SOLVE-IT: A One Page Primer

Chris Hargreaves, 18th July 2025, v1.0

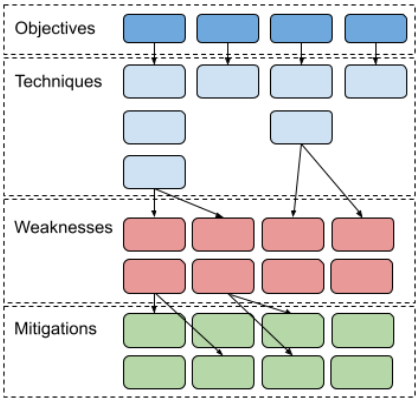
1. Overview

The SOLVE-IT knowledge base (*Systematic Objective-based Listing of Various Established digital Investigation Techniques*) is conceptually inspired by MITRE ATT&CK and aims to capture digital forensic techniques that can be used in investigations. It includes details about each technique, examples, potential ways the technique can go wrong (weaknesses), and mitigations to either avoid, detect, or minimize the consequences of a weakness if it does occur. The latest released version is available in the releases section of the GitHub repository, which includes an Excel spreadsheet that can be used to easily view the data.

2. Structure

The knowledge base on GitHub has a `/data` subfolder containing knowledge base data in JSON format, with a downloadable Excel version for easier reviewing.

Techniques are organised around objectives, which reflect the goals that an examiner might wish to achieve in an investigation, e.g. 'acquire data'. Under that objective there are several techniques that describe how an examiner could achieve that goal (indexed by *technique_id* e.g. T1002), e.g. for 'acquire data', the technique 'create disk image' could be used.



Techniques contain pointers to weaknesses associated with the technique (indexed by *weakness_id,* e.g W1004) and mapped against ASTM E3016-18 error classifications (Standard Guide for Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis). Weaknesses in turn contain references to mitigations (indexed by *mitigation_id,* e.g. M10001).

3. Applications

SOLVE-IT has many applications, and examples are described in the original DFRWS EU paper and presentation, and further examples are included in the SOLVE-IT examples repository. Applications include: reviewing a Standard Operating Procedure (SOP) for unmitigated weaknesses, designing error-focused datasets to test digital forensic tools, identifying weaknesses with no mitigations which highlights research gaps, providing an index of academic work mapping techniques, or mitigations to techniques' weaknesses, and many more.

4. Tools Provided

There are several tools provided in the repository for working with the knowledge base, most notably `generate_excel_from_kb.py` which can be used to compile an Excel version of the JSON data, and `generate_evaluation.py` which can be used to organise and present a specified subset of the techniques that have been used (e.g. in a procedure or investigation), to provide a worksheet that facilitates checking if mitigations were in place during the use of the specified set of techniques.

5. Contributing

Contributions to SOLVE-IT are encouraged: you can add or update the details of techniques, weaknesses, mitigations or tooling, or contribute documentation or applications. Details on how to contribute are available in the CONTRIBUTING.md file.