Student:	Email:
Vishal Singh Bhardvaj	

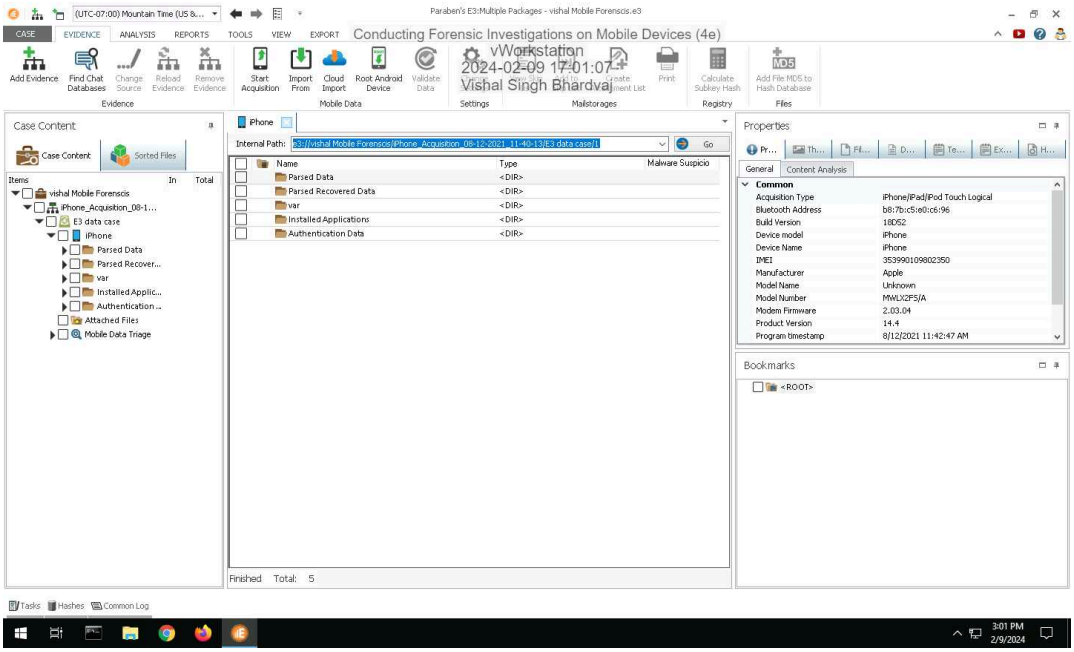
Time on Task:	Progress:
3 hours, 15 minutes	100%

Report Generated: Saturday, February 10, 2024 at 4:37 PM

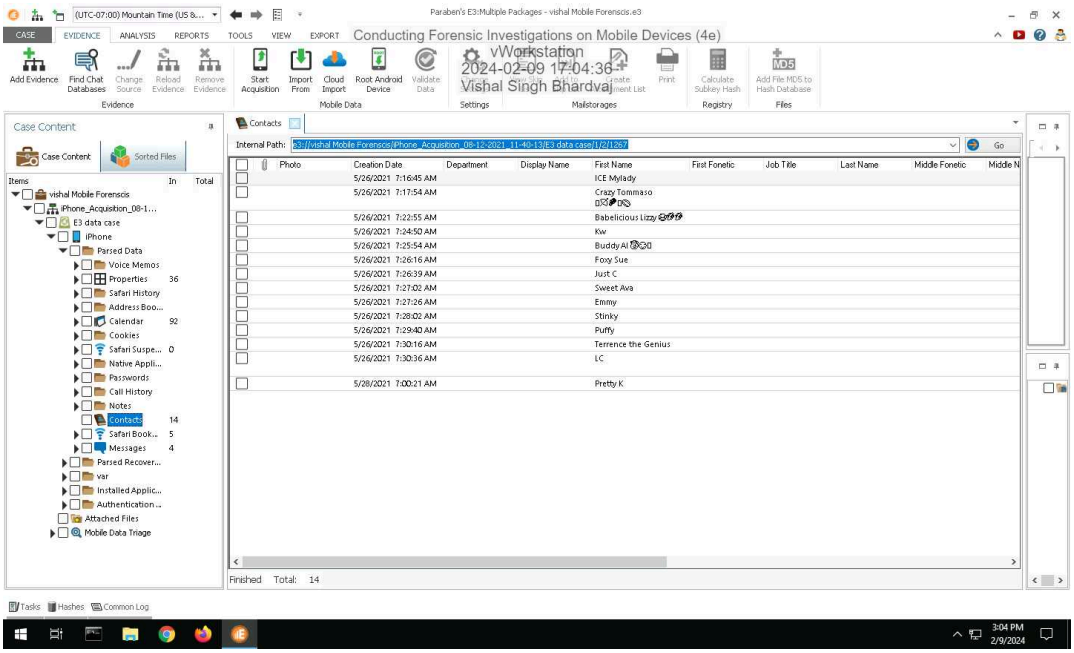
Section 1: Hands-On Demonstration

Part 1: Identify Forensic Evidence in an iOS Data Case

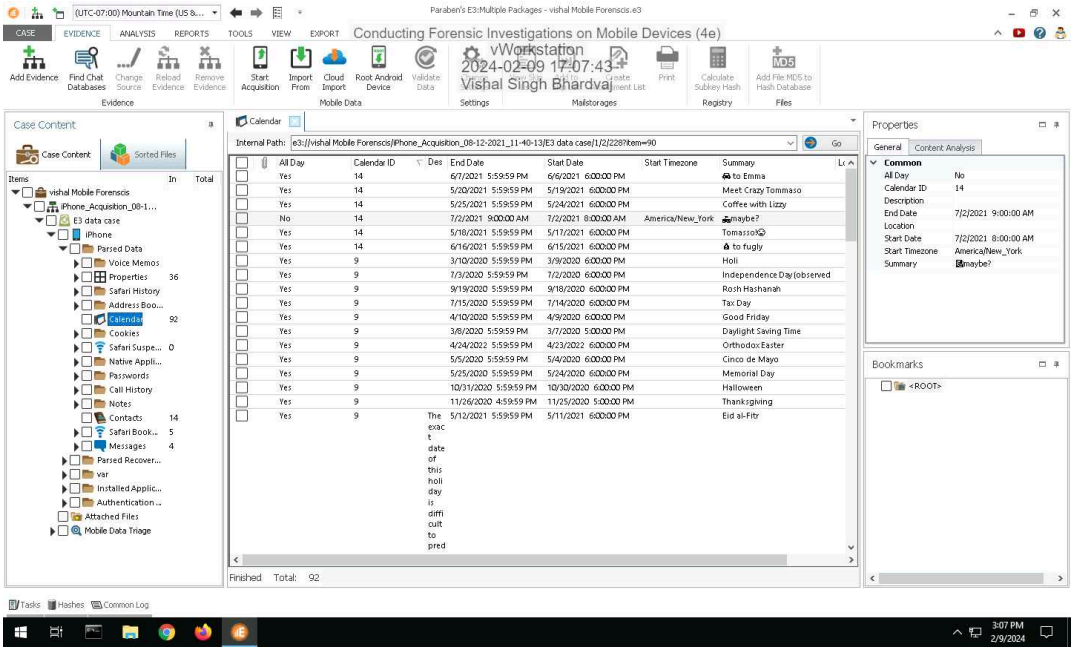
8. **Make a screen capture** showing the **contents of the Properties pane**.



