Case Scenario

Today is September 15, 2004. The time is 3:15 PM. Mr. Jim Boss, the owner of the Really Big Company called and you responded to his office. Mr. Boss advised that he suspected that his assistant, Emma Crook, was providing company sensitive material to some of his competitors. At 2:00 PM today he confronted Ms. Crook with his suspicions. He told her that he would be back at 3:00 PM for an explanation. When Mr. Boss arrived back at Ms. Crook's office at 3:00 PM, she was gone. Her office was completely cleaned out of all of her belongings. Mr. Boss tried to turn on Ms. Crook's computer, but it would not boot. Mr. Boss found a floppy diskette in the trash can. Mr. Boss wants you to examine the computer and the floppy diskette and to tell him exactly what Ms. Crook was up to. He is willing to pay for a 100% thorough examination. "Leave no stone unturned" as he said.

You examined the computer and found that the hard drive was missing. The computer was not networked. Your only evidence, if any, will be on the floppy diskette. You checked the system clock and it was accurate to within one minute.

Pre Analysis Steps

- Check the system clock is accurate
- Write protected the diskette
- Start and maintained a physical chain of custody - Explain your procedures
- Run a hash or checksum on the original media and noted the value
- Wipe and verify the wipe of the target media
- Make an exact copy of the original media to the wiped and verified media.
- Run a hash or checksum on the original media again and the value matched the original value
- Run a hash or checksum on the target media and the value matched the original value

Questions

1. Was the disk formatted? - give reasons for your answer.
2. Use a carving utility, how many documents were carved from unallocated space?
3. List the documents carved out.
4. What was the original name of the documents?
5. Who was the author of the documents?
6. When were the documents last saved?
7. What do the documents contain?
8. Which document is password protected?
9. What is the password?