Student: Alexis Cherpes	Email: cherpea@ferris.edu

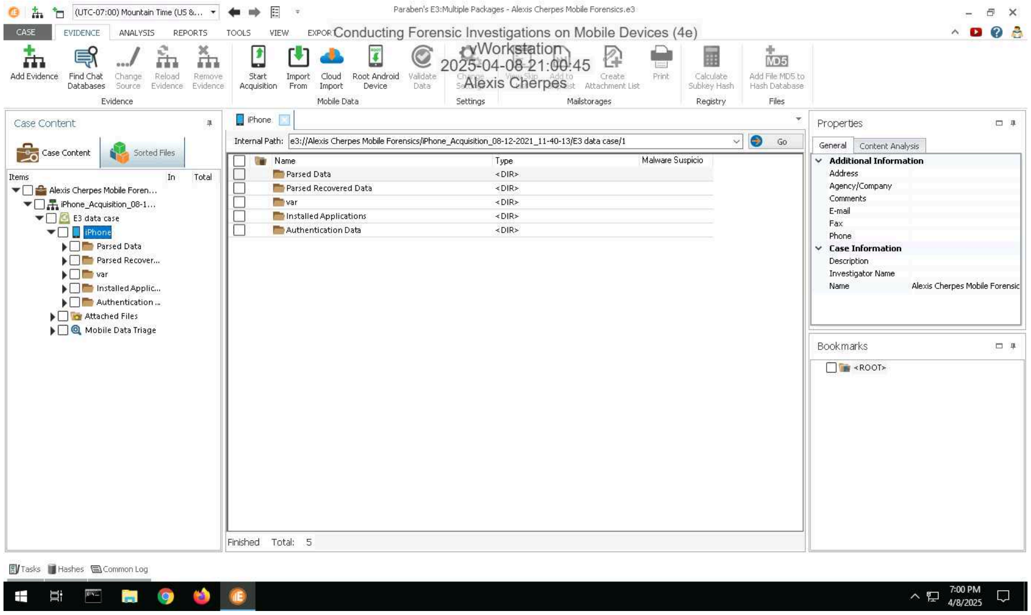
Time on Task: 2 hours, 16 minutes	Progress: 100%

Report Generated: Thursday, May 22, 2025 at 4:50 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**.



Paraben's E3:Multiple Packages - Alexis Cherpes Mobile Forensics.e3

Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-04-08 21:00:45
Alexis Cherpes

Internal Path: e3://Alexis Cherpes Mobile Forensics/iPhone_Acquisition_08-12-2021_11-40-13/E3 data case/1

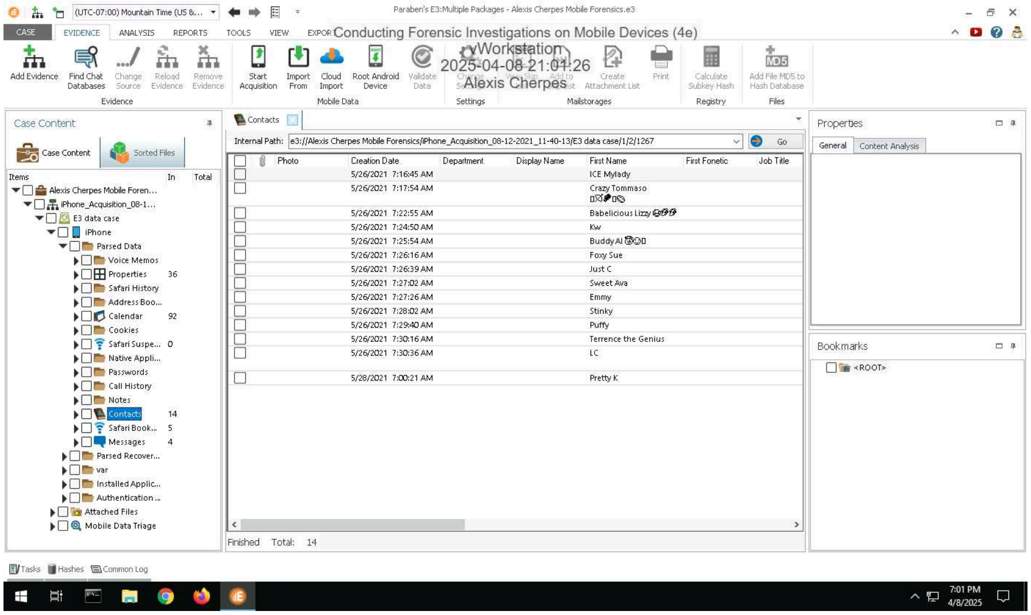
Name	Type	Malware Suspicio
Parsed Data	<DIR>	
Parsed Recovered Data	<DIR>	
var	<DIR>	
Installed Applications	<DIR>	
Authentication Data	<DIR>	

Finished Total: 5

Properties

Additional Information	
Address	
Agency/Company	
Comments	
E-mail	
Fax	
Phone	
Case Information	
Description	
Investigator Name	
Name	Alexis Cherpes Mobile Forensic

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



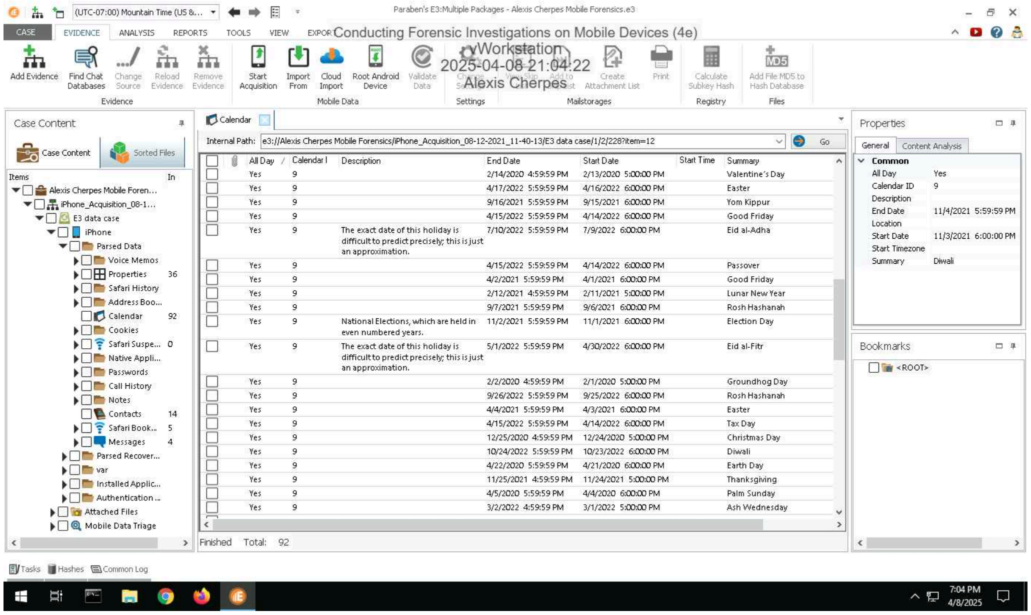
Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-04-08 21:01:26
Alexis Cherpes

Internal Path: e3://Alexis Cherpes Mobile Forensics/iPhone_Acquisition_08-12-2021_11-40-13/E3 data case/1/2/1267

□	Photo	Creation Date	Department	Display Name	First Name	First Fonetic	Job Title
□		5/26/2021 7:16:45 AM			ICE Mylady		
□		5/26/2021 7:17:54 AM			Crazy Tommaso ▯☒●▯⊘		
□		5/26/2021 7:22:55 AM			Babelicious Lizzy ☺☺☺		
□		5/26/2021 7:24:50 AM			Kw		
□		5/26/2021 7:25:54 AM			Buddy Al ☺☺▯		
□		5/26/2021 7:26:16 AM			Foxy Sue		
□		5/26/2021 7:26:39 AM			Just C		
□		5/26/2021 7:27:02 AM			Sweet Ava		
□		5/26/2021 7:27:26 AM			Emmy		
□		5/26/2021 7:28:02 AM			Stinky		
□		5/26/2021 7:29:40 AM			Puffy		
□		5/26/2021 7:30:16 AM			Terrence the Genius		
□		5/26/2021 7:30:36 AM			LC		
□		5/28/2021 7:00:21 AM			Pretty K		

