DFRWS EU 2025

SOLVE-IT: A proposed digital forensic knowledge base inspired by MITRE ATT&CK

Chris Hargreaves, University of Oxford

Harm van Beek, NFI/Open Universiteit

Eoghan Casey, University of Lausanne

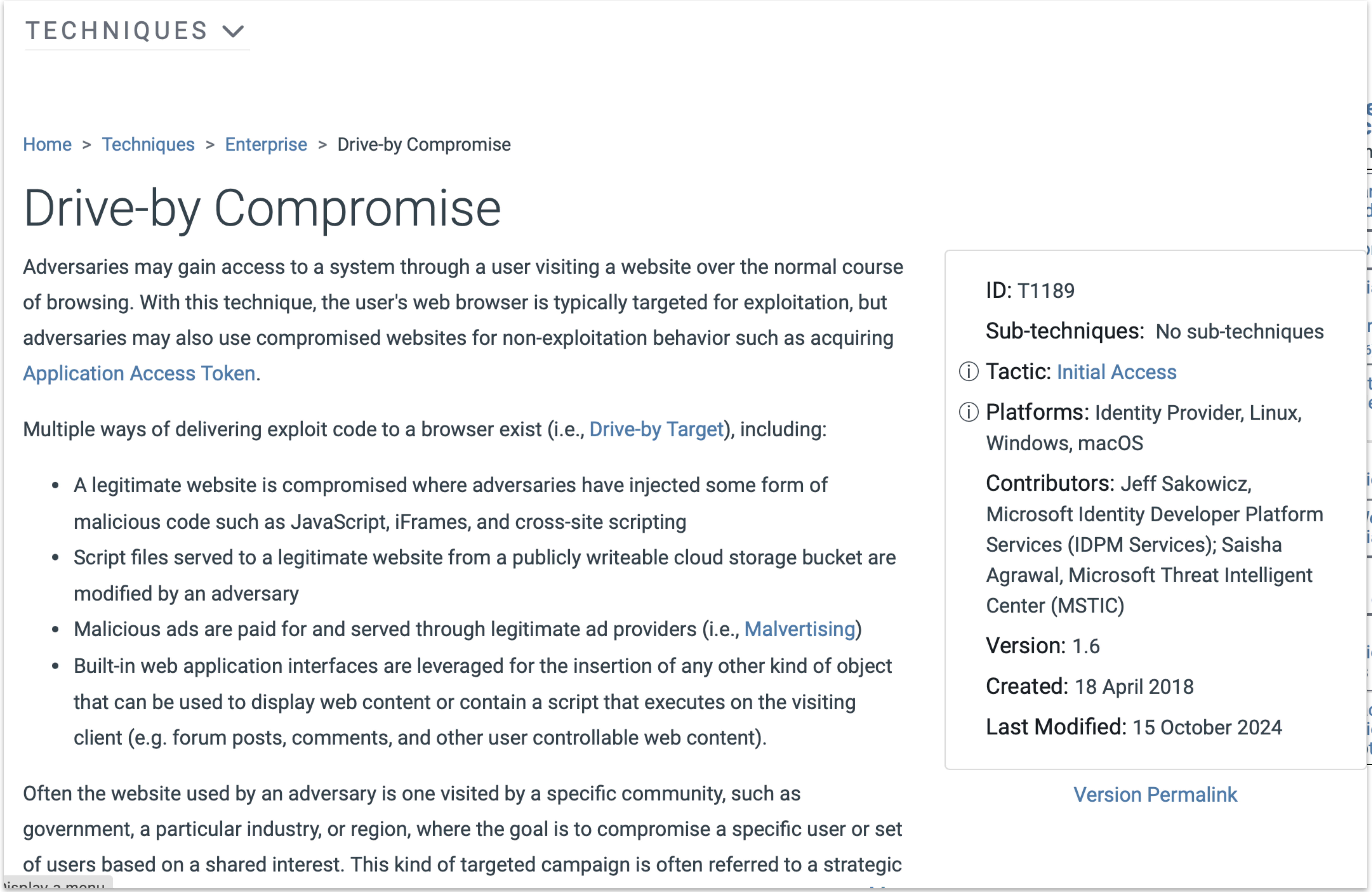
Hargreaves, C., van Beek, H. and Casey, E., 2025. SOLVE-IT: A proposed digital forensic knowledge base inspired by MITRE ATT&CK. Forensic Science International: Digital Investigation, 52, p.301864.

MITRE ATT&CK

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 44 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Col 17 te
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Advers the-Mi
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (11)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archiv Collec Data (
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Autom Collec
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Brows Sessio Hijack
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipbo
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data f Cloud
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Escape to Host	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data f Config Repos
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (17)	Event Triggered	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion		Data f Inform Repos
Search Victim-Owned Websites			Shared Modules			Execution Guardrails (2)		Device Driver Discovery		Data f
						Exploitation for Defense Evasion		Domain Trust Discovery		
						File and Directory Permissions				

https://attack.mitre.org/matrices/enterprise/

MITRE ATT&CK



Home > Techniques > Enterprise > Drive-by Compromise

Drive-by Compromise

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token.

Multiple ways of delivering exploit code to a browser exist (i.e., Drive-by Target), including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting
- Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary
- Malicious ads are paid for and served through legitimate ad providers (i.e., Malvertising)
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic

ID: T1189

Sub-techniques: No sub-techniques

ⓘ Tactic: Initial Access

ⓘ Platforms: Identity Provider, Linux, Windows, macOS

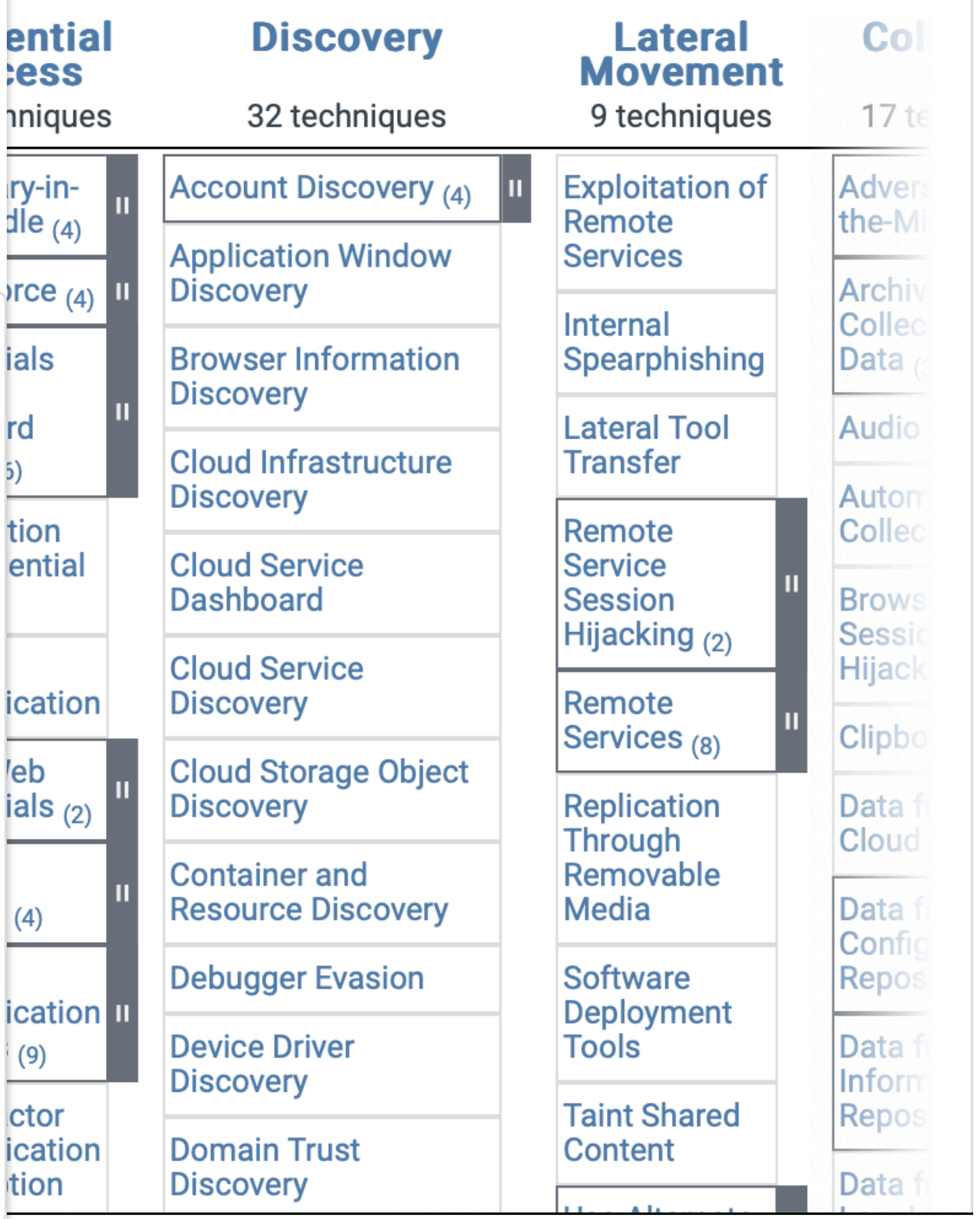
Contributors: Jeff Sakowicz, Microsoft Identity Developer Platform Services (IDPM Services); Saisha Agrawal, Microsoft Threat Intelligent Center (MSTIC)

Version: 1.6

Created: 18 April 2018

Last Modified: 15 October 2024

Version Permalink



Discovery 32 techniques	Lateral Movement 9 techniques
Account Discovery (4)	Exploitation of Remote Services
Application Window Discovery	Internal Spearphishing
Browser Information Discovery	Lateral Tool Transfer
Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)
Cloud Service Dashboard	Remote Services (8)
Cloud Service Discovery	Replication Through Removable Media
Cloud Storage Object Discovery	Software Deployment Tools
Container and Resource Discovery	Taint Shared Content
Debugger Evasion	
Device Driver Discovery	
Domain Trust Discovery	

https://attack.mitre.org/matrices/enterprise/

Also has examples, mitigations, detection etc.

MITRE ATT&CK

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Col
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	32 techniques	9 techniques	17 te

Credential Access	Discovery	Lateral Movement	Col
ary-in- ddle (4)	Account Discovery (4)	Exploitation of Remote Services	Adver the-Mi
orce (4)	Application Window Discovery	Internal Spearphishing	Archiv Collec Data (
tials	Browser Information Discovery	Lateral Tool Transfer	Audio
ord (6)	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Autom Collec
ation dential s	Cloud Service Dashboard	Remote Services (8)	Brows Sessio Hijack
tication	Cloud Service Discovery	Replication Through Removable Media	Clipbo
Veb tials (2)	Cloud Storage Object Discovery	Software Deployment Tools	Data f Cloud
e (4)	Container and Resource Discovery	Taint Shared Content	Data f Config Repos
tication s (9)	Debugger Evasion		Data f Inform Repos
actor tication ption	Device Driver Discovery		Data f
	Domain Trust Discovery		

Mitigations

ID	Mitigation	Description
M1048	Application Isolation and Sandboxing	Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist.[68][69] Other types of virtualization and application microsegmentation may also mitigate the impact of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist for these types of systems.[69]
M1050	Exploit Protection	Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. [70] Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. [71] Many of these protections depend on the architecture and target application binary for compatibility.
M1021	Restrict Web-Based Content	For malicious code served up through ads, adblockers can help prevent that code from executing in the first place. Script blocking extensions can help prevent the execution of JavaScript that may commonly be used during the exploitation process.
M1051	Update Software	Ensure all browsers and plugins kept updated can help prevent the exploit phase of this technique. Use modern browsers with security features turned on.

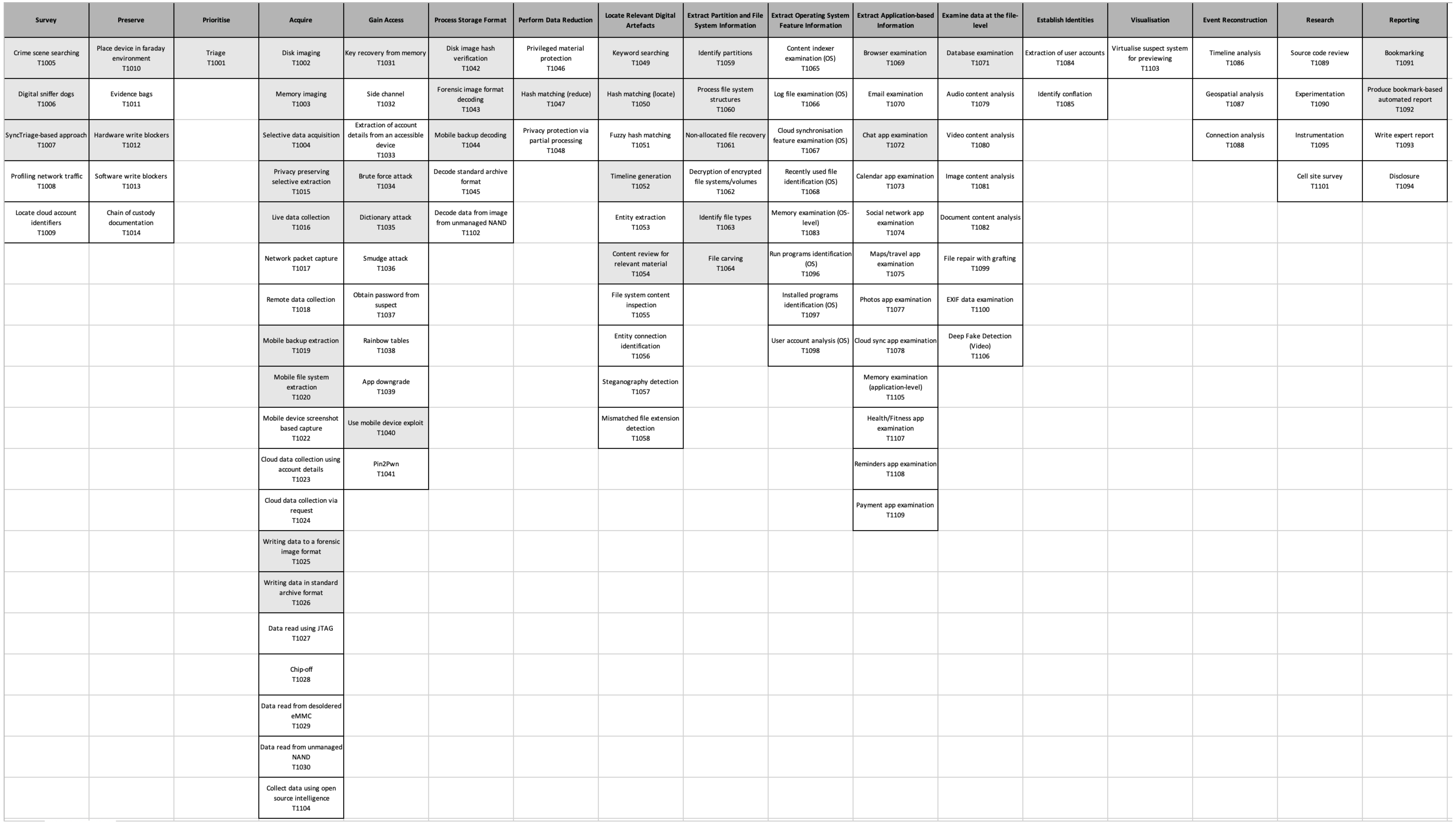
Detection

ID	Data Source	Data Component	Detects

https://attack.mitre.org/matrices/enterprise/

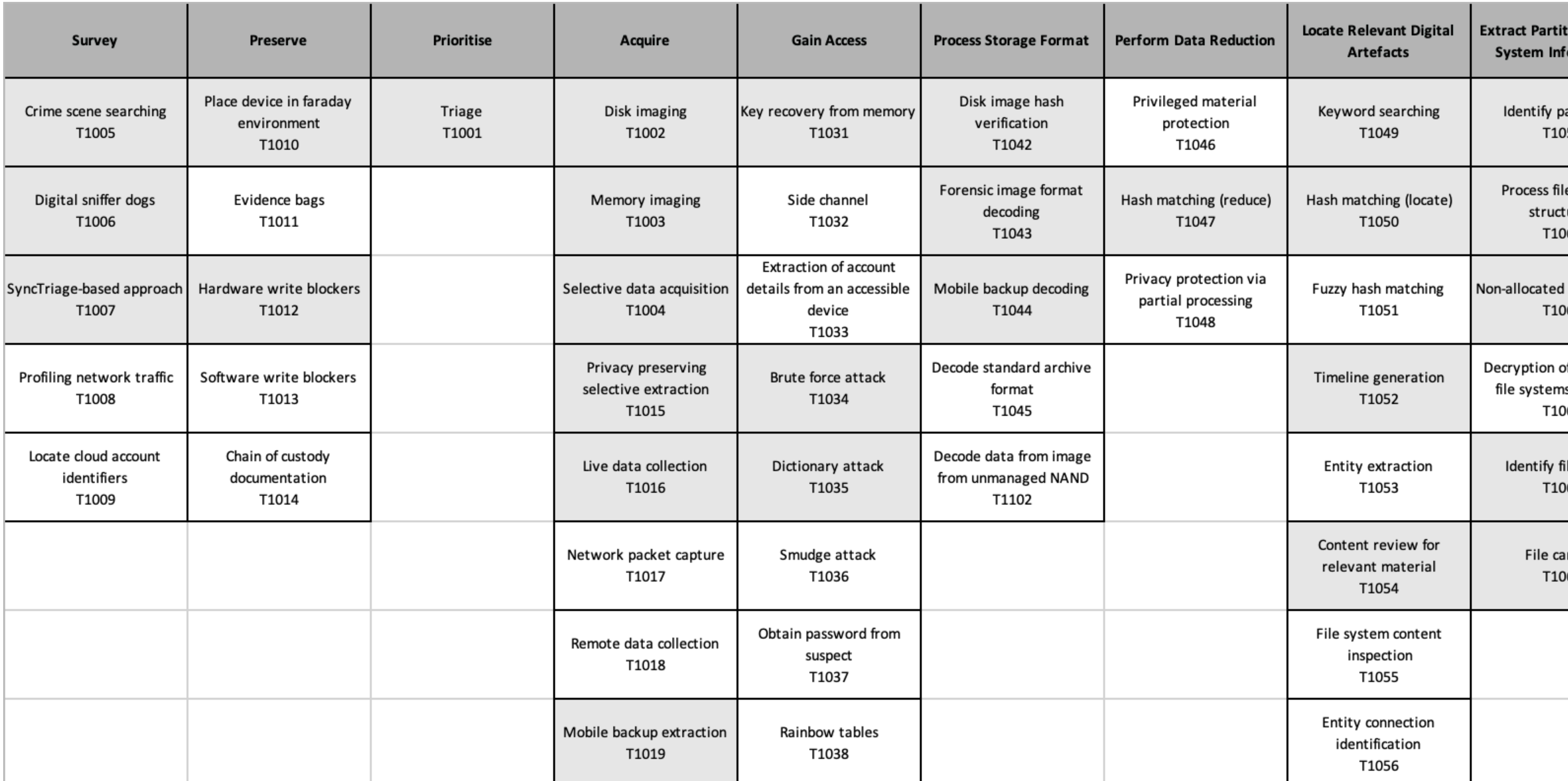
Can we construct something similar for digital forensics **and** is it useful?

Systematic **O**bjective-based **L**isting of **V**arious **E**stablished (digital) **I**nvestigation **T**echniques



Survey	Preserve	Prioritise	Acquire	Gain Access	Process Storage Format	Perform Data Reduction	Locate Relevant Digital Artefacts	Extract Partition and File System Information	Extract Operating System Feature Information	Extract Application-based Information	Examine data at the file-level	Establish Identities	Visualisation	Event Reconstruction	Research	Reporting
Crime scene searching T1005	Place device in faraday environment T1010	Triage T1001	Disk imaging T1002	Key recovery from memory T1031	Disk image hash verification T1042	Privileged material protection T1046	Keyword searching T1049	Identify partitions T1059	Content indexer examination (OS) T1065	Browser examination T1069	Database examination T1071	Extraction of user accounts T1084	Virtualise suspect system for previewing T1103	Timeline analysis T1086	Source code review T1089	Bookmarking T1091
Digital sniffer dogs T1006	Evidence bags T1011		Memory imaging T1003	Side channel T1032	Forensic image format decoding T1043	Hash matching (reduce) T1047	Hash matching (locate) T1050	Process file system structures T1060	Log file examination (OS) T1066	Email examination T1070	Audio content analysis T1079	Identify conflation T1085		Geospatial analysis T1087	Experimentation T1090	Produce bookmark-based automated report T1092
SyncTriage-based approach T1007	Hardware write blockers T1012		Selective data acquisition T1004	Extraction of account details from an accessible device T1033	Mobile backup decoding T1044	Privacy protection via partial processing T1048	Fuzzy hash matching T1051	Non-allocated file recovery T1061	Cloud synchronisation feature examination (OS) T1067	Chat app examination T1072	Video content analysis T1080			Connection analysis T1088	Instrumentation T1095	Write expert report T1093
Profiling network traffic T1008	Software write blockers T1013		Privacy preserving selective extraction T1015	Brute force attack T1034	Decode standard archive format T1045		Timeline generation T1052	Decryption of encrypted file systems/volumes T1062	Recently used file identification (OS) T1068	Calendar app examination T1073	Image content analysis T1081				Cell site survey T1101	Disclosure T1094
Locate cloud account identifiers T1009	Chain of custody documentation T1014		Live data collection T1016	Dictionary attack T1035	Decode data from image from unmanaged NAND T1102		Entity extraction T1053	Identify file types T1063	Memory examination (OS-level) T1083	Social network app examination T1074	Document content analysis T1082					
			Network packet capture T1017	Smudge attack T1036			Content review for relevant material T1054	File carving T1064	Run programs identification (OS) T1096	Maps/travel app examination T1075	File repair with grafting T1099					
			Remote data collection T1018	Obtain password from suspect T1037			File system content inspection T1055		Installed programs identification (OS) T1097	Photos app examination T1077	EXIF data examination T1100					
			Mobile backup extraction T1019	Rainbow tables T1038			Entity connection identification T1056		User account analysis (OS) T1098	Cloud sync app examination T1078	Deep Fake Detection (Video) T1106					
			Mobile file system extraction T1020	App downgrade T1039			Steganography detection T1057			Memory examination (application-level) T1105						
			Mobile device screenshot based capture T1022	Use mobile device exploit T1040			Mismatched file extension detection T1058			Health/Fitness app examination T1107						
			Cloud data collection using account details T1023	Pin2Pwn T1041						Reminders app examination T1108						
			Cloud data collection via request T1024							Payment app examination T1109						
			Writing data to a forensic image format T1025													
			Writing data in standard archive format T1026													
			Data read using JTAG T1027													
			Chip-off T1028													
			Data read from desoldered eMMC T1029													
			Data read from unmanaged NAND T1030													
			Collect data using open source intelligence T1104													

SOLVE-IT



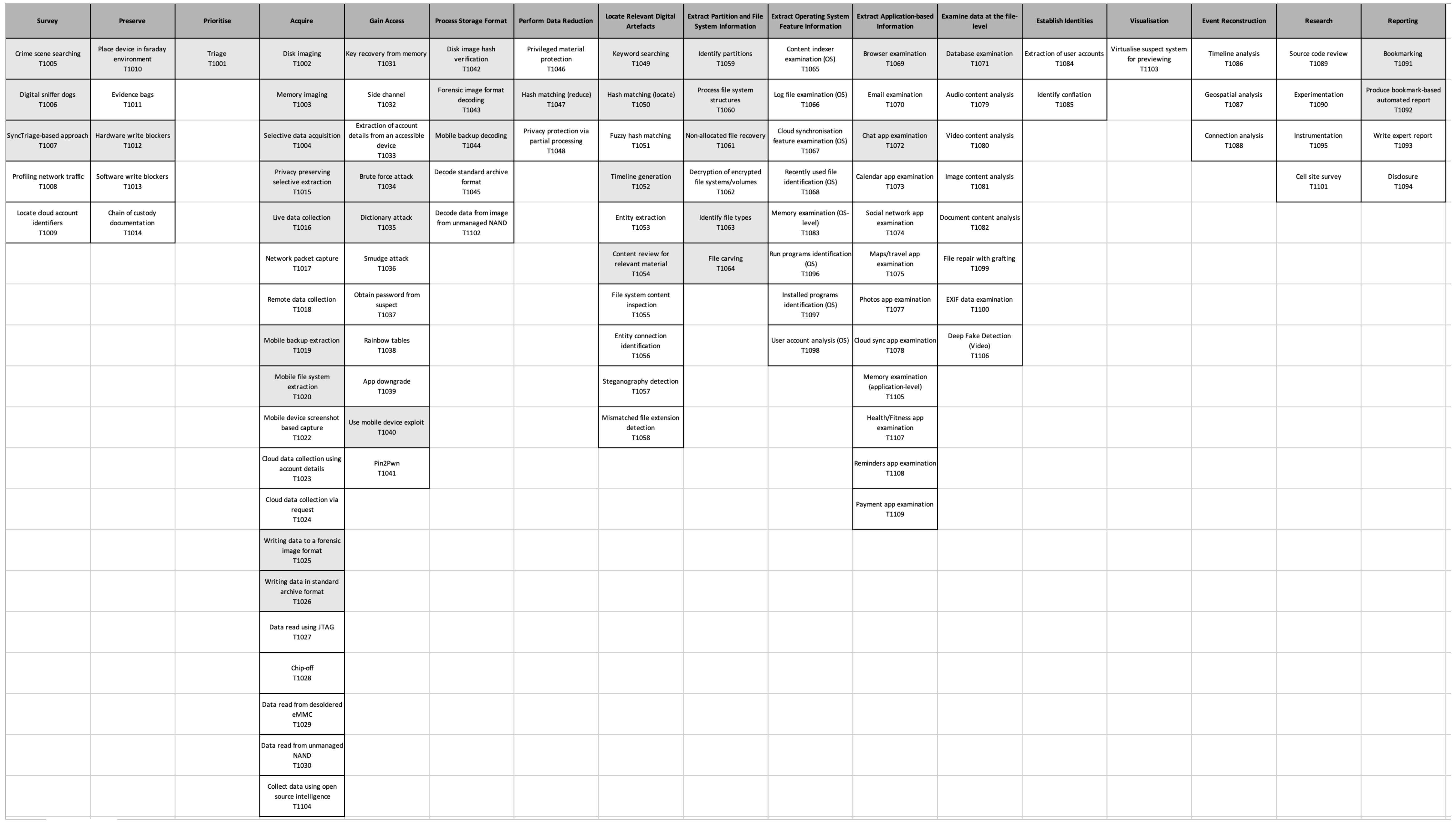
Survey	Preserve	Prioritise	Acquire	Gain Access	Process Storage Format	Perform Data Reduction	Locate Relevant Digital Artefacts	Extract Partit System Inf
Crime scene searching T1005	Place device in faraday environment T1010	Triage T1001	Disk imaging T1002	Key recovery from memory T1031	Disk image hash verification T1042	Privileged material protection T1046	Keyword searching T1049	Identify pa T105
Digital sniffer dogs T1006	Evidence bags T1011		Memory imaging T1003	Side channel T1032	Forensic image format decoding T1043	Hash matching (reduce) T1047	Hash matching (locate) T1050	Process file struct T10
SyncTriage-based approach T1007	Hardware write blockers T1012		Selective data acquisition T1004	Extraction of account details from an accessible device T1033	Mobile backup decoding T1044	Privacy protection via partial processing T1048	Fuzzy hash matching T1051	Non-allocated T10
Profiling network traffic T1008	Software write blockers T1013		Privacy preserving selective extraction T1015	Brute force attack T1034	Decode standard archive format T1045		Timeline generation T1052	Decryption o file systems T10
Locate cloud account identifiers T1009	Chain of custody documentation T1014		Live data collection T1016	Dictionary attack T1035	Decode data from image from unmanaged NAND T1102		Entity extraction T1053	Identify fi T10
			Network packet capture T1017	Smudge attack T1036			Content review for relevant material T1054	File ca T10
			Remote data collection T1018	Obtain password from suspect T1037			File system content inspection T1055	
			Mobile backup extraction T1019	Rainbow tables T1038			Entity connection identification T1056	

SOLVE-IT

Partition and File m Information	Extract Operating System Feature Information	Extract Application-based Information	Examine data at the file-level	Establish Identities	Visualisation	Event Reconstruction	Research	Reporting
tify partitions T1059	Content indexer examination (OS) T1065	Browser examination T1069	Database examination T1071	Extraction of user accounts T1084	Virtualise suspect system for previewing T1103	Timeline analysis T1086	Source code review T1089	Bookmarking T1091
ess file system tructures T1060	Log file examination (OS) T1066	Email examination T1070	Audio content analysis T1079	Identify conflation T1085		Geospatial analysis T1087	Experimentation T1090	Produce bookmark-based automated report T1092
cated file recovery T1061	Cloud synchronisation feature examination (OS) T1067	Chat app examination T1072	Video content analysis T1080			Connection analysis T1088	Instrumentation T1095	Write expert report T1093
tion of encrypted stems/volumes T1062	Recently used file identification (OS) T1068	Calendar app examination T1073	Image content analysis T1081				Cell site survey T1101	Disclosure T1094
tify file types T1063	Memory examination (OS-level) T1083	Social network app examination T1074	Document content analysis T1082					
ile carving T1064	Run programs identification (OS) T1096	Maps/travel app examination T1075	File repair with grafting T1099					
	Installed programs identification (OS) T1097	Photos app examination T1077	EXIF data examination T1100					
	User account analysis (OS) T1098	Cloud sync app examination T1078	Deep Fake Detection (Video) T1106					

