Course Syllabus Part I
CYBR 420, Cyber Investigations and Forensics

3 Credit Hours

Course Description
This course examines basic methods of investigation, information acquisition, and management of Internet and computer forensic cases. Topics include record-searching, note taking and report writing, and using scientific methodology in Cyber Investigations. Coverage also includes basic tools and techniques for forensic analysis of computers, networks, systems, and mobile devices.

Course Prerequisites
None

Course Objectives

Students who successfully complete this course should be able to:

1. Describe basic concepts associated with different types of computer forensics investigations.
2. Prepare a forensics investigative plan.
3. Build a toolkit for computer forensics investigations.
4. Explain the process for collecting evidence and investigating common artifacts during a digital forensics exam.
5. Conduct a basic computer forensics investigation.

Grading Scale
Click here to enter the grading scale. The grading scale should be consistent within a program. This is needed for data analytics.

Example 1:

93 – 100% = A	87 – 89% = B+	77 – 79% = C+	67 – 69% = D+
90 – 92% = A-	83 – 86% = B	73 – 76% = C	63 – 66% = D
	80 – 82% = B-	70 – 72% = C-	60 – 62% = D-
			0 – 59% = F

Topic Outline

I. Introduction to cyber Investigations and Digital Forensics
   a. Forensic science explained
   b. Role of the forensic examiner
   c. Laws associated with investigations
   d. Preparing for a cyber investigation
   e. Review of key technical concepts

II. Cyber Investigation Tools
   a. Windows operating system tools
   b. Linux operating systems tools
   c. Communications (email, IM, etc.) tools
   d. Website tools
   e. Mobile and cloud computing

III. Cyber Investigation Process
   a. Creating an investigative plan
   b. Collecting, preserving, and validating evidence
   c. Following chain of custody
   d. Analyzing evidence
   e. Evaluating log files
   f. Documentation

IV. Conducting a Technical Investigation
   a. Scene identification
   b. Evidence collection
   c. Forensic tool determination
   d. Use of appropriate forensics tools and methods
   e. Analysis of evidence
   f. Documentation and report creation