# SOLVE-IT Exercise: Weakness Enumeration with TRWM and SHWAMA

## Overview for instructors

| | |
|---|---|
| Version | 0.1 DRAFT |
| Author | Chris Hargreaves |
| Prerequisites | ● An introduction to the SOLVE-IT knowledge base<br>● An introduction to the TRWM methodology |
| Intended Learning Outcomes (ILOs) | At the end of this exercise you will be able to:<br>● Use a systematic approach to determine the technique results, weaknesses and mitigations for a technique in the SOLVE-IT knowledge base. |
| Instructor notes | This exercise will ask students to take a technique from SOLVE-IT, or one that is missing, and to systematically enumerate the weaknesses and mitigations associated with the technique.<br><br>TRWM is the general approach of systematically considering: Technique, Result, Weaknesses and Mitigations.<br><br>TRWM-A is the use of TRWM where specifically the ASTM E3016-18 error classifications are used to iterate through potential weaknesses.<br><br>SHWAMA is the *SOLVE-IT Helper for Weakness And Mitigation Analysis*, which takes the form of a Google Sheet that can be duplicated and used by students to work through the systematic approach. A static Excel copy can also be exported. |

# SOLVE-IT Exercise: Weakness Enumeration with TRWM and SHWAMA

## 1. Pre-requisites

To complete this exercise you should have a general understanding of the SOLVE-IT knowledge base. You should also have been introduced to the TRWM[1] methodology, and have access to the SHWAMA[2] worksheets to help with this.

## 2. Aim

The aim of this exercise is for you to systematically enumerate the weaknesses for a technique in the SOLVE-IT knowledge base.

## 3. Overview of the Tasks

This exercise consists of a workthrough of the SHWAMA worksheets, which use the TRWM-A[3] methodology. This section consists of 'Getting started' followed by subsections for each stage of the walkthrough.

### 3.1 Getting started

Open the template SHWAMA worksheet in Google Drive[4]. You should see something similar to what is shown in Figure 1 below:

[1] TRWM is the approach that systematically reviews in turn Technique, technique Result, Weaknesses, and Mitigations.
[2] SHWAMA (SOLVE-IT Helper for Weakness And Mitigation Analysis)
[3] TRWM-A is the version of the TRWM methodology that specifically uses the ASTM E3016-18 error classifications to iterate through potential weaknesses.
[4] https://docs.google.com/spreadsheets/d/1DRHCP7zAHBfz2TZ8yf3fhcc-bRZD25BT2oUAo1ZN6R4

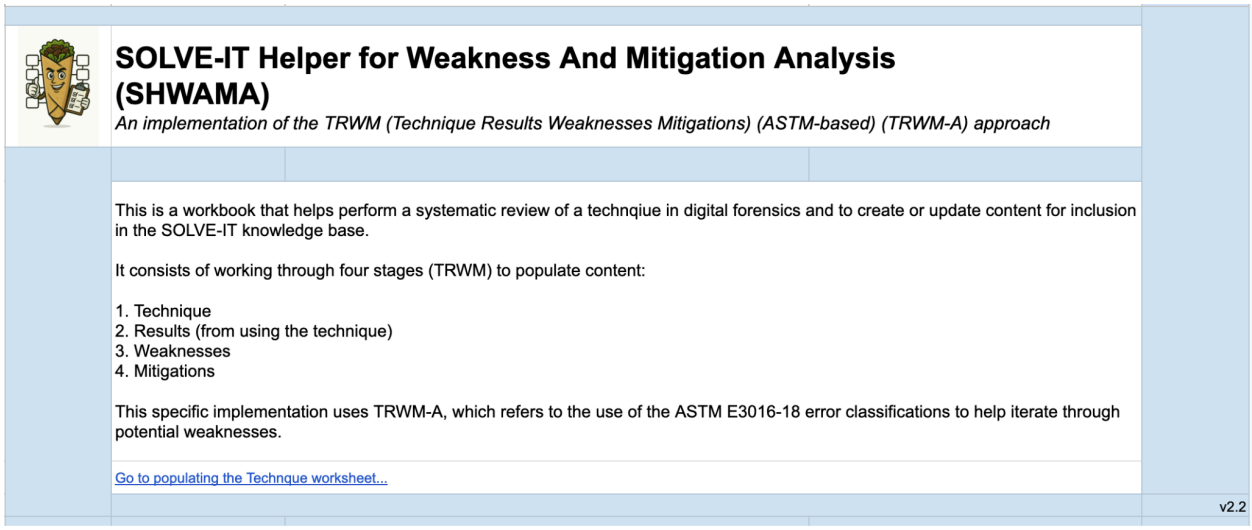



*Figure 1: Shows the 'Information' worksheet of the SHWAMA workbook in Google Drive.*

This workbook will be a read only copy. You should create a copy that you can edit, as shown below in Figure 2:

