CERIAS

The Center for Education and Research in Information Assurance and Security

When TikTok is No Longer: A Forensic Analysis of Rednote on Android

Mingyang Xie*, Xiao Hu*, Akif Ahsen Ozer, Umit Karabiyik

OVERVIEW

This project presents a forensic analysis of Rednote application on the Android system. We simulated typical user interactions with Rednote application to populate data and utilized forensic tools to examine the mobile device for digital evidence that is important in relation to each event.
Under review of ISDFS 2025

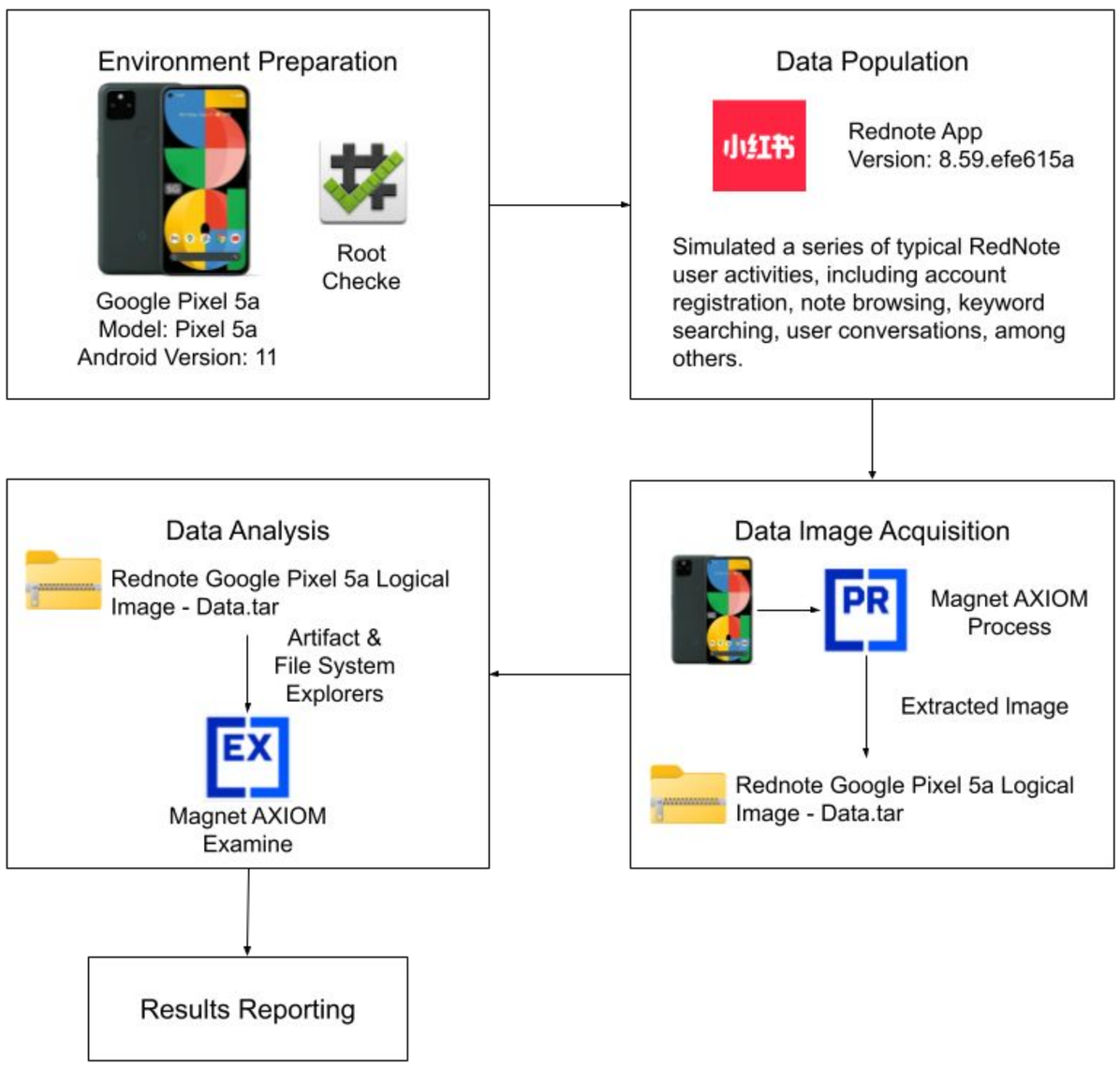
GOALS

Identified accessible Rednote application records that document user activity storage locations in the Android system, to assist in digital forensic investigations of Rednote applications on Android devices.

METHODOLOGY

For this project, the methodology followed the same procedures: environment preparation, data population, data image acquisition, data analysis and report.

- **Flow Chart :**



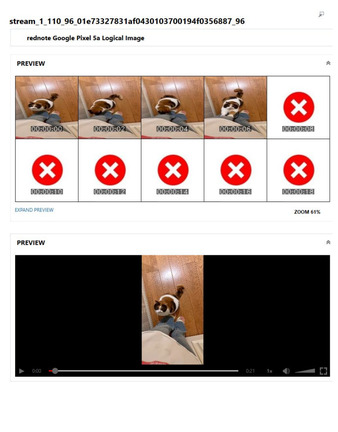
- **The Versions of Device and Softwares**

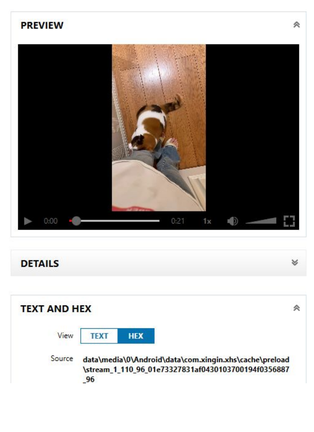
Software	Version	Usage
RedNote (Android)	v.8.59.efe615a	Data Population
Magnet AXIOM Process	8.8.9.42722	Data Population
Magnet AXIOM Examine	8.8.9.42722	Analysis and Examination

FINDINGS

- In the Android system, RedNote locally records users' device information, personal profiles, search history, uploaded videos, favor and liked notes, privacy post notes and published post notes, cookies, preload videos, and browsing history of notes.
