ITM 642: Digital Forensics

Sanjay Goel
School of Business
University at Albany, State University of New York

INSTRUCTOR INFORMATION

Name: Sanjay Goel
Email: goel@albany.edu
Phone: (518) 442-4925
Office Location: BA 310b, University at Albany
Office Hours: TBD

CLASS INFORMATION

Time: N/A
Location: Online
Dates: TBD
Credit(s): 3
Call #: TBD

RESOURCES

Website: http://www.albany.edu/~goel/classes/

There is one text for the class with separate readings assigned from various sources. In addition, there several reference books and materials that you can refer to for further information if necessary.

Text

Wiles, J. & Reyes, A. (2007). *The Best Damn Cybercrime and Digital Forensics Book Period.* Burlington, MA: Syngress Publishing Inc., Elsevier, Inc., p. 1-736.
Free Online at: http://www.sciencedirect.com/science/book/9781597492287

References:

Casey, E. (2004). *Digital Evidence and Computer Crime , 2nd edition.* San Diego, CA: Academic Press., p. 1-688.

Nelson, B., Philips, A., & Steuart, C. (2009). *Guide to Computer Forensics and Investigations, 4th edition*, Canada: Thomson Course Technology, p. 1-682.

Middleton, B. (2004). *Cyber Crime Investigator's Field Guide*, New York, NY: Auerbach Publications., p. 1-296.

Farmer, D., & Venema, W. (2005). *Forensic Discovery.* Boston, MA: Addison-Wesley Professional, p. 1-240. Free Online at: http://www.porcupine.org/forensics/forensic-discovery/.

Carrier, B. (2008). *Forensic File System Analysis.* Boston, MA: Addison-Wesley Professional. Some sections free through O'Reilly Safari (All available for 10-day free trial) at: http://proquest.safaribooksonline.com/0321268172

Readings: Reference readings will be posted at the end of each presentation. Available readings will be accessible via http://eres.ulib.albany.edu You must click on "Electronic Reserves & Reserve Pages" and then type in "ITM642" in the empty box. Click under the Course Number section (which is hyperlinked) you will be asked to input a password. The password to access this information will be provided via email and is case-sensitive. All of the readings is divided by Unit and contains readings in pdf format or web links to readings.

COURSE OVERVIEW

Computer forensics is a relatively new field focused on solving computer crime that is an amalgamation of forensics investigative techniques, computer security, and law. Computer forensics is the study of cyber attack reporting, detection, and response by logging malicious activity and gathering court-admissible chains-of-evidence using various forensic tools that are able to trace back the activity of the criminals. The course provides students with training in identification, collection and preserving evidence from computers and networks. This course also teaches how to perform computer crime investigations and covers the recovery and analysis of digital evidence as well as addressing legal and technical issues. Students learn specific forensic examination techniques for Windows and Unix/Linux systems using selected tools. Students also gain knowledge in the area of network forensics that covers auditing and investigation of network and host system intrusions, tracing emails, and analyzing Internet fraud. Students learn how to seize a computer from a crime scene without damaging it or risking it becoming inadmissible in a court of law as well as image and mirror hard drives. Specific tools are used for network and computer forensics such as HELIX, Knoppix, PSK, and WinHex editor. EnCase is the most comprehensive and popular tool among law enforcement agencies, however, it is very expensive. An academic version with less functionality may be used for similar software. Finally, ethics, law, policy, and standards concerning digital evidence are discussed in the class.

Course Prerequisites

It is assumed that students will come in with varied backgrounds in information systems with some general background of computer security. It would be helpful if students have some knowledge of the following topics:

1. Computer Networks
2. Computer Architecture
3. Basic Information Security

Course Format

This course is being offered as an online course. However, the intent of the course is to provide students with an interactive learning environment through instructor audio, discussion groups, and interactive quizzes. The purpose of the course is to train students in the practice of risk analysis by elucidating the concepts through examples and case studies. Students are expected to use critical thinking skills as they go through the material rather than accepting facts at face value. Even though the course is spread over 3 weeks, it is important that students stay on schedule so that they can participate with other students in discussions. The class work would include instruction video of lecture material, quizzes, discussion postings, final project, and readings.

Learning Objectives

At the end of the course, students should be able to:

1. Perform investigative techniques for digital forensics.
2. Acquire data and preserve digital evidence, according to the standards required for presentation in a U.S. Court of Law.
3. Use different forensic tools and techniques for recovery and analysis of both data to be used as evidence.
4. Determine collection and preservations procedures and implications based on knowledge of the operating system.
5. Differentiate between file systems in use (FAT, NTFS, etc.) and their implications on file retention and deletion
6. Reconstruct events and create timeline of activity.

7. Analyze unknown binaries found on a computing system.
8. Collect and preserve evidence from internal network, email, and other internet sources.
9. Interact with the prosecutors, create case summaries, and provide expert testimony.