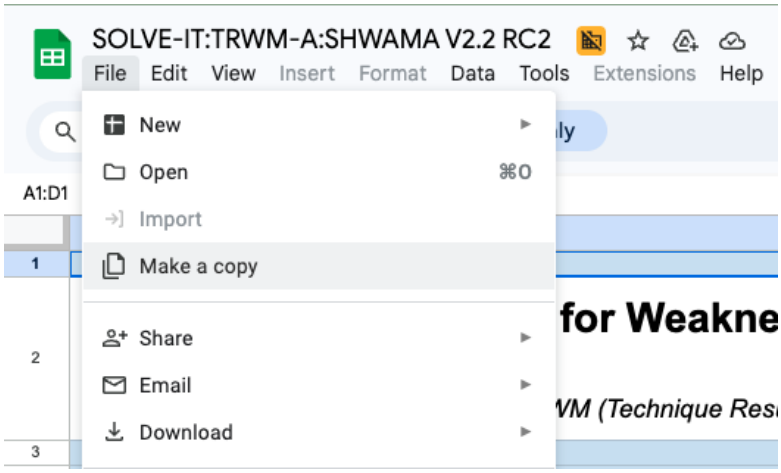



Figure 2: Shows the interface for creating a copy of the read only workbook.

An overview of the process is shown in the information sheet - TRWM refers to: Technique, Results, Weaknesses, Mitigations. These steps are discussed in the subsections that follow.

## 3.2 (T) - Technique

First, the technique must be selected. You may be asked by your instructor to consider a specific technique or you may be free to choose your own.

If these are not details provided already, establishing the definition(s) of what this technique entails is the starting point. Look at digital forensic literature and propose a definition for this technique.

You may at this point also want to look for other details to complete, e.g. synonyms, examples of tools and processes that make use of this technique, and/or cases that have used it.

These details will help you with scoping during the next parts of the task.

Within the helper worksheet, you will find placeholders to assist you with completing these fields. An example for a completed technique (T1073: Calendar app examination) is shown in Figure 3 below. This example is used throughout the rest of the exercise explanation[5].

[5] The full worksheet for the *T1073:Calendar app examination* example is available here: https://docs.google.com/spreadsheets/d/1_NW3kVW7Op8fkKVXNetYbS96WZd8hrerK0ePQso7ndA

## SOLVE-IT Helper for Weakness And Mitigation Analysis (SHWAMA)

*An implementation of the TRWM (Technique Results Weaknesses Mitigations) (ASTM-based) (TRWM-A) approach*

**Explanation**

This phase is to document the nature of the technique, and provide a description and examples of use.

Ideally the name and description of the technique would come from an academic, government or industry source, but some techqniues do not have a clean definition in literature.

Additional explanatory notes for each field are provided on the right hand side.

| ***Field*** | ***Contents*** | ***Notes*** |
|---|---|---|
| SOLVE-IT repo link: | https://github.com/SOLVE-IT-DF/solve-it/blob/main/data/techniques/T1073.json | *You can copy the link from the project repo address bar e.g. https://github.com/SOLVE-IT-DF/solve-it/blob/main/data/techniques/T1000.json* |
| Technique ID: | T1073 | *This is only needed if this is an existing techqniue, ignore this if a new technique is being proposed.* |
| Technique name: | Calendar app examination | *Current or proposed name for the technique.* |
| Technique description: | The analysis of built in or third-party calendar applications. | *A description or defintion of the technique. This will ideally be backed by literature from academia, government or industry.* |
| Synonyms: | | *Many techniques in digital forensics are referred to by multiple names. Synonyms for the technique can be added here to assist SOLVE-IT users in finding the relevant technique.* |
| Technique details: | This techqniue has the potential to associate the owner of the smartphone to specific locations at specific times (adapted from Alghafli et al. 2011) | *This field can be used to provide more details beyond the definition, to keep that definition concise.* |
| Examples: | | *Here examples can be provided that make use of the technique.* |
| References: | Alghafli, K.A., Jones, A. and Martin, T.A., 2011. Guidelines for the digital forensic processing of smartphones. 9th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, 5th -7th December 2011<br><br>Metz (2009) E-mail and appointment falsification analysis, Forensic Focus, https://www.forensicfocus.com/articles/e-mail-and-appointment-falsification-analysis | *Where possible, please provide references to support the details provided above.*<br><br>*References should not be added just because they are about a topic, but should have meaningful implications in terms of explaining a technique.*<br><br>*For large references, consider supplying the page or chapter number if appropriate.*<br><br>*Harvard referencing is used for now, but we will move to bibtex representations in future.* |

Go to populating the Results worksheet...