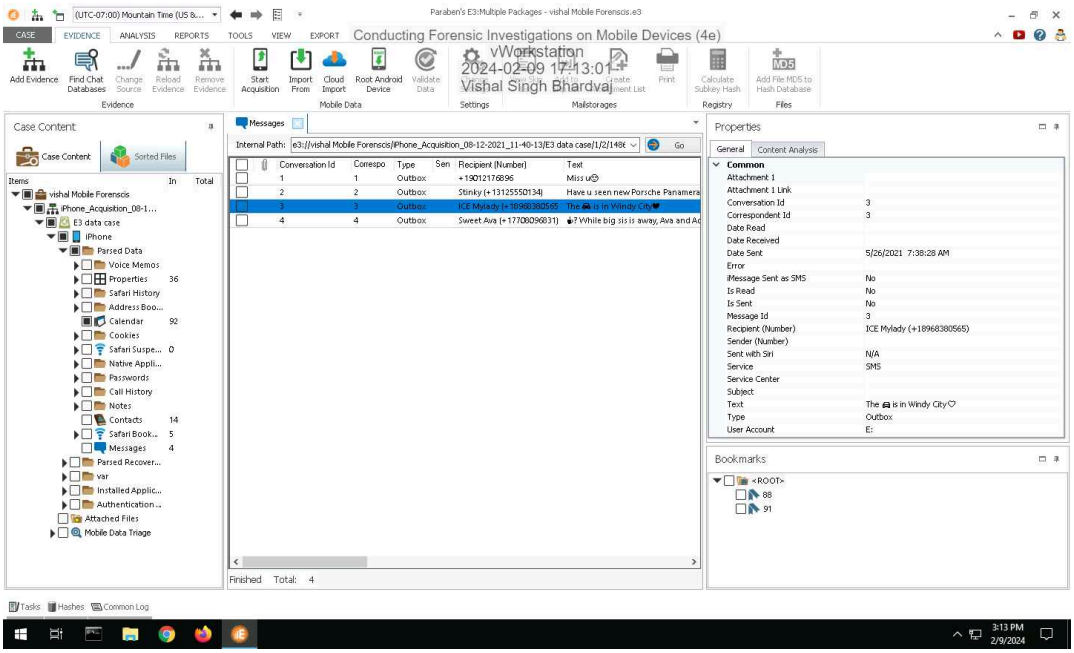
11. **Make a screen capture** showing the **contents of the Contacts grid**.



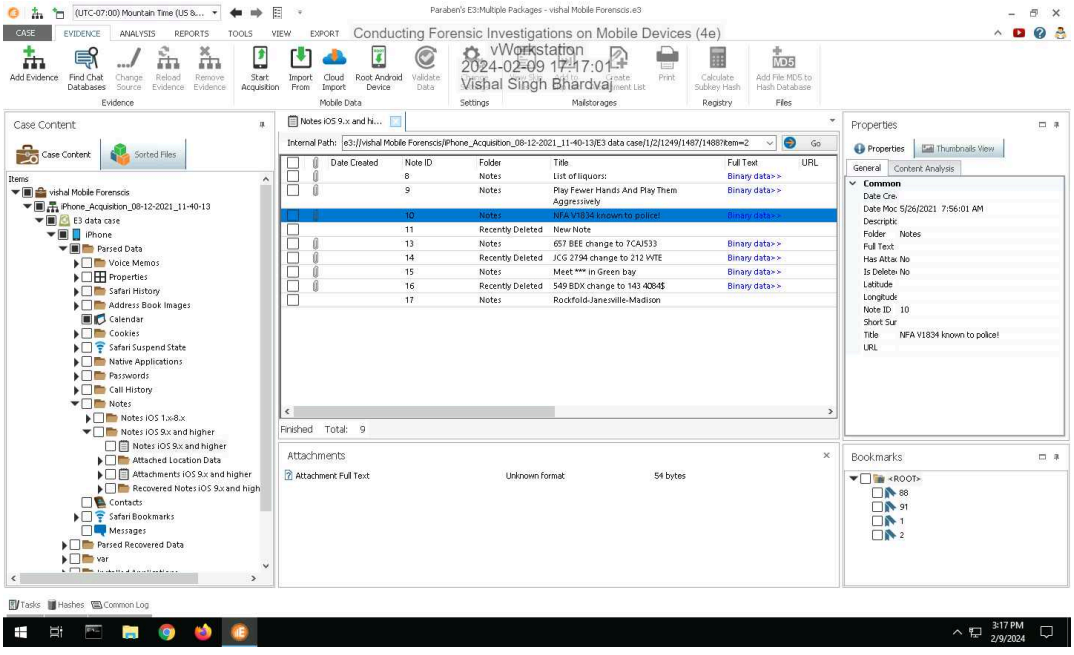
14. **Make a screen capture** showing the **contents of the Calendar grid**.



