Student:	Email:
muhammad zahid	zahid1mz@cmich.edu

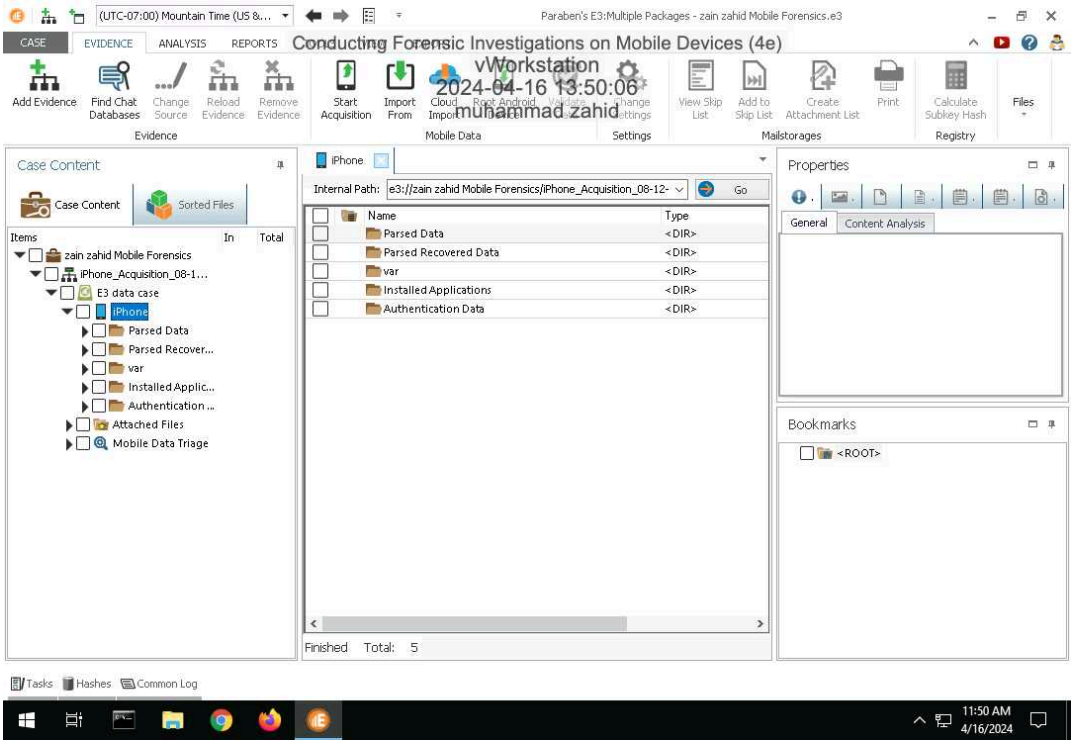
Time on Task:	Progress:
5 hours, 56 minutes	100%

Report Generated: Tuesday, April 16, 2024 at 5:06 PM

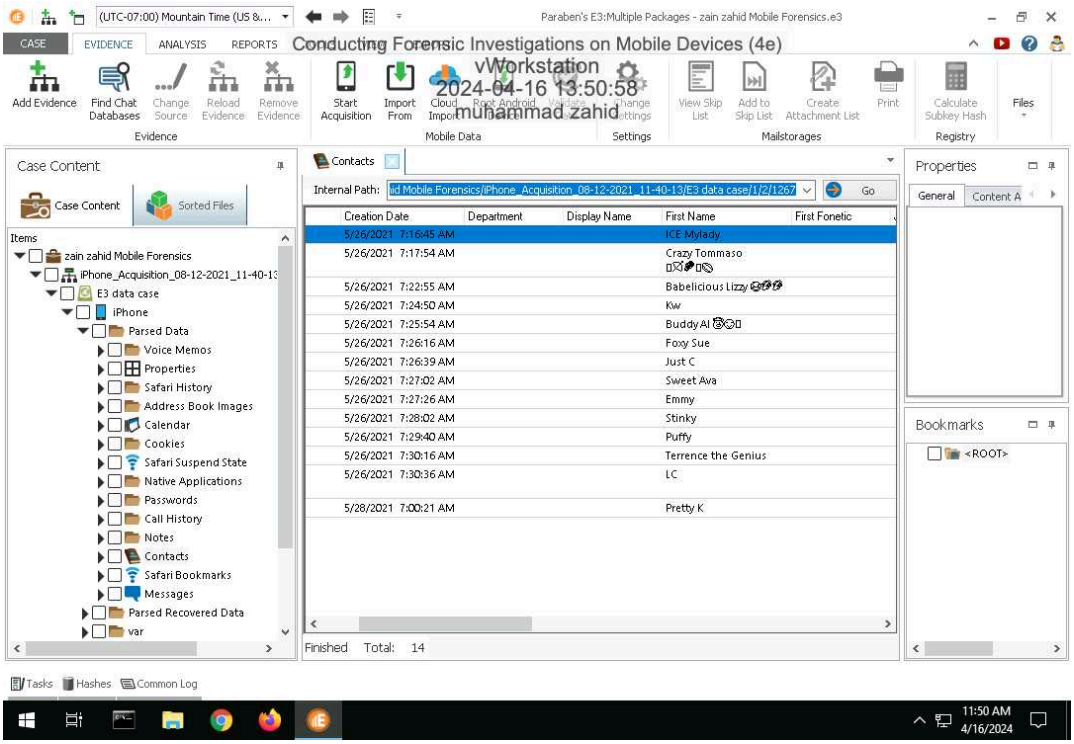
Section 1: Hands-On Demonstration

Part 1: Identify Forensic Evidence in an iOS Data Case

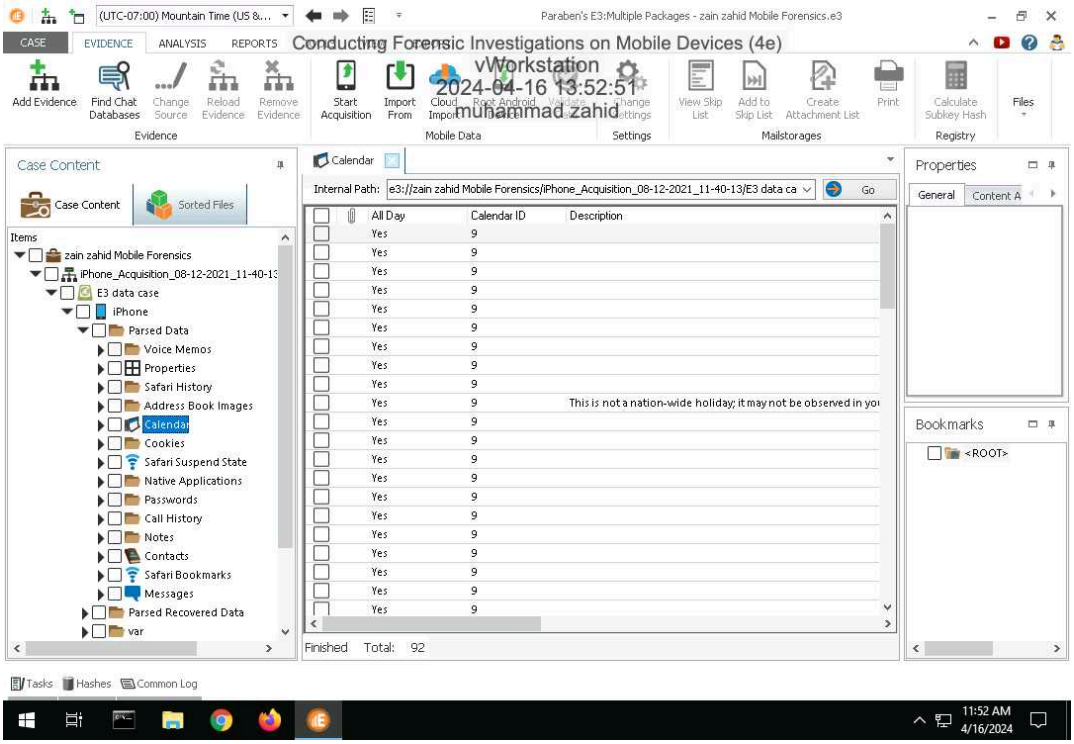
8. **Make a screen capture** showing the **contents of the Properties pane**.