Finished Total: 14

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



Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-04-08 21:04:22
Alexis Cherpes

Internal Path: e3://Alexis Cherpes Mobile Forensics/iPhone_Acquisition_08-12-2021_11-40-13/E3 data case/1/2/228?item=12

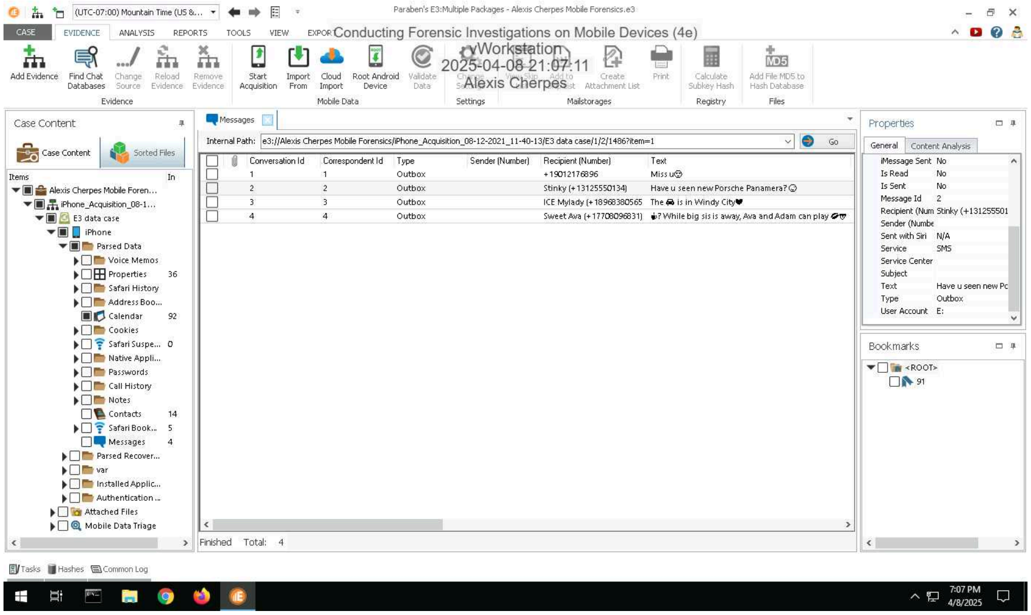
□	All Day	Calendar I	Description	End Date	Start Date	Start Time	Summary
□	Yes	9		2/14/2020 4:59:59 PM	2/13/2020 5:00:00 PM		Valentine's Day
□	Yes	9		4/17/2022 5:59:59 PM	4/16/2022 6:00:00 PM		Easter
□	Yes	9		9/16/2021 5:59:59 PM	9/15/2021 6:00:00 PM		Yom Kippur
□	Yes	9		4/15/2022 5:59:59 PM	4/14/2022 6:00:00 PM		Good Friday
□	Yes	9	The exact date of this holiday is difficult to predict precisely; this is just an approximation.	7/10/2022 5:59:59 PM	7/9/2022 6:00:00 PM		Eid al-Adha
□	Yes	9		4/15/2022 5:59:59 PM	4/14/2022 6:00:00 PM		Passover
□	Yes	9		4/2/2021 5:59:59 PM	4/1/2021 6:00:00 PM		Good Friday
□	Yes	9		2/12/2021 4:59:59 PM	2/11/2021 5:00:00 PM		Lunar New Year
□	Yes	9		9/7/2021 5:59:59 PM	9/6/2021 6:00:00 PM		Rosh Hashanah
□	Yes	9	National Elections, which are held in even numbered years.	11/2/2021 5:59:59 PM	11/1/2021 6:00:00 PM		Election Day
□	Yes	9	The exact date of this holiday is difficult to predict precisely; this is just an approximation.	5/1/2022 5:59:59 PM	4/30/2022 6:00:00 PM		Eid al-Fitr
□	Yes	9		2/2/2020 4:59:59 PM	2/1/2020 5:00:00 PM		Groundhog Day
□	Yes	9		9/26/2022 5:59:59 PM	9/25/2022 6:00:00 PM		Rosh Hashanah
□	Yes	9		4/4/2021 5:59:59 PM	4/3/2021 6:00:00 PM		Easter
□	Yes	9		4/15/2022 5:59:59 PM	4/14/2022 6:00:00 PM		Tax Day
□	Yes	9		12/25/2020 4:59:59 PM	12/24/2020 5:00:00 PM		Christmas Day
□	Yes	9		10/24/2022 5:59:59 PM	10/23/2022 6:00:00 PM		Diwali
□	Yes	9		4/22/2020 5:59:59 PM	4/21/2020 6:00:00 PM		Earth Day
□	Yes	9		11/25/2021 4:59:59 PM	11/24/2021 5:00:00 PM		Thanksgiving
□	Yes	9		4/5/2020 5:59:59 PM	4/4/2020 6:00:00 PM		Palm Sunday
□	Yes	9		3/2/2022 4:59:59 PM	3/1/2022 5:00:00 PM		Ash Wednesday

Finished Total: 92

Common

All Day	Yes
Calendar ID	9
Description	
End Date	11/4/2021 5:59:59 PM
Location	
Start Date	11/3/2021 6:00:00 PM
Start Timezone	
Summary	Diwali

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



Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-04-08 21:07:11
Alexis Cherpes

Internal Path: e3://Alexis Cherpes Mobile Forensics/iPhone_Acquisition_08-12-2021_11-40-13/E3 data case/1/2/1486?item=1

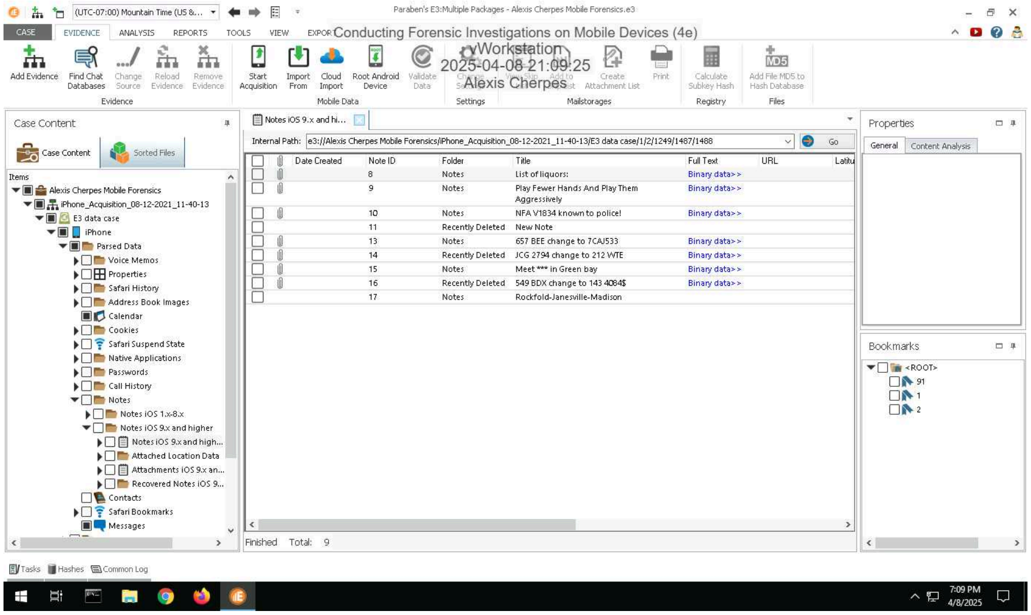
Conversation Id	Correspondent Id	Type	Sender (Number)	Recipient (Number)	Text
1	1	Outbox		+19012176896	Miss u😍
2	2	Outbox		Stinky (+13125550134)	Have u seen new Porsche Panamera? ☺
3	3	Outbox		ICE Mylady (+18968380565	The 🚗 is in Windy City❤
4	4	Outbox		Sweet Ava (+17708096831)	👆? While big sis is away, Ava and Adam can play 💋😈