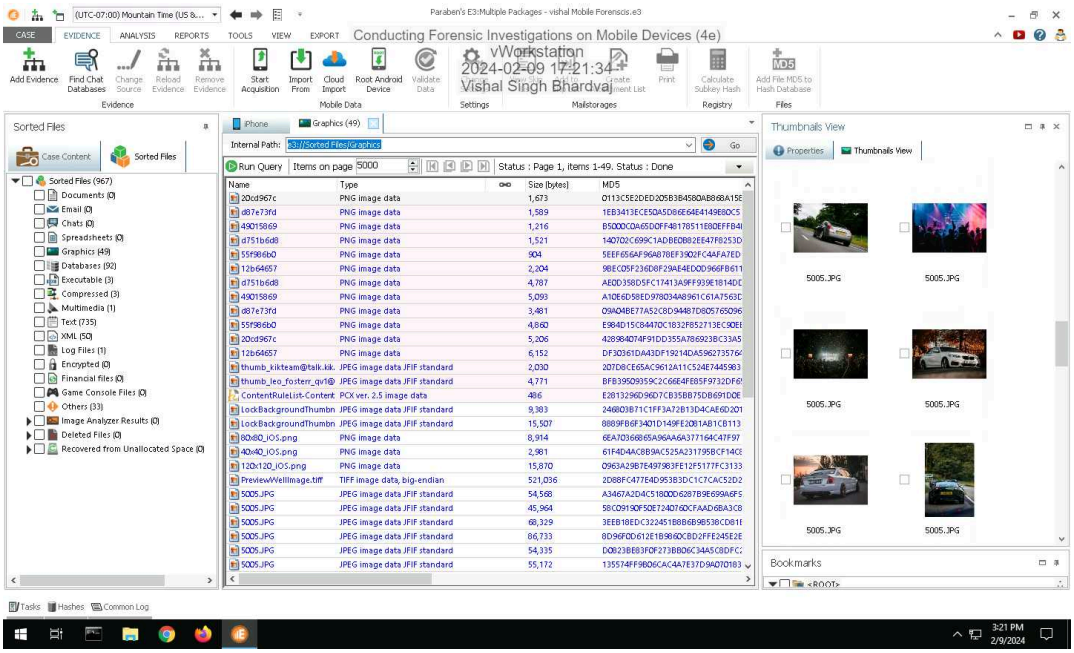
20. **Make a screen capture** showing the **contents of the Messages grid**.



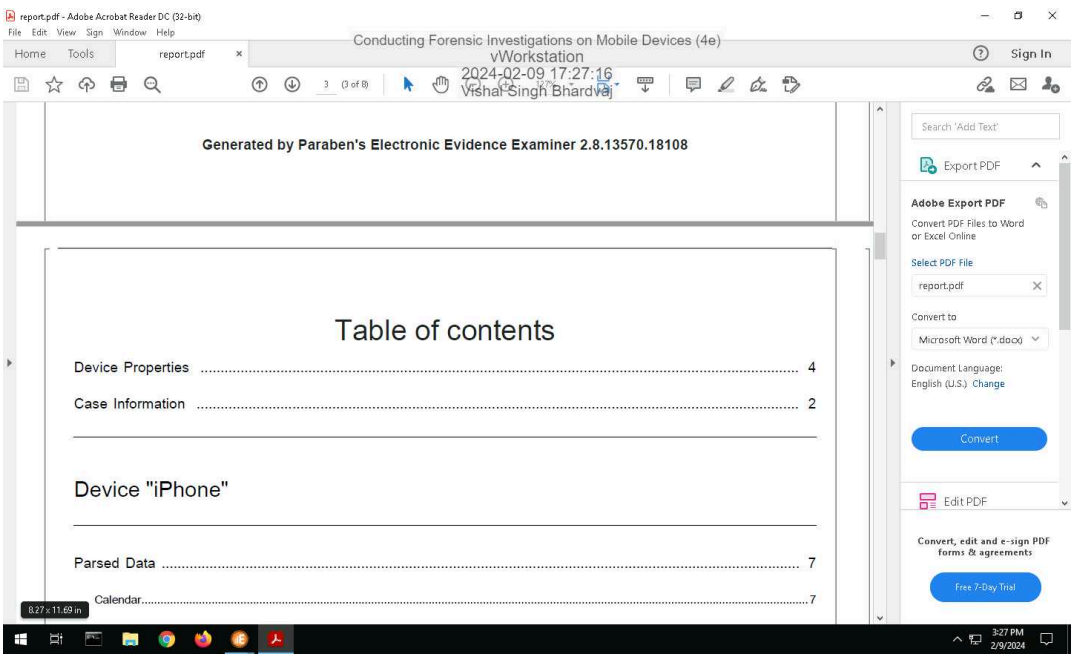
24. **Make a screen capture** showing the **contents of the Notes grid**.



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

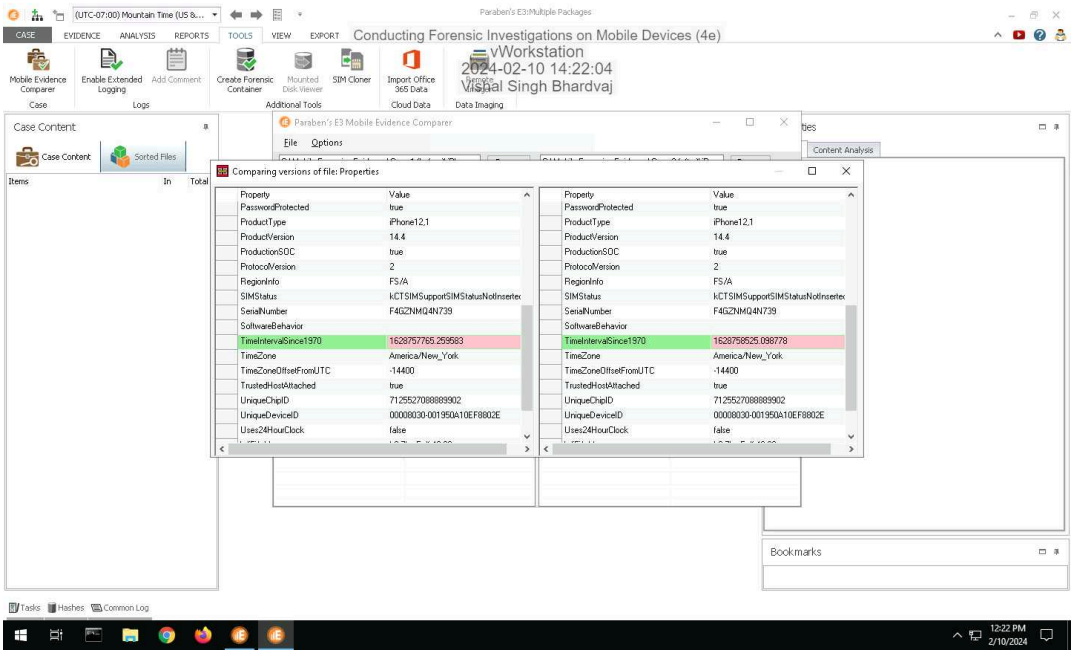


44. **Make a screen capture** showing the **Table of contents in the investigative report**.