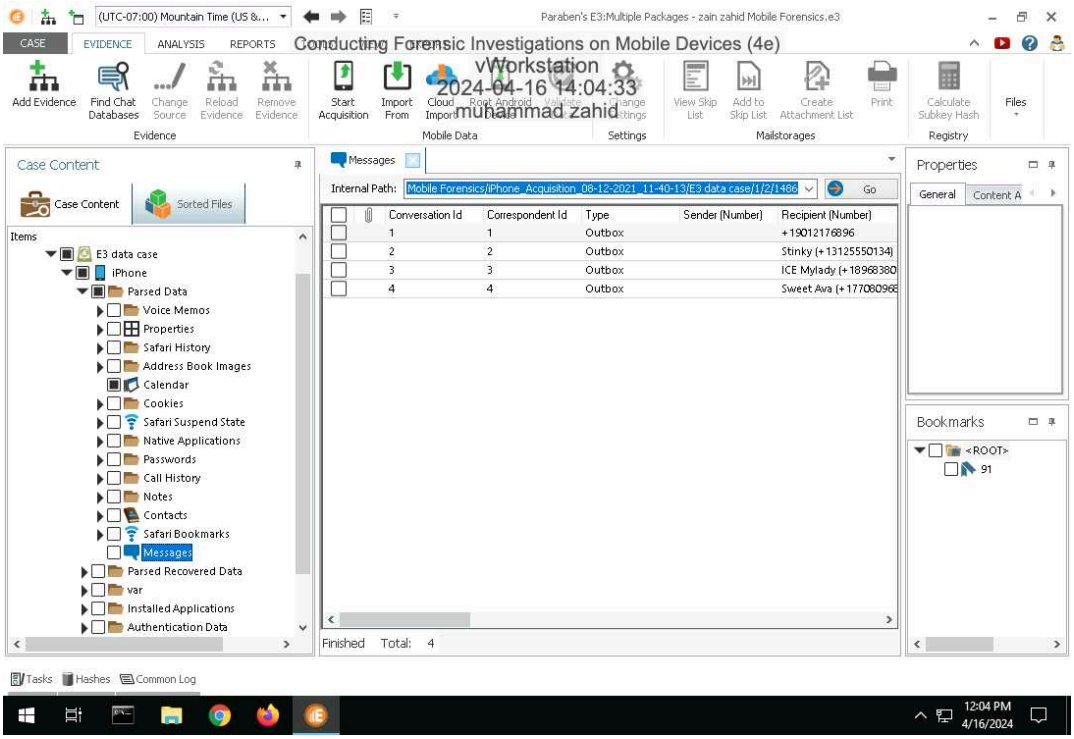
11. **Make a screen capture** showing the **contents of the Contacts grid**.



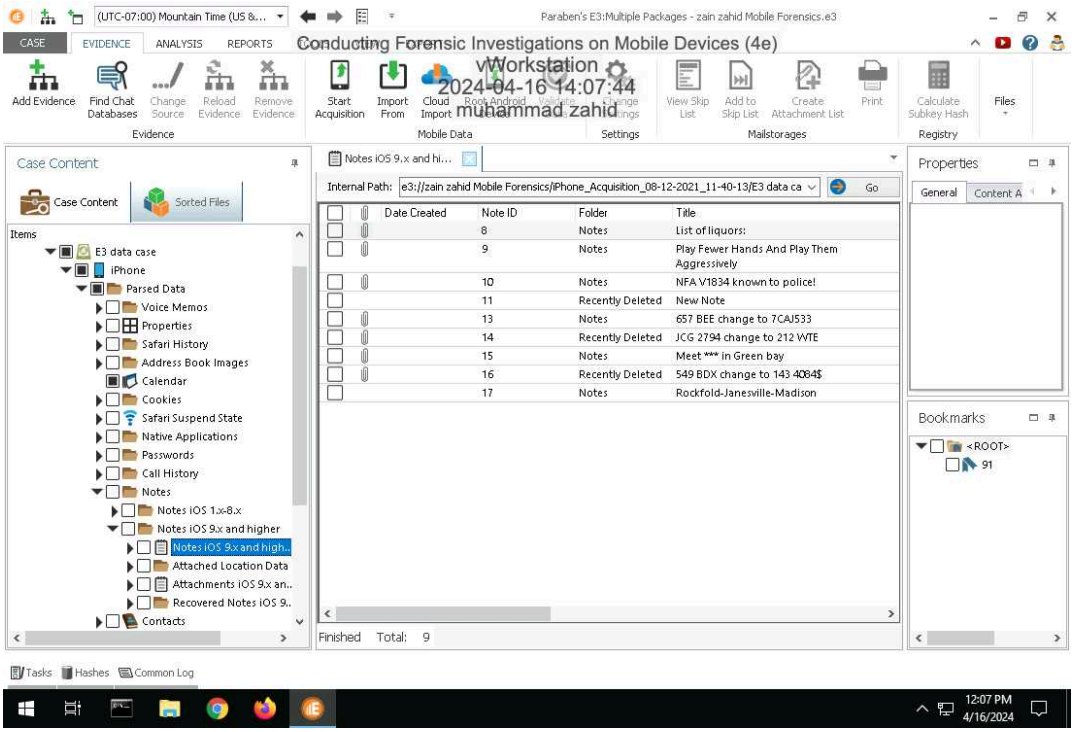
14. **Make a screen capture** showing the **contents of the Calendar grid**.



