

THE JOURNAL OF  
**DIGITAL FORENSICS,  
SECURITY AND LAW**

**Journal of Digital Forensics,  
Security and Law**

Volume 1 | Number 3

Article 3


2006

## The Design of an Undergraduate Degree Program in Computer & Digital Forensics

Gary C. Kessler  
*Champlain College*

Michael E. Schirling  
*Burlington Police Department*

Follow this and additional works at: <https://commons.erau.edu/jdfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

### Recommended Citation

Kessler, Gary C. and Schirling, Michael E. (2006) "The Design of an Undergraduate Degree Program in Computer & Digital Forensics," *Journal of Digital Forensics, Security and Law*. Vol. 1 : No. 3 , Article 3.

DOI: <https://doi.org/10.15394/jdfsl.2006.1009>

Available at: <https://commons.erau.edu/jdfsl/vol1/iss3/3>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact [commons@erau.edu](mailto:commons@erau.edu).



(c)ADFSL



## **The Design of an Undergraduate Degree Program in Computer & Digital Forensics**

**Gary C. Kessler**  
Champlain College  
163 So. Willard Street  
Burlington, VT 05401  
+1 802-865-6460  
+1 802-865-6446 (fax)  
*gary.kessler@champlain.edu*

**Michael E. Schirling**  
Burlington Police Department  
1 North Avenue  
Burlington, VT 05401  
+1 802-658-2704  
*mschirling@bpdvt.org*

### **ABSTRACT**

Champlain College formally started an undergraduate degree program in Computer & Digital Forensics in 2003. The underlying goals were that the program be multidisciplinary, bringing together the law, computer technology, and the basics of digital investigations; would be available as on online and on-campus offering; and would have a process-oriented focus. Success of this program has largely been due to working closely with practitioners, maintaining activity in events related to both industry and academia, and flexibility to respond to ever-changing needs. This paper provides an overview of how this program was conceived, developed, and implemented; its evolution over time; and current and planned initiatives.

**Keywords:** Computer forensics education, digital forensics education, digital investigation education, online law enforcement education.

### **1. BACKGROUND**

Champlain College is a small, private college in Burlington, Vermont, with roughly 1900 traditional undergraduate students and nearly a thousand online and continuing education students. Founded in 1878, the college has historically been a business-oriented, two-year college. In 1995, the college started a transformation from an A.S.-granting institution to one that, today, offers A.S., B.S., and M.S. degrees in over 30 programs in an educational environment that balances liberal studies and practical knowledge.

The undergraduate degree program in Computer & Digital Forensics (C&DF) was launched in the Fall 2003 semester. The following sections will describe the process by which the program was developed, the philosophy behind its design and implementation, its evolution to date, current initiatives, and planned future directions.

## **2. THE FIRST STEP: INTRODUCTION TO COMPUTER FORENSICS**

In 2002, the first author was the director of the Computer Networking program at Champlain College and a technical consultant to the Vermont Internet Crimes Task Force (ICTF), and the second author was a detective with the Burlington Police Department and coordinator of the ICTF. At that time, the ICTF was starting to provide first responder training to local law enforcement officers related to searching and seizing computers, investigating cybercrimes, and understanding the type of information that might be found on digital devices. In conjunction with the director of the college's Criminal Justice (CJ) program, the authors proposed offering an introductory computer forensics course with the thought that it would be popular with continuing education, CJ, and computer technology students. This "experimental" course was offered in the Fall 2002 semester, and filled during pre-registration.

The course was well-received by students and a number of events occurred during that first semester that led to the development of the degree program. First, the college received so many requests for the course that it was clear that a Spring 2003 offering would also fill up. Second, the Admissions Department at the college started to receive requests by students wishing to apply to our "computer forensics program." Third -- and most compelling -- a number of research papers came to the attention of the authors that clearly identified a national need for computer forensics education in support of law enforcement (ISTS 2002; Stambaugh et al. 2000; Stambaugh et al. 2001).

