

# Conducting Forensic Investigations on Mobile Devices (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

Student:

Loksharan Saravanan

Email:

loksharan.soc@gmail.com

Time on Task:

2 hours, 12 minutes

Progress:

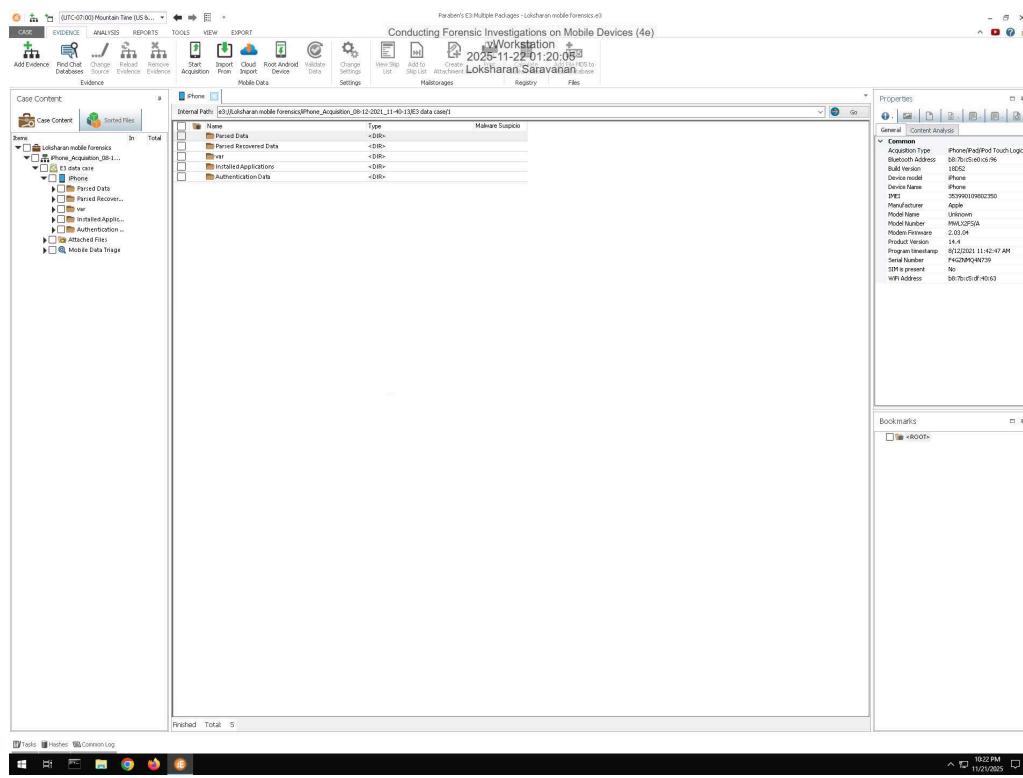
100%

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.



# Conducting Forensic Investigations on Mobile Devices (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

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

The screenshot shows the Paraben's E3 Multiple Podager interface for conducting forensic investigations on mobile devices. The main window displays the 'Contacts' grid under the 'Evidence' tab. The grid lists 14 contacts with their first name, last name, job title, and middle name. The properties panel on the right shows general details for the selected contact, 'Pretty K'. The left sidebar shows the case content tree, which includes various evidence types like Photos, Videos, and Text messages. The bottom status bar indicates the date and time as 2025-11-22 01:20:57.

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

The screenshot shows the Paraben's E3 Multiple Podager interface for conducting forensic investigations on mobile devices. The main window displays the 'Calendar' grid under the 'Evidence' tab. The grid lists numerous calendar events with details such as start date, end date, and description. The properties panel on the right shows general details for the selected event. The left sidebar shows the case content tree, including various evidence types like Photos, Videos, and Text messages. The bottom status bar indicates the date and time as 2025-11-22 01:21:14.