Finished Total: 4

Properties — General

iMessage Sent	No
Is Read	No
Is Sent	No
Message Id	2
Recipient (Num	Stinky (+131255501
Sender (Numbe	
Sent with Siri	N/A
Service	SMS
Service Center	
Subject	
Text	Have u seen new Pc
Type	Outbox
User Account	E:

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



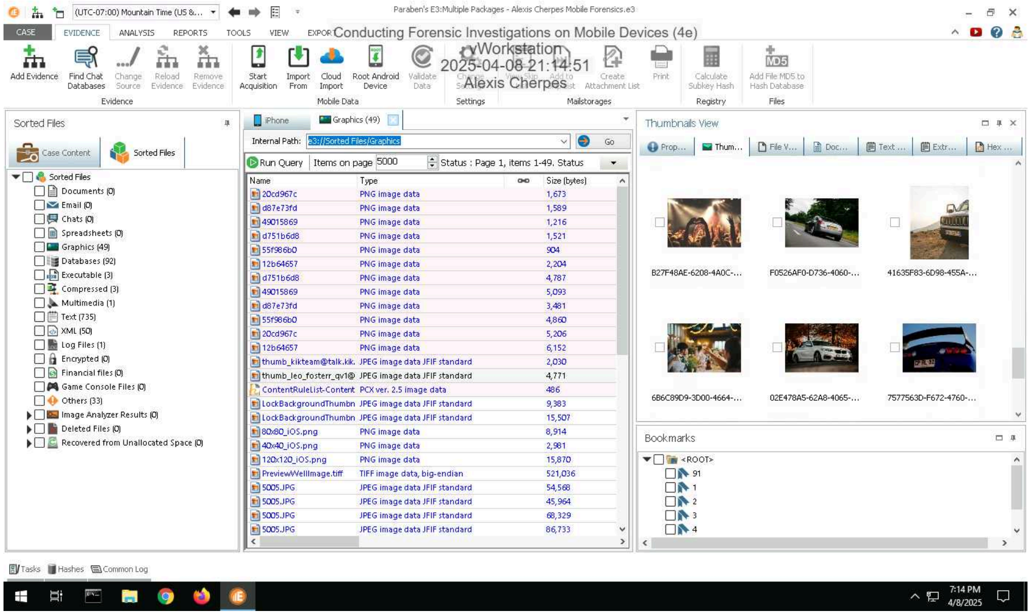
Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-04-08 21:09:25
Alexis Cherpes

Internal Path: e3://Alexis Cherpes Mobile Forensics/iPhone_Acquisition_08-12-2021_11-40-13/E3 data case/1/2/1249/1487/1488

Date Created	Note ID	Folder	Title	Full Text	URL
	8	Notes	List of liquors:	Binary data>>	
	9	Notes	Play Fewer Hands And Play Them Aggressively	Binary data>>	
	10	Notes	NFA V1834 known to police!	Binary data>>	
	11	Recently Deleted	New Note		
	13	Notes	657 BEE change to 7CAJ533	Binary data>>	
	14	Recently Deleted	JCG 2794 change to 212 WTE	Binary data>>	
	15	Notes	Meet *** in Green bay	Binary data>>	
	16	Recently Deleted	549 BDX change to 143 4084$	Binary data>>	
	17	Notes	Rockfold-Janesville-Madison		

Finished Total: 9

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



Internal Path: e3://Sorted Files/Graphics

Run Query Items on page 5000 Status : Page 1, items 1-49. Status

Name	Type	Size (bytes)
20cd967c	PNG image data	1,673
d87e73fd	PNG image data	1,589
49015869	PNG image data	1,216
d751b6d8	PNG image data	1,521
55f986b0	PNG image data	904
12b64657	PNG image data	2,204
d751b6d8	PNG image data	4,787
49015869	PNG image data	5,093
d87e73fd	PNG image data	3,481
55f986b0	PNG image data	4,860
20cd967c	PNG image data	5,206
12b64657	PNG image data	6,152
thumb_kikteam@talk.kik.	JPEG image data JFIF standard	2,030
thumb_leo_fosterr_qv1@	JPEG image data JFIF standard	4,771
ContentRuleList-Content	PCX ver. 2.5 image data	486
LockBackgroundThumbn	JPEG image data JFIF standard	9,383
LockBackgroundThumbn	JPEG image data JFIF standard	15,507
80x80_iOS.png	PNG image data	8,914
40x40_iOS.png	PNG image data	2,981
120x120_iOS.png	PNG image data	15,870
PreviewWellImage.tiff	TIFF image data, big-endian	521,036
5005.JPG	JPEG image data JFIF standard	54,568
5005.JPG	JPEG image data JFIF standard	45,964
5005.JPG	JPEG image data JFIF standard	68,329
5005.JPG	JPEG image data JFIF standard	86,733

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

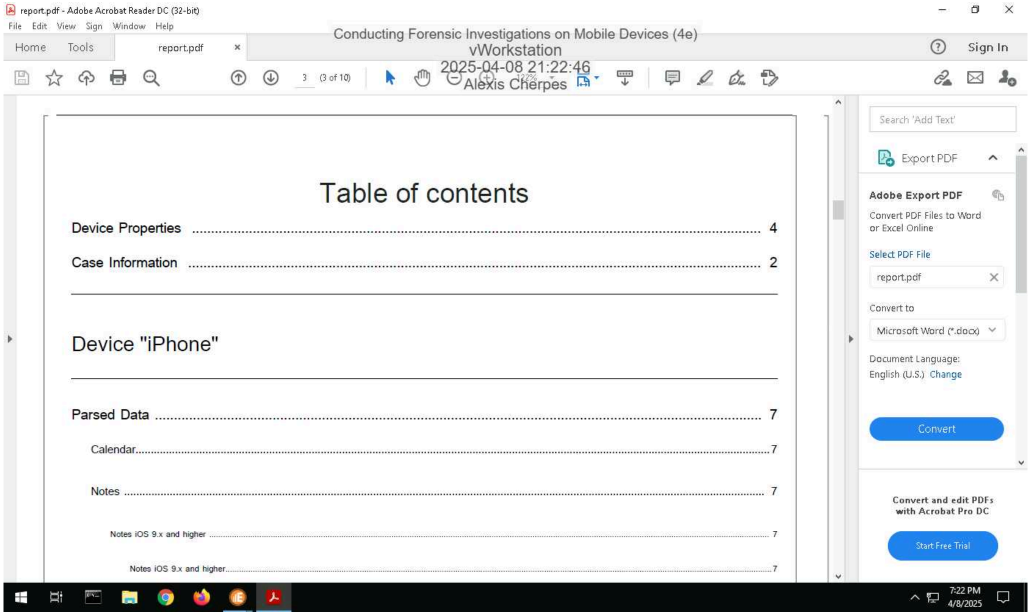


Table of contents

Device Properties 4

Case Information 2

Device "iPhone"

