Cyber Criminalistics Syllabus - DRAFT 1

Prerequisites

None. Labs are at the introductory level and no prior knowledge of computer science or networking is required.

Textbooks

- Cyber Criminology, K. Jaishankar, CRC Press, ISBN 978-1-4398-2949-3
- Digital Crime and Forensic Science in Cyberspace, Kanellis, Kiountouzis, Kolokotronis and Martakos, Idea Group Publishing, ISBN 1591140873-3

Course Description

This course introduces the student to the investigation and analysis of cyber crime and cyber criminals through lecture and hands-on lab exercises in cyber criminalistics (i.e., digital investigation and forensics). Likewise, as an underpinning, the student will be introduced to cyber criminology as "the study of causation of crimes that occur in the cyberspace and its impact in the physical space".[1] The course ties the two broad topic areas (digital investigation and introductory digital forensics) together with lectures, case studies and laboratory exercises.

At least 50% of class time is spent in hands-on lab exercises in digital forensics, network tracking, introduction to the tools of the cyber criminalist, digital evidence management and analyzing the forensic remnants of a cyber event. Additionally, the student will learn techniques of cyber crime scene assessment and cyber criminal profiling. During the course of the laboratory exercises, students will create a personal lab notebook recording their lab exercises and will manage evidence including maintaining a proper chain of custody.

Course Objectives

This course introduces students to the use of the tools of the cyber criminalist, application of cyber crime scene assessment and cyber offender profiling, and the causation of cyber crime and its impact in the physical world. The first half of the course consists of introductions to various concepts. The second half expands upon the concepts introduced in the first half with more laboratory exercises and case studies. The second half also introduces the final project, a term paper length research report on a topic selected by the student and approved by the instructor.

[1] K. Jaishankar, Cyber Criminology, CRC Press 2011

Learning Objectives

1. *Terminology*. The student will be able to explain the meaning of terms used to describe common techniques and concepts in cyber criminology, digital forensics and investigation, cyber crime scene assessment and cyber offender profiling
2. *Skill*. The student will us the tools of the cyber criminalist to analyze digital incidents. The student will assess cyber crime scenes and develop offender profiles. The student will learn and apply theories and concepts of cyber criminology to criminalistics using case studies and lab exercises.
3. *Advanced Systems Concepts*. The student will be able to describe how cyber crime scene assessment and offender profiling work and will perform an assessment and create an offender profile. The student will perform a forensic analysis of a seized suspect computer. The student will perform a trace of a suspect through cyberspace.
4. *Laboratory Exercises*. All lab exercises will be recorded in the student's lab notebook which will be handed in at the end of the semester and will show as an additional lab grade. Additionally, students are expected to check out evidence from the class evidence custodian using proper chain of custody documentation. This documentation becomes part of the lab notebook.

Specific topic coverage includes:

- Criminological theories as applied to cyber crime
- Introduction to the use of computer forensics
- Introduction to the use of network forensics and cybertrail tracking
- Introduction to the criminalistic aspects of cyber crimes against persons (e.g. cyber stalking), hacking, malware, and other classes of cyber crimes
- Cybercrime scene assessment and cyber offender profiling
- Digital evidence management

Course Outline

("CC" = Cyber Criminology text and "DC" = Digital Crime text)

Topic	Topics	Chapter Readings	Assignments (To Be Determined)
1 LECTURE	• Intro to Cyber Criminology and Cyber Criminalistics • Cyber crime framework	CC – Introduction DC – Ch 1, 15	

2 **LAB**	• Setting up the student's lab notebook and understanding chain of custody • Lab – Network attack and forensics introductory exercise		
3 **LECTURE**	• Malware and digital forensics - intro	CC – Ch 18 DC – Ch 2, 3, 4, 5	
4 **LAB**	• Lab – Bonnie and Clyde, part 1 – computer forensics		
5 **LECTURE**	• Cybercrime scene assessment intro – video and lecture – case study: The Priest Case		
6 **LECTURE**	• Cyber offender profiling – lecture and exercise		
7 **LECTURE**	• Cybercrimes against persons - intro: cyberstalking, cyber bullying	CC – Ch 14, 16, 20 DC – Ch 12	
8 **LAB**	• Lab – Maltego intro, tracing the cybertrail		
9 **LECTURE**	• Hacking and hacktivism intro	CC – Ch 3, 19	
10 **LAB**	• Lab – Bonnie and Clyde, part 2 – computer forensics		
11 **LECTURE**	• Cyber fraud – Nigerian study	CC Ch 1	
12 **LECTURE**	• Tracing intrusions on the network - intro	DC – Ch 6	

13 **LAB**	• Lab – Tracing a network intrusion		
14 **LECTURE**	• Cyberstalking case development	CC – Ch 15, 17	
15 **LAB**	• Lab - Developing a cyberstalking case involving Facebook		
16 **LECTURE**	• Cybercrime scene assessment		
17 **LAB**	• Lab – Bonnie and Clyde, part 3 – Cybercrime scene assessment and offender profiles		
18 **LECTURE**	• Deviant behavior – pornography, pedophilia and on-line gambling – case study: “The Porn Guy”	CC – Ch 2, 5, 6	
19 **LAB**	• Lab exercise – computer forensic analysis for evidence of deviant behavior		
20 **LECTURE**	• Digital piracy	CC – Ch 11	
21 **LAB**	• Lab – Developing a digital piracy case using forensic computer analysis and forensic network analysis		
22 **LAB**	• Steganography and Lab – detecting steganography	DC – Ch 9	
23	**Final Projects Due – Final Presentations**		
24	**Final Presentations**		