

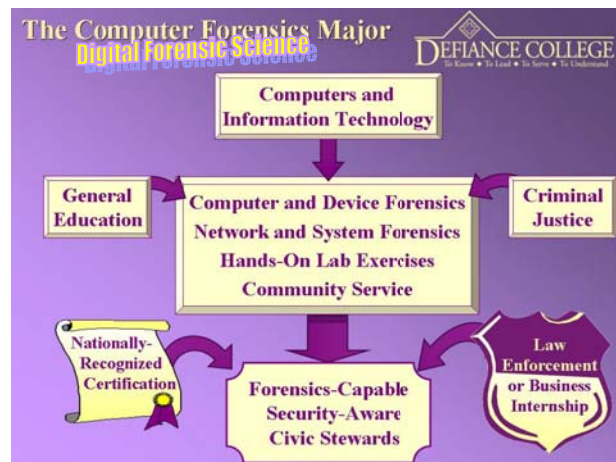
**Digital Forensic Science** (formerly called Computer Forensics) is a new and growing field in the area of hi-tech crime investigation. Participants in this program will learn how to provide a secure computer environment and learn techniques for collecting and analyzing evidence in a digital form, such as from a computer, smartphone or PDA. A graduate of this program will be prepared for entry-level positions as a data recovery technician or member of a security team who monitors and supports computer-based security systems. Graduates would be able to implement procedures/software to maintain a secure computer environment for a business/organization or criminal justice agency. One would also be able to obtain evidence that could be used in a court of law, and would be able to monitor and support security systems.

### Educational Goals:

- to apply basic principles of criminal and business law to ensure the admissibility of evidence in a criminal or civil proceeding.
- to apply the basic concepts of network design, data communications, and Internet principles and practices in the search for and recovery of lost data, and in intrusion detection.
- to use multiple operating systems at the network administrator level of security in order to obtain/work with evidence from different types of computer systems.
- to apply basics of PC management techniques to identify and manipulate the hardware components of a computer system in the process of documenting for a criminal or civil case.
- to apply the basics of security systems, intrusion detection, search and seizure, and economic crime investigation to the network and PC environment.
- to develop professional ethics appropriate to the field of digital forensics.
- to routinely use the PC or other appropriate technology as a tool in his/her daily data recovery, intrusion detection, and business/office-related activities.

### The Major

Students in this program develop a background consisting of general education, criminal justice, and computer technology fundamentals with a CompTIA A+ certification, while being entrenched in the culture of civic engagement. Upon this foundation they add the core of the program in computer, device, network and system forensics, complete with hands-on laboratory activities and community service work. This education is enhanced through obtaining a nationally-recognized certification related to law enforcement or computer security, and an internship with a law enforcement agency or business partner. The students graduate with a major in digital forensic science, two professional certifications in hand, the practical experience of an internship, and the satisfaction of directly benefiting their surrounding community during the process.



## **Digital Forensic Science (CF) Specialty Courses**

### **CF105 CompTIA A+ Computer Essentials Exam Preparation (3)**

This is the first of two courses intended to prepare students to earn the CompTIA A+ certification with the IT Technician designation: a prerequisite to enter the Computer Forensics major of study. In this course, the student learns the basics of computer hardware and operating systems, covering skills such as installation, building, upgrading, repairing, configuring, troubleshooting, and preventive maintenance. At the end of the course, the student should be prepared to complete the CompTIA A+ Essentials Exam, validating the basic skills needed by an entry-level service technician.

Prerequisites: Familiarity with PCs and Windows applications. This is not a course for the novice user.

### **CF106 CompTIA A+ 220-602 Exam Preparation (3)**

This is the second of two courses intended to prepare students to earn the CompTIA A+ certification with the IT Technician designation: a prerequisite to enter the Computer Forensics major of study. In this course, the student continues to develop and refine abilities in installation, building, repairing, configuration, troubleshooting, optimizing, diagnosing and preventive maintenance, preparing for such activities in an enterprise environment or interacting with customers. At the end of the course, the student should be prepared to complete the CompTIA A+ 220-602 Exam, earning the A+ certification as an IT Technician.

