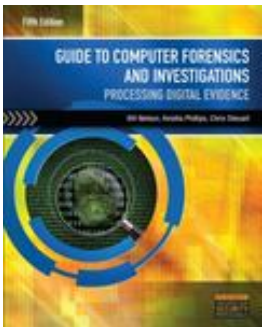
California State University
DOMINGUEZ HILLS

WWW.CSUDH.EDU

College of Natural and Behavioral Sciences
Department of Computer Science
http://csc.csudh.edu

COURSE TITLE:	Computer Forensics /Lab
COURSE NUMBER:	**CTC 328**
INSTRUCTOR NAME:	**MEHRDAD S. SHARBAF, PH.D. MSHARBAF@CSUDH.EDU, OFFICE: ROOM SAC1115, PHONE: 310-243-3398, OFFICE HOURS: TBA**
DATE:	FALL SEMESTER, 2016
COURSE LENGTH:	**_15_ WEEKS**
WEB COMPANION	**N/A**
BLACKBOARD WEB SITE	**HTTP://toro.csudh.edu**
COURSE SCHEDULE:	SAT → 12:30pm-4:45pm
UNIT OF ACADEMIC MEASUREMENT (SELECT ONE):	**___ QUARTER SYSTEM** **__X SEMESTER SYSTEM**
PREREQUISITES:	CSC 116 (INTRODUCTION TO COMPUTER HARDWARE & TOOLS) OR CONSENT OF INSTRUCTOR. STUDENTS SHOULD HAVE A WORKING KNOWLEDGE OF HARDWARE AND OPERATING SYSTEMS (OSS) TO MAXIMIZE THEIR SUCCESS ON PROJECTS AND EXERCISES THROUGHOUT THE COURSE.
COURSE DESCRIPTION:	This course presents methods 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. The course provides a range of laboratory and hands-on assignments that provides a balanced introduction to the theoretical and practical aspects of computer forensic investigation. Students will learn the basics of data acquisition, computer forensic analysis, e-mail investigations, image file recovery, and investigative report writing.

	TEXTBOOKS AND MATERIALS	(CHECK ONE)	
		REQUIRED	OPTIONAL (SUPPLEMENTAL)
TEXTBOOK (S)	 **GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS, 5TH EDITION** includes DVD **Bill Nelson** **Amelia Phillips, Christopher Steuart** **ISBN-10:** 1285060032 | **ISBN-13:** 9781285060033 752 Pages	✓	
References	HANDOUT	✓	
RESOURCES & SUPPLIES	An Internet browser (e.g. Internet Explorer), connection to the Internet. A storage device for your files (Flash Drive, writable CD, etc.).	✓	

PERFORMANCE OBJECTIVES:

Upon completion of this course, the student should be able to do the following:

- Define and demonstrate understanding of Computer Forensics
- Demonstrate understanding of enforcement agency investigations
- Demonstrate understanding of corporate investigations
- Understand what it means to maintain “professional conduct”
- Describe a search warrant
- Prepare a case
- Begin and execute an investigation

- Demonstrate understanding of data-recovery workstations and software
- Demonstrate understanding of file systems
- Explore Microsoft disk structures
- Examine New Technology File System (NTFS) disks
- Demonstrate understanding of Microsoft boot tasks
- Determine the physical layout of a Computer Forensics lab
- Select a basic forensic workstation
- Create forensic boot media
- Retrieve evidence data remotely using a network connection
- Use command-line forensics tools
- Explore forensics tools
- Explore Computer Forensics hardware
- Identify digital evidence
- Secure digital evidence at an incident scene
- Catalog digital evidence
- Store digital evidence
- Obtain a digital hash of a file, and use this to validate evidence

INSTRUCTIONAL METHODS:

- ✓ This course will be delivered through the use of lectures, presentations, demonstrations, discussions, and limited hands-on experience.
- ✓ Practice:

GRADING:

Student performance will be evaluated based upon the following criteria: Evaluation of the course will include any class assignments or deliverable exercises, and the projects. The instructor will supply the students with a full grading scheme at the beginning of the course.

