Student:	Email:
Karan Atul Vora	kxv230021@utdallas.edu

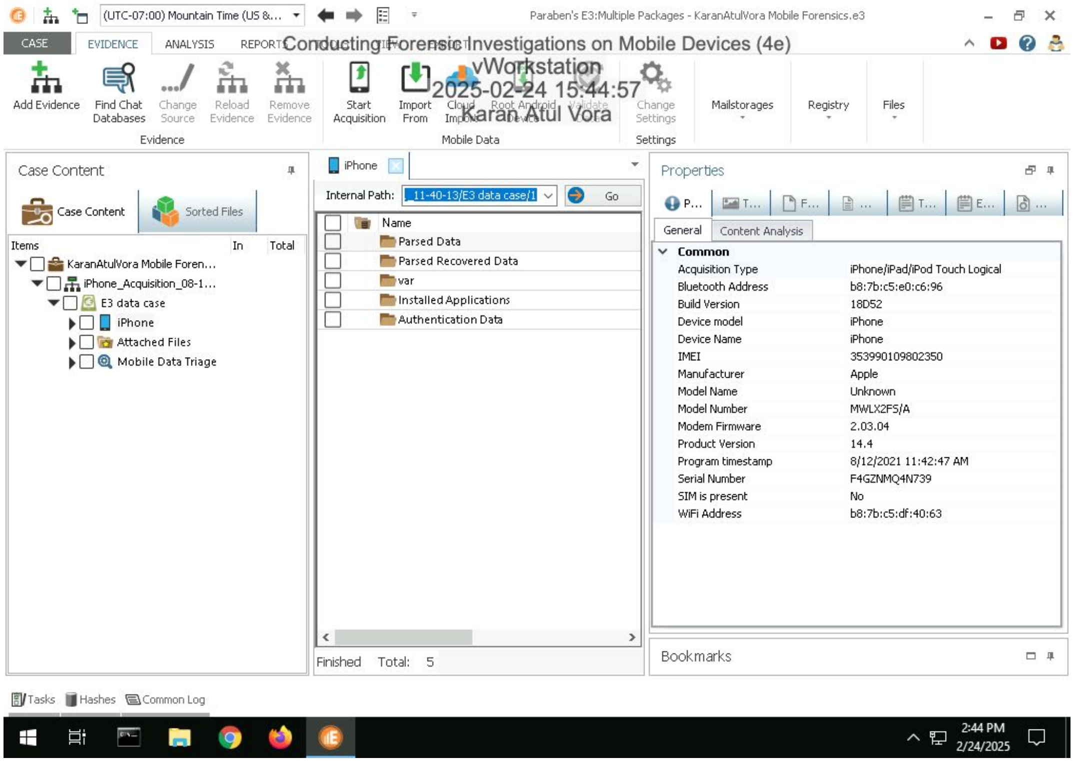
Time on Task:	Progress:
1 hour, 35 minutes	100%

Report Generated: Monday, February 24, 2025 at 6:16 PM

Section 1: Hands-On Demonstration

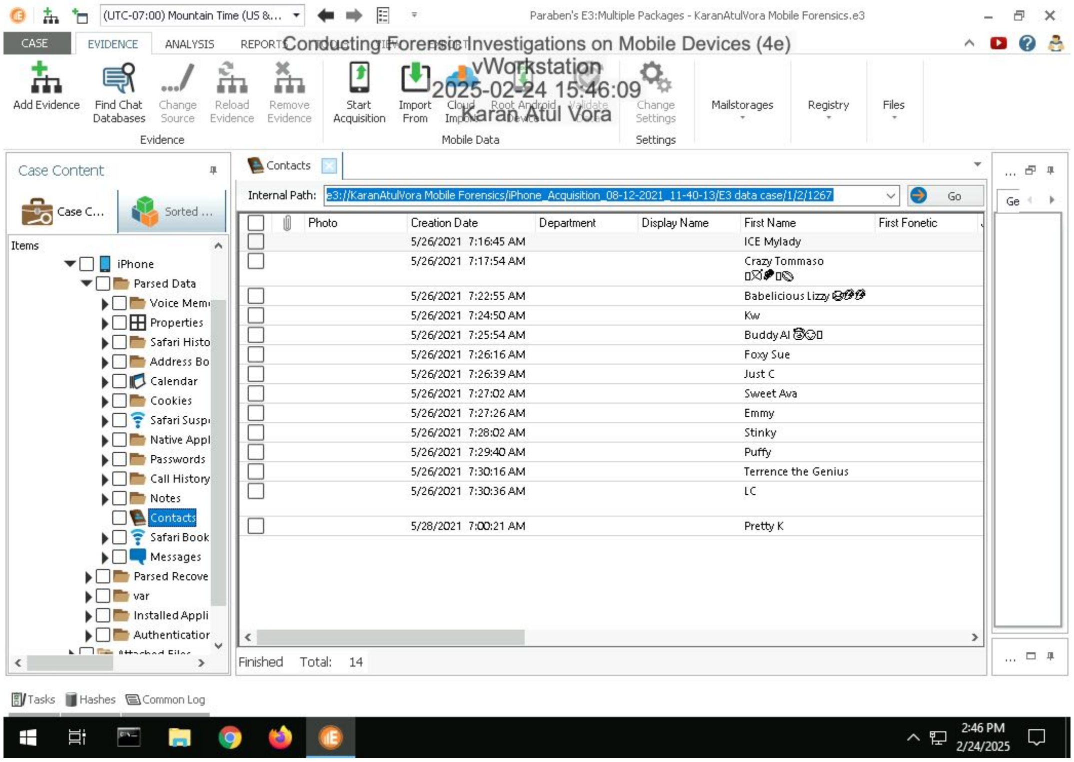
Part 1: Identify Forensic Evidence in an iOS Data Case

8. **Make a screen capture** showing the **contents of the Properties pane**.



Common	
Acquisition Type	iPhone/iPad/iPod Touch Logical
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**.

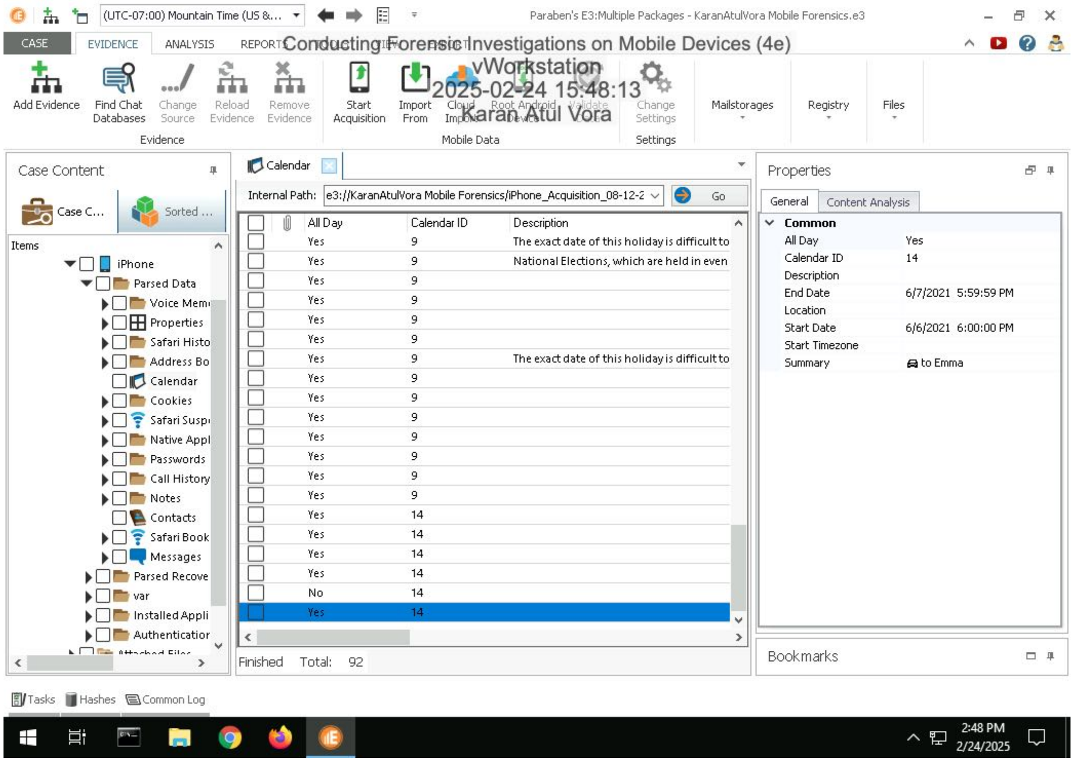


Internal Path: e3://KaranAtulVora Mobile Forensics/iPhone_Acquisition_08-12-2021_11-40-13/E3 data case/1/2/1267 Go

Photo	Creation Date	Department	Display Name	First Name	First Fonetic
	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://KaranAtulVora Mobile Forensics/iPhone_Acquisition_08-12-2 Go

