From Clues to Causal Chains: Constraint-Driven Event Reconstruction

Lorenz Hornung
Open Universiteit
lorenz.hornung@ou.nl

Jan Gruber
Karlsruhe Institute of Technology
jan.gruber@kit.edu

Formal Modeling in Digital Forensics

- **Event reconstruction** reasons about past actions performed within a system [3].
- While **formal models** of digital systems allow for precise event reconstruction, they require **complete system knowledge** and involve **costly computations** [3]. To tackle these challenges, several approaches have been proposed, including:
  - Defining properties of evidence to focus on the **specific reconstruction** problem: while an action's **characteristic** evidence (relative to a set of alternatives) consists of those observable traits that are produced exclusively by that action [1], observation of an action's **sufficient** evidence guarantees it's occurrence, and the absence of an action's **necessary** evidence refutes its occurrence [4].
  - Implementation of **computational tools**: proof-of-concepts modeling in formalisms equipped with model-checking [4, 5, 8].

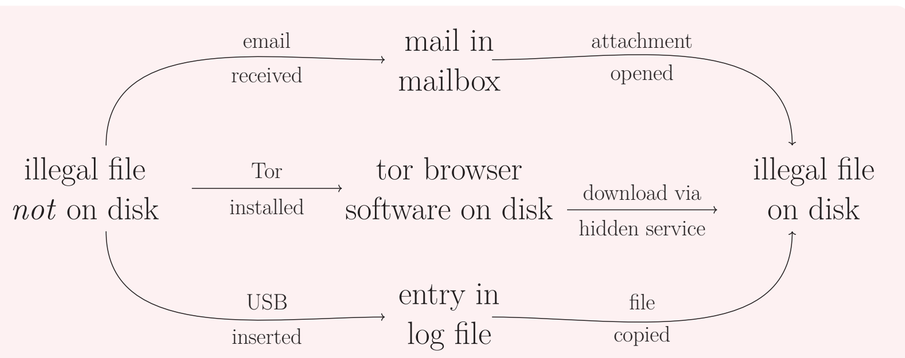
Automated Planning to the Rescue?

Approaches assume the existence of a formal model of the system with complete information. The **construction** of such models and **efficient reasoning** in the context of **partial knowledge** are not addressed.

