

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

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

**Student:**

Jose Cruz

Email:

jose.cruz2@udc.edu

## Time on Task:

8 hours, 34 minutes

## Progress:

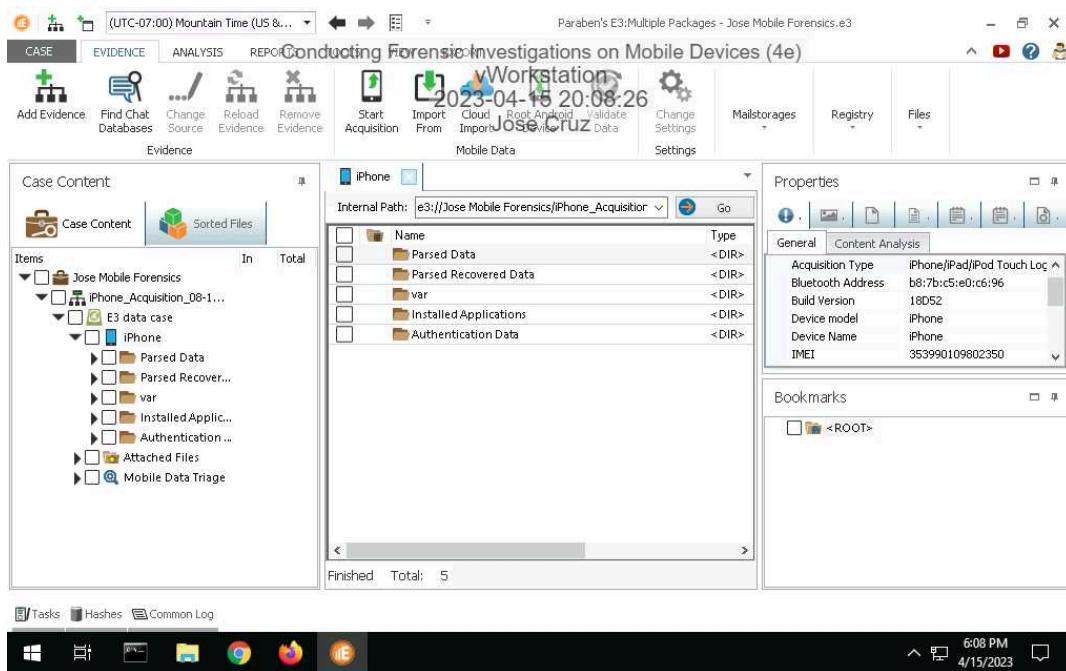
100%

Report Generated: Saturday, April 15, 2023 at 10:21 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:Mobile Packages software interface. The main window title is "Conducting Forensic Investigations on Mobile Devices (4e)". The top menu bar includes options like CASE, EVIDENCE, ANALYSIS, and REPORT. The central pane displays a "Mobile Data" view with a "Contacts" tab selected. The left sidebar under "Case Content" shows various data types: Case Content, Sorted Files, and a list of items including Safari History, Address Book, Calendar, Cookies, Safari Suspend, Native Application, Passwords, Call History, Notes, Contacts, Safari Bookmarks, Messages, Parsed Recovered Data, var, and Installed Application. The main content area shows a table of contacts with columns: Creation Date, Department, Display Name, and First Name. The table lists 14 entries. The right pane shows "Properties" for the selected contact and a "Bookmarks" section. The bottom status bar shows the date and time as 4/15/2023 6:10 PM.

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

The screenshot shows the Paraben's E3:Mobile Packages software interface, similar to the previous one but with a different internal path. The main window title is "Conducting Forensic Investigations on Mobile Devices (4e)". The top menu bar includes options like CASE, EVIDENCE, ANALYSIS, and REPORT. The central pane displays a "Mobile Data" view with a "Calendar" tab selected. The left sidebar under "Case Content" shows various data types: Case Content, Sorted Files, and a list of items including Safari History, Address Book, Calendar, Cookies, Safari Suspend, Native Application, Passwords, Call History, Notes, Contacts, Safari Bookmarks, Messages, Parsed Recovered Data, var, and Installed Application. The main content area shows a table of calendar events with columns: Start Timezone, Summary, and Location. The table lists 92 entries. The right pane shows "Properties" for the selected event and a "Bookmarks" section. The bottom status bar shows the date and time as 4/15/2023 6:10 PM.

