CS 393 Mid-term Exam

Name: ________________________ Posting Code: ______________________

You may use any resource (books, internet, notes, etc) as long as you complete this exam without help from anyone else. You must turn in this exam by 4:30 pm on Friday March 14. 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. Questions 1-11 are 10 points each and question 12 is 20 points. Good luck.

1. What is a "protected computer"? What amount of monetary damage to a protected computer system is necessary to violate the Computer Fraud and Abuse Act (18 USC 1030)? What factors can be included in this cost?

2. What is a cryptographic checksum and how is it used?

3. How would you go about creating two files with the same MD5 signature?

4. Compare and contrast these methods for system logging: logging to a remote host, logging to a write-once media and logging to a line printer.

5. What are the danger(s) involved in doing a live system review before making a forensic copy of the system disk drive(s)?

6. Describe in detail how you can hide data in the slack space. What do you need to do to keep it from being overwritten? From being discovered?

7. What is the US Computer Assistance Law Enforcement Act? Does a department computer lab manager need to worry about it?

8. Give the steps to seize a disk drive from a PC in a way that will stand up in court.

9. A forensic copy was made before sealing the original disk drive in an evidence bag. The copy has been damaged and another one needs to be created. What should you do?

10. What actions are made illegal in the UA BOR Regulations on Information Resources?

11. How many different combinations are possible for 10 character passwords (without salt) where the characters are limited to [a-zA-Z0-9]? How many attempts per second are needed to brute-force this in 1 week? Is there a system out there that can do it?

12. A case example on page 61 in Casey describes how the Melissa virus author was discovered via an Ethernet address hidden in a MS Word document. Give the pros/cons of this from the viewpoint of a forensics investigator. Should all documents contain this information (i.e. do the pros outweigh the cons)?