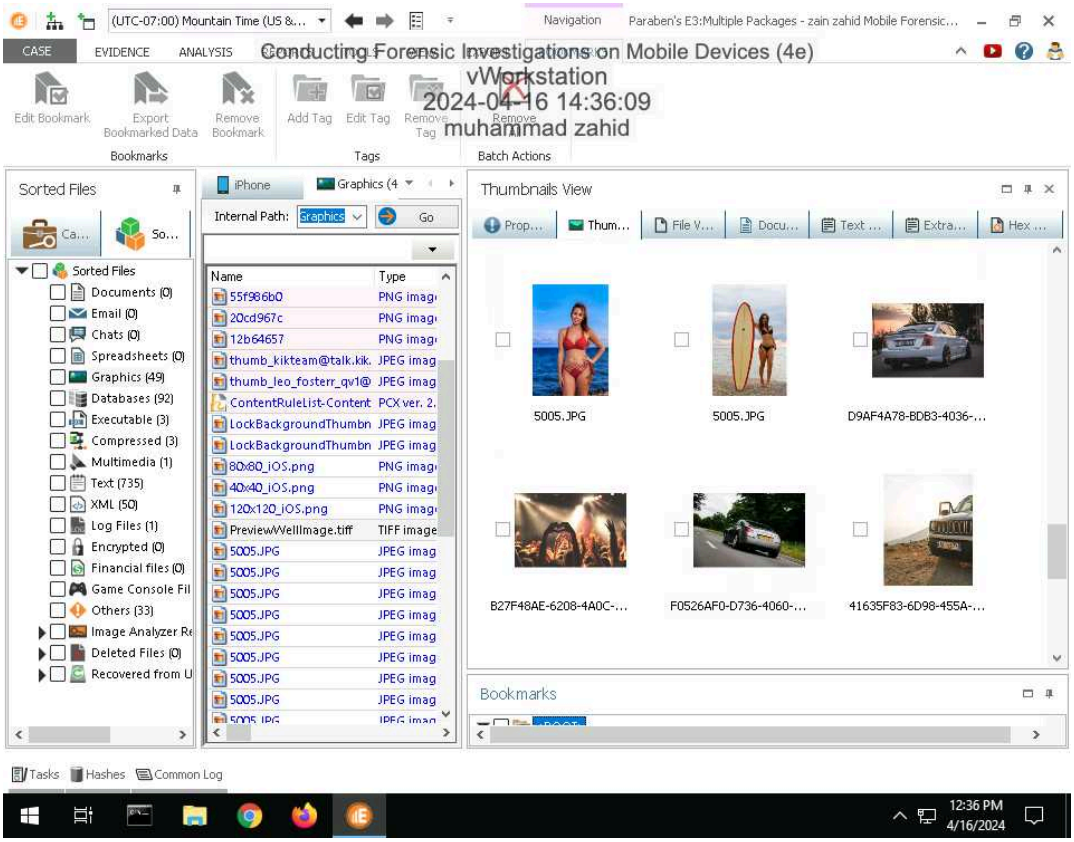
20. **Make a screen capture** showing the **contents of the Messages grid**.



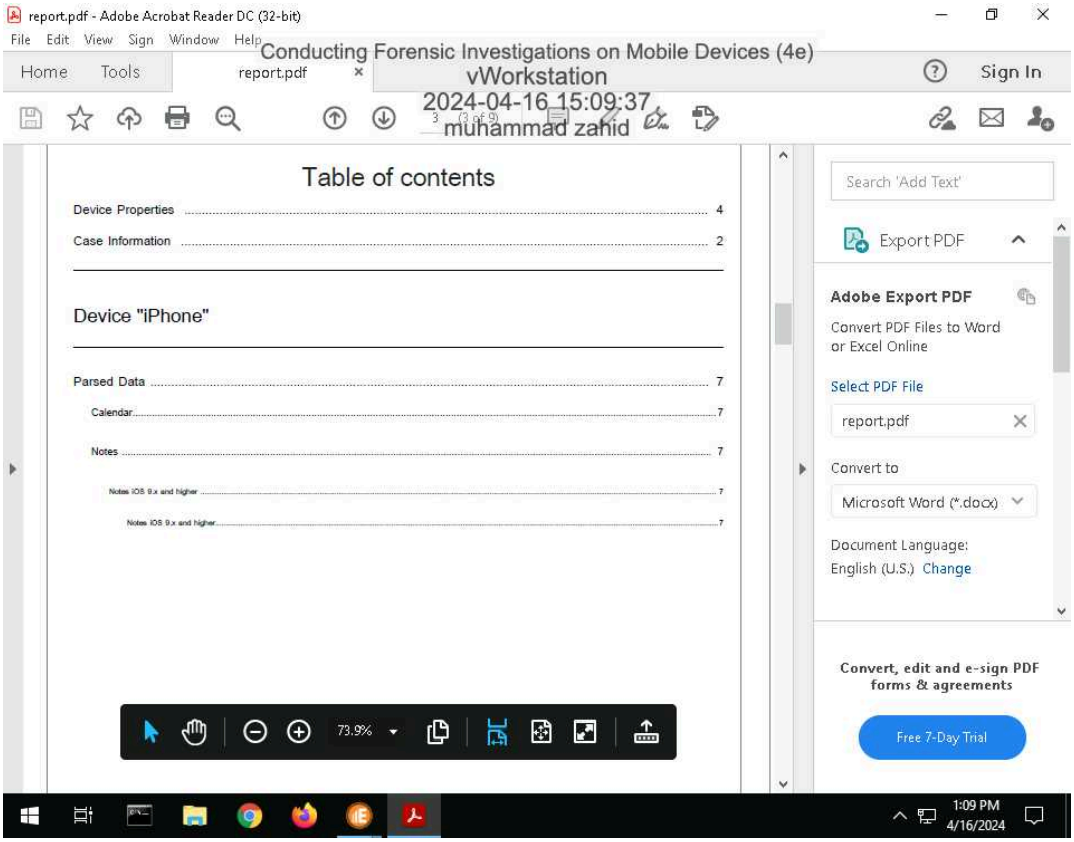
24. **Make a screen capture** showing the **contents of the Notes grid**.



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

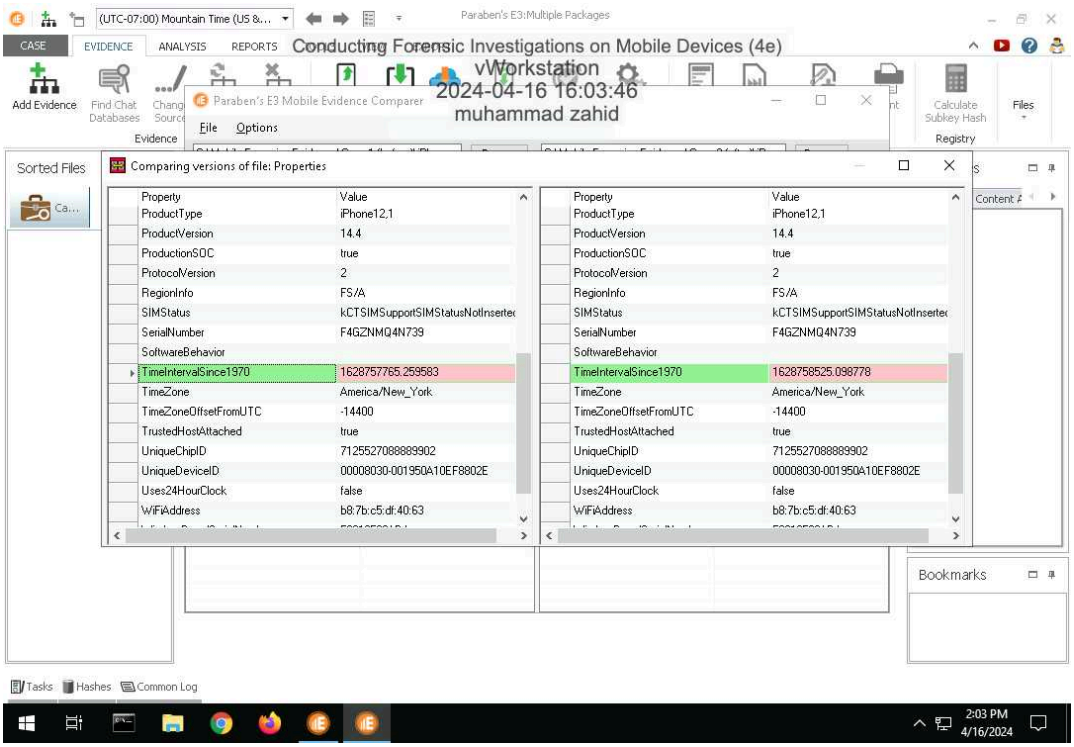


44. **Make a screen capture** showing the **Table of contents in the investigative report**.