Quizzes	**100**
Test I & II	**200**
Final Exam	**200**
Group Research Project Report	**200**
Group Project Presentation	**100**
Labs	**300**
Class Activity	**100**
Total:	**1200**

Grading Scheme:

96-100%	A	73-76%	C
90-95%	A-	70-72%	C-
87-89%	B+	67-69%	D+
83-86%	B	61-66%	D
80-82%	B-	< 60%	F
77-79%	C+		

COURSE POLICIES: **Late and Incomplete Deliverables:**

- Deliverables (Class Assignments, Projects) submitted late are not accepted.

- Deliverables (Class Assignment, Projects) not submitted before the end of the final class will earn 0%.
- Any exceptional, non-academic circumstances need to be discussed with the instructor as soon as they arise, prior to the due date of the deliverable. At the time of the discussion, NO make-up work will be assigned.
- The instructor reserves the right not to award credit for deliverables that are incomplete. Partial credit is awarded at the instructor's discretion, and only for work that merits such an award. Assignments that are incomplete or incongruous with the specifications may be returned to the student.

ATTENDANCE: Students are required to be prepared and attend all classes. The attendance policy is strictly enforced, and poor attendance may adversely affect your final grade due to class assignments. **Very Important Note:** Attendance is expected and required. The student is responsible for materials missed during an absence, whether excused or not. Excessive absences or tardiness will result in lowered grades.

MAKE-UP WORK: There will be no makeup or early examinations and late assignments will not be accepted.

ACADEMIC INTEGRITY: Academic integrity is of central importance in this and every other course at CSUDH. You are obliged to consult the appropriate sections of the University Catalog and obey all rules and regulations imposed by the University relevant to its lawful missions, processes, and functions.
All work turned in by a student for a grade must be student'' own work. Plagiarism and cheating (e.g. stealing or copying the work of others and turning it in as your own) will not be tolerated, and will be dealt with according to University policy. The consequences for being caught plagiarizing or cheating range from a minimum of a zero grade for the work you plagiarized or cheated on, to being dropped from the course.

ADA STATEMENT: Students with disabilities, who believe they may need an academic adjustment in this class, are encouraged to contact Disabled Student Services as soon as possible to better ensure receipt of timely adjustments.

QUIZZES: Quizzes will be given throughout the semester, at a rate of approximately 1 per chapter. Quizzes will always cover the material covered since the last Quiz or Exam. The quizzes will be combinations of objective and multiple choice questions. Makeup quizzes will not be given. However, the lowest quiz grade will be dropped. Any class material missed by the student is the student's responsibility to acquire.

MIDTERM & FINAL EXAM: Test is during the 8^{th}& 14^{th} week of the class and the date for the final exam is based on the final examination schedule printed in the campus Class Schedule. All projects are due no later than the last week of the semester.

Tentative Course Schedule

WEEK #	DATE	TOPIC	*Reading Assignment/ Computer Lab Topic/In Class Assignments*
Week 1	8/20/16	Course Introduction & Requirements/ Overview / Understanding the Digital Forensics Profession and Investigation	Chapter 1 /Hands-On Project for Lab
Week 2	8/27/16	The Investigator's Office & Laboratory/ Report Writing for High-Tech Investigations	Chapter 2&14/ Quiz 1/ Hands-On Project for Lab
Week 3	9/3/16	Data Acquisition	Chapter 3 /Quiz 2 / Hands-On Project for Lab
Week 4	9/10/16	Processing Crime & Incident Scenes	Chapter 4/Quiz 3/ Hands-On Project for Lab
Week 5	9/17/16	Working with Windows and DOS Systems	Chapter 5/Quiz 4/ Hands-On Project for Lab
Week 6	9/24/16	Current Computer Forensics Tools	Chapter 6/Quiz 5/ Hands-On Project for Lab
Week 7	10/1/16	Linux and Macintosh File Systems	Chapter 7/ Quiz 6/ Hands-On Project for Lab
Week 8	10/8/16	**Test I**	Covers Chapters 1-7/Lab Make Up
Week 9	10/15/16	Recovering Graphics Files	Chapter 8/ Hands-On Project for Lab
Week 10	10/22/16	Digital Forensics Analysis and Validation	Chapter 9/Quiz 7/ Hands-On Project for Lab
Week 11	10/29/16	Virtual Machines Forensics, Live Acquisition, and Network Forensics	Chapter 10/Quiz 8/ Hands-On Project for Lab
Week 12	11/5/16	E-mail and Social Media Investigations	Chapter 11/ Quiz 9/ Hands-On Project for Lab
Week 13	11/12/16	Expert Testimony in Digital Investigations	Chapter 15/ Quiz 10/ Hands-On Project for Lab
Week 14	11/19/16	**Test II**	Covers the Chapters after Midterm Exam 1, 8-11, and 15/Lab Make Up
	11/26/16	**Thanksgiving-NO Classes**	
Week 15	12/3/16	Group Research Project Report Presentation	***Due for Group Research Project Report,* Due for All the Lab Assignments**
Week 16	12/10/2016	**Final Exam Week**	**The Final Exam covers all chapters**