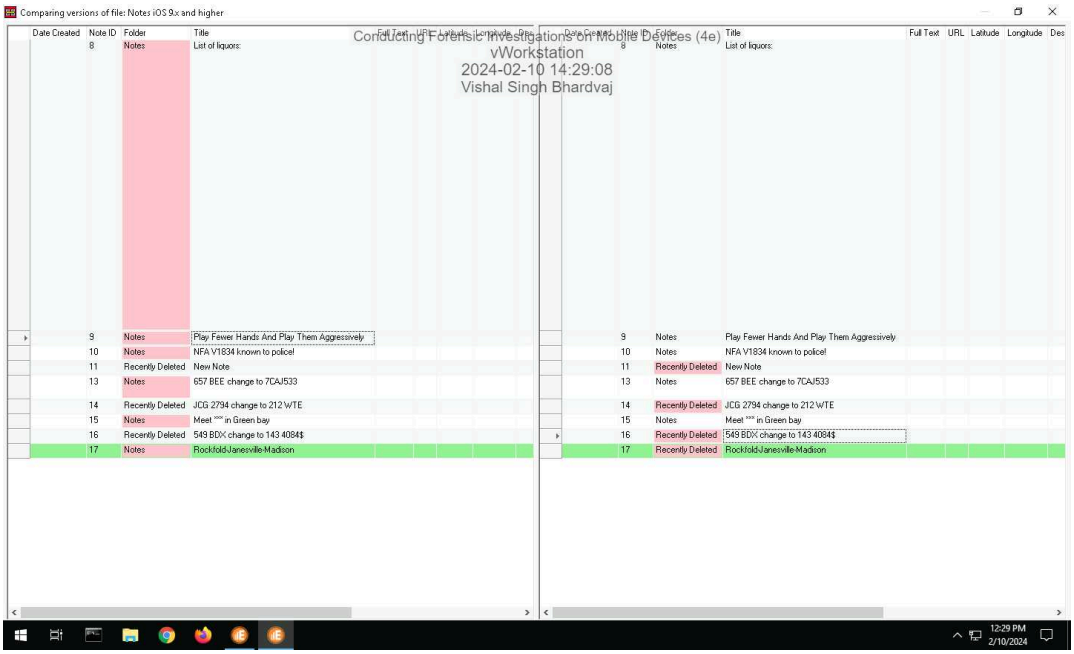


Part 2: Compare iOS Data Cases

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



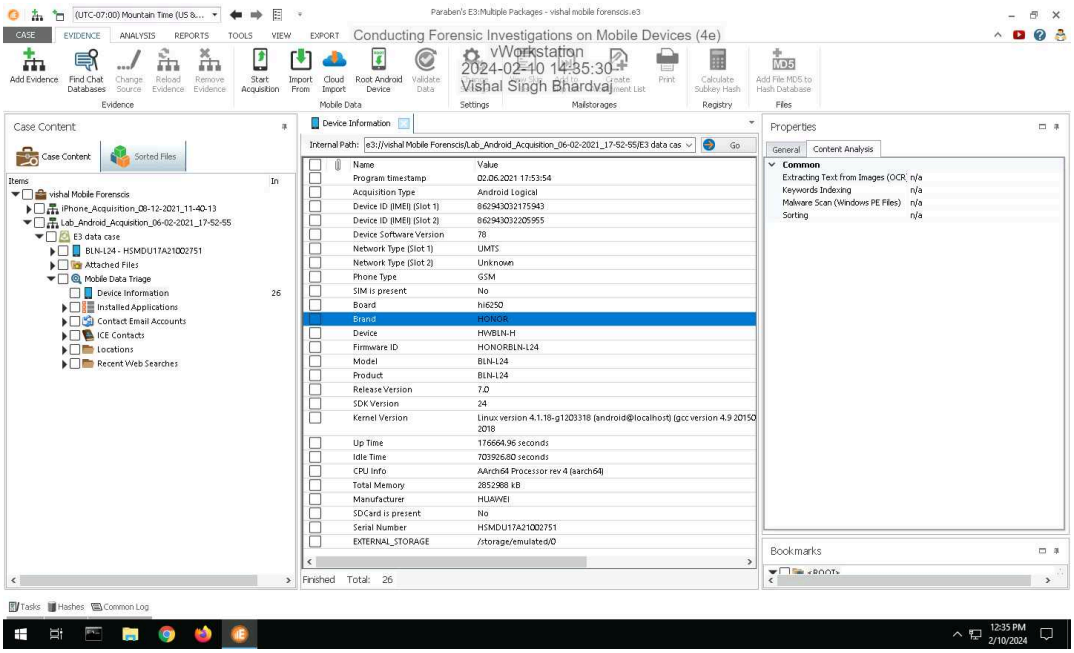
15. **Make a screen capture** showing the **additional note in the newer data case**.