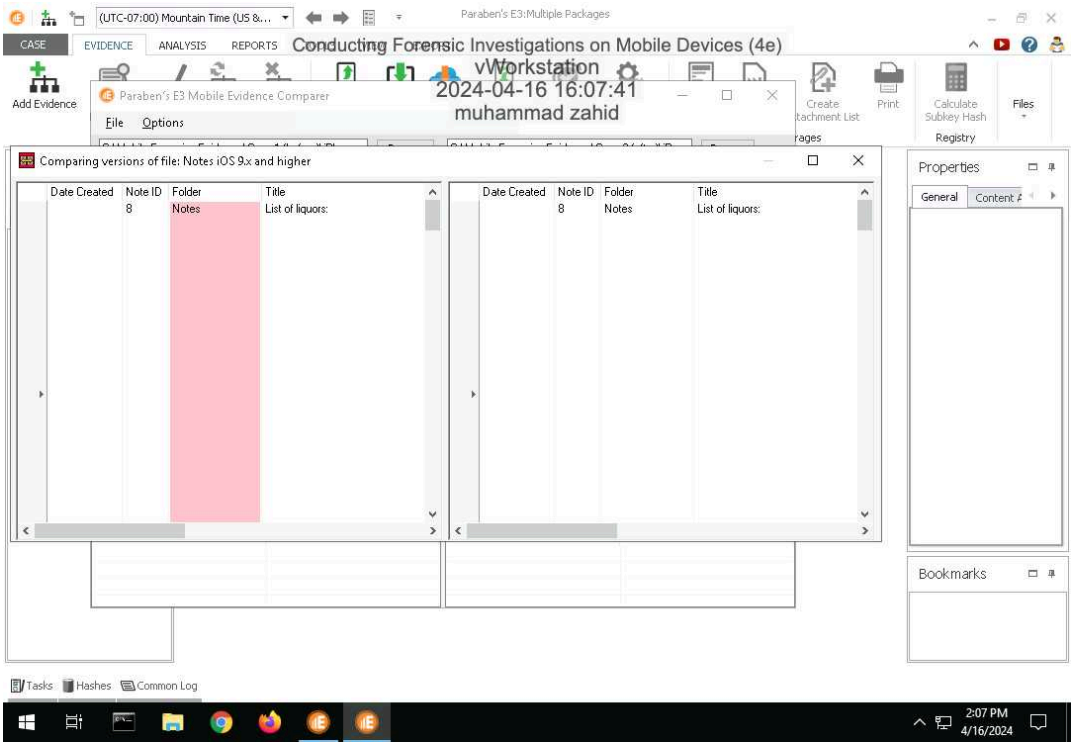


Part 2: Compare iOS Data Cases

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



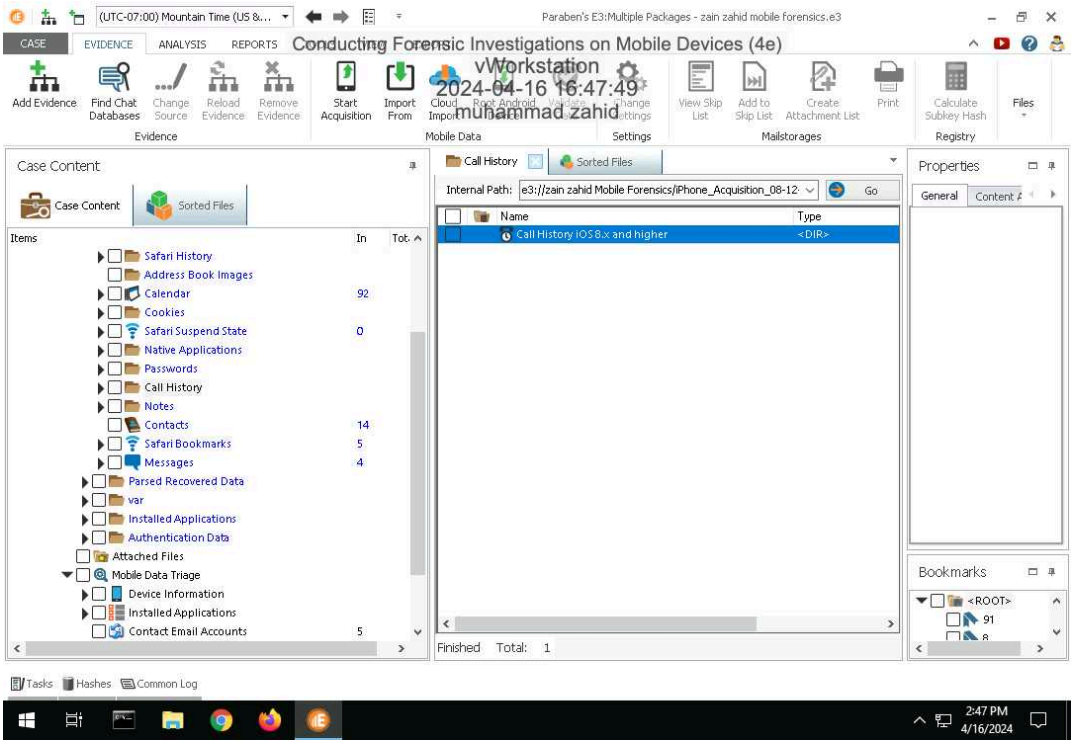
15. **Make a screen capture** showing the **additional note in the newer data case**.



