CERIAS

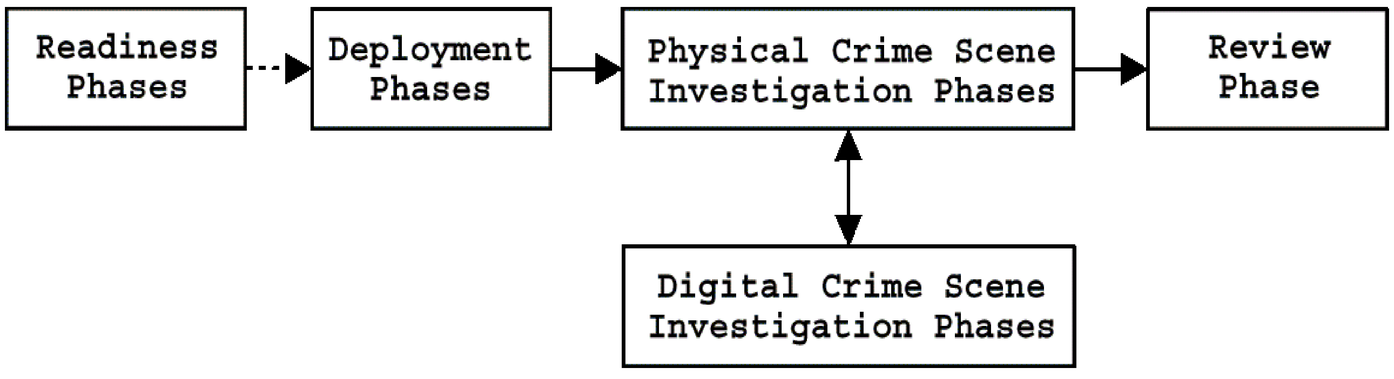
A Digital Investigation Process Model

Brian D. Carrier and Eugene H. Spafford

Goal: To develop a model for the digital investigation process, so that requirements can be developed for forensic analysis tools and procedures.

Summary: The procedures for a physical crime scene are applied to the digital crime scene.

An Investigation Cycle



Readiness: Train investigators, develop procedures, and test equipment.

Deployment: Detect a crime or incident, verify it, and obtain authorization to respond or investigate.

Physical Crime Scene Investigation

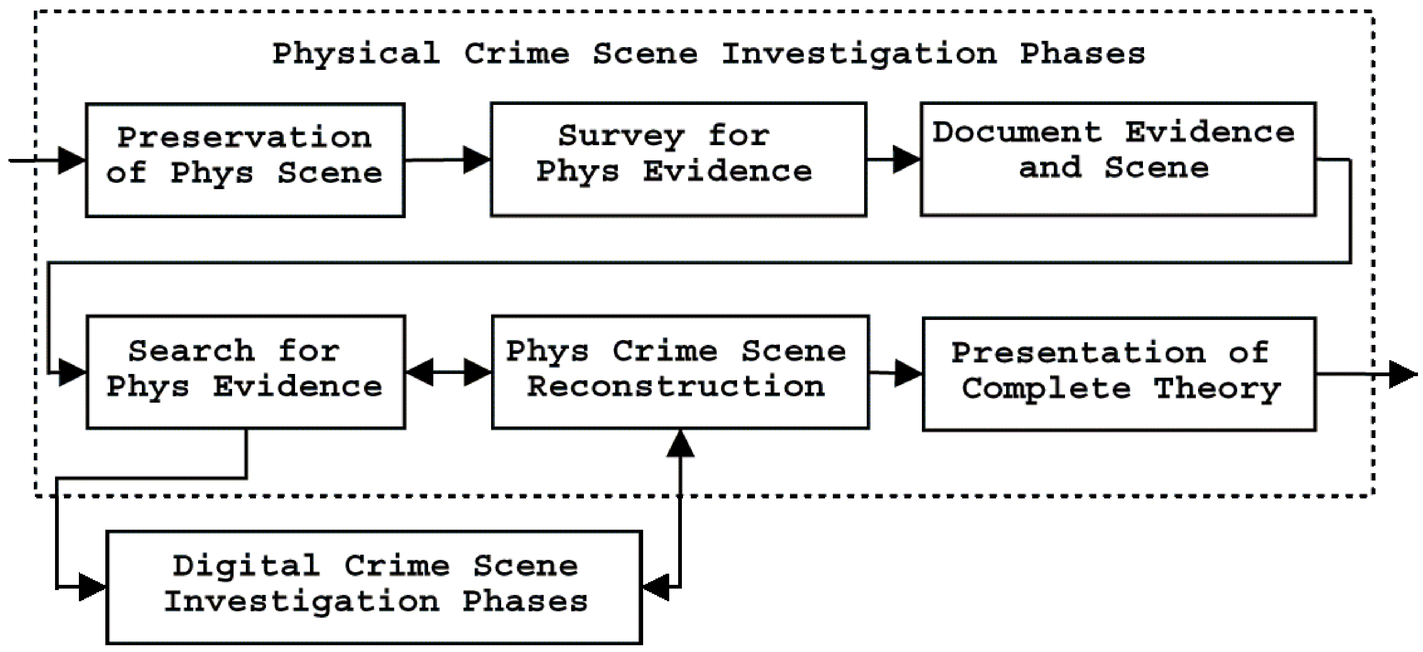
Preservation: Secure the physical area around the digital device.