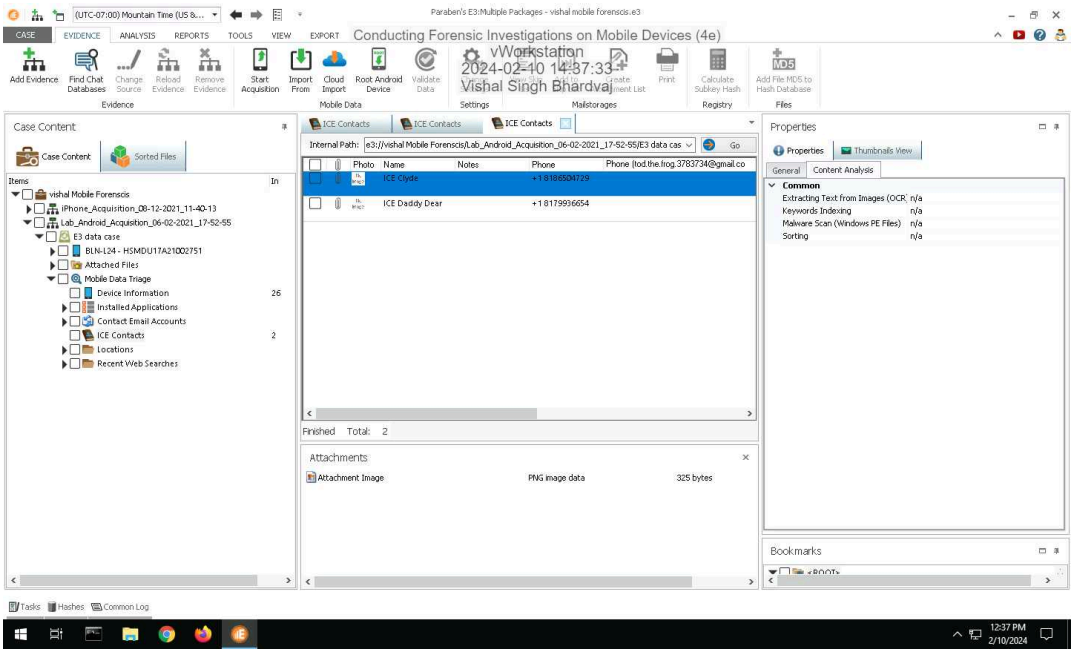
Section 2: Applied Learning

Part 1: Identify Forensic Evidence in Android User Data

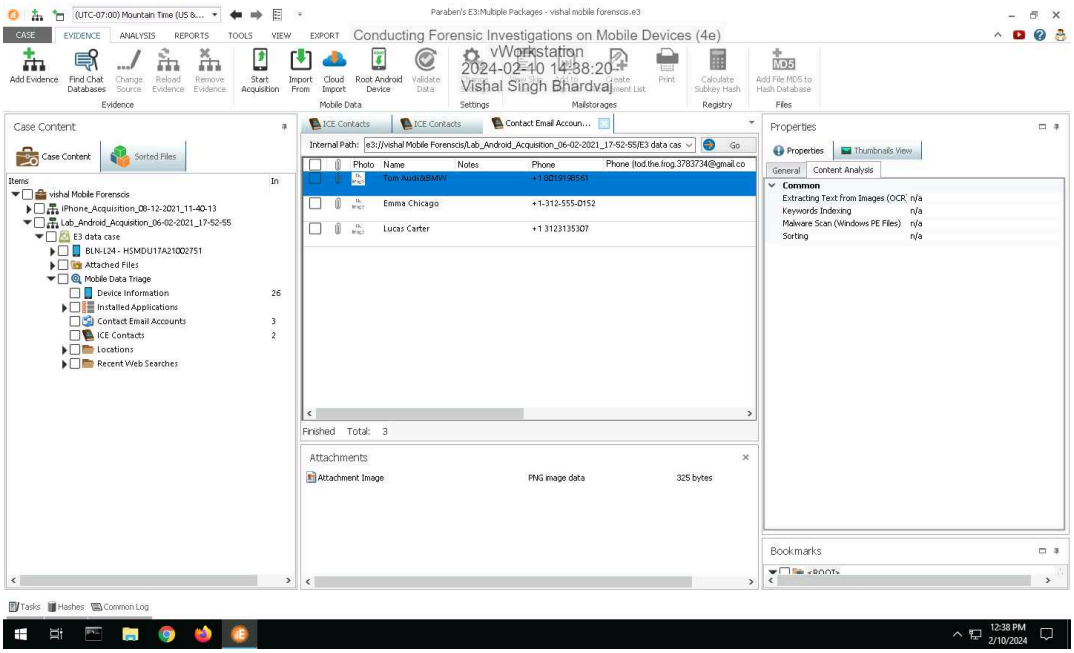
7. **Make a screen capture** showing the **Device Information**.



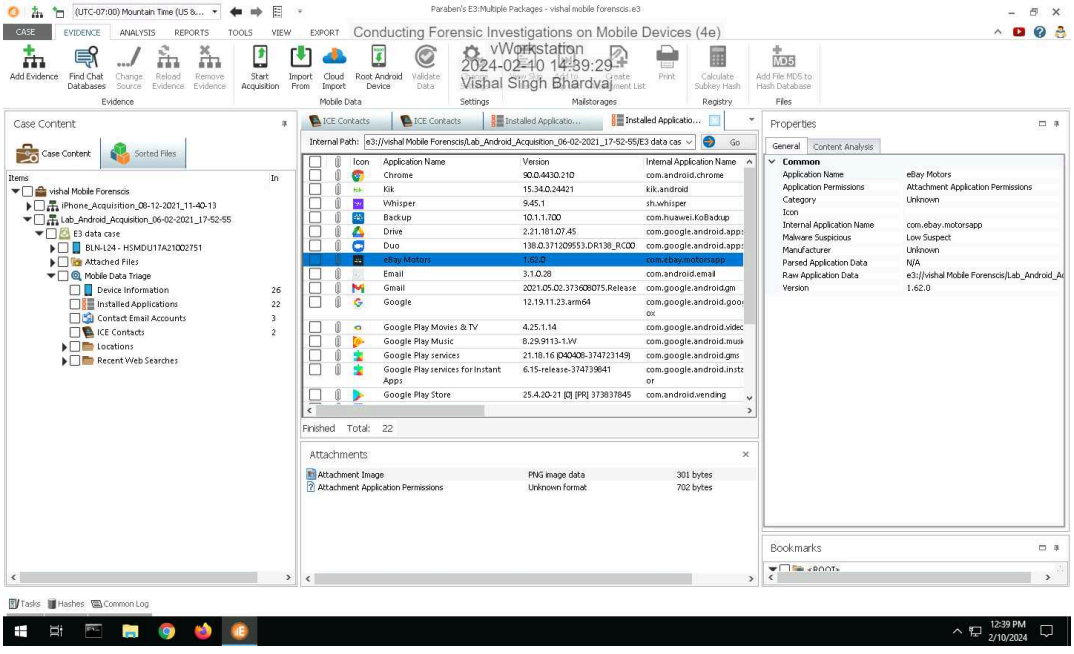
9. **Make a screen capture** showing the **ICE Contacts**.



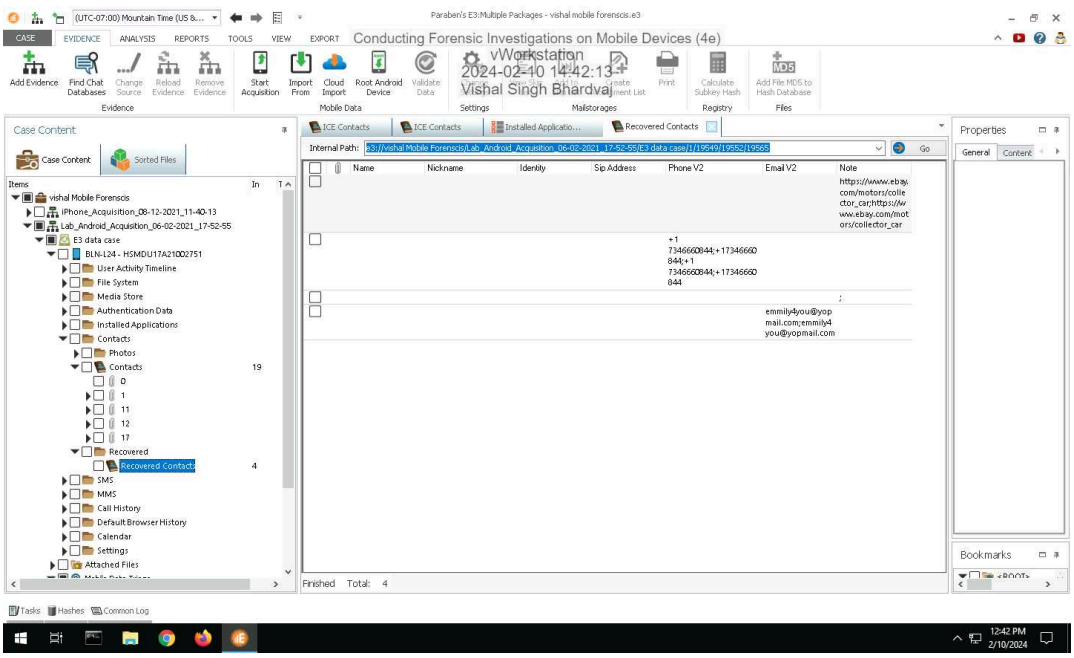
12. **Make a screen capture** showing the **Contact Email Accounts**.



