Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2004 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2004

A Model and Guide for an Introductory Computer Security Forensics Course

Doug White
Roger Williams University

Alan Rea
Western Michigan University

W. Brett McKenzie
Roger Williams University

Louis Glorfeld
University of Arkansas

A Model and Guide for an Introductory Computer Security Forensics Course

Doug White
Roger Williams University
dwhite@rwu.edu

Alan Rea
Western Michigan University
alan.rea@wmich.edu

Brett McKenzie
Roger Williams University
wmckenzie@rwu.edu

Louis Glorfeld
University of Arkansas
lglorfeld@walton.uark.edu

ABSTRACT

This paper discusses the critical need for instructors to bring aspects of computing forensics into Information Technology courses and posits that we make computer forensics a course—or a major portion of a course—offered under the auspices of IT security across all IT-related disciplines, but especially those with a business orientation.

To facilitate computer forensics implementation in IT courses, the authors briefly discuss the major aspects of computer forensics, such as legal investigations and policy formation. The authors primarily focus on aspects that most IT students will be involved in during this process: collection, logging, verification, and preservation of electronic evidence needed by investigators.

Topics include both managerial and technical aspects. Students learn how to develop investigative documentation and study chain of custody documents. They also learn how to safely handle hardware to capture, examine, and preserve disk images, analyze system log files, and find hidden and deleted files.

Keywords

Computer Forensics, Security, Education

INTRODUCTION

The word forensics is defined as *pertaining to law* (Brown, 2003). Forensics has long been the study of the collection and preservation of information. In particular, computer forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis (Kruse and Heiser, 2002). This type of study is particularly relevant to computer crime scenes and other events. In the simplest computer crime scenarios, an investigation may involve the standard techniques used at any physical crime scene, but the task has become more challenging with the advent of computer networks and the Internet. Modern cyber-criminals may utilize groups of networks and many compromised computers to implement an international crime that while detectable, is very difficult to prosecute. In fact, Kabay (1998) concluded that only about 10 percent of attacks against computer systems were reported to any kind of authority or the public. Kabay also found that U.S. Department of Defense (DoD) studies showed very few attacks were even detected by managers.

In the past, electronic evidence was non-discoverable and difficult to admit in the evidentiary process. Today, it is law in the United States that information generated and stored on computers and in other electronic forms is discoverable (Feldman and Kohn, 2001). This has created a distinct need for experts who are able to forensically analyze and develop evidence that is electronic in nature as a part of the discovery process for civil and criminal litigation (Feldman, 2001). Today, the need for forensics experts is more pressing than ever (Warrick, et al., 2001) and students need to have the opportunity to study these techniques to move into analytical areas of the IT security field.

Computer forensic analysis is complicated and requires extensive knowledge before anyone might be encouraged to actually conduct an investigation. Although this paper does not cover specific knowledge or methodology for the analysis of particular items, it provides a guideline for the implementation of an introductory course IT forensics (or the inclusion of forensic components in existing courses). A working knowledge of hardware, software, various operating systems, as well as the tools used in the analysis all present a daunting collection of information to present in a course. Add to this the legal components and need for quality documentation, and the course will provide a challenging experience for both the instructor and students.

LITERATURE REVIEW

An initial examination reveals that a great deal of the Computer Forensics coursework is offered as professional development rather than traditional academic coursework. However, institutions are beginning to develop coursework in the area. The National Institute for Justice in conjunction with The University of Central Florida, maintains a list of institutions that offer complete programs. These include James Madison University, Purdue University, the University of Central Florida, and Utica College (NIJ, 2004). Many community colleges and other universities are currently offering courses in the Forensics area. This implies that the field is rapidly developing as a university curriculum.

For this paper, four different syllabi were used in the development of a new course syllabus described in this paper (Appendix A). While most of these courses were being delivered from criminal justice studies divisions, the content of the coursework is similar. Additionally, the guidelines (Appendix B) specified by the Southeast Cybercrime Institute (SCI) define key criteria for both the Certified Computer Examiner and the Certified Computer Forensic Examiner, professional certifications in the field.

