SOLVE-IT Exercise: Reviewing class exercise examination workflows

Overview for instructors

Version	0.1 DRAFT
Author	Chris Hargreaves
Prerequisites	● Completion of a practical, examination based-exercise ● An introduction to the SOLVE-IT knowledge base ● Python, Excel
Intended Learning Outcomes (ILOs)	At the end of this exercise you will be able to: ● Deconstruct a forensic tool workflow or process into its component parts at the granularity of SOLVE-IT techniques. ● Evaluate a digital forensic process you carried out using the SOLVE-IT knowledge base and identify weaknesses. ● Consider the residual weaknesses when mitigations are used.
Instructor notes	This exercise is designed as an add-on to the end of a practical examination of a data source e.g. a disk image or phone extraction. Students will need to consider the tools and processes used, dissect them into component parts and map them against SOLVE-IT techniques. They will then need to use the SOLVE-IT knowledge base to enumerate known weaknesses in those techniques, consider mitigations in place, highlighting any unmitigated weaknesses, and therefore potential problems with the examination. Students should also be encouraged to think about weaknesses in techniques that are not currently mapped, and submit those to the knowledge base for inclusion.

SOLVE-IT Exercise: Reviewing class exercise examination workflows

1. Pre-requisites

This exercise assumes you have just completed an examination of a digital data source, e.g. a forensic image or phone extraction.

The exercise also assumes you are familiar with the SOLVE-IT knowledge base structure, but you will gain insight into the content and details during the exercise.

2. Aim

The overall aim of the exercise is for you to gain experience of dissecting often opaque forensic tool workflows into component parts at the resolution of SOLVE-IT techniques. This allows the potential weaknesses at each stage to be identified and if necessary, mitigated.

3. Overview of the Tasks

The aim of this exercise will be met as you compile and complete a *SOLVE-IT evaluation worksheet* based on your examination. To get to the point where this can be done there are several steps to work through:

1. Review of the examination you carried out and identification of SOLVE-IT techniques used.
2. Compilation of *SOLVE-IT evaluation worksheet* using the provided python scripts.
3. Completion of the worksheet, documenting the mitigations in place for the enumerated weaknesses.
4. [optional] Identification of techniques, weaknesses or mitigations that are missing from the SOLVE-IT knowledge base and submitting them for review.

3.1 Review of your examination

This task should produce a list of SOLVE-IT techniques that were used as part of your investigation, and ideally any dependencies between them.

You should consult your notes on the examination you undertook. Think about what you did, what processes you ran using the tools.

You can evaluate your response to this task by thinking about if you can map all the way from the raw data in the disk image or phone extraction (or perhaps even the physical item that contained the digital data!), all the way through to tagged artefacts that are relevant to your examination.

3.2 Compilation of a SOLVE-IT evaluation worksheet

This task should result in an Excel-based *SOLVE-IT evaluation worksheet*. You will first need to download the SOLVE-IT repository, install the Python requirements, and this should allow you to run the `generate-evalution.py` script. An example of using this script[1] can be found in the SOLVE-IT examples repository

3.3 Completion of the SOLVE-IT evaluation worksheet

This task should result in a series of weaknesses associated with your process mapped against the mitigations that are in place for each of them.

You will need to review each of the mitigations in turn (or a subset as defined by your instructor), and decide if the proposed mitigations are in place or not. The worksheet will highlight any weaknesses that have zero mitigations in place, and these may be worth thinking about further.

You should document any assumptions you make in completing the worksheet so that they can be discussed and evaluated as to whether they were reasonable assumptions to make.

3.4 Identification of techniques, weaknesses or mitigations

This task is optional and should only be carried out if instructed to do so. For this task you can reflect on the techniques that you used, the weaknesses presented and the mitigation strategies offered in the worksheet.

Any of these concepts could be missing details in the SOLVE-IT knowledge base. You may have used a technique that you think is not covered in the knowledge base. You might have thought of a potential weakness in one of the techniques you used, or you might have identified a mitigation for a weakness that you had in your examination.

List these out as suggested updates for the SOLVE-IT knowledge base. With permission of your instructor, you can use the SOLVE-IT issue tracker[2] to select the correct issue template and submit a proposal to update the knowledge base content.

[1] https://github.com/SOLVE-IT-DF/solve-it-examples/tree/main/forensic_workflow_example_forensic_imaging

[2] https://github.com/SOLVE-IT-DF/solve-it/issues

4. Reflection

Consider the examination that you conducted. Were you aware of the potential problems that could have been present as you were conducting parts of the process? Could any of the workflow or tooling be improved to make the potential problems clearer, and make you use some of the mitigations identified?