Student:	Email:
Loksharan Saravanan	loksharan.soc@gmail.com

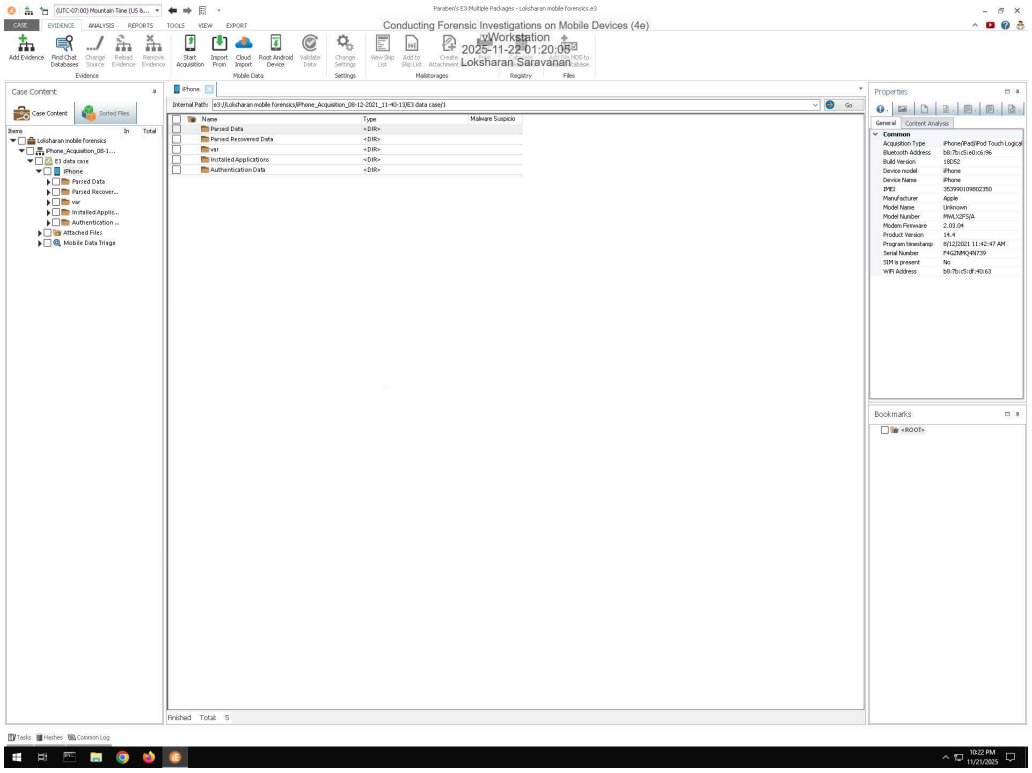
Time on Task:	Progress:
2 hours, 12 minutes	100%

Report Generated: Wednesday, December 10, 2025 at 10:33 PM

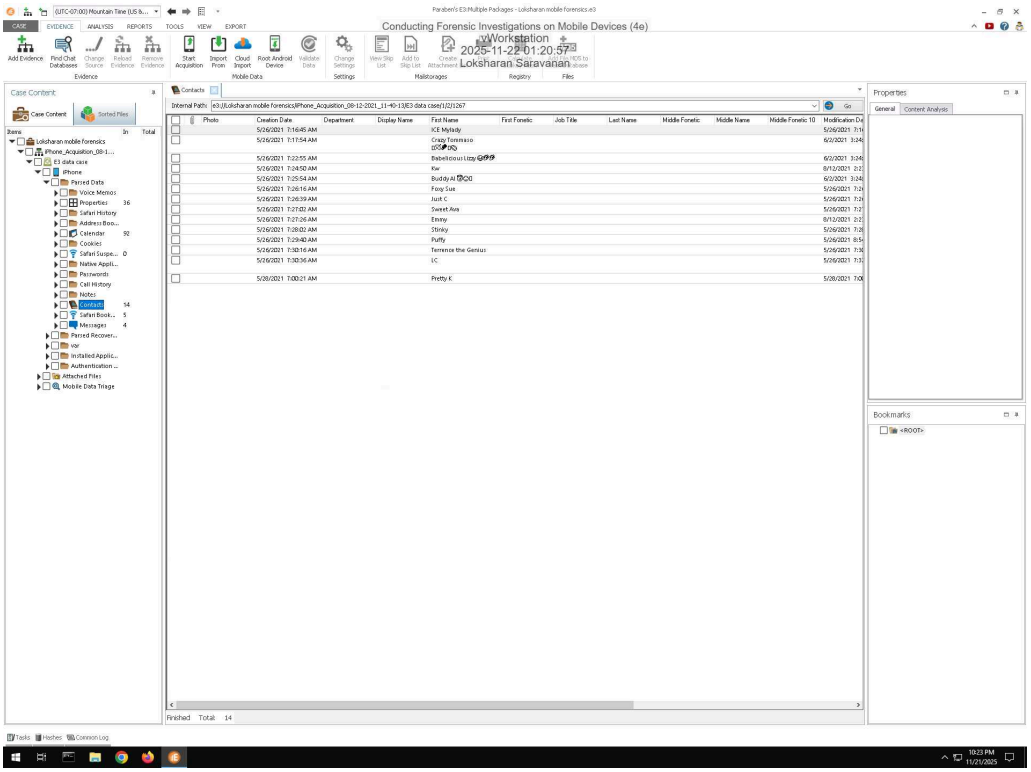
Section 1: Hands-On Demonstration

Part 1: Identify Forensic Evidence in an iOS Data Case

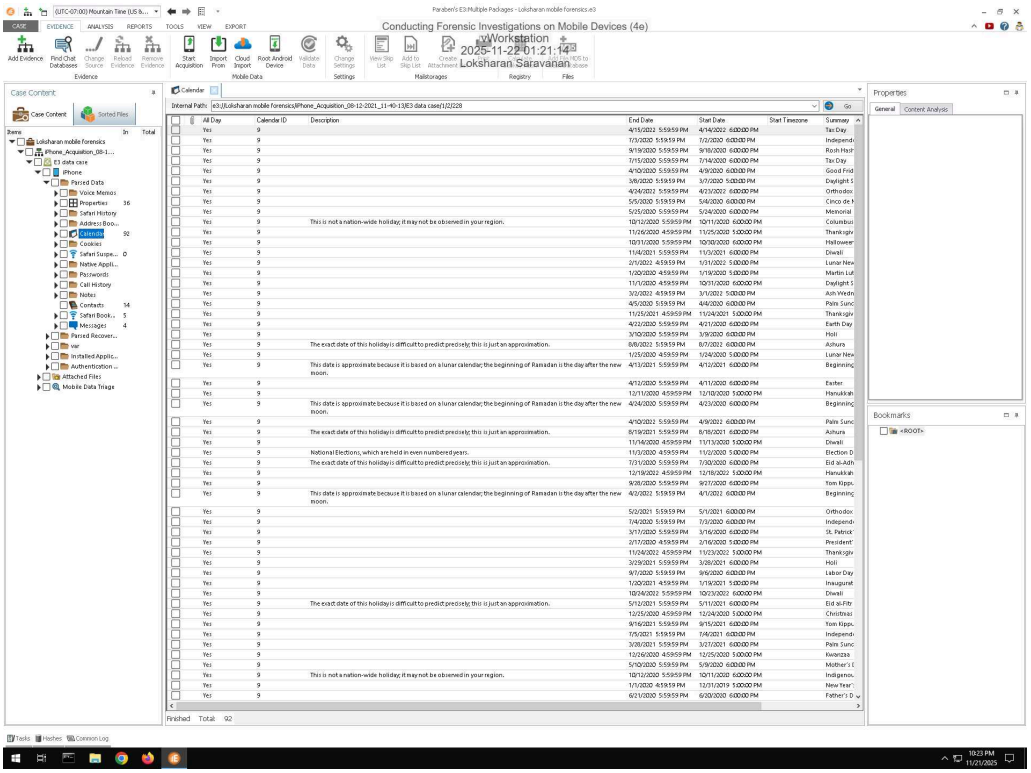
8. **Make a screen capture** showing the **contents of the Properties pane**.



