UNIL | Université de Lausanne
Ecole des sciences criminelles

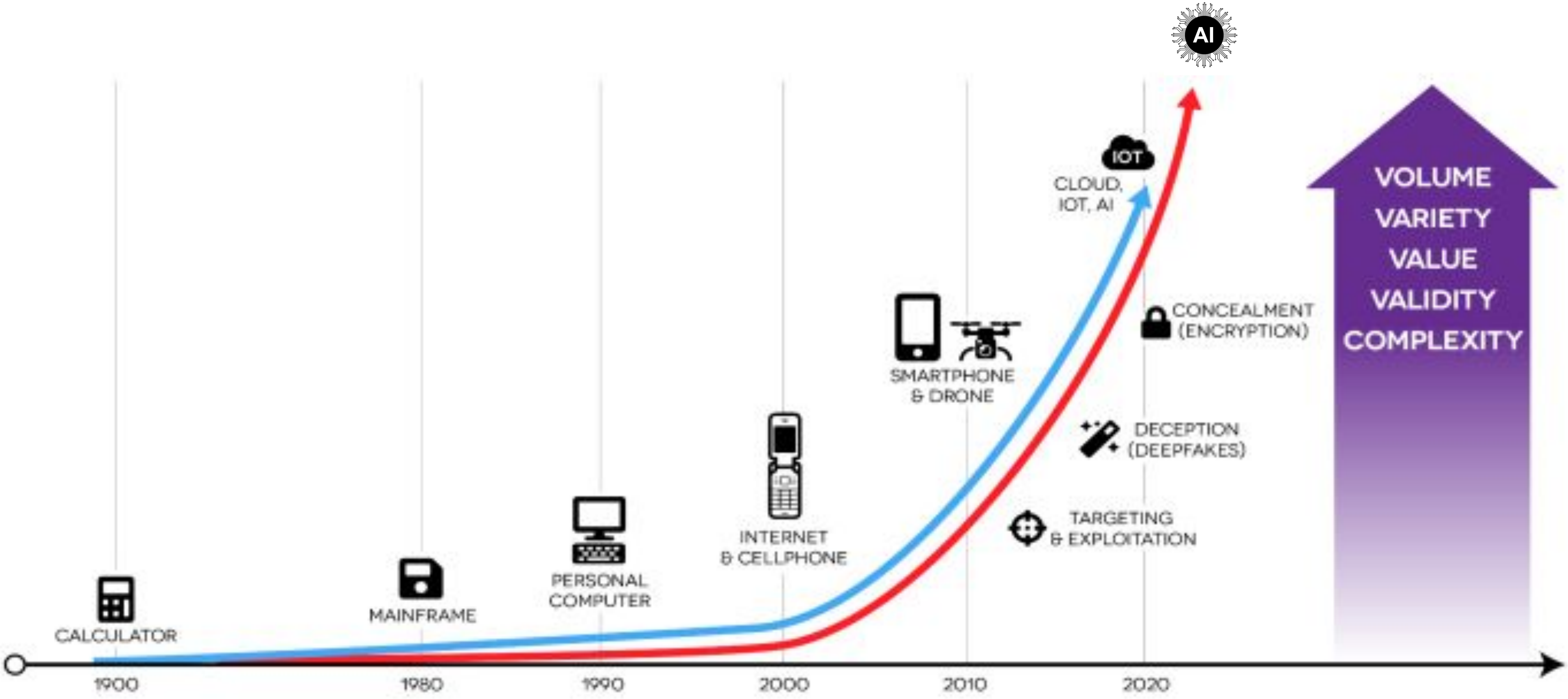
Handling Error and Uncertainty in Forensic Computing

Eoghan Casey

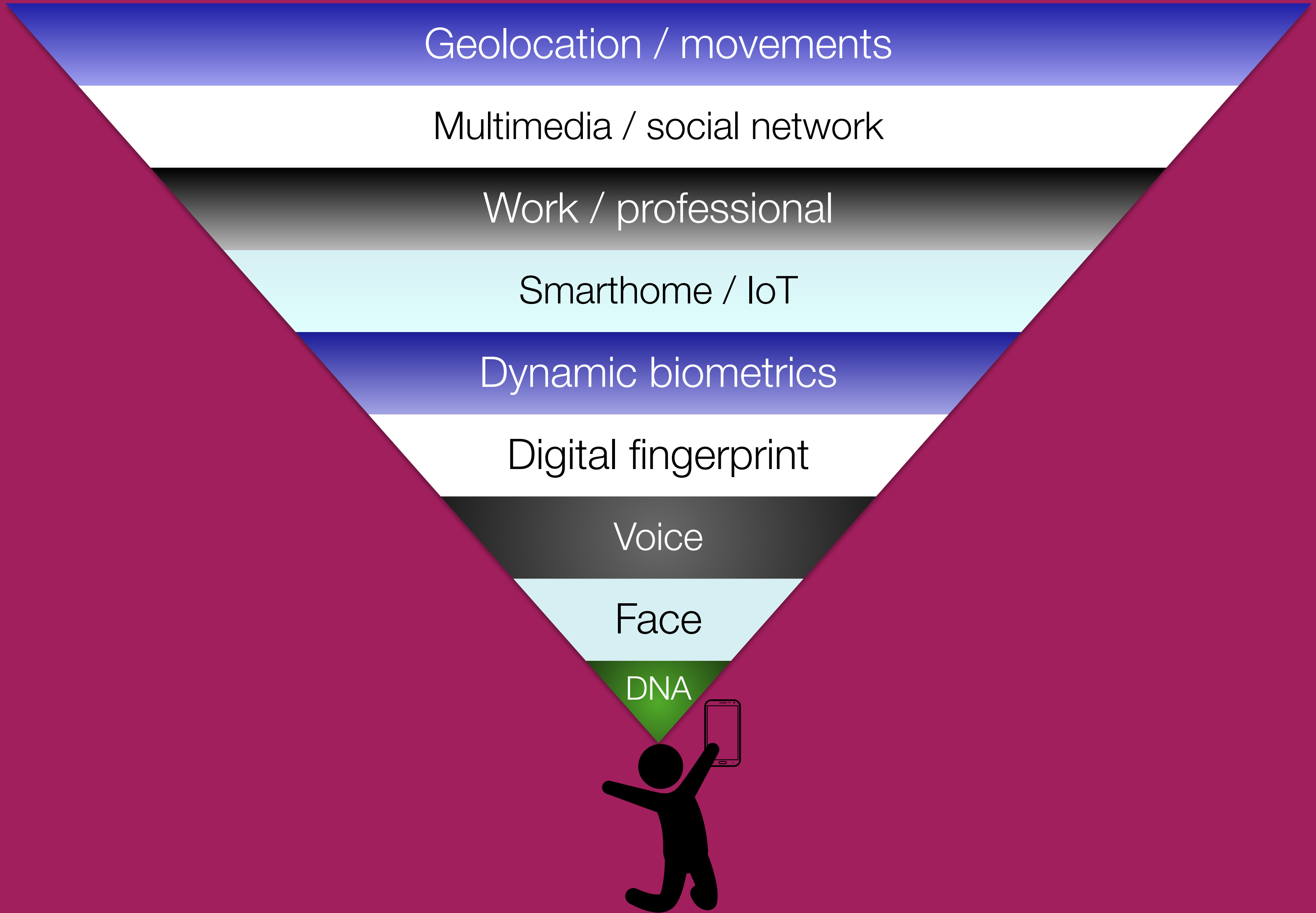
University of Lausanne, Digital Forensic Science

| le savoir vivant

Digitalised Traceability Rising Rapidly



Digital Evidence Gives False Sense of Certainty



Geolocation / movements

Multimedia / social network

Work / professional

Smarthome / IoT

Dynamic biometrics

Digital fingerprint

Voice

Face

DNA

Uncertainty in Forensic Computing

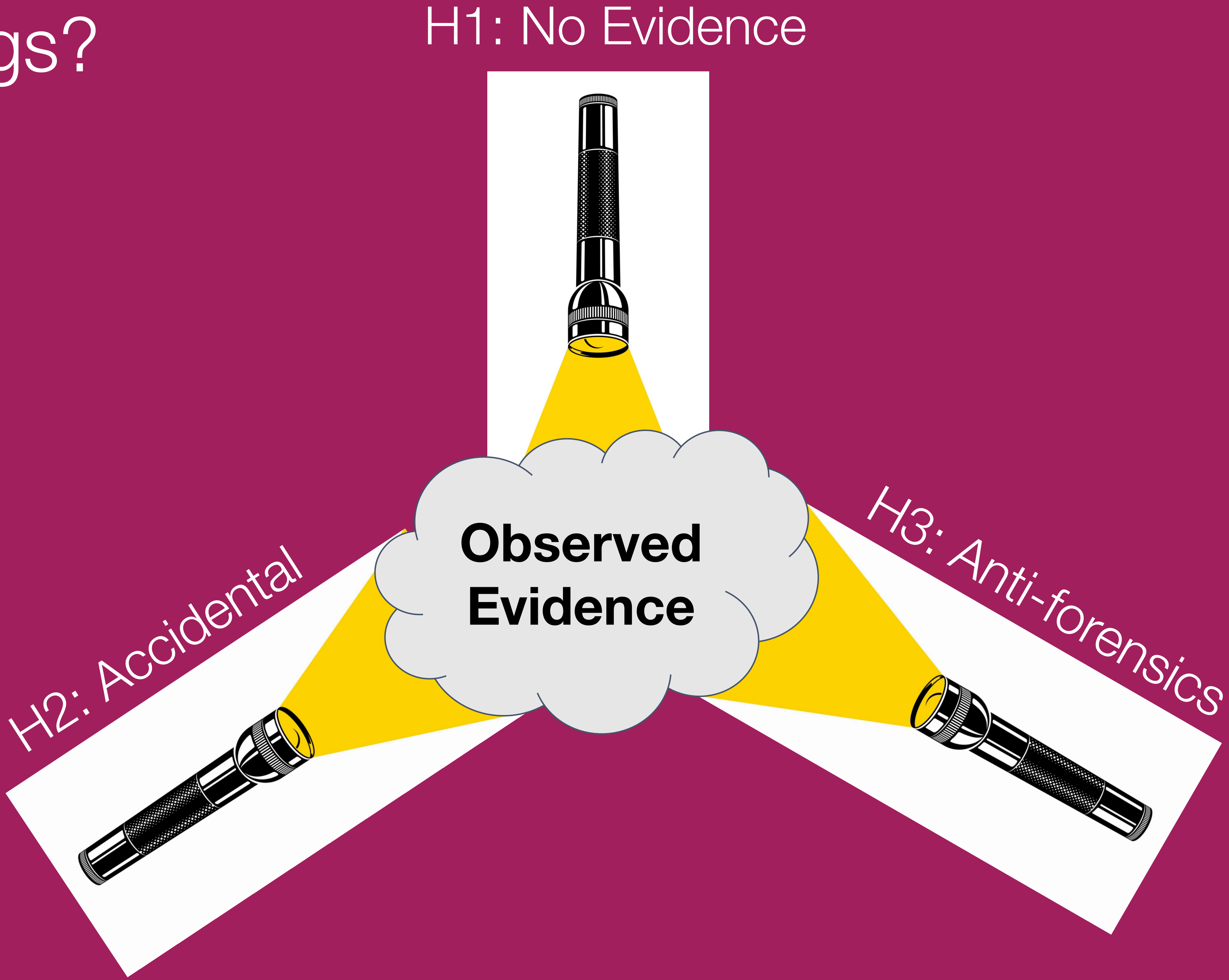
You are observing results of an event, not the event itself

Forensic Computing:

- ✘ DOES NOT determine the cause of events
- ✓ DOES give indications of how digital evidence measures when different causes are considered
- ⁇ DISCUSS: Analysis of Competing Hypotheses ¿¿

No Findings?

Analysis of
Observed
Evidence
in Light of
Competing
Hypotheses



H1: No Evidence

H2: Accidental

H3: Anti-forensics

Observed Evidence

Pierre Margot

Since it is not possible to go back in time, we can only construct a model that is descriptive of a given crime scenario, supported by what is observed.

