# Building Theoretical Underpinnings for Digital Forensics Research

*By*

## Sarah Mocas

*Presented At*

The Digital Forensic Research Conference

**DFRWS 2003 USA**   Cleveland, OH (Aug 6th - 8th)

**http:/dfrws.org**

# Building Theoretical Underpinnings for Digital Forensics

Dr. Sarah Mocas

Portland State University

# Goals

- **Framework for Research and Tools Development**

- Model for *Investigative Context*

- Abstractions for *Technical Environment*

- Isolate Underlying Concepts for Properties of Evidence and Process

# Investigative Context

❑ *Investigative Context - A set of  precipitating events, a set of constraints and a set of potential outcomes.*



**Precipitating Events**

**Constraints**

**Outcomes**

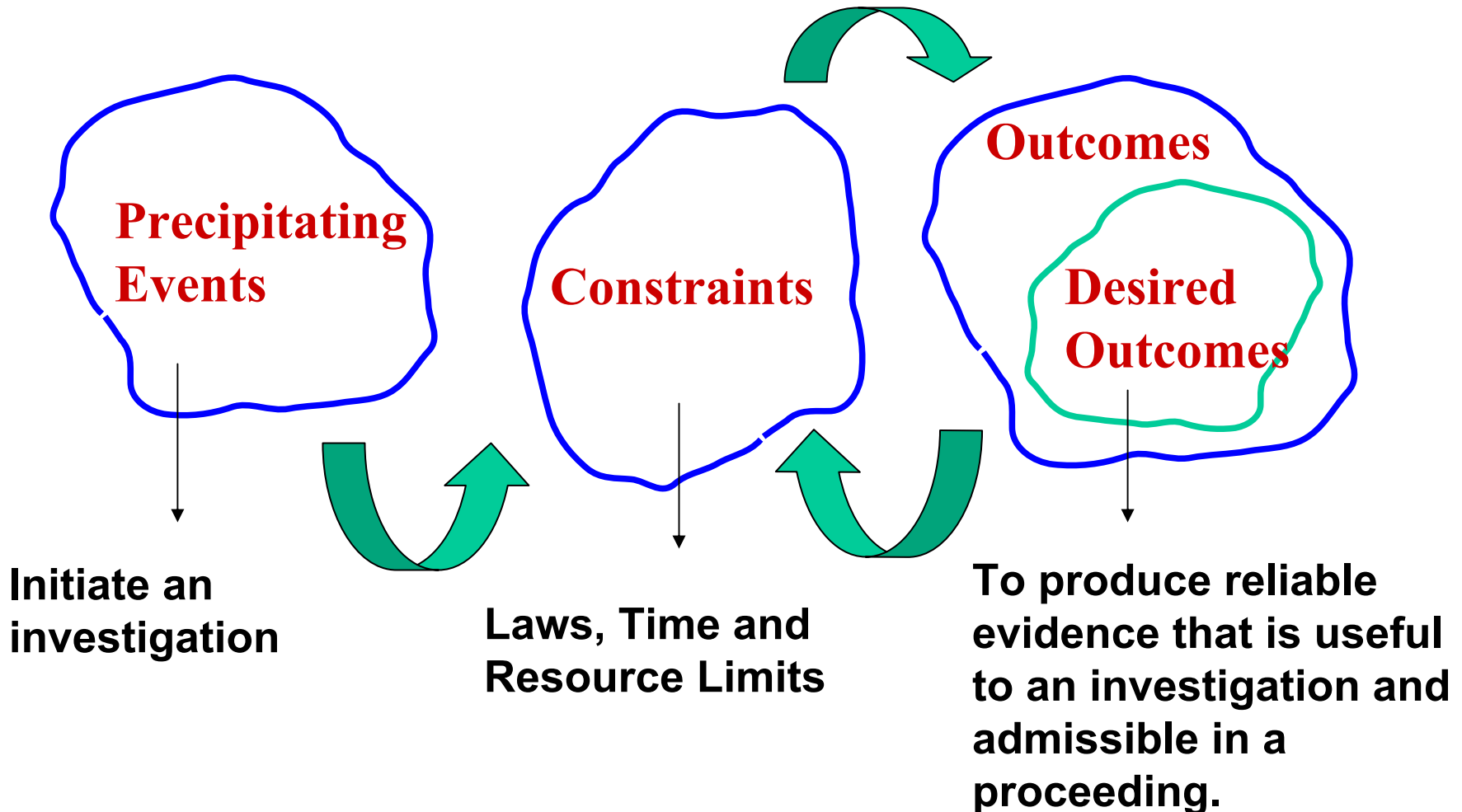**Desired Outcomes**
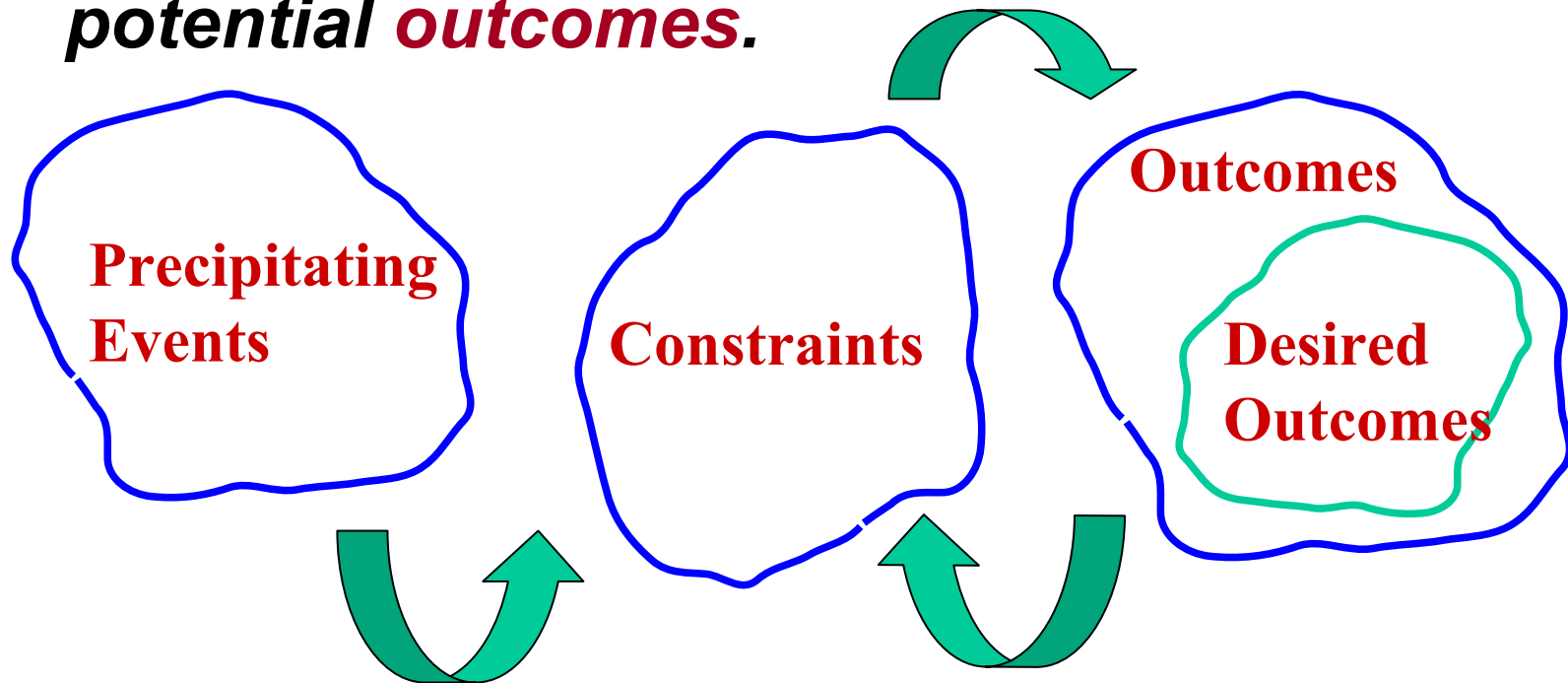
**Law Enforcement, National Security, Business**