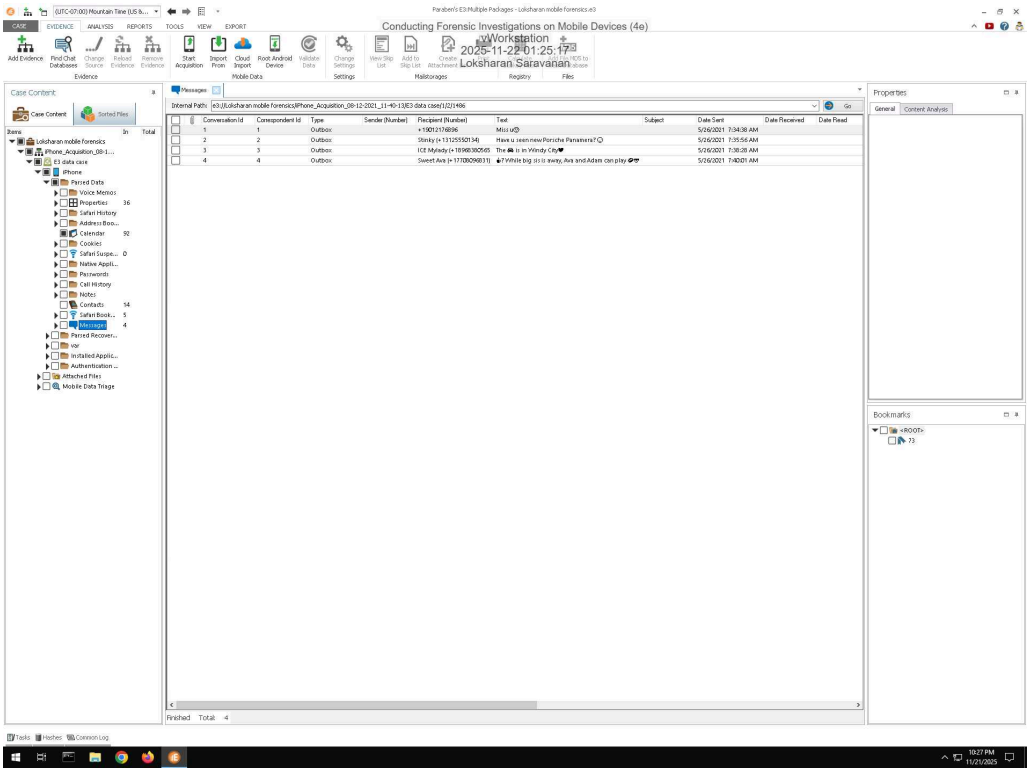
11. **Make a screen capture** showing the **contents of the Contacts grid**.



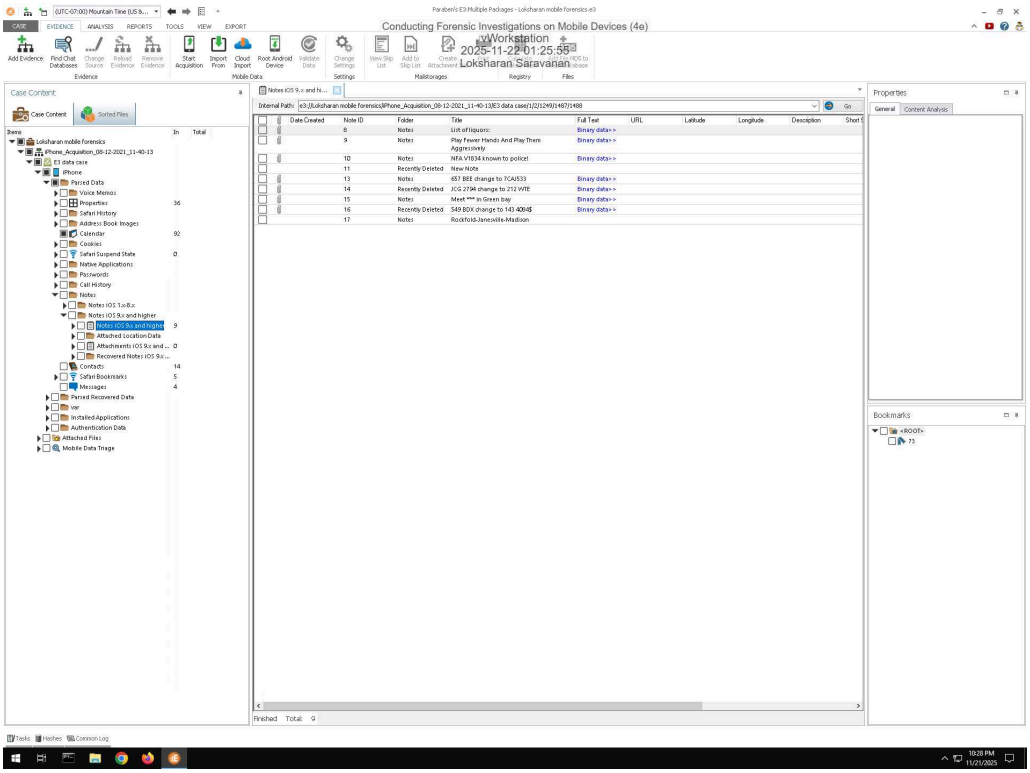
14. **Make a screen capture** showing the **contents of the Calendar grid**.



