CIS 3605 002 – Introduction to Digital Forensics

12:30pm--1:50pm, Tuesday/Thursday, SERC 206, Fall 2015

Instructor

Name: Xiuqi (Cindy) Li
Email: xli@temple.edu
Phone: 215-204-2940
Fax: 215- 204-5082, address to my name
Office: SERC 353

Office Hours: Tuesday/Thursday: 2pm—3:30pm
Or by appointment.

Communication

- Your **TU Email** will be used for me to send important information about the course. **Please get into habit of checking your TU emails frequently.**
    - **Note that some emails sent via TU blackboard may be delivered to your SPAM or Junk email folder. Please also check those folders to see if you miss any information.**
- To speed up the response to your email, I would appreciate it if you could provide me the following information in your **email subject**:
    - The course you are taking: **CIS3605 002**
    - Your **FULLNAME** in the format: **Lastname, Firstname**
    - Email content summary

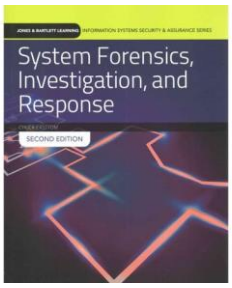
Pre-requisites

CIS2107: Computer Systems and Low Level Programming, Min grade: C-
Or
(CIS2229 Architecture, Operating Systems and Networking, Min grade: C-
& CIS2168 Data Structures, Min grade: C-)

Textbooks

Title: Guide to Computer Forensics and Investigations (**with DVD**), **5th Edition**
Authors: Bill Nelson, Amelia Phillips, Christopher Steuart
Publisher: Cengage Learning, **2015**
ISBN 13**: 978-1285060033**
Notes:

- **Required book.**
- **CD is required if you need to do hands-on work on your own computer.**



Title: System Forensics Investigation and Response, **2nd Edition**
Author: Chuck Easttom
Publisher: Jones & Bartlett Learning, **2014**
ISBN 13**: 978-1284073942**
Notes:

- **Book copy: optional, selected chapters are covered**
- **Online virtual lab that accompanies the book: required. The detailed purchasing information will be posted on the blackboard.**

Location of course materials

TU Blackboard (https://blackboard.temple.edu) is used for important announcements, assignments, lecture notes, tests, and data files used in the textbook. For your own benefit, please check the Blackboard very often for the latest information.

Course summary (catalog description)

This course is a broad introduction to the field of Digital Forensics. It covers various fundamental topics necessary for digital forensics investigation. The course begins with foundations of electronic evidence including cybercrime laws, the 4th Amendment, compliance and requirements, collection and handling, analysis, and reporting. The course also covers fundamentals of file systems with specific details pertaining to Microsoft FAT file systems. Students will learn two important forensics techniques–-file recovery and file carving–-among other things. Finally, forensics artifacts relevant to Windows Systems and Networks are discussed with relevant lab activities and students are also introduced to Antiforensics. Hands-on lab activities familiarize students with several relevant investigation techniques and the use of open source forensics tools.

Topics covered

- Fundamentals of digital forensics investigation
- Foundations of electronic evidence - compliance and requirements
- Cybercrime laws
- Digital Forensics Process
- Digital Forensics lab and tools
- Fundamentals of file systems
- Forensics File recovery and file carving
- Forensics artifacts relevant to Windows Systems and Networks
- Using open source forensics tools

Certain topics may not be covered in detail due to limitation in time and lab environment.

Objectives

By the end of the semester, you will be able to

- Summarize the basic principles of digital forensics
- Understand various stages of digital forensics investigation
- Summarize important laws relevant to digital forensics investigation

- Describe the digital forensic lab and tools
- Understand storage management and its importance in forensics
- Understand the file system fundamentals and the internals of Windows FAT file system
- Use forensics tools to recover and carve files
- Use forensics tools to conduct Windows forensic analysis and Network forensic analysis
- Understand Antiforensics and its impact on Digital Forensics Analysis

Grading components

Quizzes: 12%
Midterm and Final: 60%
Assignments: 28%

Assignments (including hands-on labs and projects) are mostly exercises from the textbook. Some of them may be outside the textbook.

Only part of assignments will be required for submission and therefore counted in the total grade. The others are for self-practice purpose and will not be required for submission.

Questions in quizzes and tests will be in varied formats.

Details about each quiz and test will be posted before that quiz or test.

