Basic Data Carving Test #1

(by Nick Mikus)

Digital Forensics Tool Testing Image (#11)

http://dftt.sourceforge.net

Introduction

This test image is a FAT32 file system and is intended to test data carving tools and their ability to extract various file formats. The image contains several allocated and deleted files and the header one JPEG file was modified (to show the importance of ignoring corrupted files). All files are random files that that were in my possession or that I created from scratch. This image was created from a USB thumb-drive that was wiped and formatted using the `mkfs.vfat` program. The FAT boot sector has been corrupted so that the image cannot be mounted and therefore data carving methods must be used to extract the files.

Download

This test image is a 'raw' partition image (i.e. 'dd') of a FAT32 file system. The file system is 62MB and is compressed to 11MB. The MD5 of the image is `0069813c892a462f88dc6d376624f7d9`. This image is released under the GPL, so anyone can use it.

- zip

Files

The following files and the MD5 hash and description were created on the file system.

Num	Name	MD5	Size	Note	Sectors
1	`2003_document.doc`	`e72f388b36f9370f19696b164c308482`	`19968`	A Valid DOC file	(0-38) 281 -320
2	`enterprise.wav`	`7629b89adade055f6783dc1773274215`	`318895`	A valid WAV file	(0-622) 16021 -16644
3	`haxor2.jpg`	`84e1dceac2eb127fef5bfdcb0eae324b`	`24367`	An invalid JPEG with only 1 header byte corrupted. This byte is located at offset 19 within the file.	(0-47)16645 -16692
4	`holly.xls`	`7917baf0219645afef8b381570c41211`	`23040`	A valid XLS file	(0-44) 16693-16738

5	lin_1.2.pdf	e026ec863410725ba1f5765a1874800d	1399508	A linearized PDF	(0-2733) 16741 -19475
6	nlin_14.pdf	5b3e806e8c9c06a475cd45bf821af709	122434	A non-linearized PDF	(0-239) 19477 -19716
7	paul.jpg	37a49f97ed279832cd4f7bd002c826a2	29885	A valid jpeg	(0-58) 19717 -19776
8	pumpkin.jpg	6c9859e5121ff54d5d6298f65f0bf3b3	444314	A valid EXIF jpeg	(0-867) 19777-20644
9	shark.jpg	d83428b8742a075b57b0dc424cd297c4	99298	A valid JPEG	(0-193) 20645-20839
10	sm1.gif	d25fb845e6a41395adaed8bd14db7bf2	5498	A valid GIF	(0-10) 20841-20852
11	surf.mov	5328d2b066f428ea95b2793849ab97fa	550653	A valid MOV	(0-1075) 20853-21928
12	surf.wmv	ff085d0c4d0e0fdc8f3427db68e26266	1036994	A valid WMV	(0-2025) 21929-23955
13	test.ppt	7b74c2c608d92f4bb76c1d3b6bd1decc	11264	A deleted PPT	(0-21) 23957 -23978
14	wword60t.zip	c0be59d49b7ee0fdc492d2df32f2c6c6	78899	A valid ZIP	(0-154) 23981 -24135
15	domopers.wmv	63c0c6986cf0a446cb54b0ac65a921a5	8037267	A deleted wmv	(0-15697) 321-16018

Author

Nick Mikus (nick.mikus at gmail.com) created the test cases and the test image. This test was released on March 14, 2005.

Disclaimers

This is a simple test case I composed when testing data carving tools. It is by no means all inclusive.