Initial research into the need for such a program consisted primarily of conversations with practitioners in the field and experts from law enforcement and prosecutorial agencies throughout the United States. All cited a dramatic increase in the need for digital forensic capacity due to both a real increase in electronic crime as well as increased awareness of the role of computing devices as the instrument, target, or record-keeper of all types of crimes. The consensus was that the creation of a program that would prepare undergraduates with practical knowledge of the computer forensic analysis and investigative process would be well received by both public and private sector organizations. While some additional specialized workplace training would be needed, it was thought that college graduates with a practical background and knowledge of the field would be beneficial to those organizations and agencies looking to employ individuals with these skills.

### **3. THE SECOND STEP: DESIGNING AND IMPLEMENTING THE CURRICULUM**

#### **3.1 Curriculum Design Philosophy**

With the success of the experimental course, the college undertook a serious investigation into the feasibility and viability of an undergraduate program in computer forensics. The first step was the formation of an Advisory Board composed of individuals external and internal to the college (all programs at the college have such a board). The external members included eight educators, civilian and law enforcement digital forensics practitioners, technical consultants, and a forensic accountant from the local area and around the country that were either colleagues known to Champlain College faculty or particularly well-known in computer forensics circles; none was directly affiliated with the college. The internal members comprised Champlain College computer technology and CJ faculty and representatives from the admissions office, career planning, and student advising center. The external members were initially tasked with providing their views of what they thought needed to be included in the program, while the internal members were initially tasked with finding relevant academic guidelines or models that might prove helpful. The internal board was also responsible for writing the actual proposal for the college's Curriculum Committee while the external members continued to provide oversight, critiques, and suggestions guiding the content of the curriculum and even some of the core courses themselves.

Looking for models from other colleges and universities turned up computer forensics or electronic crime concentrations within other two- or four-year programs, graduate certificates, A.S. degree programs, computer forensics courses taught within Information Security programs -- but no other four-year degree program specifically targeting digital investigations. The external advisory board members and college faculty developed the following overriding philosophical guidelines for the curriculum.

First, recognizing that digital forensics is a multidisciplinary field, it was determined that a breadth of courses was required. Students need to study the law as well as basic computer and data network operations as a basis for understanding the process of computer forensics and digital investigations. For that reason, the curriculum includes courses from several programs so that students obtain a good foundation before actually getting into the actual computer forensics courses. Building interdisciplinary student teams is also important; most CJ students do not eagerly embrace the thought of working with computers and most computer technology students do not ordinarily take criminal and business law courses. Digital investigations need individuals with a combination of these skills so classes that combine these two groups of students helps both appreciate the "other side" (Nowicki 2003).

Second, the intention has always been to prepare students to work in computer

forensics environments in both the private and public sectors. Students have a variety of career paths available, including positions as a:

- Sworn local, state, or federal law enforcement officer concentrating on electronic crime, criminal investigations, or criminal intelligence
- Non-sworn law enforcement, military, or government examiner working on criminal or civil investigations, intelligence gathering, or foreign counter-intelligence
- Corporate investigator within an organization's internal information security, policy enforcement, and/or audit function
- Computer forensics/data recovery analyst working for a third-party

Finally, the focus of the program had to be about life-long learning and the digital forensics *process* rather than about the *tools*. Given the tremendous acceleration of change in cyberlaw, computer technology, and digital forensics techniques, only those who know how to learn can possibly keep up and advance. Just as an individual does not earn a CJ degree and then step immediately into a patrol car, C&DF students need to understand how digital investigations are generically carried out rather than getting bogged down in the microdetail of how any one tool accomplishes the task. Indeed, our students gain an exposure to EnCase (Guidance Software), FTK (AccessData), Helix (e-fense), Knoppix, ProDiscover (Technology Pathways), WinHex (X-Ways Software), and many other tools, and get an opportunity to compare and contrast features, capabilities, and weaknesses. But the tools are just the tools and are meaningless outside of the context of a process.

