

## Introduction

Mobile devices are the most common computing platform in the world. They are also the most commonly used device for accessing the Internet. As we know from personal use, smartphones provide a variety of different features and allow users to perform almost every task previously done with computers. The capabilities provided by smartphones expand often, therefore the process for investigating mobile devices is constantly evolving.

Smartphones can (and do) substitute for desktop computers in almost every way because they are portable, always connected, and more convenient to use for most applications. As a result, smartphones carry immensely valuable information in many forensic investigations. They often provide recent chats, call logs, location data, pictures, and much more. In most cases, they carry more personal information than a traditional PC, which is why smartphones and other mobile devices often become the focus of modern forensic investigations.

In this lab, you will use Paraben's E3 to analyze data from iOS and Android smartphones.

## Lab Overview

**SECTION 1** of this lab has two parts, which should be completed in the order specified.

1. In the first part of the lab, you will analyze an iOS data case, document evidence, and generate an investigative report using Paraben's E3.
  
2. In the second part of the lab, you will use E3's Mobile Evidence Comparer to compare two iOS data cases generated from the same device.

**SECTION 2** of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods. You will continue your investigation and analyze an Android data case.

Finally, you will explore the virtual environment on your own in **SECTION 3** of this lab to answer a set of questions and challenges that allow you to use the skills you learned in the lab to conduct independent, unguided work - similar to what you will encounter in a real-world situation.

## Learning Objectives

Upon completing this lab, you will be able to:

1. Identify evidence within iOS data cases.
2. Identify evidence within Android data cases.
3. Compare different data cases from the same mobile device.
4. Document evidence and generate a formal investigative report.
5. Draft a Case Summary and Conclusion as part of a formal investigative report.

## Topology

This lab contains the following virtual machines. Please refer to the network topology diagram below.

- vWorkstation (Windows: Server 2019)



## Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- Paraben's E3

## Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

### SECTION 1

1. Lab Report file, including screen captures of the following:

- Contents of the Properties pane
- Contents of the Contacts grid
- Contents of the Calendar grid
- Contents of the Messages grid
- Contents of the Notes grid
- At least three car pictures in the Thumbnail View
- Table of contents in the investigative report
- Difference in data case properties
- Additional note in the newer data case

2. Any additional information as directed by the lab:

- None

### SECTION 2

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

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

---

1. Lab Report file, including screen captures of the following:

- Device Information
- ICE Contacts
- Contact Email Accounts
- Installed Applications
- Recovered contact information from the Android phone
- User Activity Timeline between 9:17:47 AM and 9:24:51 AM on 6/2/2021
- Contents of the Own Whispers grid
- Contents of the History grid
- Contents of the list\_item 1-5 table
- Keep Notes account owner
- Investigative Report's Table of Contents

2. Any additional information as directed by the lab:

- None

## **SECTION 3**

1. Lab Report file, including screen captures of the following:

- None

2. Any additional information as directed by the lab:

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

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

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

---

- Case Summary
- Findings and Analysis
- Conclusion

## Section 1: Hands-On Demonstration

**Note:** In this section of the lab, you will follow a step-by-step walk-through of the objectives for this lab to produce the expected deliverables.

### 1. Review the Tutorial.

Frequently performed tasks, such as making screen captures and downloading your Lab Report, are explained in the Cloud Lab Tutorial. The Cloud Lab Tutorial is available from the User menu in the upper-right corner of the Student Dashboard. You should review these tasks before starting the lab.

### 2. Proceed with Part 1.

## Part 1: Identify Forensic Evidence in an iOS Data Case

**Note:** In this lab, you will assume the role of a digital forensics specialist working with the Madison Police Department. Detectives have recently retrieved two smartphones (iOS and Android) that belong to the suspects in an organized car theft operation. The suspects refer to themselves using the codenames Bonnie and Clyde. You have been tasked with identifying evidence related to the car thefts from the confiscated smartphones.

In this part of the lab, you will analyze evidence acquired from the seized iPhone. In E3, mobile evidence is acquired through the use of development debugging calls from the E3 software to the mobile device. Drivers must be loaded for the operating system running E3 to be able to understand the device and the debugging calls that are used to create the connection. Once the connection is made, E3 will determine what level of data transfer should occur, based on the acquisition options the user has selected. Because a live acquisition is not possible in the virtual lab environment, you will use an existing E3 data case containing previously acquired iPhone data.

In the next steps, you import an E3 data case for the iPhone and review the parsed data for relevant evidence.

1. On the vWorkstation desktop, **double-click** the **Electronic Evidence Examiner** icon to open the E3 application.

# Conducting Forensic Investigations on Mobile Devices (4e)

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



E3 icon

**Note:** E3 may take several minutes to load. The E3 welcome screen opens with shortcuts to the most common activities that forensic investigators will perform within the tool.

2. At the Welcome screen, **click the Add Evidence button** to open the New Case dialog box.

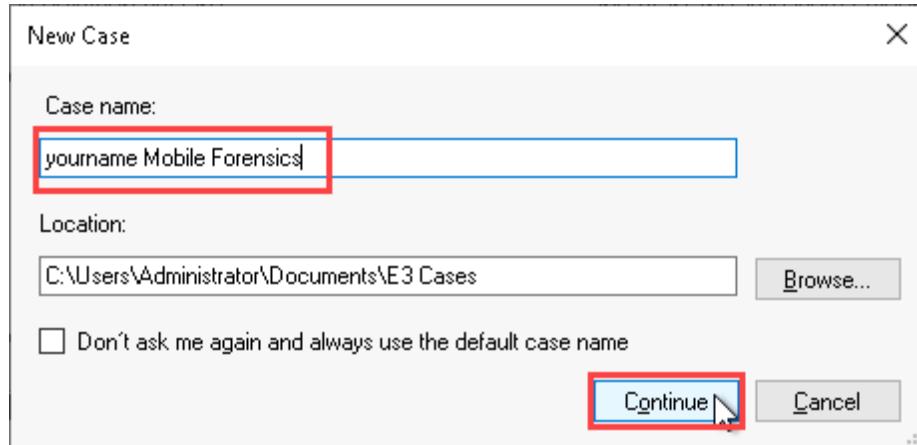


Welcome page - Add Evidence

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

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

3. In the New Case dialog box, type **yourname Mobile Forensics** in the Case name field, replacing *yourname* with your own name, then **click Continue** to create your new case file and open the Add New Evidence dialog box.

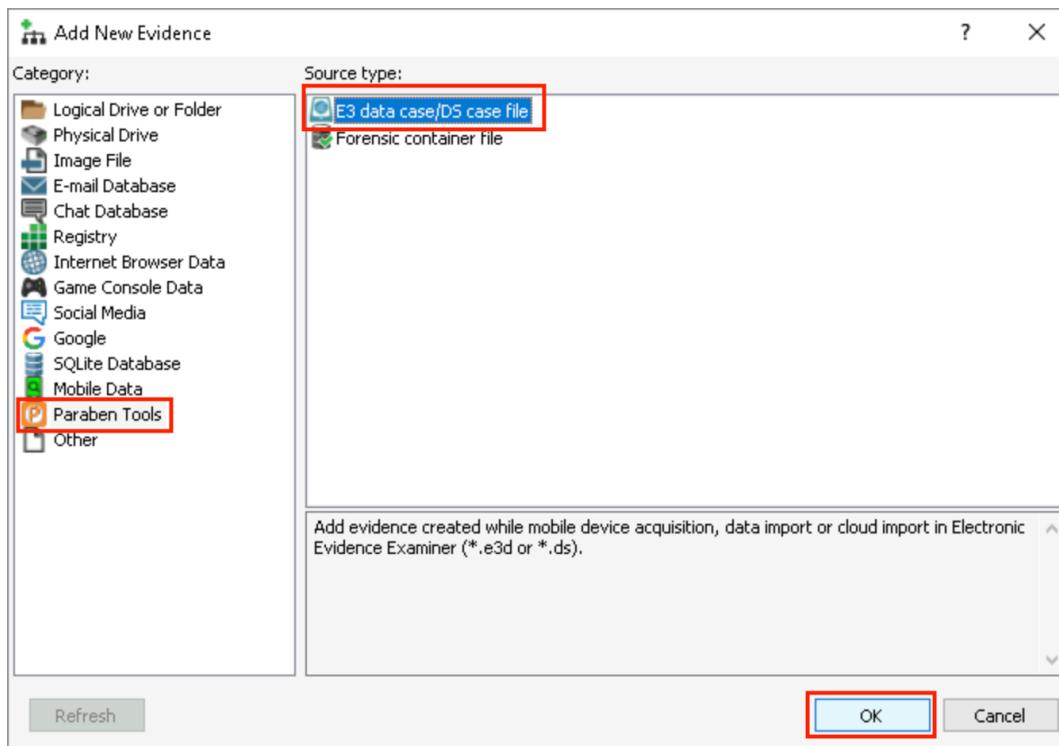


New Case

4. In the Add New Evidence dialog box, **click the Paraben Tools category**, then **select the E3 data case/DS case file source type** and **click OK** to continue.

# Conducting Forensic Investigations on Mobile Devices (4e)

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

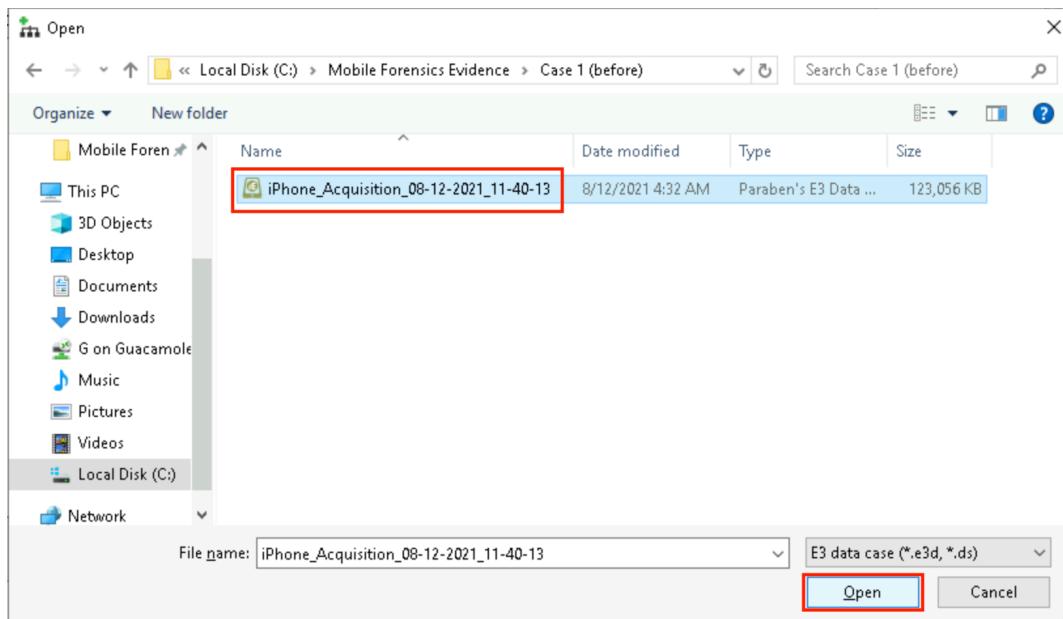


Add New Evidence

5. In the Open dialog box, navigate to C:\Mobile Forensics Evidence\Case 1 (before), then select the **iPhone\_Acquisition\_08-12-2021\_11-40-13.e3d** file and click Open to import the Paraben evidence file containing the acquired iOS data.

