You are an intern at the Monopoly Land Secret Service (MLSS) which deals with counterfeiting. You've been there 6 weeks and you have been working under star agent Sam McLastname. Mr. McLastname has shown you the ropes. He has shown you how to use Autopsy to look at file systems, Wireshark to do network forensics and Volatility to analyze volatile memory. He is working on a big case going after the infamous "not_a_counterfeiter6892". Don't be misled by the name, the user behind that username is actually an alleged counterfeiter. The MLSS has been working for years to unmask this suspect but they have managed to evade the MLSS unlike anybody else. However, Sam McLastname has an investigation prepared on his computer, he has finally found enough evidence to bring not_a_counterfeiter6892 to justice. He texts you that at 9 am the next day, he's going to send the evidence to the judge. So you anxiously wait at his desk, getting to work early for once at 8:30. You wait there for 30 minutes and he doesn't show up. Another 15 minutes pass and you begin to get worried, why would he be late on a day like today, by 9:30 you decide to go to the front desk to see if anybody has seen him. The receptionist hasn't seen him but hands you a postcard addressed to him. It read simply

That's what you get for getting too close
-not_a_counterfeiter6892

It is now your job to build a case against not_a_counterfeiter6892 and find Sam McLastname before it's too late.

Part 1: Specific Questions (30 points)

You are able to take a copy of Sam McLastname's disk, but before you put all the evidence together, there are also a few specific questions he has written down to answer.

1. How large is the file Monopoly_Money1.png in KB
    a. ANSWER 13.6
2. How many .jpeg files are marked as evidence
    a. ANSWER: 5 (there are 5 jpegs and 2 pngs)
3. What city is referenced in correspondence.pdf
    a. ANSWER: Tacoma
4. At what time (relative to the start of the packet capture) was the 253rd packet sent in suspect.pcap?
    a. ANSWER: At 11.719256213 seconds
5. What processes are running in Fake Monopoly Money Process.png
    a. Zsh, Fake Monopoly M, ps

Part 2: Investigation (50 points)

Using at least 3-5 pieces of evidence, write why you think not_a_counterfeiter6892 is or isn't guilty. Be creative

Part 3: Evidence Creation (20 points)

Pretend that you are designing an assignment. Write about what tools you would use to create evidence for a similar fake investigation.