# Conducting Forensic Investigations on Mobile Devices (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

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

The screenshot shows the Paraben's E3 Multiple Platforms software interface. The main window title is "Conducting Forensic Investigations on Mobile Devices (4e)". The top menu bar includes CASE, EVIDENCE, ANALYSIS, REPORTS, TOOLS, VIEW, and EXPORT. The evidence pane on the left shows a tree structure of evidence items, including "Loksharan mobile forensics" and "Phone\_Acquisition\_08-12-2021\_11-40-3". The central grid is titled "Messages" and displays a list of messages with columns: ConversationId, Correspondent Id, Type, Sender Number, Recipient Number, Text, Subject, Date Sent, Date Received, and Date Read. The grid contains 4 rows of data. The right pane is titled "Properties" and shows tabs for General and Content Analysis. The bottom status bar indicates "10:27 PM" and "11/21/2023".

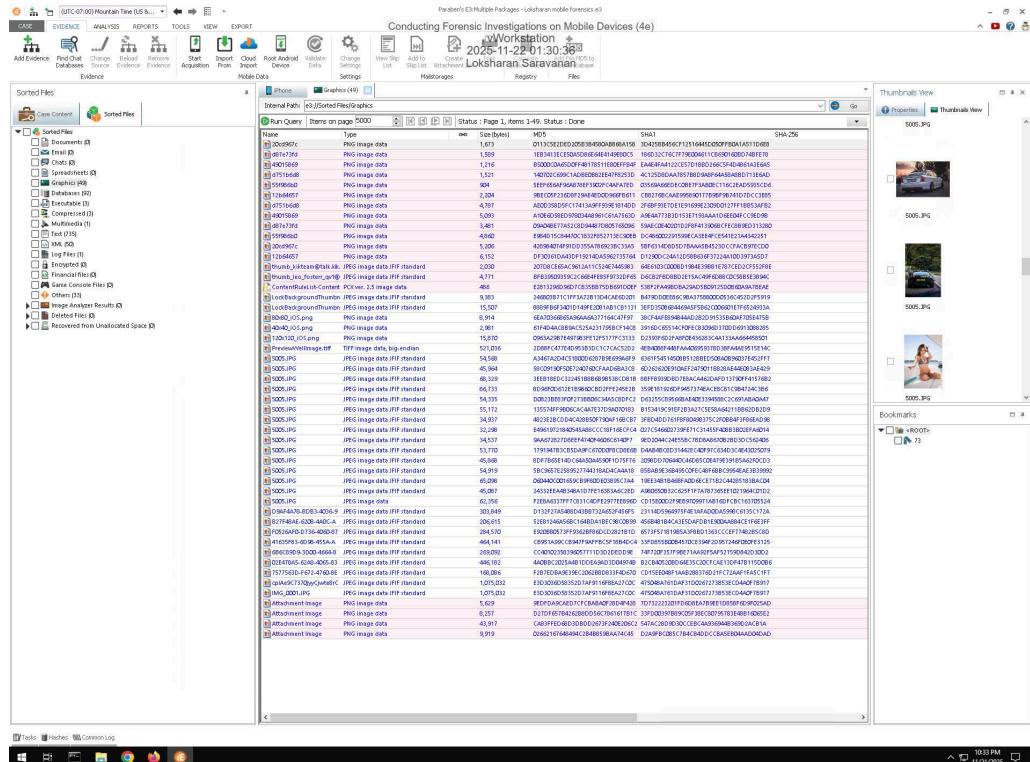
## 24. Make a screen capture showing the contents of the Notes grid.

The screenshot shows the Paraben's E3 Multiple Platforms software interface. The main window title is "Conducting Forensic Investigations on Mobile Devices (4e)". The top menu bar includes CASE, EVIDENCE, ANALYSIS, REPORTS, TOOLS, VIEW, and EXPORT. The evidence pane on the left shows a tree structure of evidence items, including "Loksharan mobile forensics" and "Phone\_Acquisition\_08-12-2021\_11-40-3". The central grid is titled "Notes" and displays a list of notes with columns: Date Created, Note ID, Title, Text, URL, Latitude, Longitude, Description, and Short. The grid contains 17 rows of data. The right pane is titled "Properties" and shows tabs for General and Content Analysis. The bottom status bar indicates "10:38 PM" and "11/21/2023".

