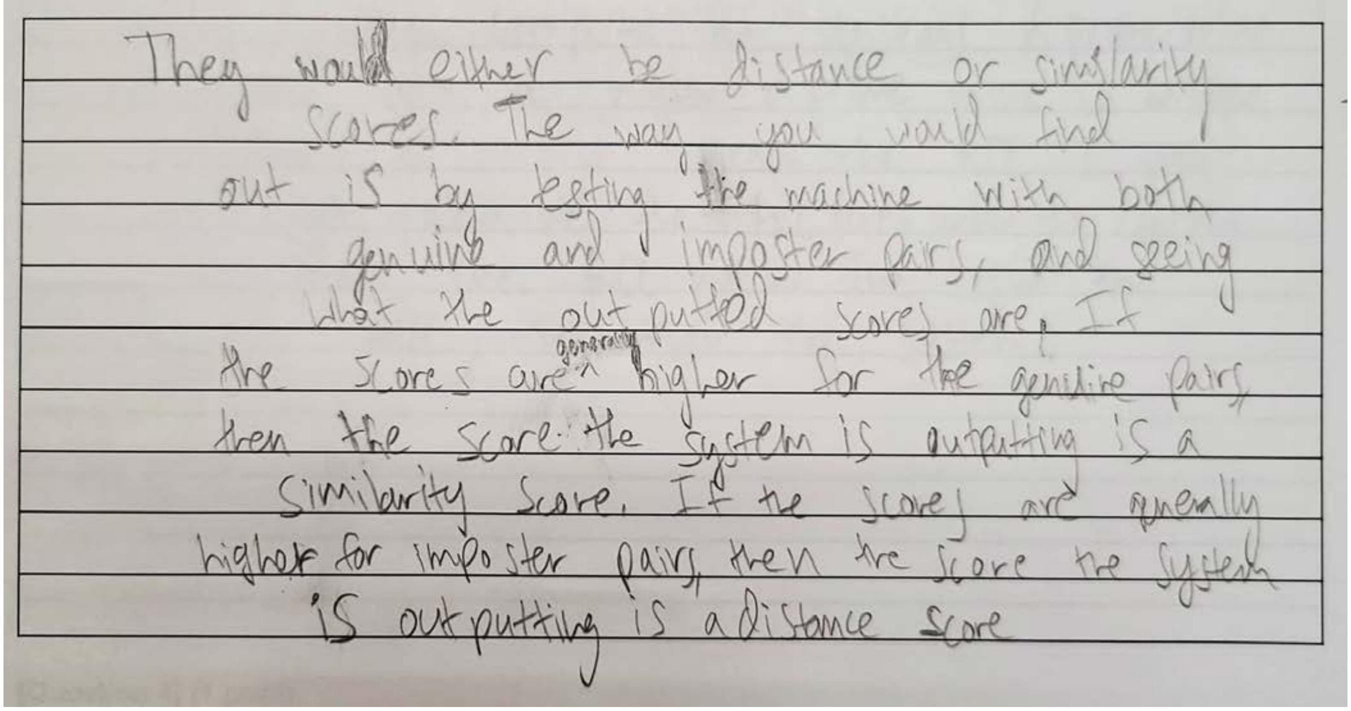
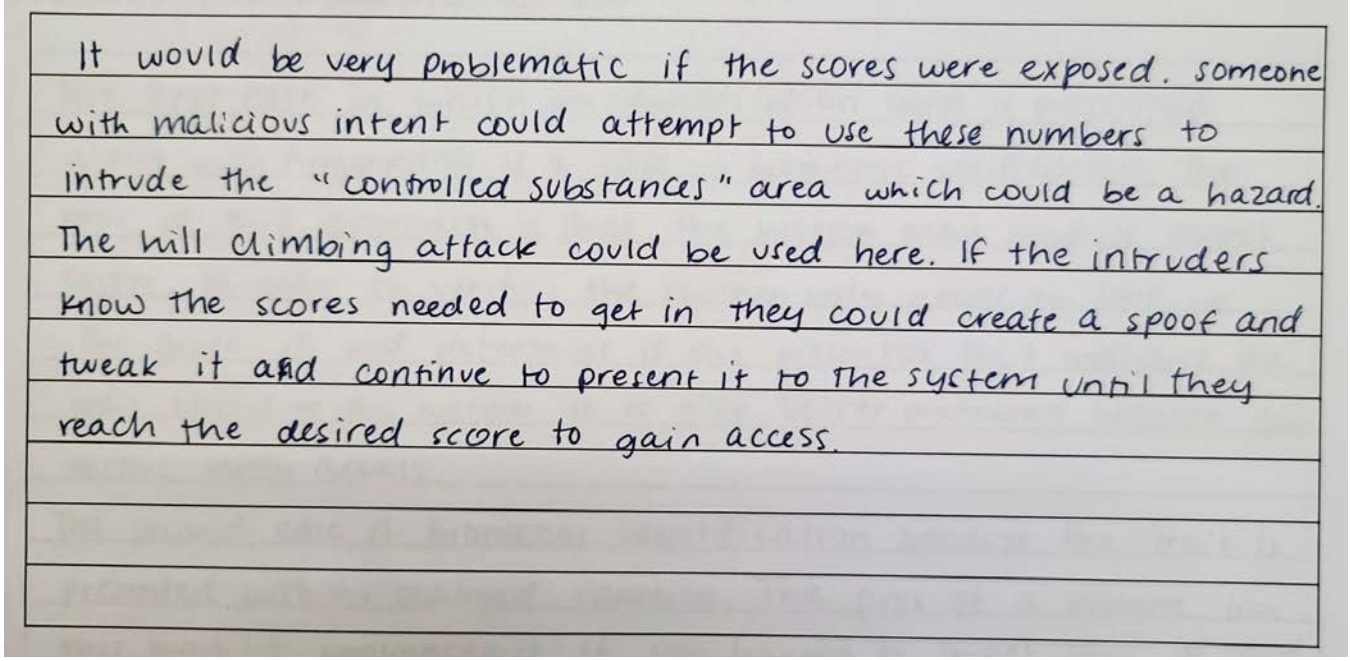
[Question 1] (1 point)
(...)

