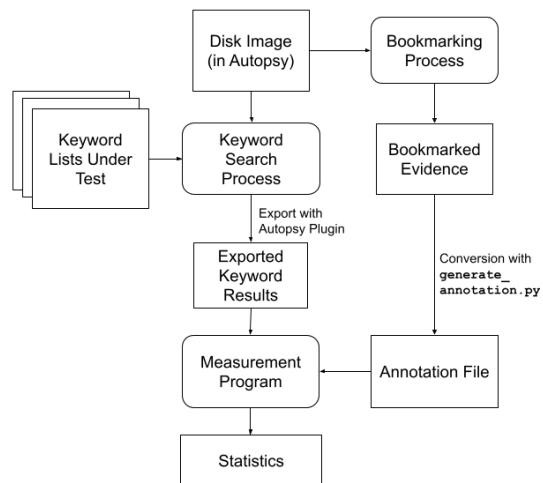


Readme

This set of tools allows keyword lists from autopsy to be evaluated. Please cite as

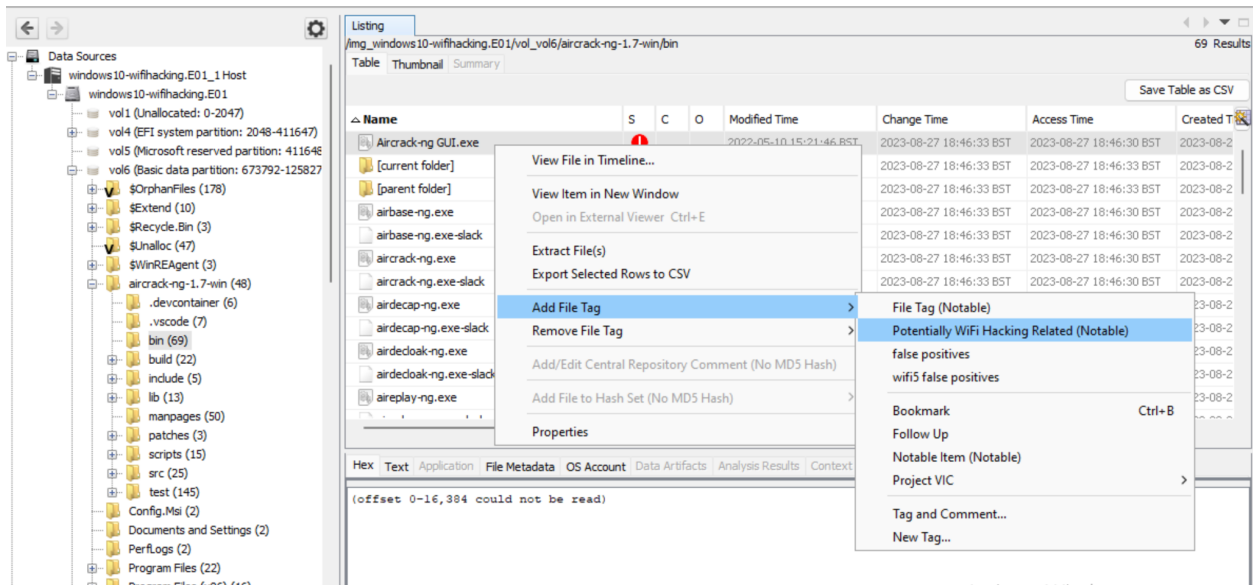
Citation TBC.

The diagram below indicates the overall process and the subsections describe parts of the process.

