A discussion of sources and quality/reliability of events for timelines

Céline Vanini, Chris Hargreaves, Frank Breitinger

Presentation for **DFRWS EU 2023 – Bonn**

23/03/2023

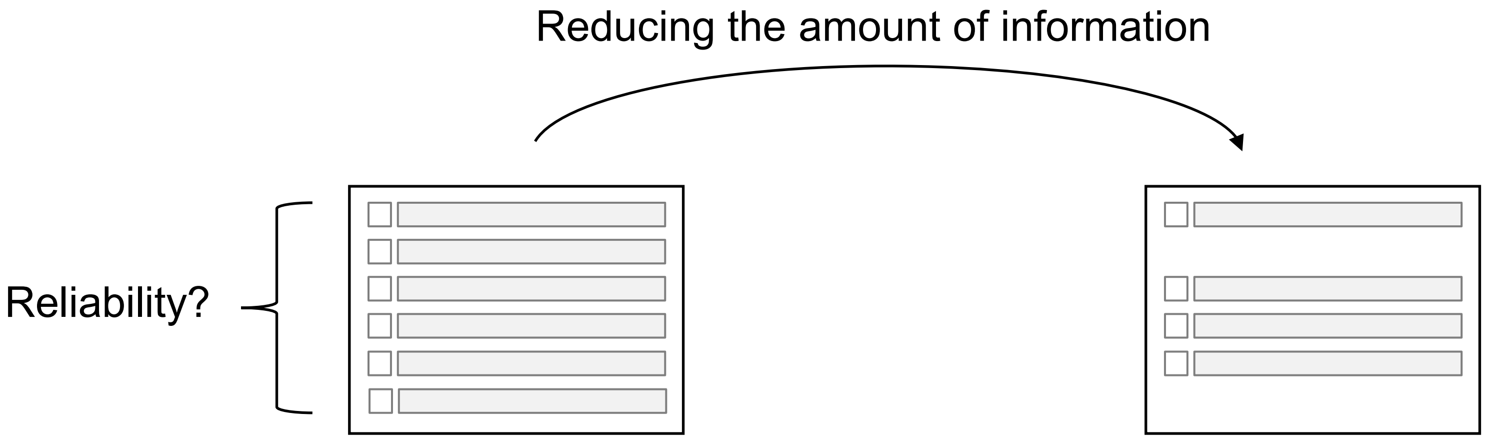
DFRWS
DIGITAL FORENSIC RESEARCH CONFERENCE

UNIVERSITY OF OXFORD

Unil
UNIL | Université de Lausanne
Ecole des Sciences criminelles

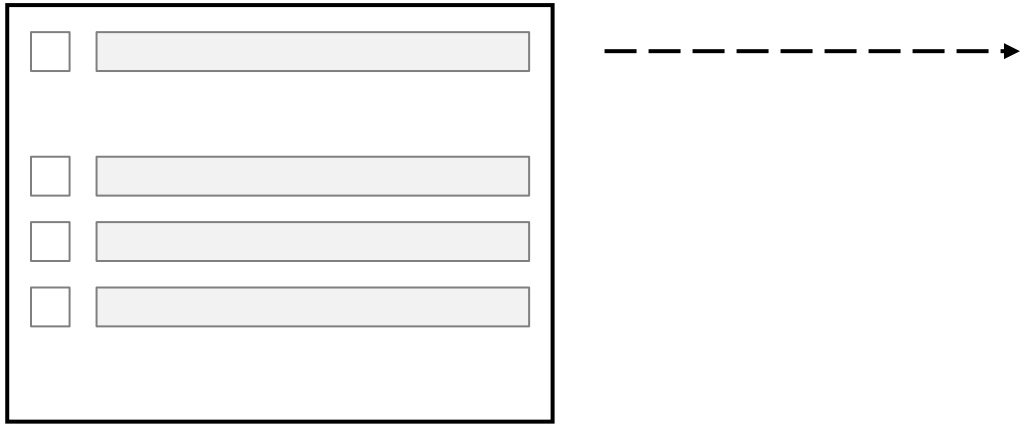
General trends

- Event reconstruction = timeline (analysis)
- What is the general trend?



