



Universität Augsburg
Fakultät für Angewandte
Informatik

Evaluating Tamper Resistance of Digital Forensic Artifacts during Event Reconstruction

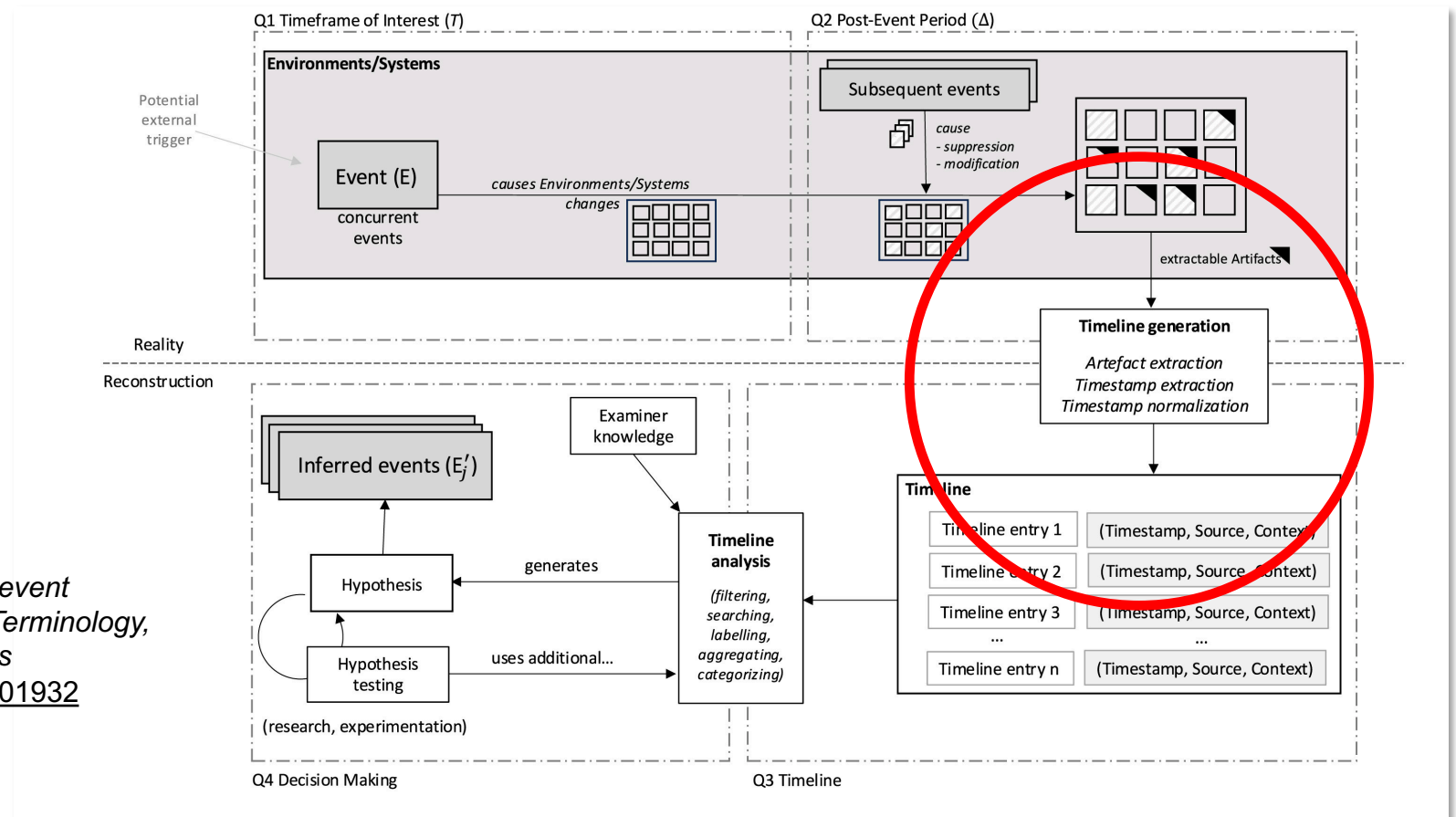
Céline Vanini (University of Lausanne, CH)
Chris Hargreaves (University of Oxford, UK)
Frank Breiter (University of Augsburg)

Event Reconstruction

What do we mean by it?