By way of analogy, forestry students should understand a forest ecosystem rather than just know the name of every tree.

The Advisory Board was formed, and the curriculum design proposal process formally commenced, in November 2002. The curriculum started through the college's proposal process in February 2003 and was accepted by the Trustees in May. While the members have changed over the years, the Advisory Board continues to play an important role in the evolution of the program and is continually asked to work with the C&DF program faculty in reassessing the content of the program and the courses.

### **3.2 C&DF Curriculum Details**

The C&DF degree requires 120 credit hours. Table 1 lists the core courses that comprise the C&DF curriculum. The computer technology and criminal justice courses, drawn from our established Computer Networking and Criminal Justice programs, provide students with the necessary, broad background in:

- Computers and data networking
- Computer operating systems

- Basic programming concepts
- U.S. criminal justice system
- Fourth Amendment privacy protections
- Investigation techniques

**TABLE 1. C&DF Core Courses<sup>1</sup>**

<b>Digital Investigation</b>	<b>Computer Technology</b>	<b>Other Courses</b>
Introduction to Criminalistics	Computers & Telecommunications	Interpersonal Communication
Analysis of Digital Media	Data Communications	Intercultural Communication
Computer Forensics I	Operating Systems	Statistics
Computer Forensics II	Computer & Network Security	Financial Accounting
Cybercrime	<b>Criminal Justice</b>	Business Law
Forensic Accounting	Criminal Law	Critical Thinking
White Collar Crime	Criminal Procedure	Ethics in Human Services
Senior Seminar	Criminal Investigation	
Internship	Investigative Interviewing	

The "Other Courses" in Table 1 provide breadth and general education, with a strong focus on the college's core competencies of verbal and written communications, ethics, creative and critical thinking, technical and quantitative literacy, and global and multicultural awareness.

The core courses developed specifically for this program include:<sup>2</sup>

- *Introduction to Criminalistics/Forensic Science Lab*: An introductory course designed to expose students to the numerous aspects of the various forensic science disciplines, including both digital and non-digital methods. Topics include the history of forensic science, physical evidence, evidence collection, crime scene management, fingerprints, forensic toxicology, serology, firearms, forensic psychology, and DNA.
- *Analysis of Digital Media*: This course examines aspects of digital media with an emphasis on understanding the advantages and limitations of using digitally produced data, the various ways in which digital data can be enhanced, and procedures to ensure proper handling and presentation.

<sup>1</sup> Curriculum details can be found online at <http://digitalforensics.champlain.edu>.

<sup>2</sup> Course syllabi can be found online at <http://digitalforensics.champlain.edu/syllabus>.

- *Computer Forensics I:* Topics related to criminal justice and computer technology, with a focus on the forensic use of information on computers are covered. Subject matter includes types of computer and Internet crime, the investigation life cycle, evidence collection, legal issues, search and seizure guidelines, case law, the process of computer and Internet investigations, hard drive terms and concepts, computer forensic tools, networking and TCP/IP basics, cryptography and steganography, mobile devices, and future challenges.
- *Computer Forensics II:* Students learn advanced concepts in digital/computer forensic analysis and Internet investigations, with a balance of legal and technical aspects. Topics include advanced legal concepts, subpoenas and search warrants, seizing digital media, imaging and authenticating drives, file systems, and forensic hardware and software.
- *Cybercrime:* Economic and other crimes perpetrated over the Internet or other telecommunications networks are the focus of this course, discussing crimes ranging from auction fraud, identity theft, and social engineering to child sexual exploitation, e-mail scams, and phishing. Investigative techniques, technical issues, and legal aspects are described.
- *Forensic Accounting:* This course provides an introduction to forensic (fraud) accounting and covers fraud examination techniques, interview techniques, rules of evidence relating to fraud, internal control methodology, asset misappropriation, and financial statement misrepresentation. The course also covers the rules of evidence as they relate to several different fraudulent activities including illegal activities such as wagering, money laundering, cash skimming and embezzlement.
- *White Collar Crime:* White-collar crimes, from fraud and embezzlement to Medicaid/Medicare fraud, are the subject of this course with particular emphasis on the use of the Internet and computers to commit these crimes. The course describes the many ways white-collar crimes are committed, the “essential elements” of many of these crimes, and the evidence necessary to prove these crimes.
- *Senior Seminar in Digital Investigation:* A capstone, senior-level course that provides students with an opportunity to prepare a thesis or perform some other comparable project. It is intended to bring together elements from the entire program and demonstrate original work.