Prerequisite: CF105

### **CF110 Introduction to Computer and Digital Forensics (3)**

This course will provide students with a working foundation of the types of computer and electronic crimes being committed today. This course will identify techniques used by offenders to compromise computer systems as well as vulnerabilities of computer and electronic systems. Emphasis will be placed on criminal theory/behavior of this type of offender.

### **CF205 Computer Security Fundamentals (3)**

This course will introduce students to a variety of commonly used computer software systems and their respective security concerns. Specific areas to be studied include wireless technology, PDAs, remote computer access, file transfer mechanisms, networking tools, and various backup devices.

Prerequisite: A+ certification

### **CF210 Operating Systems (3)**

This course provides an overview of operating systems with an emphasis on widely used operating systems and how operating systems manage memory and file allocation. Special attention is given to the security and logging mechanisms provided by the operating system.

Prerequisite: A+ certification

### **CF215 Computer Forensics and Security Ethics (3)**

This course brings together philosophy, law and technology to provide a rigorous, in-depth exploration and analysis of a broad range of topics regarding the ethical implications of widespread use of computer technology. It is designed to provoke students to reflect upon the social and ethical ramifications of managing information. Special consideration will be given to current topics involving computer forensics or computer security issues.

### **CF305 Seizure and Forensic Examination of Computer Systems (3)**

This course will introduce students to the processes involved in seizing hardware, computer equipment and data, and searching them for evidence. This includes how information can be altered, deleted and hidden on various digital media. Topics to be covered will include: establishing probable cause for a search, evidence protection, and the chain of evidence. This includes the industry best practices for examining computers that might contain crime-related information. This course will involve hands-on experience using software to capture and search for evidence.

Prerequisite: CF110, CF205, CF210, CJ217, CJ221

### **CF310 Advanced Topics in Computer Data Analysis and Recovery (3)**

This course will build on the fundamentals covered in CF305. Students will continue the examination of digital evidence, using commercially available and alternative tools. Advanced topics will include: cell phone and Personal Data Assistant (PDA) forensics. Operating system specifics will be explored. Cryptography and steganography will be studied along with password defeating strategies. Lab management utilizing the Scientific Working Group on Digital Evidence (SWGDE) guidelines, along with technical writing and case organization will also be covered.

Prerequisite: CF305

### **CF315 Fundamentals of Computer Networks (3)**

This course is a study of data communication concepts, network topologies, transmission media, wireless transmission, network access control, communication protocols, network architecture, LANs, and WANs. Emphasis is placed on analysis of common communication protocols. Topics covering managing the network will also be covered.

Prerequisites: A+ or Network+ certification

### **CF405 Network Forensics (3)**

Computer and network forensics studies cyber-attack prevention, planning, detection, and response with the goals of counteracting cybercrime, cyberterrorism, and cyberpredators, and making them accountable. It incorporates many areas of concern, including network security, intrusion detection, incident response, infrastructure protection, and computer crime investigation. The topics covered in this course include fundamentals of computer and network forensics, forensic duplication and analysis, network surveillance, intrusion detection and response, incident response, anonymity and pseudonymity, cyber law, computer security policies and guidelines. Emphasis will be placed on hands-on laboratory exercises, to learn to effectively use tools such as WireShark/Ethereal for analyzing network packet data, in order to build a foundation for performing network surveillance and intrusion detection in the more advanced course, CF410.

Prerequisites: CF205, CF315

### CF410 Intrusion Detection (3)

This course will introduce students to the various methods used to detect external and internal intrusion of computer systems. The importance of setting up anomaly and misuse detection measures, host based, multi-host based and network based monitoring strategies and techniques and types of responses will be covered. Various investigative tools will be presented. This course will involve hands-on experiences using intrusion detection software.