*Figure 3: Shows the 'Technique' worksheet of the SHWAMA workbook in Google Drive.*

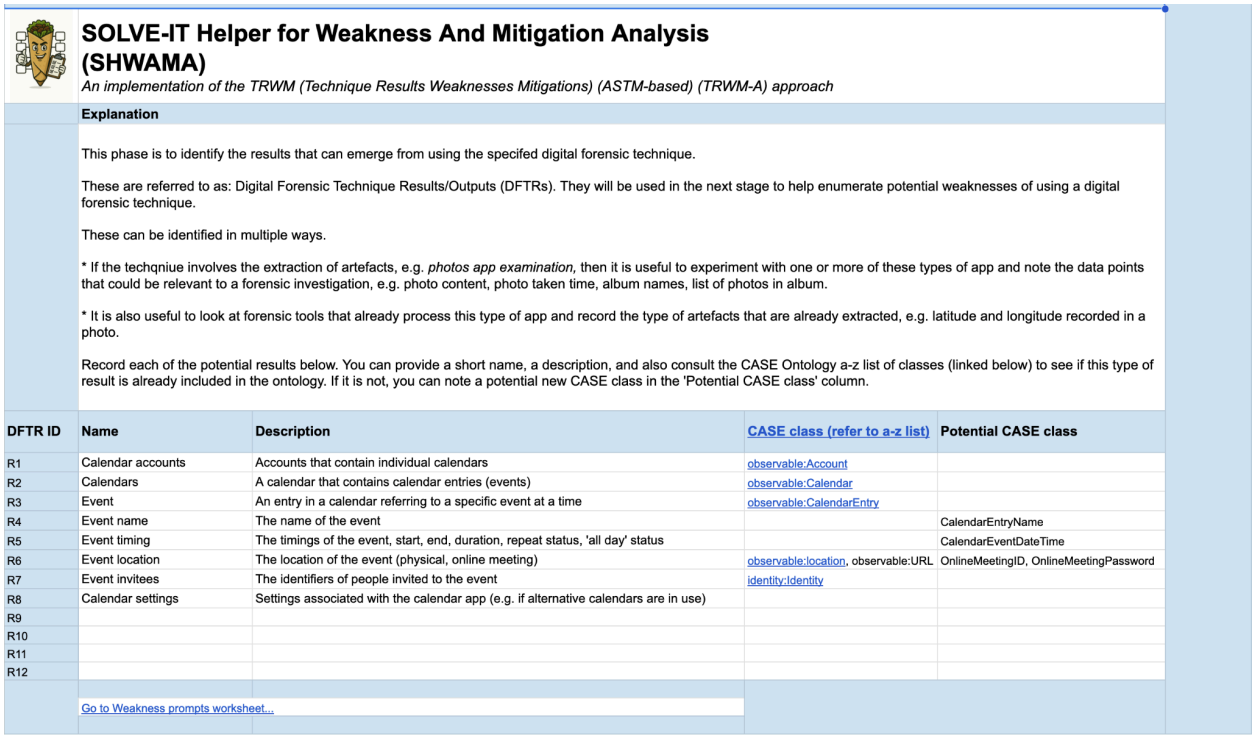
## 3.3 (R) - Results

This next step is more involved and requires consideration of the digital forensic technique and the nature of the results of using the technique. There are multiple approaches to assist with this:

- **If the technique is the examination of a type of app, you should consider that app carefully.**
    - There may be multiple implementations of the app type, e.g. for *T1072: Chat app examination*, examples are WhatsApp, Telegram, Signal, and iMessage, but there are many others. The more implementations you consider the more comprehensive your output will be.

    - You should explore an example of the app under consideration. Think about what pieces of data are forensically useful. This might include user generated content, timestamps, settings and configurations.
- **Examine forensic tool implementation outputs**
    - The existing data extraction performed by forensic tools of the app or apps of the same type can also be insightful.
    - Review the tool output for processing the app or a similar app and note other potentially useful forensic artefacts.
    - Other techniques used by tools can also be considered e.g. timeline generation. Think about what results these techniques produce.
- **Compile a list of all potential Digital Forensic Tool Results (DFTRs)**
    - Using the artefacts identified and other information collected, compile a list of all the potential results from using the technique.
    - Within the helper sheet, there are spaces for a name for the result, a description, and you can also consult the CASE Ontology documentation class A-Z[6] to see if any of the types of results are already included in the ontology. If any result is not, you can also note a potential new CASE class in the column provided.

The relevant parts of the helper sheet are shown in Figure 4 below populated for the Calendar example. You can see some CASE classes already exist and several others are proposed.



**SOLVE-IT Helper for Weakness And Mitigation Analysis (SHWAMA)**

*An implementation of the TRWM (Technique Results Weaknesses Mitigations) (ASTM-based) (TRWM-A) approach*

**Explanation**

This phase is to identify the results that can emerge from using the specifed digital forensic technique.

These are referred to as: Digital Forensic Technique Results/Outputs (DFTRs). They will be used in the next stage to help enumerate potential weaknesses of using a digital forensic technique.

These can be identified in multiple ways.

