

---

# 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?