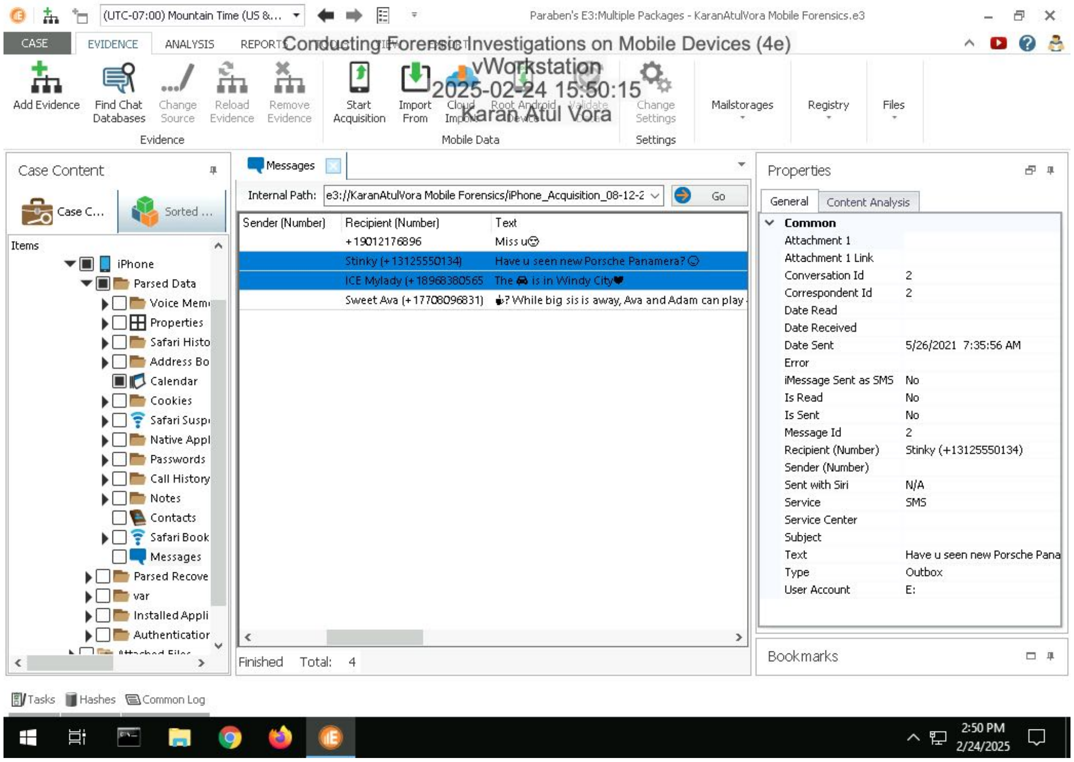
All Day	Calendar ID	Description
Yes	9	The exact date of this holiday is difficult to
Yes	9	National Elections, which are held in even
Yes	9	
Yes	9	
Yes	9	
Yes	9	
Yes	9	The exact date of this holiday is difficult to
Yes	9	
Yes	9	
Yes	9	
Yes	9	
Yes	9	
Yes	9	
Yes	9	
Yes	14	
Yes	14	
Yes	14	
Yes	14	
No	14	
Yes	14	

Finished Total: 92

Common

All Day	Yes
Calendar ID	14
Description	
End Date	6/7/2021 5:59:59 PM
Location	
Start Date	6/6/2021 6:00:00 PM
Start Timezone	
Summary	to Emma

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



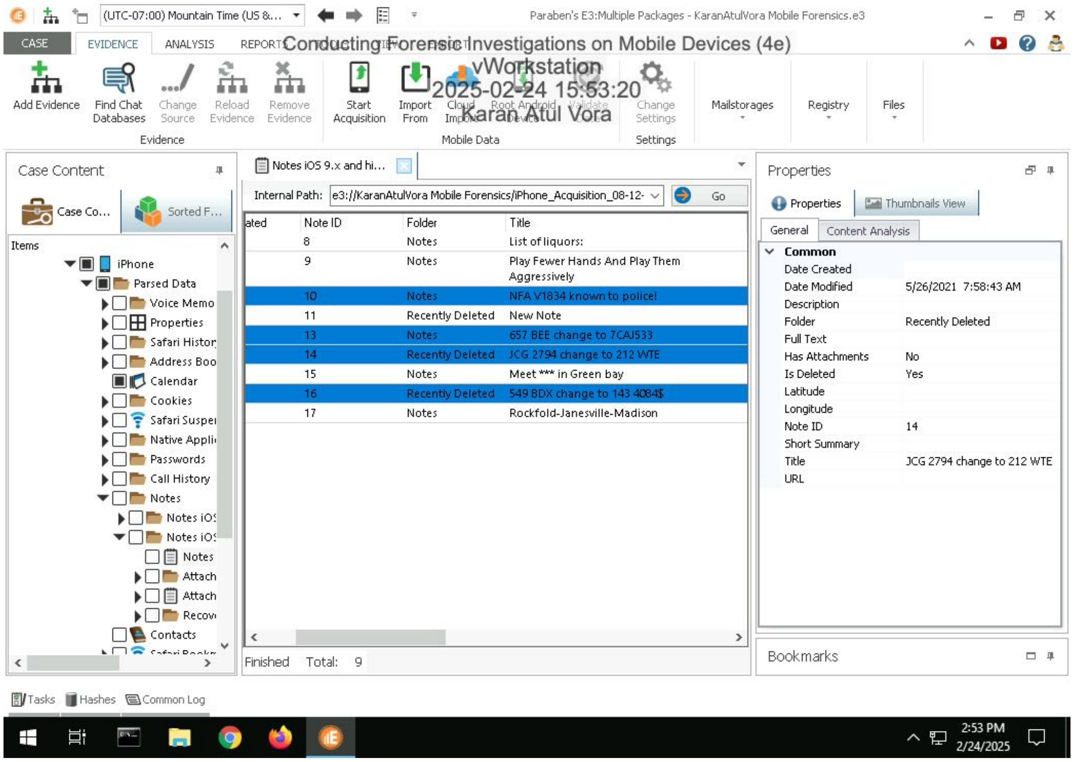
Internal Path: e3://KaranAtulVora Mobile Forensics/iPhone_Acquisition_08-12-2

Sender (Number)	Recipient (Number)	Text
	+19012176896	Miss u😔
	Stinky (+13125550134)	Have u seen new Porsche Panamera? ☺
	ICE Mylady (+18968380565	The 🚗 is in Windy City❤
	Sweet Ava (+17708096831)	🍎? While big sis is away, Ava and Adam can play

Finished Total: 4

Common	
Attachment 1	
Attachment 1 Link	
Conversation Id	2
Correspondent Id	2
Date Read	
Date Received	
Date Sent	5/26/2021 7:35:56 AM
Error	
iMessage Sent as SMS	No
Is Read	No
Is Sent	No
Message Id	2
Recipient (Number)	Stinky (+13125550134)
Sender (Number)	
Sent with Siri	N/A
Service	SMS
Service Center	
Subject	
Text	Have u seen new Porsche Pana
Type	Outbox
User Account	E:

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



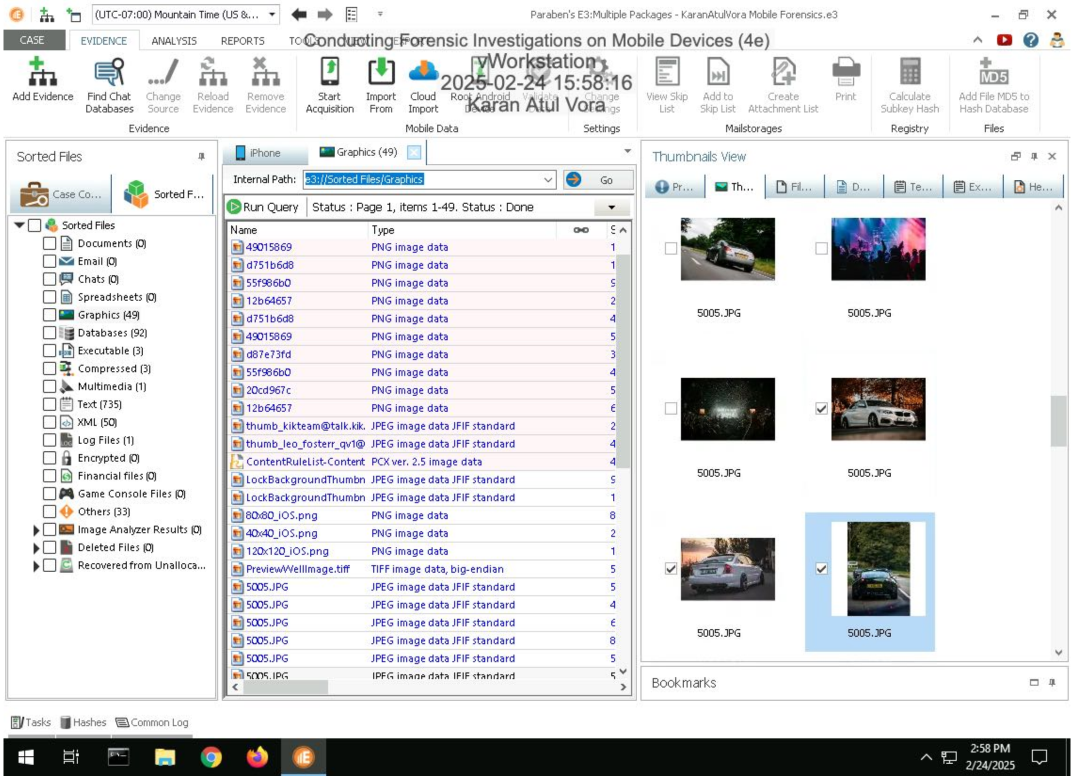
Internal Path: e3://KaranAtulVora Mobile Forensics/iPhone_Acquisition_08-12-

ated	Note ID	Folder	Title
	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

Finished Total: 9

Common	
Date Created	
Date Modified	5/26/2021 7:58:43 AM
Description	
Folder	Recently Deleted
Full Text	
Has Attachments	No
Is Deleted	Yes
Latitude	
Longitude	
Note ID	14
Short Summary	
Title	JCG 2794 change to 212 WTE
URL	

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



- ☐ 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 Unalloca...