# Investigative Context

- *Investigative Context - A set of  events that initiate the investigation, a set of constraints on the scope of the investigation (laws, time, resource limits) and a set of potential investigative outcomes.*

- **Desired Outcomes - The subset of outcomes that the investigator is interested in. (Goals)**

# Investigative Context

- **Example: Law Enforcement Context**
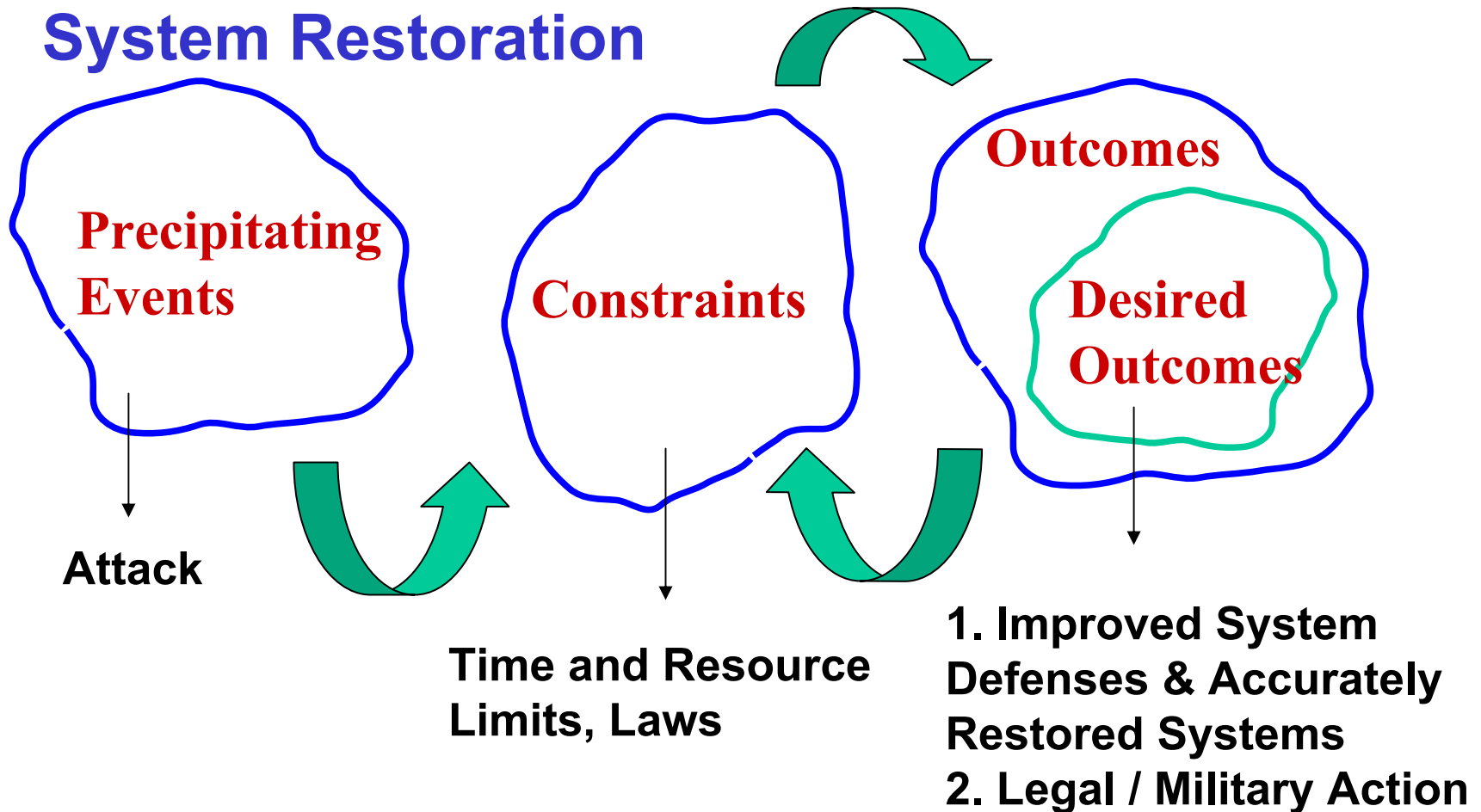
**Precipitating Events**

