PURDUE UNIVERSITY

Developing Specialization in Computer Forensics - Curriculum and Outreach

Dr. Melissa Dark, Assistant Director for Educational Programs, CERIAS

PURDUE UNIVERSITY

The Early Years – 2000-2002

- CERIAS Mission
  - The mission of CERIAS is to advance the knowledge and practice of information assurance and security through the performance of world-class research, the delivery of the highest quality education, and by serving as an unbiased source of information locally, nationally, and internationally.
- Special effort
  - Audiences with acute need and minimal resources
  - Law enforcement and K12 education

PURDUE UNIVERSITY

The Next Few Years – 2002-2004

PURDUE UNIVERSITY

The Early Years – Partnerships

- Infragard
- Indiana FBI and Secret Service
  - Special Agents Dan Nielson and Buddy Burns
- Indiana State Police
  - Colonel Don Brackman
- Department of Education
  - Learning Anytime Anywhere Partnership

PURDUE UNIVERSITY

The Early Years – People

- Gene Spafford
- Brought in 1 individual on soft money as a research scientist – Dr. Marc Rogers
- Wrote a capacity building grant with University of Alaska Fairbanks

PURDUE UNIVERSITY

The Middle Years – 2002-2004

- Grant funded 2002
- Invested in faculty development for another professor – Jim Goldman
- Marc Rogers – soft funded 2003-04, then takes a tenure track position in C&IT in 2004
- ITAP and Scott Ksander
- Continue building partnerships

PURDUE UNIVERSITY

The Middle Years – 2002-04

- Establish the Cyberforensics Lab - 2004
  - The mission of the cyber forensics lab is to act as a national center and provide support for education/training, research (applied & basic), and investigations in the area of cyber forensics.
  - The lab's mandate extends to the four communities involved in the emerging scientific discipline of digital forensic sciences/cyber forensics: Law Enforcement, Military, Private Sector, and Academia.

PURDUE UNIVERSITY

The Recent Years – 2004-06

- National White Collar Crime Center decides to put a staff member at Purdue as an adjunct faculty – 2005
- The Cyberforensics lab is built
- Purdue decides to allocate one more strategic planning position to cyber forensics in small scale digital device forensics
- Now we are six strong
  - Spafford, Rogers, Goldman, Wedge, Ksander, Mislan

PURDUE UNIVERSITY

The Recent Years - Outreach

- Computer Forensic Analysis: Introduction to Hardware Write Blockers and Preview Tools
- Introduction to email forensics
- Fast Cyber Forensics Triage
- Introduction to Cell Phone Forensics
- Basic Bagging & Tagging
- Fast Forensics Triage
- Introduction to Cellphone Forensics
- Digital Forensics Research Workshop
- Coordinated Computer Incident Response

PURDUE UNIVERSITY

The Recent Years - Curriculum

- **C&IT 499C: Cyber Forensics: Advanced Technical Issues**
  This course will introduce students to advanced technical issues pertaining to cyberforensic examinations. There will be a strong emphasis on the purely technical aspects and details of cyberforensic examinations. Topics will include advanced media structure and file system issues, recovery and analysis of Internet-related artifacts, and contextual analysis of digital data
  The course combines theory and hands on learning. Students will employ a variety of techniques to recover a wide array of digital artifacts associated with FAT, NTFS, UFS, and EXTxFS filesystems, as well as some application-specific artifacts. The primary focus will be on articulating what is proven or disproven (or what theory is supported or unsupported) by each of these artifacts.
  The instructor for this course is Tim Wedge.
  (499C course webpage)
- **C&IT 499D: Small Scale Digital Device Forensics**
  This course is designed to provide an introduction to Small Scale Digital Devices and the Forensic procedures related to PDAs, Cellphones, Embedded Chip Devices, and Digital Audio and Video Players.The major focus will be on the forensic acquisition, analysis, and presentation of the digital evidence found on these devices.
  The course combines theory and hands on learning. There are numerous PDA, Cellphone, and Embedded Chip Device labs and a practical exam, in which students will have the opportunities to conduct actual forensic examinations.
  The instructor for this course is Rick Mislan.
- **C&IT 499E: Computer Hardware Essentials**
  This 4 week, 16 hour course will provide a detailed, technical examination of key data storage concepts. Students will learn, on both a physical and conceptual level how data is stored on physical media. The course is targeted for students interested in cyberforensics courses - a solid competence with these concepts is essential to those students. The material would also greatly enhance the ability of students in other CIT tracks to relate abstract concepts to physical objects.
  The course is an intense look below the usual layer of abstraction at technical specifications, parameters, and theory of operation associated with digital data storage. There will be a major focus on conceptually applying data storage parameters to "real-world" practical isses such as troubleshooting drive access problems and storage device interface compatibility issues.
  The instructors for this course are Rick Mislan and Tim Wedge.
- **C&IT 499F/581F: Basic Computer Forensics**
  This course is designed to provide an introduction to a specific area under the larger scientific discipline of digital forensics. Computer forensics is primarily focused on cyber crime scene analysis (e.g., workstations, servers), and media analysis (e.g., primary or secondary storage, PDAs, memory sticks etc.). The other areas of digital forensics, network forensics and software forensics are not covered in this course per se.
  The course combines theory and hands on learning. There are 8 labs and a practical exam, in which students have to conduct an actual forensic examination.
  The instructor for this course is Dr. Marc Rogers.

PURDUE UNIVERSITY

The Recent Years - Curriculum

- **C&IT 581A: Advanced Topics in Cyber Forensics**
  This course is designed as a graduate level seminar class. The focus of the course is on research topics in cyber forensics. Students are required to choose a research topic in the area focusing on current and near term issues. Topics can range from public policy, behavioral characteristics, to tool testing and development. The only restriction for a topic, is that it has to be relevant to cyber forensics.
- **C&IT 581V: Advanced Topics in Small Scale Digital Device Forensics**

PURDUE UNIVERSITY

The Recent Years - Curriculum

- Our forensics courses are part of three programs of study
  - Interdisciplinary Master of Science in Information Security
  - Interdisciplinary Area of Specialization in Homeland Security
  - Master of Science in Technology

PURDUE UNIVERSITY

The Recent Years - Partnerships

- National Cybercrime Training Partnership (NCTP)- National White Collar Crime Center
- National White Collar Crime Research Consortium (WCCRC)- National White Collar Crime Center
- Scientific Working Group on Digital Evidence (SWGDE)
- High Tech Crime Investigators Association (HTCIA)
- High Tech Crime Network (HTCN)
- (ISC)2 -CISSP/SSCP QA Board
- Center for Forensic Sciences
- Office of the Inspector General in Indiana

PURDUE UNIVERSITY

The Recent Years – Funding & Infrastructure

- Funding
  - DHS – proposals and awards
  - NIJ – proposals and awards
  - NSF – proposals, no awards yet
- Infrastructure
  - High Performance Computing Lab
  - Secure Space

PURDUE UNIVERSITY

Looking Forward

- Establish an Area of Specialization in Cyberforensics
- Continue building funding
- Set up a cost center
- Expand student recruiting efforts
- Cost Center for Service Activities
- State Appropriated Center?