This is not a general model, but a specific retrodictive model that can only be probabilistic in nature. In the majority of cases, the quality of the vestige is such that it is incomplete, imperfect and degraded by time passing, and these losses increase uncertainty or may support only approximations about the past event.

Traceology, the bedrock of forensic science and its associated semantics by *Pierre Margot*

in The Routledge International Handbook of Forensic Intelligence and Criminology

Intro to Case Assessment & Interpretation

Stage	Activities
1. Observation	**Make initial observations**
2. Hypothesis generation	**Generate a set of plausible hypotheses** (initial observations, case circumstances)
3. Inference to the best explanation	**Rank the hypotheses** (initial observations, current knowledge, past experience)
4. Prediction of likely observations	**Predict likelihoods for the range of possible future observations** (postulating that each of the hypotheses were true)
5. "Second Phase" observation	**Search for predicted likely observations**
6. Strength of evidence assignation	**Assign likelihood values to the observed digital evidence** (in light of each hypothesis / proposition)
7. Communication	**Express evaluative opinions**

Are you Asking the Correct Question?

Considering Plausible Alternative Explanations

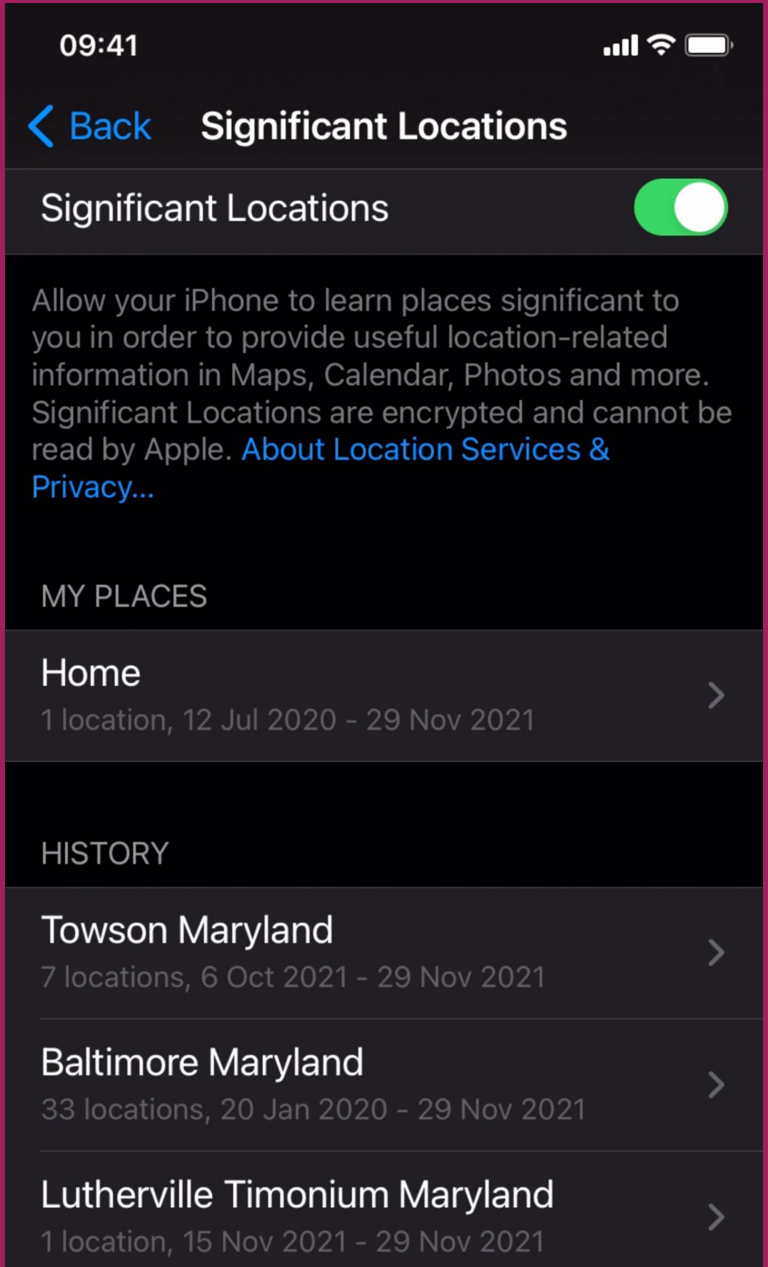
Homicide - Geofencing and CCTV

Molina’s phone & car were near the scene at the time of the crime

1) Murder - shooting
2) Video - white Honda vehicle registered to Molina
3) Google - Android logged into Molina’s account was in the area

Consider alternative explanations…

Significant Locations



Significant Locations

Significant Locations ●

Allow your iPhone to learn places significant to you in order to provide useful location-related information in Maps, Calendar, Photos and more. Significant Locations are encrypted and cannot be read by Apple. About Location Services & Privacy...

MY PLACES

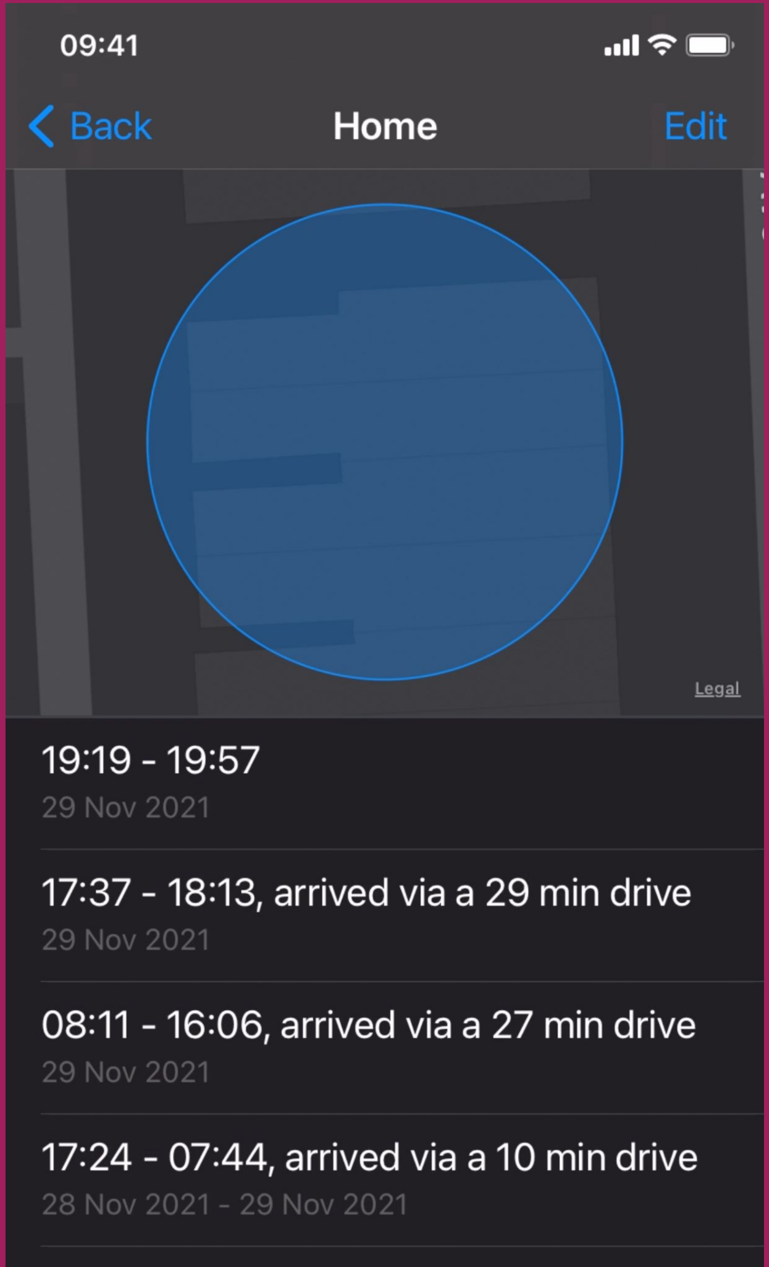
Home
1 location, 12 Jul 2020 - 29 Nov 2021

HISTORY

Towson Maryland
7 locations, 6 Oct 2021 - 29 Nov 2021

Baltimore Maryland
33 locations, 20 Jan 2020 - 29 Nov 2021

Lutherville Timonium Maryland
1 location, 15 Nov 2021 - 29 Nov 2021



Home

19:19 - 19:57
29 Nov 2021

17:37 - 18:13, arrived via a 29 min drive
29 Nov 2021

08:11 - 16:06, arrived via a 27 min drive
29 Nov 2021

17:24 - 07:44, arrived via a 10 min drive
28 Nov 2021 - 29 Nov 2021

Frequent Locations History (FLH)

- ❖ A place where the device visited at least 2 times
  - ➢ and remained at the place for some time

- ❖ FLH entry created 24 - 72 hours after the 2nd visit

- ❖ FLH entry details:
  - ➢ Latitude
  - ➢ Longitude
  - ➢ Confidence
  - ➢ Uncertainty
  - ➢ Entry Timestamp*
  - ➢ Exit Timestamp*
  - ➢ Update Timestamp

*** Entry and Exit Timestamps are not the precise time that a place was visited, but are a value approximately three minutes to one hour after the actual time of entry and exit.**

Digital Forensic Report

“Frequent Location 58 places the defendant’s iPhone at the scene of the murder at the time of the murder.”

The center point of Frequent Location 58 was at about 326 Harvard Street, two doors down from the scene of the murder, with a radius, or “uncertainty,” of 43 meters (143 feet), which encapsulates the crime scene at 332 Harvard Street

UNIL | Université de Lausanne

Ecole des sciences criminelles

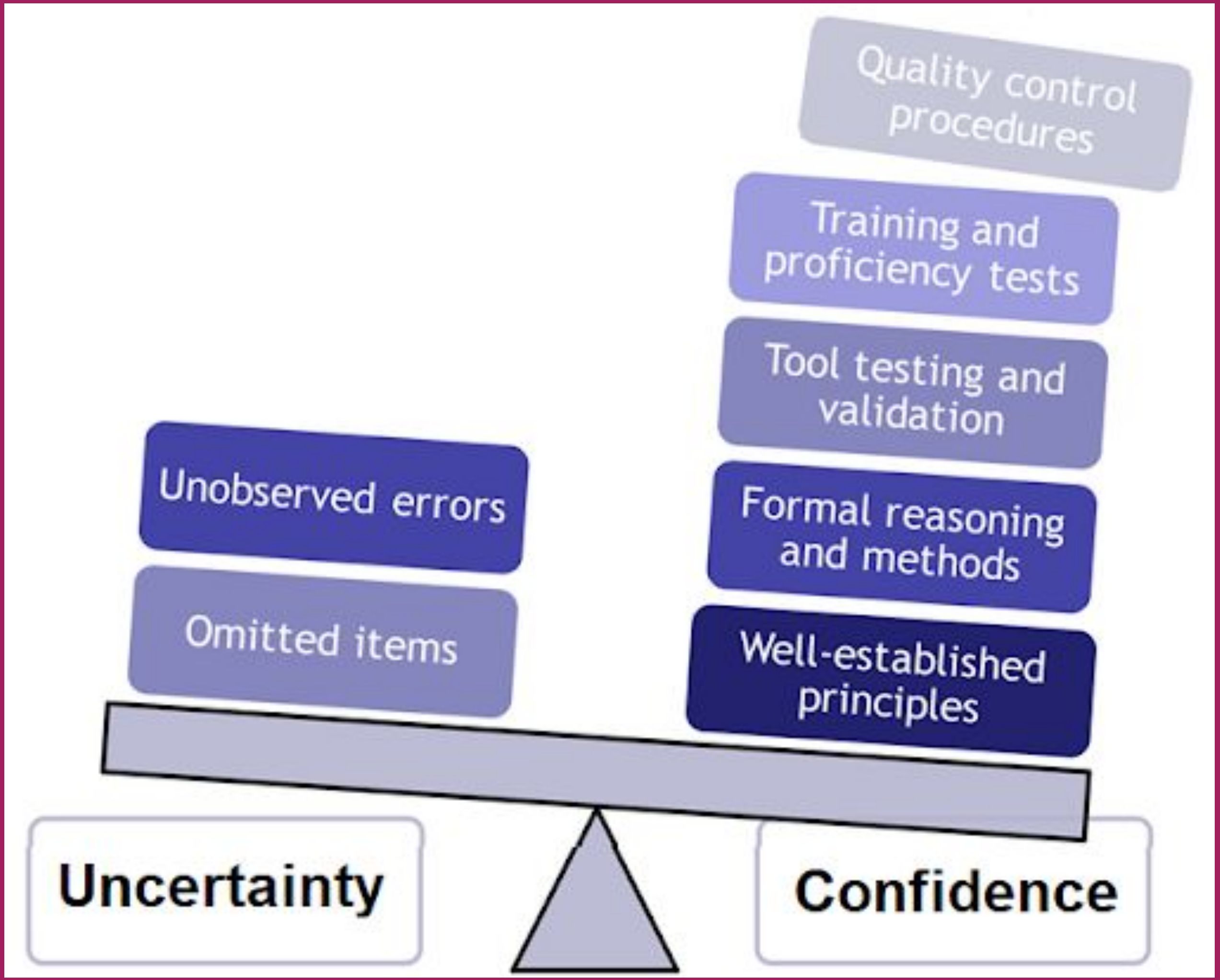
Are you Correctly Observing Digital Evidence?

