DIGITAL FORENSICS (DFSC)

DFSC 1316. DF and IA Fundamentals I. 3 Hours.
This course introduces students to the fundamentals of Digital Forensics (DF) and Information Assurance (IA) technologies. Topics include basics of DF and IA, numbering systems, logic, Boolean operations, network packets, OSI layers, TCP/IP protocols, basic scripting and compiled languages, and basics of hardware and file system forensics.

DFSC 2316. DF and IA Fundamentals II. 3 Hours.
This course focuses on Digital Forensics (DF) and Information Assurance (IA) processes and methodologies. Topics include preparation of the investigator, proper acquisition of evidence, authentication, analyzing data without modifying it, reporting findings, and risk assessment of evidence. In addition, current methodologies such as cryptography and network security, Internet programming, smartphone forensics, network forensics, and cloud forensics will be discussed.
Prerequisite: DFSC 1316.

DFSC 2320. Hardware Forensics. 3 Hours.
Techniques in the duplication, recovery and restoration of digital evidence. Includes hard disks, floppy drives, CD formats, DVD formats, zip drives, mobile phones, PDA?s smart cards, memory technologies, and other devices capable of storing digital information.
Prerequisite: DFSC 1316.

DFSC 3316. Cryptography and Network Scrty. 3 Hours.
This course involves the study of both the theory and practice of cryptography and computer and network security, and focuses on the security aspects of the web and the internet. It surveys cryptographic tools used to provide security, such as shared key encryption, public key encryption, key exchange, and digital signature algorithms. It then reviews how these tools are used in the current Internet protocols and network security applications, including wireless network protocols. System security issues, such as viruses, worms, intrusion, and firewalls will also be discussed.
Prerequisite: DFSC 2316 and MATH 2395 .

DFSC 3320. Digital Forensics Tools. 3 Hours.
This course explores tools for the recovery of information on protected or damaged hardware for the purpose of providing evidence of misuse or abuse of systems. Topics also include the chain of evidence, protocols for data recovery, cryptographic analysis, password recovery, the bypassing of specific target operating systems, and obtaining data from digital devices that have been damaged or destroyed.
Prerequisite: DFSC 1316.

DFSC 4317. Information Security. 3 Hours.
This course provides an introduction to basic security needs. The course will include, but not be limited to individuals vs. government privacy issues, federal encryption standards, the different layers of security currently available, the practical application of user level and system level cryptography, and strategies for evaluation and selection of security methods.
Prerequisite: DFSC 2316 and 3 advanced DFSC hours.

DFSC 4318. Malware. 3 Hours.
This course focuses on analyzing, dissecting, debugging, and reverse-engineering malicious software. Topics include conventional and advanced static and dynamic analysis of malware in a virtual environment using disassemblers, debuggers, packers/unpackers and virtual machine tools.
Prerequisite: DFSC 3320 and a basic knowledge of the C programming language, fundamentals of x86 disassembly and Windows programming are required.

DFSC 4319. Principles of Data Quality. 3 Hours.
This course provides a rigorous exploration of data quality concepts, assessment techniques, and problems in organizational information systems, databases, and data warehouses. A combination of state-of-the-art literature review and hands-on projects is used to develop knowledge and ability to analyze and clean the data.
Prerequisite: 6 advanced COSC/DFSC hours.

DFSC 4338. Cyber Warfare. 3 Hours.
This course examines the philosophies, targets, and tactics of organizations involved in the development of cyber offensive and defensive capabilities. Topics include emerging cyber warfare trends and the role of the private sector and the U.S. government in identifying, protecting, detecting, responding to, and recovering from cyber warfare threats.
Prerequisite: DFSC 4318.

DFSC 4340. Spcl Tpcs In Digital Forensics. 3 Hours.
Topics of general interest are offered on a timely basis. Previous topics include DC3 Challenge.
Prerequisite: 6 advanced hours of DFSC and senior standing.