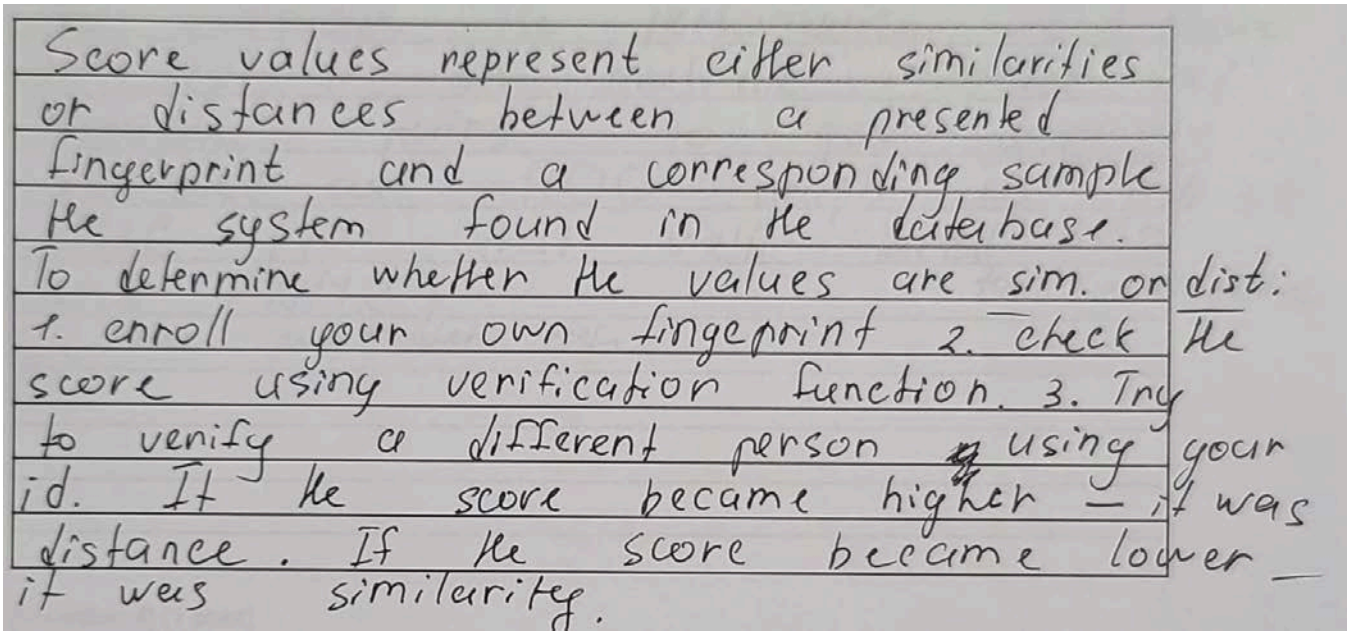
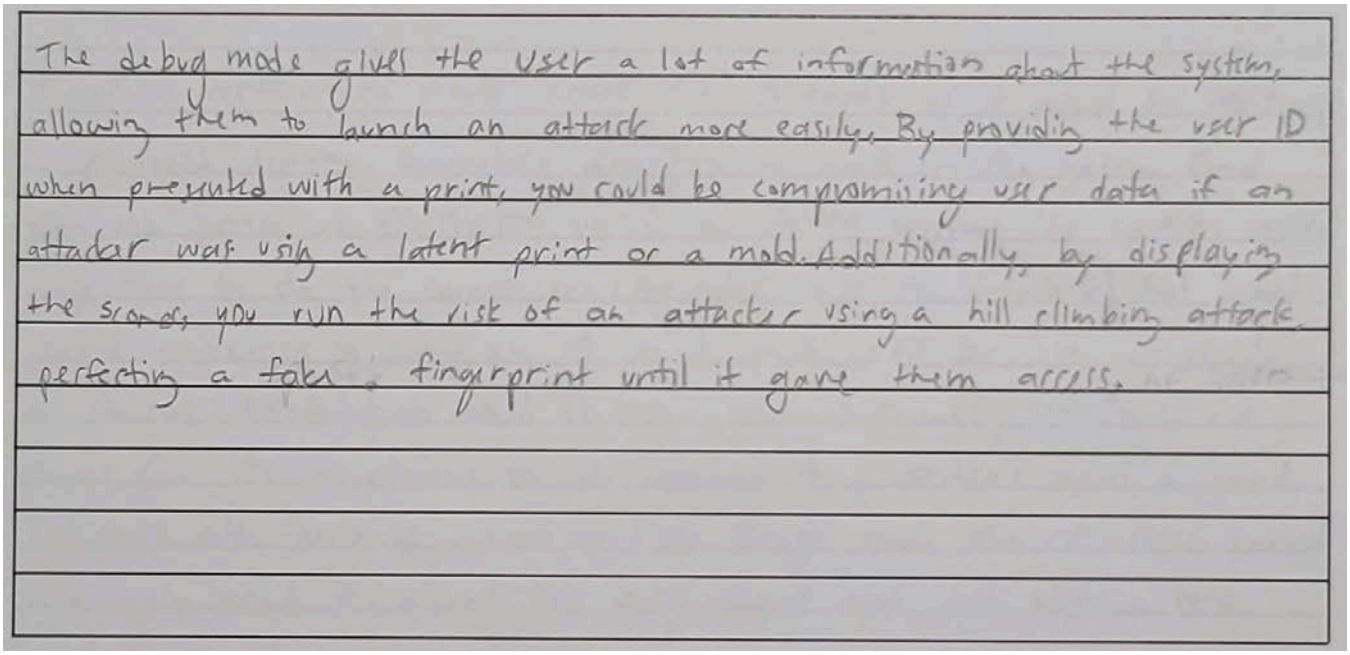
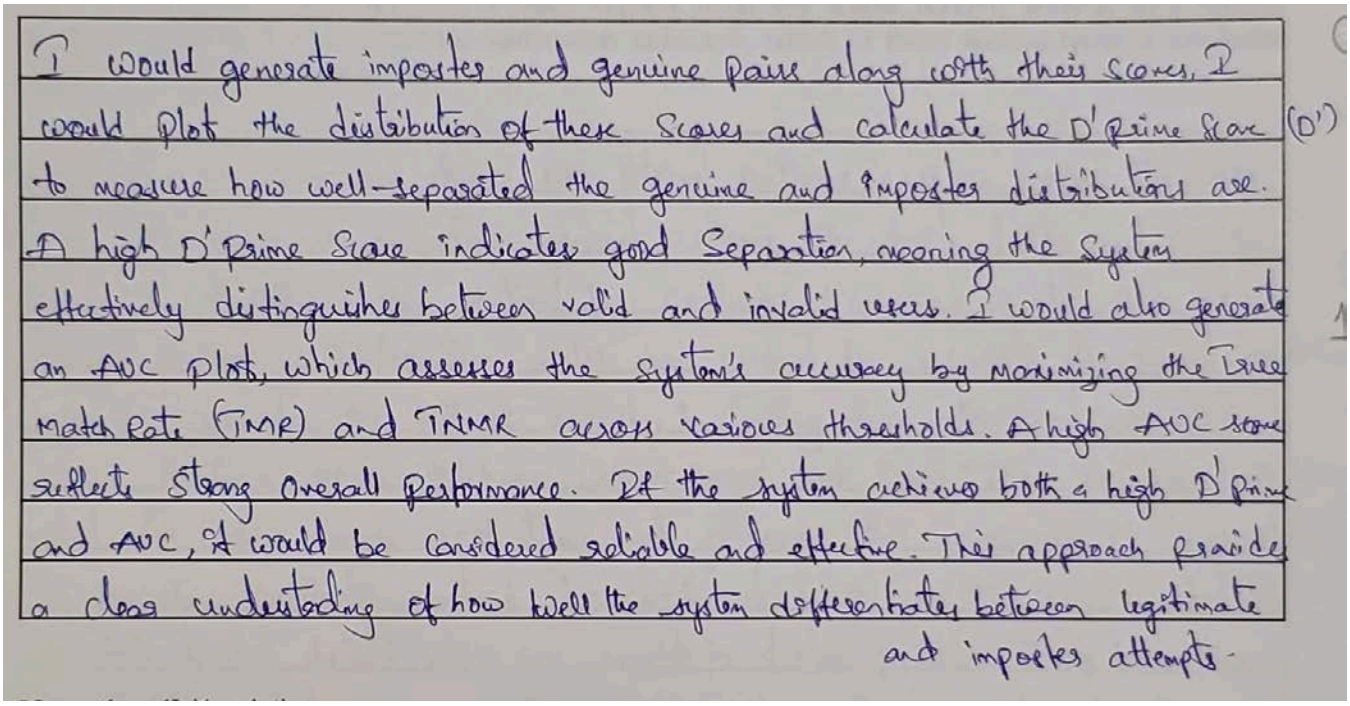
Based on your understanding of biometric systems, what could the “Score” values displayed in debug mode represent? How would you systematically investigate and determine whether these values correspond to **similarities** or **distances**? Provide a detailed plan for your approach. Assume the biometric software is fully functional, allowing you to freely enroll, identify, and verify individuals in both regular and debug modes.


