

# CSc82100: Network Forensics

*Prof. Ping Ji, Spring 2009*

Ph.D. Program in Computer Science, Graduate Center  
City University of New York

**Meeting Time & Place:** Thursday, 11:45am – 1:45pm, in Room 4422

**Instructor:** Prof. Ping Ji

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

Office: 4439

Office Hour: Thursday, 2:30 – 3:30pm, 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:

1. *Real World Linux Security*, Bob Toxen, Prentice Hall, ISBN 0-13-046456-2
2. *Tao of Network Security Monitoring – Beyond Intrusion Detection*, Richard Bejtlich, Addison Wesley, ISBN 0-321-24677-2
3. *Wi-Foo – the Secrets of Wireless Hacking*, Andrew Vladimirov, Konstantin Gavrilenko, Andrei Mikhailovsky, Addison Wesley, ISBN 0321202171

**Class Website:** <http://web.jjay.cuny.edu/~pji/csc82100.html>

**Course Description:** This course assumes students with basic knowledge in Computer Networks, Operating Systems, Statistics and acquainted with at least one programming language. The first part of this course is organized in traditional lectures, which cover topics including Monitoring and Measurement principles and tools for network traffic collection and investigation, Anonymity and other camouflage techniques, IP-trackback and stepping stone detection, IP-prefix Hijacking, Accountability, In-depth Packet Analysis, Wireless Networks and its Security, Spam inspection and Intrusion Detection and Response. The second part of the course is organized in seminars, which will explore most recent research in Network Security and Forensics. Students will also have chance to study the state-of-art research in the field that is particularly interesting to them, and work on research projects accordingly. A final course project is required.

**Course Workload:** One in-class exam will be given on Apr. 23, and a Final Project is required. 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. In addition, each student is required to present more than two research papers chosen from the reading list or on their own. Students are encouraged to present topics that they are most interested in as well as topics related to their final projects. Course workload and grading scales are specified in the following table. Please note, not finishing ANY of the course work will result in an INC or an F in final grade.

In-Class Exam	1	40%
Paper presentation	Once (more than 2 papers)	20%
Final project	1	40%