A discussion of quality/reliability of events for timelines

Céline Vanini

Presentation for the
Women in Forensic Computing Workshop
Bonn

20.03.2023

Women in Forensic Computing
WORKSHOP

UNIL | Université de Lausanne
Ecole des Sciences criminelles

Thank you!


FAU
Friedrich-Alexander-Universität
Erlangen-Nürnberg


WinFC
Women in Forensic Computing
WORKSHOP

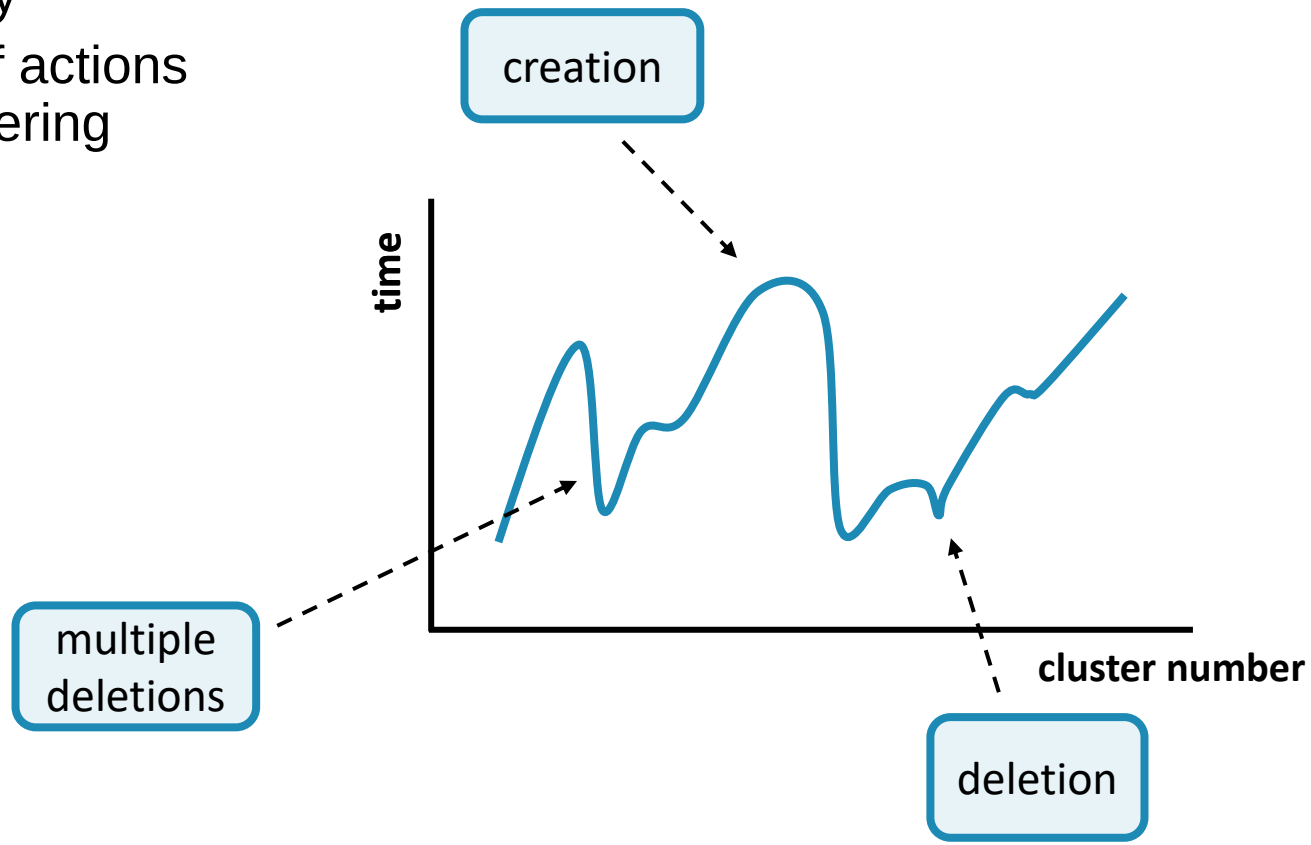
About me

- PhD student (1st year)
- Master’s degree in digital forensic science (UNIL)
- Bachelor’s degree in forensic science (UNIL)

