HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN 1

BÀI THỰC HÀNH 13

THỰC TẬP CƠ SỞ

Họ và tên : Đinh Quang Hiếu

Mã sinh viên: B19DCAT065

Giảng viên giảng dạy: Hoàng Xuân Dậu

HÀ NỘI, THÁNG 5/2022

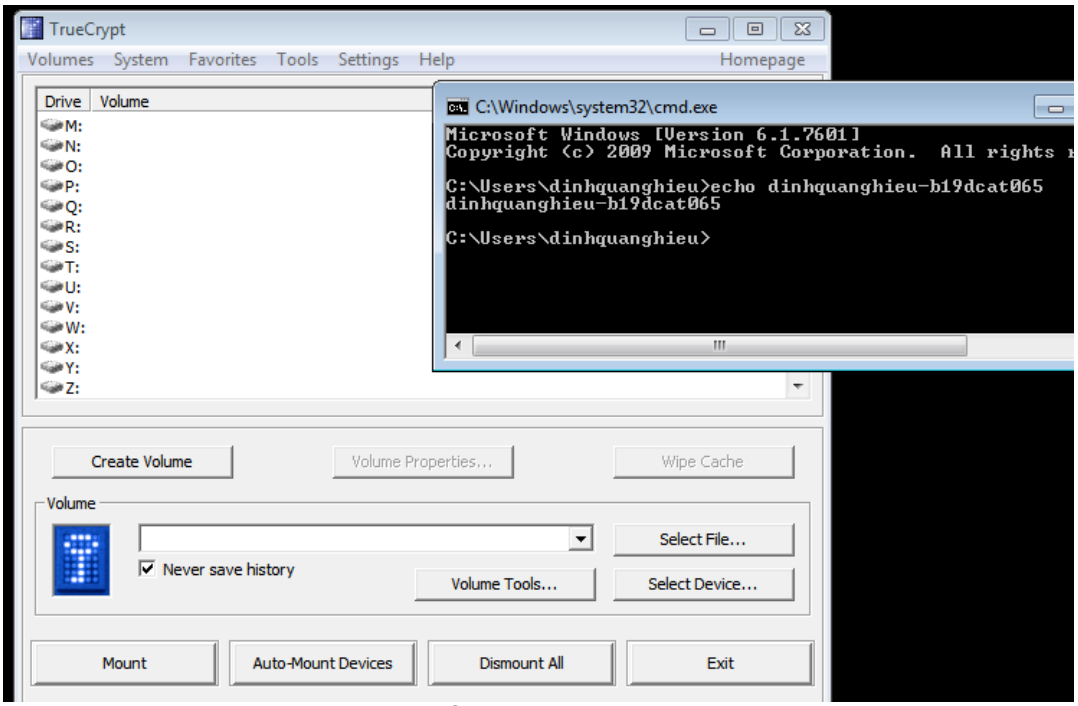
Bài 13: Đảm bảo an toàn với mã hóa

1. Lý thuyết

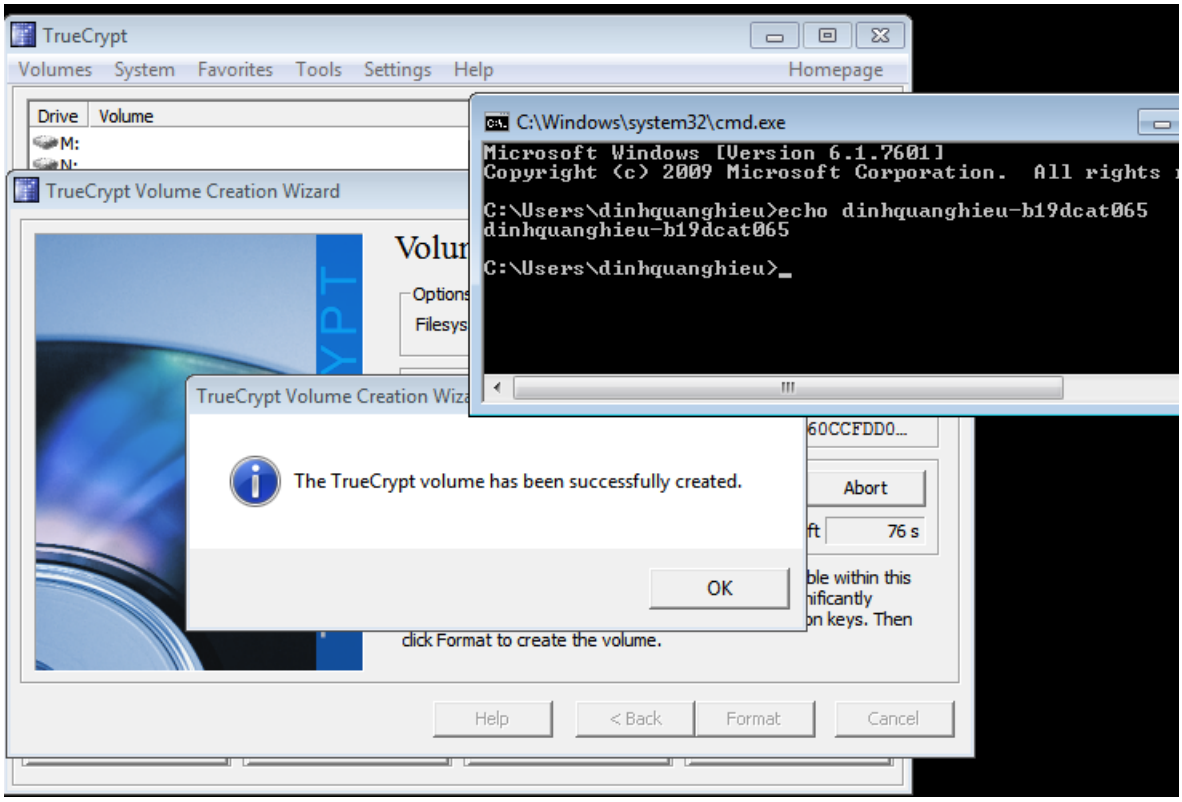
- TrueCrypt:
  - Là một tiện ích phần mềm miễn phí để mã hóa nhanh (OTFE). Nó có thể tạo một đĩa ảo được mã hóa trong một tệp, mã hóa một phân vùng hoặc toàn bộ thiết bị lưu trữ (xác thực trước khi khởi động).
  - Vào ngày 28 tháng 5 năm 2014 trang web phát triển của TrueCrypt đăng thông báo tới người dùng rằng TrueCrypt sẽ ngừng tiếp tục nâng cấp, tuy nhiên TrueCrypt vẫn là một trong những phần mềm mã hóa đáng tin cậy nhất.
  - Các mật mã được TrueCrypt hỗ trợ là AES , Serpent và Twofish . Ngoài ra, có sẵn năm tổ hợp thuật toán khác nhau : AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES và Twofish-Serpent. Các hàm băm mật mã có sẵn để sử dụng trong TrueCrypt là RIPEMD-160 , SHA-512 và Whirlpool
- Cách hoạt động TrueCrypt:
  - Hiện đang sử dụng chế độ hoạt động XTS . Trước đó, TrueCrypt đã sử dụng chế độ LRW trong các phiên bản cũ. Chế độ XTS được cho là an toàn hơn chế độ LRW, do đó an toàn hơn chế độ CBC.
  - Tương thích ngược với các tập cũ hơn bằng chế độ LRW và chế độ CBC

