ISM 4324 – Computer Forensics

Fall 2011

Class Schedule:	Wednesday 4:00PM-6:50PM, FL411 (Fleming Hall), Boca Raton Campus
Instructor:	Mr. James Cooley
Office:	CM 171 (Computer Center – Behind Fleming Hall)
Office Hours:	By appointment or before class. I can usually accommodate same-day appointment requests around your schedule and I try to leave time available before class for students to stop by.
Office Phone Number:	561-297-2040
Email:	james.cooley@fau.edu
Class Textbook:	Digital Evidence and Computer Crime, 3rd Edition Eoghan Casey, Academic Press ISBN 978-0-12-374268-1

Course Description

This course will cover the methods and techniques used when performing investigations of computer data. These methods and techniques cover the investigation into what possible damage or prohibited activity has been done on a computer, when it was done, and how it was done. In addition, legal aspects of an investigation will be presented including computer crime law, reporting investigations utilizing the scientific method, and expectations in court and expectations from law enforcement. The content is intended to cover the challenges and needs of the rapidly changing world of computers and the internet.

Information regarding the acquisition of evidence will be presented with a focus on the Windows operating system in order to maximize the scope of information that can be covered in the course. Some information regarding other operating systems will be presented in class to demonstrate some of the differences between forensics on different operating systems, but tests and quizzes will only cover Windows forensics.

This class is a hands-on experience which includes several lab exercises described in the class text book, which can be completed in class. Additional hours in the computer lab will be made available outside of the normal class times for students wishing to practice, or finish up labs from previous classes. The schedule of additional lab hours will be posted after the first couple of weeks of class.

This course also covers techniques and tools which may be used to violate the law if used outside of class. The legal restrictions on the use of the techniques and tools will be covered in class.

Course Objectives

(1) Understand computer forensics principles and issues: including the need for digital forensics in the current age, forensic and investigative techniques, and the evolving nature of forensics due to societal and legal requirements.

(2) Develop and apply critical thinking and problem-solving and decision-making skills.

(3) Develop and apply enthusiasm for learning. Class participation is very encouraged in this course. Enriching classroom discussions and learning by communicating interest, suggestions for improvements, additional readings and Internet resources, is a major goal. Express diligence, enthusiasm, patience, and thoroughness in dealing with complicated laws, procedures and less-than-perfect-constantly-evolving technology.

Workload Expectations

This is a three credit hour course. FAU's COB is an AACSB accredited college of business. AACSB standards require that faculty build classes for a *minimum* of 2-to-1 out-of-class to in-class workload. It is customary to expect from two-three hours of out of class work (reading, research, study and preparation) per credit hour. Thus, on average, one should not expect to spend fewer than 6 hours per week of non-class study time for this course.

Necessary skills with Windows:

1. Download and safe files (remember where you save the files!)
2. Browse the computer with Windows Explorer
3. Open up a command prompt
4. Use the start menu, and task bar to launch and manage running programs

Software: The software used in the class is either free software or limited functionality demos that can be downloaded from the creators of the software. Some of this software cannot be used for professional or business-related tasks without an appropriate license from the software manufacturer. It is the student’s responsibility to comply with all software agreements and copyright laws with regards to software used at home. Although this software can be used at home, students who attend class regularly will learn the software to a satisfactory level to pass this course without the need to use the software at home.

Grading

Homework Assignments	**20%**
In-class Labs	**15%**
Midterm	**20%**
Project	**25%**
Final Exam	**20%**

Grading Scale:

A = > 93	B- = 80-83	D+ = 67-70
A- = 90-93	C+ = 77-80	D = 63-67
B+ = 87-90	C = 73-77	D- = 60-63
B = 83-87	C- = 70-73	F = <60

You must have a 73 or higher final grade to pass this course.

Course Components

Class attendance and participation

Regular class attendance and participation is a must. A student with irregular class attendance should expect a negative effect on his/her performance and grade. Class participation is expected and encouraged. Please, make every effort not to be late to class. Try to be considerate of your fellow students. You must be present to perform and receive credit for the in-class labs.

Assignments

Assignments will be given on a regular basis in order to help solidify the material being covered in class. These assignments will be given two weeks before they are due and will cover multiple chapters. These assignments must be submitted digitally to the appropriate drop box on Blackboard no later than midnight the night they are due. Late assignments will have their grades reduced, and **will be worth no credit if they are late by a week or more**.

Midterm Exam

The mid-term exam is a multiple-choice/fill in the blank exam given over Blackboard. This exam will cover topics covered in class and in the book. I will publish a study guide no later than one week prior to the exam. The exam will follow the objectives discussed on the study guide closely so a student that understands the material presented on the study guide should do very well on the exam. The exam is open book, and open notes. The internet may not be used to access any information other than information published in Blackboard such as course slides. However, the pace of the exam will not allow you to look up every question so you need to ensure that you understand the material prior to arriving for the exam. The midterm exam is given prior to the last day to drop prior to a W. Students will be able to see their current standing in the class on Blackboard prior to the last day to withdraw from the course.