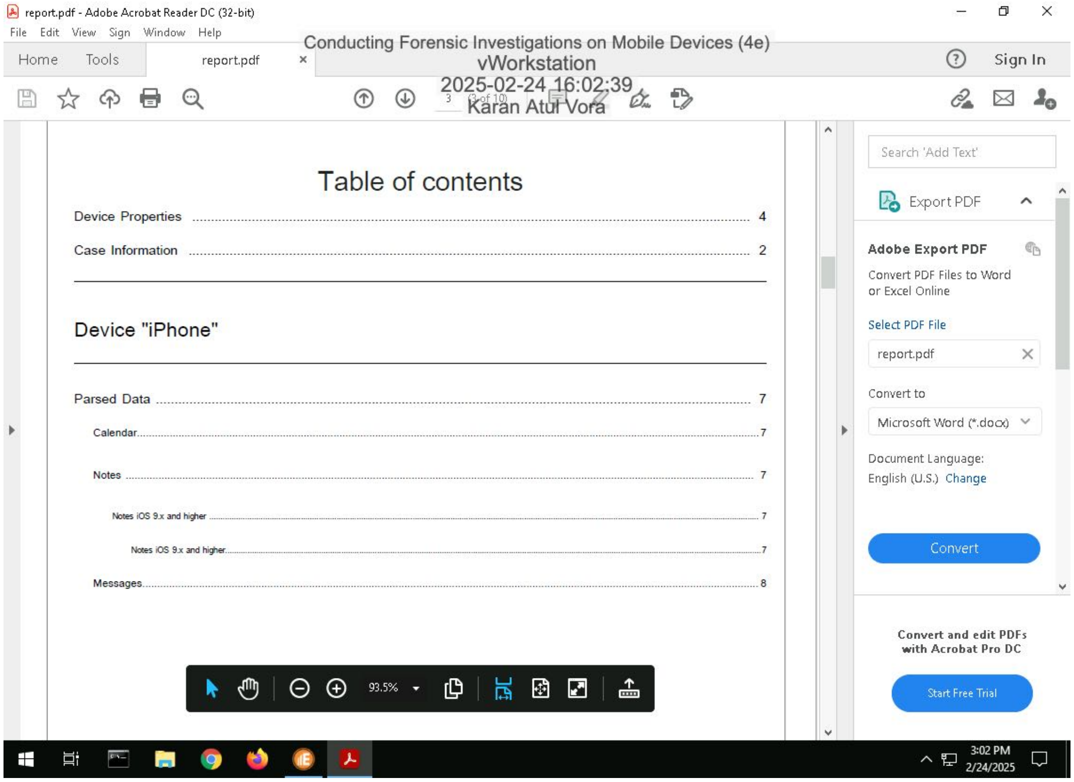
Internal Path: e3://Sorted Files/Graphics

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

Name	Type	⚯	S
49015869	PNG image data		1
d751b6d8	PNG image data		1
55f986b0	PNG image data		9
12b64657	PNG image data		2
d751b6d8	PNG image data		4
49015869	PNG image data		5
d87e73fd	PNG image data		3
55f986b0	PNG image data		4
20cd967c	PNG image data		5
12b64657	PNG image data		6
thumb_kikteam@talk.kik.	JPEG image data JFIF standard		2
thumb_leo_fosterr_qv1@	JPEG image data JFIF standard		4
ContentRuleList-Content	PCX ver. 2.5 image data		4
LockBackgroundThumbn	JPEG image data JFIF standard		9
LockBackgroundThumbn	JPEG image data JFIF standard		1
80x80_iOS.png	PNG image data		8
40x40_iOS.png	PNG image data		2
120x120_iOS.png	PNG image data		1
PreviewWellImage.tiff	TIFF image data, big-endian		5
5005.JPG	JPEG image data JFIF standard		5
5005.JPG	JPEG image data JFIF standard		4
5005.JPG	JPEG image data JFIF standard		6
5005.JPG	JPEG image data JFIF standard		8
5005.JPG	JPEG image data JFIF standard		5
5005.JPG	JPEG image data JFIF standard		5

☐ 5005.JPG	☐ 5005.JPG
☐ 5005.JPG	☑ 5005.JPG
☑ 5005.JPG	☑ 5005.JPG

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



Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-02-24 16:02:39
Karan Atul Vora

Table of contents

Device Properties 4
Case Information 2

Device "iPhone"

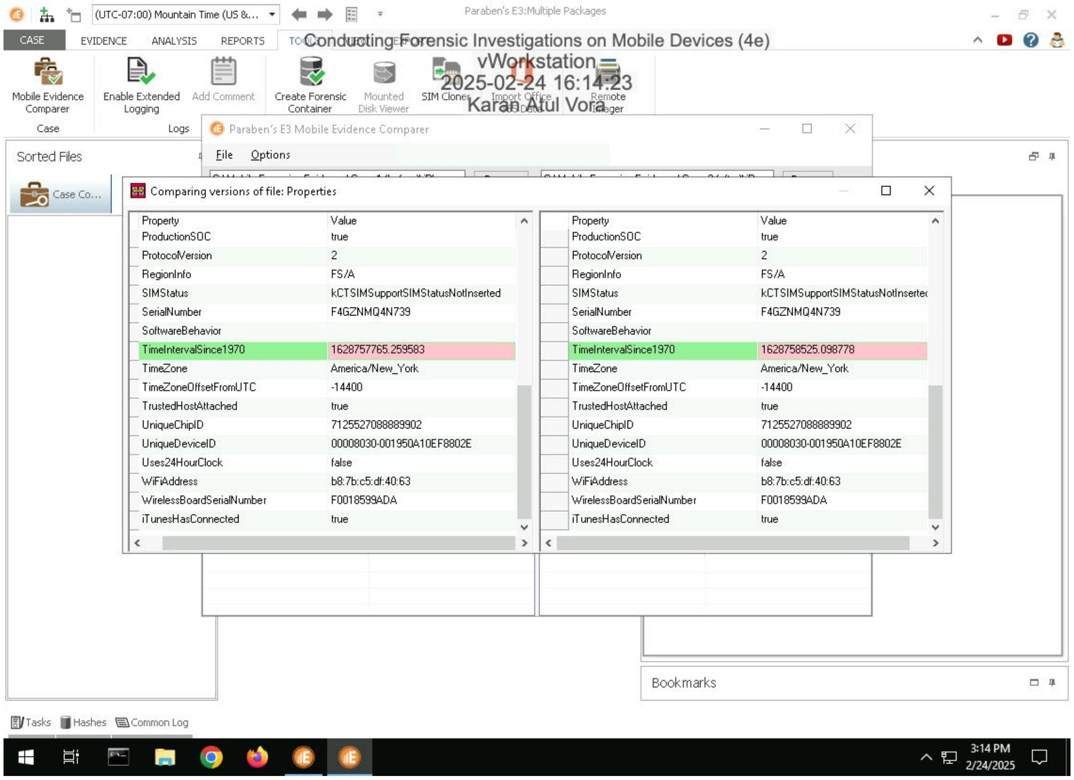
Parsed Data 7
Calendar 7
Notes 7
Notes iOS 9.x and higher 7
Notes iOS 9.x and higher 7
Messages 8

Adobe Export PDF
Convert PDF Files to Word or Excel Online
Select PDF File
report.pdf
Convert to
Microsoft Word (*.docx)
Document Language:
English (U.S.) Change
Convert

