DIGITAL FORENSIC PROCEDURE

Procedure Name:
Mounting an EnCase E01 Logical Image file with FTK Imager

Category:
Image Mounting

Procedure Development

Development Owner	Organization
Mr. O	DFIR Team

Document

Document Owner(s)	Organization Role
Mr. O	DFIR Team

Version Control

Version	Date	Author	Change Description
1.0	8/28/13	Mr. O	Document creation.
[**Version #**]	[**mm/dd/yy**]	[**Change owner**]	• [**Change 1**] • [**Change 2**] • [**Change *n***]

Table Contents

Purpose

The purpose of this document is to detail the steps that are required to mount an EnCase E01 logical image with FTK Imager.

Why

The ability to mount an image, not just with FTK Imager, can provide the following benefits.

- Mount a full disk image with its partitions all at once; the disk is assigned a PhysicalDrive*n* name and the partitions are automatically assigned a drive letter beginning with either the first available, or any available drive letter of your choice.

- Read a full disk image mounted physically, and assigned a Physical Drive *n* name using Imager or using any Windows application that performs Physical Name Querying.

- Read and write to the mounted image using a cache file. The original content is not altered.

- Mount images of multiple drives and/or partitions. The mounted images remain mounted until un-mounted or until Imager is closed.

- Easily un-mount mounted images in any order, individually or all at once.

- View a logically mounted image in Windows Explorer as though it were a drive attached to the computer, providing the following benefits:

- View file types with Windows associations in their native or associated application, when that application is installed locally.

- Run anti-virus applications on the mounted image.

- Share and view the logically mounted image as a drive in Windows Explorer from remote computers when Remote Access has been configured correctly.

- Copy files from the mounted image to another location.

Prerequisites

An EnCase logical image (E01) file. e.g. The C:\ Partition of a physical disk.
MD5 hash value from EnCase image verification.

Note: This procedure uses Guidance Software's EWF file format. Other image types such as those generated by Access Data or DD can be used.

Environment

Examiner Machine: WinXP Workstation
Mounting Tool: FTK Imager 3.1

Document Conventions

The following table describes the conventions that this procedure uses.

Conventions	Description
Figure	A screen shot for illustrative purposes
Table	Refers to a table of data
Section	A numeric value referring to a location in the procedure. e.g. 1.5

Procedure

Important: Before you start this procedure, note the EnCase verified MD5 hash value of the acquired image. You can compare the MD5 value after your analysis and the image has been unmounted. Additionally, always use a working copy of the image, never the original.

1.0 – Note the location of your working copy of acquired image on your examiner machine.