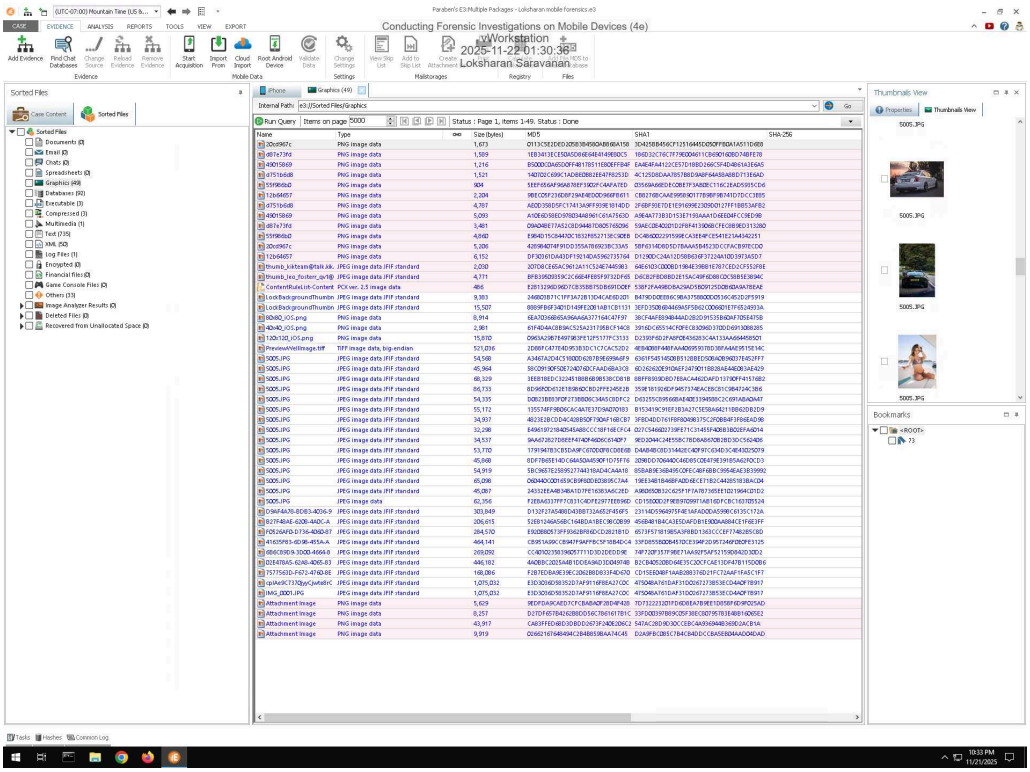
20. **Make a screen capture** showing the **contents of the Messages grid**.



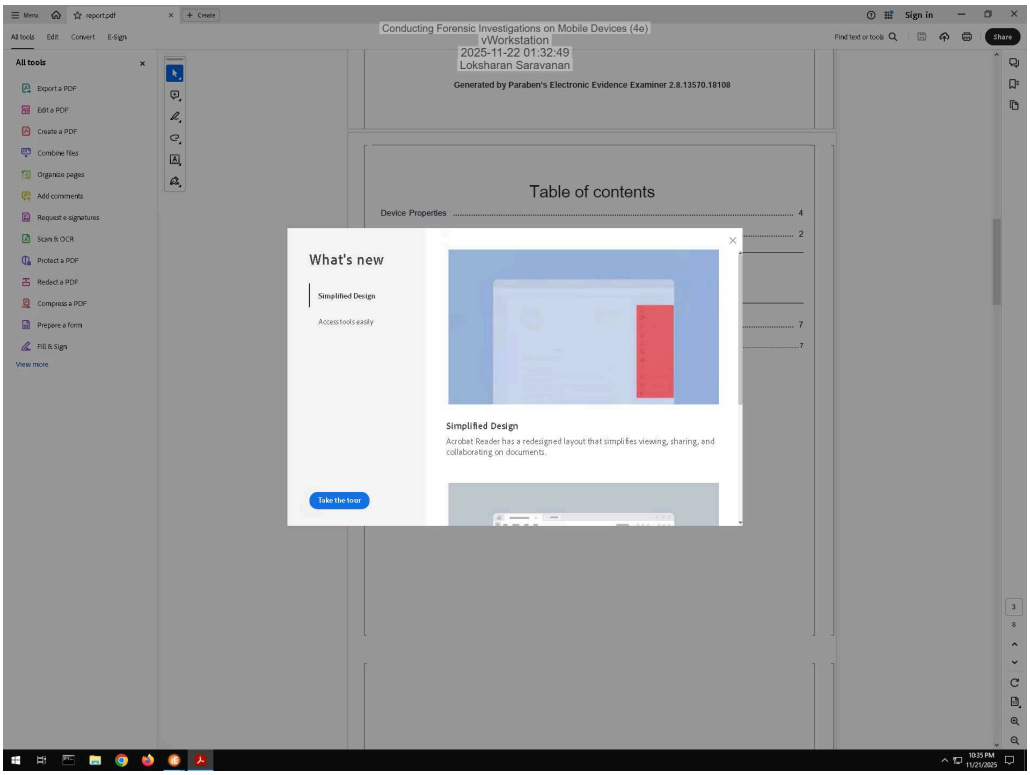
24. **Make a screen capture** showing the **contents of the Notes grid**.



34. **Make a screen capture** showing **at least two car pictures in the Thumbnail View**.

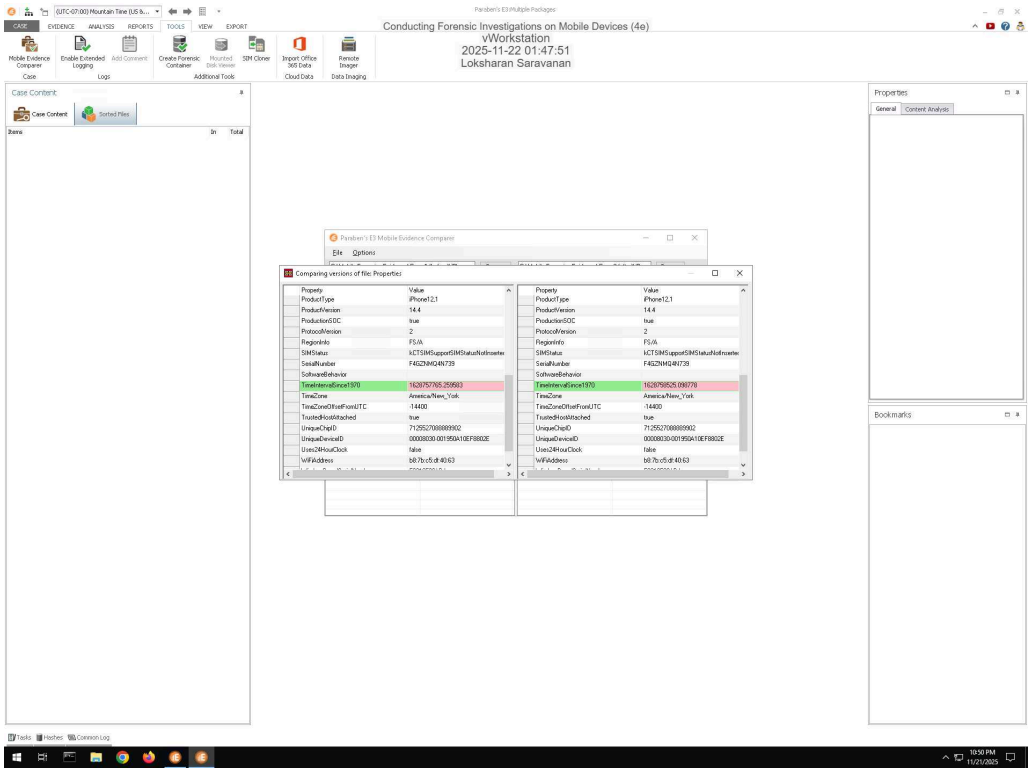


44. **Make a screen capture** showing the **Table of contents in the investigative report**.

