NTFS Undelete (and leap year) Test #1

Digital Forensics Tool Testing Image (#7)

http://dftt.sourceforge.net

Introduction

This test image is a 6MB NTFS file system with eight deleted files, two deleted directories, and a deleted alternate data stream. The files range from resident files, single cluster files, and multiple fragments. No data structures were modified in this process to thwart recovery. They were created in Windows XP, deleted in XP, and imaged in Linux.

Download

This test image is a 'raw' partition image (i.e. 'dd') of a NTFS file system. The file system is 6MB and is compressed to 186 KB (lots of zeros). The MD5 of the image is `e7dbb96759d9cd62b729463ebfe61dab`. This image is released under the GPL, so anyone can use it.

- zip

Files

These are the files that should be recovered, their sizes, and their MD5 values. (Fill in the blank results form)

Num	MFT Entry	Name	Size	MD5	Note
1	37	`\res1.dat`	101	`9036637712b491904cd0bfbdbe648453`	Resident file (data is stored in MFT entry and not in a cluster)
2	31	`\sing1.dat`	780	`59b20779f69ff9f0ac5fcd2c38835a79`	single cluster file
3	32-128-3	`\mult1.dat`	3801	`ffd27bd782bdce67750b6b9ee069d2ef`	multiple cluster, non-fragmented file
4	32-128-6	`\mult1.dat:ADS`	1234	`ba1b9eedb1c091ddca253d35dde8f616`	multiple cluster, second data attribute (Alternate Data Stream)
5	29	`\frag1.dat`	1584	`7a3bc5b763bef201202108f4ba128149`	fragmented file
6	30	`\frag2.dat`	3873	`0e80ab84ef0087e60dfc67b88a1cf13e`	fragmented file with `frag1.dat`

					mixed in
7	33	`\dir1\`	1024	N/A	directory
8	36	`\dir1\mult2.dat`	1715	`59cf0e9cd107bc1e75afb7374f6e05bb`	multiple cluster, non-fragmented in deleted directory
9	34	`\dir1\dir2\`	1024	N/A	directory in deleted directory
10	35	`\dir1\dir2\frag3.dat`	2027	`21121699487f3fbbdb9a4b3391b6d3e0`	fragmented file in deleted directories
11	38	`\dir3\sing2.dat`	1005	`c229626f6a71b167ad7e50c4f2fccdb1`	single cluster file in a directory whose MFT entry has been reallocated (to `res1.dat`)

Layout

Here is the actual layout of the image.

Cluster	File
4073	`\frag1.dat` (part 1 of 2)
4074	`\frag2.dat` (part 1 of 3)
4075	`\frag1.dat` (part 2 of 2)
4076-4077	`\frag2.dat` (part 2 of 3)
4078	`\sing1.dat`
4079-4082	`\mult1.dat`
4083-4084	`\mult1.dat:ADS`
4085	`\frag2.dat` (part 3 of 3)
4086-4089	`\$Secure:$SDH` (Not deleted)
4090	`\dir1\dir2\frag3.dat` (part 1 of 2)
4091-4092	`\dir1\mult2.dat`
4093	`\dir1\dir2\frag3.dat` (part 2 of 2)
4094	`\dir3\sing2.dat`

Bonus

This image was created on Feb 29, 2004 so check the dates in your tools to see if your tool properly handles leap year.

Author

Brian Carrier (carrier at cerias.purdue.edu) created the test cases and the test image. This test was released on February 29, 2004.

Disclaimers

Neither Purdue University or CERIAS sponsor this work.

These tests are not a complete test suite. These were the first ones that I thought of and no formal theory was put into their design.

Passing these tests provides no guarantees about a tool. Always use additional test cases (and email them to me so we can all benefit!).