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

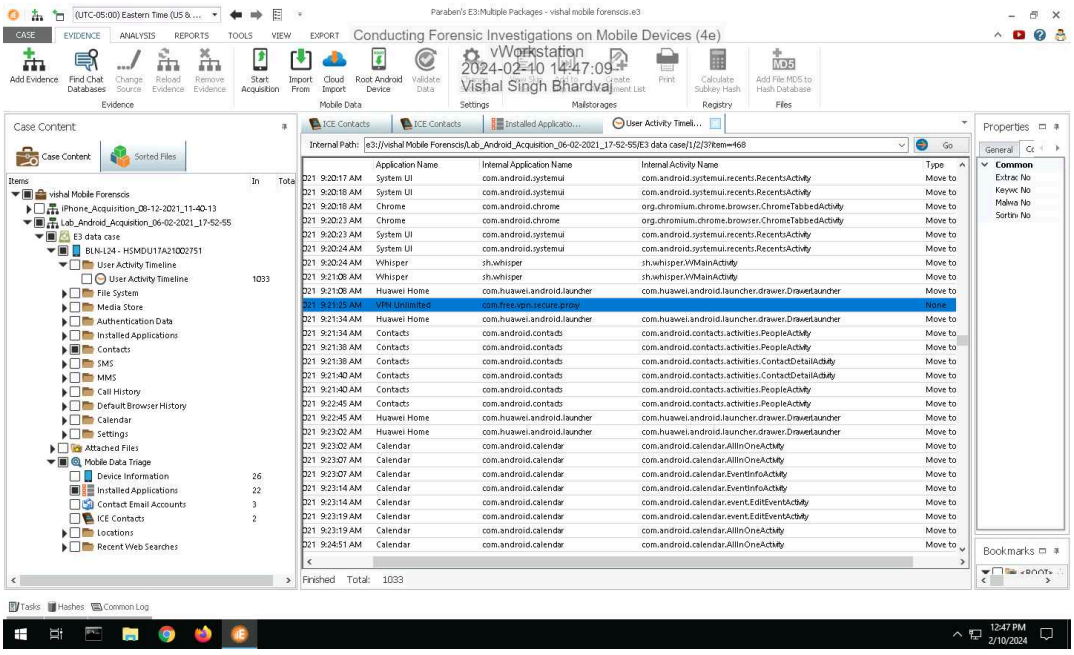


19. **Make a screen capture** showing the **recovered contact information from the Android phone**.