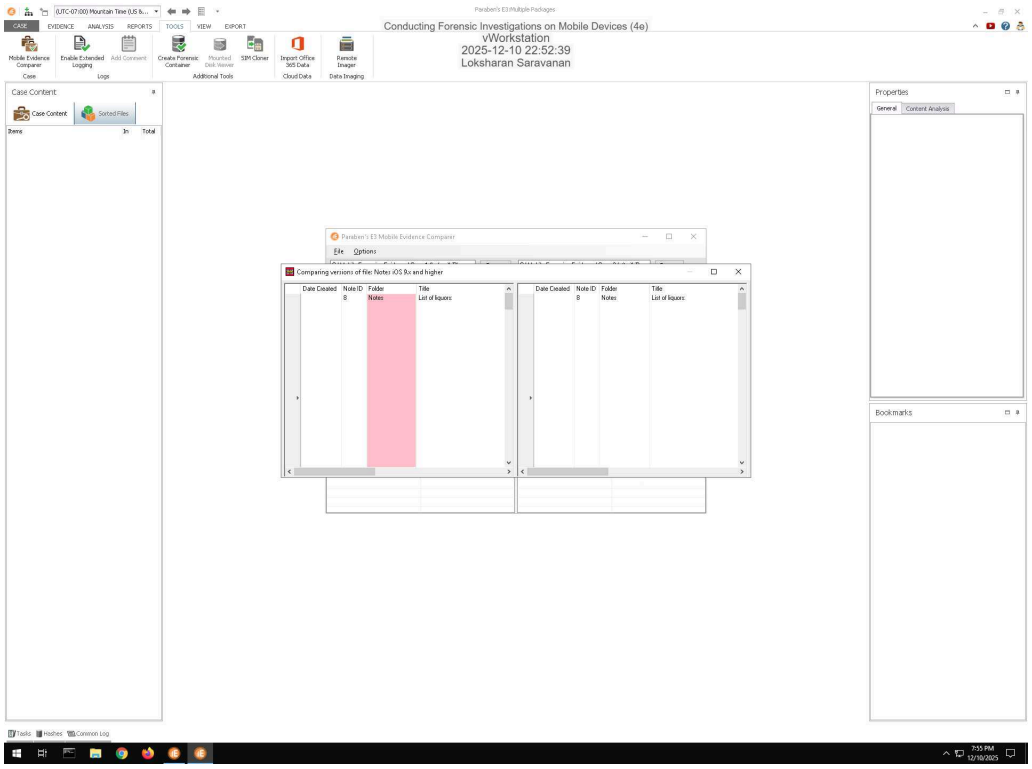


Part 2: Compare iOS Data Cases

10. **Make a screen capture** showing the **difference in data case properties**.



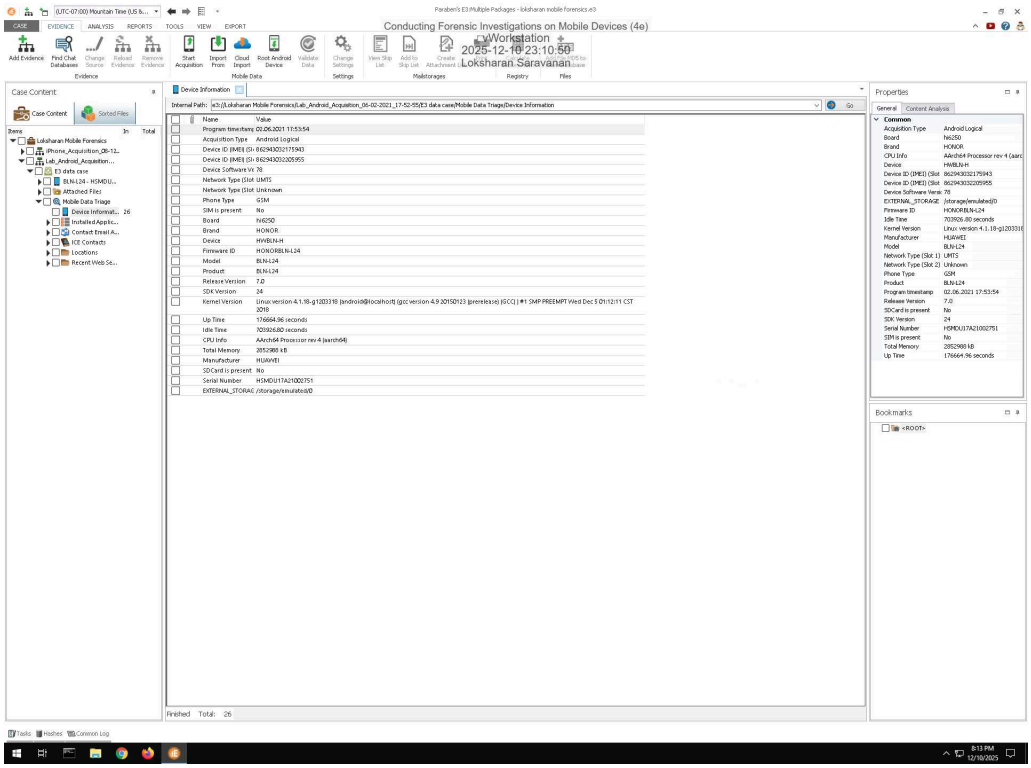
15. **Make a screen capture** showing the **additional note in the newer data case**.