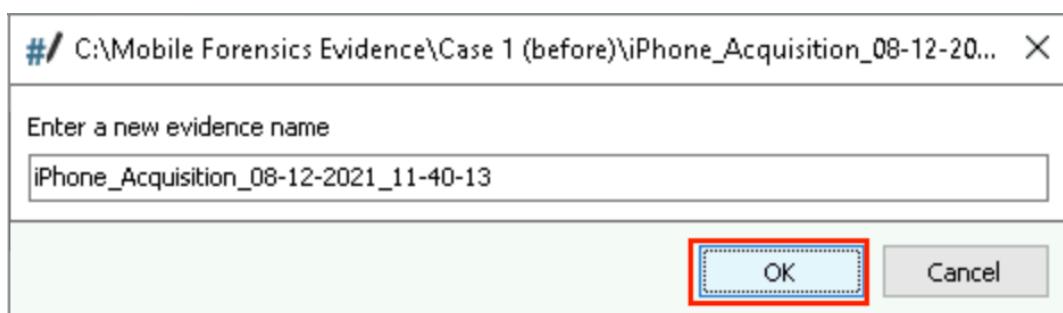
# Conducting Forensic Investigations on Mobile Devices (4e)

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



Open dialog box

- When prompted, click **OK** to accept the default name for the drive image and add the data from the drive image to your case file.



Evidence name

**Note:** The *yourname* Mobile Forensics case will appear in the Case Content pane. The Case Content pane is the primary display and navigation area for all evidence in the open case file. Within the Case Content pane's tree-view structure, you can access case nodes, evidence nodes, evidence type nodes, folder nodes, and data gridsstreams. Technically, the Case Content pane does not store the actual evidence, but provides a series of links to elements within the physical evidence.

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

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

When you select a specific node or grid within the Case Content pane, the contents of the enclosing folder or database will be displayed in the Data Viewer in the center pane. Within the Data Viewer, you can select individual files, folders, and records. Additional information about the currently selected node, grid, file, folder, or record will be displayed in the Viewers pane on the right, which provides multiple ways to view your current selection.

7. In the Case Content pane, **navigate to *yourname* Mobile Forensics / iPhone\_Acquisition\_08-12-2021\_11-40-13 / E3 data case / iPhone** to display information about the iPhone in the Properties pane on the right.

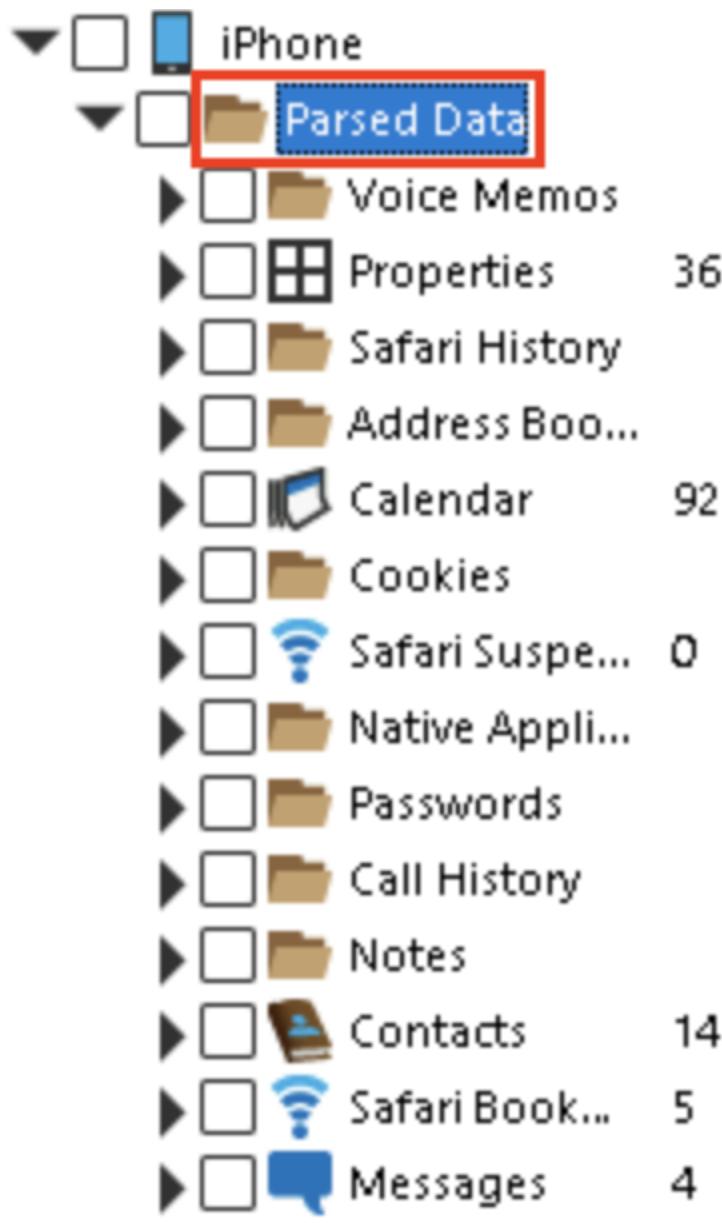
The screenshot shows the 'Case Content' pane with the following structure:

- yourname Mobile Forensics
  - iPhone\_Acquisition\_08-12-2021\_11-40-13
    - E3 data case
      - iPhone
    - Attached Files
    - Mobile Data Triage

iPhone Properties

**Note:** The Properties pane contains several details about the iPhone this data was acquired from, including Device model, Device name, Model number, Modem Firmware number, IOS Version, Serial Number, Wi-Fi address, and more. When correlating evidence from an iPhone with other sources of evidence – for example, packet captures or cloud backups – many of these details can be indispensable to building a comprehensive case.

8. Make a screen capture showing the **contents of the Properties pane**.
  
9. In the Case Content pane, **expand** the **iPhone node**, then **expand** the **Parsed Data folder**.



## Parsed Data

**Note:** Parsed Data is an artificial folder that E3 builds while acquiring data from an iOS device. During acquisition, the data is parsed to allow the raw structure of the mobile data to be displayed in a tree

---

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

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

---

form. However, most of the firmware variants associated with mobile data do not maintain a typical tree structure, so the data is broken into groups. These groups refer back to the apps associated with the data (Messages, Calendars, Contacts, etc.). Some of these apps will exist in the file system and others will be separated. The firmware and location of the app data will ultimately determine how the data is displayed.

10. In the Case Content pane, **click the Contacts folder** to open the Contacts grid in the Data Viewer.

▶	<input type="checkbox"/>	 Native Appli...
▶	<input type="checkbox"/>	 Passwords
▶	<input type="checkbox"/>	 Call History
▶	<input type="checkbox"/>	 Notes
▶	<input type="checkbox"/>	 <b>Contacts</b> 14
▶	<input type="checkbox"/>	 Safari Book... 5
▶	<input type="checkbox"/>	 Messages 4

Contacts

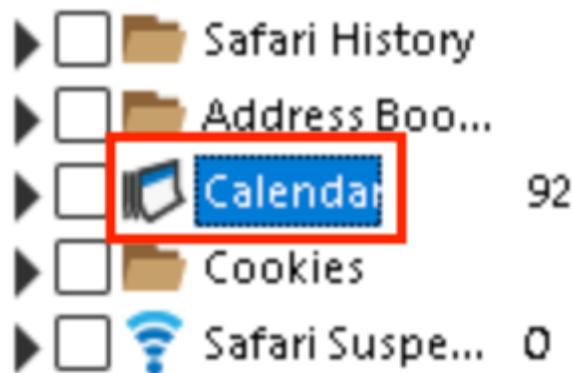
**Note:** The Contacts grid contains the full names, phone numbers, and email addresses of contacts stored in the iPhone, as well as timestamps for creation and modification dates. When dealing with iPhone evidence with tens or hundreds of contacts, you can easily sort the data in ascending or descending order by clicking the column header. You can also change the column order and remove specific columns by right-clicking any column and selecting Columns from the context menu.

11. **Make a screen capture showing the contents of the Contacts grid.**
12. In the Case Content pane, **click the Calendar folder** to open the Calendar grid in the Data Viewer.

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

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

---



### Calendar

**Note:** The Calendar grid contains the summary and description for calendar events stored in the iPhone, as well as start date, end date, timezone, location, and a value called CalendarID. The CalendarID value can be especially useful for forensic investigators, as it distinguishes system-generated events from user-generated events. Events with a CalendarID value of 9 refer to events created on the device automatically, such as holidays. Events with a CalendarID value of 14 refer to events created on the device by the user.

13. In the Calendar grid, **review the summary details** for events that were created by the device user.

**Note:** You should notice that one of the events has a car icon in the summary field. Given the context of the investigation, this could be evidence of a car theft that was planned for this day.

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

**Note:** In the next steps, you will bookmark the potentially incriminating Calendar event so you can later include it in a formal evidence report.

