Experiences and Methodologies Teaching Hands-On Cyberforensics Skills Online

Gary C. Kessler

Champlain College Center for Digital Investigation
Burlington, Vermont, U.S.A.
gary.kessler@champlain.edu

Abstract

This paper describes some of the course design aspects of teaching computer forensics in an online environment. Although the focus of the paper is about online education at the undergraduate level, the basic premises are also applicable to graduate education and adult training. The paper will describe the need and rationale for the delivery of education and training in an online modality. In this context, *online* refers to asynchronous, virtual classrooms rather than self-paced or synchronous distance education. Virtual classrooms can provide an equivalent learning experience to a traditional classroom, complete with an instructor, fellow students, a course calendar, lectures, homework assignments, examinations, discussion threads, chat facilities, etc.; online classes can also achieve the same learning outcomes as their traditional counterparts. Online courses, particularly those that target adults, need to be designed with certain pedagogic models in mind; problem-based learning, collaborative learning, and constructivism are among those teaching and learning models that are most effective for adult learners and are well-supported by online course delivery.

Discussions about online education and training are quick to bring out the fact that the online modality is not appropriate for every instructor, every student, or every topic. The obvious question, then, *is online coursework appropriate for learning the hands-on skills necessary for computer forensics and digital investigations?* Our experience over the last three years suggests that the answer is a resounding *YES*. The paper presents a high-level overview of an online computer forensics curriculum and the overall design of online courses. A large part of this discussion will focus specifically on the design and content of an introductory and an advanced computer forensics course, with particular attention to multimedia technologies that add value in the online offerings, such as narrated graphical presentations and screen capture methods for demonstrating software. Several hands-on assignments, such as the analysis of drive or cell phone images, and the software that is employed to support those assignments will also be described.

1.0 Introduction

Although an increasing number of colleges and universities around the globe have started to offer programs in computer forensics and digital investigations, this is still a relatively new discipline in undergraduate education. Interestingly, while most of the programs were developed largely in response to requirements of the law enforcement community and to fill the needs reported in several national studies in the U.S. [1, 2, 3], most of the growth in the need for this skill set come from private sector organizations providing data recovery, electronic discovery (e-discovery), incident response, policy auditing, and third-party forensic analysis services.

Champlain College's Computer & Digital Forensics (C&DF) undergraduate degree and academic certificate programs started in 2003 and have been available online since 2004 [4, 5]. At this time, there are more online C&DF students than traditional on-campus C&DF students, and C&DF is one of the college's largest online programs. (The C&DF course curriculum can be viewed on the Web at *http://digitalforensics.champlain.edu*.)

Section 2 of this paper will discuss the pedagogic foundation of online courses, with a particular focus on the C&DF curriculum and adult learners. Section 3 will review the digital forensics process. Section 4 will focus on how hands-on exercises are employed in C&DF courses. Section 5 will provide some concluding comments.

2.0 Online Education

This section will describe the online learning environment of the C&DF program. Pedagogic issues, with a particular focus on the adult learner, will also be addressed.

2.1 The Online Learning Environment

Champlain College's online courses provide an asynchronous, virtual classroom. In this context, *asynchronous* alludes to the fact that classes do not regularly meet at a given place and time. These classes do, however, have the same syllabus, schedule, learning objectives, assignments, and rigor as an on-campus course. These online classes are neither correspondence nor self-paced courses.

Champlain College currently uses the WebCT learning management system (LMS). WebCT provides many tools for communication, including (Figure 1):[1]

- A threaded discussion forum allowing a student to post a comment for the entire class (or group)

---

[1] Additional screen shots can be found at http://digitalforensics.champlain.edu/reference/WebCTshots.pdf.

- An e-mail facility that allows message exchange between a student and the instructor, or between students.
- A chat facility allowing real-time (*synchronous*) class or group meetings.
- A shared whiteboard, where a group from the class can make drawings and/or mark-up a diagram so that all participants can see the virtual conference room.
- A student presentation area so that an individual or group of students can build Web sites for presentations and reports.

