Digital Forensics (DF)

Courses

DF 242 Computer Forensics I 4 Cr.
This course provides the student with an ability to perform basic forensic techniques and use appropriate media analysis software. Knowledge of the security, structure and protocols of network operating systems and devices are covered as students learn to gather evidence in a networked environment and to image and restore evidence properly without destroying its value. Students learn and practice gaining evidence from a computer system while maintaining its integrity and a solid chain of custody. Within the laboratory, students gain hands-on experience in the use of current investigative tools. Classroom 3 hours, laboratory 2 hours. Cross-listed as CJ 442. Prerequisites: CJ 341 or IA 241 and a C or higher in IS 130 or CS 140.

DF 311 Network Forensics 3 Cr.
Introduces digital forensic concepts and practices on local area networks, wide area networks and large scale networks such as the Internet. Lectures include topics based on table of contents in (Davidoff and Ham 2012) such as investigative techniques, and how to conduct an investigation, manage evidence and follow a cyber-trail. A large part of the course involves demonstrations and hands-on labs, including: use of network forensic tools such as packet monitors, security information and event managers (SIEMs), tracers, and other tools useful for analyzing events. Many of the labs involve analysis of packet captures of both actual attacks and theoretical malfeasance by offenders. Students have a final lab exercise instead of a final exam and are expected to research and present a final project. Prerequisite: IS 460 or CS 260.

DF 312 Malware Forensics 3 Cr.
This predominantly laboratory-based course is an introduction to malware forensics including both static and dynamic analysis. Students study profiling, malware behavior, behavior of malware on computer networks, anti-reversing and anti-debugging techniques, and packers. Prerequisite: CS 212.

DF 395 Cyber Criminalistics 3 Cr.
This survey course uses lecture, case studies and hands-on lab exercises in digital investigation and cyber forensics to introduce students to the investigation and analysis of cybercrime and cyber criminals. Topics include: cybercrime typology, cyber-criminal profiling, network tracking, introduction to the tools of the cyber- criminalist, techniques of cybercrime scene assessment, digital evidence management and analyzing the forensic remnants of a cyber event. During the course of the laboratory exercises, students create a personal lab notebook recording their lab exercises and manage evidence including maintaining a proper chain of custody. Prerequisites: Open to CJ 2nd semester sophomores or higher, or by instructor permission.

DF 411 Cyber Investigation 3 Cr.
An introduction to cyber investigation, including elements of cybercrime, cyberwarfare and cyberterrorism. The course examines investigative techniques for cyber-investigators, case studies of representative cybercrimes and cyber warfare incidents, some cyber investigation tools and expert witnessing. The course builds up to a mock trial where students act as a cyber-investigation task force on an actual case of cybercrime. This is a course that incorporates extensive reading as well as hands-on lab exercises. Prerequisites: Open to CS or CSIA 2nd-semester sophomores or higher, or by instructor permission.

DF 423 Advanced Digital Forensics 3 Cr.
This course Expands upon concepts learned throughout the digital forensics concentration in the BSCSIA major. It is based upon the Certified Cyber Forensic Professional (CCFP) certification review class and covers the six domains (Ethics and Law, Forensic Science, Investigation, Digital Forensics, Application forensics and Hybrid and Emerging Technologies). Students completing this class successfully are prepared to take the CCFP certification exam and, if they pass, are qualified to become certified either as CCFPs or (ISC) Associates until they achieve three years of field experience. Prerequisite: DF 242, DF 311, DF 411 or permission of instructor.