Without further information and based on your experience with biometric systems, what would the “Score” outputs in debug mode convey? If you were to investigate and establish their meaning (e.g., distance, similarity, confidence, etc.), how would you proceed? Please describe it in detail. Consider that you have the provided software fully operational and, therefore, you are able and free to enroll, identify, and verify as many individuals as you want, in either regular or debug modes.



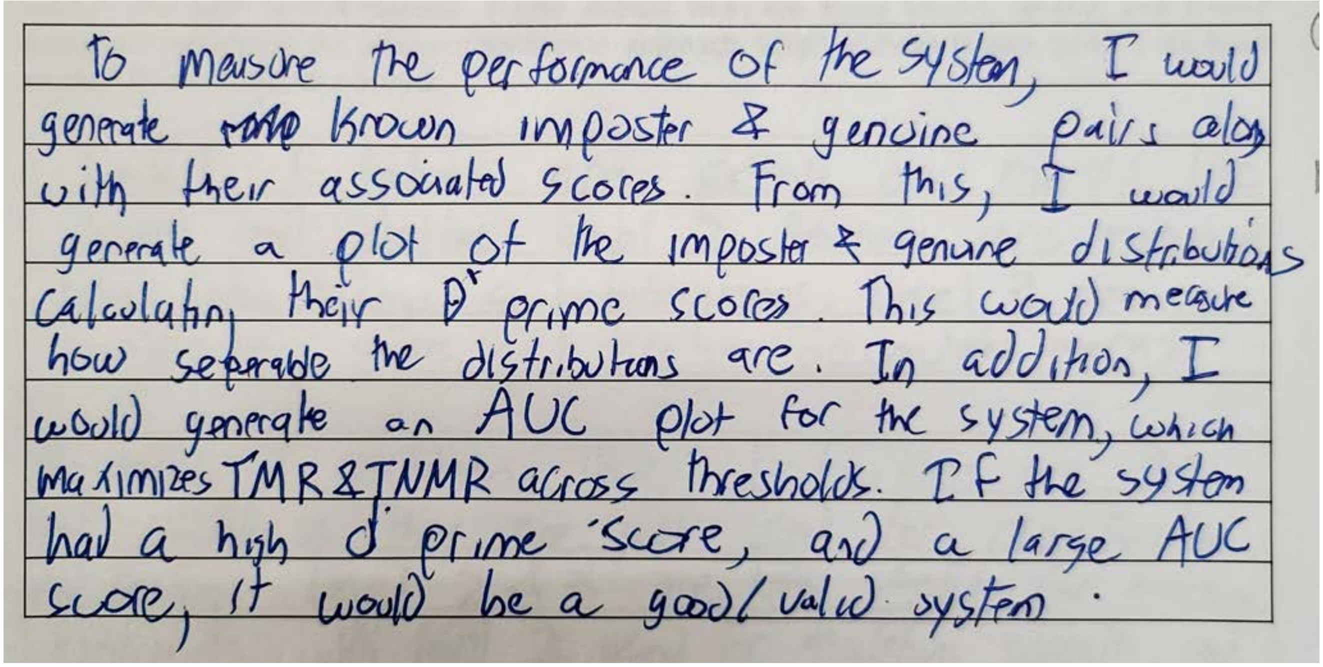
They would either be distance or similarity scores. The way you would find out is by testing the machine with both genuine and imposter pairs, and seeing what the outputted scores are. If the scores are generally higher for the genuine pairs, then the score the system is outputting is a similarity score. If the scores are generally higher for imposter pairs, then the score the system is outputting is a distance score

