Syllabus

Cybercrime Investigations & Forensics II

Spring 2008
Section A

T/Th 10:00-11:15 AM
Lecture Classroom is FAC 101

Course Description: A technical approach to the seizure and forensic examination of a windows personal computer

Prerequisites:
- Students should have a solid understanding of computer hardware and storage concepts
- Students are required to have adequate knowledge of the Internet, email usage, the Microsoft Office suite, and search engine techniques

Textbook and Resources:
- Assigned reading materials
- http://www.utica.edu/faculty_staff/qma

Instructor: Qingkai Ma
Office: DePerno 101
Email Address: qma@utica.edu
Phone: 792-3774
Office Hours: TR 11:15am-12:15pm, 2:15-3:15pm or by appointment

Course Objectives: This course will provide students with applied knowledge of evidential and technical aspects of digital/computer forensics. The purpose of this course is to teach the fundamental concepts of electronic evidence seizure and examination. Forensic techniques, methodologies and tools are presented, and will be utilized by the students in a series of labs and assignments; technical roadblocks that the investigator may face along the way are also discussed.

COURSE REQUIREMENTS AND GRADING

Class Participation/Class Assignments:
30% of your grade is reserved for class participation and assignments. Students are expected to read the assigned material and participate in class discussions.

Midterm paper
20% of your grade is based on a midterm paper on one forensics technologies. Students are required to give a short presentation on their paper topic.

Projects:
25% of your grade is based on a scenario-based individual project

Exam:
25% of your final grade is based on an exam in mid April.

The Grading Scale: I will be using the Utica College’ standard grading scale. For your benefit, here is how the grades look like in numbers. A 93-100, A- 90-92.9, B+ 88-89.9, B 83-87.9, B- 80-82.9, C+ 78-79.9, C 73-77.9, C- 70-72.9, D+ 68-69.9, D 63-67.9, D- 60-62.9, and F 0-59. If you are a CJ and/or ECI major and get a lower grade than C- in a CJ core course, you will have to repeat it. You will earn your grade as the
semester progresses. Remember, I am just the score keeper.

**Email Messages:**
Remember to put [CRJ356] in the beginning of the subject of every email you sent to me. Also remember to put your name in the email. E-mail messages that are missing this information are likely to be automatically redirected to a folder I will seldom check. I can’t guarantee prompt response to your emails. Usually your emails will be responded within 24 hours.

**Late Work:**
There will NOT be any late grading, make up exams and/or extra credit assignments. The only exception would be made for medical emergencies, with a written note by the doctor, or as the case may be, with his/her verifiable contact information. It is your responsibility to get in touch with me if you do miss any exam and/or assignment.

**Attendance:**
Class attendance will be recorded on every class day at the beginning of the class. Plus, this is a demanding course and students are strongly advised to attend. Those who are involved in sports please contact your respective coaches to provide me a written schedule for practice sessions and games so that you do not get marked absent. Consistent with Criminal Justice Department policy, grading penalties will be imposed for excessive lack of attendance, which the Department has defined as more than six (6) unexcused absences from class for classes that meet three times a week, four (4) unexcused absences from class that meets twice a week, and two (2) from a class that meets once a week. The student will be notified by e-mail that he or she has reached the point where a penalty will be imposed for additional unexcused absences. The student’s grade will be lowered one letter grade (e.g., from A to B, or from B+ to C+, etc.) for each subsequent unexcused absence. Assignments are due on the established due date whether the student is present or not. It is the student’s obligation to ensure that the assignment is delivered on or before the established due date.

**NOTE**
Any students who has a need for accommodation based on the impact of a disability should contact me privately to discuss the specific situation within the first week of the class. You may also contact Academic Support Services at 315-792-3032 or khenke@utica.edu to coordinate reasonable accommodations for students with documented disabilities.
Classroom etiquette and Discipline:
Every student is expected to respect the learning atmosphere of others. Do not disrupt the learning of your classmates by coming in late or leaving early during the class. Since it is both disruptive and rude to leave a room before the scheduled end of class, I expect any student that has to leave early to let me know in advance.

It is your responsibility to be in class on time. Students arriving more than 10 minutes after the scheduled start of the class will not be admitted to the classroom, and certainly do not get added to the attendance sheet. And if you are “absent,” how could you get points for class participation!

No talking on the sidebars is permitted. I don’t take well to indiscipline and would not hesitate to ask the disruptive students to leave the class or even drop the course.