15. In the Data Viewer, **click the checkbox** for the **Calendar event containing potential evidence** to select it.

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

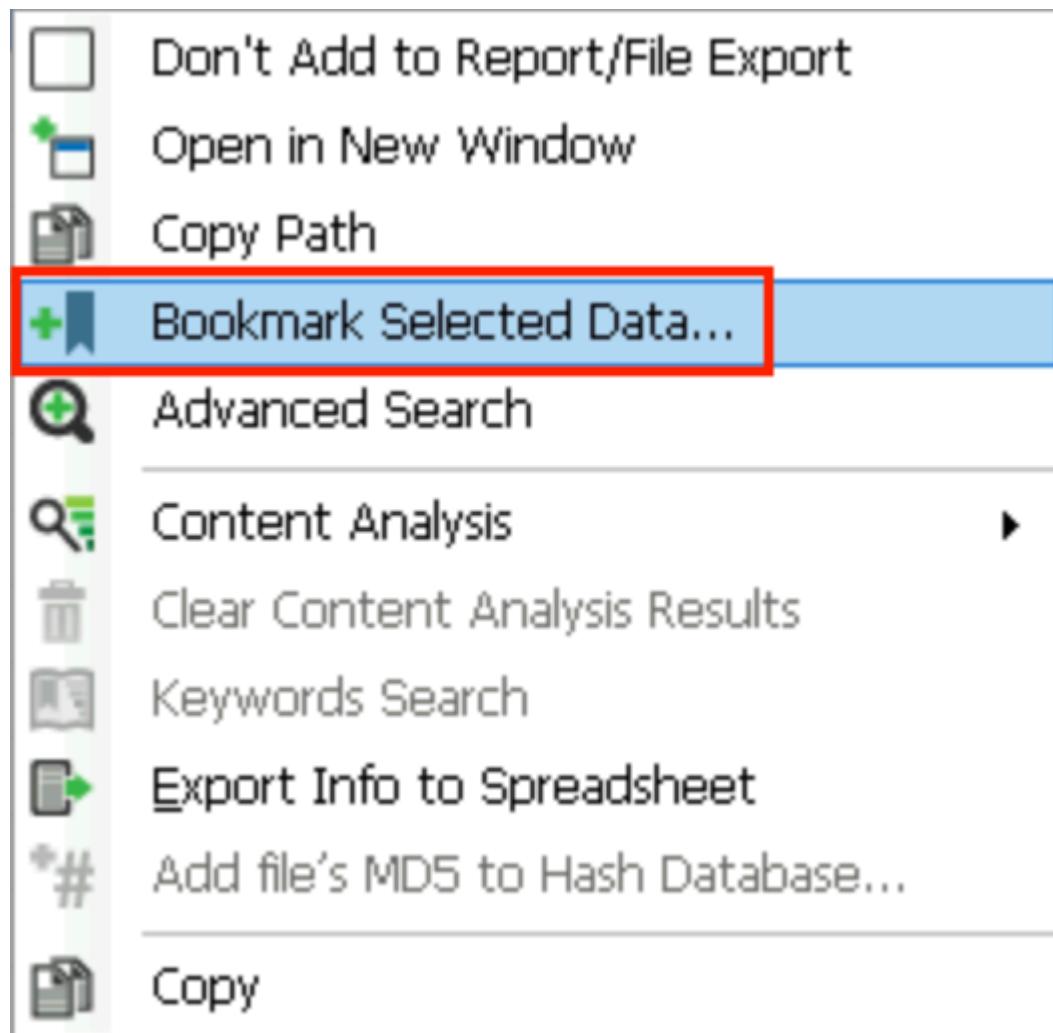
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

---



Checkbox

16. Right-click the selected event, then select **Bookmark Selected Data** to open the Bookmark Selected Data dialog box.



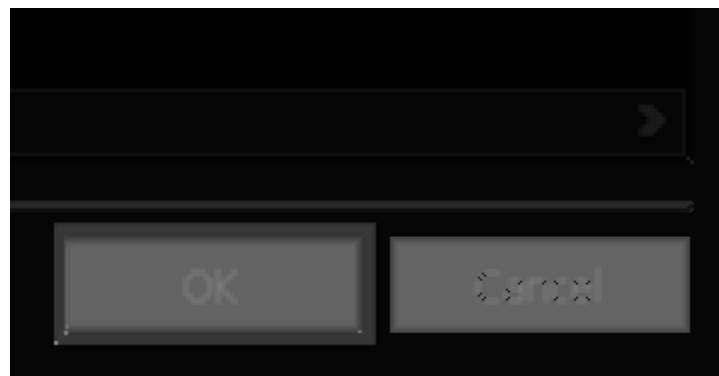
## Bookmark Selected Files

17. In the Bookmark Selected Files dialog box, **click OK** to save the bookmark and close the dialog box.

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

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

---



Bookmark Selected Files dialog box

18. In the Case Content pane, click the **Messages folder** to open the Messages grid in the Data Viewer.



Messages

**Note:** The Messages grid contains data related to text messages stored in the iPhone, including the sender, recipient, text content, date received, date sent, read receipts, service, and more. Service refers to the message type, namely SMS or iMessage. iOS supports both the standard SMS messages that are compatible with all mobile devices and Apple's proprietary iMessage system, which functions exclusively on Apple devices.

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

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

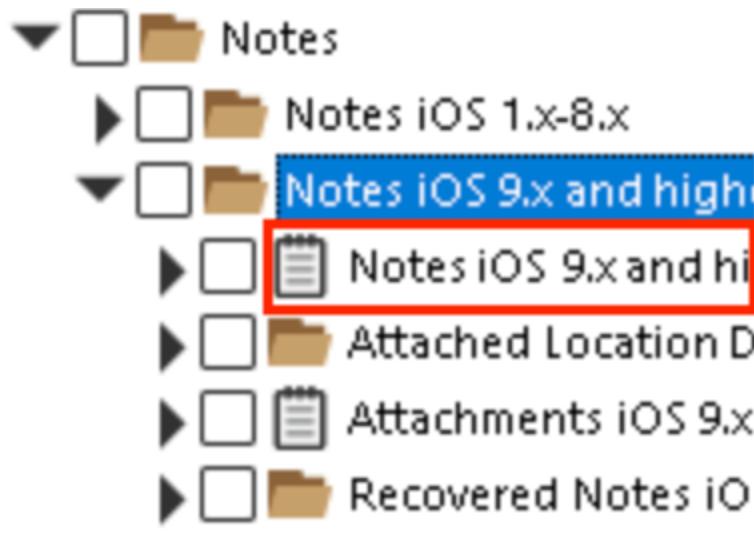
19. In the Messages grid, **review** the **text message data** for messages containing evidence associated with the car thefts.

**Note:** Upon reviewing the outgoing text messages on the suspect's phone, you should locate two messages that could be associated with the car thefts. The first is a message to Stinky asking about a specific car. The second is a message to ICE Mylady that indicates a car is located in Windy City.

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

21. **Repeat steps 15-17** to save bookmarks for the two text messages.

22. In the Case Content pane, **navigate to Notes / Notes iOS 9.x and higher**, then **select** the **Notes iOS 9.x and higher** grid to open it in the Data Viewer.



Notes iOS 9.x and higher

**Note:** Notes are often valuable sources of information in a forensic investigation, as users will often use this quick and easy word-processing tool to capture or save important, text-based information, such as instructions, to-do lists, and even journals.

# Conducting Forensic Investigations on Mobile Devices (4e)

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

23. In the Notes grid, **review the notes data** for notes containing evidence associated with the car thefts.

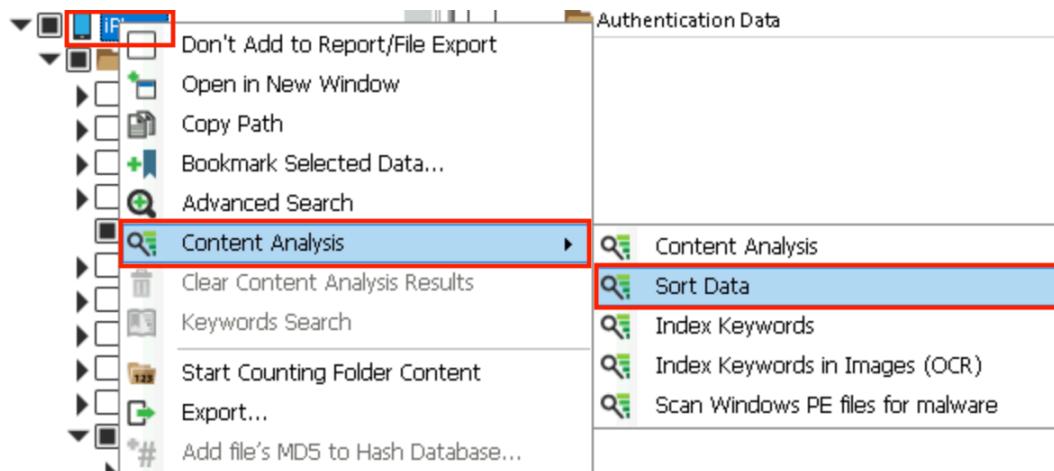
**Note:** As you review the contents of the notes on the suspect's phone, you should find additional evidence related car thefts in the notes data. Specifically, you should see a note confirming that the suspect knew a specific license plate number was known to police. You also see three notes relating to license plates being replaced.

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

25. **Repeat steps 15-17** to save bookmarks for the four notes.

**Note:** So far, your investigation has been limited to the parsed data for specific native iPhone apps. In the next steps, you will use E3's Content Analysis function to search for photos and image files stored in the acquired iPhone data, including unparsed data.

26. In the Case Content pane, **right-click the iPhone node** and **select Content Analysis > Sort Data** to open the Content Analysis Wizard.

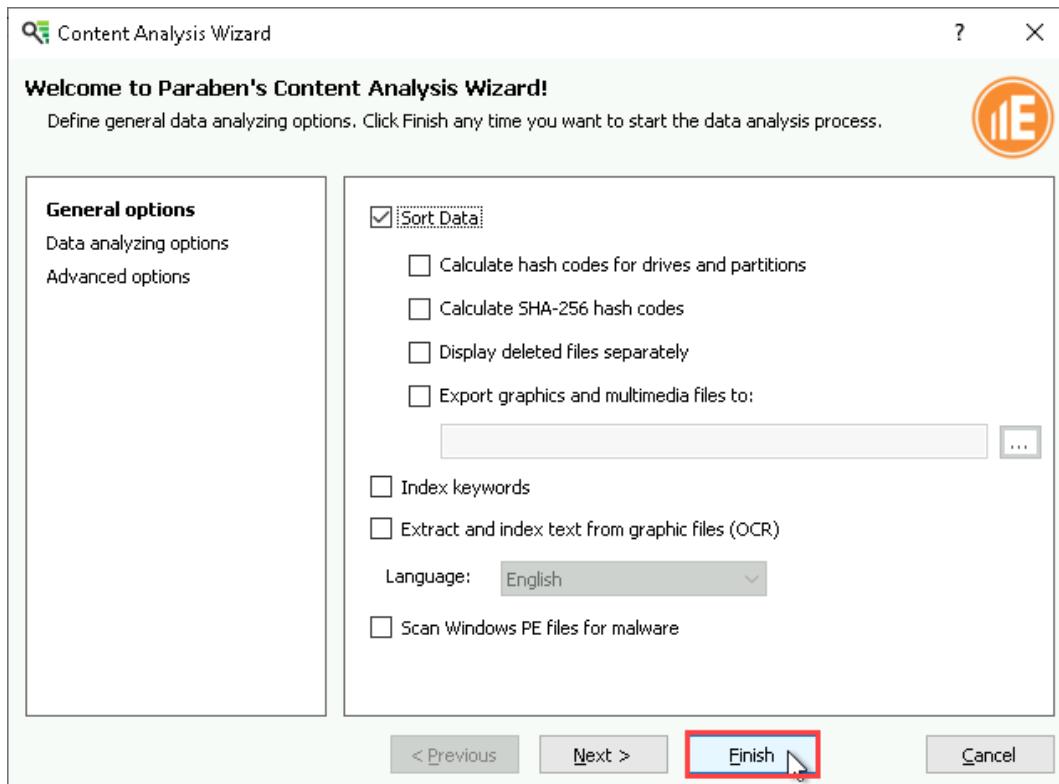


Content Analysis > Sort Data

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

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

27. In the Content Analysis Wizard, **confirm** the Sort Data option is selected, then **click Finish** to launch the content analysis process.