Convert and edit PDFs with Acrobat Pro DC
Start Free Trial

Part 2: Compare iOS Data Cases

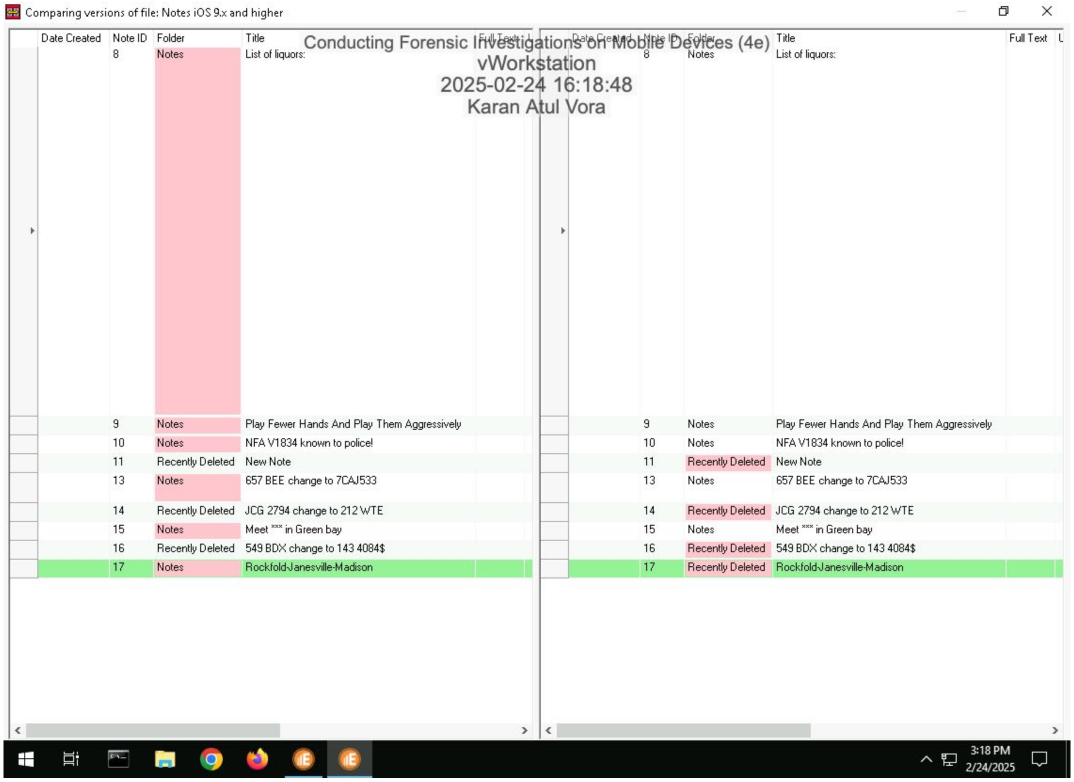
10. **Make a screen capture** showing the **difference in data case properties**.



Property	Value
ProductionSOC	true
ProtocolVersion	2
RegionInfo	FS/A
SIMStatus	kCTSIMSupportSIMStatusNotInserted
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

Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-02-24 16:18:48
Karan Atul Vora

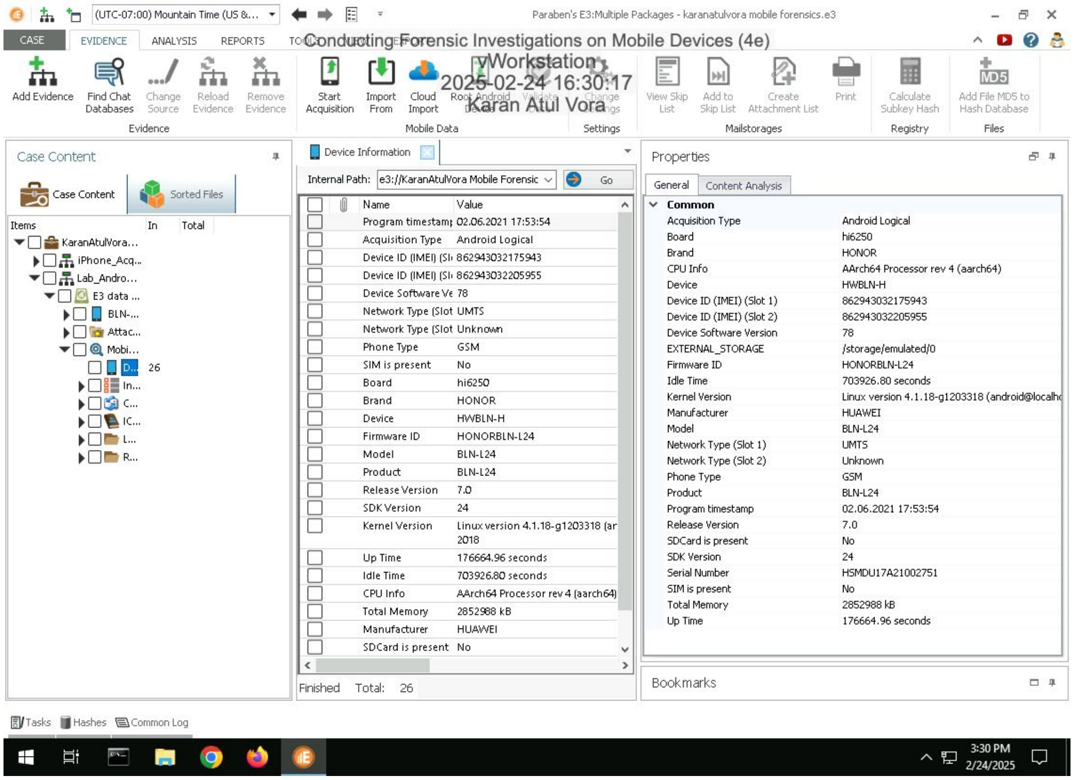
Date Created	Note ID	Folder	Title	Full Text
	8	Notes	List of liquors:	
	9	Notes	Play Fewer Hands And Play Them Aggressively	
	10	Notes	NFA V1834 known to police!	
	11	Recently Deleted	New Note	
	13	Notes	657 BEE change to 7CAJ533	
	14	Recently Deleted	JCG 2794 change to 212 WTE	
	15	Notes	Meet *** in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

Date Created	Note ID	Folder	Title	Full Text
	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**.



Device Information

Internal Path: e3://KaranAtulVora Mobile Forensic Go

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 (ar 2018
Up Time	176664.96 seconds
Idle Time	703926.80 seconds
CPU Info	AArch64 Processor rev 4 (aarch64)
Total Memory	2852988 kB
Manufacturer	HUAWEI
SDCard is present	No

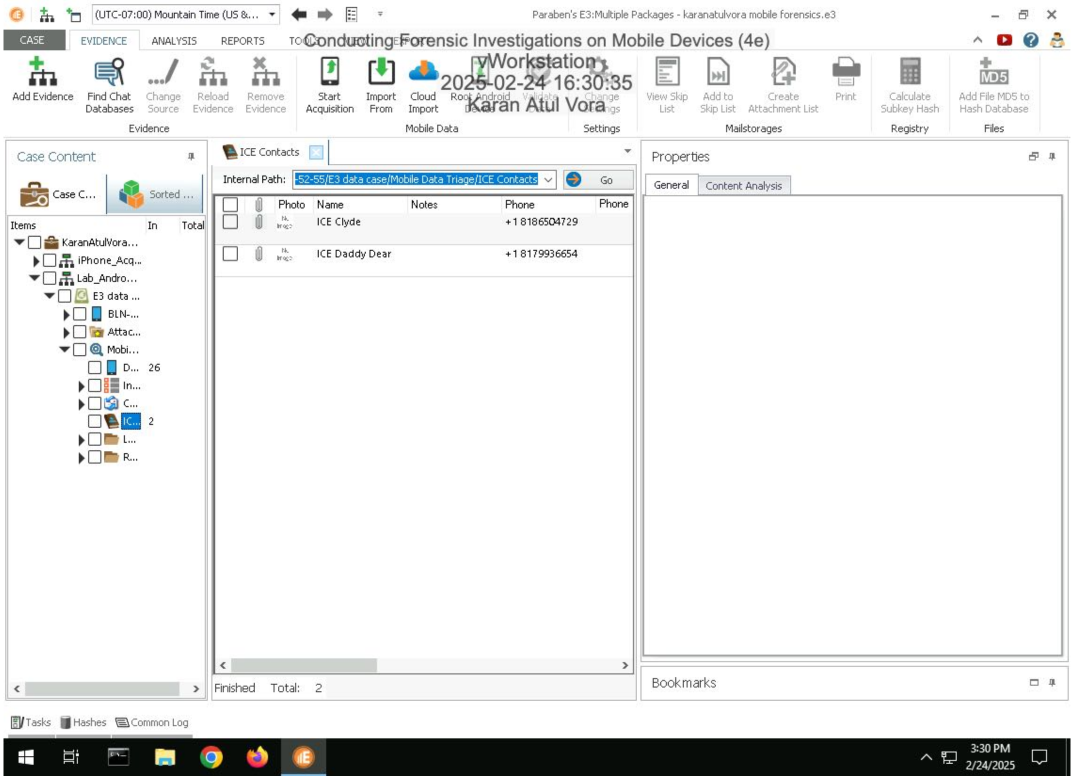
Finished Total: 26

Properties

General | Content Analysis

Common	
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
Firmware ID	HONORBLN-L24
Idle Time	703926.80 seconds
Kernel Version	Linux version 4.1.18-g1203318 (android@localho
Manufacturer	HUAWEI
Model	BLN-L24
Network Type (Slot 1)	UMTS
Network Type (Slot 2)	Unknown
Phone Type	GSM
Product	BLN-L24
Program timestamp	02.06.2021 17:53:54
Release Version	7.0
SDCard is present	No
SDK Version	24
Serial Number	HSMDU17A21002751
SIM is present	No
Total Memory	2852988 kB
Up Time	176664.96 seconds

