Design and Implementation of Digital Forensics Labs: A Case Study for Teaching Digital Forensics to Undergraduate Students

Hongmei Chi, Christy Chatmon, Edward Jones, and Deidre Evans

Computer and Information Sciences Department
Florida Agricultural & Mechanical University
Overview

- IA at FAMU-CIS
- Our approach to teaching digital forensics
- Student responses
- Conclusions/Future Works
- Questions
Introduction

- 90% of current crimes involve computers in some way

- Computer criminals/violators leave a lot of clues & digital evidence
  - An employee is suspected of violating a company’s Internet-usage
  - A hard disk is found in the house of a suspected terrorist
  - Abnormal logs are observed on a server – a security breach is suspected
  - A person is suspected of a murder or kidnapping
Introduction

- What is Digital Forensics?
  - The application of computer investigation and analysis techniques in the interests of determining potential legal evidence
  - Capturing and Classifying digital evidence

- Increased need for computer forensics professionals and technicians → growth in digital forensics education & training
Introduction

- **FAMU:**
  - 13,000 students with 95% being African-American

- **FAMU CIS:**
  - 300 undergrads and 30 graduate students enrolled in Department of Computer and Information Sciences
IA at FAMU-CIS

- Positive track record in Information Assurance Education (IAE)
  - Three-course undergraduate IA curriculum track certified by NSA and CNSS training standards
    - NSTISSI 4011 (INFOSEC Professional) [2005-11]
    - NSTISSI 4014 (Information Systems Security Officer – EL) [2005-08]
    - NSTISSI 4012 (Senior Systems Manager) [Preparing for Review]
### IA at FAMU-CIS

- FAMU’s CIS positive track record in IAE

<table>
<thead>
<tr>
<th>IA Courses</th>
<th>Year</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS 4360: Intro to Computer Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>30</td>
<td>24</td>
<td>44</td>
<td>30</td>
<td>18</td>
<td>27</td>
<td>173</td>
</tr>
<tr>
<td>CIS 4361: Applied Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>N/A</td>
<td>38</td>
<td>21</td>
<td>40</td>
<td>17</td>
<td>15</td>
<td>131</td>
</tr>
<tr>
<td>CIS 4364: Digital Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>12</td>
<td>16</td>
<td>17</td>
<td>45</td>
</tr>
<tr>
<td>Certificates Awarded</td>
<td></td>
<td>N/A</td>
<td>5</td>
<td>10</td>
<td>29</td>
<td>7</td>
<td>6</td>
<td>57</td>
</tr>
</tbody>
</table>
IA at FAMU-CIS

- Stand-Alone Security Lab
Our Approach to teaching DF

- Skills needed for DF Professionals:
  - Legal Procedures & Laws of Evidence
  - Investigative Techniques
  - Computer Technology

- Audience for our DF Course
  - Computer Science majors
  - Criminal Justice majors
  - Local law enforcement
Our Approach to teaching DF

- Course accommodations for non-CIS majors:
  - (Lectures) introduce relevant computing concepts & terminology
  - (Hands-on Labs) apply computing concepts directly to tasks related to digital forensics
Our Approach to teaching DF

- (2) types of hands-on lab assignments:
  - Windows-based labs (Introductory)
    - To prepare those students with less computing knowledge & experience
  - Windows and Linux based labs (Advanced Topics)

- Blended lab student teams (CJ & CIS)
  - To ensure that teams have subject matter expertise & technical knowledge
  - To facilitate exchange of knowledge
Our Approach to teaching DF

- Labs are designed to expose students to:
  - Evidence Identification
  - Preservation Extraction
  - Documentation
  - Interpretation

- Labs cover four aspects of investigations:
  - Email investigation
  - Web activities investigation
  - Window registry investigation
  - Live and memory investigation
Our Approach to teaching DF

- **Teaching DF: Challenge #1**
  - Commercial DF tools are expensive
    - Average cost - $3,000 to $5,000 per license

- **Solution:**
  - Open source & freeware forensics tools
Our Approach to teaching DF