Content Analysis Wizard

28. When prompted, **click OK** to close the Task Status Notification dialog box.

# Conducting Forensic Investigations on Mobile Devices (4e)

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

---

Task Status Notification



**Name:** Sorting

**Source:** yourname Mobile Forensics/iPhone\_Acquisition\_08-12-2021\_11-40-13/E3 data case/iPhone

**State:** Finished

Don't show this message again

OK

Task Status Notification

29. In the Case Content pane, **click the Sorted Files tab** to switch to the Sorted Files view.



Sorted Files tab

30. In the Sorted Files pane, **expand the Sorted Files node** to view the file types available in the case.

Sorted Files

Case Content      Sorted Files

Sorted Files

- Documents (0)
- Email (0)
- Chats (0)
- Spreadsheets (0)
- Graphics (49)
- Databases (92)
- Executable (3)
- Compressed (3)
- Multimedia (1)
- Text (735)
- XML (50)
- Log Files (1)
- Encrypted (0)
- Financial files (0)
- Game Console Files (0)
- Others (33)
- ▶  Image Analyzer Results (0)
- ▶  Deleted Files (0)
- ▶  Recovered from Unallocated Space (0)

Sorted Files expanded

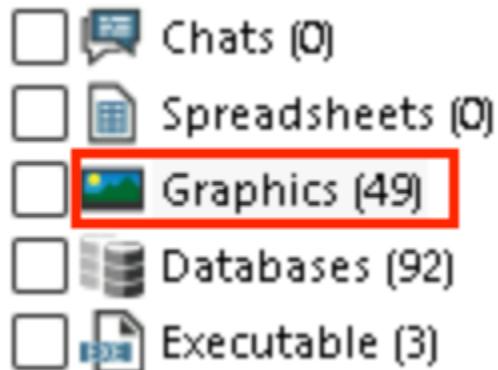
## Conducting Forensic Investigations on Mobile Devices (4e)

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

---

**Note:** You should see the following file types on the suspect's smartphone: graphic files, databases, executables, compressed files, multimedia, text, XML, log files, and others.

31. In the Sorted Files pane, **click the Graphics category** to display a list of images identified on the iPhone in the center pane.



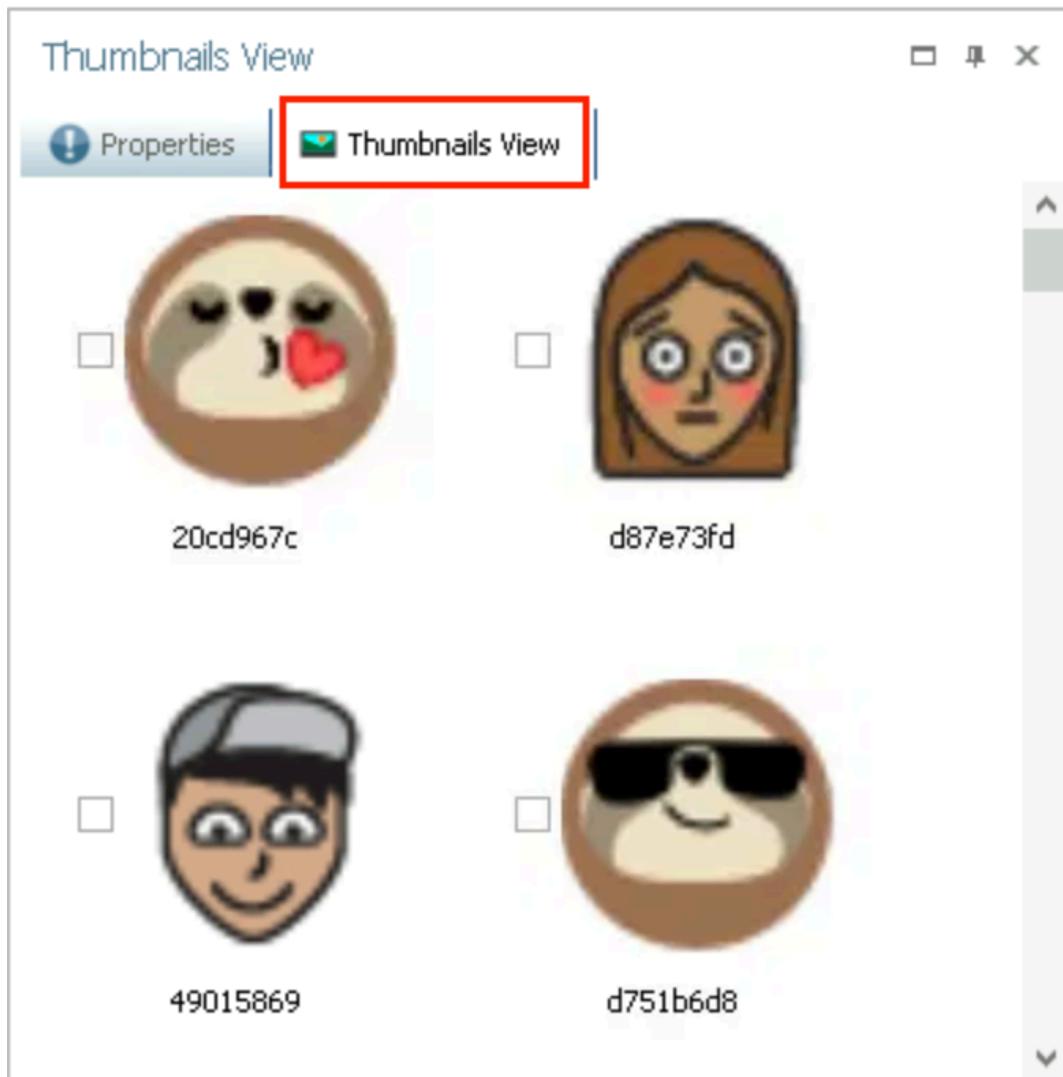
Graphics

32. In the Properties Pane, **select the Thumbnails View tab** to display the images as thumbnails.

If necessary, expand the right pane to display more images in the Thumbnails View.

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

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



Thumbnails View

33. In the Thumbnails View, **review the images** for evidence associated with the car thefts.

**Note:** As you review the thumbnails, you should discover 13 pictures of cars. Many of these images include the license plates of the vehicles. You suspect these may be the new license plates added to the cars after they were stolen.

## 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.

35. Repeat steps 15-17 to save bookmarks for the images.

**Note:** In the next steps, you will use E3's reporting functionality to generate an investigative report containing the evidence you found. Good reports are a critical part of an investigation. The report allows the investigator to effectively and concisely present the distilled evidence and create a non-technical summary for decision makers, executives, and attorneys. A well-constructed report can also be crucial in ongoing investigations where months or years will pass before new evidence is introduced. Good reporting ensures that no critical evidence or information is forgotten or overlooked.

36. On the E3 toolbar, click the **Reports** tab, then click the **Generate Report** button to open the Reports Wizard.

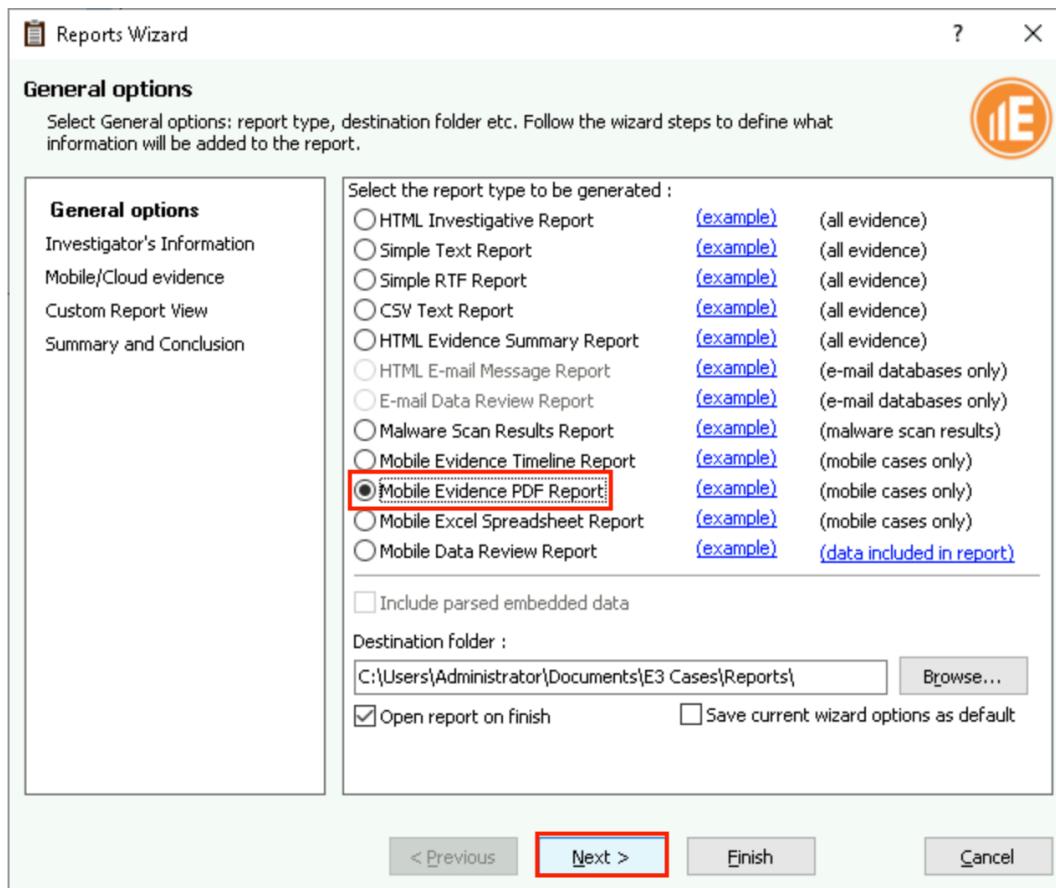


Generate Report

37. On the General Options page, select the **Mobile Evidence PDF Report** radio button, then click **Next** to continue.

# Conducting Forensic Investigations on Mobile Devices (4e)

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



## General Options

38. On the Investigator's Information page, type **yourname** in the Investigator name field, replacing **yourname** with your own name, then click **Next** to continue.