* If the techqniue involves the extraction of artefacts, e.g. *photos app examination*, then it is useful to experiment with one or more of these types of app and note the data points that could be relevant to a forensic investigation, e.g. photo content, photo taken time, album names, list of photos in album.

* It is also useful to look at forensic tools that already process this type of app and record the type of artefacts that are already extracted, e.g. latitude and longitude recorded in a photo.

Record each of the potential results below. You can provide a short name, a description, and also consult the CASE Ontology a-z list of classes (linked below) to see if this type of result is already included in the ontology. If it is not, you can note a potential new CASE class in the 'Potential CASE class' column.

| DFTR ID | Name | Description | CASE class (refer to a-z list) | Potential CASE class |
|---|---|---|---|---|
| R1 | Calendar accounts | Accounts that contain individual calendars | observable:Account | |
| R2 | Calendars | A calendar that contains calendar entries (events) | observable:Calendar | |
| R3 | Event | An entry in a calendar referring to a specific event at a time | observable:CalendarEntry | |
| R4 | Event name | The name of the event | | CalendarEntryName |
| R5 | Event timing | The timings of the event, start, end, duration, repeat status, 'all day' status | | CalendarEventDateTime |
| R6 | Event location | The location of the event (physical, online meeting) | observable:location, observable:URL | OnlineMeetingID, OnlineMeetingPassword |
| R7 | Event invitees | The identifiers of people invited to the event | identity:Identity | |
| R8 | Calendar settings | Settings associated with the calendar app (e.g. if alternative calendars are in use) | | |
| R9 | | | | |
| R10 | | | | |
| R11 | | | | |
| R12 | | | | |

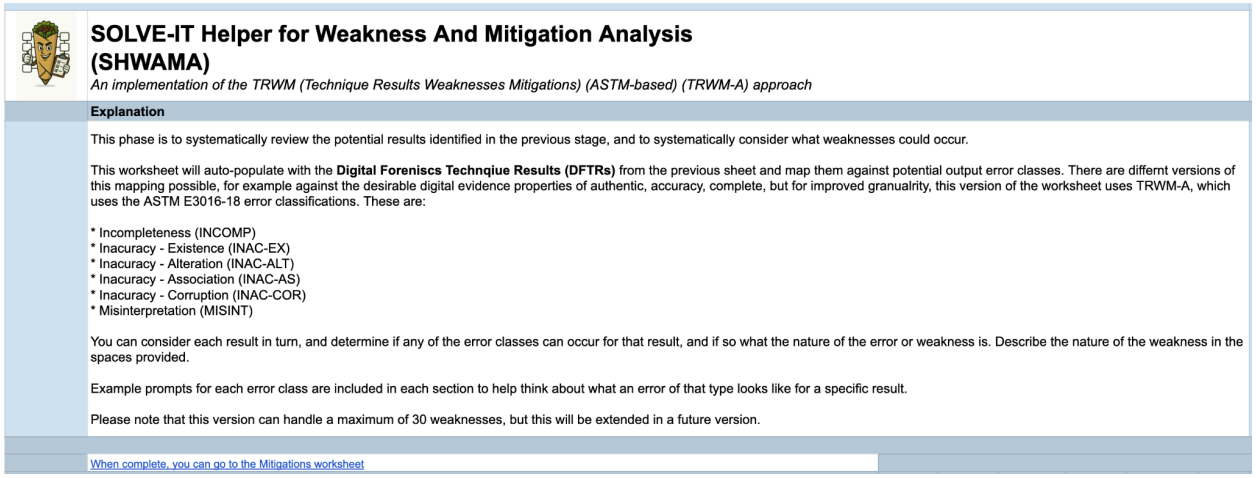
Go to Weakness prompts worksheet...

*Figure 4: Shows the 'Results' worksheet of the SHWAMA workbook in Google Drive.*

[6] https://ontology.caseontology.org/documentation/entities-az.html

## 3.4 (W) - Weaknesses

This stage is focused on enumerating the weaknesses associated with the technique. The guidance provided in the helper sheet is shown in Figure 5.



**SOLVE-IT Helper for Weakness And Mitigation Analysis (SHWAMA)**

*An implementation of the TRWM (Technique Results Weaknesses Mitigations) (ASTM-based) (TRWM-A) approach*

**Explanation**

This phase is to systematically review the potential results identified in the previous stage, and to systematically consider what weaknesses could occur.

This worksheet will auto-populate with the **Digital Foreniscs Technqiue Results (DFTRs)** from the previous sheet and map them against potential output error classes. There are differnt versions of this mapping possible, for example against the desirable digital evidence properties of authentic, accuracy, complete, but for improved granualrity, this version of the worksheet uses TRWM-A, which uses the ASTM E3016-18 error classifications. These are:

* Incompleteness (INCOMP)
* Inacuracy - Existence (INAC-EX)
* Inacuracy - Alteration (INAC-ALT)
* Inacuracy - Association (INAC-AS)
* Inacuracy - Corruption (INAC-COR)
* Misinterpretation (MISINT)

You can consider each result in turn, and determine if any of the error classes can occur for that result, and if so what the nature of the error or weakness is. Describe the nature of the weakness in the spaces provided.

