Computer Forensics and Security Management (MSCFSM)

View PDF of Computer Forensics and Security Management Admissions Checklist
Prospective students should use this checklist to obtain specific admissions requirements on how to apply to Graduate School.

View PDF version of the Computer Forensics and Security Management catalog description

Program Contact Information

Program Co-Directors:
Dr. Anthony Skjellum
Department of Computer and Information Sciences
CH116
1530 3rd Ave South
Birmingham, AL 35294-1170

tony@cis.uab.edu

Dr. John Sloan
Department of Justice Sciences
UBOB 210
1530 3rd Ave South
Birmingham, AL 35294-4562

prof@uab.edu

Dr. Molly Wasko
Department of Management, Information Systems, and Quantitative Methods
BEC 319
1530 3rd Ave South
Birmingham, AL 35294-4460

mwasko@uab.edu

Program Information

The Master of Science in Computer Forensics and Security Management (MSCFSM) is an interdisciplinary professional practice graduate program involving faculty from the Departments of Computer & Information Sciences and Justice Sciences (College of Arts and Sciences), and
the Departments of Management, Information Systems Quantitative Methods, and Accounting & Finance (School of Business). The program prepares graduate students with backgrounds in criminal justice, computer and information sciences, information systems, information technology, and forensic accounting to practice in the fields of computer forensics and security management including information security and forensic accounting. The program develops required skills, including familiarity with industry practices, innovative methods, critical thinking, and problem solving that are crucial for competitiveness and success in entry- or advanced-level positions in the areas of computer forensics, information security management, and forensic accounting. The program is designed to increase the pipeline of prospective, high-quality, entry- and advanced level employees involved with protecting physical and virtual systems vital to the U.S. whose incapacitation or destruction would have debilitating effects on national security and/or the nation’s economic system. The program also provides current public and private sector employees an opportunity to obtain advanced high-quality training in the core areas of computer forensics, information security management, and forensic accounting, to facilitate career advancement.

The program is modeled after traditional MBA programs, which includes a core curriculum and one or more areas of specialization. In the program, students complete a core curriculum which includes courses in computer forensics/cybercrime investigation, information security management, and ethics. Students then choose a specialization in either computer forensics/cybercrime investigation or fraud examination, both of which include a field practicum (internship) with an appropriate public or private sector agency or organization.

**Faculty**

**Anthony Barnard**, Professor (Computer and Information Sciences), Networks and Network Security;

**John Grimes**, Assistant Professor (Justice Sciences), Cyber-Intelligence, Open-Source Intelligence, Criminal Law and Procedure

**Allen Johnston**, Associate Professor (Management, Information Systems, and Quantitative Methods), Information Assurance and Computer Security; Privacy

**Julio Rivera**, Associate Professor (Accounting and Finance), Forensic Accounting, IT Auditing; Fraud

**Tommie Singleton**, Associate Professor (Accounting and Finance), Forensic Accounting; Information Technology Audits; Fraud

**Anthony Skjellum**, Professor and Chair, Co-Program Director (Computer and Information Sciences), High-Performance Computing; Information Security; Cybercrime

**John Sloan**, Professor and Chair, Co-Program Director (Justice Sciences), Ethics; Cybercrime and Victimization; Research Methods
Thamar Solorio, Assistant Professor (Computer and Information Sciences), Natural Language Processing; Cybercrime

Gary Warner, Instructor and Director of Research in Computer Forensics (Computer and Information Sciences/Justice Sciences), Computer Forensics; Cybercrime Investigation; Information Security

Molly Wasko, Associate Professor and Chair, Co-Program Director (Management, Information Systems, and Quantitative Methods), Information Security Management, Incident Response, Risk Management and Business Continuity.

Sallie Wright, Instructor (Information Technology) Information Assurance and Security

**Admission Requirements**

Students accepted into the program will have graduated with a baccalaureate degree from a regionally accredited college or university or recognized university from abroad. Most students accepted into the program will have achieved a minimum overall undergraduate grade point average (GPA) of 3.0 on a 4.0 scale and will have earned a combined score of 350 or higher on the verbal and quantitative sections of the Graduate Record Examination (GRE) or a total score of 550 or higher on the Graduate Management Aptitude Test (GMAT). An Admissions Committee consisting of the Program Directors and a minimum of 2 affiliated faculty members will screen applicants and make recommendations to the UAB Graduate School for admission into the program.

