ITT Technical Institute

CJ243P

The Criminalistics of Cybercrime

Onsite Course

SYLLABUS

Credit hours: 4

Contact/Instructional hours: 66 (46 Theory Hours, 20 Lab Hours)

Prerequisite(s) and/or Corequisite(s):

Prerequisite: CJ242P Forensics and Crime Scene Investigation

Course Description:

This course examines the scope of cybercrimes and the cybersecurity threat and legal considerations facing law enforcement and cybersecurity professionals in dealing with discovering, investigating and prosecuting cybercrimes. The role of intrusion detection in information security and different tools used to detect intrusion will also be discussed.

SYLLABUS: The Criminalistics of Cybercrime

Instructor: _____

Office hours: _____

Class hours: _____

Major Instructional Areas

1. The essence of criminalistics in cybercrime
2. Traditional problems associated with computer and electronics crime
3. History of cybercrimes and electronics criminal activities
4. Classification of computer and electronics crimes
5. Prosecution and government efforts against cybercrime
6. Applying the First and Fourth Amendments to computer-related crime
7. Intrusion detection and tools used for detection
8. Aspects of data analysis in computer crime

Course Objectives

After successful completion of this course, the student will have the opportunity to:

1. Define computer crime and examine the categories of computer crimes.
2. Identify the basic components of a computer system in relationship to the computer forensic tools that interact with those components.
3. Explore the criminology of computer crime by identifying the five theories used to explain computer crime.
4. Describe the evolution of computer crime by examining the category Computers as Means
5. Examine the types of crimes associated with the category of Computers as Targets.
6. Examine the crime of identity theft focusing on investigation, prosecution, and preventative issues.
7. Identify and describe the various social engineering techniques employed by criminals.
8. Describe the statutory issues related to cybercrime investigations.
9. Describe the relationship between the 1st Amendment and computer crime by examining the issues of decency, child pornography, and associated case law.
10. Explain the relationship between the 4th Amendment and computer crime by examining important case law and the unique search and seizure issues related to technology.
11. Explore the emerging issues of computer crime and the relevant investigative issues.
12. Utilize the resources, tools, and knowledge of the course to conduct an electronic crime scene investigation.
13. Describe the technological trends that investigators must be aware of when conducting an investigation.

Related SCANS Objectives

None

Teaching Strategies

The curriculum is designed to promote a variety of teaching strategies that support the outcomes described in the course objectives and that foster higher cognitive skills. Delivery makes use of various media and tools in the classroom.

Course Resources

Student Textbook Package

Britz, M. T. (2013). *Computer forensics and cyber crime: An introduction* (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

References and Resources

ITT Tech Virtual Library

Login to the ITT Tech Virtual Library (https://studentportal.itt-tech.edu) to access online books, journals, and other reference resources selected to support ITT Tech curricula.

- **General References**

  The following web sites provide additional information relevant to computer forensics and cybercrime:

General Resources

http://www.justice.gov/criminal-ccips http://staff.washington.edu/dittrich/forensics.html
http://justice.gov/criminal-ccipshttp://www.vaonline.org/internet_gen.html

Types of Cybercrime
http://www.bjs.gov/index.cfm?ty=tp&tid=41
Case Studies
http://www.knowbe4.com/case-studies/
Cybercrime Agencies
http://www.iacis.com/

Legal Aspects of Cybercrime
http://cyber.law.harvard.edu/daubert/tx.htm
http://www.epic.org/privacy/terrorism/DOJ_guidance.pdf

All links to web references outside of the virtual library are always subject to change without prior notice.

Evaluation & Grading

COURSE REQUIREMENTS

1. **Attendance and Participation**
   Regular attendance and participation are essential for satisfactory progress in this course.

2. **Completed Assignments**
   Each student is responsible for completing all assignments on time.

3. **Team Participation (if applicable)**
   Each student is responsible for participating in team assignments and for completing the delegated task. Each team member must honestly evaluate the contributions by all members of their respective teams.