Example prompts for each error class are included in each section to help think about what an error of that type looks like for a specific result.

Please note that this version can handle a maximum of 30 weaknesses, but this will be extended in a future version.

When complete, you can go to the Mitigations worksheet

Figure 5: Shows the introductory text of the Weakness Prompts worksheet.

Within the helper sheet, the Digital Forensic Tool Results (DFTRs) are auto populated from the previous sheet. Figure 6 shows the section for one of those DFTRs (the Calendar Accounts). Within each result, there are spaces provided, along with prompts, to consider what an error looks like (based on the ASTM E3016-18 error classes) for each of the DFTRs.

This allows each result type to be systematically considered against the possible error classes resulting in a thorough assessment of the weaknesses associated with a digital forensic technique.

Note that not all error types will have entries for all DFTRs.

Also note that on the right, there are prefilled checkmarks showing the primary error class for a weakness (based on the subsection that has been completed). You may also override these with additional error classes if appropriate. For example, For *calendar accounts*, the weakness “Presentation of an account that does not exist” has a main category of INAC-EX, but as this could also result in misinterpretation, the MISINT box has been manually checked.

| | | | | INCOMP | INAC-EX | INAC-ALT | INAC-AS | INAC-COR | MISINT | Error class summary |
|---|---|---|---|---|---|---|---|---|---|---|
| | **R1** | **Calendar accounts** | Accounts that contain individual calendars | *Note, these are precompleted to align with the main error class, but additional error classes sometimes apply to a weakness and can be marked with an X.* | | | | | | |
| | **INCOMP** | ***Prompts: failure to recover live artefacts, failure to recover deleted artefacts, other reasons why an artefact might be missed?*** | | | | | | | | |
| | | | Failure to recover live calendar accounts | X | | | | | | INCOMP |
| | | | Failure to recover deleted but recoverable calendar accounts | X | | | | | | INCOMP |
| | | | | X | | | | | | INCOMP |
| | | | | X | | | | | | INCOMP |
| | | | | X | | | | | | INCOMP |
| | **INAC-EX** | ***Prompts: presenting an artefact for something that does not exist*** | | | | | | | | |
| | | | Presentation of an account that does not exist | | X | | | | X | INAC-EX, MISINT |
| | | | | | X | | | | | INAC-EX |
| | | | | | X | | | | | INAC-EX |
| | | | | | X | | | | | INAC-EX |
| | | | | | X | | | | | INAC-EX |
| | **INAC-ALT** | ***Prompts: modifying the content of some digital data*** | | | | | | | | |
| | | | | | | X | | | | INAC-ALT |
| | | | | | | X | | | | INAC-ALT |
| | | | | | | X | | | | INAC-ALT |
| | | | | | | X | | | | INAC-ALT |
| | | | | | | X | | | | INAC-ALT |
| | **INAC-AS** | ***Prompts: presenting live data as deleted and vice versa*** | | | | | | | | |
| | | | Presenting a live account as deleted | | | | X | | | INAC-AS |
| | | | Presenting a deleted account as live | | | | X | | | INAC-AS |
| | | | | | | | X | | | INAC-AS |
| | | | | | | | X | | | INAC-AS |
| | | | | | | | X | | | INAC-AS |
| | **INAC-COR** | ***Prompts: could the process corrupt data, could the process fail to detect corrupt data?*** | | | | | | | | |
| | | | | | | | | X | | INAC-COR |
| | | | | | | | | X | | INAC-COR |
| | | | | | | | | X | | INAC-COR |
| | | | | | | | | X | | INAC-COR |
| | | | | | | | | X | | INAC-COR |
| | **MISINT** | ***Prompts: could results be presented in a way that encourages misinterpretation?*** | | | | | | | | |
| | | | Failing to display that an account was flagged as inactive | | | | | | X | MISINT |
| | | | | | | | | | X | MISINT |
| | | | | | | | | | X | MISINT |
| | | | | | | | | | X | MISINT |
| | | | | | | | | | X | MISINT |

Figure 6: Shows the spaces for weakness enumeration of a single Digital Forensic Tool Result (DFTR) (*Calendar accounts* in this case) mapped against the ASTM E3016-18 error classifications.

Once this sheet is complete, there is a summary provided in the next worksheet (*3b_Weakness (aggregate) (ASTM)* ). This is shown below in Figure 7 and provides a more compact overview of the details that have been provided. There are no details to complete for this worksheet, it is just for information.