COMPUTER FORENSICS PROCESSES AND COURSE IMPLEMENTATION

Forensics is derived from the law and is therefore subject to specific local laws and evidentiary process. This in turn creates a difficult environment for forensics specialists who—much like lawyers and other professionals—must be familiar with a great many different processes and prevailing legal structures. The following section will outline the process of computer forensics analysis and how this process might be covered in an introductory course. Computer forensics revolves around a fairly simple process that is difficult to implement: 1) Determine an Analysis is Warranted, 2) Obtain Evidence, 3) Validate and Verify Evidence, 4) Analyze Evidence and 5) Develop Documentation. See Appendix C for a detailed topic outline.

Determine an Analysis is Warranted

Before any sort of analysis is conducted, it is critical that the examiner determine that both the Fourth Amendment of the U.S. Constitution (in the case of criminal investigation) and company policy have been reviewed. In both cases, it is necessary to involve either law enforcement or corporate legal representatives to accurately assess the situation and determine that any action taken will not result in harmful action on the part of the investigator. Review of the U.S. Department of Justice website (http://www.usdoj.gov/criminal/cybercrime) is also recommended to determine the current position on various types of federal cybercrimes.

In the case of corporate activity, policy must be a guide to action. These investigations involve private companies and lawyers who address company policy violations and litigation disputes, such as wrongful termination (Nelson, et al. 2004). While not subject to the Fourth Amendment, company investigations must nevertheless adhere to legal guidelines and more importantly, organizational policy. Much like criminal law, litigation is likely the outcome if individuals are dismissed or chastised for violations of a policy which does not exist.

Unlike security systems implementations, which are typically assessed on a risk vs. return approach for cost considerations, the benefit of a forensics analysis cannot be assessed in terms of dollars. Typically, the determination of the need for forensics analysis should be initiated if either a criminal investigation agency or the organization’s legal and human resouces staff has determined that a need for investigation exists and that the examiner ascertained that the admissibility of evidence in court can be achieved. This is often a challenge for IT staff who are not properly trained in law or well versed in corporate policy and the laws pertaining to admissibility of evidence in the court system.

Thus, an introductory IT forensics course should include materials which cover both Fourth Amendment law, corporate and civil policy law, and the laws of evidentiary procedure. Most textbooks on forensics and the study of cyber-crime have basic coverage of these procedures. Emphasis should be placed on students understanding the need for legal counsel to ensure that evidence is admissible in either civil or criminal proceedings which may result from the forensics analysis. Equally important is the understanding that action taken as a result of an analysis, particularly in regard to employee activity, also falls under these guidelines regardless of whether criminal activity is involved.

Obtain Evidence

After it has been determined that an analysis is warranted, the computer forensic specialist takes action. Making sure that clean, well-documented evidence is collected is a crucial function of computer forensics.

Logging Evidence

An IT forensics investigator knows that every action taken in regard to a suspect system must be logged and well documented if the evidence is to be useful. This is critical for maintaining a chain of custody of the evidence at hand. Kruse and Heiser (2002) provide the following questions which might be asked about the evidence logs:

- Who collected it?
- How and where was it collected?
- Who took possession of it?
- How was it stored and protected in storage?
- Who took it out of storage and why?

The process of logging the evidence begins before any other actions take place in order to secure the chain of custody. If this is broken, all of the evidence may not be useable in court and the analysis would be wasted.

In particular, logs of activity involving the computers and their handling are critical. Several key issues should be covered in the IT forensics course:

- Photographs and other documentation of the scene and the systems involved.
- Chain of evidence logs which detail the whereabouts, examination, contact, and storage of the evidence.
- Documentation of any actions taken regarding the evidence, in detail.
- Methodology for identification and tracking of the evidence.

This component of the course should provide the students with skills in notetaking and observation as well as organization and standard approaches to evidence management. The instructor should spend time discussing and conducting exercises on techniques as well as how to carefully document each piece of media, each image of the media, and any other materials related to the case in the chain of custody log. This may be done using commercial tools for logging activity or something as simple as Notepad with timestamps. These documents must be clear and concise and describe how the evidence and case materials were handled and secured.

The Collection Process

Once logs are in place, collection can begin. The primary focus of the collection process is to obtain a static image of the system which is being examined. In practice, organizations may only allow a snapshot of the system at a given point in time due to the inability to remove the machine from service. This process must be conducted in strict accordance with the rules of evidence and any actions taken on the machine should be heavily documented.

