**Instructor Contact Information**
Name: Sanjay Goel  
Affiliation: Assistant Professor, School of Business & Director of Research, CIFA, University at Albany  
Email: goel@albany.edu  
Phone: (Goel) 442-4925  
Office Location: BA310b  
Office Hours: (Goel) M 11:30pm - 1:00pm

**Guest Instructors**

| Fabio R. Auffant II  
Technical Lieutenant  
NYSP Computer Crime Unit | Adnans Baykal  
NYS Office of Cyber  
Security & Critical  
Infrastructure Coordination | Damira Pon  
NYS Center for  
Information Forensics  
& Assurance | Sean Smith  
NY Prosecutors  
Training Institute |

**Class Information**
Time: 9AM – 4 PM  
Location: Earth Sciences Building - B19  
Dates: April 13-14 (Friday and Saturday)

**Resources**
Website: http://www.albany.edu/~goel/classes/spring2007/inf742/

Text and References: There is no specific text for the class. There are however several reference books which you may consult and readings that you have to finish for the class.

References:

Readings: TBD

**Course Description**
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 hackers. The course provides students with training in collection and preserving evidence from computers and networks. Specifically students learn procedures for identification, preservation, and extraction of electronic evidence. 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 an expensive tool. Finally, ethics, law, policy, and standards concerning digital evidence are discussed in the class.

**Project and Assignments**
Students will receive in class assignments as well as a take home project/exam which will be due May 13, 2007. For in class assignments forensics software will be loaded on to the computers in the lab or provided to the students on disks. For take home project/exam students would need to install the software on their own computers or on lab computers at the University.
**Grading**
Grading will be 50% class participation/assignments/quizzes and 50% take-home project/exam.

**Class Schedule**

**Day 1**
- 9:00 – 9:30: Introductions
- 9:30 – 10:30: Introduction to Computer Forensics
- 10:30 – 10:45: Break
- 10:45 – 12:15: Collecting Evidence: Physical & Digital
- 12:15 – 1:30: Lunch
- 1:30 – 2:45: Email & Internet Tracing
- 2:45 – 3:00: Break
- 3:00 – 4:30: File Systems & Evidence Artifacts

**Day 2**
- 9:00 – 10:30: Forensics Lab I
- 10:30 – 10:45: Break
- 10:45 – 12:15: Forensics Lab II
- 12:15 – 1:30: Lunch
- 1:30 – 2:30: Post Intrusion Analysis
- 2:30 – 2:45: Break
- 2:45 – 3:45: Legal Issues
- 3:45 – 4:00: Summary