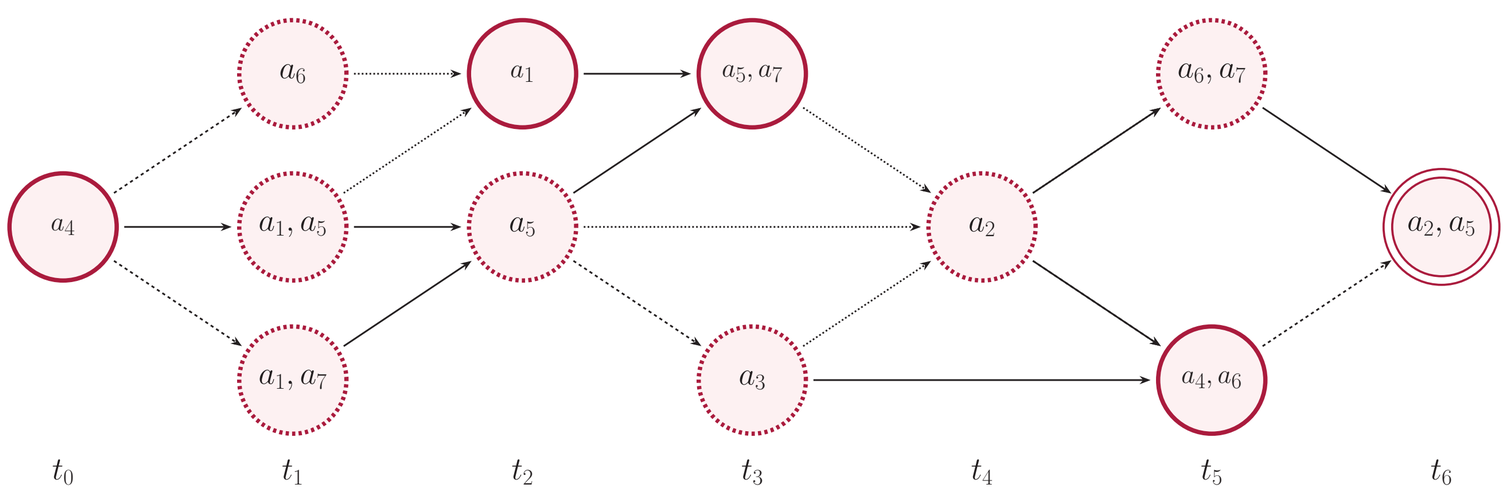
Background on Automated Planning

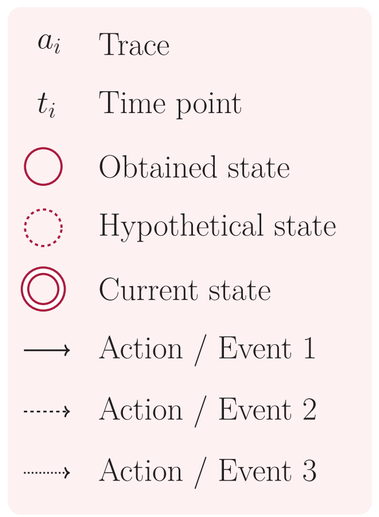
- Automated planning is a **well-established research area** with a substantial theoretical and practical foundation [2, 7].
- A **planning problem** consists of an input and a question to be solved:
  - *Input*: states (the system can be in), initial states (starting states of the system), actions (characterizing the transitions between the states), and goal states (what states we want to obtain)
  - *Question*: Can we find a combination of actions that allow us to reach one goal state from one initial state?

Planning Problem: Provenance of an Illegal File on a Disk



Hypotheses as Combination of Events: Does Your Hypothesis Explains all Traces?





Planning Problems to Reconstruct Events

- We build on the logic framework of automated planning [6] to solve the specific reconstruction problem [1].
- We express **artifacts as propositional variables** and **time points as valuations** over the set of artifacts.
- We define **events as transitions** between time points and characterize them by their **pre-conditions** (the conditions to be applied) and **post-conditions** (the effect of being applied).
- Utilizing logic programming and SAT-solving, we address planning problems that encompass all (or a subset of) acquired traces, thereby **implicitly constructing a model** of the forensic scenario.

Any Benefits for Digital Forensics?

- Introducing automated planning provides rigorous tools to:
  - **Evaluate hypotheses**: Do they cover all traces and the current state?
  - **Identify hypotheses**: Can we find a solution to a planning problem?
  - **Discover clues**: Can we reveal traces aligned with our hypotheses?

Another Formalism: Do We Really Need It?

Defining event reconstruction as a planning problem places it in a broad research field and **unifies past approaches**, potentially aggregating their insights. Yet, only simple examples have been modeled, leaving open whether this approach yields more insight than existing techniques.

[1] Andreas Dewald. "Characteristic Evidence, Counter Evidence and Reconstruction Problems in Forensic Computing". In: *IMF*. IEEE Computer Society, 2015, pp. 77–82.
[2] Malik Ghallab, Dana Mau, and Paolo Traverso. *Automated planning and acting*. New York: Cambridge University Press, 2016.
[3] Pavel Gladyshev and Ahmed Patel. "Finite State Machine Approach to Digital Event Reconstruction". In: *Digital Investigation* 1.2 (2004), pp. 130–149.
[4] Jan Gruber et al. "Formal Verification of Necessary and Sufficient Evidence in Forensic Event Reconstruction". In: *Proceedings of the Digital Forensics Research Conference Europe (DFRWS EU)*. Ed. by Edita Bajramovic and Ricardo J. Rodríguez. Bonn: dfrws.org, Mar. 2023, pp. 1–11.
[5] Slim Rekhis and Noureddine Boudriga. "A formal logic-based language and an automated verification tool for computer forensic investigation". In: *Proceedings of the 2005 ACM Symposium on Applied Computing (SAC), Santa Fe, New Mexico, USA, March 13-17, 2005*. Ed. by Hisham Haddad et al. ACM, 2005, pp. 287–291.
[6] Jussi Rintanen. "Chapter 19. Planning and SAT". In: *Frontiers in Artificial Intelligence and Applications*. Ed. by Armin Biere et al. IOS Press, 2021.
[7] Stuart J. Russell and Peter Norvig. *Artificial Intelligence: A Modern Approach*. Upper Saddle River, NJ: Prentice Hall, 2003.
[8] Somayeh Soltani and Seyed-Amin Hosseini-Seno. "A formal model for event reconstruction in digital forensic investigation". In: *Digit. Investig.* 30 (2019), pp. 148–160.

Open Universiteit

Karlsruhe Institute of Technology