Mitigating Errors, Weaknesses & Uncertainty

| le savoir vivant

ASTM - Error Mitigation Analysis

- Tools
- Personnel
- Procedures
- Documentation
- Oversight
- Reasoning
- Defined principles & processes

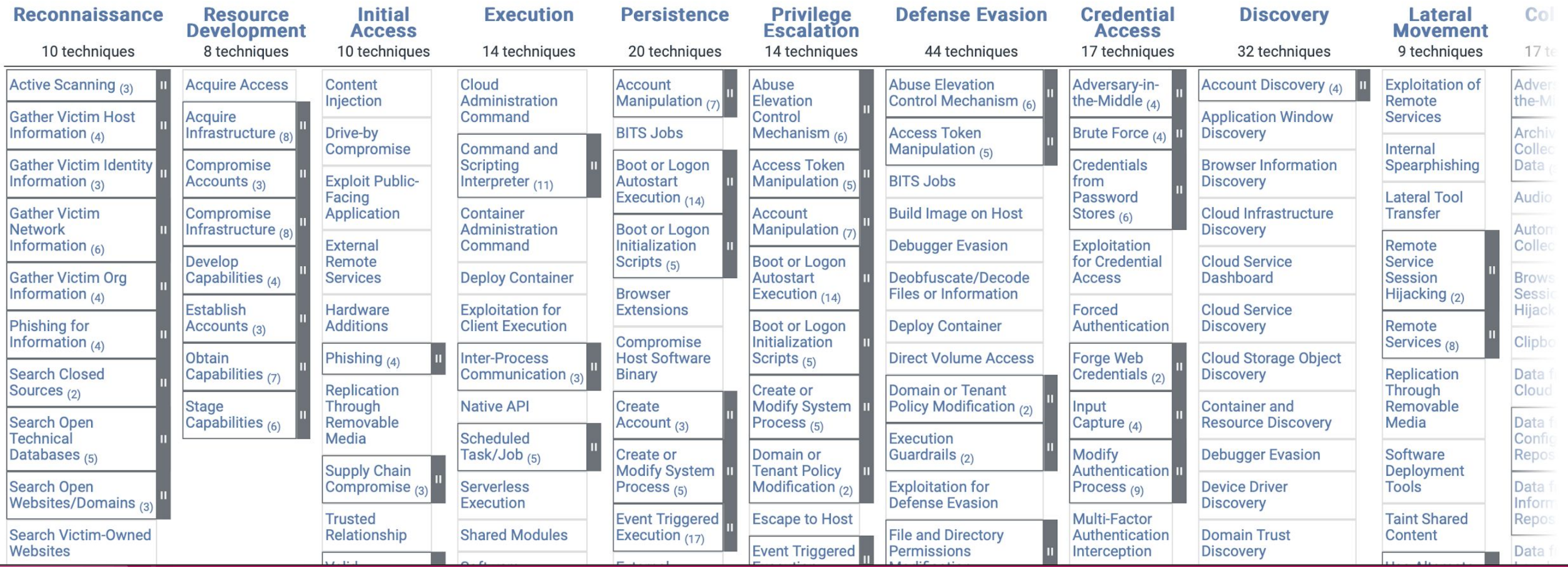

Quality control procedures
Training and proficiency tests
Tool testing and validation
Unobserved errors
Formal reasoning and methods
Omitted items
Well-established principles
Uncertainty
Confidence

SOLVE-IT

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

Systematic Objective-based Listing of Various Established (Digital) Investigation Techniques

MITRE ATT&CK MODEL



Reconnaissance
10 techniques
- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (4)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (3)
- Search Victim-Owned Websites

Resource Development
8 techniques
- Acquire Access
- Acquire Infrastructure (8)
- Compromise Accounts (3)
- Compromise Infrastructure (8)
- Develop Capabilities (4)
- Establish Accounts (3)
- Obtain Capabilities (7)
- Stage Capabilities (6)

Initial Access
10 techniques
- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (4)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship

Execution
14 techniques
- Cloud Administration Command
- Command and Scripting Interpreter (11)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Serverless Execution
- Shared Modules

Persistence
20 techniques
- Account Manipulation (7)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Host Software Binary
- Create Account (3)
- Create or Modify System Process (5)
- Event Triggered Execution (17)

Privilege Escalation
14 techniques
- Abuse Elevation Control Mechanism (6)
- Access Token Manipulation (5)
- Account Manipulation (7)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (5)
- Domain or Tenant Policy Modification (2)
- Escape to Host
- Event Triggered

Defense Evasion
44 techniques
- Abuse Elevation Control Mechanism (6)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain or Tenant Policy Modification (2)
- Execution Guardrails (2)
- Exploitation for Defense Evasion
- File and Directory Permissions

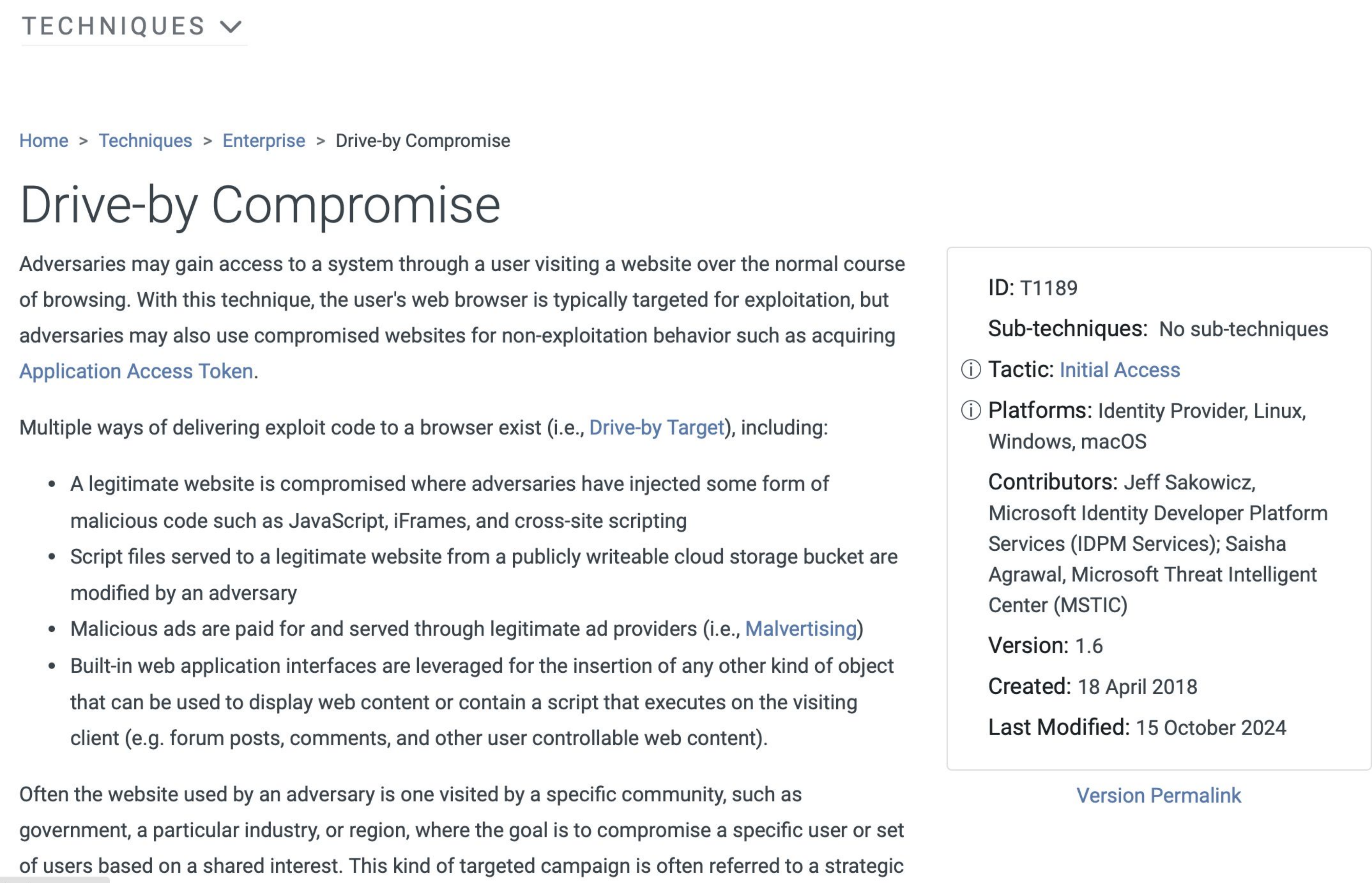
Credential Access
17 techniques
- Adversary-in-the-Middle (4)
- Brute Force (4)
- Credentials from Password Stores (6)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (9)
- Multi-Factor Authentication Interception

Discovery
32 techniques
- Account Discovery (4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery

Lateral Movement
9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (8)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content

Col
17 te
- Adver the-Mi
- Archiv Collec Data (
- Audio
- Autom Collec
- Brows Sessio Hijack
- Clipbo
- Data f Cloud
- Data f Config Repos
- Data f Inform Repos
- Data f

MITRE ATT&CK MODEL



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

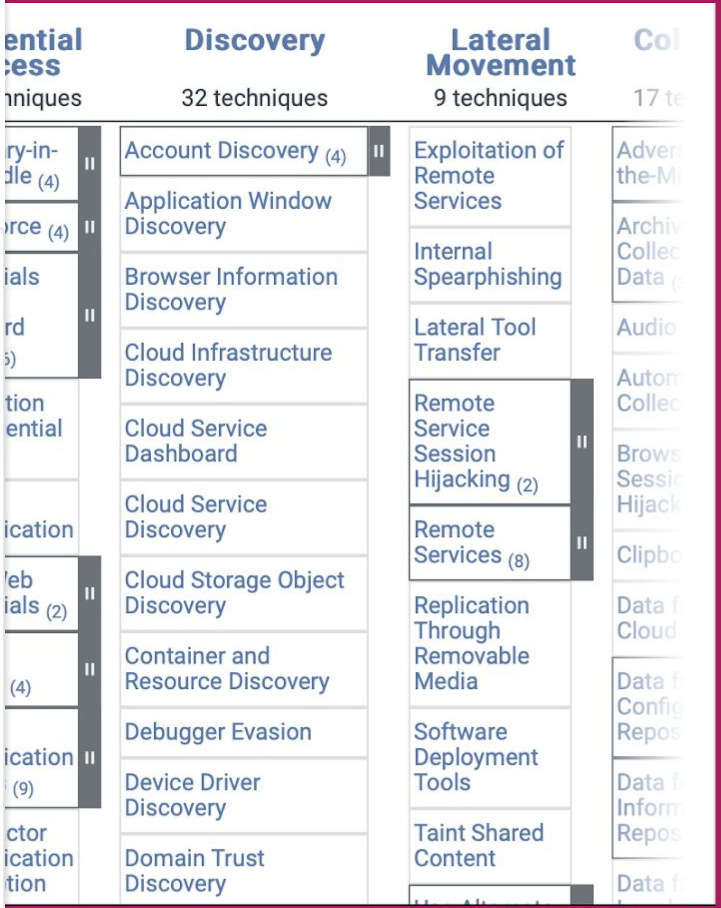
Contributors: Jeff Sakowicz, Microsoft Identity Developer Platform Services (IDPM Services); Saisha Agrawal, Microsoft Threat Intelligent Center (MSTIC)