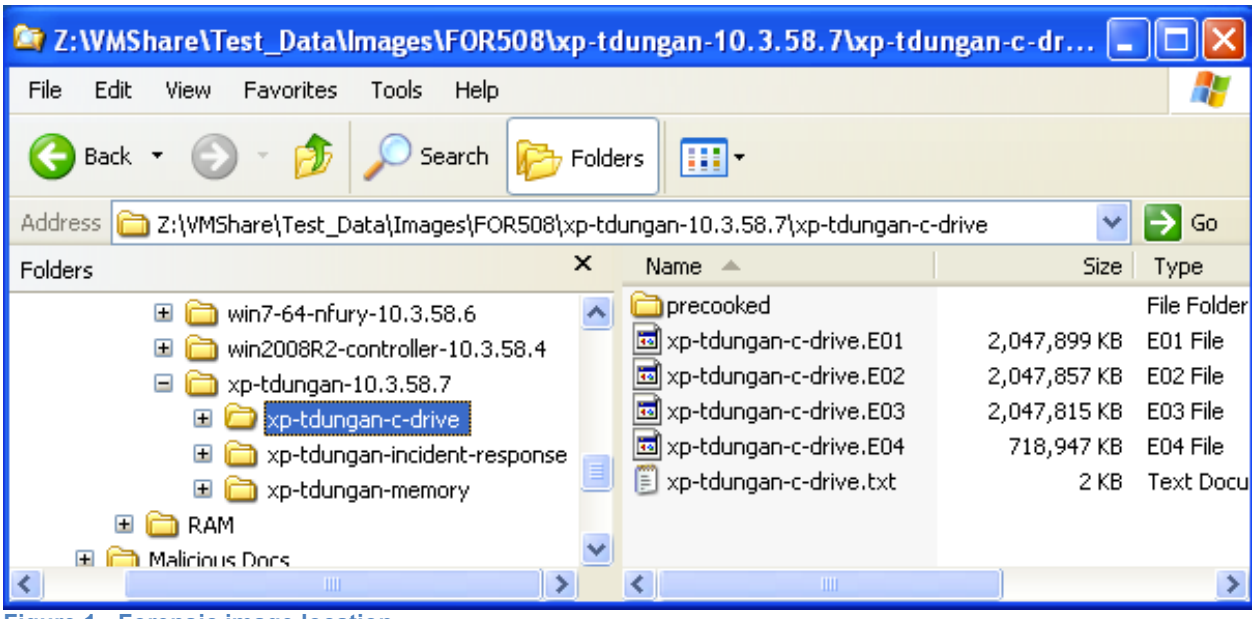

Figure 1 - Forensic image location

Location:
Z:\VMShare\Test_Data\Images\FOR508\xp-tdungan-10.3.58.7\xp-tdungan-c-drive

1.1 – Locate your FTK Imager install and launch it.

Figure 2 - FTK Imager

1.2 – With FTK Imager open, select **File >> Image Mounting**

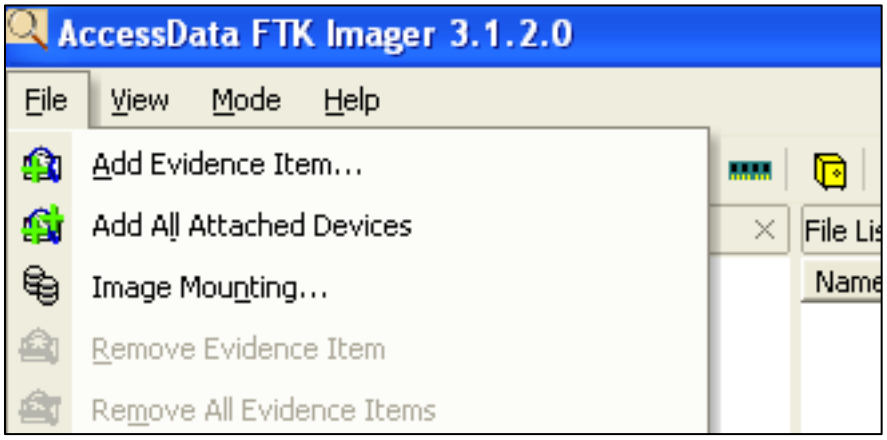

Figure 3 - Image mounting

1.3 – After selecting **Image Mounting**… the **Mount Image To Drive** window becomes available.