# 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:Mobile Packages interface. The main window title is "Conducting Forensic Investigations on Mobile Devices (4e)". The top menu bar includes options like CASE, EVIDENCE, ANALYSIS, and REPORT. The central pane displays a "Messages" grid with the following data:

Text	Subject	Date Sent	Date Received
Miss u ☺		5/26/2021 7:34:38 AM	
Have u seen new Porsche Panamera? ☺		5/26/2021 7:35:56 AM	
The 🚗 is in Windy City ☺		5/26/2021 7:38:28 AM	
☺ While big sis is away, Ava and Adam can play ☺		5/26/2021 7:40:01 AM	

The left sidebar shows "Case Content" with various evidence items listed under "Items". The right sidebar shows "Properties" and "Bookmarks". The bottom status bar indicates the date and time as 4/15/2023 and 6:13 PM.

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

The screenshot shows the Paraben's E3:Mobile Packages interface. The main window title is "Conducting Forensic Investigations on Mobile Devices (4e)". The central pane displays a "Notes" grid with the following data:

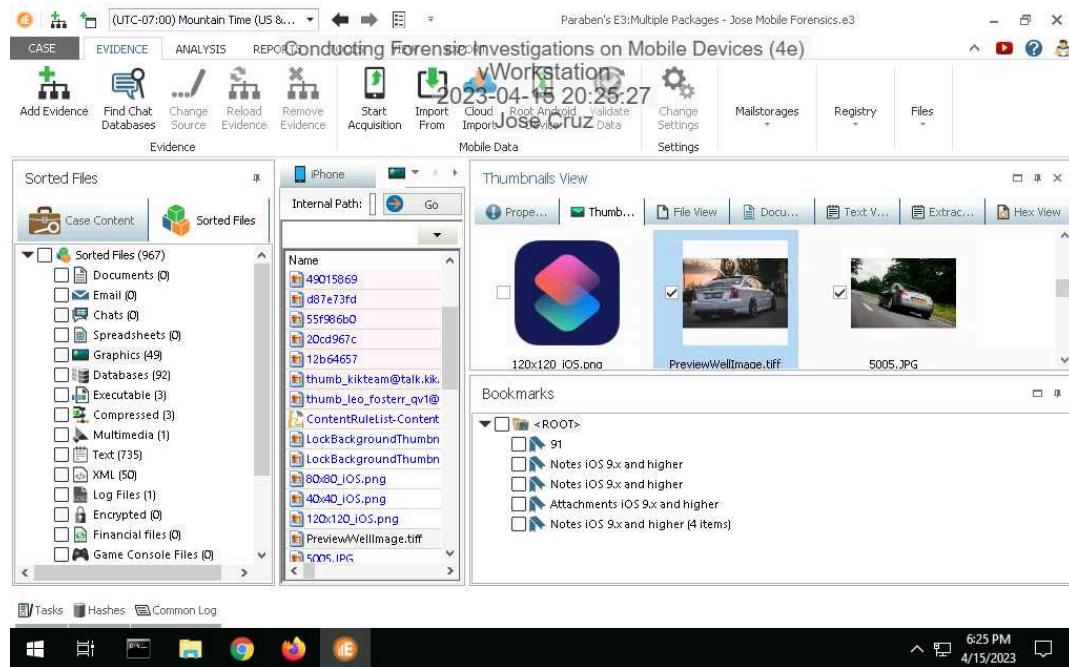
Name	Type	Malware
Notes iOS 9.x and higher	<DIR>	
Attached Location Data	<DIR>	
Attachments iOS 9.x and higher	<DIR>	
Recovered Notes iOS 9.x and higher	<DIR>	

The left sidebar shows "Case Content" with various evidence items listed under "Items". The right sidebar shows "Properties" and "Bookmarks". The bottom status bar indicates the date and time as 4/15/2023 and 6:20 PM.

