

CSIS 4440 Project Proposal

TITLE:

Mobile Application Security Analysis and Digital Forensics

Team Members

- Bright Ekeator (Team Lead) 300318200
- Ifeoluwa Aribi 300389564

Tools And Apps Overview for each Student in the Team:

Student Name: Bright Ekeator

Tools: Andriller

Apps: Imo, Tinder

Novelty: The novelty of this project is in the ability to use the tools to analyze the application's private data directories, shared preferences in order to extract and reconstruct fragmented user interaction data from proprietary or encrypted storage formats that are not immediately readable on its primary format, specifically by: 1) Developing custom queries or scripts to parse unallocated space within the app's database files for unique and time-sensitive artifacts. 2) Documenting the specific encryption/obfuscation techniques used by Imo and Tinder for local data storage and creating a clear chain of custody documentation for these extracted artifacts.

Student Name: Ifeoluwa Aribi

Tools: AndroBugs, MobSF

Apps: Tim Hortons, Reddit

Novelty:

The novelty of this project lies in the combined use of AndroBugs and MobSF for both **static** and **dynamic** vulnerability analysis of Tim Hortons and Reddit applications. The focus is on uncovering **hidden misconfigurations, insecure data storage practices, and residual authentication tokens** that persist beyond app session termination. Specifically, this involves:

1. Automating security scanning pipelines to correlate static code-level vulnerabilities (from MobSF) with runtime permission abuses and exported components detected by AndroBugs.
2. Designing a forensic workflow to trace exposed personal data and session cookies within mobile local storage and network traffic, identifying risks such as credential leakage and unprotected API endpoints.
3. Documenting and categorizing critical vulnerabilities affecting user privacy and session management, followed by generating reproducible forensic evidence reports suitable for court admissibility.

This contribution provides a **forensically validated vulnerability mapping** across both corporate (Tim Hortons) and community-based (Reddit) apps, highlighting how insecure mobile implementations can lead to traceable digital footprints and potential evidence trails for forensic investigators.

Integrated Component:

The integration between Student 1's and Student 2's work aims to build a **comprehensive mobile forensic and security analysis framework** that connects local data extraction with application vulnerability assessment. While Student 1 focuses on **recovering stored and encrypted user data** from IMO and Tinder using Andriller, Student 2 complements this by performing **static and dynamic vulnerability analysis** of Tim Hortons and Reddit using AndroBugs and MobSF.

The integration will be presented through a **Vulnerability Correlation Matrix**, linking insecure local data storage findings from Student 1 with insecure transmission, misconfigurations, and runtime permissions identified by Student 2. This combined analysis will demonstrate how sensitive user data can transition from device storage to network layers, exposing potential forensic evidence and security risks across both social and corporate mobile applications.

Together, this approach provides a **holistic forensic and security lifecycle view**—from data creation and storage to exposure and transmission—offering both technical and evidential insights into mobile app security and privacy vulnerabilities.

AI Use Section:

- ***Table of AI Tools and Specific Use:***

AI Tool Name	Version, Account Type	Specific feature for which the AI tool was used
Gemini (LLM)	Pro, Free	Drafting the initial project proposal structure and outlining the novelty sections for each student
ChatGPT (GPT-4o)	Free account (OpenAI, 2025)	Used for conceptual brainstorming on forensic workflow integration between Andriller and AndroBugs and drafting of research rationale.

- ***Value Addition:***

Customized the generic output to fit the specific 4440 Project Proposal Template (e.g., adding Contract, Work Log, and Novelty paragraph). Synthesizing AI outputs into an original, evidence-based proposal tailored to the specific apps under analysis (Imo, Tinder, Reddit, Tim Hortons).

- ***Appendix:***

- I want to create a project proposal structure for my project outlining the novelty sections. The tools I want to explore are Andriller, AndroBugs and mobfs. The apps are Imo, Tinder, Tim Hortons, Reddit.
- Create a possible workflow integration of the tools and apps described above

Project Contract:

Project Title: Mobile Application Security Analysis and Digital Forensics

This contract is entered into by and between the team members of F25_4440_G12 to ensure professional and efficient collaboration throughout the project lifecycle.

- Meeting Schedule:** The team shall meet a minimum of **3** times per week, specifically on **Mondays, Wednesdays and Fridays** at any agreed time for a minimum of one hour. Meetings will be conducted either physically or via communication platforms
- Communication Protocol:** All general project communication and file sharing will take place via **WhatsApp group**. Urgent communications will be done via phone calls. Response time for urgent queries is set at a maximum of 4 hours.
- Conflict Resolution:** Any disputes regarding workload, technical direction, or grading will first be discussed openly by all team members. If unresolved, the conflict will be elevated to the level of class instructor.
- Work Submission:** All final documents (Proposal, Final Report) will be peer-reviewed by the non-submitting member(s) 24 hours prior to the official submission deadline.
- Code & Repository:** All project code (scripts, custom Burp extensions, etc.) will be committed to the designated GitHub repository at least once per week.

Signatures

_____BAE_____

Bright Ekeator

_____Ifeoluwa_____

Ifeoluwa Aribu

Work Date/Hours logs for student (or each team member):

Date	Student Name	Number of Hours	Description of Work
2025-10-20	Bright Ekeator, Ifeoluwa Aribu	30 Minutes	Met with instructor to discuss project scope, tool selection, and proposal feedback.
2025-10-20	Bright Ekeator, Ifeoluwa Aribu	1 hour	Team meeting to discuss project objectives, divide tasks, and plan analysis workflow for selected apps.

2025-10-24	Bright Ekeator, Ifeoluwa Aribu	2 hrs	Team meeting to set up the project proposal structure and created the GitHub repository for collaborative work.
2025-10-24	Bright Ekeator	3 hrs	Installed Andriller and set up test environment for Imo and Tinder APK extraction.
2025-10-24	Ifeoluwa Aribu	2 hrs	Installed MobSF and AndroBugs; configured analysis environment for Tim Hortons app.

Closing

This project represents a detailed and methodical approach to mobile application security analysis and digital forensics. By combining static and dynamic analysis, local data extraction, and vulnerability mapping across both social and corporate apps, the team will deliver a comprehensive view of mobile app security and privacy risks. The work provides actionable insights into how sensitive data is stored, transmitted, and potentially exposed, supporting both technical understanding and forensic investigation practices. The methodology, tools, and integrated findings aim to produce reproducible and court-admissible forensic evidence where applicable, while highlighting common security misconfigurations and privacy risks in widely used mobile applications.

References

1. AndroBugs Framework. (2024). Retrieved from <https://github.com/AndroBugs>
2. Mobile Security Framework (MobSF). (2024). Retrieved from <https://github.com/MobSF/Mobile-Security-Framework-MobSF>
3. Andriller: Android Forensics Tool. (2024). Retrieved from <https://github.com/BlackArrow/andriller>
4. Imo Application. (2025). Retrieved from <https://imo.im/>
5. Tinder Application. (2025). Retrieved from <https://tinder.com/>
6. Tim Hortons App. (2025). Retrieved from <https://www.timhortons.com/ca/apps.php>
7. Reddit Application. (2025). Retrieved from <https://www.reddit.com/>
8. OWASP Mobile Security Testing Guide. (2023). Retrieved from <https://owasp.org/www-project-mobile-security-testing-guide/>

9. GitHub Documentation. (2025). Using repositories for team collaboration. Retrieved from <https://docs.github.com/>
10. OpenAI ChatGPT. (2025). Used for conceptual planning and drafting sections of the proposal. Retrieved from <https://openai.com>