ITE345 Digital Forensics Tools and Techniques **4 cr.**

Catalog Description:
This course teaches the basics of responding to computer incidents. It focuses on gathering important evidence for digital investigations. Throughout the course, students learn key concepts of digital forensics, like what cybercrime is, types of evidence, and best practices. Students also learn practical skills, such as choosing the right tools and following a step-by-step process for investigations. The course covers forensic analysis and how to respond to cyber incidents confidently. It's designed for beginners, giving hands-on experience with industry tools to provide an edge in the field. Four lecture hours per week.

Prerequisites: ITE315 or CSC435.

Course Narrative:

Digital forensics, formerly known as computer forensics, has represented a professional discipline for many years. Nevertheless, most of the established experts in this field are self-taught. The exponential growth of the Internet and the widespread adoption of computers have significantly amplified the demand for digital investigation skills. Computers have become both the tools for committing crimes and the repositories of crucial evidence, encompassing a wide array of activities from corporate policy violations and embezzlement to email harassment, murder, proprietary information leaks, and even acts of terrorism.

Today, law enforcement, network administrators, attorneys, and private investigators increasingly rely on the expertise of professional digital forensics practitioners to investigate both criminal and civil cases.

This course is not designed to provide all-encompassing training in digital forensics. However, it serves as a foundation for those who are new to this field, offering an introductory understanding of digital forensics. While many existing digital forensics resources are geared toward experts, this course is tailored for beginners who possess a background in computer and networking fundamentals. The emerging generation of digital forensics professionals requires more initial training due to the rapid evolution of operating systems, computer and mobile device hardware, and forensics software tools.

This course encompasses current and previous operating systems as well as a wide range of hardware, spanning from basic workstations to high-end network servers and a variety of mobile devices. While this course primarily emphasizes a select set of forensics software tools, it also evaluates and discusses other tools currently available in the field.

Course Goals:

The purpose of this course is to develop students' knowledge and understanding of digital forensics tools and techniques. Specific goals are:

- G1: Gain a deep understanding of the fundamental principles of incident response and the intricacies of evidence collection in digital forensic investigations.
- G2: Master core concepts in digital forensics, including the definition of cybercrime, types of evidence, and industry best practices.
- G3: Acquire the skills and knowledge required to select appropriate forensic tools and follow a structured process for conducting comprehensive digital forensic investigations.
- G4: Develop expertise in forensic analysis, including a thorough understanding of each essential step in the investigative process.
- G5: Evaluate the proficiency in crafting and executing effective cyber incident response strategies, enabling confident management of cybersecurity incidents in various contexts.

Course Outcomes (Objectives):

Upon successful completion of the course, a student will be able to:

- O1: Implement hands-on experiments by requiring each student to successfully use a set of approved forensic tools in simulated scenarios.
- O2: Operate digital forensic investigations, conducting detailed reports and analysis where applicable.
- O3: Integrate hands-on experience by selecting and applying forensic tools, conducting digital forensic investigations, and performing forensic analysis.

O4: Evaluate the making and execution of effective cyber incident responses, empowering them to handle security incidents.
O5: Develop the expertise needed to excel in the field of digital forensics and incident response from a skilled professional's perspective.

Topics:

- Understanding the Digital Forensics Profession and Investigations
    - An Overview of Digital Forensics
    - Preparing for Digital Investigations
    - Maintaining Professional Conduct
    - Preparing a Digital Forensics Investigation
    - Procedures for Private-Sector High-Tech Investigations
    - Understanding Data Recovery Workstations and Software
    - Conducting an Investigation
- The Investigator's Office and Laboratory
    - Understanding Forensics Lab Accreditation Requirements
    - Determining the Physical Requirements for a Digital Forensics Lab
    - Selecting a Basic Forensic Workstation
    - Building a Business Case for Developing a Forensics Lab
- Data Acquisition
    - Understanding Storage Formats for Digital Evidence
    - Determining the Best Acquisition Method
    - Contingency Planning for Image Acquisitions
    - Using Acquisition Tools
    - Validating Data Acquisitions
    - Performing RAID Data Acquisitions
    - Using Remote Network Acquisition Tools
    - Using Other Forensics Acquisition Tools
- Processing Crime and Incident Scenes
    - Identifying Digital Evidence
    - Collecting Evidence in Private-Sector Incident Scenes
    - Processing Law Enforcement Crime Scenes
    - Preparing for a Search
    - Securing a Digital Incident or Crime Scene
    - Seizing Digital Evidence at the Scene
    - Storing Digital Evidence
    - Obtaining a Digital Hash
- Working with Windows and CLI Systems
    - Understanding File Systems
    - Exploring Microsoft File Structures
    - Examining NTFS Disks
    - Understanding Whole Disk Encryption
    - Understanding the Windows Registry
    - Understanding Microsoft Startup Tasks
    - Understanding Virtual Machines