Version: 1.6

Created: 18 April 2018

Last Modified: 15 October 2024

Version Permalink



ential cess
niques

- ry-in- dle (4)
- rce (4)
- ials
- rd 5)
- tion ential
- ication
- eb ials (2)
- (4)
- ication (9)
- ctor ication tion

Discovery
32 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery

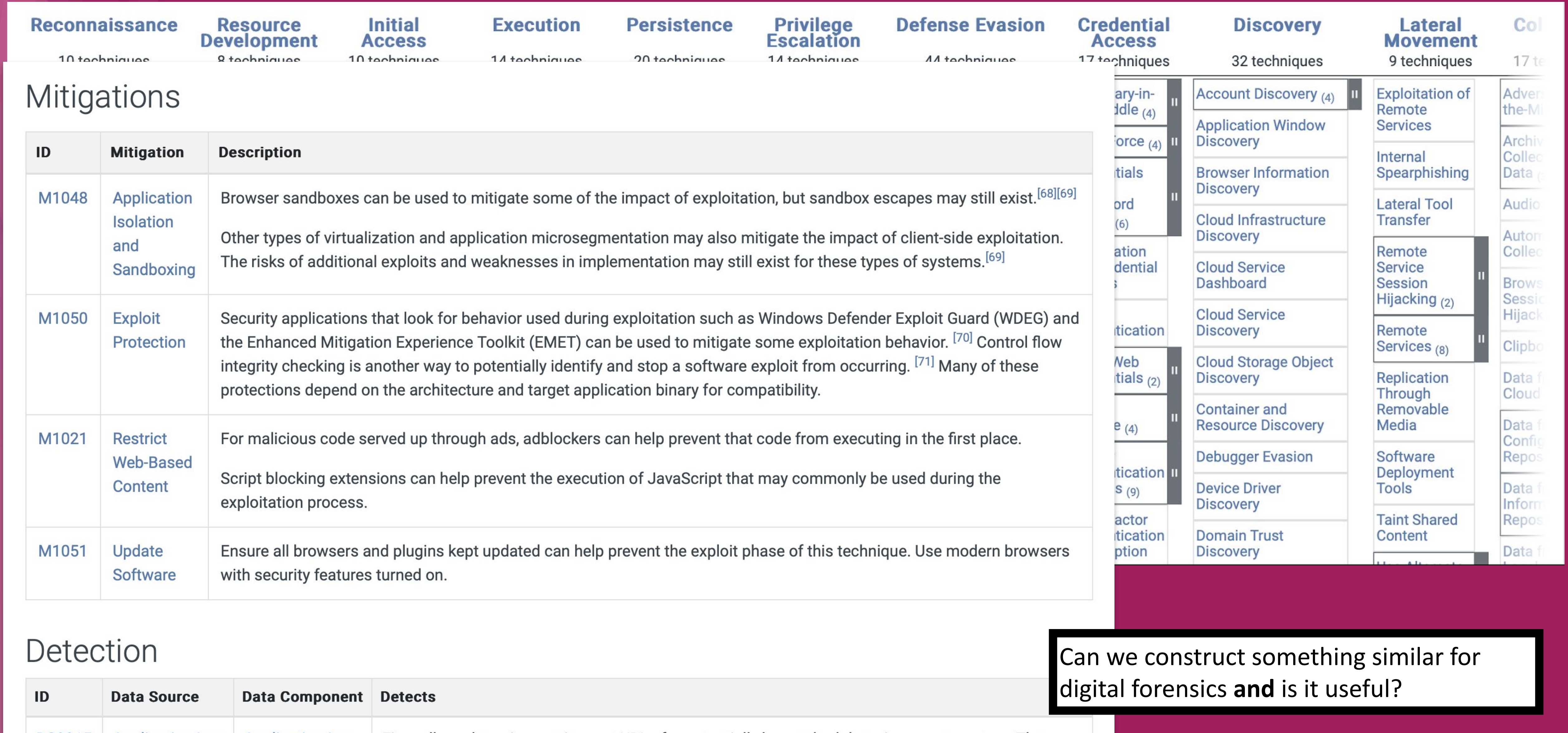
Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (8)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content

Col
17 t

- Adve the-M
- Archi Collec Data
- Audio
- Autom Collec
- Brows Sessi Hijack
- Clipbo
- Data f Cloud
- Data f Config Repos
- Data f Inform Repos
- Data f

MITRE ATT&CK MODEL



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

ary-in-
ddle (4)
orce (4)
tials
ord
(6)
ation
dential
s
tication
Web
tials (2)
e (4)
tication
s (9)
actor
tication
ption

Account Discovery (4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery

Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (8)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content

Adve
the-M
Archi
Colle
Data
Audio
Autom
Collec
Brows
Sessio
Hijack
Clipbo
Data f
Cloud
Data f
Config
Repos
Data f
Inform
Repos
Data f

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.

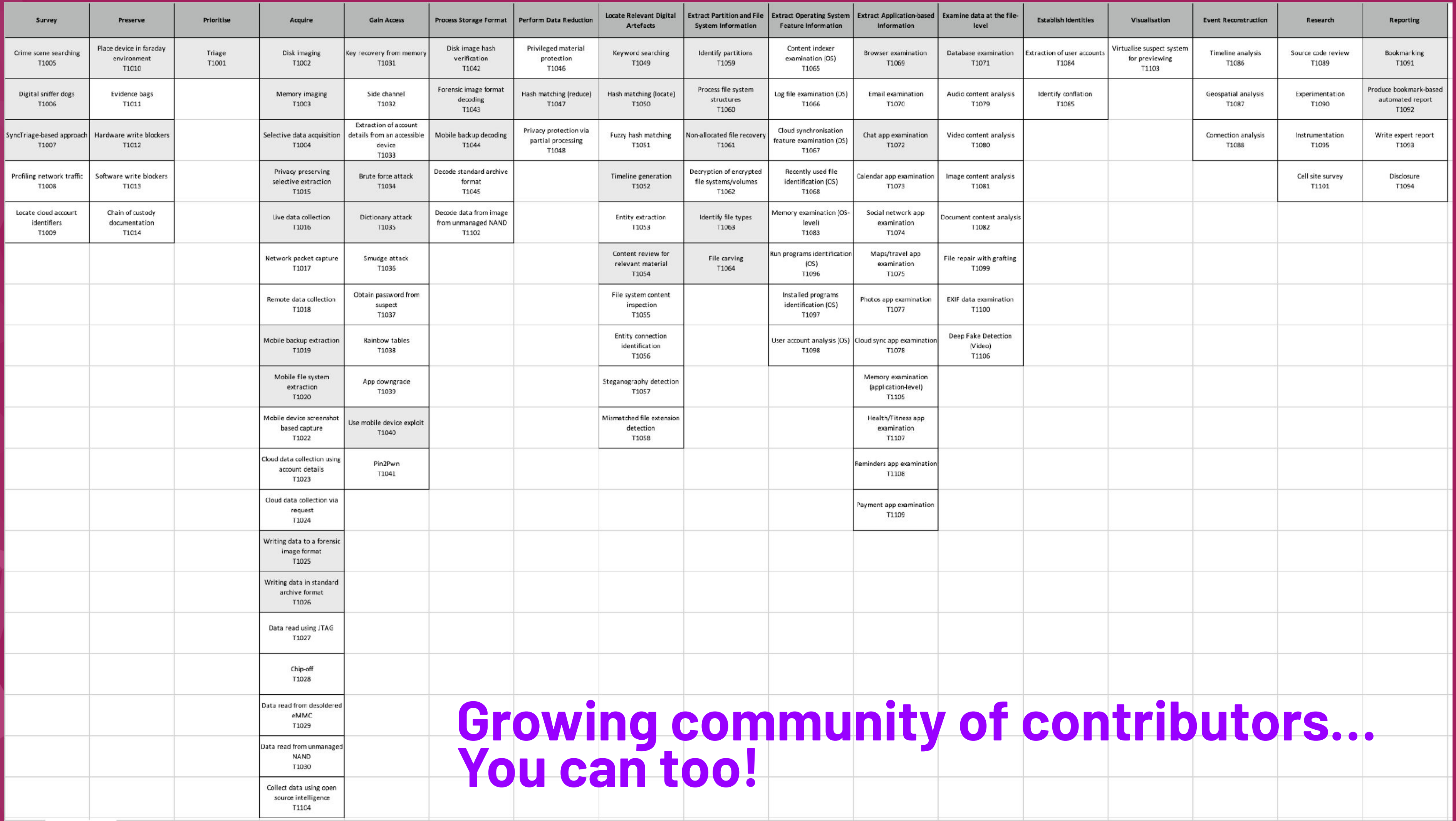
Detection

ID	Data Source	Data Component	Detects

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

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

Hundreds of techniques with associated weaknesses and mitigations

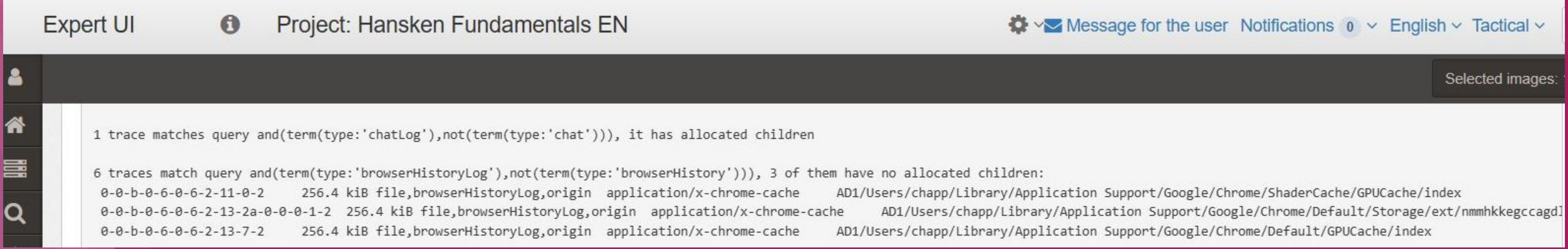


Survey	Preserve	Prioritise	Acquire	Gain Access	Process Storage Format	Perform Data Reduction	Locate Relevant Digital Artefacts	Extract Partition and File System Information	Extract Operating System Feature Information	Extract Application-based Information	Examine data at the file-level	Establish Identities	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 explcit 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													

**Growing community of contributors…
You can too!**

SOLVE-IT Supporting Forensic Tools

Msg: Browser history log doesn't contain expected browser history entries



```
1 trace matches query and(term(type:'chatLog'),not(term(type:'chat'))), it has allocated children

6 traces match query and(term(type:'browserHistoryLog'),not(term(type:'browserHistory'))), 3 of them have no allocated children:
 0-0-b-0-6-0-6-2-11-0-2     256.4 kiB file,browserHistoryLog,origin  application/x-chrome-cache     AD1/Users/chapp/Library/Application Support/Google/Chrome/ShaderCache/GPUCache/index
 0-0-b-0-6-0-6-2-13-2a-0-0-0-1-2  256.4 kiB file,browserHistoryLog,origin  application/x-chrome-cache     AD1/Users/chapp/Library/Application Support/Google/Chrome/Default/Storage/ext/nmmhkkegccagdl
 0-0-b-0-6-0-6-2-13-7-2     256.4 kiB file,browserHistoryLog,origin  application/x-chrome-cache     AD1/Users/chapp/Library/Application Support/Google/Chrome/Default/GPUCache/index
```