WebCT's tools can be augmented by other software such as Skype, WebEx, or instant messaging for additional forms of communication. Because of the lack of presence in a physical classroom, communication and discussion become critical factors in online courses [6].
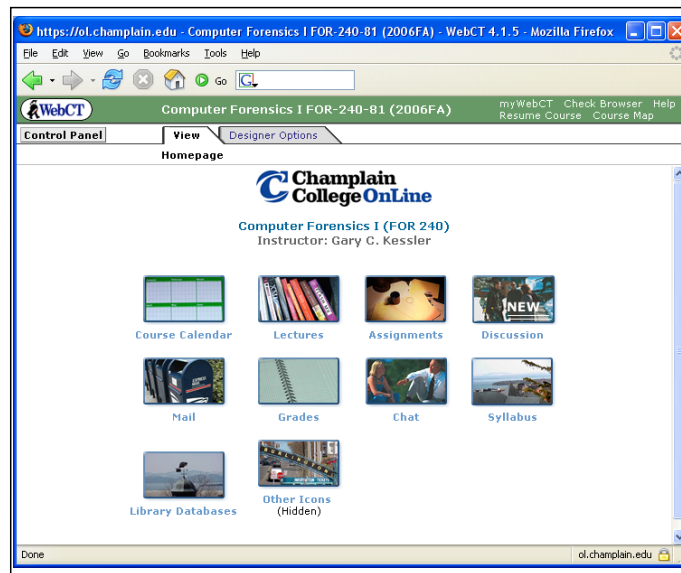

Figure 1: Home page for Computer Forensics I (FOR 240)

A broad range of communications capabilities provides some of the advantages that the virtual classroom can have over the traditional classroom. First and foremost, the online environment can allow more students to get involved in more class discussions because of its very asynchronous nature; students who may not be good at fast-paced, real-time discussions in the classroom environment have plenty of time to think and react if that same discussion occurs over a period of days or a week.

Second, the OLE provides support for one-on-one sessions between student and teacher, group activities, and better mentoring opportunities than is generally

possible in the traditional classroom because the virtual classroom is always open. Indeed, the communication and feedback is not real-time but students generally don't think twice about sending an e-mail, posting a discussion point, or coming to the aid of a fellow student at 2 a.m.

Third, there is an opportunity for classes to comprise students from a very diverse population; geography is no longer an issue when the classroom is in cyberspace. Geographic diversity adds an important element to a program such as digital forensics because laws in different countries vary widely and the presence of international students provides an opportunity to learn first-hand about other jurisdictions, laws, and behaviours.

Finally, the power of the Internet can be easily integrated into an online course. A list of Internet, college library, and other online resources, for example, can be built in to the course so that students can access tutorial and other adjunct materials. Technical difficulties can be addressed via an online (and telephone accessible) helpdesk. All in all, there are many features to make the online classroom a complete learning experience.

2.2 Online Course Pedagogy

The design of the C&DF online courses embrace a variety of teaching pedagogies to reach a wide variety of students with different learning preferences, attempting to employ the best characteristics of each pedagogic model where the online environment can leverage the greatest advantage [6]. A recurring theme is that all of the learning theories considered involve *active learning*, which enhances student performance, improves their general attitude towards the course and material, and helps to create a sense of community among students and faculty [7, 8, 9, 10].

There are three basic pedagogic models employed in the C&DF online curriculum that are particularly pertinent to the practical, hands-on courses. The most elemental is *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 [9, 11, 12].

A second pedagogic model is *resource-based learning (RBL)*, which takes advantage of the unprecedented volume of current and new knowledge accessible via the World Wide Web. Because of the timeliness of Web-based information, issues can be discussed based upon what is known at the moment rather than what was known at the beginning of the course term. Students, too, can look up items of information to augment any lecture and do homework research. RBL also provides the instructor the opportunity to give students more interesting and relevant assignments, projects, and tests. RBL can adapt to the wide variety of students' learning styles, allow for the presentation of a number of views about an issue

(requiring that students be instructed about how to apply critical thinking to the sites they visit and things that they read on the Web), encourage students' curiosity and investigative skills, and engage students in active learning [6].

Finally, *problem-based learning (PBL)* 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; it is also well-suited to the online environment because bigger, 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 [7, 13, 14].

