Conducting Forensic Investigations on Mobile Devices (4e)

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

Student:	Email:
Jake Simpson	jaksimps@iu.edu

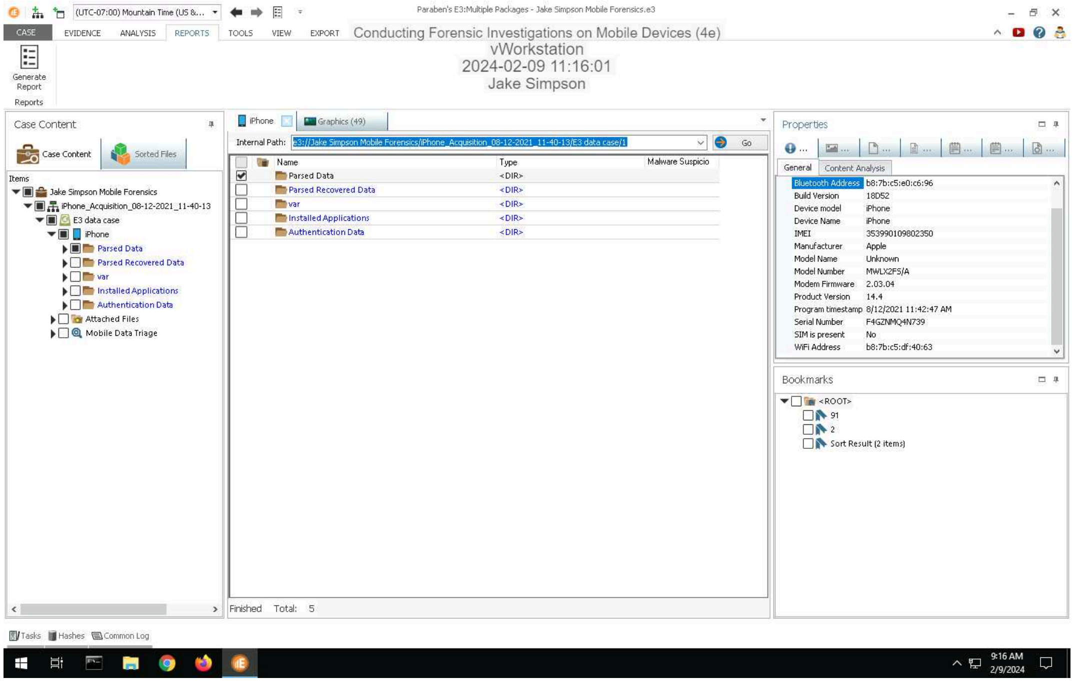
Time on Task:	Progress:
0 hours, 53 minutes	100%

Report Generated: Saturday, February 10, 2024 at 2:47 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**.

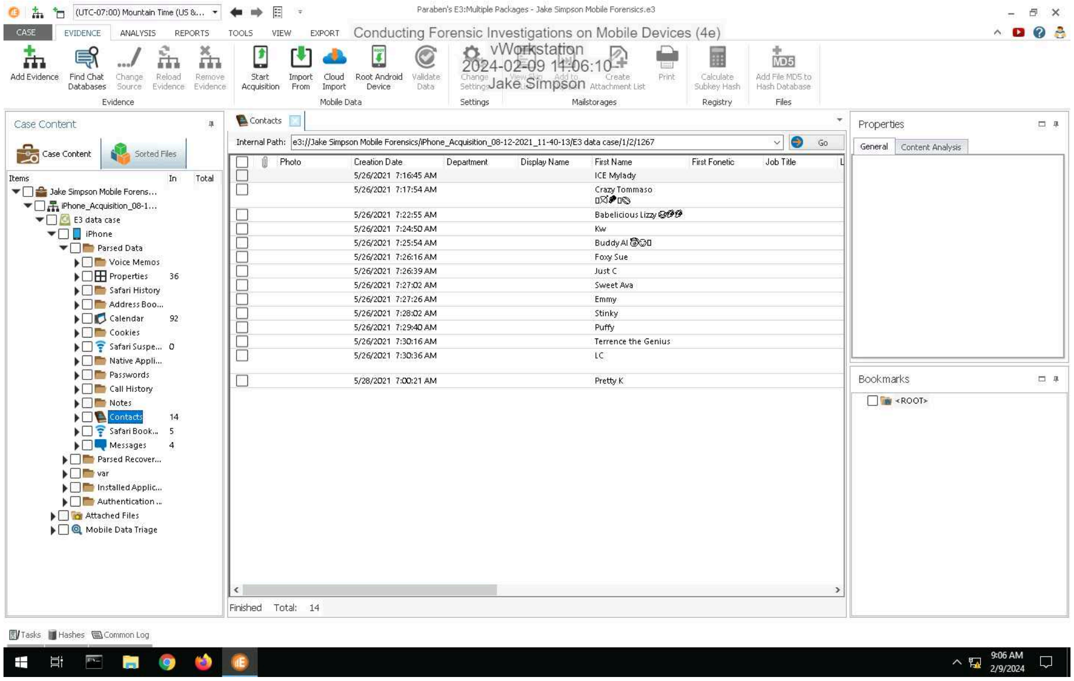


Internal Path: e3://Jake Simpson Mobile Forensics/iPhone_Acquisition_08-12-2021_11-40-13/E3 data case/1

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

Bluetooth Address	b8:7b:c5:e0:c6:96
Build Version	18D52
Device model	iPhone
Device Name	iPhone
IMEI	353990109802350
Manufacturer	Apple
Model Name	Unknown
Model Number	MWLX2FS/A
Modem Firmware	2.03.04
Product Version	14.4
Program timestamp	8/12/2021 11:42:47 AM
Serial Number	F4GZNMQ4N739
SIM is present	No
WiFi Address	b8:7b:c5:df:40:63

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

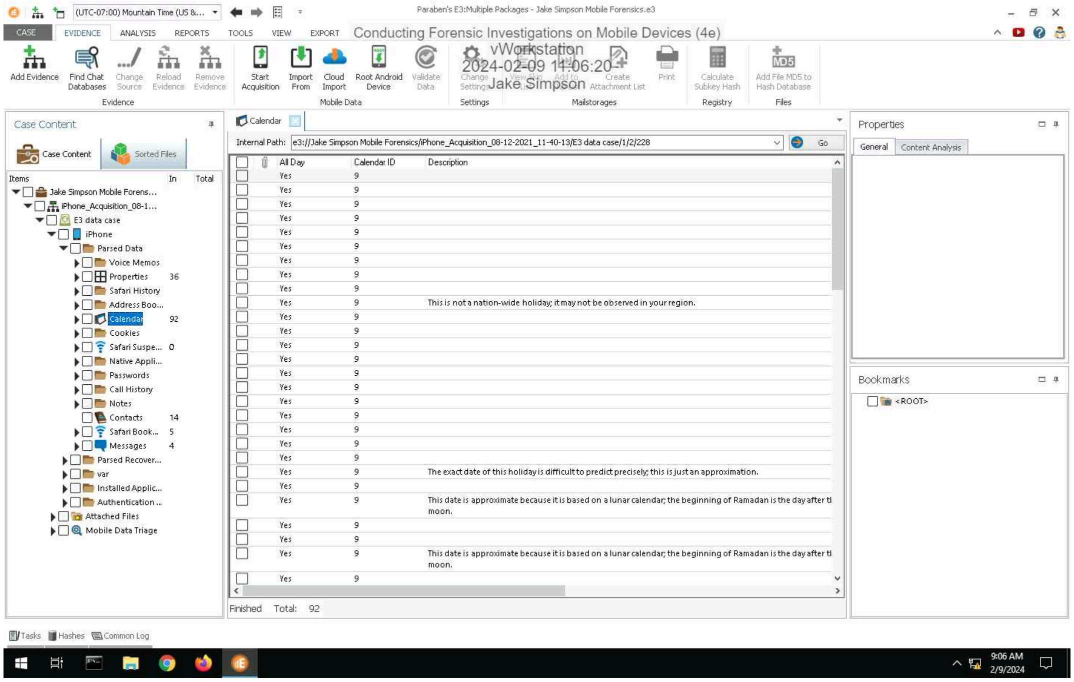


Internal Path: e3://Jake Simpson Mobile Forensics/iPhone_Acquisition_08-12-2021_11-40-13/E3 data case/1/2/1267

□	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**.