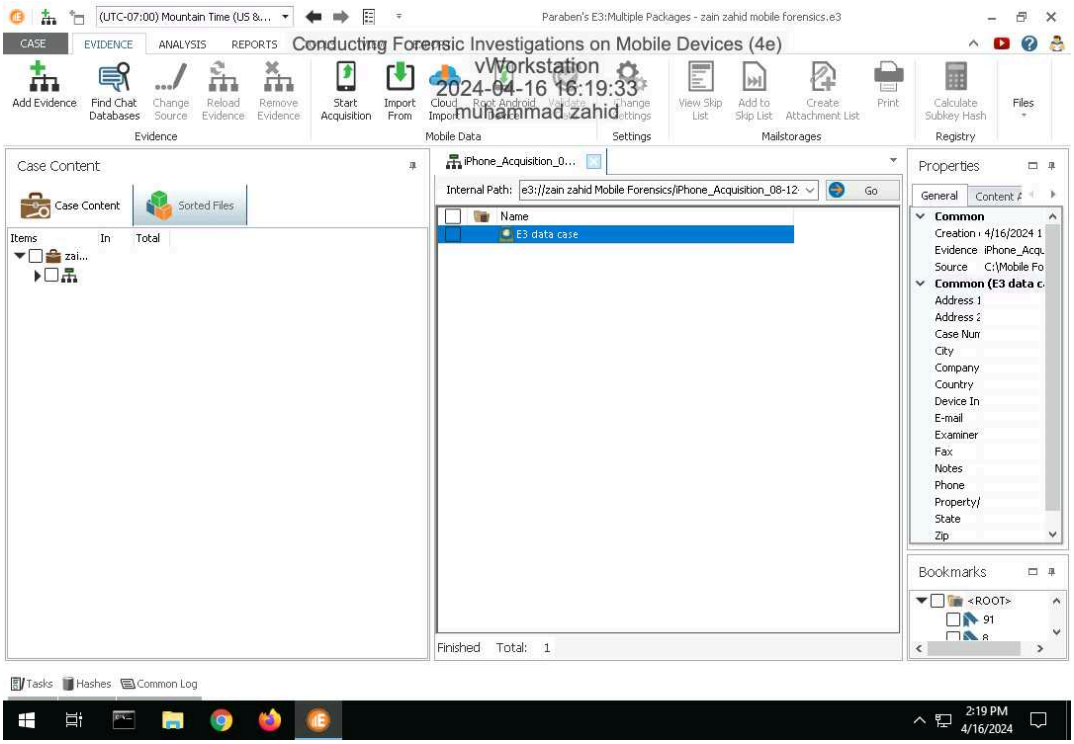
Section 2: Applied Learning

Part 1: Identify Forensic Evidence in Android User Data

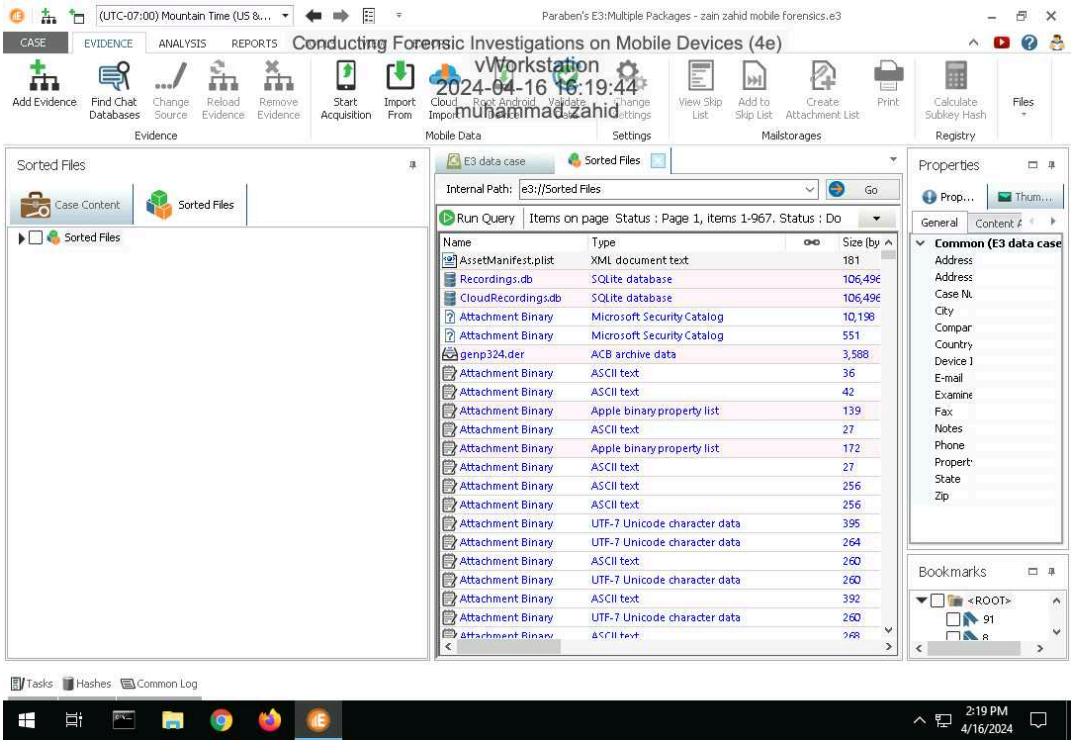
7. **Make a screen capture** showing the **Device Information**.



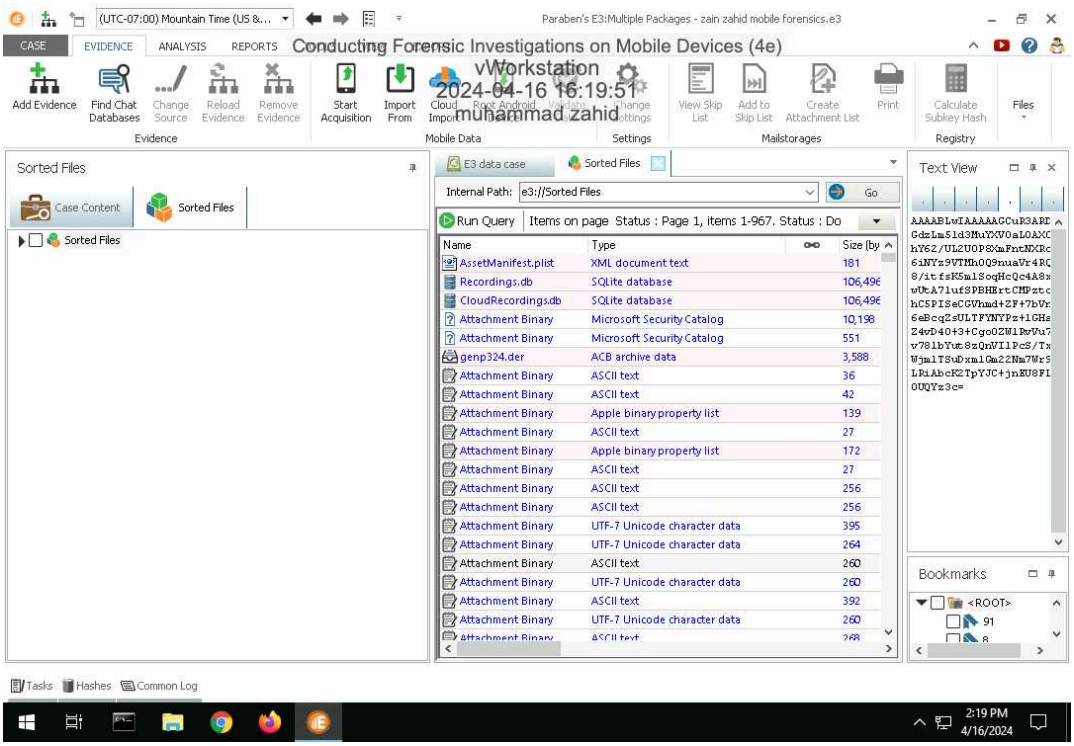
9. **Make a screen capture** showing the **ICE Contacts**.