- Current Digital Forensics Tools
    - Evaluating Digital Forensics Tool Needs
    - Digital Forensics Software Tools
    - Digital Forensics Hardware Tools
    - Validating and Testing Forensics Software
- Recovering Graphics Files
    - Recognizing a Graphics File
    - Understanding Data Compression
    - Identifying Unknown File Formats
    - Understanding Copyright Issues with Graphics

- Digital Forensics Analysis and Validation
    - Determining What Data to Collect and Analyze
    - Validating Forensic Data
    - Addressing Data-Hiding Techniques
- E-Mail and Social Media Investigations
    - Exploring the Role of E-mail in Investigations
    - Exploring the Roles of the Client and Server in E-mail
    - Investigating E-mail Crimes and Violations
    - Understanding E-mail Servers
    - Using Specialized E-mail Forensics Tools
    - Applying Digital Forensics Methods to Social Media Communications
- Mobile Device Forensics and the Internet of Anything
    - Understanding Mobile Device Forensics
    - Understanding Acquisition Procedures for Mobile Devices
    - Understanding Forensics in the Internet of Anything
- Cloud Forensics
    - An Overview of Cloud Computing
    - Legal Challenges in Cloud Forensics
    - Technical Challenges in Cloud Forensics
    - Acquisitions in the Cloud
    - Conducting a Cloud Investigation
    - Tools for Cloud Forensics

Assignments and Examination:

The course consists of lectures, homework assignments, quizzes, hands-on lab assignments, and two exams – a midterm and a final. The course grade will be determined using the following approximate weights: final exam: 20%, midterm exam: 20%, written homework 20%, hands-on lab assignments 20%, and quizzes: 20%.

Course Objective / Assessment Mechanism matrix

	Homework	Quizzes	Hands-on Lab	Midterm	Final
CO01	✓	✓	✓	✓	✓
CO02	✓		✓		
CO03	✓	✓	✓	✓	✓
CO04	✓		✓	✓	✓
CO05	✓	✓	✓	✓	✓

Bibliography:

1. Guide to Computer Forensics and Investigations 7th Edition, 2024, Bill Nelson, Cengage Learning, 9780357672884.
2. Digital Forensics, Investigation, and Response, 4th Edition, 2021, Chuck Easttom Jones & Bartlett Learning 9781284226065, 1284226069
3. Computer Forensics 2nd Edition, 2014, Marie-Helen Maras, Jones & Bartlett Learning, 9781449692223, 1449692222
4. Cybercrime and Digital Forensics 3rd Edition, 2022, Thomas J. Holt; Adam M. Bossler; Kathryn C. Seigfried-Spellar, Routledge, 9780367360061, 0367360063
5. Network Forensics 1st Edition, 2012, Sherri Davidoff; Jonathan Ham, Pearson PTG, 9780132564717, 0132564718
6. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics 2nd Edition, 2014, Sammons, John, Syngress Publishing, 9780128016350, 0128016353
7. Forensic Science 5th Edition, 2019, Suzanne Bell, CRC Press, 9781138048126, 1138048127
8. System Forensics, Investigation, and Response 3rd Edition, 2017 Chuck Easttom, Jones & Bartlett Learning, 9781284121841, 1284121844
9. A Practical Guide to Digital Forensics Investigations 2nd Edition, 2021, Darren R. Hayes, Pearson IT Certification PTG, Reflowable, 9780789759917, 0789759918
10. Learn Computer Forensics 1st Edition A beginner's guide to searching, analyzing, and securing digital evidence, 2020, William Oettinger, Packt Publishing, 9781838648176, 1838648178
11. Digital Forensics and Cyber Investigation 1st Edition, 2023, Kyung-Shick Choi, Cognella Academic Publishing, 9781516536368, 1516536363