Fall 2015

CSCI 5623

Golden G. Richard

University of New Orleans

Follow this and additional works at: http://scholarworks.uno.edu/syllabi

Recommended Citation

http://scholarworks.uno.edu/syllabi/190

This Syllabus is brought to you for free and open access by ScholarWorks@UNO. It has been accepted for inclusion in University of New Orleans Syllabi by an authorized administrator of ScholarWorks@UNO. For more information, please contact scholarworks@uno.edu.
I have read and understood the policy on academic dishonesty (“cheating”) as outlined in the syllabus for the Fall 2015 CSCI 5623 course. In particular, I understand that copying or providing to other students, in whole or in part, solutions (text or source code) to CSCI 5623 assignments from any source (including work done by former and current CSCI students, other humans, animals, zombies, materials downloaded from the Internet, etc.) not directly sanctioned by Prof. Richard is not acceptable. I understand that all work must be exclusively my own, with the exception of any team projects, for which I am allowed to collaborate with my assigned partner(s).

THERE IS NO FLEXIBILITY IN THIS POLICY. IF YOU CHEAT, YOU FAIL, AND YOUR ACADEMIC CAREER IS LIKELY TO BE PREMATURELY TERMINATED. THE “REASON” YOU CHEATED IS IMMATERIAL. This policy applies equally to students “transmitting” or “receiving” answers.

Print your name: __________________________________________________________

Sign your name: __________________________________________________________

Date: _____________________________________________________________________

No grades will be assigned to your work until you sign and hand in this agreement.
CSCI 5623
Introduction to Digital Forensics
Fall 2015 Syllabus
Prof. Golden G. Richard III

Me:
Office ➜ Math 329c in the GNOCIA
Phone ➜ 504-280-6045
Email ➜ golden@cs.uno.edu
Office Hours ➜ 4-6pm MW, 2-3pm F or by appt

You:
A student who has credit in CSCI 4401. CSCI 4621/5621 and CSCI 5623 may be taken in any order.

Meeting:
Section 001 ➜ 1-2pm MWF in Math 322

Textbooks:


Additional reading material will be assigned in class.

Grading:
Midterm Examination ➜ 35%
Final Examination ➜ 35% (comprehensive)
Laboratory Assignments ➜ 30%
More Details

ASSIGNMENTS: There will be a number of laboratory assignments in this course. There are dedicated machines in the Networking, Security, and Systems Administration Laboratory (NSSAL) in Math 322 for your use. Generally, you will have to work on assignments in the lab, because commercial software is available there that you will not have access to outside the lab. You should consider the due date for each assignment to be a hard deadline. When the due date arrives, turn in what you have—I do give partial credit, but…

NO LATE SUBMISSIONS WILL BE ACCEPTED. ANY SOLUTION SUBMITTED AFTER THE DUE DATE WILL RECEIVE A GRADE OF ZERO.

Submission procedures will be discussed in class.

TESTS: The final examination is comprehensive with an emphasis on material after the midterm. Any missed test will receive a grade of zero unless arrangements are made with me. Both the midterm and final are closed book, closed notes. The tests may include questions related to your laboratory assignments—take careful notes when you are working on assignments and study these notes before the examinations. Be prepared to explain techniques you used in the lab.

To satisfy University of New Orleans requirements for graduate students taking 4000-level courses, graduate students will be required to answer additional questions on all examinations.

CHEATING: Don’t cheat. If you do, I will catch you, and I will pursue the harshest possible penalties. All submitted work must be exclusively your own. Cheating is:

- Copying, in whole or in part, the solutions of former students, current students, or any other living being, alive or dead. “Copying” includes transmission through email, port knocking, the Web, smoke signals, ESP, steganography, or any other means.
- Obtaining solutions from the Internet or other any archival source.
- Even looking at a solution is cheating. If you see something that looks like a solution to a class assignment, avert your eyes and run away as fast as you can.

The official UNO policy statement on academic integrity states:

Students are expected to conduct themselves according to the principles of academic integrity as defined in the statement on Academic Dishonesty in the UNO Student Code of Conduct. Any student or group found to have committed an act of academic dishonesty shall have their case turned over to the Office of
Student Accountability and Advocacy for disciplinary action, which may result in penalties as severe as indefinite suspension from the University. Academic dishonesty includes, but is not limited to: cheating, plagiarism, fabrication, or misrepresentation, and being an accessory to an act of academic dishonesty.

Discussing assignments at a high level for clarification, discussing problems concerning the computing equipment, and studying in groups for examinations is not cheating, but every character you type for laboratory assignments, written assignments, and the examinations had better be your own!