Let’s see with a simplistic example..

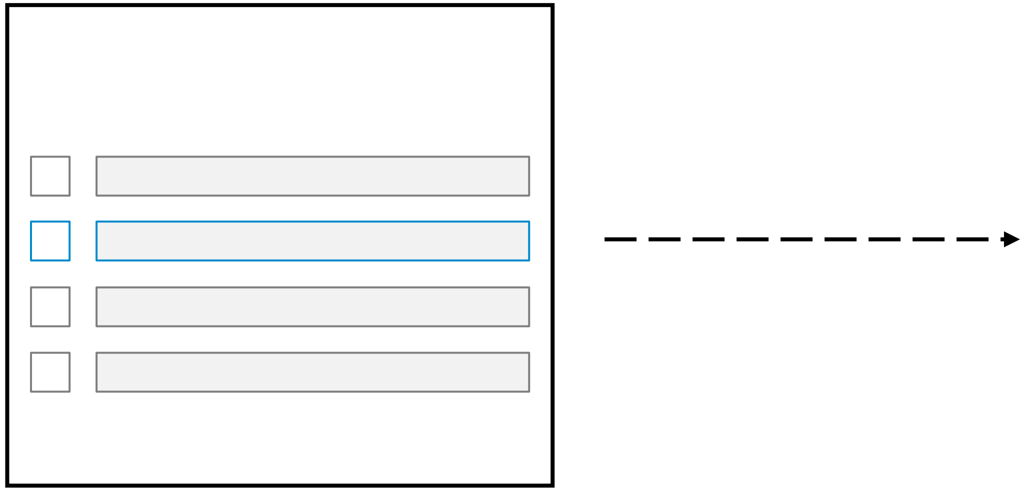
- Filtered timeline:



timestamp was manipulated

Let’s see with a simplistic example..

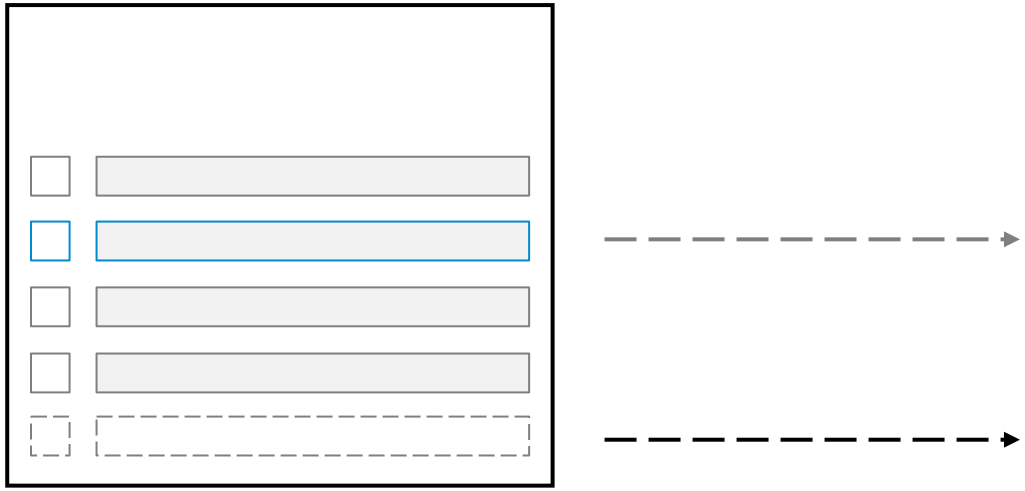
- Filtered timeline:



timestamp was manipulated

Let’s see with a simplistic example..