Score values represent either similarities or distances between a presented fingerprint and a corresponding sample the system found in the database. To determine whether the values are sim. or dist: 1. enroll your own fingerprint 2. check the score using verification function. 3. Try to verify a different person using your id. If the score became higher — it was distance. If the score became lower — it was similarity.

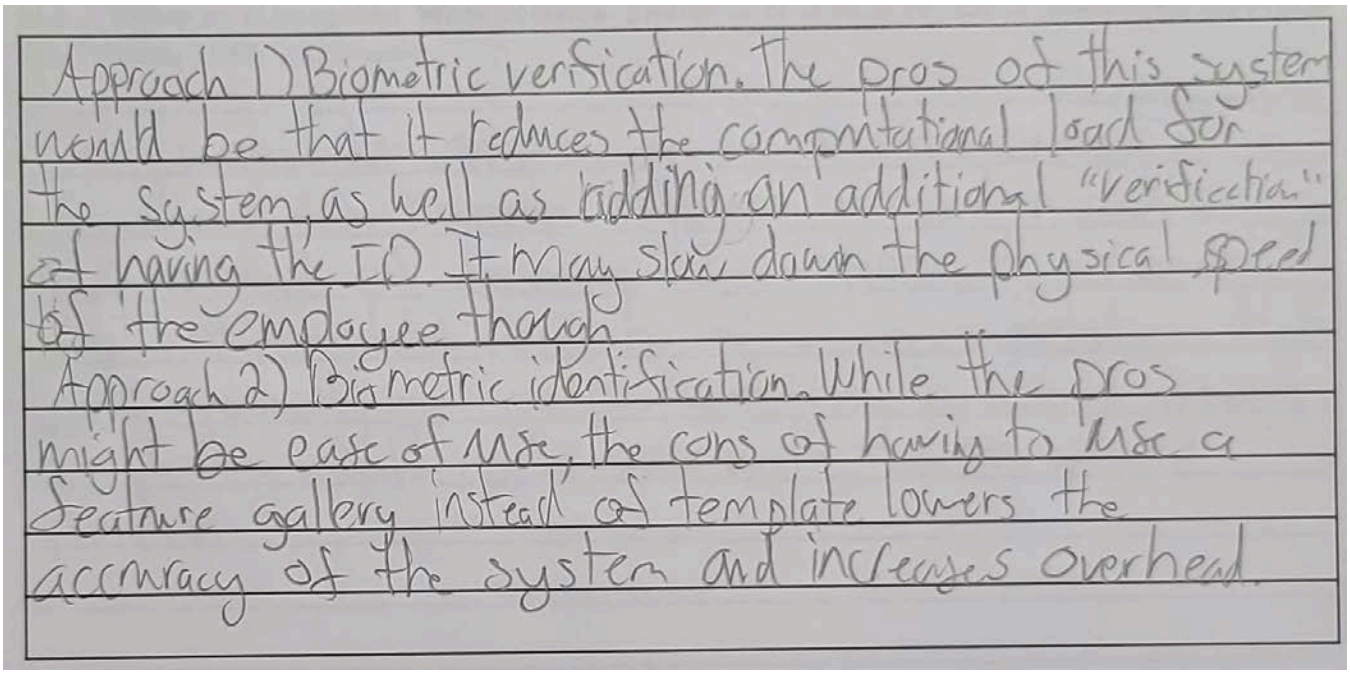
**[Question 2]** (1 point)
What risks arise from deploying that fingerprint recognition system in production while it remains in debug mode? If an attacker were to exploit this configuration, in what ways could they compromise or manipulate the system? Provide a detailed explanation.


