



Annual ADFSL Conference on Digital Forensics, Security and Law

2010
Proceedings


May 21st, 9:30 AM

The Defiance College Undergraduate Major in Digital Forensic Science: Setting the Bar Higher

Gregg H. Gunsch

Defiance College, ggunsch@defiance.edu

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

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

Scholarly Commons Citation

Gunsch, Gregg H., "The Defiance College Undergraduate Major in Digital Forensic Science: Setting the Bar Higher" (2010). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 6.
<https://commons.erau.edu/adfsl/2010/friday/6>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



The Defiance College Undergraduate Major in Digital Forensic Science: Setting the Bar Higher

Gregg H. Gunsch
Defiance College
701 N. Clinton St.
Defiance, OH 43512
419-783-2460
419-784-0426 fax
ggunsch@defiance.edu

ABSTRACT

This paper provides background information to accompany the panel discussion on Curriculum Design and Implementation in Computer Forensics Education. It is specifically focused on the content and delivery of Defiance College's undergraduate (B.S.) program majoring in Digital Forensic Science (DFS). The genesis and evolution of the Defiance College DFS program are described, along with its successes, challenges and known opportunities for improvement. The desired outcomes of the panel discussion include articulating the necessary components of an undergraduate program, refining expectations of knowledge and skills required of students upon graduation, and suggesting strategies for achieving those expectations despite inevitable resource limitations and diverse student demographics.

Keywords: education, undergraduate, digital forensics, computer forensics, pedagogy, skills development

1. GENESIS

The Defiance College major in Computer Forensics was launched in August 2006 after several years of development effort by an Advisory Board comprised of local law enforcement personnel, representatives from industry, the Ohio Peace Officer Training Academy, and members of Defiance College. Creation of the program was largely driven by the urging of Defiance County Sheriff David Westrick, who recognized that the workload of digitally-related cases was ever-increasing and unsustainable, and that entry-level practitioners were needed to help alleviate that load locally and nationally. At that time, there was a single detective in this corner of northwest Ohio with the knowledge and skills to process digital evidence: Deputy Steven Mueller had worked on cases for thirty separate agencies in the region (presently, over forty). Defiance College was in a unique position to build upon a long-established and vibrant criminal justice program, firmly founded on the college's culture of active engagement with the community and law enforcement.

Concurrent with the development of the computer forensics major, Defiance College (DC) was also partnering with several community agencies to establish the Family Justice Center of Northwest Ohio (FJCNWO), a collection of centers providing comprehensive services and support for victims of domestic violence, stalking, and sexual assault [4]. The FJCNWO officially launched in Oct 2006 with a substantial grant from President George Bush's \$20M Family Justice Center Initiative [3]. A portion of the grant was allocated to DC for the establishment of a computer forensics laboratory, both for delivery of the major as well as training of law enforcement personnel in support of the FJCNWO mission. Involvement with the FJCNWO provides both a context for the education of DC students as well as opportunities to apply that education in community service, particularly for those students in the social work, education, business administration, art, criminal justice, and computer forensics programs.

By the spring of 2006, DC had secured tentative approval of the computer forensics major from the

Ohio Board of Regents, pending the hiring of a qualified faculty member to manage the program and deliver the courses. In the SP06 semester, several students attended the first offering of an introductory computer forensics course held by existing DC faculty and visiting guest speakers. Six of those students were sophomores who “stepped out on faith” that they would be able to graduate in 2008 with a degree in computer forensics, or at least a self-made major resembling one. It was then that Dr. Gregg Gunsch and Defiance College discovered each other. He was hired to start August 2006, and final approval of the program was immediately granted by the Ohio Board of Regents.

Delivery of the program required creating content for six new lecture courses and their associated labs, and the arrangement of two senior capstone activities: an internship and earning a nationally-recognized computer forensics certification. It is important to note that this program is not a concentration or track of an existing computer science or similar program. It is a self-contained integrated major, drawing from other programs to be interdisciplinary, but is more than a handful of specialty courses added to an existing core.

The six pioneering students were entering their junior year of college, but content-wise, they were entering the sophomore year of study in their major. Rather than have them extend for a fifth year, or graduate with self-made majors consisting of only a portion of the computer forensics program, we accelerated the “natural” sequence of course offerings so that they could graduate in May 2008. Through hard work and personal attention we were able to implement the accelerated program and to graduate all six students with the full major in Computer Forensics. Since 2006 the program has grown to 41 full and part-time students, with an expected inbound enrollment of 35-40 new students in Fall 2010.