- Filtered timeline:

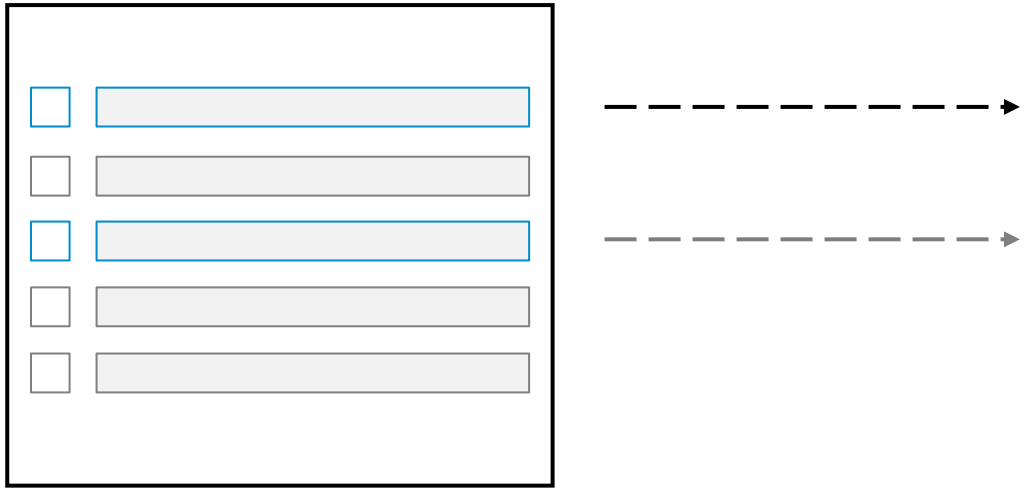


timestamp was manipulated

incorrect time zone

Let’s see with a simplistic example..

- Filtered timeline:

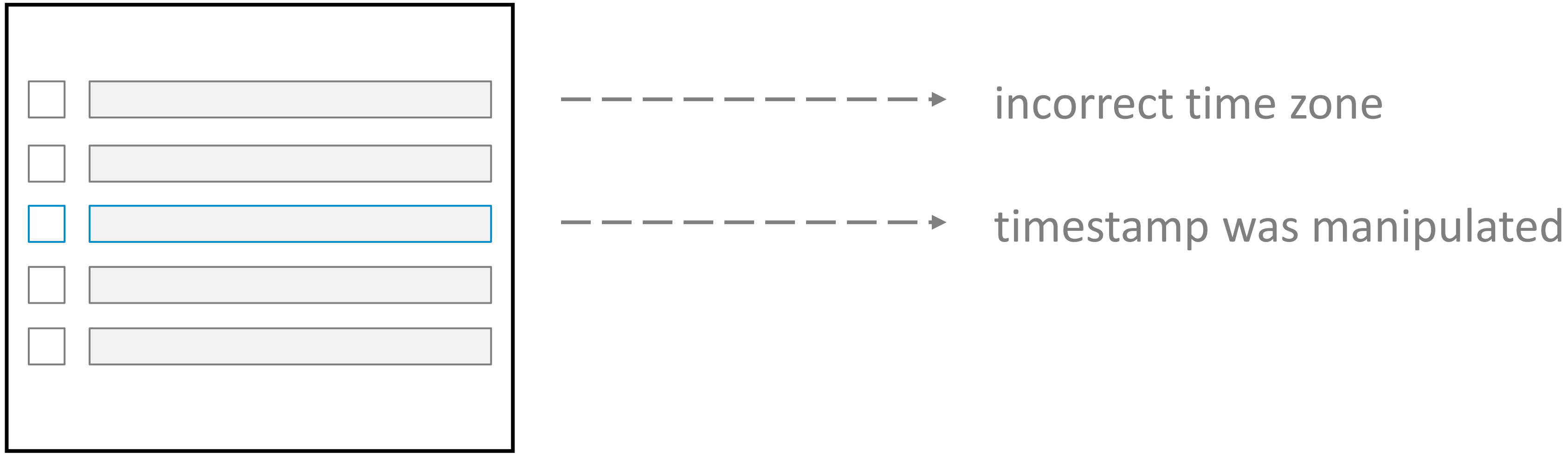


incorrect time zone

timestamp was manipulated

Let’s see with a simplistic example..