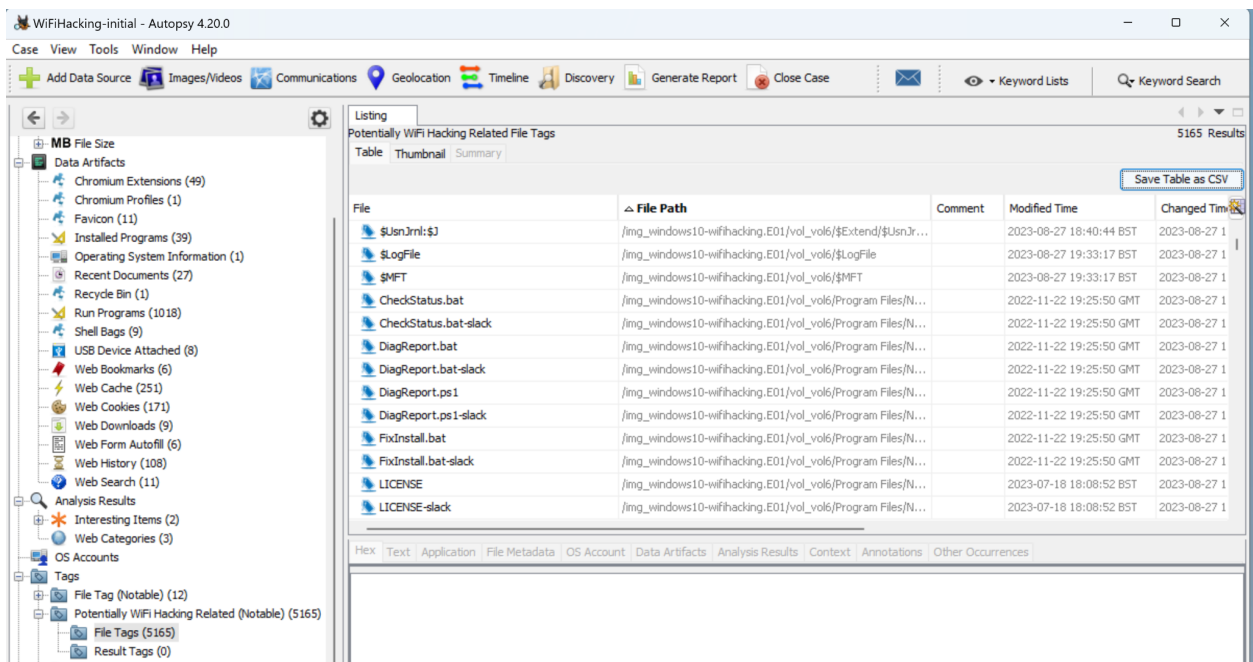


Bookmarking Process

Bookmark files using Autopsy that are considered relevant for the keyword lists under test.



Once finished, export those results by viewing the results and ‘Save Table as CSV’ This produces the “Bookmarked Evidence” in the diagram.



You will also need to hash all the files in the case, and export a full file list (comma delimited) using the Report function of Autopsy (Files - Text), **including all columns**. Note that the annotation script used later is hard coded with column numbers so if Autopsy changes this output the script may need to be updated.

Generate Report

Select and Configure Report Modules

Report Modules:

☐ HTML Report

☐ Excel Report

☒ Files - Text

☐ Data Source Summary Report

☐ Save Tagged Hashes

☐ Extract Unique Words

☐ TSK Body File

☐ Google Earth KML

☐ CASE-UCO

☐ Keyword Export Report Module

☐ FEA - Email Validation - 1.0

☐ FEA - BC Wallet Validation

☐ FEA - Credit Card Validation

☐ Portable Case

A delimited text file containing information about individual files in the case.

☐ Tab delimited

☒ Comma delimited

< Back

Next >

Finish

Cancel

Help

Generate Report

Configure File Report

Select items to include in File Report:

☒ Name

☒ File Extension

☒ File Type

☒ Is Deleted

☒ Last Accessed

☒ File Created

☒ Last Modified

☒ Size

☒ Address

☒ Hash Value

☒ Known Status

☒ Permissions

☒ Full Path

Select All

Deselect All

< Back

Next >

Finish

Cancel

Help

Annotation File

Use the `generate_annotation_from_autopsy.py` script to generate an “Annotation File” from the exported bookmarks.

