INDXParse: A suite of tools for inspecting NTFS artifacts

INDXParse is a suite of tools forensic investigators can use to inspect NTFS artifacts. Although INDXParse was once a single tool for working with directory index entries, the project now includes many more capabilities. These includes file enumeration, metadata extraction, logical tree browser GUI, and more.

Download

All INDXParse tools are free and open source. The source for INDXParse is hosted on Github here.

Highlights

INDX parsing INDXParse.py is a tool that parses NTFS directory index entries, or INDEX records, from INDX attributes. Investigators have often used this technique to recover metadata about previously deleted files.

Timelining list-mft is a tool that lists the files and directories present on a NTFS file system using only the MFT file. It is fairly performant, and uses a constant amount of memory — `list-mft` easily processes an 8GB MFT.

GUI browser [MFTView] is a graphical interface used to explore MFT files. It provides a familiar tree view to explore the files and directories present on a NTFS file system using only the MFT file. It also enables an investigator to manually inspect each record and review parsed attributes.

Record inspector get-file-info is a tool for inspecting individual NTFS MFT records. An analyst can use it to review the metadata associated with a file path, including timestamps, attributes, and data runs. You'll find the tool useful to challenge or confirm artifact interpretations and recover evidence of deleted files.

Fuse driver fuse-mft is a FUSE file system driver that exposes the file system tree defined by an MFT. This allows an investigator to use battle tested tools (such as `ls`, `cat`, or `tree`) to explore the files, directories, and metadata using only the raw MFT (a relatively small file that compresses well).

Slack extractor [extract-mft-record-slack] is a tool that extracts the record slack space from the end of each MFT record. Investigators inspect these buffers for evidence of previously deleted files.

Free All INDXParse tools are free and open source. Forensic practitioners drive the development by contributing ideas, bug reports, and patches. Since the source is in the open and covered by a liberal licnse, you'll never have to worry about the tools disappearing.

Reusable library [mft.py] is the pure Python module that implements many of the features described above. Its easily to integrate into existing projects, and has been thoroughly tested over many real-life investigations.

Installation

Te INDXParse suite of tools that are distributed together. To acquire INDXParse, download the latest ZIP archive from here or use `git` to clone the source repository:

```
1 git clone https://github.com/williballenthin/INDXParse.git
```

Some of the individual tools have dependencies on other freely available Python modules. You should install these using `pip`, as described here.

- williballenthin.com
  - INDX parsing
  - python-registry module
  - Shellbags analysis
  - python-evtx module
- GitHub
- Twitter
- Curated RSS
- search
- Contact