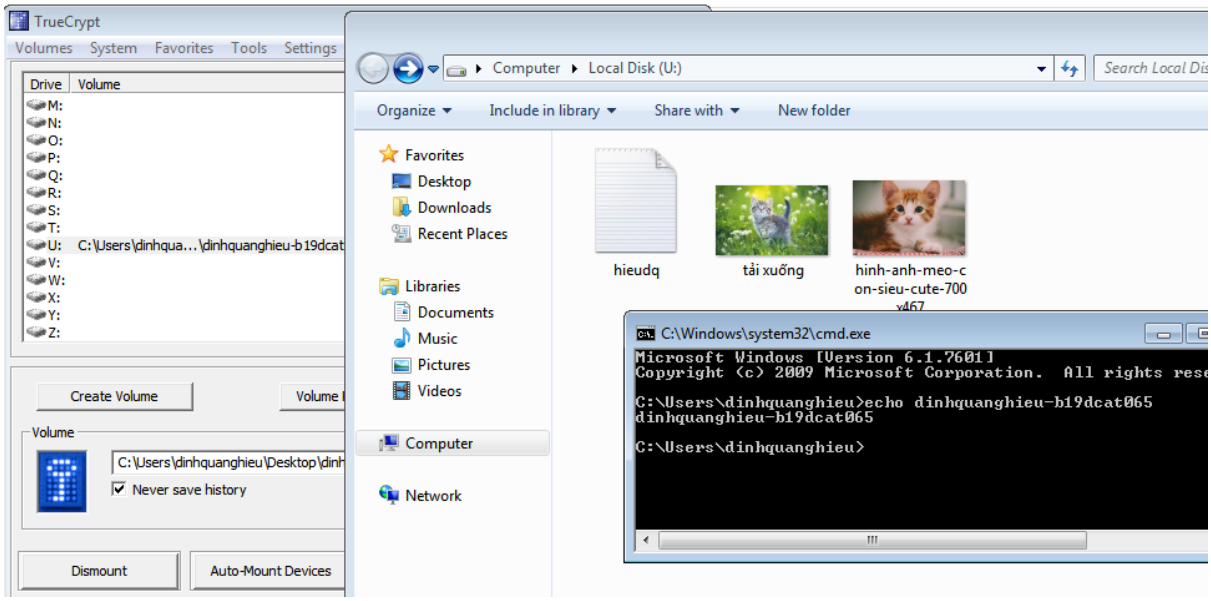
2. Các bước thực hiện

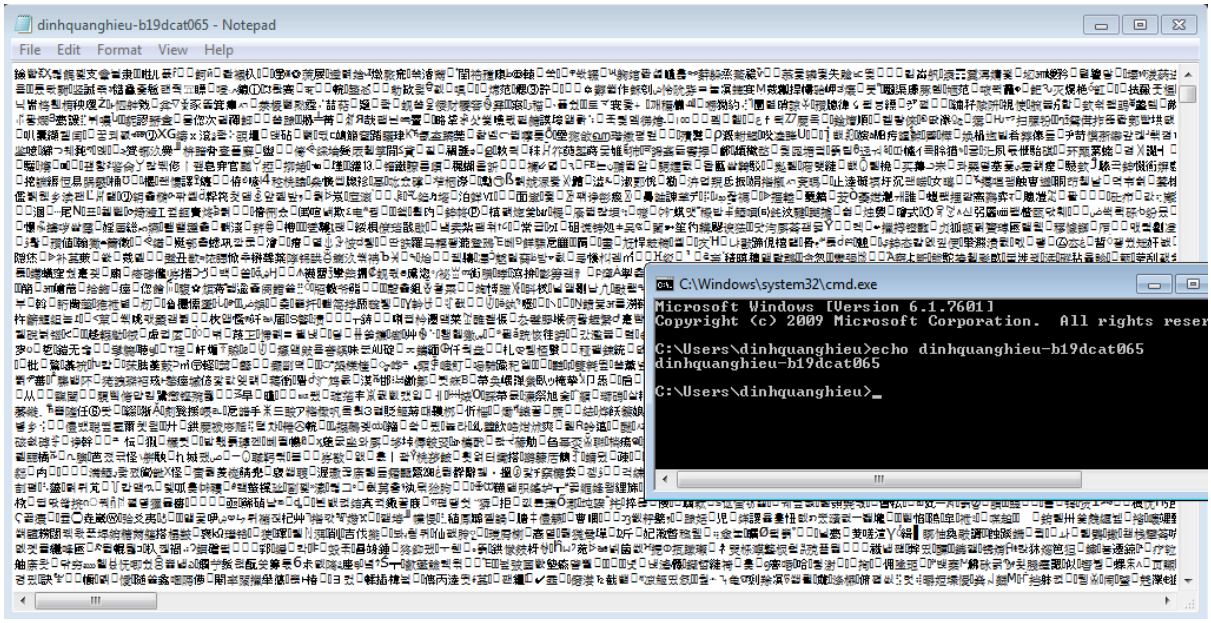
- **Cài đặt TrueCrypt trên hệ điều hành windows**