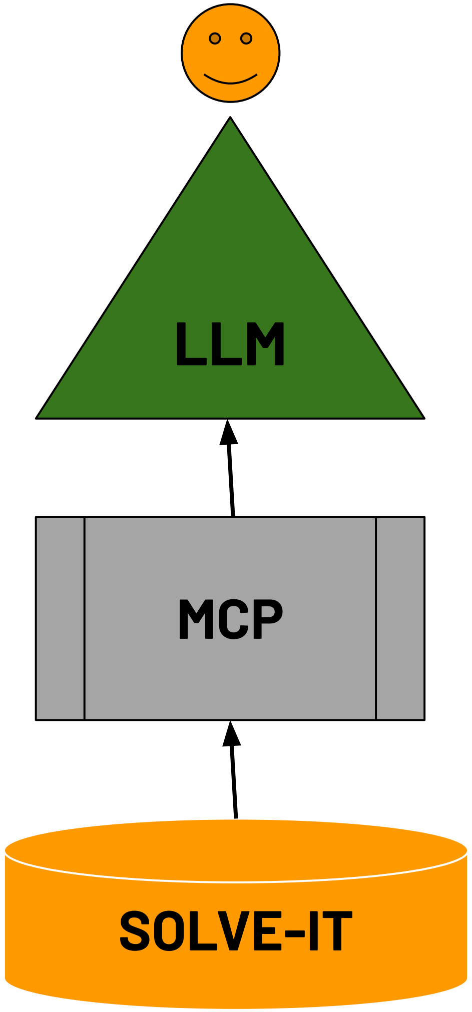
Weakness W1085 “Missing messages from the live set of messages"
Mitigations ["M1054", "M1027", "M1055", "M1056"],
References ["New msgstore – Who ‘Dis? A Look At An Updated WhatsApp
https://thebinaryhick.blog/2022/06/09/new-msgstore-who-dis-a-look-at-an-updated-whatsapp-on-android/

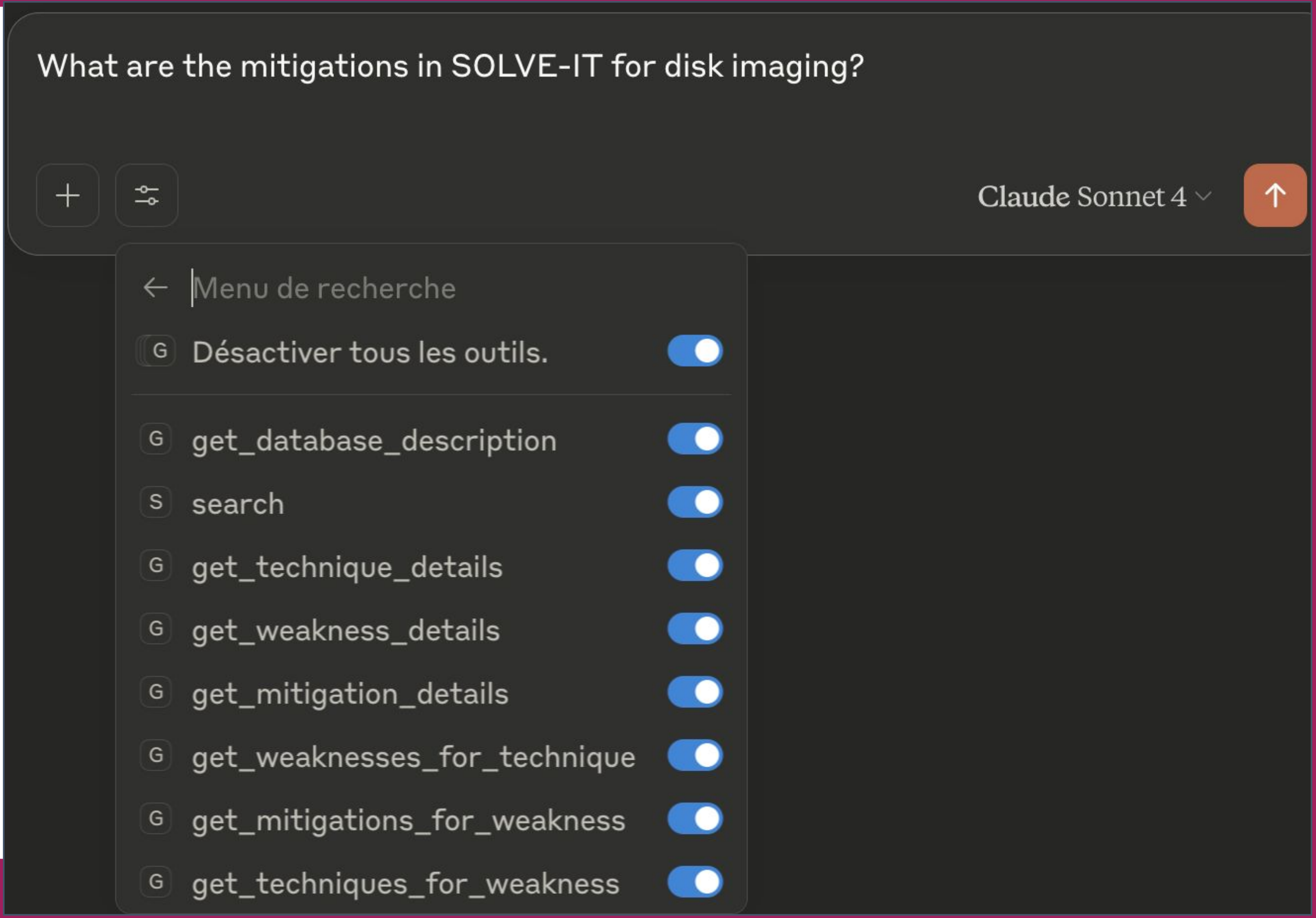
Weakness
Mitigations…

Growing community of contributors... You can too!

AI applications via Model Context Protocol (MCP)

Helping you learn, use, and develop SOLVE-IT



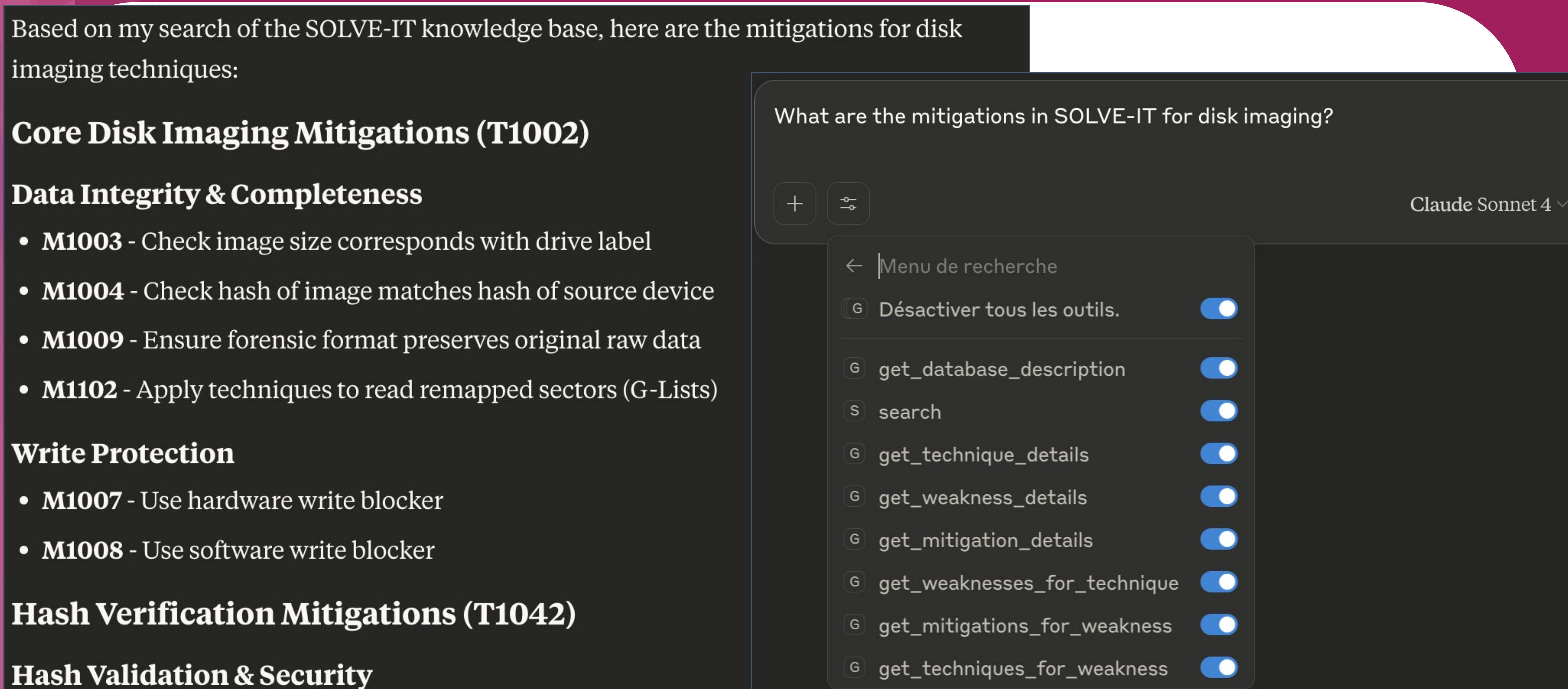


What are the mitigations in SOLVE-IT for disk imaging?

- G get_database_description
- S search
- G get_technique_details
- G get_weakness_details
- G get_mitigation_details
- G get_weaknesses_for_technique
- G get_mitigations_for_weakness
- G get_techniques_for_weakness

AI applications via Model Context Protocol (MCP)

Helping you learn, use, and develop SOLVE-IT



Based on my search of the SOLVE-IT knowledge base, here are the mitigations for disk imaging techniques:

Core Disk Imaging Mitigations (T1002)

Data Integrity & Completeness

- **M1003** - Check image size corresponds with drive label
- **M1004** - Check hash of image matches hash of source device
- **M1009** - Ensure forensic format preserves original raw data
- **M1102** - Apply techniques to read remapped sectors (G-Lists)

Write Protection

- **M1007** - Use hardware write blocker
- **M1008** - Use software write blocker

Hash Verification Mitigations (T1042)

