



Universidad Carlos III de Madrid

Report for Autopsy Demo - Mobile devices

Juan Diego Llano Miraval

Fecha: 18/05/2024

procedure

1. Which device was this image taken from?

R. It is a Nexus 5X, I was able to look at the device properties and check the model:

Listing

/LogicalFileSet1/Mobile_image/Live Data

TableThumbnailSummary

Name	S	C
Dumpsys Data		
device_datetime_utc.txt		
device_properties.txt		
task_stats.txt		
usage_stats.txt		
wifi_stats.txt		

HexTextApplicationFile MetadataO

StringsExtracted TextTranslation

Page: 1 of 1 Page<=>Matches on

[ro ril.svite l x]: [false]
[ro.secure]: [1]
[ro.serialno]: [0260414f8582cab2]
[ro.setupwizard.enterprise_mode]: [1]
[ro.setupwizard.rotation_locked]: [true]
[ro.sf.lcd_density]: [420]
[ro.telephony.call_ring.multiple]: [0]
[ro.telephony.default_cdma_sub]: [0]
[ro.telephony.default_network]: [22]
[ro.treble.enabled]: [false]
[ro.url.legal]: [http://www.google.com/intl/
[ro.url.legal.android_privacy]: [http://www.g
[ro.vendor.build.date]: [Thu Aug 30 04:37:31
[ro.vendor.build.date.utc]: [1535603851]
[ro.vendor.build.fingerprint]: [google/bullh
[ro.vendor.extension_library]: [libqti-perfd-c
[ro.vendor.product.brand]: [google]
[ro.vendor.product.device]: [bullhead]
[ro.vendor.product.manufacturer]: [LGE]
[ro.vendor.product.model]: [Nexus 5X]

2. What is the device’s IMEI number?
- R. The IMEI is 353626075095047, on the sim DB file we can retrieve the device ID.

/LogicalFileSet1/Mobile_image/Agent Data

Table

Thumbnail

Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Me
agent_mmssms.db-journal				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated
agent_sim.db	▼		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	16384	Allocated	Allocated
agent_sim.db-journal				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated
calendar.db	▼		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	24576	Allocated	Allocated
calendar.db-journal				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated
contacts2.db			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	16384	Allocated	Allocated

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Table

data

1 entries

Page 1 of 1

Export to CSV

_id	sim_card...	sim_serial_number	sim_cou...	sim_ope...	sim_oper...	subscriber_id	phone_n...	phone_t...	voicemail...	voicema...	device_id
1	READY	89254021124117898122	ke	63902	Safaricom	639021121789812		GSM	Voicemail		353626075095047

3. What mobile network does the SIM belong to?
- R. From the previous image we can also get the operator of the sim: Safaricom.
4. When was this text message received “Nitumie kwa hii namba plz (0707701525) itatoa jina Douglas Mugendi.”
- R. From tge mmssms.db we can check the messages sent. From there we looked for the requested message and got the following date: 1571833969012, in the normal date format it is: Wednesday, October 23, 2019 2:32:49.012 PM GMT+02:00 DST

