Course Syllabus

CIS8630
(CRN 16433)
Business Computer Forensics and Incident Response

Spring 2014
(Version 3.0 5 February 2014)

Instructors :

Name        Richard Baskerville
Office       RCB Building, 35 Broad Street, 919
Office Hours Wednesdays, 1.00 pm – 3.00 pm, or by appointment
Office Phone (404) 413-7362
Office Fax   (404) 413-7394
Email        baskerville@acm.org

Lab Assistant

Name        Mala Kaul
Office       RCB Building, 35 Broad Street, 9th Floor
Office Hours TBA, or by appointment
Phone        (404) 413-7390
Email        mkaul1@gsu.edu

Venue
Thursday 5.30 – 9.45 pm, Room 601

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

Required Materials
A laptop computer and portable computer storage media, such as USB memory thumbsticks,
blank data CDs, etc. as described in labs. See special considerations.

Course Web Site: http://www.cis.gsu.edu/rbaskerville/cis8630/index.html
Most course readings will be available via GSU library subscriptions or from the course web site. The exception is the iPremier HBR case study (3 files) that must be downloaded directly from Study.Net. The download link for this case is:

http://www.study.net/r_mat.asp?crs_id=30041467

See “Readings” below for a complete list of required reading material.

**Readings**


**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 organization's 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**

The course website, and/or Desire2Learn may be used as a repository for required course material that arises during the class. Students must arrange to bring a wireless Internet laptop to each class, and for 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 computer laboratory work, discussion, and 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 and assigned readings, (2) interaction with professional experts that will allow students to contextualize incident response and 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 except for note-taking and reference to course materials. Students agree to forebear from the use of computers during the class for email, web-surfing, gaming, etc.

**Withdrawals**

Students who withdraw before the midpoint 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. For the exact midpoint date see [http://calendar.gsu.edu/calendar](http://calendar.gsu.edu/calendar).

**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.

**Assessment**

Learning objectives will be assessed by both individual and group performance through the following course features:

* **Labs**
  The course will include lab assignments to be completed by individual students either during class or outside of class. The lab assignments are based on Virtual Machines running EnCase, which can be used during class or by remote access outside of class. Remote access times are sometimes shared with other forensics students, and may only be available during certain assigned times. The CIS Forensics Study Center is located on the 9th floor of the RCB Building, and has additional workstations available on a first-come, first-served basis.

* **Discussions**
  The course will include in-class discussions of the topics outlined in the schedule. These discussions include three cases: (1) Omega Engineering, (2) iPremier, and (3) Bank Solutions.
Students will have individual opportunities to contribute thoughtful and critical oral observations during class discussions focused on the course objectives. There will be readings assigned for most class meetings. Students will have opportunities during the semester to introduce and comment on these readings during in-class discussions. Outside of class meeting times, there will also be opportunities for course-related discussions online using an email group server, wiki pages, and/or online social networking.

**Team Activities**
Some course activities will be organized as teamwork. These include: (1) RollingCat case, and (2) The testimony tournament. Assessment of performance in the RollingCat may be pass/fail. The testimony tournament assessment is generally based on the ability of individual students to sustain challenges to the quality of the knowledge developed by their team’s forensics analysis of the RollingCat case. This activity will be competitive, and “bonus” credit may be awarded to winning teams. These activities are further described in the activity descriptions distributed in advance of the activities.

Students will form self-managing teams for the purpose of completing team activities. Each team is expected to persist through the course. Peer appraisals will be part of the overall grading/evaluation of individual performance. Consensus on the relative contributions of each of the team members will be derived through assessment of documented facts and records, evaluation of team output, and evaluation of team processes. Unless team members inform the instructor in writing to the contrary, the assumption will be that each team member contributed equally to the assessed products of the team.

**Quizzes**
There will be two short objective quizzes that assess individual familiarity with the principles and readings: (1) E-Discovery and Evidence, and (2) Incident Response and Forensics. Students will actively participate in the construction and evaluation of these quizzes.

**Grading Policy**

<table>
<thead>
<tr>
<th>Activity</th>
<th>Points Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Labs</td>
<td>25</td>
</tr>
<tr>
<td>Team activities</td>
<td>25</td>
</tr>
<tr>
<td>Quizzes</td>
<td>25</td>
</tr>
<tr>
<td>Discussion Participation</td>
<td>25</td>
</tr>
<tr>
<td>Total:</td>
<td>100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Letter Grade</th>
<th>Percentage Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>96% - Higher</td>
</tr>
<tr>
<td>A</td>
<td>90% - 95%</td>
</tr>
<tr>
<td>A-</td>
<td>87% - 89%</td>
</tr>
<tr>
<td>B+</td>
<td>83% - 86%</td>
</tr>
<tr>
<td>Letter Grade</td>
<td>Percentage Range</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>B</td>
<td>80% - 82%</td>
</tr>
<tr>
<td>B-</td>
<td>77% - 79%</td>
</tr>
<tr>
<td>C+</td>
<td>73% - 76%</td>
</tr>
<tr>
<td>C</td>
<td>70% - 72%</td>
</tr>
<tr>
<td>C-</td>
<td>67% - 69%</td>
</tr>
<tr>
<td>D</td>
<td>60% - 66%</td>
</tr>
<tr>
<td>F</td>
<td>0% - 59%</td>
</tr>
</tbody>
</table>

**Academic Honesty**


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)

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Discussion Topic</th>
<th>Readings</th>
<th>Forensic Lab Activities</th>
<th>Visiting Experts</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>16-Jan</td>
<td>E-Discovery (Dysart, 2011) (Baskerville, 2010)</td>
<td>Bunting Ch 1,2 Lab #2: File Systems &amp; Virtual Machines</td>
<td>Jeff Ruetten, eMag Solutions*</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>23-Jan</td>
<td>Evidence (Barker et al., 2009)</td>
<td>Bunting Ch 4 Lab #4: EnCase Workshop</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>23-Jan</td>
<td>Investigations (Glisson et al., 2011)</td>
<td>Bunting Ch 6 Lab #5: Search &amp; GREP</td>
<td>Richard Austin, Hewlett Packard (Cancelled)</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>30-Jan</td>
<td>Case: Omega Engineering (McCrea, 2008)</td>
<td>Bunting Ch 7 Lab #6: Password Cracking</td>
<td>Scott Vincent, Lockheed Martin*</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>30-Jan</td>
<td></td>
<td>Bunting Ch 9 Lab #7: Steganography</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>6-Feb</td>
<td>Quiz #1</td>
<td>Bunting Appendix B Lab #8: EnCase Reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>13-Feb</td>
<td>Case: iPremier (Austin et al., 2007)</td>
<td>RollingCat Case #1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>13-Feb</td>
<td>Incident Response Network Forensics (Werlinger et al., 2010) (Ahmad et al., 2012)</td>
<td>RollingCat Case #2</td>
<td>Charlie Britt &amp; Peter Lester, PriceWaterhouseCoopers*</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>20-Feb</td>
<td>Expert Testimony Windows Artifacts (Lim, 2008)</td>
<td>RollingCat Case #3</td>
<td>Dave McDonald, GSU (8.15-9.45)*</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>20-Feb</td>
<td>Quiz #2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>27-Feb</td>
<td>Case: Bank Solutions Student Team Web Presentations (Camara et al., 2011)</td>
<td>Testimony Tournament</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>27-Feb</td>
<td>Student Team Web Presentations</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>