# Conducting Forensic Investigations on Mobile Devices (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

## 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.

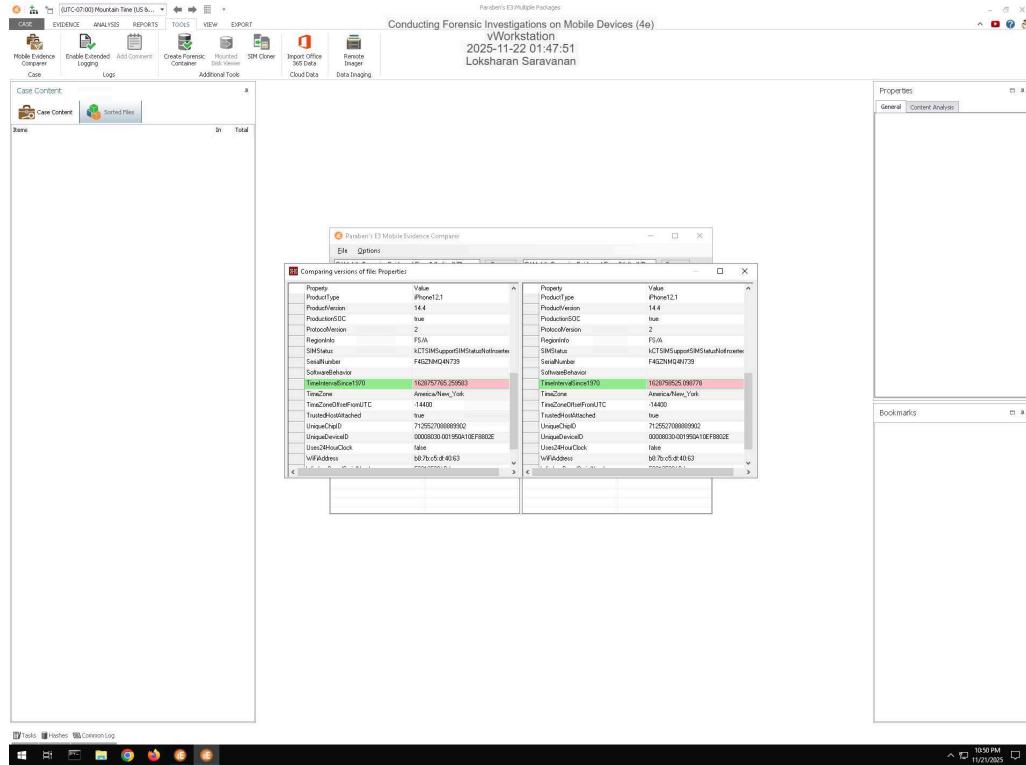
The screenshot shows the Adobe Acrobat Reader interface. The main window displays a 'Table of contents' page titled 'Device Properties'. Below it, a 'What's new' section highlights 'Simplified Design' with a note: 'Acrobat Reader has a redesigned layout that simplifies viewing, sharing, and collaborating on documents.' A 'Take the tour' button is present. The status bar at the bottom indicates the date and time as 18:35 PM 11/21/2025.