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



Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-02-24 16:30:35
Karan Atul Vora

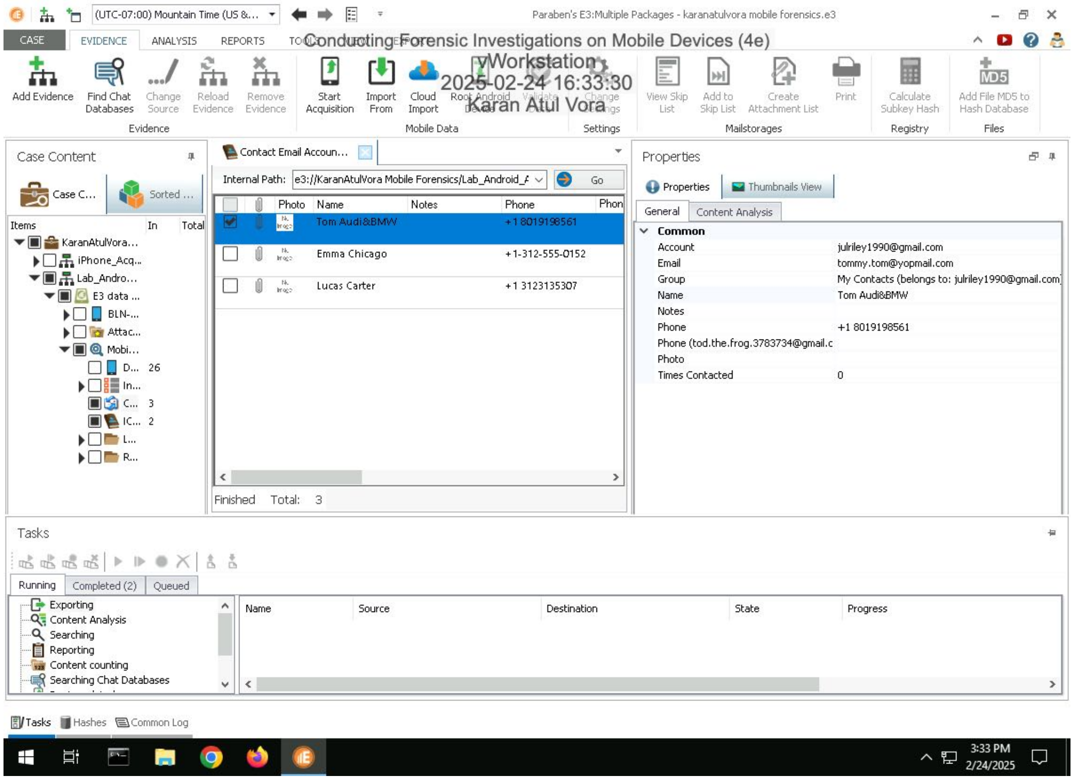
Paraben's E3:Multiple Packages - karanatulvora mobile forensics.e3

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

	Photo	Name	Notes	Phone	Phone
□		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
2025-02-24 16:33:30
Karan Atul Vora

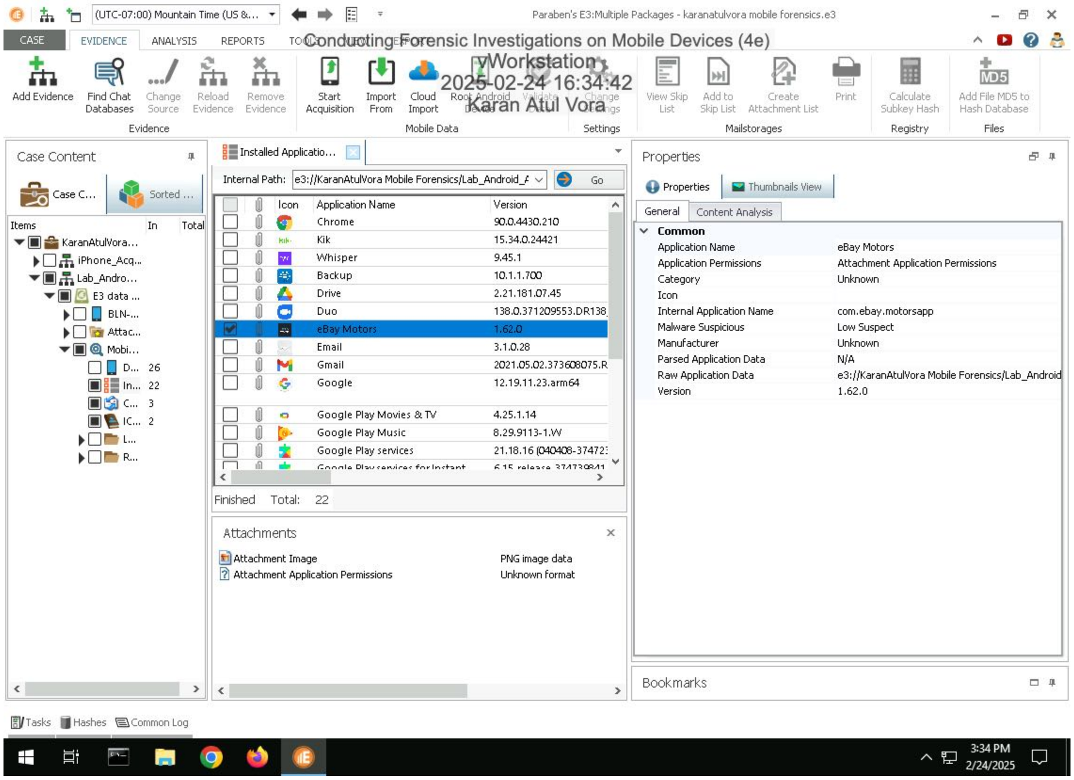
Internal Path: e3://KaranAtulVora Mobile Forensics/Lab_Android_A

		Photo	Name	Notes	Phone	Phon
☑			Tom Audi&BMW		+1 8019198561	
□			Emma Chicago		+1-312-555-0152	
□			Lucas Carter		+1 3123135307	

Finished Total: 3

Common	
Account	julriley1990@gmail.com
Email	tommy.tom@yopmail.com
Group	My Contacts (belongs to: julriley1990@gmail.com)
Name	Tom Audi&BMW
Notes	
Phone	+1 8019198561
Phone (tod.the.frog.3783734@gmail.c	
Photo	
Times Contacted	0

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



Internal Path: e3://KaranAtulVora Mobile Forensics/Lab_Android_A

Icon	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.R
	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 (040408-37472:
	Google Play services for Instant	6.15 release 374739841

Finished Total: 22

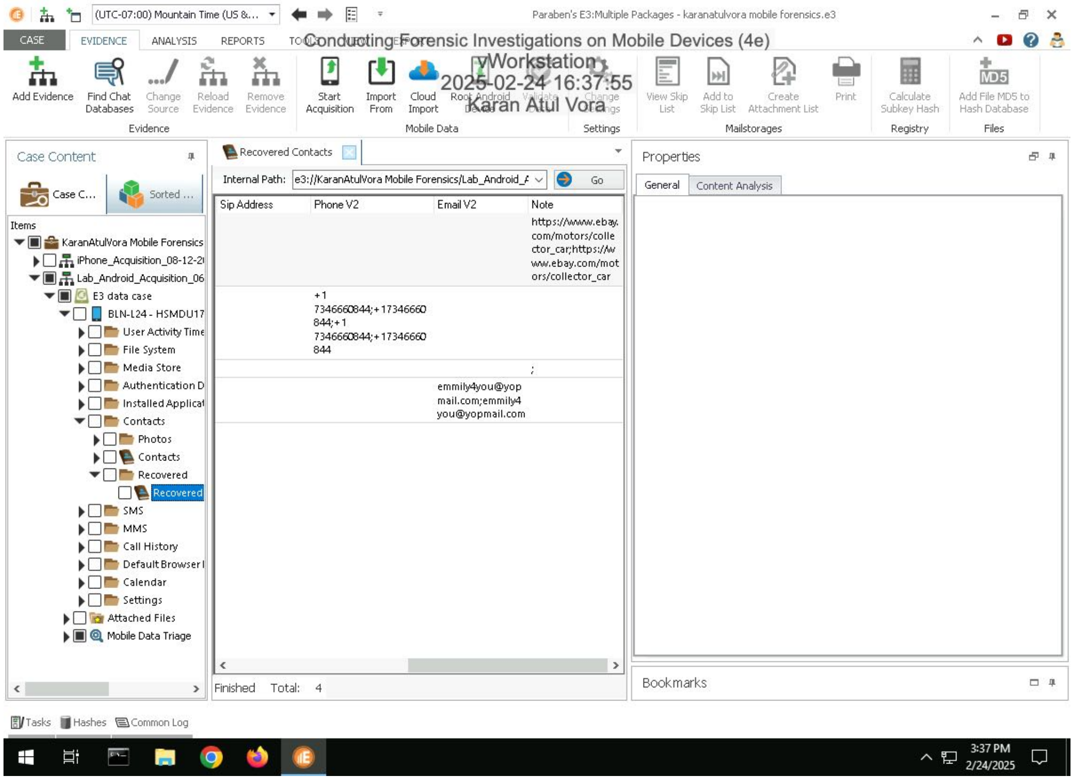
Attachments

Attachment Image	PNG image data
Attachment Application Permissions	Unknown format

