Cyber Crime Technology (CCT)

CCT 110. Introduction to Cyber Crime. 3.0 Credits. Class-3.0. Clinical-0.0. Lab-0.0. Work-0.0
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.

CCT 121. Computer Crime Investigation. 4.0 Credits. Class-3.0. Clinical-0.0. Lab-2.0. Work-0.0
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.
Prerequisites: Take CTI 130, minimum grade of C

CCT 231. Technology Crimes & Law. 3.0 Credits. Class-3.0. Clinical-0.0. Lab-0.0. Work-0.0
This course covers the applicable technological laws dealing with the regulation of cyber security and criminal activity. Topics include an examination of state, federal and international laws regarding cyber crime with an emphasis on both general and North Carolina statutes. Upon completion, students should be able to identify the elements of cyber crime activity and discuss the trends of evolving laws.

CCT 240. Data Recovery Techniques. 3.0 Credits. Class-2.0. Clinical-0.0. Lab-3.0. Work-0.0
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.
Prerequisites: Take CCT 121, minimum grade of C

CCT 241. Advanced Data Recovery. 3.0 Credits. Class-2.0. Clinical-0.0. Lab-3.0. Work-0.0
This course further explores the methodologies necessary to assist in the investigation and analysis of cyber crimes. Topics include commercial and open-source software tools for working with evidence acquisition, data recovery, and encryption. Upon completion, students should be able to perform the data recovery and analysis for a complete criminal or corporate investigation.
Prerequisites: Take CCT 240, minimum grade of C

CCT 260. Mobile Phone Examination. 3.0 Credits. Class-1.0. Clinical-0.0. Lab-4.0. Work-0.0
This course introduces the unique skills and methodologies necessary to assist in the investigation and prosecution of cyber crimes involving mobile phones. Topics include the basics of the cellular networks as well as data extraction from GSM, iDEN and CDMA handsets. Upon completion, students should be able to use the course processes and methodologies to obtain forensic evidence from GSM, iDEN and CDMA handsets.

CCT 289. Capstone Project. 3.0 Credits. Class-1.0. Clinical-0.0. Lab-6.0. Work-0.0
This course provides experience in cyber crime investigations or technology security audits in either the public or private domain. Emphasis is placed on student involvement with businesses or agencies dealing with technology security issues or computer crime activities. Upon completion, students should be able to successfully analyze, retrieve erased evidence and testify in mock proceedings against these criminal entrepreneurs.
Prerequisites: Take 1 group: Take CCT 231 CCT 241, minimum grade of C; Take CCT 220 CCT 241, minimum grade of C