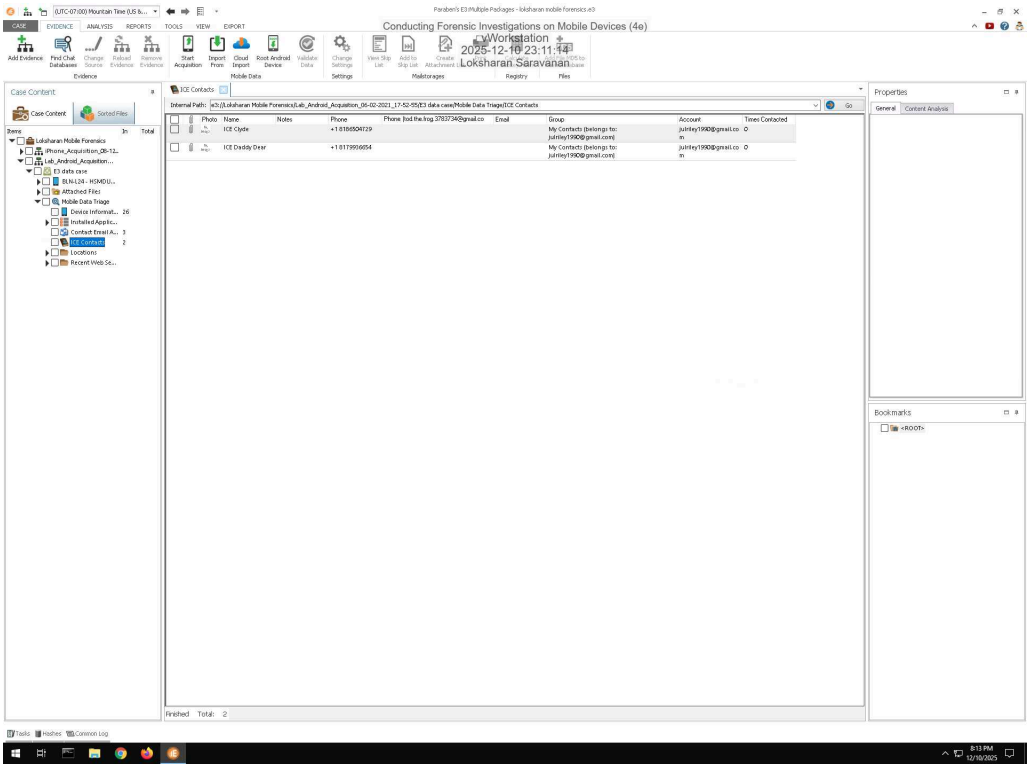
Section 2: Applied Learning

Part 1: Identify Forensic Evidence in Android User Data

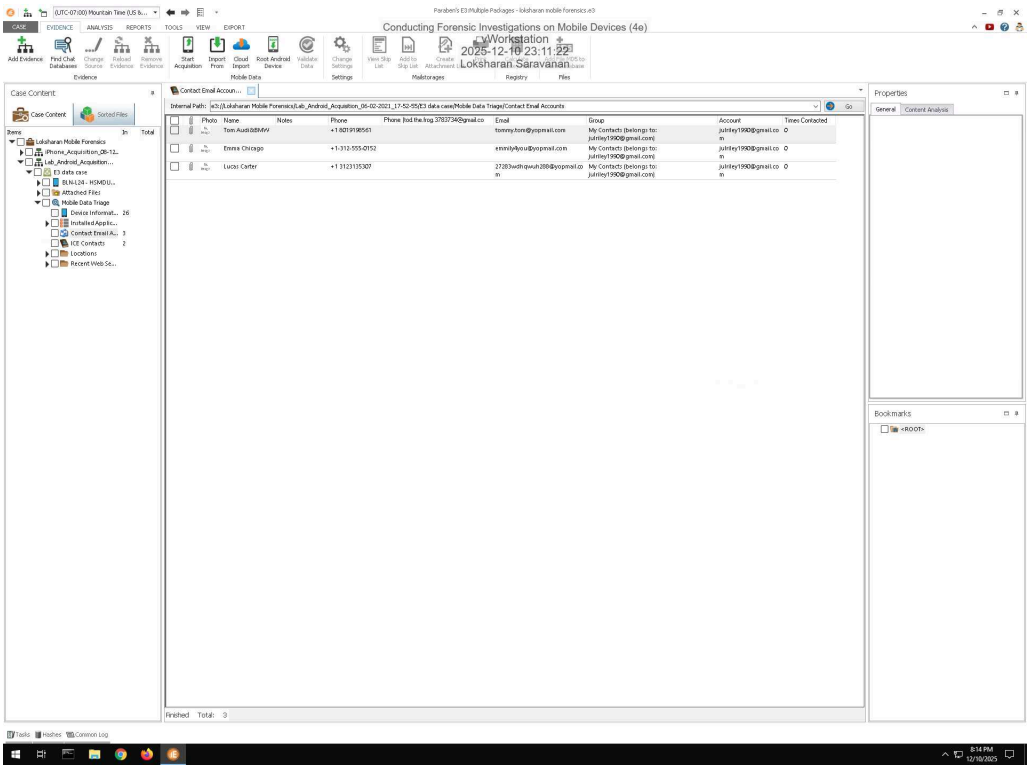
7. **Make a screen capture** showing the **Device Information**.



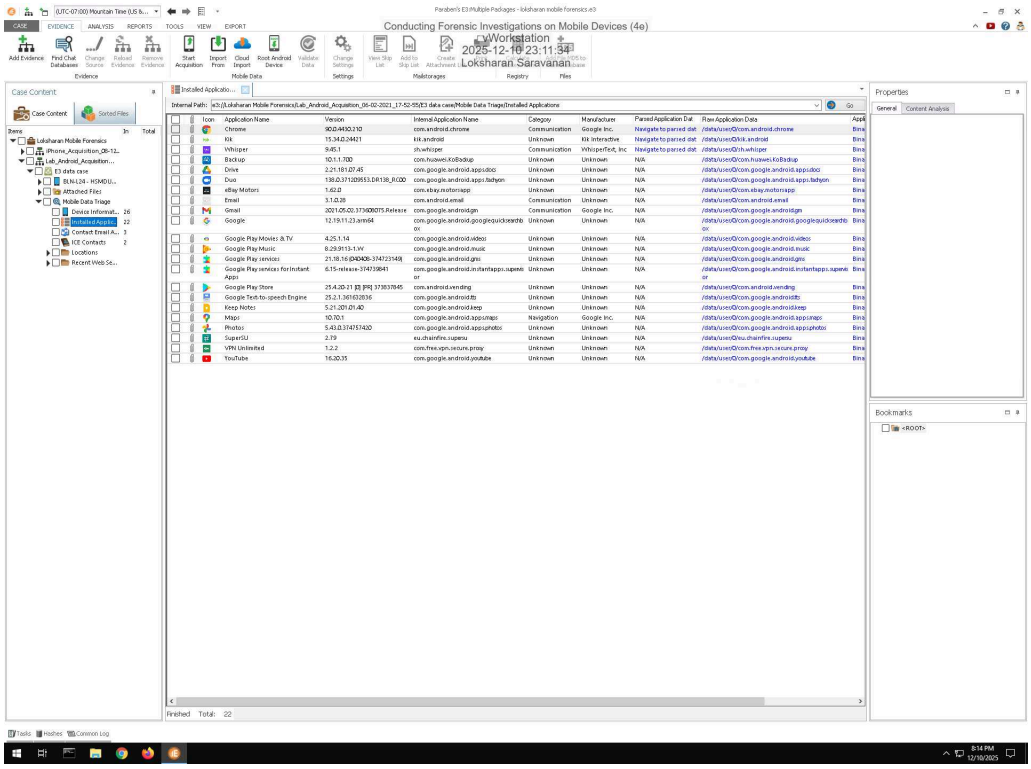
9. **Make a screen capture** showing the **ICE Contacts**.