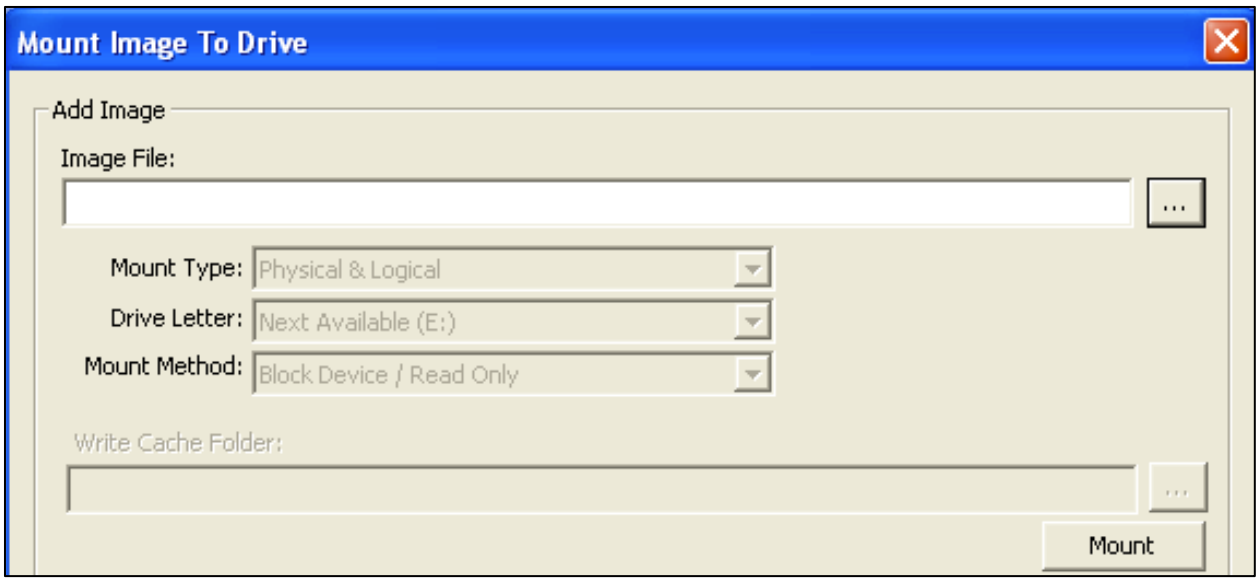

Figure 4 - Mount Image to Drive

1.4 – Click the … ellipse box at the far right of the **Image File**: selector box. Then locate your EnCase E01 image file as noted section 1.0.