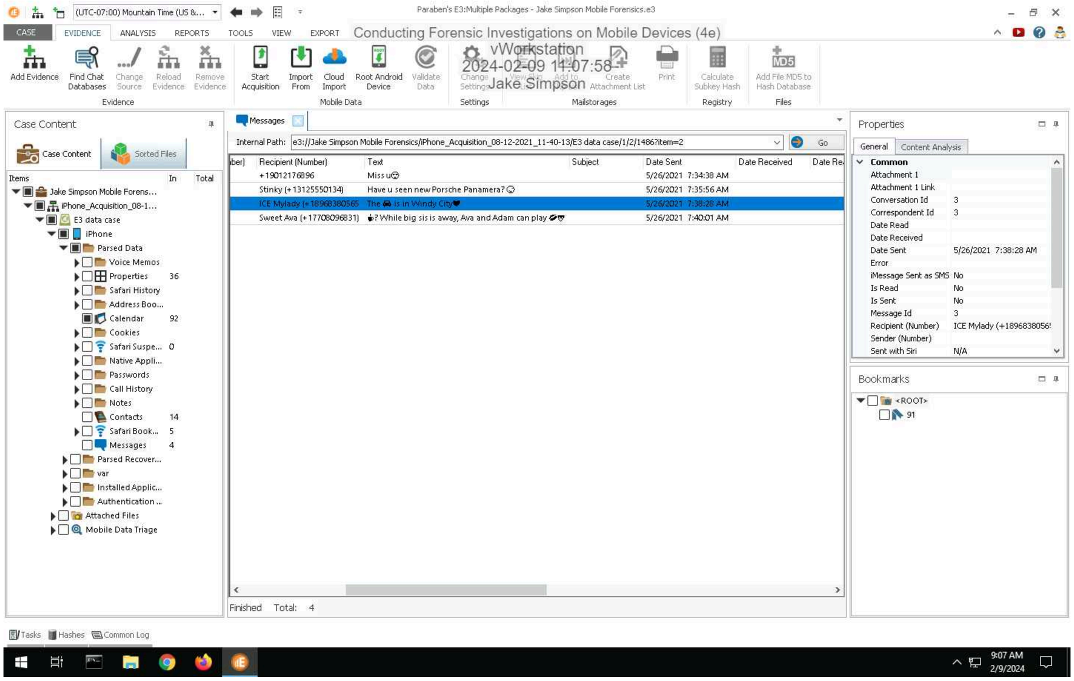


Internal Path: e3://Jake Simpson Mobile Forensics/iPhone_Acquisition_08-12-2021_11-40-13/E3 data case/1/2/228

□	All Day	Calendar ID	Description
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	This is not a nation-wide holiday; it may not be observed in your region.
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	
□	Yes	9	The exact date of this holiday is difficult to predict precisely; this is just an approximation.
□	Yes	9	
□	Yes	9	This date is approximate because it is based on a lunar calendar; the beginning of Ramadan is the day after tl moon.
□	Yes	9	
□	Yes	9	
□	Yes	9	This date is approximate because it is based on a lunar calendar; the beginning of Ramadan is the day after tl moon.
□	Yes	9	

Finished Total: 92

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



Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2024-02-09 11:07:58
Jake Simpson

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

ber)	Recipient (Number)	Text	Subject	Date Sent	Date Received	Date Re
	+19012176896	Miss u😍		5/26/2021 7:34:38 AM		
	Stinky (+13125550134)	Have u seen new Porsche Panamera? ☺		5/26/2021 7:35:56 AM		
	ICE Mylady (+18968380565	The 🚗 is in Windy City🖤		5/26/2021 7:38:28 AM		
	Sweet Ava (+17708096831)	🍑? While big sis is away, Ava and Adam can play 💋😈		5/26/2021 7:40:01 AM		

Finished Total: 4

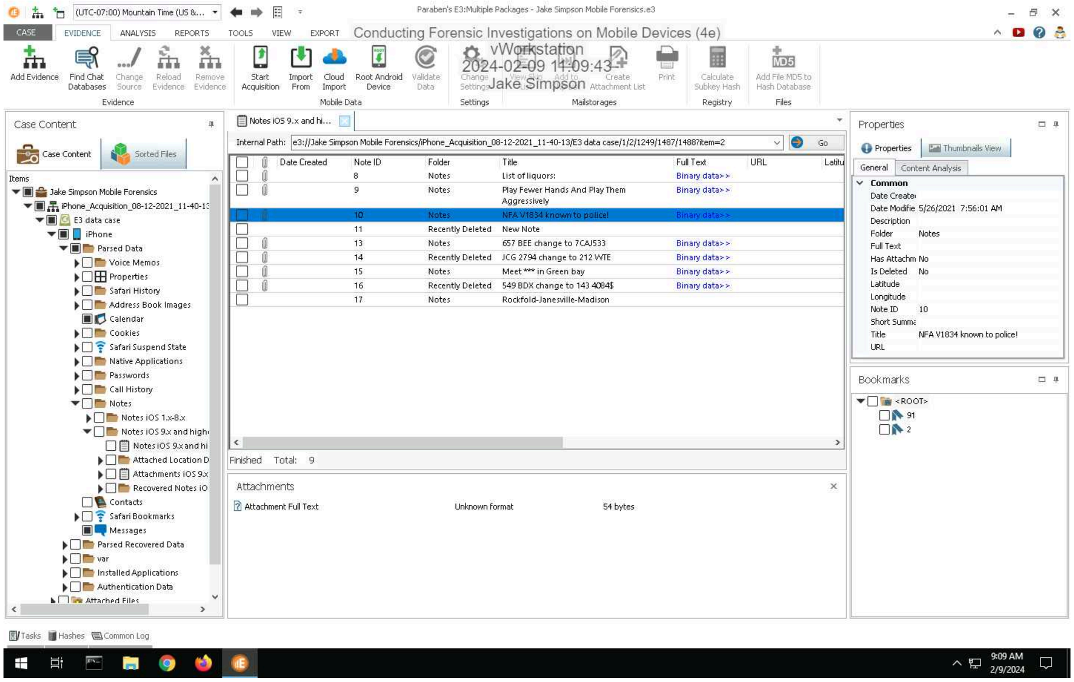
Items	In	Total
Jake Simpson Mobile Forens...		
iPhone_Acquisition_08-1...		
E3 data case		
iPhone		
Parsed Data		
Voice Memos		
Properties	36	
Safari History		
Address Boo...		
Calendar	92	
Cookies		
Safari Suspe...	0	
Native Appli...		
Passwords		
Call History		
Notes		
Contacts	14	
Safari Book...	5	
Messages	4	
Parsed Recover...		
var		
Installed Applic...		
Authentication ...		
Attached Files		
Mobile Data Triage		

General | Content Analysis

Common	
Attachment 1	
Attachment 1 Link	
Conversation Id	3
Correspondent Id	3
Date Read	
Date Received	
Date Sent	5/26/2021 7:38:28 AM
Error	
iMessage Sent as SMS	No
Is Read	No
Is Sent	No
Message Id	3
Recipient (Number)	ICE Mylady (+1896838056!
Sender (Number)	
Sent with Siri	N/A

<ROOT>
91

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



Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2024-02-09 11:09:43
Jake Simpson

Internal Path: e3://Jake Simpson Mobile Forensics/iPhone_Acquisition_08-12-2021_11-40-13/E3 data case/1/2/1249/1487/1488?item=2

Date Created	Note ID	Folder	Title	Full Text	URL	Latitu
	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

