San José State University
Department of Justice Studies
FS 130, Digital Forensic Analysis, Spring, 2022

Course and Contact Information

Instructor:	Tom Arnold
Office Location:	Upstairs Student Union near ballroom in seating area
Email:	tom.arnold@sjsu.edu
Office Hours:	12:00 to 13:00 on class days
Class Days/Time:	TBD
Classroom:	TBD
Prerequisites:	Any FS12, CS47 or instructor consent *Strongly recommend JS/FS 100W*

Course Description

Course and lab material dive into computer forensic investigations. The lab portion follows the outline of the course and gives students a hands-on experience to process artifacts. The course focuses on identification, acquisition, processing, and analysis of artifacts and digital evidence. This simulated case and other artifacts will be introduced during lab session and expanded in subsequent sessions as new artifacts are identified and examined. Case scenarios will carry forward to other, specialized digital forensic disciplines.

Course Learning Outcomes (CLO)

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

1. *Basic functions, operation, and network communications of computer and mobile phone devices*
2. *Demonstrate knowledge of evidence identification, acquisition, and analysis*
3. *Demonstrate knowledge of various systemic artifacts and methods for answering investigative questions.*
4. *Apply investigative techniques to identify suspicious and material events*
5. *Apply techniques to identify evidence, acquire mobile device evidence, and analyze artifacts*

Required Texts/Readings

Textbook

Carvey, Harlan (2016). *Window Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry (2nd Edition)*. Syngress. ISBN: 978-0-12-803291-6.

Carrier, Brian (2005). *File System Forensic Analysis*. Pearson Education, Inc. ISBN-13: 978-0-32-126817-4.

Other Readings

(Optional reference)

Tamma, Rohit, Skulkin, Oleg, Mahalik, Heather, Bommisetty, Satish (2020) *Practical Mobile Forensics (4th Edition).* Packt Publishing, Ltd. ISBN 978-1-83864-752-0.

(Optional reference)

Operating System Tutorial. (2016) Tutorials Point (I) Pvt. Ltd.

https://www.tutorialspoint.com/operating_system/os_pdf_version.htm

(Optional reference)

Carvey, Harlan (2018). *Investigating Windows Systems*. Syngress. ISBN: 978-0-12-811415-5.

Other technology requirements / equipment / material

Lab systems will be setup and used by students in a virtual machine environment, running VMWare and the Spartan Investigative Platform (SIP). The SIP contains all of the tools and case material that will be used during the course.

Library Liaison

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

Course Requirements and Assignments

General attendance and lab work (0%): Participation in class discussion requires arriving on time and being prepared to critically discuss the implications of key issues of the week's topics. This requires completing the weekly readings and other assignments prior to arriving in class. Active work to complete lab exercises and work with a partner.

How things work exam *(20%):* This quiz covers general computing information that any forensic analyst or digital evidence specialist must know. Topics range from general computing hardware, operating system architecture, typical application architecture, system remembrance, volatile and non-volatile elements, common file systems, basic networking, and basic device operation for common computers and mobile devices. The quiz is CLOSED book, administered during class session. This is a timed quiz that is short answer. This exam addresses CLO 1.

Lab Practical #1 – Windows system processing (20%): Within the lab, students will identify case-relevant artifacts, filter data, evaluate and describe the relevance of the artifact to the case, and draw defensible conclusions. This practical exam addresses CLO's 2 & 3.

Lab Practical #2 – Artifact analysis (20%): Within the lab, students will be presented artifact extracts to identify and review. Describe how to sift out relevant elements, explain relevance, and draw a supported conclusion. This practical exam addresses CLO's 4 & 5.

Final Examination (40%): You will be administered a final examination worth 50% of your final grade. The exam is OPEN book and covers material from lectures (including all media presented), CRITICAL THINKING from lab exercises, assigned readings, and lecture**.** The final exam will be administered remotely via Canvas. Exam will be open during a period to be announced by the instructor, and students will have 2 hours-15 minutes to complete. The exam will be a combination of essay and multiple-choice questions. This examination specifically addresses CLO's 1, 2, 3, 4 & 5.