Fundamental phase in digital forensic investigations where examiners attempt to answer the questions of **who, what, when, whom/what with, where, and how** after a crime or incident occurred

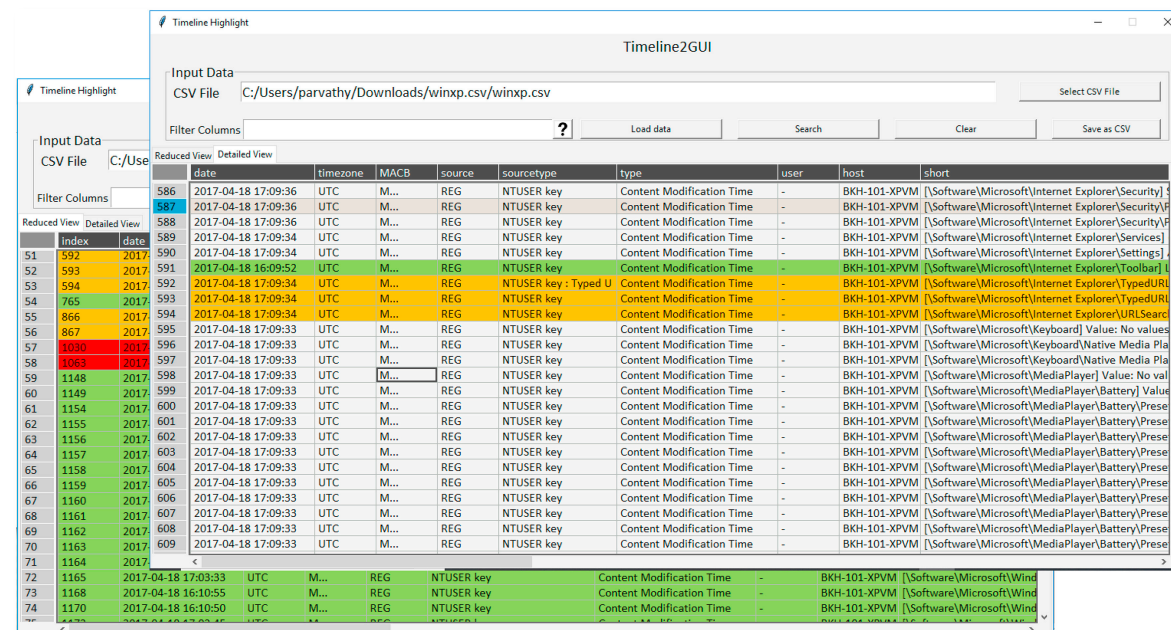
Diagram from SoK: *Timeline based event reconstruction for digital forensics: Terminology, methodology, and current challenges*
<https://doi.org/10.1016/j.fsidi.2025.301932>



Timeline generation

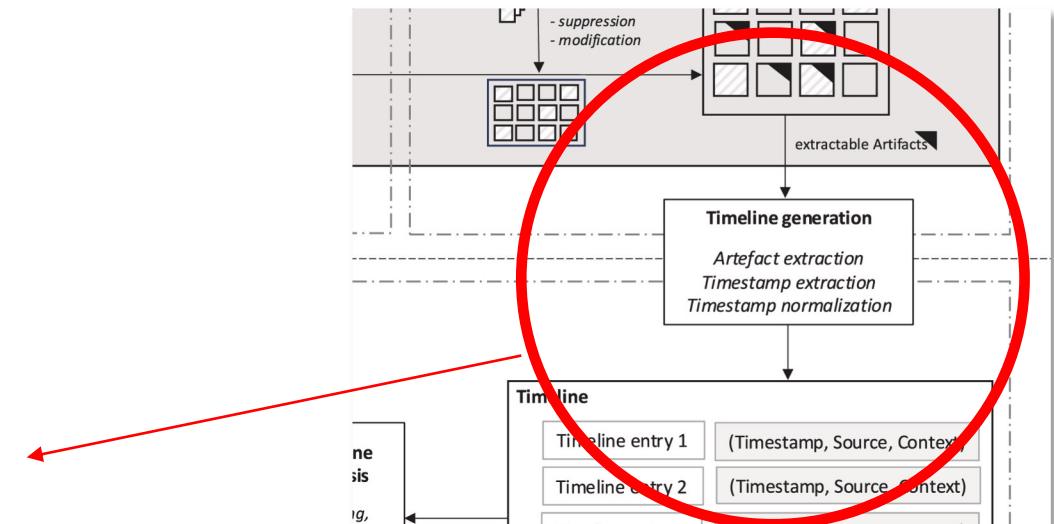
Event reconstruction != timelines

Reconstruction process often starts with the **creation of a timeline** using automatic tools (e.g., Plaso) that extract information contained (e.g., file system, application-related files) and then chronologically organize the data from these different sources.