- Filtered timeline:



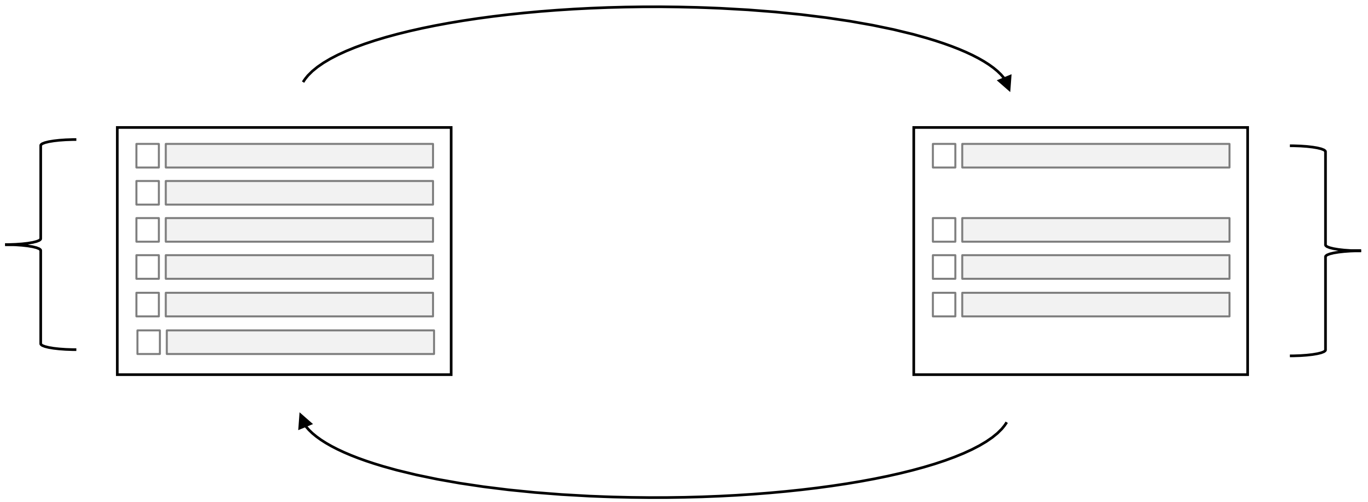
incorrect time zone

timestamp was manipulated

What about sources that are not included in timelines?

Quality/reliability of events for timeline

- Take a step back



Reducing the amount of information

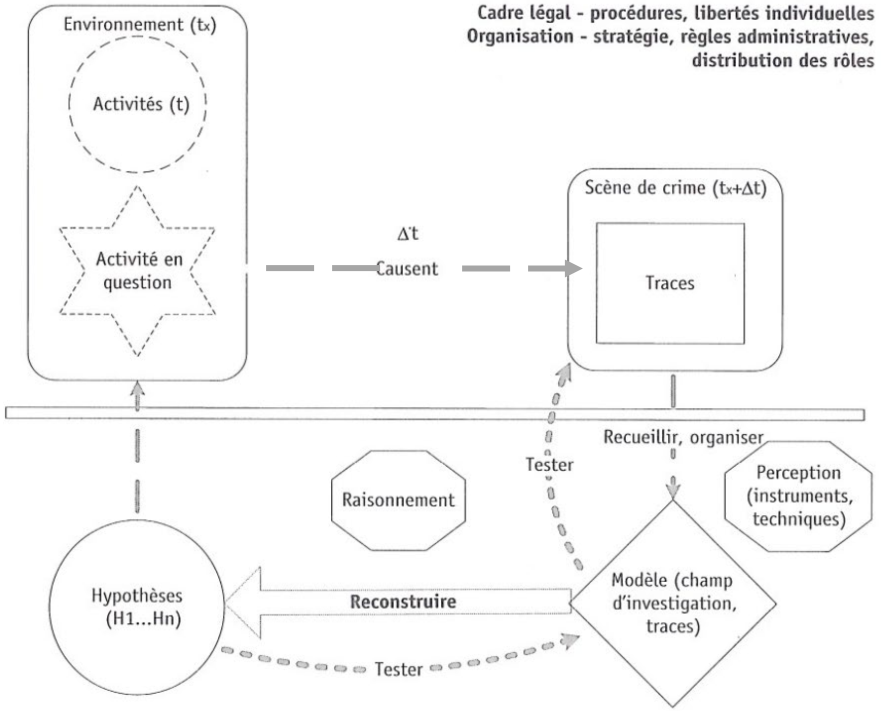
Reliability?