SOLVE-IT

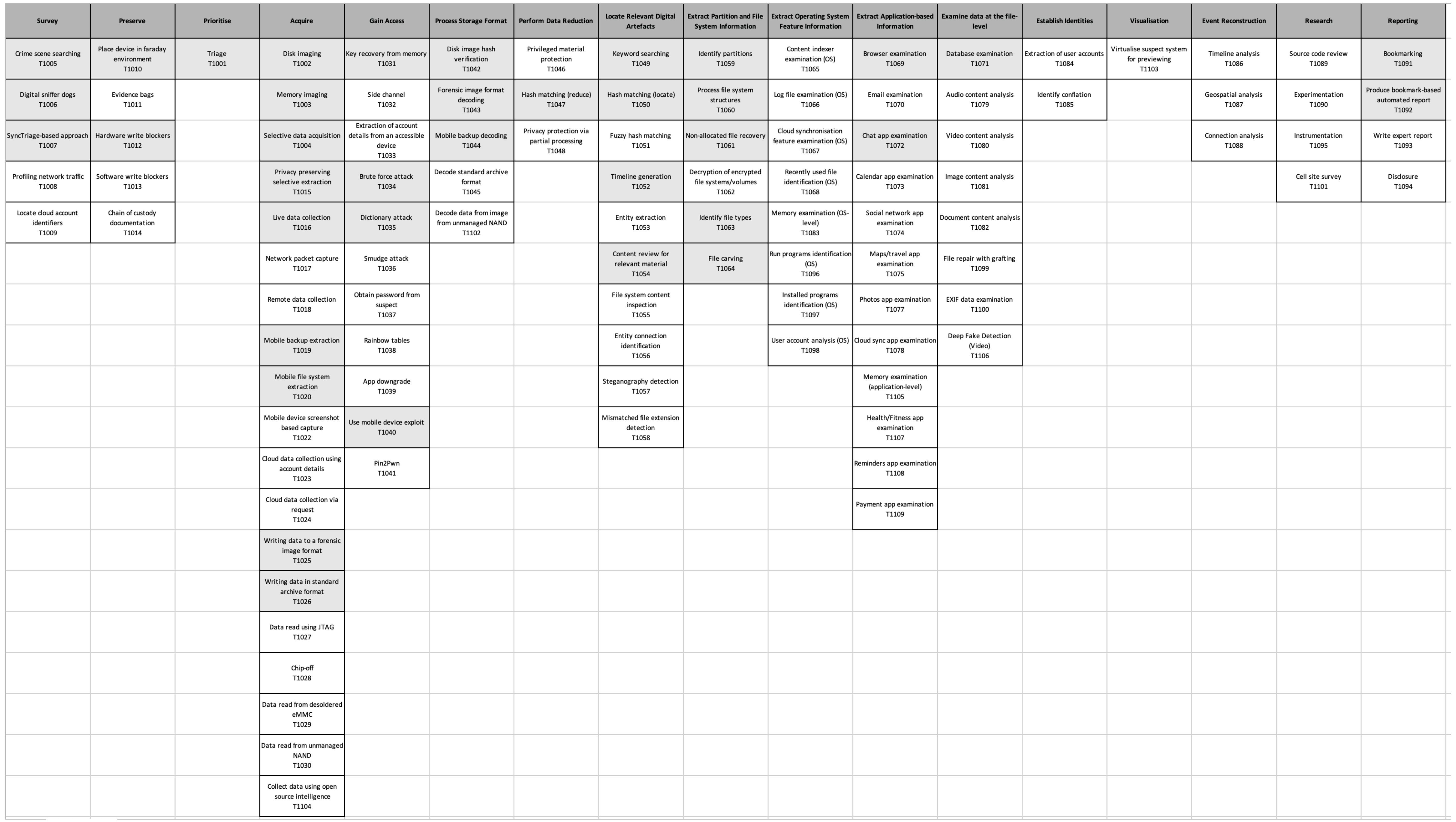
- 104 techniques
- 17 categories
- 33 populated
- 3 community contributors
- 156 weaknesses identified
- 108 mitigations indexed



Survey	Preserve	Prioritise	Acquire	Gain Access	Process Storage Format	Perform Data Reduction	Locate Relevant Digital Artefacts	Extract Partition and File System Information	Extract Operating System Feature Information	Extract Application-based Information	Examine data at the file-level	Establish Identities	Visualisation	Event Reconstruction	Research	Reporting
Crime scene searching T1005	Place device in faraday environment T1010	Triage T1001	Disk imaging T1002	Key recovery from memory T1031	Disk image hash verification T1042	Privileged material protection T1046	Keyword searching T1049	Identify partitions T1059	Content indexer examination (OS) T1065	Browser examination T1069	Database examination T1071	Extraction of user accounts T1084	Virtualise suspect system for previewing T1103	Timeline analysis T1086	Source code review T1089	Bookmarking T1091
Digital sniffer dogs T1006	Evidence bags T1011		Memory imaging T1003	Side channel T1032	Forensic image format decoding T1043	Hash matching (reduce) T1047	Hash matching (locate) T1050	Process file system structures T1060	Log file examination (OS) T1066	Email examination T1070	Audio content analysis T1079	Identify conflation T1085		Geospatial analysis T1087	Experimentation T1090	Produce bookmark-based automated report T1092
SyncTriage-based approach T1007	Hardware write blockers T1012		Selective data acquisition T1004	Extraction of account details from an accessible device T1033	Mobile backup decoding T1044	Privacy protection via partial processing T1048	Fuzzy hash matching T1051	Non-allocated file recovery T1061	Cloud synchronisation feature examination (OS) T1067	Chat app examination T1072	Video content analysis T1080			Connection analysis T1088	Instrumentation T1095	Write expert report T1093
Profiling network traffic T1008	Software write blockers T1013		Privacy preserving selective extraction T1015	Brute force attack T1034	Decode standard archive format T1045		Timeline generation T1052	Decryption of encrypted file systems/volumes T1062	Recently used file identification (OS) T1068	Calendar app examination T1073	Image content analysis T1081				Cell site survey T1101	Disclosure T1094
Locate cloud account identifiers T1009	Chain of custody documentation T1014		Live data collection T1016	Dictionary attack T1035	Decode data from image from unmanaged NAND T1102		Entity extraction T1053	Identify file types T1063	Memory examination (OS-level) T1083	Social network app examination T1074	Document content analysis T1082					
			Network packet capture T1017	Smudge attack T1036			Content review for relevant material T1054	File carving T1064	Run programs identification (OS) T1096	Maps/travel app examination T1075	File repair with grafting T1099					
			Remote data collection T1018	Obtain password from suspect T1037			File system content inspection T1055		Installed programs identification (OS) T1097	Photos app examination T1077	EXIF data examination T1100					
			Mobile backup extraction T1019	Rainbow tables T1038			Entity connection identification T1056		User account analysis (OS) T1098	Cloud sync app examination T1078	Deep Fake Detection (Video) T1106					
			Mobile file system extraction T1020	App downgrade T1039			Steganography detection T1057			Memory examination (application-level) T1105						
			Mobile device screenshot based capture T1022	Use mobile device exploit T1040			Mismatched file extension detection T1058			Health/Fitness app examination T1107						
			Cloud data collection using account details T1023	Pin2Pwn T1041						Reminders app examination T1108						
			Cloud data collection via request T1024							Payment app examination T1109						
			Writing data to a forensic image format T1025													
			Writing data in standard archive format T1026													
			Data read using JTAG T1027													
			Chip-off T1028													
			Data read from desoldered eMMC T1029													
			Data read from unmanaged NAND T1030													
			Collect data using open source intelligence T1104													

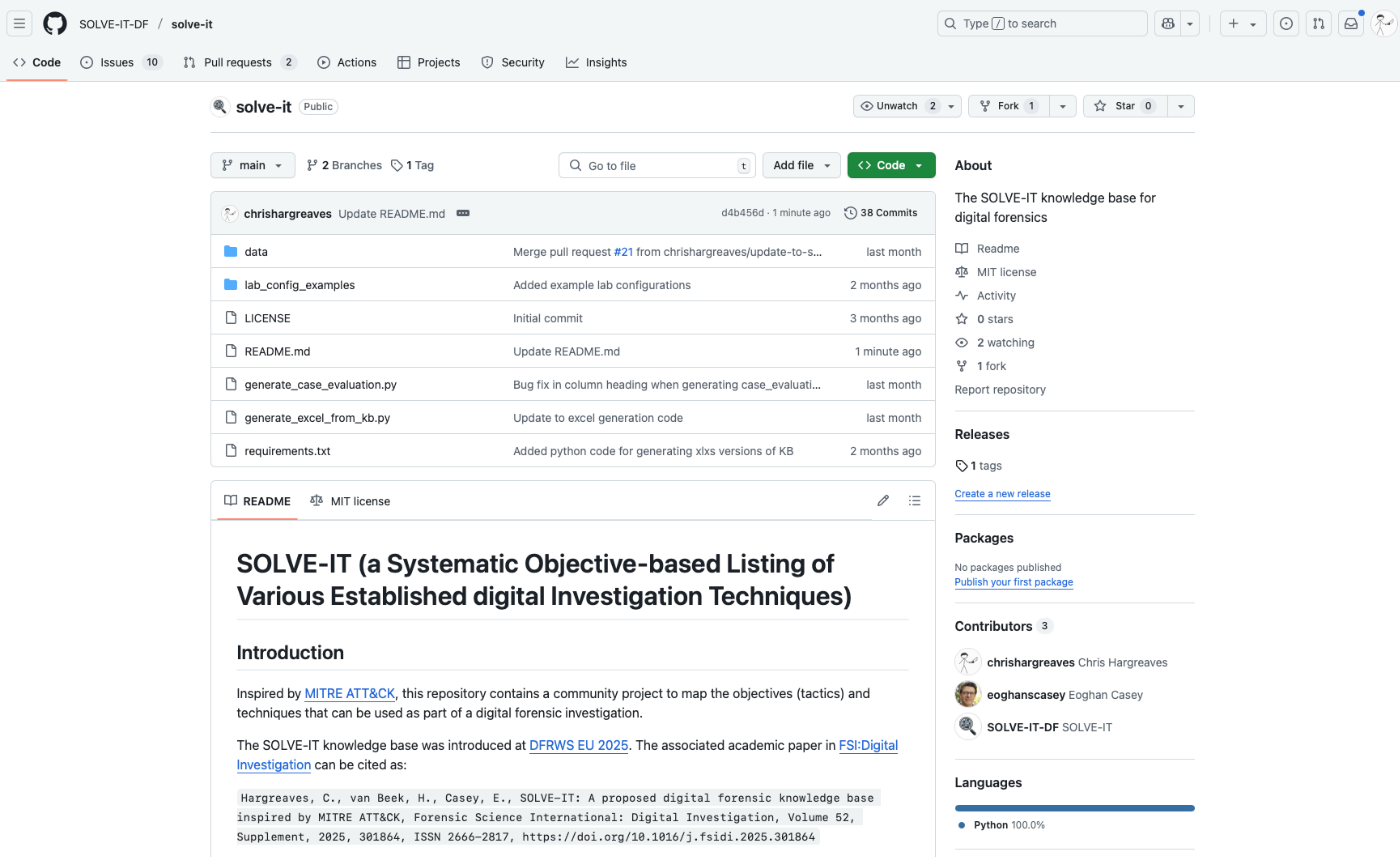
SOLVE-IT

- ~~104~~ 107 techniques
- 17 categories
- ~~33~~ 37 populated
- ~~3~~ 5 community contributors
- ~~156~~ 171 weaknesses identified
- ~~108~~ 125 mitigations indexed



Survey	Preserve	Prioritise	Acquire	Gain Access	Process Storage Format	Perform Data Reduction	Locate Relevant Digital Artefacts	Extract Partition and File System Information	Extract Operating System Feature Information	Extract Application-based Information	Examine data at the file-level	Establish Identities	Visualisation	Event Reconstruction	Research	Reporting
Crime scene searching T1005	Place device in faraday environment T1010	Triage T1001	Disk imaging T1002	Key recovery from memory T1031	Disk image hash verification T1042	Privileged material protection T1046	Keyword searching T1049	Identify partitions T1059	Content indexer examination (OS) T1065	Browser examination T1069	Database examination T1071	Extraction of user accounts T1084	Virtualise suspect system for previewing T1103	Timeline analysis T1086	Source code review T1089	Bookmarking T1091
Digital sniffer dogs T1006	Evidence bags T1011		Memory imaging T1003	Side channel T1032	Forensic image format decoding T1043	Hash matching (reduce) T1047	Hash matching (locate) T1050	Process file system structures T1060	Log file examination (OS) T1066	Email examination T1070	Audio content analysis T1079	Identify conflation T1085		Geospatial analysis T1087	Experimentation T1090	Produce bookmark-based automated report T1092
SyncTriage-based approach T1007	Hardware write blockers T1012		Selective data acquisition T1004	Extraction of account details from an accessible device T1033	Mobile backup decoding T1044	Privacy protection via partial processing T1048	Fuzzy hash matching T1051	Non-allocated file recovery T1061	Cloud synchronisation feature examination (OS) T1067	Chat app examination T1072	Video content analysis T1080			Connection analysis T1088	Instrumentation T1095	Write expert report T1093
Profiling network traffic T1008	Software write blockers T1013		Privacy preserving selective extraction T1015	Brute force attack T1034	Decode standard archive format T1045		Timeline generation T1052	Decryption of encrypted file systems/volumes T1062	Recently used file identification (OS) T1068	Calendar app examination T1073	Image content analysis T1081				Cell site survey T1101	Disclosure T1094
Locate cloud account identifiers T1009	Chain of custody documentation T1014		Live data collection T1016	Dictionary attack T1035	Decode data from image from unmanaged NAND T1102		Entity extraction T1053	Identify file types T1063	Memory examination (OS-level) T1083	Social network app examination T1074	Document content analysis T1082					
			Network packet capture T1017	Smudge attack T1036			Content review for relevant material T1054	File carving T1064	Run programs identification (OS) T1096	Maps/travel app examination T1075	File repair with grafting T1099					
			Remote data collection T1018	Obtain password from suspect T1037			File system content inspection T1055		Installed programs identification (OS) T1097	Photos app examination T1077	EXIF data examination T1100					
			Mobile backup extraction T1019	Rainbow tables T1038			Entity connection identification T1056		User account analysis (OS) T1098	Cloud sync app examination T1078	Deep Fake Detection (Video) T1106					
			Mobile file system extraction T1020	App downgrade T1039			Steganography detection T1057			Memory examination (application-level) T1105						
			Mobile device screenshot based capture T1022	Use mobile device exploit T1040			Mismatched file extension detection T1058			Health/Fitness app examination T1107						
			Cloud data collection using account details T1023	Pin2Pwn T1041						Reminders app examination T1108						
			Cloud data collection via request T1024							Payment app examination T1109						
			Writing data to a forensic image format T1025													
			Writing data in standard archive format T1026													
			Data read using JTAG T1027													
			Chip-off T1028													
			Data read from desoldered eMMC T1029													
			Data read from unmanaged NAND T1030													
			Collect data using open source intelligence T1104													

Overall Implementation: Hosted in GitHub



chrishargreaves Update README.md d4b456d · 1 minute ago 38 Commits

data	Merge pull request #21 from chrishargreaves/update-to-s...	last month
lab_config_examples	Added example lab configurations	2 months ago
LICENSE	Initial commit	3 months ago
README.md	Update README.md	1 minute ago
generate_case_evaluation.py	Bug fix in column heading when generating case_evaluati...	last month
generate_excel_from_kb.py	Update to excel generation code	last month
requirements.txt	Added python code for generating xlxs versions of KB	2 months ago

About

The SOLVE-IT knowledge base for digital forensics

Readme
MIT license
Activity
0 stars
2 watching
1 fork
Report repository

Releases

1 tags

Create a new release

Packages

No packages published
Publish your first package

Contributors 3

chrishargreaves Chris Hargreaves
eoghanscasey Eoghan Casey
SOLVE-IT-DF SOLVE-IT

Languages

● Python 100.0%

SOLVE-IT (a Systematic Objective-based Listing of Various Established digital Investigation Techniques)

Introduction

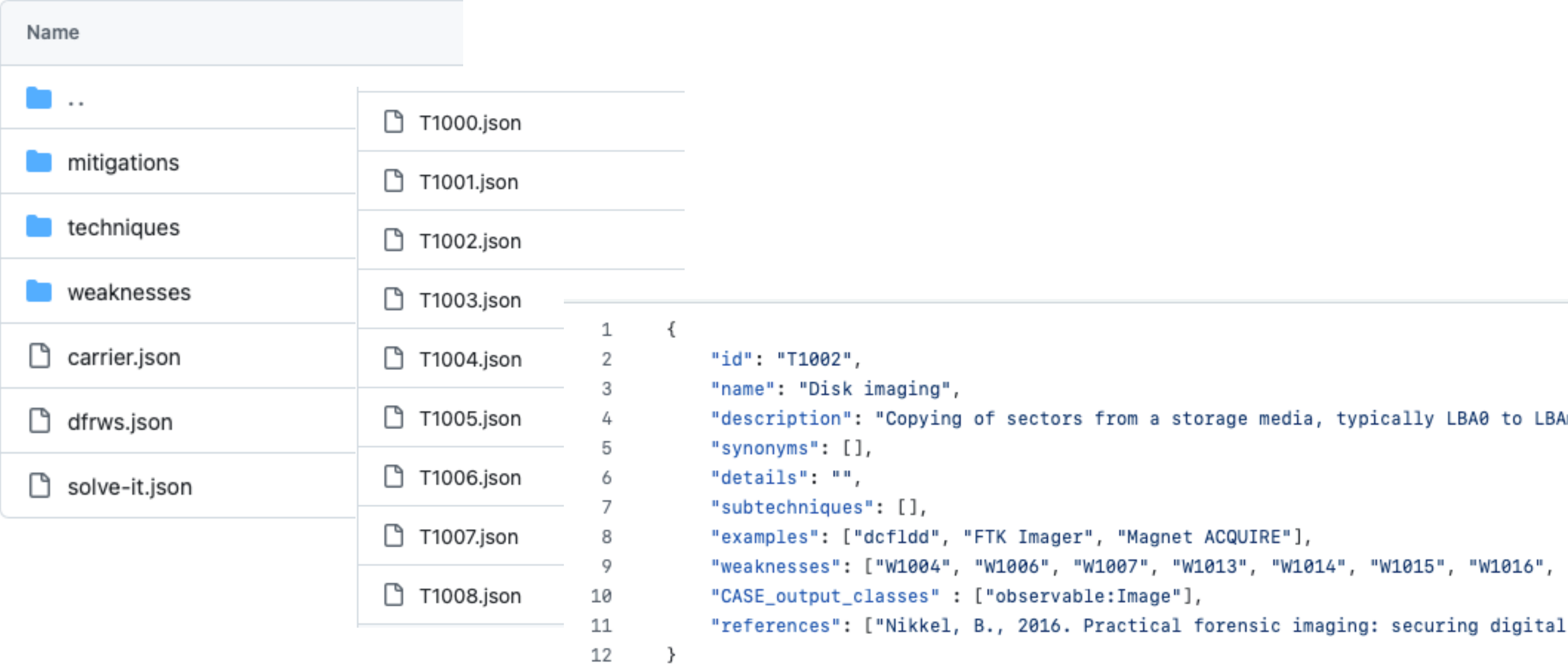
Inspired by MITRE ATT&CK, this repository contains a community project to map the objectives (tactics) and techniques that can be used as part of a digital forensic investigation.

The SOLVE-IT knowledge base was introduced at DFRWS EU 2025. The associated academic paper in FSI:Digital Investigation can be cited as:

```
Hargreaves, C., van Beek, H., Casey, E., SOLVE-IT: A proposed digital forensic knowledge base
inspired by MITRE ATT&CK, Forensic Science International: Digital Investigation, Volume 52,
Supplement, 2025, 301864, ISSN 2666-2817, https://doi.org/10.1016/j.fsidi.2025.301864
```

https://github.com/SOLVE-IT-DF/solve-it

Overall Implementation: Details are stored as JSON



Name

..

mitigations

techniques

weaknesses

carrier.json

dfrws.json

solve-it.json

T1000.json

T1001.json

T1002.json

T1003.json

T1004.json

T1005.json

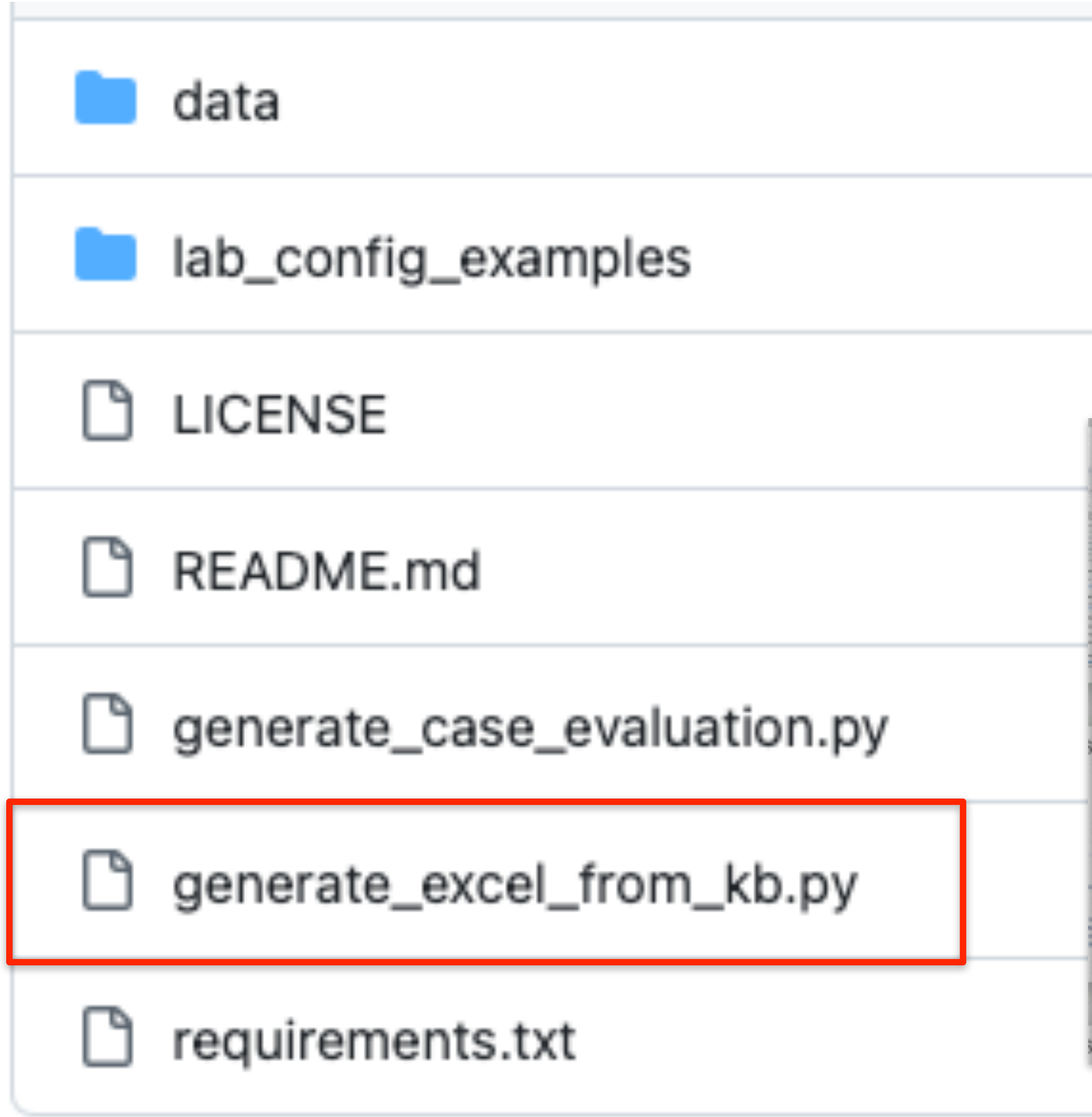
T1006.json

T1007.json

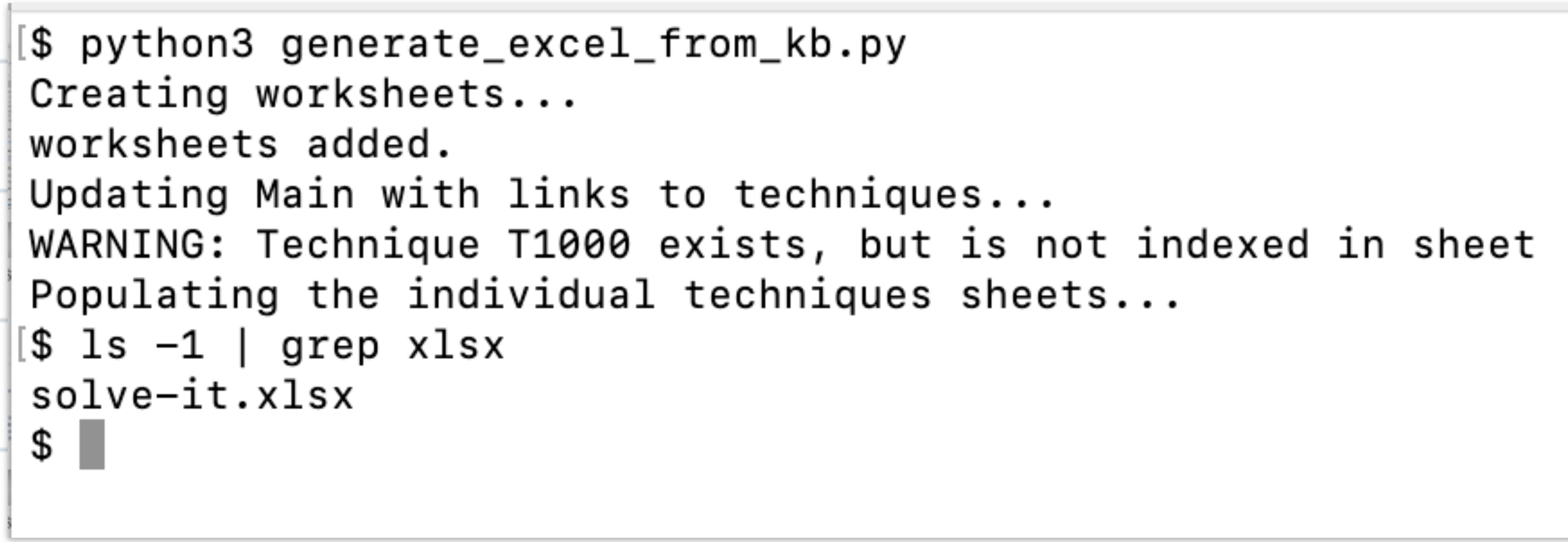
T1008.json

```
{
    "id": "T1002",
    "name": "Disk imaging",
    "description": "Copying of sectors from a storage media, typically LBA0 to LBA
    "synonyms": [],
    "details": "",
    "subtechniques": [],
    "examples": ["dcfldd", "FTK Imager", "Magnet ACQUIRE"],
    "weaknesses": ["W1004", "W1006", "W1007", "W1013", "W1014", "W1015", "W1016",
    "CASE_output_classes" : ["observable:Image"],
    "references": ["Nikkel, B., 2016. Practical forensic imaging: securing digital
}
```

Overall Implementation: Scripts



- data
- lab_config_examples
- LICENSE
- README.md
- generate_case_evaluation.py
- generate_excel_from_kb.py
- requirements.txt



```
[$ python3 generate_excel_from_kb.py
Creating worksheets...
worksheets added.
Updating Main with links to techniques...
WARNING: Technique T1000 exists, but is not indexed in sheet
Populating the individual techniques sheets...
[$ ls -1 | grep xlsx
solve-it.xlsx
$ 
```

Design Concepts

Objectives

The goal that one might wish to achieve in a digital forensic investigation, e.g. *acquire data* or *gain access.*

Techniques

How one might achieve an objective in digital forensics by performing an action, e.g. for the objective of ‘acquire data’, the technique ‘disk imaging’ could be used.

Weaknesses

These represent potential problems resulting from using a technique. They are classified according to the error categories in ASTM E3016-18.

Mitigations

Something that can be done to prevent a weakness from occurring, or to minimise its impact.

Objectives: Design

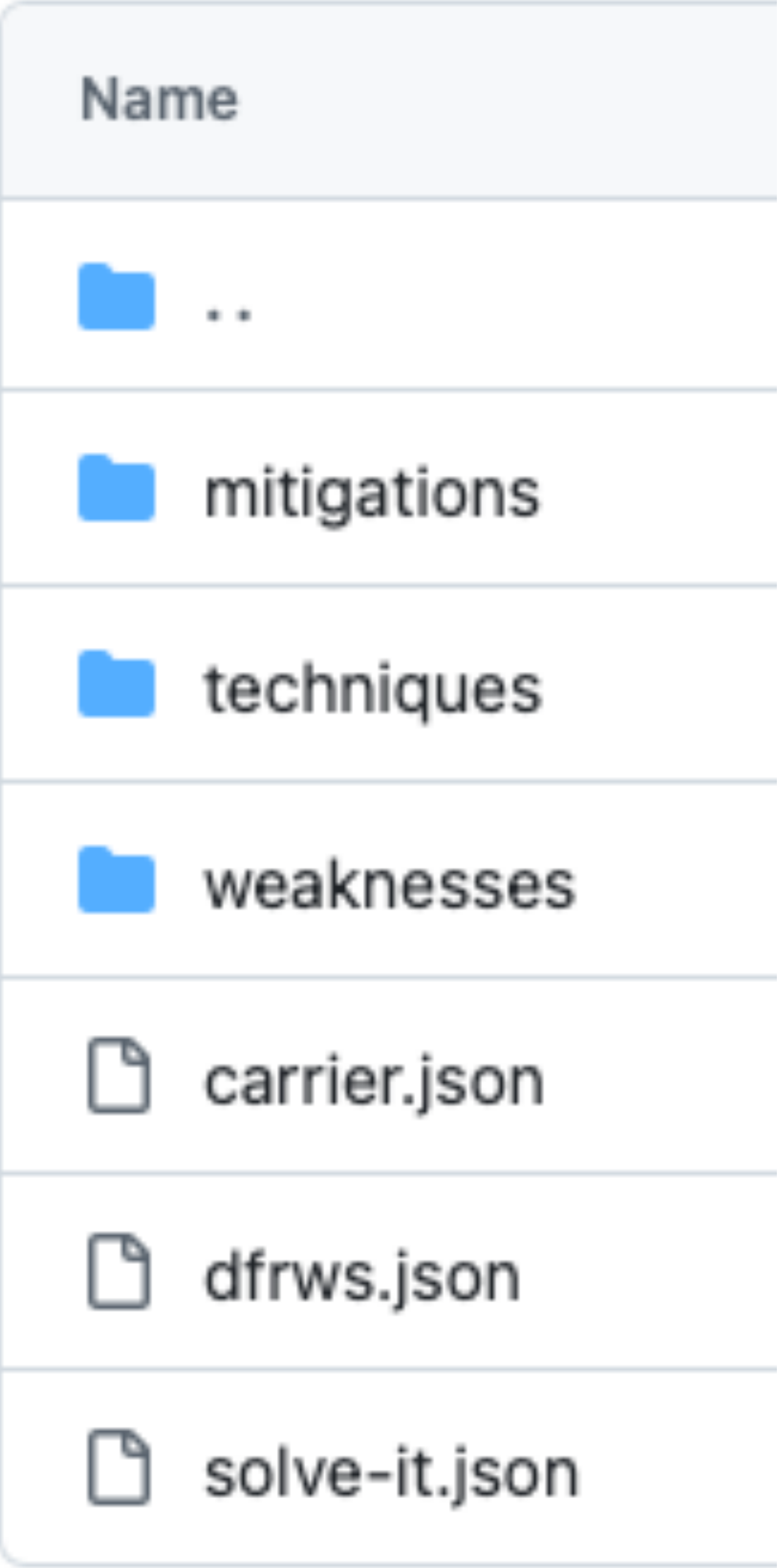
Survey	Preserve	Prioritise	Acquire	Gain Access	Process Storage Format	Perform Data Reduction	Locate Relevant Digital Artefacts	Extract Partition ar System Informat
Crime scene searching T1005	Place device in faraday environment T1010	Triage T1001	Disk imaging T1002	Key recovery from memory T1031	Disk image hash verification T1042	Privileged material protection T1046	Keyword searching T1049	Identify partitic T1059
Digital sniffer dogs T1006	Evidence bags T1011		Memory imaging T1003	Side channel T1032	Forensic image format decoding T1043	Hash matching (reduce) T1047	Hash matching (locate) T1050	Process file syst structures T1060
SyncTriage-based approach T1007	Hardware write blockers T1012		Selective data acquisition T1004	Extraction of account details from an accessible device T1033	Mobile backup decoding T1044	Privacy protection via partial processing T1048	Fuzzy hash matching T1051	Non-allocated file re T1061
Profiling network traffic T1008	Software write blockers T1013		Privacy preserving selective extraction T1015	Brute force attack T1034	Decode standard archive format T1045		Timeline generation T1052	Decryption of encr file systems/volu T1062
Locate cloud account identifiers T1009	Chain of custody documentation T1014		Live data collection T1016	Dictionary attack T1035	Decode data from image from unmanaged NAND T1102		Entity extraction T1053	Identify file typ T1063
			Network packet capture T1017	Smudge attack T1036			Content review for relevant material T1054	File carving T1064
			Remote data collection T1018	Obtain password from suspect T1037			File system content inspection T1055	
			Mobile backup extraction	Rainbow tables			Entity connection	

Objectives: Design

“The goal that one might wish to achieve in a digital forensic investigation, e.g. acquire data or gain access.”