All of these courses were developed, and subsequently taught, by subject matter experts in the area. Although Vermont is a rural state, access to expertise in computer science and cybercrime investigation is close at hand. The Burlington area is home to several colleges (including the University of Vermont) as well as a large IBM memory chip research and manufacturing facility. Located just 90 miles from a major border crossing south of Montreal, northwest Vermont also has a large contingent of federal law enforcement agencies, ranging from the FBI and U.S. Secret Service to the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) and Immigration and Customs Enforcement (ICE). The Vermont ICTF is composed of local, state, and federal law enforcement officers with extensive experience handling computer-related cases and examinations, several of whom have lectured regionally, nationally, and internationally. A Champlain College adjunct faculty member teaching video courses had a consultancy addressing the manipulation of digital images. A local state's attorney had an interest in, and wide knowledge of, cyber-related laws. The college, in general, and the CJ program, in particular, has a strong relationship supporting local law enforcement agencies. All together, the college was fortunate with the number of local experts in the area, supplemented by colleagues around the country. To date, all original course developers are still actively teaching in the program.

Core courses were each designed with an eye towards creating a solid foundation of legal principles, an appreciation for the current state of the art and science of digital forensics, and practical skills that will allow graduates to immediately step into advanced training on the specific tools and techniques deployed in the workplace. Working with the college's instructional development team, each course combines theoretical and practical knowledge so that students understand the applicability and use of the subject matter. Problem-based learning and written project work are commonly used throughout the program (Burgess and Russell 2003; Harkness, Lane and Harwood 2003; McKenzie 2002; Swan 2004).

An internship is optional, primarily because there is insufficient capacity to manage and mentor students in the local area. Nevertheless, interns have been placed in some out-of-area locations and the program continually seeks opportunities and cooperative agreements with sites around the country, as well as initiatives that might increase local internship opportunities.

The C&DF program was approved by the college in Spring 2003 and officially commenced that fall. As a timely demonstration of how academia catches up to real-world events, the blackout of the northeastern U.S. occurred that August and the summer was filled with additional cyberattacks, just weeks before this curriculum got underway. The authors and a colleague from the Vermont State Police wrote a white paper for the U.S. Attorney's Office (District of Vermont) about the relationship between digital forensics, criminal investigation, and



intelligence gathering in the face of hacking and cyberterrorism (Kessler, Schirling and Sheets 2003). This paper marked the beginning of a close, ongoing partnership between the C&DF program and the local law enforcement community of cybercrime investigators -- including local, state, and federal agencies -- building on the already longstanding relationship between the college's CJ program and law enforcement.

The summer of 2003 also saw one of the first articles providing a taxonomy of, and guide for, computer forensics education (Yasinsac, Erbacher, Marks, Pollitt and Sommer 2003). This article described motivations and energy around the subject matter that was similar to what the college experienced, and independently affirmed the need for an interdisciplinary approach, a focus on the digital investigative process, and the use of hands-on exercises. It also defined the skills needed by four classes of computer forensics practitioner; namely, the technician, policy maker, professional, and researcher.

