COURSE OUTLINE : CS/IS 183
D Credit – Degree Applicable
COURSE ID 010279
Cyclical Review: August 2020

COURSE DISCIPLINE : CS/IS

COURSE NUMBER : 183

COURSE TITLE (FULL) : Digital Forensics Fundamentals

COURSE TITLE (SHORT) : Digital Forensics Fundamentals

CALIFORNIA STATE UNIVERSITY SYSTEM C-ID : ITIS 165 – Digital Forensics Fundamentals

CATALOG DESCRIPTION

CS/IS 183 is an introduction to the methods used to properly conduct a computer forensics investigation beginning with a discussion of ethics, while mapping to the objectives of the International Association of Computer Investigative Specialists (IACIS) certification. Topics covered include: an overview of computer forensics as a profession; the computer investigation process; understanding operating systems boot processes and disk structures; data acquisition and analysis; technical writing; and a review of familiar computer forensics tools.

Total Lecture Units: 3.00

Total Laboratory Units: 0.00

Total Course Units: 3.00

Total Lecture Hours: 54.00

Total Laboratory Hours: 0.00

Total Laboratory Hours To Be Arranged: 0.00

Total Contact Hours: 54.00

Total Out-of-Class Hours: 108.00

Recommended Preparation: CS/IS 194 or 196, or equivalent, or knowledge of workstation hardware and storage.

ENTRY STANDARDS

	Subject	Number	Title	Description	Include
1	CS/IS	194	Information Technology Essentials	install, configure and maintain devices, PCs and software for end users;	Yes
2	CS/IS	194	Information Technology Essentials	understand the basics of networking and security/forensics;	Yes
3	CS/IS	196	Advanced Networking: Security	design and administer an organization's security policy;	Yes
4	CS/IS	196	Advanced Networking: Security	detect and remove malicious content from network resources;	Yes

EXIT STANDARDS

1 Define computer forensics;
2 summarize the certification requirements for computer forensics labs;
3 measure the different ways for proper data acquisition;
4 classify the rules for proper digital evidence handling;
5 analyze how data is stored and managed by an operating system;
6 analyze various computer forensics tools;
7 validate the evidence during the analysis process;
8 identify and reconstruct graphics files;
9 describe the importance of network forensics;
10 analyze email investigations;
11 describe guidelines for testifying in court;
12 maintain a high level of ethical behavior in their work.

STUDENT LEARNING OUTCOMES

1 explain how to prepare for a computer investigation;
2 explain how to properly gather evidence and maintain records of chain of custody;
3 use forensic tools to analyze digitally stored evidence;

COURSE CONTENT WITH INSTRUCTIONAL HOURS

	Description	Lecture	Lab	Total Hours
1	Computer Forensics as a Profession • overview of digital forensics • maintaining professional conduct • understanding data recovery	4	0	4
2	Computing Investigation Processes	4	0	4
3	Microsoft Operating Systems, Boot Processes and Disk Structures • boot sequence • FAT disks • NTFS disks • disk partitions	4	0	4
4	Macintosh and Linux Operating Systems, Boot Processes and Disk Structures • boot sequence • Mac file structure	4	0	4
5	The Investigator's Office • forensic lab accreditation requirements • physical requirements for digital forensics lab • basic forensic workstation	5	0	5
6	Current Computer Forensics Tools • digital forensics software tools • digital forensics hardware tools	5	0	5
7	Digital Evidence Controls • Linux validation methods • Windows validation methods	4	0	4
8	Crime/Incident Scene Processing • identifying digital evidence • preparing for a search	4	0	4
9	Data Acquisition • mini WinFE boot CDs and USB drives • Linux boot CD	4	0	4
10	Computing Forensics Analysis	3	0	3

11	Email Investigations • Email crimes and violations • Email servers • specialized Email forensic tools	3	0	3
12	Graphic Image Recovery • recognizing graphic files • understanding data compression	3	0	3
13	High Tech Reports • guidelines for writing reports • generating report findings with forensic software tools	3	0	3
14	Expert Witness Overview • code of ethics • ethical difficulties in expert witness	4	0	4
				54

OUT OF CLASS ASSIGNMENTS

1 reports (e.g. reports on assigned reading topics such as crime/incident scene processing best practices;
2 labs on NETLAB (e.g. simulated labs that provide hands on learning such as introduction to Autopsy Forensic Browser).

METHODS OF EVALUATION

1 hands-on projects (e.g. computing forensics analysis);
2 problem-solving assignments (e.g. use of computer forensics tools);
3 Presentations (e.g. computer forensics case scenarios and analysis);
4 midterm examinations;
5 final examination.

METHODS OF INSTRUCTION

☑ Lecture
□ Laboratory
□ Studio
□ Discussion
☑ Multimedia

□ Tutorial
□ Independent Study
□ Collaboratory Learning
☑ Demonstration
□ Field Activities (Trips)
□ Guest Speakers
□ Presentations

TEXTBOOKS

Title	Type	Publisher	Edition	Medium	Author	IBSN	Date
Guide to Computer Forensics and Investigations	Required	Cengage	6	print	Nelson, Bill, Amelia Phillips	978-1337568944	2019