Attachments

Attachment Full Text	Unknown format	54 bytes

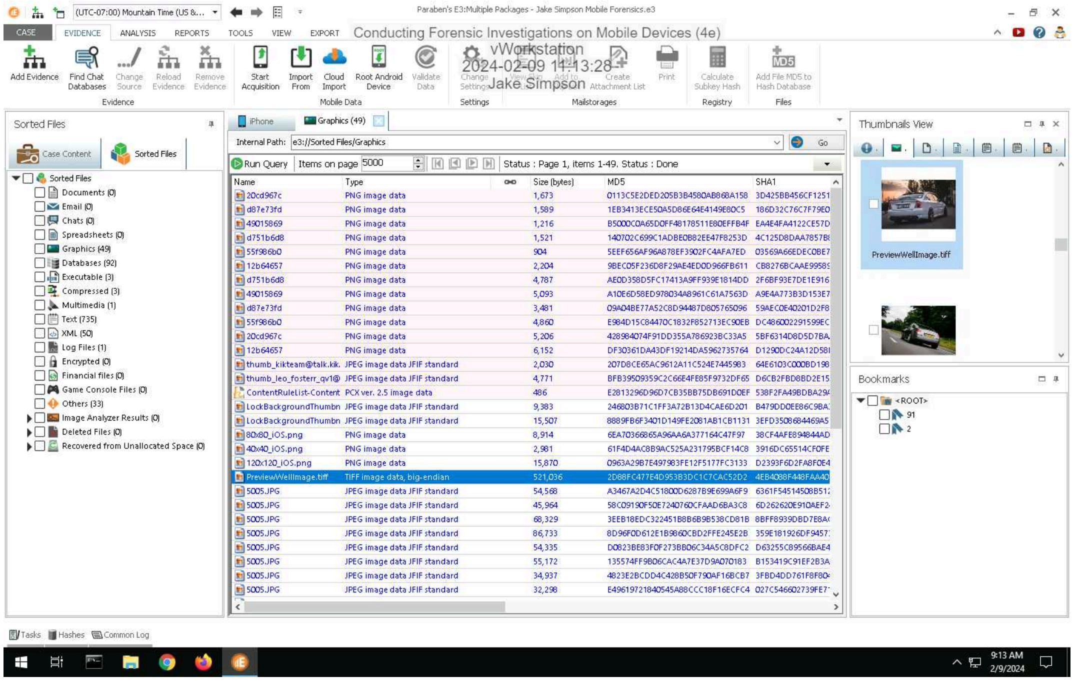
Items
Jake Simpson Mobile Forensics
iPhone_Acquisition_08-12-2021_11-40-13
E3 data case
iPhone
Parsed Data
Voice Memos
Properties
Safari History
Address Book Images
Calendar
Cookies
Safari Suspend State
Native Applications
Passwords
Call History
Notes
Notes iOS 1.x-8.x
Notes iOS 9.x and high
Notes iOS 9.x and hi
Attached Location D
Attachments iOS 9.x
Recovered Notes iO
Contacts
Safari Bookmarks
Messages
Parsed Recovered Data
var
Installed Applications
Authentication Data
Attached Files

General | Content Analysis

Common	
Date Create	
Date Modifie	5/26/2021 7:56:01 AM
Description	
Folder	Notes
Full Text	
Has Attachm	No
Is Deleted	No
Latitude	
Longitude	
Note ID	10
Short Summa	
Title	NFA V1834 known to police!
URL	

<ROOT>
91
2

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



Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2024-02-09 11:13:28
Jake Simpson

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)

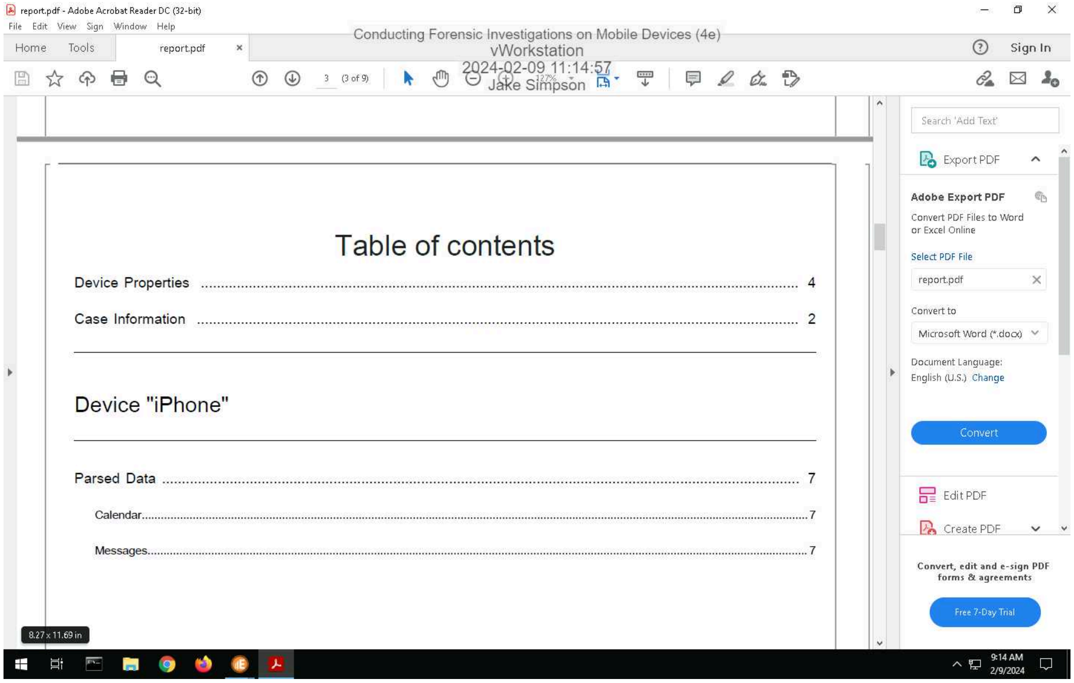
Internal Path: e3://Sorted Files/Graphics

Items on page 5000

Status : Page 1, items 1-49. Status : Done

Name	Type	Size (bytes)	MD5	SHA1
20cd967c	PNG image data	1,673	0113C5E2DED205B3B4580AB868A158	3D425BB456CF1251
d87e73fd	PNG image data	1,589	1EB3413ECE50A5D86E64E4149E80C5	186D32C76C7F79E0
49015869	PNG image data	1,216	B5000C0A65D0FF48178511E80EFFB4F	EA4E4FA4122CE57D
d751b6d8	PNG image data	1,521	140702C699C1ADBE0B82EE47F8253D	4C125D8DAA7857B
55f986b0	PNG image data	904	5EEF656AF96A878EF3902FC4AFA7ED	03569A66EDEC0BE7
12b64657	PNG image data	2,204	9BEC05F236D8F29AE4ED0D966FB611	CB8276BCAAE9958
d751b6d8	PNG image data	4,787	AE0D358D5FC17413A9FF939E1814DD	2F6BF93E7DE1E916
49015869	PNG image data	5,093	A10E6D58ED978034A8961C61A7563D	A9E4A773B3D153E7
d87e73fd	PNG image data	3,481	09A04BE77A52C8D94487D805765096	59AEC0E40201D2F8
55f986b0	PNG image data	4,860	E984D15C84470C1832F852713EC90EB	DC48600229159 9EC
20cd967c	PNG image data	5,206	428984074F91DD355A786923BC33A5	5BF6314D8D5D7BA
12b64657	PNG image data	6,152	DF30361DA43DF19214DA5962735764	D1290DC24A12D58
thumb_kikteam@talk.kik.	JPEG image data JFIF standard	2,030	207D8CE65AC9612A11C524E7445983	64E6103C000BD198
thumb_leo_fosterr_qv1@	JPEG image data JFIF standard	4,771	BFB39509359C2C66E4FE85F9732DF65	D6CB2FBD8BD2E15
ContentRuleList-Content	PCX ver. 2.5 image data	486	E2813296D96D7CB35BB75DB691D0EF	538F2FA49BDBA29
LockBackgroundThumbn	JPEG image data JFIF standard	9,383	246803B71C1FF3A72B13D4CAE6D201	B479DD0EE86C9BA
LockBackgroundThumbn	JPEG image data JFIF standard	15,507	8889FB6F3401D149FE2081AB1CB1131	3EFD3508684469A5
80x80_iOS.png	PNG image data	8,914	6EA70366865A96AA6A377164C47F97	38CF4AFE894844AD
40x40_iOS.png	PNG image data	2,981	61F4D4AC8B9AC525A231795BCF14C8	3916DC65514CF0FE
120x120_iOS.png	PNG image data	15,870	0963A29B7E497983FE12F5177FC3133	D2393F6D2FA8F0E4
PreviewWellImage.tiff	TIFF image data, big-endian	521,036	2D88FC477E4D953B3DC1C7CAC52D2	4EB4088F448FAA40
5005.JPG	JPEG image data JFIF standard	54,568	A3467A2D4C51800D6287B9E699A6F9	6361F54514508B51
5005.JPG	JPEG image data JFIF standard	45,964	58C09190F50E724076OCFAAD6BA3C8	6D262620E910AEF2
5005.JPG	JPEG image data JFIF standard	68,329	3EEB18EDC322451B8B6B9B538CD81B	8BFF8939DBD7E8A
5005.JPG	JPEG image data JFIF standard	86,733	8D96F0D612E1B9860CBD2FFE245E2B	359E181926DF9457
5005.JPG	JPEG image data JFIF standard	54,335	D0823BE83F0F273BB06C34A5C8DFC2	D63255C89566BAE4
5005.JPG	JPEG image data JFIF standard	55,172	135574FF9B06CAC4A7E37D9A070183	B153419C91EF2B3A
5005.JPG	JPEG image data JFIF standard	34,937	4823E2BCDD4C428B50F790AF16BCB7	3FBD4DD761F8F80
5005.JPG	JPEG image data JFIF standard	32,298	E49619721840545A88CCC18F16ECFC4	027C546602739FE7