Hash Validation & Security

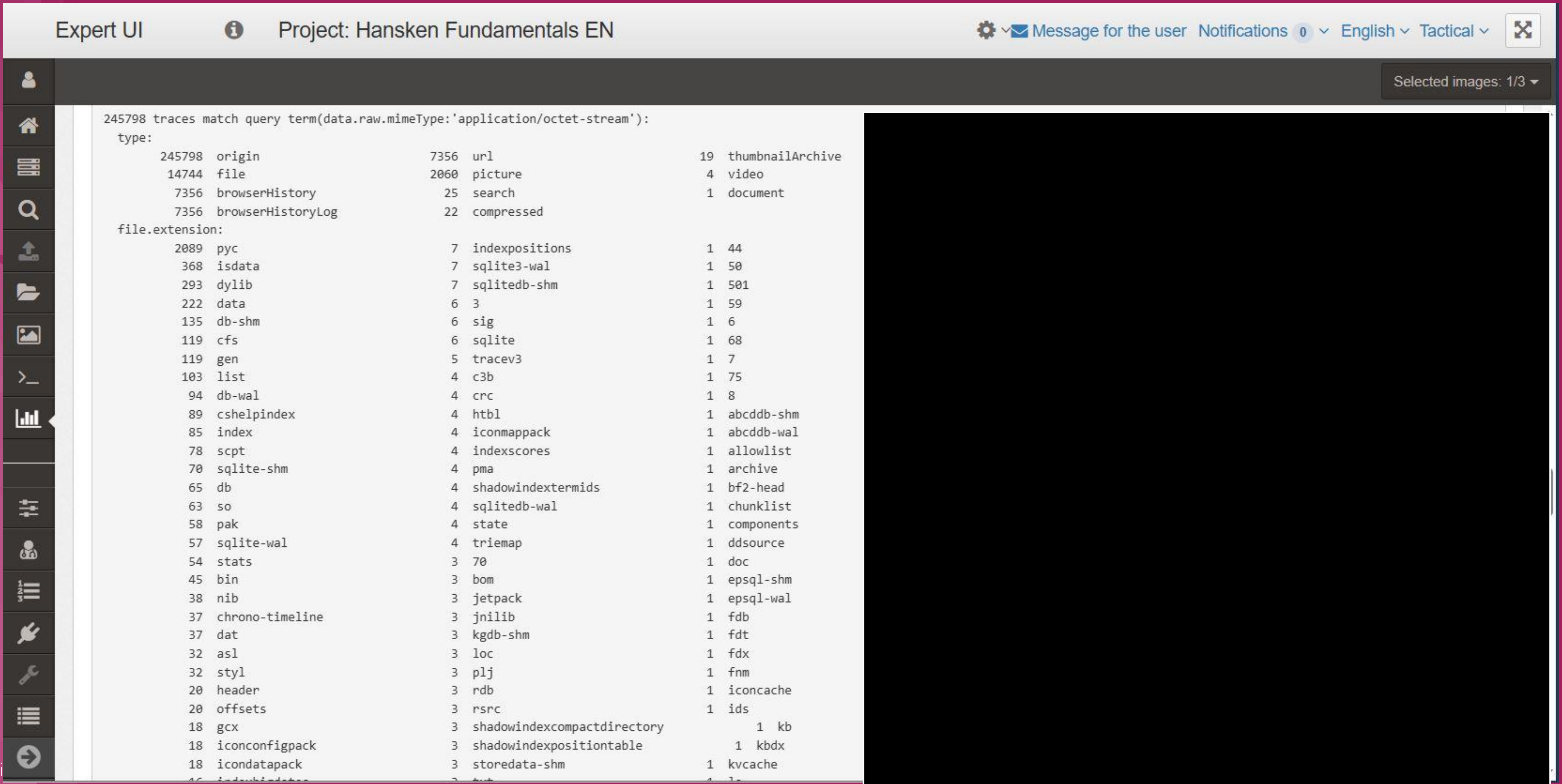
What are the mitigations in SOLVE-IT for disk imaging?

G Désactiver tous les outils. ●

G get_database_description ●
S search ●
G get_technique_details ●
G get_weakness_details ●
G get_mitigation_details ●
G get_weaknesses_for_technique ●
G get_mitigations_for_weakness ●
G get_techniques_for_weakness ●

AI applications via Model Context Protocol (MCP)

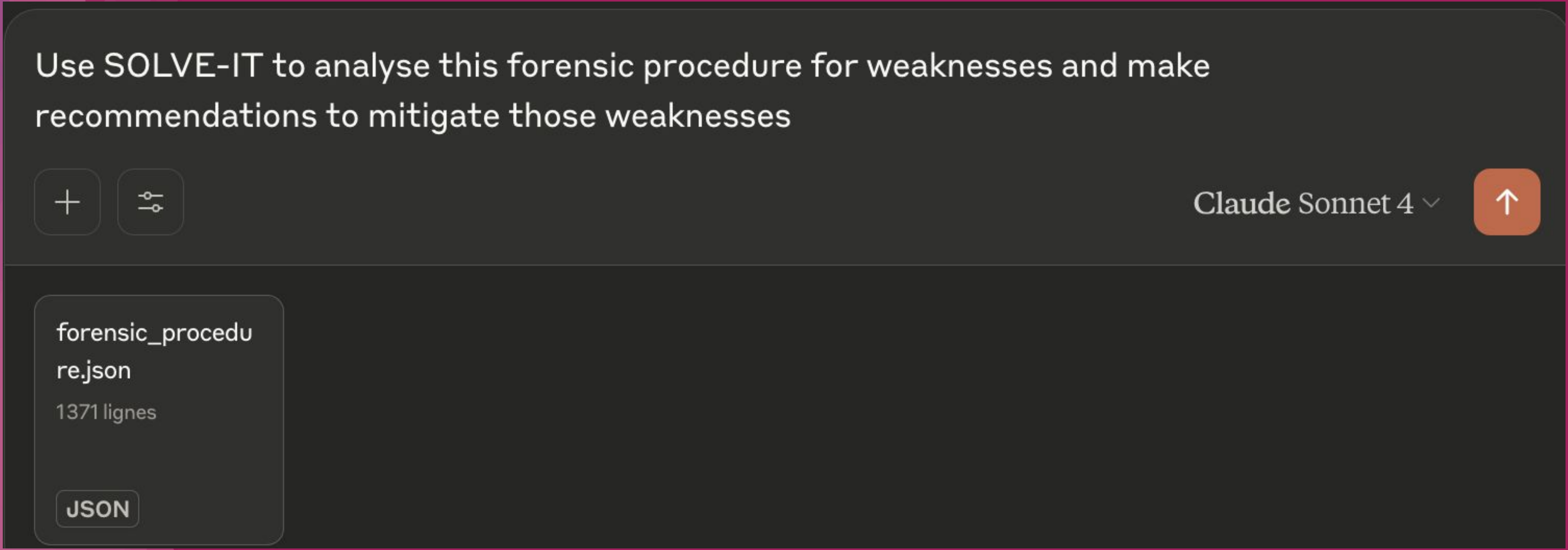
Helping you learn, use, and develop SOLVE-IT



```
245798 traces match query term(data.raw.mimeType:'application/octet-stream'):
  type:
      245798  origin                     7356  url                          19  thumbnailArchive
       14744  file                       2060  picture                       4  video
        7356  browserHistory               25  search                        1  document
        7356  browserHistoryLog            22  compressed
  file.extension:
        2089  pyc                           7  indexpositions                1  44
         368  isdata                        7  sqlite3-wal                   1  50
         293  dylib                         7  sqlitedb-shm                  1  501
         222  data                          6  3                             1  59
         135  db-shm                        6  sig                           1  6
         119  cfs                           6  sqlite                        1  68
         119  gen                           5  tracev3                       1  7
         103  list                          4  c3b                           1  75
          94  db-wal                        4  crc                           1  8
          89  cshelpindex                   4  htbl                          1  abcddb-shm
          85  index                         4  iconmappack                   1  abcddb-wal
          78  scpt                          4  indexscores                   1  allowlist
          70  sqlite-shm                    4  pma                           1  archive
          65  db                            4  shadowindextermids            1  bf2-head
          63  so                            4  sqlitedb-wal                  1  chunklist
          58  pak                           4  state                         1  components
          57  sqlite-wal                    4  triemap                       1  ddsource
          54  stats                         3  70                            1  doc
          45  bin                           3  bom                           1  epsql-shm
          38  nib                           3  jetpack                       1  epsql-wal
          37  chrono-timeline               3  jnilib                        1  fdb
          37  dat                           3  kgdb-shm                      1  fdt
          32  asl                           3  loc                           1  fdx
          32  styl                          3  plj                           1  fnm
          20  header                        3  rdb                           1  iconcache
          20  offsets                       3  rsrc                          1  ids
          18  gcx                           3  shadowindexcompactdirectory       1  kb
          18  iconconfigpack                3  shadowindexpositiontable        1  kbdx
          18  icondatapack                  3  storedata-shm                 1  kvcache
```

AI applications via Model Context Protocol (MCP)

Helping you learn, use, and develop SOLVE-IT



Use SOLVE-IT to analyse this forensic procedure for weaknesses and make recommendations to mitigate those weaknesses

SOLVE-IT 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.

Uncertainty in Digital Traces

- Incompleteness (INCOMP)
- Misinterpretation (MISINT)
- Inaccuracy (INAC)
    - exist (INAC-EX)
    - alteration (INAC-ALT)
    - association (INAC-AS)
    - corruption (INAC-COR)

An abstract model for digital forensic analysis tools - A foundation for systematic error mitigation analysis
Hargreaves, Nelson, Casey (2024)
DFRWS EU 2024
https://doi.org/10.1016/j.fsidi.2023.301679

Are you Answering the Question Correctly?

Evaluating Plausible Alternative Explanations

Warning: False Logic

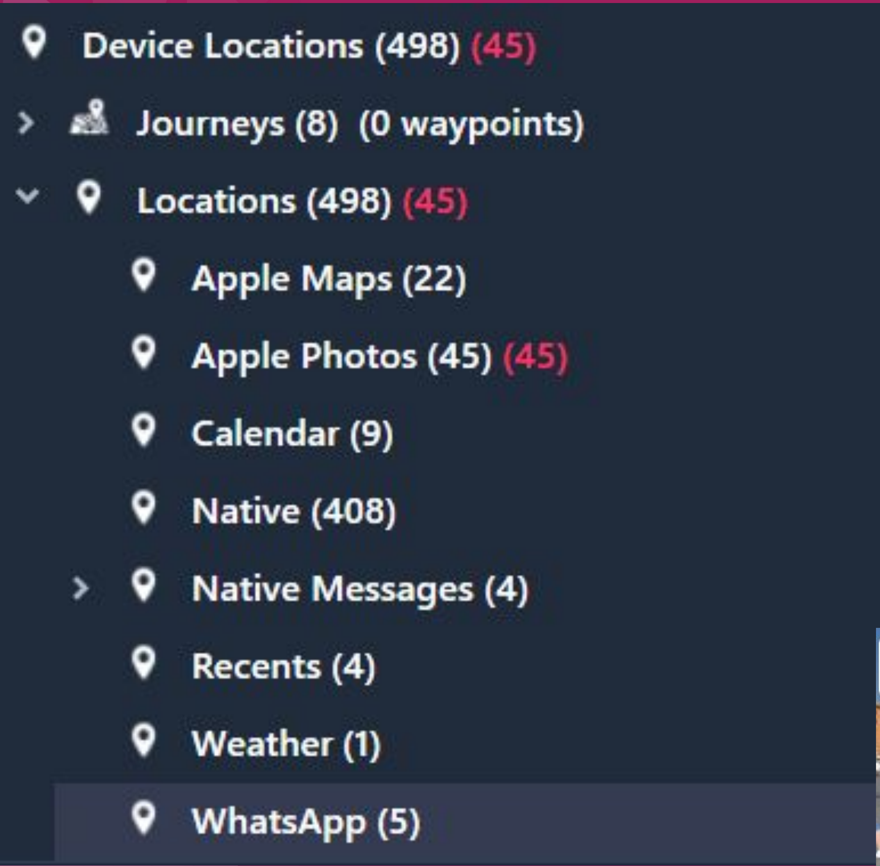
1) I am an expert in forensic analysis of mobile devices
2) I extracted geolocation data from the mobile device
3) The geolocation data was generated on the mobile device
4) Therefore, the device was at the given location