[Question 2] (1 point)
How problematic would it be to deploy this fingerprint recognition system in the production environment and let it run unwarily in debug mode? If someone were to exploit these exposed scores, how could they attack the system? Please explain in detail.



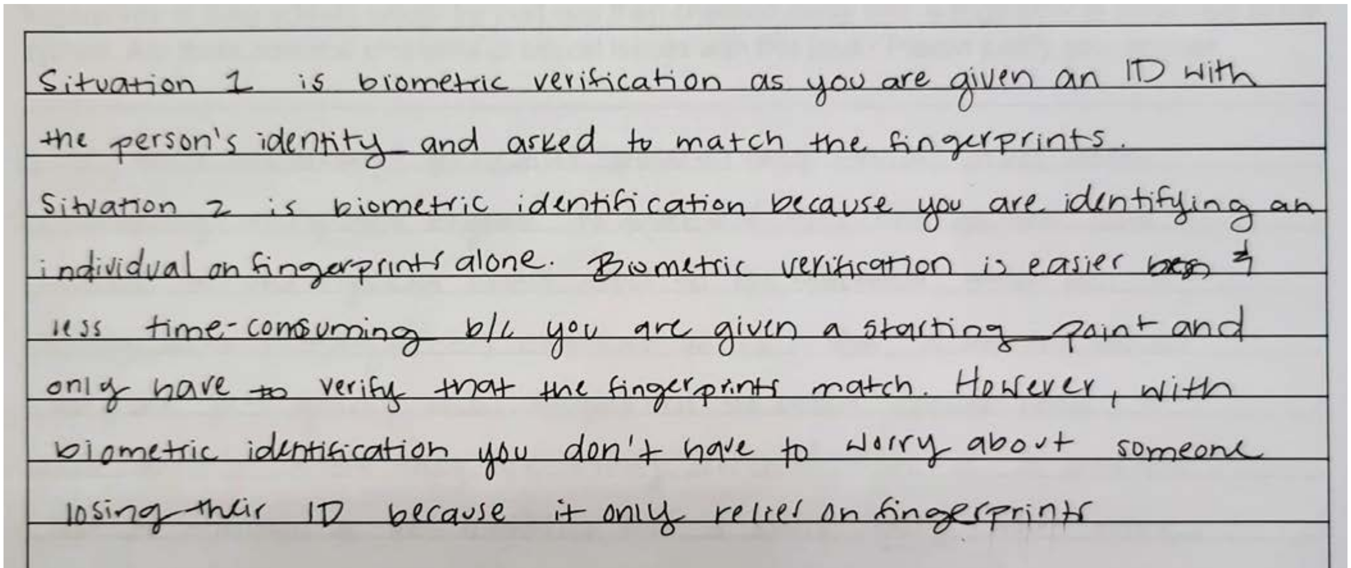
It would be very problematic if the scores were exposed. someone with malicious intent could attempt to use these numbers to intrude the “controlled substances” area which could be a hazard. The hill climbing attack could be used here. If the intruders know the scores needed to get in they could create a spoof and tweak it and continue to present it to the system until they reach the desired score to gain access.