Yasinsac, et al., (2003) also cited a case study that found that the lack of a dedicated lab facility was a hindrance to the computer forensics educational process. This observation was particularly pertinent to the C&DF program since not only was there no dedicated hardware lab, but the courses were intended to be offered online as well as on-campus (see the next section). Champlain College has found that in most cases, students can engage in hands-on exercises using their own computers and media supplied in class. Demonstration or evaluation versions of many software tools have proven to be quite adequate for purposes of software familiarization and case exercises. The FTK demo, for example, is fully functional software when used with small evidence files and instructors have designed assignments around the EnCase demo software (which is also fully functional but can only read the evidence files that ship with the demo). Pathway Technologies provides full versions of their ProDiscover software for the duration of a course and, of course, open source Linux tools without any restrictions are widely available on the Internet. A wide range of other open source tools, some of which students themselves find, are employed in the courses. Network-based exercises employ online activity, such as visits to 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). Furthermore, some students employ virtual computer software (e.g., VMware) in order to "build" additional computers for themselves with which they can experiment with other operating systems and virtual networks.

Disk images with which to create hands-on exercises come from a variety of sources, including forensics challenges posted by the Digital Forensic Research Workshop and the Honeynet Project, samples created by C&DF faculty, and test images posted by the National Institute of Standards and Technology (NIST). Disk images and evidence files can be distributed in a variety of

formats (e.g., **.dd** or **.e01** files) on CD or thumb drives. Students can also create their own images from CDs, floppies, thumb drives, or other media.

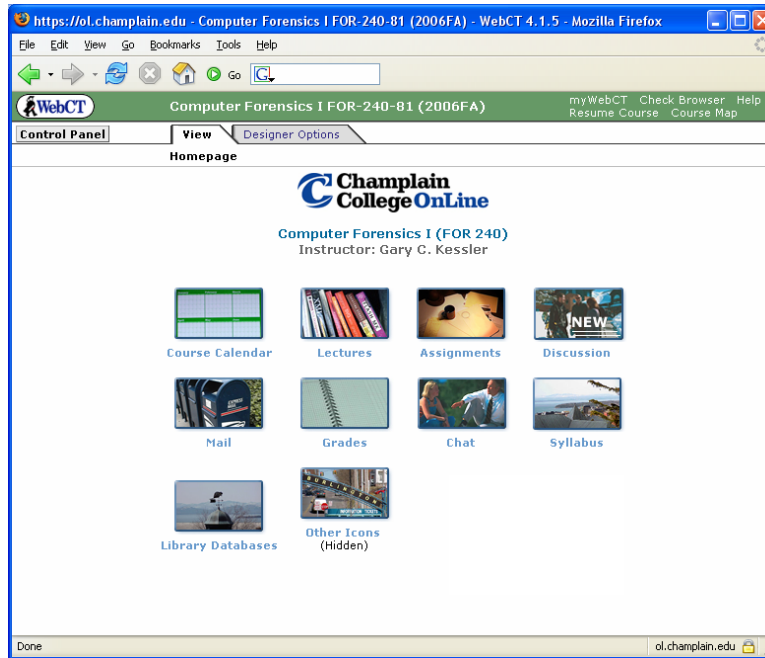
Indeed, the lack of a lab does have a downside in that students do not spend a great deal of time working with computer forensics hardware in the acquisition phase. The analysis, examination, interpretation, and reporting phases of digital investigations, however, can be covered quite nicely in virtual laboratories. Internships also often help make up for the deficiency in the acquisition process.

#### **4. THE THIRD STEP: THE CURRICULUM GOES ONLINE**

Another goal for the C&DF program was that it be available online. The advisory board and program developers believed that this was the only way to serve one of the program's largest potential audiences -- law enforcement officers around the country looking for educational credentialing in this subject matter. Built in to the program design was that each course should be able to have the same learning objectives regardless of whether it was offered online or on-campus (Weller 2002).