With your E01 image file selected Click **Open**

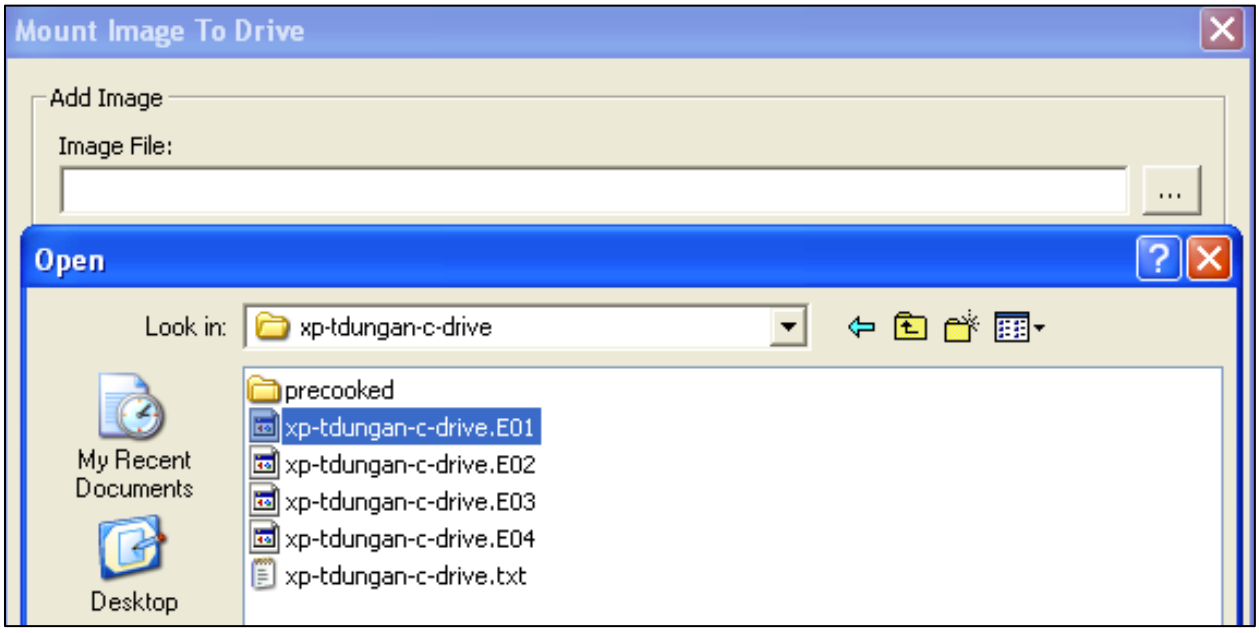

Figure 5 - Image File selector

1.5 – After selecting Open, the image file and path will appear in the Image File selector box as shown in Figure 6 below.

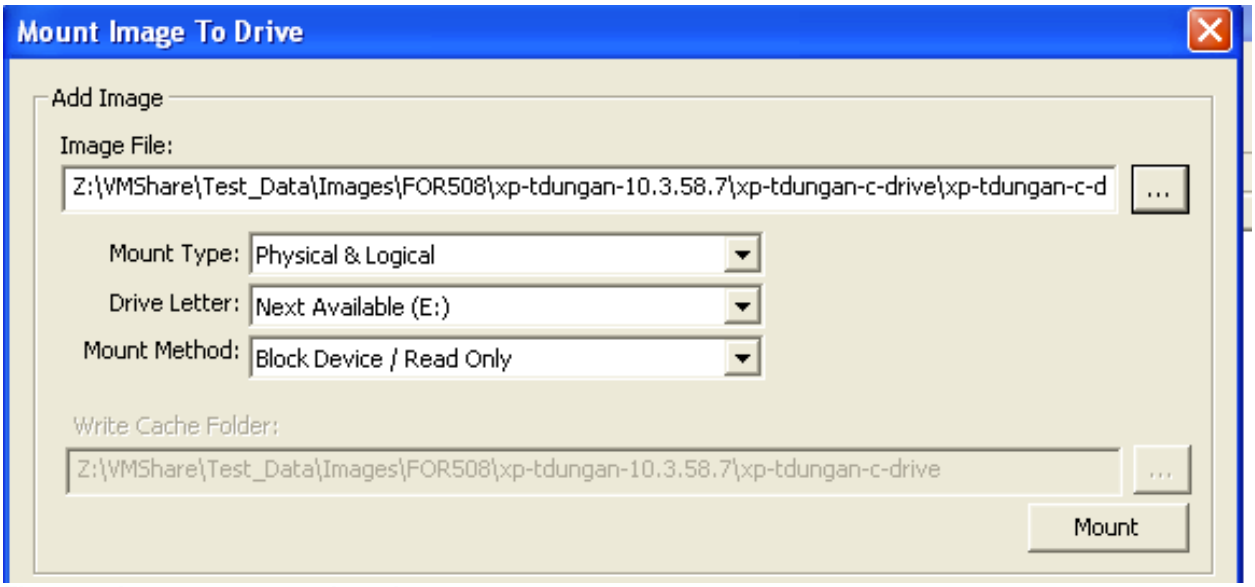

Figure 6 - Image to mount selected

1.6 – With our image file and path selected, choose the options as shown above in Figure 6 for the following items:

Mount Type: Physical & Logical
Drive Letter: Next Available (drive letter)
Mount Method: Block Device /Read Only

Explanation: Taken from the Access Data FTK Imager help file, shown below are the Mount Method descriptions.

Mount Method Description

Block Device/Read Only – Reads the device as a block device, meaning that the mounted device must be viewed using any Windows application that performs Physical Name Querying. Block Device/Writable – Allows you to write to the evidence, make notes, and so forth. The changes and notations are saved in a cache file, but no changes are made to the original. If selected, provide path information for the cache file in the Write Cache Folder field. File System/Read Only - Reads the device as a read-only device that you can view using Windows Explorer.

