CIS 522
Computer Forensics and Incidence Response
Spring 2015

Instructor          Dr. Tom Roberts
Office              Business
Phone               (318) 257-3514
E-Mail              troberts@latech.edu
Office Hours        Tuesday 12-3 Wednesday 1-6 Thursday 1-2
                    And by Appointment

Text                Guide to Computer Forensics and Investigations
                    Nelson, Phillips, and Steuart
                    5th Edition

Lecture notes posted on Moodle

Course Objective and Overview:

This course is designed to give students an understanding of basic computer forensics and
the handling of evidence. The course is rigorous. You are advised to pay careful
attention to the class lectures and especially sample problems and lab exercises. Exam
questions are based primarily on the material covered in class and are designed to test
your understanding of the underlying concepts of computer forensics and evidence
handling. Note the course will cover the technical and legal aspects of evidence
collection. I urge you to ask questions if you don't understand. You can come during my
office hours, email me or (better yet, since everyone will benefit) ask in class. There are
not any dumb questions in this course. You have to make sure there are no vague areas
in your knowledge before exams. You will have to work hard to get an A in the class.
On the other hand, many people do get an A in my class so hard work does pay off.

Responsibility

The student shall be responsible for all material covered in the class lectures. Each
exam will include not only the material from the assigned text chapters, but also from the
readings, tours, guest lectures and any other materials covered in the class lectures.

You are also responsible for any announcements made in class. Often times I have to
change the Class Schedule or I may announcements relevant for assignments. Schedule
changes will be posted on my website. We will have several external speakers during the
semester.

I do expect class participation from every individual in the course. Students often learn
many things from student colleagues and questions in class. This participation is vital to
classroom discussion. It will be a part of the evaluation of this course.
Projects – This class will an individual forensics project. It will have two parts. Part A will be hiding information for a forensic investigation case. This will be due on April 15. Part B will be a forensic investigation that will include a digital forensic investigation and report. The Forensic Report will be due on May 15.

Paper – Students in CIS 522 will have to write a paper (5-10) concerning some aspect of computer forensics. This could be a case or a topic. This will be due on the last day of class. The topic must be approved by the April 15 or Tax Day.

Evaluation

The Graduate final course grade will be computed from the following inputs:

<table>
<thead>
<tr>
<th>Evaluation Item</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Midterm Exam</td>
<td>20%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>20%</td>
</tr>
<tr>
<td>Project Part A</td>
<td>20%</td>
</tr>
<tr>
<td>Project Part B</td>
<td>20%</td>
</tr>
<tr>
<td>Paper</td>
<td>10%</td>
</tr>
<tr>
<td>Class Participation</td>
<td>10%</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

The final course grade will be determined as follows:

- 90 or above: A
- 80-89.99: B
- 70-79.99: C
- 60-69.99: D
- Less than 60%: F

Make-up Exams

There will not be any make up exams unless there are dire circumstances. It is up to the student to notify the professor under all circumstances and the student will be held accountable. Documentation for the absence will be required. A grade of 0 will be placed in place of the exam until the percentage is replaced. Under absolutely no circumstances will the final be made up.

Disabilities

Anyone with a disability that may limit participation with regular classroom activities should inform the professor at the beginning of the term. Proper adjustments will be made to compensate for limitations. Remember that informing the professor of these disabilities is the responsibility of the student.
Qualified students needing testing or classroom accommodations based on a disability are encouraged to make their requests to me at the beginning of the quarter either during office hours or by appointment. Note: Prior to receiving disability accommodations, verification of eligibility from the Testing and Disability Services Office is needed. Disability information is confidential. Information for Testing and Disability Services may be obtained in Wyly Tower 318 or www.latech.edu/ods.” (Refer students who do not present an accommodations memo from the Office of Disability Services to that office or to www.latech.edu/ods for assistance.

**Academic Integrity**

In accordance with the Academic Honor Code, students pledge the following: Being a student of higher standards, I pledge to embody the principles of academic integrity.” I have adopted a very simple but strict policy within the overall university guidelines to maintain academic integrity. In all cases of academic dishonesty (for example, cheating of any kind in labs, quizzes and exams or plagiarism in project reports), the involved student(s) will get the grade of Fail (F) for the whole course. Exceptions will be made only in rare cases, in which the student makes a convincing case of the situation beyond the control of the student.

**Disaster Planning**

**Emergency Notification System:** All Louisiana Tech students are strongly encouraged to enroll and update their contact information in the Emergency Notification System. It takes just a few seconds to ensure you’re able to receive important text and voice alerts in the event of a campus emergency. For more information on the Emergency Notification System, please visit [http://www.latech.edu/administration/ens.shtml](http://www.latech.edu/administration/ens.shtml).

If a disaster were to strike on the Ruston Campus or CenturyLink, this course would continue via the discussion board and assignments online via Moodle.

**Tentative Course Schedule (Subject to Change)**

<table>
<thead>
<tr>
<th>Date</th>
<th>Scheduled</th>
</tr>
</thead>
<tbody>
<tr>
<td>W1</td>
<td>3-11-15 Class Introduction</td>
</tr>
<tr>
<td>W2</td>
<td>3-18-15 Forensic Evidence and Investigations</td>
</tr>
<tr>
<td>W3</td>
<td>3-25-15 Computer Forensics and Digital Detective</td>
</tr>
<tr>
<td>W4</td>
<td>4-1-15 Tools and Equipment</td>
</tr>
</tbody>
</table>
W5
4-8-15    Policies and Procedures
        Investigator’s Office and Laboratory

W6
4-15-15    Midterm Exam
            Project Part A –
            Detailed Evidence List/Location Report Due

W7
4-22-15    Windows and DOS
            Analysis and Validation

W8
4-29-15    Graphic Files
            VMs and Network Forensics

W9
5-6-15    E-Mail
            Mobile Devices
5-8-15    Graduate Paper Due - Midnight

W10
5-13-15    Final Exam
5-15-15    Project Part B – Forensic Report Due

W11
5-20-15    Guest Speaker