DIGITAL FORENSICS (DFSC)

DFSC 5310. Princple& Policy-Info Assuranc. 3 Hours.
An investigation into the development of security planning and policy formation, risk management, security education, training and awareness programs. This course examines physical and electronic approaches to data protection and derives appropriate assessment strategies for determining the assurance quality of target systems.

DFSC 5315. Network and Cyber Security. 3 Hours.
This course provides the framework and procedures for securing computer systems and data networks. Topics include the methodologies for the design of security systems, establishing security protocols, and the identification of best practices in administration, testing, and response protocols for secure communications systems.

DFSC 5316. File System Forensics. 3 Hours.
This course focuses on the important concepts associated with the structures, encoding, boot process and storage technologies of modern computers, and the implications of those concepts regarding the analysis of volumes and file systems for forensics purposes.

DFSC 5317. Digital Security. 3 Hours.
This course introduces the student to basic security needs. The course will include, but not be limited to examination of individual vs. government privacy issues, federal encryption standards, the different layers of security currently available, cryptography, and strategies for evaluation and selection of security methods.

DFSC 5318. Cyber Law. 3 Hours.
The focus will be on how the law impacts digital security in diverse ways. Discussion will emphasize the concept of criminal intent, the digital victim and address jurisdictional issues and provide an overview of legal terms and issues with which the security manager must address.

DFSC 5325. Organization System Security. 3 Hours.
This course provides advanced study of system security concepts as applied to the protection of organizational systems including (1) principles of security modeling, accountability and access control, (2) the ISO model for network infrastructure design and protection, (3) communication security and control management, (4) auditing and monitoring, (5) incident management, and(6) law, investigations and ethics.
Prerequisite: DFSC 5310.

DFSC 5327. Digital Forensics Investigatn. 3 Hours.
This course explores tools for the recovery of information on hardware or hidden within other formats. Topics also include cryptographic analysis, password recovery, the bypassing of specific target operating systems, and obtaining data from a digital device that has been destroyed.

DFSC 5328. Software Forensic Evidence Mgt. 3 Hours.
Analysis of investigative techniques and tools in the detection, investigation and analysis of digital crimes. This course examines the nature of cyberevidence and the tracking and identification of cybercriminals.

DFSC 5336. Business Continuity Management. 3 Hours.
This course examines identification and assessment of threat, risk, vulnerability and business continuity in case of disaster, as applied to enterprise IT systems. It incorporates the physical safeguards and policies necessary to meet the requirements for the protection of data in a fixed site. This course also discusses techniques and strategies designed to keep enterprise data in service under critical circumstances.

DFSC 5340. Spcl Tpcs In Digital Forensics. 3 Hours.
Topics and courses are selected to suit individual needs of students. The course may be repeated for additional credit.
Prerequisite: Approval by the graduate advisor.

DFSC 6310. Cyber Warfare & Terrorism. 3 Hours.
This course will focus on philosophies, tactics, and targets of cyber terrorist organizations. The course includes discussion of emerging cyber war trends and the roles of the private sector and U.S. Government in responding to, mitigating and preventing electronic offensive actions.

DFSC 6312. Multimedia Forensics. 3 Hours.
This course examines the theory and practice of multimedia security and forensics. Topics include image processing, JPEG compression, audio compression (MP3, Advanced Audio Coding, and VOIP), MPEG compression, multimedia source identification, biometrics, steganography, steganalysis, multimedia forgery detection, and pattern recognition techniques for multimedia analysis, multimedia forensics software, and advances in multimedia forensics.

DFSC 6313. Wireless Network Security. 3 Hours.
This course provides advanced study of the full range of algorithms, mechanisms, and technologies in securing various types of wireless communication networks, such as cellular networks, Wireless Local Area Networks, Bluetooth Networks, Mobile Ad Hoc Networks, and Wireless Sensor Networks. Research and applications will be explored.

