

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN



AN TOÀN VÀ PHỤC HỒI DỮ LIỆU
Bài tập 4.3 Khảo sát các Data Recovery Tools

GVLT: Thầy Thái Hùng Văn
SV: Nguyễn Phan Mạnh Hùng 1312727

I/ Các phần mềm khảo sát

- 1) Winhex
- 2) Active File Recovery
- 3) Data Recovery Wizard
- 4) PC Inspector File Recovery

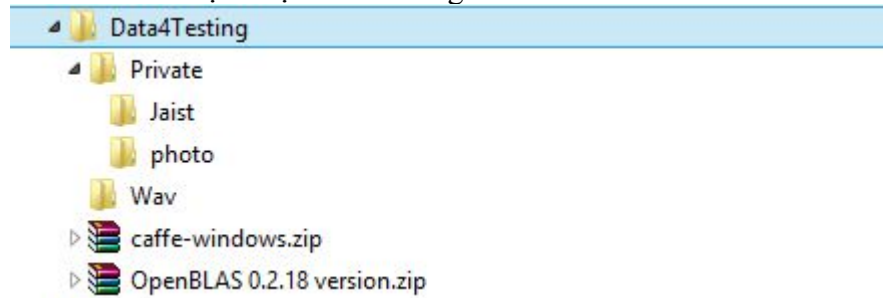
II/ Các chức năng chính

- 1) Winhex
 - Chỉ gồm 1 chế độ quét duy nhất để tìm các file theo phân loại của người dùng.
- 2) Active File Recovery
 - Quick Scan: quét nhanh đĩa, hiển thị cấu trúc cây thư mục và phát hiện những file bị xóa (còn thông tin mô tả) và file chưa bị xóa.
 - Super Scan: quét toàn bộ đĩa và phân tích chữ ký (signature) riêng của từng loại file và gom nhóm từng file tìm được theo loại để phục hồi.
- 3) Data Recovery Wizard
 - Scan: tương tự như Quick Scan của Active File Recovery.
 - Deep Scan: tương tự như Super Scan.
- 4) PC Inspector File Recovery
 - Chỉ có một chế độ quét duy nhất tìm file bị xóa.

III/ Các bước khảo sát

1) Chuẩn bị:

- USB 2.0, fat32, 1GB
- Cấu trúc dữ liệu được mô tả trong ảnh sau



Thư mục Data4Testing được chép trực tiếp vào Usb.

Thư mục photo: 36 ảnh tên: 01.jpg -> 36.jpg, kích thước tối đa là 406KB

Thư mục Jaist: 2 file pdf kích thước 126KB và 5687KB

Thư mục Data4Testing tổ chức như sau

Private	5/5/2016 4:08 PM	File folder	
Wav	5/5/2016 4:10 PM	File folder	
Beethoven Virus - Diana Boncheva.mp3	4/6/2016 2:03 PM	MP3 Format Sound	3,470 KB
caffe-windows.zip	4/29/2016 9:38 PM	WinRAR ZIP archive	8,513 KB
Git-2.8.1-64-bit.exe	4/29/2016 12:12 PM	Application	30,438 KB
OpenBLAS 0.2.18 version.zip	4/28/2016 6:55 PM	WinRAR ZIP archive	21,225 KB
PyScripter-v2.5.3-x64-Setup.exe	8/19/2015 9:57 PM	Application	4,924 KB

2) Tiến hành

a) Kịch bản 1:

Xóa các file sau (lệnh delete thông thường của windows):

02.jpg - 213 kb

04.jpg - 143 kb

05.jpg - 157 kb

alarm02.wav - 324 kb

alarm04.wav - 400 kb

caffe-windows.zip - 8513kb

- Lưu ý: Đây là 6 file được tính trong (số file khôi phục) trong các bảng dưới đây. Các file bị xóa hoặc mất sẽ được nêu thêm ở phần “Chi tiết”.