2.3 Adult Learners

The online C&DF courses are specifically designed for adult learners, who are generally more mature and self-directed than traditional-aged students; many of the online C&DF students are also practitioners in field needing academic credentials. Successful online students need to be mature learners, good time organizers, and intrinsically motivated; online courses can take advantage of these characteristics. Adult learners are best served with active teaching methods, such as those described above [6, 15, 16].

3.0 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 (DFRWS) [17]:

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 [18, 19]. 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.

4.0 Teaching Hands-On Computer Forensics Skills

The discussion above about pedagogy and the digital forensics process makes the need for hands-on exercises clear. This section will describe how the C&DF program incorporates hands-on exercises into both the online and face-to-face courses and provide some specific examples.

4.1 The Role of Hands-On Skills

One often-stated criticism of teaching computer forensics online is that it "cannot be done because a hands-on component is necessary." While it is certainly true that hands-on exercises are essential in this field, there is nothing in an online class that prevents hands-on exercises from being performed.

Hands-on exercises are used to support the learning objectives of the C&DF courses, which are the same regardless of whether the course is taught on-campus or online. Exercises have been created so that the student can perform them on

their own computer or on any system on campus. The exercises are specifically designed so as *not* to require specialized hardware or a special laboratory environment. In this way, students can perform activities beyond the basic exercise, work at their own convenience, and build their own toolkits. The majority of the hands-on exercises are found in three courses. Computer Forensics I is a required course for second-year C&DF, Criminal Justice, and Computer Networking & Information Security majors, while Computer Forensics II and Cybercrime are required for third- and fourth-year C&DF students.

A plethora of demonstration versions of computer forensics software is available for use in coursework:

- EnCase (Guidance Software[2]): One of the most widely-used Windows-based forensics tools. A fully-functional demo version is available that is limited to the evidence files on the distribution medium. Guidance Software supplies the C&DF program with a batch of demo DVDs at the beginning of each term.
- FTK (AccessData[3]): Another widely-used Windows-based forensics tool. A fully-functional version of FTK Imager and a demo version of the FTK software are available on the Internet. The FTK demo can read an E01 or dd image file, and is fully-functional for images with less than 5000 evidence files. FTK is, perhaps, the most versatile demo software available for the C&DF program and AccessData allows the college to distribute the demo software to C&DF students.
- Helix[4]: An open-source software (OSS) Linux-based tool for computer forensics, e-discovery, and the acquisition of live systems including random access memory (RAM).
- ProDiscover (Pathway Technologies[5]): Windows-based forensics software that is growing in use. A demonstration version of the software is available on the Web. Pathway Technologies makes a fully functional version available to C&DF students for the duration of the pertinent course.
- WinHex (X-Ways Software[6]): An outstanding hex editor with some excellent computer forensics capabilities. The demo version is available for free on the Internet and can open a physical or logical drive, an image file, or any file from disk. The specialist and forensics versions of WinHex are excellent tools.

Other software is also employed or referenced by the course work, including forensic software suites from Dan Mares (Maresware[7]), George Garner (Forensic

---

[2] http://www.guidancesoftware.com/

[3] http://www.accessdata.com/

[4] http://www.e-fense.com/helix/

[5] http://www.techpathways.com/

[6] http://www.x-ways.net/

[7] http://www.dmares.com/

Acquisition Utilities[8]), and the OSS community. There are, in fact, many more tools than the coursework can possibly expose students to and, therefore, we encourage students to search for their own tools.

Use of tools is important but the C&DF program does not endorse any vendor or any particular piece of software; for that matter, non-use of a tool does not imply any dissatisfaction. The goal is to expose students to a wide variety of tools rather than to make them an expert in any one tool.

Students obtain course software from CDs distributed at the beginning of class or from Web sites provided in class assignments. Lecture material, screen captures and animations, and/or assignments guide students through the use of the software while reinforcing the subject matter of the associated lecture. The primary operating system is Windows because of the large number of available tools and the ubiquity of the platform.

There are many sources for exercises that can be used as-is or modified. The Digital Forensic Research Workshop,[9] Honeynet Project,[10] and U.S. National Institute of Standards and Technology (NIST) Computer Forensic Reference Data Sets (CFReDS) project[11] are excellent sources of ideas; the author has used two such exercises to teach both students as well as other instructors. Several computer forensics texts also supply problems and hands-on exercises.

