GAVILAN COLLEGE

5055 Santa Teresa Blvd
Gilroy, CA 95023

Course Outline

COURSE: CSIS 184 DIVISION: 50 ALSO LISTED AS: AJ 184

TERM EFFECTIVE: Spring 2021 CURRICULUM APPROVAL DATE: 12/08/2020

SHORT TITLE: COMPUTER FORENSICS

LONG TITLE: Computer Forensics

Units	Number of Weeks	Type	Contact Hours/Week	Total Contact Hours
3	18	Lecture:	3	54
		Lab:	0	0
		Other:	0	0
		Total:	3	54
		Total Learning Hrs:	162	

COURSE DESCRIPTION:

Introduction to computer crime investigation processes. The student is introduced to the hardware, software, networks and devices found in typical home and business settings. Techniques and equipment used to collect evidence, ensure integrity, locate and prepare data for forensic investigation. Covers chain of custody requirements for admissible evidence, data formats for a variety of modern equipment, and recovery of deleted or encrypted information. This course has the option of a letter grade or pass/no pass. This course is also listed as AJ 184.

PREREQUISITES:

COREQUISITES:

CREDIT STATUS: D - Credit - Degree Applicable

GRADING MODES

L - Standard Letter Grade
P - Pass/No Pass

REPEATABILITY: N - Course may not be repeated

SCHEDULE TYPES:

02 - Lecture and/or discussion
03 - Lecture/Laboratory
04 - Laboratory/Studio/Activity
047 - Laboratory - LEH 0.7
05 - Hybrid
72 - Dist. Ed Internet Delayed
73 - Dist. Ed Internet Delayed LAB
737 - Dist. Ed Internet LAB-LEH 0.7

STUDENT LEARNING OUTCOMES:

By the end of this course, a student should:

1. Identify, remove, and replace all major components of a typical personal computer.
2. Describe the special requirements of chain of custody for digital evidence.
3. Describe the most common network topologies and protocols and identify key hardware components for these topologies.
4. Inventory files on disk, perform searches for specific files, and locate temporary files such as caches on Mac, Windows, UNIX.

CONTENT, STUDENT PERFORMANCE OBJECTIVES, OUT-OF-CLASS ASSIGNMENTS

Curriculum Approval Date: 12/08/2020

9 Hours

CONTENT: Basic components of computer hardware, troubleshooting, tour of 3 main operating systems. Disassemble / reassemble hardware, boot computer. Mount hard disk in separate computer. Boot into forensics toolkit.

STUDENT PERFORMANCE OBJECTIVES (SPO): Identify components, operating system, file system. Utilize boot into forensics toolkit.

9 Hours

CONTENT: Basic operation of computer networks, routers, switches. Physical identification of standard and diagnostic equipment. Logical identification of equipment on the network. Typical structure of server room. Diagnostic of running network, wired and wireless. Use networking toolkit to map machines, services running, and actual physical location of data available on network.

SPO: Find data on the network through typical services: file-sharing, web, ftp, email. Trace to physical location.

9 Hours

CONTENT: Mobility, mobile equipment and operating systems. Phone capabilities and strategies. SIM cards. Structure of telecom networks and their relation to IP networking. Social media, strategies for capturing dynamic web sites. Hands on practice with mobile operating systems. Application of screen captures, screen recording.

SPO: Recognize and operate variety of mobile OSs. Recognize and record activity on non-static, dynamic, or social media website.

9 Hours

CONTENT: Forensics toolkit. Linux Operating System. Basic utilities: disk mapping, photo thumbnails, log file analysis. Mount target disk as read-only. Plan and perform investigation and analysis of disk contents.

SPO: Utilize boot forensics software and mount target disk for investigation. Utilize basic file system tools for examining contents of target drive.

9 Hours

CONTENT: Forensics toolkit - UNIX utilities. DD, GREP, STRINGS, TRACEROUTE, WAVEMON, IPTRAF, NMAP, WIRESHARK Hands-on practice with utilities in realistic setting.

SPO: Identify proper UNIX utility for a given situation. Use each utility.

7 Hours

CONTENT: Requirements for evidence and testimony. Establishing and recording chain of custody. Report writing. Start-to-finish simulation of investigation, beginning with target disk, investigation, and report writing.

SPO: Assess hardware and software situation, determine the appropriate tools, plan and execute an investigation.

2 Hours

FINAL EXAM

METHODS OF INSTRUCTION:

Lecture, Computer Demonstration, Online Documents and Tutorials, Web Research

OUT OF CLASS ASSIGNMENTS:

Required Outside Hours: 40

Assignment Description:

Read textbook and study for quizzes/exams.

Required Outside Hours: 28

Assignment Description:

Complete workbook exercises.

Required Outside Hours: 40

Assignment Description:

Homework Assignments such as: (1) Research and identify: component appearances, manufactures, connectors/cables, vendors. (2) Research: linking logical resources (IP addresses) with physical hardware. Layout of the internet. VPNs. Typical

and atypical operation of standard network services (web, ftp, email, chat, video). (3) Search for and record on 3 different mobile OSs of friends and family: phone book, recent received calls, recent placed calls, recent sent text messages, recently used mobile app. (4) Research: file systems--their function and usage. Disk operation. Attributes of various media: cd, flash drive, sd card, hard disk, floppy disk, RAM, ROM. (5) Research: other useful utilities, vendor offerings, history and future of forensics toolkit. (6) Research: important cases regarding digital evidence and procedure. Turning points. Unresolved issues.

METHODS OF EVALUATION:

Writing assignments

Percent of total grade: 35.00 %

Percent range of total grade: 25% to 50% Reading Reports, Workbook Exercises, Term or Other Papers

Problem-solving assignments

Percent of total grade: 35.00 %

Percent range of total grade: 25% to 50% Homework Reports, Workbook Exercises

Skill demonstrations

Percent of total grade: 15.00 %

Percent range of total grade: 15% to 25% Demonstration, Performance Exams

Objective examinations

Percent of total grade: 15.00 %

Percent range of total grade: 15% to 25% Multiple Choice, True/False, Matching Items, Completion

REPRESENTATIVE TEXTBOOKS:

Britz, Marjie T.. Computer Forensics and Cyber Crime: An Introduction, 4th Edition. New York, NY: Pearson Education, Inc.,2021.

ISBN: 9780134871110

Reading Level of Text, Grade: 12+ Verified by: Ellen Venable

Required Other Texts and Materials

flash drive, workbook manual

ARTICULATION and CERTIFICATE INFORMATION

Associate Degree:

CSU GE:

IGETC:

CSU TRANSFER:

Transferable CSU, effective 201130

UC TRANSFER:

Not Transferable

SUPPLEMENTAL DATA:

Basic Skills: N

Classification: Y

Noncredit Category: Y

Cooperative Education:

Program Status: 1 Program Applicable

Special Class Status: N

CAN:

CAN Sequence:

CSU Crosswalk Course Department:

CSU Crosswalk Course Number:

Prior to College Level: Y

Non Credit Enhanced Funding: N

Funding Agency Code: Y

In-Service: N

Occupational Course: C

Maximum Hours:

Minimum Hours:

Course Control Number: CCC000523120

Sports/Physical Education Course: N

Taxonomy of Program: 070700