



Department of Engineering Technology

The Practice of Digital Forensics DIG 5835 Syllabus

Course Description:

This course will provide students with an understanding of the practice of digital forensics in the real world. The focus will be on understanding how to apply the forensic methodology.

Prerequisites: CGS5131 (Computer Forensics I) or permission of the instructor. Students must have previous actual or instructional experience conducting forensic examinations utilizing both command-line and graphical user interface tools. Some LINUX experience is strongly suggested.

Instructor: Mark M. Pollitt, MS

Course Overview:

This course will explore the application of digital scientific techniques to solve information assurance, forensic and legal problems. The course will focus on how practitioners can define customer needs, ensure technically and forensically sound evidence collection, plan an effective examination strategy, employ efficient tools and techniques, and be an effective advocate for the product and the process. Students will utilize case studies to test different scientific and investigative approaches. The Course will culminate with a Moot Court exercise based upon an examination conducted by the student.

For the Spring Semester of 2007, this course will be conducted as a hybrid distance learning and resident course. There will be twelve online sessions followed by one - four hour sessions held at the University of Central Florida campus (please see course schedule for details). Distance students, with the permission of the instructor, may be accommodated for the resident portion of the class using video conferencing or local court testimony.

Course Delivery

The course is organized into modules called weeks which will be accomplished in sequence according to the class schedule. This is NOT a self-paced course! There will be

required readings, weekly discussion topics and assigned deliverables which must be accomplished during the week assigned. Any deviations from these requirements must be approved by the instructor.

Weeks begin at 12:01 AM Tuesday morning and continue through until Midnight of the following Monday night. Each week there will be a “Welcome” document which will provide a brief overview of the lessons for the week. It will usually describe the topic to be covered, the lectures to view and MAY provide the discussion question(s). Be forewarned, that sometimes the discussion questions and hints about the deliverables are contained within the lectures.

These lectures are done in Macromedia Flash®. The files may be viewed directly from Web CT or there will be a link to download the video as a “.zip” file. Unzip the file into a separate folder and click on the .html file. Be aware that the lectures can be as large as 60 megabytes, so you may want to download these when you have very good bandwidth!

The required readings will be posted as part of the weekly posting by the instructor. Generally, they will mirror those in the syllabus, but may have changes, additions or deletions as determined by the instructor. When in doubt, please post a question to the “Ask the Professor” section of the WebCT discussion area.

Learning Objectives:

Setting the Stage of Digital Forensics

At the conclusion of this section, the student will have a clear understanding of the origins, nature, process and terminology used in the practice of digital forensics. Students will be able to define: digital evidence, digital forensics, forensic acquisition, imaging, Standard Operating Procedures (SOP's), forensic examination and investigative analysis.

Customer Requirements

Before committing time, effort and money to a digital forensic matter, it is essential to define the customer requirements along with any limitations. The student will be able to effectively evaluate a forensic request, conduct a follow-up interview and document an examination goal, requirements statement, and proposed forensic product.

Process Limitations

There are many constraints placed on the examiner and the examination process. The students will be able to articulate a number of practical, legal and temporal limitations and how to design an examination process while staying within these

bounds. Students will be able to clearly state a cost-benefit proposition given a hypothetical examination request. Emphasis will be placed on protecting the examiner from liability in connection with the examination process.

Developing an Examination Plan

The key to an efficient and effective forensic examination is to develop a plan which will seek to meet the customer's requirements, stay within the process constraints, and provide the best product for the investment. The students will be able to design and document an Examination Plan for a hypothetical case.

Selecting Tools for Implementation

The tools available to conduct digital forensic examinations are rapidly evolving and students will be exposed to a number of tool types, including proprietary, commercial and open source. Specific tools will be reviewed for strengths and weaknesses. Students will be exposed to the tool validation including the Computer Forensic Tool Testing Program at the National Institute of Standards and Technology. Students will be able to suggest appropriate tools for specific hypothetical examinations.

Analysis versus Examination

Forensic examination is only one phase of the information lifecycle. It is important for the student to understand the roles and responsibilities of each of investigators, examiners, analysts, and attorneys. By understanding the knowledge, skills and abilities of each of these roles, the examiner will be able to effectively perform his or her function and assist in developing a high performance team. Students will be asked to role play in connection with a hypothetical case.

Effectively Presenting the Product

An examination is of little or no value if it is not communicated. Students will examine several methods of documenting and presenting the results of a digital forensic examination. Students will be required to perform a simulated examination, create several different reports and do a formal presentation, using exhibits, as an expert witness.

Required Text:

George Mohay, Alison Anderson, Byron Collie, Olivier de Vel and Rodney McKemmish, *Computer and Intrusion Forensics* (Norwood, MA: Artech House, 2003) ISBN 1-58053-369-8

Course Policies:

Attendance – A large part of the educational experience is contained in the lectures and class interaction. Therefore, class attendance is required. If you need to miss a class the instructor must be notified in advance or within 24 hours of the class completing, failure to do so will result in a lower grade. Online participation will be graded on the basis of the frequency, quality and originality of online discussion postings. The quality will be evaluated first, originality second and only then will quantity be assessed. **Online weeks will begin on the Tuesday listed in the Course Schedule. Postings must be completed by midnight on the following Monday,** as the discussion area will be closed after that time.

Late Work - work turned in late will be accepted, but will be reduced ½ grade for lateness (even with approval to turn it in late).

Participation - class participation is expected and an integral part of your grade - be active in class.