- In an offline environment, the Rednote app displays only the most recent chat history rather than the conversation record after extended periods. This limitation likely occurs because chat logs are stored in the cloud. Furthermore, the chat logs viewable on the phone cannot be found as plaintext content in the mirror backup and also include note comments. This suggests the application likely encrypts this content before storage.

Contents	Location
The videos user published	\data\data\com.xingin.xhs\files\videolocal\
Notes of faved, liked, privacy posts and publish posts	\data\data\com.xingin.xhs\cache\profile\
Device's information	\data\data\com.xingin.xhs\shared_prefs\cn.jiguang.sdk.device.xml
System user agent and search history	\data\data\com.xingin.xhs\shared_prefs\com.xingin.xhs_preferences.xml
Cookies	\data\data\com.xingin.xhs\shared_prefs\app_webview-Default\Cookies
Browsing history of notes	\data\data\com.xingin.xhs\databases\PlayHistoryRecordDB (historyRecord table)
Account information	\data\data\com.xingin.xhs\files\mmkv\com.xingin.xhs
Preload videos	\data\media\0\Android\data\com.xingin.xhs\cache\preload





CONCLUSION

- The forensic artifacts and methods related to smart devices analyzed in this study, as well as publicly available datasets containing critical data paths and vulnerabilities, can provide solid technical support for related investigations.
- Digital forensics on smart devices has an invaluable role to play in criminal investigations, and there is a need for continued progress in these areas.

PURDUE UNIVERSITY

{xie447, hu961, ozer, umit}@purdue.edu