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



Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2024-02-09 11:14:57
Jake Simpson

Table of contents

Device Properties 4

Case Information 2

Device "iPhone"

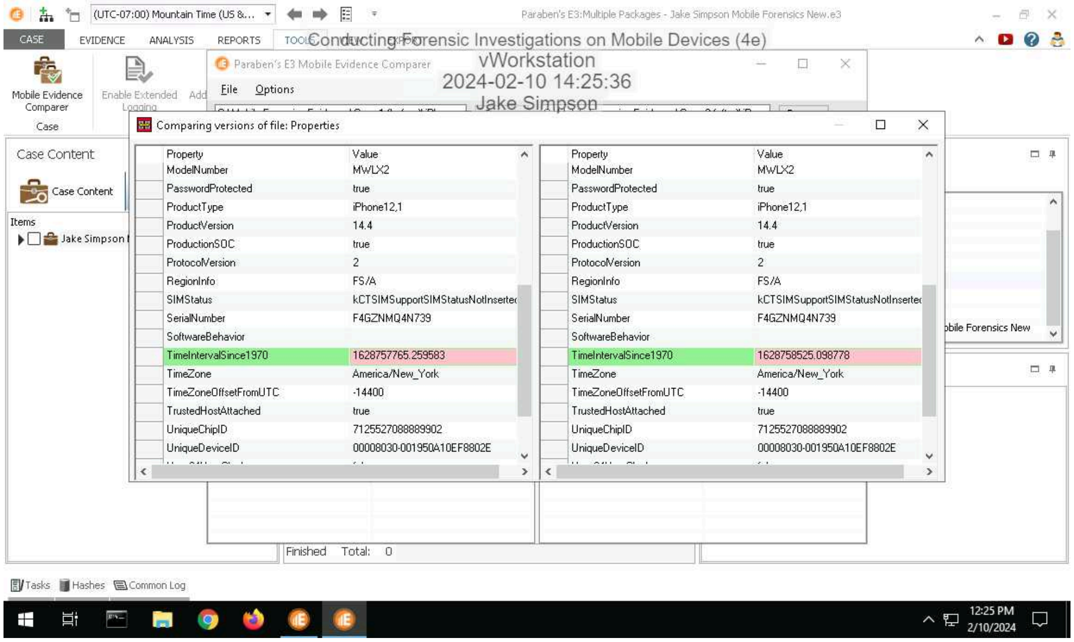
Parsed Data 7

Calendar........ 7

Messages........ 7

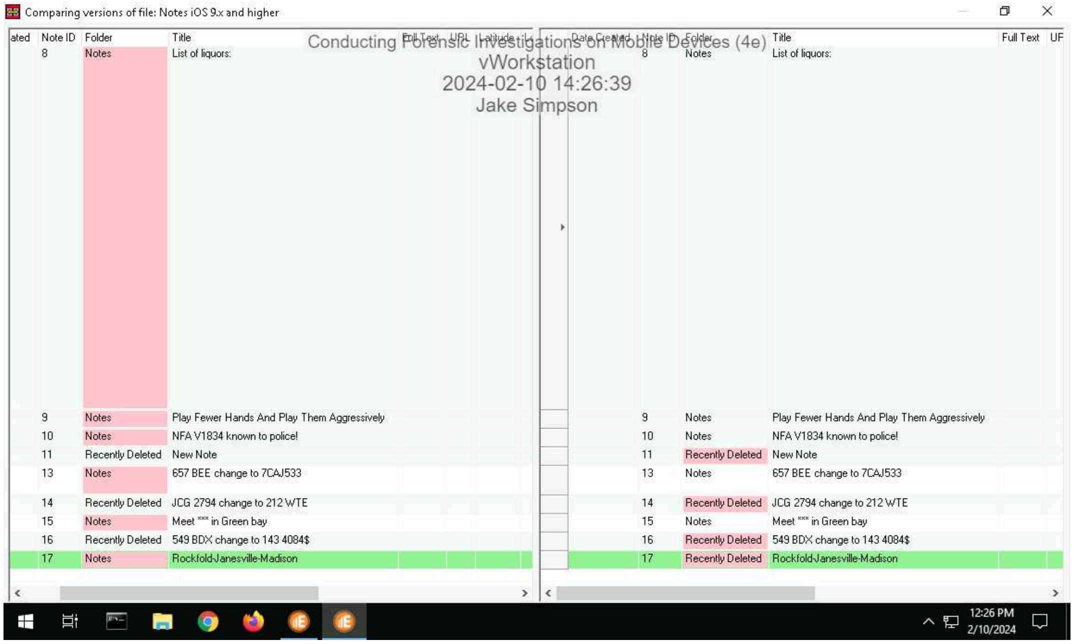
Part 2: Compare iOS Data Cases

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



Property	Value	Property	Value
ModelNumber	MWLX2	ModelNumber	MWLX2
PasswordProtected	true	PasswordProtected	true
ProductType	iPhone12,1	ProductType	iPhone12,1
ProductVersion	14.4	ProductVersion	14.4
ProductionSOC	true	ProductionSOC	true
ProtocolVersion	2	ProtocolVersion	2
RegionInfo	FS/A	RegionInfo	FS/A
SIMStatus	kCTSIMSupportSIMStatusNotInserted	SIMStatus	kCTSIMSupportSIMStatusNotInserted
SerialNumber	F4GZNMQ4N739	SerialNumber	F4GZNMQ4N739
SoftwareBehavior		SoftwareBehavior	
TimeIntervalSince1970	1628757765.259583	TimeIntervalSince1970	1628758525.098778
TimeZone	America/New_York	TimeZone	America/New_York
TimeZoneOffsetFromUTC	-14400	TimeZoneOffsetFromUTC	-14400
TrustedHostAttached	true	TrustedHostAttached	true
UniqueChipID	7125527088889902	UniqueChipID	7125527088889902
UniqueDeviceID	00008030-001950A10EF8802E	UniqueDeviceID	00008030-001950A10EF8802E

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


Comparing versions of file: Notes iOS 9.x and higher
Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2024-02-10 14:26:39
Jake Simpson
12:26 PM
2/10/2024

