COURSE OUTLINE: CYB304 - IT SECURITY FORENSIC

Prepared: IT Studies
Approved: Corey Meunier, Chair, Technology and Skilled Trades

Course Code: Title	CYB304: IT SECURITY FORENSICS
Program Number: Name	5911: CYBERSECURITY
Department:	PPP triOS
Academic Year:	2021-2022
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:	60
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: **Please refer to program web page for a complete listing of program outcomes where applicable.**	**5911 - CYBERSECURITY** VLO 7 Plan and conduct disaster recovery, forensic investigations and incident responses to support Business Continuity of an organization. VLO 8 Implement and conduct penetration testing to identify and exploit an organization's network system vulnerability. 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. EES 5 Use a variety of thinking skills to anticipate and solve problems. EES 6 Locate, select, organize, and document information using appropriate technology and information systems. EES 7 Analyze, evaluate, and apply relevant information from a variety of sources. 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:	Definition Grade Point Equivalent A+ 90 - 100% 4.00 A 80 - 89% 4.00 B 70 - 79% 3.00 C 60 - 69% 2.00

D 50 - 59% 1.00
F(Fail) below 50% 0.00

Books and Required Resources:

Guide to Computer Forensics and Investigations by Bill Nelson, Amelia Phillips, and Chris Steuart
Publisher: Cengage
ISBN: 978-1-337-56894-4

Course Outcomes and Learning Objectives:

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

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

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Final Exam	60%
Professional Performance	10%
Quizzes, Tests & Projects	30%

Date: June 30, 2022

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