June, 2008

The Power of Simple Hands-On Cyberforensics Exercises: A Guide for Faculty

Gary C. Kessler
Jim Hoag

Proceedings of the 12th Colloquium for Information Systems Security Education
University of Texas, Dallas
Dallas, TX June 2 - 4, 2008

The Power of Simple Hands-On Cyberforensics Exercises: A Guide for Faculty

Gary C. Kessler† and Jim Hoag,‡ *Champlain College*

Abstract – Computer forensics is a hands-on discipline. Introductory skills, however, can be taught using simple exercises that require neither expensive laboratory facilities nor even face-to-face courses. This paper describes a simple floppy disk analysis project that allows an instructor to address issues ranging from the computer forensics process and basics of file systems to long file names, file signatures, and hashing. Projects are essential to teaching this discipline as they support active learning, constructivism, and active learning. These hands-on projects also offer an opportunity for courses to be taught online and for students to build their own toolkits using open source or commercial software.

Index terms – computer forensics education, computer forensics training, file systems, hands-on exercises

I. Introduction

An increasing number of colleges and universities around the globe have started to offer programs in computer forensics and digital investigations, although this remains a relatively new discipline in undergraduate education [1]. While most of the programs were developed in response to requirements of the law enforcement community or governmental agencies [2,3,4], most of the growth currently comes from private sector organizations providing data recovery, electronic discovery (e-discovery), incident response, policy auditing, and third-party forensic analysis services [5].

Computer forensics courses may be offered as part of a larger digital forensics degree program or as a component of a criminal justice, computer science, information security, or other related discipline. It is imperative that these courses have hands-on exercises in order to reinforce:

- *Active learning*, which enhances student performance, reinforces skill knowledge, improves the students' attitude towards the course and material, and helps to create a sense of community among students and faculty [6,7].

- *Constructivism*, the learning theory that suggests that cognitive structures are the building blocks of learning and that learners use their existing cognitive framework to understand new subject matter. When faced with new material, students need to learn new cognitive structures *and* how to build the linkages between them. The goal of instruction, then, is to help the student learn how to apply new information to what they already know so that they synthesize and integrate the new material [7,8].

- *Problem-based learning (PBL)*, which uses "ill-defined" problems or scenarios to provide a fun and interesting way for students to synthesize and/or expand their knowledge. Because real-life problems tend to be more relevant and tangible than contrived situations, students usually are more motivated to work hard on these projects, often making many assumptions that are applicable to their experience or work environment, further helping to improve their problem solving skills. PBL is well-suited to constructivism because students apply what they know to fully define the problem and find what may be many solutions to the stated problem. PBL is also well-suited to the online environment because students are no longer limited to a finite lab time or the resources in the lab space; in many cases, this means that larger, more interesting problems can be devised by the instructor and solved using the Internet as an information resource. Hands-on exercises are the very foundation of PBL [9,10].

† *Associate Professor, Computer & Digital Forensics and Director, Champlain College Center for Digital Investigation, Burlington, VT; Adjunct Associate Professor, Edith Cowan University, Mt. Lawley, Western Australia. +1 802-865-6460, gary.kessler@champlain.edu.*

‡ *Assistant Professor and Program Director, Computer Networking & Information Security, Champlain College, Burlington, VT. +1 802-865-6459, jhoag@champlain.edu*

These pedagogic issues form the basis for Champlain College's Computer & Digital Foresnics (C&DF) program, which is offered both online and face-to-face. Hands-on exercises do not need to rely on large lab facilities or expensive software. Some very simple exercises can be employed both to introduce a wide variety of technical (and legal) topics and to provide the students with an opportunity to build their own forensics toolkits [11].

Section II of this paper will review the digital forensics process. This will be followed in Section III by a description of a simple introductory hands-on exercise used to cover a broad set of topics. Section IV will address some other issues related to hands-on exercises, followed by some concluding comments.

