

# FCM 745: Network Forensics

*Prof. Ping Ji, Fall 2008*

Master's Program in Forensics Computing  
Department of Mathematics and Computer Science  
John Jay College of Criminal Justice,  
City University of New York

**Meeting Time & Place:** Tuesday, 6:20 – 8:20pm, Room 4100N

**Instructor:** Prof. Ping Ji

Office: 4230N

Phone: 212-237-8841

E-mail: [pji@jjay.cuny.edu](mailto:pji@jjay.cuny.edu)

Office Hour: Tuesday, 2:30 – 4:30pm, or by appointment.

**Text Book:** There is NO specific text book for this course. Reading materials will be assigned through the semester. A few recommended book readings are as follows:

1. *Tao of Network Security Monitoring – Beyond Intrusion Detection*, Richard Bejtlich, published by Addison Wesley, ISBN 0-321-24677-2
2. *Digital Evidence and Computer Crime – Forensics Science, Computers and the Internet*, Eoghan Casey, published by Elsevier, 2<sup>nd</sup> Edition, ISBN 0-12-163104-4.
3. *Cyber Crime Investigator's Field Guide*, Bruce Middleton, published by Auerbach Publication, 2<sup>nd</sup> Edition, ISBN 0-8493-2768-7

**Class Website:** <http://web.jjay.cuny.edu/~pji/fcm745.html>

**Course Description:** This course assumes students with knowledge in Computer Networks and Security, Operating Systems, Basic Statistics and acquainted with at least one programming language. The first part of this course is organized in traditional lectures, which cover Network Monitoring and Measurement Tools for network traffic collection and investigation, and Data Processing and Forensics technologies for Internet based applications. The second part of the course is organized in seminars, which will explore advanced topics in Network Security and Forensics. Students will have chance to study and present state-of-art works in the field that are particularly interesting to them, and work on research projects accordingly. Topics of interests include but are not limited to:

- **Part I. The Fundamentals (Traditional Lectures)**
  - Internet Trace Related Log Files
  - Network Security Monitoring and Management Techniques
    - Network Monitoring Techniques and Products (e.g., TCPdump, Snort, Ethereal, Honeypot, etc)
    - Network Monitoring Processes
    - The Intruder vs Network Security Monitoring
  - IP Traceback, Stepping Stone Detection
  - Anonymity
  - Security and Forensics in Wireless Network Environment

- **Part II. Advanced Topics (Seminars)**
  - Intrusion Detection Systems (IDS)
  - VoIP Security
  - Multimedia Forensics and Multicast Fingerprinting
  - Steganography and Stegnoanalysis
  - Pseudonymity, P3P and Various Camouflaging Techniques
  - Wireless Forensics

The above topics (and the order of the knowledge being introduced) are subject to change based on students' feedback and coordination with other courses in the Master' Program of Forensics Computing.

**Course Workload:** Three programming projects will be assigned through the semester, in addition to a relatively large Final Project. Students are responsible for choosing the Final Project topic on their own. However, the instructor will help the students to identify a reasonable task to work on. One in-class Midterm will be given. In addition, each student is required to present more than two assigned papers chosen from the reading list. A student may choose to present a topic that he/she is most interested in. However, the papers are assigned to students for presentations on a first-come-first-serve basis, which means if two or more students are interested in presenting the same set of papers, the student who requests the topic first will get the chance to present the corresponding papers. Course workload and grading scale are specified in the following table. Please note, not finishing ANY of the course works will result in an INC or an F in final grade.

Programming assignments	3 times	30%
Paper presentation	Once (more than 2 papers)	15%
Midterm	1	25%
Final project	1	30%

Comments: [pji@jjay.cuny.edu](mailto:pji@jjay.cuny.edu)