2. EVOLUTION

The original CF program, as designed by the Defiance College Computer Forensics Advisory Board and approved by the Ohio Board of Regents in 2006, consisted of the following courses. All of the courses beginning with “CF” were created for this new major; the rest previously existed.

- IT 110 – Programming I
- IT 130 – Database Design
- IT 320 – Networking Fundamentals
- IT 330 – Information Technology Ethics
- CF 110 – Intro to Computer and Digital Forensics
- CF 120 – PC System Software
- CF 130 – Operating Systems
- CF 230 – Seizure and Forensic Examination of Computer Systems
- CF 310 – Advanced Topics in Computer Data Analysis and Recovery
- CF 320 – Network Forensics
- CF 340 – Intrusion Detection
- CF 450 – National Certification
- CF 497 – Forensic Internship
- CJ 111 – Intro to Criminal Justice
- CJ 155 – Criminal Law
- CJ 217 – Criminal Investigation

- CJ 221 – Criminal Evidence and Procedure
- CJ 471 – Criminology
- MA106 – Pre-Calculus Mathematics
- BA363 – Business Law
- AC221 – Financial Accounting
- AC222 – Managerial Accounting

It had been the expectation of all involved that improvements would be forthcoming after the major's first offering. The most apparent shortcoming was that there existed no "program prerequisites" to ensure that students have the background and academic qualifications to succeed in this major and career. This was especially crucial to remedy given the incongruity between the type of student who would flourish in the technologically-challenging computer forensic major and the type of student typically attending DC, a liberal arts-based college. Students coming to DC generally don't anticipate pursuing a technological degree, and those students looking for a technological degree typically don't look to a liberal art-based college. This presented both a challenge for recruitment of the right students, as well as a challenge to ensure they were adequately prepared for the core forensics courses of the major.

This shortcoming was also articulated by one of the first graduates: although she felt competent in computer forensic knowledge and had developed useful practical skills, she was uncomfortably unsure of her understanding of computer hardware/software fundamentals. Finally, along with these realizations came an additional impetus for change: due to steadily-falling student demand and anticipated departure of the IT faculty, the Management Information Systems (MIS) major was to be terminated. Rather than retain the existing IT courses, we used this as an opportunity to restructure the computer forensics program to accomplish the following:

- provide a strong computer technology foundation at the front end of the program,
- filter out students whom are not well-suited for the field of computer forensics, and
- align course content and prerequisites for smooth flow through the program.

The biggest change was to replace the two tangentially-relevant 100-level IT courses with a pair of new foundation-building courses to prepare students to earn the *CompTIA A+ Certification with the IT Technician endorsement*. Obtaining this certification was to become the prerequisite to the more advanced CF courses, effectively creating a "gate" to the core computer forensics program for only properly prepared students. Advantages of requiring students to become entry-level service technicians before starting the meat of the computer forensics program include:

- Conformance with National Best Practices: New computer analysts joining the FBI's Regional Computer Forensics Laboratories must earn this same A+ certification before being sent to the FBI Computer Analysis and Response Team (CART) forensic training.
- Preparation: Students will have established crucial foundational knowledge and be significantly better prepared to succeed in the core computer forensics courses.
- Screening: This certification requirement would do for the computer forensics program what freshmen chemistry does for forensic science – ensures that only students with the affinity and background for the discipline move forward into the major's core courses. This prevents a student from heading down a path of likely failure, as well as helps ensure that classes don't get dragged down by having to backfill remedial knowledge.

The other relevant IT courses were repurposed to better prepare students for computer forensics, and the remaining CF courses were restructured/renumbered to smoothen the program's flow. The

following courses constitute the current major [1], requiring 67 semester credit hours:

- CF 105 – CompTIA A+ Computer Essentials Exam Preparation
- CF 106 – CompTIA A+ 220-602 Exam Preparation
- CF 110 – Introduction to Computer and Digital Forensics
- CF 205 – Computer Security Fundamentals
- CF 210 – Operating Systems
- CF 215 – Computer Forensic and Security Ethics
- CF 305 – Seizure and Forensic Examination of Computer Systems
- CF 310 – Advanced Topics in Computer Data Analysis and Recovery
- CF 315 – Fundamentals of Computer Networks
- CF 405 – Network Forensics
- CF 410 – Intrusion Detection
- CF 450 – National Certification
- CF 497 – Computer Forensic Field Experience and Seminar
- CJ 111 – Introduction to Criminal Justice
- CJ 155 – Criminal Law
- CJ 217 – Criminal Investigation
- CJ 221 – Criminal Evidence and Procedure
- CJ 471 – Criminology
- MA106 – Pre-Calculus Mathematics
- BA363 – Business Law
- AC221 – Financial Accounting
- AC222 – Managerial Accounting