Evaluation Criteria Table

The final grade will be based on the following weighted categories:

Categories	Weights (%)
Written Assignments	**25%**
Project Phase I	**15%**
Project Phase II	**15%**
Lab Assignments	**25%**
Final Project	**20%**
Total	**100%**

Grade Conversion Table

Final grades will be calculated from the percentages earned in class as follows:

A	90 - 100%	4.0
B+	85 - 89%	3.5
B	80 - 84%	3.0
C+	75 - 79%	2.5
C	70 - 74%	2.0
D+	65 - 69%	1.5
D	60 - 64%	1.0
F	<60%	0.0

Course Outline

Unit	Lsn	Lesson Title	Content Topics	Reading	Activity Type				
					Writing Assessment	Lab	Discussion	Project	Ungraded Activities
1	1	Understanding Computer Crime	Defining Computer Crime Categories of Computer	Chapter 1: Introduction and Overview of Computer Forensics and Cybercrime	X				
2	1	Understanding Computer Hardware	Computer Components Data Storage Compiling a Boot Disk	Chapter 2: Computer Terminology and History Chapter 10: Computer Forensic: Terminology and Requirements	X	X			PC Interfaces 101
3	1	The Criminology of Computer Crime	Criminological Theory	Criminology of Computer Crime I.pd Criminology of Computer Crime II.p	X	X	X		

Unit	Lsn	Lesson Title	Content Topics	Reading	Activity Type				
					Writing Assessment	Lab	Discussion	Project	Ungraded Activities
4	1	History of Computer Crime	Targeting Computers	Chapter 3: Traditional Computer Crime: Early Hackers and Theft of Components Chapter 4: Contemporary Computer Crime	X	X			A Study on Cyber-stalking Understanding Investigative Hurdles A Study on Cyberstalking Und
5	1	Computer Crimes: Computers as Targets	Targeting Computers	Chapter 3: Traditional Computer Crime: Early Hackers and Theft of Components Chapter 4: Contemporary Computer Crime Chapter 6: Terrorism and Organized Crime	X	X	X		How a Bookmaker and a Whiz Kid Took On a DDOS-based Online Extortion Attack
6	1	The Prosecution of Computer Crime	Computer Fraud and Abuse Act of 1984 Child Pornography Statutes Law Enforcement Initiatives	Chapter 5: Identity Theft and Identity Fraud Chapter 7: Avenues for Prosecution and Government Efforts			X	X	Taking Charge Taking Charge.pd
7	1	Computer Crimes:	Social Engineering: The Hackers Perspective Social Engineering: The Investigators				X	X	Social Engineering SANS Social Engineering

Unit	Lsn	Lesson Title	Content Topics	Reading	Activity Type				
					Writing Assessment	Lab	Discussion	Project	Ungraded Activities
		People as Targets	Perspective						
8	1	Computer Crime and the 1st Amendment	Decency Child Pornography Case Law	Chapter 8: Applying the First Amendment to Computer-Related Crime	X		X		CPPA, COPA, CIPA: Which Is Which? Child-Pornography Possessors Arrested in Internet-Related Crimes 'Toon porn' pushes erotic envelope online and Is anything taboo in 'toon porn'?
9	1	Computer Crime and the 4th Amendment	History of the Fourth Amendment and Technology Private vs. Public Sector Searches Electronic Communications Privacy Act of 1986 Privacy Protection Act Communication Assistance for Law Enforcement Act Privacy Other Legal Considerations	Chapter 9: The Fourth Amendment and Other Legal Issues Chapter 11: Searching and Seizing Computer-Related Evidence	X	X		X	Inside Dateline: To Catch a Predator III http://www.usdoj.gov/criminal/cybercrime/
10	1	Conducting an Electronic Crime	Approaching and Securing the Crime Scene Scene Processing Scene Departure	Chapter 11: Searching and Seizing Computer-Related Evidence		X			Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition

Unit	Lsn	Lesson Title	Content Topics	Reading	Activity Type				
					Writing Assessment	Lab	Discussion	Project	Ungraded Activities
		Scene Investigation							Electronic Crime Scene Investigatio
11	1	Emerging Issues	Wireless Communications Remote Storage (data stripping) Encryption Technology Virtual Pornography	Chapter 12: Processing of Evidence and Report Preparation Chapter 13: Conclusions and Future Issues				X	