Properties — General — Common

Application Name	eBay Motors
Application Permissions	Attachment Application Permissions
Category	Unknown
Icon	
Internal Application Name	com.ebay.motorsapp
Malware Suspicious	Low Suspect
Manufacturer	Unknown
Parsed Application Data	N/A
Raw Application Data	e3://KaranAtulVora Mobile Forensics/Lab_Android
Version	1.62.0

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

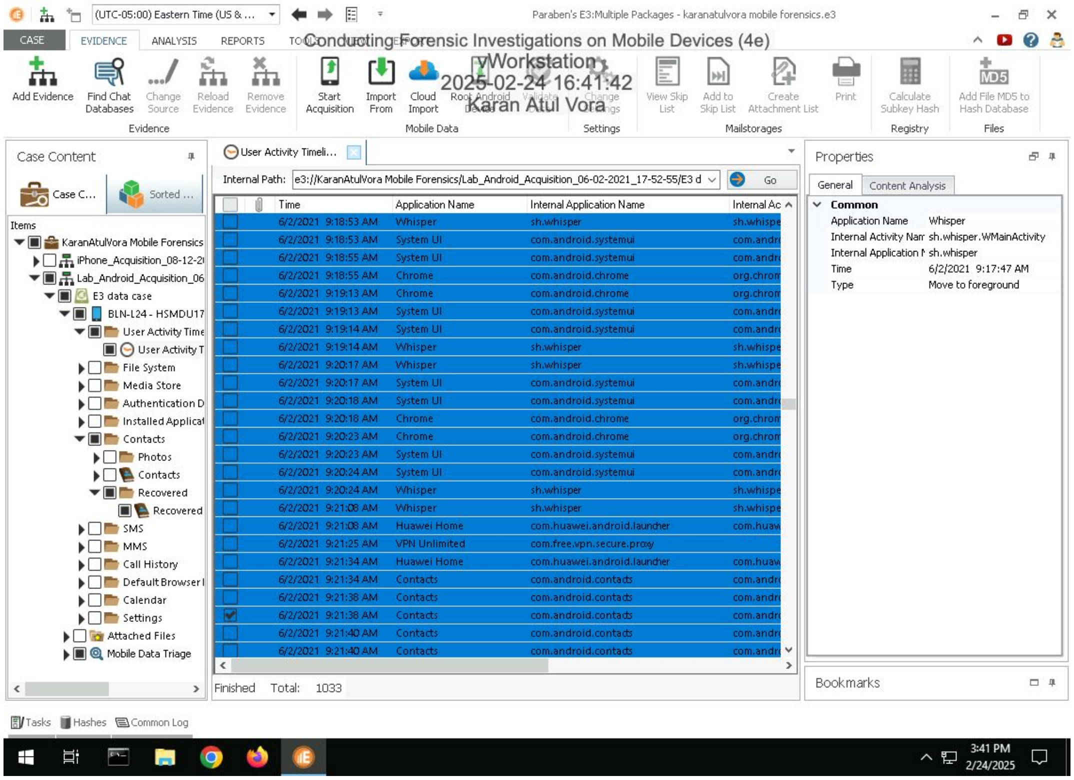

Paraben's E3:Multiple Packages - karanatulvora mobile forensics.e3
Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-02-24 16:37:55
Karan Atul Vora
Recovered Contacts
Finished Total: 4
3:37 PM
2/24/2025

Internal Path: e3://KaranAtulVora Mobile Forensics/Lab_Android_A

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	

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://KaranAtulVora Mobile Forensics/Lab_Android_Acquisition_06-02-2021_17-52-55/E3 d

	Time	Application Name	Internal Application Name	Internal Ac
□	6/2/2021 9:18:53 AM	Whisper	sh.whisper	sh.whispe
□	6/2/2021 9:18:53 AM	System UI	com.android.systemui	com.andr
□	6/2/2021 9:18:55 AM	System UI	com.android.systemui	com.andr
□	6/2/2021 9:18:55 AM	Chrome	com.android.chrome	org.chrom
□	6/2/2021 9:19:13 AM	Chrome	com.android.chrome	org.chrom
□	6/2/2021 9:19:13 AM	System UI	com.android.systemui	com.andr
□	6/2/2021 9:19:14 AM	System UI	com.android.systemui	com.andr
□	6/2/2021 9:19:14 AM	Whisper	sh.whisper	sh.whispe
□	6/2/2021 9:20:17 AM	Whisper	sh.whisper	sh.whispe
□	6/2/2021 9:20:17 AM	System UI	com.android.systemui	com.andr
□	6/2/2021 9:20:18 AM	System UI	com.android.systemui	com.andr
□	6/2/2021 9:20:18 AM	Chrome	com.android.chrome	org.chrom
□	6/2/2021 9:20:23 AM	Chrome	com.android.chrome	org.chrom
□	6/2/2021 9:20:23 AM	System UI	com.android.systemui	com.andr
□	6/2/2021 9:20:24 AM	System UI	com.android.systemui	com.andr
□	6/2/2021 9:20:24 AM	Whisper	sh.whisper	sh.whispe
□	6/2/2021 9:21:08 AM	Whisper	sh.whisper	sh.whispe
□	6/2/2021 9:21:08 AM	Huawei Home	com.huawei.android.launcher	com.huaw
□	6/2/2021 9:21:25 AM	VPN Unlimited	com.free.vpn.secure.proxy	
□	6/2/2021 9:21:34 AM	Huawei Home	com.huawei.android.launcher	com.huaw
□	6/2/2021 9:21:34 AM	Contacts	com.android.contacts	com.andr
□	6/2/2021 9:21:38 AM	Contacts	com.android.contacts	com.andr
☑	6/2/2021 9:21:38 AM	Contacts	com.android.contacts	com.andr
□	6/2/2021 9:21:40 AM	Contacts	com.android.contacts	com.andr
□	6/2/2021 9:21:40 AM	Contacts	com.android.contacts	com.andr

Finished Total: 1033

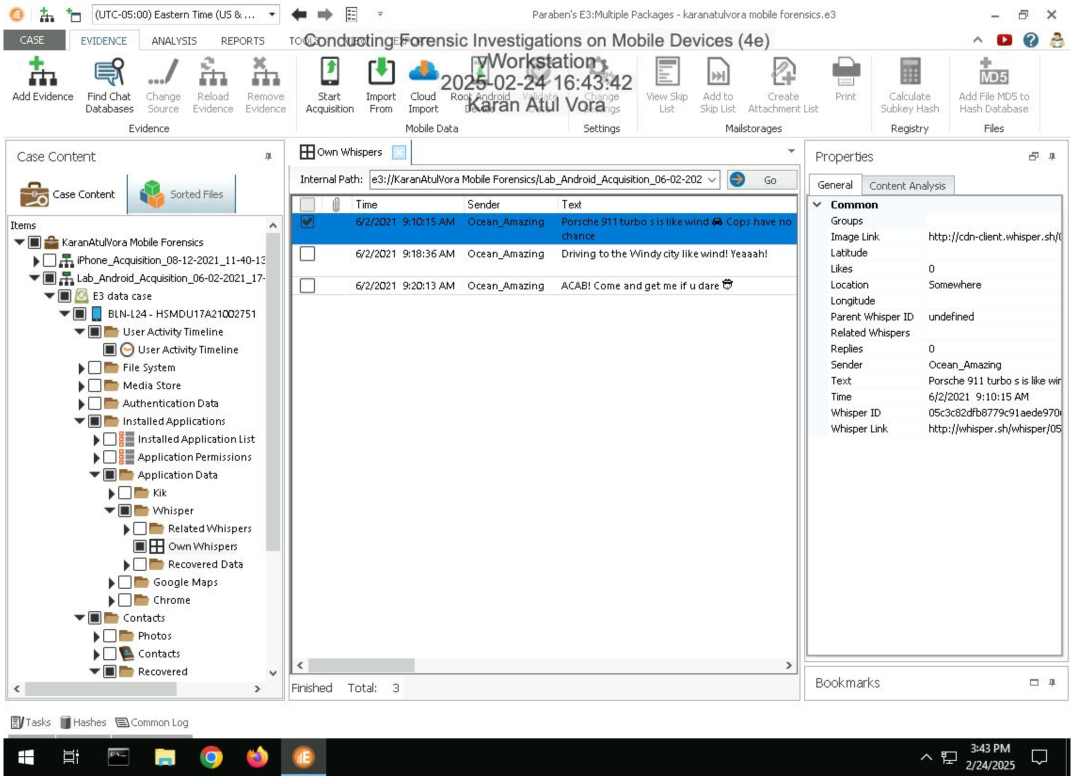
Properties

General | Content Analysis

Common

Application Name	Whisper
Internal Activity Nam	sh.whisper.WMainActivity
Internal Application N	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**.