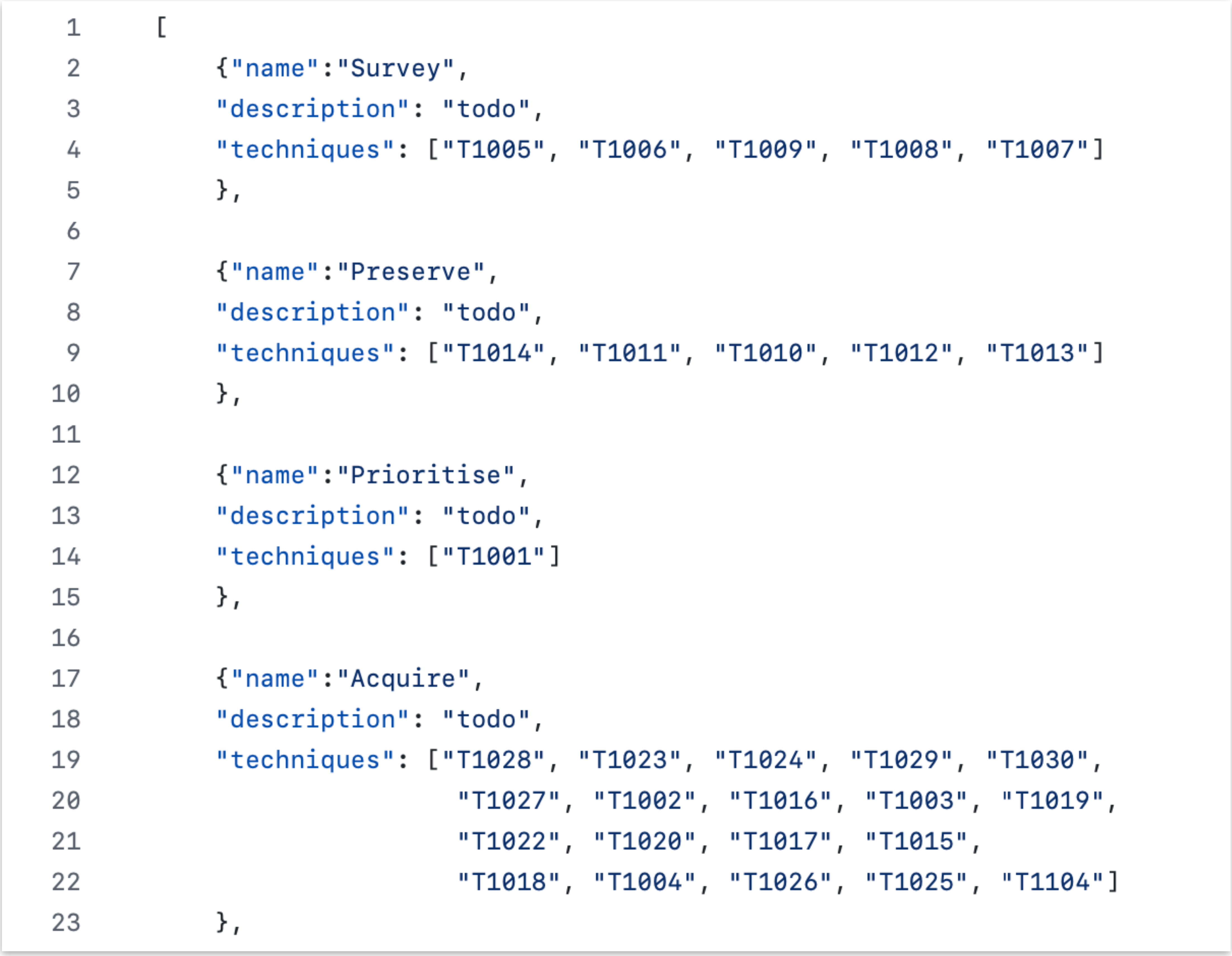
- Various process models that can be used for this
    - *Carrier* - acquire, analyse, present
    - *DFRWS/Palmer* - identification, preservation, collection, examination, analysis, presentation
    - *SOLVE-IT* - a new organisation, based on the need to categorise a large number of specific techniques

Objectives: Implementation



Name

- ..
- mitigations
- techniques
- weaknesses
- carrier.json
- dfrws.json
- solve-it.json



```
[
    {"name":"Survey",
    "description": "todo",
    "techniques": ["T1005", "T1006", "T1009", "T1008", "T1007"]
    },

    {"name":"Preserve",
    "description": "todo",
    "techniques": ["T1014", "T1011", "T1010", "T1012", "T1013"]
    },

    {"name":"Prioritise",
    "description": "todo",
    "techniques": ["T1001"]
    },

    {"name":"Acquire",
    "description": "todo",
    "techniques": ["T1028", "T1023", "T1024", "T1029", "T1030",
                     "T1027", "T1002", "T1016", "T1003", "T1019",
                     "T1022", "T1020", "T1017", "T1015",
                     "T1018", "T1004", "T1026", "T1025", "T1104"]
    },
```

solve-it.json describes the primary organisation of the techniques, but…

… you can configure the SOLVE-IT tooling to use any different organisational structure needed.

Techniques: Design

Survey	Preserve	Prioritise	Acquire	Gain Access	Process Storage Format	Perform Data Reduction	Locate Relevant Digital Artefacts	Extract Partition ar System Informat
Crime scene searching T1005	Place device in faraday environment T1010	Triage T1001	Disk imaging T1002	Key recovery from memory T1031	Disk image hash verification T1042	Privileged material protection T1046	Keyword searching T1049	Identify partitic T1059
Digital sniffer dogs T1006	Evidence bags T1011		Memory imaging T1003	Side channel T1032	Forensic image format decoding T1043	Hash matching (reduce) T1047	Hash matching (locate) T1050	Process file syst structures T1060
SyncTriage-based approach T1007	Hardware write blockers T1012		Selective data acquisition T1004	Extraction of account details from an accessible device T1033	Mobile backup decoding T1044	Privacy protection via partial processing T1048	Fuzzy hash matching T1051	Non-allocated file re T1061
Profiling network traffic T1008	Software write blockers T1013		Privacy preserving selective extraction T1015	Brute force attack T1034	Decode standard archive format T1045		Timeline generation T1052	Decryption of encr file systems/volu T1062
Locate cloud account identifiers T1009	Chain of custody documentation T1014		Live data collection T1016	Dictionary attack T1035	Decode data from image from unmanaged NAND T1102		Entity extraction T1053	Identify file typ T1063
			Network packet capture T1017	Smudge attack T1036			Content review for relevant material T1054	File carving T1064
			Remote data collection T1018	Obtain password from suspect T1037			File system content inspection T1055	
			Mobile backup extraction	Rainbow tables			Entity connection	

Techniques: Design

Survey	Preserve	Prioritise	Acquire	Gain Access	Process Storage Format	Perform Data Reduction	Locate Relevant Digital Artefacts	Extract Partition ar System Informat
Crime scene searching T1005	Place device in faraday environment T1010	Triage T1001	Disk imaging T1002	Key recovery from memory T1031	Disk image hash verification T1042	Privileged material protection T1046	Keyword searching T1049	Identify partitic T1059
Digital sniffer dogs T1006	Evidence bags T1011		Memory imaging T1003	Side channel T1032	Forensic image format decoding T1043	Hash matching (reduce) T1047	Hash matching (locate) T1050	Process file syst structures T1060
SyncTriage-based approach T1007	Hardware write blockers T1012		Selective data acquisition T1004	Extraction of account details from an accessible device T1033	Mobile backup decoding T1044	Privacy protection via partial processing T1048	Fuzzy hash matching T1051	Non-allocated file re T1061
Profiling network traffic T1008	Software write blockers T1013		Privacy preserving selective extraction T1015	Brute force attack T1034	Decode standard archive format T1045		Timeline generation T1052	Decryption of encr file systems/volu T1062
Locate cloud account identifiers T1009	Chain of custody documentation T1014		Live data collection T1016	Dictionary attack T1035	Decode data from image from unmanaged NAND T1102		Entity extraction T1053	Identify file typ T1063
			Network packet capture T1017	Smudge attack T1036			Content review for relevant material T1054	File carving T1064
			Remote data collection T1018	Obtain password from suspect T1037			File system content inspection T1055	
			Mobile backup extraction	Rainbow tables			Entity connection	

Techniques: Design

Survey	Preserve	Prioritise	Acquire	Gain Access	Process Storage Format	Perform Data Reduction	Locate Relevant Digital Artefacts	Extract Partition ar System Informat
Crime scene searching T1005	Place device in faraday environment T1010	Triage T1001	Disk imaging T1002	Key recovery from memory T1031	Disk image hash verification T1042	Privileged material protection T1046	Keyword searching T1049	Identify partitic T1059
Digital sniffer dogs T1006	Evidence bags T1011		Memory imaging T1003	Side channel T1032	Forensic image format decoding T1043	Hash matching (reduce) T1047	Hash matching (locate) T1050	Process file syst structures T1060
SyncTriage-based approach T1007	Hardware write blockers T1012		Selective data acquisition T1004	Extraction of account details from an accessible device T1033	Mobile backup decoding T1044	Privacy protection via partial processing T1048	Fuzzy hash matching T1051	Non-allocated file re T1061
Profiling network traffic T1008	Software write blockers T1013		Privacy preserving selective extraction T1015	Brute force attack T1034	Decode standard archive format T1045		Timeline generation T1052	Decryption of encry file systems/volu T1062
Locate cloud account identifiers T1009	Chain of custody documentation T1014		Live data collection T1016	Dictionary attack T1035	Decode data from image from unmanaged NAND T1102		Entity extraction T1053	Identify file typ T1063
			Network packet capture T1017	Smudge attack T1036			Content review for relevant material T1054	File carving T1064
			Remote data collection T1018	Obtain password from suspect T1037			File system content inspection T1055	
			Mobile backup extraction	Rainbow tables			Entity connection	

Techniques: Design

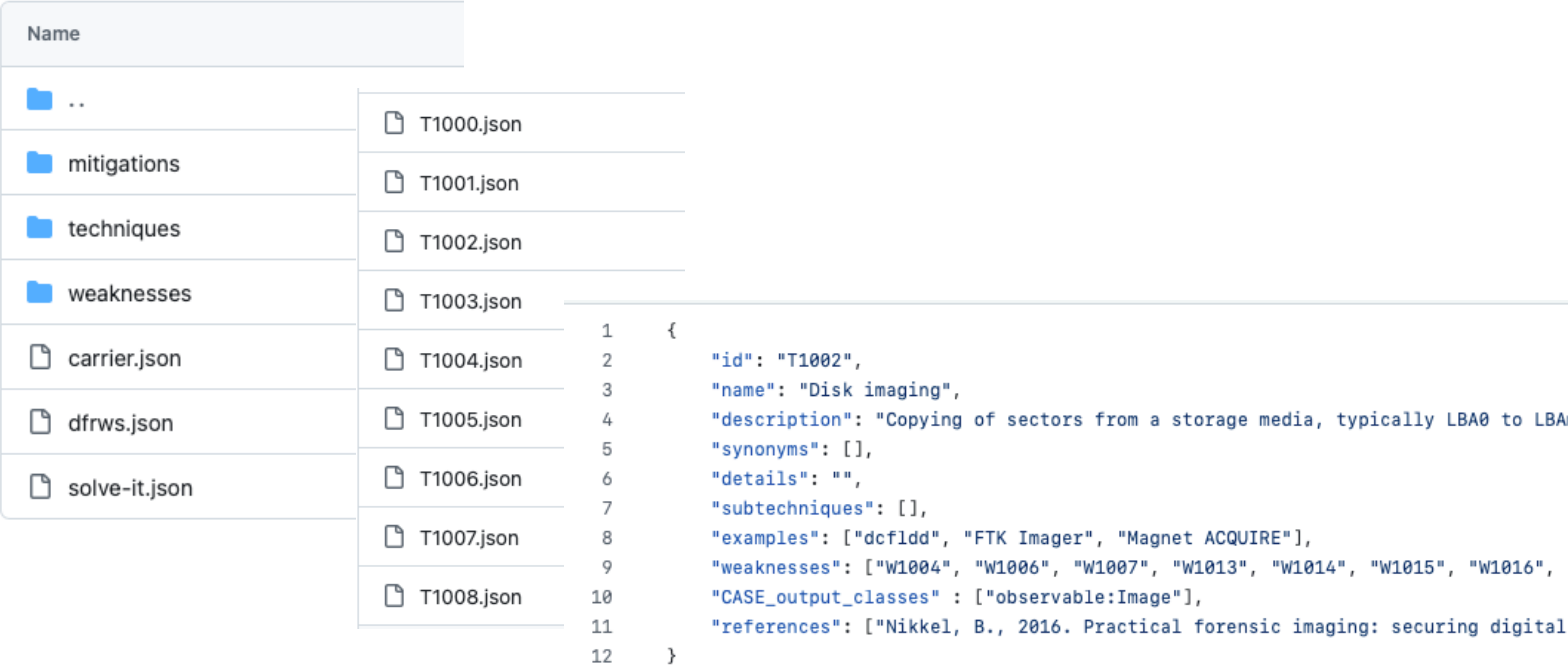
Survey	Preserve	Prioritise	Acquire	Gain Access	Process Storage Format	Perform Data Reduction	Locate Relevant Digital Artefacts	Extract Partition ar System Informat
Crime scene searching T1005	Place device in faraday environment T1010	Triage T1001	Disk imaging T1002	Key recovery from memory T1031	Disk image hash verification T1042	Privileged material protection T1046	Keyword searching T1049	Identify partitic T1059
Digital sniffer dogs T1006	Evidence bags T1011		Memory imaging T1003	Side channel T1032	Forensic image format decoding T1043	Hash matching (reduce) T1047	Hash matching (locate) T1050	Process file syst structures T1060
SyncTriage-based approach T1007	Hardware write blockers T1012		Selective data acquisition T1004	Extraction of account details from an accessible device T1033	Mobile backup decoding T1044	Privacy protection via partial processing T1048	Fuzzy hash matching T1051	Non-allocated file re T1061
Profiling network traffic T1008	Software write blockers T1013		Privacy preserving selective extraction T1015	Brute force attack T1034	Decode standard archive format T1045		Timeline generation T1052	Decryption of encr file systems/volu T1062
Locate cloud account identifiers T1009	Chain of custody documentation T1014		Live data collection T1016	Dictionary attack T1035	Decode data from image from unmanaged NAND T1102		Entity extraction T1053	Identify file typ T1063
			Network packet capture T1017	Smudge attack T1036			Content review for relevant material T1054	File carving T1064
			Remote data collection T1018	Obtain password from suspect T1037			File system content inspection T1055	
			Mobile backup extraction	Rainbow tables			Entity connection	

Techniques: Design

How one might achieve an objective in digital forensics by performing an action, e.g. for the objective of ‘acquire data’, the technique ‘disk imaging’ could be used.

- **id**: the technique’s ID, e.g. T1001;
- **name**: the name of the technique;
- **description**: A short description of what the technique involves;
- **synonyms**: any possible synonyms for the technique;
- **details**: further details beyond the short description;
- **sub-techniques**: some techniques may have sub-techniques, and can be listed here, referenced by technique ID;
- **examples**: examples related to the technique. These can be datasets that use the techniques, example cases that made use of the techniques either from published cases or synthetic ones, or specific tools that provide the technique;
- **weaknesses**: this field allows potential weaknesses associated with techniques to be referenced, pointing to indexed weaknesses within the knowledge base;
- **CASE_output_classes**: any potential CASE Ontology entities that allow the technique output to be represented;
- **references**: references can and should be included to support definitions and examples for the techniques.

Implementation: Techniques



Name

..

mitigations

techniques

weaknesses

carrier.json

dfrws.json

solve-it.json

T1000.json

T1001.json

T1002.json

T1003.json

T1004.json

T1005.json

T1006.json

T1007.json

T1008.json

```
{
    "id": "T1002",
    "name": "Disk imaging",
    "description": "Copying of sectors from a storage media, typically LBA0 to LBA
    "synonyms": [],
    "details": "",
    "subtechniques": [],
    "examples": ["dcfldd", "FTK Imager", "Magnet ACQUIRE"],
    "weaknesses": ["W1004", "W1006", "W1007", "W1013", "W1014", "W1015", "W1016",
    "CASE_output_classes" : ["observable:Image"],
    "references": ["Nikkel, B., 2016. Practical forensic imaging: securing digital
}
```

Weaknesses: Design

Survey
Preserve
Prioritise
Acquire
Gain Access
Process Storage Format
Perform Data Reduction
Locate Relevant Digital Artefacts
Extract Partition ar System Informat
Crime
Digit
SyncTriag
Profilin
Locate

1	**Technique name:**	Disk imaging	back to main						
2	**Technique ID:**	T1002							
3	**Category:**	['Acquire']							
4	**Description:**	Copying of sectors from a storage media, typically LBA0 to LBAmax into an imaging format. The could be from a traditional hard disk, SSD, USB stick, or data from an eMMC chip that has been desoldered and placed in a reader.							
5	**Synonyms:**	[]							
6	**Details:**								
7	**Subtechniques:**	[]							
8	**CASE output entities:**	['observable:Image']							
9	**Examples:**	['dcfldd', 'FTK Imager', 'Magnet ACQUIRE']							
10									
11	**Potential weaknesses:**								
12	**Weakness ID:**	**Detail:**	**INCOMP**	**INAC-EX**	**INAC-AS**	**INAC-ALT**	**INAC-COR**	**MISINT**	**Mitigations**
13	W1004	Acquisition does not include all sectors from LBA0 to LBA max	x						M1003,
14	W1006	Acquistion does not include data in HPA	x						M1005,
15	W1007	Acquistion does not include data in DCO	x						M1006,
16	W1013	Acquisition includes extra bytes		x					M1003,M1009,
17	W1014	Imaging process changes original data				x			M1007,M1008,
18	W1015	Powering on SSD results in sectors being wiped by TRIM operation	x			x	x		
19	W1016	Data copied from sectors on source are stored incorrectly				x	x		M1009,
20	W1136	Not recovering data from a failed hard drive	x						M1089,
21	W1143	Acquisition method does not read remapped sectors e.g. G-Lists	x						M1102,
22									
23	**Mitigations:**								

Weaknesses are presented when you look at a specific technique in the exported spreadsheet.

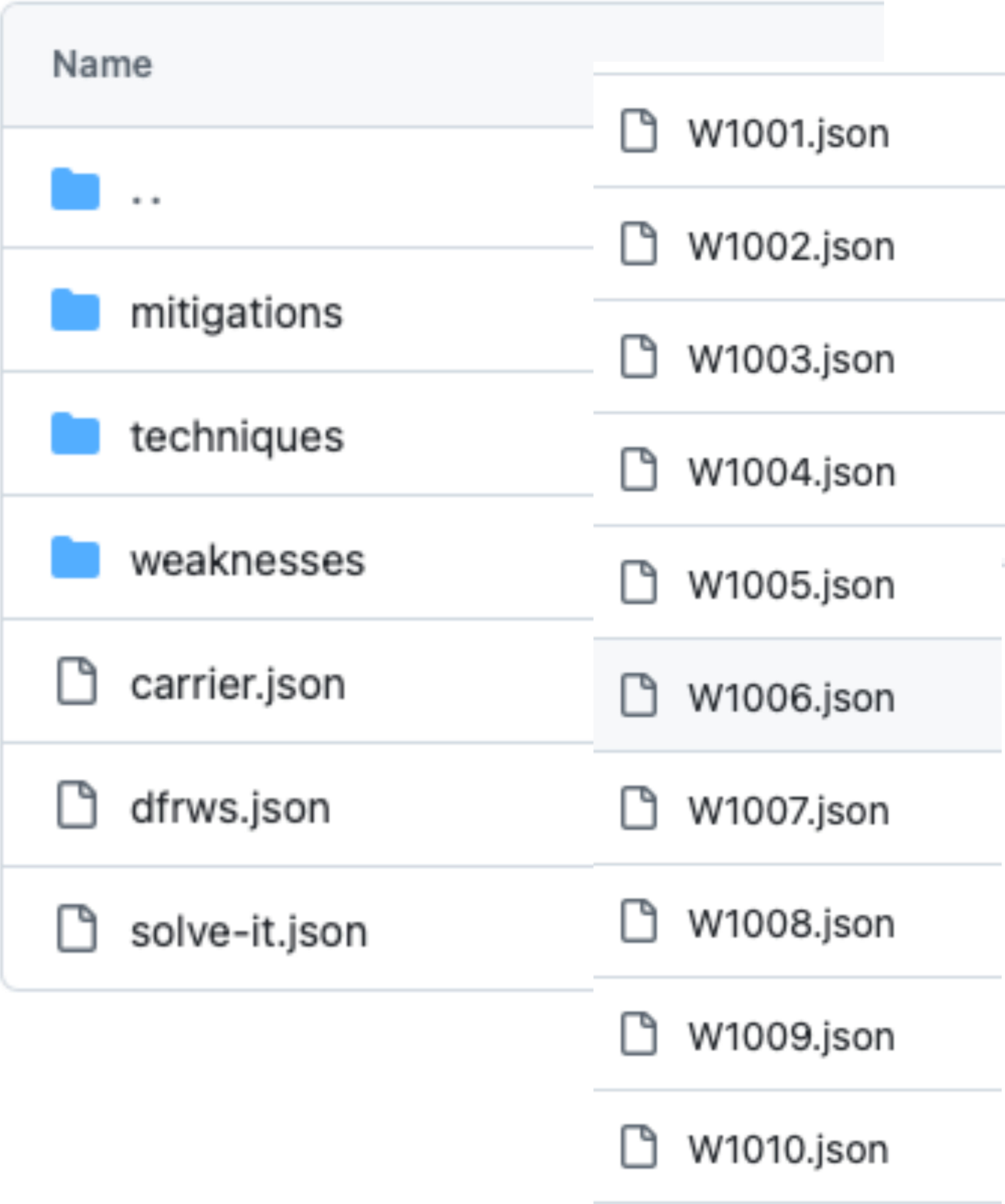
Weaknesses: Design

These represent potential problems resulting from using a technique. They are classified according to the error categories in ASTM E3016-18

- **id**: the weakness's ID (e.g. W1001);
- **name**: a short description of the weakness;
- **mitigations**: provides indexed references to any mitigations that could minimise or reduce the impact of individual weaknesses;
- **references**: These should be included to support definitions and examples, including to error-focused datasets demonstrating the weakness;

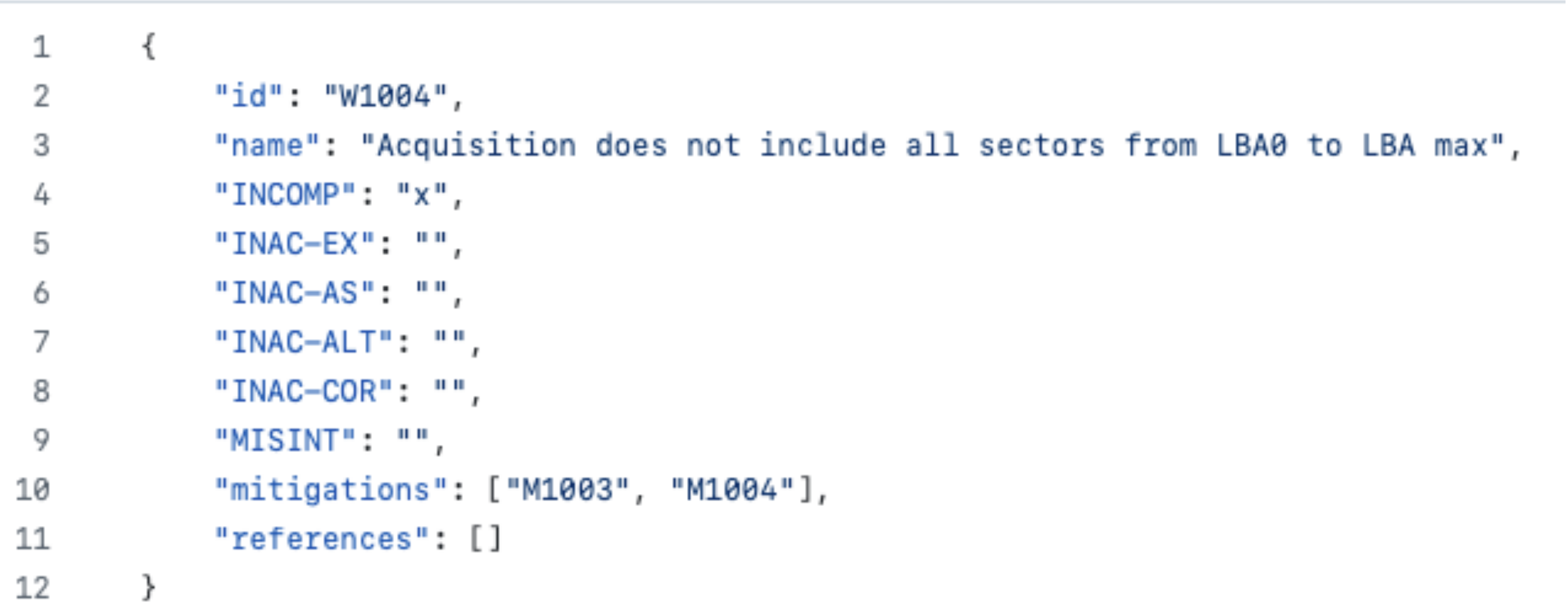
- **INCOMP**: weakness results in incompleteness;
- **INAC-EX**: weakness results in inaccuracy:existence;
- **INAC-AS**: weakness results in inaccuracy:association;
- **INAC-ALT**: weakness results in inaccuracy:alteration;
- **INAC-COR**: weakness results in inaccuracy:corruption;
- **MISINT**: weakness results in potential misinterpretation;

Weaknesses: Implementation



Name
..
mitigations
techniques
weaknesses
carrier.json
dfrws.json
solve-it.json

- W1001.json
- W1002.json
- W1003.json
- W1004.json
- W1005.json
- W1006.json
- W1007.json
- W1008.json
- W1009.json
- W1010.json



```
{
    "id": "W1004",
    "name": "Acquisition does not include all sectors from LBA0 to LBA max",
    "INCOMP": "x",
    "INAC-EX": "",
    "INAC-AS": "",
    "INAC-ALT": "",
    "INAC-COR": "",
    "MISINT": "",
    "mitigations": ["M1003", "M1004"],
    "references": []
}
```

Mitigations: Design

Survey	Preserve	Prioritise	Acquire	Gain Access	Process Storage Format	Perform Data Reduction	Locate Relevant Digital Artefacts	Extract Partition an System Informat

Crime scene s T100

Digital sniff T100

SyncTriage-base T100

Profiling netw T100

Locate cloud identifi T100

Technique name:	Disk imaging	back to main						
Technique ID:	T1002							
Category:	['Acquire']							
Description:	Copying of sectors from a storage media, typically LBA0 to LBAmax into an imaging format. The could be from a traditional hard disk, SSD, USB stick, or data from an eMMC chip that has been desoldered and placed in a reader.							
Synonyms:	[]							
Details:								
Subtechniques:	[]							
CASE output entities:	['observable:Image']							
Examples:	['dcfldd', 'FTK Imager', 'Magnet ACQUIRE']							
Potential weaknesses:								
Weakness ID:	**Detail:**	**INCOMP**	**INAC-EX**	**INAC-AS**	**INAC-ALT**	**INAC-COR**	**MISINT**	**Mitigations**
W1004	Acquisition does not include all sectors from LBA0 to LBA max	x						M1003,
W1006	Acquistion does not include data in HPA	x						M1005,
W1007	Acquistion does not include data in DCO	x						M1006,
W1013	Acquisition includes extra bytes		x					M1003,M1009,
W1014	Imaging process changes original data				x			M1007,M1008,
W1015	Powering on SSD results in sectors being wiped by TRIM operation	x			x	x		
W1016	Data copied from sectors on source are stored incorrectly				x	x		M1009,
W1136	Not recovering data from a failed hard drive	x						M1089,
W1143	Acquisition method does not read remapped sectors e.g. G-Lists	x						M1102,
Mitigations:								
M1003	Check image size corresponds with drive label							

Mitigations are mapped to, and visible within specific weaknesses…

Surve

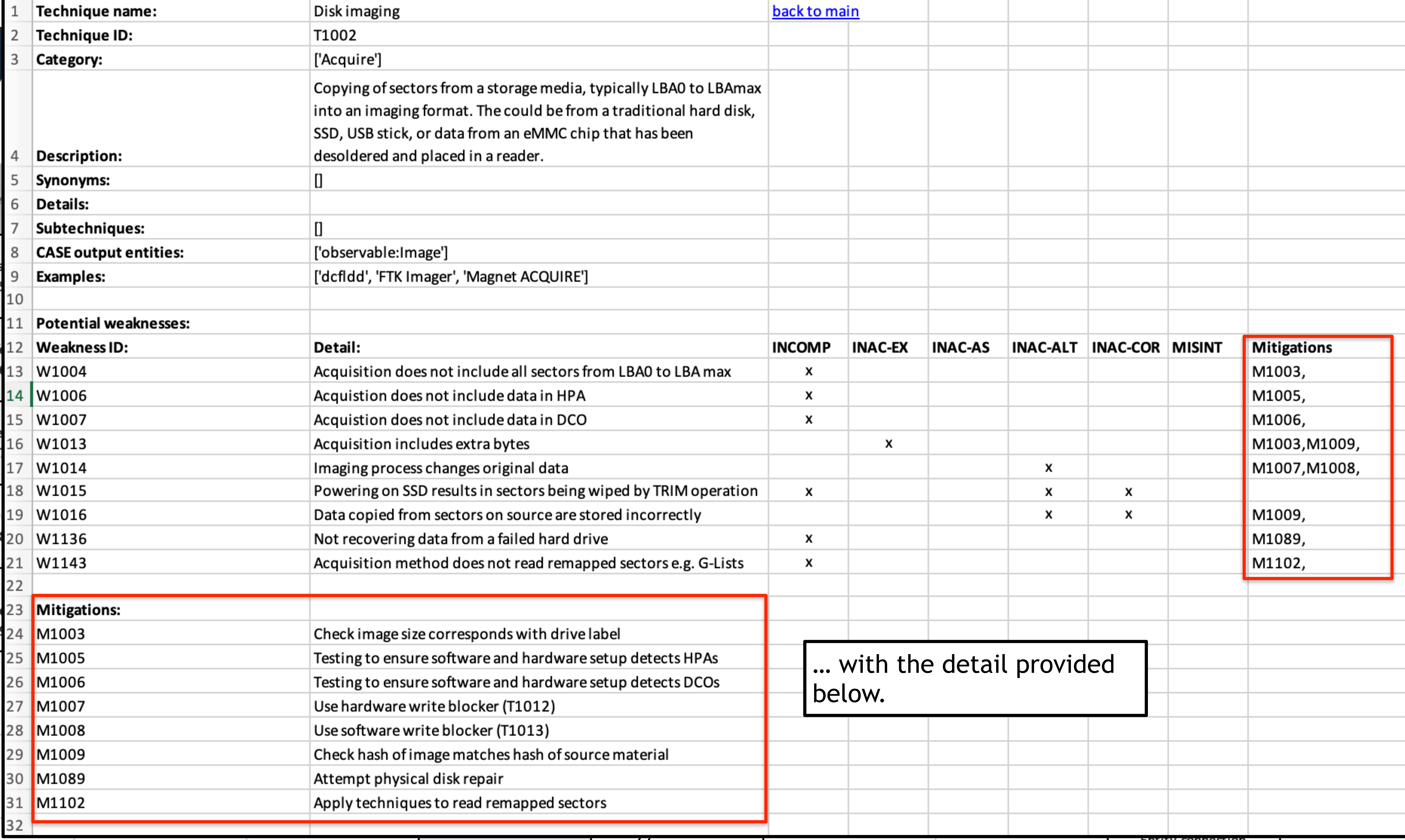
Crime scene s
T1005

Digital sniff
T1006

SyncTriage-base
T1007

Profiling netw
T1008

Locate cloud
identifi
T1009



Technique name:	Disk imaging	back to main
Technique ID:	T1002	
Category:	['Acquire']	
Description:	Copying of sectors from a storage media, typically LBA0 to LBAmax into an imaging format. The could be from a traditional hard disk, SSD, USB stick, or data from an eMMC chip that has been desoldered and placed in a reader.	
Synonyms:	[]	
Details:		
Subtechniques:	[]	
CASE output entities:	['observable:Image']	
Examples:	['dcfldd', 'FTK Imager', 'Magnet ACQUIRE']	

Potential weaknesses:

Weakness ID:	**Detail:**	**INCOMP**	**INAC-EX**	**INAC-AS**	**INAC-ALT**	**INAC-COR**	**MISINT**	**Mitigations**
W1004	Acquisition does not include all sectors from LBA0 to LBA max	x						M1003,
W1006	Acquistion does not include data in HPA	x						M1005,
W1007	Acquistion does not include data in DCO	x						M1006,
W1013	Acquisition includes extra bytes		x					M1003,M1009,
W1014	Imaging process changes original data				x			M1007,M1008,
W1015	Powering on SSD results in sectors being wiped by TRIM operation	x			x	x		
W1016	Data copied from sectors on source are stored incorrectly				x	x		M1009,
W1136	Not recovering data from a failed hard drive	x						M1089,
W1143	Acquisition method does not read remapped sectors e.g. G-Lists	x						M1102,

Mitigations:

M1003	Check image size corresponds with drive label
M1005	Testing to ensure software and hardware setup detects HPAs
M1006	Testing to ensure software and hardware setup detects DCOs
M1007	Use hardware write blocker (T1012)
M1008	Use software write blocker (T1013)
M1009	Check hash of image matches hash of source material
M1089	Attempt physical disk repair
M1102	Apply techniques to read remapped sectors

… with the detail provided below.

