Syllabus for CYB-5600

CYBER FORENSICS AND INVESTIGATION

COURSE DESCRIPTION

This course covers the fundamental concepts, tools, and techniques of digital forensics and cyber investigation. Topics include the identification, preservation, collection, examination, analysis, and presentation of digital evidence for administrative, civil, and criminal investigations. Applications of appropriate tools and technologies used for securing, handling, and preserving digital evidence are explored. The legal and ethical aspects associated with digital forensics and cyber investigation are examined in depth.

COURSE TOPICS

- Fundamentals of digital forensics
- Digital forensics and cyber acquisition and investigation techniques
- Acquisition and analysis of forensic information
- Legal issues in digital forensics

COURSE OBJECTIVES

After completing this course, students should be able to:

CO 1 Explain key factors in digital forensics investigations.

CO 2 Critique various operating systems and file systems.

CO 3 Collect and appraise digital evidence using various tools.

CO 4 Assess collected data for potential value.

CO 5 Critique technical aspects of digital evidence acquisition.

CO 6 Evaluate and specify appropriate software, hardware, and tools to equip a forensics lab.

CO 7 Construct investigative reports.

CO 8 Explain techniques used to perform as an expert witness.

CO 9 Appraise the legal and ethical implications of digital forensic investigations.

COURSE MATERIALS

You will need the following materials to complete your coursework. Some course materials may be free, open source, or available from other providers. You can access free or open-source materials by clicking the links provided below or in the module details documents. To purchase course materials, please visit the University's textbook supplier.

Required Textbook

- Johansen, G. (2020). *Digital forensics and incident response: Incident response techniques and procedures to respond to modern cyber threats* (2nd ed.). Birmingham, UK: Packt Publishing. **ISBN 13: 978-1838649005**

Required Labs

- InfoSec Learning Labs Access Code

COURSE STRUCTURE

Cyber Forensics and Investigation is a three-credit online course consisting of **eight** modules. Modules include an overview, topics, learning objectives, study materials, and activities. Module titles are listed below.

- **Module 1: Digital Forensic Fundamentals**
  Course objectives covered in this module: CO 1, CO 8, CO 9
- **Module 2: Forensic Evidence Collection: Network**
  Course objectives covered in this module: CO 1, CO 2, CO 3, CO 4, CO 5
- **Module 3: Forensic Evidence Collection: Host**
  Course objectives covered in this module: CO 1, CO 2, CO 3, CO 4, CO 5, CO 6
- **Module 4: Forensic Evidence Collection: Imaging**
  Course objectives covered in this module: CO 1, CO 2, CO 3, CO 4, CO 6
- **Module 5: Forensic Analysis: Network**
  Course objectives covered in this module: CO 1, CO 2, CO 3, CO 4, CO 5, CO 6
- **Module 6: Forensic Analysis: System Memory**

Course objectives covered in this module: CO 2, CO 3, CO 4, CO 5, CO 6, CO 7, CO 8

- **Module 7: Forensic Analysis: System Storage**
  Course objectives covered in this module: CO 1, CO 2, CO 3, CO 4, CO 5, CO 6, CO 7, CO 8

- **Module 8: Incident Reporting**
  Course objectives covered in this module: CO 1, CO 7, CO 8, CO 9

ASSESSMENT METHODS

For your formal work in the course, you are required to participate in online discussion forums, complete written assignments, and complete a final project. See below for details.

Consult the Course Calendar for due dates.

Promoting Originality

One or more of your course activities may utilize a tool designed to promote original work and evaluate your submissions for plagiarism. More information about this tool is available in SafeAssign.

Discussion Forums

You are required to complete **six** discussion forums. The discussion forums are on a variety of topics associated with the course modules.

Communication with your mentor and among fellow students is a critical component of online learning. Participation in online class discussions involves two distinct activities: an initial response to a discussion question and at least two subsequent comments on classmates' responses.

All of these responses must be substantial. Meaningful participation is relevant to the content, adds value, and advances the discussion. Comments such as "I agree" and "ditto" are not considered value-adding participation. Therefore, when you agree or disagree with a classmate or your mentor, state and support your position.

You will be evaluated on the quality and quantity of your participation, including your use of relevant course information to support your point of view and your awareness of and responses to the postings of your classmates. Remember, these are discussions: responses and comments should be properly proofread and edited, mature, and respectful.