Champlain College uses the WebCT learning management system, creating an online learning environment (OLE) accessible from anywhere on the Internet via a Web browser (Figure 1). Students -- and employers -- often confuse *online* with *self-paced*. These classes, however, are instructor-led courses complete with a syllabus, course calendar, weekly lectures, homework assignments, projects, tests, classmates, class discussions, etc. -- i.e., a virtual classroom that is schedule-friendly (within bounds) and geography-independent. And, students quickly discover, online classes are generally harder than their on-campus counterparts, requiring strong communication and time management skills, self-discipline, and intrinsic motivation (Adkins and Nitsch 2005; Hartley and Bendixen 2001).

Students employ the same hands-on exercises in online classes as they do in on-campus classes. Students are supplied with the necessary software in courses for hands-on projects, employing low-cost, free, or demonstration software, as necessary. Instructor demonstrations, of course, can be provided in class or in the OLE; in the latter case, such demonstrations are provided as a series of screen shots, detailed instructions, and/or Flash- or Java-based animation. These demos, in fact, may be slightly more effective in the online mode than on-campus because students can replay them as often as they need. Students image, examine, and analyze their own systems or media sent to them by the instructor (e.g., on CDs or thumb drives). Because of the pervasiveness of Windows-based software, students are required to have a computer available to them that runs the Windows operating system, and advised to have a large disk drive and plenty of memory.



**FIGURE 1.** Screen shot of home page of online Computer Forensics I course

Another advantage of the online course delivery mechanism is that individuals from anywhere in the world can take these courses. In many instances, especially in law enforcement agencies and small companies, the size of the workforce or the location of primary operations (rural locations) may limit the accessibility to specialized training and education of this nature. By creating a parallel delivery method using the online educational model, these rural or small agencies and corporations can gain the same advantages as their larger brethren.

Computer Forensics I became available in an online format in the Fall 2003 semester. The C&DF curriculum as a whole has been online since Fall 2004. Although some concern has been expressed about how well online courses can teach subject matter that requires hands-on skills, the literature is filled with articles addressing this very issue, demonstrating that properly designed online courses can achieve the same learning outcomes as on-campus courses. Kessler (2006) describes an informal study showing that students in online C&DF courses perform as well as on-campus students taking the same courses. Similar results, in more formal and broader studies, are echoed by Dutton, et al., (2002) and Ragan and Kloeppel (2004). Indeed, successful online students need to be mature learners and have good time discipline, so full-time online study is limited to adult learners. Nevertheless, the OLE has not been a disadvantage in C&DF education. What has been learned is that students do not need to be sitting together in a laboratory environment with an instructor to

learn how to use tools and other software, although being able to communicate with others is an essential element to getting over the learning curves. Additional detail about the online pedagogy as it relates to the C&DF curriculum can be found in Kessler (in press).

### **5. STATUS AND FUTURE DIRECTIONS**

The Champlain College C&DF program started in Fall 2003. In Spring 2004, the program was recognized by the National Institute of Justice (NIJ) Electronic Crime Program and Electronic Crime Partnership Initiative (ECPI) as a model curriculum for e-crime education primarily because of the multidisciplinary approach to the subject matter. The C&DF curriculum was also one of the models used by the NIST Technical Working Group for Education and Training in Digital Forensics in developing their guidelines for computer forensics curricula (NIST, in press). Indeed, the college has worked with faculty from around the country in developing similar programs; all of academia working together will still be hard-pressed to meet the nation's needs in this space, so other programs are viewed as possible collaborators and partners rather than competitors.

Fall 2004 saw the first full incoming class and there are currently over 70 full-time, traditional-aged undergraduates enrolled in the program (as of September 2006). Another 75 students are online, most pursuing the academic certificate; roughly a third of the students come from New England and New York, a handful from Canada and the U.K., and the remainder are in other areas around the U.S. The college is currently developing articulation agreements with two-year colleges, building a small lab for undergraduate research projects, and designing a master's degree in digital investigation management.

