Android 10 Image

Description

An image of Android 10 was created using a stock Android image from Google. Several popular applications (apps) were populated with user data utilizing the capabilities of each individual app. The stock Android apps were also populated with user data.

All times listed in this document are 24-hr, Eastern Standard Time (UTC -0500).

Some of the data available in the apps were sync'd with data that had been previously populated. Information about the previously populated data can be found in the documentation of the respective images, which can be found at https://thebinaryhick.blog.

Phone Information

Make:	Google Pixel 3
Model:	G013A
Storage:	64 GB
RAM:	4GB
Carrier:	Google Fi
Phone Number:	919-579-4674
Serial:	8CEX1N716
Wi-Fi MAC:	7c:d9:5c:ac:a2:cf
BT MAC:	7c:d9:5c:ac:a2:ce

Android Version Information

Version:	10
Build:	QQ1A.200105.003
Patch Level:	January 1, 2020
Kernel:	4.9.185-g9f181f6db9d7-ab6027027 #0 Fri Nov 22 18:17:08 UTC 2019
Baseband:	g845-00086-191011-B-5933466
Passcode:	0731 (User 1)
Passcode:	1234 (User 2)

PROCEDURE

1. The phone was reset to factory defaults, including a wipe of the device. Android was then installed.
2. A Google Fi account was added in order to apply cellular service to the device.
3. The bootloader was unlocked.
4. Magisk, a rooting application, was added to the device in order to gain root level access to the operating system.
5. Thirty-one (31) non-stock apps were installed from the Google Play store and populated with user data based on each app's respective capabilities.
6. Stock Android apps were populated with user data based on each app's respective capabilities.
7. A second user profile was added to the device. User activity data was generated.

GOOGLE ACCOUNT INFORMATION

Email Address: thisisdfir@gmail.com (default – added to device on 01/29/2020)
Password: ^zAvQPkHn3,CaUBUJ4R33si4Yrd8NJ+%V

Email Address: thisisdfirtwo@gmail.com (2nd user profile – added on 02/14/2020)
(RmyrwZrcdLG2?UB8nPi3t7/xVb>zyh89

NON-STOCK APP INFORMATION

The non-stock apps that were loaded and tested are alphabetically listed below. Information about the app, including user interaction, is also listed.

Name: Calculator Pro+ - Private Message & Call Screening
Version Number: 4.1.58
Install Date: 01/29/2020
Install Time: 12:03

Note:

Date	Time	Action	Message
01/31/2020	20:37	Uninstalled App	

Name: Discord
Version Number: 10.2.8
Install Date: 01/29/2020
Install Time: 12:02

User Name: thisisdfir

Date	Time	Action	Message
01/29/2020	13:20	Signed in	
	15:20	Joined Server	
01/31/2020	20:39	Message sent	Well hello there.
	20:41	Message received	Hey there! Thanks for helping out.
	20:42	Picture received	
	20:43	Picture saved	
	21:09	Message sent	Thanks!
	21:18	Picture sent	

Name: Dust
Version Number: 6.1.3.2887
Install Date: 01/29/2020
Install Time: 12:04

User Name: thisisdfir100

Date	Time	Action	Message
1/29/2020	16:15	Signed in	

Name: Facebook Messenger
Version Number: 219.0.0.10.122
Install Date: 01/29/2020
Install Time: 12:08

Username: 919-579-4674
Password: fallout-lamp-lymphoma

Note:

Date	Time	Action	Message
01/29/2020	13:50	Sign in	
02/01/2020	13:48	Added user via QR Code	
	13:49	Message sent	Hi there!
	13:50	Message received	Hey, how are you?
	13:51	Message sent	Good. Hope you are.
	13:52	Message received	I am. Thanks!
	13:57	Picture received	
	13:58	Picture saved	
	13:59	Picture sent	
	14:00	Outgoing audio call	(1:10)
	14:02	Incoming video call	(1:17)
02/09/2020	13:10	Shared live location (ended at 13:14)	

Name: GalleryVault
Version Number: 3.14.82
Install Date: 01/29/2020
Install Time: 12:06

Note: Passcode was set to 1234

Date	Time	Action
01/31/2020	21:20	Set passcode
	20:41	Added picture

Name: Google Podcasts
Version Number: 1.0.0.266384425
Install Date: 01/29/2020
Install Time: 12:04

Note: This is not a stock app. Some episodes were played through Android Auto; see entries for that app for playback dates/times.

