Course Descriptions

CRJ 708. Law, Evidence, and Ethics
Examines the rules of evidence followed in criminal investigation, criminal trials and administrative proceedings. Pays special attention to the methods and ethical obligations of government agents assigned to gather evidence.

CRJ 710. Issues in Criminal Justice
Begins an overview of the operations and problems of the criminal justice system. Examines crime statistics, the causes of crime, and other issues of concern to criminologists. Highlights the role of the courts and the legal constraints derived from the Constitution on arrest, prosecution, and conviction.

CRJ 727. Cybercriminology
An exploration of the links between computers, deviance and social control. This will include analysis of the technological, social and geo-political context from which cybercrime and information warfare have emerged and the nature, extent and causes of digital deviance, such as hacking and cyber-terrorism. Societal and political reactions to cybercrime are considered, as are social policy questions of privacy and freedom on the Internet. (Prerequisite: CRJ710 Issues in Criminal Justice)

CRJ 733. The Constitution and Criminal Justice
Provides an intensive review of recent landmark Supreme Court decisions that interpret Constitutional guarantees and limit government actions. Examines problems of reconciling individual rights with societal concerns about safety and crime prevention.

CRJ/PAD 750 Security of Information and Technology
Surveys organizational responses to risk associated with the integrity of information and technology. Reviews the legal basis for privacy and security of information and related technology. Presents methods and procedures for the assessment of risk, and examines strategies for mitigation of risk involving operational procedure, software and hardware, and building systems.

FCM 700. Theoretical Foundations of Computing Security
The theoretical foundations of computing and systems analysis are discussed. Topics include combinatorial and counting methods, graph theory, recurrence relations, theory of computation, and complexity analysis. Examples concerning the modeling and analysis of networks, routine protocols, scheduling problems, and algorithm and software complexity are used to illustrate the principles involved. (Prerequisites: Undergraduate FCM course requirements)

FCM 710. Architecture of Secure Operating Systems
The design, implementation and administration of modern operating systems are reviewed. Topics covered include concurrent execution, process and memory management, local and networked file systems. Security models, access control mechanisms and security enhanced version of current operating systems are discussed. (Prerequisites: Undergraduate FCM course requirements)

FCM 740. Data Communications Forensics and Security
Study of the problems of securing, monitoring and investigating the content of private communications. Issues considered included such topics as securing and monitoring private data exchanges over the Internet or between systems, vulnerabilities of communications protocols and media, cryptography, and steganography. The course includes laboratory work in the use of specialized investigative and security software. (Prerequisites: FCM 700 Theoretical Foundations of

FCM 742. Network Security
Fundamentals of computer networks and distributed processing. Network security policy, risk assessment and management, and protocols for secure network infrastructures are emphasized. *(Prerequisites: Undergraduate FCM course requirements)*

FCM 745. Network Forensics
Concerns the forensic and security issues related to access to data stored on computer systems and the transmission of data between systems. Topics include detecting and monitoring intrusions of networks and systems, authentication protocols, viruses and worms, and management of intrusion response teams. The course includes laboratory work, such as attack and defend exercises. *(Prerequisites: FCM 700 Theoretical Foundations of Computing Security; FCM 710 Architecture of Secure Operating Systems; FCM 742 Network Security)*.

FCM 752. The Law and High Technology Crime
A survey of basic constitutional and statutory issues pertaining to high technology crime and its investigation. Special attention is paid to the rules of evidence as they apply to electronic or digital evidence, the role of expert witnesses, and the laws and regulations governing electronic surveillance.

FCM 753. Digital Forensic Applications
Intensive application of computer and network forensics in simulated casework along with critique of actual cases. Includes design of a digital forensics lab, forensic analysis, preparation of case reports and expert testimony. *(Prerequisites: FCM 700 Theoretical Foundations of Computing Security; FCM 710 Architecture of Secure Operating Systems; FCM 742 Network Security; FCM 752 Law and High Technology Crime; FCM 760 Forensic Management of Digital Evidence)*

FCM 760. Forensic Management of Digital Evidence
Students are introduced to information systems used in forensic computing and the methods for analyzing the information exposed by these systems. Emphasis will be on technology permitting the retrieval, preservation, and analysis of computer data which might be used in potential legal cases. Among the topics studied are evidence collection and preservation, data copying, data warehousing and data mining, probability and statistics methods, classification, prediction and cluster analysis. *(Prerequisites: Undergraduate FCM course requirements)*

FCM 780. Forensic Computing Capstone Seminar and Fieldwork
This course is intended to give students a chance to meld theory and practice through actual experience in the field. It offers supervised fieldwork on a forensic computing or computer security problem, sometimes with the participation of program faculty. Biweekly seminar meetings with supervising faculty complement the fieldwork. Students are assigned to work with either an agency or corporate partner of the graduate program. *(Prerequisite: Successful completion of Qualifying Exam)*

FCM 791. Forensic Computing Prospectus Seminar
Assists in the identification and delineation of researchable topics. Provides an introduction to scholarly and research report writing, library research, and documentation styles and techniques. Development by the end of the semester of a thesis prospectus. *(Prerequisites: Successful completion of Qualifying Exam and permission of program directors)*
This course is a calculus-based course intended to provide a solid understanding of probability and mainstream statistical techniques for research and professional applications in the field. Prerequisite: One year of undergraduate calculus.