Mobile backup extraction

Rainbow tables

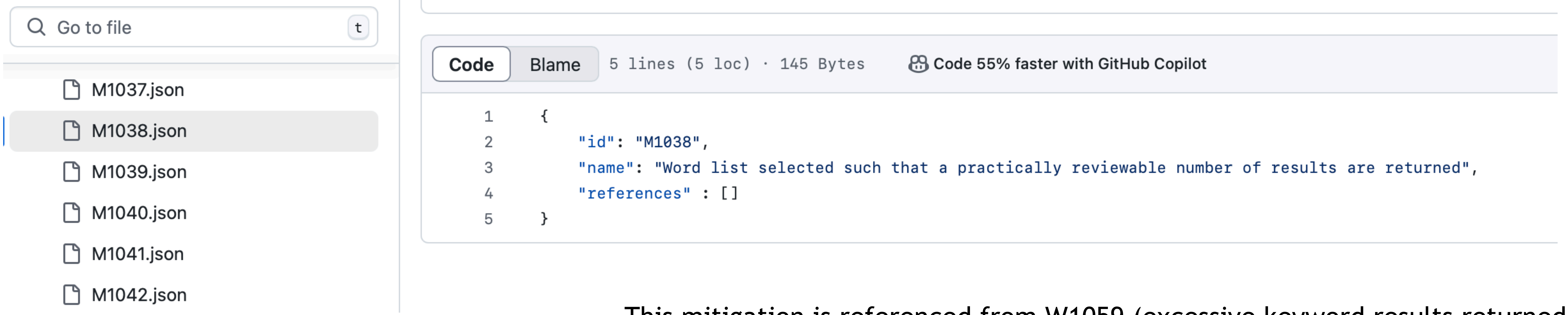
Entity connection

Mitigations: Design

Something that can be done to prevent a weakness from occurring, or to minimise its impact

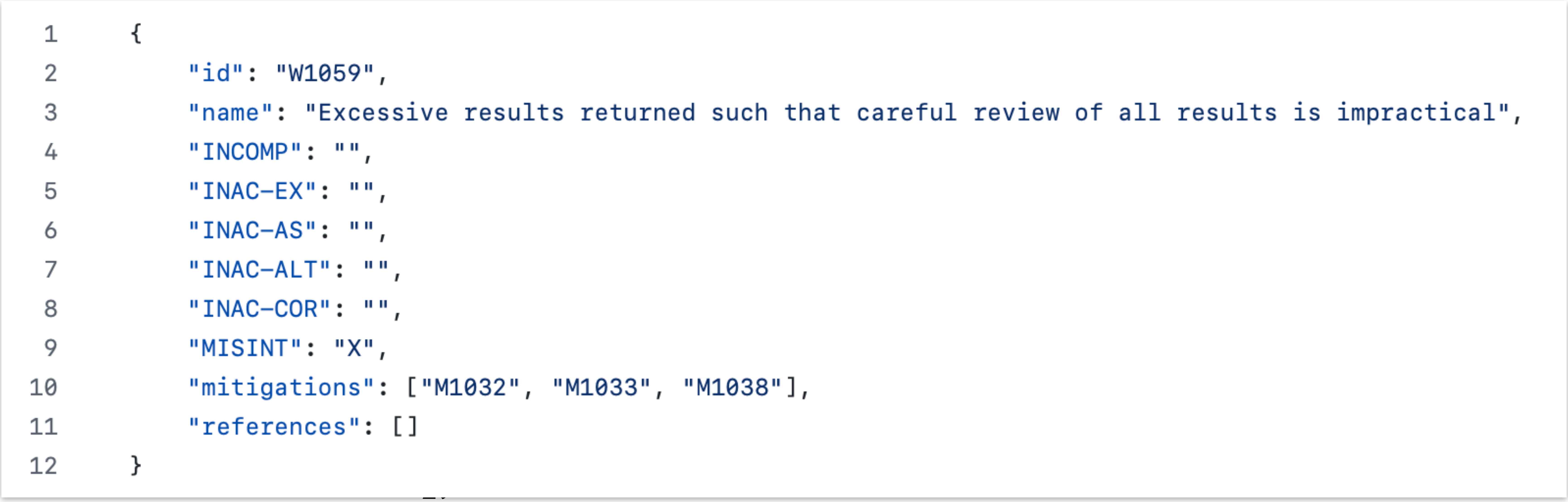
- **id**: the mitigation's ID (e.g. M1001);
- **name**: a short description of the mitigation;
- **details**: A longer description for the mitigation;
- **technique**: an optional index to a related technique. This can be used when a mitigation is sufficiently complex to be considered a technique in its own right;
- **references**: these should be included to support the description of the mitigation.

Mitigations: Implementation



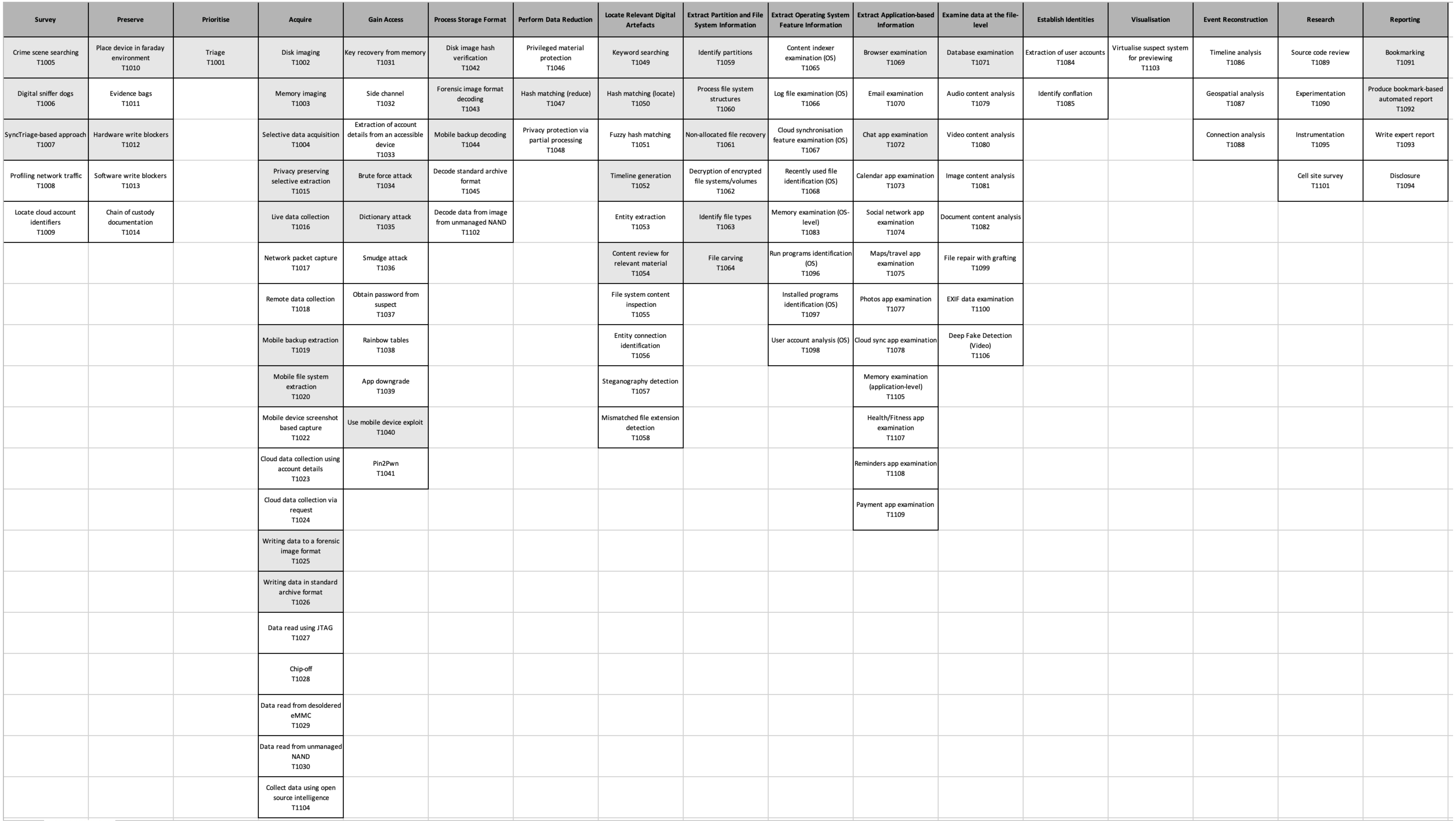
```
{
    "id": "M1038",
    "name": "Word list selected such that a practically reviewable number of results are returned",
    "references" : []
}
```

This mitigation is referenced from W1059 (excessive keyword results returned)



```
{
    "id": "W1059",
    "name": "Excessive results returned such that careful review of all results is impractical",
    "INCOMP": "",
    "INAC-EX": "",
    "INAC-AS": "",
    "INAC-ALT": "",
    "INAC-COR": "",
    "MISINT": "X",
    "mitigations": ["M1032", "M1033", "M1038"],
    "references": []
}
```

Example



Survey	Preserve	Prioritise	Acquire	Gain Access	Process Storage Format	Perform Data Reduction	Locate Relevant Digital Artefacts	Extract Partition and File System Information	Extract Operating System Feature Information	Extract Application-based Information	Examine data at the file-level	Establish Identities	Visualisation	Event Reconstruction	Research	Reporting
Crime scene searching T1005	Place device in faraday environment T1010	Triage T1001	Disk imaging T1002	Key recovery from memory T1031	Disk image hash verification T1042	Privileged material protection T1046	Keyword searching T1049	Identify partitions T1059	Content indexer examination (OS) T1065	Browser examination T1069	Database examination T1071	Extraction of user accounts T1084	Virtualise suspect system for previewing T1103	Timeline analysis T1086	Source code review T1089	Bookmarking T1091
Digital sniffer dogs T1006	Evidence bags T1011		Memory imaging T1003	Side channel T1032	Forensic image format decoding T1043	Hash matching (reduce) T1047	Hash matching (locate) T1050	Process file system structures T1060	Log file examination (OS) T1066	Email examination T1070	Audio content analysis T1079	Identify conflation T1085		Geospatial analysis T1087	Experimentation T1090	Produce bookmark-based automated report T1092
SyncTriage-based approach T1007	Hardware write blockers T1012		Selective data acquisition T1004	Extraction of account details from an accessible device T1033	Mobile backup decoding T1044	Privacy protection via partial processing T1048	Fuzzy hash matching T1051	Non-allocated file recovery T1061	Cloud synchronisation feature examination (OS) T1067	Chat app examination T1072	Video content analysis T1080			Connection analysis T1088	Instrumentation T1095	Write expert report T1093
Profiling network traffic T1008	Software write blockers T1013		Privacy preserving selective extraction T1015	Brute force attack T1034	Decode standard archive format T1045		Timeline generation T1052	Decryption of encrypted file systems/volumes T1062	Recently used file identification (OS) T1068	Calendar app examination T1073	Image content analysis T1081				Cell site survey T1101	Disclosure T1094
Locate cloud account identifiers T1009	Chain of custody documentation T1014		Live data collection T1016	Dictionary attack T1035	Decode data from image from unmanaged NAND T1102		Entity extraction T1053	Identify file types T1063	Memory examination (OS-level) T1083	Social network app examination T1074	Document content analysis T1082					
			Network packet capture T1017	Smudge attack T1036			Content review for relevant material T1054	File carving T1064	Run programs identification (OS) T1096	Maps/travel app examination T1075	File repair with grafting T1099					
			Remote data collection T1018	Obtain password from suspect T1037			File system content inspection T1055		Installed programs identification (OS) T1097	Photos app examination T1077	EXIF data examination T1100					
			Mobile backup extraction T1019	Rainbow tables T1038			Entity connection identification T1056		User account analysis (OS) T1098	Cloud sync app examination T1078	Deep Fake Detection (Video) T1106					
			Mobile file system extraction T1020	App downgrade T1039			Steganography detection T1057			Memory examination (application-level) T1105						
			Mobile device screenshot based capture T1022	Use mobile device exploit T1040			Mismatched file extension detection T1058			Health/Fitness app examination T1107						
			Cloud data collection using account details T1023	Pin2Pwn T1041						Reminders app examination T1108						
			Cloud data collection via request T1024							Payment app examination T1109						
			Writing data to a forensic image format T1025													
			Writing data in standard archive format T1026													
			Data read using JTAG T1027													
			Chip-off T1028													
			Data read from desoldered eMMC T1029													
			Data read from unmanaged NAND T1030													
			Collect data using open source intelligence T1104													

Survey	Preserve	Prioritise	Acquire	Gain Access	Process Storage Format	Perform Data Reduction	Locate R A
Crime scene searching T1005	Place device in faraday environment T1010	Triage T1001	Disk imaging T1002	Key recovery from memory T1031	Disk image hash verification T1042	Privileged material protection T1046	Keywo
Digital sniffer dogs T1006	Evidence bags T1011		Memory imaging T1003	Side channel T1032	Forensic image format decoding T1043	Hash matching (reduce) T1047	Hash ma
SyncTriage-based approach T1007	Hardware write blockers T1012		Selective data acquisition T1004	Extraction of account details from an accessible device T1033	Mobile backup decoding T1044	Privacy protection via partial processing T1048	Fuzzy h
Profiling network traffic T1008	Software write blockers T1013		Privacy preserving selective extraction T1015	Brute force attack T1034	Decode standard archive format T1045		Timelin
Locate cloud account identifiers T1009	Chain of custody documentation T1014		Live data collection T1016	Dictionary attack T1035	Decode data from image from unmanaged NAND T1102		Entity
			Network packet capture T1017	Smudge attack T1036			Conter releva
			Remote data collection T1018	Obtain password from suspect T1037			File sys in
			Mobile backup extraction T1019	Rainbow tables T1038			Entity iden

Example - T1002 - Disk imaging

Technique name:	Disk imaging	back to main				
Technique ID:	T1002					
Category:	['Acquire']					
Description:	Copying of sectors from a storage media, typically LBA0 to LBAmax into an imaging format. The could be from a traditional hard disk, SSD, USB stick, or data from an eMMC chip that has been desoldered and placed in a reader.					
Synonyms:	[]					
Details:						
Subtechniques:	[]					
CASE output entities:	['observable:Image']					
Examples:	['dcfldd', 'FTK Imager', 'Magnet ACQUIRE']					
Potential weaknesses:						
Weakness ID:	**Detail:**	**INCOMP**	**INAC-EX**	**INAC-AS**	**INAC-ALT**	**IN**
W1004	Acquisition does not include all sectors from LBA0 to LBA max	x				
W1006	Acquistion does not include data in HPA	x				
W1007	Acquistion does not include data in DCO	x				
W1013	Acquisition includes extra bytes		x			
W1014	Imaging process changes original data				x	
W1015	Powering on SSD results in sectors being wiped by TRIM operation	x			x	
W1016	Data copied from sectors on source are stored incorrectly				x	

Example - Disk imaging (Weaknesses and Mitigations)

D								
Sy								
Details:								
Subtechniques:	[]							
CASE output entities:	['observable:Image']							
Examples:	['dcfldd', 'FTK Imager', 'Magnet ACQUIRE']							
Potential weaknesses:								
Weakness ID:	**Detail:**	**INCOMP**	**INAC-EX**	**INAC-AS**	**INAC-ALT**	**INAC-COR**	**MISINT**	**Mitigations**
W1004	Acquisition does not include all sectors from LBA0 to LBA max	x						M1003,
W1006	Acquistion does not include data in HPA	x						M1005,
W1007	Acquistion does not include data in DCO	x						M1006,
W1013	Acquisition includes extra bytes		x					M1003,M1009,
W1014	Imaging process changes original data				x			M1007,M1008,
W1015	Powering on SSD results in sectors being wiped by TRIM operation	x			x	x		
W1016	Data copied from sectors on source are stored incorrectly				x	x		M1009,
W1136	Not recovering data from a failed hard drive	x						M1089,
W1143	Acquisition method does not read remapped sectors e.g. G-Lists	x						M1102,
Mitigations:								
M1003	Check image size corresponds with drive label							
M1005	Testing to ensure software and hardware setup detects HPAs							
M1006	Testing to ensure software and hardware setup detects DCOs							
M1007	Use hardware write blocker (T1012)							
M1008	Use software write blocker (T1013)							
M1009	Check hash of image matches hash of source material							
M1089	Attempt physical disk repair							
M1102	Apply techniques to read remapped sectors							

Example - Disk imaging (Weaknesses and Mitigations)

De								
Sy								
Details:								
Subtechniques:	[]							
CASE output entities:	['observable:Image']							
Examples:	['dcfldd', 'FTK Imager', 'Magnet ACQUIRE']							
Potential weaknesses:								
Weakness ID:	**Detail:**	**INCOMP**	**INAC-EX**	**INAC-AS**	**INAC-ALT**	**INAC-COR**	**MISINT**	**Mitigations**
W1004	Acquisition does not include all sectors from LBA0 to LBA max	x						M1003,
W1006	Acquistion does not include data in HPA	x						M1005,
W1007	Acquistion does not include data in DCO	x						M1006,
W1013	Acquisition includes extra bytes		x					M1003,M1009,
W1014	Imaging process changes original data				x			M1007,M1008,
W1015	Powering on SSD results in sectors being wiped by TRIM operation	x			x	x		
W1016	Data copied from sectors on source are stored incorrectly				x	x		M1009,
W1136	Not recovering data from a failed hard drive	x						M1089,
W1143	Acquisition method does not read remapped sectors e.g. G-Lists	x						M1102,
Mitigations:								
M1003	Check image size corresponds with drive label							
M1005	Testing to ensure software and hardware setup detects HPAs							
M1006	Testing to ensure software and hardware setup detects DCOs							
M1007	Use hardware write blocker (T1012)							
M1008	Use software write blocker (T1013)							
M1009	Check hash of image matches hash of source material							
M1089	Attempt physical disk repair							
M1102	Apply techniques to read remapped sectors							

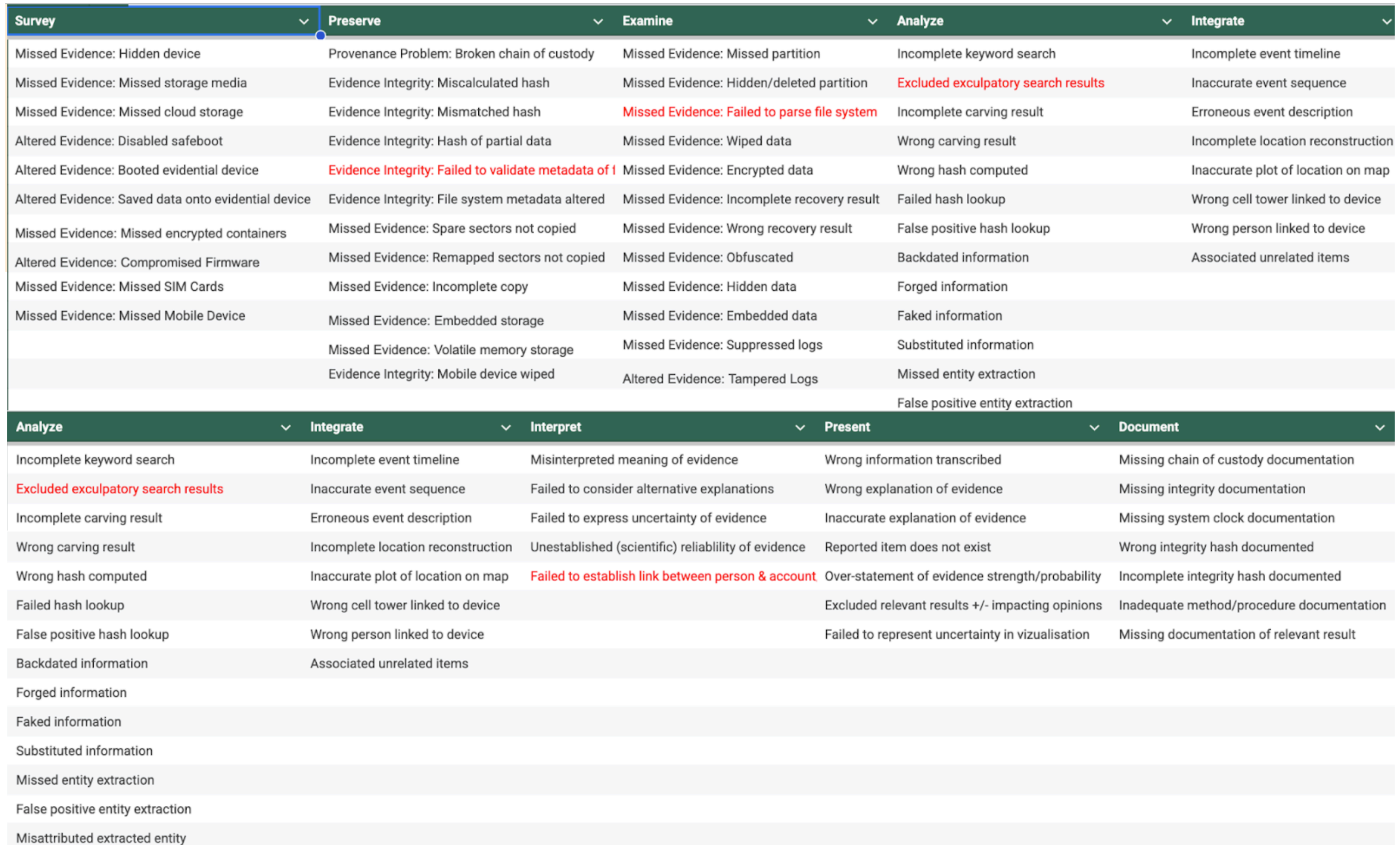
Example - Disk imaging (Weaknesses and Mitigations)

De								
Sy								
Details:								
Subtechniques:	[]							
CASE output entities:	['observable:Image']							
Examples:	['dcfldd', 'FTK Imager', 'Magnet ACQUIRE']							
Potential weaknesses:								
Weakness ID:	**Detail:**	**INCOMP**	**INAC-EX**	**INAC-AS**	**INAC-ALT**	**INAC-COR**	**MISINT**	**Mitigations**
W1004	Acquisition does not include all sectors from LBA0 to LBA max	x						M1003,
W1006	Acquistion does not include data in HPA	x						M1005,
W1007	Acquistion does not include data in DCO	x						M1006,
W1013	Acquisition includes extra bytes		x					M1003,M1009,
W1014	Imaging process changes original data				x			M1007,M1008,
W1015	Powering on SSD results in sectors being wiped by TRIM operation	x			x	x		
W1016	Data copied from sectors on source are stored incorrectly				x	x		M1009,
W1136	Not recovering data from a failed hard drive	x						M1089,
W1143	Acquisition method does not read remapped sectors e.g. G-Lists	x						M1102,
Mitigations:								
M1003	Check image size corresponds with drive label							
M1005	Testing to ensure software and hardware setup detects HPAs							
M1006	Testing to ensure software and hardware setup detects DCOs							
M1007	Use hardware write blocker (T1012)							
M1008	Use software write blocker (T1013)							
M1009	Check hash of image matches hash of source material							
M1089	Attempt physical disk repair							
M1102	Apply techniques to read remapped sectors							

Demonstrative Examples (Applications)

Applications: Scoping error focused datasets

Digital Evidence Weakness Taxonomy

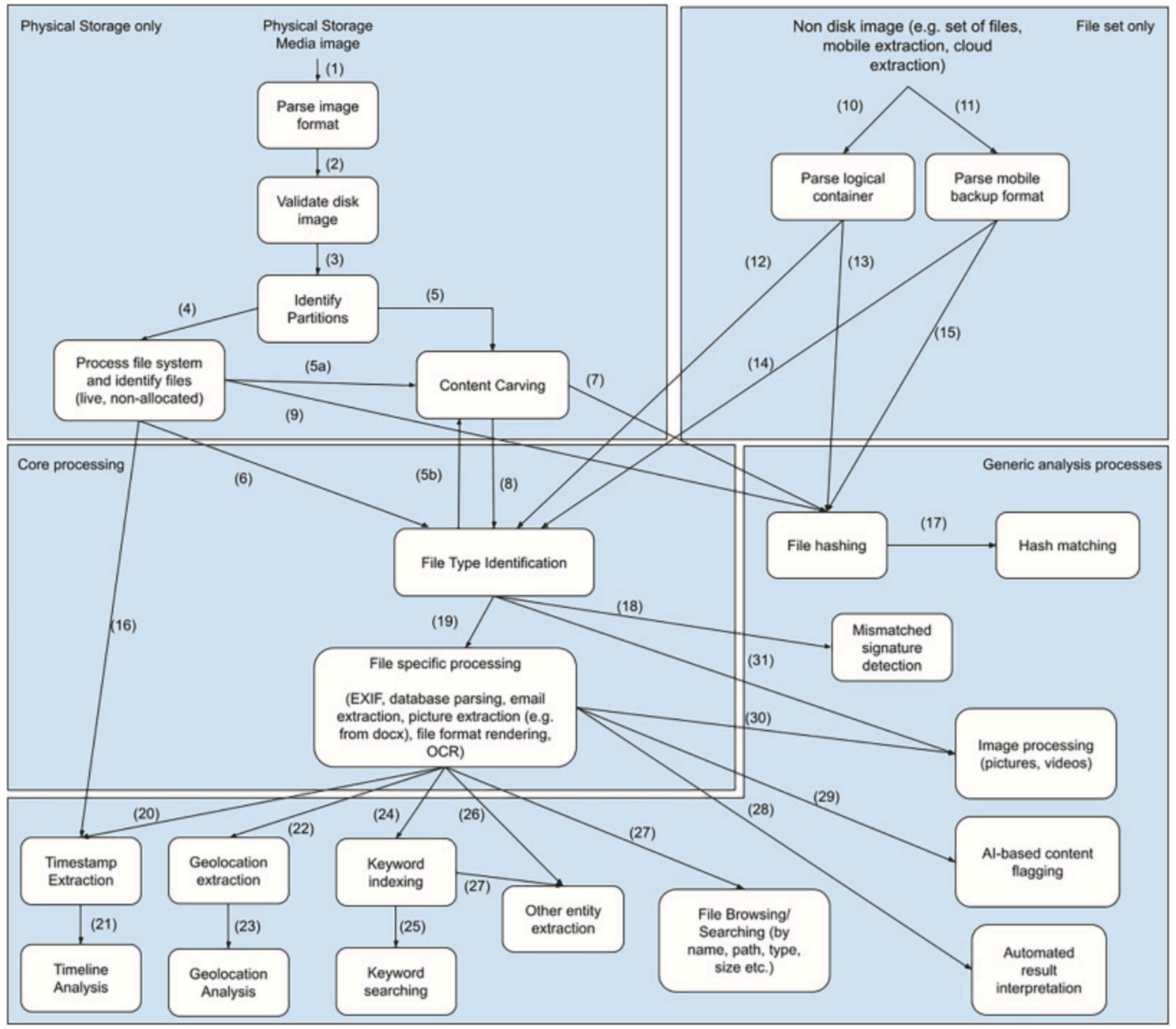


Survey	Preserve	Examine	Analyze	Integrate
Missed Evidence: Hidden device	Provenance Problem: Broken chain of custody	Missed Evidence: Missed partition	Incomplete keyword search	Incomplete event timeline
Missed Evidence: Missed storage media	Evidence Integrity: Miscalculated hash	Missed Evidence: Hidden/deleted partition	Excluded exculpatory search results	Inaccurate event sequence
Missed Evidence: Missed cloud storage	Evidence Integrity: Mismatched hash	Missed Evidence: Failed to parse file system	Incomplete carving result	Erroneous event description
Altered Evidence: Disabled safeboot	Evidence Integrity: Hash of partial data	Missed Evidence: Wiped data	Wrong carving result	Incomplete location reconstruction
Altered Evidence: Booted evidential device	Evidence Integrity: Failed to validate metadata of I	Missed Evidence: Encrypted data	Wrong hash computed	Inaccurate plot of location on map
Altered Evidence: Saved data onto evidential device	Evidence Integrity: File system metadata altered	Missed Evidence: Incomplete recovery result	Failed hash lookup	Wrong cell tower linked to device
Missed Evidence: Missed encrypted containers	Missed Evidence: Spare sectors not copied	Missed Evidence: Wrong recovery result	False positive hash lookup	Wrong person linked to device
Altered Evidence: Compromised Firmware	Missed Evidence: Remapped sectors not copied	Missed Evidence: Obfuscated	Backdated information	Associated unrelated items
Missed Evidence: Missed SIM Cards	Missed Evidence: Incomplete copy	Missed Evidence: Hidden data	Forged information	
Missed Evidence: Missed Mobile Device	Missed Evidence: Embedded storage	Missed Evidence: Embedded data	Faked information	
	Missed Evidence: Volatile memory storage	Missed Evidence: Suppressed logs	Substituted information	
	Evidence Integrity: Mobile device wiped	Altered Evidence: Tampered Logs	Missed entity extraction	
			False positive entity extraction	

