DEVELOPING AN UNDERGRADUATE COURSE IN DIGITAL FORENSICS

Warren Harrison
PSU Center for Information Assurance
Portland State University
Portland, Oregon 97207
warren@cs.pdx.edu

What is Digital Forensics?

- Extracting ***evidence*** from computers or other digital devices
- Usually involves extracting the contents of files and interpreting their meaning

Portland State UNIVERSITY

Recent Interest in Academic Courses in Digital Forensics


Search
USA TODAY
Home News Travel Money Sports Life Tech Weather
Tech Inside Tech

Cybercrime spurs college courses in digital forensics

By Jon Swartz, USA TODAY

SAN FRANCISCO — One of the hottest new courses on U.S. college campuses is a direct result of cybercrime.

Classes in digital forensics — the collection, examination and presentation of digitally stored evidence in criminal and civil investigations — are cropping up as fast as the hackers and viruses that spawn them.

About 100 colleges and universities offer undergraduate and graduate courses in digital forensics, with a few offering majors. There are programs at Purdue University, Johns Hopkins University, the University of Tulsa, Carnegie Mellon University and the University of Central Florida. Five years ago, there were only a handful.

"I teach students to be like (TV supersleuth) MacGyver," says Sujeet Shenoi, a computer science professor at the University of Tulsa.

over 100 courses from computer science, criminology, information systems, accounting and information technology

Portland State University

3

Challenges for Digital Forensics

- Technical aspects of digital forensics are mundane
- Simply involves retrieving data from existing or deleted files, interpreting their meaning and putting them within the context of the investigation
- Real challenges involve artificial limitations imposed by constitutional, statutory and procedural issues – we often loose sight of the goal of retrieving *evidence*

Portland State University

4

Issues in Teaching a Course on Digital Forensics

- Who is the class for?
  - what should this class prepare students to do?
- Topical Content
  - what should be covered in the course?
- Facilities and Resources
  - what do you need to have access to in order to teach the class
- Student Evaluation and Assessment
  - how do you measure what they've learned?

Portland State UNIVERSITY

5

Categories of Digital Forensics Personnel

- *Technicians* - carry out the technical aspects of gathering evidence - sufficient technical skills to gather information from digital devices, understand software and hardware as well as networks.
- *Policy Makers* - establish forensic policies that reflect broad considerations - main focus is on the big picture, but must be familiar with computing and forensics.
- ***Professionals -*** the link between policy and execution - must have extensive technical skills as well as a broad and deep understanding of the legal procedures.
- YASINSAC, A., ERBACHER, R., MARKS, D. and POLLITT, M., "Computer Forensics Education", IEEE Security and Privacy, July/August 2003, pp 15-23.

Portland State UNIVERSITY

6

Skills for Digital Forensics Professionals

- Identify relevant electronic evidence associated with violations of specific laws.
- Identify and articulate probable cause necessary to obtain a search warrant and recognize the limits of warrants.
- Locate and recover relevant electronic evidence from computer systems using a variety of tools.
- Recognize and maintain a chain of custody.
- Follow a documented forensics investigation process.

7

Portland State UNIVERSITY

Potential Target Audiences

- Computer science students with an interest in a “different” kind of career
- Accounting majors interested in auditing electronic systems
- Criminology majors who want to do digital investigations
- The curious …

8

Portland State UNIVERSITY

The Delivery Team

- Technical knowledge
  - file systems
  - system software
  - data organization
  - specific operating systems
- Criminal justice system knowledge
  - court system
  - investigative process

9

Portland State UNIVERSITY

Topical Content

- Concept of evidence and its role in prosecution and defense
- Overview of the legal and judicial system
- The investigative process
- Electronic artifacts of evidential value
- File systems and evidence recovery

10

Portland State UNIVERSITY

Evidence

- Most digital forensics courses over emphasize the technical at the cost of neglecting the whole point of the exercise
- Ultimately, the point is to gather evidence for subsequent legal (criminal or civil) purposes
- What you can do technically is important, but what you can't do because of artificial constraints is even more important

Portland State UNIVERSITY

Identify relevant electronic evidence

- Relevant evidence is any evidence that makes the existence of a fact that is of consequence to the case either more or less probable than it would be without the evidence.
- Two of the skills that bear directly on this are:
  - identifying the "elements of the crime" and relating electronic artifacts to these elements, and
  - presenting evidence to a non-technical audience in coherent, logical manner

Portland State UNIVERSITY

The Elements of a Crime

- *outcome*
  - what happened
- *circumstances*
  - how did it happen
- *mental state*
  - what was the actor's state of mind