agent_mmssms.db

0

0000-00-00 00:00:00

0000-00-00 00:00:00

0000-00-00 00:00:00

0000-00-00 00:00:00

28672

Allocated

Allocated

unknov

agent_mmssms.db-journal

0

0000-00-00 00:00:00

0000-00-00 00:00:00

0000-00-00 00:00:00

0000-00-00 00:00:00

0

Allocated

Allocated

unknov

agent_sim.db

0

0000-00-00 00:00:00

0000-00-00 00:00:00

0000-00-00 00:00:00

0000-00-00 00:00:00

16384

Allocated

Allocated

unknov

agent_sim.db-journal

0

0000-00-00 00:00:00

0000-00-00 00:00:00

0000-00-00 00:00:00

0000-00-00 00:00:00

0

Allocated

Allocated

unknov

calendar.db

0

0000-00-00 00:00:00

0000-00-00 00:00:00

0000-00-00 00:00:00

0000-00-00 00:00:00

24576

Allocated

Allocated

unknov

calendar.db-journal

0

0000-00-00 00:00:00

0000-00-00 00:00:00

0000-00-00 00:00:00

0000-00-00 00:00:00

0

Allocated

Allocated

unknov

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Table

mmssms

33 entries

Page 1 of 1

Export to CSV

_id	body	type	address	date
29	Hey girl	2	0713259913	1575372836037
30	Hey dubz	2	0754061641	1575372827522
31	So am i	2	0707544404	1575372818114
27	Hey there friend	2	0707 544404	1575371765502
33	Renew your Safaricom HOME Fibre TODAY by dialing *400*40# or download the Safaricom HOME App from Appstore or Playstore. I...	1	SAFARICOM	1578658987745
32	Dear customer, Secure your line with Jitambulishe today. Call 456 to enroll your voice and get Ksh 20 airtime. Thank you	1	SAFARICOM	1576583829382
28	I'm good, miss penny	1	+254707544404	1575371804656
26	Secure your line from fraudsters using your voice as your password. Call 456 for free to enroll your Voice on Jitambulishe.	1	SAFARICOM	1574665355429
25	Get 50% MORE Airtime that has NO EXPIRY for Calls and SMSs across ALL NETWORKS. Dial *544*2# now and enjoy. Don't miss out o...	1	SAFARICOM	1574658137681
24	Jambo! Important Info: Dial *456# to access key Safaricom services like Bonga enrollment, *544# & *444# for Data & Minutes Offers ...	1	SAFARICOM	1574406204358
23	Biggest betting site in Kenya with BIG ODDS + FREE WITHDRAWALS AFTER WIN+1000 FREE KARIBU BONUS is BACK!Karibu and join ...	1	ScorePesa	1574320297241
22	Get 50% Extra airtime with No Expiry Date for Calls and SMSs across all networks. Dial *544# then select option 2 to buy Extra airtime f...	1	SAFARICOM	1574317382073
21	Your WhatsApp code: 467-794You can also tap on this link to verify your phone: v.whatsapp.com/467794Don't share this code with ...	1	WhatsApp	1574253441494
20	Get 50% MORE Airtime that has NO EXPIRY for Calls and SMSs across ALL NETWORKS. Dial *544*2# now and enjoy. Don't miss out o...	1	SAFARICOM	1573460008154
19	Did you know you can enjoy upto 100% Bonus to call your friends and Family? Simply dial *460# to register on Stori Ibambe.	1	SAFARICOM	1573196571992
18	WE ARE BACK!Visit www.scorepesa.co.ke or Sms word REGISTER to 29008 to Join the best betting site in KenyaENJOY 1K KARIBU BO...	1	ScorePesa	1573190206140
17	Earn Bonga Points which you can redeem for Talk-time (Minutes), Data, SMS or a Phone. To register dial *456# and select Bonga to ...	1	SAFARICOM	1573023757970
16	<#> Your 6-digit Twitter confirmation code is 649677./XGYNXWncmi	1	Twitter	1572937292508
15	Get 50% MORE Airtime that has NO EXPIRY for Calls and SMSs across ALL NETWORKS. Dial *544*2# now and enjoy. Don't miss out o...	1	SAFARICOM	1572937013583
14	Your WhatsApp code: 598-243You can also tap on this link to verify your phone: v.whatsapp.com/598243Don't share this code with ...	1	WhatsApp	1572936902987
13	335093 is your Facebook confirmation code	1	FACEBOOK	1572936323067
12	Congratulations!! You have received 50.00 KSH Bonus Airtime (no expiry) to call and text across ALL NETWORKS! For balance Send t...	1	Safaricom	1572934675529
11	Recharge of 50.00 KSH by Mpesa account 254707544404 was successful. Balance:50.00 KSH,expiry date:2020-02-03.Tariff: Uwezo. Bun...	1	Safaricom	1572934663673
10	Did you know you can now browse and Chat with NO EXPIRY DATE? To connect more simply Dial *54...	1	SAFARICOM	1572680407085
9	Did you know that recharging airtime using M-PESA is FREE? Simply go to M-PESA menu and select Buy Airtime. Safaricom keeps y...	1	SAFARICOM	1572591792239
8	Register for MPESA today at a Safaricom shop or MPESA agent to conveniently Send Money to friends and relatives, pay for Goods ...	1	SAFARICOM	1572418959247
7	Dear Customer;KCB Mpesa soft loan is now available at 5% send 555555 to activate loan. @10,000/= @50,000/= @100,000/= @250,00...	1	+254758635848	1572196883743
6	Secure your line from fraudsters using your voice as your password. Call 456 for free to enroll your Voice on Jitambulishe.	1	SAFARICOM	1571986940203
5	Nitumie kwa hii namba plz (0707701525) itatoa jina Douglas Mugendi.	1	+254794660124	1571833969012

