CERIAS

Foundations for Digital Investigations

Brian Carrier and Eugene Spafford

What is a Digital Investigation?

A process that develops and tests hypotheses to answer questions about digital events:

- When did John Doe copy the design document?
- Who gained access to the server last night?
- Why did the server crash?

DIGITAL CRIME SCENE - DIGITAL CRIME S

Problem:

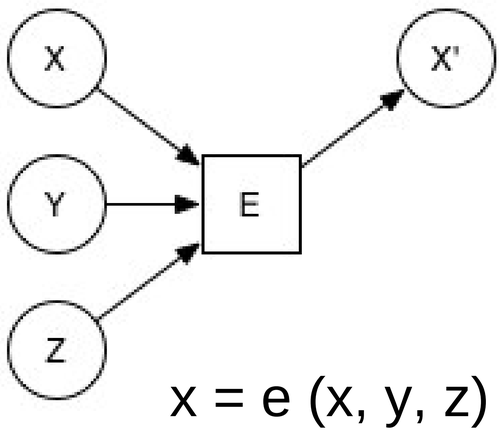
Need a rigorous framework to define tool requirements for development and testing (Daubert Guidelines).

Process model phases are arbitrary and not rigorous.

WARNING - BYTES AHEAD - WARNING

Solution: Develop a framework based on how digital evidence is created.

Concept: An effect of an event is the only evidence that it occurred.



$x = e(x, y, z)$

Concept: Each data object has an equation based on the events it was an effect of:

$$d_{blk1} = a^{-1}_{f}(d_{fs2}, e_{wr}(d_{os}, d_{note}, a_{f}(d_{fs1}, d_{blk5}, d_{in2})))$$

The investigation answers questions by solving these equations (using different techniques and assumptions):

- Search for cause and effect objects to correlate events
- Finite state machine analysis