

IS 6363 Computer Forensics Spring 2006

Class Information:

Class Time: 5:30-6:45 p.m. Tue/Thu

Class Location: BB 3.03.10

Lab Location & Hours: BB 3.03.10 (Hours as posted. Should mirror APL hours.)

Instructor Information:

Nicole Beebe, PhD student

Office: BB 4.04.02 (desk in back corner of room)

Phone: 458-6299 (Cell: 269-5647)

Email: nicole.beebe@utsa.edu; or WebCT email

Office hours: 7:00 – 8:00 p.m. T/Th or by appointment

Prerequisites: IS 6303 – Introduction to Voice & Data Security

A basic understanding (introductory education) of hardware, software (operating systems, file systems, Windows™, and basic Linux commands), and networking, however, is recommended. While students will be taught what they need to know in these areas during the course, those with little familiarity of such concepts will have to spend more time outside of class reading and learning to keep up.

Course Overview & Objectives:

This is an introductory course in collecting, examining, and preserving digital evidence in support of criminal investigations, civil investigations, and sensitive business matters. The course examines the issues, tools, techniques, and processes needed to successfully prepare for, respond to, and investigate such matters. Students will receive a broad understanding of the entire cyber forensics discipline and will explore the following topics:

- The need for cyber forensics in criminal & civil investigations and in business
- Types of computer crimes, cyber threats, and digital evidence
- Legal & ethical issues involved in conducting cyber forensic investigations
- How businesses & police prepare for, detect, and respond to incidents, including basic crime scene processing
- Tools & techniques for proper evidence preservation & collection
- Tools & techniques for cyber forensic investigations & examinations
- Basic file systems, computer data storage processes, etc.

Because this course is not cross-listed with IS 4483 (its undergraduate equivalent), nor is IS 4483 a prerequisite course, a significant portion of the material in both courses will overlap. However, because this is a *graduate level* cyber forensics course, we will cover more material overall. Students will be expected to gain more understanding through reading, homework assignments, and basic self-study than at the undergraduate level. Also, you should attain a higher level of understanding (i.e. concept integration and application) than at the undergraduate level.

Course Assignments, Evaluation, and Grading:

Students will be graded and evaluated as follows:

In-Class Exercises & Homework Assignments: 30% (weighted equally; two dropped)

Exams: 30%

Exam 1: 10%

Exam 2: 10%

Final Exam: 10%

Group Projects: 40% (project milestones graded throughout semester)

Digital Forensic Case

Create & document scenario (5%)

Create evidence drive (10%)

Conduct analysis, write report, give presentation (15%)

Cell Phone Forensic Analysis Report (10%)

Exams. There will be three in-class, scheduled exams. The exams will consist short answer essay questions, along with multiple choice, true/false, etc. Students will take the exam via WebCT *in-class*. Exam #3 will be administered during the final exam time (!!No Exceptions!!) and will be comprehensive in nature. Exam #3 is optional for students who have averaged an 'A' (90% or higher) on all other graded items and who have completed all of the homework assignments (regardless of two grades being dropped).

In-Class Exercises & Out-of-Class Assignments. There will also be several in-class exercises, as well as out-of-class homework assignments. All assignments and exercises will be relatively short and practical ("hands-on") in nature. In a class such as this, practical experience (i.e. experiential learning) is absolutely vital to understanding the material. Out-of-class assignments are shown on the syllabus. In-class exercises will occur at the discretion of the instructor and may be unannounced. All exercises and homework assignments will be handed in during class and graded on four-point scale (1=minimal apparent effort; 2=apparent effort, but inadequate demonstration of concept comprehension; 3=apparent effort with good comprehension/accuracy; 4=excellent effort/comprehension/accuracy). Correct answers to assignments will either be provided and discussed in class, or posted on WebCT as appropriate. Students will have access to the IS department lab to complete the assignments.

Group Projects.

(1) Digital Forensic Case. Students will participate in one semester-long group project, wherein they will create an evidentiary hard drive and subsequently analyze one created by another student group. In doing so, the students will apply and integrate what they have learned during the course. The project will have three graded milestones during the course of the semester. The project will culminate with both a written paper and an oral presentation in front of the class. Both products (written paper and group project) will be a group effort. After the project is complete, each student will evaluate their teammates' contribution to the project. Each individual's grade on the group project will be a combination of the group project grade and their individual contribution to the effort, as rated by their peers. Further guidance for the group project & presentation will be provided during class.