Survey: Cursory search of the physical crime scene for obvious pieces of evidence about the incident.

Documentation: Take pictures and sketches of physical evidence.

Search: Conduct a thorough search of the physical crime scene for evidence. Digital investigation begins when digital devices are collected.

Reconstruction: Reconstruct the physical and digital events that occurred at the crime scene.



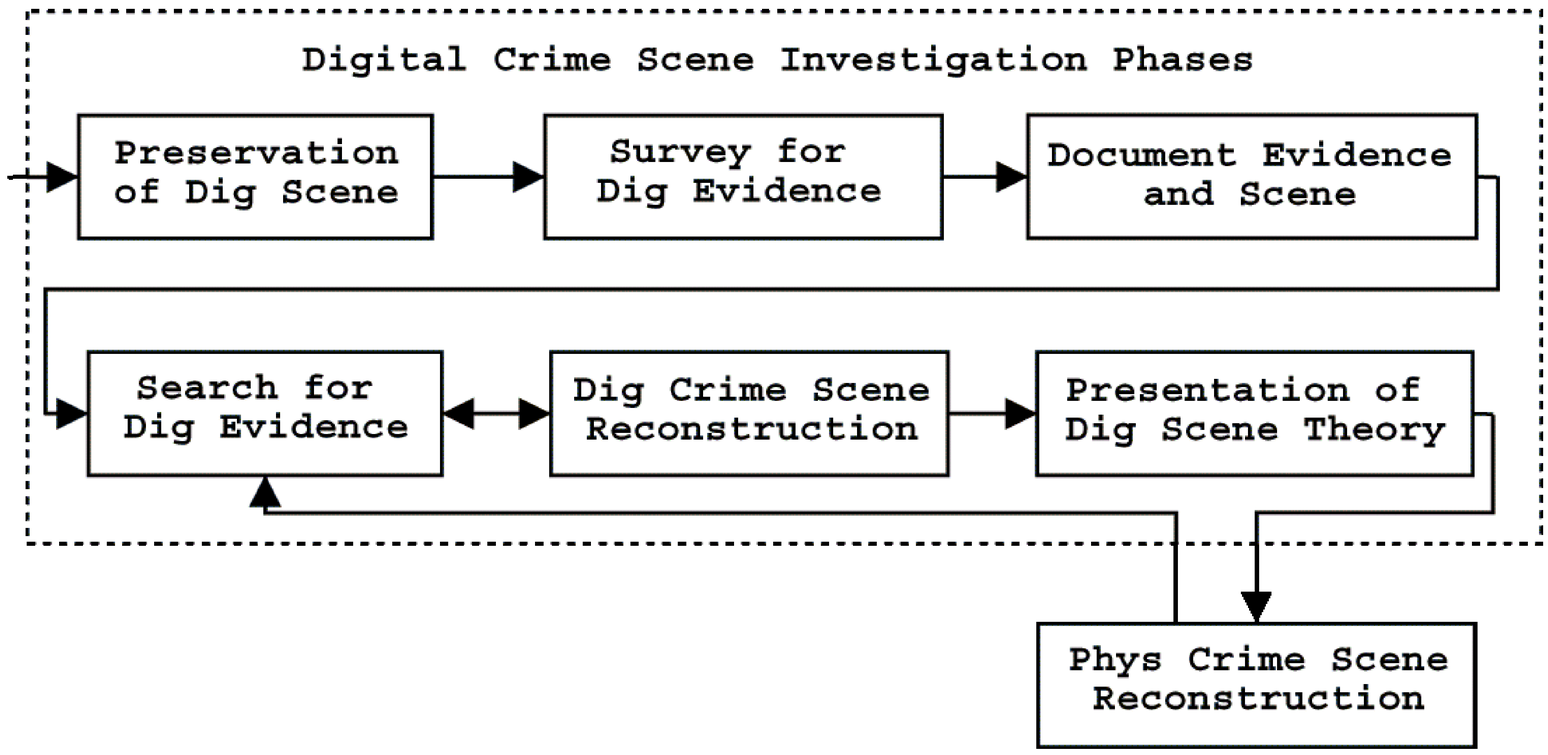
PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center

CERIAS

Digital Crime Scene Investigation



1. Preservation

Goal: Secure the digital crime scene and prevent data from changing.

Methods: Suspend suspect processes, acquire volatile and non-volatile data.

2. Survey

Goal: Search for obvious pieces of digital evidence based on the type of device and type of incident. Develop a hypothesis and search strategy.

Methods: Use specialized examination tools and experience of similar incidents.

3. Documentation

Goal: Document the evidence and crime scene.

Methods: Document evidence as it is found using its physical & logical locations.

4. Search

Goal: Conduct a thorough search of the crime scene for remaining digital evidence.

Methods: Use specialized tools and search based on existing evidence, each file, each sector, keywords, file type etc.

5. Event Reconstruction

Goal: Identify the events that occurred at the crime scene.

Methods: Use the state of the digital evidence to identify the cause or effect role that the object played in events at the crime scene.

Related Publications:

Getting Physical With the Digital Investigation Process: International Journal of Digital Evidence, Fall 2003.

Digital Crime Scene Event Reconstruction: American Academy of Forensic Sciences (AAFS) Annual Meeting 2004, February 2004.

PURDUE UNIVERSITY

CERIAS®

Discovery Park e-Enterprise Center