**Constraints**

**Outcomes**

**Desired Outcomes**

Initiate an investigation

Laws, Time and Resource Limits

To produce reliable evidence that is useful to an investigation and admissible in a proceeding.

# Investigative Context

□ **Example: Military - Post Attack Analysis and System Restoration**



**Precipitating Events**

Attack

**Constraints**

Time and Resource Limits, Laws

**Outcomes**

**Desired Outcomes**

1. Improved System Defenses & Accurately Restored Systems
2. Legal / Military Action

# Investigative Context

❑ **Example: Business - System Security**



Precipitating Events

Constraints

Outcomes

Desired Outcomes

**Business Priority**

**Time, Cost and Resource Limits, also Laws**

**Monitor and Improve System Security**

Intrusion Detection, Honey Pot, etc.
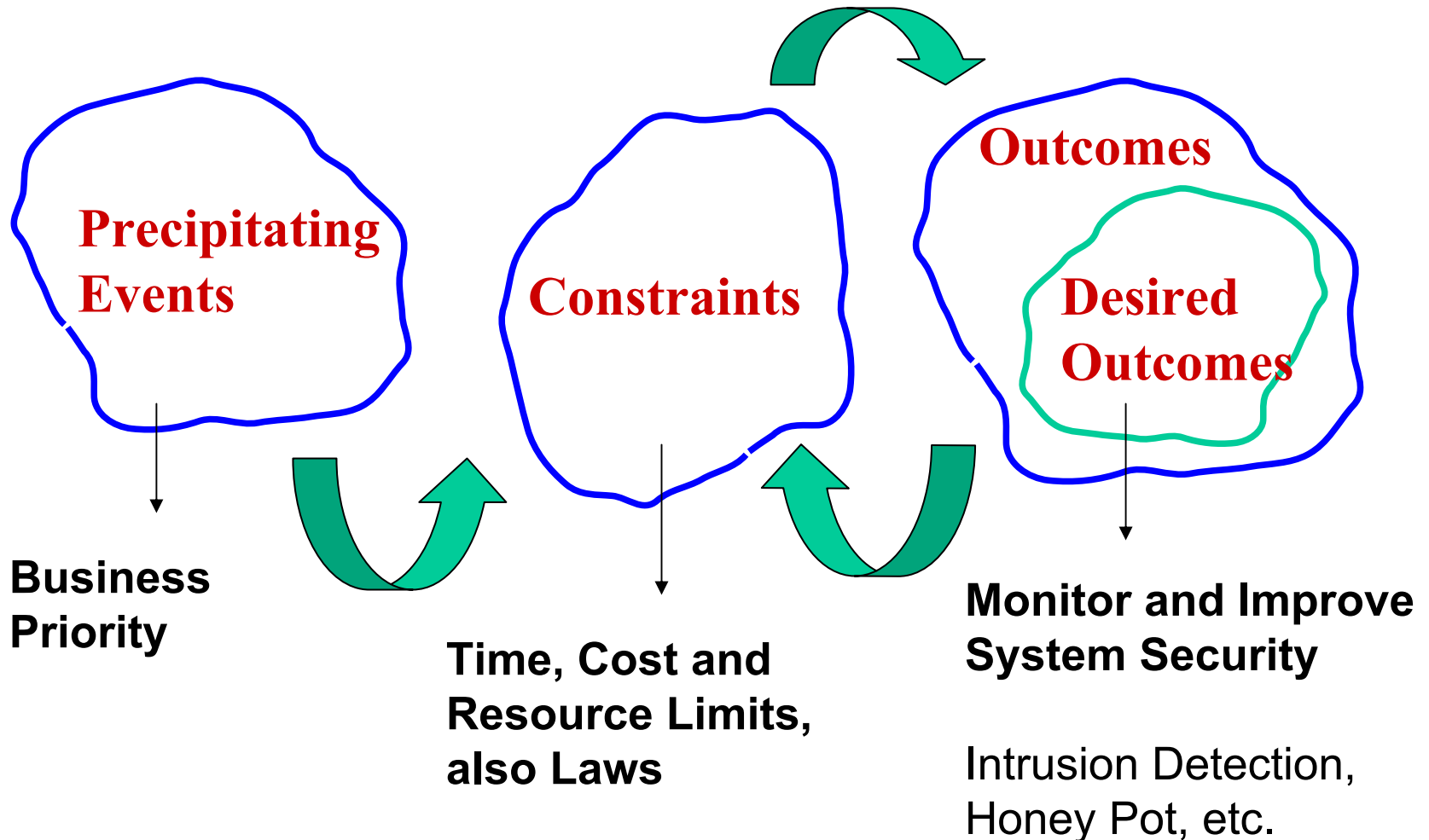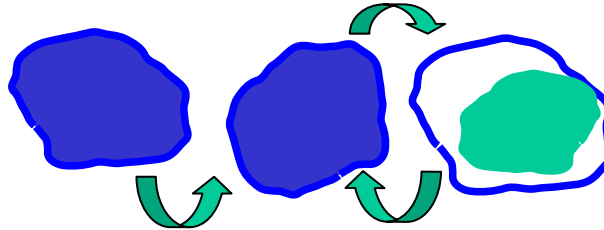
# Investigative Context