# Conducting Forensic Investigations on Mobile Devices (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

## Part 2: Compare iOS Data Cases

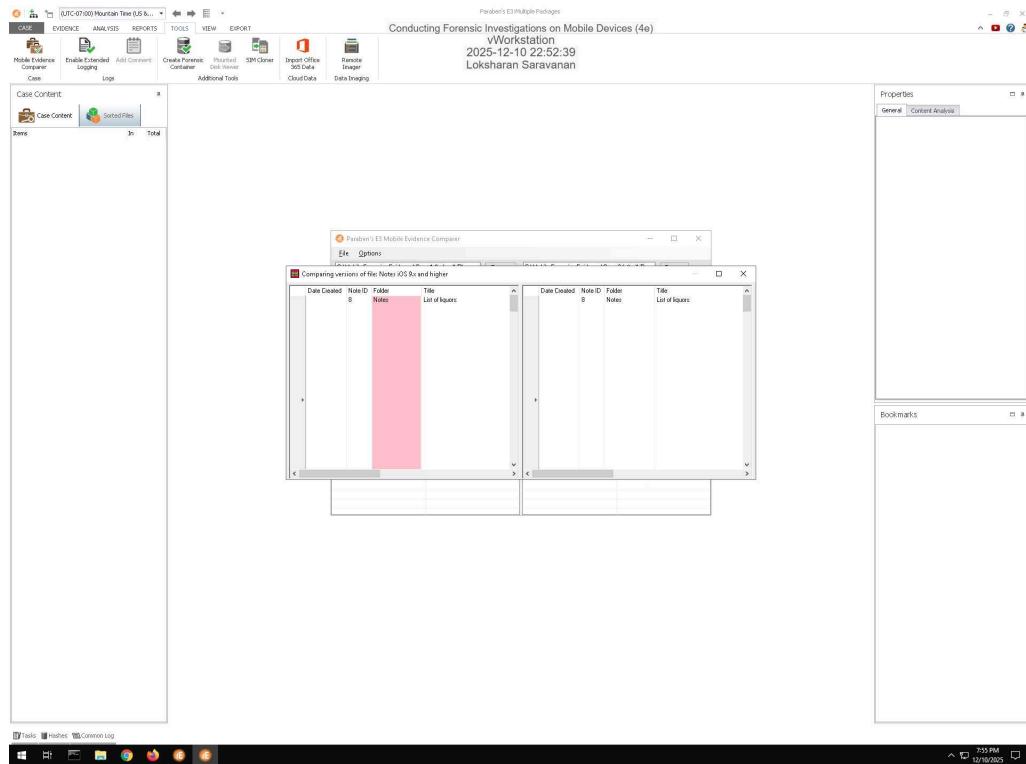
10. Make a screen capture showing the difference in data case properties.



# Conducting Forensic Investigations on Mobile Devices (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

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



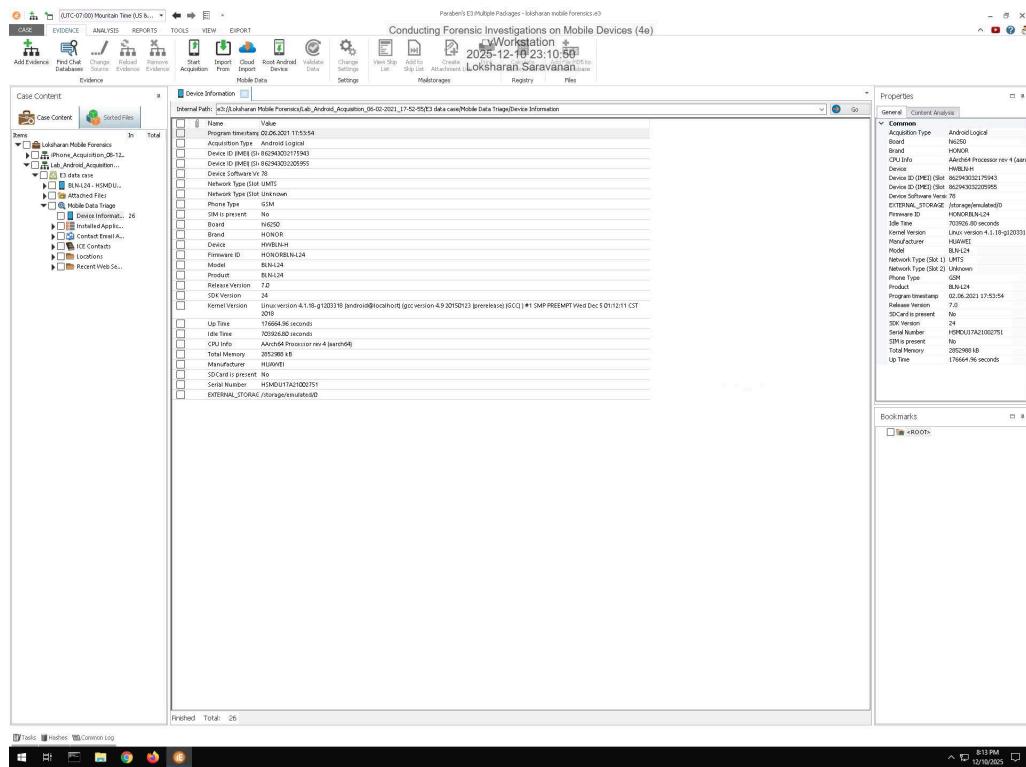
# Conducting Forensic Investigations on Mobile Devices (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

