

## **CSC 548 – DIGITAL FORENSICS**

**CREDIT HOURS:** 3

**PREREQUISITES:** CSC 302 or 331, 455 or 447; or Instructor Permission. CSC 562 recommended.

**GRADE REMINDER:** Must have a grade of C or better in each prerequisite course

### **CATALOG DESCRIPTION**

Study of computer and cyber forensics. Learn and demonstrate understanding of different aspects of computer and cyber-crime and ways in which to uncover, protect, exploit, and document digital evidence. Students will be exposed to different types of tools (both software and hardware), techniques and procedures, and be able to use them to study and practice forensic investigations.

### **PURPOSE OF COURSE**

To acquire the hands-on skills necessary for computer forensics through the use of case studies, hands-on exercises, and a final project. To study the perspectives of computer and related legal processes for evidence discovery, collection, and protection. To discuss relevant computer crimes from state and federal law, methods of interaction with law enforcement and prosecutors, admissibility of expert witness testimony and the use of forensic reports in civil, regulatory and internal investigations

### **EDUCATIONAL OBJECTIVES**

Upon successful completion of the course, students should be able to:

1. Identify the needs for forensic analysis in key critical infrastructure in various segments of our society.
2. Understand the complexity of the networks that make security and forensics a necessity.
3. Distinguish the need for cyber forensics in the use of discovering, protecting, and documenting digital evidence.
4. Demonstrate how to select and utilize appropriate software forensics tools used in forensic analysis.
5. Demonstrate the selection and use of hardware forensics equipment to protect and analyze forensic evidence.

### **COURSE CALENDAR**

This course meets for a minimum of 37.5 lecture contact hours during the semester, including the final exam. Students have significant assignments based on readings from the primary literature, participate in classroom discussions regarding current research topics, complete periodic homework and laboratory/programming assignments, and periodic exams in addition to the final exam. Students are expected to prepare for any class assignments or quizzes over the material covered in class or in the reading material. Successful completion of these activities requires at a minimum six additional hours of outside of classroom work each week.

### **CONTENT**

### **Hours**

Understanding Digital Forensics.....3

The profession and need for forensics  
History of forensics

Tools .....	9
Current software	
Required hardware	
Performing Investigations .....	9
Data Acquisition	
Crime scene processing	
Processing Windows systems	
Processing LINUX and Macintosh file systems	
Virtual machine forensics	
Detailed Forensics Applications .....	9
Email and Social Media	
Mobile devices	
Cloud forensics	
Results .....	9
Report writing	
Expert testimony	
Ethics for the expert witness	
Exams (plus final) .....	6
	TOTAL 45

## REFERENCES

Phillips, Nelson, Enfinger and Steuart, Guide to Computer Forensics and Investigators, 5<sup>th</sup> Ed. Course Technology 2015

Bunting, EnCase Computer Forensics -- The Official EnCE: EnCase Certified Examiner Study Guide 3rd Edition Sybex, 2012

Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition 3rd Edition Academic Press, 2011