The debug mode gives the user a lot of information about the system, allowing them to launch an attack more easily. By providing the user ID when presented with a print, you could be compromising user data if an attacker was using a latent print or a mold. Additionally, by displaying the scores, you run the risk of an attacker using a hill climbing attack, perfecting a fake fingerprint until it gave them access.

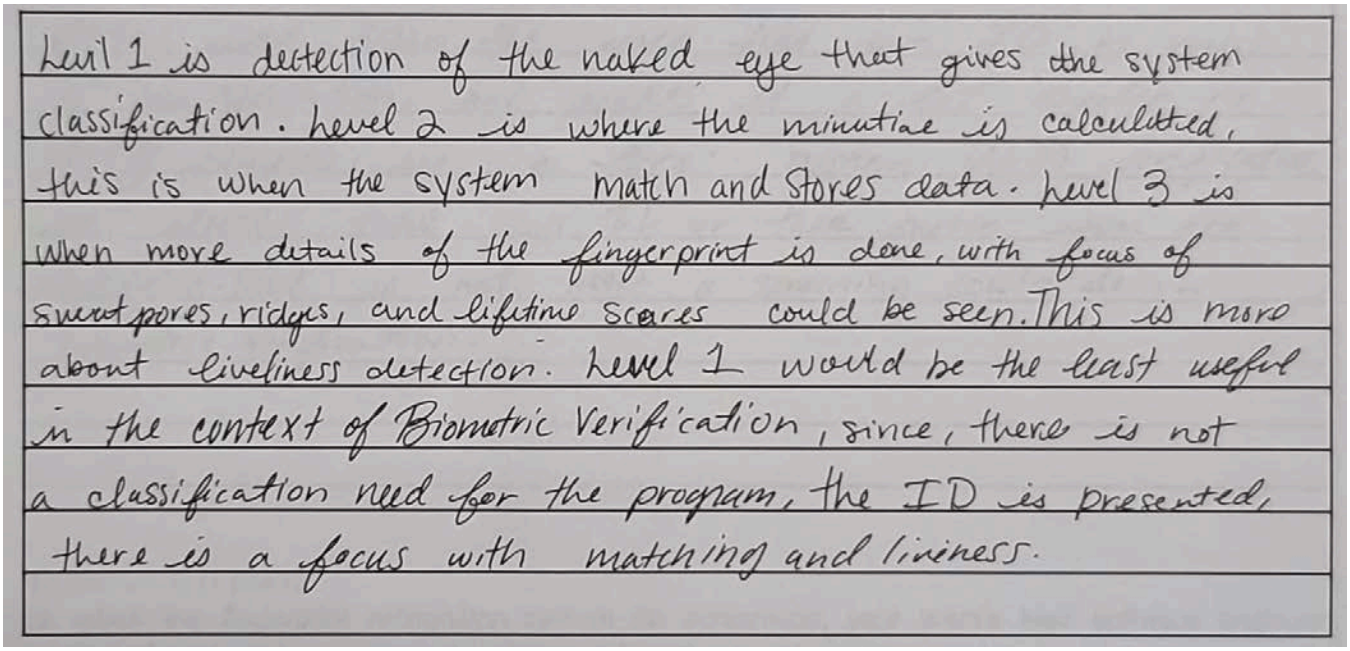
**[Question 3]** (1 point)
Given the system's "Score" values (representing either similarities or distances), how would you evaluate the overall performance of such a biometric solution? Specify the metrics you would report and the types of graphs you would generate to illustrate the results.