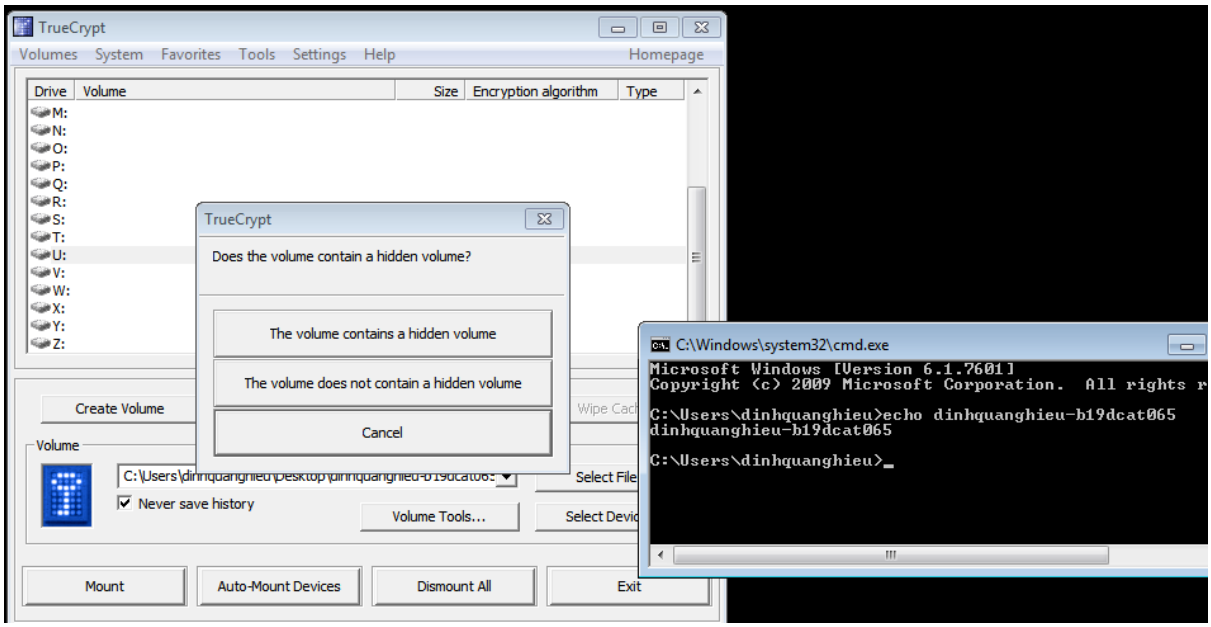
- **Sử dụng công cụ TrueCrypt để hóa thư mục. Đặt tên thư mục theo mã sinh viên và có chứa 1 số file khác nhau.**