Analyze	Integrate	Interpret	Present	Document
Incomplete keyword search	Incomplete event timeline	Misinterpreted meaning of evidence	Wrong information transcribed	Missing chain of custody documentation
Excluded exculpatory search results	Inaccurate event sequence	Failed to consider alternative explanations	Wrong explanation of evidence	Missing integrity documentation
Incomplete carving result	Erroneous event description	Failed to express uncertainty of evidence	Inaccurate explanation of evidence	Missing system clock documentation
Wrong carving result	Incomplete location reconstruction	Unestablished (scientific) reliablility of evidence	Reported item does not exist	Wrong integrity hash documented
Wrong hash computed	Inaccurate plot of location on map	Failed to establish link between person & account	Over-statement of evidence strength/probability	Incomplete integrity hash documented
Failed hash lookup	Wrong cell tower linked to device		Excluded relevant results +/- impacting opinions	Inadequate method/procedure documentation
False positive hash lookup	Wrong person linked to device		Failed to represent uncertainty in vizualisation	Missing documentation of relevant result
Backdated information	Associated unrelated items			
Forged information				
Faked information				
Substituted information				
Missed entity extraction				
False positive entity extraction				
Misattributed extracted entity				

Casey (2023)

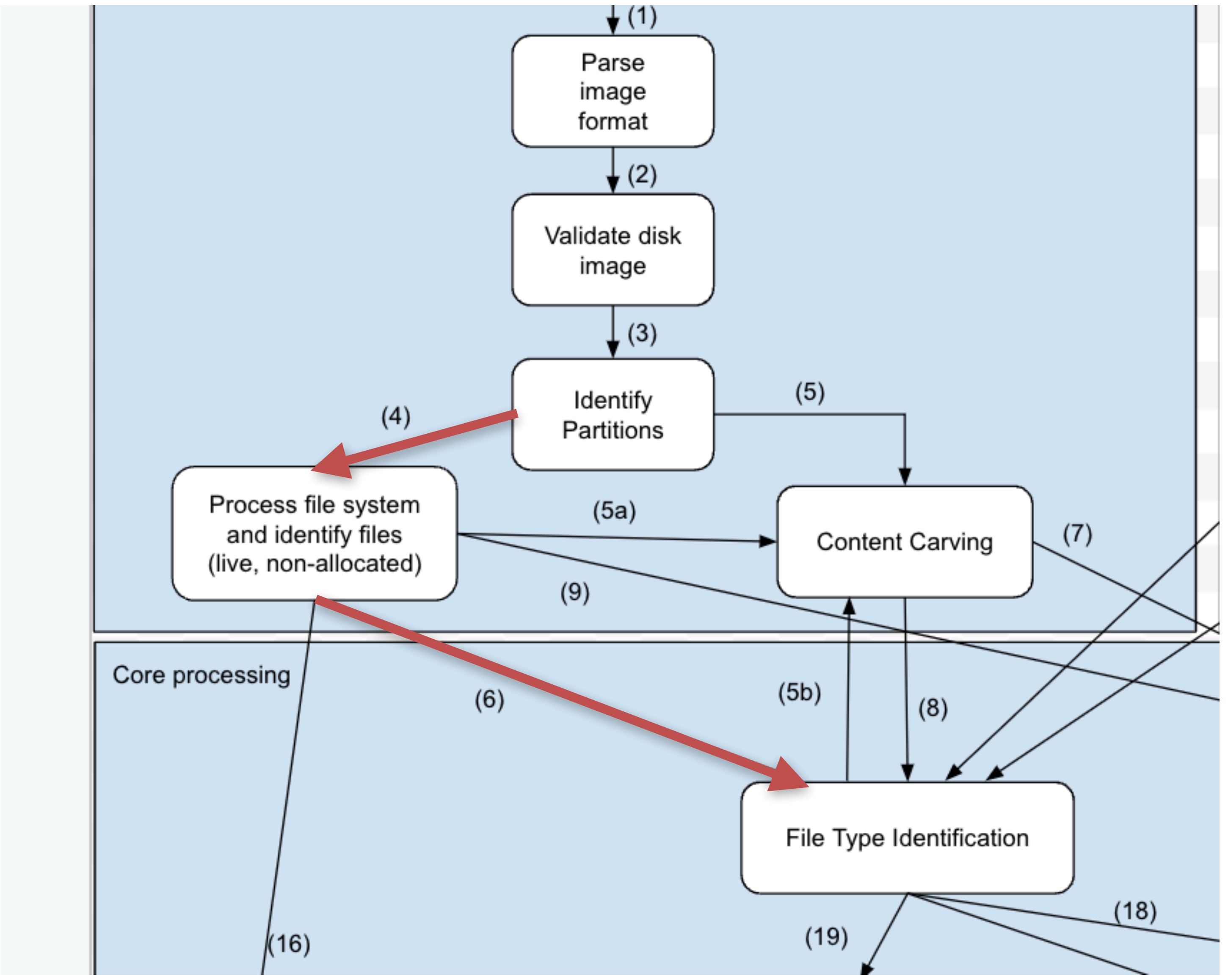
An abstract model for digital forensic analysis tools:
A foundation for systematic error mitigation analysis

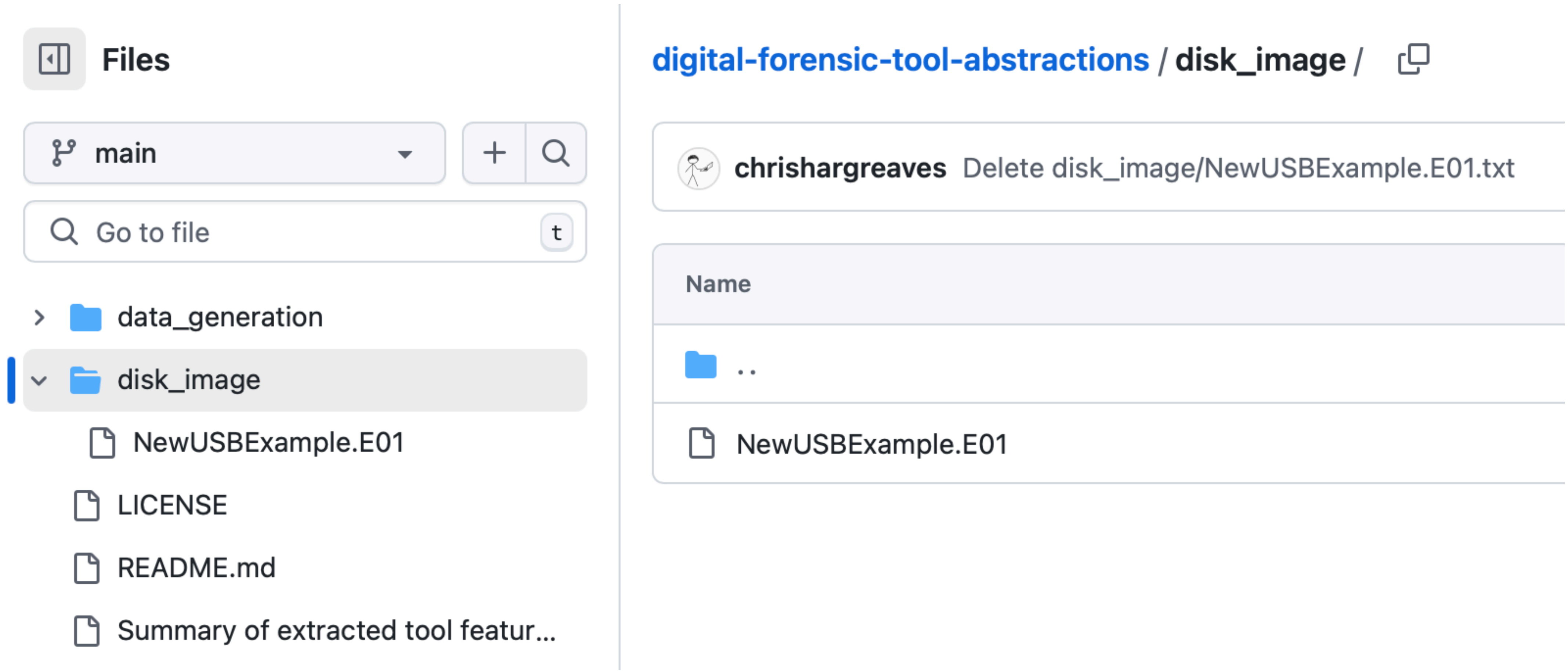

Physical Storage only
Physical Storage Media image
(1)
Parse image format
(2)
Validate disk image
(3)
Identify Partitions
(4)
(5)
Process file system and identify files (live, non-allocated)
(5a)
Content Carving
(7)
(9)
Non disk image (e.g. set of files, mobile extraction, cloud extraction)
File set only
(10)
(11)
Parse logical container
Parse mobile backup format
(12)
(13)
(14)
(15)
Core processing
(6)
(5b)
(8)
Generic analysis processes
File Type Identification
File hashing
(17)
Hash matching
(16)
(19)
(18)
Mismatched signature detection
(31)
File specific processing
(EXIF, database parsing, email extraction, picture extraction (e.g. from docx), file format rendering, OCR)
(30)
Image processing (pictures, videos)
(29)
(20)
(22)
(24)
(26)
(27)
(28)
AI-based content flagging
Timestamp Extraction
Geolocation extraction
Keyword indexing
(27)
Other entity extraction
File Browsing/ Searching (by name, path, type, size etc.)
(21)
(23)
(25)
Timeline Analysis
Geolocation Analysis
Keyword searching
Automated result interpretation

Potential Error Introduced at this Stage: Image format parsing could fail to present all blocks from within a forensic container image in their 'flat' (dd) representation (INCOMP), or present incorrect data within sectors (INAC-ALT). Alternatively it could present incorrect forensic image metadata (INAC-ALT). Some imaging tools include "maps" to record when disk regions were not recovered, mitigating INCOMP issues; but failure to incorporate such a map into downstream analysis can lead to process and analysis errors from "preserving" the original faults in the copy process (INAC-COR).

Hargreaves et al (2024)

Applications: Scoping error focused datasets



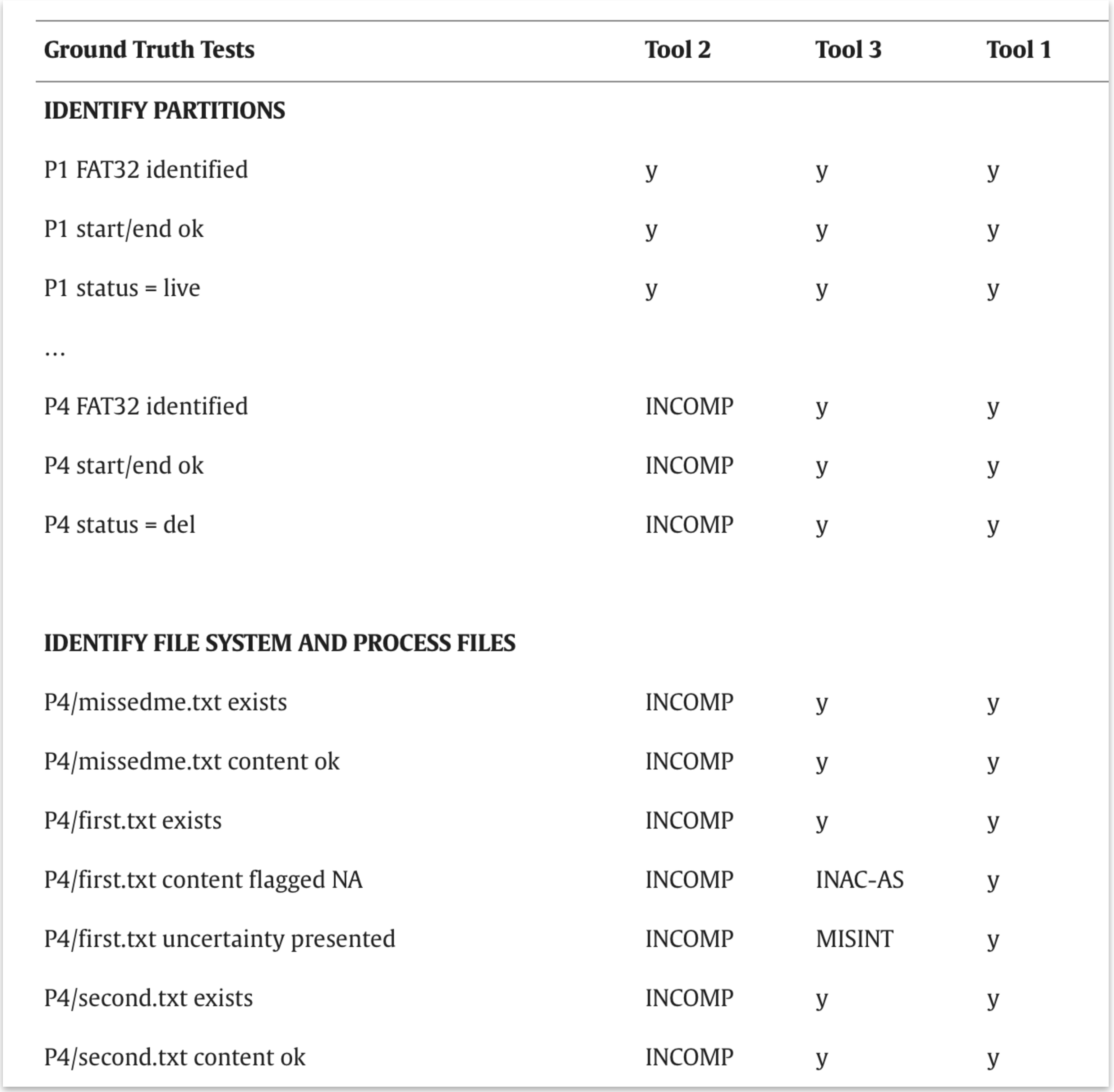


- data_generation
- disk_image
  - NewUSBExample.E01
- LICENSE
- README.md
- Summary of extracted tool featur...

digital-forensic-tool-abstractions / disk_image /

chrishargreaves Delete disk_image/NewUSBExample.E01.txt

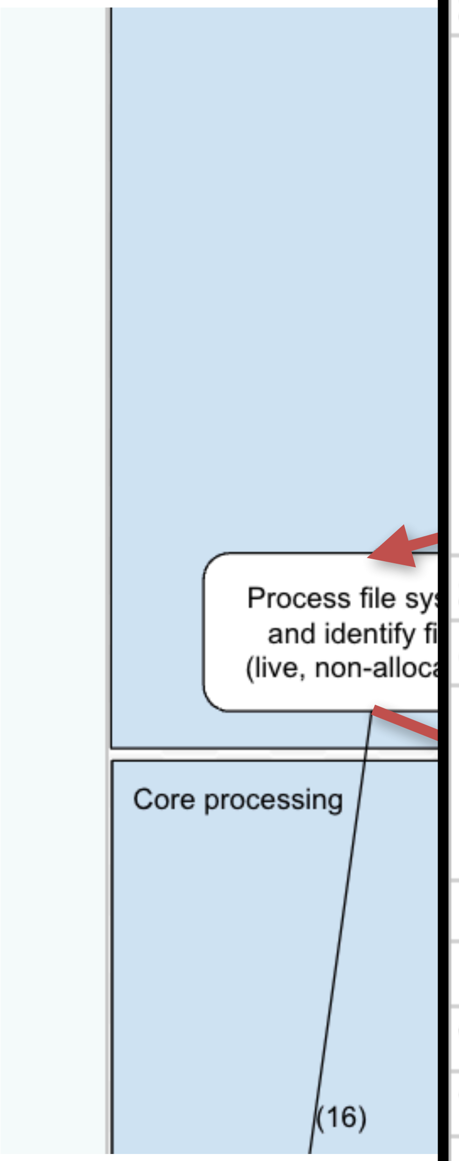
Name
..
NewUSBExample.E01

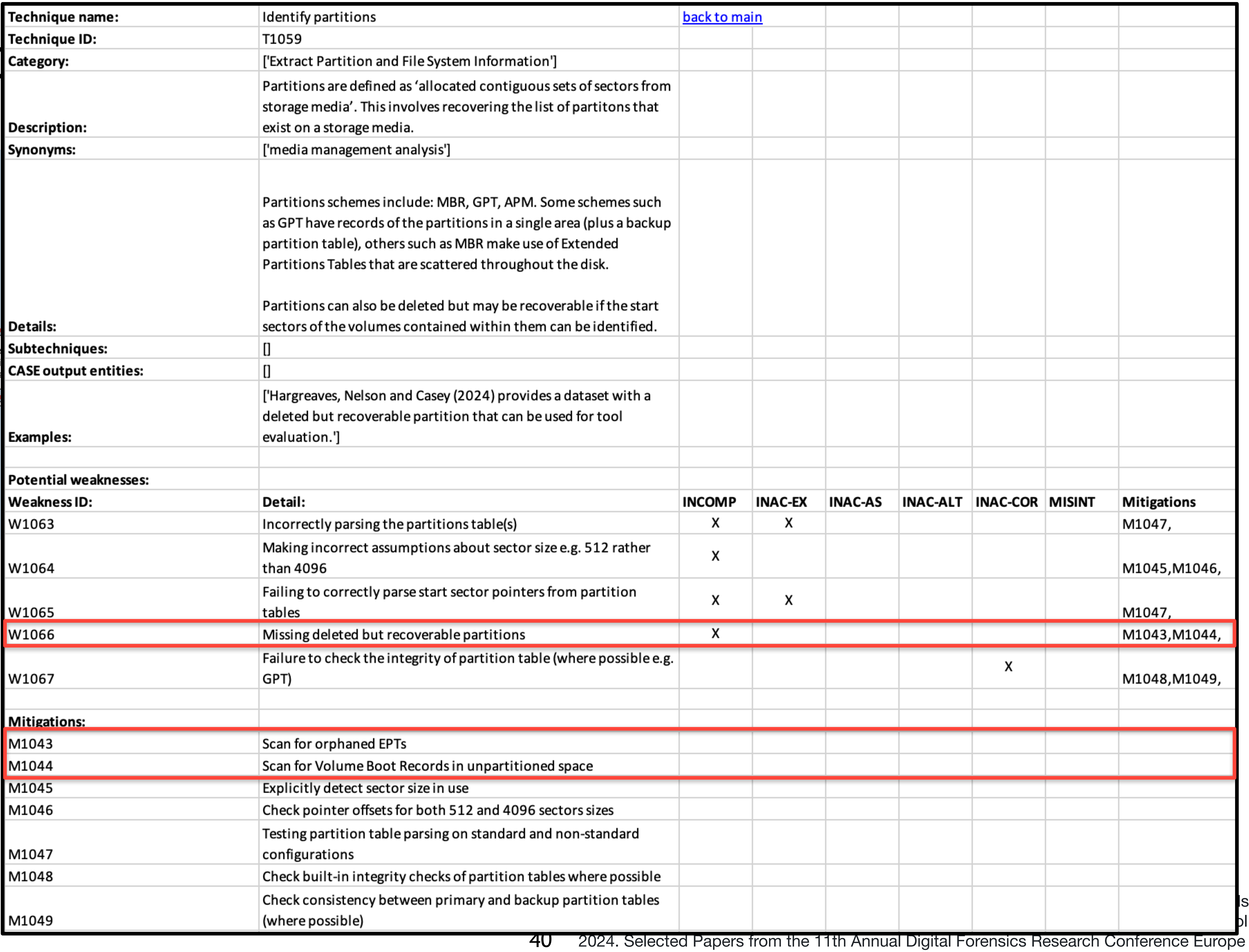


Ground Truth Tests	Tool 2	Tool 3	Tool 1
IDENTIFY PARTITIONS			
P1 FAT32 identified	y	y	y
P1 start/end ok	y	y	y
P1 status = live	y	y	y
…			
P4 FAT32 identified	INCOMP	y	y
P4 start/end ok	INCOMP	y	y
P4 status = del	INCOMP	y	y
IDENTIFY FILE SYSTEM AND PROCESS FILES			
P4/missedme.txt exists	INCOMP	y	y
P4/missedme.txt content ok	INCOMP	y	y
P4/first.txt exists	INCOMP	y	y
P4/first.txt content flagged NA	INCOMP	INAC-AS	y
P4/first.txt uncertainty presented	INCOMP	MISINT	y
P4/second.txt exists	INCOMP	y	y
P4/second.txt content ok	INCOMP	y	y

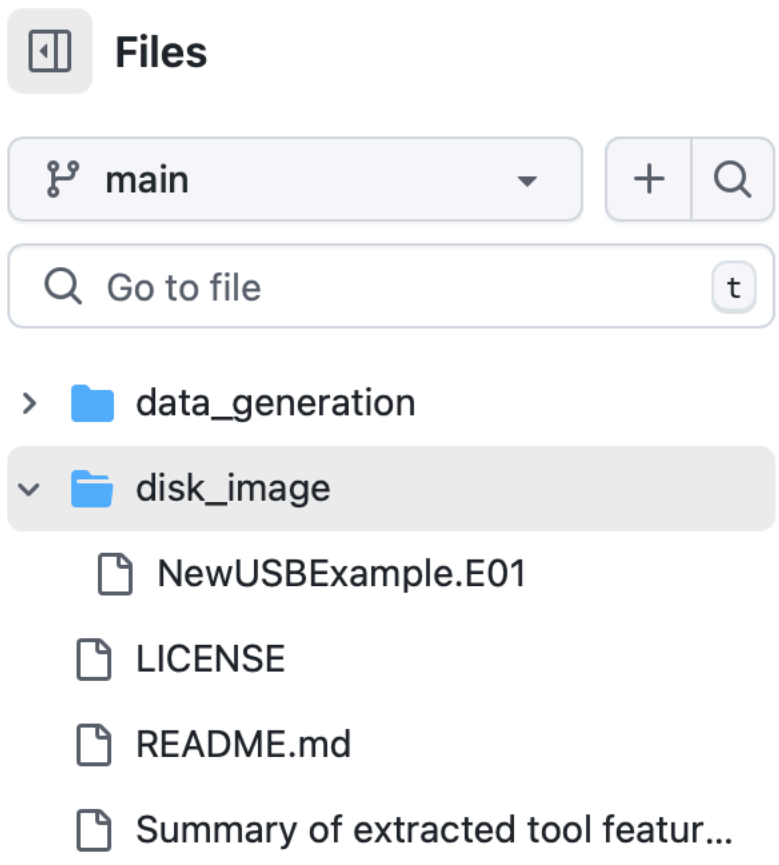
Hargreaves, C., Nelson, A. and Casey E, An abstract model for digital forensic analysis tools - A foundation for systematic error mitigation analysis, Forensic Science International: Digital Investigation. Vol. 48. Pages 301679. 2024. Selected Papers from the 11th Annual Digital Forensics Research Conference Europe (DFRWS EU 2024).

Applicatio





Technique name:	Identify partitions	back to main						
Technique ID:	T1059							
Category:	['Extract Partition and File System Information']							
Description:	Partitions are defined as 'allocated contiguous sets of sectors from storage media'. This involves recovering the list of partitons that exist on a storage media.							
Synonyms:	['media management analysis']							
Details:	Partitions schemes include: MBR, GPT, APM. Some schemes such as GPT have records of the partitions in a single area (plus a backup partition table), others such as MBR make use of Extended Partitions Tables that are scattered throughout the disk. Partitions can also be deleted but may be recoverable if the start sectors of the volumes contained within them can be identified.							
Subtechniques:	[]							
CASE output entities:	[]							
Examples:	['Hargreaves, Nelson and Casey (2024) provides a dataset with a deleted but recoverable partition that can be used for tool evaluation.']							
Potential weaknesses:								
Weakness ID:	**Detail:**	**INCOMP**	**INAC-EX**	**INAC-AS**	**INAC-ALT**	**INAC-COR**	**MISINT**	**Mitigations**
W1063	Incorrectly parsing the partitions table(s)	X	X					M1047,
W1064	Making incorrect assumptions about sector size e.g. 512 rather than 4096	X						M1045,M1046,
W1065	Failing to correctly parse start sector pointers from partition tables	X	X					M1047,
W1066	Missing deleted but recoverable partitions	X						M1043,M1044,
W1067	Failure to check the integrity of partition table (where possible e.g. GPT)					X		M1048,M1049,
Mitigations:								
M1043	Scan for orphaned EPTs							
M1044	Scan for Volume Boot Records in unpartitioned space							
M1045	Explicitly detect sector size in use							
M1046	Check pointer offsets for both 512 and 4096 sectors sizes							
M1047	Testing partition table parsing on standard and non-standard configurations							
M1048	Check built-in integrity checks of partition tables where possible							
M1049	Check consistency between primary and backup partition tables (where possible)							



ls - A foundation for
ol. 48. Pages 301679.
2024. Selected Papers from the 11th Annual Digital Forensics Research Conference Europe (DFRWS EU 2024).

Can capture problems encountered as technology changes

iOS 10 -> iOS 11,
change to sms.db,
timestamp resolution change, only
for new messages!

(Barnhart, 2017)

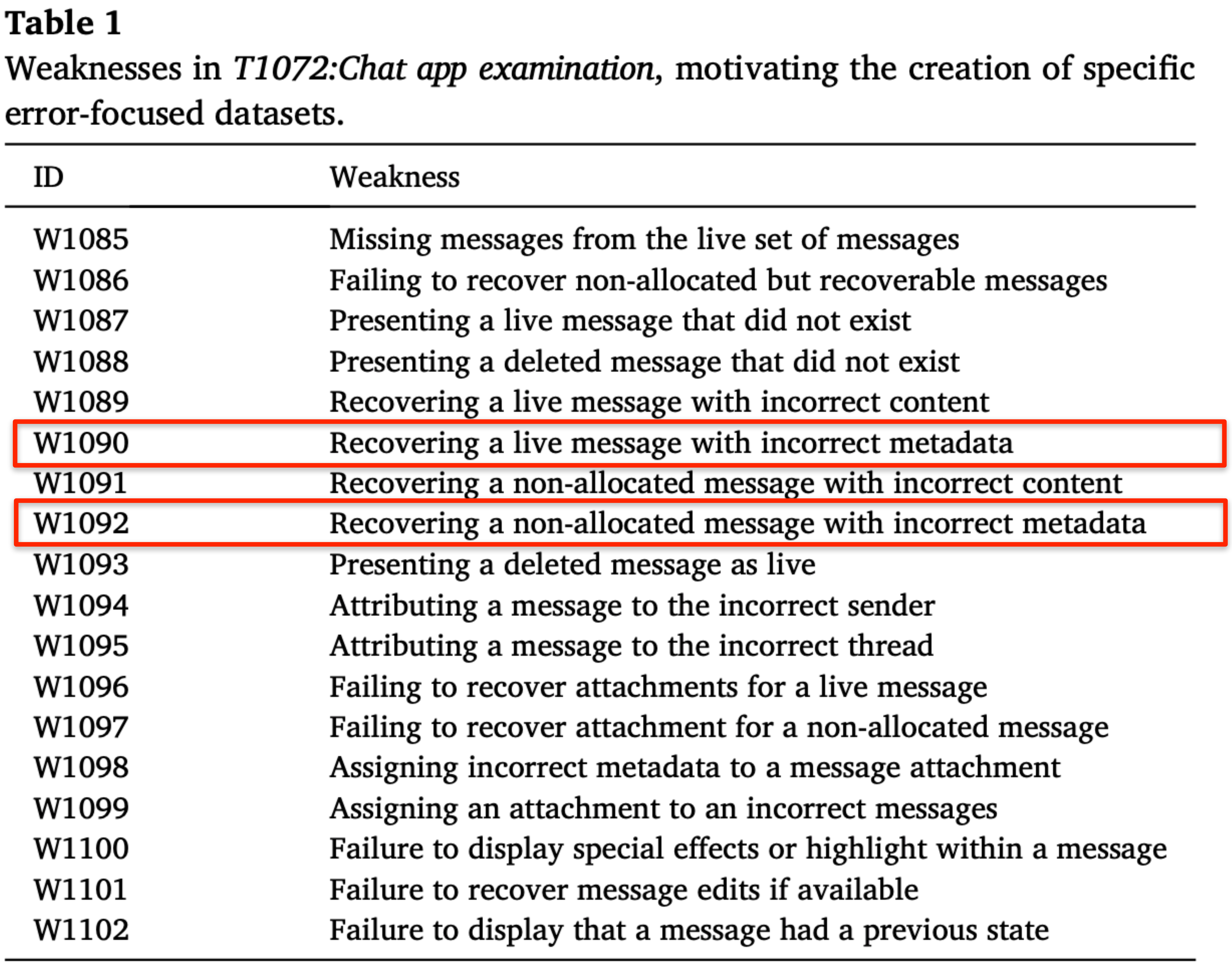


Table 1
Weaknesses in *T1072:Chat app examination*, motivating the creation of specific error-focused datasets.

