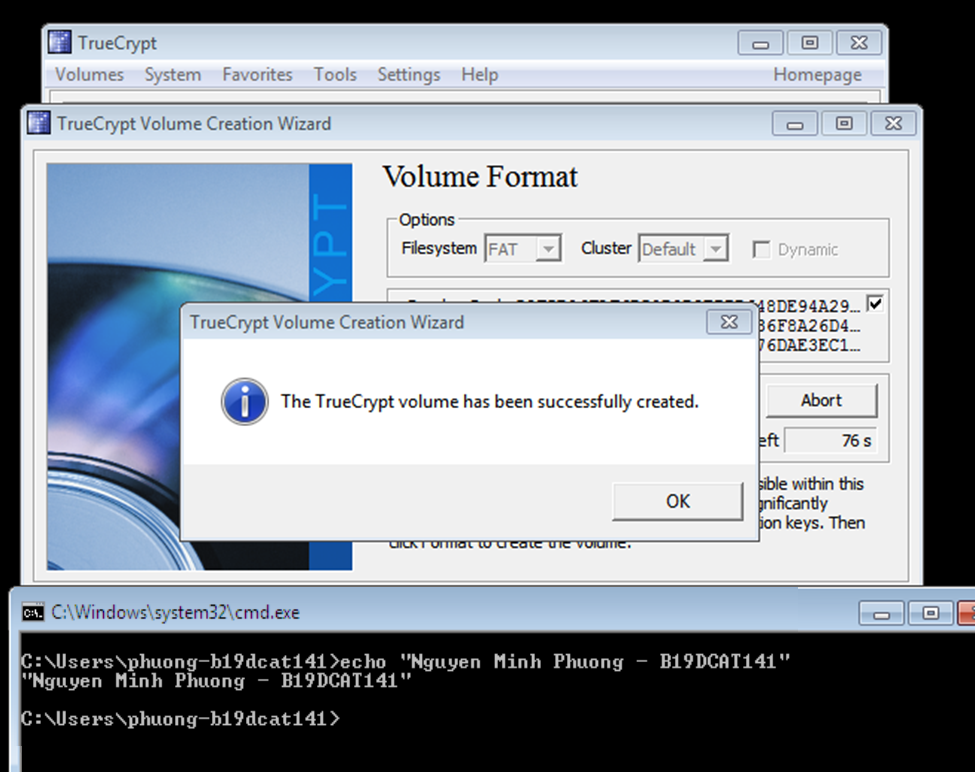
- Bấm Create Volume, chọn Tạo vùng mã hóa dạng tệp