[Question 3] (1 point)
Considering the type of the system's score (either similarity or distance), if you were to measure the performance of this solution, how would you proceed? Please describe what metrics you would report and what graphs you would generate.



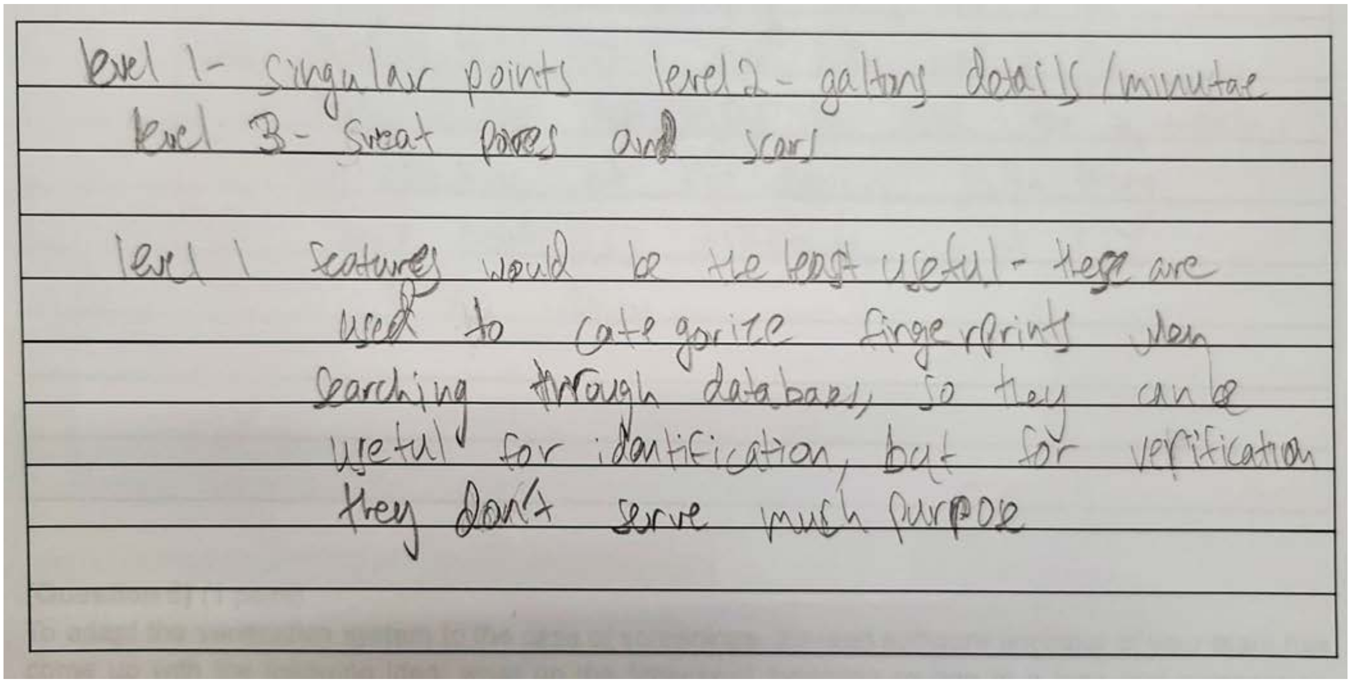
To measure the performance of the system, I would generate known imposter & genuine pairs along with their associated scores. From this, I would generate a plot of the imposter & genuine distributions calculating their D' prime scores. This would measure how separable the distributions are. In addition, I would generate an AUC plot for the system, which maximizes TMR & TNMR across thresholds. If the system had a high d' prime score, and a large AUC score, it would be a good/valid system.

