San José State University
Department of Justice Studies
JS 269: Cyber Forensics
Summer 2022

Course and Contact Information

Instructor:	Dr. Bryce Westlake
Office Location:	Health Building 210B
Phone:	408-924-2743
Email:	Bryce.Westlake@sjsu.edu
Office Hours:	TBD

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.

Assignments

Online Discussion (20%): The purpose of this assignment is for students to apply cybercrime-related topics to current events. There will be two discussion questions each week, examining specific elements and key issues 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.

The Threat of Deep Fakes (15%): The purpose of this assignment is for students to learn how easy/difficult it is to create a deep fake, and the impact they can have on society. Students will have the option of creating a 30 to 60-seconds deep fake video or writing a 4 to 6-page paper (excluding title page and references) on the role of Deep Fakes in facilitating disinformation. This assignment will specifically address CLO's 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%				

Library Liaison

Anamika Megwalu (anamika.megwalu@sjsu.edu) (408) 808.2089 https://libguides.sjsu.edu/cybersecurity

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/".

Summer 2022 Course Schedule

Week	Date	Topics	Readings & Assignments
0	June 1st	**Introduction** -Course Overview	None
1	June 1st to June 5th	**The Internet and Crime** - What is Cybercrime - How Cybercrime Functions - The Deep Web - Cryptocurrency	*Readings* The Current State of Cybercrime Scholarship (Holt & Bossler, 2014) Defining Cybercrime (Payne, 2019) The Historical Evolutions of Cybercrime (Choi, 2019) IC3 2020 Report (FBI, 2021) Exploring the Deep Web (Trend Micro, 2015)
2	June 6th to June 12th	**Crimes Against the Computer** - Malware - Copyright - Phishing - Botnets - Spam	*Readings* 2020 Cybersecurity Outlook Report (VMWare, 2020) The Evolution of Cybercrime and Cyberdefense (Trend Micro, 2018) The Kill Chain (Lockheed Martin, 2015) MITRE ATT&CK Framework (Petters, 2019) The Modern Bank Heists (VMWare, 2021) **Writing Assignment #1:** Tell Me a Story (June 12th, 2022)
3	June 13th to June 19th	**Personal Crimes** - Human Trafficking - Cyberbullying - Sex Crimes - Radicalization - Deep Fakes - Fake News	*Readings* Information Overload Helps Fake News Spread (Menczer & Hills, 2020) Intimate Partner Violence and the Internet (Clevenger & Gilliam, 2019) Risk and Protective Factors for Cyberbullying Perpetration and Victimization (Wilson, Witherup, & Payne, 2019) The Past, Present, and Future of Online Child Sexual Exploitation (Westlake, 2019) The Role of the Internet in Facilitating Violent Extremism and Terrorism (Scrivens, Gill, & Conway, 2019) **Presentation:** Malware or Data Breach (June 19th, 2022)
4	June 20th to June 26th	**Privacy and Security** - Surveillance - Identity Theft - Fraud - Hacking	*Readings* Technology Use Abuse and Public Perception (Furnell, 2019) Identity Theft: Nature, Extent, and Global Response (Golladay, 2019) Private Traits and Attributes are Predictable (Kosinski et al., 2013) What is Hacking (Guru99) Facebook Studies (Various Authors) **Video/Reflection Assignment:** Deep Fake (June 26th, 2022)
5	June 27th to July 2nd	**Combating Cybercrime** - Jurisdiction - Police Relations - Digital Forensics - CAN-SPAM	*Readings* Cybercrime Legislation in the United States (Bossler, 2019) Forensic Evidence and Cybercrime (Rodgers, 2019) Digital Forensics (SWGDE, Various) Police and Extralegal Structures to Combat Cybercrime (Holt, 2019) Police Legitimacy in the Age of Social Media (Nhan-Noakes, 2019) **Written Assignment #2:** Combating Cybercrime Internationally (July 2nd)