## Section 2: Applied Learning

### Part 1: Identify Forensic Evidence in Android User Data

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



# Conducting Forensic Investigations on Mobile Devices (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

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

The screenshot shows the EnCase Forensic interface with the title bar "Conducting Forensic Investigations on Mobile Devices (4e)". The main pane displays a list of "ICE Contacts" under the "Mobile Data" tab. There are two entries:

Photo	Name	Notes	Phone	Phone (Ind the log)	Email	Group	Account	Time Contacted
	ICE Daddy-Daddy		+18179990054			My Contacts (belong to: julytey190@gmail.com)	julytey190@gmail.com	n

The left sidebar shows the "Case Content" tree, including sections like "Data Sources", "Logs", "Media", and "Mobile Data". The bottom status bar shows "Tools", "Help", "Common Log", the date "12/10/2023", and the time "8:11 PM".

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

The screenshot shows the EnCase Forensic interface with the title bar "Conducting Forensic Investigations on Mobile Devices (4e)". The main pane displays a list of "Contact Email Accounts" under the "Mobile Data" tab. There are three entries:

Photo	Name	Notes	Phone	Phone (Ind the log)	Email	Group	Account	Time Contacted
	Tom Austin/MV		+18019100561		tommy.tony@ymail.com	My Contacts (belong to: julytey190@gmail.com)	julytey190@gmail.com	n
	Emma Chicago		+13125550152		emmytayu@ymail.com	My Contacts (belong to: julytey190@gmail.com)	julytey190@gmail.com	n
	Lucas Carter		+13121235307		27203d1qquwh200@openvdip.com	My Contacts (belong to: julytey190@gmail.com)	julytey190@gmail.com	n

The left sidebar shows the "Case Content" tree, including sections like "Data Sources", "Logs", "Media", and "Mobile Data". The bottom status bar shows "Tools", "Help", "Common Log", the date "12/10/2023", and the time "8:14 PM".

# Conducting Forensic Investigations on Mobile Devices (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

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

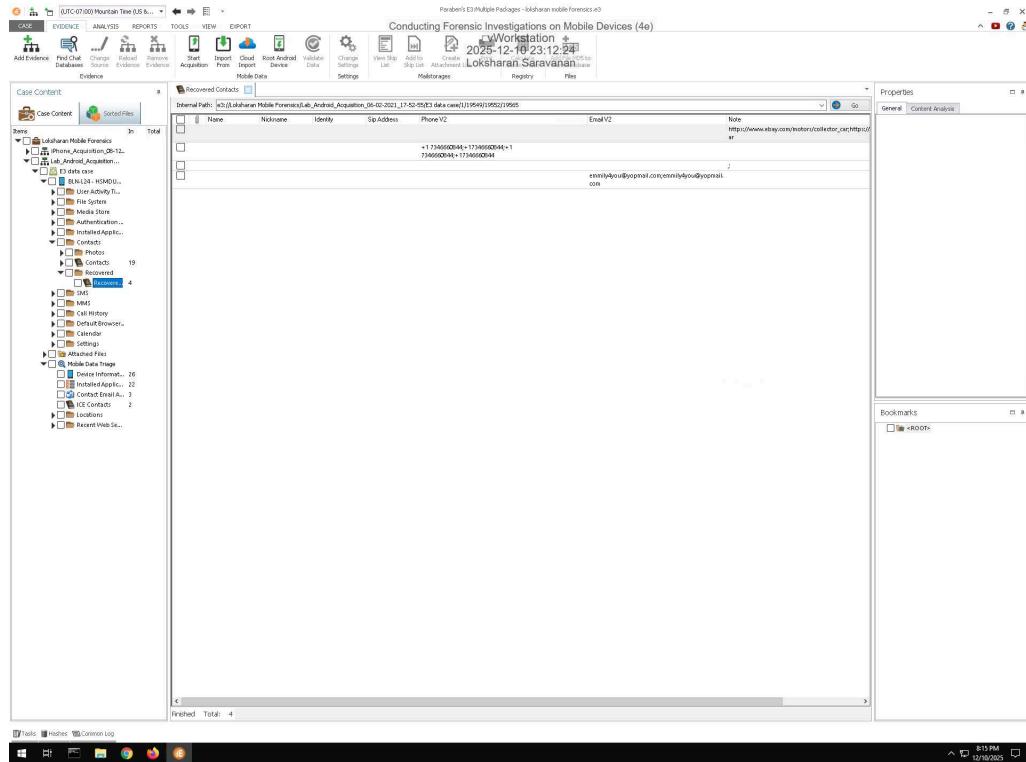
The screenshot shows the 'Installed Applications' section of the Paraben's E3 mobile forensics interface. The left sidebar displays the case structure, including 'Case Content' and 'Sorted Filter'. The main pane lists installed applications with columns for Internal Application Name, Category, Manufacturer, Parent Application ID, and Run Application URL. The list includes various Google apps like Chrome, Play Store, and Gmail, along with system apps like System UI and System Server. A properties panel on the right shows general and content analysis details. The bottom status bar indicates the task is finished with a total of 22 items.