STUDENTS WITH DISABILITIES:

The official UNO policy for handling disabilities that may impact your ability to excel in UNO courses is:

It is University policy to provide, on a flexible and individualized basis, reasonable accommodations to students who have disabilities that may affect their ability to participate in course activities or to meet course requirements. Students who seek accommodations for disabilities must contact the Office of Disability Services prior to discussing their individual needs for accommodation with their instructors.

GRADING SCALE: The following grading scale is used. I never curve. Grading in college courses is objective—please don’t ask me to change your grade on an assignment unless you clearly deserve it and can demonstrate that this is the case.

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>90-100</td>
</tr>
<tr>
<td>B</td>
<td>80-89</td>
</tr>
<tr>
<td>C</td>
<td>70-79</td>
</tr>
<tr>
<td>D</td>
<td>60-69</td>
</tr>
<tr>
<td>F</td>
<td>0-59</td>
</tr>
</tbody>
</table>

CLASS MATERIALS: Powerpoint slides and other materials are available via Moodle. Please try to view the slides online as much as possible and avoid printing them! The trees we have left will love you.

LEARNING OUTCOMES: At the conclusion of this course, the successful student should be able to:

1. Appreciate and apply basic, sound digital forensics principles;
2. Identify the current capabilities and limitations of state-of-the-art digital forensics techniques;
3. Use and understanding terminology associated with digital forensics investigation and research;
4. Complete basic digital forensics investigations based on the principles presented in the course;
5. Demonstrate a deeper understanding of the field of digital forensics by reading and reporting on classic and contemporary research papers in the field.
Topics

This list is designed to give you a taste of the topics we'll cover in the course—the order of presentation may vary.

- **Introduction to Digital Forensics**
  - What is it? Why use it? Isn't it evil?
  - Spectrum of computer-related crime / investigative scenarios
  - What is “digital evidence”?
  - Where can evidence be hidden?
  - What are the limits of data recovery?
  - Commercial vs. open-source tools for digital forensics investigations

- **Overview of the Investigative Process**
  - Preparatory steps
  - Identification of evidence
  - Documentation
  - Collection and preservation of digital evidence
  - “Order of volatility”
  - Examination and analysis of digital evidence
  - Timelines
  - Reporting

- **Legal Issues**
  - What is computer crime? What’s not?
  - Investigation vs. the right to privacy
  - Fourth and Fifth amendments to the U.S. Constitution
  - Protection of encryption keys under 5th amendment
  - Chain of custody
  - Court order, search warrant and wiretapping laws
  - DMCA
  - Patriot Act
  - Computer fraud and abuse laws
  - Admissibility of evidence in court, including Daubert

- **Preservation of Evidence**
  - Overview of devices that can contain digital evidence
  - On the scene: procedures for preservation of evidence
    - Scene documentation
    - Pull the plug?
    - Seizure
Imaging procedures
  • Commercial solutions
  • Open-source solutions

Special considerations for volatile evidence (e.g., older PDAs)

Considerations for “live” forensics analysis

Collecting Digital Evidence: The Investigative Process

• Beginning an investigation
• The evidentiary trail: audit and non-repudiation
• Documenting the investigation
• The importance of establishing timelines
• Eliminating irrelevant and targeting relevant data: hash dictionaries

Sources of digital evidence
  • Deleted and undeleted files
  • Temporary files
  • Print spooler
  • Swap space
  • Slack space
  • Hibernation files
  • The Windows registry
  • Web browser caches
  • Log files

• Filesystem internals
  • FAT-flavored filesystems
  • HPFS/NTFS
  • Linux filesystems: ext2, ext3, ext4
  • Macintosh HFS / HFS+
  • Other Unix flavors

• Recovery of deleted files
  • Simple file recovery
  • File carving

• Commercial suites for digital forensics investigation
  • Encase
  • FTK
  • X-ways Forensics
  • ...

• Open-source tools
  • Linux as a forensics investigation platform
  • Sleuthkit

• Case studies

Mobile Device Forensics
- Why?
  - Challenges in mobile device forensics: What’s different?
  - Best Practices
  - Tools and Techniques

- **Live Digital Forensics**
  - Why?
  - Tools and techniques
    - Acquisition of memory and system state
    - Memory analysis
    - VM Introspection
    - “whole system” capture
    - The Volatility memory analysis framework
  - Challenges in live digital forensics
    - Modification of system state
    - Malware

- **The Other Side: Ensuring Privacy**
  - Basic precautions to protect privacy
  - Secure file deletion
  - Encrypted filesystems
  - Volatile computing

- **An Introduction to Intrusion Forensics and Malware Analysis**
  - Malware analysis
  - Network forensics

- **Cryptography with Applications in Digital Forensics**
  - Private key systems
  - Public key systems
  - Hashes/message digests
  - Steganography
  - Defeating cryptography in digital forensics investigations
    - Human factors
    - Keystroke capture devices
    - Wiretapping
    - Van Eck radiation