Particularly, imaging involves the creation of static images of the evidence for analysis. Analysis should rarely, if ever, be conducted on the actual evidence. Even booting the original drive will change the files on most operating systems and immediately, the validity of the evidence will come into question.

Ideally, the collection process involves a compromised system which can be identified and examined. In practice, this may be much more convoluted and involve multiple systems in multiple organizations which may have all been compromised in the commission of a crime. In the worst case, this may involve multiple jurisdictions or sovereignties, all of which may have varying rules for collection of evidence.

Collection of evidence is a challenging process but represents the major skill set to be developed in the forensics IT course. The primary skills for students to develop are care and documentation. Care means the students must learn that every action taken may create new problems.

Thus, students must learn to be observant of systems and to utilize techniques that are least obtrusive on the hardware they are examining. Initial activities should focus on remote booting from CDs and disk imaging techniques which do not trigger processes on the machine being examined. While this is an ideal situation which rarely exists in practice, it is nevertheless an important first step in the development of collection skills.

Validate and Verify the Evidence

After evidence is obtained and cataloged, it must be validated and verified to prove it is intact and admissible in proceedings. Two major issues exist in the management of forensic evidence: maintenance of integrity and timestamping (Kruse and Heiser, 2002). When an image has been created, it is important to provide validity of the image for future reference. This is typically done using two techniques for redundancy: MD5 hashes and CRCs.

MD5

A hashing algorithm such as MD5 is a means of creating a "hash" or "message digest" for the media. This is a small string that accurately describes the drive in its entirety. Creating such a hash for any images used is useful in demonstration that the image was unchanged from the original documented image. By comparing hashes on any image used, assurance is provided that the image is an exact duplicate of the original.

Covering this technique in the forensics IT course typically involves a limited discussion of MD5 and other hashing algorithms as well as a brief introduction as to how hashes are created. Most professional tools provide this as a matter of course, but in manual imaging, hashes will need to be created by the investigator.

CRC

CRC (cyclical redundancy checks) are also used as a secondary validation to insure that no changes are occurring on a more limited view of the data. This type of bitwise mathematics provides an additional piece of assurance that the image is legitimate and was unchanged during the copying process.

Careful notes should be taken to timestamp all evidence and document its origins, dates, and handling throughout this process. Time stamping will further assist in the analysis as times may be necessary to develop evidence and attempt to describe activities of the suspected user.

Analyze the Evidence

Finally, with the data collected and secured, analysis of the image of the original may take place. This analysis may be simply a listing of files and contents or may involve much greater complexity such as cryptanalysis if the disk has been encrypted in some fashion. It may be necessary for the examiner to slowly reconstruct the contents from hidden or deleted files or attempt to determine what sorts of things have been on the disk. Knowledge about disk formatting, swap files, and passwords and encryption is beneficial when undertaking an analysis of the evidence.

Disk Formatting and File Deletion

Many users believe that formatting media "erases" the media. This fallacy has led to the disclosure of private data and litigation when organizations dispose of equipment. It also has allowed investigators to recover evidence from media the suspect thought had been cleaned. Hard drives are not erased when formatted. In fact, neither the Microsoft Quick nor the Microsoft Full formats remove files from the data areas of disks. Formatting typically only removes the pointers stored in the file allocation table (FAT) on the disk and changes the filenames to have an unreadable first character. The files themselves are still residing on the disk and can be recovered by a variety of means. While this is an oversimplification of the process for the different systems listed, the idea is correct. This means that until the operating system needs the space which has been freed, the files remain there.

Most commercial tools support file and subdirectory recovery and this is certainly a heavily-used approach in most forensics training. Deleted files are recoverable by both manual means (dd, etc.) and commercial products such as WinHex and Norton Unerase. Other products allow for the examination of graphics files and their formats (JPG, GIF, etc.) and are of particular use in pornography cases. Many suspects are not sophisticated users capable of complex activity to secure their files, and even sophisticated users rarely DoD-wipe files when they delete them.

This implies that students should be exposed to a full spectrum of system tools and other custom tools that are available to deal with media as it is stored. Students also must understand the need for great caution when examining files, as opening files such as Word documents may trigger dangerous macros or cause accidental notification of the suspect (e.g., an automatic email receipt). Tools such as Quick View Plus should be made available to allow the students to examine files in a neutral environment.