INCORRECT: presents interpretation as fact

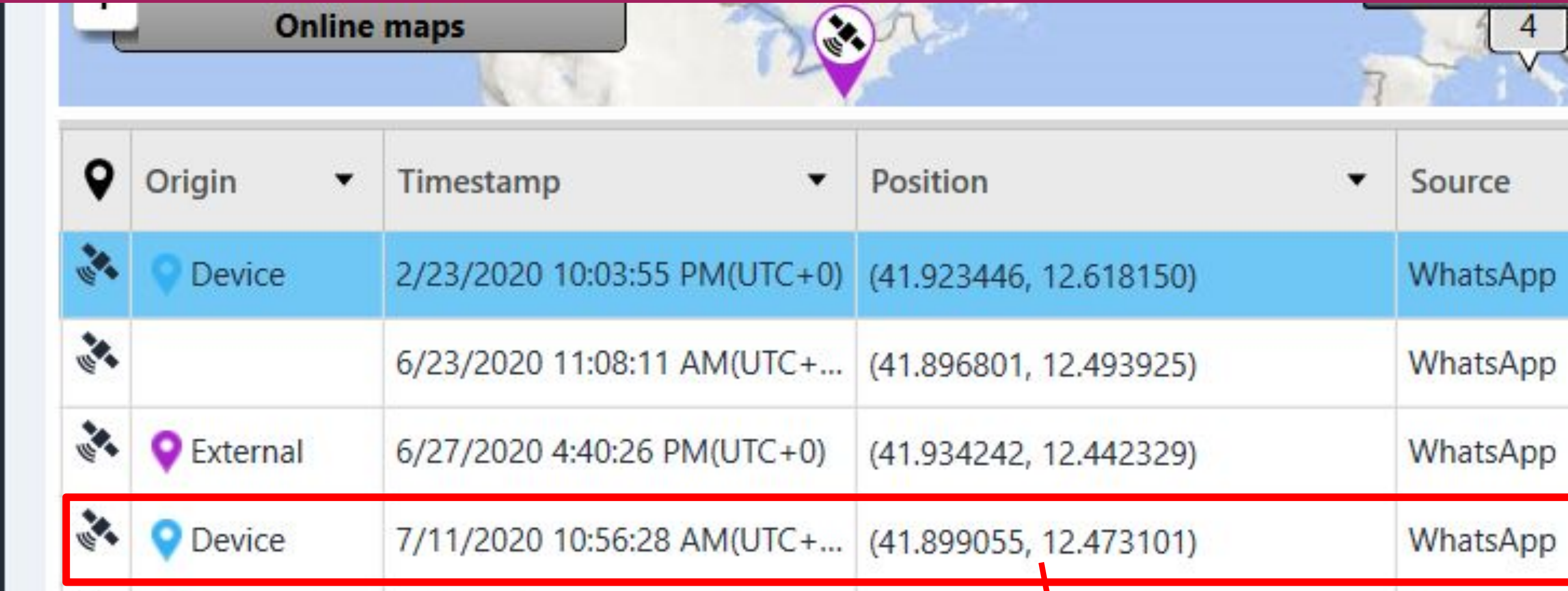
Are there any alternative hypotheses?

UNIL | Université de Lausanne
Ecole des sciences criminelles

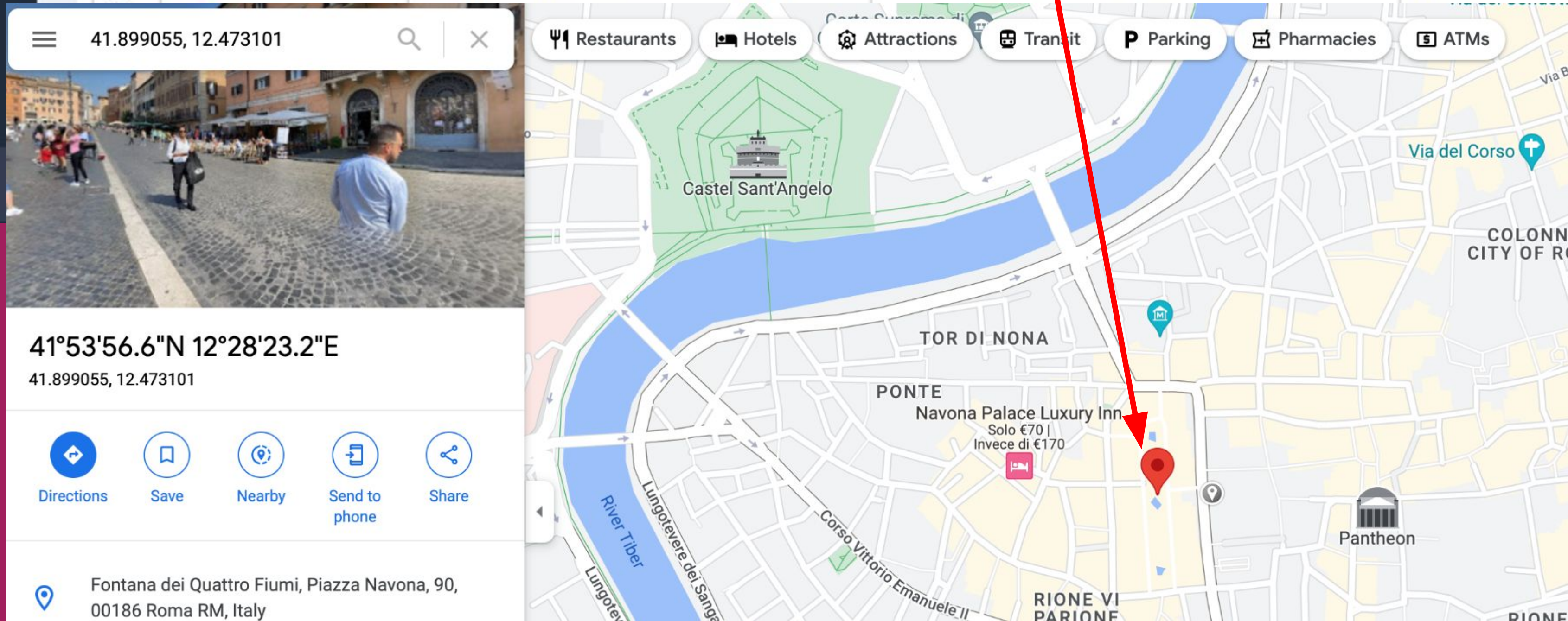
Audience Poll: Where was device on 7/11/20 ?



- Device Locations (498) (45)
- Journeys (8) (0 waypoints)
- Locations (498) (45)
  - Apple Maps (22)
  - Apple Photos (45) (45)
  - Calendar (9)
  - Native (408)
  - Native Messages (4)
  - Recents (4)
  - Weather (1)
  - WhatsApp (5)



	Origin	Timestamp	Position	Source
	Device	2/23/2020 10:03:55 PM(UTC+0)	(41.923446, 12.618150)	WhatsApp
		6/23/2020 11:08:11 AM(UTC+...	(41.896801, 12.493925)	WhatsApp
	External	6/27/2020 4:40:26 PM(UTC+0)	(41.934242, 12.442329)	WhatsApp
	Device	7/11/2020 10:56:28 AM(UTC+...	(41.899055, 12.473101)	WhatsApp



41.899055, 12.473101

41°53'56.6"N 12°28'23.2"E
41.899055, 12.473101

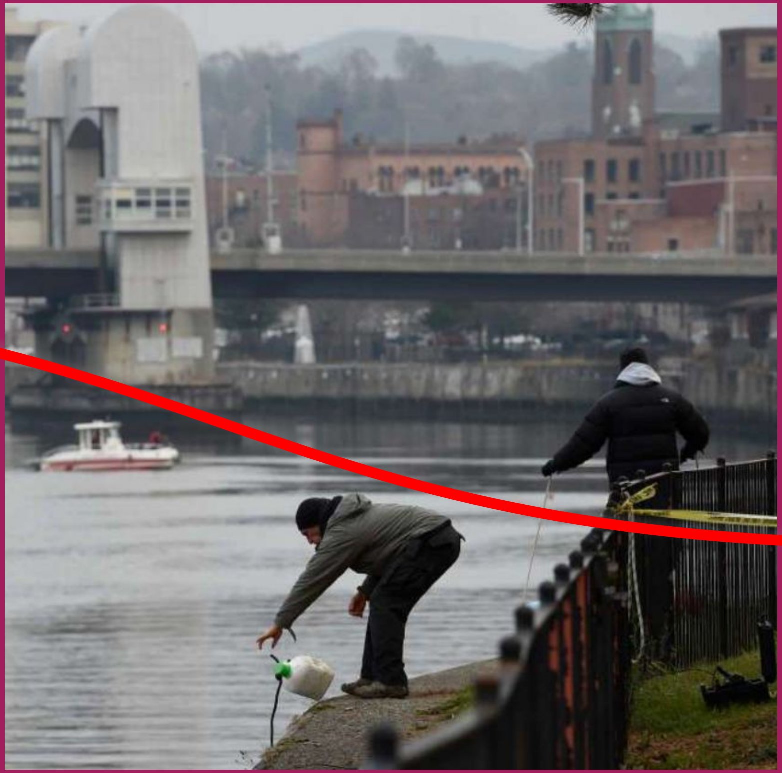
Fontana dei Quattro Fiumi, Piazza Navona, 90, 00186 Roma RM, Italy

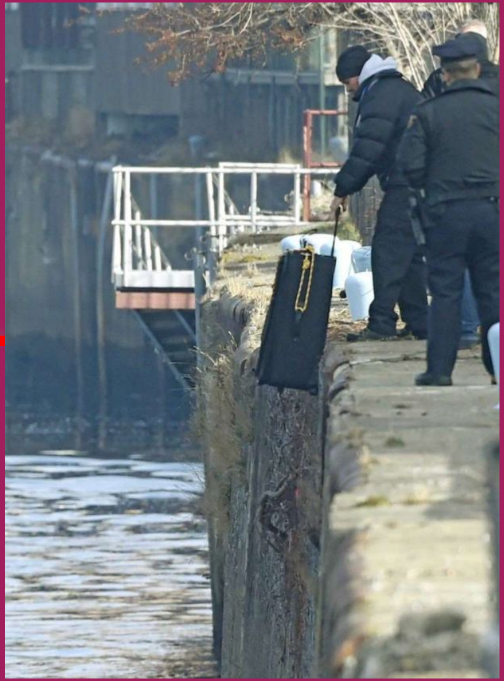
1) In Piazza Navona
2) At another location
3) More A/1 than B/2

Google Location Services

COURT: **“[prosecution] failed to meet their burden of demonstrating that the science underlying Google location services has gained general acceptance in the in the relevant scientific community.”**

?





Oquendo’s attorney: “We're just asking for the courtroom to determine if this is good science”

Body of Noel Alkaramla found inside a suitcase

Warning: Misinterpreting Timestamps

- Timestamps
  1. I am an expert in forensic analysis of computers
  2. I extracted file system data with creation dates
  3. The creation date was generated on a the computer
  4. Therefore, the file was created at that time

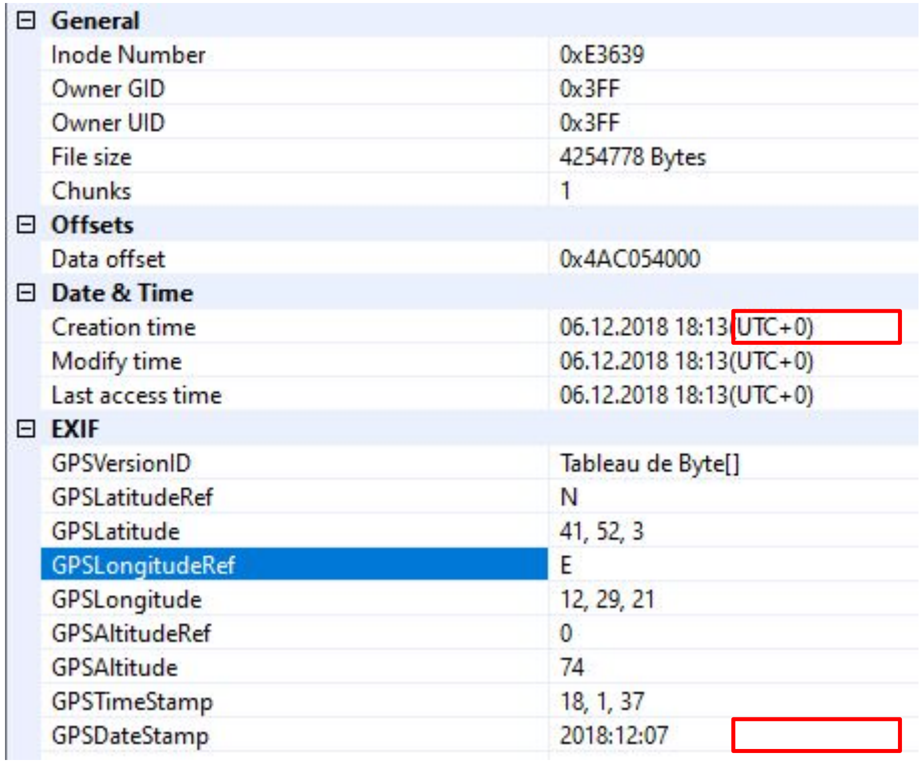
  - Observation: the file creation timestamp is 2 Dec 2024
  - Interpretation: the file was created on 2 Dec 2024

- What are some alternative hypotheses?