[Question 4] (1 point)
The managers of the hospital chain have decided to acquire the fingerprint recognition solution. The discussion now involves (1) the need for presenting an identification card, along with the fingerprints, or (2) simply presenting the fingerprints and letting the system find who the person is. Which of these two situations is a case of **biometric verification** and which one is a case of **biometric identification**? What are the **pros** and **cons** of each approach?



Situation 1 is biometric verification as you are given an ID with the person's identity and asked to match the fingerprints. Situation 2 is biometric identification because you are identifying an individual on fingerprints alone. Biometric verification is easier & less time-consuming b/c you are given a starting point and only have to verify that the fingerprints match. However, with biometric identification you don't have to worry about someone losing their ID because it only relies on fingerprints

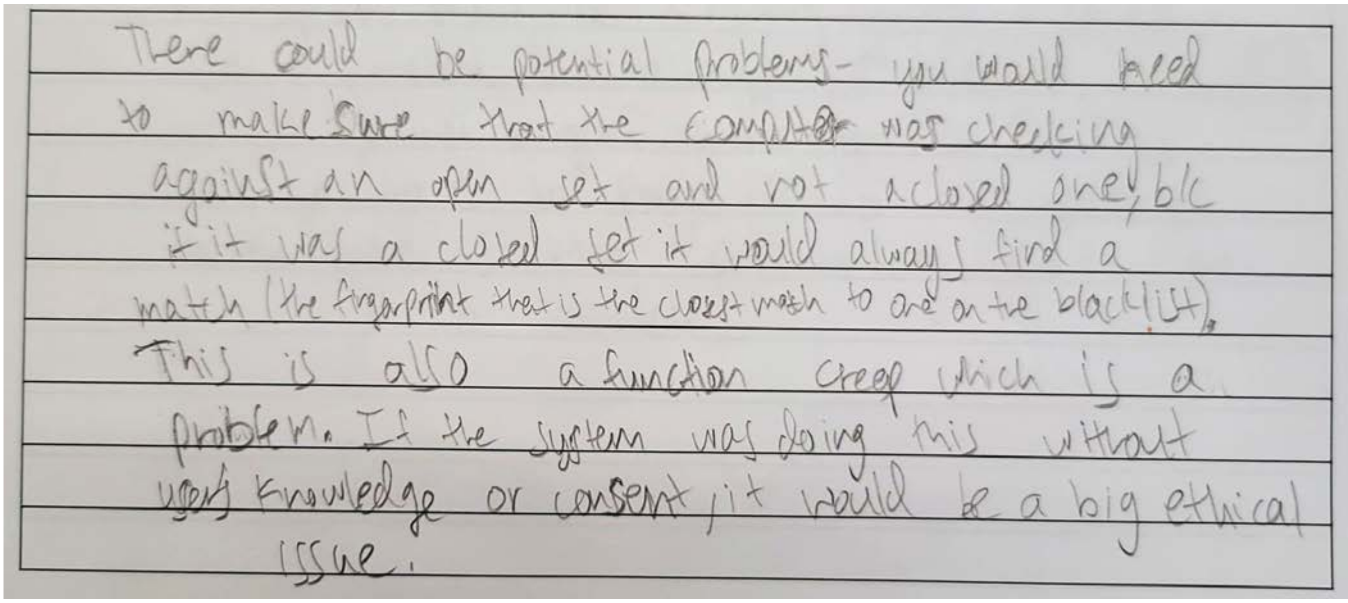
[Question 5] (1 point)
The managers have finally decided to adopt a biometric verification approach. They are planning to acquire a version of the system that uses a single-finger USB optical sensor, whose resolution is equal to 1200 ppi, and an identification card reader. The complete specs say the software provides level-1, level-2, and even level-3 features. Please explain **what are these level-1, level-2, and level-3 features**. Considering the biometric verification approach, which of these feature types is the **least useful**? Please justify your answer.