# Conducting Forensic Investigations on Mobile Devices (4e)

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

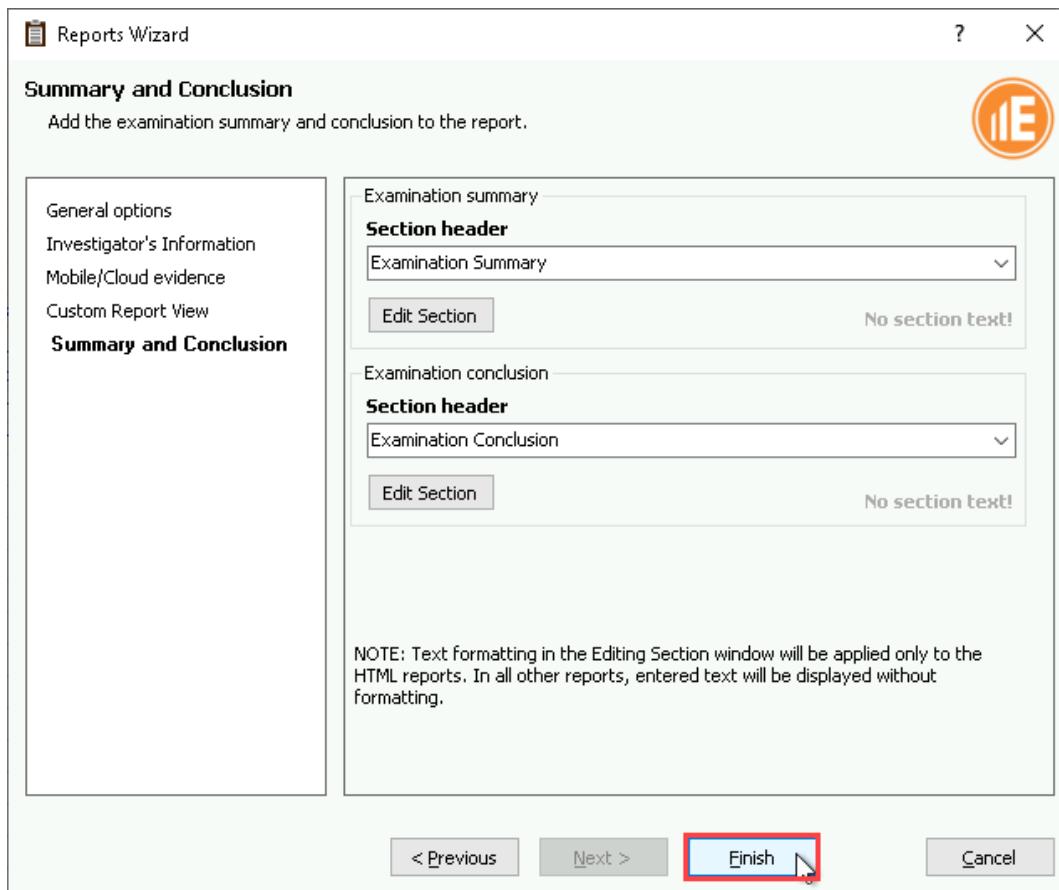
The screenshot shows the 'Reports Wizard' interface for 'Investigator's Information'. On the left, a sidebar lists 'General options', 'Investigator's Information' (which is selected), 'Mobile/Cloud evidence', 'Custom Report View', and 'Summary and Conclusion'. The main panel contains fields for 'Investigator name' (with 'yourname' typed in and highlighted by a red box), 'Agency/Company', 'Phone', 'Fax', 'Address', 'E-mail', and a large 'Comments' text area. A checkbox labeled 'Save changes to the case' is checked. At the bottom, buttons for '< Previous', 'Next >', 'Finish', and 'Cancel' are visible, with 'Next >' being the one highlighted by a red box.

## Investigator's Information

39. On the Mobile/Cloud evidence page, **click Next** to accept the default settings and continue.
40. On the Custom Report View page, **click Next** to accept the default settings and continue.
41. On the Summary and Conclusion page, **click Finish** to generate the report.

# Conducting Forensic Investigations on Mobile Devices (4e)

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



## Summary and Conclusion

**Note:** After about 30 seconds, the report will automatically open in Adobe Reader.

43. Review the report, then navigate to the Table of contents page.
44. Make a screen capture showing the Table of contents in the investigative report.
45. Close the Adobe Reader window.
46. Click OK to close the Task Status Notification dialog box.

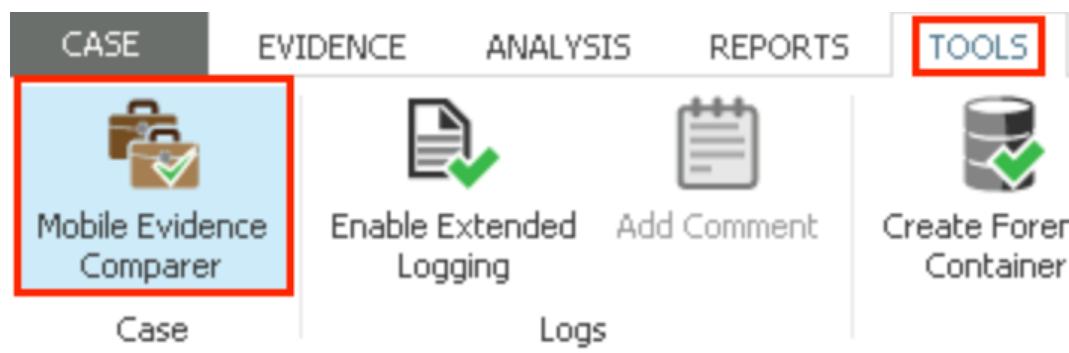
47. Close the E3 window.

## Part 2: Compare iOS Data Cases

**Note:** In this part the lab, you will compare the same iOS data case you reviewed in Part 1 with a second iOS data case that was generated from the same device one day later. Rather than manually comparing the data from the two cases, you will use E3's Mobile Evidence Comparer. For investigators, this unique feature can be a tremendous time-saver. In real-world investigations, the Mobile Evidence Comparer can be used to quickly determine if a mobile device has been compromised or has been used improperly. It is often used in corporate or government environments where the mobile device is issued to a user and is easily accessible for data acquisition.

In the next steps, you will re-open E3 and add the data cases to the Mobile Evidence Comparer.

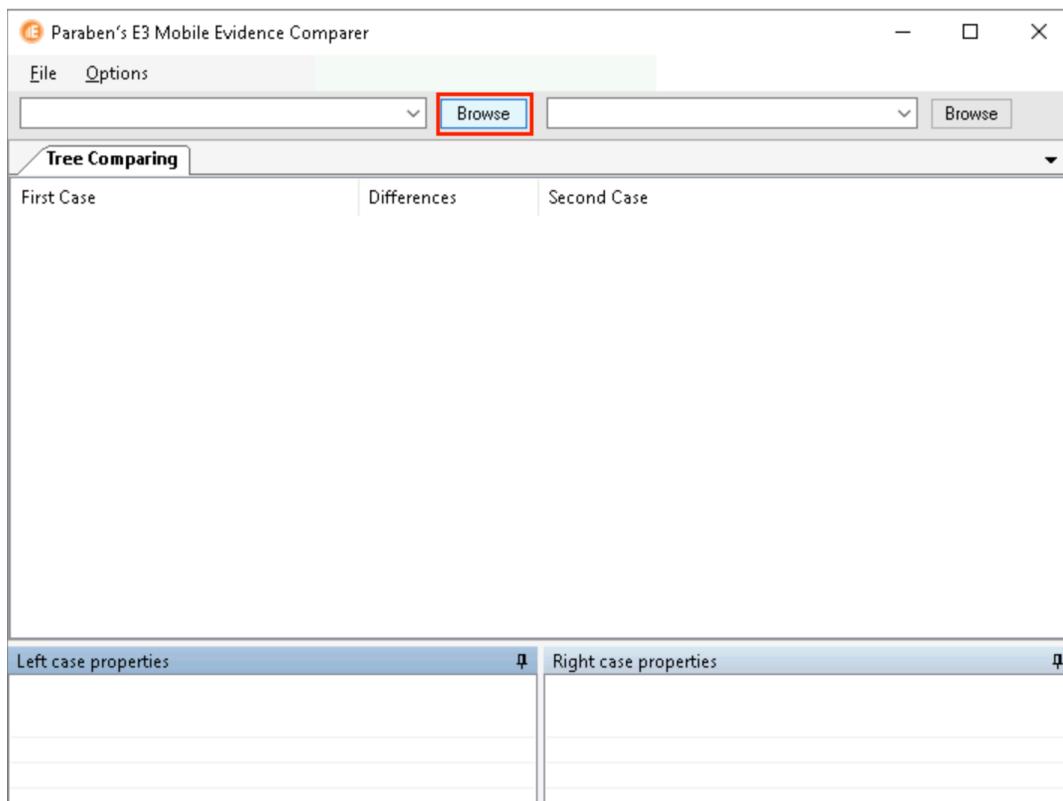
1. On the vWorkstation desktop, **double-click** the **Electronic Evidence Examiner** icon to re-open the E3 application.
2. **Close** the **Welcome** screen.
3. From the E3 toolbar, **click** the **Tools** tab, then **click** the **Mobile Evidence Comparer** button to open the Mobile Evidence Comparer in a new window.



# Conducting Forensic Investigations on Mobile Devices (4e)

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

4. In the Mobile Evidence Comparer, click the **left Browse button** to open the Open dialog box.

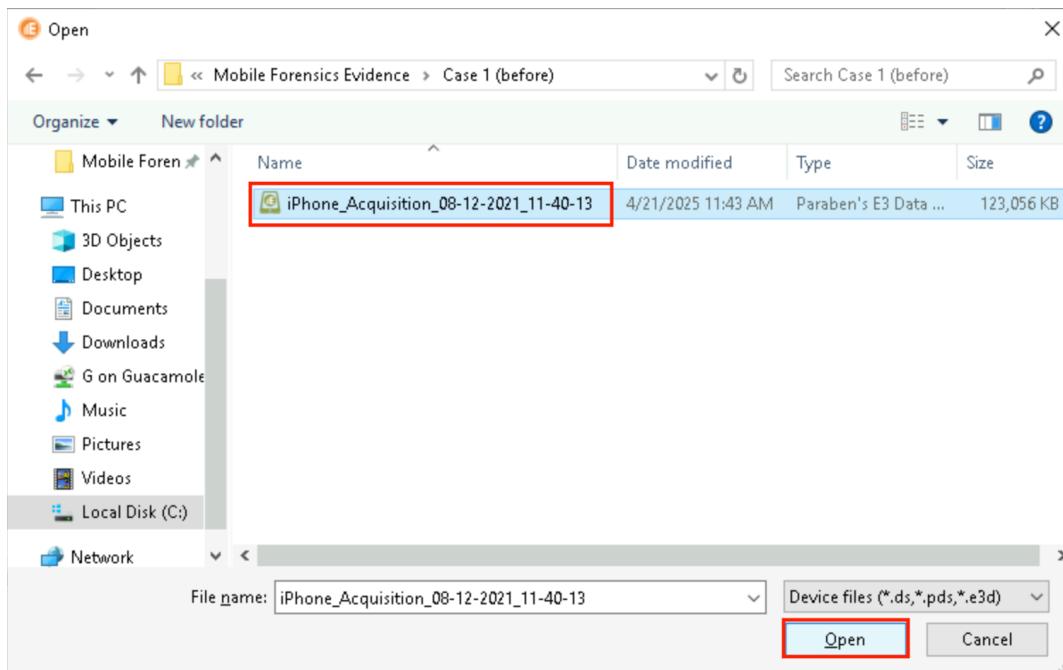


Left Browse Button

5. In the Open dialog box, navigate to **This PC > Local Disk (C:) > Mobile Forensics Evidence > Case 1 (before)**, select the **iPhone\_Acquisition\_08-12-2021\_11-40-13.e3d** case and click **Open** to import the first Paraben data case for the iPhone.