The screenshot shows the Timeline2GUI application window. The 'Input Data' section shows a CSV file 'C:/Users/parvathy/Downloads/winxp.csv/winxp.csv' loaded. Below this is a table with columns: date, timezone, MACB, source, sourcetype, type, user, host, and short. The table contains multiple rows of event data, including timestamps, timezones, MACB values, sources, sourcetypes, types, users, hosts, and short descriptions.

	date	timezone	MACB	source	sourcetype	type	user	host	short
586	2017-04-18 17:09:36	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\Internet Explorer\Security]
587	2017-04-18 17:09:36	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\Internet Explorer\Security]
588	2017-04-18 17:09:36	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\Internet Explorer\Security]
589	2017-04-18 17:09:34	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\Internet Explorer\Services]
590	2017-04-18 17:09:34	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\Internet Explorer\Settings]
591	2017-04-18 16:09:52	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\Internet Explorer\Toolbar]
592	2017-04-18 17:09:34	UTC	M...	REG	NTUSER key - Typed U	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\Internet Explorer\TypedURL]
593	2017-04-18 17:09:34	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\Internet Explorer\TypedURL]
594	2017-04-18 17:09:34	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\Internet Explorer\URLSearch]
595	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\Keyboard] Value: No values
596	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\Keyboard\Native Media Pla
597	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\Keyboard\Native Media Pla
598	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\MediaPlayer] Value: No val
599	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\MediaPlayer\Battery] Value
600	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\MediaPlayer\Battery]Pres
601	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\MediaPlayer\Battery]Pres
602	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\MediaPlayer\Battery]Pres
603	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\MediaPlayer\Battery]Pres
604	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\MediaPlayer\Battery]Pres
605	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\MediaPlayer\Battery]Pres
606	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\MediaPlayer\Battery]Pres
607	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\MediaPlayer\Battery]Pres
608	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\MediaPlayer\Battery]Pres
609	2017-04-18 17:09:33	UTC	M...	REG	NTUSER key	Content Modification Time	-	BKH-101-XPVM	[Software\Microsoft\MediaPlayer\Battery]Pres



Problem description

Prior research has often concentrated on methods to reduce timeline complexity, such as filtering, labeling, and aggregation

But what if someone tampers with the artifacts?

Can lead to incorrect ordering, aggregation, or filtering of entries, contradicting information → leading to substantial errors in interpretation

Good news: Several studies show that tampering is difficult (causing subsequent changes) → can be identified

CAS 2020/O/6689

World Anti-Doping Agency v.
Russian Anti-Doping Agency

38.4 Files in the LIMS database dating back to 2012, 2013, 2014, and 2015 were deleted or altered on 6 January 2019.

38.5 On 8 January 2019, the System Administrator issued a command to back-date the LIMS system to 23 May 2015. While the system was back-dated, he replaced the LIMS database with a prior version of the database (a back-up file purportedly dated 21 December 2018), and deleted 623 database files from nine folders, including folders labelled 2012-2015. He also used a specialised software tool (which has to be downloaded from the Internet and installed on the machine) to back-date the timestamps on the associated database files to 23 May 2015, and he used automated scripts to alter the LIMS database and to back-date multiple databases and associated files to various dates. According to WADA I&I, the effect was to give 'the erroneous and fraudulent impression' that the back-up version of the database that was restored onto the LIMS system on 8 January 2019 (which was the version made available to WADA for copying) had been on the LIMS system since 23 May 2015. The System Administrator then deleted the scripts containing these back-dating and altering commands.

source: https://www.tas-cas.org/fileadmin/user_upload/CAS_Award_6689.pdf

Why should you read the article?

Contributions

We evaluate the relative tamper resistance of different artifacts (data sources)

1. We assess the **resilience of artifacts** by providing an extensive discussion of factors that may affect their resistance to any active modifications and/or deletions in a contextual manner

2. We propose a **scoring system** that can be used to support the evaluation

- Article illustrates the use of the scoring with a set of case study examples

We also provide an EXCEL sheet!

