CS 493/693 Exam 1
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 October 11. All questions are worth 20 points. Some of these questions may not have an answer – what I am looking for is how you would approach the problem and the probability of success of that approach. Your grade on questions 1 and 4 will be based on a ranking of all the responses. Good luck.

1. List all of the digital evidence you might leave if you left Chapman, walked over to the UAF library and checked out a book, walked to the Wood Center and bought a slice of pizza and then spent 1 hour enjoying a beverage in the pub. For each piece of evidence, rate the likelihood of it being captured on a scale of 1 to 10.

2. Pick any computer system and an application that runs on it. How would you determine what files were created/modified while the application ran? Show any command(s) used and the results.

3. How long would it take to you find/create a file with the same MD5 signature as a file provided to you? Clearly state any assumptions that you make.

4. Give the steps (make it as *complete* as possible) to seize a disk drive from a PC in a way that will stand up in court.

5. What are the danger(s) involved in doing a live system review before making a forensic copy of the system disk drive(s)? How do you determine the accuracy of the date/time stamps on the system disk drive(s)?

6. The Melissa virus author was discovered via an ethernet address hidden in a MS Word document. Provide a 2-3 paragraph summary of the computer forensic techniques used to track down the author.

7. Should connecting a laptop to a UAF video projector make that person a “user” of UAF “Information Resources” and therefore subject to BOR regulations? Justify your position using common sense and BOR regulations/policy.