# Conducting Forensic Investigations on Mobile Devices (4e)

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



Open dialog box

6. In the Mobile Evidence Comparer, **click the right Browse button** to open the Open dialog box.
7. In the Open Evidence dialog box, **navigate to This PC > Local Disk (C:) > Mobile Forensics > Case 2 (after)**, then **select the iPhone\_Acquisition\_08-12-2021\_11-55-18.e3d case** and **click Open** to import the second Paraben data case for the iPhone.

**Note:** The differences in the two cases are highlighted in blue and green by default. Blue indicates that the file was modified in some way, with the exact differences specified in the Differences column. Green indicates that the file is not available in one of the cases.

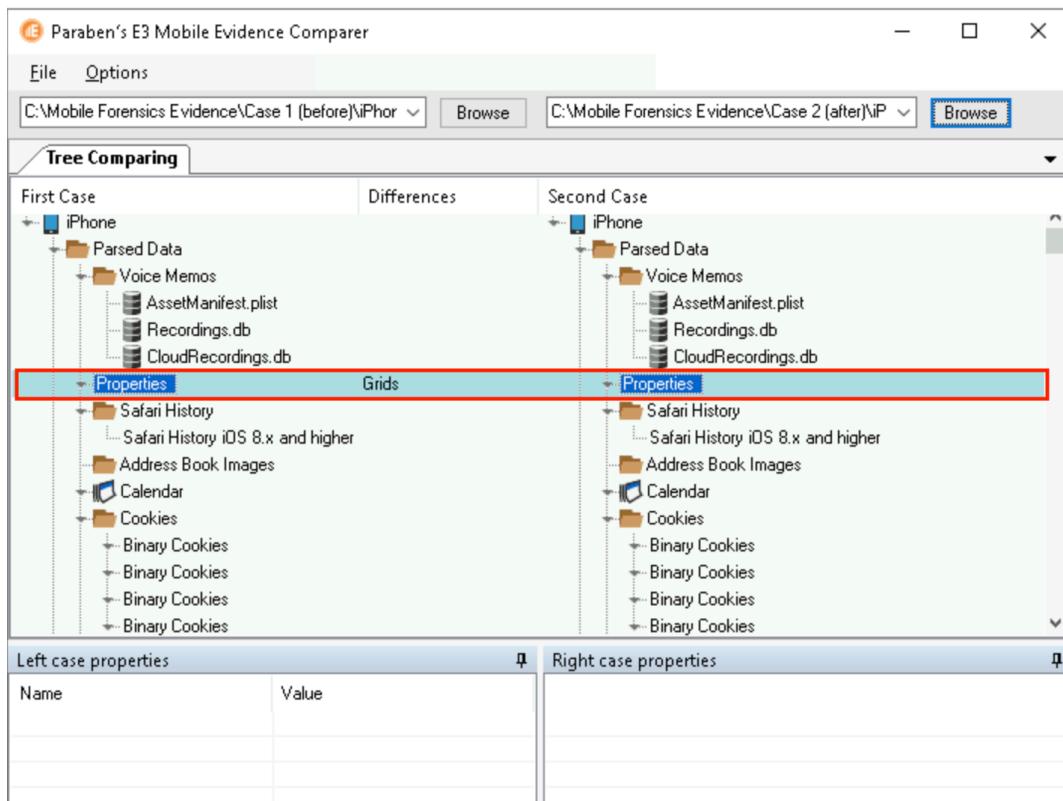
In the next steps, you will examine the first blue row in greater detail.

8. In the Mobile Evidence Comparer, **double-click the blue Properties row** to open the

# Conducting Forensic Investigations on Mobile Devices (4e)

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

Comparing versions of file: Properties window.



## Properties

**Note:** The contents of the *Comparing versions of file* window will depend on the nature of the difference. In this case, the difference resides in the grid, so the Mobile Evidence Comparer will display the grid view of the Properties file. When the difference exists in the size or content of a file, the Mobile Evidence Comparer will display a byte-level view of the difference.

9. In the Comparing window, scroll down to the **TimeintervalSince1970** row.

# Conducting Forensic Investigations on Mobile Devices (4e)

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

Comparing versions of file: Properties	
Property	Value
ProductVersion	14.4
ProductionSOC	true
ProtocolVersion	2
RegionInfo	FS/A
SIMStatus	kCTSIMSSupportSIMStatusNotInserter
SerialNumber	F4GZNMQ4N739
SoftwareBehavior	
TimeIntervalSince1970	1628757765.259583
TimeZone	America/New_York
TimeZoneOffsetFromUTC	-14400
TrustedHostAttached	true
UniqueChipID	7125527088889902
UniqueDeviceID	00008030-001950A10EF8802E
Uses24HourClock	false
WiFiAddress	b8:7b:c5:df:40:63
WirelessBoardSerialNumber	F0018599ADA

Property	Value
ProductVersion	14.4
ProductionSOC	true
ProtocolVersion	2
RegionInfo	FS/A
SIMStatus	kCTSIMSSupportSIMStatusNotInserter
SerialNumber	F4GZNMQ4N739
SoftwareBehavior	
TimeIntervalSince1970	1628758525.098778
TimeZone	America/New_York
TimeZoneOffsetFromUTC	-14400
TrustedHostAttached	true
UniqueChipID	7125527088889902
UniqueDeviceID	00008030-001950A10EF8802E
Uses24HourClock	false
WiFiAddress	b8:7b:c5:df:40:63
WirelessBoardSerialNumber	F0018599ADA

Comparing window

**Note:** When displaying differences in a grid, the Mobile Evidence Comparer will highlight the row where the differences occur in green. The specific value that differs will be highlighted in pink.

In this case, the difference resides in the timestamp for the phone's data case, which makes sense, given that the data cases were generated a full day apart.

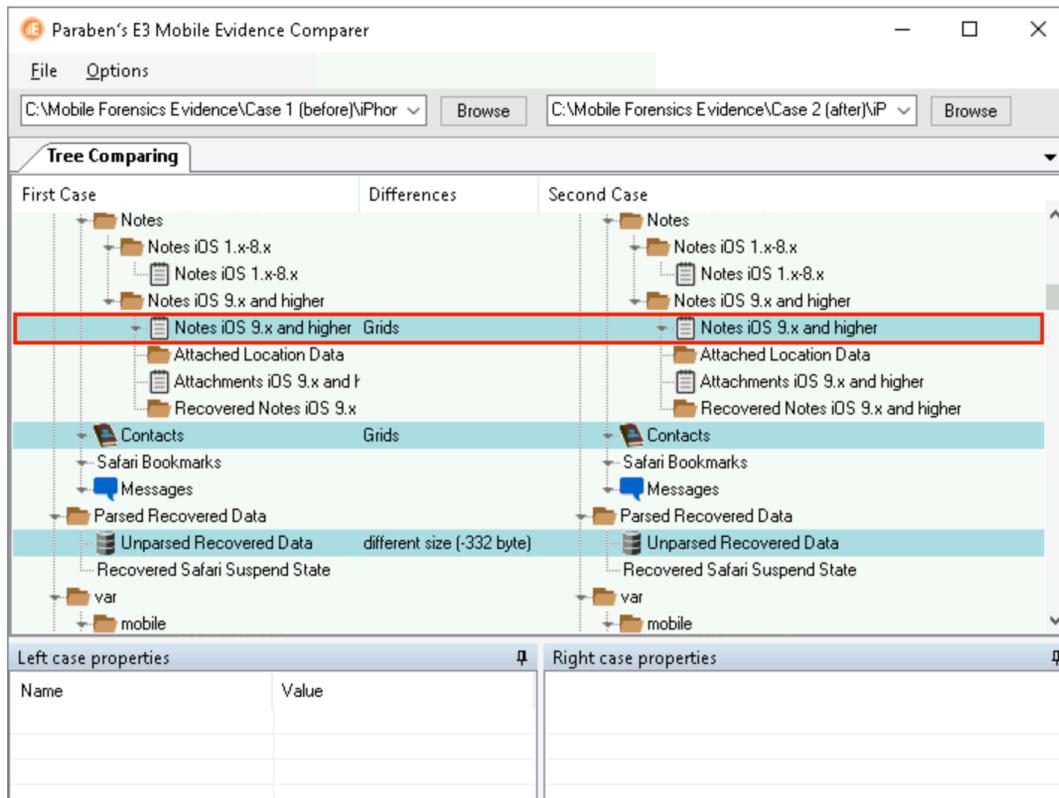
10. Make a screen capture showing the **difference in data case properties**.

11. Close the **Comparing window**.

12. In the Mobile Evidence Comparer window, **scroll down** to locate the **Notes iOS 9.x and higher** row.

# Conducting Forensic Investigations on Mobile Devices (4e)

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



Notes iOS 9.x and higher row

13. Double-click the **Notes iOS 9.x and higher** row to open the Comparing window.

14. Maximize the **Comparing window** to display the full contents of the grid.

**Note:** You should see that several Notes have been deleted in the newer data case.

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

16. Close any **open windows**.

**Note:** This concludes Section 1 of the lab.

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

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

---

## Section 2: Applied Learning

**Note:** SECTION 2 of this lab allows you to apply what you learned in SECTION 1 with less guidance and different deliverables, as well as some expanded tasks and alternative methods. You will continue your investigation and analyze an Android data case.

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

**Note:** In Section 1, you completed your analysis of the recovered iOS phone and prepared a formal investigative report on your findings. Next, you will need to analyze the data on the Android phone that was also seized from the suspects. You have yet to determine which phone belongs to Bonnie and which phone belongs to Clyde, so as a first step, you will focus your investigation on the user data, including contacts and browsing history.

In the next steps, you will add the Android evidence to E3 and review the information available within Mobile Data Triage.

1. From the vWorkstation desktop, **launch the E3 application**.
2. From the Welcome screen, **open the *yourname* Mobile Forensics case file** that you created in Section 1.
3. On the E3 toolbar, **click the Add Evidence button**, then **import** the **Lab\_Android\_Acquisition\_06-02-2021\_17-52-55 / E3 data case** from the C:\Mobile Forensics Evidence folder.
4. When prompted, **accept** the default name for the evidence.
5. In the Case Content pane, **navigate to *yourname* Mobile Forensics / Lab\_Android\_Acquisition\_06-02-2021\_17-52-55 / E3 data case**, then **expand** the **Mobile Data Triage node**.

**Note:** Similar to the Parsed Data folder that you reviewed in Section 1, Mobile Data Triage automatically surfaces and sorts files from some of the most commonly referenced sources of evidence. The Parsed Data folder is generated by E3 as a matter of necessity during the evidence acquisition process, while the Mobile Data Triage view is a curated collection of evidence derived from the parsed data that is presented in relevant categories for the benefit of the investigator.

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

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

---

6. In the Case Content pane, **select the Device Information category** and **review** its contents in the Data Viewer.

**Note:** Like the Properties tab for the iPhone, this category will show you basic information about the phone, including brand, manufacturer, model, and serial number. In this case, you can confirm that the suspect has an Honor smartphone from Huawei.

