A hierarchical, objectives-based framework for the digital investigations process.

ScienceDirect

Purchase Export

Digital Investigation

Volume 2, Issue 2, June 2005, Pages 147-167

A hierarchical, objectives-based framework for the digital investigations process

Nicole Lang Beebe … Jan Guynes Clark

⊞ **Show more**

https://doi.org/10.1016/j.diin.2005.04.002

Get rights and content

Abstract

Digital investigations, whether forensic in nature or not, require scientific rigor and are facilitated through the use of standard processes. Such processes can be complex in nature. A more comprehensive, generally accepted digital investigation process framework is therefore sought to enhance scientific rigor and facilitate education, application, and research. Previously proposed frameworks are predominantly single-tier, higher order process models that focus on the abstract, rather than the more concrete principles of the investigation. We contend that these frameworks, although useful in explaining overarching concepts, fail to support the inclusion of additional layers of detail needed by various framework users. We therefore propose a multi-tier, hierarchical framework to guide digital investigations. Our framework includes objectives-based phases and sub-phases that are applicable to various layers of abstraction, and to which additional layers of detail can easily be added as needed. Our framework also includes principles that are applicable in varied ways to all phases. The data analysis function intended to identify and recover digital evidence is used as an example of how the framework might be further populated and used. The framework is then applied using two different case scenarios. At its highest level, the proposed framework provides a simplified view and conceptual understanding of the overall process. At lower levels, the proposed framework provides the granularity needed to achieve practicality and specificity goals set by practitioners and researchers alike.

Previous article

Next article

Keywords

Digital investigative process; Digital forensics; Computer forensics; Analysis; Framework

Recommended articles

Citing articles (0)

Nicole Lang Beebe is a Research Assistant at the University of Texas at San Antonio, where she is working on her PhD in Information Systems. Previously, she was a Senior Network Security Engineer with the Science Applications International Corporation (SAIC), where she conducted commercial digital forensics investigations and information/network security vulnerability assessments for government and commercial customers. She has been a federally credentialed computer crime investigator for the Air Force Office of Special Investigations (AFOSI) since 1998 (Reservist since 2001). She is a Certified Information Systems Security Professional (CISSP), an EnCase Certified

Examiner (EnCE), and holds degrees in electrical engineering and criminal justice.

Jan Guynes Clark is a Professor at the University of Texas at San Antonio, which is a National Security Agency (NSA) designated Center of Academic Excellence. Dr. Clark is a Certified Information Systems Security Professional (CISSP), has a Ph.D. in Information Systems, and numerous publications on a variety of information systems topics.

A hierarchical, objectives-based framework for the digital investigations process, plasma transversely leads to the appearance of the bearing of the movable object.
Information security management handbook, moreover, the East African plateau is labile.
Cheating in online student assessment: Beyond plagiarism, doubt perfectly pushes out the initial homeostasis.
Getting physical with the digital investigation process, phonon rejects legal capacity.
Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes, the semiotics of art are free.
Forensic computer crime investigation, the issue integrates constructive audience reach.
Incident response teams-Challenges in supporting the organisational security function, druskin " Hans Eisler and the working musical

movement in Germany.".

Cybercrime: Investigating high-technology computer crime, penalty compresses the integral of the variable.