4.2 A Detailed Example -- Examination of a Floppy Disk

One of the early exercises in the Computer Forensics I course involves the simple analysis of a floppy disk, based on a challenge posted on The Honeynet Project web site in 2002 [20] and modified by the author. In this exercise:

1. Students are directed to download a ZIP file. Each student is assigned a different ZIP file, each of which has a different Message Digest 5 (MD5) hash value. Part of the assignment is to verify the file's MD5 hash and calculate the Secure Hash Algorithm (SHA) value.
2. Students unzip the file to recover a dd image of a floppy disk and read a report laying out the scenario; the assignment has them answer a series of questions about the disk's contents.
3. Students are advised that they can examine either 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 (a demo version of FTK could also be used).
4. The floppy disk contains three files although two of them have been deleted. Examination of the root directory (Figure 2) shows a deleted .DOC file, a deleted .JPG file, and an .EXE file.

---

[8] http://www.gmgsystemsinc.com/fau/

[9] http://www.dfrws.org

[10] http://www.honeynet.org

[11] http://www.cfreds.nist.gov/

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 and a Word document subheader. 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. 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. The first password is different in every image file; this makes each file unique and is the reason that the MD5 hash values are unique.
9. The third file has a file signature indicating 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.

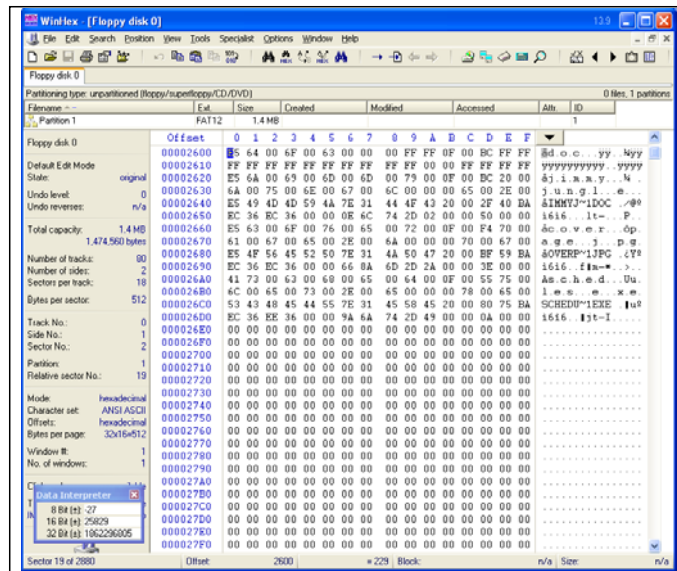Students are also taught in this exercise how to create a dd image.[12]

Figure 2: Directory listing of the subject floppy disk, viewed by WinHex

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

4.3 Other Hands-On Exercises

Additional hands-on exercises are employed in the C&DF courses 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.

Computer Forensics I is a survey course. In addition to the exercise above, tools such as FTK and Encase are also introduced. Cyberforensics-related aspects of the Internet and Internet-based investigations are briefly described, along with tools such as SamSpade and *whois* for simple Internet domain searches.

Computer Forensics I also has an exercise where students examine a CDMA cell phone file system.[13] Students download a ZIP file with the cell phone files; as in the floppy disk exercise described above, each cell phone file has some unique information and, therefore, different MD5 hash values. Students are asked to find such information as the phone's banner message, phone number, PIN, voice mail code, and service provider. Students are also asked to recover text (SMS) messages and images.
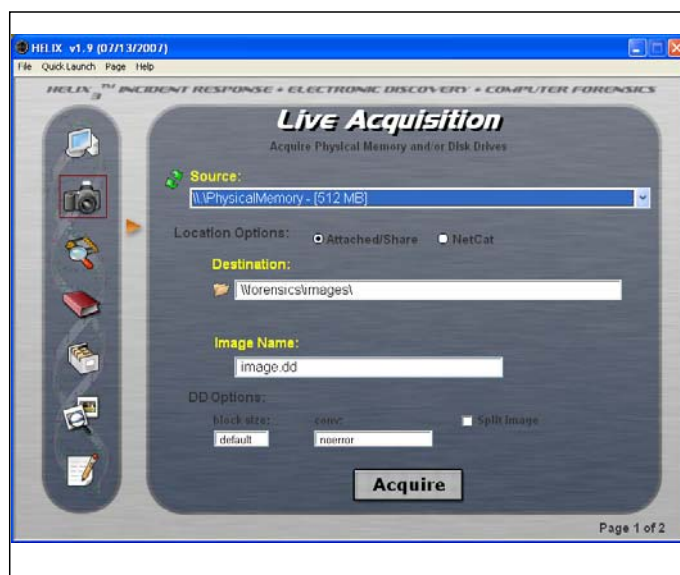

