

**INF 742: Computer Forensics**  
**University at Albany, State University of New York**  
**Spring 2007 Syllabus**

**Instructor Contact Information**

Name: Sanjay Goel

Affiliation: Assistant Professor, School of Business & Director of Research, CIFA, University at Albany

Email: [goel@albany.edu](mailto:goel@albany.edu)

Phone: (Goel) 442-4925

Office Location: BA310b

Office Hours: (Goel) M 12:30pm - 2:00pm

<b>Guest Instructors</b>			
Fabio R. Auffant II Technical Lieutenant NYS Computer Crime Unit	Adnan Baykal NYS Center for 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 - 219

Dates: April 20-21 (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:

Nelson, B., Philips, A., Enfinger, F., and Steuart, C., *Guide to Computer Forensics and Investigations*, 2<sup>nd</sup> Ed., Canada: Thomson Course Technology.

Middleton, B., *Cyber Crime Investigator's Field Guide*, New York: Auerbach Publications.

**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 and academic/demo versions are not available. 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. 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.

## **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 – 1:15 Lunch  
1:15 – 2:30 Email & Internet Tracing  
2:30 – 2:45 Break  
2:45 – 4:15 File Systems & Evidence Artifacts  
4:15 – 4:30 Break  
4:30 – 6:00 Legal Issues in Forensics

### **Day 2**

9:00 – 10:30 Forensics Lab I  
10:30 – 10:45 Break  
10:45 – 12:15 Forensics Lab II  
12:15 – 1:15 Working Lunch (Complete Labs)  
1:15 – 2:30 Post Intrusion Analysis (using Ethereal)  
2:30 – 3:00 Summary