13

Portland State UNIVERSITY

Admissibility of evidence follows the *Daubert Standard*

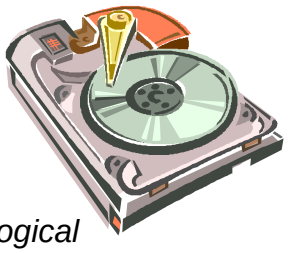
- Has the technique been empirically tested?
- Has the technique been subjected to peer review?
- What is known regarding error rate?
- Does the technique rely upon the special skills and equipment of one expert, or can it be replicated by other experts elsewhere?
- **Can the technique/results be explained so that the court and the jury can understand its meaning?**

14

Portland State UNIVERSITY

Special issues with electronic evidence

- Expectation of Privacy – legal/illegal searches
- Jurisdiction of the data
- Reliability of evidence
- Presentation of the evidence



these limit the examiners' technological capabilities

15

Portland State UNIVERSITY

Identify and articulate *probable cause*

- Important because
  - widespread misunderstanding of probable cause issues and 4th Amendment/statutory protections among the students
  - serious misunderstanding of the criminal justice system and related processes.
- Key to acquiring evidence
  - no PC, no evidence

16

Portland State UNIVERSITY

Overview of the legal and judicial system

- Most students don't understand the structure of the legal system or the role of evidence within the legal system
- Most students don't understand constitutional issues with regards to search & seizure
- These are important in order to understand the constraints placed on gathering evidence and what it is going to be used for

17

Portland State UNIVERSITY

The Investigative Process *The Search Warrant*

- the affidavit
- probable cause
- the search warrant
- when a warrant isn't needed
- Electronic Communications Privacy Act (ECPA)

18

Portland State UNIVERSITY

The Investigative Process
Seizing the Equipment/Information

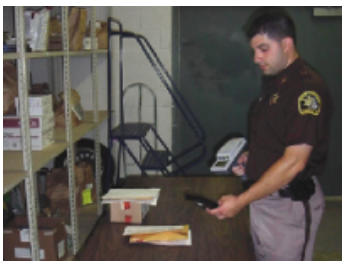
- planning the search
- executing the search
  - seizing hardware?
  - seizing information?
- recognizing relevant artifacts
- documenting the scene
- packaging and transporting th evidence

Portland State UNIVERSITY

19

The Investigative Process
Chain of Custody

- must enforce tight controls over evidence access
- must identify who has possession of the evidence and where it is at all times
- students learn the importance, and become accustomed to enforcing a chain of custody.



Portland State UNIVERSITY

20

Forensics Analysis of Seized Computers or information

- finding relevant electronic evidence
  - user created files
  - computer created files
- places to look
  - requires specific knowledge of OS, file system and/or software packages
- following a documented investigation process

Portland State UNIVERSITY

Recognizing Electronic Evidence – User Created Files

- Address books
- E-mail files
- Audio/video files
- Image/graphics files
- Calendars
- Internet bookmarks or favorites
- Database files
- Spreadsheet files
- Documents or text files

Portland State UNIVERSITY

Recognizing Electronic Evidence – Computer Created Files

- Backup files
- Log files
- Configuration files
- Printer spool files
- Cookies
- Swap files
- Hidden files
- System files
- History files
- Temporary files

23

Portland State UNIVERSITY

Recognizing Electronic Evidence – Places to look

- Bad clusters
- Computer date, time, and password
- Deleted files
- Free space
- Hidden partitions
- Lost clusters
- Metadata
- Other partitions
- Reserved areas
- Slack space
- Software registration information
- System areas
- Unallocated space

24

Portland State UNIVERSITY

Primary Search and Seizure Reference

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section - Criminal Division, United States Department of Justice, July 2002

www.cybercrime.gov/s&smanual2002.htm

25

Portland State UNIVERSITY

Primary Electronic Crime Scene Management Reference

Electronic Crime Scene Investigation: A Guide for First Responders, U.S. Department of Justice, July 2001

www.ncjrs.org/pdffiles1/nij/187736.pdf

26

Portland State UNIVERSITY

Primary Evidence Presentation Reference

Digital Evidence in the Courtroom: A Guide for Preparing Digital Evidence for Courtroom Presentation, The National Center for Forensic Science, March 2003

www.ncfs.org/DE_courtroomdraft.pdf

Portland State UNIVERSITY

File Systems and Evidence Recovery

- Basic file systems – start with FAT, advance to NTFS
- Disk organization
  - master boot records
  - partitions
  - file allocation tables
  - adding and deleting files

Portland State UNIVERSITY

Recovering Deleted Files

- use debug to re-link deleted FAT files and recover block chains
- use open source forensics tools to explore common evidentiary artifacts (logs, cookies, MAC times, browser cache, etc.)

