San José State University
Department of Justice Studies
JS 269: Cyber Forensics
Spring 2019

Course and Contact Information

Instructor:	Dr. Bryce Westlake
Office Location:	Health Building 211
Personal Cell-Phone:	(408) 924.2743
Email:	Bryce.Westlake@sjsu.edu
Office Hours:	Monday & Wednesday 2:00 pm to 5:00 pm

Course Format

Technology Intensive, Hybrid, and Online Courses

I will utilize the Canvas Learning Management System as a means for distributing course materials such as syllabus, handouts, lecture slides, assignment instructions, and communications about changes to the course. You are responsible for regularly checking with the messaging system through MySJSU to learn of updates.

Catalog Description

This online course explores the history and evolution of cybercrime, examines the challenges faced by society at protecting oneself from a faceless threat, and introduces the steps for detecting, collecting, and analyzing digital evidence for criminal investigation.

Course Description

This online course introduces students to the growing, and continually changing, legal, technical, and social issues faced by society and law enforcement in addressing cybercrime. Students will examine current events and prominent cyberattacks, to understand the delicate balance between maintaining personal privacy and providing global security. Students will explore the criminological challenges in combatting a crime that can be invisible, may have no discernable victims (or offenders), and does not adhere to international boundaries. Finally, students will learn about the latest digital forensics methods being used by investigators to identify, preserve, and extract electronic evidence.

Course Learning Outcomes (CLO)

Upon successful completion of this course, students will be able to:

- (CLO 1) Distinguish between the different types of cybercrimes, including how they are conducted, who/what they target, where/why they persist, and the role the Internet plays in changing traditional crimes (e.g., bullying) and creating new crimes (e.g., phishing).
- (CLO 2) Identify the challenges faced nationally and internationally at combating cybercrime, and the steps being taken by organizations and law enforcement to address these challenges.
- (CLO 3) Take what they have learned in class and apply it to cybercrime-related current events.
- (CLO 4) Know steps to be taken to increase their own security and privacy online.

Course Requirements

Textbook

None

Other Readings

Supplied electronically via Canvas.

Library Liaison

Silke Higgins (silke.higgins@sjsu.edu), (408) 808.2118
http://libguides.sjsu.edu/justicestudies

Assignments

Online Discussion (20%): For each topic there will be associated online discussion(s) on Canvas, examining specific elements and key issues or current events related to that lecture's overall topic. Students will be expected to provide their viewpoint and critically discuss the implications of the issue or event to our understanding of cybercrime and how it is addressed by societies. This assignment will specifically address CLO's 1, 2, 3, & 4.

Reflection Papers (15%): You will write four reflection papers, each at least two to three (full) pages in length. Each paper will focus on a specific topic and question, which I will provide to students via discussion. Students will be expected to provide their viewpoint and critically discuss the implications of the issue or event to our understanding of cybercrime and how it is addressed by societies. This assignment will specifically address CLO's 1, 2, & 3.

Presentation -Data Breach or Malware (15%): The purpose of this assignment is for students to become familiar with some of the most impactful data breaches and malware attacks over the past decade. Students will give a maximum 15-minute presentation on an influential data breach or malware attack. Students will describe the data breach or malware attack, how it was detected, the resulting damage, and the technical and managerial implications of the incident. This assignment will specifically address CLO's 1 & 3.

Paper #1 –Tell Me a Story (20%): The purpose of this assignment is to provide students with practical experience regarding the concept of personal privacy, or lack thereof, on the Internet. Students will write an 8-10-page paper (excluding title page and references) about their investigation of two topics. First, students will input their name into a search engine, with minimal other identifying information, and describe whether the data returned was about them, and how they felt about that information being readily accessible. They will describe the age (i.e., how old), personal nature (e.g., address, phone number, banking information), and online profile (e.g., your likes/dislikes, purchases, hobbies) it presented about them. Second, students will use any cyber methods they can devise to find information on the course instructor. Students will be required to record the steps they took (e.g., search terms) to acquire the information and what information they obtained, including where it was found. Students will then describe this process and reflect on the steps others may take to find personal information about them. This assignment will specifically address CLO's 1, 3, & 4.

Paper #2 –Combating Cybercrime Internationally (30%): The purpose of this assignment is for students to explore the legal issues regarding how governments and social control agencies can police a virtual environment without physical boundaries and borders. Select a type of cybercrime discussed in the course and determine how partnerships/cooperation/resource-sharing could, realistically, be improved between them and the United States. Students will write a 12 to 15-page paper (excluding title page and references) on the laws, if any, that exist in each country and what each could learn from the other. Discussion should include how privacy and rights can be balanced with security. This assignment will specifically address CLO's 1 & 2.