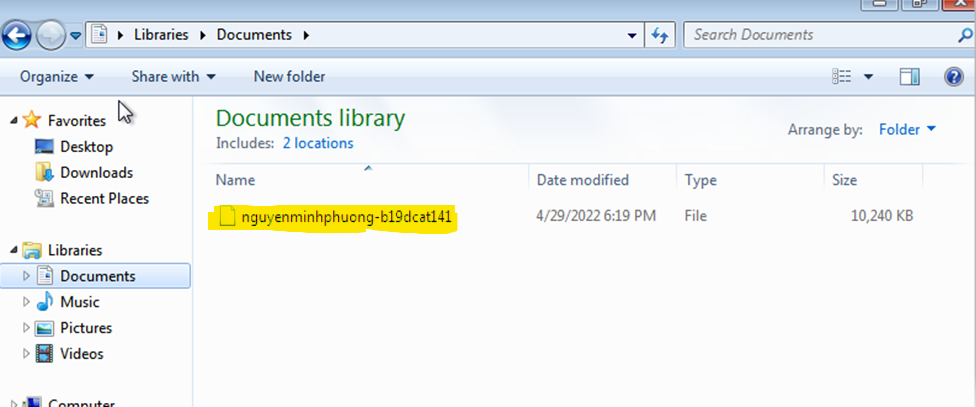






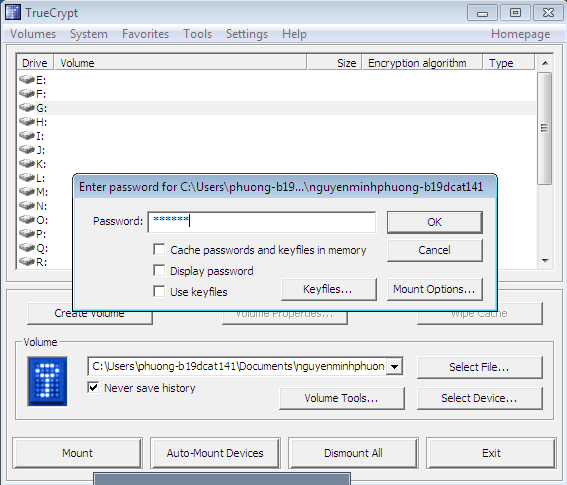




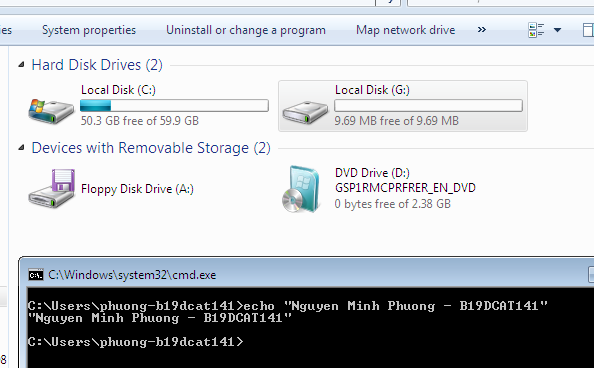


Gắn vùng mã hóa chuẩn

- Select file, chọn file vùng mã hóa vừa tạo, ấn Mount, nhập mật khẩu

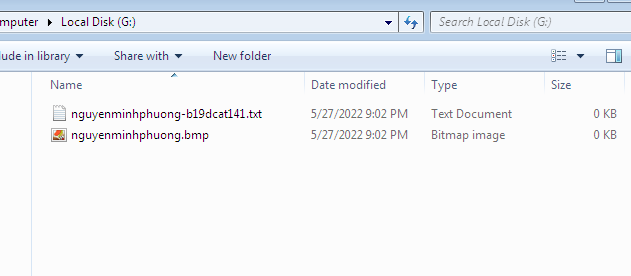


- Vùng mã hóa được gắn vào ổ đĩa ảo G:. Ổ đĩa ảo này hoạt động giống như một ổ đĩa hệ thống bình thường, ngoại trừ một điều là nó được mã hóa toàn bộ. Một tệp bất kỳ sẽ được mã hóa mỗi khi người dùng sao chép, di chuyển hoặc lưu nó vào trong ổ đĩa ảo này (tiến trình này gọi là sự mã hóa tức thời)



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

- Tạo folder B19DCAT141, có file ảnh ImageFile và TextFile. Dữ liệu trong ổ đĩa ảo này sẽ được mã hóa.