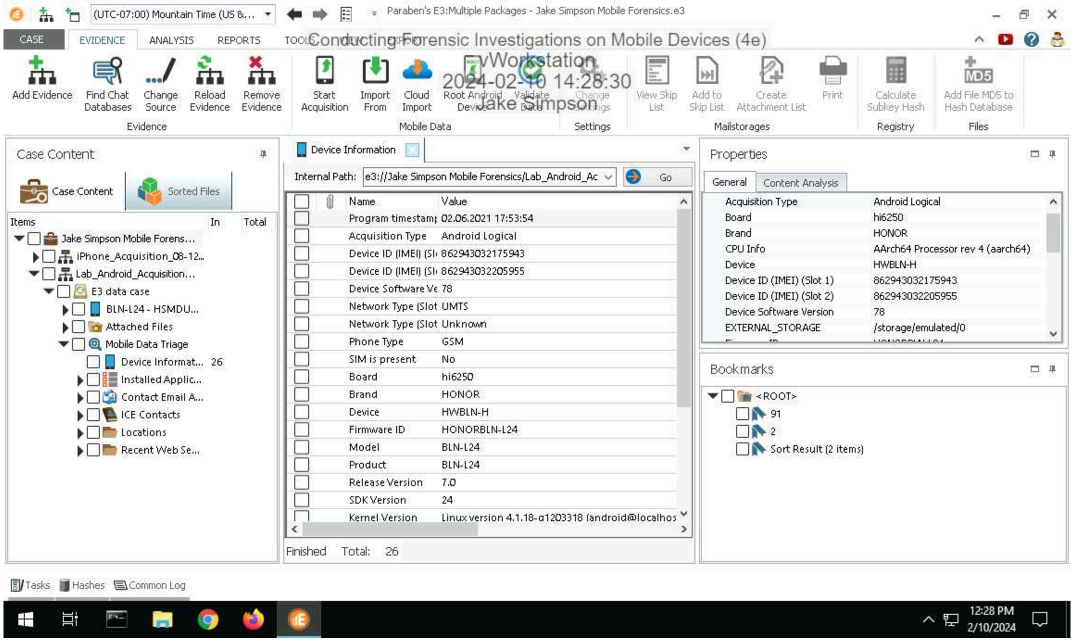
ated	Note ID	Folder	Title	Full Text	URL	Latitude
	8	Notes	List of liquors:			
	9	Notes	Play Fewer Hands And Play Them Aggressively			
	10	Notes	NFA V1834 known to police!			
	11	Recently Deleted	New Note			
	13	Notes	657 BEE change to 7CAJ533			
	14	Recently Deleted	JCG 2794 change to 212 WTE			
	15	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	UF
	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 - Jake Simpson Mobile Forensics.e3

Internal Path: e3://Jake Simpson Mobile Forensics/Lab_Android_Ac

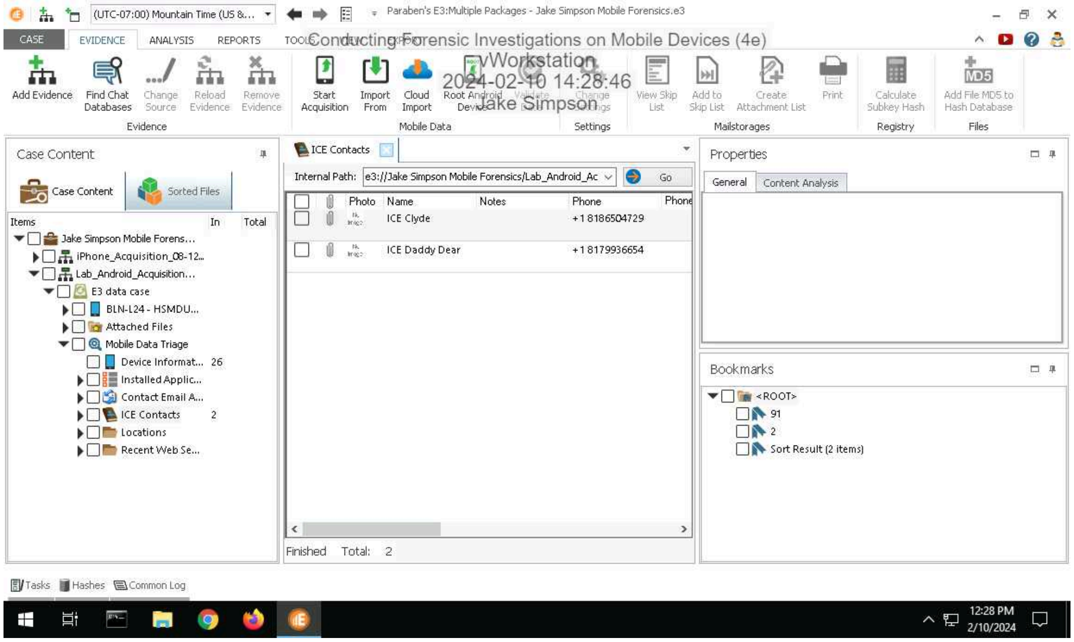
Name	Value
Program timestamp	02.06.2021 17:53:54
Acquisition Type	Android Logical
Device ID (IMEI) (Sl	862943032175943
Device ID (IMEI) (Sl	862943032205955
Device Software Ve	78
Network Type (Slot	UMTS
Network Type (Slot	Unknown
Phone Type	GSM
SIM is present	No
Board	hi6250
Brand	HONOR
Device	HWBLN-H
Firmware ID	HONORBLN-L24
Model	BLN-L24
Product	BLN-L24
Release Version	7.0
SDK Version	24
Kernel Version	Linux version 4.1.18-g1203318 (android@localhos

Finished Total: 26

Properties

Acquisition Type	Android Logical
Board	hi6250
Brand	HONOR
CPU Info	AArch64 Processor rev 4 (aarch64)
Device	HWBLN-H
Device ID (IMEI) (Slot 1)	862943032175943
Device ID (IMEI) (Slot 2)	862943032205955
Device Software Version	78
EXTERNAL_STORAGE	/storage/emulated/0

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



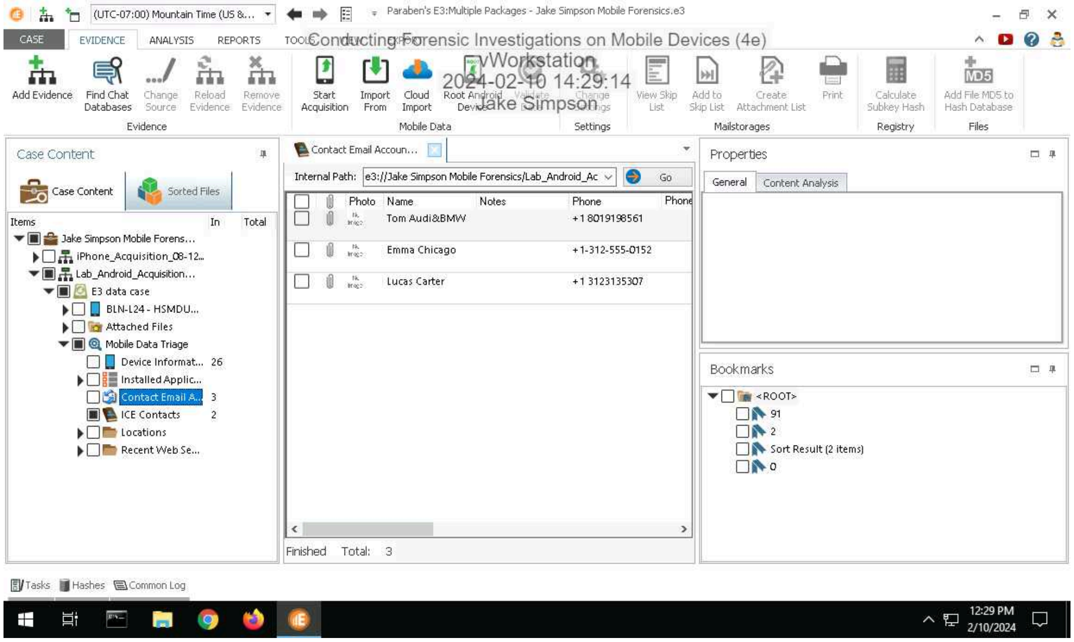
Paraben's E3:Multiple Packages - Jake Simpson Mobile Forensics.e3

Internal Path: e3://Jake Simpson Mobile Forensics/Lab_Android_Ac

Photo	Name	Notes	Phone	Phone
No image	ICE Clyde		+1 8186504729	
No image	ICE Daddy Dear		+1 8179936654	

Finished Total: 2

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



Items | In | Total
- Jake Simpson Mobile Forens...
  - iPhone_Acquisition_08-12...
  - Lab_Android_Acquisition...
    - E3 data case
      - BLN-L24 - HSMDU...
      - Attached Files
      - Mobile Data Triage
        - Device Informat... 26
        - Installed Applic...
        - Contact Email A... 3
        - ICE Contacts 2
        - Locations
        - Recent Web Se...

Contact Email Accoun...