ID	Weakness
W1085	Missing messages from the live set of messages
W1086	Failing to recover non-allocated but recoverable messages
W1087	Presenting a live message that did not exist
W1088	Presenting a deleted message that did not exist
W1089	Recovering a live message with incorrect content
W1090	Recovering a live message with incorrect metadata
W1091	Recovering a non-allocated message with incorrect content
W1092	Recovering a non-allocated message with incorrect metadata
W1093	Presenting a deleted message as live
W1094	Attributing a message to the incorrect sender
W1095	Attributing a message to the incorrect thread
W1096	Failing to recover attachments for a live message
W1097	Failing to recover attachment for a non-allocated message
W1098	Assigning incorrect metadata to a message attachment
W1099	Assigning an attachment to an incorrect messages
W1100	Failure to display special effects or highlight within a message
W1101	Failure to recover message edits if available
W1102	Failure to display that a message had a previous state

Can capture problems encountered as technology changes

WhatApp field change in version 2.22.11.82, *messages* table -> *message* table

BinaryHick (2022)

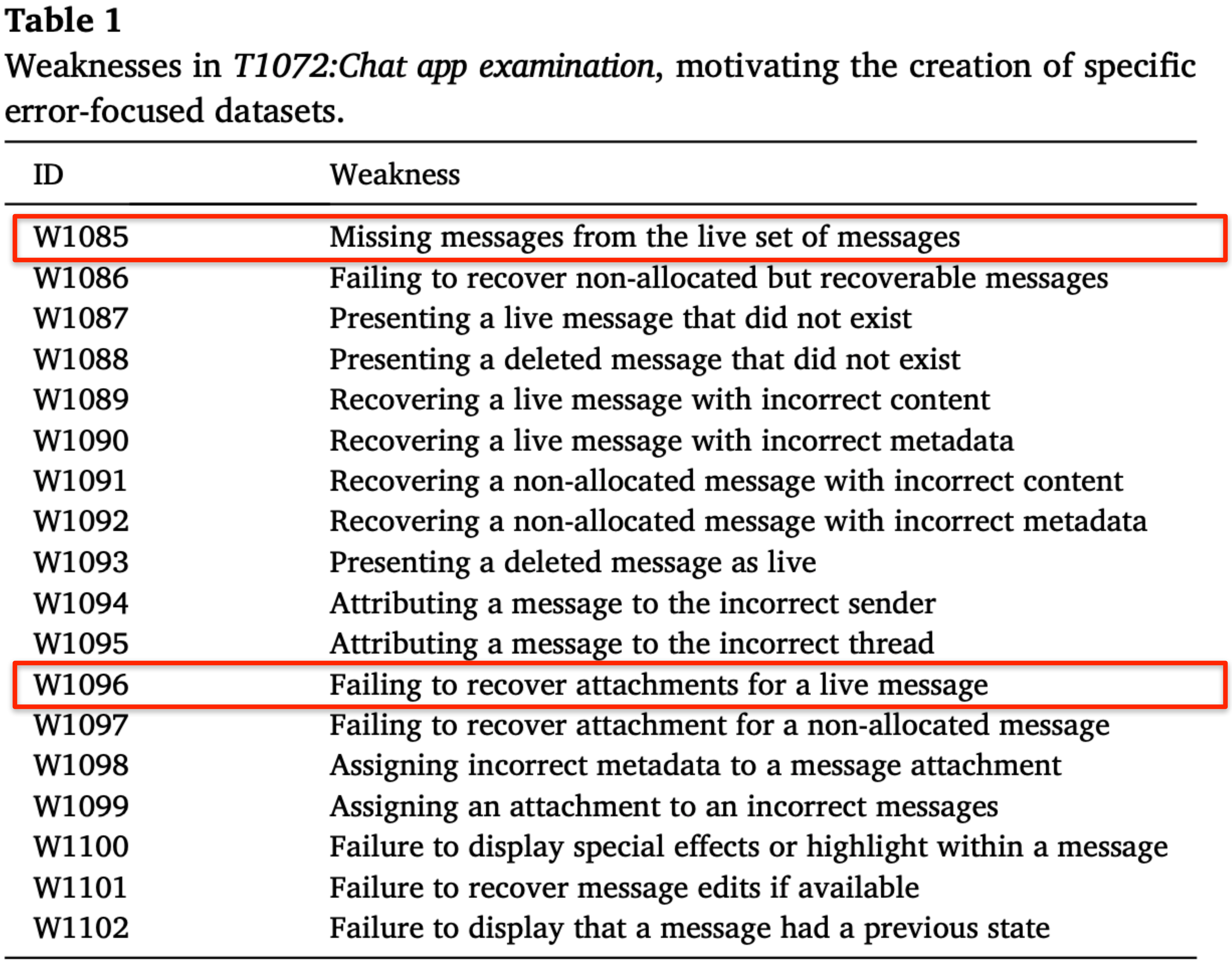


Table 1
Weaknesses in *T1072:Chat app examination*, motivating the creation of specific error-focused datasets.

ID	Weakness
W1085	Missing messages from the live set of messages
W1086	Failing to recover non-allocated but recoverable messages
W1087	Presenting a live message that did not exist
W1088	Presenting a deleted message that did not exist
W1089	Recovering a live message with incorrect content
W1090	Recovering a live message with incorrect metadata
W1091	Recovering a non-allocated message with incorrect content
W1092	Recovering a non-allocated message with incorrect metadata
W1093	Presenting a deleted message as live
W1094	Attributing a message to the incorrect sender
W1095	Attributing a message to the incorrect thread
W1096	Failing to recover attachments for a live message
W1097	Failing to recover attachment for a non-allocated message
W1098	Assigning incorrect metadata to a message attachment
W1099	Assigning an attachment to an incorrect messages
W1100	Failure to display special effects or highlight within a message
W1101	Failure to recover message edits if available
W1102	Failure to display that a message had a previous state

For tool testing, it can help think about what needs to go into test datasets to ensure correct extraction

ACME Forensics Messenger App parser

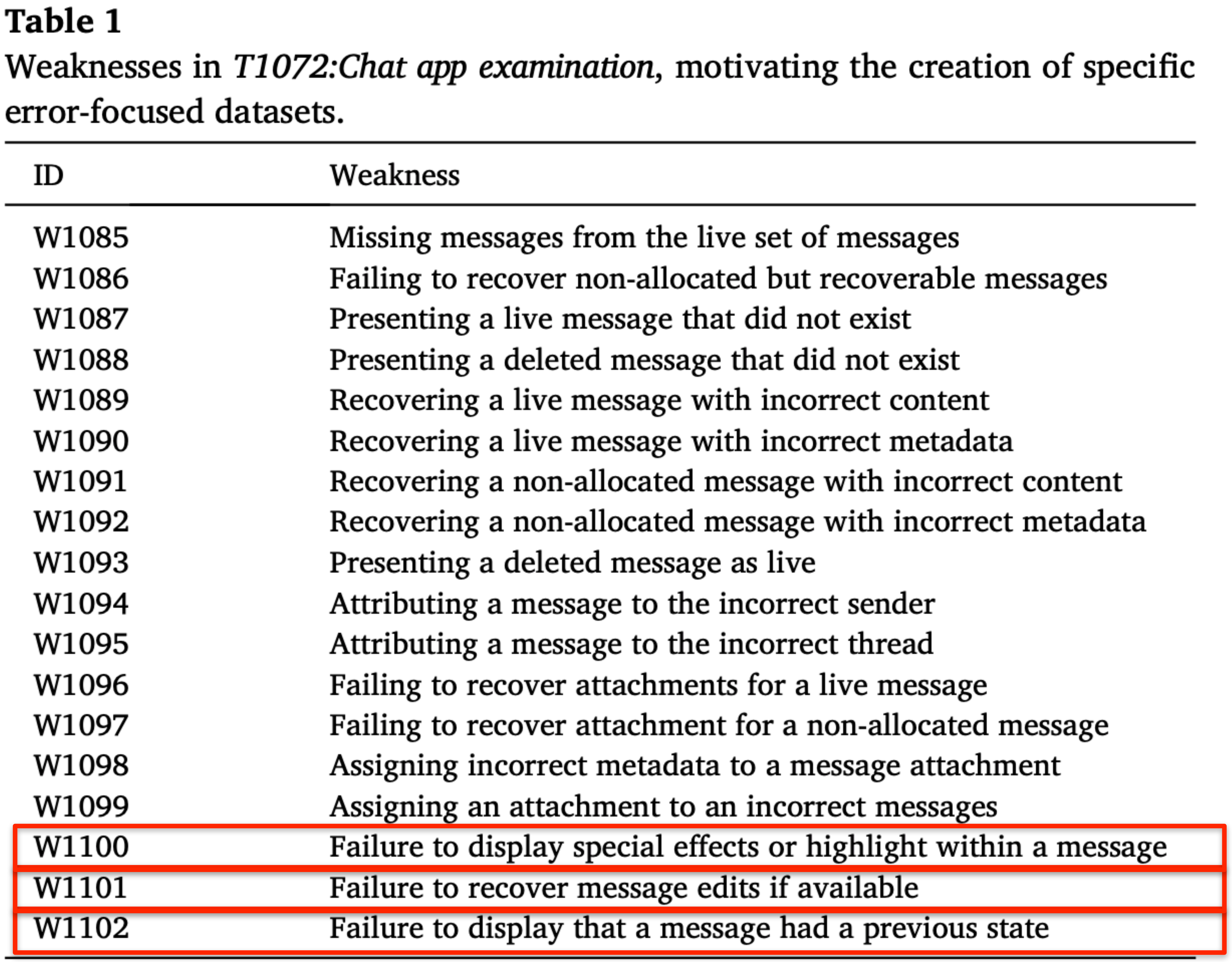
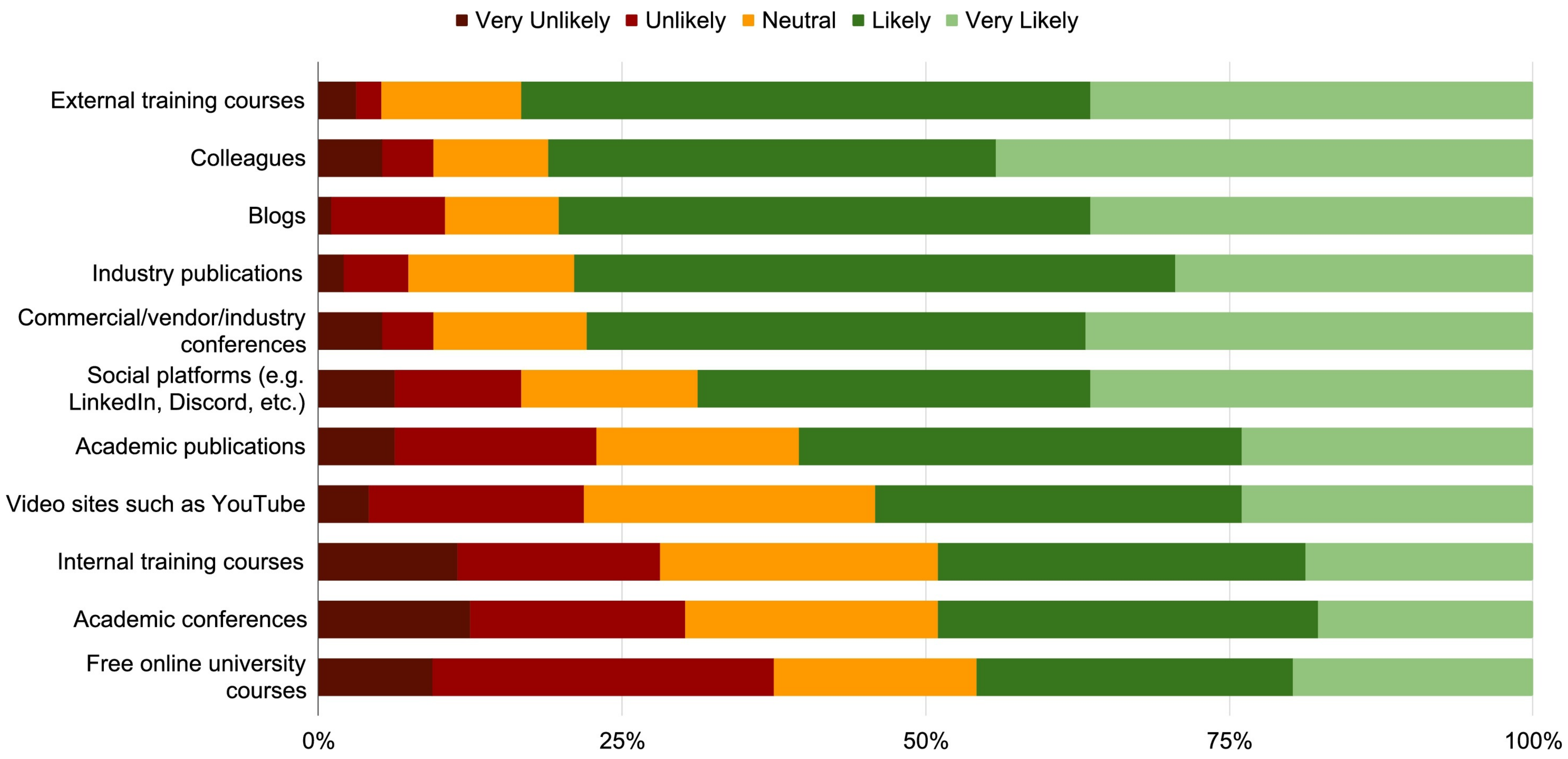


Table 1

Weaknesses in *T1072:Chat app examination*, motivating the creation of specific error-focused datasets.

ID	Weakness
W1085	Missing messages from the live set of messages
W1086	Failing to recover non-allocated but recoverable messages
W1087	Presenting a live message that did not exist
W1088	Presenting a deleted message that did not exist
W1089	Recovering a live message with incorrect content
W1090	Recovering a live message with incorrect metadata
W1091	Recovering a non-allocated message with incorrect content
W1092	Recovering a non-allocated message with incorrect metadata
W1093	Presenting a deleted message as live
W1094	Attributing a message to the incorrect sender
W1095	Attributing a message to the incorrect thread
W1096	Failing to recover attachments for a live message
W1097	Failing to recover attachment for a non-allocated message
W1098	Assigning incorrect metadata to a message attachment
W1099	Assigning an attachment to an incorrect messages
W1100	Failure to display special effects or highlight within a message
W1101	Failure to recover message edits if available
W1102	Failure to display that a message had a previous state

Applications: Highlighting mitigations for specific weaknesses



Hargreaves, C., Breitinger, F., Dowthwaite, L., Webb, H. and Scanlon, M., 2024. DFPulse: The 2024 digital forensic practitioner survey. *Forensic Science International: Digital Investigation*, *51*, p.301844.

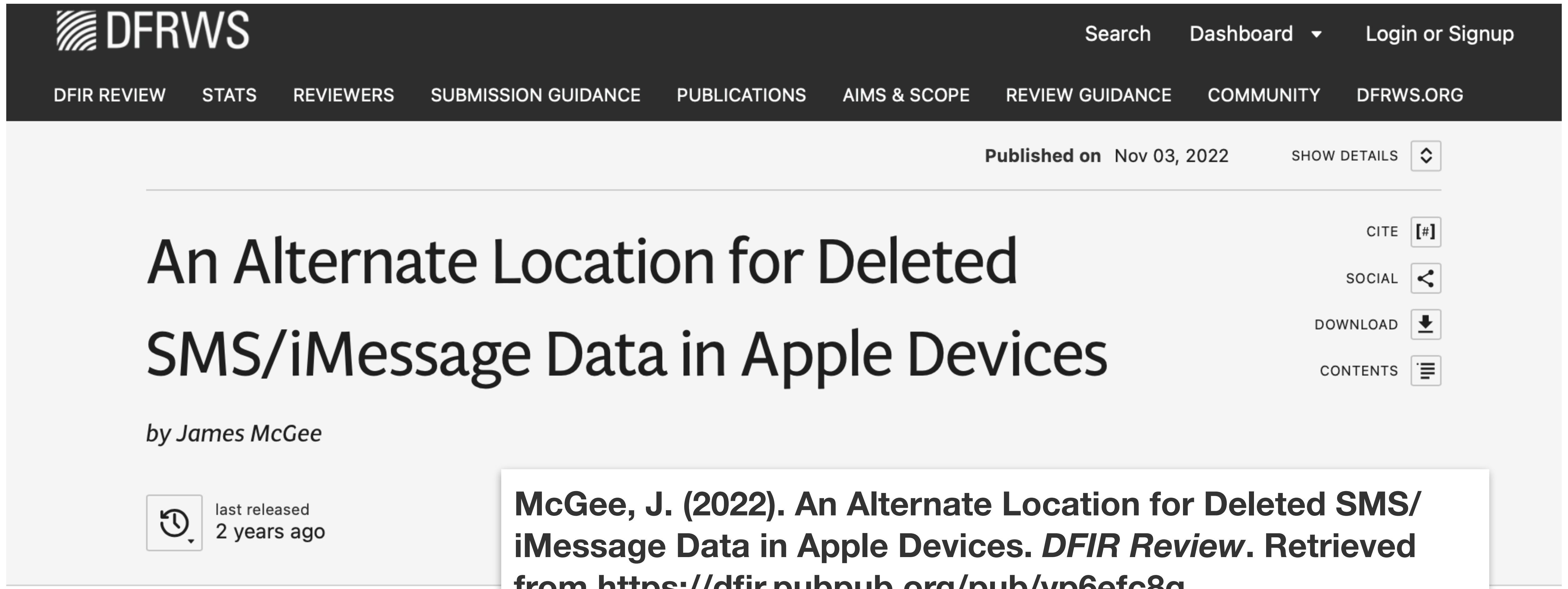
- Visibility of academic work to practitioners is quite poor
- Techniques in SOLVE-IT *should* be more accessible (?)
- Techniques then provide a listing of possible problems with a technique (weaknesses), which *should* be of interest (?)
- … and then mitigations are provided (which may be other techniques)
- This could provide an **accessible index into academic work**, indexed based on tangible, understandable techniques and processes.

Applications: Highlighting mitigations for specific weaknesses

T1072: Chat app examination

W1086: Failing to recover non-allocated but recoverable messages

M1077: Ensure potential secondary locations for stored message content are reviewed



Published on Nov 03, 2022

An Alternate Location for Deleted SMS/iMessage Data in Apple Devices

by James McGee

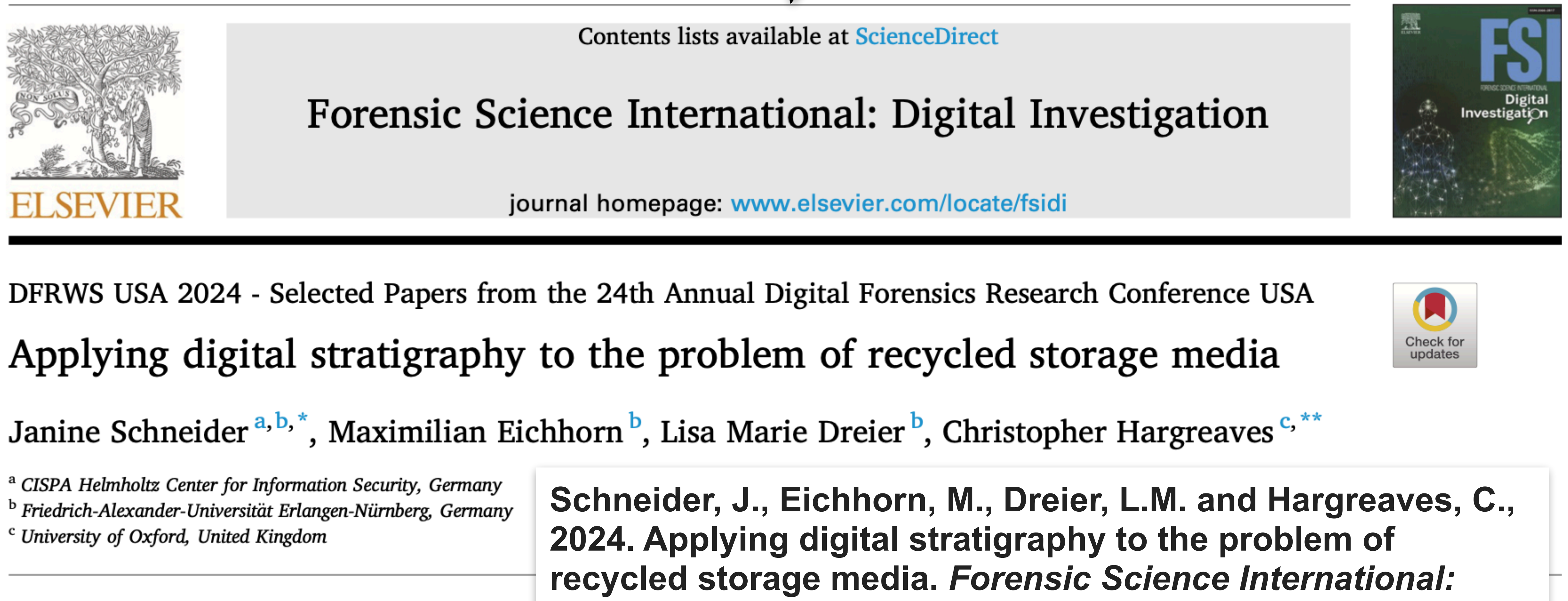
last released
2 years ago

McGee, J. (2022). An Alternate Location for Deleted SMS/iMessage Data in Apple Devices. *DFIR Review*. Retrieved from https://dfir.pubpub.org/pub/yp6efc8q

T1064: File carving

W1106: Incorrect attribution of salvaged content to a current file system rather than a previous one

M1061:Use digital stratigraphy to attempt to attribute data within a specific file system



Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS USA 2024 - Selected Papers from the 24th Annual Digital Forensics Research Conference USA

Applying digital stratigraphy to the problem of recycled storage media

Janine Schneider[a,b,*], Maximilian Eichhorn[b], Lisa Marie Dreier[b], Christopher Hargreaves[c,**]

[a] CISPA Helmholtz Center for Information Security, Germany
[b] Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
[c] University of Oxford, United Kingdom

Schneider, J., Eichhorn, M., Dreier, L.M. and Hargreaves, C., 2024. Applying digital stratigraphy to the problem of recycled storage media. *Forensic Science International: Digital Investigation*, *49*, p.301761.

Applications: Identifying weaknesses in an investigation, process or tool

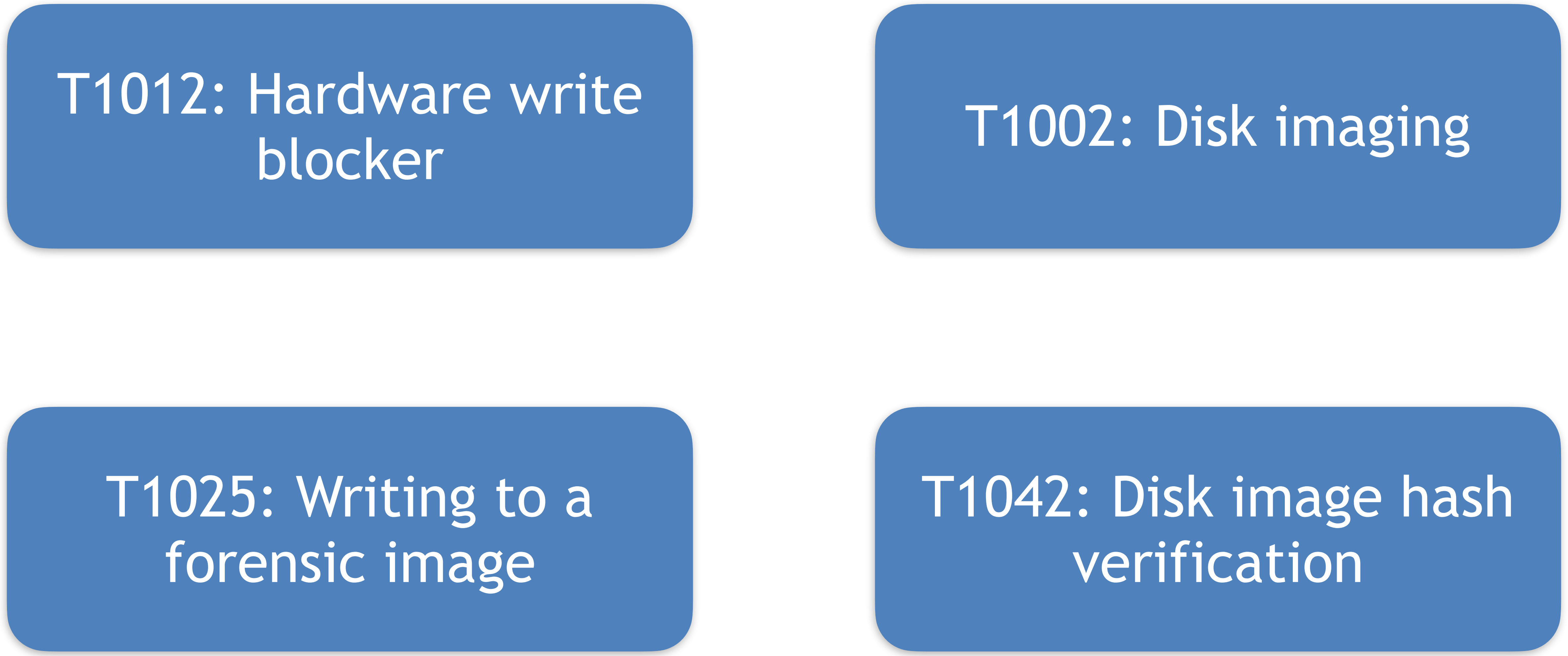
```
generate_case_evaluation.py Txxxx Txxxx Txxxx
```

A case

A Standard Operating Procedure (SOP)

A tool workflow

A forensic disk imaging example



T1012: Hardware write blocker

T1002: Disk imaging

T1025: Writing to a forensic image

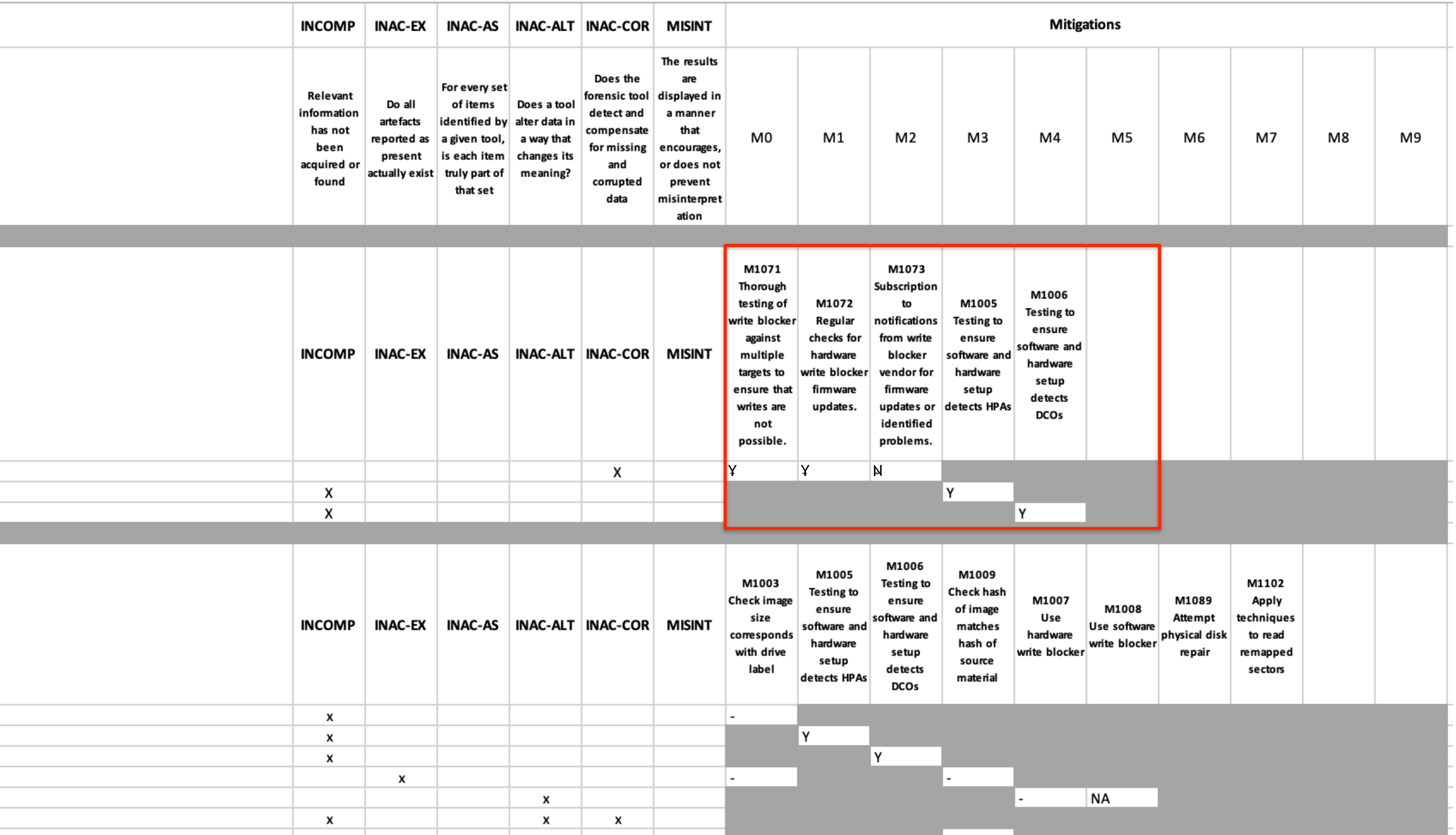
T1042: Disk image hash verification

- `generate_case_evaluation.py T1012 T1002 T1025 T1042`

	Potential Weaknesses	INCOMP	INAC-EX	INAC-AS	INAC-ALT	INAC-COR	MISINT	Mitigations									
		Relevant information has not been acquired or found	Do all artefacts reported as present actually exist	For every set of items identified by a given tool, is each item truly part of that set	Does a tool alter data in a way that changes its meaning?	Does the forensic tool detect and compensate for missing and corrupted data	The results are displayed in a manner that encourages, or does not prevent misinterpretation	M0	M1	M2	M3	M4	M5	M6	M7	M8	M9
T1012: Hardware write blockers	T1012: Hardware write blocker Potential Weaknesses	INCOMP	INAC-EX	INAC-AS	INAC-ALT	INAC-COR	MISINT	M1071 Thorough testing of write blocker against multiple targets to ensure that writes are not possible.	M1072 Regular checks for hardware write blocker firmware updates.	M1073 Subscription to notifications from write blocker vendor for firmware updates or identified problems.	M1005 Testing to ensure software and hardware setup detects HPAs	M1006 Testing to ensure software and hardware setup detects DCOs					
W1118	Hardware write blocker fails to prevent modifications to the attached device.					X		-	-	-							
W1119	Hardware write blocker hides the existence of an HPA.	X									Y						
W1120	Hardware write blocker hides the existence of an DCO.	X										Y					
T1002: Disk imaging	T1002: Disk imaging Potential Weaknesses	INCOMP	INAC-EX	INAC-AS	INAC-ALT	INAC-COR	MISINT	M1003 Check image size corresponds with drive label	M1005 Testing to ensure software and hardware setup detects HPAs	M1006 Testing to ensure software and hardware setup detects DCOs	M1009 Check hash of image matches hash of source material	M1007 Use hardware write blocker	M1008 Use software write blocker	M1089 Attempt physical disk repair	M1102 Apply techniques to read remapped sectors		
W1004	Acquisition does not include all sectors from LBA0 to LBA max	x						-									
W1006	Acquistion does not include data in HPA	x							Y								
W1007	Acquistion does not include data in DCO	x								Y							
W1013	Acquisition includes extra bytes		x					-			-						
W1014	Imaging process changes original data				x							-	NA				
W1015	Powering on SSD results in sectors being wiped by TRIM operation	x			x	x											
W1016	Data copied from sectors on source are stored incorrectly				x	x					-						
W1136	Not recovering data from a failed hard drive	x												-			
W1143	Acquisition method does not read remapped sectors e.g. G-Lists	x													-		
T1025: Writing data to a forensic image format	T1025: Writing to a forensic image	INCOMP	INAC-EX	INAC-AS	INAC-ALT	INAC-COR	MISINT	M1009 Check hash of image matches hash of source material									
W1043	Data is written to forensic format that does not preserve the original raw data				X			-									
T1042: Disk image hash verification	T1042: Disk image hash verification Potential Weaknesses	INCOMP	INAC-EX	INAC-AS	INAC-ALT	INAC-COR	MISINT	M1021 Verify the disk image integrity with multiple hash algorithms e.g. MD5 and SHA1 (Kessler 2016)	M1022 Restrict access to stored disk images	M1023 Ensure and check logs of access to stored disk images	M1070 Ensure hash algorithm(s) used are resistant to collisions through data manipulation	M1075 Testing programme to validate hashes of data in images is calculated correctly	M1085 Use of multiple tools to verify disk image hash	M1076 Testing programme to validate hashes of metadata in images is calculated correctly	M1074 Validate image hash against one stored externally to the image in a trusted location.		
W1042	Disk image was tampered with, but manipulated to have a collision with original hash					x		-	-	-	-						
W1124	Failure to compute hash correctly: this could result in a message indicating corrupt evidence, thus stopping or delaying further investigation			X								-	-				
W1125	Failure to validate hash properly: this could allow errors from earlier to propagate e.g. incorrect sectors					X						-	-				