Parsed Data 7

Calendar........ 7

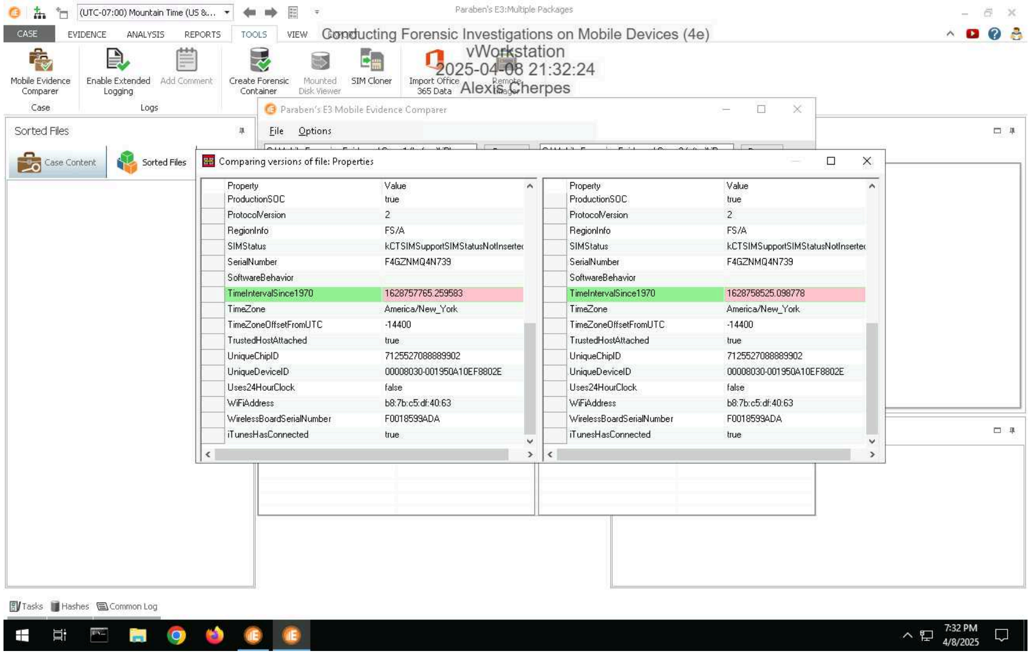
Notes 7

Notes iOS 9.x and higher 7

Notes iOS 9.x and higher........ 7

Part 2: Compare iOS Data Cases

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

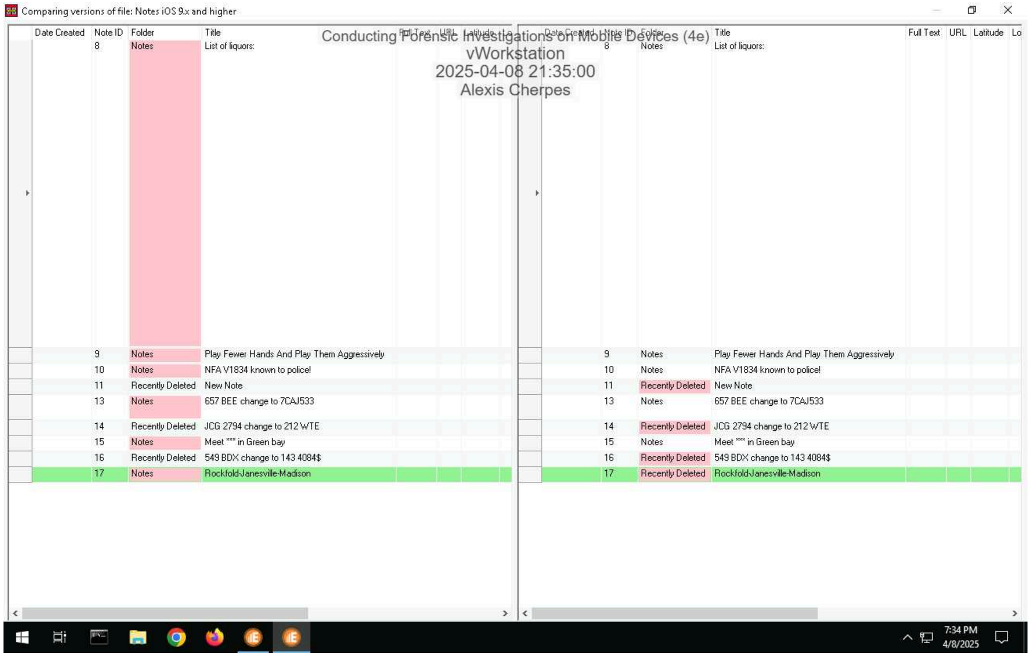


Comparing versions of file: Properties

Property	Value
ProductionSOC	true
ProtocolVersion	2
RegionInfo	FS/A
SIMStatus	kCTSIMSupportSIMStatusNotInsertec
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
iTunesHasConnected	true

Property	Value
ProductionSOC	true
ProtocolVersion	2
RegionInfo	FS/A
SIMStatus	kCTSIMSupportSIMStatusNotInsertec
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
iTunesHasConnected	true

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



Comparing versions of file: Notes iOS 9.x and higher

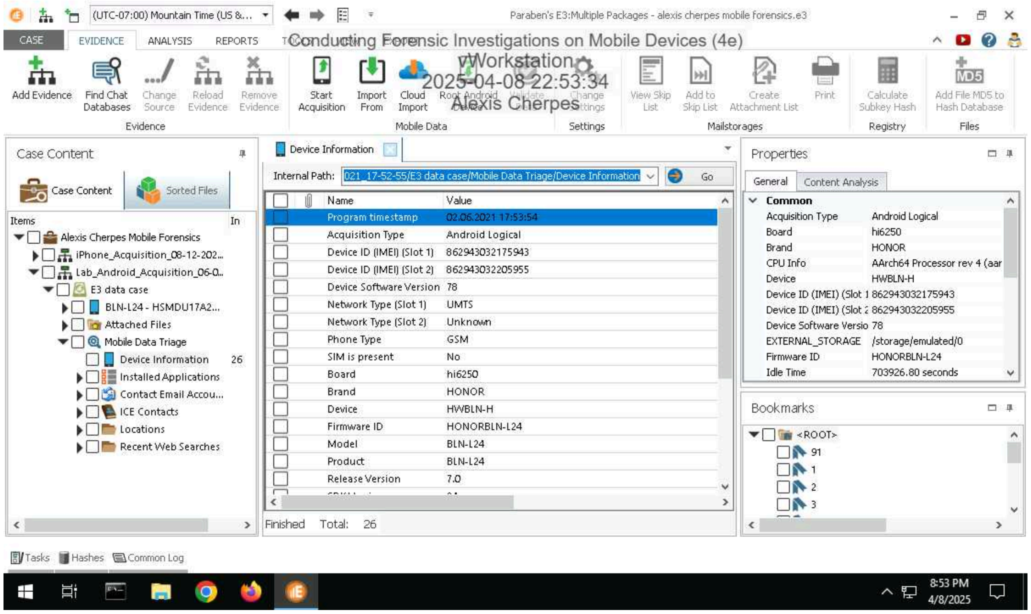
Date Created	Note ID	Folder	Title	Full Text	URL	Latitude
	8	Notes	List of liquors:			
	9	Notes	Play Fewer Hands And Play Them Aggressively			
	10	Notes	NFA V1834 known to police!			
	11	Recently Deleted	New Note			
	13	Notes	657 BEE change to 7CAJ533			
	14	Recently Deleted	JCG 2794 change to 212 WTE			
	15	Notes	Meet *** in Green bay			
	16	Recently Deleted	549 BDX change to 143 4084$			
	17	Notes	Rockfold-Janesville-Madison			

Date Created	Note ID	Folder	Title	Full Text	URL	Latitude	Lo
	8	Notes	List of liquors:				
	9	Notes	Play Fewer Hands And Play Them Aggressively				
	10	Notes	NFA V1834 known to police!				
	11	Recently Deleted	New Note				
	13	Notes	657 BEE change to 7CAJ533				
	14	Recently Deleted	JCG 2794 change to 212 WTE				
	15	Notes	Meet *** in Green bay				
	16	Recently Deleted	549 BDX change to 143 4084$				
	17	Recently Deleted	Rockfold-Janesville-Madison				

Section 2: Applied Learning

Part 1: Identify Forensic Evidence in Android User Data

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



Paraben's E3:Multiple Packages - alexis cherpes mobile forensics.e3

Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-04-08 22:53:34
Alexis Cherpes