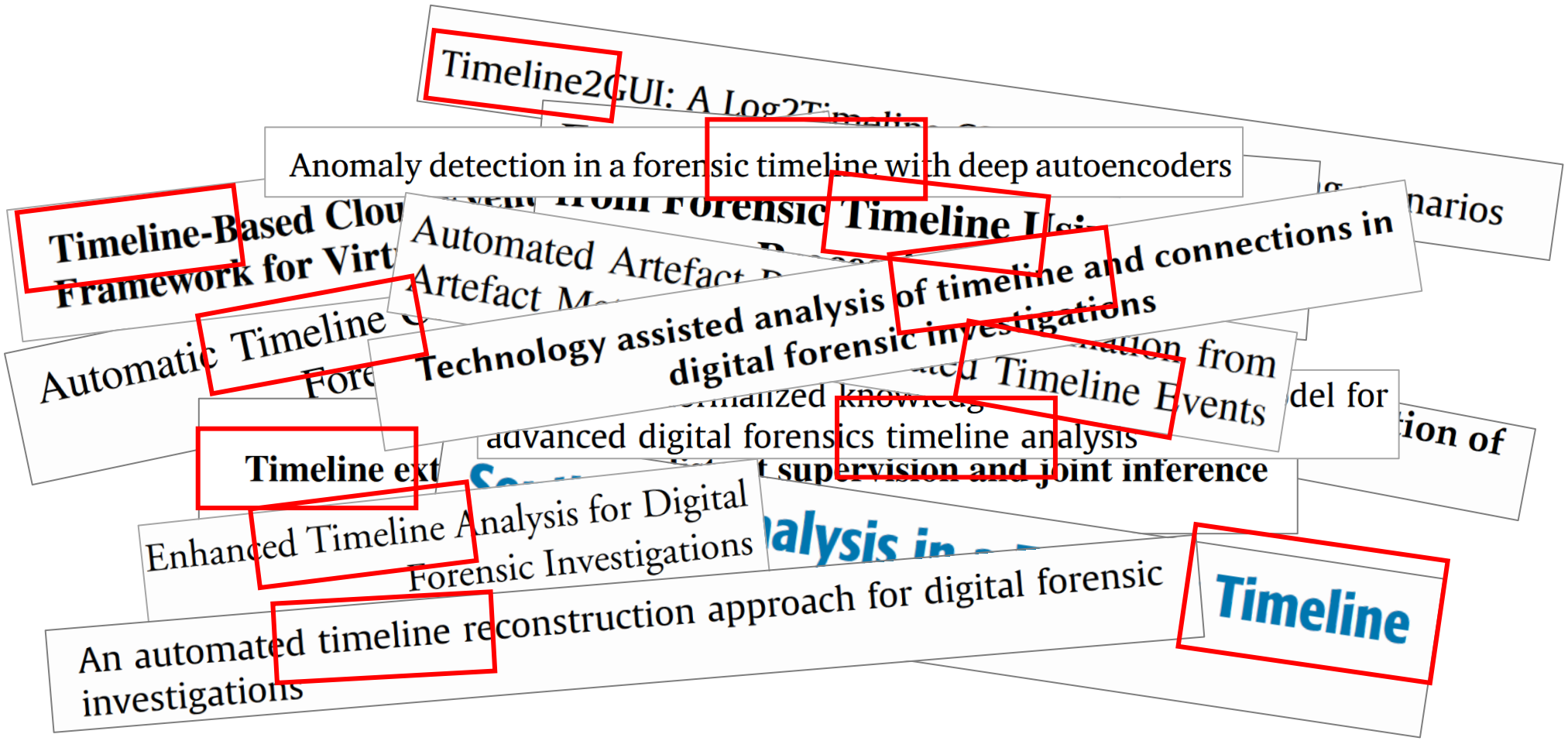
Event reconstruction… but why?

- Research on digital stratigraphy
- Goal: reconstruct sequences of actions on a file system or detect tampering (e.g., backdating) based on the position of files

