San José State University
Department of Justice Studies
FS 12, Introduction to Digital Evidence Investigations, Fall, 2022

Course and Contact Information

Instructor:	Tom Arnold
Office Location:	Student Union second floor seating area or TBD by instructor
Telephone:	(use Canvas for email)
Email:	tom.arnold@sjsu.edu
Office Hours:	12:30 to 13:00 Monday and Wednesday or by appointment
Class Days/Time:	Mon & Wed, 13:30 to 14:45 hours
Classroom:	Clark Building Rm 226
Prerequisites:	*None. Strongly recommend JS/FS 100W, FS 11*

Course Description

Introduces to the field of digital evidence investigation, including introduction to computing systems and environments, laws and jurisdiction, identification of computer and network artifacts, process for handling and analysis of digital artifacts, critical thinking required to evaluate digital artifacts, and development of case-relevant event timelines. Focuses on the policies, procedures, and best practices for conducting electronic examinations, in adherence to the rules of evidence for civil and criminal court proceedings in the US. Some will be included to supplement procedural topics.

Course Learning Outcomes (CLO)

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

1. *Understand basic computer and mobile device operating systems, file systems, and network technologies and how digital evidence artifacts are created and stored.*
2. *Explain the role and responsibilities of a digital forensic examiner*
3. *Demonstrate knowledge of evidentiary procedures for conducting digital evidence examinations on mobile devices, computers, cloud environments, data center servers, and across networks*
4. *Apply analytical methods to parse and identify significant facts from select digital artifacts*
5. *Explain the methods for evaluation of file systems, memory, network, mobile, and software artifacts and relevance to any case*

Required Texts/Readings

Textbook

Maras, Marie-Helen. (2015). *Computer Forensics: Cybercriminals, Laws, and Evidence (2nd Edition)*. Jones & Bartlett Learning. ISBN13: 978-1-4496-9222-3.

Other Readings

Topics and material to be assigned during class

Other technology requirements / equipment / material

none

Library Liaison

Anamika Megwalu
408-808-2089 (anamika.megwalu@sjsu.edu)

Course Requirements and Assignments

In-Class Discussion and Quizzes (10% of final course grade): As a result of in-class participation and discussion of critical elements, quizzes cover elements from reading, lecture, demonstrations, discussion, and current events reviewed during class session. Your grade will reflect the importance of being active in this course, which relies in great part on the reflections, discussions, and exercises in class. 100% attendance is mandatory. These quizzes will be administered remotely via Canvas, and students must complete the quiz during the assigned and allocated time. **Under NO circumstance will a second attempt be permitted for a quiz**. Failing to complete or take a quiz will result in zero (0) points score for the quiz. Quizzes are timed and open book/notes. Material will address CLO's 1, 2, 3, 4, & 5.

Paper – Critical Thinking and Analysis (20% of final course grade): The purpose of this assignment is for students to select a current topic from the Web or news feeds describing a criminal or civil case where digital evidence may play or plays a key role. Students will identify, analyze, and describe digital artifacts (individual digital evidence objects) relevant to the case and report on how these objects were evaluated and what relevance the artifact(s) had on the case. A key component will be how the student describes the characteristics of the artifact how the artifact(s) support conclusions made in the case. The news item must be no older than one-year from start of term. Artifacts may include, but not limited to, log files, Web activity logs, chat logs, link (.lnk) files, prefetch (PF) files, jump (JMP) lists, registry objects, network captures (PCAP), SIM data, BFU & AFU data, file system data, or Shellbags. Scores will be awarded on how complete the material is evaluated by the student. 50% of the score on the paper will be based on the student's explanation of the digital artifact(s) and the level of technical detail provided. Students will deliver a 5-to-7-page report due by the 14th week (by 21 Nov 2022 23:59:59). Late assignments/papers will lose 10% for every calendar day that they are late, including weekend days and holidays, **up to a maximum of 3-days**. After 3-days, a score of zero (0) points will be awarded and the paper will **not** be accepted. This assignment addresses CLO's 4 &5.

