NORTHWESTERN CONNECTICUT COMMUNITY COLLEGE

COURSE SYLLABUS

Course Title: Computer Forensics and Investigations **Course #:** CST* 156 / CJS * 156

Course Description: 3 Credits An introduction to the procedure and technical aspects of securing digital and computer evidence in relation to law enforcement. Topics include the forensics labs and their setup, Fourth Amendment, incident handling, first responder requirements, investigative reports, technical considerations in collecting evidence, and proper procedure to insure admissibility in court.

Pre-requisite/Co-requisite: ENG* 096

Goals: Students are expected to

- Develop skills in procedure and protocol during evidence collection
- Develop skills in proper navigation of various operating systems and application software
- Develop an understanding of the function and operation of digital storage devices
- Develop an understanding of the Fourth Amendment as it applies to crime scenes
- Develop communication skills to produce documentation in evidence collection.
- Develop an understanding of the common digital forensic tools currently available

Outcomes: Upon successful completion of this course students will be able to:

- Explain the key steps in forensic investigations
- Describe the need for forensic investigators
- Describe the enterprise theory of investigation (ETI)
- Describe legal issues involved in computer forensics
- Describe how to report the results of forensic investigations
- Explain how to evaluate physical security needs
- Explain evidence lockers and how to secure them
- Explain how to Create a forensic work area
- Explain how to configure a computer forensic lab
- Explain and evaluate equipment needs
- Explain basic forensic workstation requirements
- Explain the tools and software forensic investigators use
- Explain data destruction industry standards
- Explain how to Investigate computer crime
- Describe how to Develop policies and procedures
- Explain how to Investigate a company policy violation
- Describe the methodology of investigation
- Explain how to Evaluate a case (perform case assessment)
- Explain how to Develop and follow an investigation plan
- Explain how to Obtain a search warrant
- Explain how to Collect evidence
- Explain how to Implement an investigation
- Explain how to Image an evidence disk
- Examine digital evidence
- Explain how to close a case
- Explain how to evaluate a case
- Describe electronic evidence

- Describe the role of the first responder
- Describe types of electronic devices and collect them as potential evidence
- Explain the key steps in Building a first responder toolkit
- Describe evidence-collecting tools and equipment
- Describe first responder procedures
- Explain how to Secure and evaluate electronic crime scenes
- Explain how to Conduct preliminary interviews
- Explain how to Document electronic crime scenes
- Explain how to Collect and preserve electronic evidence
- Explain how to Package electronic evidence
- Explain the key steps in Transporting electronic evidence
- Explain the key steps in reports about crime scenes
- Identify some common mistakes of first responders
- Identify incidents
- Identify security incidents
- Describe Report incidents
- Explain CSIRTs
- Explain who works in a CSIRT
- Explain the types of incidents and levels of support
- Explain how a CSIRT handles a case
- Describe CERTs all over the world
- Explain the need for an investigative report
- Explain report specifications
- Explain report classification
- Describe the layout of an investigative report
- Explain the guidelines for writing a report
- Describe supporting material
- Explain the importance of consistency
- Explain the salient features of a good report
- Explain the investigative report format
- Describe the elements of a sample forensic report
- Explain the best practices for investigators