Windows EWF Extractor

Release 0.1

Lucile Roudier, Victoria Sananikone, Erwan Cordier, Claudio Teixe

Apr 09, 2023

CONTENTS:

1 Usage 3
1.1 Named Arguments 3

2 Requirements 5

3 Internals 7

4 Indices and tables 9

Python Module Index 11

Index 13

This project extracts and parses interesting files and data from a Windows EWF image.

The main extracted files are:

- System registry
- User hives
- **Internet Navigator History:**
  - Edge
  - Internet Explorer
  - Firefox
  - Chrome
- The MFT
- Windows Event Logs

CHAPTER ONE

USAGE

Windows EWF Artifact Extractor

```
usage: win_ewf_extractor.py [-h] [-c CFG] [-o OUTPUT] [-f EWF_FILE]
```

1.1 Named Arguments

-c, --cfg YAML configuration file - Possible fields: extract_registry extract_browsers extract_event_logs extract_mft

-o, --output Output directory for extracted artifacts - ./output by default

-f, --ewf_file Path to first Encase Windows file (.E01 extension)

CHAPTER TWO

REQUIREMENTS

Python dependencies can be installed with using pip:

```
$ python3 -m pip install -r requirements.txt
```

You will also need *sleuthkit* and *libtsk19* installed:

Installation manual here

On debian based systems:

```
# apt-get install sleuthkit libtsk19
```

CHAPTER

THREE

INTERNALS

class modules.artifact_extraction.**ArtifactExtractor**

This class is an abstract class implemented by modules extracting and parsing a specific artifact.

class modules.disk_utils.**EWFImgInfo**(*ewf_handle*)

This class represents a EWF image and contains everything needed by the rest of the project.

modules.disk_utils.**find_file_systems**(*img_info: EWFImgInfo*) → list[pytsk3.FS_Info]

This function finds the various filesystems in a given EWF image.

modules.disk_utils.**find_file**(*path*, *fs*, *root_dir*)

Recursively search for a file with the given path

class modules.registry.**RegistryExtractor**(*output_dir*, *config*)

This class implements ArtifactExtractor to extract system Registry

CHAPTER FOUR

INDICES AND TABLES

- genindex
- modindex
- search

PYTHON MODULE INDEX

W

win_ewf_extractor, **??**

INDEX

A

ArtifactExtractor (*class in modules.artifact_extraction*), 7

E

EWFImgInfo (*class in modules.disk_utils*), 7

F

find_file() (*in module modules.disk_utils*), 7

find_file_systems() (*in module modules.disk_utils*), 7

M

module
    win_ewf_extractor, 1

R

RegistryExtractor (*class in modules.registry*), 7

W

win_ewf_extractor
    module, 1