	A	B	C	D
1	Example Event Reconstruction: [example name]			
2				
3		Factor	Discussion and category	Score
4		User visible	<input type="text"/>	#N/A
5		Permissions	<input type="text"/>	#N/A

FACTORS

Factors

- *Factors = characteristics* that influence **resistance to tampering**
- Help examiners judge resilience & assign confidence
- Arise from technical (OS, file format) + contextual (access, tools) aspects
- **Seven key factors** which are discussed over the upcoming slides

The idea: the higher the resilience, the more difficult it is to change this artifact

→ If contradicting information is found, it is likely that the artifact with the higher resilience is correct

Methodology for Identifying Factors

Two-pronged approach

Factors Influencing Evidence Manipulation

From Literature:

- Prior studies examined manipulation; did not list challenges directly but we could infer
- Inference revealed key factors:
 - “full access to the image R and were not restricted in any way regarding the tools that could be used to perform the tampering task.” (Freiling and Hösch)
 - **Permission** (extent of access)
 - **Software availability** (tools usable for tampering)

From Own Work & Experience:

- Experimental results highlighted organization of the source as an important factor.

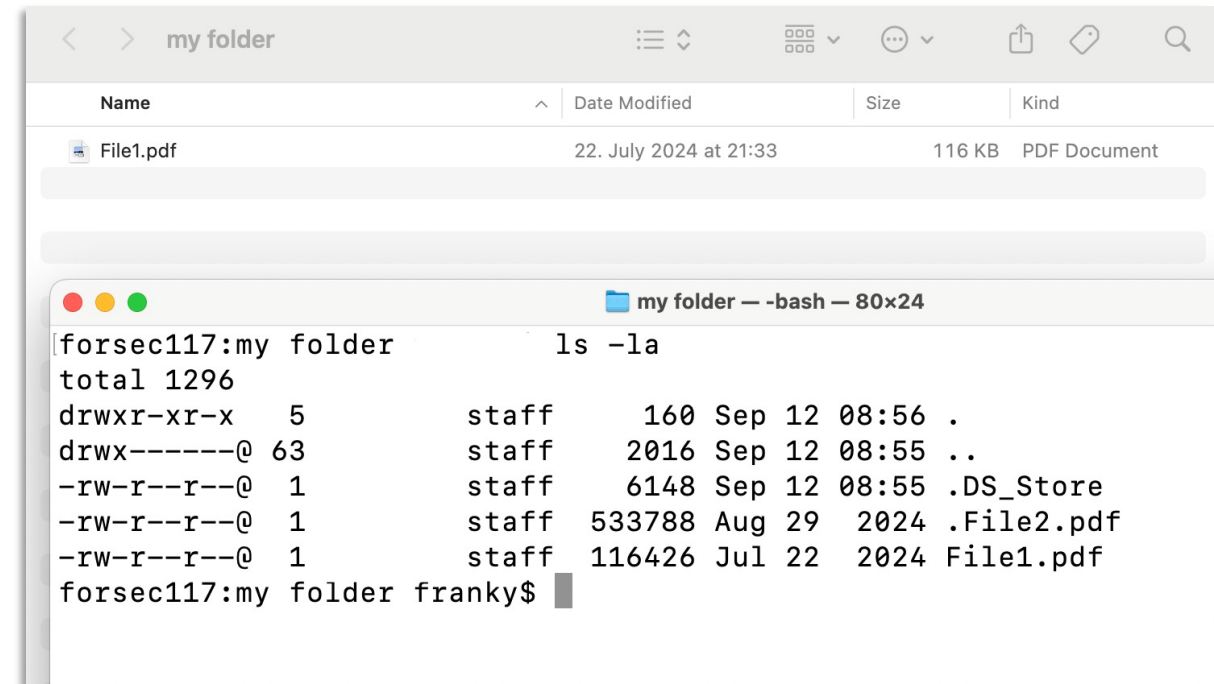
Visibility of the Source to User

Factor 1

Considers whether the source containing the data is visible to the user

Categories into which a source could fall:

- User visible via GUI;
- User visible via other UI method (e.g., terminal);
- Visible via user setting change (enabled);
- Visible via user setting change (not enabled);
- Cannot be made visible.