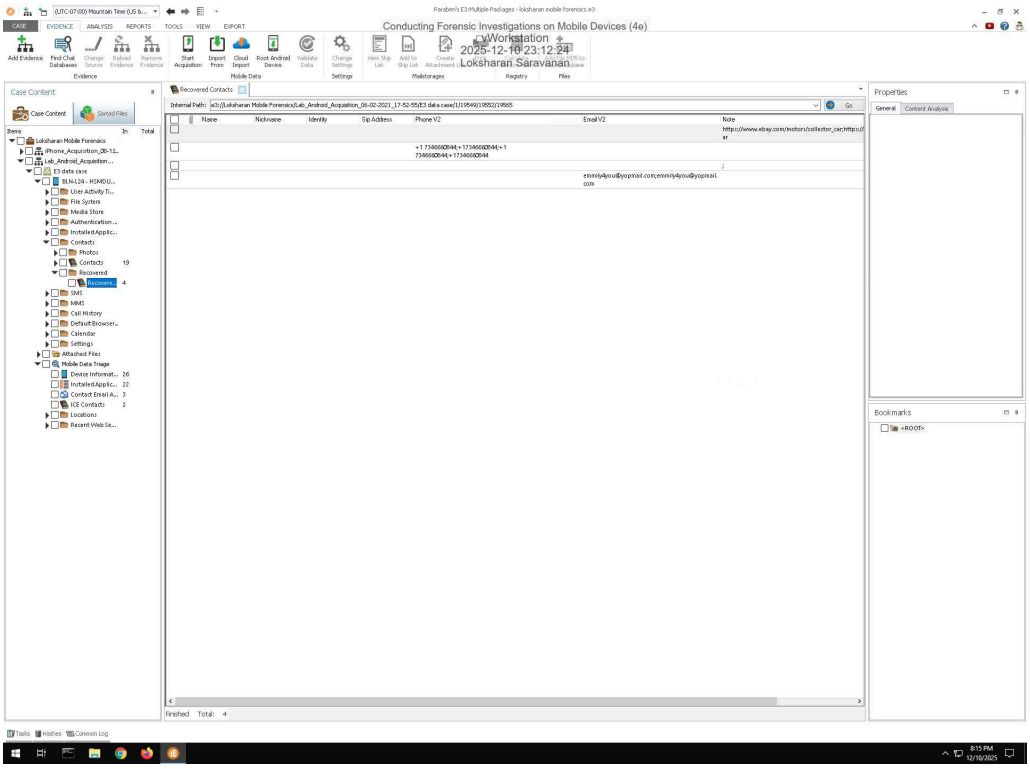
12. **Make a screen capture** showing the **Contact Email Accounts**.



15. **Make a screen capture** showing the **Installed Applications**.

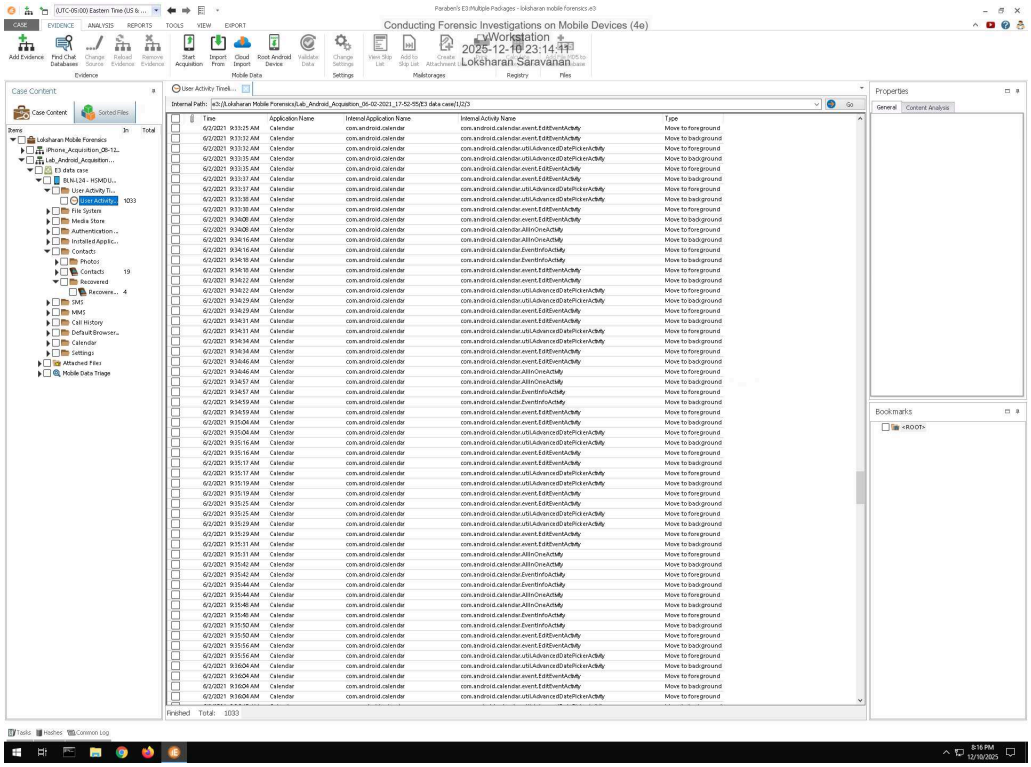


19. **Make a screen capture** showing the **recovered contact information from the Android phone**.

