GAVILAN COLLEGE
5055 Santa Teresa Blvd
Gilroy, CA 95023

Course Outline

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

TERM EFFECTIVE: Spring 2016 CURRICULUM APPROVAL DATE: 10/26/2015

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

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 CSIS 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
05 - Hybrid
72 - Dist. Ed Internet Delayed

STUDENT LEARNING OUTCOMES:

1. Student can identify, remove, and replace all major components of a typical personal computer.

Measure: performance exams

PLO:

ILO: 7

GE-LO:

Year assessed or anticipated year of assessment: 2014-2015

2. Student can perform basic file operations on Mac, Windows, UNIX.

Measure: homework, quiz, performance exam

PLO:

ILO: 7

GE-LO:

Year assessed or anticipated year of assessment: 2014-2015

3. Student can describe the most common network topologies and protocols and identify key hardware components or these topologies.

Measure: homework, quizzes

PLO:

ILO: 7,2, 3

GE-LO:

Year assessed or anticipated year of assessment: 2014-2015

4. Students can inventory files on disk, perform searches for specific files, and locate temporary files such as caches.

Measure: homework, quiz, performance exam

PLO:

ILO: 7,3,2

GE-LO:

Year assessed or anticipated year of assessment: 2014-2015

5. Students can describe the special requirements of chain of custody for digital evidence.

Measure: homework, quiz, exam

PLO: 1, 4, 5, 6

ILO: 1, 2, 3, 7

GE-LO:

Year assessed or anticipated year of assessment: 2014-2015

PROGRAM LEARNING OUTCOMES:

1) Reflect critically on developments in criminal justice policy and the relationship of these policies to the wider political and social environment.

2) Compare and evaluate diverse and competing arguments and analysis in disciplinary (justice system) and interdisciplinary contexts.

3) Demonstrate knowledge of the history, structure, and processes of law enforcement, the judicial system, correctional system, and the juvenile justice system.

4) Define and utilize key terms, concepts, and theories in the criminal justice system.

5) Interpret, assess and compare competing types of evidence and data.

6) Effectively communicate orally and in writing the results of their analysis and conclusions

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

Curriculum Approval Date: 10/26/2015

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): Ability to identify components, operating system, file system. Ability to boot into forensics toolkit.

OUT-OF-CLASS ASSIGNMENTS: Research & identify: component appearances, manufactures, connectors/cables, vendors.

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

OUT-OF-CLASS ASSIGNMENTS: 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).

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

OUT-OF-CLASS ASSIGNMENTS: 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.

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: Ability to boot forensics software and mount target disk for investigation. Usage of basic file system tools for examining contents of target drive.

OUT-OF-CLASS ASSIGNMENTS: Research: file systems--their function and usage. Disk operation. Attributes of various media: cd, flash drive, sd card, hard disk, floppy disk, RAM, ROM.

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

SPO: Ability to identify proper UNIX utility for a given situation. Ability to use each utility.

OUT-OF-CLASS ASSIGNMENTS: Research: other useful utilities, vendor offerings, history and future of forensics toolkit.

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

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

OUT-OF-CLASS ASSIGNMENTS: Research: important cases regarding digital evidence and procedure. Turning points. Unresolved issues.

2 Hours FINAL EXAM

METHODS OF INSTRUCTION:

Lecture, Computer demonstration, Lab workbook, Online documents and tutorials, Web research.

METHODS OF EVALUATION:

CATEGORY 1 - The types of writing assignments required:
Percent range of total grade: 35 % to 50
Reading Reports
Lab Reports
Term or Other Papers
CATEGORY 2 - The problem-solving assignments required:
Percent range of total grade: 35 % to 50 %
Homework Problems
Lab Reports
CATEGORY 3 - The types of skill demonstrations required:
Percent range of total grade: 15 % to 25 %
Class Performance/s
Field Work
Performance Exams
CATEGORY 4 - The types of objective examinations used in the course:
Percent range of total grade: 15 % to 25 %
Multiple Choice
True/False
Matching Items
Completion

REPRESENTATIVE TEXTBOOKS:

Required:
Britz. Computer Forensics and Cyber Crime: An Introduction. Prentice Hall, 2013. Or other appropriate college level text.
ISBN: 0132677717
Reading level of text, Grade: 12+ Verified by: ev
Other textbooks or materials to be purchased by the student: flash drive, lab 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: AJ
CSU Crosswalk Course Number: 184
Prior to College Level: Y
Non Credit Enhanced Funding: N
Funding Agency Code: Y
In-Service: N
Occupational Course: C
Maximum Hours: 3
Minimum Hours: 3
Course Control Number: CCC000523129
Sports/Physical Education Course: N
Taxonomy of Program: 210500