# COURSE OUTLINE: CYB304 - IT SECURITY FORENSIC

Prepared: IT Studies
Approved: Martha Irwin, Dean, Business and Information Technology

| | |
|---|---|
| **Course Code: Title** | CYB304: IT SECURITY FORENSICS |
| **Program Number: Name** | 2198: CYBERSECURITY<br>5911: CYBERSECURITY |
| **Department:** | PPP triOS |
| **Academic Year:** | 2024-2025 |
| **Course Description:** | In this course, students will learn about computer forensics and methods of investigating security breaches. Students are introduced to digital forensic tools in order to acquire, preserve, and manage digital evidence to support investigations. They will also learn to analyze cyber intrusion, reconstruct vital data, examine organizational policy violations, and resolve disputes. |
| **Total Credits:** | 4 |
| **Hours/Week:** | 4 |
| **Total Hours:** | 56 |
| **Prerequisites:** | There are no pre-requisites for this course. |
| **Corequisites:** | There are no co-requisites for this course. |
| **Vocational Learning Outcomes (VLO's) addressed in this course:**<br>**Please refer to program web page for a complete listing of program outcomes where applicable.** | **2198 - CYBERSECURITY**<br>VLO 7 Plan and conduct disaster recovery, forensic investigations and incident responses to support Business Continuity of an organization<br>VLO 8 Implement and conduct penetration testing to identify and exploit an organization's network system vulnerability<br>VLO 9 Perform various types of cyber analysis to detect actual security incidents and suggest solutions<br>**5911 - CYBERSECURITY**<br>VLO 7 Plan and conduct disaster recovery, forensic investigations and incident responses to support Business Continuity of an organization.<br>VLO 8 Implement and conduct penetration testing to identify and exploit an organization's network system vulnerability.<br>VLO 9 Perform various types of cyber analysis to detect actual security incidents and suggest solutions. |
| **Essential Employability Skills (EES) addressed in this course:** | EES 4 Apply a systematic approach to solve problems.<br>EES 5 Use a variety of thinking skills to anticipate and solve problems.<br>EES 6 Locate, select, organize, and document information using appropriate technology and information systems.<br>EES 7 Analyze, evaluate, and apply relevant information from a variety of sources.<br>EES 10 Manage the use of time and other resources to complete projects. |

**Course Evaluation:**

Passing Grade: 50%, D

A minimum program GPA of 2.0 or higher where program specific standards exist is required for graduation.

**Other Course Evaluation & Assessment Requirements:**

A+ = 90-100%
A = 80-89%
B = 70-79%
C = 60-69%
D = 50-59%
F < 50%

Students are expected to be present to write all tests in class, unless otherwise specified. If a student is unable to write a test due to illness or a legitimate emergency, that student must contact the professor prior to class and provide reasoning. Should the student fail to contact the professor, the student shall receive a grade of zero on the test.

If a student is not present 10 minutes after the test begins, the student will be considered absent and will not be given the privilege of writing the test.
Students exhibiting academic dishonesty during a test will receive an automatic zero. Please refer to the College Academic Dishonesty Policy for further information.

In order to qualify to write a missed test, the student shall have:
a.) attended at least 75% of the classes to-date.
b.) provide the professor an acceptable explanation for his/her absence.
c.) be granted permission by the professor.

NOTE: The missed test that has met the above criteria will be an end-of-semester test.

Labs / assignments are due on the due date indicated by the professor. Notice by the professor will be written on the labs / assignments and verbally announced in advance, during class.

Labs and assignments that are deemed late will have a 10% reduction per academic day to a maximum of 5 academic days at 50% (excluding weekends and holidays). Example: 1 day late - 10% reduction, 2 days late, 20%, up to 50%. After 5 academic days, no late assignments and labs will be accepted. If you are going to miss a lab / assignment deadline due to circumstances beyond your control and seek an extension of time beyond the due date, you must contact your professor in advance of the deadline with a legitimate reason that is acceptable.

It is the responsibility of the student who has missed a class to contact the professor immediately to obtain the lab / assignment. Students are responsible for doing their own work. Labs / assignments that are handed in and are deemed identical or near identical in content may constitute academic dishonesty and result in a zero grade.