Students should have the opportunity to examine actual disk images and to develop documentation of activities such as recovering deleted files and reconstructing both text and graphics remainders found on the image.

Hidden Files

Another avenue to explore is hiding data. A great deal of focus is often placed on dramatic sounding tricks like steganography but more commonly, users take advantage of simple approaches to hide data, such as using the hidden operators (in Unix/Linux the "." operator) for files or simply changing the nature of a file. For example, one could rename a JPG file as “WIN32.CAB” and place this on a floppy disk. Even if a security guard examined the media, he or she would likely not examine such a file. Windows will not handle the file correctly since it is not examining the header, but merely the extension to determine how it should be handled.

To defeat this tactic, most commercial forensics packages test signatures by examining the actual hexadecimal headers on the file rather than extensions. Again, however, the more the student knows about what is and is not “normal” with a file, the more agile the student will be as an investigator. So despite the James Bond approaches like steganography (which certainly exist), it is much more common to encounter James Smith techniques like changing the file's attributes to hidden or placing the files in a folder normally not examined.

Swap and Page Files

Another area in which forensics investigators commonly recover all sorts of information is from the swap areas that both Windows and Linux systems use to create virtual memory. It's common for these operating systems to create one- to one-and-a-half times the amount of RAM as virtual memory and use this to cache web pages and other information that is being used by the system. There is no easy way to encrypt this partition and have it remain usable, so most users simply allow the operating system to manage the swap space in terms of cleaning it. Certainly a regular DoD wipe of the swap space or some elaborate technique of encrypting the swap while the machine is not in use is possible, but, how many users are capable of this, and how many of those capable users would actually take such action regularly?

Thus, students should learn to examine the swap area using whatever tool the instructor has decided is appropriate. Recently visited websites, web-based email, passwords used on the Internet, Word documents, Notepad files, etc. are all possibly sitting in a swap partition waiting to be examined. The instructor is cautioned to contrive these portions of the image for class examination, as open examination of lab machines may result in embarrassing situations during class presentations.

Log Files

Another component of the process is the examination and understanding of log files. Almost any sort of operating system will contain at least a rudimentary logging system to record system events. Admittedly, log scrubbing is an assumption but most forensics investigations do not involve sophisticated hacking activity but rather average users who are either being investigated or have been arrested. Familiarity with the basic logging systems which are in use on standard platforms and better still, familiarity with approaches to logging which may enable the recovery of clues about activity will be rewarding to the investigator.

Basically, coverage of the standard logging tools, such as syslog or with Windows logging system, as well as the actual names of the log files (e.g. /var/log/messages) can provide the investigator with a great ability when looking at an image, particularly when looking at recovered files and directories. In Windows based systems this is more complex as the files are not stored in a straightforward manner. This may require the introduction of other tools such as REGEDIT and other registery tools which allow for examination of the more complex log storage approaches in use on a Windows machine.

It is also recommended to cover standard security tools in this section as they also generate logs for the system that even an experienced hacker may miss. Tools such as Tripwire and Whisker are commonly used on Linux based systems to provide insurance against file alteration and there are a wide variety of Intrusion Detection Systems (IDS) and other firewalling in use by most commercial organizations (on Windows and Linux).

The last item to point out is to be sure to have the students understand that time at the actual scene is precious and may be the only opportunity to visit the scene. Logs may be printed, tapes may be tossed in a corner. So, as with password recovery, leave no stone unturned while you have access to the scene. The logs deleted on the system may be sitting on a pile of printouts.

Passwords and Encryption

It is very likely a forensics investigator will encounter password-protected documents during his or her analysis of the evidence, simply because today it is so easy to password-protect files. In fact, Microsoft tools allow for easy password protection of almost anything. Encryption is also available in the form of PGP or other tools. These approaches make the investigator's job more difficult – but also may make it easier if passwords gave the suspect a false sense of security.

