

CS 493/693 Final Exam
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 7:45pm on Thursday Dec 15. I will be out of town Dec 10 – 14, but will be available via e-mail. Your grade on each question will be based on a ranking of all the responses. Good luck.

1. What is your definition of computer forensics? Explain why you included what you did and why you left anything out (that you might find in other people's definitions of computer forensics.) (20 points)
2. What is the difference between an evidence file (from EnCase) and a mirror-image copy? What are the pros/cons of each? (20 points)
3. Today, does a law enforcement officer (LEO) need a court order to access stored e-mail on a server? unread e-mail on a server? e-mail downloaded and stored on a PC? In other words, if an LEO gets this information without the permission of the owner of the data, is it valid in court? (20 points)
4. We've looked at some of the problems and benefits of electronic voting. There is also a desire to have voting via the internet. For such a system to be accepted, the voter must be convinced that their vote will count, be anonymous and be auditable. Candidates must be convinced that the votes are counted accurately. Explain how to design such a system. You may use/modify a proposed system by someone else as long as you document what they proposed and how you would be modifying it (if at all). Finally, explain how your system would provide fast and accurate tallies, feedback to the voter to verify who they voted for, and the ability to do a real re-count (i.e. not have a machine spit out the same numbers it did in the first place.) (60 points)