Written Assignments

You are required to complete **two** written assignments. The written assignments are on a variety of topics associated with the course modules.

Infosec Learning Labs

You are required to complete **eight** Infosec Learning Labs. Each lab is either 90 minutes or 120 minutes in duration, regulated by a timer. They are designed to be completed in one sitting to simulate a real experience, so you cannot save your progress to return later. For an optimal experience, use a Chrome web browser with an Internet connection to run the labs.

While working through each lab, keep in mind you will need to answer several questions at the end of each lab, including writing a reflection that describes your overall impressions and experience of completing the lab. You will also need to submit a screenshot toward the end of your lab with a timestamp and your name. **Submit both the screenshot and your lab reflection results** to your mentor using the appropriate "Infosec Lab Results" link in Moodle.

Go to the **Infosec Learning Labs** area of the course website for further details about completing and submitting lab assignments.

Final Project

For the final project, you are required to use the DD image provided in the scenario to perform a forensic analysis on the system. You will use open source tools to compile your analysis into a detailed forensic report by following the procedures laid out in the Guidelines. Go to the **Final Project** area of the course website for further details.

Course Reflection

For this course—and throughout the Master of Science in Cybersecurity (MSCYB) program—you will complete a course reflection which includes collecting digital artifacts, participating in course reflection discussion forums, and writing a course reflection essay. Reference the **Course Reflection** area of the course website for full requirements and instructions.

GRADING AND EVALUATION

Your grade in the course will be determined as follows:

- **Online discussions (6)—**24%
- **Written assignments (2)—**12%
- **Infosec labs (8)—**24%
- **Final project—28**%

- **Course reflection—**12%
    - **Course reflection discussions (2)—**6%
    - **Course reflection essay—**6%

All activities will receive a numerical grade of 0–100. You will receive a score of 0 for any work not submitted. Your final grade in the course will be a letter grade. Letter grade equivalents for numerical grades are as follows:

A	=	93–100	B	=	83–87
A–	=	90–92	C	=	73–82
B+	=	88–89	F	=	Below 73

To receive credit for the course, you must earn a letter grade of C or higher on the weighted average of all assigned course work (e.g., assignments, discussion postings, projects). Graduate students must maintain a B average overall to remain in good academic standing.

STRATEGIES FOR SUCCESS

First Steps to Success

To succeed in this course, take the following first steps:

- Read the entire Syllabus carefully, making sure that all aspects of the course are clear to you and that you have all the materials required for the course.

- Take time to read the entire Online Student Handbook. The Handbook answers many questions about how to proceed through the course and how to get the most from your educational experience at Thomas Edison State University.

- Familiarize yourself with the learning management systems environment—how to navigate it and what the various course areas contain. If you know what to expect as you navigate the course, you can better pace yourself and complete the work on time.

- If you are not familiar with web-based learning, be sure to review the processes for posting responses online and submitting assignments before class begins.

Study Tips

Consider the following study tips for success:

- To stay on track throughout the course, begin each week by consulting the Course Calendar. The Course Calendar provides an overview of the course and indicates due dates for submitting assignments, posting discussions, and scheduling and taking examinations.

- Check Announcements regularly for new course information.

COMMITMENT TO DIVERSITY, EQUITY, AND INCLUSION

Thomas Edison State University recognizes, values, and relies upon the diversity of our community. We strive to provide equitable, inclusive learning experiences that embrace our students' backgrounds, identities, experiences, abilities, and expertise.

ACCESSIBILITY AND ACCOMMODATIONS

Thomas Edison State University recognizes disability as a facet of diversity and seeks to advance access to its educational offerings. Students with disabilities may seek accommodations by contacting the Office of Student Accessibility Services via email at ada@tesu.edu or phone at (609) 984-1141, ext. 3415. Individuals who are deaf or hard of hearing may call the TTY line at (609) 341-3109.

ACADEMIC POLICIES

To ensure success in all your academic endeavors and coursework at Thomas Edison State University, familiarize yourself with all administrative and academic policies including those related to academic integrity, course late submissions, course extensions, and grading policies.

For more, see:

- University-wide policies
- Undergraduate course policies and regulations
- Graduate academic policies
- Nursing student policies
- Academic code of conduct