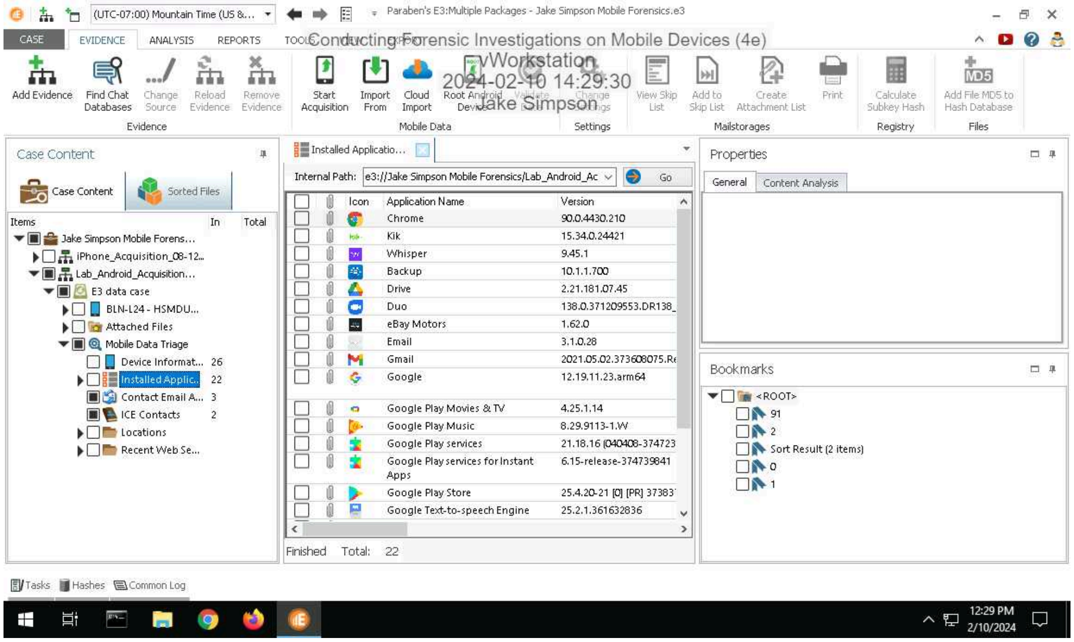
Internal Path: e3://Jake Simpson Mobile Forensics/Lab_Android_Ac

Photo	Name	Notes	Phone	Phone
No Image	Tom Audi&BMW		+1 8019198561	
No Image	Emma Chicago		+1-312-555-0152	
No Image	Lucas Carter		+1 3123135307	

Finished Total: 3

Bookmarks:
- <ROOT>
  - 91
  - 2
  - Sort Result (2 items)
  - 0

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



Items | In | Total
- Jake Simpson Mobile Forens...
  - iPhone_Acquisition_08-12...
  - Lab_Android_Acquisition...
    - E3 data case
      - BLN-L24 - HSMDU...
      - Attached Files
      - Mobile Data Triage
        - Device Informat... 26
        - Installed Applic... 22
        - Contact Email A... 3
        - ICE Contacts 2
        - Locations
        - Recent Web Se...

Installed Applicatio...

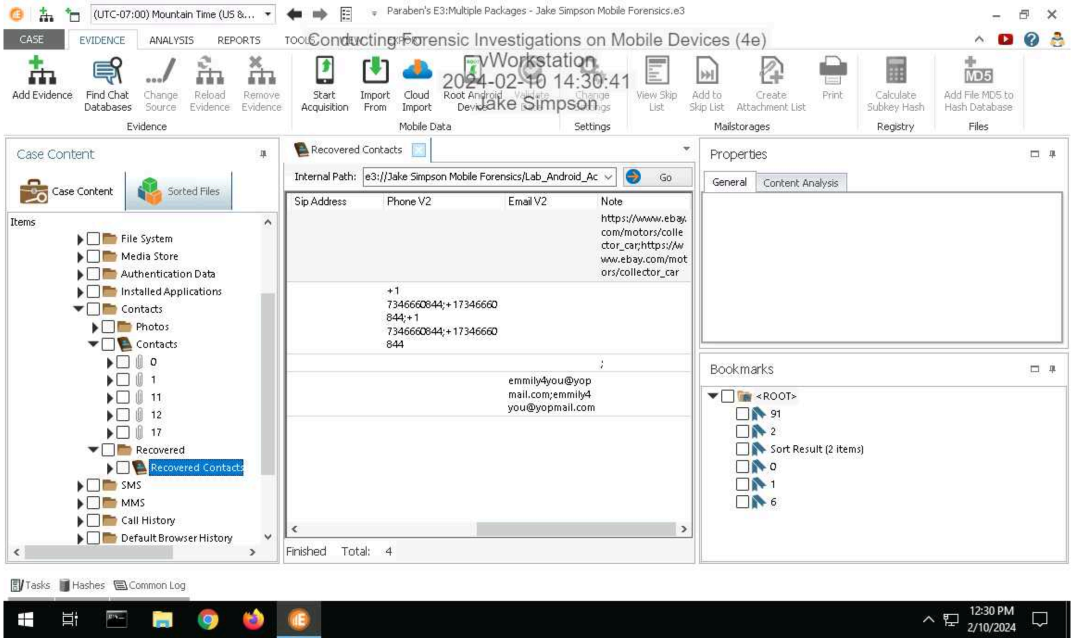
Internal Path: e3://Jake Simpson Mobile Forensics/Lab_Android_Ac

Application Name	Version
Chrome	90.0.4430.210
Kik	15.34.0.24421
Whisper	9.45.1
Backup	10.1.1.700
Drive	2.21.181.07.45
Duo	138.0.371209553.DR138_
eBay Motors	1.62.0
Email	3.1.0.28
Gmail	2021.05.02.373608075.Re
Google	12.19.11.23.arm64
Google Play Movies & TV	4.25.1.14
Google Play Music	8.29.9113-1.W
Google Play services	21.18.16 (040408-374723
Google Play services for Instant Apps	6.15-release-374739841
Google Play Store	25.4.20-21 [0] [PR] 37383
Google Text-to-speech Engine	25.2.1.361632836

Finished Total: 22

Bookmarks:
- <ROOT>
  - 91
  - 2
  - Sort Result (2 items)
  - 0
  - 1

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



Recovered Contacts

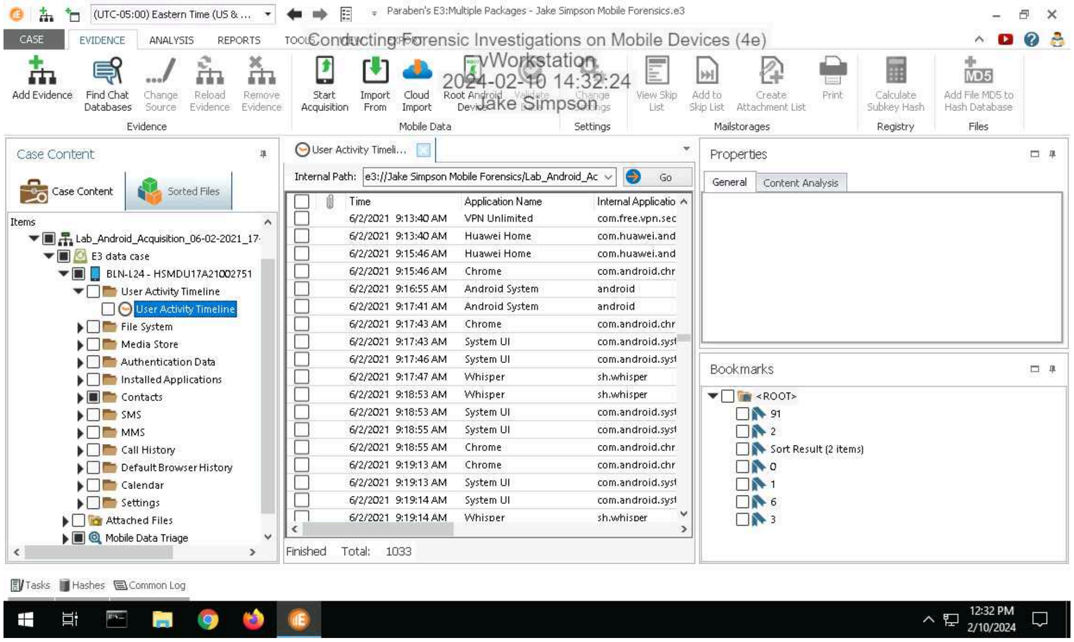
Internal Path: e3://Jake Simpson Mobile Forensics/Lab_Android_Ac

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

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**.