# 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 Adobe Acrobat Reader DC open to a PDF document titled 'report.pdf'. The top menu bar includes File, Edit, View, Sign, Window, and Help. The toolbar includes Home, Tools, and a search bar. The main content area displays the 'Table of contents' for 'Conducting Forensic Investigations on Mobile Devices (4e)'. The table of contents lists sections such as Device Properties, Case Information, Device "iPhone", Parsed Data, Calendar, Notes, and Notes iOS 9.x and higher. On the right side, there is a sidebar with various document management tools like Export PDF, Edit PDF, Create PDF, Comment, Combine Files, Organize Pages, Compress PDF, Redact, and Protect. The bottom taskbar shows standard Windows application icons.

## Part 2: Compare iOS Data Cases

# Conducting Forensic Investigations on Mobile Devices (4e)

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

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

The screenshot shows the Paraben's E3 software interface. The title bar indicates the case name is "Conducting Forensic Investigations on Mobile Devices (4e)" and the date is "2023-04-15 20:41:40". The main window is titled "Comparing versions of file: Properties" and shows two columns of properties for "Case" and "Sorted F". The properties listed include ProductType (iPhone12,1), ProductVersion (14.4), ProductionSOC (true), ProtocolVersion (2), RegionInfo (FS/A), SIMStatus (kCTSISupportSIMStatusNotInserted), SerialNumber (F4GZNMQ4N739), SoftwareBehavior, TimeIntervalSince1970 (1628757765.259583), TimeZone (America/New\_York), TimeZoneOffsetFromUTC (-14400), TrustedHostAttached (true), UniqueChipID (7125527088889902), UniqueDeviceID (00008030-001950A10EF8802E), Uses24HourClock (false), and WiFiAddress (b8:7b:c5:df:40:63). The "Sorted F" column has a single entry for TimeIntervalSince1970 (1628758525.098778). The bottom status bar shows the date and time as "4/15/2023 6:41 PM".

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

The screenshot shows the Paraben's E3 software interface. The title bar indicates the case name is "Conducting Forensic Investigations on Mobile Devices (4e)" and the date is "2023-04-15 20:47:17". The main window is titled "Comparing versions of file: Notes iOS 9.x and higher" and shows two columns of notes for "Case" and "Sorted F". The notes listed include: Note ID 9, Title "Play Fewer Hands And Play Them Aggressively", Folder "Notes"; Note ID 10, Title "NFA V1834 known to police!", Folder "Notes"; Note ID 11, Title "New Note", Folder "Recently Deleted"; Note ID 13, Title "657 BEE change to 7CAJ533", Folder "Notes"; Note ID 14, Title "JCG 2794 change to 212 WTE", Folder "Recently Deleted"; Note ID 15, Title "Meet \*\*\* in Green bay", Folder "Notes"; Note ID 16, Title "549 BDX change to 143 4084\$", Folder "Recently Deleted"; Note ID 17, Title "RockfoldJanesville-Madison", Folder "Notes". The "Sorted F" column has an additional note with Note ID 11, Title "New Note", Folder "Recently Deleted". The bottom status bar shows the date and time as "4/15/2023 6:47 PM".

# 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.

The screenshot shows the Paraben's E3 forensic tool interface. The main window displays 'Device Information' for an Android device. Key details shown include:

Name	Value
Firmware ID	HONORBLN-L24
Model	BLN-L24
Product	BLN-L24
Release Version	7.0
SDK Version	24
Kernel Version	Linux version 4.1.18-g1203318 (android@localhost) 2018
Up Time	176664.96 seconds
Idle Time	703926.80 seconds
CPU Info	AArch64 Processor rev 4 (aarch64)
Total Memory	2852988 kB
Manufacturer	HUAWEI
SDcard is present	No
Serial Number	HSMDU17A21002751
EXTERNAL_STORAG	/storage/emulated/0

The 'Properties' panel on the right shows the manufacturer is HUAWEI. The 'Bookmarks' panel contains several entries related to iOS 9.x and higher. The bottom status bar shows the date as 4/15/2023 and the time as 6:58 PM.

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

The screenshot shows the Paraben's E3 forensic tool interface. The main window displays 'ICE Contacts' for an Android device. Two contacts are listed:

Photo	Name	Notes	Phone	Phone
	ICE Clyde		+1 8186504729	
	ICE Daddy Dear		+1 8179936654	

The 'Properties' panel on the right shows the contacts belong to 'My Contacts'. The 'Attachments' panel shows an 'Attachment Image' file. The bottom status bar shows the date as 4/15/2023 and the time as 7:00 PM.

