

CYBER CRIME TECHNOLOGY (CCT)

CCT 110 Introduction to Cyber Crime 3/3

This course introduces and explains the various types of offenses that qualify as cyber crime activity. Emphasis is placed on identifying cyber crime activity and the response to these problems from both the private and public domains. Upon completion, students should be able to accurately describe and define cyber crime activities and select an appropriate response to deal with the problem.

Prerequisite: None

Corequisite: None

CCT 121 Computer Crime Investigation 5/4

This course introduces the fundamental principles of computer crime investigation processes. Topics include crime scene/incident processing, information gathering techniques, data retrieval, collection and preservation of evidence, preparation of reports and court presentations. Upon completion, students should be able to identify cyber crime activity and demonstrate proper investigative techniques to process the scene and assist in case prosecution.

Prerequisite: None

Corequisite: None

CCT 240 Data Recovery Techniques 5/3

This course introduces the unique skills and methodologies necessary to assist in the investigation and prosecution of cyber crimes. Topics include hardware and software issues, recovering erased files, overcoming encryption, advanced imaging, transient data, Internet issues and testimony considerations. Upon completion, students should be able to recover digital evidence, extract information for criminal investigation and legally seize criminal evidence.

Prerequisite: None

Corequisite: None

CCT 250 Network Vulnerabilities I 4/3

This course introduces students to penetration testing, network vulnerabilities, and hacking. Topics include an overview of traditional network security, system hardening, and known weaknesses. Upon completion, students should be able to evaluate weaknesses of traditional and wireless network for the purpose of incident response, reconstruction, and forensic investigation.

Prerequisite: Take NET 110 or CTI 120;

Corequisite: None

CCT 251 Network Vulnerabilities II 4/3

This course advances students' knowledge of penetration testing, network vulnerabilities, and hacking. Topics include analyzing advanced techniques for circumventing network security hardware and software. Upon completion, students should be able to assemble test kits for multiple operating systems, scan and footprint networks, and perform advanced forensic investigation.

Prerequisite: Take CCT 250;

Corequisite: None