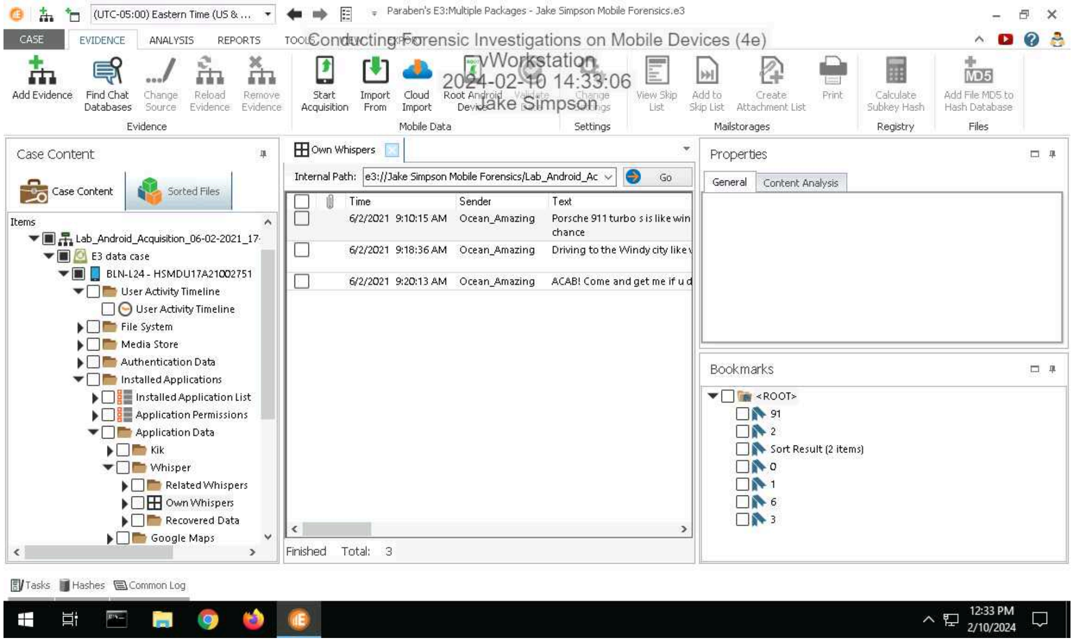
User Activity Timeli...

Internal Path: e3://Jake Simpson Mobile Forensics/Lab_Android_Ac

	Time	Application Name	Internal Applicatio
□	6/2/2021 9:13:40 AM	VPN Unlimited	com.free.vpn.sec
□	6/2/2021 9:13:40 AM	Huawei Home	com.huawei.and
□	6/2/2021 9:15:46 AM	Huawei Home	com.huawei.and
□	6/2/2021 9:15:46 AM	Chrome	com.android.chr
□	6/2/2021 9:16:55 AM	Android System	android
□	6/2/2021 9:17:41 AM	Android System	android
□	6/2/2021 9:17:43 AM	Chrome	com.android.chr
□	6/2/2021 9:17:43 AM	System UI	com.android.syst
□	6/2/2021 9:17:46 AM	System UI	com.android.syst
□	6/2/2021 9:17:47 AM	Whisper	sh.whisper
□	6/2/2021 9:18:53 AM	Whisper	sh.whisper
□	6/2/2021 9:18:53 AM	System UI	com.android.syst
□	6/2/2021 9:18:55 AM	System UI	com.android.syst
□	6/2/2021 9:18:55 AM	Chrome	com.android.chr
□	6/2/2021 9:19:13 AM	Chrome	com.android.chr
□	6/2/2021 9:19:13 AM	System UI	com.android.syst
□	6/2/2021 9:19:14 AM	System UI	com.android.syst
□	6/2/2021 9:19:14 AM	Whisper	sh.whisper

Finished Total: 1033

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



Paraben's E3:Multiple Packages - Jake Simpson Mobile Forensics.e3

vWorkstation
2024-02-10 14:33:06
Jake Simpson

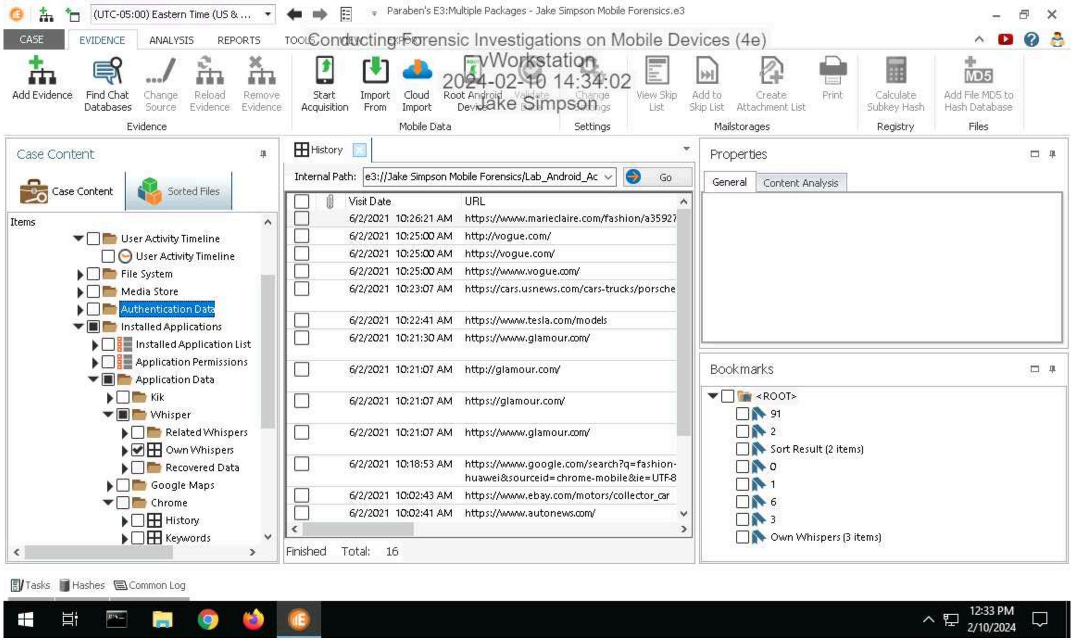
Own Whispers

Internal Path: e3://Jake Simpson Mobile Forensics/Lab_Android_Ac

Time	Sender	Text
6/2/2021 9:10:15 AM	Ocean_Amazing	Porsche 911 turbo s is like win chance
6/2/2021 9:18:36 AM	Ocean_Amazing	Driving to the Windy city like v
6/2/2021 9:20:13 AM	Ocean_Amazing	ACAB! Come and get me if u d