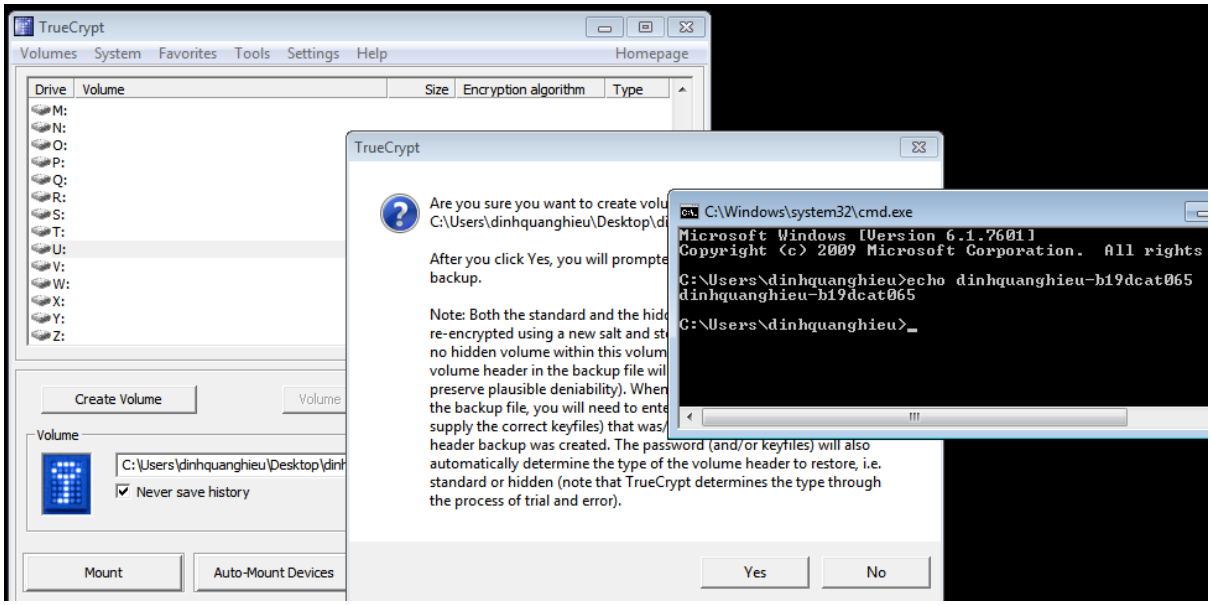

TrueCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume
M:
N:
TrueCrypt Volume Creation Wizard
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights
C:\Users\dinhquanghieu>echo dinhquanghieu-b19dcat065
dinhquanghieu-b19dcat065
C:\Users\dinhquanghieu>_
TrueCrypt Volume Creation Wiza
The TrueCrypt volume has been successfully created.
OK
Abort
76 s
click Format to create the volume.
Help
< Back
Format
Cancel