Midterm (30%) and Final Examination (40%) for total semester value of 70% of final course grade: A midterm and final examination will be presented during assigned times. These exams will be administered remotely via Canvas, and students **must complete the exam during the assigned and allocated time**. Each exam is OPEN book/notes and will cover material from lectures and assigned readings from textbook and additional reading material provided in Canvas during session modules**. Under NO circumstance will a second attempt be permitted for a student missing an exam.** Each exam will be **cumulative** and comprised of multiple choice and short answer questions. These examinations will specifically address CLO's 1, 2, 3 and 4.

Grading Information

A plus = 97.0 to 100.0	A = 90.0 to less than 97.0	A minus = 85.0 to less than 90.0
B plus = 80.0 to less than 85.0	B = 75.0 to less than 80.0	B minus = 70.0 to less than 75.0
C plus = 65.0 to less than 70.0	C = 60.0 to less than 65.0	C minus = 50.0 to less than 60.0
F = less than 50.0		

- 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.
- Late assignments/papers will lose 10% for every calendar day that they are late, including weekend days and holidays, up to a maximum of 3-days. After 3-days, a score of zero (0) points will be awarded and the paper will not be accepted.

Success in this course is based on the expectation that students will spend, for each unit of credit, a minimum of 45 hours over the length of the course (normally three hours per unit per week) for instruction, preparation/studying, or course related activities. Other course structures will have equivalent workload expectations as described in the syllabus.

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/"

FS 12: Introduction to Digital Evidence Investigations
Fall 2022 Course Schedule

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

Week	Topic	Weekly Overview (Subject to Change)
1	Course introduction and introduction to Cybercrime; How computers work Part I	Cybercrime characteristics, the electronic kill-chain, computer devices as victim and perpetrator. Introduction to how computer technology works and relevance to digital evidence. (Maras, Ch 1)
2	How computers work Part II & III. Operating systems, file systems, network protocols and cryptography	Windows, *NIX, iOS & Android operating systems, embedded systems, the application stack, common network protocols, and introduction to cryptography relevant to digital evidence
3	Introduction to forensic investigations and digital evidence artifacts	Basic procedures, methods and investigative processes (Maras, Ch 2) Types, authentication, and standards; basic handling and preparation for investigation, (NIST PDF review)
4	No class due to OSDF con & and PCI con	Work on your projects
5	Electronic laws	Laws regulating access to electronic evidence (Maras, Ch 3) The jurisdiction problem; Demonstration of memory analysis
6	Searches and seizures	Privacy protection, rights, and search warrants; evidence seizure and capture in civil and administrative cases; Part 1 of incident response - dead or alive (Chapter 4)
7	Electronic Evidence Collection	Location of evidence, systemic acquisition and preservation of digital evidence (Chapter 8), integrity and myths.
8	Crime Scene Investigation Part I	Real Incident Response methods and process characteristics in 2022; CSI characteristics and basic methods (Chapter 9)
9	Crime Scene Investigation Part II, and guest speaker	Finding and handling digital evidence objects. Collection of tirage evidence, rapid forensic analysis and collection of full image (Chapter 10)
10	Time, timelines & temporal issues (midterm)	Understand the enigma and challenges time presents, systemic temporal issues, temporal proximity, time stamps, time "stomping", other time stamps, case relevance, why timelines are important to all investigations, and preparation of and analysis of reliable timeline [Midterm exam]
11	Network forensic analysis	"If it didn't cross a network, it didn't happen" – Basic packet capture and evaluation, network logs and the crime scene, common misses
12	Digital artifacts Part I	Systemic digital artifacts in Windows operating system computers
13	Digital artifacts Part 2	Systemic digital artifacts in Windows/Linux operating system computers, logs, and log artifacts
14	Email and messaging	Email protocols, message formats, MIME, and value for digital evidence (Chapter 11), [PROJECT Due 21 Nov 2022 23:59:59]
14	Mobile Devices	SMS and chat; introduction to mobile devices as evidence covering methods and process (PDF's provided by instructor for current best practices and deeper dive into mobile device operating systems, analysis, and challenges (Chapter 13)
16	Capstone review & Netwars CTF	Final preparation and review of course topics and material.