Internal Path: 021_17-52-55/E3 data case/Mobile Data Triage/Device Information

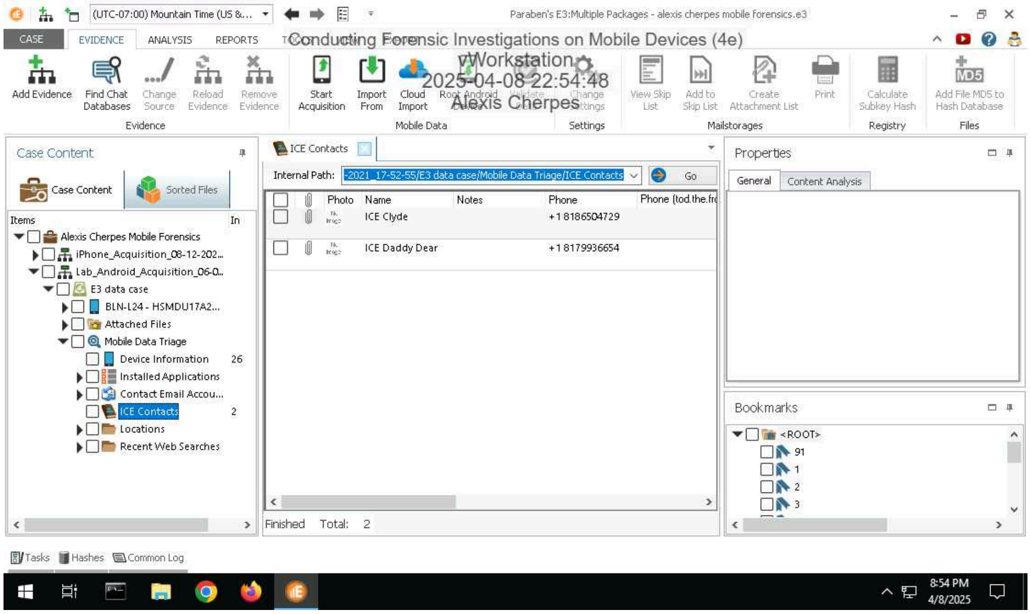
Name	Value
Program timestamp	02.06.2021 17:53:54
Acquisition Type	Android Logical
Device ID (IMEI) (Slot 1)	862943032175943
Device ID (IMEI) (Slot 2)	862943032205955
Device Software Version	78
Network Type (Slot 1)	UMTS
Network Type (Slot 2)	Unknown
Phone Type	GSM
SIM is present	No
Board	hi6250
Brand	HONOR
Device	HWBLN-H
Firmware ID	HONORBLN-L24
Model	BLN-L24
Product	BLN-L24
Release Version	7.0

Finished Total: 26

Common

Acquisition Type	Android Logical
Board	hi6250
Brand	HONOR
CPU Info	AArch64 Processor rev 4 (aar
Device	HWBLN-H
Device ID (IMEI) (Slot 1	862943032175943
Device ID (IMEI) (Slot 2	862943032205955
Device Software Versio	78
EXTERNAL_STORAGE	/storage/emulated/0
Firmware ID	HONORBLN-L24
Idle Time	703926.80 seconds

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



Paraben's E3:Multiple Packages - alexis cherpes mobile forensics.e3

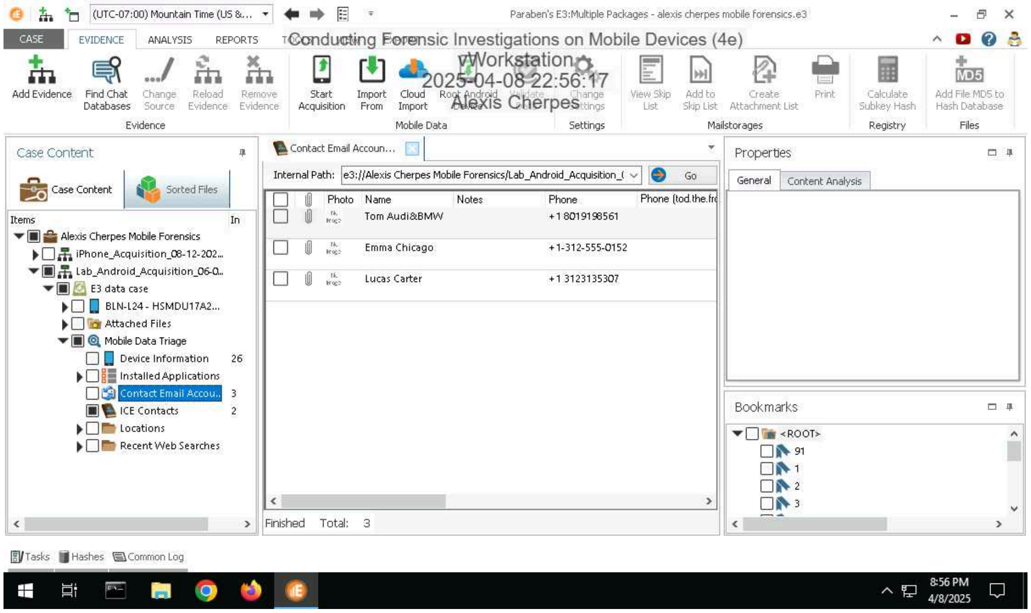
Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-04-08 22:54:48
Alexis Cherpes

Internal Path: -2021_17-52-55/E3 data case/Mobile Data Triage/ICE Contacts

Photo	Name	Notes	Phone	Phone (tod.the.fr
	ICE Clyde		+1 8186504729	
	ICE Daddy Dear		+1 8179936654	

Finished Total: 2

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



Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-04-08 22:56:17
Alexis Cherpes

Items / In
- Alexis Cherpes Mobile Forensics
  - iPhone_Acquisition_08-12-202...
  - Lab_Android_Acquisition_06-0...
    - E3 data case
      - BLN-L24 - HSMDU17A2...
      - Attached Files
      - Mobile Data Triage
        - Device Information 26
        - Installed Applications
        - Contact Email Accou... 3
        - ICE Contacts 2
        - Locations
        - Recent Web Searches

Contact Email Accoun...

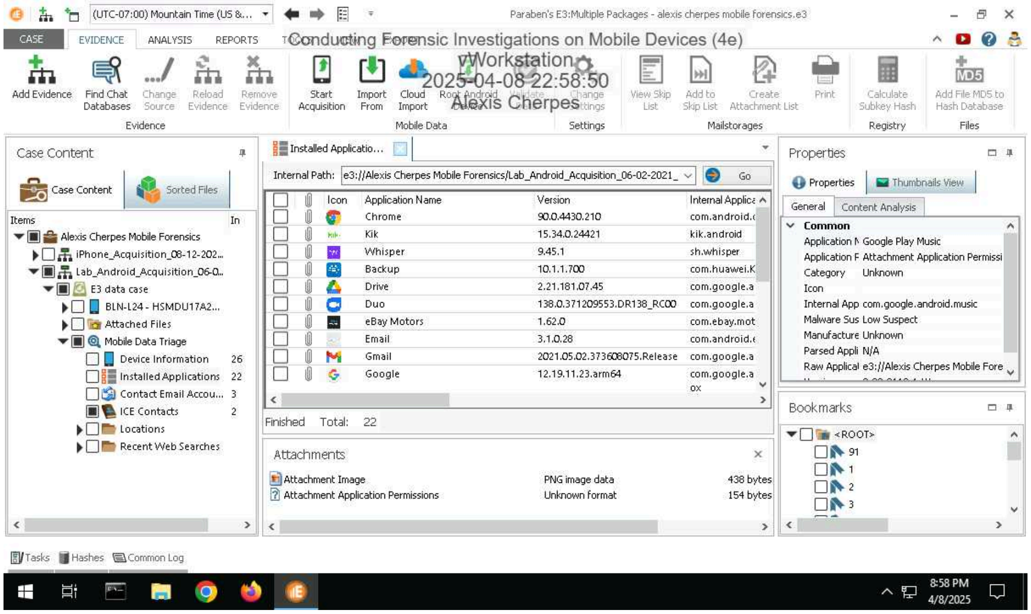
Internal Path: e3://Alexis Cherpes Mobile Forensics/Lab_Android_Acquisition_(Go

Photo	Name	Notes	Phone	Phone (tod.the.fr
	Tom Audi&BMW		+1 8019198561	
	Emma Chicago		+1-312-555-0152	
	Lucas Carter		+1 3123135307	

Finished Total: 3

<ROOT>
- 91
- 1
- 2
- 3

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



Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-04-08 22:58:50
Alexis Cherpes

Items / In
- Alexis Cherpes Mobile Forensics
  - iPhone_Acquisition_08-12-202...
  - Lab_Android_Acquisition_06-0...
    - E3 data case
      - BLN-L24 - HSMDU17A2...
      - Attached Files
      - Mobile Data Triage
        - Device Information 26
        - Installed Applications 22
        - Contact Email Accou... 3
        - ICE Contacts 2
        - Locations
        - Recent Web Searches

Installed Applicatio...