	Winhex	Active File Recovery		Data Recovery Wizard		PC Inspector
		Quick Scan	Super Scan	Scan	Deep Scan	
Số file khôi phục	5/6	6/6	6/6	6/6	6/6	6/6
Chi tiết	Không khôi phục được caffe-windows.zip hoàn chỉnh. Nội dung bị tách lẻ và nhiều phần bị thiếu. Các file được khôi phục nhưng mất tên hoàn toàn		Các file được khôi phục vẫn giữ được tên, chỉ bị mất kí tự đầu.			

b) Kịch bản 2

- Xóa file tương tự kịch bản 1.

- Tại vị trí chứa entry file của 02.jpg và caffe-windows.zip, ta xóa hoàn toàn thông tin (ghi đè lên 32 byte 0)

	Winhex	Active File Recovery		Data Recovery Wizard		PC Inspector
		Quick Scan	Super Scan	Scan	Deep Scan	
Số file khôi phục	5/6	2/6	6/6	4/6	4/6	2/6
Chi tiết	- Kết quả tương tự như trên. - Cây thư mục vẫn hiển thị chính xác các file còn	- Tình trạng tương tự như của PC Inspector.	- Phục hồi được hoàn toàn tuy vậy vẫn bị mất các file đặc	- Phục hồi được hết ngoại trừ caffe-windows.zip, 02.jpg. - Vẫn bị	- Không phục hồi được caffe và 02. - Phụ hồi được	- Phục hồi được file wav. - Bên cạnh các file bị xóa không hồi phục

	nguyên và bị xóa.		biệt như *.exe do không phân tích được signature.	mất các file có entry nằm sau các entry của 02 và caffe.	các file không hiển thị được do entry nằm sau entry của 02 và caffe, kể cả các file *.exe	được, các file có entry nằm sau 02.jpg và caffe-windows.zip không được hiển thị dù không bị xóa và cũng không thể recover được.
--	-------------------	--	---------------------------------------------------	----------------------------------------------------------	-------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------

c) Kịch bản 3

- Xóa file tương tự kịch bản 1.
- Đổi tên 03.jpg thành test.exe.

	Winhex	Active File Recovery		Data Recovery Wizard		PC Inspector
		Quick Scan	Super Scan	Scan	Deep Scan	
Số file khôi phục	5/6	6/6	6/6	6/6	6/6	6/6
Chi tiết	- Khôi phục được hoàn toàn trừ caffe-windows.zip. - Nhận biết được test.exe là ảnh và lưu lại dưới dạng ảnh khi recover.	- Tình trạng tương tự như của PC Inspector.	- Phục hồi được hoàn toàn. - Nhận biết được test.exe là file ảnh.	- Tình trạng tương tự như của PC Inspector	- Tương tự PC Inspector .	- Phục hồi được hết. - Không nhận biết được file test.exe là ảnh.

d) Kịch bản 4

- Tình trạng file tương tự kịch bản 2.
- Format (quick format) lại ổ đĩa thành định dạng ntfs.

	Winhex	Active File Recovery		Data Recovery Wizard		PC Inspector
		Quick Scan	Super Scan	Scan	Deep Scan	
Số file khôi phục	5/6	0/6	6/6	0/6	4/6	0/6
Chi tiết	- Không khôi phục được caffe-windows .- Khôi phục	- Không khôi phục lại được bất kì dữ	- Khôi phục được hoàn toàn		- Khôi phục được hết ngoại trừ	- Không khôi phục được file

	lại được các file khác ngoại trừ các file *.exe.	liệu nào.	dữ liệu ban đầu, ngoại trừ file *.exe		caffé-win dows và 02.jpg. - Khôi phục lại được tất cả các file khác kể cả *.exe	nào trong 6 file xóa ban đầu và tất cả các file còn lại cũng không khôi phục được.
--	--------------------------------------------------	-----------	---------------------------------------	--	------------------------------------------------------------------------------------	------------------------------------------------------------------------------------

IV/ Tham khảo

Các phần mềm sử dụng được chọn lựa từ:

- <http://www.gfi.com/blog/the-top-23-free-data-recovery-tools/>
- Tài liệu học tập môn An toàn phục hồi dữ liệu - Thầy Thái Hùng Văn