Internal Application Name	Category	Manufacturer	Parent Application ID	Run Application URL
com.chrome	Communication	Google Inc.	N/A	/data/u/0/com.google.android.chrome
KIK	Kit-interactive	Kit-interactive	N/A	/data/u/0/com.kik.kikandroid
sh whisper	Communication	Whisperfect, Inc	N/A	/data/u/0/com.whisper
Backup	Unknown	Unknown	N/A	/data/u/0/com.google.android.backup
Call Log	Unknown	Unknown	N/A	/data/u/0/com.google.android.apps.dialer
Duo	Unknown	Unknown	N/A	/data/u/0/com.google.android.apps.duo
Play Protect	Unknown	Unknown	N/A	/data/u/0/com.google.android.apps.guardian
Play Store	Unknown	Unknown	N/A	/data/u/0/com.google.android.apps.gplaystore
Gmail	Communication	Google Inc.	N/A	/data/u/0/com.google.android.apps.gmail
Google	Unknown	Unknown	N/A	/data/u/0/com.google.android.apps.googleplus
Google Play Movies & TV	Unknown	Unknown	N/A	/data/u/0/com.google.android.videos
Google Play Music	Unknown	Unknown	N/A	/data/u/0/com.google.android.music
Google Play Services	Unknown	Unknown	N/A	/data/u/0/com.google.android.gms
Google Play services for instant Apps	Unknown	Unknown	N/A	/data/u/0/com.google.android.instantapps.supplier
Keep Notes	Unknown	Unknown	N/A	/data/u/0/com.google.android.keep
Maps	Navigation	Google Inc.	N/A	/data/u/0/com.google.android.maps
Photos	Unknown	Unknown	N/A	/data/u/0/com.google.android.apps.photos
Verizon	Unknown	Unknown	N/A	/data/u/0/com.verizon.freestyle
YouTube	Unknown	Unknown	N/A	/data/u/0/com.google.android.youtube