Relevance?
Evaluation?

Which problems could affect the analysis process?
How do they impact the evaluation/interpretation?
…

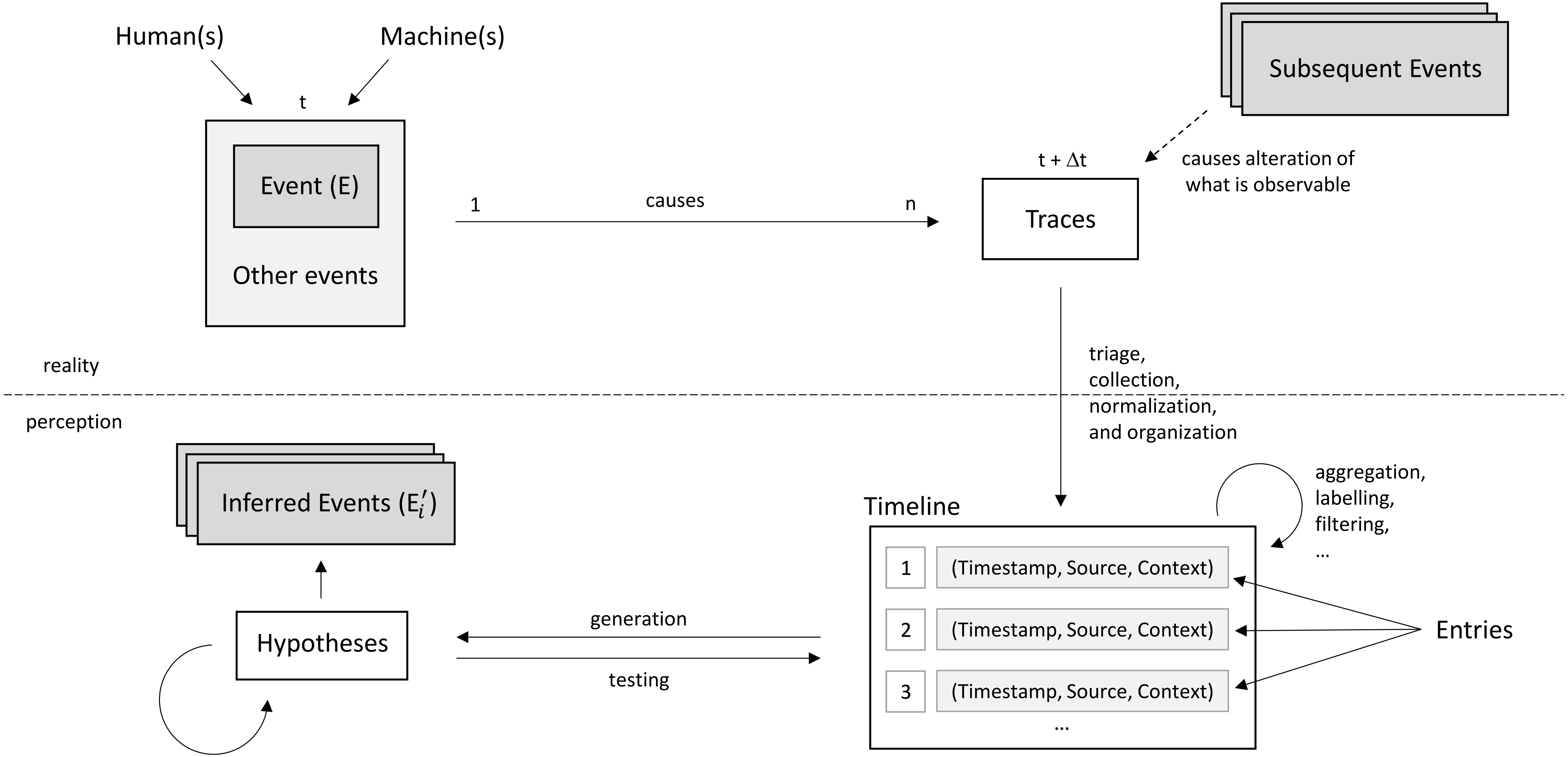
Towards a model for event reconstruction in DFS

