Abstract

In this paper, a process model for digital investigations is defined using the theories and techniques from the physical investigation world. While digital investigations have recently become more common, physical investigations have existed for thousands of years and the experience from them can be applied to the digital world. This paper introduces the notion of a digital crime scene with its own witnesses, evidence, and events that can be investigated using the same model as a physical crime scene. This paper provides a useful review of previous work and then maps the digital investigative process to the physical investigative process. Their product is called the Integrated Digital Investigation Process and defines 17 phases organized into 5 groups: Readiness, Deployment, Physical Crime Scene Investigation, Digital Crime Scene Investigation and Review Phases. The proposed model integrates the physical crime scene investigation with the digital crime scene investigation to identify a person who is responsible for the digital activity and applies to both law enforcement and corporate investigations [2]. The focus of the investigation is on the reconstruction of events using evidence so that hypothesis can be developed and tested. This paper also includes definitions
and description of the basic and core concepts that the framework [3].

References

- Brian Carrier; Eugene H. Spafford, "An Event-Based Digital Forensic Investigation Framework."

Index Terms

Computer Science
Emerging Trends in Technology

Keywords

Digital Forensics Law Enforcement Evidence Digital Investigation Incident Response Crime Scene Investigation