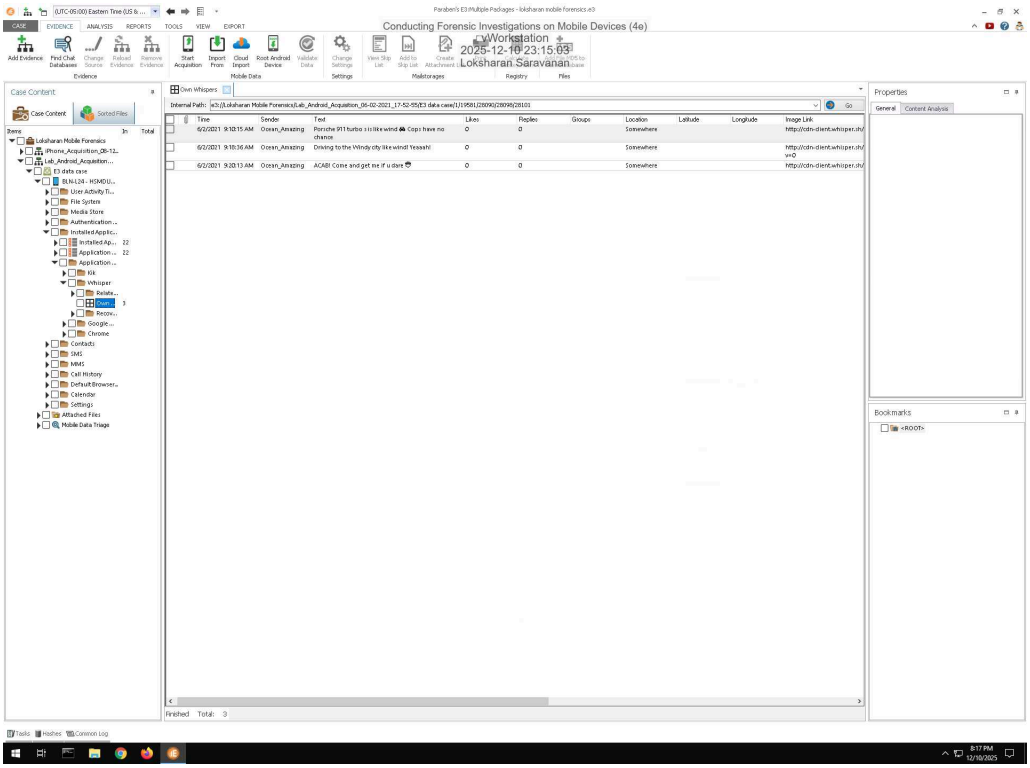


Part 2: Identify Forensic Evidence in Android Application Data

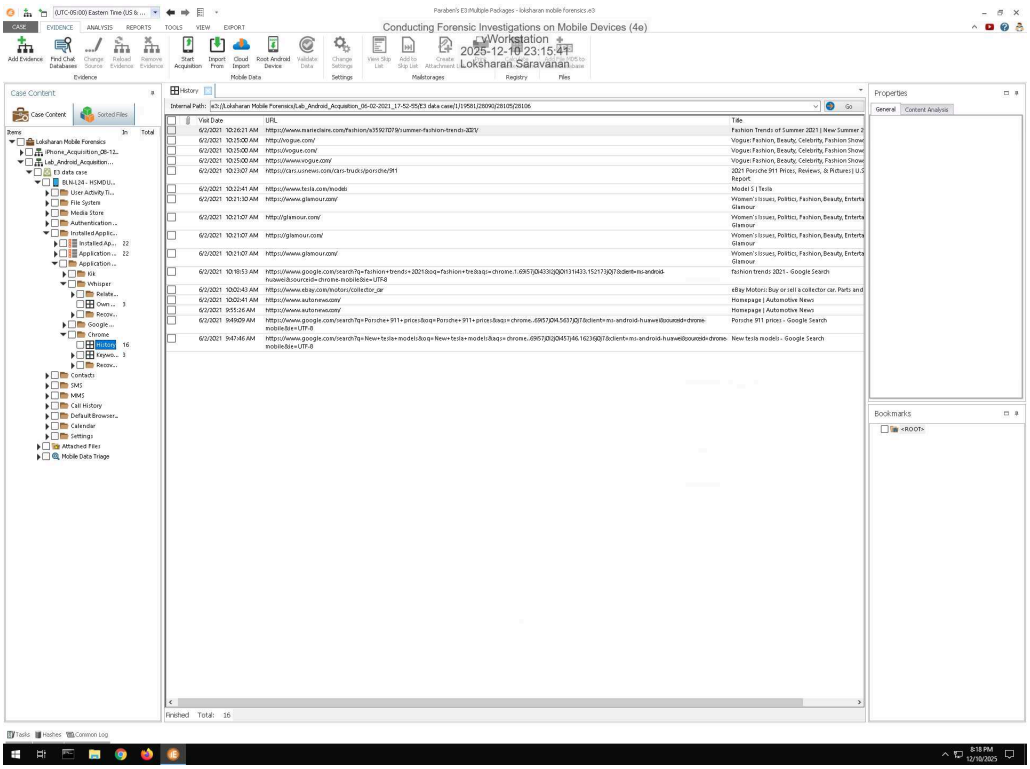
4. **Make a screen capture** showing the **User Activity Timeline between 9:17:47 AM and 9:24:51 AM on 6/2/2021**.



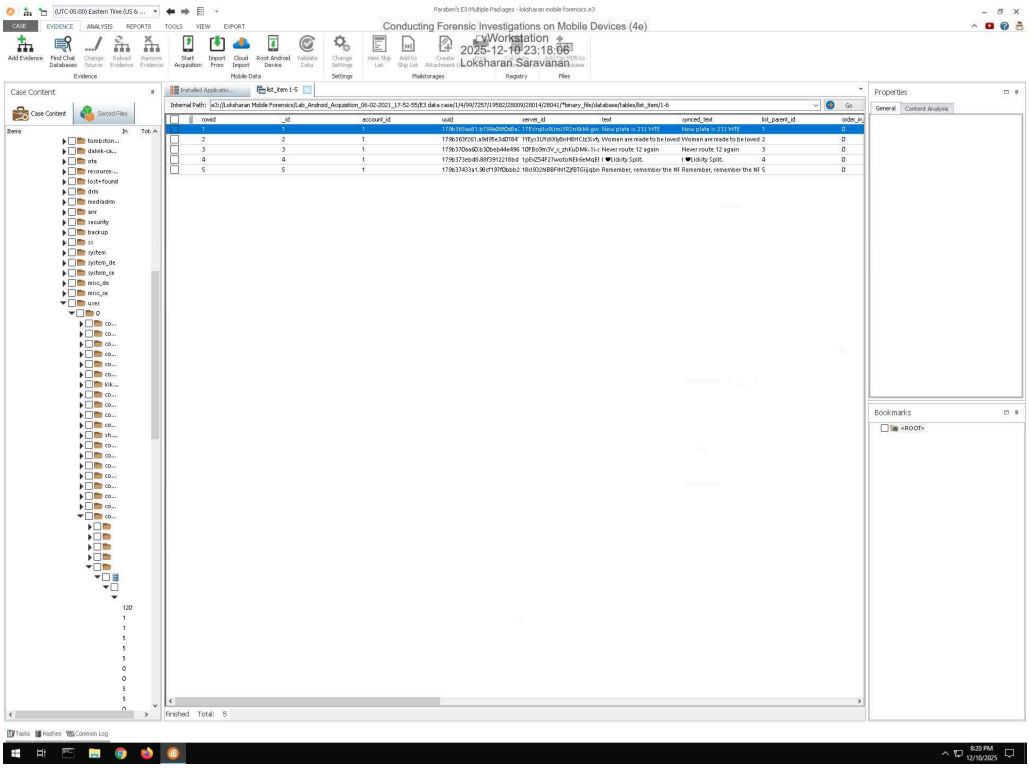
7. **Make a screen capture** showing the **contents of the Own Whispers grid**.