In early 2009 we made one other significant change: renaming the major to “Digital Forensic Science.” The justification was that “computer forensics,” while a commonly-used term, was inadequate to describe the scope of devices that process, store or transmit information in digital form. Nationally and internationally, this difference is being recognized in the careful selection of titles of organizations and activities such as the Digital Forensic Research Workshop, the Digital Forensic Certification Board, the Journal of Digital Forensic Practice, and the International Journal of Digital Forensics and Incident Response. Of greater significance is that Digital Forensics is now a recognized science according to the American Academy of Forensic Sciences (AAFS). In addition, we emphasize the application of scientific principles: in the classroom, students are taught to apply methods that are disciplined, systematic and repeatable in the collection, preservation, analysis, and reporting of digital evidence. The processes of hypothesis generation, experiment planning and execution, observation, and hypothesis support, refutation and revision are routinely discussed and practiced. Materials from the Scientific Working Group on Digital Evidence (SWG-DE) are included in our curriculum, and reflected in the catalog. Therefore, it is appropriate to claim that the students are taught to be scientist-practitioners, and that the most descriptive title of our program is Digital Forensic Science. This change was promptly approved by the Ohio Board of Regents. The CF course

designations remained the same (as opposed to becoming DF or DFS) at the request of the registrar.

3. PROGRAM DESCRIPTION

The four-year, in-residence, undergraduate DFS program fits the niche of developing entry-level practitioners who are ready for apprenticeship and have the well-rounded background expected from a liberal arts education to become life-long self-learners: oral and written language skills, civic and social sciences, natural sciences, arts and humanities, religion, physical education and life skills, etc. While there is some element of vocational training involved, the focus is on the development of critical reasoning skills, understanding the underlying principles of the tools and systems to which they are applied, and self-directed research to adapt to new situations. This embodies a tension between education and training, between preparing minds for life-long learning and a vocation. The program achieves this through a mix of traditional lecture, hands-on laboratory exercises, and engagement learning where the student amplifies his/her education through service to the community.

Students in the DFS program are actually being prepared to enter one of two career fields: digital forensics and computer/network security. The tools and techniques of digital forensics for information in motion are also applicable while recognizing and responding to intrusions into a company's computer network. During the first year of the DFS program, students complete the two foundational A+ preparation courses, an introduction to digital/computer forensics, an introduction to criminal justice, and criminal law. During the sophomore year, students learn computer security fundamentals, general principals of operating and file systems, criminal investigations, criminal evidence and procedures, and ethics focused on computer security and forensics. In the junior year, students dig into the real meat of forensics work, starting with post-mortem acquisition and analysis of hard drives, and progressing through to live system analysis, mobile device forensics, password recovery, and criminology. They also learn the fundamentals of network communications and packet analysis. In their senior year, the students tackle network forensics and intrusion detection, and apply themselves towards accomplishing the two senior capstones. One is to complete 120+ hours of field experience (loosely called an "internship") with one or more agencies performing digital forensics or network security tasks; typically, the forensics experience has been with law enforcement, and network security with industry. The second capstone is to earn a nationally-recognized, vendor-neutral, digital forensic certification such as the GCFA, CCE, or CFCE. Throughout the program the students make extensive use of the dedicated digital forensics laboratory, becoming familiar with a variety of commercial and freeware tools, including FTK, EnCase, WinHex, TSK/Autopsy, Wireshark, Snort/Squid, flavors of dd, etc., and tool collections such as Helix. [1]

4. SUCCESSES

4.1. Service Learning

The dominant defining characteristic of Defiance College is the emphasis on service or engagement learning: putting education into practice through betterment of the local or global community. Engagement learning is a natural teaching technique for creating problem solvers, and it is an effective means of incorporating real-world context into the classroom and developing a mature attitude of service before self. Students in the DFS program seek ways of integrating service experiences into the classroom. Some of the activities they have accomplished include:

- Examined the computer of a client of the Family Justice Center of Northwest Ohio (FJCNWO) who believed she was a victim of electronic stalking, then removed the existing malware and fortified the computer's security suite
- Performed on-site security assessments of FJCNWO facilities
- Developed Internet safety awareness training materials and educated the incoming freshmen
- Provided Internet safety and identity theft awareness training to clients of the FJCNWO

- Recovered personal data (music files, financial records, family photos) from a crashed hard drive of a community member. We wrapped crime tape around the computer and treated it as a suspected music piracy case, so that the students exercised the sequence of events from collection through forensic analysis, while performing a useful service in the process.
- Hand-carved a large number of photographs from a corrupted digital camera memory card belonging to the nine-year-old son of an adult DC student. During this exercise we explored the limitations of and differences among the data carving (recovery) routines of FTK and foremost, and in the process, were able to recover the only existing photos of the child's recently deceased pet cat.
- Assisted the prosecutor's office of a major city with a cold case homicide investigation. This was the first of what we expect to be an oft-repeated service activity.
- Assisted high-school age students develop Internet-safety presentations for a FJCNWO Faith-Based Youth Initiative

The students also engage in community service opportunities outside of the classroom, including:

- Through DC's Citizen Leader program, one student is organizing a computer repair and secure data wiping service for the community
- DC students have formed a school charter of the High Technology Crime Investigation Association, and begun the process of developing the next incarnation of HTCIA's Internet Safety for Children Campaign public website [2]
- Students in the DFS, criminal justice, and (traditional) forensic sciences programs are helping to organize and conduct our second "Got Clue" crime investigation summer camp for area high school students
- Many DFS students are members of the Criminal Justice Society, where they have supported local law enforcement training sessions and campus disaster preparedness exercises

4.2 Certification Experiences

The pioneer class of 2008 chose to challenge the SANS GCFA certification for their capstone. To prepare, they all enrolled in SEC508 through the SANS Mentor program, held on campus and led by Dr. Gunsch. We spent significantly more contact time together than the Mentor program required, integrating the SANS materials into the other on-going courses and going far beyond that programmed into the SANS training. All six pioneers passed their certification exam on the first try.

As a result, greater emphasis on TSK as a tool for understanding FAT and NTFS file system structures has been incorporated into the junior-level courses, with routine side-by-side comparisons to other tools such as FTK and WinHex, and additional discussions on computer-related laws have been included throughout the program. The current seniors have formed a self-study group, purchased practice exams, and are actively preparing to challenge the GCFA examination before graduation in May 2010.

4.3 Internship Experiences

Each senior is required to complete 120 or more hours of field experience under the supervision of a forensic examiner or network security analyst. The students journal their experiences and produce a final report to benefit their fellow and future students. To date, internships have been held with the Toledo, Fairborn and Lima Police Departments, the Defiance County Sheriff's Office, the Ohio Peace Officer Training Academy, the Ohio Bureau of Workman's Compensation, and two insurance companies. The students have actively participated in tool validation, case management, and analyzing cases involving child pornography, drug, homicide, fraud, and employee misconduct.

4.4 Graduate Placement

All of the graduates who actively and intentionally sought employment in the digital forensics field so far have readily found employment. Hiring agencies include the DEA, the Ohio Attorney General's Office, and private companies contracting their forensic services to law enforcement and industry.

4.5 Program Growth

Since the initial launch in 2006, the DFS program has experienced steady growth in terms of the number and preparedness of incoming students. There are currently 41 students actively enrolled in the program, ranging from freshmen straight out of high school to adult transfer students and military veterans through the Yellow Ribbon Program. There has been some degree of the "starry-eyed CSI effect" on the part of the less mature students, but those students quickly realized they have neither the aptitude nor predilection for DFS and moved elsewhere. The ideal new student would already be comfortable with computer hardware; for example, someone who repairs computers or has built a high-end gaming machine. Prospects are contacted early and encouraged to start or join a high school computer club and earn the A+ certification before or shortly after arriving at Defiance College. One of the sophomores did just that prior to arriving at DC in 2008, and several of the incoming freshmen appear to be able to achieve that goal.

A targeted recruiting campaign has been launched to enroll 35 to 40 qualified freshmen to enter in August 2010. As mentioned previously, simply drawing from the demographic typically attracted to a rural liberal arts-based college is not a practical approach; recruiting has to reach students with an affinity for digital technology. Through deliberate outreach in an ever-widening network, the Office of Enrollment Management has been able to connect with and attract a growing pool of qualified student candidates. To meet this anticipated growth spurt, Defiance College has begun the search for an additional full-time faculty member to supplement the current permanent and adjunct members.