<table>
<thead>
<tr>
<th>Tool:</th>
<th>Features:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cain Abel</td>
<td>Password recovery for Windows</td>
</tr>
<tr>
<td>SAMinside</td>
<td>Password recovery for Windows</td>
</tr>
<tr>
<td>John The Ripper</td>
<td>Password recovery for Windows and Linux</td>
</tr>
<tr>
<td>Camouflage</td>
<td>Digital steganography</td>
</tr>
<tr>
<td>Helix</td>
<td>Imager; Password recovery; Cookie viewer; Internet history viewer; Register viewer; File recovery; Protected storage viewer; Scan for pictures</td>
</tr>
<tr>
<td>Sleuth</td>
<td>Create timeline of file activity; Sorts files based on file type; Performs extension checking and hash database lookups; Analyze image partition structures process data units at content location</td>
</tr>
</tbody>
</table>
## Our Approach to teaching DF

<table>
<thead>
<tr>
<th>Tool:</th>
<th>Features:</th>
</tr>
</thead>
<tbody>
<tr>
<td>WinHex</td>
<td>Disk editor; Data recovery; Analyze and compare files; Disk cloning; Drive and file wiper; Encryption</td>
</tr>
<tr>
<td>Log Parser</td>
<td>View event log; View the registry; Use queries to retrieve valuable information from data</td>
</tr>
<tr>
<td>Paraben Demo</td>
<td>Cell phone forensics; Email investigation</td>
</tr>
<tr>
<td>AccessData Forensic Toolkit (FTK)</td>
<td>Imager; Registry viewer; Password recovery; Query searching; Data carving; Integrated viewers and media player to view any set of data</td>
</tr>
</tbody>
</table>
Our Approach to teaching DF

- **Teaching DF:** Challenge #2
  - Finding *real data* for students to practice their skills

- **Solution:**
  - Honeynet project ([http://www.honeynet.org/challenges](http://www.honeynet.org/challenges))
    - Deploy honeynets all around the world, capture attacks in the wild, analyze this information and share findings
    - Three types of challenges offered:
      - Scan of the Month Challenges
      - The Reverse Challenge
      - The Forensic Challenge
  - New case studies posted often *(no longer updated monthly)*
  - Useful to help security community develop forensic and analysis skills to decode real attacks
Our Approach to teaching DF

- Scan24 challenge case study: *(example)*
  
  **Scenario:**
  
  - Joe Jacobs, 28, was arrested yesterday on charges of selling illegal drugs to high school students.
  - Local police officer posed as a student at Smith Hill High School and was approached by Joe to purchase marijuana.
  - Jacobs has denied selling drugs at any other school and refuses to provide police with the name of his supplier/producer.

http://old.honeynet.org/scans/scan24/report.txt
Our Approach to teaching DF

- Scan24 challenge case study: (example)
- **Student task:**
  - The police have imaged the suspect’s disk and have provided you (the student) with a copy.
  - Examine the disk and provide answers to the following questions:
    - Who is Joe Jacob’s supplier of marijuana, and what is the address listed for the supplier?
    - What crucial data are available within the coverpage.jpg file, and why is this data crucial?
    - What (if any) other high schools besides Smith Hill High School does Joe Jacobs frequent?
    - For each file, what processes were taken by the suspect to mask them from others?
    - What processes did you (the investigator) use to successfully examine the entire contents of each file?
- **(Bonus Question):**
  - What Microsoft program was used to create the Cover Page file? What is your proof (Proof is the key to getting this question right, not just guessing).
Student Responses

- Overall very positive responses

- Feedback from a few students:
  - “The labs use real-world cases. Solving these real challenge cases inspired me to work in a digital forensics related field in the future.”

  - The hands-on labs using FTK, Helix, and Slueth Tools and being able to act as investigator is very interesting. I would like to work as a digital forensics professional in the future.”

- Student term project:
  - Design a lab assignment using one or two open source tools.
Future Works

- Expand the design variations of our labs using the most popular forensics tools
- Explore other design approaches to ensure that the labs are adaptable to different levels of student expertise (non-major service course for the university)
- Develop a set of hands-on labs playing games/competitions using such environments as CyberCl EGE
Conclusion

- Hands-on labs were most useful to help students grasp difficult concepts and procedures, especially the non-majors

- Utilizing open-source tools & available “real data” to analyze, gave the students a rich experience and increased excitement about potentially pursuing an information security related profession
Questions?