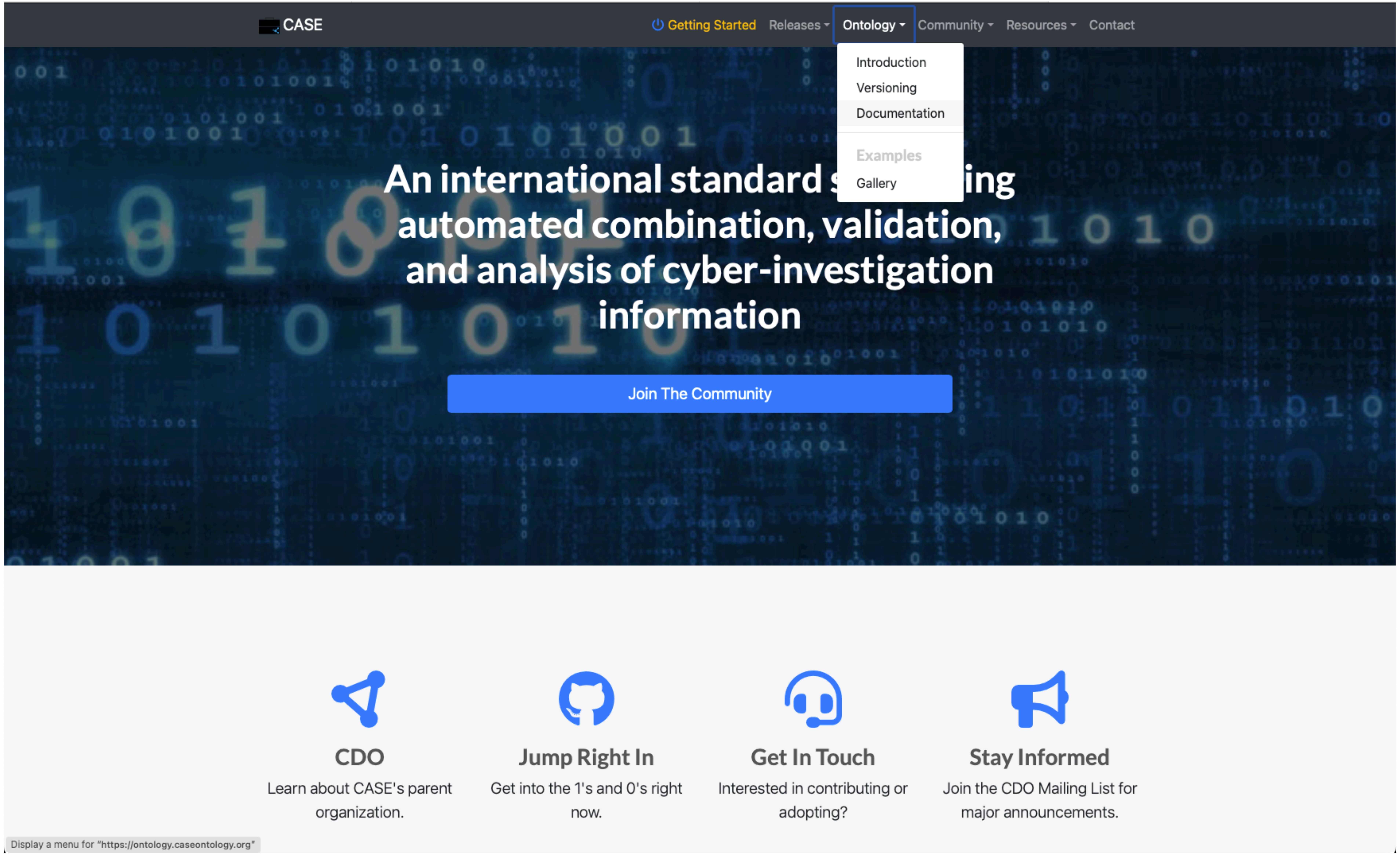
	Potential Weaknesses	INCOMP	INAC-EX	INAC-AS	INAC-ALT	INAC-COR	MISINT	Mitigations									
		Relevant information has not been acquired or found	Do all artefacts reported as present actually exist	For every set of items identified by a given tool, is each item truly part of that set	Does a tool alter data in a way that changes its meaning?	Does the forensic tool detect and compensate for missing and corrupted data	The results are displayed in a manner that encourages, or does not prevent misinterpretation	M0	M1	M2	M3	M4	M5	M6	M7	M8	M9
T1012: Hardware write blockers	**Potential Weaknesses**	**INCOMP**	**INAC-EX**	**INAC-AS**	**INAC-ALT**	**INAC-COR**	**MISINT**	**M1071 Thorough testing of write blocker against multiple targets to ensure that writes are not possible.**	**M1072 Regular checks for hardware write blocker firmware updates.**	**M1073 Subscription to notifications from write blocker vendor for firmware updates or identified problems.**	**M1005 Testing to ensure software and hardware setup detects HPAs**	**M1006 Testing to ensure software and hardware setup detects DCOs**					
W1118	Hardware write blocker fails to prevent modifications to the attached device.					X		-	-	-							
W1119	Hardware write blocker hides the existence of an HPA.	X									Y						
W1120	Hardware write blocker hides the existence of an DCO.	X										Y					
T1002: Disk imaging	**Potential Weaknesses**	**INCOMP**	**INAC-EX**	**INAC-AS**	**INAC-ALT**	**INAC-COR**	**MISINT**	**M1003 Check image size corresponds with drive label**	**M1005 Testing to ensure software and hardware setup detects HPAs**	**M1006 Testing to ensure software and hardware setup detects DCOs**	**M1009 Check hash of image matches hash of source material**	**M1007 Use hardware write blocker**	**M1008 Use software write blocker**	**M1089 Attempt physical disk repair**	**M1102 Apply techniques to read remapped sectors**		
W1004	Acquisition does not include all sectors from LBA0 to LBA max	x						-									
W1006	Acquistion does not include data in HPA	x							Y								
W1007	Acquistion does not include data in DCO	x								Y							
W1013	Acquisition includes extra bytes		x					-			-						
W1014	Imaging process changes original data				x							-	NA				
W1015	Powering on SSD results in sectors being wiped by TRIM operation	x			x	x											
W1016	Data copied from sectors on source are stored incorrectly				x	x					-						
W1136	Not recovering data from a failed hard drive	x												-			
W1143	Acquisition method does not read remapped sectors e.g. G-Lists	x													-		
T1025: Writing data to a forensic image format	**Potential Weaknesses**	**INCOMP**	**INAC-EX**	**INAC-AS**	**INAC-ALT**	**INAC-COR**	**MISINT**	**M1009 Check hash of image matches hash of source material**									
W1043	Data is written to forensic format that does not preserve the original raw data				X			-									
T1042: Disk image hash verification	**Potential Weaknesses**	**INCOMP**	**INAC-EX**	**INAC-AS**	**INAC-ALT**	**INAC-COR**	**MISINT**	**M1021 Verify the disk image integrity with multiple hash algorithms e.g. MD5 and SHA1 (Kessler 2016)**	**M1022 Restrict access to stored disk images**	**M1023 Ensure and check logs of access to stored disk images**	**M1070 Ensure hash algorithm(s) used are resistant to collisions through data manipulation**	**M1075 Testing programme to validate hashes of data in images is calculated correctly**	**M1085 Use of multiple tools to verify disk image hash**	**M1076 Testing programme to validate hashes of metadata in images is calculated correctly**	**M1074 Validate image hash against one stored externally to the image in a trusted location.**		
W1042	Disk image was tampered with, but manipulated to have a collision with original hash					x		-	-	-	-						
W1124	Failure to compute hash correctly: this could result in a message indicating corrupt evidence, thus stopping or delaying further investigation			X								-	-				
W1125	Failure to validate hash properly: this could allow errors from earlier to propagate e.g. incorrect sectors					X						-	-				

	Potential Weaknesses	INCOMP	INAC-EX	INAC-AS	IN
		Relevant information has not been acquired or found	Do all artefacts reported as present actually exist	For every set of items identified by a given tool, is each item truly part of that set	Do alte a cha m
T1012: Hardware write blockers	**Potential Weaknesses**	**INCOMP**	**INAC-EX**	**INAC-AS**	**IN**
W1118	Hardware write blocker fails to prevent modifications to the attached device.				
W1119	Hardware write blocker hides the existence of an HPA.	X			
W1120	Hardware write blocker hides the existence of an DCO.	X			
T1002: Disk imaging	**Potential Weaknesses**	**INCOMP**	**INAC-EX**	**INAC-AS**	**IN**
W1004	Acquisition does not include all sectors from LBA0 to LBA max	x			
W1006	Acquistion does not include data in HPA	x			
W1007	Acquistion does not include data in DCO	x			
W1013	Acquisition includes extra bytes		x		
W1014	Imaging process changes original data				
W1015	Powering on SSD results in sectors being wiped by TRIM operation	x			



	INCOMP	INAC-EX	INAC-AS	INAC-ALT	INAC-COR	MISINT	Mitigations									
	Relevant information has not been acquired or found	Do all artefacts reported as present actually exist	For every set of items identified by a given tool, is each item truly part of that set	Does a tool alter data in a way that changes its meaning?	Does the forensic tool detect and compensate for missing and corrupted data	The results are displayed in a manner that encourages, or does not prevent misinterpretation	M0	M1	M2	M3	M4	M5	M6	M7	M8	M9
	INCOMP	INAC-EX	INAC-AS	INAC-ALT	INAC-COR	MISINT	M1071 Thorough testing of write blocker against multiple targets to ensure that writes are not possible.	M1072 Regular checks for hardware write blocker firmware updates.	M1073 Subscription to notifications from write blocker vendor for firmware updates or identified problems.	M1005 Testing to ensure software and hardware setup detects HPAs	M1006 Testing to ensure software and hardware setup detects DCOs					
					X		Y	Y	N							
	X									Y						
	X										Y					
	INCOMP	INAC-EX	INAC-AS	INAC-ALT	INAC-COR	MISINT	M1003 Check image size corresponds with drive label	M1005 Testing to ensure software and hardware setup detects HPAs	M1006 Testing to ensure software and hardware setup detects DCOs	M1009 Check hash of image matches hash of source material	M1007 Use hardware write blocker	M1008 Use software write blocker	M1089 Attempt physical disk repair	M1102 Apply techniques to read remapped sectors		
	x						-									
	x							Y								
	x								Y							
		x					-			-						
				x							-	NA				
	x			x	x											

Applications: Interfacing with CASE



An international standard s ing automated combination, validation, and analysis of cyber-investigation information

CDO

Learn about CASE's parent organization.

Jump Right In

Get into the 1's and 0's right now.

Get In Touch

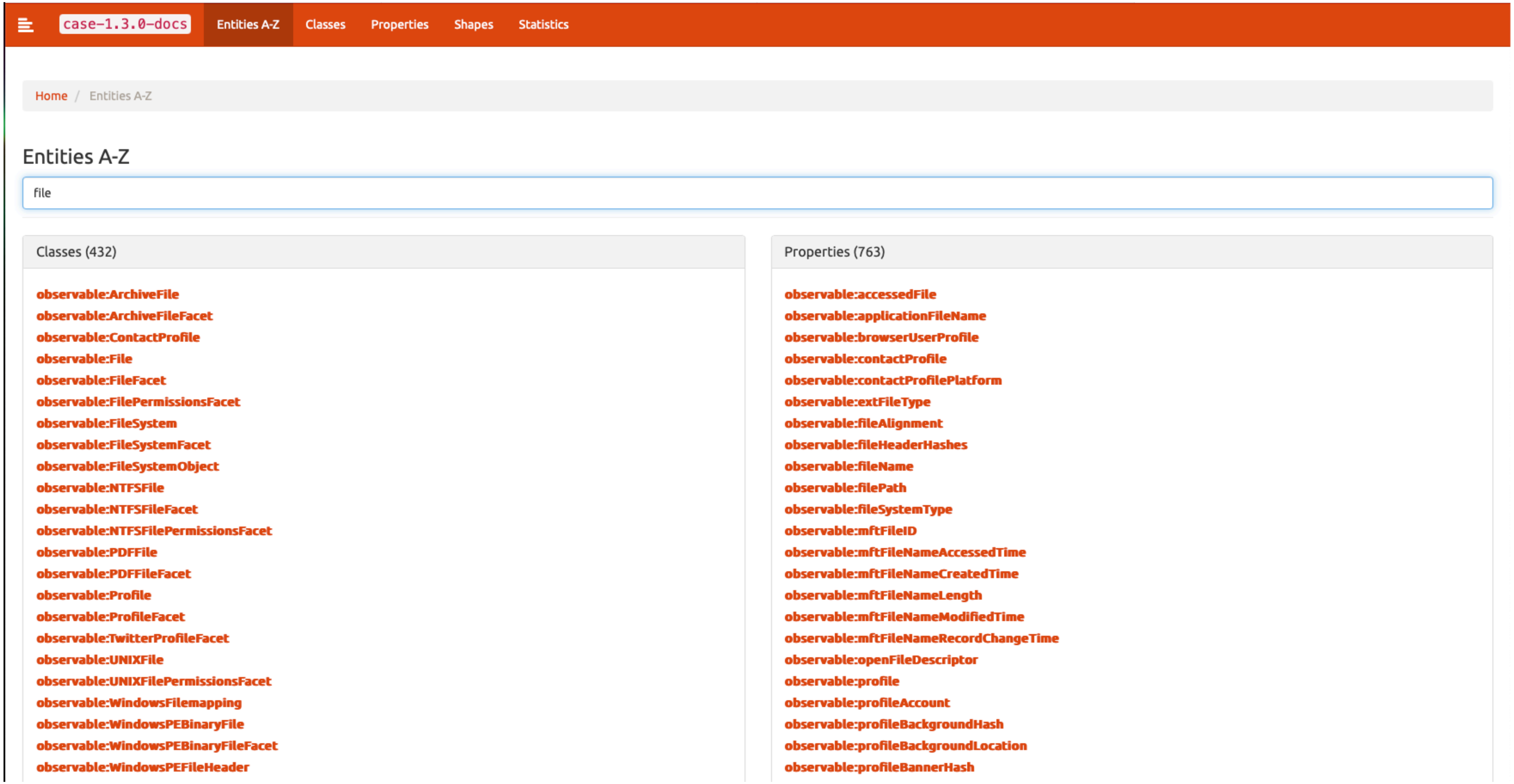
Interested in contributing or adopting?

Stay Informed

Join the CDO Mailing List for major announcements.

https://caseontology.org/

Applications: Interfacing with CASE



Entities A-Z

file

Classes (432)

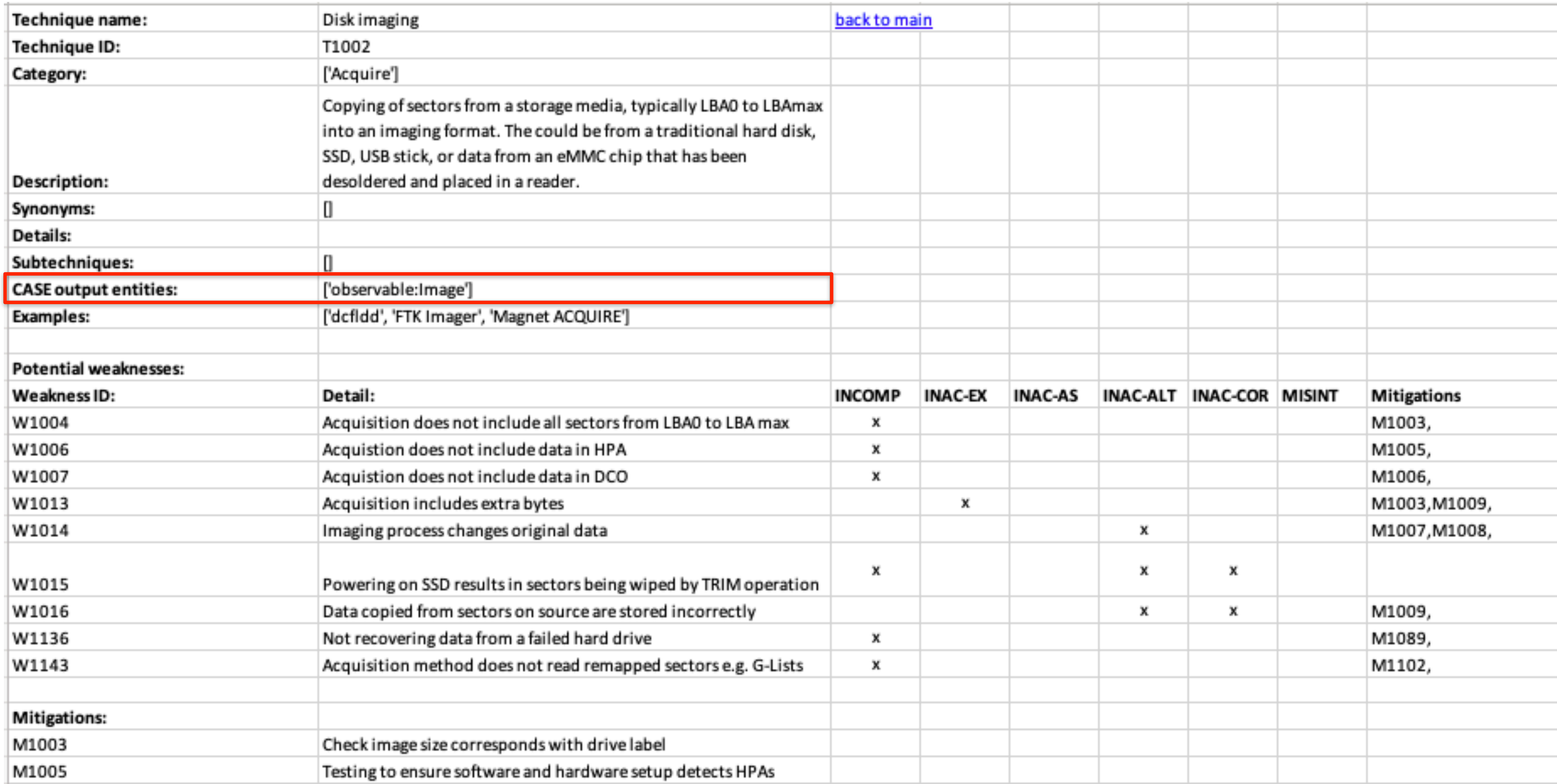
observable:ArchiveFile
observable:ArchiveFileFacet
observable:ContactProfile
observable:File
observable:FileFacet
observable:FilePermissionsFacet
observable:FileSystem
observable:FileSystemFacet
observable:FileSystemObject
observable:NTFSFile
observable:NTFSFileFacet
observable:NTFSFilePermissionsFacet
observable:PDFFile
observable:PDFFileFacet
observable:Profile
observable:ProfileFacet
observable:TwitterProfileFacet
observable:UNIXFile
observable:UNIXFilePermissionsFacet
observable:WindowsFilemapping
observable:WindowsPEBinaryFile
observable:WindowsPEBinaryFileFacet
observable:WindowsPEFileHeader

Properties (763)

observable:accessedFile
observable:applicationFileName
observable:browserUserProfile
observable:contactProfile
observable:contactProfilePlatform
observable:extFileType
observable:fileAlignment
observable:fileHeaderHashes
observable:fileName
observable:filePath
observable:fileSystemType
observable:mftFileID
observable:mftFileNameAccessedTime
observable:mftFileNameCreatedTime
observable:mftFileNameLength
observable:mftFileNameModifiedTime
observable:mftFileNameRecordChangeTime
observable:openFileDescriptor
observable:profile
observable:profileAccount
observable:profileBackgroundHash
observable:profileBackgroundLocation
observable:profileBannerHash

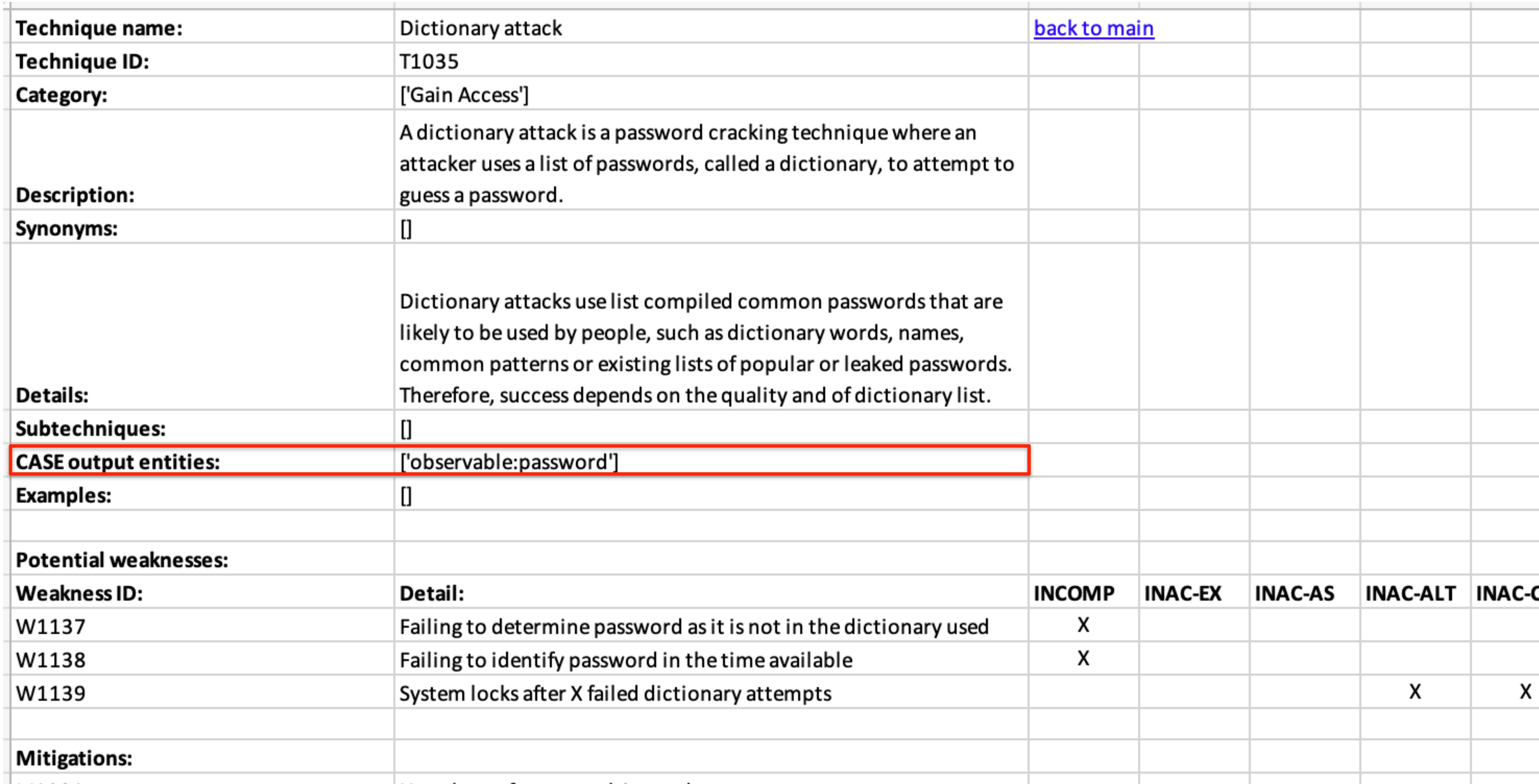
https://ontology.caseontology.org/documentation/entities-az.html

Applications: Interfacing with CASE



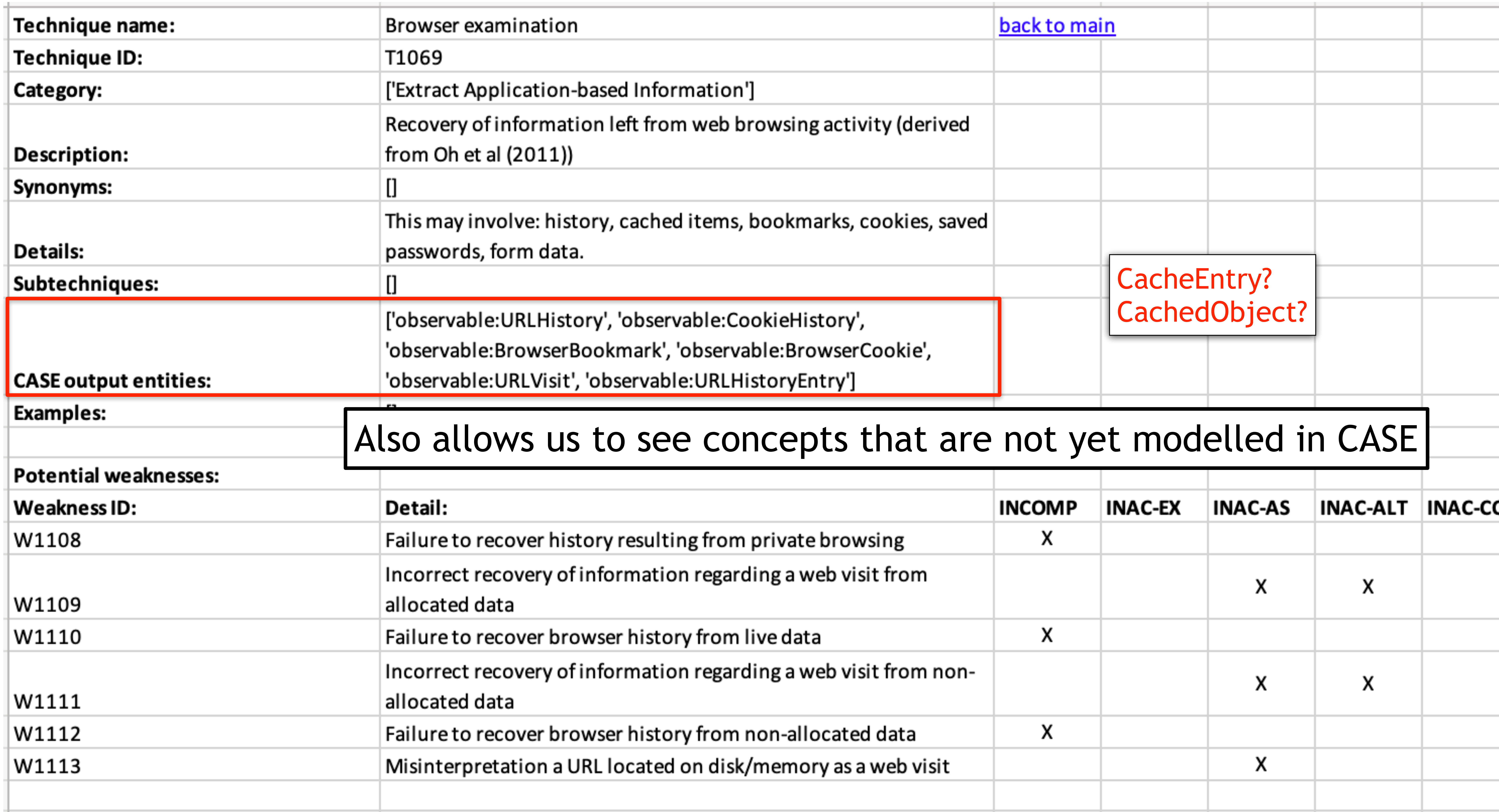
Technique name:	Disk imaging	back to main						
Technique ID:	T1002							
Category:	['Acquire']							
Description:	Copying of sectors from a storage media, typically LBA0 to LBAmax into an imaging format. The could be from a traditional hard disk, SSD, USB stick, or data from an eMMC chip that has been desoldered and placed in a reader.							
Synonyms:	[]							
Details:								
Subtechniques:	[]							
CASE output entities:	['observable:Image']							
Examples:	['dcfldd', 'FTK Imager', 'Magnet ACQUIRE']							
Potential weaknesses:								
Weakness ID:	**Detail:**	**INCOMP**	**INAC-EX**	**INAC-AS**	**INAC-ALT**	**INAC-COR**	**MISINT**	**Mitigations**
W1004	Acquisition does not include all sectors from LBA0 to LBA max	x						M1003,
W1006	Acquistion does not include data in HPA	x						M1005,
W1007	Acquistion does not include data in DCO	x						M1006,
W1013	Acquisition includes extra bytes		x					M1003,M1009,
W1014	Imaging process changes original data				x			M1007,M1008,
W1015	Powering on SSD results in sectors being wiped by TRIM operation	x			x	x		
W1016	Data copied from sectors on source are stored incorrectly				x	x		M1009,
W1136	Not recovering data from a failed hard drive	x						M1089,
W1143	Acquisition method does not read remapped sectors e.g. G-Lists	x						M1102,
Mitigations:								
M1003	Check image size corresponds with drive label							
M1005	Testing to ensure software and hardware setup detects HPAs							

Applications: Interfacing with CASE



Technique name:	Dictionary attack	back to main				
Technique ID:	T1035					
Category:	['Gain Access']					
Description:	A dictionary attack is a password cracking technique where an attacker uses a list of passwords, called a dictionary, to attempt to guess a password.					
Synonyms:	[]					
Details:	Dictionary attacks use list compiled common passwords that are likely to be used by people, such as dictionary words, names, common patterns or existing lists of popular or leaked passwords. Therefore, success depends on the quality and of dictionary list.					
Subtechniques:	[]					
CASE output entities:	['observable:password']					
Examples:	[]					
Potential weaknesses:						
Weakness ID:	**Detail:**	**INCOMP**	**INAC-EX**	**INAC-AS**	**INAC-ALT**	**INAC-C**
W1137	Failing to determine password as it is not in the dictionary used	X				
W1138	Failing to identify password in the time available	X				
W1139	System locks after X failed dictionary attempts				X	X
Mitigations:						

Applications: Interfacing with CASE



Technique name:	Browser examination	back to main				
Technique ID:	T1069					
Category:	['Extract Application-based Information']					
Description:	Recovery of information left from web browsing activity (derived from Oh et al (2011))					
Synonyms:	[]					
Details:	This may involve: history, cached items, bookmarks, cookies, saved passwords, form data.					
Subtechniques:	[]					
CASE output entities:	['observable:URLHistory', 'observable:CookieHistory', 'observable:BrowserBookmark', 'observable:BrowserCookie', 'observable:URLVisit', 'observable:URLHistoryEntry']					
Examples:	[]					
Potential weaknesses:						
Weakness ID:	**Detail:**	**INCOMP**	**INAC-EX**	**INAC-AS**	**INAC-ALT**	**INAC-CC**
W1108	Failure to recover history resulting from private browsing	X				
W1109	Incorrect recovery of information regarding a web visit from allocated data			X	X	
W1110	Failure to recover browser history from live data	X				
W1111	Incorrect recovery of information regarding a web visit from non-allocated data			X	X	
W1112	Failure to recover browser history from non-allocated data	X				
W1113	Misinterpretation a URL located on disk/memory as a web visit			X		

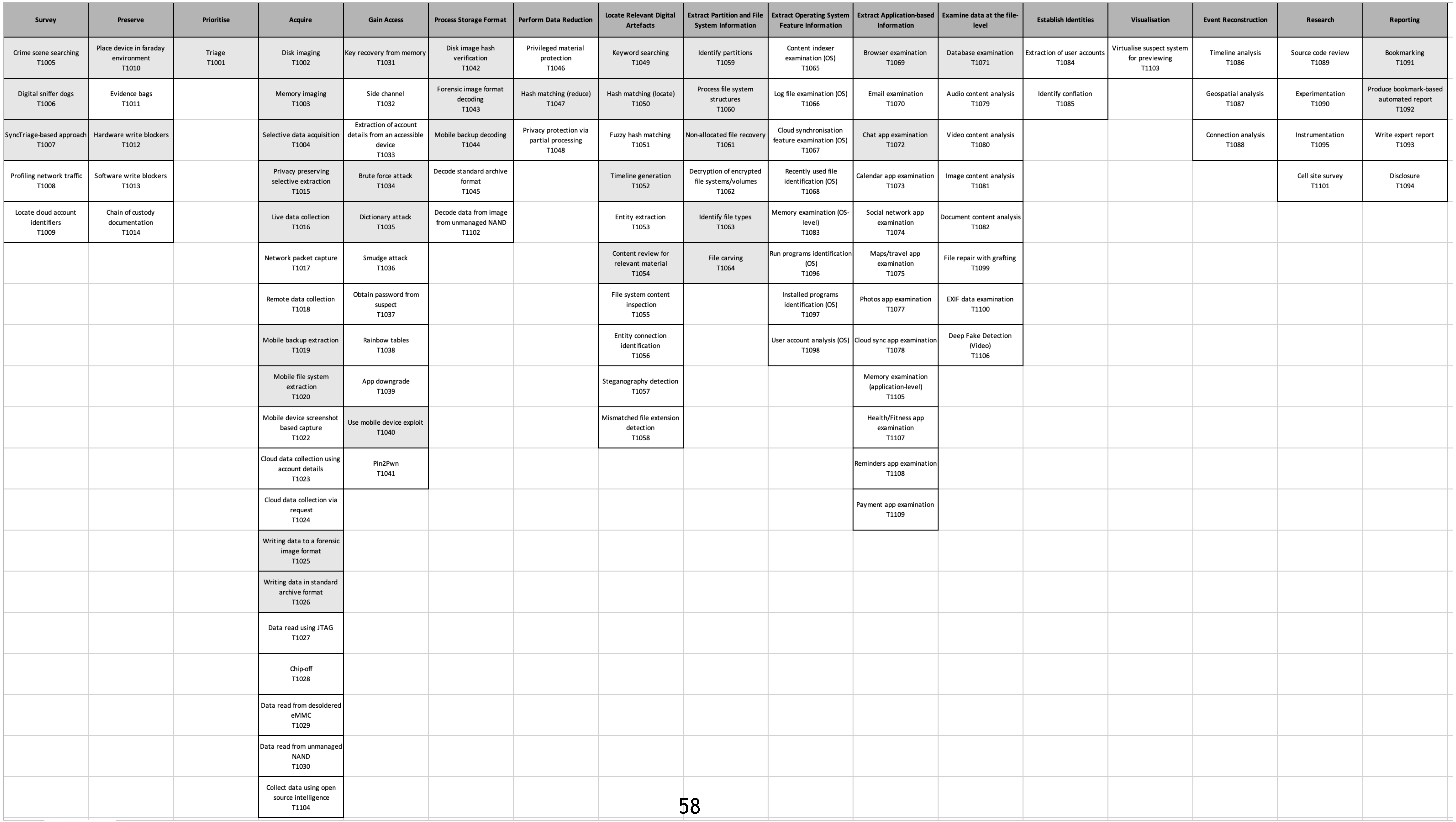
CacheEntry?
CachedObject?