The relationship between the C&DF program and the local law enforcement community became more formalized in 2006 with the creation of the Champlain College Center for Digital Investigation (C3DI), largely funded by a "capacity building" grant from the Bureau of Justice Assistance. The primary objective of C3DI is to augment both the computer forensics examiners serving law enforcement agencies in Vermont and C&DF program faculty. This initiative will provide real assistance to law enforcement, ongoing practical experience for C&DF instructors, and internship opportunities for students.

### **6. CONCLUSION**

Champlain College developed and implemented the C&DF curriculum in 2002 and 2003, in response to events occurring nationally and internationally that affected law enforcement, government, business, and academia. Today, many colleges and universities are starting -- or planning -- to offer similar programs at all degree levels. This is a very positive sign; as we recognize our society's and economy's dependence on information, digital investigations have ramifications for criminal investigations, intelligence collection, regulatory

compliance, and corporate policy enforcement.

The C&DF program has undergone some modification every year since its inception due, of course, to the rapid changes in the field. Key elements to keeping current are the faculty experts, expertise provided by the advisory board, close contact with practitioners throughout the country, and alliance with colleagues throughout the academic and training communities. And last, but certainly not least, a close relationship with the law enforcement community has been imperative to maintaining relevance and addressing an important national need.

## **7. ACKNOWLEDGEMENTS**

This project was partially supported by Grant No. 2004-MU-MU-K001 awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Justice.

## **8. REFERENCES**

- Adkins, M. and Nitsch, W.B., (2005). Student Retention in Online Education. *The Encyclopedia of Distance Learning*, 4, 1680-1686.
- Burgess, J.R.D. and Russell, J.E.A. (2003). The Effectiveness of Distance Learning Initiatives in Organizations. *Journal of Vocational Behavior*, 63, 289-303.
- Dutton, J., Dutton, M. and Perry, J. (2002, July). How do Online Students Differ from Lecture Students? [Electronic version]. *Journal of Asynchronous Learning Networks*, 6(1), 1-20. [http://www.sloan-c.org/publications/jaln/v6n1/pdf/v6n1\\_dutton.pdf](http://www.sloan-c.org/publications/jaln/v6n1/pdf/v6n1_dutton.pdf), September 6, 2006.
- Harkness, W.L., Lane, J.L. and Harwood, J.T. (2003, July). A Cost-effective Model for Teaching Elementary Statistics with Improved Student Performance [Electronic version]. *Journal of Asynchronous Learning Networks*, 7(2), 1-20. [http://www.sloan-c.org/publications/jaln/v7n2/pdf/v7n2\\_harkness.pdf](http://www.sloan-c.org/publications/jaln/v7n2/pdf/v7n2_harkness.pdf), September 6, 2006.
- Hartley, K. and Bendixen, L.D. (2001, December). Educational Research in the Internet Age: Examining the Role of Individual Characteristics [Electronic version]. *Educational Researcher*, 30(9), 22-26. <http://www.aera.net/pubs/er/pdf/vol30-09/AERA300905.pdf>, October 20, 2004.
- Institute for Security Technology Studies (ISTS). (2004, February). *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis Report*. Hanover, NH: ISTS. <http://www.ists.dartmouth.edu/TAG/gar/ISTSGapAnalysis2004.pdf>, September 6, 2006.

