CS-585F: Computer-Related Law and Computer Forensics, FALL 2002 Semester

Course Syllabus

Summary Course Description:

Basic principles of the American legal environment: the United States Constitution, various court systems and jurisdictional issues, and handling and resolution within the legal system of conflicts (lawsuits). Civil rights, privacy, and defamation. Aspects of the legal environment particularly relevant to computers. Civil responsibilities and liabilities of hardware vendors, software vendors, and computer service providers. Criminal liability. Intellectual property issues: trade secrets, patent, trademark, and copyright. Misappropriation of information.

Identification, preservation, extraction, and interpretation of information present on computer storage media to analyze what transpired in a computer security incident, to determine the identities of the perpetrators, and to provide evidence admissible in court. Techniques used to determine whether any criminal activity might have occurred and to acquire the evidence necessary for prosecution while avoiding alteration of or damage to the original data. Analysis of the content of recovered evidence, and authentication of its selfsameness to the data originally seized. The inner workings of fixed (i.e., hard) disk drives and of other electromagnetic, optical, and other storage media. Encryption, steganography, and other techniques used to hide data within computer systems. Computer viruses, Trojan Horse software, and other malware (hostile code). Various software tools useful for forensic examination. Forensic investigative techniques useful in the Microsoft ***Windows*** environment and in the ***UNIX/Linux*** environment. Procedures for rapid intervention in and response to security incidents so as to preserve the integrity of the evidence while deterring the production of further damage.

Required Textbooks:

1. ROSENOER, JONATHAN (1997). *CyberLaw: The Law of the Internet.* New York, NY: Springer. KF390.5.C6R668 1996; 343.73099'9—dc20; 96-25479; ISBN 0-387-94832-5 (hardcover).

2. KRUSE, WARREN G., II; & HEISER, JAY G. (2001). *Computer Forensics: Incident Response Essentials.* Boston, MA: Addison-Wesley. QA76.9.A25 K78 2001; 005.8—dc21; 2001-034106; ISBN 0-201-70719-5.

Recommended Supplementary Materials:

3. BICK, JONATHAN (2000). *101 Things You Need to Know about Internet Law.* New York, NY: Three Rivers Press (Random House). KF390.5.C6 B49 2000; 343.7309'944—dc21; 00-037726; ISBN 0-609-80633-5. [This is a delightfully written little monograph that provides easy-to-digest legal information, although it is non-rigorous and is lacking references, particularly to cases.]

4. GORDON, KAREN ELIZABETH (1993). *The Deluxe Transitive Vampire: The Ultimate Handbook of Grammar for the Innocent, the Eager, and the Doomed.* New York, NY: Pantheon Books. ISBN 0679418601. [This book is a concise, wittily written tutorial on the fine points of grammar and punctuation.]

5. DUPRE, LYN (1998). *Bugs in Writing Revised. A Guide to Debugging Your Prose.* Reading, MA: Addison-Wesley. ISBN 0-201 37921-X. [The author specifically addresses the needs of computer professionals and other technical people to write clearly.]

Learning Objectives:

By the end of this course, the student should be able to:

(1) Explain the major philosophies underlying and the major principles elucidated in the Unites States Constitution, and in particular those amendments known as the Bill of Rights.

(2) Explain the differences in definition between civil and criminal law.

(3) Explain the hodgepodge of Federal, State, and local courts in the United States legal system, and determine which court has jurisdiction in particular circumstances.

(4) Analyze the rights and obligations of various individual persons and organizations with regard to privacy, both in the customer-vendor/service provider environment and in the employer-employee milieu.

(5) Adjudicate questions of copyright and other intellectual property issues as they apply in the computer environment.

(6) Identify, preserve, extract, and interpret information present on computer storage media in a Microsoft ***Windows*** environment, and analyze what had transpired in the course of a computer security incident, while simultaneously preserving the evidence in a form usable in court and resistant to attack by defense counsel.

(7) Identify, preserve, extract, and interpret information present on computer storage media in a ***UNIX/Linux*** environment, and analyze what had transpired in the course of a computer security incident, while simultaneously preserving the evidence in a form usable in court and resistant to attack by defense counsel.

(8) Analyze the information obtained following a computer security incident, both to determine whether any criminal activity might have occurred and to identify the perpetrators.

(9) Testify effectively in court as an expert witness, both to authenticate and to interpret the evidence.

(10) Utilize appropriate software tools to recover data that may have been hidden by the perpetrator or malfeasant using cryptographic or other techniques.

(11) Intervene in and respond to security incidents so as to preserve the integrity of the evidence while deterring the production of further damage.

Instructor:

Dr. Charles Abzug

Course Practices.

Grading Policy.

Homework.

Philosophy Regarding Classes Missed by Students.

Class Meetings:

Classes meet during the Fall 2002 semester on Wednesday evenings from 1800 to 2030 hrs in ISAT/CS Room 243.