

Georgia State University  
Department of Computer Information Systems

## Course Syllabus

### CIS8630

(CRN xxxxx)

Business Computer Forensics and Incident Response

Spring 2010

#### Instructors :

Name	Richard Baskerville
Office	RCB Building, 35 Broad Street, 919
Office Hours	Thursdays, 1.30 pm – 3.30 pm, or by appointment
Office Phone	(404) 413-7362
Office Fax	(404) 413-7394
Email	baskerville@acm.org

#### Venue

TBA

#### Prerequisites

CIS 8080 or ACCT 8680  
CSP 1, 6, 7.

#### Required Materials

Computer storage media, such as 3.5” floppy disks, thumbsticks, blank data CDs, etc. as described in labs.

#### Readings

- Bunting, S. *EnCase Computer Forensics--The Official EnCE: EnCase Certified Examiner Study Guide* Wiley Publishing, Indianapolis, 2008.
- Rowlingson, R. "A Ten Step Process for Forensic Readiness," *International Journal of Digital Evidence* (2:3) 2004, pp 1-28.
- Luoma, V.M. "Computer forensics and electronic discovery: The new management challenge," *Computers & Security* (25:2) 2006, pp 91-96.
- Volonino, L., Anzaldua, R., and Godwin, J. *Computer Forensics: Principles and Practices* Pearson Education, Upper Saddle River, New Jersey, 2007.
- Volonino, L., Sipior, J. C., & Ward, B. T. (2007). Managing the Lifecycle of Electronically Stored Information. *Information Systems Management*, 24(3), 231-238.

## Catalog Description

This course provides a strategic exploration into the prevention and response to intentional abuse of business information systems. This abuse frequently leads to diversion of resources, interruptions of service and corruption of data that develops into a variety of losses that can seriously impair an organizations performance. Students will be prepared to plan and manage organizational incident and forensics preparedness, including information security policies, information controls, information practices, incident response plans, forensic readiness, and preservation of evidence in the form of electronically stored information. The course includes experiments in the use of forensics tools for investigation of organizational policy violations.

## Course Objectives

Through successful completion of this course, students will develop abilities to

1. Explain the organizational relationship between activities directed toward policy enforcement, computer forensics, data recovery, incident response, and privacy protection.
2. Plan strategies for information systems control governance and policy enforcement.
3. Plan strategies for organizational readiness for computer incident response such that collection, preservation, presentation and preparation of computer-based evidence will optimally satisfy the requirements of business continuity, criminal law enforcement and civil litigation.
4. Create and evaluate organizational information services policies for incident response and business continuity.
5. Evaluate at both strategic and technical levels the organization's computer incident response systems, architecture, and staff capabilities.
6. Plan, organize, and manage an organization's computer incident response processes and computer forensics investigation processes.
7. Explain the ethical, technical and economic rationale for specific organization information systems incident response and forensic capabilities.
8. Detect typical forms of computer crime and abuse and recognize/preserve the relevant evidence.

## Special Considerations

Sharepoint and/or the course web site may be used as a repository for examples of course problems, model solutions, examples of projects, and further required course material that arises during the class. Students must arrange for their own access to a homework computer and the World Wide Web (Internet access is available free in the GSU labs). All student work submitted in fulfillment of course requirements is deemed to be granted in the public domain (copyright-free) for the purposes of use as instructional material or examples of student work in future courses. Constructive assessment of this course by students plays an indispensable role in shaping education at Georgia State. Upon completing the course, students are asked to take the time to fill out the online course evaluation. The course syllabus provides a general plan for the course. Deviations may be necessary.

## Method of Instruction

Classroom sessions will regard the same topics as the readings assignments, but seek further depth through discovery learning. It is essential that students read the assigned material before

coming to class. Instruction will follow these three approaches: (1) topic discussion of course concepts, (2) interaction with professional experts that will allow students to contextualize computer forensics concepts in actual business settings, and (3) in-class and homework lab activities that apply these concepts to simulated computer forensics investigative situations. A forensics study center with specially equipped forensics workstations is available in the CIS department for homework assignments. Preparation is essential and all students are required to have read the assigned readings. Individuals may be “cold called” to introduce a topic or to initiate discussion. In assigning the participation grade, both class attendance and the quality of oral contributions during class discussions will be considered.

### **Class Attendance Policy**

Roll will not be taken on a regular basis. It is the student’s responsibility to attend class, obtain assignments, and turn in work on time. Absence from class does not relieve you of any of these responsibilities. One absence will be considered excused if it is due to an emergency, a religious holiday, or some other extenuating circumstance. Please notify the instructor in advance if possible. Unless an absence is excused, students will NOT be allowed to make up missed work. Further absences may impact a student’s grade due to missed in-class activities.

### **Flicker and Noise Distractions**

By continued enrollment in this class, students agree to practice a “click-free”, “flicker-free” and “noise-free” environment for fellow students in this classroom. Students agree that mobile devices such as telephones, pdas, Blackberries, etc. will be silenced and unused during class. Students agree to forebear from the use of computers during the class for email, web-surfing, gaming, etc.

### **Withdrawals**

Students who withdraw by October 15 will receive a grade of W. Students withdrawing after this date will receive a grade of WF unless a hardship authorization is obtained from the Dean of Students.

### **Incompletes**

A grade of I will be given only in exceptional circumstances. A student must have completed all but one of the requirements of the course in order to be eligible to receive a grade of I.