Defiance College enjoys a rather unique status by having majors in Criminal Justice, Forensic Science, and Digital Forensic Science. The two applied sciences programs build heavily on the strong, 30-year old Criminal Justice major, which richly adds to the students' knowledge and provides context for their education. Development of a fourth field, Forensic Accounting, is underway, starting first as a concentration for business students but later will grow into a complete major as demand dictates.

4.6 Advisory Board

The advisory board that drafted the original plan for the computer forensics program was recently augmented with a great deal of additional local and national talent. The new DFS Program Advisory Board has 25 members, covering a wide range of perspectives, including local law enforcement agencies, the FBI, DoD and DEA, Fortune 500 security practitioners, forensic tool developers, insurance and banking industry, investigative firms, graduate and undergraduate academia, and LE training. The roles of the Advisory Board are to provide guidance on the academic directions of the DFS program, assist in marketing the program to prospective students and employers, assist in recruitment of qualified students and faculty, help to identify funding opportunities for capacity-building and sustainment, help to identify or create internship opportunities for the students, and assist in job placement for the graduates. The board has also provided great advice directly to the students regarding what employers value, and what will make the students stand out during the job search process – an appreciated side benefit of which has been the unsolicited affirmation of what their professor tells them.

5. OPPORTUNITIES FOR IMPROVEMENT

This section discusses several open issues whose resolution should further strengthen the DFS program. It is hoped that the panel discussion on Curriculum Design and Implementation in Computer Forensics Education at the ADFS� conference could help to resolve some of them.

5.1 Focus of the Program

Students in the DFS program are actually being prepared to enter one of two career areas: digital forensics and computer/network security. For example, topics such as seizure and examination of computer systems prepare a student for the digital forensics field, while intrusion detection of on-going activity is generally a network security issue. A case can be made for recognizing the significant amount of overlap between the two fields, particularly in the tools and techniques used for analysis as well as the methods used by the offenders. However, it has been suggested that we may be unnecessarily broad, requiring students to assimilate knowledge from too many areas at once. The open question is, “Are we biting off more than we should chew?”

Should we drop some of the network security-oriented content and corresponding internship flavor, and focus strictly on digital forensics? Is that even possible? Alternatively, should we develop two distinct tracks through the program as capacity and demand allow? Or is it the case that the original designers of the program were correct and the two fields are so intertwined that someone entering either field at the apprentice-level should have familiarity with both?

5.2 Learning Objectives

As part of the cyclic re-accreditation process, DC operates a self-study program for continual, deliberate improvement. Part of this self-study includes the establishment of and assessment against a set of learning objectives, both for the general education process as well as each of the majors. The current objectives for the DFS major are:

- **Digital Evidence Scene Documentation:** The student will demonstrate competence in crime scene documentation by photographing, creating diagrams, and tagging evidence items in a mock crime scene.
- **Digital Evidence Image Acquisition:** The student will demonstrate competence in digital evidence collection by successfully duplicating three digital evidence devices (hard drive, USB drive, floppy disk), using two distinct methods under two operating systems, and proving that exact copies were made while the original evidence remains unchanged.
- **Digital Evidence Analysis and Reporting:** The student will demonstrate competence in digital evidence analysis and reporting by successfully completing an examination of a set of digital evidence images and documenting the examination in a report suitable for legal proceedings.
- **Network Security Monitoring:** The student will demonstrate an understanding of network monitoring by installing and configuring an intrusion detection system, then monitoring, detecting, analyzing, and reporting on irregular network events created by the instructor and classmates.
- **Testing Against an External Standard:** The student will demonstrate competence in the breadth of foundational computer forensics knowledge by successfully passing the qualifying examination for a nationally-recognized digital/computer forensics certification; e.g., SANS GCFA, ISCCE CCE, or IACIS CFCE (law enforcement).

The open question is, “Are these the right objectives?” Do these capture the essence of the major and help determine if the students are being taught – and retain – the correct information to be successful in the field? If these are not the right objectives to assess, then what are? What process can be used to determine the proper set of objectives?

5.3 Certifications

Each student is expected to earn two industry certifications while in the DFS program: the CompTIA A+ certification at the front end, and a nationally-recognized digital forensics certification as a senior capstone. The open question is, “What happens if they don’t?”

