1. **COURSE TITLE: Advanced Computer Forensics and Cyber Crime**
2. **CATALOG COURSE NUMBER: 2215 CATALOG PREFIX: CYBR**

**SECTION: \_\_\_\_\_\_\_\_\_\_\_**

1. **PREREQUISITE(S): CYBR 1115 – Introduction to Computer Forensics and Cyber Crime**
2. **COURSE TIME/LOCATION: (*Course Syllabus – Individual Instructor Specific*)**
3. **CREDIT HOURS: 4.0 LECTURE HOURS: 4**

**LABORATORY HOURS: OBSERVATION HOURS:**

1. **FACULTY CONTACT INFORMATION:** ***(Course Syllabus – Individual Instructor Specific)***
2. **COURSE DESCRIPTION:**  This course is an introduction into the concepts, terminologies, and terms to skillfully complete a computer investigation from acquiring digital evidence to reporting findings.
3. **LEARNING OBJECTIVES:**
4. Chapter 1 – Students will demonstrate a systematic approach to preparing for a digital investigation.
5. Chapter 2 – Students will explain how to set up a digital forensics lab.
6. Chapter 3 – Students will prepare to use GUI acquisition tools and analyze remote acquisitions.
7. Chapter 4 – Students will describe the definition of search warrants and how they assist in a typical digital forensics case.
8. Chapter 5 – Students will be able to identify which files are altered during computer startup and how files systems deal with deleted and slack space.
9. Chapter 5 – Students will show how to decrypt a drive and explain the purpose of virtual machines.
10. Chapter 6 – Students will report on current digital forensics software and hardware tools.
11. Chapter 7 – Students will illustrate an understanding of Linus Oss and Macintosh file systems.
12. Chapter 8 – Students will explain how to recover graphics files.
13. Chapter 9 – Students will collect data and analyze by writing an investigation plan.
14. Chapter 10 – Students will review network logs for evidence and use network monitoring tools to detect unauthorized use.
15. Chapter 11 – Students will examine email crimes and violations.
16. Chapter 12 – Students will identify storage and acquisition procedures on mobile devices.
17. Chapter 13 – Students will summarize the legal and technical challenges in conducting cloud forensics.
18. Chapter 14 – Students will generate report finds with forensic software tools.
19. Chapter 15 – Students will prepare forensics evidence for a testimony.
20. Chapter 16 – Students will examine codes of ethics for various companies.
21. **ADOPTED TEXT(S):**

*Guide to Computer Forensics and Investigations, 6th Edition*

Cengage Learning

Nelson/Phillips/Steuart

Copyright 2019

ISBN: 978-1-337-56894-4

**9a: SUPPLEMENTAL TEXTS**

1. **OTHER REQUIRED MATERIALS:**

Web-Based Labs Printed Access Card for access to the web-based labs for students.

1. **GRADING SCALE:**

Grading will follow the policy in the catalog. The scale is as follows:

A: 90 – 100

 B: 80 – 89

 C: 70 – 79

 D: 60 – 69

 F: 0 – 59

1. **GRADING PROCEDURES OR ASSESSMENTS: (*Course Syllabus – Individual Instructor Specific)***

|  |  |  |
| --- | --- | --- |
| *Category* | ***EXAMPLE ONLY****Total Points* | *% of Grade* |
| Chapter Assignments (10x30) | 300 | 30% |
| Quizzes (10x20) | 200 | 20% |
| Unit Exams (3x100) | 300 | 30% |
| Assignments (5x10) | 50 | 5% |
| Annual Report Project (100) | 100 | 10% |
| Attendance | 50 | 5% |
| Total | 1000 | 100% |

1. **COURSE METHODOLOGY OR COURSE FORMAT:**

May include but not limited to: Lectures, independent and group projects, in-class and home assignments, tests, quizzes and lab exercises.

1. **COURSE OUTLINE: *(Course Syllabus – Individual Instructor Specific)***

Week 1: (Chapter 1) Understanding the digital forensics profession and investigation.

Week 2: (Chapter 2) The investigator’s office and laboratory.

Week 3: (Chapter 3) Data acquisition.

Week 4: (Chapter 4) Processing crime and incident scenes.

Week 5: (Chapter 5) Working with Windows and CLI systems.

Week 6: (Chapter 6) Current digital forensics tools

Week 7: (Chapter 7) Linus and Macintosh file systems and Midterm Test.

Week 8: (Chapter 8) Recovering graphics files

Week 9: (Chapter 9) Digital forensics analysis and validation.

Week 10: (Chapter 10) Virtual machine forensics, live acquisitions, and network forensics.

Week 11: (Chapter 11) Email and social media investigations.

Week 12: (Chapter 12) Mobile device forensics and the Internet of anything.

Week 13: (Chapter 13) Cloud forensics.

Week 14: (Chapter 14) Report writing for high-tech investigations.

Week 15: (Chapter 15) Expert testimony in digital investigations and (Chapter 16) Ethics for the expert witness.

Week 16: Final Test

1. **SPECIFIC MANAGEMENT REQUIREMENTS:**

None

1. **OTHER INFORMATION:**

**FERPA:** Students need to understand that your work may be seen by others. Others may see your work when being distributed, during group project work, or if it is chosen for demonstration purposes. Students also need to know that there is a strong possibility that your work may be submitted to other entities for the purpose of plagiarism checks.

**DISABILITIES:** Students with disabilities may contact the Disabilities Service Office, Central Campus, at 800-628-7722 or 937-393-3431.