II. The Digital Investigation Framework

Every digital investigation is different because the nature of every computer and network is different, as are the cases being investigated, and the skill set and experience of the investigators themselves. Scientific crime scene investigation is a process, however, and digital investigations need a generic framework. One of the more common investigative models is the following six-step process devised by the Digital Forensics Research Workshop [12]:

1. *Identification* refers to the method by which an investigator learns that there is some incident to investigate. Many events have an innocuous explanation so that this step is where triage occurs, and incidents need to be categorized to determine the appropriate response.
2. *Preservation* describes the steps by which the integrity of the evidence is maintained. The evidentiary chain is critically important to law enforcement (LE) and the use of any information in court, but also has ramifications to non-LE exams; if evidence data is altered (particularly in any unknown way), the examiner has no true idea of what is being examined.
3. *Collection* is the process by which data from the evidence medium is acquired. This step includes the hardware and software, and policies and procedures, used to gather the evidentiary information.
4. *Examination* addresses how the evidence data is viewed. This step deals with the tools and procedures to sort through and examine the evidence (within the constraints of a search warrant or other set of instructions that define the scope of the exam).
5. *Analysis* is the means by which an investigator draws conclusions from the evidence. This is the stage where the fruits of the digital investigation join with the rest of the criminal investigation. Digital evidence frequently provides important clues with which to solve a case and/or secure a conviction, but rarely alone is the basis for a conviction.
6. *Presentation* refers to the methods by which the results of the digital investigation are presented to the court, jury, or other fact-finders. The reporting of evidence, particularly digital evidence, is one of the hardest parts of the computer forensics process for two primary reasons. First, most lay people do not understand the technical aspects of how this information has been acquired. Second, television shows such as the *Law & Order* and *CSI* franchises have set a level of expectation by the lay public that suggests that all pertinent evidence will jump right out at the examiner. The reporting of the evidence has to convincingly show the intended audience how the evidence was acquired, examined, analyzed, and interpreted.

One might observe that each step in the digital forensics process has a parallel (albeit not an exact one) to Bloom's taxonomy of the cognitive domain, i.e., the framework above moves up the spectrum of knowledge, comprehension, application, analysis, synthesis, and evaluation [13]. Practical skills focus on the first three categories and education builds on those skills to develop the student's capabilities in the latter three categories. Hands-on exercises are clearly important in reinforcing both skills and education.

III. Computer Forensics With a Floppy Disk

The discussion above about the digital forensics process makes the need for hands-on exercises clear. This section will describe one such exercise in detail that exemplifies how many topics can be covered even in a single exercise. All of the hands-on exercises in the C&DF program are employed in both online and face-to-face courses.

A. Floppy Disk Analysis Exercise

The exercise described here is a simple analysis of a floppy disk, based on a challenge posted on the Web [14] and modified by the first author. In this exercise:[1]

1. Students are directed to download a ZIP file containing the forensic image of a floppy disk. Each student is assigned a different ZIP file, each of which has a unique Message Digest 5 (MD5)

[1] The exercise, image files, and lecture material for this sample assignment can be found at http://digitalforensics.champlain.edu /reference/project2.zip.

hash value. Part of the assignment is to verify the file's MD5 hash and calculate the Secure Hash Algorithm (SHA) hash value.

2. Students unzip the file to recover a dd image of a floppy disk and read a report laying out the problem assignment scenario. The assignment requires the students to answer a series of questions about the contents of the disk.
3. Students are advised that they can directly examine the dd image file or restore the image to a floppy using *rawrite*. Analysis can be performed using any hex editor and links to a demo version of WinHex are provided.
4. The floppy disk contains three files, two of which have been deleted. Examination of the root directory (Figure 1) shows a deleted .DOC file, a deleted .JPG file, and an .EXE file.

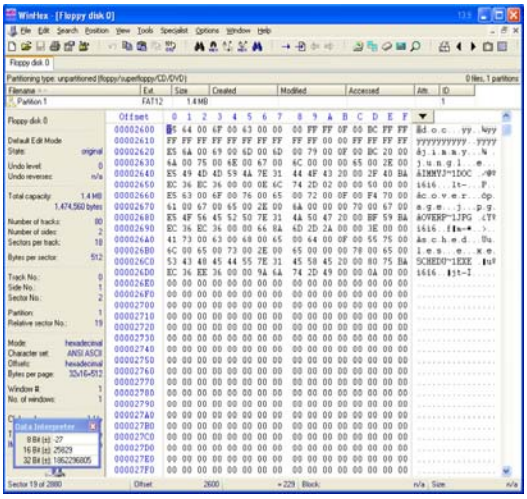

Figure 1: Root directory of the subject floppy disk, viewed by WinHex

5. Students are led through a process of recognizing file signatures and performing data carving so that they can recover the three files.
6. The first file has an MS Office signature at the beginning of the file and a Word document subheader at byte offset 512. Students need to recover the file and answer a question about its contents.
7. The second file has the file signature of a JPEG image (Figure 2). Students need to recover the file and answer a question about it.
8. The file slack of the JPEG file contains two character strings that start with "pw1=" and "pw2=", representing two passwords (Figure 3). The first password is different in every dd image; this makes each file unique and is the reason that the MD5 hash values are unique.
9. The third file has a .EXE file extension but the file signature indicates that it is a ZIP archive rather than an executable file. After recovering the file, the students will find that it is a password-protected archive; if they employ one of the passwords found in the JPEG file's slack space, they can open the file and answer questions about its contents.