level 1- singular points level 2- galtons details /minutae
level 3- sweat pores and scars

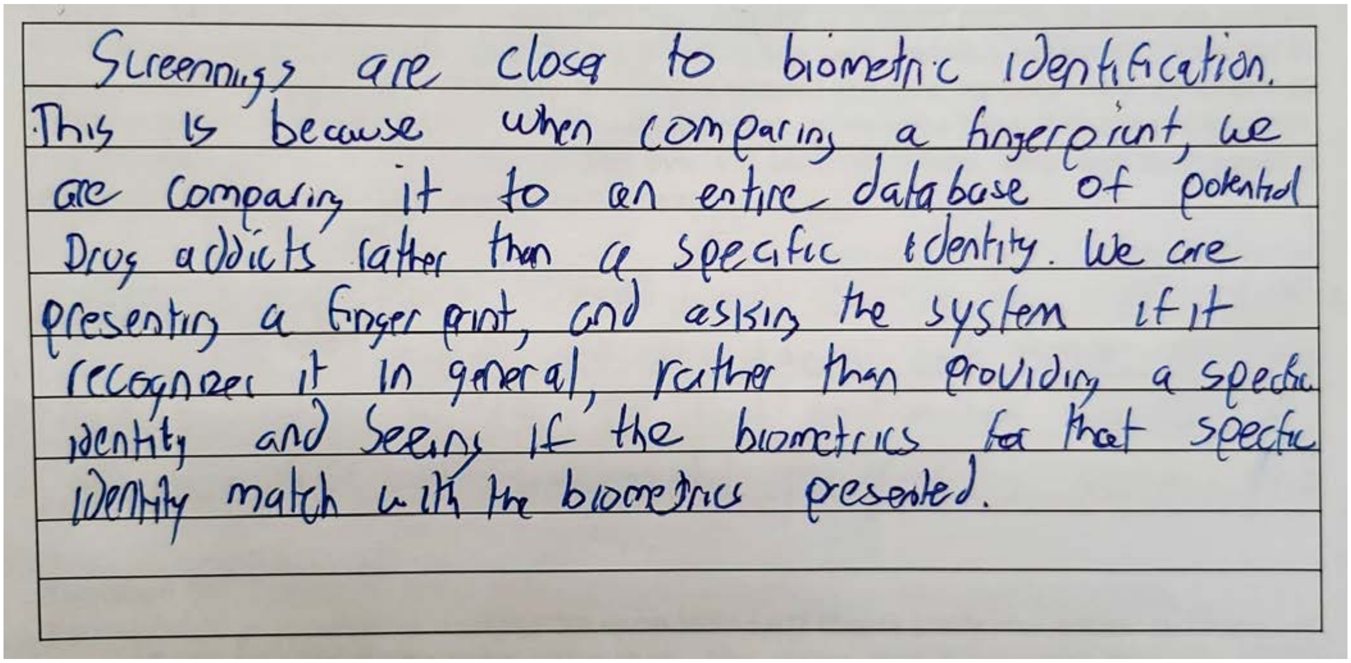
level 1 features would be the least useful - these are used to categorize fingerprints when searching through databases, so they can be useful for identification, but for verification they don't serve much purpose

[Question 6] (1 point)
After deciding to adopt a biometric verification approach, one of the hospital directors was wondering if it would be possible to extend the system usage to the case of *screenings*, where a blacklist with the fingerprints of drug addicts would be built and then checked every time a fingerprint is presented to the system. Are there potential problems or ethical issues with this idea? Please justify your answer.