Writing Requirements – all reports will be submitted, in printed electronic form, in a format prescribed by the instructor. Text documents must be in Microsoft Word, presentations shall be in PowerPoint and spreadsheets in Excel (all versions 2003 or earlier). Deviations from this policy must have prior approval of the instructor. The instructor will grade submissions using the mark-up and comments features of Word. Students should therefore become familiar with these features and ensure that their papers are saved in an appropriate format. **All reports, notes and exhibits must be compiled into a printed portfolio to be submitted prior to moot court.** Deviations from this policy must have prior approval of the instructor.

Incomplete Grade - A grade of “I” (Incomplete) may be assigned by the instructor when a student is unable to complete a course due to extenuating circumstances, and when all requirements can be completed in a short time following the end of the term. The student is responsible to arrange with the instructor for the completion of the requirements of the course.

Assignments:

Students will accomplish seven forensic examinations which will be documented and reported in the prescribed fashion. Students will be required to conduct peer reviews of other student’s reports and their reports will be reviewed by other students. Peer reviewers may have their grades adjusted for less than rigorous reviews. Students will be required to write one Standard Operating Procedure as assigned. These assignments will be submitted via Web CT when due. All reports (including all examination notes) and the SOP compiled into a printed portfolio to be submitted to the instructor at least one week prior to moot court. These assignments are worth 50% of the student’s grade.

Students will be assigned to create a courtroom exhibit for a particular issue. They will use this exhibit during their moot court testimony. This exhibit and their testimony is worth 20% of the student's grade.

Most weeks will require one or more student postings to the discussion area designated in the week's assignment. Students are expected to frame an articulate, thoughtful and pertinent answer to the question posed. You are to consider web postings as formal business communications. Answers must be in grammatically correct English with appropriate spelling, punctuation and structure. Postings which do not meet these tests will not receive credit. Students are encouraged to reference additional material in their postings; however they must properly cite these materials. Failure to cite external materials is plagiarism and will be dealt with appropriately. In order to receive full credit for the week's discussion, students must make one or more additional thoughtful response to other student's postings. These follow-up postings must add value to the discussion. Postings that are "me too", "good point", or "I agree" will not receive credit. In other words, you must make one original posting in answer to the discussion question and at least one additional response to another student's original response in order to get full credit for participation in that week. My suggestion is that you try to post your original post as early in the week as possible and a follow-up post by mid-week.

Laboratory exercises will be assigned. These exercises will require that the student utilize the assigned software and operating system and address the specific requirements for the particular exercise. Failure to do so will result in partial or no credit for the exercise. Students must have available an Intel x86 platform running Windows 2000® or Windows XP®. It is strongly advised that you have at least 1 gigabyte of RAM and at least 20 gigabytes of free hard disk space. While most of the exercises can be accomplished utilizing a non-dedicated machine, the student will find it more convenient to utilize a dedicated computer. Assignments will be posted to the Assignments Section where the reports can be uploaded in Word Format.

Quizzes may be used to determine student comprehension at the discretion of the instructor.

Grading Policies:

<u>Requirement</u>	<u>Weight</u>
Assignments	50%
Exhibit & testimony	20%
Class discussion & Quizzes	30%

Grades

A: Signifies outstanding work, well above average, performing at a level higher than stipulated in the expected course requirements. This requires including much

- more than the requirements indicated for each assignment. (90-93=A-, 94-96=A, 97-100=A+)
- B: Performing above the average for an undergraduate student in the course. (80-83=B-, 84-86=B, 87-89=B+)
 - C: Performing the work as assigned and at the expected level for an undergraduate student. (70-73=C-, 74-76=C, 76-79=C+)
 - D: Signifies performance below the expected level for an undergraduate student. (65-69%)
 - F: significantly below the expected work level for the course, in completion or quality. (Less than 65%)

Notes:

Plus (+) or minus (-) designations indicate work slightly better or worse than average for that grade (A, B, C or D).

For all assignments: late materials will be allowed at the discretion of the instructor, but the assignment grade will be reduced by 25% of the assignment's value (even with approval to turn it in late).

DIG 5835 Course Schedule

Week Beginning	Topic	Readings	Assignments
Week 1 Jan. 9	Course Introduction	CIF Ch. 1	Obtain text, Post Discussion Question
Week 2 Jan. 16	The Forensic Process	CIF Ch. 2 & 3	Lab 1 Imaging
Week 3 Jan. 23	Quality Assurance	WebCT Link	SOP Exercise
Week 4 Jan. 30	Examination Planning and Design	CIF Ch. 5	Lab 2 Data Recovery
Week 5 Feb. 6	Forensic Tool Selection and Application	WebCT Links	Lab 3 Validation/Verification
Week 6 Feb. 13	Cross Platform Forensics		
Week 7 Feb. 20	Network Investigations	WebCT links	Lab 4 Linux Tools
Week 8 Feb. 27	Forensic and Investigative Roles	CIF Ch. 6 & 7	
Week 9 Mar. 6	Legal Issues for Examiners	Links posted on WebCT	Lab 5 Log file analysis
Mar. 13	Spring Break		
Week 10 Mar. 20	Courts and Legal Process	Web CT	Lab 6 Registry Examinations
Week 11 Mar. 27	Law of Evidence	Web CT	Lab 7 email Examinations
Week 12 April 3	Expert Testimony & Trial Exhibits	WebCT links	Portfolios Due
April 14	Tentative Moot Court date		Trial Exhibit