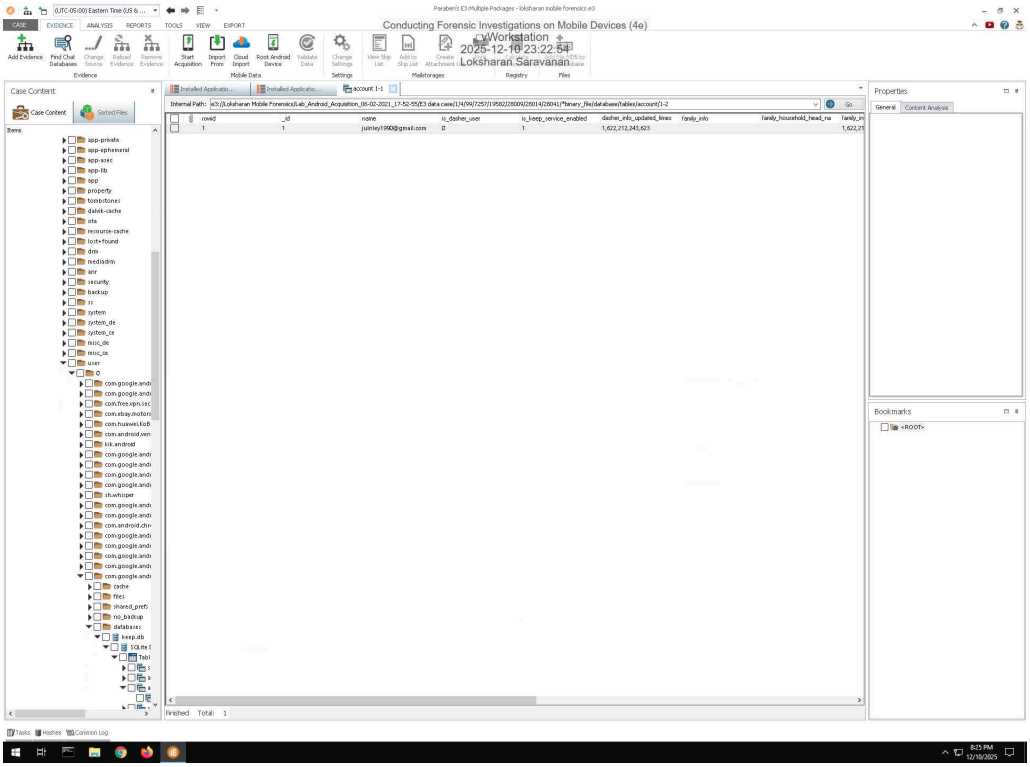
10. **Make a screen capture** showing the **contents of the History grid**.



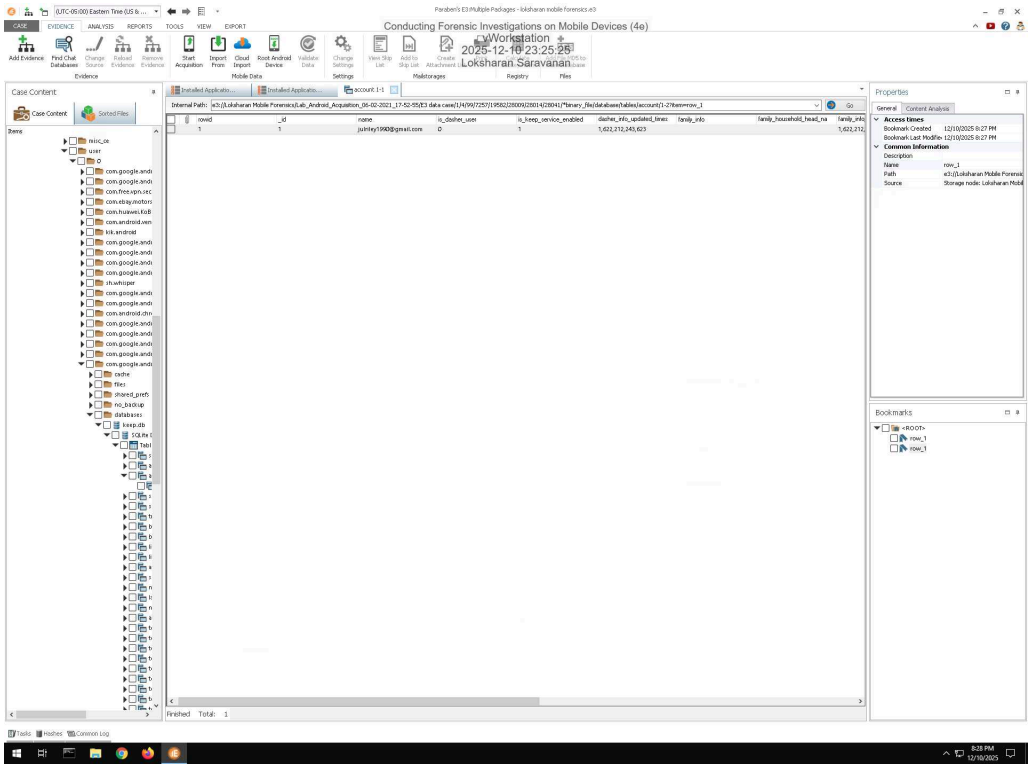
17. **Make a screen capture** showing the **contents of the list_item 1-5 table**.



20. **Make a screen capture** showing the **Keep Notes account owner**.



23. **Make a screen capture** showing the **Investigative Report's Table of Contents**.



Section 3: Challenge and Analysis

Part 1: Research Report Writing for Digital Forensics

Prepare a brief summary of the appropriate structure and best practices for preparing a digital forensics report.

A digital forensics report should follow a clear, structured format so the findings are easy to understand, defensible, and suitable for both technical and non-technical audiences. A typical report includes: (1) a Case Summary or Executive Summary that briefly explains the purpose of the investigation, the devices examined, the scope, and the major findings in simple, non-technical language; (2) a Background/Scope section describing why the investigation was initiated and what questions the examiner aimed to answer; (3) a Methodology section documenting how evidence was collected, preserved, and analyzed, including tools, procedures, and chain of custody; (4) a Findings and Analysis section presenting the artifacts recovered, their relevance, and interpretation; and (5) a Conclusion that clearly states what the evidence supports, what cannot be determined, and any limitations.
Best practices include writing clearly and objectively, avoiding speculation, separating facts from interpretations, documenting every step for reproducibility, and using consistent formatting. Reports should be organized so non-technical readers can understand the summary, while technical details, screenshots, logs, and hashes are placed in appendices to maintain clarity. Overall, the goal is to create an accurate, unbiased, well-structured report that can withstand legal or administrative review.

Part 2: Draft a Forensic Report

Case Summary

This investigation involved the forensic examination of two mobile devices an iPhone and an Android phone to identify and document any relevant digital evidence. The purpose of the analysis was to recover user activity, communications, application data, and any artifacts potentially related to the case scenario. Forensic images of both devices were acquired using approved tools, and all evidence was preserved following standard chain-of-custody procedures. The goal was to determine what activities took place on each device and whether any user actions or data were significant to the investigation.

Findings and Analysis

Analysis of the iPhone revealed multiple relevant artifacts, including stored messages, call logs, application usage records, photos, and device metadata. Recovered data showed patterns of user communication, timestamps of key activities, and evidence of application interactions. File system artifacts and recovered logs helped reconstruct portions of the user's behavior and device usage timeline.
The Android device examination produced similar categories of evidence: text messages, call history, app data, Wi-Fi connections, browser activity, media files, and selected deleted items where recoverable. System logs and application artifacts allowed reconstruction of significant events and provided context for user actions. In both devices, artifacts were analyzed using validated forensic tools, and all findings were compared against the investigation objectives to determine their relevance.

Conclusion

The forensic analysis of both the iPhone and Android devices successfully recovered relevant digital evidence that supports understanding the user's activity and behaviors during the timeframe of interest. The findings from messages, logs, application data, and system artifacts helped establish a clear timeline and provided insight into the actions performed on each device. No evidence outside the defined scope was introduced, and all procedures followed accepted forensic standards. Overall, the examination met the objectives of the investigation and produced reliable results that can be used for further decision-making or legal review.