Grading Information

- To receive a grade for this course, all course requirements must be met, and every assignment must be completed. Failure to complete any one assignment may result in a failing grade for this course.
- Individual assignment rubrics are provided on Canvas.
- Late assignments/papers will lose 10% for every calendar day that they are late, including weekend days.

Determination of Grades

A (plus)	97% - 100%	A	93% - <97%	A (minus)	90% - <93%
B (plus)	85% - <90%	B	80% - <85%	B (minus)	75% - <80%
C (plus)	71% - <75%	C	67% - <71%	C (minus)	63% - <67%
D (plus)	59% - <63%	D	54% - <59%	D (minus)	50% - <54%
F	Below 50%				

University Policies

Per University Policy S16-9, university-wide policy information relevant to all courses, such as academic integrity, accommodations, etc. will be available on Office of Graduate and Undergraduate Programs' Syllabus Information web page at http://www.sjsu.edu/gup/syllabusinfo/".

Spring 2019 Course Schedule

This course schedule is subject to change with fair notice, at the instructor's discretion. All reading assignments listed should be completed prior to class on that date. Additional readings may be assigned.

Week	Date	Topics	Readings
1	03/18/18	**Introduction** -Course Overview -What is Cybercrime -Types of Cybercrime -Computer Basics	*Articles* The Current State of Cybercrime Scholarship (Holt & Bossler) Cyber Criminology as an Academic Discipline (Jaishankar) The Internet as a Conduit for Criminal Activity (Wall) *Optional (For More Information on Computer Functioning)* How does the Internet Work? (Strickland) How Firewalls Work? (Tyson) What is an 'IP Address'? (Gil) **Assignment:** Reflection #1 – What is Cybercrime (March 22nd)
2	03/25/18	**Personal Security** -Online Identity -Privacy & Security -Identity Theft/Fraud -(Social) Networks -Scams	*Articles* The Secret War (Popular Mechanics) What is Social Engineering (Webroot) TBD
3	04/01/18	**Spring Break (No Class)** **Assignment:** Paper #1 – Tell Me a Story (April 3rd)	
4	04/08/18	**Deep Web** -TOR -Dark Web -Digital currency (Bitcoin) -Organized Crime -Corporate Crime	*Articles* Tor Project: Overview (TOR) Exploring the Deep Web (Trend Micro) How BitCoin Works (Forbes) A Hacker's Race to Build the Amazon.com of Stolen Credit Cards (WeirderWeb) White-Collar Cybercrime (Payne, 2018) **Assignments:** Data Breach Presentation (April 8th) Reflection #2 – Deep Web (April 12th)
5	04/15/18	**Computer Crimes** -Malware (viruses, worms, etc.) -Phishing -Email Spam -Legislation	*Articles* Internet Security Report 2018 (ISTR) McAfee Mobile Threat Report Q1, 2018 (McAfee) Mobile Malware Evolution 2016 (Kaspersky Lab) **Assignments:** Malware Presentation (April 15th) Reflection #3 – What Can a Hacker Do? (April 19th)
6	04/22/18	**Cyber-Terrorism** -Hacking -Violent Extremism	*Articles* Hackers Manifesto (The Mentor) How Big and Powerful is Anonymous (Vandita) The Use of the Internet for Terrorist Purposes (UNODC) Terrorism and the Internet (Conway) **Assignments:** Reflection #4 – Role of ISP (April 26th)

Week	Date	Topics	Readings
7	04/29/18	**Sex Online** -Trafficking -Child Pornography -Sexting -Revenge Pornography -Stalking/Bullying	*Articles* Fighting Human Trafficking (European Commission) Assessing the Validity of Automated Webcrawlers (Westlake, Bouchard, & Frank) Understanding Revenge Pornography (Bond & Tyrrel) *Optional* Revenge Pornography Removal Guide (Cyber Civil Rights) Seeing the Forest Through the Trees (Westlake & Frank) **Assignments:** Reflection #5 – Amanda Todd (May 3rd)
8	05/06/18	**Combating Cybercrime** -Patriot Act -International challenges -Jurisdiction and joint operations	*Articles* An Oral History of Napster (Fortune) Digital Forensics as a Forensic Science Discipline (SWGDE) Best Practices for Digital Evidence Collection (SWGDE) Best Practices for Computer Forensics (SWGDE) Collection of Dig. and Mm. Evidence Myths & Facts (SWGDE) *Optional* MSO Procedures for Computer Forensics (SWGDE) **Assignments:** Paper #2 – Combating Cybercrime International (May 12th)