I would generate imposter and genuine pairs along with their scores. I would plot the distribution of these scores and calculate the D'prime score (D') to measure how well-separated the genuine and imposter distributions are. A high D'Prime Score indicates good Separation, meaning the System effectively distinguishes between valid and invalid users. I would also generate an AUC plot, which assesses the System's accuracy by maximizing the True Match Rate (TMR) and TNMR across various thresholds. A high AUC score reflects Strong Overall Performance. If the system achieves both a high D'prime and AUC, it would be considered reliable and effective. This approach provides a clear understanding of how well the system differentiates between legitimate and imposter attempts.

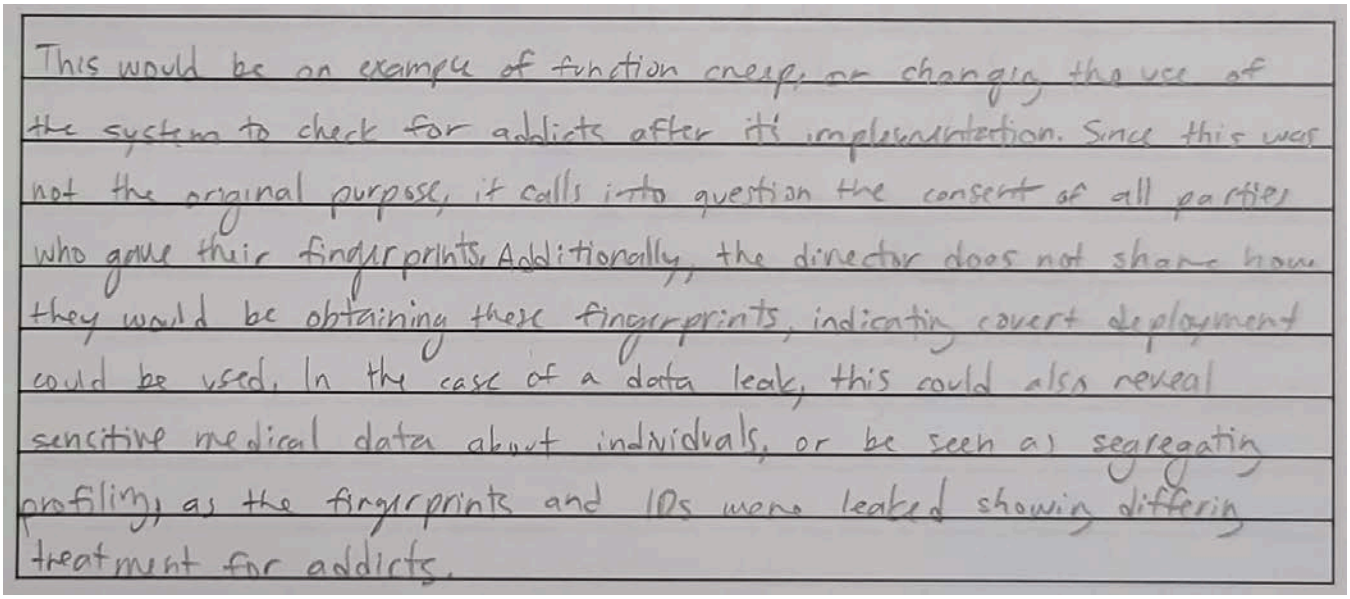
**[Question 4]** (1 point)
The hospital chain's managers have decided to acquire the fingerprint recognition solution. The discussion now involves (1) the need for presenting an identification card, along with the fingerprints, or (2) simply presenting the fingerprints and letting the system find who the person is. Which approach represents **biometric verification** and which represents **biometric identification**? Discuss the advantages and disadvantages of each method.


Approach 1) Biometric verification. The pros of this system would be that it reduces the computational load for the system, as well as adding an additional "verification" of having the ID. It may slow down the physical speed of the employee though.
Approach 2) Biometric identification. While the pros might be ease of use, the cons of having to use a feature gallery instead of template lowers the accuracy of the system and increases overhead.