In-class Labs

There will be between 8 and 10 in-class lab assignments. These lab assignments must be completed in class for credit. Students may miss one in-class lab assignment without penalty. The labs will comprise 15% of the final course grade. In-class labs will take place in the second half of the class period for which they are scheduled.

Final Exam

The final exam, like the midterm exam, will comprise multiple-choice and fill in the blank questions and is given over Blackboard. This exam will cover topics from the entire course, and not just the second half. I will provide a study guide in advance of the exam and during the class the week before the exam we will do a review of some of the materials covered in class. This is open book and open note like the midterm exam.

No make-up exams will be allowed except for emergency cases such as a medical emergency, death of an immediate member of the family or a similar event per the University policies published in the guide. Appropriate documentation documenting the cause of the missed exam is required, as well as advanced notification that the exam will be missed.

Project

Topic: Projects will be composed of teams of two or three. It is highly recommended that everyone works in a group, but solo projects may be approved if the student talks to me first and received my approval.

These projects are expected to expand on the material presented in class and teach members of the class something new. The presentation should be geared toward a professional technical audience, and ideas not previously presented in class should be briefly explained.

Some possible topics for the group project include:

- Forensic tools not covered in class
- Investigation of electronic devices not discussed in class
- Application of the Windows forensics techniques discussed in class to other operating systems such as Unix, Linux or Mac
- A case study on a published court case that utilized computer forensics heavily for evidence and how the techniques in class apply to the case.

Proposals for the group project should be submitted to the instructor via email prior to the deadline detailed in the schedule at the end of the syllabus. The proposal should include what the topic of the presentation will be on, and how the topic relates to the class material and be 2-3 paragraphs in length to give me a good idea about what is to be presented. I will reply back to the proposal within 24 hours of receipt, so if you do not hear back, resend the proposal as I may not have received it.

Due dates: There are two preliminary due dates for the project: one for team formation, and one for the proposal. Both are outlined in the class schedule at the end of this syllabus. A 10% penalty will be applied to submissions that are late, increasing by an additional 10% every two additional days until received, with a maximum penalty of 40% if no proposal is submitted, but a presentation is given.

It is the student's responsibility to find team members for the project. To help facilitate this, a discussion board will be created under Blackboard where students can try to find others to work with on a team.

Presentation: Powerpoint slides for the presentation must be emailed to the instructor no later than 24 hours prior to the presentation. The presentation should resemble a professional training seminar and should be educational in nature. If a forensics tool is being covered, a demonstration may be performed and I will make accommodations for it.

Students are expected to dress business-casual for the presentation.

Presentations should be no longer than 15 minutes long and there will be a 5 minute allowance for questions after the presentation is made.

Project grading: Oral presentations will be graded based on clarity, creativity and originality. It is important for all team members to be present and participate in the presentation. Individual grades will be affected by the level of participation each team member contributes to the presentation.

The project grade will be based on the following criteria:

1. The presentation is well prepared, organized and interesting. Coherent arguments are made, good grammar and explanation is practiced.
2. The presentation showcased all major project components
3. The presentation completed within the allocated time
4. All team members are professionally dressed and demonstrate professional behavior
5. The topic chosen is technically intensive or information rich, with the appropriate level of difficulty.

The final project grade will be the average of the common project grade and the individual student grade (based on the quality of the individual presentation and the questions asked by me).

CLASS POLICIES

Student responsibilities

It is the student's responsibility to obtain notes, read the syllabus thoroughly, know the dates of all exams, due dates, and project presentations, and to follow announcements and updates on Blackboard. It is essential for each student to study the course material, solve chapter problems and prepare for exams on the designated dates. If you miss a class it is your responsibility to make arrangements with a classmate to catch up on class notes and any announcements made in class. PowerPoint presentations will be available in Blackboard before each class session. Please maintain a healthy learning environment by not distracting others or the instructor. Please, make every effort not to be late to class. Try to be considerate of your fellow students. Cell phones need to be off or put into silent mode during class.

Every student ***must*** use their FAU email address for this course. You are expected to check your FAU email. Whenever you send an email, be sure to include a *subject*, *your name* and *the class* you are enrolled in.

Student Conduct, White Hat, Code of Ethics and White Hat Agreement Form

The computer systems in the University forensics lab grant full administrative privileges to the students so they can perform hands-on exercises and software tasks. This creates a responsibility for the student to utilize this access only for the purposes of completing assigned coursework.

Online and computer activities, including but not limited to handling personal emails, chat rooms, forums, browsing to web sites not related to the course material, or any activity with the lab computer which is not instructor approved, **is strictly prohibited**. **Any student who violates this policy will be expelled from the lab without further warning, explanations, or excuses. This policy is strictly enforced.**

The White Hat Oath and Code of Ethics, provided in a separate document should be thoroughly read by every student attending the course. The white Hat Agreement form should be signed and returned to me by each student no later than the second week of class. Otherwise the student will not be admitted in the lab after this date.