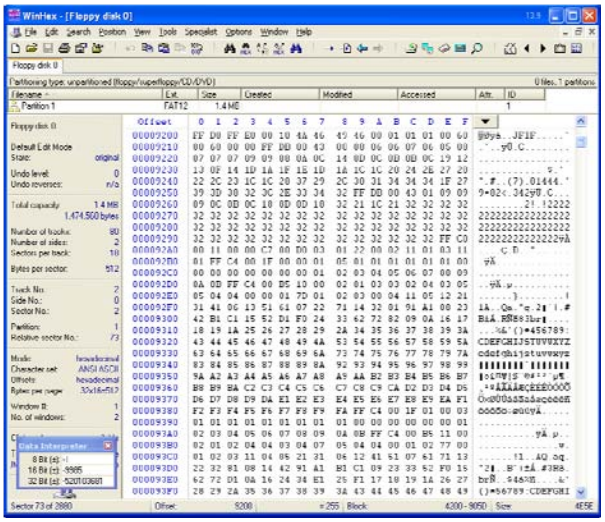

Figure 2. Start of JPEG file; note file signature in first 10 bytes.

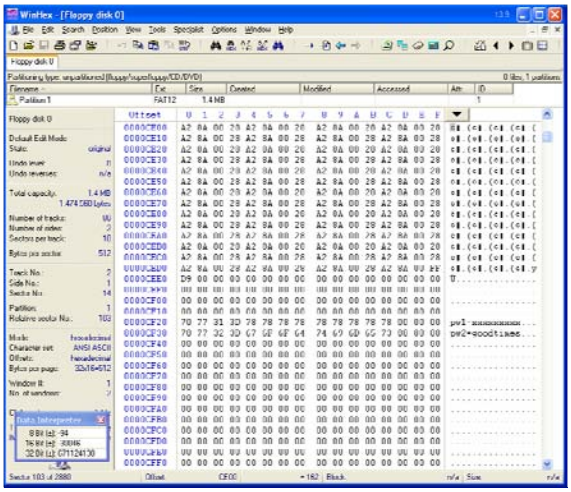

Figure 3. JPEG trailer (0xFF-D9) followed by hidden strings in file slack space.

The exercise itself is tool-agnostic. Although WinHex is the suggested tool-of-choice, any hex editor might well be used. While more powerful forensics tools such as

EnCase, FTK, or ProDiscover could be used with this exercise, they do not allow the user to see the logical structures of the file system as well as a hex editor.

B. Expected Learning Outcomes of the Exercise

An understanding of file systems is essential for any computer forensics examiner. Without that understanding, the forensics examiner is merely a button pusher that accepts whatever the forensics software reports, without truly knowing what is going on under the hood [15]. One of the first hands-on projects assigned in Champlain College's Computer Forensics I course is the examination of a floppy disk. Although a floppy disk is a relatively trivial media, this exercise allows for the discussion of a broad set of essential topics, including:

- *Generic issues related to file systems:* All file systems have a number of issues in common, such as logical structures containing user content (i.e., data) as well as logical structures with information about the data container (i.e., metadata). All file systems have some form of organization, such as directories and files. File systems use pointers and linked lists to map logical structures to physical addresses. Hardware allocation units (e.g., sectors) and software allocation units (e.g., clusters or blocks) are defined by the media and operating system; slack space results in the difference between the amount of user data and the size of these allocation units, and offers a location in which to hide data. Unallocated space offers additional locations in which to hide data and/or recover "deleted" files. All file systems have some set of steps by which a file is created and deleted. The foundation to understanding even a floppy disk requires the introduction of all of these basic concepts.