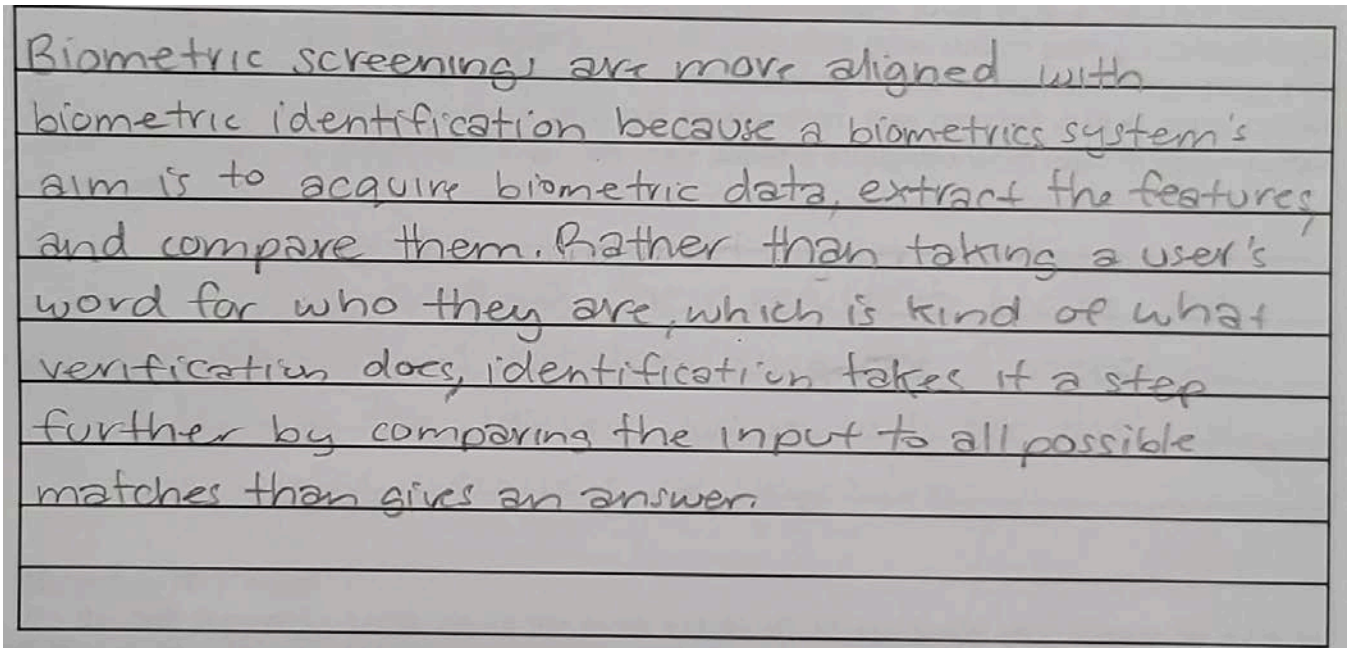
**[Question 5]** (1 point)
The hospital chain's managers have finally decided to adopt a biometric verification approach. They will acquire a version of the system that utilizes a single-finger USB optical sensor with a resolution of 1200 ppi, along with an identification card reader. The complete specifications state that the provided software supports level-1, level-2, and even level-3 features. **Explain what each of these feature levels represents.** In the context of **biometric verification**, which feature level is the least useful, and why? Please justify your answer.


Level 1 is detection of the naked eye that gives the system classification. level 2 is where the minutiae is calculated, this is when the system match and stores data. level 3 is when more details of the fingerprint is done, with focus of sweat pores, ridges, and lifetime scares could be seen. This is more about liveliness detection. level 1 would be the least useful in the context of Biometric Verification, since, there is not a classification need for the program, the ID is presented, there is a focus with matching and liveness.