GO TOROS!

Research Paper Project

Your team (3-4 members) can choose any topic which is listed in this document. You will write a report and create a presentation on this project. . You will present in order by group number.

Your group must choose a topic by week four of the semester. Your professor must approve your topic so that duplicate presentations are avoided. Therefore, topics are approved on a first come, first served basis. You can email your topic or two or three to me, and I will let you know if that topic is still available.

Research paper project should follow the APA stylebook format.

- ✓ Cover page, and table of content with the title and group member's full names.
- ✓ Body of the report should be 10 to 12 pages double spaced with a 12 point font.
- ✓ At least **8 in-text citations** in APA Style (see the APA Style guide for format).
- ✓ At least **8 references** in APA Style (see the APA Style guide for format).

Example of Research Paper Project Sections (parts of the paper)

-Title Page
-Table of Contents
-List of Figures (Optional)
-List of Tables (Optional)
-Abstract (one page maximum)
-Introduction
-Multiple Sections on the Topic
-Conclusion
-References

Topics:

1.Solid-State Drives (SSDs): Build on the existing research concerning wear leveling, effects on hashing, recovery of data from unallocated space etc.
2.Policy: Various suggestions - a state-of-affairs review looking at past, present and future policy; triage; scenes of crime; report, seizure etc.
3.Use of Software Engineering Principles in Ensuring the Forensic Integrity of Digital Forensics Software and Results Produced: Involves looking at software engineering principles and methodologies and evaluating which one would be more suitable to digital forensics software development.
4. Database Reverse Engineering: Analysis of database file formats for forensic artefacts.
5. **Laboratory Accreditation ISO Standards**: A comprehensive study detailing how and why current laboratory standards (e.g. 9001 which focuses more on calibration for DNA and chromatography etc.) do or do not apply to the digital forensic arena would be valuable - especially for management
6. **Tamper-Resistant Communication Networks**: This would involve studying Tamper-Resistant Communication Networks such as the Plan R* network (and others that are far more advanced) and

creating either a methodology or a software solution to aid digital forensics investigators in analysing such networks.
7. **Cloud Storage Artefacts**: e.g. skydrive, idrive, etc.
8. **AI and Data-Mining**: This research project could revolve around the use of AI and data-mining principles and methodologies to extract data from multiple sources in search of evidence regarding a crime committed by a person or group of people.
9. **Database forensics**: The discipline is similar to computer forensics, following the normal forensic process and applying investigative techniques to database contents and metadata.
10. **Network Forensics:** Relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation
11. **Computer Forensics**: The goal of computer forensics is to investigate digital media in a forensically sound manner with the goal of identifying, preserving, recovering, analyzing and presenting facts and opinions about the information.
12. **Mobile Devices Forensics**: The phrase *mobile device* usually refers to mobile phones; however, it can also relate to any digital device that has both internal memory and communication ability, including PDA devices, GPS devices and tablet computers.
13. **Forensics Video**: is the scientific examination, comparison and/or evaluation of video in legal matters.
14. **Forensics Audio:** is the field of forensic science relating to the acquisition, analysis, and evaluation of sound recordings that may ultimately be presented as admissible evidence in a court of law.
15. **Verification and Validation***: Forensic regulation may change in the next few years with the formalisation of certain laboratory standards across not only countries but perhaps also continents. However, there is much work to be done formalising the details in relation to the verification and validation of hard disk data recovery software, mobile phone software, hardware write blockers, etc.