# Conducting Forensic Investigations on Mobile Devices (4e)

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

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

The screenshot shows the Paraben's E3 forensic interface. The main window displays a list of contact email accounts under the heading "Contact Email Accounts". The list includes three entries: Tom Audi&BMW, Emma Chicago, and Lucas Carter, each with a photo, name, notes, and phone number. The left sidebar shows a tree view of the case content, including sections like Case Content, Evidence, and Mobile Data Triage, with "Installed Applications" selected. The top bar shows the internal path as "e3://Jose Mobile Forensics/Lab\_Android\_Acquisition\_0". The bottom status bar indicates the date and time as "4/15/2023 7:04 PM".

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

The screenshot shows the Paraben's E3 forensic interface. The main window displays a list of installed applications under the heading "Installed Applications". The list includes various apps like Chrome, Kik, Whisper, Backup, Drive, Duo, eBay Motors, Gmail, Google, Google Play Movies & TV, Google Play Music, Google Play services, and Google Play services for Instant, each with an icon, application name, and version. The left sidebar shows a tree view of the case content, including sections like Case Content, Evidence, and Mobile Data Triage, with "Installed Applications" selected. The top bar shows the internal path as "e3://Jose Mobile Forensics/Lab\_Android\_Acquisition\_0". The bottom status bar indicates the date and time as "4/15/2023 7:06 PM".

# 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.

The screenshot shows the Paraben's E3:Mobile Forensics software interface. The main window title is "Conducting Forensic Investigations on Mobile Devices (4e)". The top menu bar includes CASE, EVIDENCE, ANALYSIS, and REPORT. The evidence tab is selected. The timeline at the top right shows "2023-04-15 21:12:00". The central pane displays "Recovered Contacts" with the internal path "e3://Jose Mobile Forensics/Lab\_Android\_Acquisition\_0/Evidence/Recovered/Recovered Contacts". The table lists four contacts:

Sip Address	Phone V2	Email V2	Note
+1 7346660844	+17346660844	emmy4you@yopmail.com	https://www.ebay.com/motors/collector_car; https://www.ebay.com/motors/collector_car
+1 7346660844	+17346660844	emmy4you@yopmail.com	
+1 7346660844	+17346660844	emmy4you@yopmail.com	

The left sidebar shows the "Case Content" tree, including "E3 data case", "BLN-L24 - HSMODU17A21Q02751", "User Activity Timeline", "File System", "Media Store", "Authentication Data", "Installed Applications", "Contacts" (with sub-options Photos, Contacts, Recovered), "Recovered", "SMS", "MMS", and "Call History". The bottom status bar shows "7:11 PM 4/15/2023".

## 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.

The screenshot shows the Paraben's E3:Mobile Forensics software interface. The main window title is "Conducting Forensic Investigations on Mobile Devices (4e)". The top menu bar includes CASE, EVIDENCE, ANALYSIS, and REPORT. The evidence tab is selected. The timeline at the top right shows "2023-04-15 21:19:29". The central pane displays "User Activity Timeline" with the internal path "e3://Jose Mobile Forensics/Lab\_Android\_Acquisition\_06-02-2021\_17-52-55/E3 data case". The table lists user activity entries:

Time	Application Name	Internal Application Name	Internal
6/2/2021 9:17:47 AM	Whisper	sh.whisper	sh.whi
6/2/2021 9:18:53 AM	Whisper	sh.whisper	sh.whi
6/2/2021 9:18:53 AM	System UI	com.android.systemui	com.a
6/2/2021 9:18:55 AM	System UI	com.android.systemui	com.a
6/2/2021 9:18:55 AM	Chrome	com.android.chrome	org.cr
6/2/2021 9:19:13 AM	Chrome	com.android.chrome	org.cr
6/2/2021 9:19:14 AM	System UI	com.android.systemui	com.a
6/2/2021 9:19:14 AM	Whisper	sh.whisper	sh.whi
6/2/2021 9:20:17 AM	Whisper	sh.whisper	sh.whi
6/2/2021 9:20:17 AM	System UI	com.android.systemui	com.a
6/2/2021 9:20:18 AM	System UI	com.android.systemui	com.a
6/2/2021 9:20:18 AM	Chrome	com.android.chrome	org.cr
6/2/2021 9:20:23 AM	Chrome	com.android.chrome	org.cr
6/2/2021 9:20:23 AM	System UI	com.android.systemui	com.a