Also allows us to see concepts that are not yet modelled in CASE

Applications: Structured consideration of AI applications

Obligatory AI generated image

Applications: Structured consideration of AI applications



Survey	Preserve	Prioritise	Acquire	Gain Access	Process Storage Format	Perform Data Reduction	Locate Relevant Digital Artefacts	Extract Partition and File System Information	Extract Operating System Feature Information	Extract Application-based Information	Examine data at the file-level	Establish Identities	Visualisation	Event Reconstruction	Research	Reporting
Crime scene searching T1005	Place device in faraday environment T1010	Triage T1001	Disk imaging T1002	Key recovery from memory T1031	Disk image hash verification T1042	Privileged material protection T1046	Keyword searching T1049	Identify partitions T1059	Content indexer examination (OS) T1065	Browser examination T1069	Database examination T1071	Extraction of user accounts T1084	Virtualise suspect system for previewing T1103	Timeline analysis T1086	Source code review T1089	Bookmarking T1091
Digital sniffer dogs T1006	Evidence bags T1011		Memory imaging T1003	Side channel T1032	Forensic image format decoding T1043	Hash matching (reduce) T1047	Hash matching (locate) T1050	Process file system structures T1060	Log file examination (OS) T1066	Email examination T1070	Audio content analysis T1079	Identify conflation T1085		Geospatial analysis T1087	Experimentation T1090	Produce bookmark-based automated report T1092
SyncTriage-based approach T1007	Hardware write blockers T1012		Selective data acquisition T1004	Extraction of account details from an accessible device T1033	Mobile backup decoding T1044	Privacy protection via partial processing T1048	Fuzzy hash matching T1051	Non-allocated file recovery T1061	Cloud synchronisation feature examination (OS) T1067	Chat app examination T1072	Video content analysis T1080			Connection analysis T1088	Instrumentation T1095	Write expert report T1093
Profiling network traffic T1008	Software write blockers T1013		Privacy preserving selective extraction T1015	Brute force attack T1034	Decode standard archive format T1045		Timeline generation T1052	Decryption of encrypted file systems/volumes T1062	Recently used file identification (OS) T1068	Calendar app examination T1073	Image content analysis T1081				Cell site survey T1101	Disclosure T1094
Locate cloud account identifiers T1009	Chain of custody documentation T1014		Live data collection T1016	Dictionary attack T1035	Decode data from image from unmanaged NAND T1102		Entity extraction T1053	Identify file types T1063	Memory examination (OS-level) T1083	Social network app examination T1074	Document content analysis T1082					
			Network packet capture T1017	Smudge attack T1036			Content review for relevant material T1054	File carving T1064	Run programs identification (OS) T1096	Maps/travel app examination T1075	File repair with grafting T1099					
			Remote data collection T1018	Obtain password from suspect T1037			File system content inspection T1055		Installed programs identification (OS) T1097	Photos app examination T1077	EXIF data examination T1100					
			Mobile backup extraction T1019	Rainbow tables T1038			Entity connection identification T1056		User account analysis (OS) T1098	Cloud sync app examination T1078	Deep Fake Detection (Video) T1106					
			Mobile file system extraction T1020	App downgrade T1039			Steganography detection T1057			Memory examination (application-level) T1105						
			Mobile device screenshot based capture T1022	Use mobile device exploit T1040			Mismatched file extension detection T1058			Health/Fitness app examination T1107						
			Cloud data collection using account details T1023	Pin2Pwn T1041						Reminders app examination T1108						
			Cloud data collection via request T1024							Payment app examination T1109						
			Writing data to a forensic image format T1025													
			Writing data in standard archive format T1026													
			Data read using JTAG T1027													
			Chip-off T1028													
			Data read from desoldered eMMC T1029													
			Data read from unmanaged NAND T1030													
			Collect data using open source intelligence T1104													

Applications: Structured consideration of AI applications

We can create a corresponding specific set of categories:

In tools

In academic work
(with implementation)

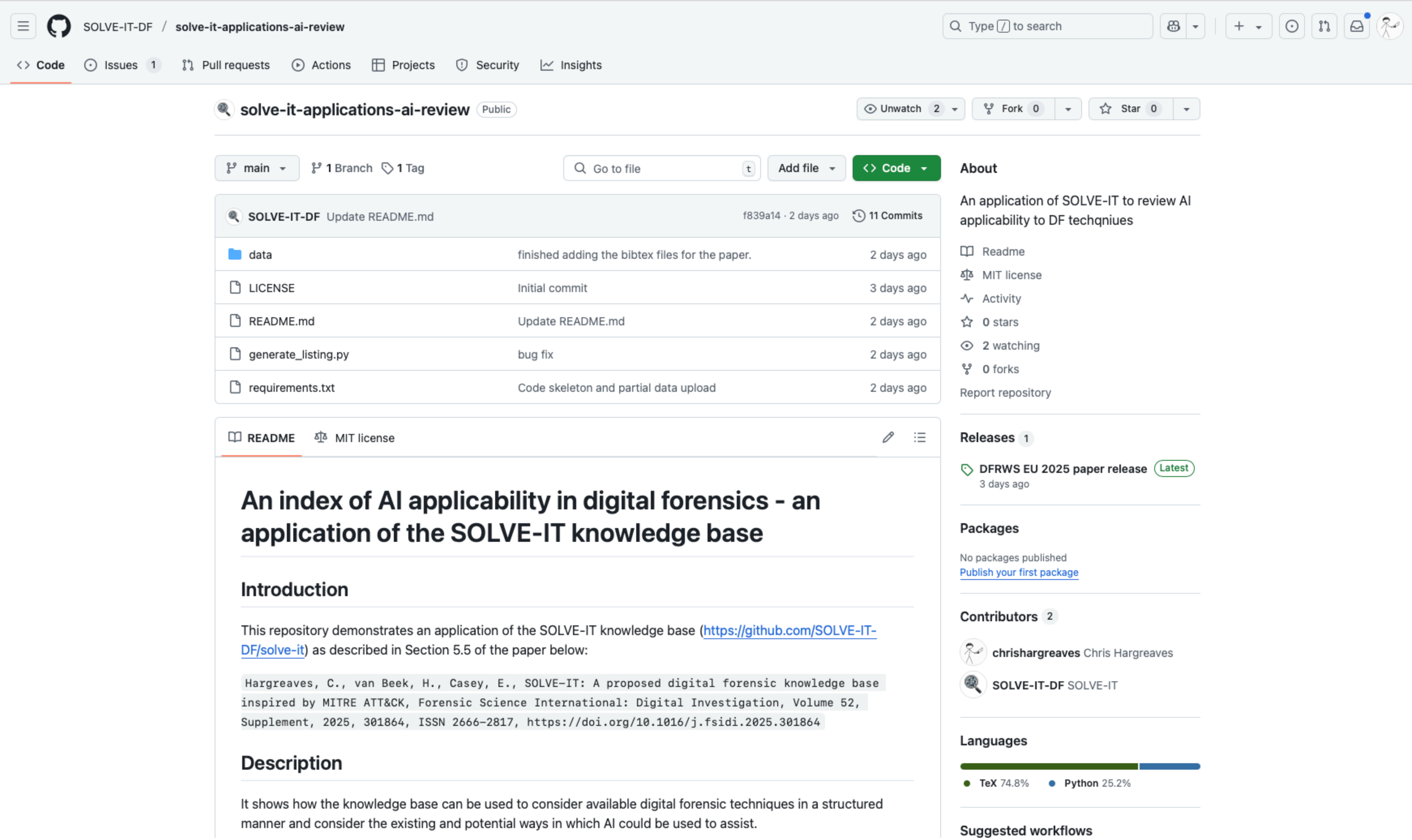
In academic work
(as an idea)

Some application can be envisaged

Non AI-based process likely sufficient

Unclassified

Applications: Structured consideration of AI applications



SOLVE-IT-DF Update README.md	f839a14 · 2 days ago	11 Commits
data	finished adding the bibtex files for the paper.	2 days ago
LICENSE	Initial commit	3 days ago
README.md	Update README.md	2 days ago
generate_listing.py	bug fix	2 days ago
requirements.txt	Code skeleton and partial data upload	2 days ago

An index of AI applicability in digital forensics - an application of the SOLVE-IT knowledge base

Introduction

This repository demonstrates an application of the SOLVE-IT knowledge base (https://github.com/SOLVE-IT-DF/solve-it) as described in Section 5.5 of the paper below:

```
Hargreaves, C., van Beek, H., Casey, E., SOLVE-IT: A proposed digital forensic knowledge base
inspired by MITRE ATT&CK, Forensic Science International: Digital Investigation, Volume 52,
Supplement, 2025, 301864, ISSN 2666-2817, https://doi.org/10.1016/j.fsidi.2025.301864
```

Description

It shows how the knowledge base can be used to consider available digital forensic techniques in a structured manner and consider the existing and potential ways in which AI could be used to assist.

About

An application of SOLVE-IT to review AI applicability to DF techqniues

Readme
MIT license
Activity
0 stars
2 watching
0 forks
Report repository

Releases 1

DFRWS EU 2025 paper release Latest
3 days ago

Packages

No packages published
Publish your first package

Contributors 2

chrishargreaves Chris Hargreaves
SOLVE-IT-DF SOLVE-IT

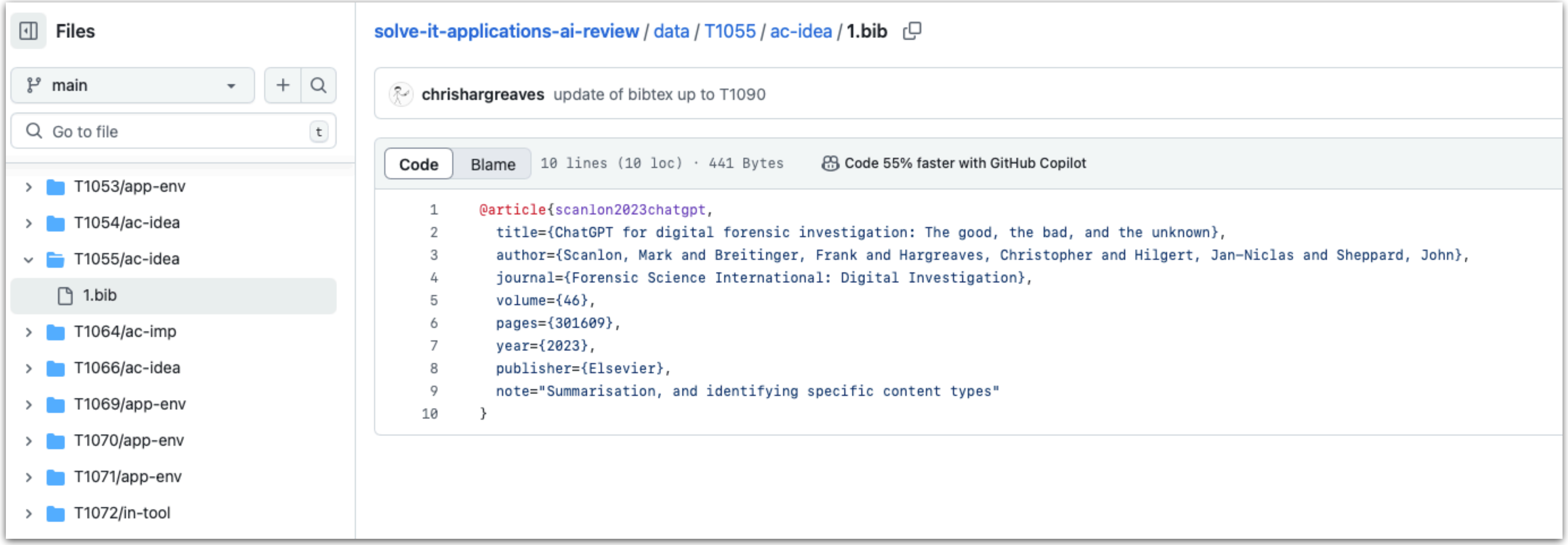
Languages

● TeX 74.8% ● Python 25.2%

Suggested workflows

https://github.com/SOLVE-IT-DF/solve-it-applications-ai-review

Applications: Structured consideration of AI applications



solve-it-applications-ai-review / data / T1055 / ac-idea / 1.bib

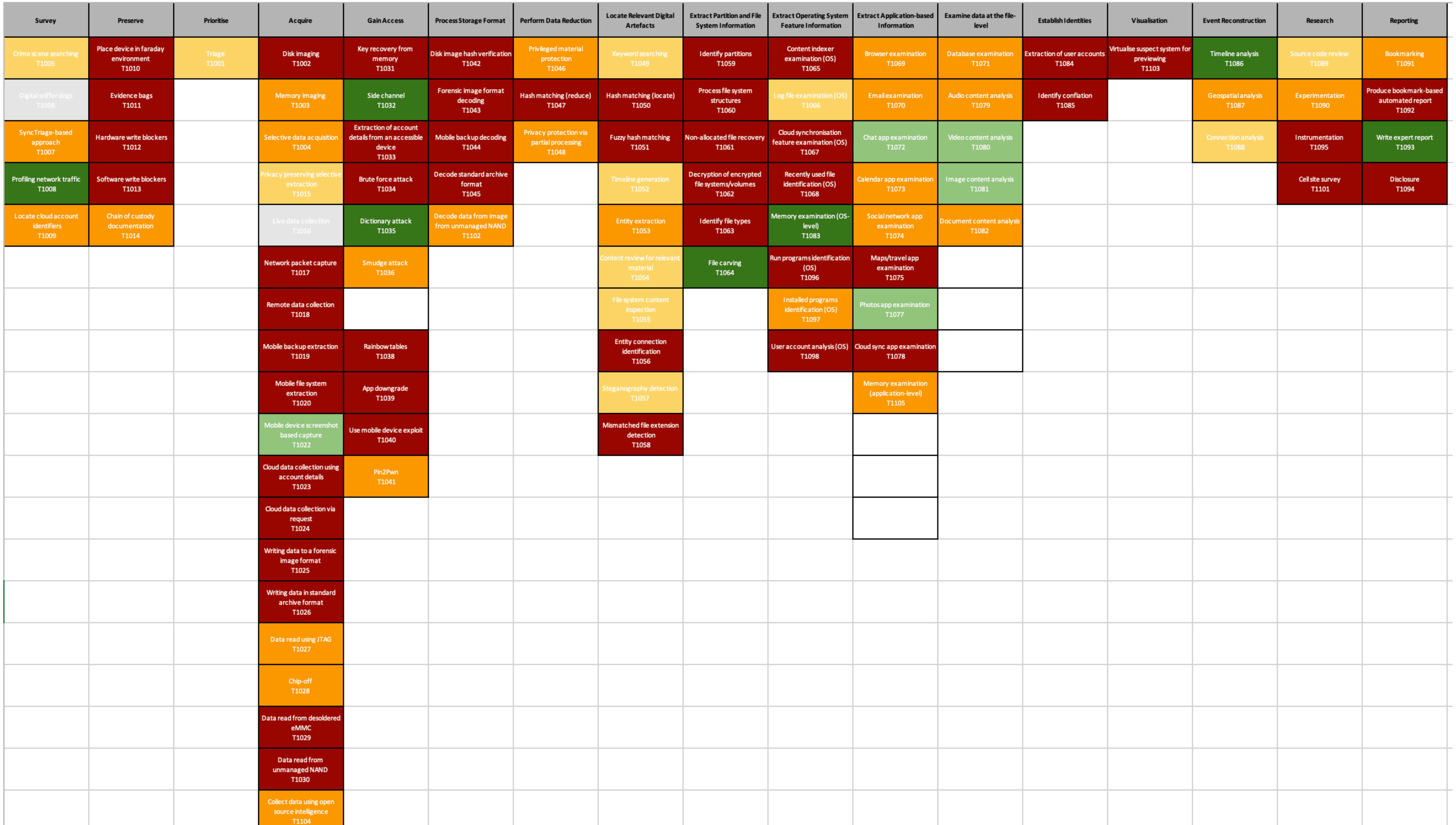
chrishargreaves update of bibtex up to T1090

```
@article{scanlon2023chatgpt,
  title={ChatGPT for digital forensic investigation: The good, the bad, and the unknown},
  author={Scanlon, Mark and Breitinger, Frank and Hargreaves, Christopher and Hilgert, Jan-Niclas and Sheppard, John},
  journal={Forensic Science International: Digital Investigation},
  volume={46},
  pages={301609},
  year={2023},
  publisher={Elsevier},
  note="Summarisation, and identifying specific content types"
}
```

"T1055: File system content inspection" contains '*ac-idea*'
represented in bibtex (with note field added)

https://github.com/SOLVE-IT-DF/solve-it-applications-ai-review

Applications: Structured consideration of AI applications



Survey	Preserve	Prioritise	Acquire	Gain Access	Process Storage Format	Perform Data Reduction	Locate Relevant Digital Artefacts	Extract Partition and File System Information	Extract Operating System Feature Information	Extract Application-based Information	Examine data at the file-level	Establish Identities	Visualisation	Event Reconstruction	Research	Reporting
Crime scene searching T1005	Place device in faraday environment T1010	Triage T1001	Disk imaging T1002	Key recovery from memory T1031	Disk image hash verification T1042	Privileged material protection T1046	Keyword searching T1049	Identify partitions T1059	Content indexer examination (OS) T1065	Browser examination T1069	Database examination T1071	Extraction of user accounts T1084	Virtualise suspect system for previewing T1103	Timeline analysis T1086	Source code review T1089	Bookmarking T1091
Digital sniffer dogs T1006	Evidence bags T1011		Memory imaging T1003	Side channel T1032	Forensic image format decoding T1043	Hash matching (reduce) T1047	Hash matching (locate) T1050	Process file system structures T1060	Log file examination (OS) T1066	Email examination T1070	Audio content analysis T1079	Identify conflation T1085		Geospatial analysis T1087	Experimentation T1090	Produce bookmark-based automated report T1092
SyncTriage-based approach T1007	Hardware write blockers T1012		Selective data acquisition T1004	Extraction of account details from an accessible device T1033	Mobile backup decoding T1044	Privacy protection via partial processing T1048	Fuzzy hash matching T1051	Non-allocated file recovery T1061	Cloud synchronisation feature examination (OS) T1067	Chat app examination T1072	Video content analysis T1080			Connection analysis T1088	Instrumentation T1095	Write expert report T1093
Profiling network traffic T1008	Software write blockers T1013		Privacy preserving selective extraction T1015	Brute force attack T1034	Decode standard archive format T1045		Timeline generation T1052	Decryption of encrypted file systems/volumes T1062	Recently used file identification (OS) T1068	Calendar app examination T1073	Image content analysis T1081				Cell site survey T1101	Disclosure T1094
Locate cloud account identifiers T1009	Chain of custody documentation T1014		Live data collection T1016	Dictionary attack T1035	Decode data from image from unmanaged NAND T1102		Entity extraction T1053	Identify file types T1063	Memory examination (OS-level) T1083	Social network app examination T1074	Document content analysis T1082					
			Network packet capture T1017	Smudge attack T1036			Content review for relevant material T1054	File carving T1064	Run programs identification (OS) T1096	Maps/travel app examination T1075						
			Remote data collection T1018				File system content inspection T1055		Installed programs identification (OS) T1097	Photos app examination T1077						
			Mobile backup extraction T1019	Rainbow tables T1038			Entity connection identification T1056		User account analysis (OS) T1098	Cloud sync app examination T1078						
			Mobile file system extraction T1020	App downgrade T1039			Steganography detection T1057			Memory examination (application-level) T1105						
			Mobile device screenshot based capture T1022	Use mobile device exploit T1040			Mismatched file extension detection T1058									
			Cloud data collection using account details T1023	Pin2Pwn T1041												
			Cloud data collection via request T1024													
			Writing data to a forensic image format T1025													
			Writing data in standard archive format T1026													
			Data read using JTAG T1027													
			Chip-off T1028													
			Data read from desoldered eMMC T1029													
			Data read from unmanaged NAND T1030													
			Collect data using open source intelligence T1104													

Applications: Identifying academic research gaps

ID	Description	Mitigation	Has none	In technique
W1001	Excluding a device that contains relevant information	0	x	['T1001']
W1002	Use of triage technology results in changes to the target media	2		['T1001']
W1003	Triage tool applies a simplification that does not correctly represent the meaning of the digital data	1		['T1001']
W1004	Acquisition does not include all sectors from LBA0 to LBA max	1		['T1002']
W1005	Dogs fail to find a digital device	0	x	['T1006']
W1006	Acquistion does not include data in HPA	1		['T1002']
W1007	Acquistion does not include data in DCO	1		['T1002']
W1008	Missing the existence of a device by missing synchronisation artefacts	2		['T1007']
W1009	Missing the existence of a device by incorrectly parsing synchronisation artefacts	1		['T1007']
W1010	Misattributing activity to the wrong device	1		['T1007']
W1011	Suggesting the existence of a device that does not exist	1		['T1007']
W1012	Interaction with the target devices to read synronisation artefacts causes changes	2		['T1007']
W1013	Acquisition includes extra bytes	2		['T1002']
W1014	Imaging process changes original data	2		['T1002']
W1015	Powering on SSD results in sectors being wiped by TRIM operation	0	x	['T1002']
W1016	Data copied from sectors on source are stored incorrectly	1		['T1002']
W1017	Files or data that is relevant to the investigation is missed	0	x	['T1004']
W1018	Data is collected that is not relevant to the investigation	0	x	['T1004']

Summary of Applications (so far)

Scoping error focused datasets

Highlighting mitigations that exist for a weakness in a technique

Identifying weaknesses in a case, SOP/process, or tool workflow

Structured consideration of AI applications

Academic research gaps (research directions)

...

Future Work

- Identify additional applications of SOLVE-IT
  - Teaching
  - Modelling dependencies and uncertainty
  - Skills assessments
  - …
- Test in operational environment regarding the ‘evaluation of process’ application
- Refactor some aspects, e.g. References, Datasets, Examples

- Community contributions to SOLVE-IT
  - Content
  - Definitions
  - Structure
  - Implementation e.g. UX & usability

Contribute

My work provides a new technique in digital forensics.

Add a new technique to SOLVE-IT…

also check if it is a mitigation to a weakness!

My work highlights a weakness in a digital forensic technique

Add a new weakness to SOLVE-IT and link it to a technique.

My work mitigates a weakness in digital forensics.

Add a new mitigation and link it to the weakness in SOLVE-IT. Also check if it needs to be it’s own technique (especially if it has its own weaknesses).

Contribute

I have a way to identify specific weaknesses for digital forensic techniques!

Great let’s apply it and index more weaknesses for some common digital forensic techniques.

I have a new process model and want to re-organise the techniques in SOLVE-IT

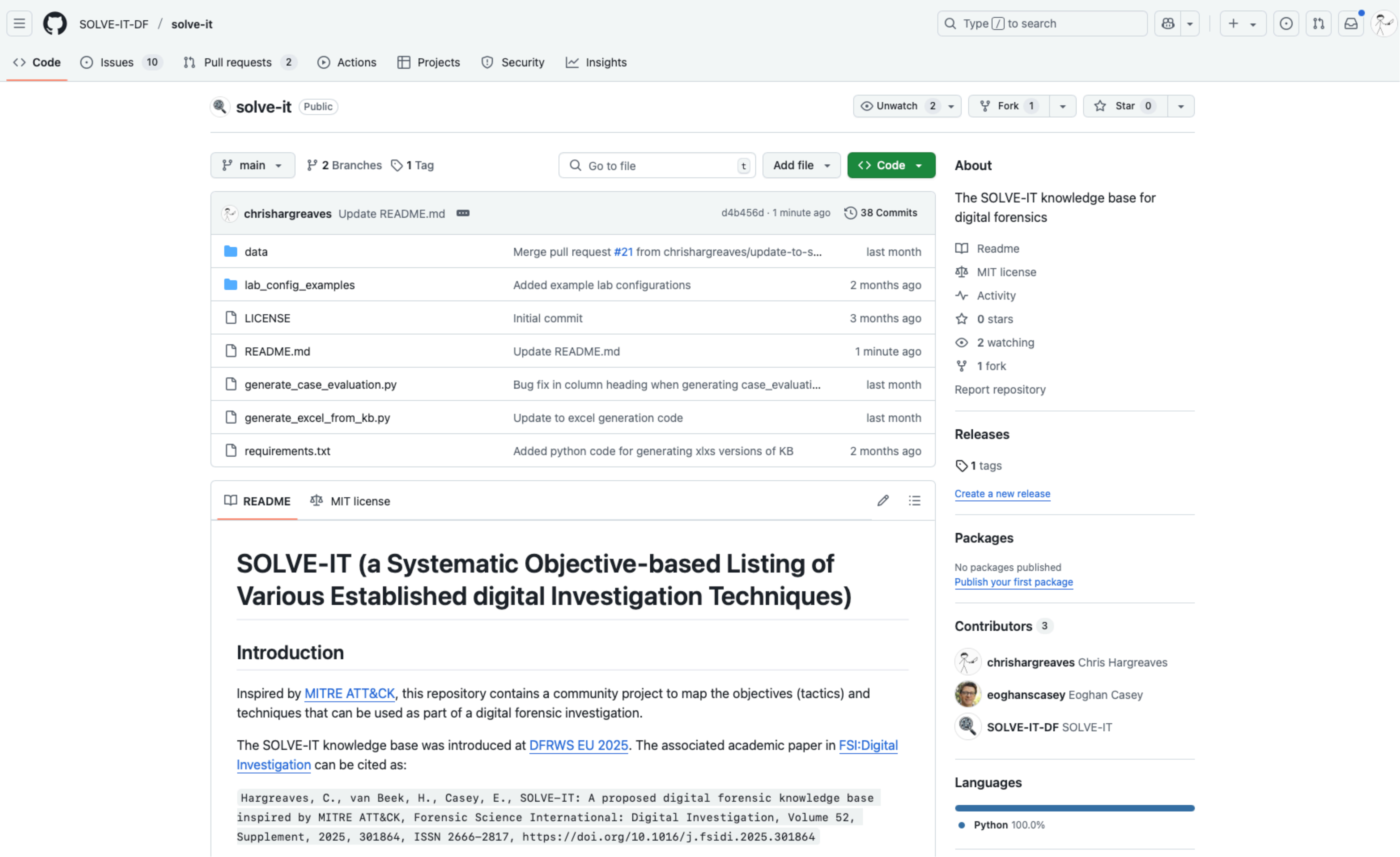
No problem. Add a JSON file with your process model and the techniques contained within each stage/phase.

I want to map an Standard Operating Procedure (SOP) or tool workflow using SOLVE-IT and enumerate potential weaknesses in those processes?

Use *generate_case_evaluation.py* script with the list of techniques used.You can also submit SOLVE-IT implementations to the project GitHub.

Resources

Website



chrishargreaves Update README.md · d4b456d · 1 minute ago · 38 Commits

data	Merge pull request #21 from chrishargreaves/update-to-s...	last month
lab_config_examples	Added example lab configurations	2 months ago
LICENSE	Initial commit	3 months ago
README.md	Update README.md	1 minute ago
generate_case_evaluation.py	Bug fix in column heading when generating case_evaluati...	last month
generate_excel_from_kb.py	Update to excel generation code	last month
requirements.txt	Added python code for generating xlxs versions of KB	2 months ago

SOLVE-IT (a Systematic Objective-based Listing of Various Established digital Investigation Techniques)

Introduction

Inspired by MITRE ATT&CK, this repository contains a community project to map the objectives (tactics) and techniques that can be used as part of a digital forensic investigation.

The SOLVE-IT knowledge base was introduced at DFRWS EU 2025. The associated academic paper in FSI:Digital Investigation can be cited as:

```
Hargreaves, C., van Beek, H., Casey, E., SOLVE-IT: A proposed digital forensic knowledge base
inspired by MITRE ATT&CK, Forensic Science International: Digital Investigation, Volume 52,
Supplement, 2025, 301864, ISSN 2666-2817, https://doi.org/10.1016/j.fsidi.2025.301864
```

About

The SOLVE-IT knowledge base for digital forensics

Releases

Packages

Contributors 3

- chrishargreaves Chris Hargreaves
- eoghanscasey Eoghan Casey
- SOLVE-IT-DF SOLVE-IT

Languages

https://github.com/SOLVE-IT-DF/solve-it

Questions?

https://github.com/SOLVE-IT-DF/solve-it