- *Issues related to a specific file system:* In the Windows/DOS environment, a floppy disk uses the FAT12 file system. FAT12 is a simple file system for the instructor to teach and the student to learn. A thorough understanding of FAT12, however, leads one to understand the fundamental concepts of file systems in general. In addition, knowledge of FAT12 makes learning FAT16 trivial, pushes the student up the learning curve for understanding FAT32, and aids in the understanding of the NTFS and ext file systems. Knowledge of FAT12 also helps the student understand file systems used on alternate media devices, such as CDs, DVDs, and mobile devices.

- *Data carving:* Recovering the contents of deleted files on a floppy often requires software to carve data process of searching unallocated space for the clusters comprising a "deleted" file

In addition, other concepts related to file systems can be introduced and demonstrated, including:

- The interaction of the modified, accessed, and creation (MAC) times associated with each file
- The relationship and features of long and short file names
- The role of file signatures in determining the contents of a file
- The use of hash values in verifying that two files appear to be identical

C. Other Hands-On Exercises

Additional hands-on exercises are employed throughout the C&DF curriculum to build students' practical skills, all with the object of teaching students about the computer forensics process, making them aware of the different forms of digital evidence, and demonstrating a myriad set of tools. The exercises cover a breadth of topics related directly to computer and network forensics, as well cryptography, steganography, and other forms of anti-forensics.

All of the exercises in the program are tool-agnostic, except for a few that are designed specifically to help the student gain familiarity with specific tools (e.g., EnCase, FTK, Helix, and ProDiscover). Other hands-on exercises include:

- Cyberforensics-related aspects of the Internet and Internet-based investigations using domain search tools such tools such as DNSstuff.com, SamSpade, and *whois*, as well as tools to examine e-mail headers, browser histories, chat and messaging logs, and social networks.

- Packet sniffing tools to examine network traffic, including issues related to examining wireless local area networks.

- Examination of the file system of a code-division multiple access (CDMA) cell phone to find such information as the phone's banner message, phone number, PIN, voice mail code, service provider, call history, text (SMS) messages, and multimedia images.[2]

[2] A sample cell phone image file can be found at http://digitalforensics.champlain.edu/reference/cell_phone.zip.

- Imaging RAM using tools such as dd and Helix, and using a variety of tools for RAM content analysis. (This exercise is particularly interesting to students because they are looking at contents of a system with which they are ostensibly familiar and even then are surprised by what they find in RAM.)

As students progress through the program and use more tools, one project is to create a rubric for comparison and then to actually apply their own perspective about which tools are best for different types of forensics functions, e.g., previewing a system, searching for graphic images, examining e-mails, data carving, live system imaging, report generation, etc. This helps students determine which tools best handle different kinds of digital evidence.

Hands-on exercises do not just refer to the use of technology. All courses include a writing component and later courses focus on report writing, testimony preparation, electronic discovery, rules of evidence, and civil and criminal procedures.

IV. Hands-On Exercises Revisited

Digital forensics students need a solid understanding in the computer forensics process and an exposure to as wide a variety of tools as possible. Our courses do not focus on expertise in any one piece of software because it is just not practical; if students focus on Software X version 3 in their sophomore year, version 4 is sure to be out by the time they graduate and they are not well-served if they go to work for an organization that uses Software Y. The program advisory board -- comprised largely of computer forensics practitioners and academics -- has been consistent in their opinion that graduates will require additional training at whatever organization employs them and that that is to be expected. Just as criminal justice majors do not graduate and step into a patrol car, C&DF graduates also need to be trained in the specific policies and procedures of their employers.

These exercises have been found to be equally effective in in-person as well as online classes. In both cases, students have an opportunity to build their own toolkits on their own systems, and to work on exercises at their own convenience.

V. Conclusion

Champlain's C&DF program does not attempt to make students intimately familiar with any one given computer forensics tool. The program's philosophy is to focus on the process of digital investigations rather than expertise with one version of any one product and the college's mission of life-long learning.

Hands-on exercises are critically important to a student's understanding of what digital forensics is all about. Hands-on exercises based upon real problems provide the foundation of active learning. These exercises, if carefully crafted, can be used to address a number of critical concepts. Hands-on exercises can be employed quite effectively in online forensics courses, challenging the assumption that lab exercises need to be done in an on-campus laboratory environment with an instructor or proctor hovering overhead and/or using specialized computer forensics workstations. Students are actively engaged in their own learning process, solving problems that are conceptually similar to those they will encounter in the field. Indeed, the best, most motivated students go beyond the assignment and spend far more time in their own space working with the software and other application than they could if they only had access to tools in a lab. The experiences that we have had in teaching computer forensics online suggest that these concepts could also apply to other aspects of information assurance education.

