Masters of Science in Cybersecurity

Syllabus for CYB 725 Computer Forensics and Investigations

NOTE: This syllabus document contains the basic information of this course. The most current syllabus is available in the full course.

Course Description

This course provides instruction on the investigative and forensics processes of digital evidence with a focus on identifying indicators of compromise, the use of common forensics tools, and the preservation of forensics artifacts. Topics include forensics iconology, the analysis of disk, memory, chip-off, mobile device, and OS artifacts.

Prerequisite(s)

- CYB 700: Fundamentals of Cybersecurity
- CYB 703: Network Security

Program Outcomes

This course addresses the following competencies and program outcomes of the Masters of Science in Cybersecurity:

- Program Outcome 1: Interpret and analyze operating system and machine level structures
- Program Outcome 14: Develop and implement an incident response strategy
- Program Outcome 15: Identify and assess attacks through forensics
- Program Outcome 16: Interpret legal implications of security incidents and conduct investigations using industry best practices

Course Outcomes

Upon completing this course, you will be able to do the following:

- Recognize the legal significance of digital forensic tools and techniques
- Acquire, validate, and preserve digital evidence.
- Verify the authenticity of digital evidence
- Examine digital evidence and reconstruct events in an investigation with evidence from various sources.
- Author competent forensic reports and present forensic conclusions to peers and laypeople, supporting conclusions with forensic evidence.
- Explain the basic concepts behind advanced physical recovery techniques.

Course Requirements/Components

Individual Investigations

There are four individual investigations. These assignments require examining simulated evidence using the techniques in the course. Successful completion requires submitting a forensic report of your examination and providing adequate evidence to answer a series of accompanying questions.

Forensic Challenge

There is one major semester project. This project is a large investigative scenario that simulates a real case. Successfully completing the assignment requires examining the evidence and producing a forensic report for each evidence source examined and a final threshold assessment as if you were sending the report to investigators on this case. You will work on this project with other group members but submitting work individually.

Quizzes

There are four quizzes in the course. These quizzes cover foundational concepts covered in the course. They are not cumulative. If you engage with the learning resources and the in-class demo materials, you should find the quizzes to be very manageable.

Investigation Discussions

For your first Investigation 1, I provide you with a series of questions for you to answer to help guide you through the investigation. In the real world, examiners almost never have so much guidance. You will eventually have to work out for yourself what information is relevant to investigations. Basically, you'll need to start thinking and making decisions like a professional in the field. We will use these discussions as the place where the development of that thought process occurs.

Course Outline

Module 01: Introduction to Forensic Evidence

- Types of evidence
- Qualities of evidence

Module 02: Acquisition of Evidence

- Preservation of evidence
- Validating and authenticating evidence

Module 03: Windows Forensic Artifacts

- Examining files/metadata
- Events and other logs
- Browser artifacts
- SRUM data
- Windows registry artifacts

Module 04: Disk Evidence

- Examining FAT / NTFS file systems
- Reading MACb time
- Forensic data recovery

Module 05: Forensic Iconography

- Observation
- Image format analysis
- Basic image enhancement
- Advanced analysis

Module 06: Volatile Evidence

- Evidence volatility
- Examining volatile evidence

Module 07: Mobile Device Forensics

- Mobile device seizure and forensics

Module 08: Advanced Techniques in Forensics

- Chip-off
- JTAG

Grading

The following grading scale will be used to evaluate all course requirements and to determine your final grade:

Grade	Percentage Range
A	90% or greater
A-	87% - < 90%
B+	83% - < 87%
B	80% - < 83%
B-	77% - < 80%
C+	73% - < 77%
C	70% - < 73%
C-	65% - < 70%
F	0 - < 65%

Assignments	**Percentage**
4 Individual Investigations – 15% each	60%
Discussion Participation (6 discussions)	10%
4 Quizzes	10%
1 Forensic Challenge	20%
Total	**100%**