Examples: A regular file on the desktop, hidden file, files of a different user

Permissions

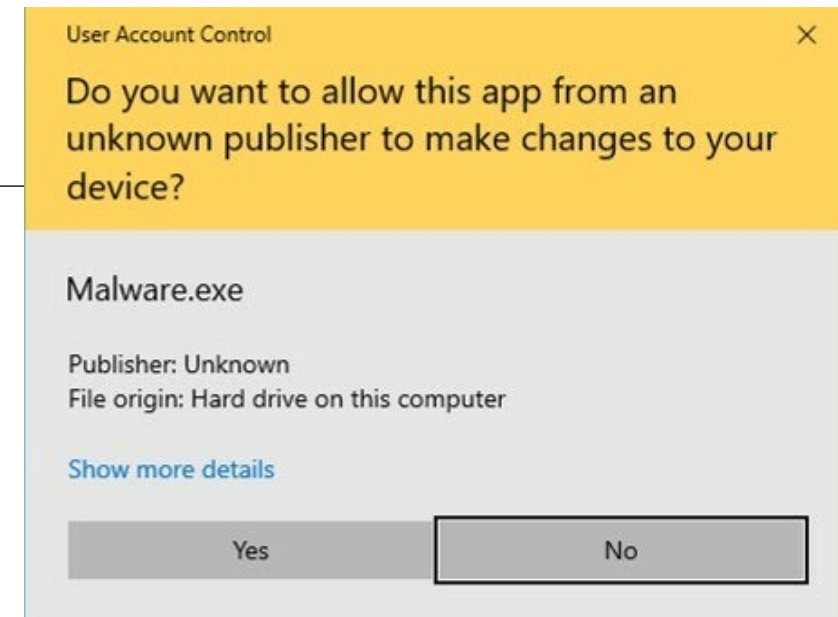
Factor 2

Considers whether permission exists to modify the source

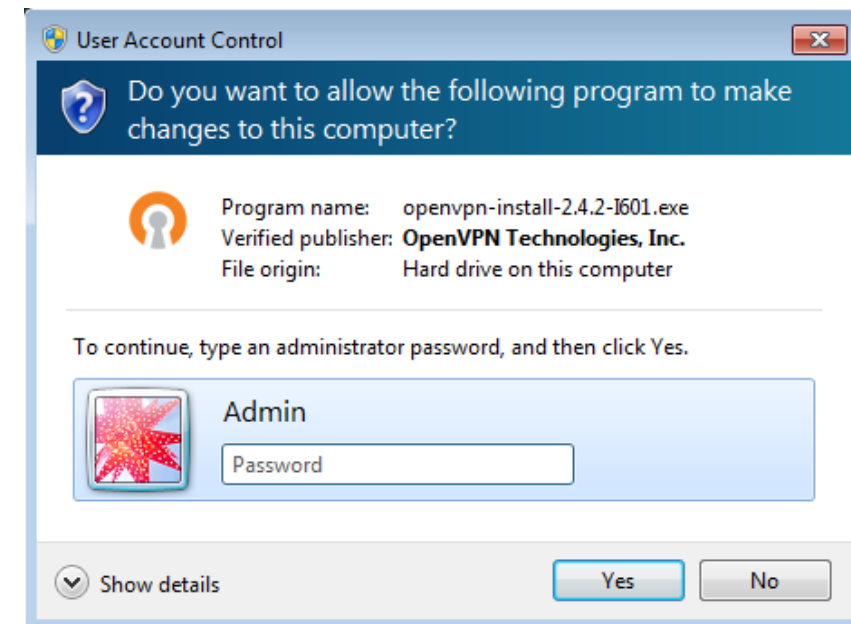
Categories into which a source could fall:

- User accessible;
- User accessible with prompt;
- User accessible with password/biometrics;
- User inaccessible, but observed facets of privilege escalation;
- User inaccessible.

Examples: A regular file on the desktop



source: <https://www.beyondtrust.com/blog/entry/user-account-control-best-practices>



