SPIDER + MapperV2

DuffyAPP-IT
@j_duffy01

Contents

SPIDER + MapperV2 Application

SPIDER

SPIDER is designed to enable members of the public from a non-forensic background to discover new artefacts (or in other words, 'things' of interest) in an iOS Filesystem Dump.

See iPhone-rootFS-tool at https://github.com/DuffyAPP-IT/iPhone-rootFS-tool as a resource for obtaining a Filesystem Dump.

SPIDER will generally return a variety of databases, text files (and potentially user media) in which your device holds personal data, and identifying where this data is held in a decrypted form on your device.

SPIDER fulfils this using personal information you have supplied in the configuration files. Each selection of data, for example a name or address, should be placed on a newline in the empty spider configuration file (generated upon launch).

MapperV2

MapperV2 is designed to facilitate two core aims.
The first is to clear empty folders, and files smaller than 50 bytes - This helps to clear the majority of mess in the iOS Filesystem Dump, and allows you to focus on the data which could potentially be of value.

Of course, there's an inherent risk here of removing files from the dump that could possibly be of use. I've found 50bytes and lower to be of a great benefit (removing many useless files) and having no impact on the user-data found. This value can be changed to your liking in the Bash Script.

MapperV2 also facilitates extracting various hidden user media files within iOS - It does this by looping through files that meet a certain specification, then executing the *nix '**file**' utility to determine the correct filetype regardless of the file extension. These files are then opened in the user's default photo/media viewer (Preview, in most cases).

I've decided to include **MapperV2** and **SPIDER** in the same repository due to their similar goals - but they're of course very different as one utilises supplied data and the other works in a 'blind' mode so to say.

Requirements

The software is delivered as a bash script, and so is not limited to any particular Operating System. However I have only tested the software on macOS High Sierra, Catalina & Big Sur.

As no OS-Specific processes or utilities are called, Linux-based Operating Systems should also be compatible.

Development Process Overview

https://www.youtube.com/watch?v=neBA5JHR1Hg - SPIDER + MAPPER - iOS Research Automation, Artefact Finding -Public Resource

https://www.youtube.com/watch?v=g459FT92fcQ - Utilising SPIDER To Find Interesting Artefacts In iOS