Cell phones, calculators, palm pilots and pagers
Turn these off before you come to class. These are enormously disturbing to your fellow students. If by chance you forget to turn it off, and your phone or pager rings, I expect you to turn it off immediately. If I see that you are on the phone for any reason whatsoever, I will probably ask you to leave the classroom and not return for the rest of the semester. When you are in class I expect you to be paying attention to what is happening.

I do not want people to be on their palm pilots in class. If you must use your palm pilot to take notes, then you should speak to me individually before you start doing this so you can explain your situation.

If, during an examination, I see you consulting with or using any of these devices, I will ask you for your test, which will be assigned a failing grade, and you and I will speak further about how to proceed from that point.

Food
It would be better if no eating of snacks or meals—especially the ones with tempting smell or noisy wrappers—takes place as it could be distracting for your peers. I encourage you to bring coffee/tea/non-alcoholic beverage as long as you don’t spill it!

Class Discussions
In class discussions, we bring differing points of views to this class, and disagreement does not mean right or wrong. It simply gives us an opportunity to think and analyze from a variety of perspectives, without having to agree with any. I am hopeful that it would be a learning experience for you, where you will become a more thinking student.

Writing help:
If you have trouble writing, I would encourage you to read books—The Elements of Style (Strunk and White), and 100 ways to Improve Your Writing (Provost). You should also actively consider making use of the Writing Center. It is located in Hubbard Hall, Room 216.
Plagiarism and Utica College Policy:

With regard to plagiarism and intellectual honesty, the College Handbook states the following:

“The faculty at Utica College expect intellectual honesty from Students in examinations and in the writing of themes, term papers, or laboratory reports. Intellectual honesty is necessary for the free exchange of ideas.

Plagiarism, a serious form of intellectual dishonesty, is defined as the use of ideas and phrases in the writings of others as one’s own without crediting the source. Sources can include books, papers written by anyone else, editorials, opinions, reference articles, or other media. Paraphrasing must be cited and credited as well. Credit must be given either internally in the text or in formal notes.”

Plagiarism is a serious offense, the penalty for which is an “F” on the assignment and/or for the course, as well as academic probation. It is the student’s responsibility to properly cite all sources, whether obtained from hardcopy published literature, Internet-based electronic research, discussion with peers and other professionals, heard on audiotape, or viewed via videotape.

A bibliography alone is not sufficient to establish which portions of the student’s work are taken from other sources:

- Footnote or endnote forms of citation must also be used; refer to APA Reference Guide for proper format, or go to http://www.apastyle.org
- Please develop a citation for each new idea presented that was obtained through research; do not provide only one citation for an entire paragraph or page and force me to decide what was inserted/paraphrased and which ideas are your own.
- In fact, by adhering to these guidelines and creating proper citations, the student will actually get more credit for their clearly identified original ideas and high-order thinking!

When using direct material from a book or website, be sure to include such material in quotations with a citation. All other materials must be strongly paraphrased. This means that I want you to fully understand what you are reading, then put it into your own words. This does not mean simply changing a few pronouns here and there and calling it a day. After all, you are not really performing research or writing a research paper if you don’t understand what you are presenting to me.

Tentative Course Schedule - Subject To Change

<table>
<thead>
<tr>
<th>Week</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Syllabus, introduction</td>
</tr>
<tr>
<td>2</td>
<td>Intro to Computer Forensics Process</td>
</tr>
<tr>
<td>3</td>
<td>File system and disk structure and data recovery</td>
</tr>
<tr>
<td>4</td>
<td>File system and disk structure and data recovery review BIOS, POST</td>
</tr>
<tr>
<td>5</td>
<td>Imaging and preservation</td>
</tr>
<tr>
<td>6</td>
<td>File analysis</td>
</tr>
<tr>
<td>7</td>
<td>Internet Forensics</td>
</tr>
<tr>
<td>8</td>
<td>Email forensics</td>
</tr>
<tr>
<td>9</td>
<td>Midterm paper and presentation</td>
</tr>
<tr>
<td>10</td>
<td>Instant Messaging forensics</td>
</tr>
<tr>
<td>11</td>
<td>Hashing for KFF and identification</td>
</tr>
<tr>
<td>12</td>
<td>Introduction to extraction and analysis</td>
</tr>
<tr>
<td>13</td>
<td>Selected small topics</td>
</tr>
<tr>
<td>14</td>
<td>Selected small topics (cont’d)</td>
</tr>
<tr>
<td>15</td>
<td>Anti-forensics</td>
</tr>
</tbody>
</table>