ASSESSMENT & GRADING

Academic Integrity Compliance: Students MUST comply with all University standards of academic integrity. As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** If a student is discovered to NOT comply with academic integrity standards, the student will be reported to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies) AND receive either a warning, be told to rewrite the plagiarized material, receive a lowering of a paper or project grade of at least one full grade, receive a failing grade for a project containing plagiarized material or examination in which cheating occurred, receive a lowering of course grade by one full grade or more, a failing grade for the course, or any combination of these depending on the infraction.

Examples of violations include: Giving or receiving unauthorized help before, during, or after an examination; Collaborating on projects, papers, or other academic exercises which is regarded as inappropriate by the instructor(s), Submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor(s) to whom the material is being (and has in the past been) submitted; misrepresenting material or fabricating information in an academic exercise or assignment; Destroying, damaging, or stealing of another's work or working materials; and presenting as one's own work, the work of another person (for example, the words, ideas, information, code, data, evidence, organizing principles, or style of presentation of someone else). This includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, the purchase of prepared research, papers, or assignments, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations.

If you ever have any questions about whether you could be violating academic integrity standards - ASK!

Grading Rubric

Quizzes/Exams (20%) – Please work individually on all quizzes/exams. Two exams will be offered after during the course. Please go to the Toolbar and click "Other Tools". Select "Assessments" and you will see the exams. This will be graded automatically via Blackboard.

Discussion Postings (30%) – Even though this is an online course, it is expected that students will be able to learn from each other and participate in a discussion. To promote this, you will be assigned discussion postings, which will be graded. Discussions will be able to be created and viewed by going to the "Discussions" link on the top right hand corner of the page. In addition to discussion postings, responses to other student posts are also required. Initial postings will generally be due on Wednesday and responses to other postings should be up by the Sunday of that week.

***Assignments/Project (50%)* –** Students will receive assignments and exercises for this class. For assignments, forensics software will be made available to the students on disks or in accessible computer laboratories. For take home project/exam students would need to install the software on their own computers or lab computers. The primary project for the class will entail a detailed forensics analysis on a case from beginning to the end including gathering evidence from electronic media, preserving evidence, forensic examination of data, creation of time line, and preparing a report for the prosecutors. The detailed case will vary for each class and will be provided to the students at the appropriate time during the semester.

COURSE SCHEDULE

	Topics	**Readings**
1	Introduction to Computer Forensics	TBD
2	Collection and Preservation of Evidence	TBD
3	Understanding the Operating Systems	TBD
4	Forensic Examination of Windows Systems	TBD
5	Forensic Examinations of Linux/Windows Systems	TBD
6	Case Analysis	TBD
7	Exam I	TBD
8	Network Forensics	TBD
9	Email & Internet Tracing	TBD
10	Wireless and Handheld Forensics	TBD
11	Recovering Images & Child Pornography	TBD
12	Interacting with Prosecutors & Documenting the Case	TBD
13	Open Source Data Forensics Analysis	TBD
14	Exam II	TBD

Detailed Schedule

Week 1
Theme: Introduction to Digital Forensics
Topics:
Exercises:

Week 2
Theme: Collection and Preservation of Evidence
Topics: Preparing for a search, seizing/collecting evidence, data acquisition. Legal aspects of data collection and preservation.
Exercises:

Week 3
Theme: Understanding the Operating Systems
Topics: Windows, Unix/Linux and Macintosh operating systems and file/Disk structures.
Exercises:

Week 4
Theme: Forensic Examination of Windows Systems
Topics: Windows file system, boot disk, data recovery tools, logs and file system traces
Readings:
Exercises:

Week 5
Theme: Forensic Examination of Unix/Linux and Macintosh Systems
Topics: Unix file system, boot disk, data recovery tools, logs and file system traces
Exercises:

Week 6
Theme: Case Analysis
Topics:
Exercises:

Week 7 Exam I

Week 8
Theme: Network Forensics
Topics: Collecting and preserving data from computer networks, understanding data storage on different layers of the network protocol, and analyzing log files.
Exercises:

Week 9
Theme: Email and Internet Tracing
Topics: Email, newsgroups, chat networks, search engines and online databases.
Exercises:

Week 10
Theme: Open Source Data Forensics Analysis
Topics: Using open source data from the internet and public sources to perform compute investigations.
Exercises:

Week 11
Theme: Wireless Forensics (Wi-Fi) and Handheld Device Forensics
Topics:
Exercises:

Week 12
Theme: Recovering Images & Child Pornography
Topics:
Exercises:

Week 13
Theme: Interacting with Prosecutors & Documenting the Case
Topics: How to create case summaries and compile report information, provide expert witness testimony, and work with prosecutorial officials.
Exercises:

Week 14 Exam II