(2) Cell Phone Forensic Analysis. Students groups will analyze a cell phone (one of their personal cell phones were possible) using specialized digital forensic hardware/software. Each group will prepare and submit a report of findings.

Course Philosophies and Policies:

- **Learning** – First and foremost, the instructor is committed to student learning and students achieving the stated objectives in this course. If you have any problem(s) that might impede your performance in this course, please bring it to the attention of the instructor immediately.
- **Attendance & Class Participation**– Class attendance is absolutely essential for success in this course, however, attendance will not be taken. Each student is expected to attend all classes and come prepared to participate fully in class discussions and exercises. This means all reading and

homework assignments must be completed prior to class on the days they are due. Without such preparation, class discussions and exercises will suffer, as will your understanding of the material. Additionally, there will be unannounced in-class exercises. Your absence or inability to perform adequately on these exercises, either through lack of preparation (i.e. keeping up) or absence, will result in low (or zero) grades. No make-ups will be permitted with respect to in-class exercises. Understanding that illnesses, transportation issues, etc. often arise during the normal course of a semester, everyone will be permitted to drop their two lowest in-class exercise & out-of-class assignment grades. Special circumstances necessitating further, special consideration will be considered on a case-by-case basis. Such circumstances should be brought to the instructor's attention as soon as possible (i.e. before they occur whenever possible).

- **Late Assignments** – All assignments are due during class on the due date. Late assignments turned in the *next* class period after they were due will receive a maximum grade of 2. Assignments later than that will not be accepted. Late group project papers (turned in the *next* class period after it was due) will be dropped an entire grade (e.g. a paper graded as 95% will receive a recorded grade of 85% for being late). Papers later than that will not be accepted.
- **Absences** – If you miss a scheduled exam for **valid** non-academic reasons listed below, your average grade on the remaining exams will be used to substitute for the missed exam (and Exam #3 will no longer be optional). A make-up final (exam #3) will only be given under extremely special circumstances, at the discretion of the instructor. No make-up exam or grade substitution will be given unless the instructor is notified of your situation **prior** to the scheduled exam. Examples of valid non-academic reasons:
 - Serious illness documented with a note from a doctor. (Note: The UTSA clinic does not provide such notes.)
 - Business trip documented with a note from your supervisor.
 - Death in family documented with a note from a parent.
 - Accident documented with a note from a law enforcement officer.
- **Withdraws** – A "W" grade will be assigned if a student withdraws before March 28, 2006.
- **Incompletes** – Students who, for non-academic reasons beyond their control, are unable to meet the full requirements of the course should notify the instructor. Refer to catalog for details on Incomplete Grades.
- **Scholastic Dishonesty** – “Scholastic dishonesty includes, but is not limited to cheating, plagiarism, collusion, the submission for credit of any work or materials that are attributable in whole or in part to another person, taking an examination for another person, any act designed to give unfair advantage to a student or the attempt to commit such acts” (UTSA Handbook of Operating Procedures, section 2.37). Such dishonesty is NOT excusable under ANY circumstances. Your instructor places an *extremely* high importance on honesty and integrity and will take all occurrences very seriously. At a minimum, the student will receive a failing grade for the assignment or exam in question. In many cases, the wrong-doing will be formally reported, investigated, and handled through university channels. Scholastic dishonesty can result in expulsion from the university. Think twice before doing it!
- **Respect** – Successful learning requires respect—respect by the instructor for the students, respect by the students for the instructor, and respect by the students for each other. Respect is demonstrated by participating, listening, sharing. Respect does not require agreement with one another, but rather requires that the disagreement is delivered in a polite, measured way. Respect also includes considerate behavior that facilitates, rather than hinders teaching and learning. Examples of *non*-considerate behavior include: use of cell phones, pagers, and other communication devices during class, listening to headphones, eating, the use of computers for anything other than class-related note-taking, making noise packing/unpacking stuff, etc.