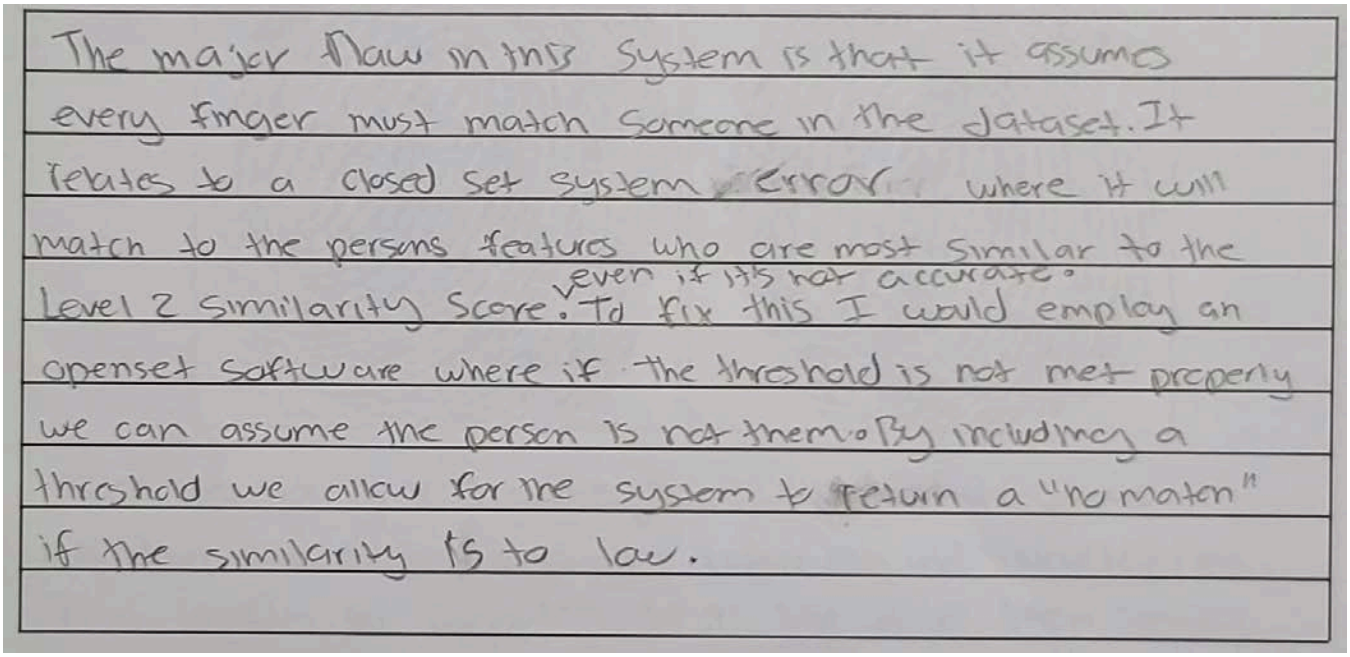
**[Question 6]** (1 point)
After adopting a biometric verification operation, one hospital director proposed extending its use to *screenings* by creating a blocklist of fingerprints belonging to drug addicts and checking against it each time a fingerprint is presented. **What potential problems or ethical concerns could arise from this idea?** Please justify your answer.


This would be an example of function creep, or changing the use of the system to check for addicts after it's implementation. Since this was not the original purpose, it calls into question the consent of all parties who gave their fingerprints. Additionally, the director does not share how they would be obtaining these fingerprints, indicating covert deployment could be used. In the case of a data leak, this could also reveal sensitive medical data about individuals, or be seen as segregating profiling, as the fingerprints and IDs were leaked showing differing treatment for addicts.

**[Question 7]** (1 point)
Setting aside the ethical concerns, **are biometric screenings more closely aligned with biometric verification or biometric identification**? Please explain your answer.


Biometric screenings are more aligned with biometric identification because a biometrics system's aim is to acquire biometric data, extract the features, and compare them. Rather than taking a user's word for who they are, which is kind of what verification does, identification takes it a step further by comparing the input to all possible matches than gives an answer.