Portland State UNIVERSITY

Internet Evidence

- Cookies
  - location, content, cookie tools
- Browser Cache
  - location, tools

Portland State UNIVERSITY

Facilities and Resources

- minimum computing resources
- the “evidence locker”
- Helix – a universal forensics environment
- commercial tools you should know about
- *structured around teams of students that work on a project throughout the term*

Portland State UNIVERSITY

Minimum Computing Resources

• at least one computer per team w/Internet access

• Windows XP or Win2K

• lots of RAM (>1G)

• requires removable hard drive and spare drives

Portland State UNIVERSITY

The “Evidence Locker”

• allows teams to secure their evidence – one locker per team

• maintains chain of custody with checkout log

• old gym lockers with combo locks are perfect

Portland State UNIVERSITY

33

Helix – a Universal Forensics Environment

- open source forensics environment - custom distribution of Knoppix Live Linux CD
- modified to NOT touch the host computer in any way
  - will not auto mount swap space, or auto mount any attached devices
  - is forensically sound
- Windows autorun side for analysis of live Windows systems

available at
www.e-fense.com/helix/

Portland State UNIVERSITY

34

Commercial Tools

- Encase
- FTK
- NTI tool suite

35

Portland State UNIVERSITY

The Project – Phase I
3 weeks

- team provided with a 20G removable hard drive, formatted using FAT-32
- team selects a *primary* and *secondary* crime from a list of pre-approved crimes - and prepare a *crime summary* for the primary
- team uses standard productivity tools found on the hard drive to manufacture evidence relevant to the primary and secondary crimes
- wide range of evidence to be manufactured

36

Portland State UNIVERSITY

Sample Crime Summary

Mr. B. Bucks, received a complaint from Joe Smith claiming his credit card was used fraudulently to purchase goods from Mr Bucks' e-store, StuffRUS. The order in question was placed on Saturday, September 16th at 1:46 PM. The order totaled $8,607.99 and was placed using Smith's credit card # 1231123113131 with a confirmation e-mail to c43630@hotmail.com. The merchandise was reportedly delivered to Mr. Smith's residence at 7605 Wabash Avenue, in Portland, Oregon using Next Day delivery. However, Smith was out of town September 15th - 21st at a family camping trip in Little Rock Arkansas. The confirmation e-mail address was registered to a bogus name,

Mr. Bucks' IT team identified the IP address of the computer used to place the order to be 168.1.23.1. The owner of that IP Address is Portland State University. PSU's IT team determined from their server logs, the IP address was leased to a wireless MAC address 00-0F-3D-0E-CE-E1 between 1:00 PM and 3:00 PM September 16th. The MAC prefix 00-0F-3D is assigned to the D-LINK Corp.

While taking a statement from Smith, he stated that he discovered he lost his credit card after visiting "The Camping Supply Store" in Beaverton Oregon. He also said he talked about his trip to the employees at The Camping Supply Store and told them he was going to be gone for a week.

The investigators visited The Camping Supply Store and interviewed the employees. One of them, Ed Reed, said he was a student at Portland State University, and the investigator noticed he was carrying a laptop computer with a D-Link wireless card. The manager told the investigators Ed usually worked on Saturdays, but on the 16th, he had asked for the afternoon off to study for an examination at the university.

37

An Electronic "Hogan's Alley"

- manufactured e-commerce site (StuffRUs)
  - team provided with a POP-3 e-mail account and a mail client
- www.cs.pdx.edu/~warren/Store
- leaves cookies and sends confirmation e-mails for later forensics discovery

38

Portland State UNIVERSITY

The Project – Phase II
3 Weeks

- evidence disks and crime summaries are randomly swapped among teams in the class
- each team is tasked with identifying and recovering relevant evidence within the context of the crime summary
- based on the crime summary and statutes, the team can establish the most appropriate crime, and enumerate the elements of the crime.
- once elements of the crime are identified, the team knows facts to be proven.

Portland State UNIVERSITY

39

The Project – Phase II (cont)

- teams began by imaging the original evidence disk to create a working investigation disk
- the investigation disk is signed in and out from the locker using a chain of custody form.
- working notes are stressed as a way to avoid repeating operations and preventing the team from overlooking an analysis yet to be done
- each team is provided with a Helix CD but given broad leeway in tools.

Portland State UNIVERSITY

40

Standard References for Teams

- ALTHEIDE, C., “Forensic analysis of Windows hosts using UNIX-based tools”, *Digital Investigation*, September 2004, pp 197-212.

Portland State UNIVERSITY

The Project – Phase III

- each team delivers a Power Point presentation to the class documenting the examination
  - the crime and its elements
  - location of the evidence
  - how it was found
  - its relevance to the crime under investigation
- assessed on
  - ability to explain how the evidence was retrieved and its significance.
  - ability to articulate details of their tools to a non-technical audience
  - technical correctness

Portland State UNIVERSITY

Slides and Course Materials are Available at

- www.cs.pdx.edu/~warren/forensics
- login: forensics
- password: ccsc

Portland State UNIVERSITY