- O. Ribaux, *Forensic science: intelligence using the trace* (2014)
- O. Ribaux, *Police scientifique : le renseignement par la trace* (2014)



Environnement (tx)
Activités (t)
Activité en question
Cadre légal - procédures, libertés individuelles
Organisation - stratégie, règles administratives, distribution des rôles
Scène de crime (tx+Δt)
Δ't
Causent
Traces
Recueillir, organiser
Tester
Raisonnement
Perception (instruments, techniques)
Hypothèses (H1...Hn)
Reconstruire
Modèle (champ d'investigation, traces)
Tester

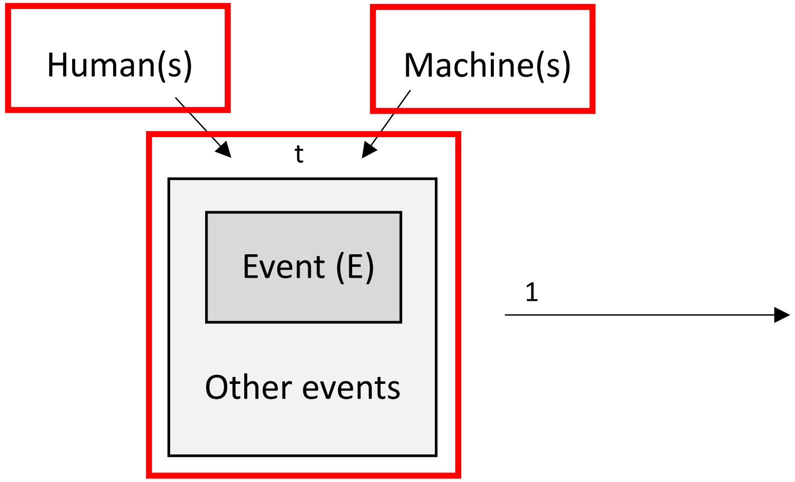
The specific case of timelines


Human(s)
Machine(s)
t
Event (E)
Other events
1
causes
n
Subsequent Events
t + Δt
causes alteration of what is observable
Traces
triage, collection, normalization, and organization
reality
perception
Inferred Events (E_i')
Timeline
aggregation, labelling, filtering, …
1
(Timestamp, Source, Context)
2
(Timestamp, Source, Context)
3
(Timestamp, Source, Context)
…
Entries
Hypotheses
generation
testing

What could affect the event reconstruction process?

Reality - Event

- Clock skew and drift
- Synchronization
- Manipulation of clocks
- NTP attacks
- System behaviors



What could affect the event reconstruction process?