The left sidebar shows the "Case Content" tree, including "E3 data case", "BLN-L24 - HSMODU17A21Q02751", "User Activity Timeline" (with sub-option "User Activity Timeline"), "File System", "Media Store", "Authentication Data", "Installed Applications", "Contacts" (with sub-options Photos, Contacts, Recovered), "Recovered", "SMS", and "MMS". The bottom status bar shows "7:19 PM 4/15/2023".

# 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.

The screenshot shows the Paraben's E3 mobile forensic interface. The main window title is "Conducting Forensic Investigations on Mobile Devices (4e)". The top menu bar includes CASE, EVIDENCE, ANALYSIS, and REPORT. The evidence tab is selected, showing a timeline of events under "Mobile Data". A specific section titled "Own Whispers" is highlighted. The left sidebar lists various data categories like User Activity Timeline, File System, Media Store, Authentication Data, Installed Applications, Application Data, and Google Maps. The "History" category is also visible. The central pane displays a grid of messages from a user named "Ocean\_Amazing". The grid columns include Time, Sender, Text, and Likes. The first message is: "6/2/2021 9:10:15 AM Ocean\_Amazing Porsche 911 turbo s is like wind. Cops have no chance". The second message is: "6/2/2021 9:18:36 AM Ocean\_Amazing Driving to the Windy city like wind! Yeaash!". The third message is: "6/2/2021 9:20:13 AM Ocean\_Amazing ACAB! Come and get me if u dare". The bottom status bar shows the date and time as 4/15/2023 7:23 PM.

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

The screenshot shows the Paraben's E3 mobile forensic interface, similar to the previous one but with a different focus. The main window title is "Conducting Forensic Investigations on Mobile Devices (4e)". The top menu bar includes CASE, EVIDENCE, ANALYSIS, and REPORT. The evidence tab is selected, showing a timeline of events under "Mobile Data". A specific section titled "History" is highlighted. The left sidebar lists various data categories like Installed Applications, Application Permissions, Application Data, and Google Maps. The "History" category is selected. The central pane displays a grid of browser history entries. The grid columns include Visit Date and URL. The entries show multiple visits to websites such as marieclaire.com, vogue.com, tesla.com, glamour.com, and google.com. The bottom status bar shows the date and time as 4/15/2023 7:25 PM.

# 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 Paraben's E3 forensic tool interface. The main window displays the 'Evidence' tab with the internal path 'e3://Jose Mobile Forensics/Lab\_Android\_Acquisition\_06-02-2021\_17-52-55/E3 data c'. A table titled 'list\_item 1-5' is open, showing the following data:

uuid	server_id	text	synced_text
179b363ae81.b799a060d8e1	17EVrglllu9UmlYRSn&M-gw	New plate is 212-WTB	
179b363f261.a9d95e3d0184	1YEys3UYcdXly0nH8HCJz3lvb	Women are made to be loved Women are made to b	
179b370aa0b30beb44e496	10FB9m3V_x_zhKuDMk-1-c	Never route 12 again	Never route 12 again
179b373ebd8.88f3912210bd	1pEvZ54F27wotoNEk6eMqEf	I ❤️ Lickity Split.	I ❤️ Lickity Split.
179b37433a1.9cf197f0bb2	18rj932NBBFIN1ZjfBTGijqbn	Remember, remember the NF Remember, rememb	

The left sidebar shows the SQLite Database structure, including tables like sqlite\_master, android\_metadata, account, sqlite\_sequence, setting, tree\_entity, blob\_node, blob, and list\_item. The list\_item table has 5 rows. The bottom status bar indicates '7:32 PM 4/15/2023'.