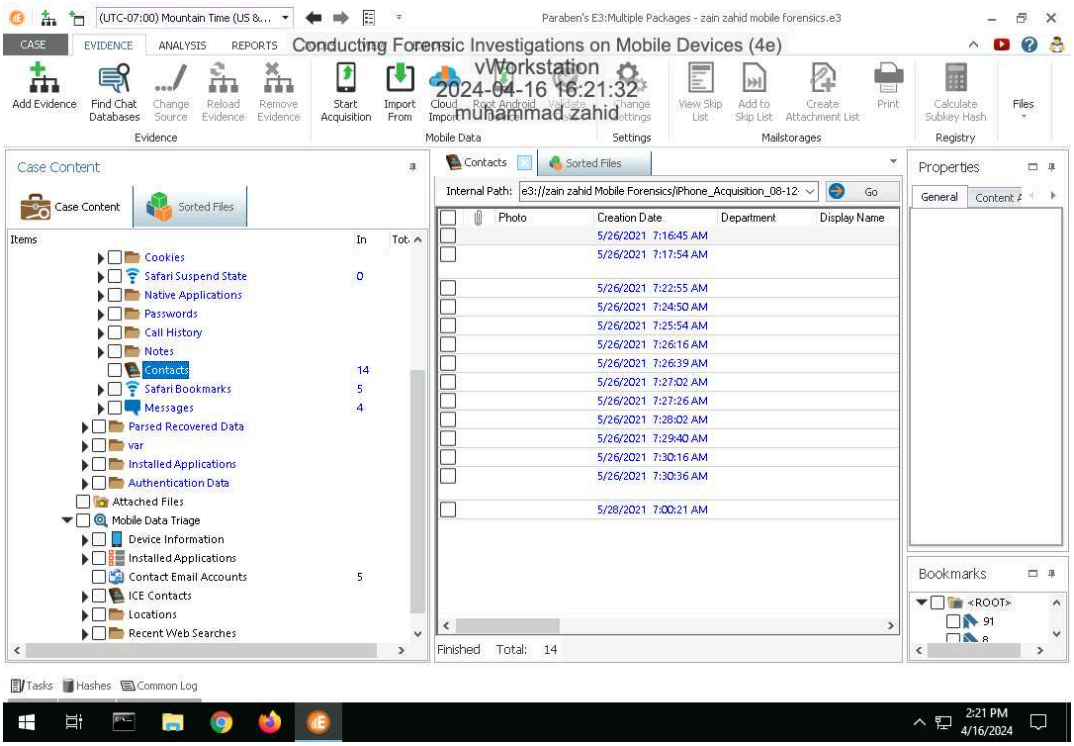
12. **Make a screen capture** showing the **Contact Email Accounts**.



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

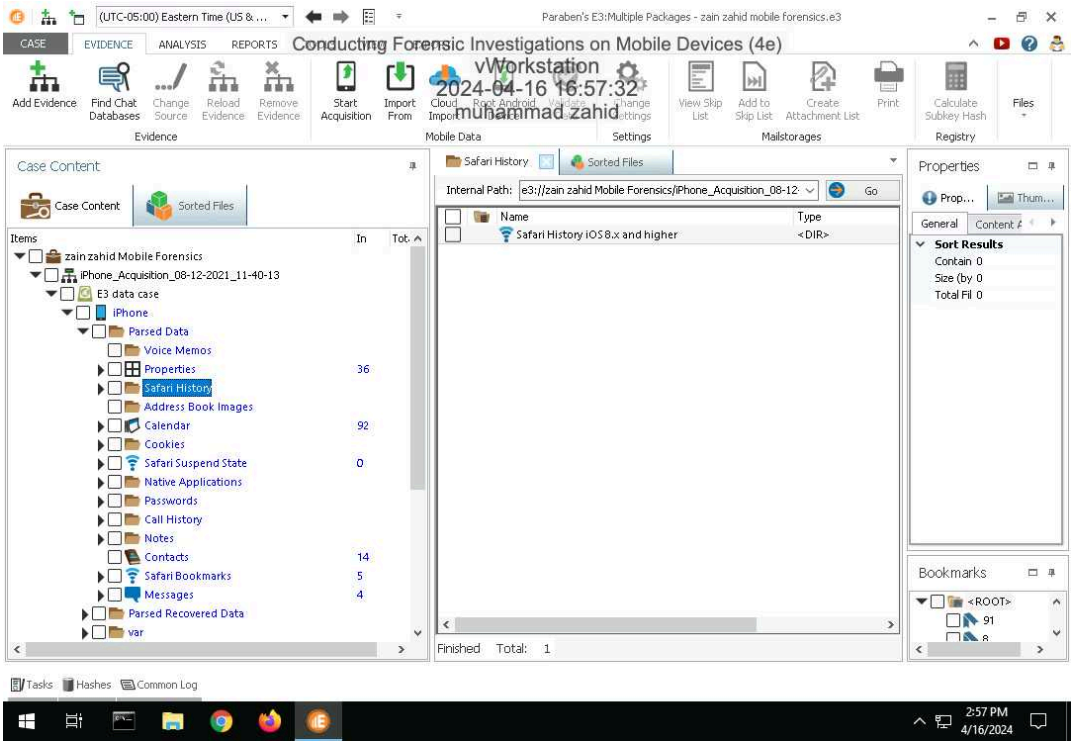


19. **Make a screen capture** showing the **recovered contact information from the Android phone**.

