Basic Data Carving Test #2

(by Nick Mikus)

Digital Forensics Tool Testing Image (#12)

http://dftt.sourceforge.net

Introduction

This test image is an EXT2 file system and is intended to test data carving tools for indirect block detection and removal. With large files, EXT2 allocates blocks (called indirect blocks) to store file metadata and the blocks are frequently allocated in between blocks that contain file content. Therefore, the file becomes fragmented and a basic carving tool may include the indirect block in the carved file. This file system image contains several allocated and deleted files, none of which have been modified. This image was created from a USB thumb drive that was wiped clean and formatted using the `mkfs.ext2` program. The super block 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 an EXT2 file system. The file system is 124MB and is compressed to 1.1MB. The MD5 of the image is `6cbd2c5248fa7030d699eb6cde051623`. This image is released under the GPL, so anyone can use it.

- zip

Files

The following files exist in the image. The sectors marked as "(IND)" and "(DIND)" represent the indirect and double indirect block pointer locations.

Num	Name	MD5	Size	Note	Sectors
1	`haxor2.bmp`	`f9633fe6b9ef2a0a5edd6de70d22c0f5`	163878	A deleted BMP	(0-22):5162-5184, (IND):5186 (24-320):5188-5484
2	`jimmy.doc`	`2f3f914dd74819df42d1d941c7275c16`	12800	A deleted DOC	(0-22):5486-5508, (IND):5510 (24):5512
3	`jn.jpg`	`270a0a913fa9603db8121fdf78d63aca`	28949	A valid JPG	(0-22):5514-5536, (IND):5538 (24-56):5540-5572
4	`lin_test.pdf`	`1c64456776075d1f0a662e1f6c09e340`	26618	A valid PDF	(0-22):5574-5596, (IND):5598 (24-50):5600-5626
5	`main_dive.jpg`	`937846adb96773ee25fcb34821230976`	8463	A valid jpeg	(0-16):5628-5644
6	`n_lin_ss.pdf`	`97be95ed3e710b63bc75e5c0775062d9`	734652	A valid pdf	(0-22):5646-5668, (IND):5670 (24-534):5672-6182, (DIND):6184, (IND):6186, (536-1046):6188-6698, (IND):6700, (1048-1434)6702 7088
7	`blogo.gif`	`5e10b2176016885a85bffc074a142524`	18663	A valid gif	(0-22):5122-5144, (IND):5146 (24-36):5148-5160
8	`sherry.jpg`	`3834e72d2ee266ccfb9733d716b89f2b`	133249	A valid	(0-22):7090-7112, (IND):7114

				JPEG	(24-260):7116-7352
9	`stats.xls`	`6351df9c1543c41c3df8eea63e06a219`	`15360`	A valid XLS	(0-22):7354-7376, (IND):7378 (24-28):7380-7384
10	`test.ppt`	`99941c129cc8cfbadc15c55086982efc`	`17408`	A valid PPT	(0-22):7386-7408, (IND):7410 (24-32):7412-7420

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.

Last Updated: March 14, 2005