For example, a user who password protects an MS Word document containing stolen trade secrets may take no further steps to protect the information due to feeling secure with the password. Particularly, if the user has created a "strong" password he or she may feel safe from investigation. An investigator gains his or her advantage by learning to carefully examine the physical crime scene. A great many strong passwords have been compromised when it was found they were stored in the user's Rolodex or written on Post-It notes. Likewise, the investigator should carefully examine the operating system. Many users allow Windows and Linux to store their passwords and usernames on the system. This, as well as a login stored in a swap file, may provide an important clue to the password, as users often use the same passwords over and over.

Additionally, it may be possible to conduct "known plain text attacks" on encrypted files if a clean unencrypted copy of one of the files in an encrypted archive or set of files can be found in the swap partition of deleted folders on the image. This type of attack, which requires the exact file, would allow the extraction of the encryption key and subsequent cracking of the encrypted files in an archive.

It is also important to expose students to password cracking tools such as John the Ripper or commercial products such as AccessData Password Recovery Toolkit. But only as a last resort should "cracking" be attempted, since this is often difficult to achieve. If the suspect uses dictionary words or has the password stored on a hard drive, tools such as a "word list export" in Forensics Toolkit may crack the password very rapidly. However, if the user has a truly strong password, it may prove very challenging. Brute force attacks involve endless permutations of numbers, symbols, and letters, and may simply take too long in the investigation. PGP encryption may easily prove to be uncrackable in any sort of feasible time period.

Thus, the instructor is encouraged to develop scenarios for cracking which involve recovery of words and passwords from the disk rather than those that involve simple passwords. This is not to say dictionary attacks should not be tried, as many users may have passwords such as 777 or their pet's name, etc. But a good investigator should also be prepared to search out passwords from the drive or the physical desktop of the suspect.

Developing Documentation

Finally, the IT forensics analyst should develop documents for the client. This is the most important component of the process. These documents will become evidence and mistakes or misrepresentations in the documentation will have dire consequences when reviewed by opposing lawyers and experts. The documentation should be clear and concise, but should contain every detail of the examination as a component of the documentation. Essentially, documentation should contain:

- A summary
- Description of the analysis
- Findings and opinions of the investigators
- Appendices containing details of:
    - Chain of custody
    - Policies on handling evidence
    - Policies on imaging
    - Information on tools used in the examination
    - Other information relevant to the investigation

Students should be reminded that good writing practices, proofreading, and quality in their documentation will play a role in how they, as an investigator, will be perceived by a jury or opposing expert. Likewise, care should be taken to produce a thorough summary of the case as most people reviewing the opinions of the investigator are primarily interested in the findings, not the grim details of the analysis.

Virtually any component of the investigation can be called into question, and care should be taken to answer questions in the documentation rather than open holes for lines of questioning. Students have a great deal of difficulty with this part of the investigation, so many exercises are needed to help them develop sound methods for dealing with documentation.

CONCLUSION

This paper has provided the reader with an overview of some ideas for the development of computer forensics as a curriculum item. While the paper did not develop specific tools for use in a course, the authors hope to provide some guidance for those interested in the development of coursework in this area. With the increase in the use of technology in virtually all walks of life, a subsequent increase in the need for competent investigators in both law enforcement and civil activity will also rise.

Computer forensics is an exciting field that continually provides a challenge to the investigator to solve a puzzle with many pieces that are sometimes hidden in a dark room. Thus, instructors are cautioned to avoid “cookie cutter” laboratory exercises and coursework. Students must learn to solve problems which have no clear answer and in particular learn to solve problems which are different in each case. We suggest a topical outline as shown in Appendix C.

Thus, much like investigators of physical scenes, computer forensics investigators must have an eye for detail and an interest in solving unstructured problems if they are to succeed. Certainly, methodology may be followed, but the danger is becoming too methodical which may allow the investigator to miss details when the circumstances vary.

Every user and computer is subtly different in both ability and configuration. The forensics course should offer many challenges to the students to allow them to explore these differences and learn their own methods of solving these infinitely different problems.