The CompTIA A+ certification requirement was envisioned to be the gate to the sophomore-level DFS courses, and is currently listed as the prerequisite to these courses. It was assumed that after the two preparation courses were completed, the students would be able to pass the pair of examinations required to earn the certification. However, in practice it has not been that simple. The certification was designed for someone with 500 hours of hands-on experience in computer troubleshooting. Two semesters of coursework, no matter how intense, does not provide the same assimilative experience. So far, students who have received hard-earned “A”s in the courses (based on homework/lab assignments, quizzes and tests) have succeeded on the first try of the certification exams with only about a 50% pass rate. More assimilation time seems necessary to complete the certification, but this tends to spill well beyond the start of the subsequent courses. Our current practice has been to allow students who have passed the A+ prep courses to proceed to the sophomore courses in the DFS program; it seemed unnecessarily punitive to “hold them back” a year because they weren’t ready to successfully pass the certification exams. An additional concern has been the out-of-pocket cost to take the exams (\$168 each) and any necessary retakes.

A similar question arises regarding the capstone digital forensics certification. Should failure of the externally-issued examination prevent or postpone a student’s graduation? This might be true for externally-accredited programs like education and nursing, but no external organization has imposed a certification requirement for the DFS program. There is a two-credit course associated with earning the certification. Can or should a grade be assigned for work done in preparation to take the examination, even if the student fails? A grade can be given based on participation in group-study activities, practice examinations, and even the degree of failure of the certification examination itself. Our current practice has been to award an “A” to students who pass the certification examination; so far, we’ve been fortunate to not have to address the “didn’t pass” situation. It will only be a matter of time, however, before a “C” student, who otherwise meets all graduation requirements, will not pass the certification examination in time for graduation. Would forcing completion of the certification process be unnecessarily punitive?

The feedback from the advisory board has been mixed. Some suggest that if the student cannot pass a certification examination, that student isn’t prepared to progress or enter the field; others recognize the realities of the academic process and need for assimilation time. The board was consistent to encourage the students to earn both certifications, even after graduation, because of the value they add to the résumé and employer. Even the A+ certification sets prospective employees apart as it shows foundational knowledge has been achieved and testimony is more trustworthy.

We feel that the DFS student should graduate with a very strong résumé and be highly marketable. The record should consist of a diploma, two certifications from industry (foundational and capstone), and a rich internship/field experience. In practice we are not certain that we can or should require students to earn the certifications to graduate, but we strongly encourage them to do so to achieve maximum competitiveness.

6. CONCLUSION

All positions on the training/education spectrum deserve attention and provide important contributions to address the growing, critical, collective need of knowledge and skills within industry and law enforcement. From short training sessions for tool proficiency and continuing professional development, all the way through advanced graduate research, high-quality programs are essential to meet that need. The four-year, in-residence, undergraduate Digital Forensic Science program at Defiance College fits the niche of developing entry-level practitioners who are ready for

apprenticeship and have the well-rounded educational background to become life-long self-learners.

The ideal freshman student would enter DC already comfortable with computer hardware and be ready to dig into technical topics quickly. The most successful graduate will leave with a very strong résumé consisting of a B.S. degree, the A+ certification, a nationally-recognized digital forensics certification such as the GCFA or CCE, a rich internship/field experience, plenty of hands-on lab experience with a variety of tools, and a balanced education fully grounded in service-oriented learning in the liberal arts tradition.

BIOGRAPHY

Dr. Gregg Gunsch is a Professor of Digital Forensic Science at Defiance College, one of only a small handful of colleges and universities in the US to offer an undergraduate major in digital forensic science. He is a retired USAF LtCol, is a registered Professional Engineer (OH), and holds the CISSP, GCFA, CCE, and DFCP (Founder) certifications. Prior to arriving at Defiance College in 2006, Dr. Gunsch led graduate research and taught courses in information system security/assurance for thirteen years at the Air Force Institute of Technology, Wright-Patterson AFB, OH.

REFERENCES

- [1] 'Digital Forensic Science Major, Behavioral and Applied Social Sciences Division, Defiance College', http://www.defiance.edu/pages/BASS_majors_DFS.html, 21 Feb 2010
- [2] 'International High Technology Crime Investigation Association', <http://www.htcia.org>, 21 Feb 2010
- [3] 'The Family Justice Center Alliance', <http://www.familyjusticecenter.org>, 21 Feb 2010
- [4] 'The Family Justice Center of Northwest Ohio', <http://www.fjcnwo.org>, 21 Feb 2010