DFSC 6347. Directed Mgt & Development Prj. 3 Hours.
This course will provide the rationale and necessity for a full range of security concepts and techniques and how to apply them to multiple operating systems. The course will cover methodologies for the design of operating system security and forensic techniques for operating systems. Also covered will be the identification of best practices in the administration, testing and security for operating systems. Continuous enrollment in DFSC 6347 is required until graduation.
Prerequisite: 24 hours graduate coursework.

DFSC 6410. Cyber Forensics Principles. 4 Hours.
This course explores the skill set and conceptual understanding required by digital and cyber forensic scientists and researchers operating in a heterogeneous hardware, software, and network environment. Topics may include hardware and software principles, forensic protocols, data acquisition and discovery of date evidence, applicable law, the design, benefits and limitations of commercial tools, analysis techniques, and report writing.

DFSC 7106. Seminar in Digital Forensics. 1 Hour.
This course immerses students in emerging trends and issues in digital and cyber forensics. The content of the course may vary from semester to semester but includes analysis of current research, security concerns, standards publications, and professional issues.

DFSC 7300. E-Discovery. 3 Hours.
This course explores the initial phase of litigation to find and provide relevant electronic information and records, or electronically stored information, related to a legal case. Technical content of this course includes records management policies and procedures, and E-Discovery applications and technologies for locating and extracting information and records from massive volumes of data in timely and cost efficient ways.

DFSC 7320. Ethics for Digital Forensics. 3 Hours.
This course examines the ethical issues surrounding the collection, preparation, interpretation, and reporting of digital evidence. The American Academy of Forensic Sciences' "Code of Conduct" and the Digital Forensics Certification Board?s ? Code of Ethics and Standards of Professional Conduct? are critically examined and explored. Students examine case materials that feature ethical conflicts and approaches to resolving ethical dilemmas.

DFSC 7330. DF Laboratory Management. 3 Hours.
This course examines techniques to cost-effectively establish and manage a computer forensics laboratory, and its subsequent support to successfully conduct computer-related criminal investigations. Topics include case and evidence management, development of laboratory policies and procedures, funding a digital forensic lab, competency and proficiency testing, equipment validation and verification, lab accreditation from organizations such as the American Society of Crime Lab Directors (ASCLD), and compliance with ISO standards.

DFSC 7340. DF Tools & Techniques. 3 Hours.
This course explores the use of commercial and open-source tools for the identification, collection, and analysis of digital evidence. Topics include the principles of locating and seizing digital evidence, best practices in evidence management, protocols for comprehensive analysis, and a comparative analysis of digital and cyber forensic tool performance.

DFSC 7341. DF Infrastructure. 3 Hours.
This course focuses on the development of laboratory policies and procedures, funding a digital forensics lab, training and certification of examiners, competency and proficiency testing. Topics include validation and verification of digital forensics equipment, compliance with ISO standards, and management of the forensic laboratory.

DFSC 7350. Operating System Forensics. 3 Hours.
This course explores required background knowledge, theory, and practical skills in operating system forensics, including hard disk data acquisition, volume analysis, file system data structure analysis, registry analysis, memory analysis, malware detection, and timeline analysis.
Prerequisite: DFSC 5316.

DFSC 7351. Cloud Computing Forensics. 3 Hours.
This course focuses on the security, vulnerabilities, digital evidence retrieval, analysis, and maintenance in virtualized infrastructures and cloud environments. Topics include the chain of cloud service providers, cloud customers and the complexity of dynamic chain of dependencies between them, and the approaches, methods, and tools that can be used in forensic analysis in virtual and cloud environments.

DFSC 7352. Network Forensic Analysis. 3 Hours.
This course examines start-to-finish methodology and tools for managing network forensics investigation, enables students to uncover powerful forensic evidence from routers, firewalls, intrusion detection and prevention systems, web proxies, and other network devices. Topics may include network evidence acquisition, packet analysis, network flow analysis, wireless network forensics, network log analysis, and network device forensics.
Prerequisite: DFSC 6410.