Own Whispers

Internal Path: e3://KaranAtulVora Mobile Forensics/Lab_Android_Acquisition_06-02-202 Go

	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

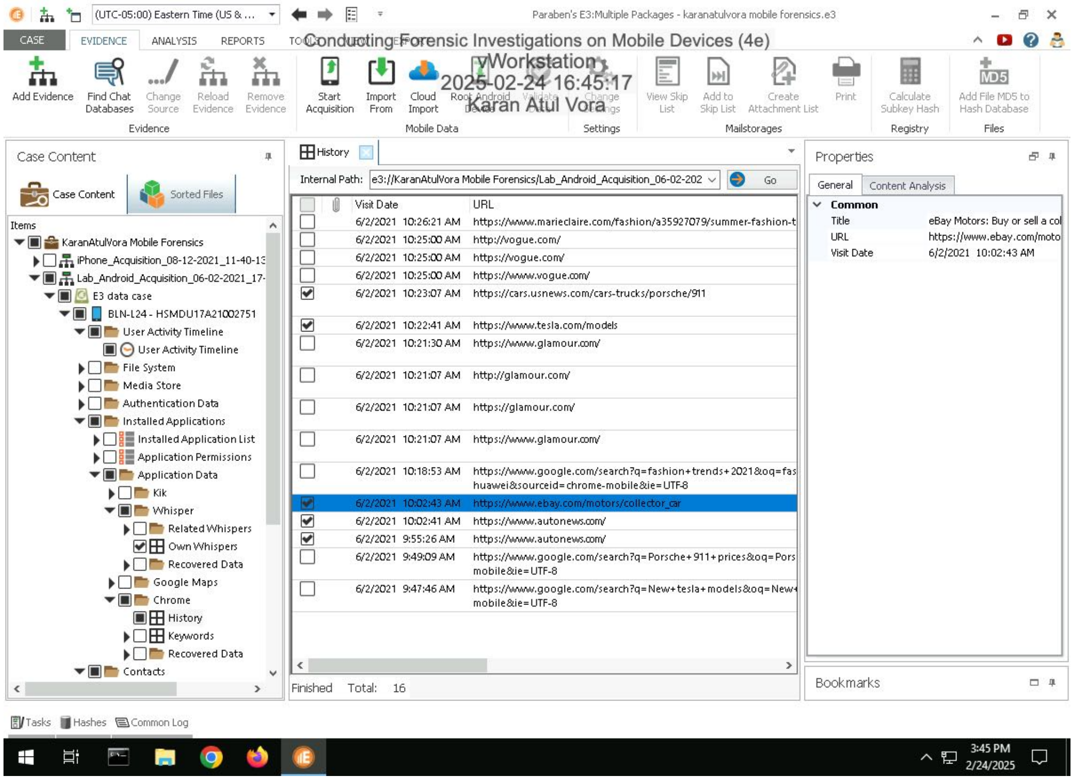
Properties

General | Content Analysis

Common	
Groups	
Image Link	http://cdn-client.whisper.sh/(
Latitude	
Likes	0
Location	Somewhere
Longitude	
Parent Whisper ID	undefined
Related Whispers	
Replies	0
Sender	Ocean_Amazing
Text	Porsche 911 turbo s is like wir
Time	6/2/2021 9:10:15 AM
Whisper ID	05c3c82dfb8779c91aede970
Whisper Link	http://whisper.sh/whisper/05

Bookmarks

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



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

Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-02-24 16:45:17
Karan Atul Vora

Internal Path: e3://KaranAtulVora Mobile Forensics/Lab_Android_Acquisition_06-02-202

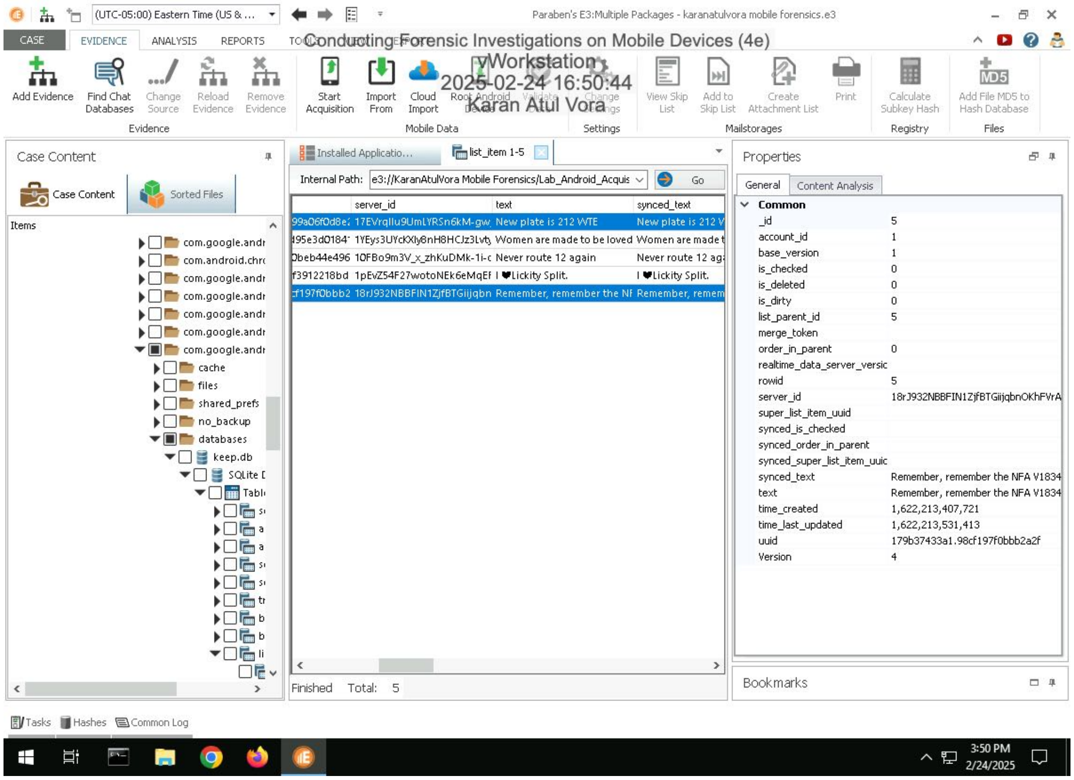
☐	Visit Date	URL
☐	6/2/2021 10:26:21 AM	https://www.marieclaire.com/fashion/a35927079/summer-fashion-t
☐	6/2/2021 10:25:00 AM	http://vogue.com/
☐	6/2/2021 10:25:00 AM	https://vogue.com/
☐	6/2/2021 10:25:00 AM	https://www.vogue.com/
☑	6/2/2021 10:23:07 AM	https://cars.usnews.com/cars-trucks/porsche/911
☑	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=fas 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/
☑	6/2/2021 9:55:26 AM	https://www.autonews.com/
☐	6/2/2021 9:49:09 AM	https://www.google.com/search?q=Porsche+911+prices&oq=Pors mobile&ie=UTF-8
☐	6/2/2021 9:47:46 AM	https://www.google.com/search?q=New+tesla+models&oq=New+ mobile&ie=UTF-8

Finished Total: 16

Properties — General — Common

Title	eBay Motors: Buy or sell a col
URL	https://www.ebay.com/moto
Visit Date	6/2/2021 10:02:43 AM

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



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

Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-02-24 16:50:44
Karan Atul Vora