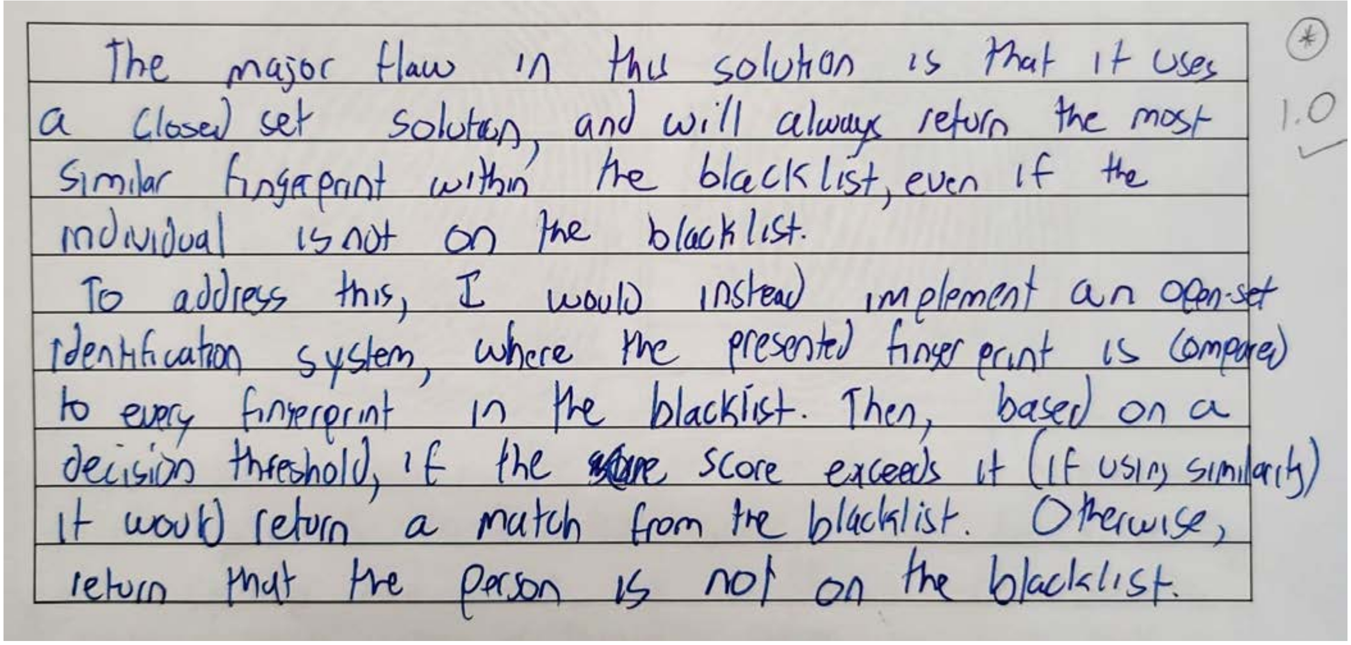
There could be potential problems- you would need to make sure that the computer was checking against an open set and not a closed one, b/c if it was a closed set it would always find a match (the fingerprint that is the closest match to one on the blacklist). This is also a function creep which is a problem. If the system was doing this without users knowledge or consent, it would be a big ethical issue.

[Question 7] (1 point)
Regardless of the problems and ethical aspects, **are screenings closer to biometric verification or biometric identification?** Please explain your answer.



Screenings are closer to biometric identification. This is because when comparing a fingerprint, we are comparing it to an entire database of potential Drug addicts rather than a specific identity. We are presenting a fingerprint, and asking the system if it recognizes it in general, rather than providing a specific identity and seeing if the biometrics for that specific identity match with the biometrics presented.