❑ **Motivation from Computer Security**

- ▪ **Security Policy - Set of rules designed to meet a particular goal of securing a computer.** (Constraints)

- ▪ **A security policy depends on the concerns of the owner - Security Goals based on Risk Analysis.** (Desired Investigative Outcomes)

- ▪ **Commercial and Military Security - Historically**
  - • Commercial - protect financial assets
  - • Military - preserving confidentiality of sensitive information

Landwehr, *Computer Security*, IJIS, 2001

# Investigative Context

## Questions

- Under what constraints is a particular tool or process acceptable?

- When can information produced in one context be used as evidence in another context?

**Investigative context is a way for researchers and tool developers to discriminate.**

# Technical Context

□ **Technical Environment** - The set of devices and the relationships between devices from which data is retrieved in support of an investigation.

- **Hard Drive, PDA**
- **Internet & Networks**
- **"Live" Systems**
- **Wireless**
- **More ...**
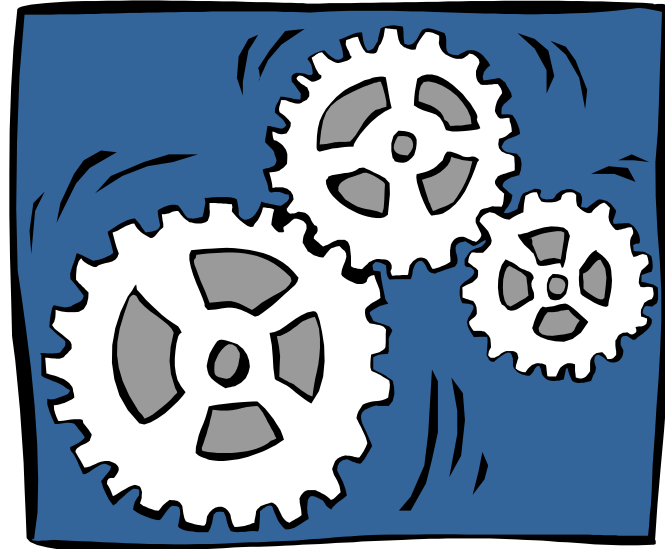
# Technical Context

❑ **Static Technical Environment** - Only the investigative process has the potential to modify information related to the investigation.