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		

Note: Final course grade will NOT be curved.

To receive a grade for this course, all course requirements MUST be met, and every assignment/quiz/lab practical/Final exam MUST be completed. Failure to complete any one assignment may result in a failing grade for this course.

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, including but not limited to instruction and labs. 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 130: Digital Forensic Analysis
Spring 2021 Course Schedule

This course schedule is subject to change with fair notice, at the instructor's discretion. Changes will be communicated via Canvas, and 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 "How things work" P1: Core computing and mobile device concepts**	Introduction to course and requirements. Core hardware and firmware components of a computing/mobile devices. Lab00: Introduction and setup of VMWare Player environment Lab01: Introduction to the SIP
2	**"How things work" P2: Operating systems, and BDH math. Setup & config of Autopsy, loading e01 image and navigating**	Examination of operating systems and how stuff works (Carvey Ch 1 p. 23-70) Lab02: Setup, config, and exploration of Autopsy
3	**"How things work" P3: File systems, networking, & crypto for 4n6's [How things work Exam]**	File systems, networking, & crypto for forensics (Carrier Ch 1, 2, 11 &12) Lab03: KAPE & Autopsy to explore $MFT
4	**Crime scene investigation and digital acquisition**	Basics of acquiring 4n6 evidence; where evidence data lives; data on computers, mobile devices, IoT, networks, cloud and reusable media; and evidence file formats. Basic CSI response. Lab04: CSI acquisition w/ dumpit, EDD, Kape, & FTK
5	**Hardware and software evidence acquisition**	General hardware and software response topics, live response, dead box, KAPE targe acquisition, prep of destination media. (Carrier Ch 3) Lab05: Preparing destination media and using KAPE target module, review of KAPE acquisition data
6	**Live response, image mounting, and triage**	Memory acquisition, image mounting, destination media types, and timelining, VSS data (Carvey Chapter 7 & 8) Lab06: Image mounting w AIM, setup and capture timeline from $MFT, and examine VSS
7	**Exploring windows registry**	Introduction to core registry hives & file evidence artifacts and operation (Carvey Ch 3 p. 101-308 & Ch 4 p. 195-241) Lab07: System and user profiling using registry, USB device artifacts
8	**Shell items, images, videos & other artifacts**	System and user profiling. evidence of execution, opening, and user activity; removable device examination Lab08: Autopsy ingest modules and review
9	**Host acquisition topics**	Host based live acquisition, physical v. logical, HCA & DCO, Chromebook, takeout, xLEAPP, and other data sources. Lab09: specialized acquisition, unallocated space, deleted files
10	**[Lab Practical #1] KAPE**	[Lab Practical in session 1, covering lab sessions 4 thru 9] Using KAPE to parse evidence files, KAPE modules, analysis of artifacts. Lab10: KAPE and Autopsy to parse and examine evidence files
11	**Mobile device acquisition and *NIX artifacts**	Android and iOS device introduction, methods for capture and isolation of devices, topics related to acquisition of artifacts. Intro to *NIX systems and where artifacts are located. Lab11: Android and NIX artifact review and analysis
12	**Mobile device analysis and triage**	Data acquisition, backup acquisition, and initial analysis. (Tamma Ch 3, 4, 5 p. 55-134) (Tamma Ch 8,9 & 10 p. 193-290) Lab12: Examining Android device capture
13	**Logs and log analysis**	Event log parsing and analysis covering Windows and Linux device logs and log structures; correlation with timeline [xLEAPP] Lab13: Event viewer and Autopsy timeline
14	**Working the Renzik case 1**	Working through the data and exercises on the Renzik case. Lab14: First part of Rensik case work.
15	**Working the Rensik case 2 & prep for lab practical #2**	Working through the data and exercises on the Renzik case Lab 15: Finishing the Renzik case
16	**[Lab Practical #2 CTF Capstone] Final review**	[Lab Practical #2 in session 1, CTF Hunter Case] Cumulative final review and critical thinking/decision-making exercise