Exif Temporal Incongruities

Device timestamp: December 6

GPS timestamp: December 7



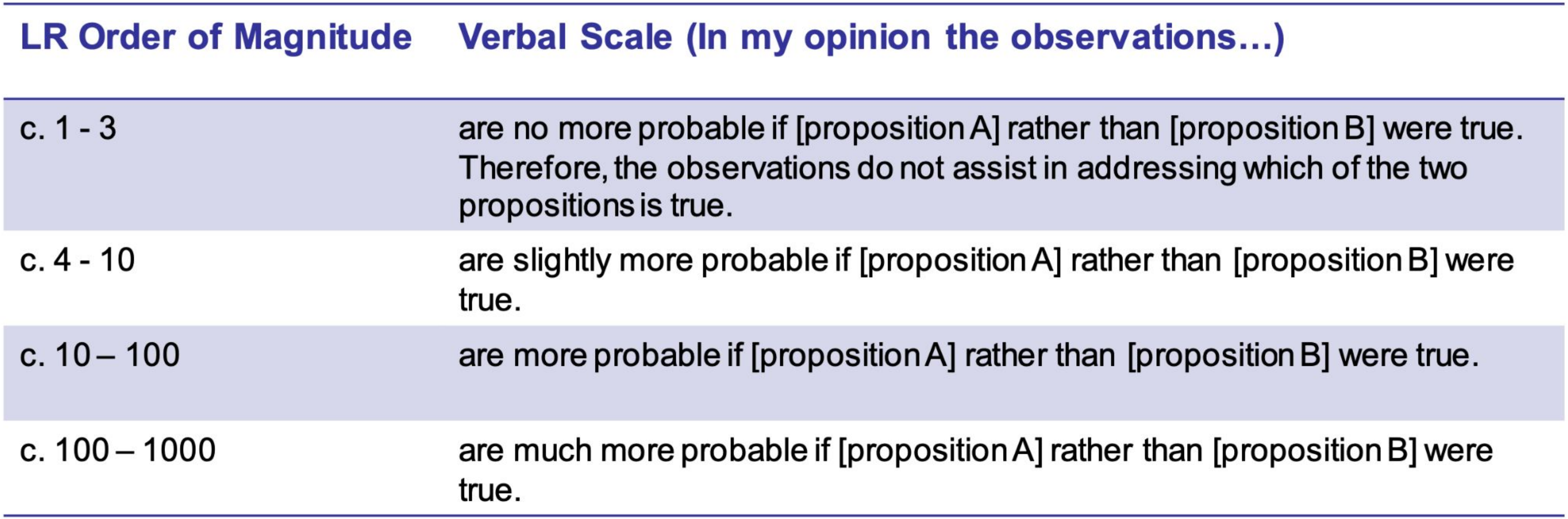
General	
Inode Number	0xE3639
Owner GID	0x3FF
Owner UID	0x3FF
File size	4254778 Bytes
Chunks	1
Offsets	
Data offset	0x4AC054000
Date & Time	
Creation time	06.12.2018 18:13(UTC+0)
Modify time	06.12.2018 18:13(UTC+0)
Last access time	06.12.2018 18:13(UTC+0)
EXIF	
GPSVersionID	Tableau de Byte[]
GPSLatitudeRef	N
GPSLatitude	41, 52, 3
GPSLongitudeRef	E
GPSLongitude	12, 29, 21
GPSAltitudeRef	0
GPSAltitude	74
GPSTimeStamp	18, 1, 37
GPSDateStamp	2018:12:07

Reminder: Case Assessment & Interpretation

Stage	Activities
1. Observation	**Make initial observations**
2. Hypothesis generation	**Generate a set of plausible hypotheses** (initial observations, case circumstances)
3. Inference to the best explanation	**Rank the hypotheses** (initial observations, current knowledge, past experience)
4. Prediction of likely observations	**Predict likelihoods for the range of possible future observations** (postulating that each of the hypotheses were true)
5. “Second Phase” observation	**Search for predicted likely observations**
6. Strength of evidence assignation	**Assign likelihood values to the observed digital evidence** (in light of each hypothesis / proposition)
7. Communication	**Express evaluative opinions**

UK FSR 118 - Evaluative Opinions

Principles: Balance, logic, robustness, transparency



LR Order of Magnitude	Verbal Scale (In my opinion the observations…)
c. 1 - 3	are no more probable if [proposition A] rather than [proposition B] were true. Therefore, the observations do not assist in addressing which of the two propositions is true.
c. 4 - 10	are slightly more probable if [proposition A] rather than [proposition B] were true.
c. 10 – 100	are more probable if [proposition A] rather than [proposition B] were true.
c. 100 – 1000	are much more probable if [proposition A] rather than [proposition B] were true.

Avoid Reporting Pitfalls

- ✘ Do not make conclusory statements
  - ✗ the SUBJECT did ABC
  - ✗ the person in the photo is the VICTIM
  - ✗ the video contains child pornography

- ✘ Do not make vague statements about uncertainty
  - ✗ seems to be ABC
  - ✗ appears to be ABC
  - ✗ could be ABC

Avoid Obscured Inferences

“I have performed data extraction using the tools set out in table 2 and obtained the observations in table 2. There were no communications between Mr X and Mr Z.”

- This statement could be read as a series of facts
- However, this is an obscured inference:
  1. The assertion being made is that there were no communications between Mr X and Mr Z
  2. The person making the assertion knows only that their extraction and analysis procedures did not find any communications between Mr X and Mr Z,
  3. Therefore, the assertion that there were none does not come within the definition of fact.

(Adapted from FSR-C-118 Issue 1, February 2021)

Inferring activity from observed traces

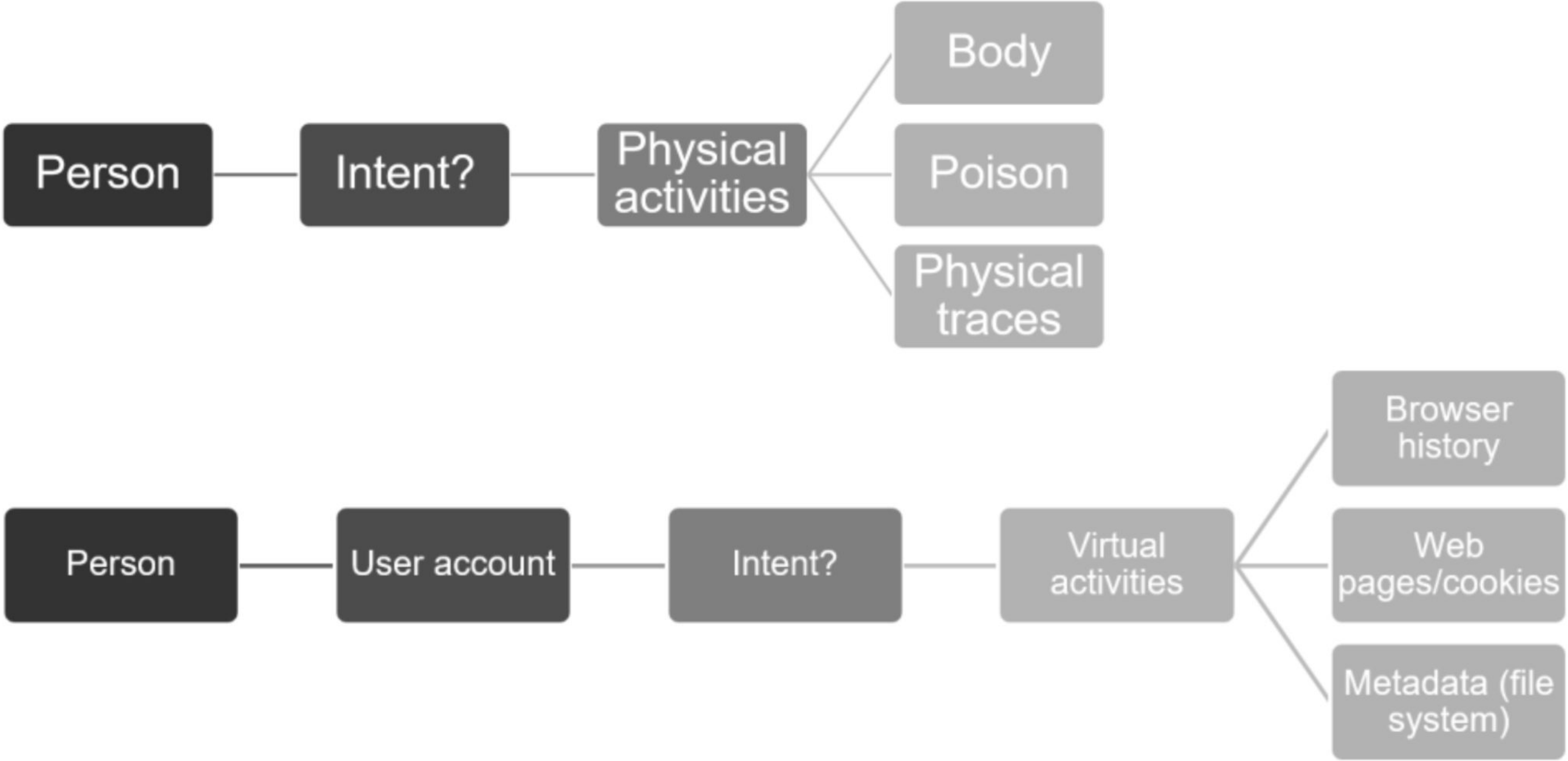
Fact or interpretation?

- Considered together, the observed traces resulted from user account “JD” opening each of the photos and copying the files to external storage media.
- Considered together, the observed Web history and downloaded files resulted from user account “JD” searching for “make a bomb,” visiting each of the websites and downloading bomb making instructions.

Reminders

- Evaluate the observations, not imagined possibilities
  - New observations may change evaluation
- Audience is a non-specialist (ex. judge, decision-maker)
  - They do not have expertise to evaluate traces
  - They need clearly expressed evaluation of traces
  - They understand verbal better than numbers
- Numerical evaluation is more precise than verbal
  - LR scale has verbal equivalent
  - C-Scale has verbal equivalent
- Copy the language in the scale, do not tweak
  - Do not transpose the conditional

Inferring Intent from Digital Evidence



Person

Intent?

Physical activities

Body

Poison

Physical traces

Person

User account

Intent?

Virtual activities

Browser history

Web pages/cookies

Metadata (file system)

Misinterpretation of Backdating

- Statement of certainty
  - User X backdated system on 18 November 2018
- Not expressed in relative terms
  - H1 highly probable. H2 low probability. H3 improbable.
- Microsoft Windows file tunneling
  - New content saved with old metadata
  - No trace of deliberate user action

C-Scale: Strength of Digital Evidence

Evaluate evidence in light of each hypothesis

C-Value	Illustrative Indicators
C0	Evidence contradicts known facts (extreme dissonance of observations in light of the hypothesis).
C1	Evidence is highly questionable (very strong dissonance of observations in light of the hypothesis).
C2	Only one source of evidence that is not difficult to tamper with.
C3	The source(s) of evidence are more difficult to tamper with but there is not enough evidence to support a firm conclusion or there are unexplained inconsistencies (dissonance) in the observed evidence in light of the hypothesis.
C4	The source(s) of evidence are much more difficult to tamper with evidence from multiple, independent sources (strong harmonious observations in light of the hypothesis).
C5	The source(s) of evidence are very much more difficult to tamper with and evidence from multiple, independent sources (very strong harmonious observations in light of the hypothesis). However, small uncertainties exist (e.g. temporal error, data loss).
C6	The evidence is tamper proof (or tamper evident) and extremely strong harmonious evidence in light of the hypothesis unquestionable.