Computer Forensics Research Databases

1

ABI/INFORM Complete
ABI/INFORM has more than 3,800 worldwide business periodicals on accounting, advertising, business, economics, finance, human resources, law, management, marketing, taxation and other related subjects. Includes: Barron's, Business Week, The Economist, Financial Times, Forbes, Fortune, Harvard Business Review, Institutional Investor, Wall Street Journal and many more.

2

Academic Search Complete
Academic Search Complete is a multi-disciplinary full-text database, with more than 8,500 full-text periodicals, including more than 7,300 peer-reviewed journals. In addition to full text, this database offers indexing and abstracts for more than 12,500 journals and a total of more than 13,200 publications including monographs, reports, conference proceedings, etc. The database features PDF content going back as far as 1887, with the majority of full text titles in native (searchable) PDF format. Searchable cited references are provided for more than 1,400 journals.

3

Business Abstracts with Full Text (H.W. Wilson)
Business Abstracts with Full Text contains the full text of articles from more than 510 publications dating back to 1995, and provides access to product evaluations, interviews, biographical sketches, corporate profiles, obituaries, surveys, statistical rankings, book reviews and reports from associations, societies, trade shows,

conferences and more.

4

Business Source Complete
More than 4,300 business periodicals (3,200 full text) covering all disciplines of business, including marketing, management, MIS, POM, accounting, finance and economics. Indexing and abstracts for scholarly business journals as far back as 1886. In addition, searchable cited references are provided for more than 1,300 journals. Includes: Business Week, Economist, Forbes, Fortune, Harvard Business Review, Institutional Investor, Wall Street Journal and many more. Also includes financial data, case studies, investment research reports, industry reports, market research reports, country reports, company profiles and SWOT analyses.

5

Cambridge Journals Online
Full text of over 250 journals published by Cambridge University Press, in a range of academic subjects including the sciences, religious studies, humanities, and social sciences. Content available for many journals back to 1996.

6

Emerald Journals
Emerald is a long established publisher with over 200 titles in the fields of management, information science and engineering.

7

IEEE Xplore
Full text access to technical literature in electrical engineering, computer science, and electronics. Includes access to the abstract records and full text articles published since 1988 with select content published since 1893 from IEEE journals, transactions, and magazines as well as conference proceedings. Also includes current and archived IEEE standards. LMU's subscription does not include online access to the full text of IEEE books.

8

Oxford Handbooks Online
The complete texts of Oxford Handbooks in Business and Management, Philosophy, Political Science, and Religion.

9

ProQuest Research Library
Index to over 4,560 scholarly and popular titles in all subjects; includes over 3,240 titles in full text. Content includes scholarly journals, trade publications, magazines, and newspapers. Coverage varies by title, but some have full text dating back as far as the early 1970s.

10

SAGE Journals Online
Full-text access to all SAGE journals; over 560 titles in Business, Humanities, Social Sciences, and Science, Technology and Medicine. Coverage dates vary; some titles are available in full-text for the full run of the journal.

11

ScienceDirect
ScienceDirect's database covers titles from the core scientific literature, including titles such as THE LANCET, Cell and Tetrahedron. More than 2,000 journals and more than

nine million full-text articles are available in ScienceDirect.

12

SpringerLink
SpringerLink is an integrated full-text database for journals, books, protocols, eReferences, and book series published by Springer. SpringerLink currently offers more than 1,800 fully peer-reviewed journals online. SpringerLink offers access to search, tables of content, abstracts, and alerting services.

13

ACM Digital Library
Full-text database of the complete collection of ACM's publications. Includes access to The ACM Guide to Computing Literature bibliography.

.:: Journals ::.

Name: Digital Evidence and Electronic Signature Law Review
URL: http://www.deaeslr.org/

Name: Digital Forensics Magazine
URL: http://www.digitalforensicsmagazine.com/

Name: International Journal of Digital Evidence
URL: http://www.utica.edu/academic/institutes/ecii/ijde/

Name: Journal of Digital Forensics Practice
URL: http://www.informaworld.com/smpp/title~content=t716100764

Name: The International Journal of Digital Forensics & Incident Response
URL: http://www.elsevier.com/wps/find/journaldescription.cws_home/702130/description#description

---

Name: The Journal of Digital Forensics, Security and Law
URL: http://www.adfsl.org/journal.htm

Some of the topics for the research are excerpted from http://www.forensicfocus.com/