VI. Acknowledgements

This work was partially supported by Grant No. 2006-DD-BX-0282 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view in this document are those of the authors and do not represent the official position of the U.S. Department of Justice.

VII. References

[1] Kessler, G.C., & Schirling, M.E. (2006). The design of an undergraduate degree program in computer & digital forensics [Electronic version]. *Journal of Digital Forensics, Security and Law*, *1*(3), 37-50. Retrieved February 10, 2008, from http://www.garykessler.net /library/C&DF_curriculum.pdf

[2] Institute for Security Technology Studies (ISTS). (2004, February). *Law enforcement tools and technologies for investigating cyber attacks: Gap analysis report*. Retrieved February 10, 2008, from http://www.ists.dartmouth.edu/TAG/gar /ISTSGapAnalysis2004.pdf

[3] Stambaugh, H., Beaupre, D., Icove, D.J., Baker, R., Cassaday, W., & Williams, W.P. (2000, August). *State*

and local law enforcement needs to combat electronic crime. National Institute of Justice, Research in Brief (NCJ 183451). Retrieved February 10, 2008, from http://www.ncjrs.gov/pdffiles1/nij/183451.pdf

[4] Stambaugh, H., Beaupre, D., Icove, D.J., Baker, R., Cassaday, W., & Williams, W.P. (2001, March). *Electronic crime needs assessment for state and local law enforcement*. National Institute of Justice, Research Report (NCJ 186276). Retrieved February 10, 2008, from http://www.ncjrs.org/pdffiles1/nij /186276.pdf

[5] Bensen, R.J. (2004, November). The increasing significance of computer forensics in litigation. *Intellectual Property & Technology Law Journal*, *16*(11), 1-4.

[6] Meyers, C. & Jones, T.B. (1993). *Promoting active learning: Strategies for the college classroom*. San Francisco: Jossey-Bass.

[7] Phillips, D.C., & Soltis, J.F. (2004). *Perspectives in learning.* New York: Teachers College Press.

[8] Donaldson, J.A., & Knupfer, N.N. (2002). Education, learning, and technology. In P.L. Rogers, *Designing instruction for technology-enhanced learning* (pp. 19-54). Hershey, PA: Idea Group Publishing.

[9] Felder, R.M., & Brent, R. (2004). The ABC's of engineering education: ABET, Bloom's taxonomy, cooperative learning, and so on. *Proceedings of the 2004 American Society for Engineering Education Annual Conference & Exposition*, Salt Lake City, 2004. Retrieved February 10, 2008, from http://www.ncsu.edu/felder-public/Papers/ASEE04(ABCs).pdf

[10] Hans, V.P. (2001). Integrating active learning and the use of technology in legal studies courses. In B.J. Duch, S.E. Groh, & D.E. Allen (Eds.), *The power of problem-based learning* (pp. 141-148). Sterling, VA: Stylus Publishing.

[11] Kessler, G.C. (2007). Experiences and methodologies teaching hands-on cyberforensics skills online [Electronic version]. In D. Edgar-Nevill (Ed.), *Proceedings of CFET 2007: 1st International Conference on Cybercrime Forensics Education and Training* [CD version], September 6-7, Canterbury Christ Church University, Canterbury, UK. Retrieved February 10, 2008, from http://www.garykessler.net/library /CFET2007_online_lab_exercises.pdf

[12] Palmer, G. (2001, August 7-8). *A road map for digital forensics research*. Digital Forensic Research Workshop (DFRWS) Technical Report (DTR) T001-01 Final. Retrieved February 10, 2008, from http://www.dfrws.org/2001/dfrws-rm-final.pdf

[13] Anderson, L.W., & Krathwohl, D.R. (Eds.). (2001). *A taxonomy for learning, teaching, and assessing: A revision of Bloom's* taxonomy of educational objectives (Abridged ed.). New York: Addison Wesley Longman.

[14] Honeynet Project. (2002). *Scan of the Month, Scan 24*. Retrieved February 10, 2008, from, http://www.honeynet.org/scans/scan24/

[15] Carrier, B. (2005). *File System Forensic Analysis*. Upper Saddle River (NJ): Addison-Wesley.