Workshop: Computer Forensics

Chris Malinowski
Computer Science and Management Engineering
CW Post, Long Island University
cmalinow@liu.edu

ABSTRACT

The expected duration is approximately three hours, and participants should have their own laptops running Windows as that is the format of the demonstration software. The number of participants would be limited only by seating and power considerations (battery life versus AC-power). In the event that any participants wish to discuss issues subsequent to the workshop, such discussion can be held over dinner, etc.

While I will stress that there are several software suites available, I intend to focus on EnCase simply as a) it has the largest client base, and b) time considerations will constrain us. Additionally, while I can provide a "full-blown" FTK package, their demo version is currently limited to 5,000 files. If I can either obtain a suitable "case" or cobble one together, then I will do so and also present the FTK demonstration. I can have EnCase 'demo disks' available for participants, however the CD's used for the workshop will unfortunately be collected (contractual obligation).

The non-EnCase discussions will be on PowerPoint (slides will be available) and will provide a nice backdrop for those skills required by Computer Science (not necessarily Information Systems) students. The GUI suites however *can* provide IS student considerations, allowing educators to consider projects which may be appropriate for specific courses, and in fact meld together CS and IS students in a combined project.

Computer Forensic Workshop

1. **Introduction: (0:15 m)**
    - What is computer / network forensics?
    - What skills are required?
    - How does it fit into the CS / IS education model?
2. **Tools required (0:20 m)**
    - Platform (Windows / Linux)
    - Available tools
        - Capabilities
        - Limitations and problems
3. **Forensic software suites (0:15 m)**
    - PowerPoint on available software suites
        - FTK
        - EnCase
        - Smart (Linux)
4. **Break (0:10 m)**
5. **Hands-on Demonstration**
    - Reprise terminology and definitions (0:10 m)
    - Demonstrate acquisition (CD / Floppy only) (0:05 m)
    - EnCase demonstration disk
        - Features walkthrough (0:20 m)
            - Views available to investigator
                - Setting focus within a case
                - View “documents”
                    - Examine document (hex / context)
                    - Identify deleted files
                        - Recoverable?
            - Searching
            - Bookmarking
            - Documenting
6. **Break (0:05 m)**
7. **Participant Exercises (0:50 m)**
    - Examine evidence
        - Locate files
        - Discrepancies?
        - Conclusions about evidence / case
8. **Q & A (0:10 m or ‘whatever’)**
9. **Further Discussion if required (working lunch / dinner location – “Dutch treat”)**