❑ **Dynamic Technical Environment** - One or more of the components from which data is retrieved has the potential for modifying information, independent of any changes to the system that might be introduced by the investigative process.

# Technical Context

## Questions
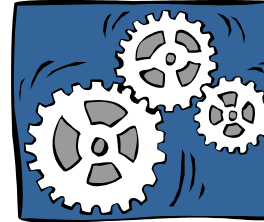
❏ In a particular technical environment, is it possible or feasible to reproduce the processes used to gather evidence?

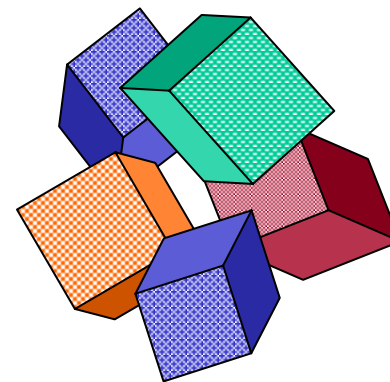❏ In a particular technical environment, how does the investigative process modify the environment?

**Lots of future work in refining "environment".**

# Properties

**In a legal setting, what properties are desirable on evidence and process?**

- ❑ Integrity
- ❑ Authentication
- ❑ Reproducibility
- ❑ Non-interference
- ❑ Minimalization

Use to frame questions, model behavior, test and evaluate tools.

# Properties

> *Action taken to secure and collect electronic evidence should not change that evidence.* (NIJ Electronic Crime Scene Investigation)

- ❏ Data Integrity - Assuring that the digital information is not modified (either intentionally or accidentally) without proper authorization.

- ❏ Duplication Integrity - Assuring that, given a date set, the process of creating a duplicate of the data does not modified the data and that the duplicate is an exact bit copy of the original.

# Properties

❑ Authentication - Knowing that the apparent author of text is in fact the true author. (Security)

- Biometrics, Cryptographic Primitives
- Partial information used in support of non-electronic evidence

❑ Authentication - Knowing that the electronic evidence is what its proponent claims. (DoJ Searching and Seizing Computers and Related Electronic Evidence)

- Is this authentication or integrity?

# Properties

*A key feature of science is that hypotheses are supported by reproducible experiments.*

- Reproducibility - Assuring that, given a data set or set of devices, the processes used to gather and/or examine evidence are reproducible.
  - Supports use of Scientific Methods

# Properties

One of the most important aspects of securing a crime scene is to preserve the scene with minimal contamination ... (NIJ Crime Scene Investigation)

❑ **Non-interference** - Assuring that the methods (or tools) used to gather and/or analyze digital evidence do not change the original data set.

❑ **Identifiable-interference** - Assuring that when methods (or tools) used to gather and/or analyze digital evidence change the original data set that changes are identifiable.

# Properties

*The law does not authorize the government to seize items which do not have evidentiary value ....* (DoJ Searching and Seizing Computers and Related Electronic Evidence)

- Minimalization - Assuring that the minimum amount of data was seized and/or searched.
  - Targeted network traffic
  - Separating out "known good" & "known bad"
  - Optimize searches on large data sets

# Properties

## Questions
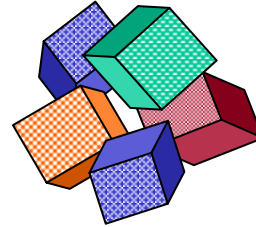
- For a particular tool or circumstance, can integrity (or any other property) be provided over the data that is processed?
    - If so, is this provable?
    - If not, is this provable?
- When is minimalization possible?

**Lots of future work left!**

# Conclusion

❑ Defined a set of properties and terms to use as organizing principles for research and tools development

❑ Challenge - Refine and Apply this Framework!