Date	Time	Action
01/30/2020	08:19	Downloaded “NPR Up First” podcast
	08:20	Downloaded “Digital Forensic Survival Podcast - 206”
	08:21	Downloaded “Internet of Things” podcast
02/13/2020	21:09	Started “Digital Forensic Survival Podcast”
		Casted to “Office Display”
	21:26	Started “Digital Forensic Survival Podcast – 207”
	21:44	Stopped playback
		Stopped casting

Name: Imgur
Version Number: 4.5.9.12223
Install Date: 01/29/2020
Install Time: 12:12

Username: thisisdfir@gmail.com
Password: lack-triumph-porous9

Note:

Date	Time	Action
02/01/2020	14:07	Downloaded picture
		(liked picture previously downloaded)
	14:09	Liked picture
	14:10	Downloaded liked picture
	14:12	Liked GIF
	14:13	Upvoted liked GIF
	14:14	Downloaded picture
	14:15	Downloaded picture

Name: imo (or imo HD)
Version Number: 9.8.000000010915
Install Date: 01/29/2020
Install Time: 12:08

Note: Phone number 919-574-4674

Date	Time	Action	Messages
01/29/2020	13:32	Signed In	
02/01/2020	14:17	Message sent	Hey there. How was Imgur?
	14:18	Message received	You tell me. You were there.
	14:19	Message sent	True. It was underwhelming.
	14:21	Picture received	
	14:22	Downloaded received picture	
	14:23	Picture sent	
	14:25	Outgoing audio call	(1:15)
	14:27	Incoming video call	(1:18)

Name: Instagram
Version Number: 126.0.0.25.121
Install Date: 01/29/2020
Install Time: 13:08

Username: thisisdfir
Email: thisisdfir@gmail.com
Password: moleskin-tepee-ageless

Note: Five following, one follower. Previous data resides in this app due to account sync'ing. Only the data that was populated during the creation of this image is described below. For information about the previous data, see the documentation for the Android 7.x, Android 8.x, and Android 9.x images. Chats that appear in the app Threads also appear here.

Date	Time	Action	Messages
01/29/2020	13:38	Sign in	
02/01/2020	14:33	Picture received	
	14:34	Saved screenshot of picture	
	14:35	Message sent	Thanks!
	14:36	Message received	No problem. You need photos.
		Incoming video call	(~1:18)

Name: kik
Version Number: 15.19.0.22104
Install Date: 01/29/2020
Install Time: 12:08

Username: ThisIsDFIR
Email: thisisdfir@gmail.com
Password: tide-asylum-defense

Note:

Date	Time	Action	Messages
01/29/2020	13:29	Sign In	
02/01/2020	14:40	Message received	I don't even know why we are doing Kik. Isn't it shutting down soon?
	14:42	Message sent	No. It was bought by Whisper, so it is staying online.
	14:43	Message received	Great (sarcasm).
	14:46	Message sent	It looks like the video calling feature is gone. And there are ads now.
	14:47	Picture received	
		Downloaded picture	
	14:48	Picture sent	

Name: Line
Version Number: 10.0.2
Install Date: 01/29/2020
Install Time: 12:05

Display Name: This Is DFIR
Phone Number: +1 919-579-4674

Note:

Date	Time	Action	Messages
01/29/2020	13:20	Sign in	
02/01/2020	14:49	Added friend by QR code	
	14:51	Message sent	And another chat app. There are so many!
	14:52	Message received	Too many I think.
		Message sent	Agreed.
	14:53	Picture received	
		Downloaded picture	

	14:54	Incoming audio call	(1:13)
	14:56	Outgoing video call	(1:26)
	14:58	Picture sent	
02/09/2020	13:05	Shared static location	

Name: Magisk Manager
Version Number: 20.3
Install Date: 01/29/2020
Install Time: 11:35

Note: This app is installed in order to root the test phone. No data was generated. App was downloaded via Chrome and installed.

Date	Time	Action	Messages
01/29/2020	11:35	Installed app	

Name: MeWe
Version Number: 6.0.9.4
Install Date: 01/29/2020
Install Time: 12:02

Username: This Is DFIR
Password: loaves-now-gushy-jim9

Note: Audio and video calls required subscriptions and were not purchased.

Date	Time	Action	Messages
01/29/2020	13:39	Sign In	
02/03/2020	21:40	Added friend	
	21:43	Message sent	So this is the first time I've used this app.
	21:46	Message received	Yeah, it just seems like a mash up of other apps.
	21:49	Message sent	It is ok. Just another chat app.
	21:50	Picture sent	
	21:57	Picture received	

Name: Signal
Version Number: 4.53.7
Install Date: 01/29/2020
Install Time: 12:06

Username: This Is DFIR
Phone Number: +19195794674

Note:

Date	Time	Action	Messages
01/29/2020	13:31	Sign in	
02/01/2020	15:12	Message received	Wonder why I can switch it back.
	15:14	Message sent	No clue. This is confusing.
	15:15	Message received	Agreed.
		Picture sent	
	15:16	Picture received	
		Downloaded picture	
	15:17	Outgoing video call	(~1:00)
	15:19	Incoming audio call	(~1:15)