Table 1 – Mount Method Description

1.7 – Once the mount methods have been selected, click the **Mount** button

1.8 – After the **Mount** button is clicked, the bottom portion of the **Mount Image to Drive** window will be populated with the resulting details of your newly mounted image.

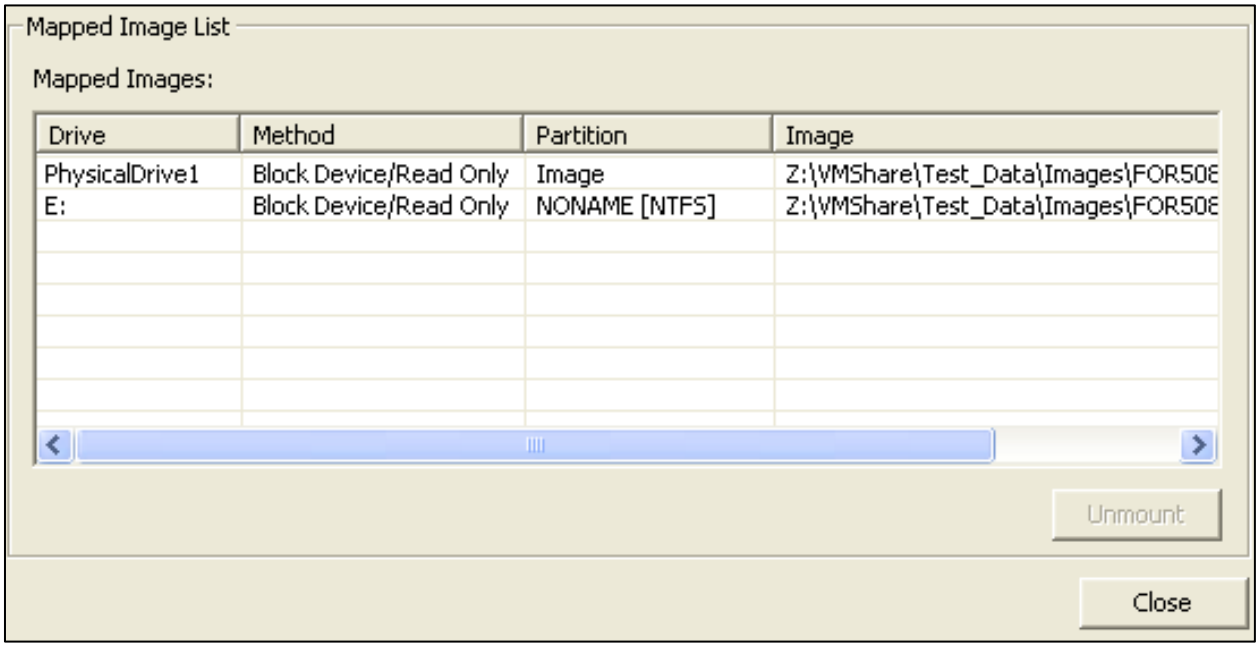

Figure 7 - EnCase image mounted as E: drive

Explanation: After selecting the **Mount** button your EnCase image will be mounted and made available to you as indicated by the drive letter in the **Drive** column.

1.9 – Now that our image has been mounted, it appears as the designated drive letter we selected. Open Windows Explorer on your examiner machine and navigate to the chosen drive letter. As shown in Figure 8 below, we can see the E: drive is used to mount our image.