Students are expected to be present to write in-classroom quizzes. There are no make-up options for missed in-class quizzes.

Students have the right to learn in an environment that is distraction-free, therefore, everyone is expected to arrive on-time in class. Should lectures become distracted due to students walking in late, the professor may deny entry until the 1st break period, which can be up to 50 minutes after class starts or until that component of the lecture is complete.

The total overall average of test scores combined must be 50% or higher in order to qualify to

| | |
|---|---|
| | pass this course. In addition, combined tests, Labs / Assignments total grade must be 50% or higher. |
| **Books and Required Resources:** | Guide to Computer Forensics and Investigations by Bill Nelson, Amelia Phillips, and Chris Steuart<br>Publisher: Cengage Edition: 6th<br>ISBN: 978-1-337-56894-4 |

**Course Outcomes and Learning Objectives:**

| **Course Outcome 1** | **Learning Objectives for Course Outcome 1** |
|---|---|
| 1. Examine methods of investigating security breaches and policy violations to resolve disputes. | 1.1 Outline how to prepare for computer investigations and summarize the difference between public-sector and private-sector investigations.<br>1.2 Explain how to prepare a digital forensics investigation by taking a systematic approach.<br>1.3 Examine procedures for private-sector digital investigations.<br>1.4 Review standard procedures in network forensics and network-monitoring tools.<br>1.5 Outline how to investigate, including critiquing a case. |
| **Course Outcome 2** | **Learning Objectives for Course Outcome 2** |
| 2. Evaluate digital forensic tools commonly used to support investigations. | 2.1 Explain how to evaluate needs for digital forensics tools.<br>2.2 Review available digital forensics software tools.<br>2.3 Outline considerations for digital forensics hardware tools.<br>2.4 Assess the methods for validating and testing forensics tool.<br>2.5 Examine what remote access tools can be used for cloud investigations. |
| **Course Outcome 3** | **Learning Objectives for Course Outcome 3** |
| 3. Set up a digital forensics analysis with cyber intrusion validation. | 3.1 Determine what data to analyze in a digital forensics` investigation.<br>3.2 Examine tools used to validate data.<br>3.3 Outline common data-hiding techniques.<br>3.4 Review standard procedures for conducting forensic analysis of virtual machines.<br>3.5 Evaluate network intrusions and unauthorized access. |
| **Course Outcome 4** | **Learning Objectives for Course Outcome 4** |
| 4. Acquire, preserve, and manage digital evidence. | 4.1 Identify digital evidence storage formats.<br>4.2 Formulate ways to determine the best acquisition method.<br>4.3 Review contingency planning for data acquisitions.<br>4.4 Explain how to use acquisition tools.<br>4.5 Examine how to validate data acquisitions.<br>4.6 Explore RAID acquisition methods.<br>4.7 Explain how to use remote network acquisition tools.<br>4.8 Outline other forensics tools available for data acquisition.<br>4.9 Explore the process of a live acquisition. |
| **Course Outcome 5** | **Learning Objectives for Course Outcome 5** |
| 5. Reconstruct data in various contexts. | 5.1 Identify the different forms of files and data that can be recovered. |

| | |
|---|---|
| | 5.2 Reconstruct data in Windows and CLI Systems.<br>5.3 Explain how to locate and recover graphics files.<br>5.4 Reconstruct .PST files and messages.<br>5.5 Trace, recover, and analyze e-mail messages by using forensics tools. |
| **Course Outcome 6** | **Learning Objectives for Course Outcome 6** |
| 6. Examine organizational policy violations. | 6.1 Outline common organizational policy violations and best practices for investigating them.<br>6.2 Compare organizational policy violation forensics cases.<br>6.3 Explain what data to collect and analyze for company policy violations. |

**Evaluation Process and Grading System:**

| Evaluation Type | Evaluation Weight |
|---|---|
| Assignments | 40% |
| Final Exam | 30% |
| Professional Performance | 10% |
| Quizzes | 20% |

**Date:** June 16, 2024

**Addendum:** Please refer to the course outline addendum on the Learning Management System for further information.