Grading scale (Final/Mid-Term Grade)

	88 – 89 = B+	78 – 79 = C+	68 – 69 = D+	
92 – 100 = A	82 – 87 = B	72 – 77 = C	62 – 67 = D	0 – 59 = F
90 – 91 = A-	80 – 81 = B-	70 – 71 = C-	60 – 61 = D-	

Important Dates

Event	**Date**
Last day to add/drop a course	Friday, Sep. 4
Last day to withdraw from the course	Tuesday, Oct. 20
Fall break (No Class)	Monday, Nov. 23 – Wednesday, Nov. 25
Thanksgiving break (No class)	Thursday, Nov. 26 – Sunday, Nov. 29
Last day of class	Monday, Dec. 7
Study days	Tuesday, Dec. 8 – Wednesday, Dec. 9
Final Exam	Thursday, Dec. 10
Final Grades due to the Registrar	Friday, Dec. 18

Late submission policy

- There will NOT be any makeup quiz. Your lowest grade in the quizzes will be dropped.
- There will **NOT be make-up exams except for documented emergencies.** It is required that you notify me **at least 24 hours before the regular exam time**.
- Assignments are expected to be submitted on time. Late assignment may be accepted depending on the course schedule. If late submission is accepted there will be penalty points deducted.
- No student will be allowed to have two or more late submissions.

Work required outside of class

Outside of class, you are required to do the following:

- Check the blackboard on a daily basis. Read important announcements and course content updates.
- Read the textbooks and any handout given.
- Watch tutorial videos if there is any.
- Complete each assignment, quiz, and test on time.

Course Calendar (Tentative)

The schedule below is a tentative schedule. The detailed and up-to-date schedule can be found in our course on the blackboard.

Week	Dates	Major Topics Covered	Related Book Chapters
1	8/25, 8/27	Syllabus, digital forensics overview, types of digital forensic investigation, forensic challenges, etc	Guide5E-Chapter1, System2E-Chapters 1, 2
2	9/01, 9/03	Cyber laws, computer crimes, digital forensic labs and requirements	Guide5E-Chapter2, System2E-Chapters 1, 2
3	9/08, 9/10	Forensic data acquisition, forensic data validation, daubert standard, rules of evidence, etc	Guide5E-Chapters3, 4, 9, System2E-Chapter1
4	9/15, 9/17	Storage management, hard disk drives, file system basics	Guide5E-Chapter5, System2E-Chapter8
5	9/22, 9/24	Windows FAT file system	Guide5E-Chapter5, System2E-Chapter8
6	9/29, 10/1	Windows forensics analysis and labs, Midterm Review	Guide5E-Chapter5, System2E-Chapter8
7	10/6, 10/8	**Midterm Exam,** Current digital forensics tools and requirements	Guide5E-Chapter6
8	10/13, 10/15	File carving, deleted file recovery, file signatures, forensic analysis of graphic files	Guide5E-Chapter 8
9	10/20, 10/22		
10	10/27, 10/29		
11	11/3, 11/5	Networking concepts	Guide5E-Chapter 10, System2E-Chapter12
12	11/10, 11/12	Network forensic analysis and labs	Guide5E-Chapter 10, System2E-Chapter12
13	11/17, 11/19		
14	11/24, 11/26	**No Class. Fall break & Thanksgiving Break**	
15	12/01, 12/03	Intro. to antiforensics, Final review	Handout
16	12/10	**Final exam**	
17	12/18	**Final grades due**	

Attendance policy

- Attendance will be checked.
- You are required to attend all classes that discuss exams, quizzes, and assignments.
- If you miss more than four classes, your grade will be dropped to the next level in the grading scale.

Accommodations for Students with special needs

Any student who has a need for accommodation based on the impact of a documented disability, including special accommodations for access to technology resources and electronic instructional materials required for the course, should contact me privately to discuss the specific situation by the end of the second week of classes or as soon as practical. If you have not done so already, please contact Disability Resources and Services (DRS) at 215-204-1280 in 100 Ritter Annex to learn more about the resources available to you. I will work with DRS to coordinate reasonable accommodations for all students with documented disabilities. (http://www.temple.edu/studentaffairs/disability/accommodations/)

Student and Faculty Academic Rights and Responsibilities

Freedom to teach and freedom to learn are inseparable facets of academic freedom. The University has a policy on Student and Faculty and Academic Rights and Responsibilities (Policy #03.70.02) which can be accessed through the following http://policies.temple.edu/PDF/99.pdf

Have a successful semester!