Internal Path: e3://KaranAtulVora Mobile Forensics/Lab_Android_Acquis

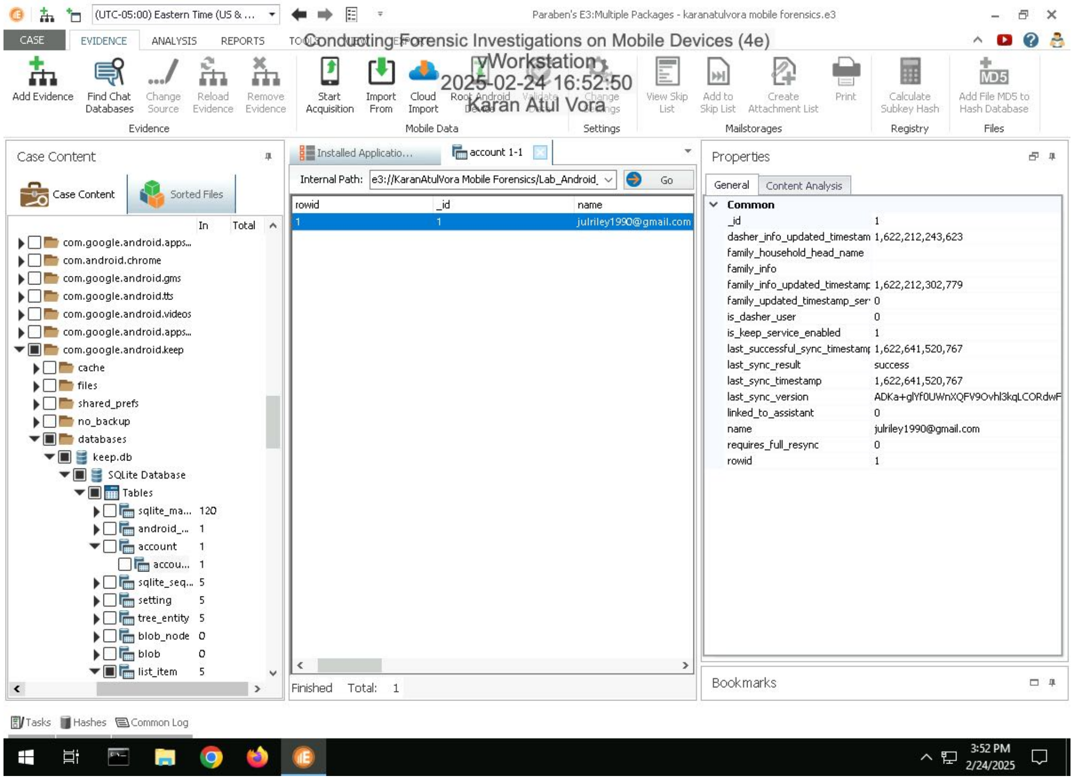
	server_id	text	synced_text
99a06f0d8e:	17EVrqIlu9UmLYRSn6kM-gw,	New plate is 212 WTE	New plate is 212 V
d95e3d0184'	1YEys3UYcKXly8nH8HCJz3Lvt,	Women are made to be loved	Women are made t
0beb44e496	10FBo9m3V_x_zhKuDMk-1i-c	Never route 12 again	Never route 12 ag:
f3912218bd	1pEvZ54F27wotoNEk6eMqEf	I ❤Lickity Split.	I ❤Lickity Split.
cf197f0bbb2	18rJ932NBBFIN1ZjfBTGiijqbn	Remember, remember the NF	Remember, remem

Finished Total: 5

Properties

Common	
_id	5
account_id	1
base_version	1
is_checked	0
is_deleted	0
is_dirty	0
list_parent_id	5
merge_token	
order_in_parent	0
realtime_data_server_versic	
rowid	5
server_id	18rJ932NBBFIN1ZjfBTGiijqbnOKhFVrA
super_list_item_uuid	
synced_is_checked	
synced_order_in_parent	
synced_super_list_item_uuic	
synced_text	Remember, remember the NFA V1834
text	Remember, remember the NFA V1834
time_created	1,622,213,407,721
time_last_updated	1,622,213,531,413
uuid	179b37433a1.98cf197f0bbb2a2f
Version	4

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



Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-02-24 16:52:50
Karan Atul Vora

Case Content

	In	Total
com.google.android.apps...		
com.android.chrome		
com.google.android.gms		
com.google.android.tts		
com.google.android.videos		
com.google.android.apps...		
com.google.android.keep		
cache		
files		
shared_prefs		
no_backup		
databases		
keep.db		
SQLite Database		
Tables		
sqlite_ma...	120	
android_...	1	
account	1	
accou...	1	
sqlite_seq...	5	
setting	5	
tree_entity	5	
blob_node	0	
blob	0	
list_item	5	

Internal Path: e3://KaranAtulVora Mobile Forensics/Lab_Android_ Go

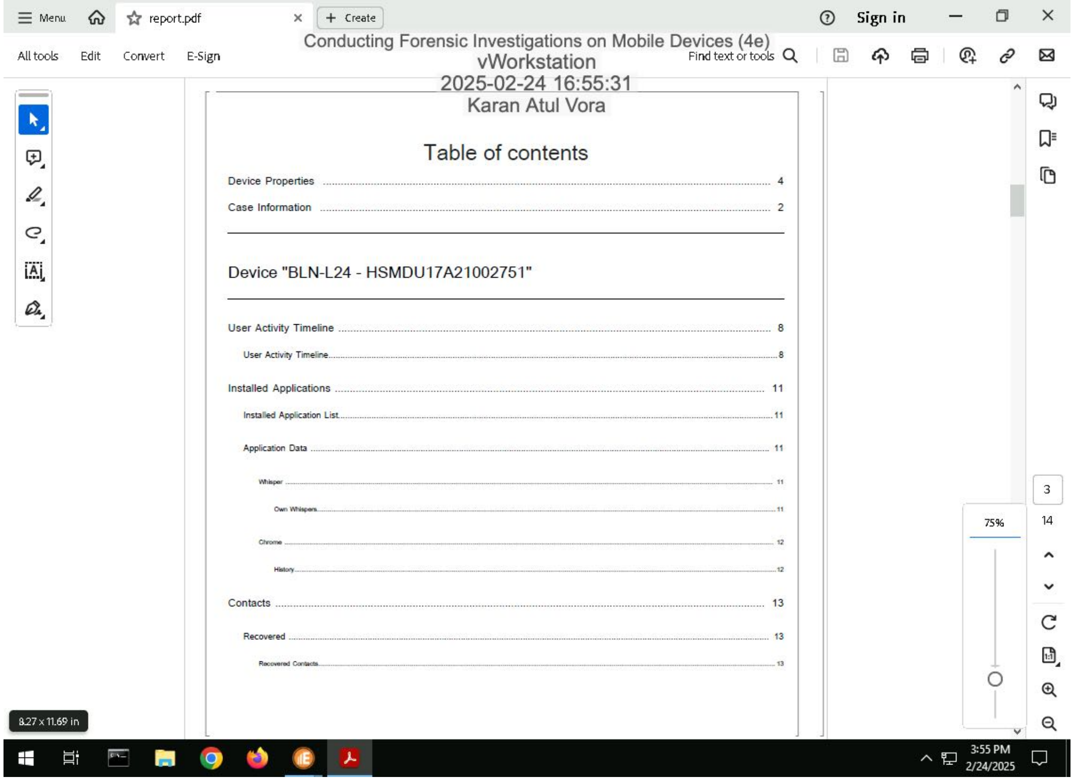
rowid	_id	name
1	1	julriley1990@gmail.com

Finished Total: 1

Common

_id	1
dasher_info_updated_timestam	1,622,212,243,623
family_household_head_name	
family_info	
family_info_updated_timestamp	1,622,212,302,779
family_updated_timestamp_ser	0
is_dasher_user	0
is_keep_service_enabled	1
last_successful_sync_timestamp	1,622,641,520,767
last_sync_result	success
last_sync_timestamp	1,622,641,520,767
last_sync_version	ADKa+glYf0UWnXQFV9Ovhl3kqLCORdwF
linked_to_assistant	0
name	julriley1990@gmail.com
requires_full_resync	0
rowid	1

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



Conducting Forensic Investigations on Mobile Devices (4e)
vWorkstation
2025-02-24 16:55:31
Karan Atul Vora

Table of contents

Section 3: Challenge and Analysis

Part 1: Research Report Writing for Digital Forensics

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

Key sections to include are: -Overview/Case Summary: A brief explanation of the case, including how the examiner became involved.Forensic Acquisition & Exam Preparation: Detailed steps of evidence acquisition and preparation, ensuring proper chain of custody.Findings and Analysis: The core of the report, explaining what was discovered during the examination, including data and tools used.Conclusion: Summarizing the results and the implications of the findings.
Best Practices: -Maintain objectivityBe clear and conciseEnsure accuracyProvide a clear timelineDocument tools and methodsUse proper chain of custodyKeep it structuredAvoid biasMake it legally defensibleProofread

Part 2: Draft a Forensic Report

Case Summary

The Madison Police Department confiscated two smartphones—one iOS and one Android—as part of an investigation into an organized car theft operation. The suspects, using the codenames Bonnie and Clyde, were linked to multiple stolen vehicles. The goal of this investigation was to extract and analyze digital evidence from these devices using Paraben's E3 forensic software to identify incriminating data such as contacts, messages, call logs, notes, images, and application data.

Findings and Analysis

iOS Device Analysis:Contacts & Messages:Several messages linked to stolen vehicles were found, including communications with a contact named "Stinky" discussing a specific car and another with "ICE Mylady" indicating a vehicle's location in Windy City.Calendar & Notes:A calendar event with a car icon suggested premeditated vehicle theft.Notes contained crucial information, including awareness of a known license plate number and details about replacing plates.Images & Evidence Comparisons:Thirteen car images, some displaying license plates, were found.A comparison of two forensic snapshots revealed missing and altered notes, indicating possible tampering between extractions.Android Device Analysis:
Device Information & User Identification:ICE contacts identified the device owner as "Bonnie."Email accounts included a contact named “Tom Audi&BMW,” suggesting a link to car sales.Browser History & Whisper Chats:Browsing history included searches related to stolen car models and transactions on eBay Motors.Whisper chat messages referenced a Porsche 911 and a transaction location in Windy City, corroborating findings from the iOS device.User Activity & Application Data:Activity logs confirmed usage of Whisper, Chrome, VPN, and contacts during the suspected crime timeframe.Keep Notes contained records of license plate alterations.

Conclusion

The forensic analysis provided substantial evidence linking the suspects to organized car theft activities. The synchronized findings from both devices—matching messages, notes, and locations—strongly indicate coordinated criminal behavior. The discovery of modified data further suggests attempts to cover their tracks. This report will support further legal proceedings and assist law enforcement in charging the suspects accordingly.