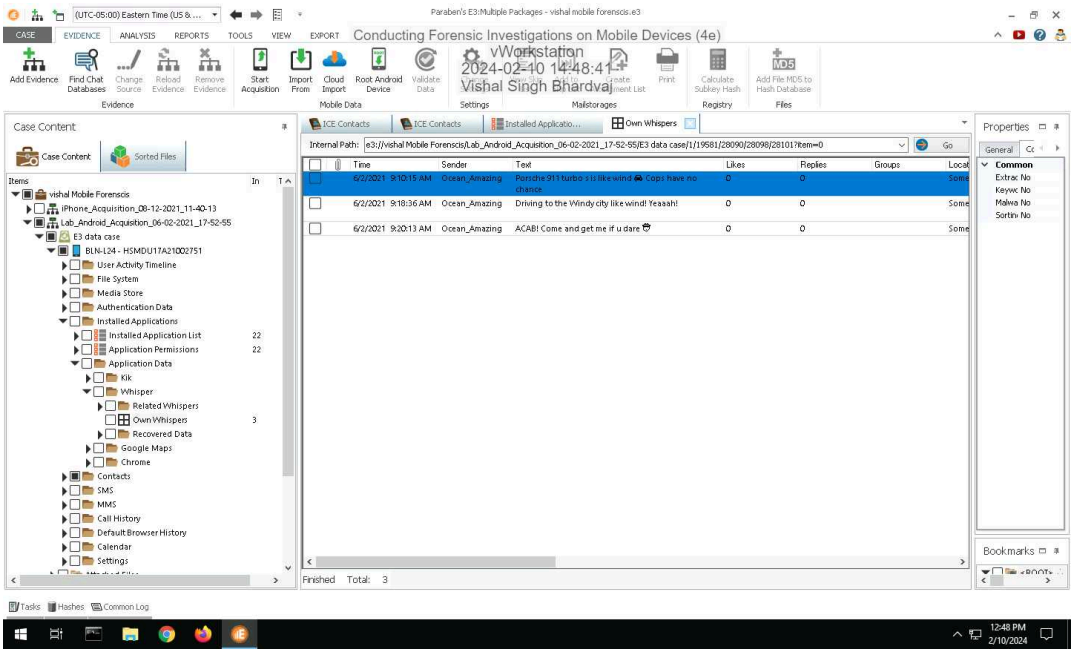


Part 2: Identify Forensic Evidence in Android Application Data

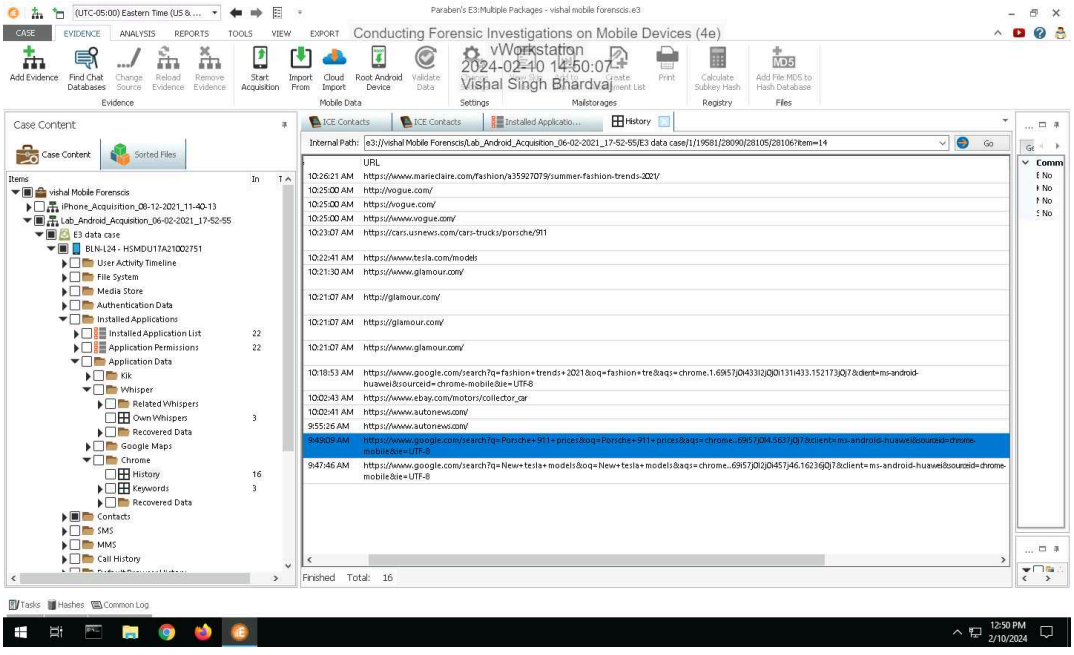
4. **Make a screen capture** showing the **User Activity Timeline between 9:17:47 AM and 9:24:51 AM on 6/2/2021**.



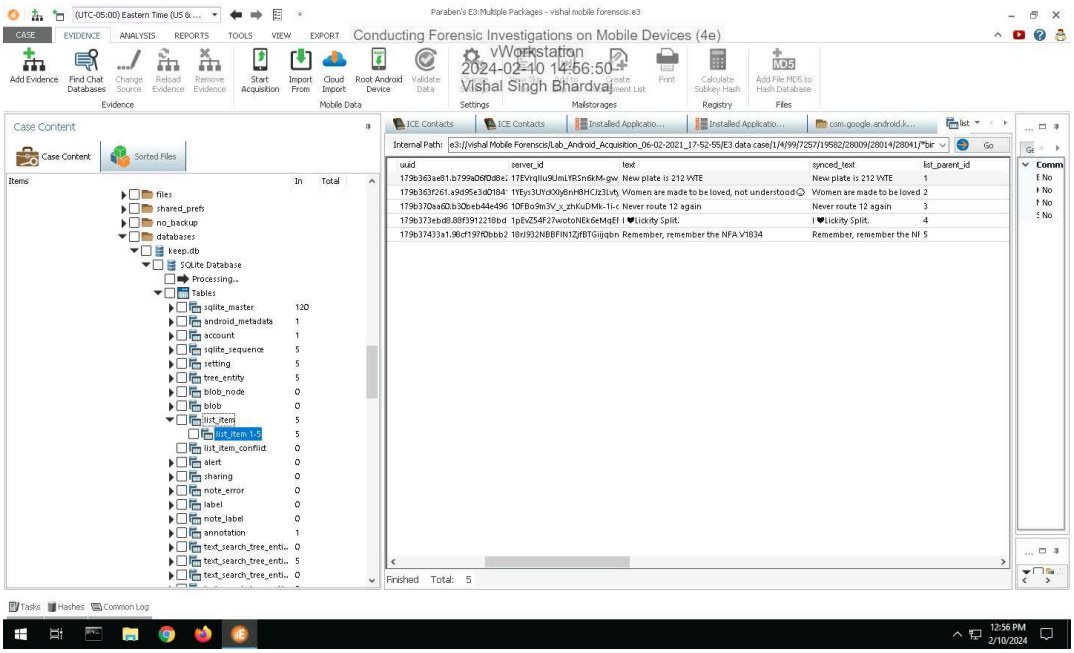
7. **Make a screen capture** showing the **contents of the Own Whispers grid**.



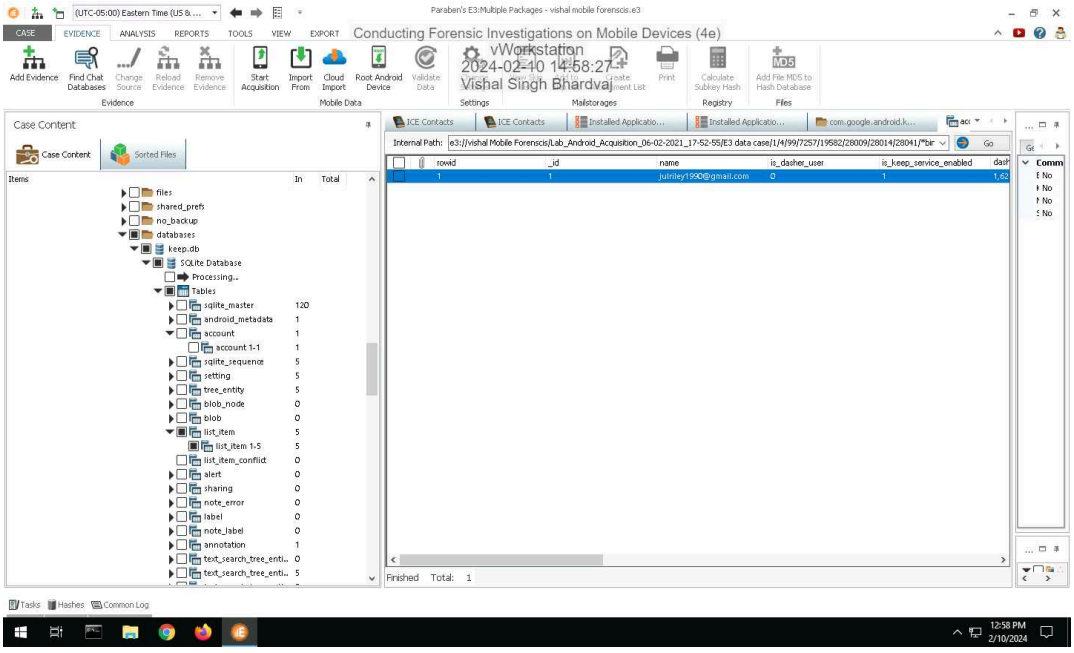
10. **Make a screen capture** showing the **contents of the History grid**.



