ITMS 483 SYLLABUS

ITMS 483 Digital Evidence

Hours: 3 credit hours / 45 contact hours

Instructor: Shawn Davis

Textbook, title, author, and year: *E-discovery: An Introduction to Digital Evidence*, Phillips, Amelia; Godfrey, Ronald; Steuart, Christopher; Brown, Christine, 2014

Specific course information

a. **Catalog description:** In this course, students learn the fundamental principles and concepts in the conduct of investigations in the digital realm. Students will learn the process and methods of obtaining, preserving and presenting digital information for use as evidence in civil, criminal, or administrative cases. Topics include legal concepts and terminology, ethics, computer crime, investigative procedures, chain of custody, digital evidence controls, processing crime and incident scenes, data acquisition, email investigations, applicable case law, and appearance as an expert witness in a judicial or administrative proceeding.
b. **Prerequisites:** ITMS 438
c. **Required for Applied Cybersecurity and Information Technology.**

Specific goals for the course

a. **Course Outcomes:** Each successful student will demonstrate foundation knowledge and application of digital evidence and e discovery concepts as they apply to the investigation of computer crimes and cyber security incidents in a large organizational environment. Students will describe and identify policy frameworks, legal and moral implications, and best practices in the collection, processing and presentation of digital evidence. Students will be able to conduct digital investigations in full compliance with applicable law, policy, and regulations, and present the investigative results as an expert witness.
b. **Course student outcomes:**
    - Acquire, process, preserve, evaluate, and present digital evidence in a forensically and legally sound manner.
    - Recall and describe law, theories, techniques, and practices that apply to digital forensic investigations.
    - Identify and describe types of computer and Internet crimes.
    - Preserve and process a crime scene involving digital evidence.
    - Explain the legal procedures and standards in the collection and analysis of digital evidence.
    - Prepare a report of a digital investigation for appropriate stakeholders and defend your findings.
    - Present an analysis of digital evidence in a legal or administrative proceeding as an expert witness.

Topics to be covered

a. Introduction to Legal Concepts and Terminology
b. Introduction to Digital Evidence
c. History and Ethics of E-discovery and Digital Evidence
d. Planning and Tools
e. Experts in Digital Evidence and E Discovery
f. Digital Evidence Case Flow
g. Case Study: From Beginning to Trial
h. Information Governance and Litigation Preparedness
i. Presenting Digital Evidence in Court
j. Digital Evidence Case Law
k. The Future of Digital Evidence