DIGITAL FORENSICS TECHNOLOGY (DGFR)

DGFR:100 Introduction to Digital Forensics (3 Credits)
An overview of digital forensics and computer-related issues facing government and businesses. Specific focus on forensic examinations and methodologies used in the field. (Formerly 2235:100)

DGFR:280 Cybercrime (3 Credits)
Examines crime and deviance in cyberspace. Particular focus is on the prevention of computer intrusion in the workplace. (Formerly 2235:280)

DGFR:281 Computer Forensic Methods (3 Credits)
Prerequisite: DGFR 100. Examination of computer forensic methods employed to identify, collect, recover, authenticate, preserve, analyze, and document electronic evidence for criminal or civil legal purposes. (Formerly 2235:281)

DGFR:282 Digital Forensic Imaging (3 Credits)
Prerequisite: DGFR 100 or CRJU 100. This course covers the general principles of photography and practical elements and advanced concepts of forensic photography. (Formerly 2235:282)

DGFR:283 Cyber Warfare (3 Credits)
Prerequisite: DGFR 280. Examines the participants, tools and techniques in digital conflicts and explores how to defend against espionage, hactivism, non-state actors and terrorists. (Formerly 2235:283)

DGFR:284 Windows Forensics (3 Credits)
Prerequisite: DGFR 281. An examination of the tools, methodology, and advanced digital forensic analysis of the Windows Registry and the Microsoft Windows operating systems. (Formerly 2235:284)

DGFR:381 Computer Forensic Methods II (3 Credits)
Prerequisite: DGFR 281. Obtaining and analyzing digital information from computer storage media to determine details of origin and content. (Formerly 2235:381)

DGFR:382 File System Analysis (3 Credits)
Prerequisite: DGFR 281. The analysis of volumes, partitions, and data files to understand the design of file systems and data structures. (Formerly 2235:382)

DGFR:383 Ethical Hacking (3 Credits)
Prerequisite: DGFR 283. An examination of the tools, methods, and structured approaches to conducting basic security testing to protect computer networks from attacks. (Formerly 2235:383)

DGFR:440 Intrusion Detection (3 Credits)
Prerequisites: DGFR:443 with a grade of C or better and junior or greater standing. This course will introduce students to the various methods used to detect external and internal intrusion of computer systems. (Formerly 2235:440)

DGFR:441 Network Forensics I (3 Credits)
Prerequisites: DGFR 281 with a grade of C or better and junior or greater standing. This course will provide the student with basic knowledge of surveillance of networking devices, identifying and preventing attacks and incident response. (Formerly 2235:441)

DGFR:442 Wireless Forensics (3 Credits)
Prerequisite: DGFR 441 with a grade of C or better and junior or greater standing. The forensic identification and tracking of attacks on wireless networks and mobile communications devices. (Formerly 2235:442)

DGFR:443 Network Forensics II (3 Credits)
Prerequisite: DGFR 441 with a grade of C or better or junior or greater standing. Deployment, building and running an NSM operation using open source software and vendor neutral tools with the Linx Operating System. (Formerly 2235:443)

DGFR:480 Digital and Scientific Evidence (3 Credits)
Prerequisite: CRJU 104. Examination of the role of scientific and digital evidence in the legal system. Courtroom admissibility and presentation rules are covered. (Formerly 2220:480)