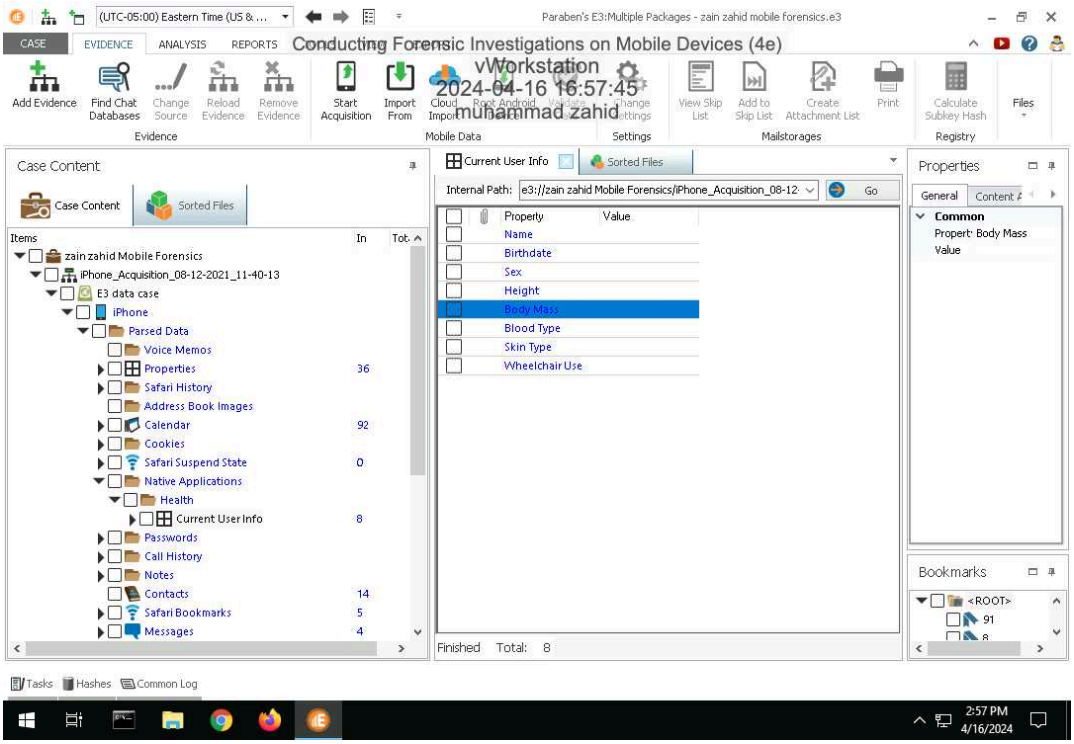


Part 2: Identify Forensic Evidence in Android Application Data

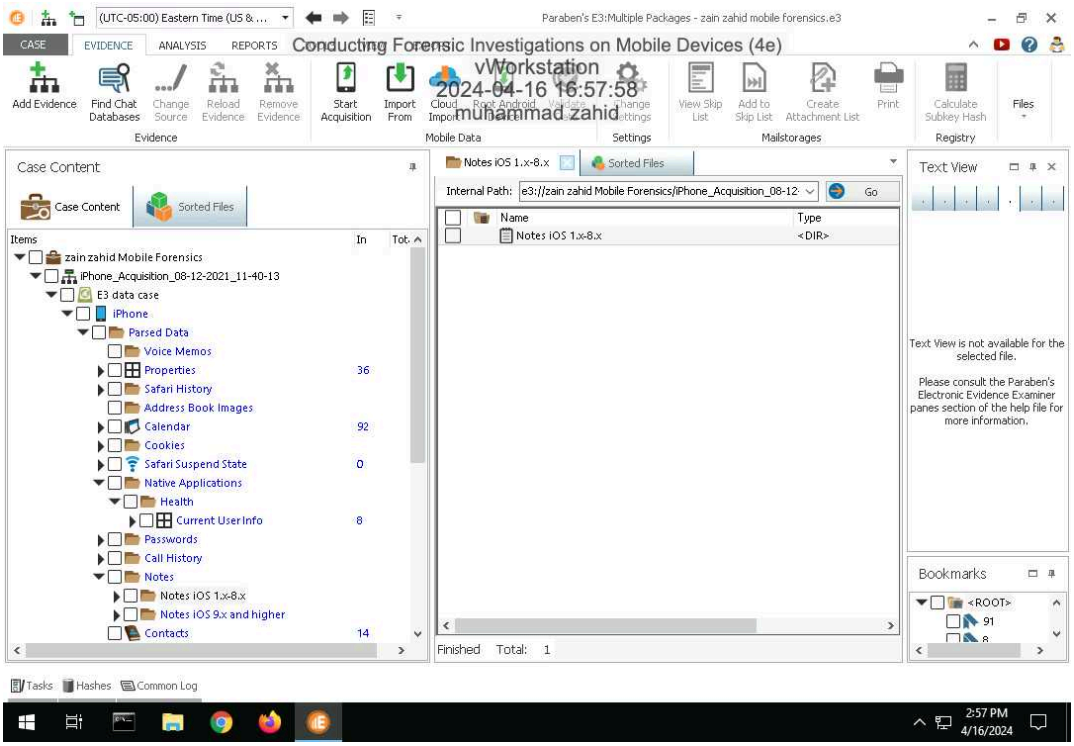
4. **Make a screen capture** showing the **User Activity Timeline between 9:17:47 AM and 9:24:51 AM on 6/2/2021**.



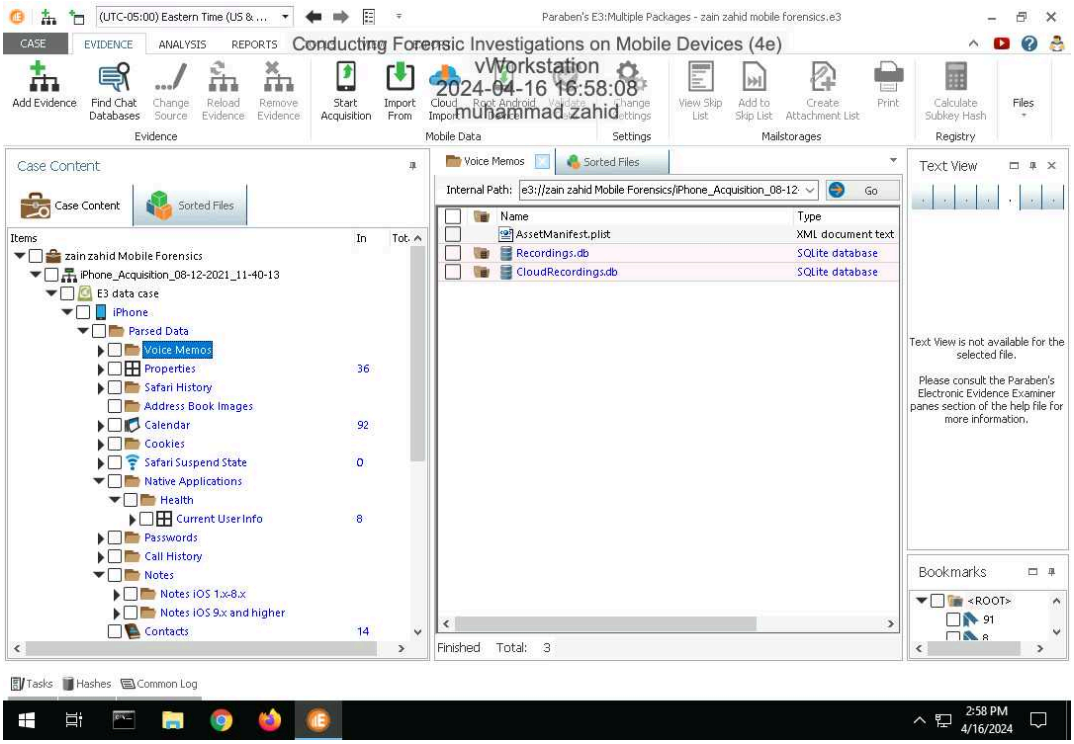
7. **Make a screen capture** showing the **contents of the Own Whispers grid**.