Inappropriate Behavior

Inappropriate behavior distracts other students and interferes with their learning experience. Inappropriate behavior may include arriving late, leaving early, talk during lectures, and so on. Rude and inappropriate behavior will not be tolerated. Upon professor's discretion, after at least 2 warnings to the student, points from the final grade will be deducted of a student who chooses to repeatedly distract others. The professor will remove a student permanently from the class in particularly egregious cases.

Academic Irregularities

FAU's honor code will be strictly enforced. Cheating, plagiarism, copying and unauthorized collaboration are unacceptable and subject to disciplinary actions. Plagiarism is turning in someone else's ideas or work. Such actions may include substantial grade penalty, including "F" in the course and a letter of fact on your student record following the rules of the University and the College of Business. Assignments in the course are graded. Therefore, it is expected that answers to assignments be the students own work and not copied from another student.

The FAU honor codes are available at:

http://www.fau.edu/regulations/chapter4/4.001_Code_of_Academic_Integrity.pdf

Religious Accommodations

This class will abide by the university's religious accommodation policy. If a student wishes to be excluded from class in order to observe a religious practice or belief, the student must notify the instructor in advance of the date. The instructor will provide an excused absence and give the student an opportunity to make up missed classwork. The requirements and restrictions of this policy are available at:

http://www.fau.edu/academic/registrar/catalog/academics.php

Incompletes

University policy states that an “I” may be given only if a student has a passing grade in the course. An incomplete is only meant for students who are unable to complete the course due to hardships beyond their control. It is not meant to accommodate students who decide that the work load is too heavy. If an “I” is given, work must be completed within the time period specified by the professor that is not to exceed 12 months from the time the “I” is given.

Accommodation of students with disabilities

In compliance with the Americans with Disabilities Act (ADA), students who require special accommodations due to a disability to properly execute coursework must register with the Office for Students with Disabilities (OSD) located in Boca Raton in SU133 (297-3880) or in Davie in MOD I (236-1222), and follow all OSD procedures. Accommodations for a student with a disability must not compromise course content or the requirements for satisfactory course completion.

FAU’s ADA Policy is available at: http://www.fau.edu/eop/ada/ada_policy.php

Internship programs

Internship programs are provided by the College of Business for any student interested in acquiring work experience with companies and other types of organizations in South Florida. Interested students must meet the following criteria to be considered for an internship: (1) students must be enrolled in the College of Business at Florida Atlantic University, (2) students must have junior level status (students can register during their sophomore year, however their records will not be activated until they achieve junior status/60 semester hours), (3) during the semester that a student registers with the Career Resource and Alumni Relations Center, he/she must be enrolled in the College of Business courses leading toward the completion of his/her degree, and (4) students must have an overall GPA of 2.5 or higher and a major GPA of 2.75. Students interested in an internship must register for a College of Business internship program, students must make an appointment through the AdvisorTrac system at https://bizadviser.fau.edu . For more information, please go to http://www.business.fau.edu/index.php?submenu=career_center&src=gendocs&link=CareerResourceMainPage&category=Career%20Resources

TENTATIVE CLASS SCHEDULE

Week	Date	Lecture	Textbook Reading
1	8/24	Introduction to the course, review of syllabus and course expectations Chapter 1 – Foundations of Digital Forensics	Chapter 1
2	8/31	Computer Crime investigations and the Courtroom Lab – Introduction to Computer Forensics Tools	Chapter 2 Chapter 3
3	9/7	Computer Crime Law Computer Basics for Digital Investigators	Chapter 4 Chapter 15
4	9/14	Conducting Investigations Lab – Exploring digital evidence	Chapter 6
5	9/21	Handling Crime Scenes Lab – Cataloging Evidence	Chapter 7
6	9/28	Reconstruction and Criminal Intent Lab – The chain link	Chapter 8 Chapter 9
7	10/5	Applying Forensic Science to Computers **Project Team Names due. Grade penalty applied after this date**	Chapter 16
8	10/12	**MIDTERM EXAM (1 1/2 hour)**	
9	10/19	Digital Evidence on Windows Systems Lab – Windows registry and filesystem forensics	Chapter 17
10	10/26	Network Basics for Digital Investigators Digital Evidence on the Internet Lab – Network Forensics Basics **Project proposals due – grade penalty applied after this date.**	Chapters 21 and 23
11	11/2	Violent Crime and Digital Evidence Digital Evidence as an alibi Lab – Exculpatory and Inculpatory evidence	Chapters 10-11
12	11/9	Sex offenders on the Internet Lab – Internet History and Steganography	Chapter 12
13	11/16	Sex offenders on the Internet (cont.) Computer intrusions Cyber stalking	Chapters 12-14
14	11/23	**Project Presentations**	
15	11/30	**Project Presentations** and review for the Final Exam	
16	12/7	**Final Exam –** 4-6:30 pm	

SYLLABUS SUBJECT TO CHANGE