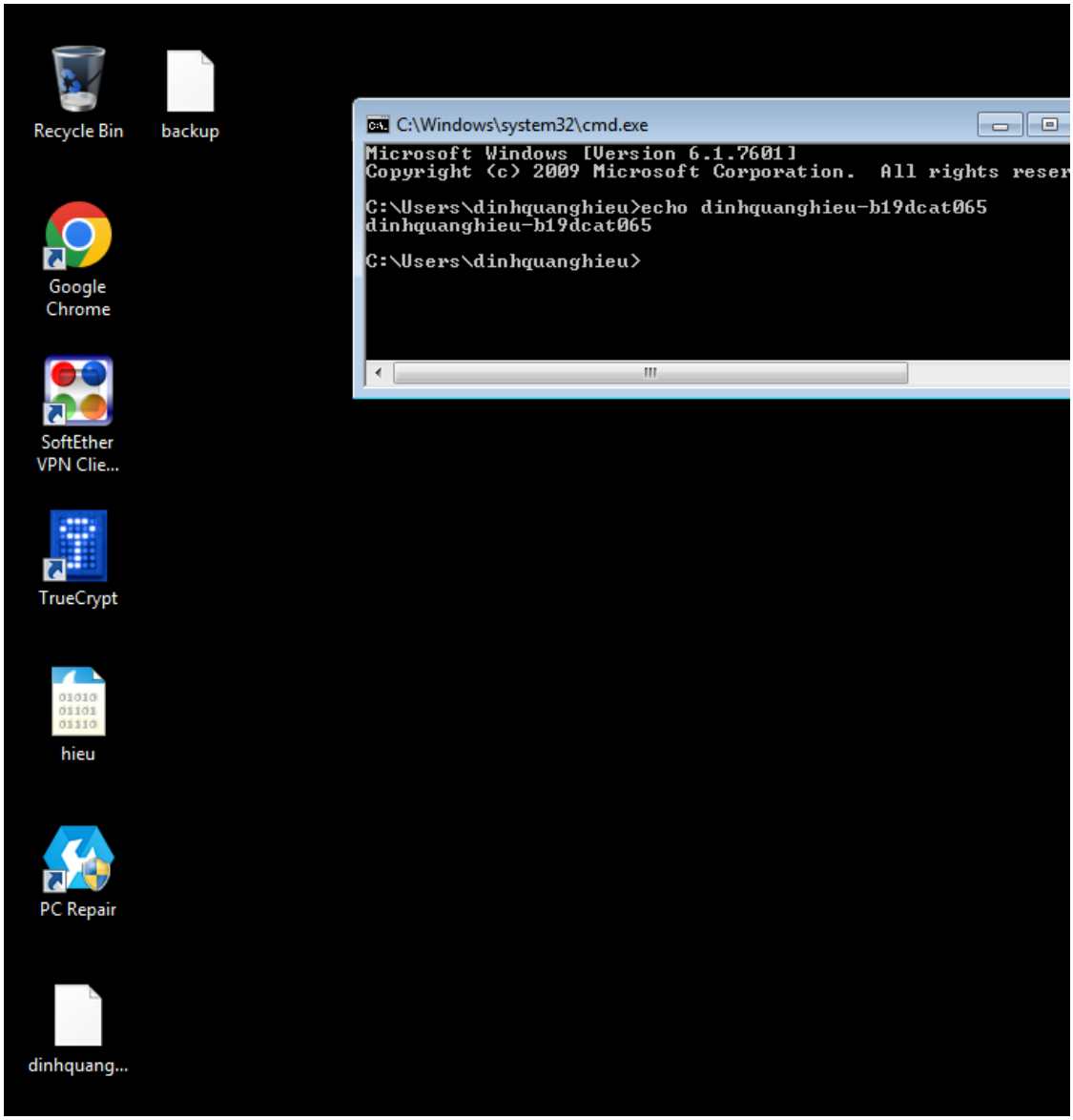

TrueCrypt
Volumes System Favorites Tools Settings
Drive Volume
M:
N:
O:
P:
Q:
R:
S:
T:
U: C:\Users\dinhqua...\dinhquanghieu-b19dcat
V:
W:
X:
Y:
Z:
Create Volume
Volume
C:\Users\dinhquanghieu\Desktop\dinh
Never save history
Dismount
Auto-Mount Devices
Computer ▸ Local Disk (U:)
Search Local Dis
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
hieudq
tải xuống
hinh-anh-meo-con-siеu-cute-700
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights
C:\Users\dinhquanghieu>echo dinhquanghieu-b19dcat065
dinhquanghieu-b19dcat065
C:\Users\dinhquanghieu>