From UNIX Timestamp

Units

Milliseconds (ms)

1571833969012

RBC 13

1

Output

Wed 23 October 2019 12:32:49.012 UTC

5. What was the number that send the message “Nitumie kwa hii namba plz (0707701525) itatoa jina Douglas Mugendi.”?








R. From the previous image we can also see that in the table we have the sender address:
+254794660124

6. An international call was received by the device. Which country did the call come from?



R. On the Contacts db we have a table for calls, inside we can see this number: +447418342582 the +44 code is from United kingdom.

Logical Reset / Mobile Image / Agent Data

Table	Thumbnail	Summary
-------	-----------	---------

Name	S	C	O	Modified Time	Change Time
 agent_sim.db-journal				0000-00-00 00:00:00	0000-00-00 00:00:00
 calendar.db			0	0000-00-00 00:00:00	0000-00-00 00:00:00
 calendar.db-journal				0000-00-00 00:00:00	0000-00-00 00:00:00
 contacts2.db			0	0000-00-00 00:00:00	0000-00-00 00:00:00
 contacts2.db-journal				0000-00-00 00:00:00	0000-00-00 00:00:00
 downloads.db			0	0000-00-00 00:00:00	0000-00-00 00:00:00

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Comments
-----	------	-------------	---------------	------------	----------------	------------------	----------

Table	calls	7 entries	Page 1 of 1	 	Export
-------	-------	-----------	-------------	---	--------

id	name	number	date	type	duration
1		0722958434	1574543382918	3	0
2		0722958434	1574543329678	3	0
3	Doobie Doo	0707544404	1574253394959	3	0
4		+447418342582	1572937001632	1	17
5		+447873056583	1572936981612	1	1
6		0712012457	1571804434845	3	0
7		0712012457	1571804351056	3	0

7. What is the name of the 7-letter wireless network the device has connected to at some point?

R. We can see the wifi configuration on the wifi.db, there we find the SSID: kongoni

wifi.db		0	0000-00-00 0
wifi.db-journal			0000-00-00 0

Hex

Text

Application

File Metadata

OS Account

Data Artifact

Table

wifi_configurations

4 entries

Page 1 of 1

networkId	SSID	macAdd...	security...
0	kongoni		WPA-PSK
1	Rogue		WPA-PSK
2	E-KRAAL-HUB		WPA-PSK
3	Robot		WPA-PSK

8. What is the mobile device owner’s username on Twitter?

R. Digging throw the files, we found an account file where we can retrieve the twitter account name:
KamiLenana

/LogicalFileSet1/Mobile_image/Live Data/Dumpsys Data

TableThumbnailSummary

Name	S	C	O	Modified Time
accessibility.txt			0	0000-00-00 00:00:00
account.txt			0	0000-00-00 00:00:00
activity.txt			0	0000-00-00 00:00:00
alarm.txt			0	0000-00-00 00:00:00
appops.txt			0	0000-00-00 00:00:00
appwidget.txt			0	0000-00-00 00:00:00

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis

StringsExtracted TextTranslation

Page: 1 of 1 Page<=>Matches on page: - of - Match<=>

User UserInfo{0:Coco:13}:
Accounts: 7
Account {name=cocoash100@gmail.com, type=com.google}
Account {name=lenanakami@gmail.com, type=com.google}
Account {name=Facebook, type=com.facebook.auth.login}
Account {name=Messenger, type=com.facebook.messenger}
Account {name=943658017, type=org.telegram.messenger}
Account {name=WhatsApp, type=com.whatsapp}
Account {name=KamiLenana, type=com.twitter.android.auth.login}

9. List the google accounts that were linked to this device?

R. From the previous image we can retrieve the google accounts too: cocoash100@gmail.com and lenanakami@gmail.com

10. Identify the forensics app installed on the device?

R. On the sd card we digged into android data, this usually have information of the apps, and we found a folder related to the forensic app: AFLogical OSE: Open source Android Forensics app and framework

/LogicalFileSet1/Mobile_image/sdcard/sdcard/Android/data/com.viaforensics.android.aflogical_ose

TableThumbnailSummary

Name	S	C	O	Modified Time	Change Time	Access Time	Created
files				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00