Readings:

Required Textbook s:

Carrier, Brian, *File System Forensic Analysis*, Addison-Wesley, 2005, pgs 569. (ISBN 0-32-126817-2)

Mandia, Kevin, Prorise, Chris, and Pepe, Matt, *Incident Response & Computer Forensics 2nd Ed.*, McGraw-Hill/Osborne, Emeryville, 2003, pgs 507. (ISBN 007222696X)

Additional Required Reading (tentative list) (will be posted on WebCT):

Beebe, Nicole Lang, and Jan Guynes Clark, "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process," *Digital Investigation* (2:2) 2005, pp 146-166

Rowlingson, Robert "A Ten Step Process for Forensic Readiness," *International Journal of Digital Evidence* (2:3), Winter 2004, pp 1-28 (www.ijde.org)

Lecture Notes posted on WebCT for various subjects (all may not be listed in syllabus)

Supplemental (Not Required) Reading & Information:

Casey, Eoghan and Palmer, Gary *Digital Evidence and Computer Crime* (Second ed.) Elsevier Ltd, London, 2004

Brown, Christopher L. T. *Computer Evidence: Collection and Preservation* Thompson, NY, 2005

DoJ "Electronic Crime Scene Investigation - A Guide for First Responders," U.S. Department of Justice, pp. 1-82 (<http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm>)

Website: <http://computer.howstuffworks.com/>

White, Ron and Downs, Timothy *How Computers Work* (Seventh ed.) Que, 2003, p 416

Casey, Eoghan "Practical Approaches to Recovering Encrypted Digital Evidence," *International Journal of Digital Evidence* (1:3), Fall 2002, pp 1-26

Curran, Kevin, and Bailey, Karen "An Evaluation of Image Based Steganography Methods," *International Journal of Digital Evidence* (2:2), Fall 2003, pp 1-40

Course Schedule*:

Date	Topic(s)	Assigned Readings Due	Out-of-Class Assignments & Project Milestones Due
8/24	Course Intro		
8/29	Digital Forensics Intro (Group project overview)	Beebe/Clark, pg 1-6,9-23 Carrier Ch.1	
8/31	"Investigations 101" (Hand out project material)		
9/5	Computer Foundations	Carrier Ch.2 (Mandia Ch.10 = supplemental)	
9/7	Volume Analysis & PC-based Partitions	Carrier Ch.4/5 (pgs 69-101)	HW: "Elements of Proof" (HW=Homework assignment)
9/12	File System Analysis	Carrier Ch.8	
9/14	FAT	Carrier Ch.9/10	GP: Scenario documentation (GP=Group Project Assignment)
9/19	NTFS Concepts & Data Structures	Carrier Ch.11/13	

9/21	NTFS Analysis	Carrier Ch.12 Mandia Ch.12, pg 308-312 Mandia Ch.11, pg 275-277 Mandia Ch. 12, pg 315-316	HW: "Deleted File Recovery"
9/26	Carving & Signature Analysis Hashing & Hash Analysis	Mandia Ch.11, pg 268-271	
9/28	Web browsing artifacts	Mandia Ch.12, pg 317-319	
10/3	Email Artifacts	Mandia Ch.12, pg 307-308	HW: "Carving/Signature Analysis" HW: "Hashing/Hash Analysis"
10/5	Keyword searching	Mandia Ch.11, pg 282-289	HW: "Web Browsing Analysis"
10/10	Exam #1		HW: "Email Recovery/Analysis"
10/12	Law, legal issues, & ethics	Lecture Notes Mandia Ch.3, pg 57-62	
10/17	Evidence collection	Mandia Ch.9 Carrier Ch. 3	GP: Evidence drive
10/19	Forensic imaging (Assign evidence drives)	Mandia Ch.7, Ch.11 pg 240-243	
10/24	Preparation phase	Article by Rowlingson Mandia Ch.3, pg 33-56/63-73	HW: "Controlled Boot Disk"
10/26	Incident response phase	Mandia Ch.4	HW: "Forensic Duplication"
10/31	Business policy for digital forensics & incident response	Lecture Notes	
11/2	Developing a digital forensics capability		
11/7	Cell phone forensics (IDEA Survey)	Lecture Notes	
11/9	Cell phone forensics (cont.)		HW: "Business Policy"
11/14	Findings presentation phase & Incident closure phase	Mandia Ch.17	
11/16	Catch-up (lecture, labs, etc.)		GP: Cell Phone Analysis Report
11/21	Exam #2		
11/23	THANKSGIVING		
11/28	Group Presentations		GP: Report of Findings
11/30	Group Presentations		
12/5	STUDY DAY		
12/12	EXAM #3 (5:00-7:45 pm)		

* This syllabus provides a general plan for the course; deviations may be necessary.