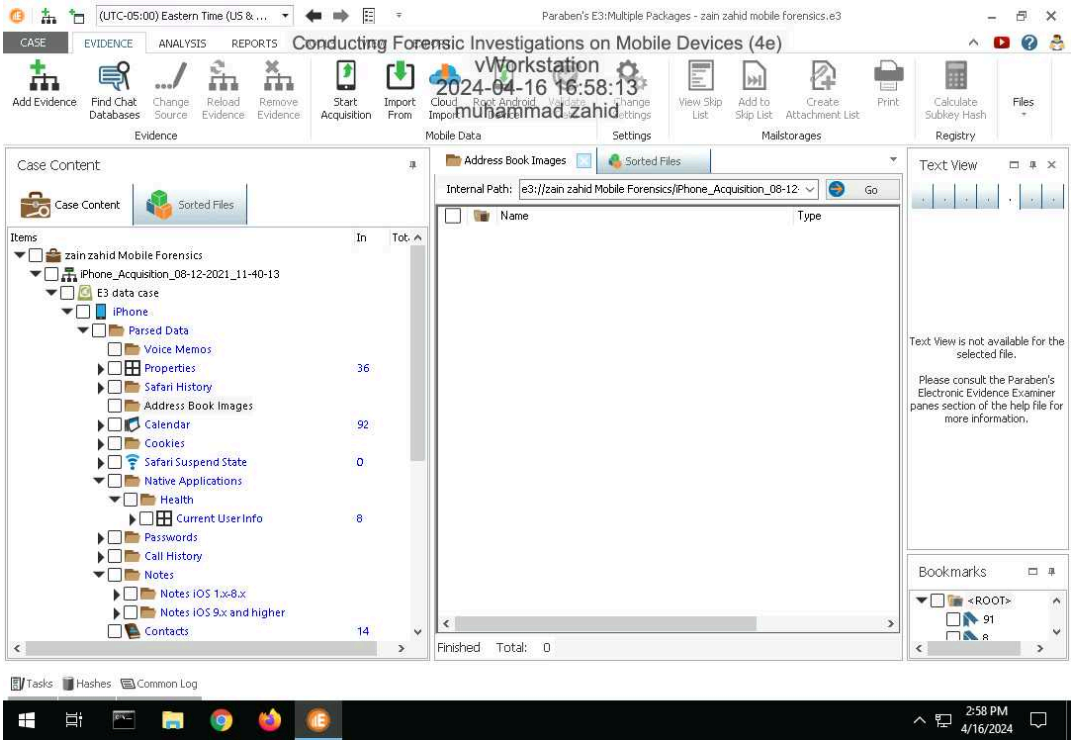
10. **Make a screen capture** showing the **contents of the History grid**.



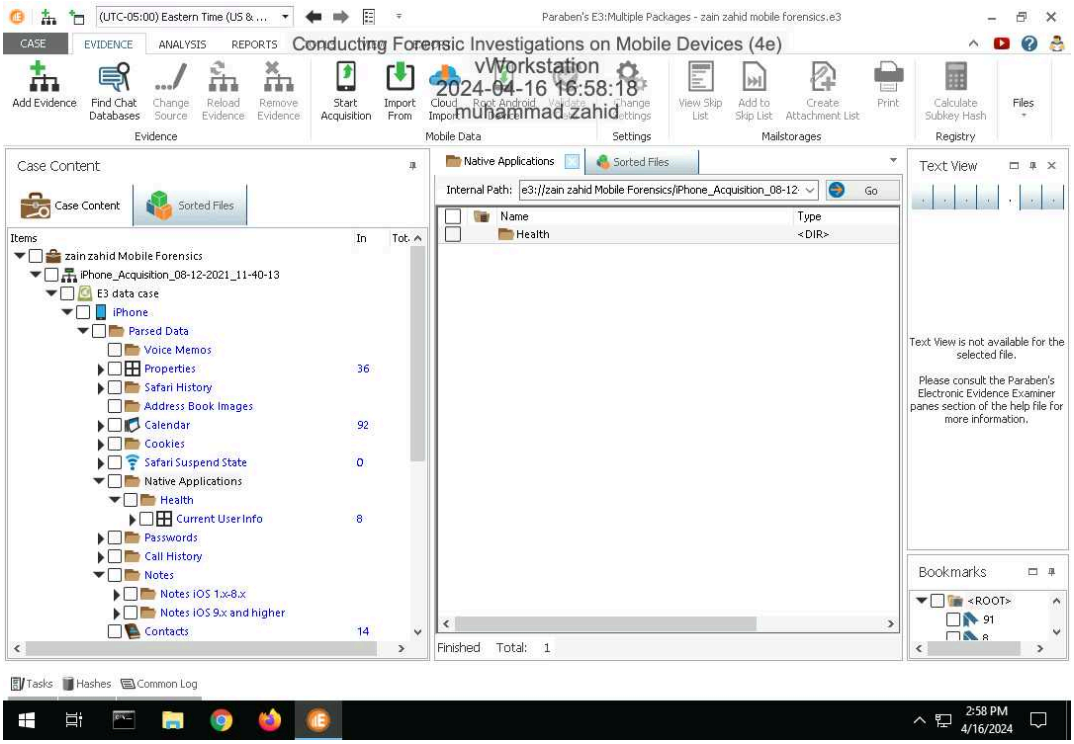
17. **Make a screen capture** showing the **contents of the list_item 1-5 table**.



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.

Preparing a digital forensics report involves adhering to a structured format and best practices to ensure clarity and reliability. The report typically begins with a title page detailing the case information and the names of involved parties, followed by a table of contents for easy navigation. An executive summary provides a concise overview of the investigation, while the introduction sets the context and scope. Methodology outlines the techniques and tools used, while evidence collection documents the forensically sound retrieval of digital evidence. Analysis presents findings, supported by evidence, with a discussion of their significance. The conclusion summarizes findings and implications, with recommendations for further action. References cite sources and tools, while appendices include supplementary materials. Throughout, maintaining objectivity, accuracy, and professionalism is paramount.

Part 2: Draft a Forensic Report

Case Summary

The investigation pertains to a complex incident involving digital security breaches and potential data manipulation within a corporate environment. Initial findings suggest unauthorized access to sensitive systems, leading to potential data tampering and compromised integrity of digital records. The scope of the breach and its impact on organizational operations remain under scrutiny. Key forensic evidence includes anomalous network activity logs, suspicious file modification timestamps, and indications of attempted data exfiltration. Further analysis is warranted to ascertain the extent of the intrusion, identify responsible parties, and recommend mitigation strategies to bolster cybersecurity defenses.

Findings and Analysis

Data Tampering: Indications of unauthorized modifications or deletions to digital files or system logs, compromising the integrity and reliability of stored information.
Phishing Attempts: Evidence of phishing emails or social engineering tactics used to trick users into divulging sensitive information, such as login credentials or financial data.
Insider Threats: Instances of privileged users or employees abusing their access rights to engage in malicious activities, such as data theft, sabotage, or unauthorized system alterations.
Exfiltration Attempts: Signs of data exfiltration or unauthorized extraction of confidential information from organizational networks, possibly for exploitation or sale on illicit markets.
Vulnerability Exploitation: Identification of exploited software vulnerabilities or misconfigurations that facilitated unauthorized access or compromise of systems, highlighting areas requiring security patching or remediation.
Forensic Artifacts: Discovery of digital forensic artifacts, such as file timestamps, registry entries, or memory dumps, providing insights into the timeline of events and tactics used by threat actors.

Conclusion

The forensic investigation revealed concerning anomalies within the digital infrastructure, indicating potential unauthorized access and data manipulation. Suspicious network activity, anomalous file modifications, and attempted data exfiltration were among the key findings. Further analysis is recommended to ascertain the extent of the breach and identify responsible parties, along with suggesting mitigation strategies to bolster cybersecurity defenses.