- Kessler, G.C. (2006, February). *The Efficacy of Online C&DF Courses: A Case Study of Four Courses in 2005*. Burlington, VT: Champlain College Technical Report, TR 2006-ITS-001.
- Kessler, G.C. (In press). Online Education in Computer and Digital Forensics: A Case Study. To appear in the *Proceedings of the 40th Hawai'i International Conference on System Sciences (HICSS-40)*, January 3-7, 2007, Waikoloa, HI.
- Kessler, G.C., Schirling, M. and Sheets, B. (2003, October 24). *A Model for a Cyberforensics Examination, Training, and Education Center: Homeland Security, Anti-Terrorism, and Law Enforcement*. A white paper developed for the Anti-Terrorism Advisory Council, U.S. Attorney's Office, District of Vermont.
- McKenzie, I.K. (2002, Fall). Distance Learning for Criminal Justice Professionals in the United Kingdom: Development, Quality Assurance and Pedagogical Proprieties. *Journal of Criminal Justice Education*, 13(2), 231-249.
- National Institute of Standards and Technology (NIST). (In press). *Education and Training in Digital Evidence: A Guide for Law Enforcement, Educational Institutions, and Students*. Gaithersburg, MD: NIST, Technical Working Group for Education -- Digital Evidence.
- Nowicki, E. (2003, September). Training and Education via the Internet. *Law & Order*, 51(9), 36-38.
- Ragan, R.E. and Kloeppel, J.W. (2004, December). Comparison of Outcomes on Like Exams Administered to In-residence and Asynchronous Distance-based Pharm.D. Students [Electronic version]. *Journal of Asynchronous Learning Networks*, 8(4), 1-20. [http://www.sloan-c.org/publications/jaln/v8n4/pdf/v8n4\\_ragan.pdf](http://www.sloan-c.org/publications/jaln/v8n4/pdf/v8n4_ragan.pdf), September 6, 2006.
- Stambaugh, H., Beaupre, D., Icové, D.J., Baker, R., Cassaday, W. and Williams, W.P. (2000, August). *State and Local Law Enforcement Needs to Combat Electronic Crime*. Washington, D.C.: National Institute of Justice, Research in Brief (NCJ 183451). <http://www.ncjrs.gov/pdffiles1/nij/183451.pdf>, September 6, 2006.
- Stambaugh, H., Beaupre, D., Icové, D.J., Baker, R., Cassaday, W. and Williams, W.P. (2001, March). *Electronic Crime Needs Assessment for State and Local Law Enforcement*. Washington, D.C.: National Institute of Justice, Research Report (NCJ 186276). <http://www.ncjrs.org/pdffiles1/nij/186276.pdf>, September 6, 2006.

Swan, K. (2004). *Relationships Between Interactions and Learning in Online Environments* [Electronic version]. The Sloan Consortium.  
<http://www.sloan-c.org/publications/books/interactions.pdf>, September 6, 2006.

Weller, M. (2002). *Delivering Learning on the Net: The Why, What & How of Online Education*. London: Kogan Page.

Yasinsac, A., Erbacher, R.F., Marks, D.G., Pollitt, M.M. and Sommer, P.M. (2003, July/August). Computer Forensics Education. *IEEE Security & Privacy*, 1(4), 15-23.

#### **AUTHOR BIOGRAPHIES**

Gary C. Kessler is an associate professor at Champlain College, where he is the director of the Computer & Digital Forensics program and the Champlain College Center for Digital Investigation. He is also a technical consultant to the Vermont Internet Crimes Task Force, a Certified Information Systems Security Professional (CISSP), a member of the High Technology Crime Investigation Association (HTCIA) and High Tech Crime Consortium (HTCC), and on the editorial board for the *Journal of Digital Forensics, Security and Law*. Gary is also a frequent speaker at industry and academic meetings. He has a B.A. in Mathematics, an M.S. in Computer Science, and is currently pursuing a doctorate in Computing Technology in Education.

Michael E. Schirling is a Deputy Chief with the Burlington Police Department, and the co-founder and coordinator of the Vermont Internet Crimes Task Force. He is on the advisory boards of the Champlain College Center for Digital Investigation (C3DI) and Computer & Digital Forensics (C&DF) program, and a member of the High Technology Crime Investigation Association (HTCIA), as well as an international lecturer on computer forensics and cybercrime. Mike is also an adjunct faculty member at Champlain College where he helped design the C&DF curriculum, as well as several of the courses. He holds a B.A. in Political Science and an M.Ed.