

# FCM 760: Forensic Management of Digital Evidence

Fall 2010

Instructor: Prof. Shamik Sengupta

Class time: Thursday: 6:20pm - 8:20pm

Office Hrs: Thursday: 5:00pm - 6:00pm or by appointment

Instructor's website: <http://jjcweb.jjay.cuny.edu/ssengupta/>

(Email: [ssengupta@jjay.cuny.edu](mailto:ssengupta@jjay.cuny.edu))

---

## Course Description:

This course provides an introduction to the topics related to Digital Forensics. With computers and other digital systems increasingly being part of our lives and society, there is an exponential growth among criminals to use technology to facilitate their offenses and avoid apprehension. Digital forensics (also known as Digital forensic science), a branch of forensic science, is the discipline that aims at fighting against such criminals and criminal activities encompassing the recovery and investigation of material found in digital systems. In this course, we specifically focus on extraction, handling and forensic management of digital evidence from both system and network perspectives.

## Texts:

Digital evidence and computer crime, Eoghan Casey, 2nd edition, Academic Press, 2004, ISBN-13: 978-0-12-163104-8, ISBN-10: 0-12-163104-4

## References:

The instructor shall also provide written notes and slides for many topics. Notes and slides will be posted either on the course website (<http://jjcweb.jjay.cuny.edu/ssengupta/>) or on the course's Blackboard site. References to current articles from journals, magazines and other websites may also be used.

## Syllabus:

The following is the tentative course syllabus. This may change depending on time available, student and instructor expectations, student feedbacks as we progress in the semester.

- Digital Evidence
- The investigative process
- Investigative reconstruction process
- Computer basics for digital investigators
- Forensic Examination of Windows systems

- Forensic Examination on the Internet
- Wireless security/ investigating Wi-Fi
- Investigating computer intrusions
- Steganography

### Grading:

This is a tentative grading division. This may change later and will be updated.

- Assignments: ~ 30%
- Mid-term exam : ~ 20%
- Take Home Final : ~ 25%
- Project (Term paper) and project presentation: ~ 25%

Assignments include simple problem solving, hands-on labs (investigation) and investigation document preparation.

Project (term paper) is your own research paper chosen from any topic within the area of this course. It should reflect your original thought and optimal length is between 25 ~ 30 pages including figures, tables and references. (Follow the format of papers from "International Journal of Digital Evidence."). This term project includes 20 minutes presentation to the class and demo (if any). You can choose to do the term project individually or collaborate with another colleague. It is expected that the collaboration project will show synergy.

### Other Points:

1. Please use "FCM 760 <YOUR SUBJECT>" in the subject line in the emails.