source: <https://security.stackexchange.com/questions/162349/secure-uac-prompt>

Software to Edit on System

Factor 3

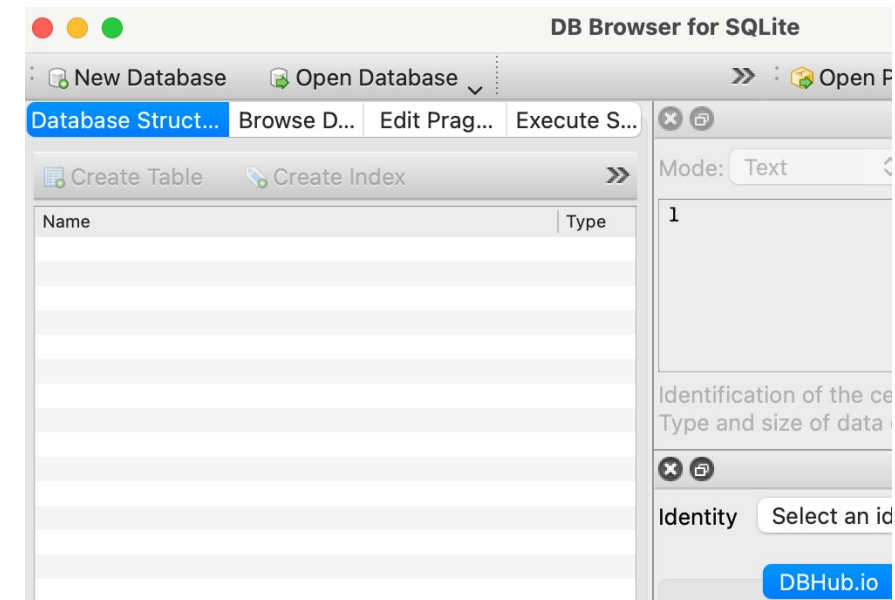
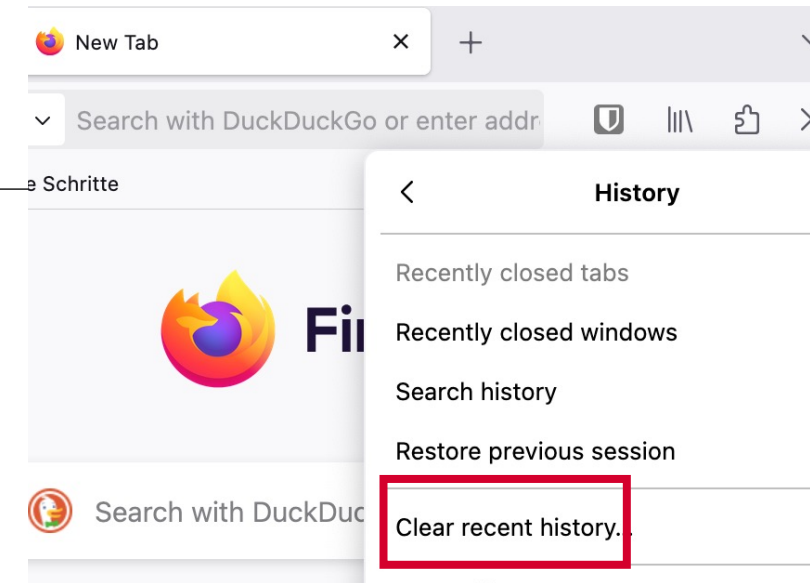
Addresses the ease by which a manipulation can be made.

Categories into which a source could fall:

- Tool available by default for UI-based* editing;
- Tool added to this system for UI-based editing;
- Tool available by default for low-level (hex) editing;
- Tool added to this system for low-level (hex) editing;
- Not on the system.

Examples: DB Browser for SQLite to manipulate DBs

*UI is used rather than GUI as manipulation tools may be a command line.



Observed Facets of Access

Factor 4

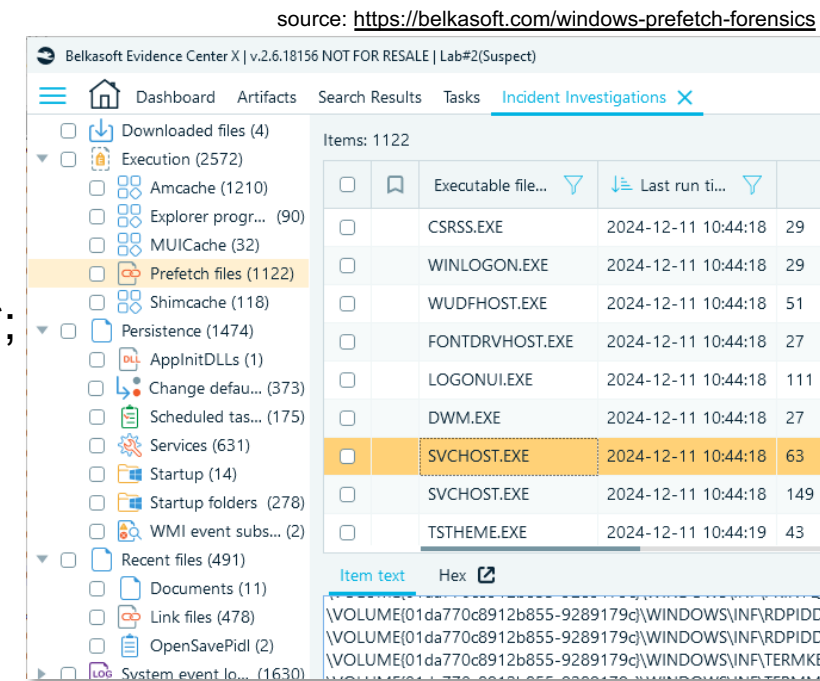
Determine if there are observed facets of actual access to that source