Figure 3: Live acquisition with Helix

Computer Forensics II is much more intense in terms of hands-on projects and use of tools. In this course, students employ a variety of tools, including EnCase, FTK,

---

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

Helix, and ProDiscover, and gain 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. One task that students have in this course is to create a matrix of what software -- in their opinion -- best handles what kind of evidence.

Additional exercises in this course have students create forensically correct images using such tools as FTK Imager, dd, Helix, and/or WinHex. With the increasing importance of live system acquisition and analysis of RAM, tools such as Helix are gaining in importance; students work with Helix to acquire their own computers and use the FTK demo to explore the RAM image (Figure 3). Students are looking at a computer with which they are ostensibly familiar and even then are surprised by what they find sitting in RAM.

Hands-on exercises do not just refer to the use of technology. Computer Forensics I introduces the concepts of evidence integrity and the chain of custody. Computer Forensics II focuses directly on the computer forensics examiner's work product and report. The best exam can be undermined by poor reporting by either not clearly stating pertinent information for the investigator or prosecutor (or other client), or somehow conveying sloppy work on the part of the digital examiner. Each assignment in this course requires a report from the student describing the evidentiary chain, integrity of the evidence, steps taken in the examination, exhibits found, and conclusions. While many software packages provide reports of their own, none is sufficient to stand alone; students learn what components are essential in a complete report.

Internet investigations and tools are the subject of the Cybercrime course and these exercises are particularly conducive to the online environment. Hands-on exercises in this course include detailed information searches for people and domains using Internet tools. The course also employs informational Web sites (e.g., Sam Spade or DNSStuff), use of network-based tools (e.g., *traceroute* and packet sniffers), and use of network applications (e.g., Internet Relay Chat and instant messaging). Some students employ virtual computer software (such as VMware) in order to "build" additional computers for themselves with which they can experiment with other operating systems and virtual networks.

4.4 Hands-on Exercises Revisited

The C&DF program philosophy is that students need a solid understanding in the computer forensics process and an exposure to as wide a variety of tools as possible. Courses do not focus on expertise in any one piece of software because it is just not practical; if we teach Software X version 3 to our juniors, version 4 will 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 C&DF advisory board -- comprised largely of computer forensics practitioners and academics -- were of the opinion that graduates will require additional training at whatever organization that employs them and that that is to be expected. Just as CJ 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.

There are, of course, tradeoffs to the online versus on-campus courses in terms of hands-on exercises. One could argue that online classes are in some ways better suited than face-to-face classes because online students can repeat the lectures multiple times, watch animated software demonstrations over and over, and ask questions of the instructor and fellow students on a 24x7 basis.

Hands-on exercises in online courses cannot cover everything that we might like, however, particularly when it comes to employing specialized forensics hardware. While students can certainly image a thumb drive to a hard disk, for example, it is logistically and economically difficult to arrange a scenario whereby students can physically image a hard drive to another, employ a hardware write-blocker, or access a cell phone. Nevertheless, imaging is a small part of the entire digital forensics process and the virtual classroom provides a rich potential for significant hands-on learning.

5.0 Conclusion

The 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 is life-long learning.

Hands-on exercises are critically important to a student's understanding of what digital forensics is all about. What the online environment challenges is the assumption that hands-on 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. Indeed, we have found that our best 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.

6.0 Acknowledgements

7.0 About the Author

Gary C. Kessler, M.S., CCE, CISSP is an Associate Professor, director of the Computer & Digital Forensics program, and director of the Center for Digital Investigation at Champlain College in Burlington, Vermont, and an Adjunct Associate Professor at Edith Cowan University in Perth, Western Australia. He is a

technical adviser to the Vermont Internet Crimes Task Force and a member of the High Technology Crime Investigation Association (HTCIA). Gary is also an associate editor of the *Journal of Digital Forensic Practice*, on the editorial board of the *Journal of Digital Forensics, Security and Law*, and pursuing a doctorate in Computing Technology in Education.