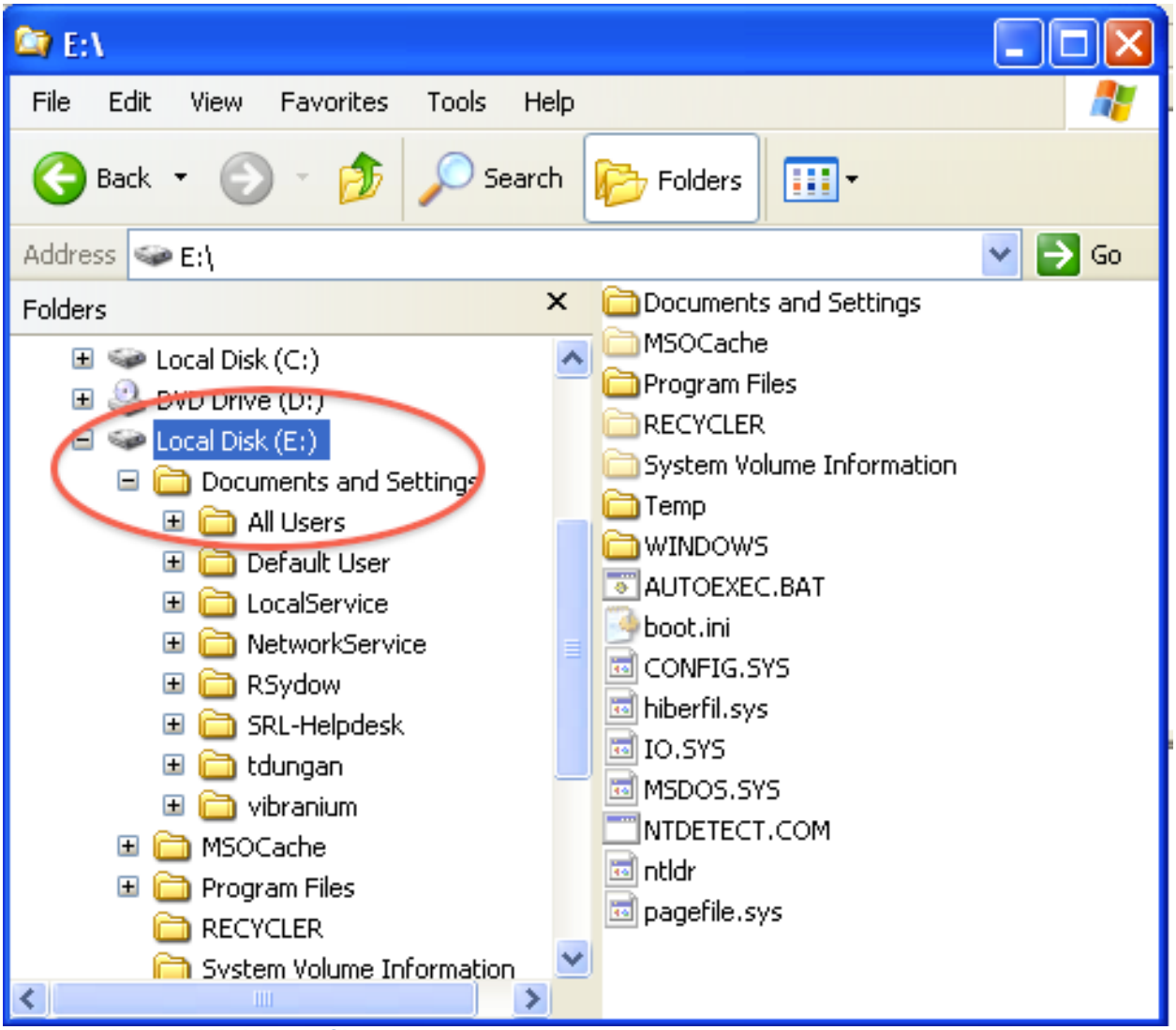

Figure 8 - Mounted E01 image file as the E: drive

Explanation: Our image and the associated file system within the image in now completely exposed for the examiner to perform analysis with their tools of choice. You can navigate through the file system viewing folder and file contents.

TIP: The first thing I do once the image is mounted is to scan the mounted image with at least two (2) antivirus products.

2.0 – Any attempts to write data to the mounted file system will result in the pop-up message as noted below in Figure 9. The image file is write protected.

