



A Cyber Forensics Ontology: Creating a New Approach to Studying Cyber Forensics

By

Ashley Brinson, Abigail Robinson, Marcus Rogers

Presented At

The Digital Forensic Research Conference

DFRWS 2006 USA Lafayette, IN (Aug 14th - 16th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

<http://dfrws.org>

A Cyber Forensics Ontology: Creating a New Approach to Studying Cyber Forensics

Ashley Brinson
Abigail Robinson
Purdue University

Introduction and Background

- Ontology vs. ontology
- Five layered hierarchical structure
- Purpose
 - Certification and Specialization
 - Curriculum Development
- Limitations
- Technology vs. Profession

Technology

■ Hardware

- LSDD
- SSDD
- Storage Devices
- Obscure Devices
- Computers

■ Software

- Analysis Tools
- Operating Systems
- File Systems

Technology

- Hardware
 - Large Scale Digital Devices
 - Grids
 - Clusters
 - Small Scale Digital Devices
 - Cell Phones
 - PDAs
 - SSDD Software

Technology

- Hardware Continued
 - Storage Devices
 - Thumb Drive
 - Digital Music Players
 - External Hard Drives
 - Obscure Devices
 - Gaming Devices
 - Recording Devices

Technology

- Software
 - Analysis Tools
 - Proprietary
 - Open Source
 - Operating Systems
 - Proprietary
 - Open Source
 - File Systems
 - Windows
 - Unix/Linux
 - Mac

Profession

- Law
 - Enforcement
 - Collection/Analysis
 - Evidence
 - Courts
 - Laws
 - Individuals

Profession

- Academia
 - Research
 - Discipline Definition
 - Problem Solving
 - Education
 - Contributions
 - Professional Outcomes

Profession

- Military
 - Offensive
 - Passive
 - Active
 - Defensive
 - Proactive
 - Reactive

Profession

- Private Sector
 - Consulting
 - Data Recovery
 - Forensic Analysis
 - Expert Witness
 - Industry
 - System Administrators
 - Legal Contact

Applicable Areas

- Certification Areas
 - Proper Depth
 - Recognition
- Curriculum Development
 - Collegiate level courses
 - Dynamic model

Conclusion

- Importance
- Further Research

Questions or Comments?