Reality - Event

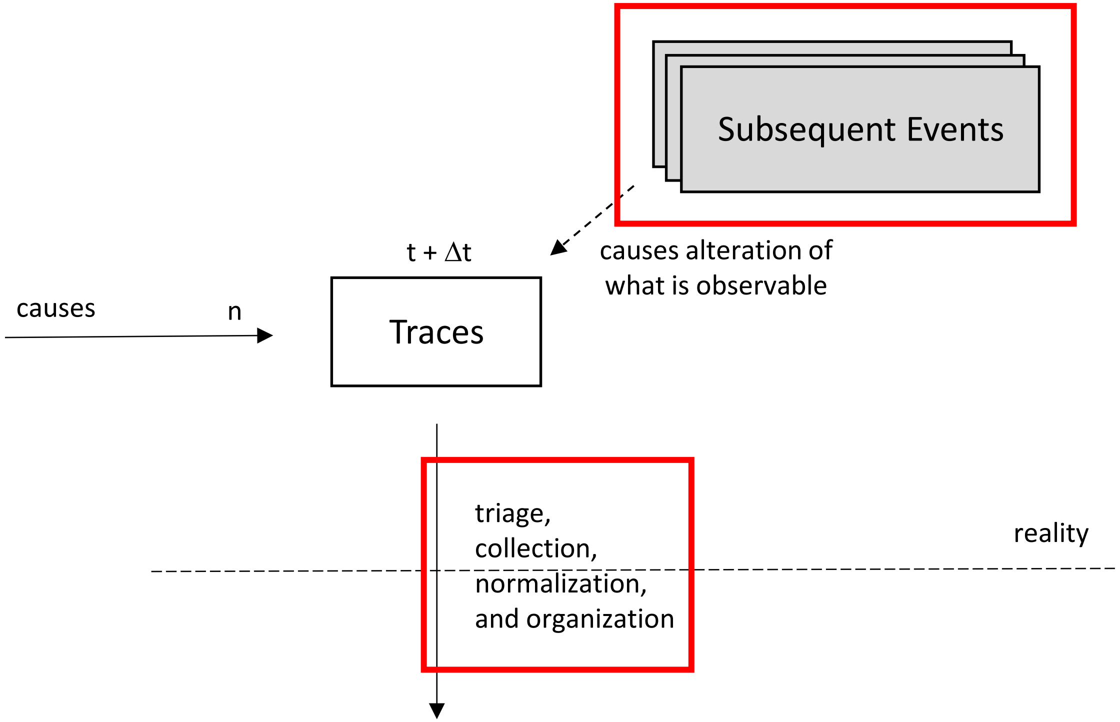
- Clock skew and drift
- Synchronization
- Manipulation of clocks
- NTP attacks
- System behaviors

Reality – Subsequent Events

- The passing of time
- Tampering
- Contamination

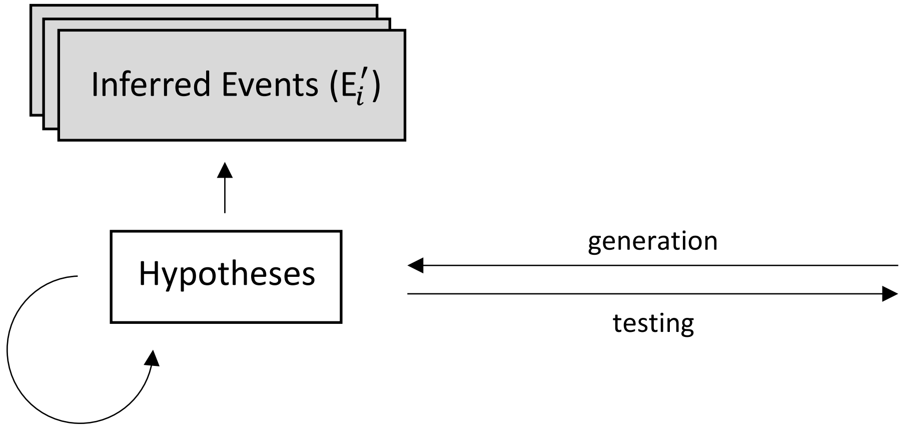
Perception - Collection

- Relevance
- …

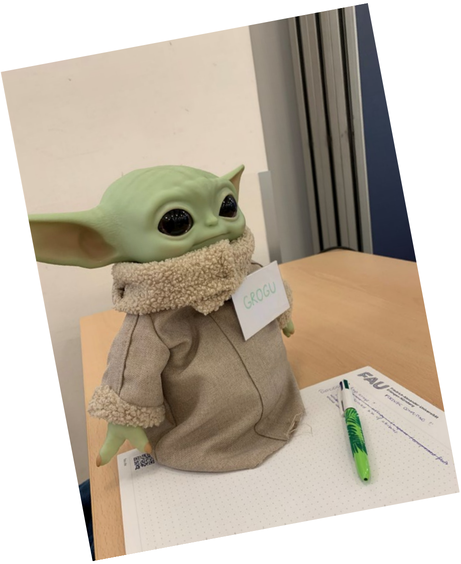


In terms of interpretation…

- Each problem may affect the last steps of the event reconstruction process
- General approach: lead to misinsterpretations



Questions?



Thank you!

Céline Vanini
celine.vanini@unil.ch

DFRWS
DIGITAL FORENSIC RESEARCH CONFERENCE

UNIL | Université de Lausanne
Ecole des Sciences criminelles