Finished Total: 3

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



Paraben's E3:Multiple Packages - Jake Simpson Mobile Forensics.e3

vWorkstation
2024-02-10 14:34:02
Jake Simpson

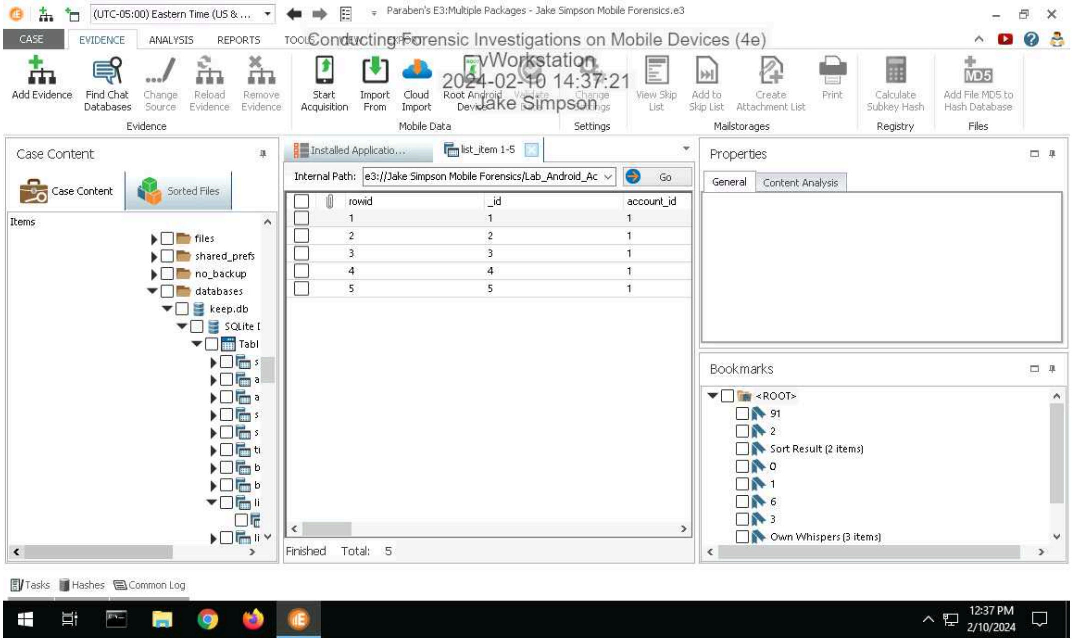
History

Internal Path: e3://Jake Simpson Mobile Forensics/Lab_Android_Ac

Visit Date	URL
6/2/2021 10:26:21 AM	https://www.marieclaire.com/fashion/a35927
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
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-huawei&sourceid=chrome-mobile&ie=UTF-8
6/2/2021 10:02:43 AM	https://www.ebay.com/motors/collector_car
6/2/2021 10:02:41 AM	https://www.autonews.com/

Finished Total: 16

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



Paraben's E3:Multiple Packages - Jake Simpson Mobile Forensics.e3

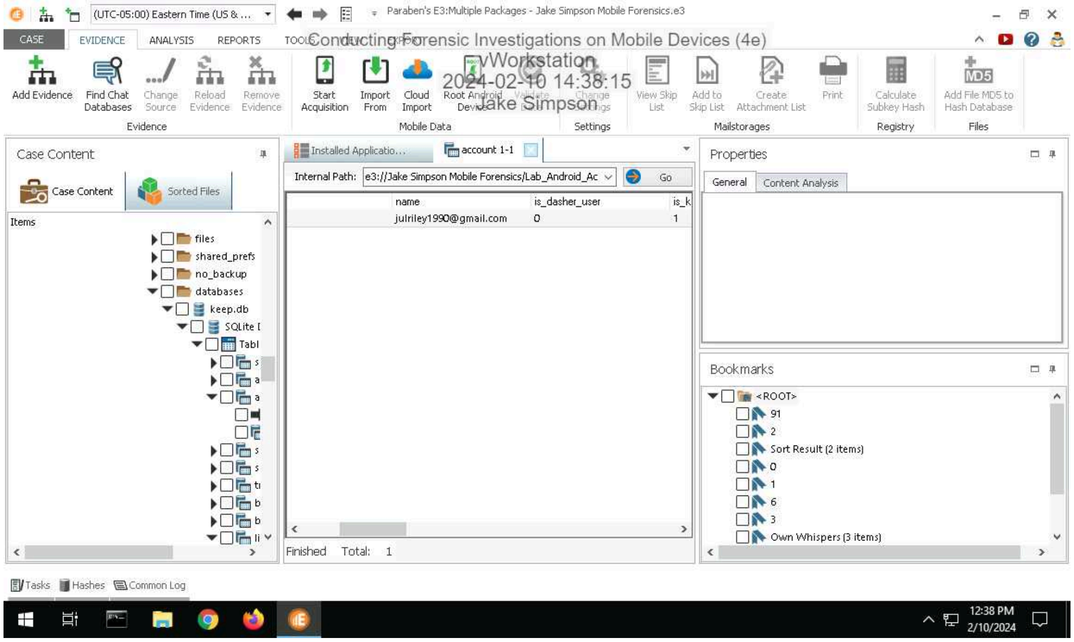
vWorkstation
2024-02-10 14:37:21
Jake Simpson

Internal Path: e3://Jake Simpson Mobile Forensics/Lab_Android_Ac

rowid	_id	account_id
1	1	1
2	2	1
3	3	1
4	4	1
5	5	1

Finished Total: 5

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



Paraben's E3:Multiple Packages - Jake Simpson Mobile Forensics.e3

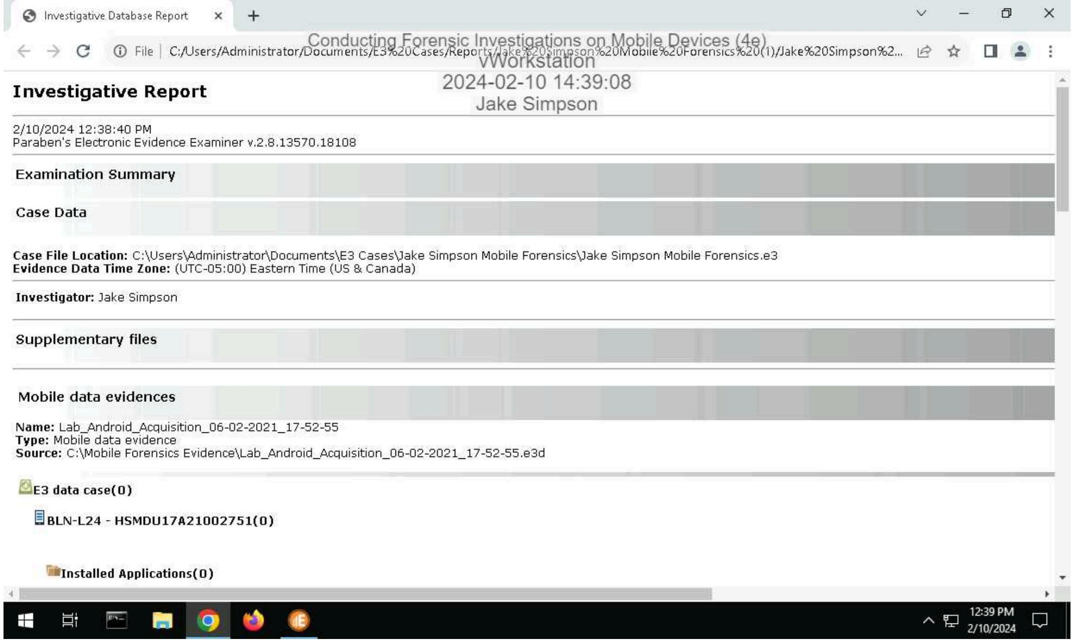
vWorkstation
2024-02-10 14:38:15
Jake Simpson

Internal Path: e3://Jake Simpson Mobile Forensics/Lab_Android_Ac

name	is_dasher_user	is_k
julriley1990@gmail.com	0	1

Finished Total: 1

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


Investigative Database Report
File
C:/Users/Administrator/Documents/E3%20Cases/Reports/Jake%20Simpson%20Mobile%20Forensics%20(1)/Jake%20Simpson%2...
12:39 PM
2/10/2024

Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2024-02-10 14:39:08
Jake Simpson

Investigative Report

2/10/2024 12:38:40 PM
Paraben's Electronic Evidence Examiner v.2.8.13570.18108

Examination Summary

Case Data

Case File Location: C:\Users\Administrator\Documents\E3 Cases\Jake Simpson Mobile Forensics\Jake Simpson Mobile Forensics.e3
Evidence Data Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Investigator: Jake Simpson

Supplementary files

Mobile data evidences

Name: Lab_Android_Acquisition_06-02-2021_17-52-55
Type: Mobile data evidence
Source: C:\Mobile Forensics Evidence\Lab_Android_Acquisition_06-02-2021_17-52-55.e3d

E3 data case(0)
BLN-L24 - HSMDU17A21002751(0)
Installed Applications(0)

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.

Case Overview, Exam notes and chain of custody of what was done, findings

Part 2: Draft a Forensic Report

Case Summary

On 02/10/2024 I was assigned a case that revolves around Auto thefts. A forensics examination of mobile device data is required to discover potential related evidence to the thefts.

Findings and Analysis

On 02/10/2024
I used Paraben E3 to load acquisitions from the suspected devices. Using the tools provided by Paraben's E3 I was able to find related and important data that was bookmarked and added to a Report which is viewable. The data includes but is not limited to search history, contacts, messages, etc.

Conclusion

Based on the forensics evidence examined in this case, the suspected devices did contain data that related to the car thefts.