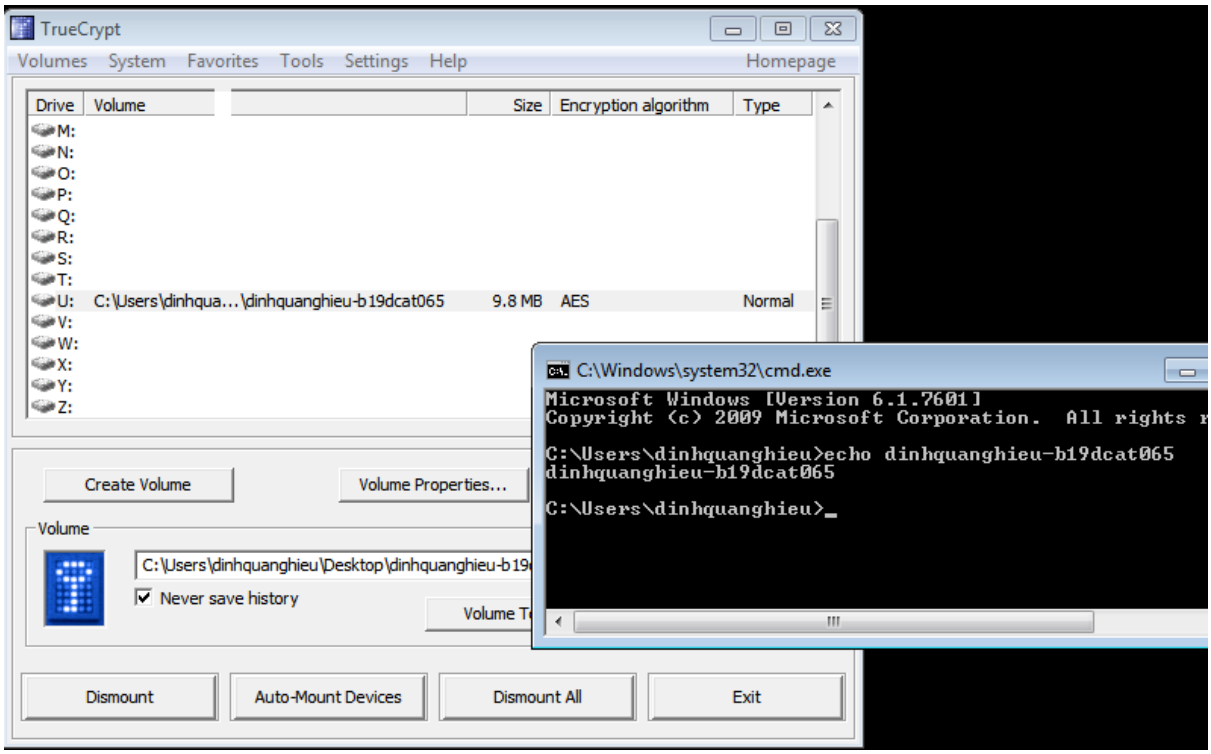
- **Sao lưu khóa mã hóa của công cụ TrueCrypt.**
  - ✓ Chọn vùng mã hóa, chọn Volume backup header.
  - ✓ Chọn The volume does not contain a hidden volume




TrueCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption algorithm Type
M:
N:
O:
P:
Q:
R:
S:
T:
U:
V:
W:
X:
Y:
Z:
Create Volume
Volume
Volume
C:\Users\dinhquanghieu\Desktop\dinh
Never save history
Mount
Auto-Mount Devices
TrueCrypt
Are you sure you want to create volu
C:\Users\dinhquanghieu\Desktop\di
After you click Yes, you will prompte
backup.
Note: Both the standard and the hidd
re-encrypted using a new salt and st
no hidden volume within this volum
volume header in the backup file wil
preserve plausible deniability). When
the backup file, you will need to ente
supply the correct keyfiles) that was
header backup was created. The password (and/or keyfiles) will also
automatically determine the type of the volume header to restore, i.e.
standard or hidden (note that TrueCrypt determines the type through
the process of trial and error).
Yes
No
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights
C:\Users\dinhquanghieu>echo dinhquanghieu-b19dcat065
dinhquanghieu-b19dcat065
C:\Users\dinhquanghieu>


Recycle Bin
backup
Google Chrome
SoftEther VPN Clie...
TrueCrypt
hieu
PC Repair
dinhquang...
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reser
C:\Users\dinhquanghieu>echo dinhquanghieu-b19dcat065
dinhquanghieu-b19dcat065
C:\Users\dinhquanghieu>

- **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



=> Các file được khôi phục