CS 493/693 Exam 2
Fall 2005

Name: _____

You may use any resource (books, internet, notes, etc) as long as you complete this exam without help from anyone else. You must give this exam to me (in person or e-mail) by 6:50 pm on Tuesday November 22. All questions are worth 20 points. Your grade on questions 1, 2 and 4-6 will be based on a ranking of all the responses. Good luck.

1. Find a case where the accused was acquitted (or had the case overturned on appeal) based on improper handling of a computer hard drive. Give a 1-2 paragraph summary of the case. What went wrong? What should the investigator(s) have done?

2. Find two states that have used electronic voting (I'll define this as a no per-ballot piece of paper generated) in an election. Describe their process for doing a "re-count". How would you, as a computer forensics expert, attack the results if your client lost of the election?

3. What is "salt" with respect to passwords? Is salt used anywhere in Windows XP?

4. Give the detailed steps you would take to show a file on my laptop was intentionally and knowingly possessed by me. Assume you have root access and are authorized to do this investigation.

5. What are the pros/cons of management running a password cracker on UAF e-mail passwords? What are the dangers of doing this with respect to the DMCA? Are there better ways to ensure that users are using "good" passwords?

6. Find the smallest worm (in terms of bytes that had to be sent to another host) that caused denial-of-service on at least 100 hosts. How did it work and could you have made it smaller?