Internal Path: e3://Alexis Cherpes Mobile Forensics/Lab_Android_Acquisition_06-02-2021_ Go

Icon	Application Name	Version	Internal Applica
	Chrome	90.0.4430.210	com.android.(
	Kik	15.34.0.24421	kik.android
	Whisper	9.45.1	sh.whisper
	Backup	10.1.1.700	com.huawei.K
	Drive	2.21.181.07.45	com.google.a
	Duo	138.0.371209553.DR138_RC00	com.google.a
	eBay Motors	1.62.0	com.ebay.mot
	Email	3.1.0.28	com.android.(
	Gmail	2021.05.02.373608075.Release	com.google.a
	Google	12.19.11.23.arm64	com.google.a ox

Finished Total: 22

Attachments

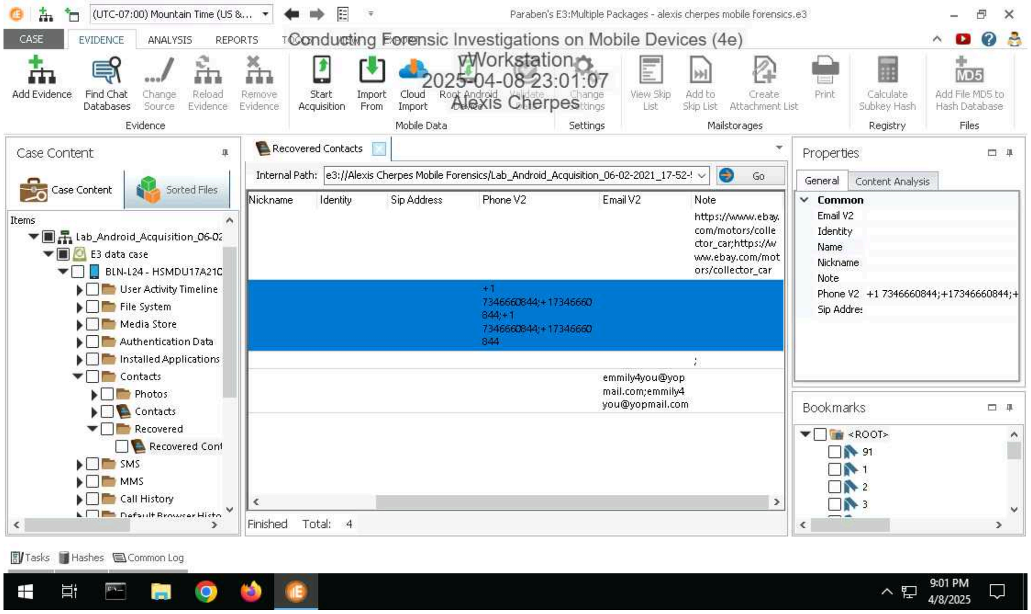
Attachment Image	PNG image data	438 bytes
Attachment Application Permissions	Unknown format	154 bytes

Common

Application N	Google Play Music
Application F	Attachment Application Permissi
Category	Unknown
Icon	
Internal App	com.google.android.music
Malware Sus	Low Suspect
Manufacture	Unknown
Parsed Appli	N/A
Raw Applical	e3://Alexis Cherpes Mobile Fore

<ROOT>
- 91
- 1
- 2
- 3

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



Internal Path: e3://Alexis Cherpes Mobile Forensics/Lab_Android_Acquisition_06-02-2021_17-52-!

Nickname	Identity	Sip Address	Phone V2	Email V2	Note
					https://www.ebay.com/motors/collector_car;https://www.ebay.com/motors/collector_car
			+1 7346660844;+17346660844;+1 7346660844;+17346660844		
					;
				emmily4you@yopmail.com;emmily4you@yopmail.com	

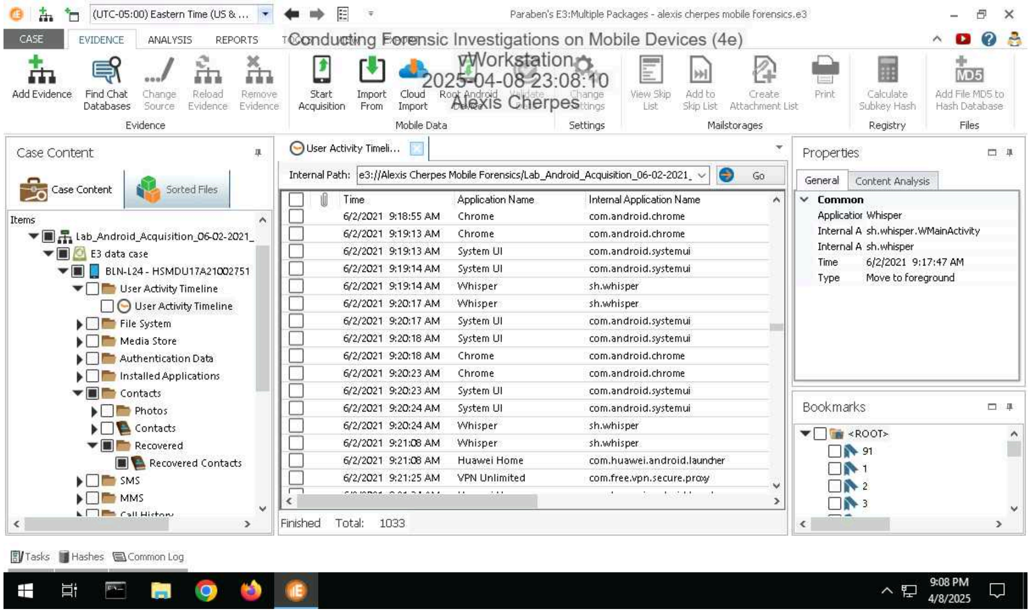
Finished Total: 4

Common

Email V2	
Identity	
Name	
Nickname	
Note	
Phone V2	+1 7346660844;+17346660844;+
Sip Addre:	

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**.