Name: Silent Phone
Version Number: 6.10
Install Date: 01/29/2020
Install Time: 12:03

Username: ThisIsDFIR
Password: jurist-turtle-percept
Phone Number: 919-636-5829

Note:

Date	Time	Action	Messages
02/01/2020	15:41	Sign In	
	15:45	Outgoing audio call	(1:10)
	15:48	Incoming audio call	(1:06)
	15:50	Message sent	Hi there!
	15:52	Message received	Hey. This is pretty neat.
		Message sent	I am going to delete this message
	15:53	Message received	Ok.
	15:54	Message deleted	(message sent at 15:52)
	15:55	Message sent	The message was deleted.
		Picture sent	
		Picture received	

Name: Skout
Version Number: 6.17.0
Install Date: 01/29/2020
Install Time: 12:07

Username: thisisdfir@gmail.com
Password: *3qpAs82ZgT9UBFZ}TZCqmg4%Av6R&nc

Note:

Date	Time	Action	Messages
01/29/2020	13:45	Signed in	
02/01/2020	15.:25	Message sent	Hi!
	15:26	Message received	This is a terrible app.
	15:27	Message sent	Agreed. At least there is no GPS capabilities.
	15:32	Picture sent	
	15:35	Picture received	

Name: Skype
Version Number: 8.37.0.98
Install Date: 01/29/2020
Install Time: 12:07

Username: +1 919-579-4674
Screen Name: This Is DFIR
Skype Name: live:756b2840ef68b86b
Password: seed-varlet-leftover
Note:

Date	Time	Action	Messages
01/29/2020	13:41	Signed in	
02/01/2020	16:09	Outgoing audio call	(1:05)
	16:18	Message received	Hey there. I forgot we didn't have two test accounts.
	16:19	Message sent	That's ok. We should be good now.
	16:20	Message received	Agreed.
	19:47	Picture received	
		Downloaded picture	
	19:48	Picture sent	
	19:49	Outgoing video call	(1:10)
	19:51	Incoming audio call	(1:16)

Name: Snapchat
Version Number: 10.74.6.0
Install Date: 01/29/2020
Install Time: 12:09

Username: thisisdfir
Name: This Is DFIR
Email Address: thisisdfir@gmail.com
Password: antelope-waxwing-tidbit

My Eyes Only: 0957

Note: Chat settings were changed from the default (delete after viewing) to delete after 24 hours. Some account data was sync'd from Snapchat servers due to previous population.

Date	Time	Action	Messages
01/29/2020	13:30	Signed In	
02/13/2020	19:51	Snap sent	
	19:57	Message received	Got it. Nice
	19:58	Message sent	Thanks. Almost done
	19:59	Message received	I know. Pretty exciting.
		Picture received	
	20:00	Outgoing video call	(~1:00)
	20:02	Incoming audio call	(1:10)
	20:04	Snap received	
	20:05	Moved picture to My Eyes Only	

Name: Spotify
Version Number: 8.5.42.812
Install Date: 01/29/2020
Install Time: 12:06

Username: thisisdfir
Name: Thisisdfir
Email Address: thisisdfir@gmail.com
Password: socket-ominous-tactics

Note:

Date	Time	Action
01/29/2020	13:46	Signed In
02/04/2020	15:52	Commercial (x2)
		Red Hot Chili Peppers – Scar Tissue

	15:53	Google Cast to Office Speaker
	15:56	Temple Of The Dog – Hunger Strike – 25th Anniversary
	16:00	Pearl Jam - Black
	16:05	Commercial (Starbucks)
		Commercial (O'Rielly's Auto Parts)
	16:06	Mother Love Bone – Come Bite The Apple
	16:12	Foo Fighters – My Hero
	16:15	Stopped playback
		Stopped Google Cast

Name: Telegram
Version Number: 5.14.0
Install Date: 01/29/2020
Install Time: 12:06

Name: This Is DFIR
Phone Number: +1 (919) 579-4674

Note:

Date	Time	Action	Messages
01/29/2020	13:31	Signed In	
02/03/2020	20:58	Message sent	Good evening.
	20:59	Message received	Hey there. How are things?
	21:00	Message sent	Good. Just finishing up for the day. How about you?
	21:01	Message received	About the same.
		Picture received	
	21:02	Picture saved	
	21:03	Picture sent	
	21:04	Incoming audio call	(1:10)
	21:06	Outgoing audio call	Call was not picked up on other line (canceled)

Name: TextNow
Version Number: 20.1.1.0
Install Date: 01/29/2020
Install Time: 12:08