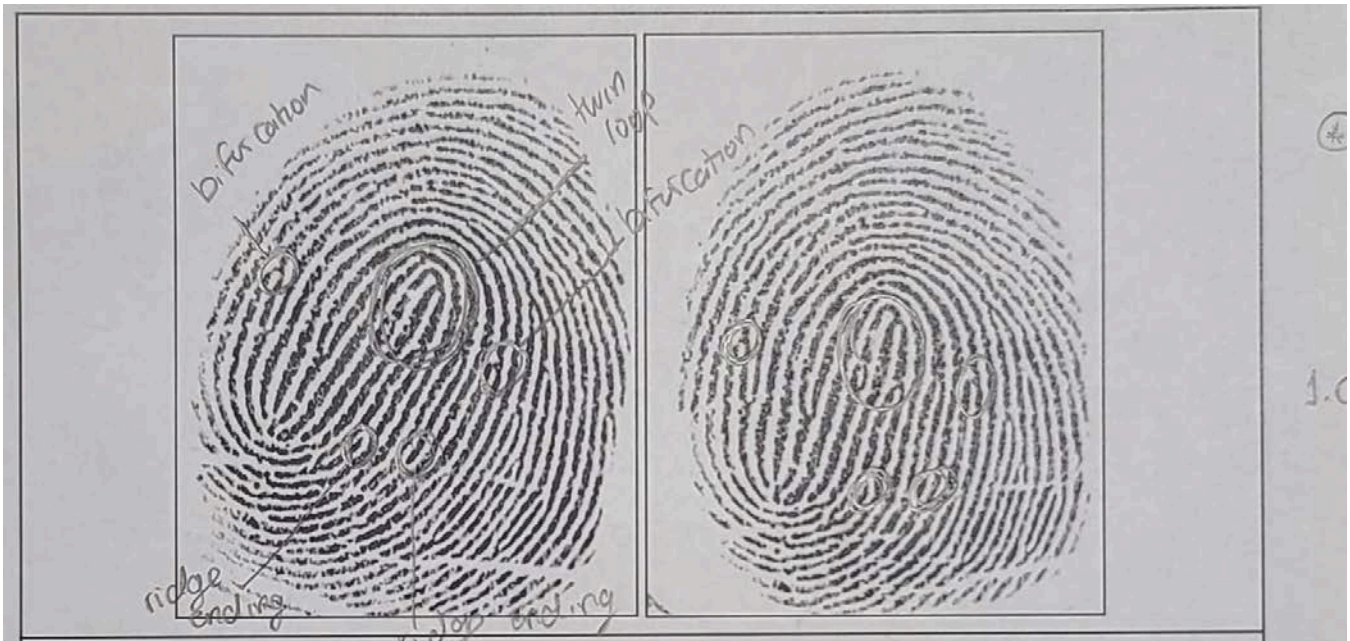
**[Question 8]** (1 point)
To adapt the fingerprint recognition system for screenings, your team's lead software engineer suggested wrapping up the fingerprint matching routine in a loop and comparing an eventually presented fingerprint with every fingerprint template belonging to the blocklist. A drug addict's identity should be taken as the one whose template presents the highest level-2 similarity score with the presented fingerprint. **What is the major flaw in this approach, and how would you correct it?**


The major flaw in this system is that it assumes every finger must match someone in the dataset. It relates to a closed set system Error where it will match to the persons features who are most similar to the Level 2 similarity score even if it's not accurate. To fix this I would employ an openset software where if the threshold is not met properly we can assume the person is not them. By including a threshold we allow for the system to return a "no match" if the similarity is to low.

**[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 designed an experimental setup in which they collected multiple fingerprint slaps from all the fingers of a large set of different people. To generate genuine and impostor pairs, they adopted the following approach: impostor pairs were generated by pairing individual finger slaps from different people, while genuine pairs were generated by pairing individual finger slaps from 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.

If they were only making genuine pairs to the same hand and not the same finger than the genuine pairs metrically would look similar to the Imposter, because if a person's thumb and Index are compared they will look foreign to each other even though they are from the same hand.

**[Question 10]** (1 point)
Do the two fingerprints below depict the same individual? Please justify your answer by marking, linking, and type-naming five or more minutiae between them. After you've done this process manually, please **explain why it is useful and important to program computers to do the same task.**




This is the same individual. Matching this one print took me about 2 minutes. Imagine that, but having to match thousands of people a day at an airport. Computers are faster, more accurate, and accountable because they keep logs.