Name: **AndrewId:**

15-498 Spring 2011
Homework #1

Note: Please submit your solutions electronically, in .pdf format, into the handout/hw1 directory. Please name your submission andrewid.pdf (or, if you resubmit, andrewid.1.pdf, andrewid.2.pdf, etc).

1. As the prosecution investigates a case, it develops a theory as to the events and the actions of potential suspects. What is the goal of the prosecution team with respect to proving the case?

2. Question #1 discussed the goal of the prosecution. This question asks, what is the goal of the defense with respect to the prosecution's theory?

3. Consider your answers to questions #1 and #2. How might this difference in goals lead the prosecution experts, and the defense experts, to take different approach?

4. What is the *chain of evidence*? How is it preserved?

5. What is an investigative protocol? Why is it important? (*Hint:* Please provide multiple reasons.)

6. What are the three most important causes of disk failure (neglect cabling and external issues)?

7. What are the three most common causes of failure on CD-RW and DVD-RW disks?

8. What is more robust, a USB flash drive or a pressed CD? Why?

9. What time stamps are held within the metadata of an ext2 file system? Where are they stored?

10. If the inodes of an ext2 file system are deleted, might it be possible to recover a significant number of whole files? Why? Or why not?

11. True or false? And why? FAT is dead.

12. Trick question (You were warned): What contains more metadata? The NTFS change log or the ext3 log? Please explain and support your answer.

13. You are presented with a hard drive. The partition is HFS+. A critical file has been deleted. You know the name and the file type. How do you approach the recovery?