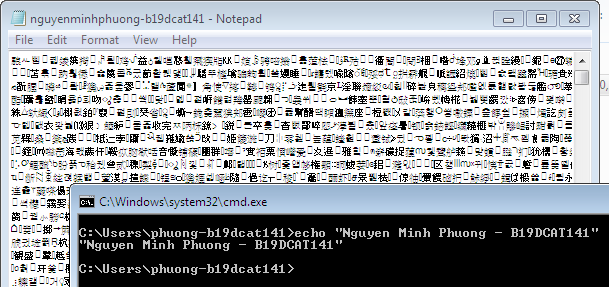
Gỡ vùng mã hóa chuẩn

- Chọn Dismount, nhập mật khẩu

- Vùng mã hóa được đóng lại

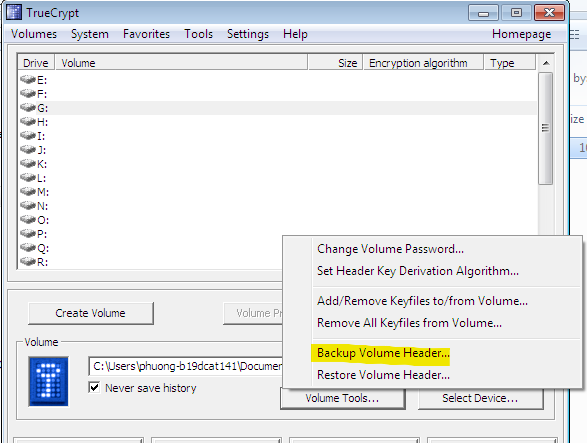
*Khi truy cập file từ bên ngoài, người dùng không thể xem nội dung file*

*=> Mã hóa thành công*

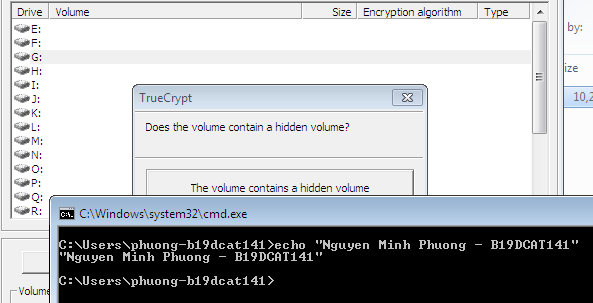


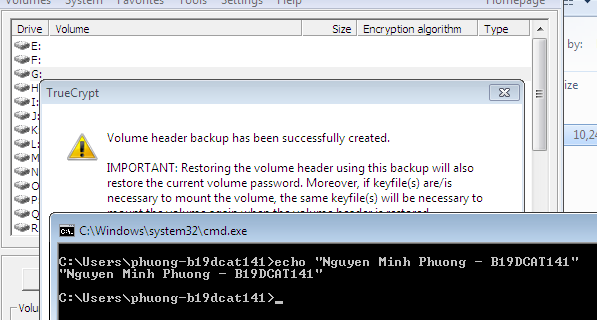
Sao lưu khóa mã hóa của công cụ TrueCrypt

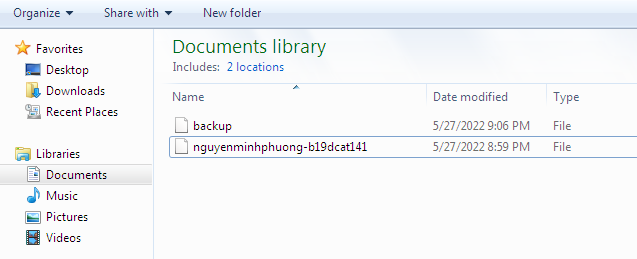
- Chọn vùng mã hóa, chọn Volume backup header. Header là nơi lưu trữ mã hóa khóa.



- Chọn The volume does not contain a hidden volume

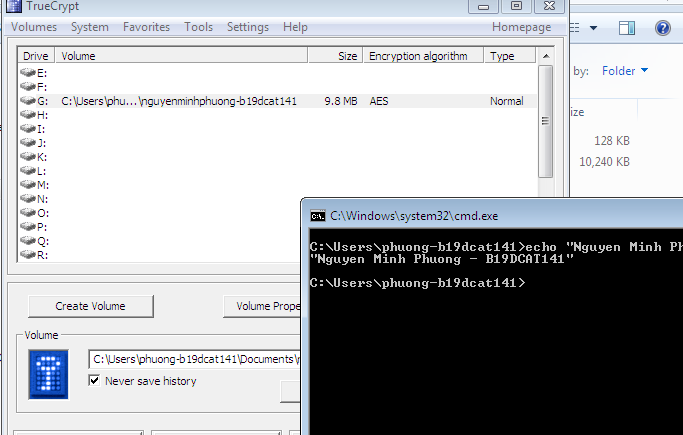






Sử dụng công cụ TrueCrypt để khôi phục các file và thưc mục mã hóa

- Chọn Mount để nối vùng mã hóa chuẩn vào ổ đĩa ảo như mô tả trong B2



=> Các file được khôi phục