Prerequisite: CF405

### CF450 National Certification (2)

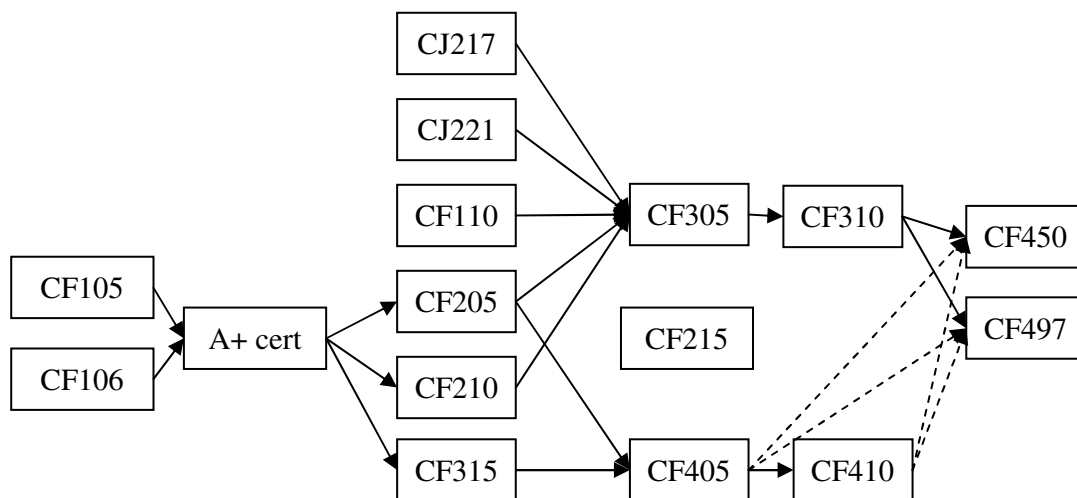
Each student must complete one of the national certification training programs from an approved list. The approved list includes, but is not limited to, the International Association of Computer Investigative Specialists (IACIS – Law Enforcement personnel only), the Seized Computer Evidence Recovery Specialist (SCERS – Law Enforcement personnel only), the SANS GIAC Certified Forensic Analyst (GCFA), and the ISFCE Certified Computer Examiner (CCE).

Prerequisites: complete a sufficient number of the computer forensics courses to qualify for the certification examination and have the permission of the instructor.

### CF497 Computer Forensic Field Experience & Seminar (4)

This course will serve as the capstone course and will require a final paper to demonstrate completion of the learning outcomes of the program. The student gains a basic exposure to an agency involved in computer forensics, and experiences the investigation of high-tech crimes through observation and participation. This course will allow the student to observe professionals at work, and to test out their own computer forensics skills for a minimum of 120 hours.

Prerequisites: complete a sufficient number of the computer forensics courses to prepare for the specific agency's requirements and have the permission of the instructor.



**Prerequisite Relationships**

**Digital Forensic Science 4-Year Plan SAMPLE – Odd Year Start (FA2009, FA2011 entry)**

**Freshman**

**Fall**

CJ111 Introduction to Criminal Justice  
CF105 CompTIA A+ Computer Essentials  
Exam Preparation  
CF110 Introduction to Computer and  
Digital Forensics  
FS101 Freshmen Seminar  
AH110 Writing the Self in Culture

**Spring**

CJ155 Criminal Law  
CF106 CompTIA A+ 220-602 Exam  
Preparation  
MA106 Pre-Calculus Mathematics  
Physical Fitness  
AH120 Writing the World

**Sophomore**

**Fall**

CJ217 Criminal Investigation  
CJ221 Criminal Evidence and Procedure  
CF205 Computer Security Fundamentals  
Physical Science  
AH220 Global Civilization

**Spring**

CA111 Fundamentals of Oral  
Communication  
CF315 Fundamentals of Computer  
Networks  
CF210 Operating Systems  
Biological Science  
SO120 Life in Society

**Junior**

**Fall**

AC221 Financial Accounting  
BA363 Business Law  
CF305 Seizure and Forensic Examination  
of Computer Systems  
PY110 Introduction to Psychology  
CJ471 Criminology

**Spring**

AC222 Managerial Accounting  
CF215 Computer Forensic and Security  
Ethics  
CF310 Advanced Topics in Computer Data  
Analysis & Recovery  
EN220 Topics in Literature  
Elective

**Senior**

**Fall**

Fine Arts  
CF405 Network Forensics  
CF497 Computer Forensic Field  
Experience and Seminar  
Elective  
Elective

**Spring**

Religion  
CF410 Intrusion Detection  
CF450 National Certification  
Elective  
Elective

---

For more information, contact

Dr. Gregg Gunsch, PE, CISSP, GCFA, CCE  
Professor of Digital Forensic Science  
419-783-2460 ggunsch@defiance.edu