REFERENCES

1. Brown, C. L. T. (2003) Developing Corporate Policies in Support of Computer Forensics, http://www.techpathways.com/uploads/CorporateForensicsSupport.pdf, July 17, 2003.
2. Feldman, J. E. and R. Kohn. (2001) Top Ten Things To Do When Collecting Electronic Evidence, Computer Forensics, Inc., http://www.forensics.com.
3. Feldman, J. E. (2001) Collecting and Preserving Electronic Media, Computer Forensics Inc., http://www.forensics.com.
4. Kabay, M.E. (1998) ICSA White Paper on Computer Crime Statistics, ICSA.
5. Kruse, W. G. II, and J. G. Heiser. (2002) *Computer Forensics: Incident Response Essentials*, Addison-Wesley, Boston, MA.
6. National Institute for Justice. (2004) http://ncfs.ucf.edu/, April 18, 2004.
7. Nelson, B., A. Phillips, F. Enfinger, C. Steuart. (2004) *Guide to Computer Forensics and Investigations*, Thomson/Course Technology, Boston, MA.
8. Warrick, J., J. Stephens, M. P. Flaherty, and J. V. Grimaldi. (2001) FBI Agents Ill Equipped to Predict Terror Acts, Washington Post. September 24, 2001. pp. A-01.

APPENDIX A: SELECT COMPUTER FORENSICS PROGRAMS AND SYLLABI

Course/Institution	URL
Canyon College: Introduction to Computer Forensics	http://www.canyoncollege.edu/cc/crim~jus/syllabus/cj475.htm
SUNY Tompkins Cortland: Computer Forensics	http://www.sunytccc.edu/academic/forensic/main.asp
Champlain College: Computer and Digital Forensics	http://digitalforensics.champlain.edu/
Wilbur Wright College	http://wright.ccc.edu/department/forensics/index.asp
Iowa Lakes Community College	http://www.iowalakes.edu/programs_study/social_human/criminal_justice/computer_forensics.htm

APPENDIX B: EQUIPMENT AND SKILL REQUIREMENTS

Certified Computer Examiner Requirements	
Software Requirements	http://www.certified-computer-examiner.com/soft.htm
Skill Requirements	http://www.certified-computer-examiner.com/skill.htm

APPENDIX C: SAMPLE COURSE OUTLINE

Sample Master Syllabus
Introduction to Computer Forensics and Electronic Discovery

Suggested Text: Computer Forensics – Warren Kruse II or other Forensics CCE/CFCE texts. Additional readings are provided based on current issues in the field as no given text can be current enough for the course.

Learning Objectives:

- Students should understand the fundamentals of computer hardware
- Students should understand the fundamentals of Linux, Windows, and other operating systems
- Students should understand how to retrieve hidden and deleted data from hard drives
- Students should understand basic principles of the evidentiary process
- Students should understand how to analyze hard drives and other images of media
- Students should understand how to develop reports for presentation in court

SUGGESTED WEEKLY COURSE SCHEDULE

Week	Topic	Application
1	Introduction to Forensics and Laboratory Protocols	Basic Use of Equipment
2	Evidentiary Process, Creating Data Images and Issues in Imaging	Building Chain of Custody Logs and Disk Hashing
3	Using AccessData and Sandstorm toolkits.	Tools for entire week
4	Using Quickview and other file management tools.	Tools for entire week
5	Developing Quality Reporting and Review of Existing reports.	Using AccessData to build reports.
6	First Practical Case. Analysis of Floppy Diskette Scenario	Analysis and Exam
7	Understanding Harddrive, CD, DVD, and other media forms	Analysis of Media
8	Analyzing Chat, Instant Messaging, AOL, and other Forms of Email.	Analysis of Media
9	Second Practical Case. Analysis of a CD-ROM Diskette	Analysis and Exam
10	Ethics and Legal issues surrounding the Examination of Media	Experiments with Other Forensics Tools (TCT, Autopsy(sleuth), and others)
11	Mock Court Examination of Defense and Prosecution Expert by Group	Lab Exercises in Court
12	Mock Court Examination of Defense and Prosecution Expert by Group	Lab Exercises
13	Hardware review of RAID, SAN, and Other massive storage issues for forensics	Examination of RAID
14	Final Practical Case. Analysis of Hard Drive Image	Analysis
15	Final Practical Case. Analysis of Hard Drive Image	Analysis and Exam

ADDITIONAL COURSE REQUIREMENTS (SUGGESTED)

1. Three practical examinations that are based on forensics examinations
2. One mock hearing that should represent 25% of the grade based on presentations and reporting.
3. Instructor might opt to allow students to take CCE examination as a component of the course.