This takes file list output from Autopsy and exported bookmarks and generates an annotation file flagging relevant and non-relevant

```
usage: generate_annotation_from_autopsy [-h] [-f--fullfilelist
FULL_FILE_LIST_PATH] [-b BOOKMARKS_PATH] [-o OUTPUT_FILE_PATH]
[--force]
```

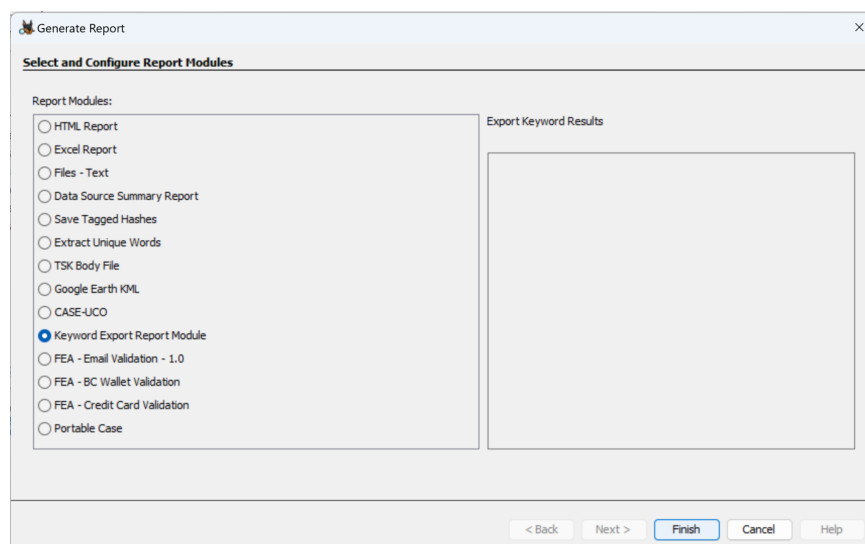
options:

```
-h, --help            show this help message and exit
-f--fullfilelist FULL_FILE_LIST_PATH
                        path to full file list CSV file
-b BOOKMARKS_PATH, --bookmarks BOOKMARKS_PATH
                        path to bookmark export csv file
-o OUTPUT_FILE_PATH, --output OUTPUT_FILE_PATH
                        path to output annotation file
--force               overwrite existing file
```







This produces the annotation file in the folder specified in -o.

Keyword Search Process

Assemble your word lists and run the search. Use the Autopsy Plugin to export the keyword results into the defined json format. The exported information will be in the Reports subfolder of your case.



« Repo... > WiFi Hacking Keywords V3 Keyword Export Report Module 10-10-2023-08...

Name	Date modified	Type
 debug.txt	10/10/2023 08:51	Text Dc
 logfile.txt	10/10/2023 08:51	Text Dc
 report-all.csv	10/10/2023 08:51	OpenO
 report-all.json	10/10/2023 08:51	JSON S
 report-LIST-wifi_list6g.csv	10/10/2023 08:51	OpenO
 report-LIST-wifi_list6g.json	10/10/2023 08:51	JSON S

Statistics Calculations

Use the script `check_results.py`

```
usage: check_results [-h] [-i [SEARCHESFOLDER]] [-a
ANNOTATION_FILE_PATH] [-o OUTPUT_FOLDER_PATH] [--ignoreslack]
[--ignoreunalloc]
```

Takes keyword hits output and an annotation file and computes stats

options:

```
-h, --help            show this help message and exit
-i [SEARCHESFOLDER], --input [SEARCHESFOLDER]
                        path to single file or directory containing
```




JSON files

```
-a ANNOTATION_FILE_PATH, --annotation ANNOTATION_FILE_PATH
                        path to annotation file
-o OUTPUT_FOLDER_PATH, --output OUTPUT_FOLDER_PATH
                        path to output folder
--ignoreslack          Ignore all slack files
--ignoreunalloc        Ignore all unallocated files
```

For example:

```
python3 check_results.py -i kw_output/ -a
wifi-annotations/updated-wifi-annotations_v4.txt -o output
--ignoreslack --ignoreunalloc
```

This will produce output as shown below. The summary_results.csv contains the statistics and the individual folders contain file listings of true and false positives and negatives.

```
>  analysis-all-2023-10-10T08-56-19.055273
>  analysis-LIST-wifi_list6g-2023-10-10T08-56-18.764368
 summary_results.csv
```

summary_results

Searches	Relevant	Non-relevant	TP	FP	TN	FN	R	P	F1	F05	F2	F3
LIST-wifi_list6g	2772	116045	1436	236	115809	1336	0.5180	0.8589	0.6463	0.7590	0.5627	0.5394
all	2772	116045	1436	236	115809	1336	0.5180	0.8589	0.6463	0.7590	0.5627	0.5394