**SOLVE-IT Helper for Weakness And Mitigation Analysis (SHWAMA)**

*An implementation of the TRWM (Technique Results Weaknesses Mitigations) (ASTM-based) (TRWM-A) approach*

**Explanation**

There is nothing to edit on this sheet currently. It presents a summary of the weaknesses identtified and their error classes.

Data on this sheet is used to help automatically populate other sheets.

| Automatic Aggregated Weakness List | ASTM | | | | | | |
|---|---|---|---|---|---|---|---|
| | INCOMP | INAC-EX | INAC-ALT | INAC-AS | INAC-COR | MISINT | Error class summary |
| Failure to recover live calendar accounts | X | | | | | | INCOMP |
| Failure to recover deleted but recoverable calendar accounts | X | | | | | | INCOMP |
| Presentation of an account that does not exist | | X | | | | X | INAC-EX, MISINT |
| Presenting a live account as deleted | | | | X | | | INAC-AS |
| Presenting a deleted account as live | | | | X | | | INAC-AS |
| Failing to display that an account was flagged as inactive | | | | | | X | MISINT |
| Failure to recover live calendars | X | | | | | | INCOMP |
| Failure to recover deleted but recoverable calendars | X | | | | | | INCOMP |
| Presenting a calendar that does not exist | | X | | | | | INAC-EX |
| Presenting a live calendar as deleted | | | | X | | | INAC-AS |
| Presenting a deleted calendar as live | | | | X | | | INAC-AS |
| Failure to recover deleted but recoverable events | X | | | | | | INCOMP |
| Failure to recover events removed as archived or synced online | X | | | | | | INCOMP |
| Failure to recover live events from a calendar | X | | | | | | INCOMP |
| Presenting a calendar entry that does not exist | | X | | | | | INAC-EX |
| Associating an event with the wrong calendar | | | | X | | X | INAC-AS, MISINT |
| Associating an event with the wrong account | | | | X | | X | INAC-AS, MISINT |
| Failure to detect modification to the event | | | | | X | X | INAC-COR, MISINT |
| Failure to recover event name | X | | | | | | INCOMP |
| Presenting a calendar name that does not exist | | X | | | | | INAC-EX |
| Missing events due to not taking into account event recurrences | X | | | | | | INCOMP |
| Presenting an event at an incorrect time due to incorrect timezone parsing | | | X | | | | INAC-ALT |
| Failure to recover event location information | X | | | | | | INCOMP |
| Presenting a location not present in the event | | X | | | | | INAC-EX |
| Failure to recover event attendee information | X | | | | | | INCOMP |
| Failure to recover event attendee acceptance detail | X | | | | | | INCOMP |
| Presenting an invitee not assoicated with the event | | X | | | | | INAC-EX |
| Failure to display invitee event acceptance detail | | | | | | X | MISINT |
| Failure to display alternative calendars in forensic tool, when they were in | | | | | | X | MISINT |
| | - | - | - | - | - | - | |

Figure 7: Once complete, the weaknesses will be summarized in the “3b_Weakness (aggregate (ASTM)” worksheet.

## 3.5 (M) - Mitigations

This final stage involves considering the mitigations for each of the weaknesses identified. Figure 8 shows the introductory text for the next sheet (4_Mitigations).

The worksheet will auto populate the weaknesses and their error class as a reminder.

While an approach as systematic as the weakness enumeration does not yet exist, there is some guidance provided as to the types of mitigations that can exist. However, they are not exhaustive and digital forensic literature, tools, techniques, and your own ideas and experience should be drawn upon to populate the mitigations for a particular weakness. You can also make use of existing mitigations in the SOLVE-IT knowledge base.

An example subset of mitigations for the calendar app examination example are shown in Figure 9.

# SOLVE-IT Helper for Weakness And Mitigation Analysis (SHWAMA)

*An implementation of the TRWM (Technique Results Weaknesses Mitigations) (ASTM-based) (TRWM-A) approach*

**Explanation**

This phase is to now think about the mitigations for the weaknesses that have been identified.

Aside from considering each weakness in turn, a systematic method of mitigation enumeration does not yet exist. However, broadly speaking some categories are:
- checking results manually or with another tool
- testing
- using an alternative approach
- using a complimentary approach
- checking for supporting or contradictory information

The weaknesses have been auto populated below and the relevant error classes summarised as a reminder.