Internal Path: e3://Alexis Cherpes Mobile Forensics/Lab_Android_Acquisition_06-02-2021_

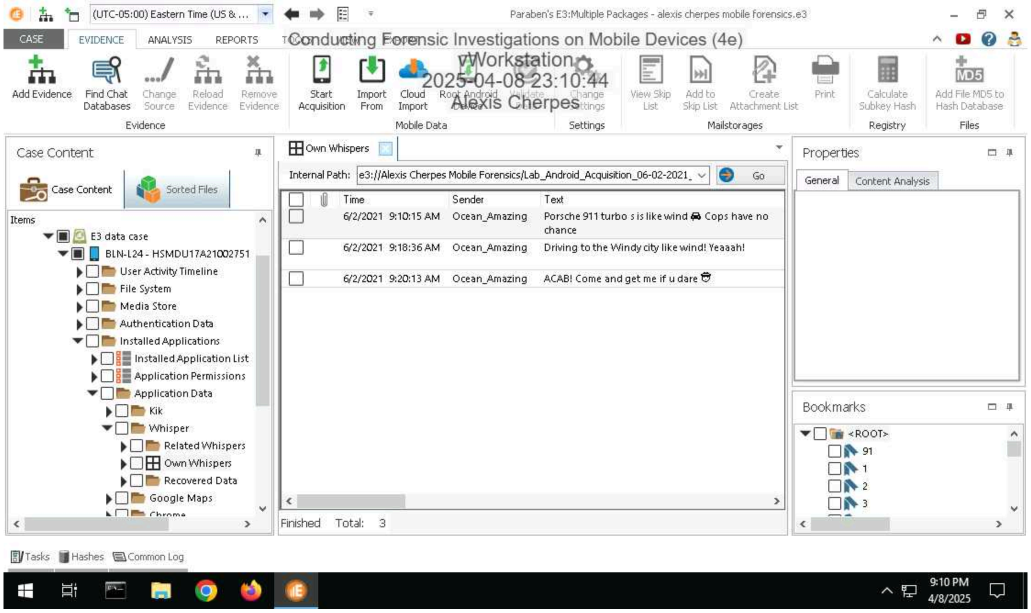
□	Time	Application Name	Internal Application Name
□	6/2/2021 9:18:55 AM	Chrome	com.android.chrome
□	6/2/2021 9:19:13 AM	Chrome	com.android.chrome
□	6/2/2021 9:19:13 AM	System UI	com.android.systemui
□	6/2/2021 9:19:14 AM	System UI	com.android.systemui
□	6/2/2021 9:19:14 AM	Whisper	sh.whisper
□	6/2/2021 9:20:17 AM	Whisper	sh.whisper
□	6/2/2021 9:20:17 AM	System UI	com.android.systemui
□	6/2/2021 9:20:18 AM	System UI	com.android.systemui
□	6/2/2021 9:20:18 AM	Chrome	com.android.chrome
□	6/2/2021 9:20:23 AM	Chrome	com.android.chrome
□	6/2/2021 9:20:23 AM	System UI	com.android.systemui
□	6/2/2021 9:20:24 AM	System UI	com.android.systemui
□	6/2/2021 9:20:24 AM	Whisper	sh.whisper
□	6/2/2021 9:21:08 AM	Whisper	sh.whisper
□	6/2/2021 9:21:08 AM	Huawei Home	com.huawei.android.launcher
□	6/2/2021 9:21:25 AM	VPN Unlimited	com.free.vpn.secure.proxy

Finished Total: 1033

Common

Applicatior	Whisper
Internal A	sh.whisper.WMainActivity
Internal A	sh.whisper
Time	6/2/2021 9:17:47 AM
Type	Move to foreground

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



Paraben's E3:Multiple Packages - alexis cherpes mobile forensics.e3

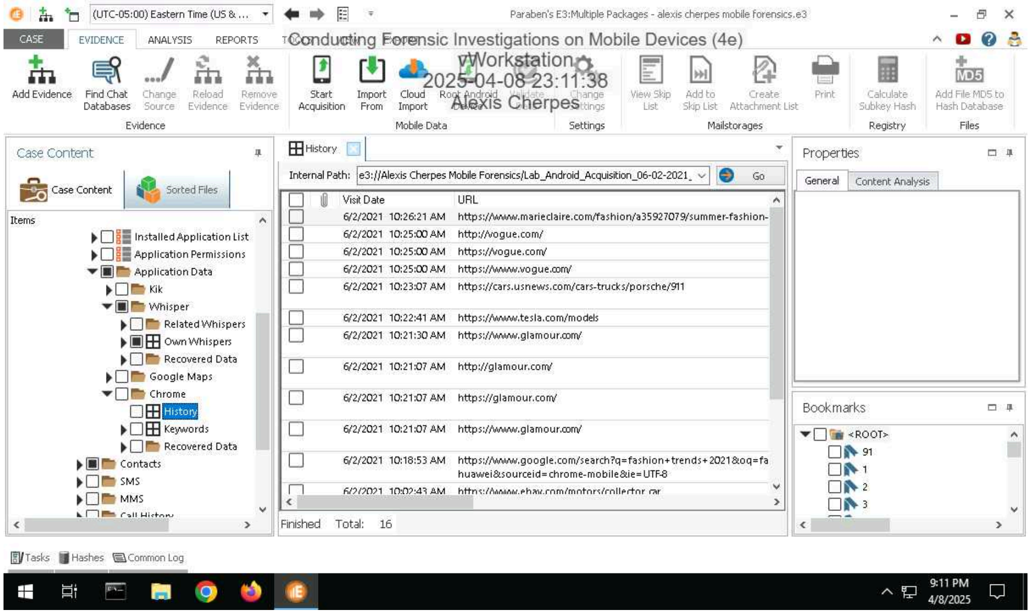
Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-04-08 23:10:44
Alexis Cherpes

Internal Path: e3://Alexis Cherpes Mobile Forensics/Lab_Android_Acquisition_06-02-2021_

☐	Time	Sender	Text
☐	6/2/2021 9:10:15 AM	Ocean_Amazing	Porsche 911 turbo s is like wind 🚗 Cops have no chance
☐	6/2/2021 9:18:36 AM	Ocean_Amazing	Driving to the Windy city like wind! Yeaaah!
☐	6/2/2021 9:20:13 AM	Ocean_Amazing	ACAB! Come and get me if u dare 🤠

Finished Total: 3

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



Paraben's E3:Multiple Packages - alexis cherpes mobile forensics.e3

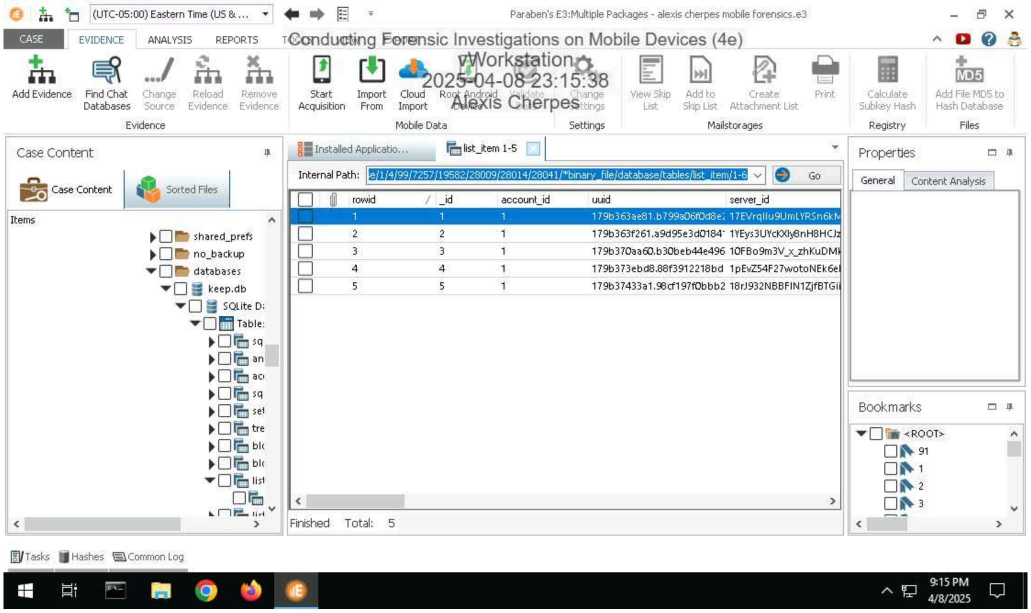
Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-04-08 23:11:38
Alexis Cherpes

Internal Path: e3://Alexis Cherpes Mobile Forensics/Lab_Android_Acquisition_06-02-2021_