DFSC 7353. RAID & Remote System Forensics. 3 Hours.
This course examines the theories and practices of RAID (Redundant Array of Inexpensive Disks) and remote system forensics. Concepts addressed in this course include disk imaging, retrieval, maintenance, backup, analysis, and presentation of digital evidence from RAID and remote systems.
Prerequisite: DFSC 7340.

DFSC 7355. Intrusion Forensic Analysis. 3 Hours.
This course provides the study and practices of intrusion detection, vulnerability assessment, and penetration testing. Topics include traffic analysis, intrusion detection methods and systems, intrusion detection system evaluation, vulnerability assessment, methods, techniques, and tools for penetration testing, and system and network security evaluation and assessment.
Prerequisite: DFSC 6410.

DFSC 7356. Mobile Device Forensics. 3 Hours.
This course explores the required background knowledge, theory, and practical skills pertaining to mobile device forensics. Topics focus on the most widespread operating systems on the mobile market. This course examines mobile device evidence collection, data recovery and analysis techniques and tools, system file recovery, deleted file recovery, and the examination of unallocated space.
Prerequisite: DFSC 7350.

DFSC 7357. Malware Forensic Analysis. 3 Hours.
This course explores the concepts and techniques for analyzing, dissecting, debugging, and reverse engineering malicious software. Forensic techniques for protection and recovery from malicious code will be examined in detail.

DFSC 7358. Live System & Memory Forensics. 3 Hours.
This course examines advanced collection and analysis of digital evidence from systems and networks when they are running. Topics may include data acquisition, memory, network connections and traffic, user accounts and passwords, environmental variables, and system and application logs. The course also includes the comparison and evaluation of live forensic tools and techniques.
Prerequisite: DFSC 5316.

DFSC 7359. Social Network Forensics. 3 Hours.
This course examines techniques used to conduct a digital forensic analysis of social networking websites and smart phone social networking applications. This course also explores social media artifacts left on computers such as artifacts in Internet history files, cache, chat logs, web logs, comments and requests in blogs.

DFSC 7360. DF Research Methods. 3 Hours.
This course examines appropriate techniques for the construction of sound research projects. It addresses the identification of appropriate research questions and hypotheses, the critical analysis of sources, the development of explanatory models, the selection of appropriate testing mechanisms and the presentation and interpretation of results. Emphasis is placed on the development of research and writing capabilities. Case studies from current digital and cyber forensic research are presented.
Prerequisite: DFSC 7362.

DFSC 7362. Computational Forensics. 3 Hours.
This course examines principles and uses of computational intelligence methodologies and algorithms in soft computing and digital forensics. Students become familiar with core concepts of each algorithm and a broad perspective of emerging applications to practical problems in digital forensics. Topics may include fuzzy sets, rough sets, artificial neural networks, evolution computing, probabilistic reasoning, and their applications to digital forensics.

DFSC 7364. Scientific Communications. 3 Hours.
This course examines aspects of scientific communication, specifically writing in the disciplines. The goal of this course is to enable students to write professionally in the field of digital and cyber forensic science. The course includes strategies on writing research papers, dissertations, grants, and conference presentations. Emphasis is placed on how to use multi-media effectively in presentations and technical communications.

DFSC 7365. Commercial Tool Verification. 3 Hours.
This course focuses on the principles and techniques in software testing, including the design of high quality tests, the theory behind criteria-based test design and its application in practice. Topics include test design, test automation, test coverage criteria, and how to test software in cutting-edge software development environments. Topics also include proving correctness, and static and dynamic analysis.
Prerequisite: DFSC 7340.

DFSC 7600. Internship. 6 Hours.
This is a ten-week, full-time internship in an approved digital forensic science laboratory. This opportunity allows graduate students to apply their theoretical knowledge, practical skills and abilities in a digital forensic science setting.

DFSC 8370. Dissertation. 3 Hours.
This course must be taken five times to obtain 15 hours of credit to satisfy degree requirements for the PhD in Digital and Cyber Forensics Science.
Prerequisite: Successful completion of requirements for admission to candidacy in the Digital and Cyber Forensic Science PhD program.