**WARNING: The weaknesses are auto populated from earlier data, so if you go back and add or remove weaknesses, mitigations may go out of sync.**

**Note that at present, this prototype can handle at most 30 weaknesses, but will be extended in future.**

| | Total weaknesses: | 29 |
|---|---|---|

When complete, go to the Compact Summary worksheet

*Figure 8: The introductory text from the "4_Mitigations" worksheet.*

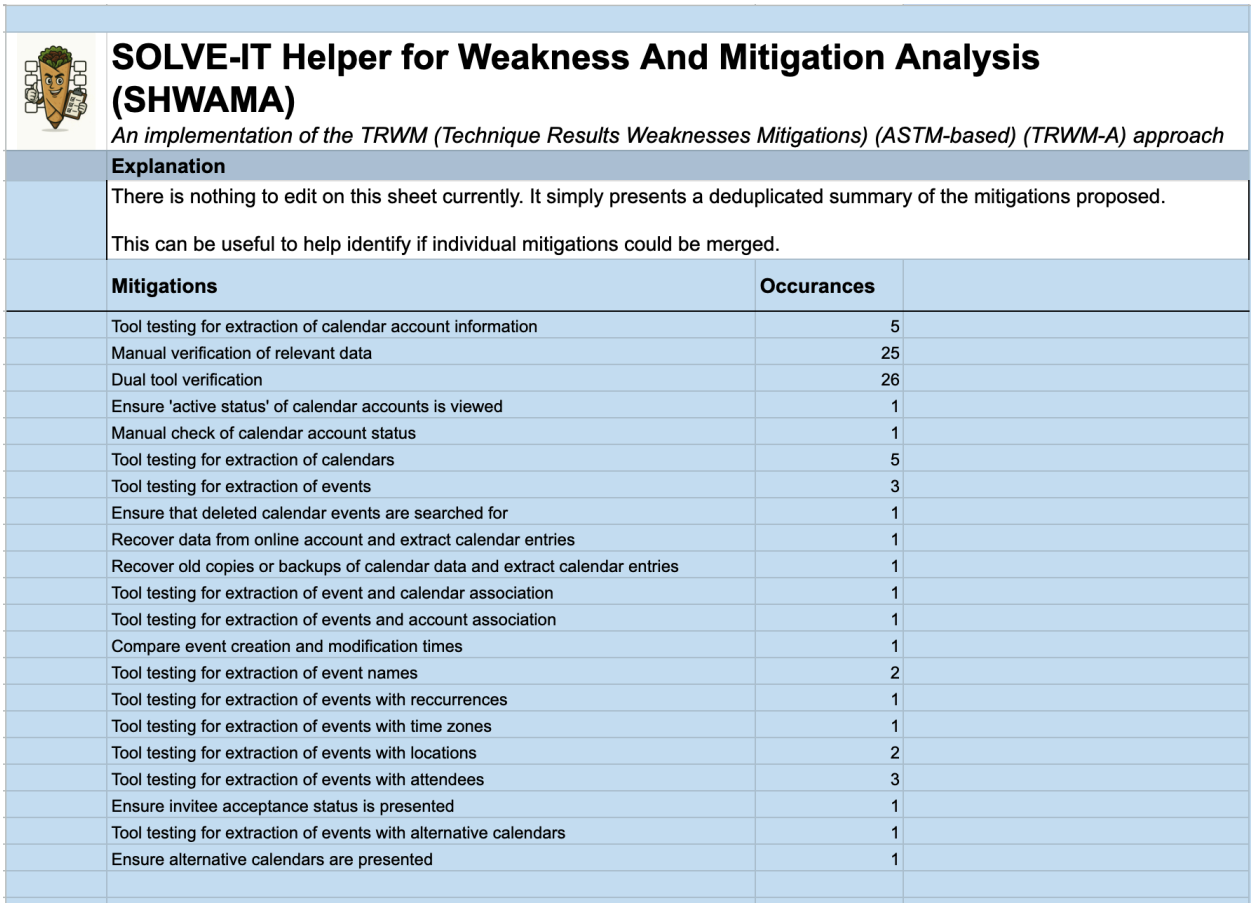
| **Weaknesses** (corresponding results are deliberately not repeated here to ensure that weakness description make sense as stand alone descriptions) | **Reminder of error classes of weakness** | **Proposed mitigation descriptions** |
|---|---|---|
| Failure to recover live calendar accounts | INCOMP | Tool testing for extraction of calendar account information<br>Manual verification of relevant data<br>Dual tool verification |
| Failure to recover deleted but recoverable calendar accounts | INCOMP | Tool testing for extraction of calendar account information<br>Manual verification of relevant data<br>Dual tool verification |
| Presentation of an account that does not exist | INAC-EX, MISINT | Tool testing for extraction of calendar account information<br>Manual verification of relevant data<br>Dual tool verification |
| Presenting a live account as deleted | INAC-AS | Tool testing for extraction of calendar account information<br>Manual verification of relevant data<br>Dual tool verification |

*Figure 9: Shows the section of the worksheet where mitigations can be proposed.*

Once complete. The summary of mitigations proposed are provided in the worksheet '4b_Mitigation Summary'. This can be helpful in identifying duplicates or close duplicates and can be used to refine the list. Figure 10 shows the results from the calendar example.

In terms of some high-level guidance, it is not an exact science as to where to be specific and where to generalise. In some cases generic 'Manual verification of relevant data' is used, and in some it is more specific e.g. "Manually check the calendar account status (live/deleted)".