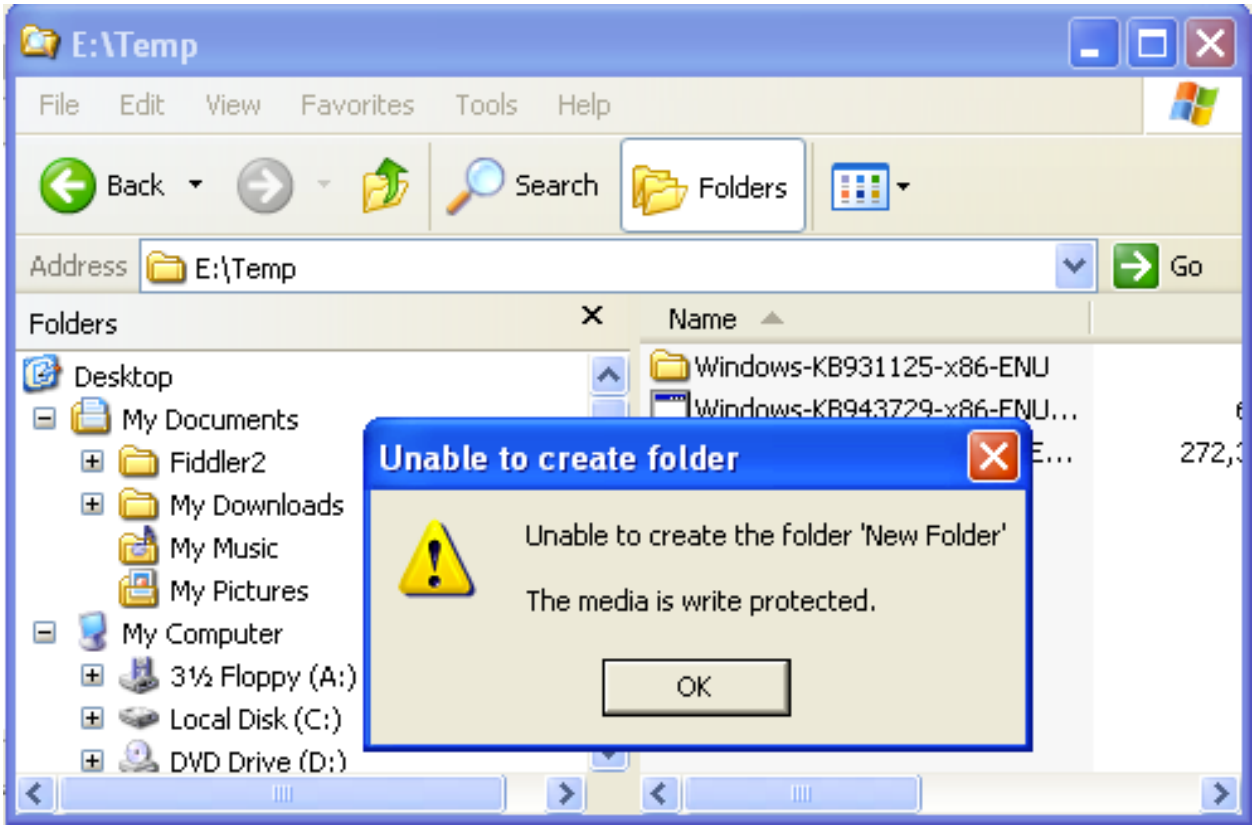

Figure 9 - Write denied

Use Cases

This is the “to get you thinking section”. How else might this be useful?

While you have the file system exposed you could…

- Run Reg Ripper across the registry hives.
- Run Corey Harrell’s auto_rip.exe.
- Mount the image into VMware as Jimmy Weg has illustrated.

References

http://www.forensicswiki.org/wiki/FTK_Imager
http://www.accessdata.com/support/product-downloads
Reg Ripper - http://regripper.wordpress.com/
Corey Harrell - http://journeyintoir.blogspot.com/
Jimmy Weg - http://regripper.wordpress.com/