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

8. In the Case Content pane, **select the ICE Contacts category** and **review** its contents in the Data Viewer.

**Note:** ICE is a common acronym for "In Case of Emergency." When analyzing smartphone data, you can infer a close connection between the owner of the device and the ICE contacts, who are typically spouses, immediate family members, or close friends.

In this case, you should see two ICE contacts: Clyde and Daddy Dear. By process of elimination, you can reasonably infer that this device belongs to Bonnie and the iOS device belongs to Clyde.

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

10. **Create a bookmark** for the Clyde ICE contact.

11. In the Case Content pane, **select the Contact Email Accounts category** and **review** its contents in the Data Viewer.

**Note:** You should see three contacts in the Contact Email Accounts folder for the suspect. They belong to Lucas Carter, Emma Chicago, and Tom Audi&BMW. Based on his name, it seems likely that Tom Audi&BMW could be a contact associated with the car thefts.

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

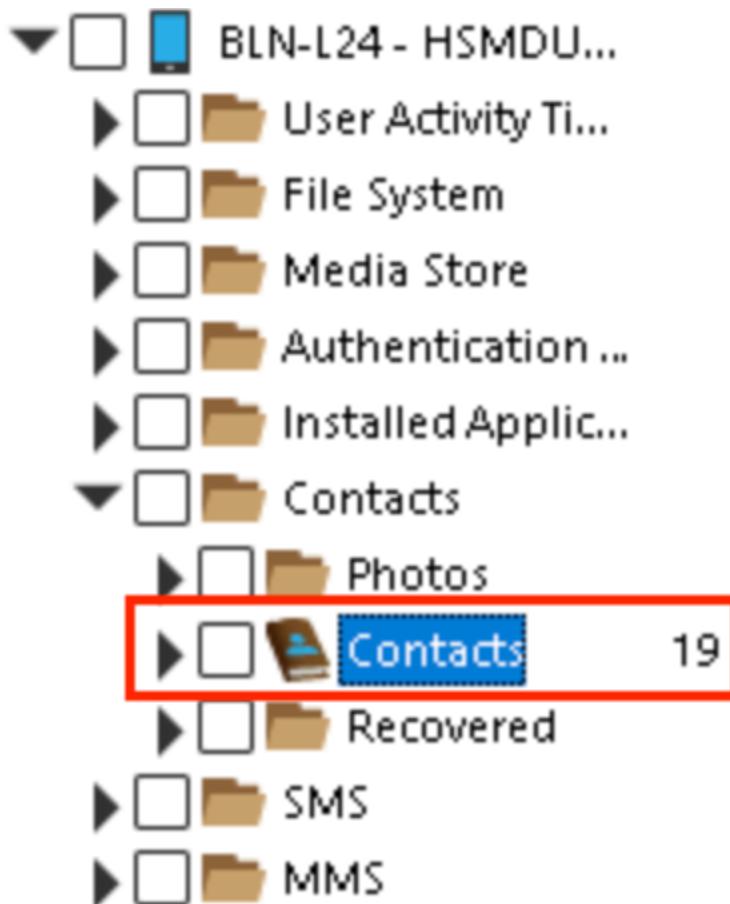
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 08

---

12. **Make a screen capture showing the Contact Email Accounts.**
13. **Create a bookmark** for the Tom Audi&BMW contact.
14. In the Case Content pane, **select the Installed Applications category** and review its contents in the Data Viewer.

**Note:** This category shows a list of the apps that the user installed on their phone. Within the installed applications, you should see that the suspect had installed the eBay Motors application. This could be where the suspect sells the vehicles after they are altered.

15. **Make a screen capture showing the Installed Applications.**
16. **Create a bookmark** for the eBay Motors app.
17. In the Case Content pane, **navigate to BLN-L24 – HSMDU17A21002751 / Contacts**, then **select the Contacts grid** to display the contents in the Data Viewer.



### Contacts

**Note:** Like iOS, the contacts grid in Android contains the full names, phone numbers, and email addresses of contacts stored on the device, as well as timestamps for creation and modification dates. In the grid, you should see information for 19 contacts. However, it is not uncommon for criminals to delete contacts after they have completed a transaction in an effort to cover their tracks.

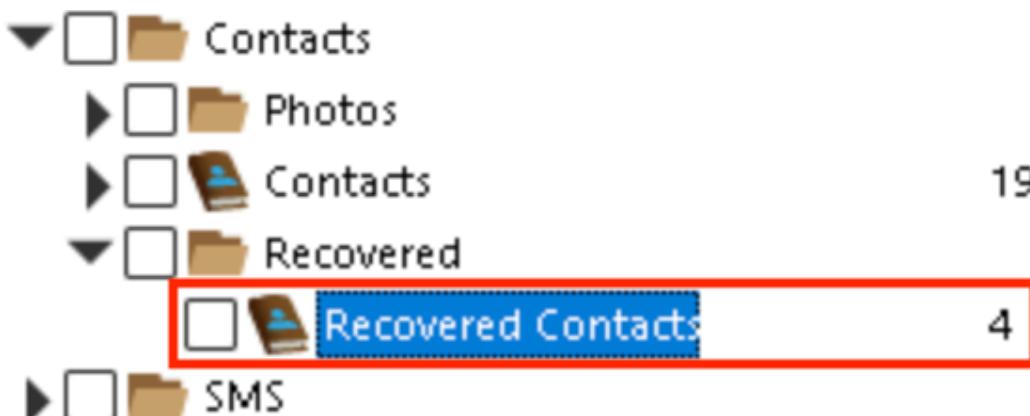
In the next steps, you will attempt to retrieve any deleted contact information on the Android smartphone.

18. In the Case Content pane, **expand the Recovered folder**, then **select the Recovered Contacts item** and review the contents in the Data Viewer.

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

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

---



Recovered Contacts

**Note:** Within the Recovered Contacts grid, you should see four contacts: the first only contains a Note with an eBay URL, the second only contains a phone number, the third is blank, and the fourth contains an email address. For the same reasons that criminals delete contacts, it is a best practice to initially save those contacts with as little identifying information as possible.

19. Make a screen capture showing the recovered contact information from the Android phone.
20. Create a bookmark for the second and fourth recovered contacts.

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

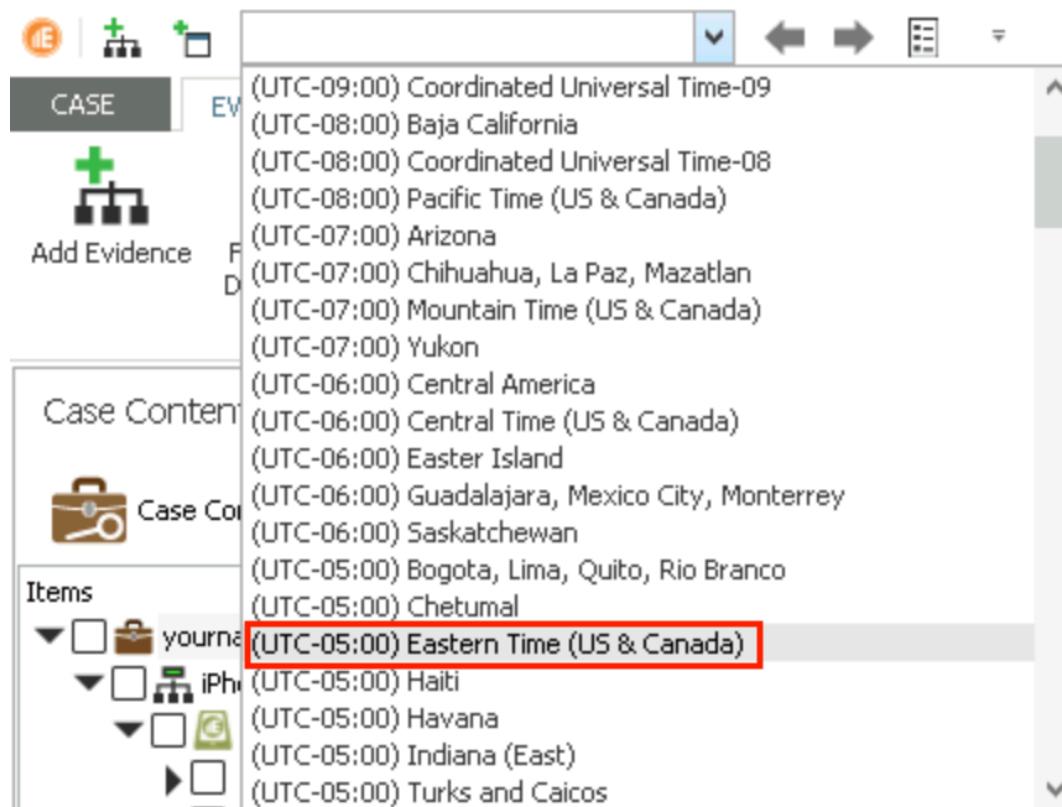
**Note:** In any forensic investigation, an investigator should attempt to re-create a timeline of the crime based on the evidence that's available to them. When working with Android devices, the User Activity Timeline feature makes this process immensely easier by providing a literal timeline of user activity on the device that shows exactly which apps were used and when.

For the next steps, assume that you have previously recovered evidence in the case that indicates that a crime occurred on 6/2/2021 between 9:17:47 AM and 9:24:51 AM (Eastern Standard Time). You will analyze the User Activity Timeline for this period and attempt to identify additional supporting evidence to guide your investigation further.

1. In the upper-left corner of the E3 window, select (UTC-05:00) Eastern Time to change the time zone.

# Conducting Forensic Investigations on Mobile Devices (4e)

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



Update the time zone

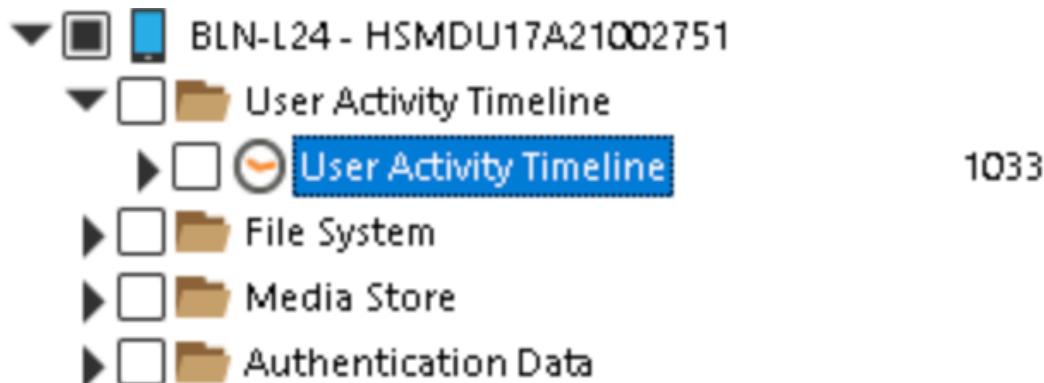
**Note:** Altering the time zone in E3 will automatically update timestamps within the case data to match the selected time zone. In this case, assume that you know that the crime occurred on the Eastern seaboard.