## Grading Policy

Activity	Points Available
Labs and Cases :	20%
Forensics Project:	20%
Quizzes:	40%
Class Participation:	20%
Total:	100%

Letter Grade	Percentage Range
A+	101% - Higher
A	90% - 100%
A-	87% - 89%
B+	83% - 86%
B	80% - 82%
B-	77% - 79%
C+	73% - 76%
C	70% - 72%
C-	67% - 69%
D	60% - 66%
F	0% - 59%

## Academic Honesty

*(Abstracted from GSU's Student Handbook Student Code of Conduct "Policy on Academic Honesty and Procedures for Resolving Matters of Academic Honesty" -<http://www.gsu.edu/~wwwcam/code/academicconduct/intro.html> )*

As members of the academic community, students are expected to recognize and uphold standards of intellectual and academic integrity. The University assumes as a basic and minimum standard of conduct in academic matters that students be honest and that they submit for credit only the products of their own efforts. Both the ideals of scholarship and the need for fairness require that all dishonest work be rejected as a basis for academic credit. They also require that students refrain from any and all forms of dishonorable or unethical conduct related to their academic work.

Students are expected to discuss with faculty the expectations regarding course assignments and standards of conduct. Here are some examples and definitions that clarify the standards by which academic honesty and academically honorable conduct are judged at GSU.

*Plagiarism.* Plagiarism is presenting another person's work as one's own. Plagiarism includes any paraphrasing or summarizing of the works of another person without acknowledgment, including the submitting of another student's work as one's own. Plagiarism frequently involves

a failure to acknowledge in the text, notes, or footnotes the quotation of the paragraphs, sentences, or even a few phrases written or spoken by someone else. The submission of research or completed papers or projects by someone else is plagiarism, as is the unacknowledged use of research sources gathered by someone else when that use is specifically forbidden by the faculty member. Failure to indicate the extent and nature of one's reliance on other sources is also a form of plagiarism. Failure to indicate the extent and nature of one's reliance on other sources is also a form of plagiarism. Any work, in whole or part, taken from the Internet or other computer based resource without properly referencing the source (for example, the URL) is considered plagiarism. A complete reference is required in order that all parties may locate and view the original source. Finally, there may be forms of plagiarism that are unique to an individual discipline or course, examples of which should be provided in advance by the faculty member. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly or creative indebtedness, and the consequences of violating this responsibility.

*Cheating on Examinations.* Plagiarism is presenting another person's work as one's own. Plagiarism includes any paraphrasing or summarizing of the works of another person without acknowledgment, including the submitting of another student's work as one's own. Plagiarism frequently involves a failure to acknowledge in the text, notes, or footnotes the quotation of the paragraphs, sentences, or even a few phrases written or spoken by someone else. The submission of research or completed papers or projects by someone else is plagiarism, as is the unacknowledged use of research sources gathered by someone else when that use is specifically forbidden by the faculty member. Failure to indicate the extent and nature of one's reliance on other sources is also a form of plagiarism. Failure to indicate the extent and nature of one's reliance on other sources is also a form of plagiarism. Any work, in whole or part, taken from the Internet or other computer based resource without properly referencing the source (for example, the URL) is considered plagiarism. A complete reference is required in order that all parties may locate and view the original source. Finally, there may be forms of plagiarism that are unique to an individual discipline or course, examples of which should be provided in advance by the faculty member. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly or creative indebtedness, and the consequences of violating this responsibility.

*Unauthorized Collaboration.* Submission for academic credit of a work product, or a part thereof, represented as its being one's own effort, which has been developed in substantial collaboration with assistance from another person or source, or computer honesty. It is also a violation of academic honesty knowingly to provide such assistance. Collaborative work specifically authorized by a faculty member is allowed.

## Course Schedule

(Subject to change)

Week	Date	Lesson Topic	Readings	Activities	Visiting Experts
1	23-Aug	Introduction: Policy Enforcement, Computer Forensics, Data Recovery, Incident Response and Privacy Protection	Volonino Ch 1		William Monahan, Georgia State University
2	30-Aug	Data Representation	"Binary Numeral System" "Hexidecimal" "ASCII"	Lab #1: Base conversions	
3	6-Sep	Basic computer storage technology	Bunting Ch 1 & 2 Volonino Ch 5, 6 & 7		
4	13-Sep	Basic computer systems software architecture	Bunting Ch 1 & 2 Volonino Ch 5, 6 & 7		
5	20-Sep	Computer Forensics Tools	Volonino Ch 2	Quiz #1	Rick Austin, Kennesaw State University
6	27-Sep	Evidence Acquisition with EnCase	Bunting Ch 4 & 5	Lab #2	
7	4-Oct	GREP and Regular Expressions	Regex Quickstart	Lab #3	
8	11-Oct	Analyzing Evidence with EnCase	Bunting Ch 6-9	Lab #4	
9	18-Oct	Report Development with EnCase	Bunting Appendix A	Lab #5	
10	25-Oct	Policy Enforcement	Volonino Ch 4 & 11	Rolling Case #1	Jonathan Jacobs US Secret Service
11	1-Nov	Incident Response	Bunting Ch 3 Volonino Ch 10	Rolling Case #2	
12	8-Nov	E-Discovery	Luoma Voloninoonino, Sipior & Ward	Rolling Case #3	Scott Vincent, Lockheed Martin
13	15-Nov	Email and Network Forensics	Volonino Ch 8	Quiz #2	
14	22-Nov	Thanksgiving Holiday			
15	29-Nov	Expert Testimony and Forensic Readiness	Rowlingson Volonino Ch 12 & 13		Mark Moore, Coca-Cola
16	6-Dec	Student Presentations			