☐	Visit Date	URL
☐	6/2/2021 10:26:21 AM	https://www.marieclaire.com/fashion/a35927079/summer-fashion-
☐	6/2/2021 10:25:00 AM	http://vogue.com/
☐	6/2/2021 10:25:00 AM	https://vogue.com/
☐	6/2/2021 10:25:00 AM	https://www.vogue.com/
☐	6/2/2021 10:23:07 AM	https://cars.usnews.com/cars-trucks/porsche/911
☐	6/2/2021 10:22:41 AM	https://www.tesla.com/models
☐	6/2/2021 10:21:30 AM	https://www.glamour.com/
☐	6/2/2021 10:21:07 AM	http://glamour.com/
☐	6/2/2021 10:21:07 AM	https://glamour.com/
☐	6/2/2021 10:21:07 AM	https://www.glamour.com/
☐	6/2/2021 10:18:53 AM	https://www.google.com/search?q=fashion+trends+2021&oq=fa huawei&sourceid=chrome-mobile&ie=UTF-8
☐	6/2/2021 10:02:43 AM	https://www.ebay.com/motors/collector car

Finished Total: 16

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



Paraben's E3:Multiple Packages - alexis cherpes mobile forensics.e3

Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-04-08 23:15:38
Alexis Cherpes

list_item 1-5

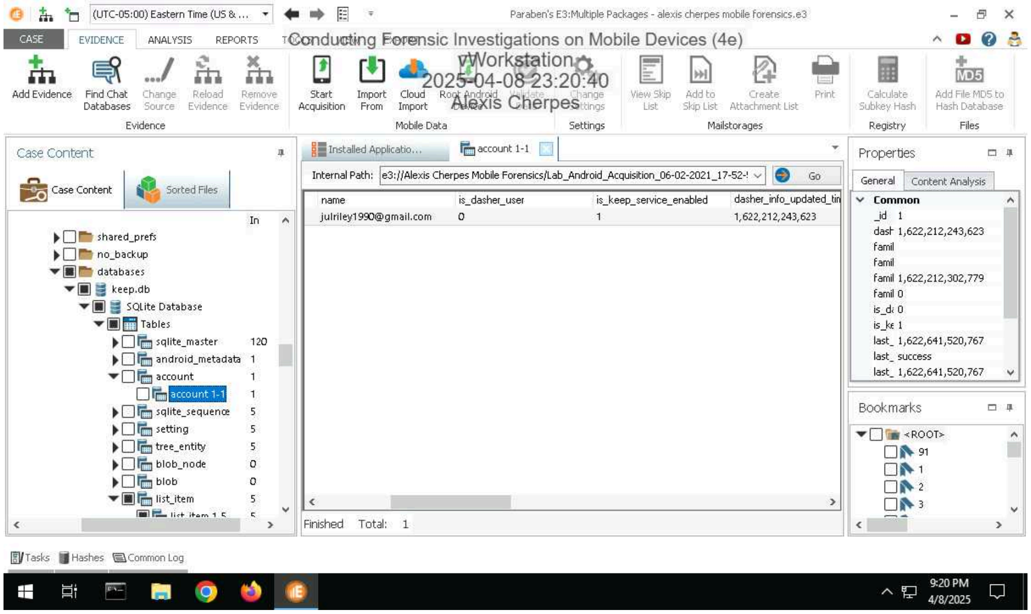
Internal Path: e/1/4/99/7257/19582/28009/28014/28041/*binary_file/database/tables/list_item/1-6

rowid	_id	account_id	uuid	server_id
1	1	1	179b363ae81.b799a06f0d8e	17EVrqIIu9UmLYRSn6kM
2	2	1	179b363f261.a9d95e3d0184	1YEys3UYcKXly8nH8HCJz
3	3	1	179b370aa60.b30beb44e496	10FBo9m3V_x_zhKuDMk
4	4	1	179b373ebd8.88f3912218bd	1pEvZ54F27wotoNEk6el
5	5	1	179b37433a1.98cf197f0bbb2	18rJ932NBBFIN1ZjfBTGi

Finished Total: 5

9:15 PM
4/8/2025

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



Paraben's E3:Multiple Packages - alexis cherpes mobile forensics.e3

Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-04-08 23:20:40
Alexis Cherpes

account 1-1

Internal Path: e3://Alexis Cherpes Mobile Forensics/Lab_Android_Acquisition_06-02-2021_17-52-!

name	is_dasher_user	is_keep_service_enabled	dasher_info_updated_tin
julriley1990@gmail.com	0	1	1,622,212,243,623

Finished Total: 1

Properties — Common

_id	1
dash	1,622,212,243,623
famil	
famil	
famil	1,622,212,302,779
famil	0
is_d	0
is_ke	1
last_	1,622,641,520,767
last_	success
last_	1,622,641,520,767

9:20 PM
4/8/2025

23. **Make a screen capture** showing the **Investigative Report's Table of Contents**.

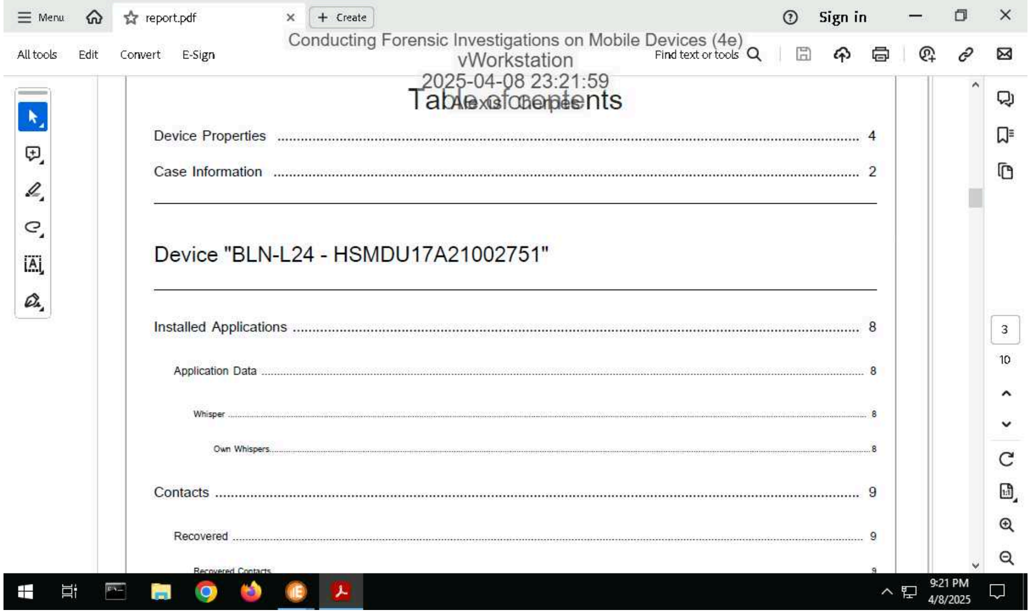


Table of contents

Device "BLN-L24 - HSMDU17A21002751"

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.

Best Practices: Maintain a detailed chain of custody.Use Licensed and reputable forensic tools for analysis.Verify the integrity of forensic images using hash.Document all steps taken.

Part 2: Draft a Forensic Report

Case Summary

The Madison Police Department is investigating an organized car theft operation involving two suspects known by the aliases Bonnie and Clyde. As part of the investigation, authorities have seized two smartphones—one iOS and one Android—belonging to the suspects. The digital forensics team has been assigned to examine the data extracted from these devices to uncover evidence connected to the car thefts.

Findings and Analysis

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 and the corresponding license plate number.Suspicious Activities: Car images with their licenses plate number gives strong indication of involvement of suspect into car theft cases.
Android- Device Identification: The Android device can be identified with the serial number of HSMDU17A21002751 and it is equipped with dual SIM capabilities. Ownership: The Android is associated to a Bonnie.Suspicious Activities: The Android device had installed applications such as Whisper which is an anonymous chatting app, and eBay Motor, which is commonly used for selling goods including stolen cars.

Conclusion

The forensic analysis of the seized Android and iPhone devices has revealed significant evidence implicating suspects with the code names of Bonnie and Clyde in an organization connected to car theft. The iPhone that was linked to Clyde had pictures of stolen cars with corresponding licenses plate numbers. The Android that was linked to Bonnie contained notes listing stolen cars and suspicious applications.