Progress Report

Name: Bright Ekeator
Student ID: 300318200
Group: F25_4440_G13

1. Work Log Table

Date	Hours	Task Description	Notes
2025-10-20	30 mins	Met with instructor to discuss project scope, tool selection, and proposal feedback.	
2025-10-20	1 hr	Team meeting to discuss project objectives, divide tasks, and plan analysis workflow for selected apps.	
2025-10-24	2 hrs	Team meeting to set up the project proposal structure and created the GitHub repository.	
2025-10-24	3 hrs	Installed Andriller and set up test environment for IMO and Tinder APK extraction.	
2025-10-27	1 hr	Installed and configured Android Studio and AVD emulator with rooted image.	
2025-10-28	30 mins	Installed IMO app on emulator and confirmed package path.	

2025-10-29	30 mins	Attempted adb backup on IMO; backup produced 1 KB file.
2025-10-30	1 hr	Pulled internal IMO app data using adb pull.
2025-10-31	30 mins	Organized project folders for analysis outputs.
2025-11-01	1 hr	Installed Python environment and Andriller; verified modules.
2025-11-02	1 hr	Extracted .ab backup using Andriller and decoded data.
2025-11-03	1 hr	Opened SQLite databases and reviewed message tables.
2025-11-04	1 hr	Identified encrypted BLOB message content.
2025-11-05	1 hr	Analyzed shared preferences for configuration data.
2025-11-06	1 hr	Documented folder sizes and data extraction process.
2025-11-07	1 hr	Drafted initial analysis report.
2025-11-07	1 hr	Re-verified data integrity and repeated extraction

		steps.
2025-11-08	3 hrs	Researched runtime key extraction and alternative decryption methods.
2025-11-08	2 hrs	Reviewed all databases and performed additional test extractions.
2025-11-12	30mins	Tried Installing another APk file for Tinder and tried sign in but unsuccessful
2025-11-14	30mins	Prepared Progress report and compared previous analysis

2. Work Description

Thus far, I have performed extensive forensic extraction and analysis of the IMO app using a rooted Android emulator. I set up the emulator, installed the IMO APK, attempted adb backup, and later performed a full adb pull of the internal data. I used Andriller to decode the extracted backup and inspected all relevant databases and shared preference files. My findings confirm that IMO uses strong encryption, with message records stored as encrypted BLOBs in SQLite databases.

For the second required app, Tinder, I attempted installation and login, but authentication consistently failed, preventing extraction. I am currently sourcing an older or alternative Tinder APK compatible with the emulator to continue the analysis.

The issues I encountered

The main issue encountered with the IMO app was the strong application-level encryption protecting the message content. The message content in the main chat databases was stored as encrypted BLOB data, preventing direct viewing and requiring a decryption key for content recovery.

A critical issue was also encountered during the setup for the **Tinder** analysis: the app **crashes immediately upon attempting to sign in**. This constant crashing prevents any user interaction from taking place, which is necessary to generate forensic artifacts. I have spent time trying to find a compatible APK version online, as the current version appears to have an incompatibility or crash loop in the emulator environment, potentially due to a jailbreak/root detection mechanism.

Planned Next Steps

- Obtain a functional Tinder APK version
- Try alternative login methods (Google, Facebook, burner number)
- Analyze login failures using proxy tools
- Once accessible, extract and analyze Tinder's internal storage
- Compare encryption and storage mechanisms between IMO and Tinder
- Prepare full final report and presentation

3. AI Use Section

AI Tool Name	Version / Account Type	Specific Feature Used
ChatGPT (GPT-5.1)	Free Version	Used for structuring report and formatting Solutions to tinder APK debugging
ChatGPT (Earlier sessions)	Free Version	Clarified ADB and forensic workflow assisted in andriller installation and use
Microsoft Word Editor	Local	Grammar and formatting refinement
Gemini	2.5	

Value Addition

All technical tasks including extraction, emulator setup, Andriller use, SQLite inspection, and verification, were done manually. AI contributed only to document organization and clarity, debugging but not technical analysis.

Appendix

How can I solve the sign in problems of my tinder

How to install xapk in place of apk on android studio emulator via command line

Step by step guide on how to use andriller

Explain in detail why I cannot view the extracted message sent between contacts on my IMO without decryption key

Debugging my tinder app issues

Guides on comparative analysis between andriller backup files and adb backup files