# Conducting Forensic Investigations on Mobile Devices (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

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



## Part 2: Identify Forensic Evidence in Android Application Data

# Conducting Forensic Investigations on Mobile Devices (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

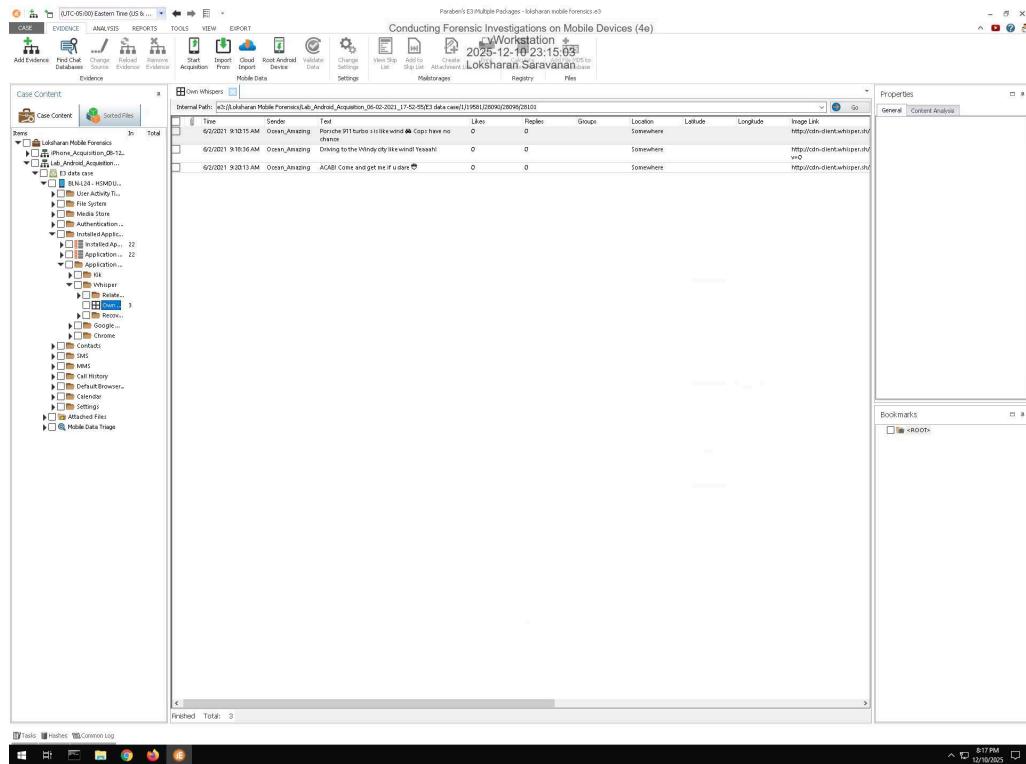
## 4. Make a screen capture showing the User Activity Timeline between 9:17:47 AM and 9:24:51 AM on 6/2/2021.

The screenshot shows the EnCase Forensic interface with the title "Conducting Forensic Investigations on Mobile Devices (4e)". The main window displays the "User Activity Timeline" for an Android device acquisition made on 06-02-2021 at 17:52:53. The timeline lists numerous events from 9:13:05 AM to 9:46:16 AM, categorized by application and activity type (Move to foreground, Move to background). The left sidebar shows the "Case Content" tree, which includes sections like "Android Forensics", "Android Acquisition", and "File System". The bottom status bar indicates the date and time as 6/2/2021 8:18 PM.

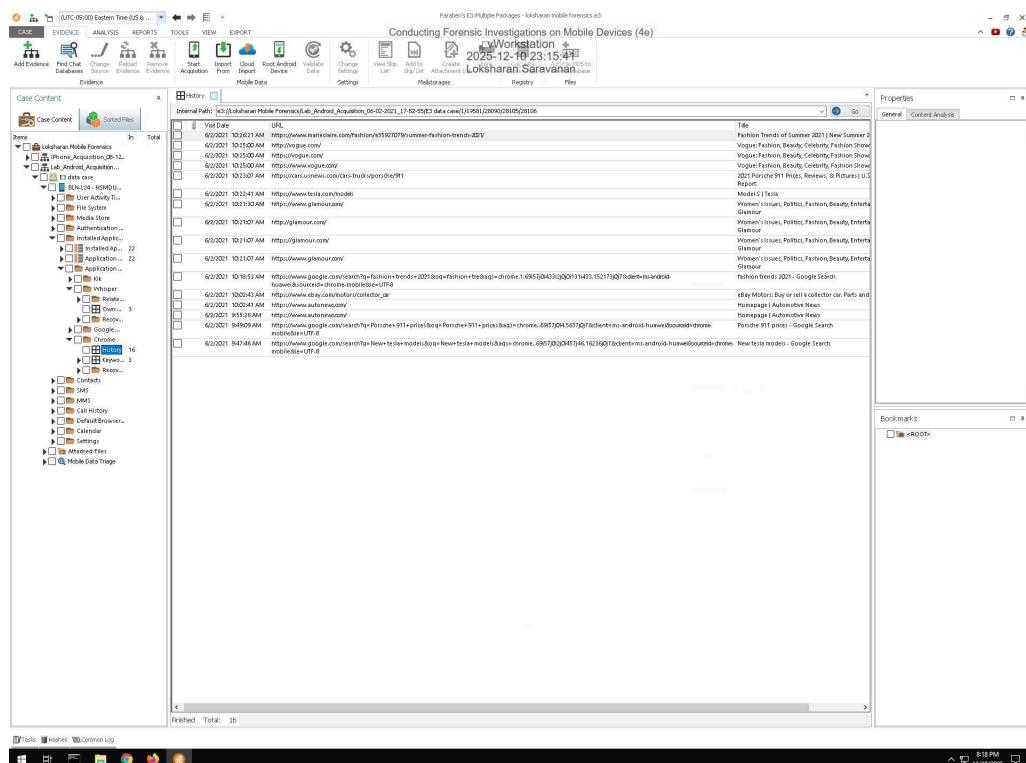
## Conducting Forensic Investigations on Mobile Devices (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

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.