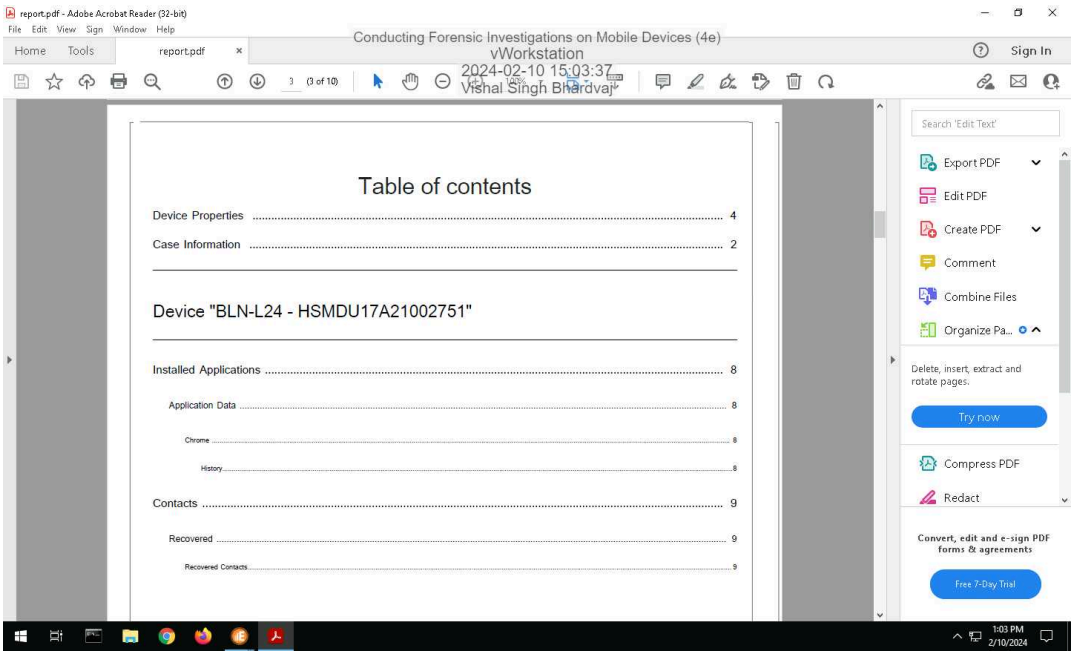
17. **Make a screen capture** showing the **contents of the list_item 1-5 table**.



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.

Overview/Case Summary:

Introduce the case, including the request for forensic examination and the involvement of the examiner.

Include details such as the date, contact person, reason for examination, and any initial actions taken.

Forensic Acquisition & Exam Preparation:

Describe the procedures followed for imaging the digital evidence, including documentation of identifiers, use of sterile storage media, and connection to a write blocker.

Detail the steps taken to ensure the integrity of the evidence, such as verifying the write blocker and conducting forensic wipes.

Findings and Report (Forensic Analysis):

Outline the forensic analysis conducted using various licensed tools, such as EnCase, SIFT, Internet Evidence Finder, RegRipper, and

Microsoft Excel.

Present the findings discovered during analysis, such as recovered data from specific sectors, internet history, screenshots, and other relevant artifacts.

Conclusion:

Summarize the findings based on the forensic evidence presented in the report.

Emphasize the importance of a thorough examination and reporting factual evidence objectively.

Best Practices:

Maintain a detailed chain of custody throughout the handling of digital evidence.

Document all steps taken during forensic acquisition and examination, including photographs of the evidence.

Verify the integrity of forensic images using hash values (e.g., MD5, SHA-1).

Use licensed and reputable forensic tools for analysis.

Ensure clarity and organization in presenting findings, using screenshots, hyperlinks, or other visual aids when necessary.

Conduct a comprehensive analysis, leaving no potential evidence unexplored.

Maintain objectivity and professionalism in reporting findings, regardless of their implications.

Part 2: Draft a Forensic Report

Case Summary

Overview/ Case Summary

The Madison Police Department is investigating an organized car theft operation involving two suspects known by the codenames Bonnie and Clyde. The suspects' smartphones, an iOS (iPhone) and an Android device, were confiscated as part of the investigation. The digital forensics unit is tasked with analyzing the data retrieved from these devices to identify evidence related to the car thefts.

Images analyzed are following-

Lab_Android_Acquisition_06-02-2021_17-52-55

iPhone_Acquisition 08-12-2021_11-40-13

iPhone Acquisition 08-12-2021_11-55-18

Findings and Analysis

Findings and Analysis:

Upon conducting a forensic examination of the digital devices, including an iPhone and an Android (Huawei) device, the following significant findings were discovered:

iPhone:

Device Identification: The iPhone is identified as an iPhone Series 12, running on product version 14.4, with the serial number F4GZNMQ4N739.

Ownership: The iPhone is linked to an individual named Clyde based on contact information and ownership details of Android phone.

Stolen Cars Evidence: Analysis of the iPhone's file sorting revealed evidence of 11 car pictures along with their corresponding license plate numbers.

Suspicious Activities: Car images with their license plat number gives strong indication of involvement of suspect into car theft cases.

Android (Huawei) Device:

Device Identification: The Android device is identified with the serial number HSMDU17A21002751 and is equipped with dual SIM capabilities.

Ownership: Contrary to the iPhone, the Android device is associated with an individual named Bonnie, as indicated by the contact list.

Stolen Cars Notes: The Android device contains notes listing stolen cars and their associated license plate numbers, including the change of a license plate number from 657 BEE to 7CAJ533.

Suspicious Applications: The Android device had installed applications such as Whisper, an anonymous chatting app, and eBay Motor, which is commonly used for selling goods including potentially stolen cars.

User Activity Timeline: Analysis of the user activity timeline between 9:17:47 and 9:24:51 on 06/02/2021 revealed suspicious activities including the use of VPN Unlimited and the Whisper app, indicating attempts to conceal online activities.

Owner's Identity: Data from the Android device's note-taking application indicates that the phone owner's email is julriley1990@gmail.com, suggesting a likely real name of Jul Riley.

Conclusion

Conclusion

the forensic analysis of the seized iPhone and Android devices has revealed significant evidence implicating suspects codenamed Bonnie and Clyde in an organized car theft operation. The iPhone, linked to Clyde, contained photos of stolen cars with corresponding license plate numbers, while the Android device, associated with Bonnie, contained notes listing stolen cars and suspicious applications indicating potential involvement in selling stolen goods. Suspicious activities such as the use of VPNs and anonymous chatting apps further support these findings. The analysis has provided crucial evidence for the ongoing investigation and strengthens the case against the suspects.