THIS IS WHAT MAKES DIGITAL FORENSIC SCIENCE SO INTERESTING



Event reconstruction in digital forensic science



Challenges with timelines

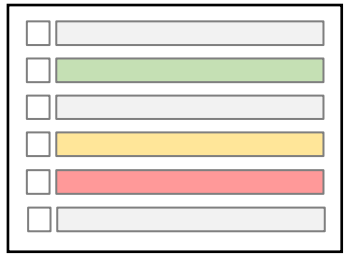
Volume

Heterogeneity

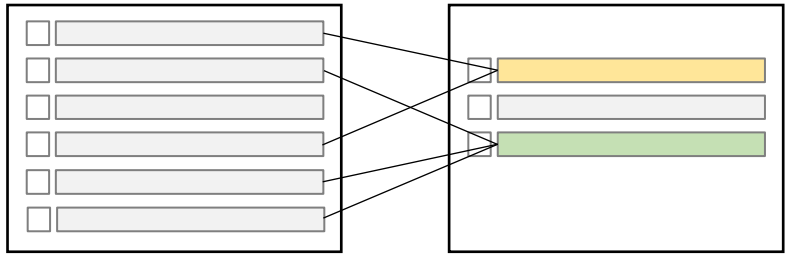
Assessing the volume problem

- Existing approaches…

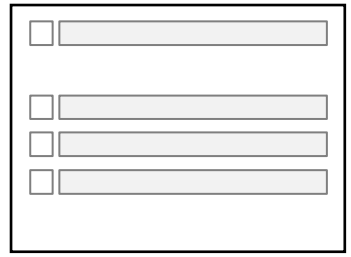
labelling



aggregating

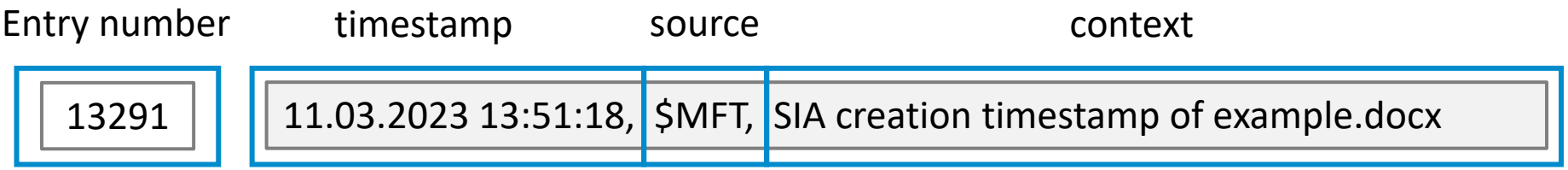


filtering



Reliability?

Example

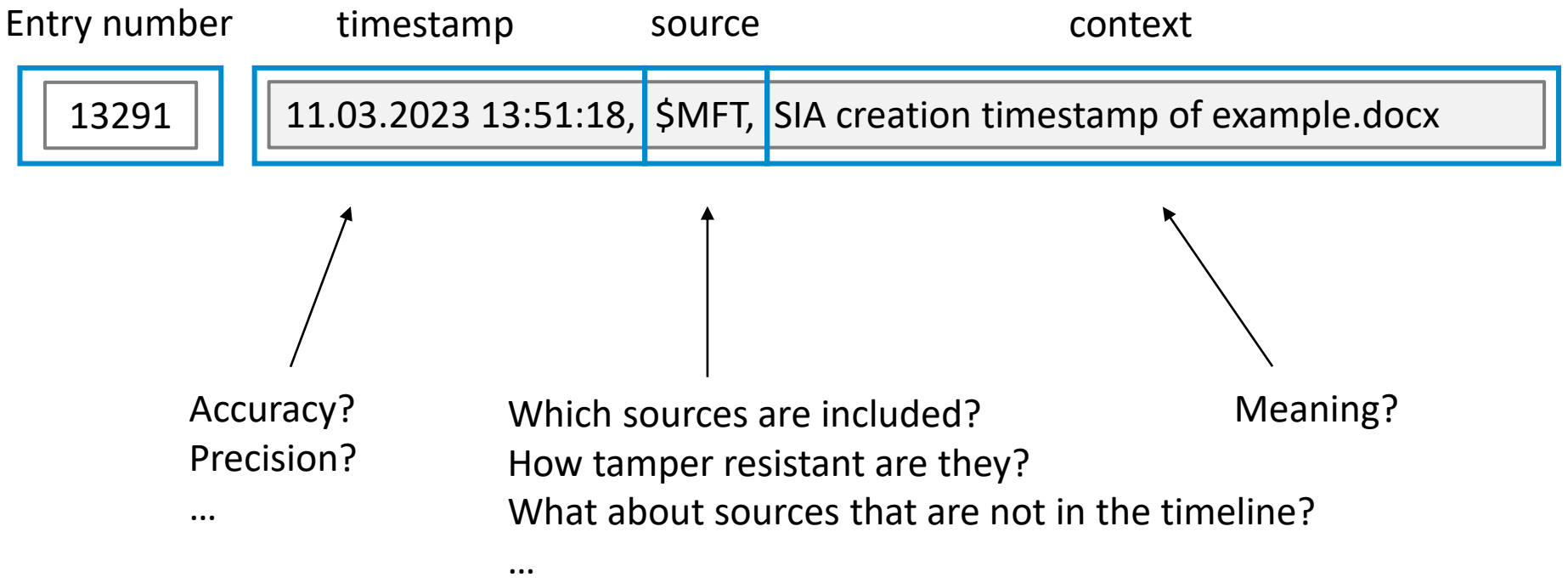

Entry number
timestamp
source
context
13291
11.03.2023 13:51:18,
$MFT,
SIA creation timestamp of example.docx

Example

File copy

9789	10.03.2023 14:23:02,	$MFT, SIA modification timestamp of example.docx
13291	11.03.2023 13:51:18,	$MFT, SIA creation timestamp of example.docx
13292	11.03.2023 13:51:18,	$MFT, SIA MFT entry timestamp of example.docx

How can we evaluate the reliability?



Taking a step back

- Understanding less timelines and more event reconstruction
- Which problems may affect the process of event reconstruction?
- How do they affect the interpretation process?
- How is it usable in practice?
- …

Questions?

Thank you!

Céline Vanini
celine.vanini@unil.ch