@



This repository ▼ Search or type a command

Explore Features Enterprise Blog

Sign up | Sign in

7

0



williballenthin / INDXParse

<> Code

(!) Issues

♣ Pulse

III Graphs

Network

HTTPS clone URL

Subversion. 3

https://github.com

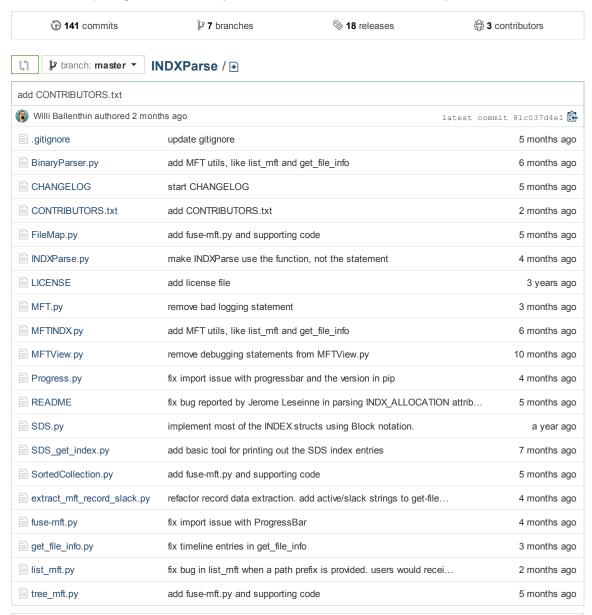
You can clone with HTTPS or

Clone in Desktop

Download ZIP

n Pull Requests

Tool suite for inspecting NTFS artifacts. http://www.williballenthin.com/forensics/mft/indxparse/



■ README

INDXParse

==========

Introduction

INDX files are features of the Windows NTFS file system. They can be thought of as nodes in a B+ tree, where each directory has an INDX file. The INDX files contain records for each file within a directory. Records contain at least the following information:

- Filename
- Physical size of file

- Logical size of file
- Modified timestamp
- Accessed timestamp
- Changed timestamp
- Created timestamp

INDX files are interesting to forensic investigators for a number of reasons. First, an investigator may use INDX files as a source of timestamps to develop a timeline of activity. Secondly, these files have significant slack spaces. With careful parsing, an investigator may recover old or deleted records from within these data chunks. In other words, the investigator may be able to show a file existed even if it has been deleted.

INDX files are not usually accessible from within the Windows operating system. Forensic utilities such as the FTK Imager may allow a user to extract the file by accessing the raw hard disk. FTK names the INDX file "\$I30". Tools like the Sleuthkit can extract the directory entries from a forensic image. INDXParse will not work against a live system.

Previous work & tools

I'd like to first mention John McCash, who mentioned he was unaware of any non-EnCase tools that parse INDX files in a SANS blog post. That got my mental gears turning.

I started out with a document called NTFS Forensics: A Programmers View of Raw Filesystem Data Extraction by Jason Medeiros. Unfortunately, while this document describes parsing INDX files in detail, a number of steps in the explanation were wrong.

The second resource I used, and used extensively, was Forensic computing by A. J. Sammes, Tony Sammes, and Brian Jenkinson. I found the relevent section was available for free via Google books. This was an excellent document, and I now plan on buying the full book.

42 LLC provides the INDX Extractor Enpack as a compiled EnScript for EnCase. This was not useful to me, because I was unable to get to the logic of the script.

The Sleuthkit has INDX structures defined in the tsk_ntfs.h header files. I didn't do much digging in the code to see if TSK does any parsing of the INDX files (I suspect it does), but I did use it to verify the file structure.

Usage

INDXParse.py accepts a number of command line parameters and switches that determine what data is parsed and output format. INDXParse.py currently supports both CSV (default) and Bodyfile (v3) output formats. The CSV schema is as follows:

- Filename
- Physical size of file
- Logical size of file
- Modified timestamp
- Accessed timestamp
- Changed timestamp
- Created timestamp

INDXParse.py will parse INDX structure slack space if provided

```
the '-d' flag. Entries identified in the slack space will be
tagged with a string of the form "(slack at ###)" where ### is
the hex offset to the slack entry. Note that slack entries will
have separate timestamps from the live entries, and could be
used to show the state of the system at a point in time.
If the program encounters an error while parsing the filename,
the filename field will contain a best guess, and the comment
"(error decoding filename)". If the program encounters an error
while parsing timestamps, a timestamp corresponding to the UNIX
epoch will be printed instead.
The full command line help is included here:
INDX $ python INDXParse.py -h
usage: INDXParse.py [-h] [-c | -b] [-d] filename
Parse NTFS INDX files.
positional arguments:
            Input INDX file path
 filename
optional arguments:
  -h, --help show this help message and exit
             Output CSV
  -b
             Output Bodyfile
             Find entries in slack space
  -d
INDXTemplate.bt is a template file for the useful 010 Editor.
Use it as you would any other template by applying it to INDX files.
TODO
  - Brainstorm more features ;-)
License
INDXParse is released under the Apache 2.0 license.
Contributors
-----
  - Jerome Leseinne for identifying a bug in the is_valid constraint and null blocks
```

© 2014 GitHub, Inc. Terms Privacy Security Contact



Status API Training Shop Blog About