Categories into which a source could fall:

- Observed facets of edit-capable software accessing the specific source*;
- Observed facets of edit-capable software accessing the source*;
- Observed facets of edit-capable software being run;
- No observed facets.

Example: For SQLite database viewers, the recent files list associated with the program may provide evidence of a specific database being accessed; prefetch file shows that software was executed

*specific vs. not specific: registry was accessed vs. a specific registry key/value was accessed.



Encryption

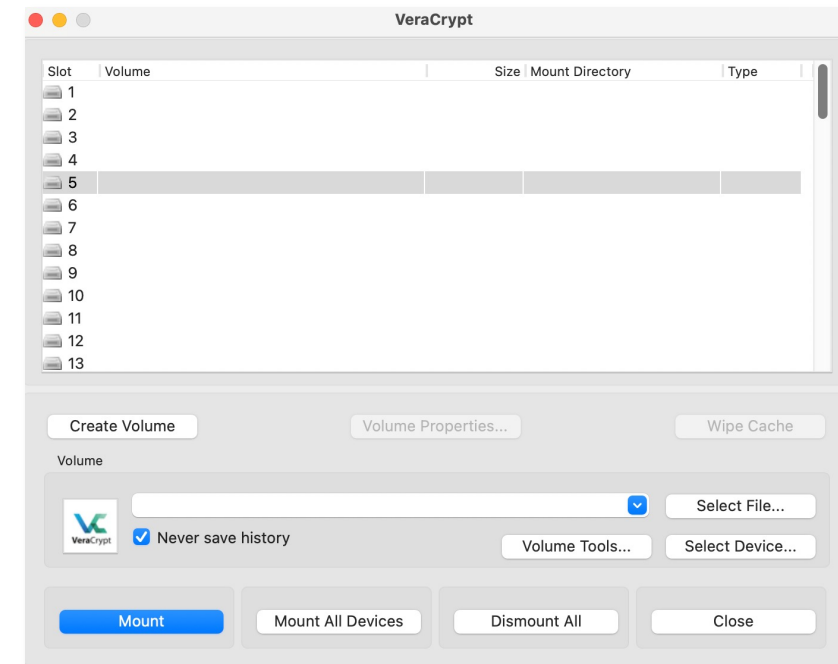
Factor 5

Consideration is if the source in question is encrypted

Categories into which a source could fall:

- No encryption;
- Encrypted but accessible live, e.g., EFS;
- Encrypted but trivial to break, e.g., ROT13 in Windows Registry;
- Encrypted but key recovery possible from local system;
- Encrypted but key stored off device available to user;
- Encrypted but key stored off device not available to user.

Example: encrypted database but the key is stored locally in a json file



(File) Format

Factor 6

The format of a source also impacts its resilience

Categories into which a source could fall:

- Binary proprietary (currently unknown);
- Binary proprietary but reverse-engineered (e.g., MFT);
- Binary open format (e.g., SQLite);
- Text-based machine format (e.g., XML, JSON);
- Plain text;
- NA (GUI edit tool available).