[Question 8] (1 point)
To adapt the verification system to the case of screenings, the lead software engineer of your team has come up with the following idea: wrap up the fingerprint matching routine in a loop and compare an eventually presented fingerprint with every fingerprint template belonging to the blacklist. A drug addict's identity should be taken as the one whose template presents the largest level-2 similarity score with the presented fingerprint. **What is the major flaw in this solution? How would you fix it?**



The major flaw in this solution is that it uses a closed set solution, and will always return the most similar fingerprint within the blacklist, even if the individual is not on the blacklist.

To address this, I would instead implement an open-set identification system, where the presented finger print is compared to every fingerprint in the blacklist. Then, based on a decision threshold, if the score exceeds it (if using similarity) it would return a match from the blacklist. Otherwise, return that the person is not on the blacklist.

1.0 ✓

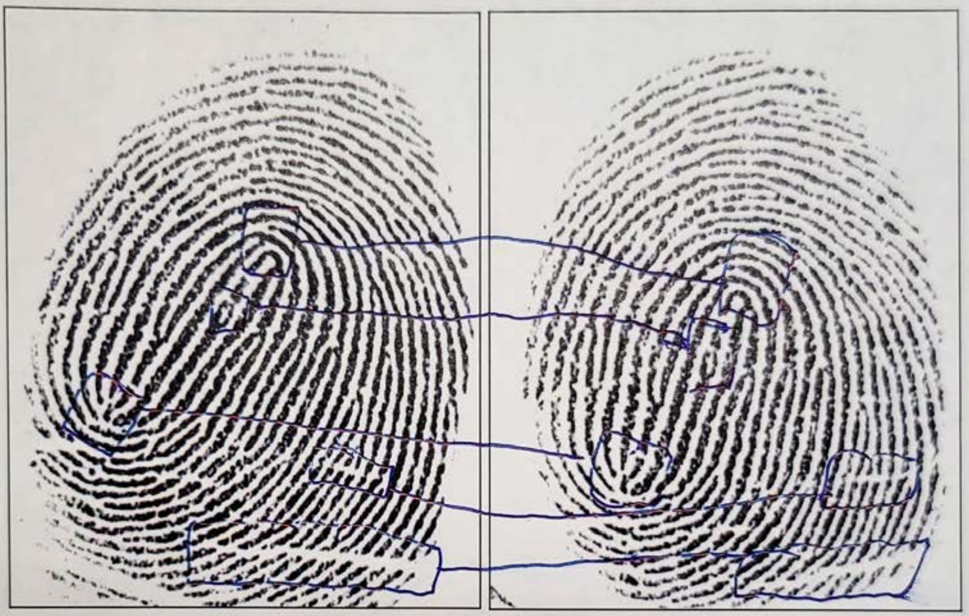
[Question 9] (1 point)

An actual case of a scientific paper submitted to a conference. While proposing a novel solution for fingerprint recognition, two authors devised an experimental setup where they collected many fingerprint slaps from all the fingers belonging to a large set of different people. To generate genuine and impostor pairs, they decided to adopt the following approach: impostor pairs were generated by pairing individual finger slaps belonging to different people, and genuine pairs were generated by pairing individual finger slaps belonging to the same person, to the same hand. With this configuration, they provided a ROC curve of their solution over the collected dataset. **Why was their paper a straightforward reject?** Please explain your answer.

Their paper was a straight reject because they are not matching the genuine pairs to the same finger only the same hand.

[Question 10] (1 point)

Are the two fingerprints below depicting the same individual? Please justify your answer by linking and naming 5 or more similar structures within them. After you've done this process manually, please **explain why it is useful and important to program computers** to do the same task.



Yes, these depict the same individual. It's important to use computer's to do the same task because they are quicker and make less mistakes to do the same matching task as humans. When you have millions of fingerprints, this becomes even more important.