Puzzle for January 30, 2002

Your UNIX system has been attacked. The *uucp* entry in your /etc/passwd file has a UID of 0. You have run *ps* to see if any unusual processes were executing. None were. You ran *ls* to find any unusual files or directories. None were reported. You ran *du* to determine if the size of any file system was unusually large (indicating hidden files). Nope.

You suspect that someone has, somehow, hidden files (or directories) and an executing process. You decide to start at the /dev directory, to see if they created any new device files. Again, an *ls* lists only those files you expect to see. But you are still suspicious, and want to confirm the results.

1. What would you do?
2. You still suspect that the attacker left an illicit process executing. But *ps* showed nothing. How would you confirm or refute your suspicion?