2. In the Case Content pane, **expand** the **User Activity Timeline folder**, then **select** the **User Activity Timeline grid** to open it in the Data Viewer.

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

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

---



### User Activity Timeline

3. **Review** the user activity that occurred between 9:17:47 AM and 9:24:51 AM on 6/2/2021.

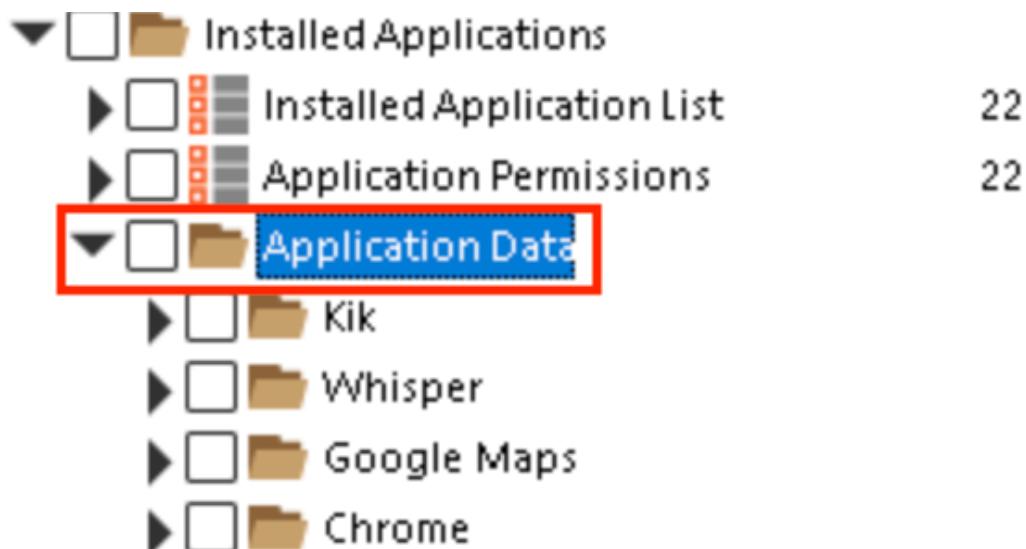
**Note:** In this time period, you should see that the suspect accessed Whisper, Chrome, VPN Unlimited, Contacts, and Calendar (as well the System UI and Huawei Home). This information will allow you to focus your investigation to these specific applications in the next steps.

4. **Make a screen capture showing the User Activity Timeline between 9:17:47 AM and 9:24:51 AM on 6/2/2021.**
5. In the Case Content pane, **navigate to Installed Applications / Application Data**.

# Conducting Forensic Investigations on Mobile Devices (4e)

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

---



## Application Data

**Note:** As the name implies, the Application Data folder contains application-specific data. You should recognize two of the applications that you found in the User Activity Timeline: Whisper and Chrome. You will begin by examining Whisper. Whisper is a chat application that allows users to connect anonymously online. Given the context of the investigation, it seems likely that the suspect may be using Whisper to contact others involved in the car theft operation or to identify buyers.

6. In the Case Content pane, **expand** the **Whisper folder**, then **select** the **Own Whispers grid** and **review** the contents in the Data Viewer.

**Note:** In the Own Whispers grid, you should see three texts that were sent from the suspect's device: one referencing a Porsche 911, one referencing the Windy City (the same location mentioned on Clyde's phone), and one mocking the cops.

7. **Make a screen capture** showing the **contents of the Own Whispers grid**.
8. **Create a bookmark** for the three Whisper texts.
9. In the Case Content pane, **expand** the **Chrome folder**, then **select** the **History grid** to display the contents in the Data Viewer.

# Conducting Forensic Investigations on Mobile Devices (4e)

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

---

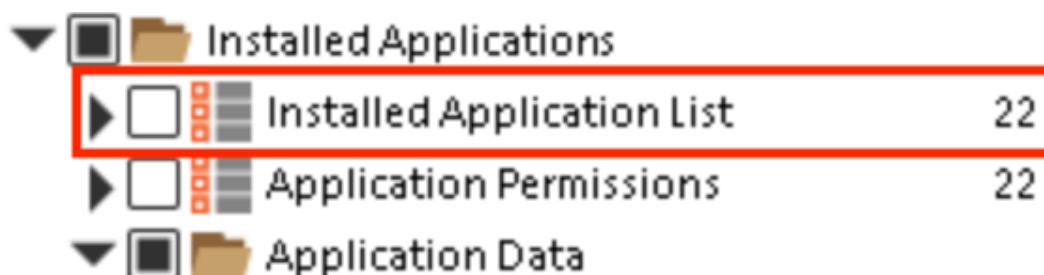
**Note:** In the Chrome History grid, you should see that the suspect visited websites several websites related to cars, including autonews.com, tesla.com, ebay.com/motors, and ran Google searches on the Porsche 911 and new Tesla models.

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

11. Create a bookmark for the relevant browser history records.

**Note:** In the next steps, you will dig deeper into the application data by directly examining SQLite databases. SQLite databases are a popular option for data storage on mobile devices. Fortunately for forensic investigators, they are easily parsed by applications such as E3, which makes the information contained within much easier to retrieve and analyze.

12. In the Case Content pane, **select the Installed Application List grid** and **review** the contents in the Data Viewer.



Installed Application List

13. In the Data Viewer, **select the Keep Notes app**, then **scroll to the right** to the **Raw Application Data column**, which contains the location of the raw application data within the filesystem.

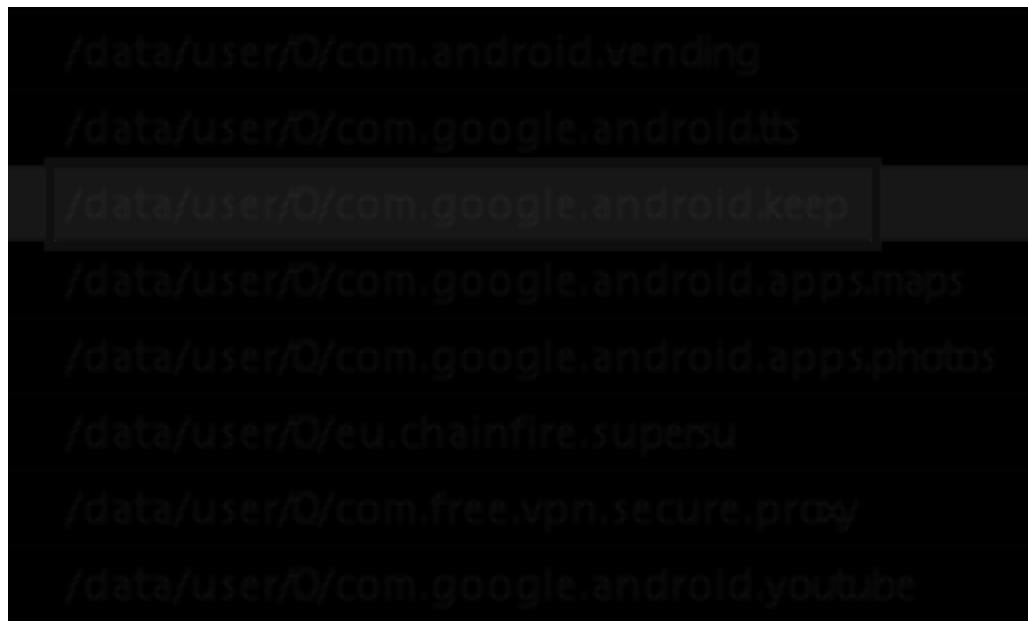
**Note:** Similar to Notes on iOS, Keep Notes is a popular app for creating personal notes on Android.

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

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

---

14. Under the Raw Application Data column, **click the file path link** to open the folder's location within the file system in a new tab.



Raw Application Data file path

**Note:** You may notice that the Case Content pane now displays a location deep within the Android file system. This is where digital forensics tools like E3 really demonstrate their value, as you would otherwise need to be sufficiently familiar with the Android file system to manually drill down into this specific location.

15. In the Data Viewer, **navigate to databases / keep.db / SQLite Database / Tables** to display the contents of the database.

**Note:** SQLite databases are commonly used in mobile apps for storing an application's core data, including application data, permissions, and file locations. SQLite databases are composed of tables, which in turn contain the actual data organized into rows and columns. In this case, you should see 52 tables within the SQLite database for Keep Notes.

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

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

---

16. In the Case Content pane, **navigate to list\_item / list\_item 1-5** and **review** the contents of the table for potential evidence.

**Note:** Within the table, you should see five records containing the text contents of the suspect's notes. Of the five notes, two appear to make reference to license plate numbers.

In a real-world investigation, you would more than likely need to spend time digging through different tables before finding relevant evidence.

17. **Make a screen capture** showing the **contents of the list\_item 1-5 table**.
18. **Create a bookmark** for the two records containing references to license plates.
19. In the Case Content pane, **navigate to Tables / account / account 1-1** and **review** the contents of the table for potential evidence.

You may need to expand the Items column header in the Case Content pane to see the full file tree.

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

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

databases	
keep.db	
SQLite Database	
Tables	
►	✓ sqlite_master 120
►	✓ android_metadata 1
►	✓ account 1
►	✓ account 1-1 1
►	✓ sqlite_sequence 5
►	✓ setting 5
►	✓ tree_entity 5
►	✓ blob_node 0
►	✓ blob 0

### Account 1-1

**Note:** The account table will provide the account name for the user that set up the Keep Notes account. In this case, you should see an email address – julriley1990@gmail.com. Given that you've already confirmed the phone belongs to Bonnie, and given that Bonnie and Clyde are almost certainly fake names, this email address may be a critical clue to Bonnie's actual identity.

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

21. Create a bookmark for the account record containing the email address.

22. Generate a **Mobile Evidence PDF Report**.

## **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.**

**24. Close any open windows.**

**Note:** This concludes Section 2 of the lab.

## Section 3: Challenge and Analysis

### Part 1: Research Report Writing for Digital Forensics

In Sections 1 and 2, you generated formal investigative reports that documented the evidence you located in both the iPhone and Android. However, you did not include a Case Summary or Conclusion.

Review the Introduction to Report Writing for Digital Forensics provided by the SANS Institute at <https://web.archive.org/web/20210303184323/https://www.sans.org/blog/intro-to-report-writing-for-digital-forensics/> for guidance on report writing. You may also conduct additional research of your own.

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

### Part 2: Draft a Forensic Report

Now that you have a better handle on the art and science of writing reports for digital forensic investigations, you will fill in the gaps that you left when you generated your investigative reports in Sections 1 and 2. Using the following template, prepare a simple report documenting the circumstances of the case, the evidence you found, and the conclusions you drew as a result.

#### **Case Summary**

#### **Findings and Analysis**

#### **Conclusion**

**Note:** This concludes Section 3 of the lab.