**.gif .jpg .xml .txt
.doc .png .csv .prt
.xls .htm .zip .pp4
.mp3 .css .js .iso
.tif .app**

Organization of the Source

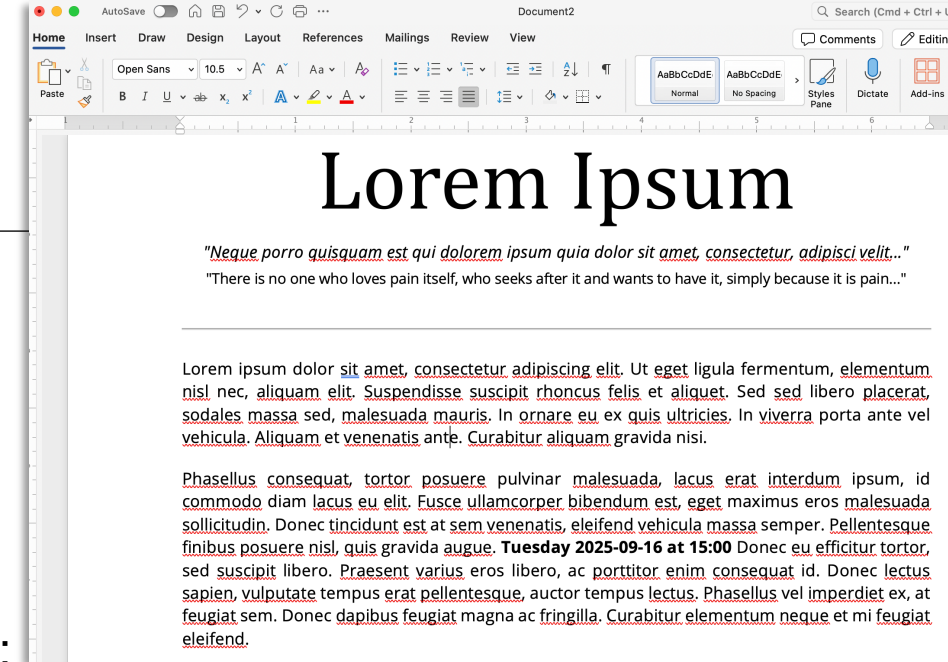
Factor 7

Data within a source is another factor impacting its resilience

Categories into which a source could fall :

- Structured (a timestamp within a known data structure, e.g., MFT);
- Semi-structured (a timestamp that is stored as a field within JSON but as a text string, e.g., “Wed 25th Jan 2022 11:35 am”);
- Unstructured (a reference to date and time of an event within the content of a Word document written by an author)

Example: Modifying EXIF information vs. removing a watermark in images



Scoring

To support the reconstruction process, we assigned scores to the categories of the seven factors expressing the **tampering concern of the source from that factor's perspective**

- reflects how easily an adversary could manipulate the source

Given a source (e.g., Windows Registry) and a factor (e.g., software to edit), we define three degrees of tampering *concern severity*:

- **high (3)** means that there is the highest tampering concern from that factor's perspective (i.e., tampering is easiest);
- **moderate (2)** means that there is a moderate tampering concern;
- **low (1)** means that there is a low tampering concern (i.e., tampering is hardest).

n	Factors	Category	Score
SI Attribute			
1	User visible	Cannot be made visible	1
2	Permissions	User inaccessible	1
3	Software to edit	Tool added to this system for UI-based editing	3
4	Facets of access	Observed facets of edit-capable software being run	2
5	Encryption	No encryption	3
6	File format	NA (UI edit tool available)	3
7	Structural	Structured	2

Demonstration

Spreadsheet can be accessed here: <https://tinyurl.com/wmf7vv2j>

(You must make a copy prior to working on it)

Copy of Tampering Scoring Sheets v0.4 - Shared

File Edit View Insert Format Data Tools Extensions Help

Search Menus 100% Arial 10 B I A

C7 fx

	A	B	C	D	E
1	Example Event Reconstruction:		[example name]		
2					
3		Factor	Discussion and category	Score	Notes
4	artifact 1	User visible		#N/A	
5		Permissions		#N/A	
6		Software to edit		#N/A	
7		Observable traces of access or modifications	I	#N/A	
8		Encryption			
9		File format			
10		Structural			
11					
12					
13					
14					
15					
16					
17					

Observable traces of edit-capable software accessing the specific source (3)

Observable traces of edit-capable software accessing the source (3)

Observable traces of edit-capable software being run (2)

Observable traces of inconsistencies found (2)

No observable traces of source access (1)

Take home messages

- When reconstructing events, it is important to **consider tampering** especially if contradicting information is found.
- The proposed **scoring system** offers an initial structure for assessing **trace reliability**.
 - **Spreadsheet:** <https://tinyurl.com/wmf7vv2j>
- While these factors are obvious to seasoned investigators, there is a need for **formal definitions, categories and examples**, i.e., convert implicit knowledge into explicit, assessable criteria.
 - Digital forensic science

Thank you for your attention!

Contact details

- Frank.Breitinger@uni-a.de
- www.FBreitinger.de

