

## **CJE 4668 - Computer Crime**

### **Course Description:**

Synthesizes knowledge of crime elements, legal issues, investigative techniques, and computer skills used in the prevention and investigation of computer generated crime. **Pre-req: CGS 1060**

### **Course Competencies:**

Competency 1: The student will utilize computers in profiling by:

- a. reviewing computing fundamentals and computer related crimes
- b. identifying networking technologies specific to computer crime
- c. identifying computer crimes in the State of Florida, investigative techniques and forensic examination
- d. exploring administrative computing in the police environment

Competency 2: The student will analyze the techniques of forensic interviewing by:

- a. describing the sensitive nature of interviewing victims of computer crime
- b. assessing interview information
- c. defining techniques for gathering information
- d. defining the probative value of evidence

Competency 3: The student will analyze information on the Internet by:

- a. describing and discussing how the Internet can augment the traditional investigative methodology
- b. exploring the history of the Internet and emergence of cyber-crime
- c. exploring various Internet crimes
- d. acquiring tools and techniques to make searches more efficient

Competency 4: The student will examine the use of computers in commercial crimes by:

- a. identifying various computer crimes
- b. examining law related to use of computers in the commission of commercial crimes
- c. utilizing appropriate terminology
- d. describing corporate and governmental protection against various computer crimes

Competency 5: The student will examine the basics of encryption by:

- a. comparing and contrasting various encryption terms
- b. recognizing cryptographic algorithms
- c. defining encryption protocols
- d. defining cryptographic techniques and key infrastructure

Competency 6: The student will explore various network exploits and vulnerabilities by:

- a. identifying common vulnerabilities
- b. defining the tools that are used to exploit vulnerabilities
- c. analyzing theoretical and practical issues in malicious programs and scripts
- d. analyzing the nature of computer worms and viruses

Competency 7: The student will analyze computer forensics of the crime scene by:

- a. examining investigations by first responders
- b. examining digital evidence
- c. assessing and documenting digital evidence
- d. reviewing case studies

Competency 8: The student will examine the process of securing a computer network by:

- a. discussing firewall operation
- b. identifying interception and tracking measures used in Internet communications
- c. recognizing hacker exploits and tools
- d. defining the nature of proxy servers
- e. exploring current trends in emerging technologies

Competency 9: The student will analyze forensic behavioral science by:

- a. identifying violent sexual Internet offenders
- b. recognizing the profiles characteristics of computer criminals
- c. assessing investigative difficulties
- d. comparing the science based methods used by police