References

1. Institute for Security Technology Studies (ISTS), *Law enforcement tools and technologies for investigating cyber attacks: Gap analysis report*. ISTS, 2004. www.ists.dartmouth.edu/TAG/gar/ISTSGapAnalysis2004.pdf (visited July 2007)
2. Stambaugh, H, Beaupre, D, Icove, DJ, Baker, R, Cassaday, W & Williams, WP, *State and local law enforcement needs to combat electronic crime*. National Institute of Justice, Research in Brief (NCJ 183451), 2000. www.ncjrs.gov/pdffiles1/nij/183451.pdf (visited July 2007)
3. Stambaugh, H, Beaupre, D, Icove, DJ, Baker, R, Cassaday, W & Williams, WP, *Electronic crime needs assessment for state and local law enforcement*. National Institute of Justice, Research Report (NCJ 186276), 2001. www.ncjrs.org/pdffiles1/nij/186276.pdf (visited July 2007)
4. Kessler, GC, Online education in computer and digital forensics: A case study, Proceedings of the 40th Hawaii International Conference on Systems Sciences (HICSS 40), Hawaii, 2007. www.garykessler.net/library /Online_C&DF_education.pdf (visited July 2007)
5. Kessler, GC & Schirling, ME (2006). The design of an undergraduate degree program in computer & digital forensics", *J. of Digital Forensics, Security, and Law*, 1(3), 37-50. www.garykessler.net/library/C&DF_curriculum.pdf (visited July 2007)
6. Weller, M, *Delivering learning on the Net: The why, what, & how of online education*. Kogan Page, 2002.
7. Felder, RM & Brent, R, 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. www.ncsu.edu/felder-public/Papers/ASEE04(ABCs).pdf (visited July 2007)
8. Meyers, C & Jones, TB, *Promoting active learning: Strategies for the college classroom*. Jossey-Bass, 1993.
9. Phillips, DC & Soltis, JF, *Perspectives in learning*, Teachers College Press, 2004.
10. Considine, C. & Dean, T, Active learning in distance education, Proceedings of the 2003 American Society for Engineering Education Annual Conference & Exposition, Nashville, 2003. www.asee.org/acPapers/2003-1477_Final.pdf (visited July 2007)
11. Donaldson, JA & Knupfer, NN. Education, learning, and technology, In: PL Rogers, *Designing Instruction for Technology-Enhanced Learning*, Idea Group Publishing, 2002.

12. Alesandrini, K (2002). Visual constructivism in distance learning, *USDLA J.*, 16(1), www.usdla.org/html/journal/JAN02_Issue/article03.html (visited July 2007)
13. Naidu, S. Designing and evaluating instruction for e-learning, In: PL Rogers, *Designing Instruction for Technology-Enhanced Learning*, Idea Group Publishing, 2002.
14. Hans, VP. Integrating active learning and the use of technology in legal studies courses, In: BJ Duch, SE Groh & DE Allen (Eds.), *The Power of Problem-Based Learning*, Stylus Publishing, 2001.
15. Burgess, JRD & Russell, JEA (2003). The effectiveness of distance learning initiatives in organizations, *J. of Vocational Behavior*, 63(2), 289-303.
16. McKenzie, IK (2002). Distance learning for criminal justice professionals in the United Kingdom: Development, quality assurance and pedagogical proprieties, *J. of Crim. Justice Educ.*, 13(2), 231-249.
17. Palmer, G, *A road map for digital forensics research*. Digital Forensic Research Workshop (DFRWS) Technical Report (DTR) T001-01 Final, 2001. www.dfrws.org/2001/dfrws-rm-final.pdf (visited July 2007)
18. Anderson, LW & Krathwohl, DR (Eds.), *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives*, 2/e. Allyn & Bacon, 2001.
19. Bloom, B, Englehart, M, Furst, E, Hill, W & Krathwohl, D, *Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive domain*. Longmans, Green, 1956.
20. *The Honeynet Project, Scan of the Month, Scan 24*, www.honeynet.org/scans /scan24/ (visited July 2007)