# Conducting Forensic Investigations on Mobile Devices (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

## 17. Make a screen capture showing the contents of the list\_item 1-5 table.

The screenshot shows the EnCase Forensic software interface. The main window displays a table titled "list\_item 1-5" with the following data:

row_id	id	account_id	uuid	device_id	parent_id	order_id
2	2	1	179f10f21a995a1d2ff	10f80a00000000000000000000000000	1	2
3	3	1	179f10f21a995a1d2ff	10f80a00000000000000000000000000	1	3
4	4	1	179f10f21a995a1d2ff	10f80a00000000000000000000000000	1	4
5	5	1	179f10f21a995a1d2ff	10f80a00000000000000000000000000	1	5

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

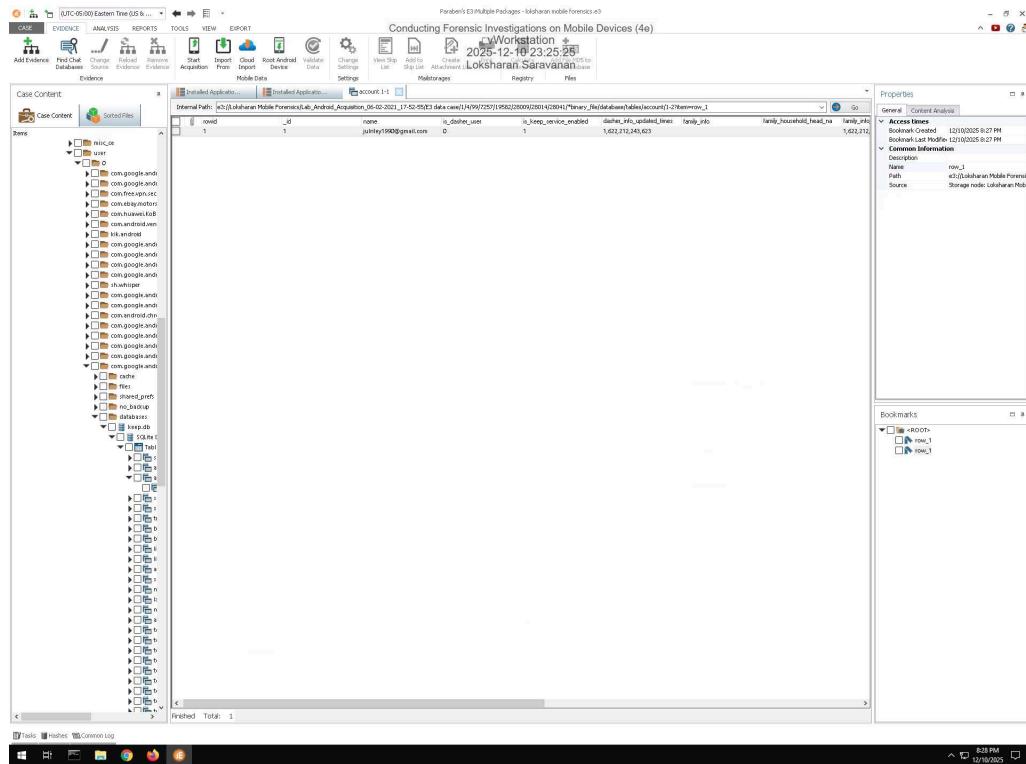
The screenshot shows the EnCase Forensic software interface. The main window displays a table titled "account 1-1" with the following data:

row_id	id	name	u_dasher_use	is_keep_service_enabled	dashr_xbo_updated_time	ready_pdo	family_household_head_ma	family_id
1	1	junitry190@gmail.com	0	1	162,212,245,623	1	1,622,1	1,622,1

## Conducting Forensic Investigations on Mobile Devices (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

**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.