However, typically the tool testing based mitigations are useful to specify what needs to be tested as these can form the basis of tangible tool testing programmes.



**SOLVE-IT Helper for Weakness And Mitigation Analysis (SHWAMA)**

*An implementation of the TRWM (Technique Results Weaknesses Mitigations) (ASTM-based) (TRWM-A) approach*

**Explanation**

There is nothing to edit on this sheet currently. It simply presents a deduplicated summary of the mitigations proposed.

This can be useful to help identify if individual mitigations could be merged.

| Mitigations | Occurances |
|---|---|
| Tool testing for extraction of calendar account information | 5 |
| Manual verification of relevant data | 25 |
| Dual tool verification | 26 |
| Ensure 'active status' of calendar accounts is viewed | 1 |
| Manual check of calendar account status | 1 |
| Tool testing for extraction of calendars | 5 |
| Tool testing for extraction of events | 3 |
| Ensure that deleted calendar events are searched for | 1 |
| Recover data from online account and extract calendar entries | 1 |
| Recover old copies or backups of calendar data and extract calendar entries | 1 |
| Tool testing for extraction of event and calendar association | 1 |
| Tool testing for extraction of events and account association | 1 |
| Compare event creation and modification times | 1 |
| Tool testing for extraction of event names | 2 |
| Tool testing for extraction of events with reccurrences | 1 |
| Tool testing for extraction of events with time zones | 1 |
| Tool testing for extraction of events with locations | 2 |
| Tool testing for extraction of events with attendees | 3 |
| Ensure invitee acceptance status is presented | 1 |
| Tool testing for extraction of events with alternative calendars | 1 |
| Ensure alternative calendars are presented | 1 |

Figure 10: Shows a summary of the mitigations proposed and the number of occurrences.

## 3.6 Final Summary Sheet

After this process, the final sheet in the workbook will summarize this information in a compact table. An example is shown below in Figure 11 and this sheet can used as the basis for populating a technique, its weaknesses and mitigations within the SOLVE-IT knowledge base.

| *Generated using TRWM/SHWAMA* | *v2.2* | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | |
| **Technique name:** | Calendar app examination | | | | | |
| **Technqiue description:** | The analysis of built in or third-party calendar applications. | | | | | |
| **Synonyms:** | | | | | | |
| **Details:** | This techqniue has the potential to associate the owner of the smartphone to specific locations at specific times (adapted from Alghafli et al. 2011) | | | | | |
| **Examples:** | | | | | | |
| **CASE output classes:** | observable:Account, observable:Calendar, observable:CalendarEntry, observable:location, observable:URL, identity:Identity | | | | | |
| **Propsed CASE classes:** | CalendarEntryName, CalendarEventDateTime, OnlineMeetingID, OnlineMeetingPassword | | | | | |
| **References:** | Alghafli, K.A., Jones, A. and Martin, T.A., 2011. Guidelines for the digital forensic processing of smartphones. 9th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, 5th -7th December 2011<br><br>Metz (2009) E-mail and appointment falsification analysis, Forensic Focus, https://www.forensicfocus.com/articles/e-mail-and-appointment-falsification-analysis | | | | | |
| **Weaknesses and mitigations:** | | **M1** | **M2** | **M3** | **M4** | **M5** |
| Failure to recover live calendar accounts | INCOMP | *Tool testing for extraction of calendar account information* | *Manual verification of relevant data* | *Dual tool verification* | | |
| Failure to recover deleted but recoverable calendar accounts | INCOMP | *Tool testing for extraction of calendar account information* | *Manual verification of relevant data* | *Dual tool verification* | | |
| Presentation of an account that does not exist | INAC-EX, MISINT | *Tool testing for extraction of calendar account information* | *Manual verification of relevant data* | *Dual tool verification* | | |
| Presenting a live account as deleted | INAC-AS | *Tool testing for extraction of calendar account information* | *Manual verification of relevant data* | *Dual tool verification* | | |
| Presenting a deleted account as live | INAC-AS | *Tool testing for extraction of calendar account information* | *Manual verification of relevant data* | *Dual tool verification* | | |
| Failing to display that an account was flagged as inactive | MISINT | *Ensure 'active status' of calendar accounts is viewed* | *Manual check of calendar account status* | | | |
| Failure to recover live calendars | INCOMP | *Tool testing for extraction of calendars* | *Manual verification of relevant data* | *Dual tool verification* | | |
| Failure to recover deleted but recoverable calendars | INCOMP | *Tool testing for extraction of calendars* | *Manual verification of relevant data* | *Dual tool verification* | | |
| Presenting a calendar that does not exist | INAC-EX | *Tool testing for extraction of calendars* | *Manual verification of relevant data* | *Dual tool verification* | | |

Figure 11: Shows an extract from the final summary sheet generated, including the technique details, weakness list, and mapped mitigations.