Students seeking admission to the program will be accepted from undergraduate programs including criminal justice, computer science, electrical and computer engineering, MIS, IT, business, accounting, as well as other science and social science fields. Students seeking admission to the program, regardless of specific undergraduate preparation, will have had formal exposure to the core areas of computer forensics – including cybercrime and its investigation; IT auditing/forensic accounting; fundamentals of computer and Internet literacy, probability and statistics, computer programming, networking, logic, and discrete mathematics/logic, and information security management. Students lacking requisite backgrounds but who meet other admission requirements may be admitted on a contingency basis and required to take a series of prerequisite courses – potentially including courses in computer programming, accounting, and law – that allow them to develop the necessary backgrounds to be successful in the program. These courses may include the following (or their equivalent): IS204 (Intro to Business Programming)/CS 201 (Intro to Object Oriented Programming); CS250 (Discrete Structures); AC200/201 (Principles of Accounting I & II); AC304 (Accounting Information Systems).

**Degree Requirements**

A total of 36 semester hours are required for the degree, including 24 hours of required courses and 12 hours of electives in one of two tracks: Cybercrime and Computer Forensics or Fraud
Examination. Students are also required to complete a field practicum.


Course Descriptions

AC572 - Forensic Accounting & Information Technology Auditing. Key legal principles and courtroom procedures relevant to forensic accounting, and survey of related topics - criminology theories, evidence management, and litigation services. Hours Credit: 3.

AC573 - Fraud Examination. Forensic accounting concepts with a primary focus on occupational fraud and abuse - its origins, perpetration, prevention, and detection. Course covers some of the material found on Certified Fraud Examiner (CFE) certification exam. Hours Credit: 3. Prerequisite: AC572

AC574 - Fraud Examination Practicum. Work-related experience in a private, public, or government organization enhancing the applications of forensic accounting theories and concepts. Hours Credit: 3. Prerequisite: AC573.


CS516 - Organizational Information Assurance. Information assurance in organizational settings, including prevention, detection, response to threats, and subdomains and their interactions. Hours Credit: 3.


CS518 - Computer Forensics Practicum. Internship placement with law enforcement agency or corporate partner-. Hours Credit: 3-6.

CS534 - Internetworking & Intranets. Underlying network technology including interconnecting networks using bridges and routers, IP addresses and datagram formats, static and dynamic routing algorithms, control messages, subnet and supernet extensions. UDP and
TCP file transfer protocols, email, network address translation and firewalls. Weekly Linux-based lab. *Hours Credit: 3.*

**CS536 - Network Security.** Conventional and public-key cryptography. Message encryption and authentication. Secure communication between computers in a hostile environment, including E-mail (PGP), virtual private networks (IPSec) and the World Wide Web (SSL). Mandatory weekly Linux-based lab. *Hours Credit: 3.*

**CS537 - Cybercrime & Forensics.** Overview of all aspects of media forensics including analysis of character encoding, file formats and digital media, examination of disk acquisition and duplication techniques and application of these techniques in criminal investigations scenarios. *Hours Credit: 3.*

**CS636 - Computer Security.** Study of computer security including assurance, authorization, authentication, key distribution, encryption, threats including phishing and key logging, and related distributed computing issues. Theory and practical applications. *Hours Credit: 3.*

**CS591 - Special Topics in Organizational Information Assurance (CISSP Training).** Preparation for Certified Information Systems Security Professional examination. *Hours Credit: 3.*

**IS577 - Information Security Management.** Provides students with a strong foundation in key security management issues, including: an understanding of key concepts and how people, technology and organizational policies should be developed and managed to safeguard an information resources. *Hours Credit: 3.*

**JS530 - Ethics and Computer Forensics.** Overview of systems of ethics with application of core principles to issues relating to cyberinvestigation, computer forensics, and related areas. *Hours Credit: 3.*

**JS502 - Introduction to Computer Forensics.** Analytical and investigative techniques in criminal or civil litigation to identify, collect, examine and preserve evidence/information magnetically stored or encoded. *Hours Credit: 3.*

**JS675 - Law, Evidence & Procedure.** Overview and examination of the legal aspects of physical evidence including rules of evidence, procedural rules, and the role of expert witnesses; moot court component. *Hours Credit: 3.*

**LS571- Expert Witness & Litigation Support.** Principles of law related to forensic accounting, including forensic evidence, and expert witnesses. The course content covers some material found on the Certified Fraud Examiner (CFE) certification exam. *Hours Credit: 3.*

Last modified 02/28/2012