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

The screenshot shows the Paraben's E3 forensic tool interface. The main window displays the 'Evidence' tab with the internal path 'e3://Jose Mobile Forensics/Lab\_Android\_Acquisition\_06-02-2021\_17-52-55/E3 data c'. A table titled 'account 1-1' is open, showing the following data:

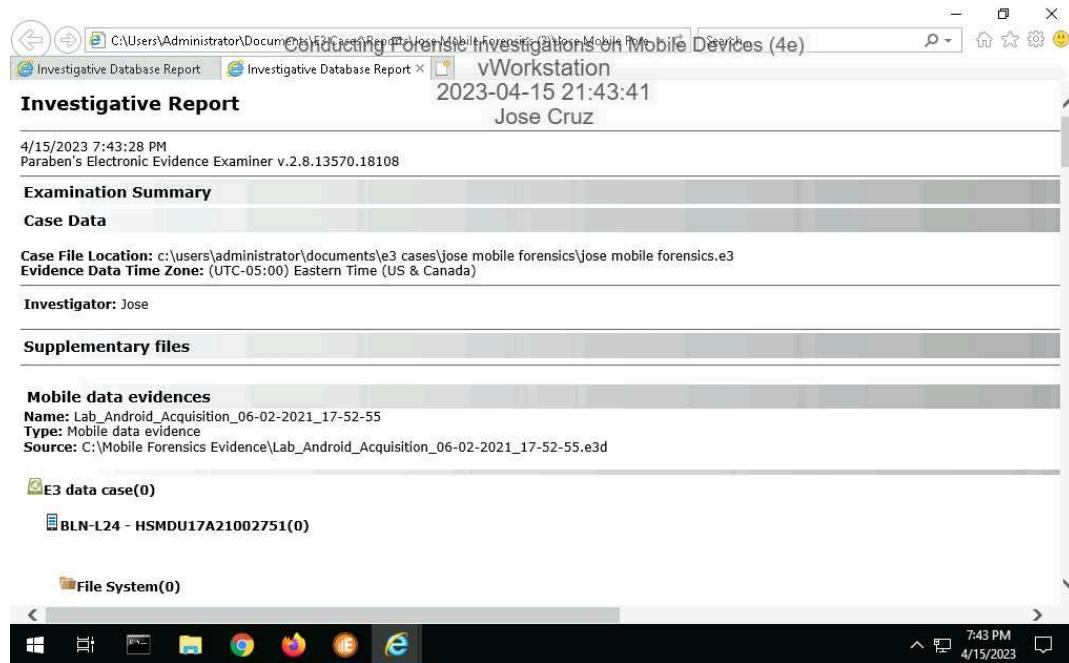
rowid	_id	name	is_dasher_user
1	1	julmiley1990@gmail.com	0

The left sidebar shows the SQLite Database structure, including tables like sqlite\_master, android\_metadata, account, sqlite\_sequence, setting, tree\_entity, blob\_node, blob, and list\_item. The account table has 1 row. The right panel shows the 'Common' properties for the account row, including '\_id' (1), 'das 1,622;', 'fam', 'fam', 'Fam 1,622;', 'fam 0', and 'is\_c 0'. The bottom status bar indicates '7:35 PM 4/15/2023'.

# 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.

1. On April 15, 2023, a report has come to a conclusion that Beverly has been working with a Russian criminal organization. Company contacted my office in regard to imaging an iPhone and android that had been recovered. Company has requested a forensic examination to see if Beverly has been involved in any crime. Company boss is requesting documents, is requesting a full forensic examination, report for possible criminal charges and civil litigation.

### Findings and Report (Forensic Analysis)

**After completing the forensic acquisition of the suspicious criminal act of hr. I began analyzing the forensic image of the iPhone and Android cellphone with a Forensic Tool. I used the following tool for forensic analysis, which are licensed to this examiner:**

Electronic Evidence Examiner

### Conclusion:

I have attached a pdf file with multiple findings that incriminate Beverly on criminal act from selling stolen cars and substances.

## **Part 2: Draft a Forensic Report**

### **Case Summary**

From examining the iPhone and Android phone there is concrete evidence that Beverly has been working with the Russian mafia doing criminal acts

### **Findings and Analysis**

The finding is from contacts, emails, deleted content and much more that Beverly has a big timeline doing crime.

### **Conclusion**

My final conclusion is that Beverly has been doing a stream of crime and the evidence is present in a PDF file. In addition, we can proceed to arrest her with all the data collected.