# DIGITAL FORENSICS (DFSC)

**DFSC 1316. Digital Forensics & Information Assurance Fundamentals I. 3 Hours.**
Students are introduced to the fundamentals of Digital Forensics (DF) and Information Assurance (IA) technologies. Topics may 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. Digital Forensics & Information Assurance Fundamentals II. 3 Hours.**
Students focus on Digital Forensics (DF) and Information Assurance (IA) processes and methodologies. Topics may 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 are discussed.
**Prerequisite:** DFSC 1316.

**DFSC 2320. Hardware Forensics. 3 Hours.**
Students explore techniques in the duplication, recovery, and restoration of digital evidence, which 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 Security. 3 Hours.**
Students study both the theory and practice of cryptography and computer and network security, and focus on the security aspects of the web and the internet. Students survey cryptographic tools used to provide security, such as shared key encryption, public key encryption, key exchange, and digital signature algorithms. In addition, students review 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 are also discussed.
**Prerequisite:** DFSC 1316.

**DFSC 3320. Digital Forensics Tools. 3 Hours.**
Students explore 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 may 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 4050. Independent Study. 1-3 Hours.**
Students conduct individual research on specific topics that are not covered in the current Digital Forensics undergraduate curriculum. Students participate in comprehensive research activities with a faculty member who is specialized in the students' interest area. Therefore, the course content varies based upon the topic that both the students and the mentoring faculty member choose. Students' performance will be evaluated based on their research progress and output. Variable Credit (1 to 3).
**Prerequisite:** Consent of the instructor.

**DFSC 4317. Information Security. 3 Hours.**
Students are provided an introduction to basic security needs. Course topics may include, but are not 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.

**DFSC 4318. Malware. 3 Hours.**
Students focus on analyzing, dissecting, debugging, and reverse-engineering malicious software. Topics may 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 1316.

**DFSC 4319. Principles of Data Quality. 3 Hours.**
Student are provided 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.**
Students examine the philosophies, targets, and tactics of organizations involved in the development of cyber offensive and defensive capabilities. Topics may 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 1316.

**DFSC 4340. Special Topics 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.