Username: thisisdfir@gmail.com
TextNow Number: 984-235-2054
Password: flirt-dewberry-wardrobe

Note:

Date	Time	Action	Messages
02/08/2020	14:54	Sign in	
	15:00	Message received	Hi there!
	15:01	Message sent	Back at it again, I see.
	15:03	Message received	Yep! Have to keep generating data.
	15:05	Outgoing audio call	(1:50)
	15:08	Incoming audio call	Call was missed
	15:09	Picture received	
	15:10	Picture sent	
	15:11	Message received	I wonder why I can't call you or send you pictures
	15:35	Picture saved	

Name: Threads (by Instagram)
Version Number: 126.0.0.25.121
Install Date: 01/29/2020
Install Time: 12:02

Username: thisisdfir
Email: thisisdfir@gmail.com
Password: moleskin-tepee-ageless

Note: Account information is the same as Instagram. Messages that appear in Instagram also appear here.

Date	Time	Action	Messages
01/29/2020	13:33	Signed In	
	21:14	Message received	So what appears here does not show up in Instagram?
	21:19	Message sent	No it does. Only the chats with people you identify as "close friends" will appear here.
	21:23	Incoming video call	(1:17)
	21:26	Picture sent	
	21:27	Picture received	

Name: TikTok
Version Number: 14.7.5
Install Date: 01/29/2020
Install Time: 12:07

Username: 9195744674
Password: relation-meal-tenpin

Note:

Date	Time	Action	Message
01/29/2020	13:43	Signed in	
02/08/2020	16:06	Added friend	
	16:09	Message sent (to self)	People love this app. I don't see the appeal
	16:11	Message sent	I do not see the appeal of this app
	16:12	Message received	That is because you are old.
02/09/2020	12:56	Uploaded video	Video had caption "Nice Day!"
	13:17	Someone liked video	Comment: "Very nice!"
	13:21	Liked comment left at 13:17	
	13:22	Replied to comment	Thanks!
	13:26	Liked a video	
		Left comment	Looks nice there, too.

Name: TOR Browser
Version Number: 68.4.1
Install Date: 01/29/2020
Install Time: 12:03

Note:

Date	Time	Action
01/31/2020	21:31	Started browser
	21:32	Searched "enigma machine" via Duck Duck Go
	21:32	Visited Wikipedia page
	21:36	Downloaded picture from Wikipedia page
	21:38	Searched "dfrws" via Duck Duck Go
	21:39	Visited "http://dfrws.org"
	21:41	Quit browser

Name: Twitter
Version Number: 8.29.0-release.00
Install Date: 01/29/2020
Install Time: 12:09

Username: @TDfir
Password: ides-cudgel-husking

Note: Previous data resides in this app due to account sync'ing. Only the data that was populated during the creation of this image is described below. For information about the previous data, see the documentation for the Android 7.x, Android 8.x, and Android 9.x images.

Date	Time	Action	Messages
01/29/2020	14:45	Signed in	
02/03/2020	21:30	Saved 2 pictures from previous chats	
	21:32	Message sent	Good ol' Twitter.
	21:33	Message received	There you are.
	21:34	Picture sent	
		Message sent	Remember that guy?
	21:36	Message received	I do!
	21:37	Picture received	

Name: Venmo
Version Number: 7.45.0
Install Date: 01/29/2020
Install Time: 12:02

Username: @ThisIs-DFIR
Password: perfuse-show-rubric-the

Note:

Date	Time	Action	Messages
01/31/2020	17:23	Sign in	
02/13/2020	20:47	Sent Payment ($5.00) (Private)	Android 10 image.
	20:48	Message received	Thanks!
	20:49	Received payment ($5.00) (Friends)	For the Android 10 image again.
	20:50	Message sent	Thank you.

Name: Viber
Version Number: 12.2.2.1
Install Date: 01/29/2020
Install Time: 12:05

Phone: 919-579-4674

Note:

Date	Time	Action	Messages
02/08/2020	15:15	Sign in	
	15:20	Message sent	You there?
	15:21	Message received	Yes sir.
	15:22	Message sent	Good. Here comes a picture.
	15:23	Picture sent	
		Message received	Got it.
	15:24	Picture received	
	15:26	Incoming video call	Call was missed.
	15:28	Incoming video call	Call was missed.
	15:29	Outgoing video call	(1:10)
	15:30	Incoming audio call	(1:15)
02/09/2020	13:06	Shared static location	

Name: WhatsApp
Version Number: 2.20.11
Install Date: 01/29/2020
Install Time: 12:09

Phone: 919-574-4674

Note:

Date	Time	Action	Messages
01/29/2020	13:37	Signed in	
02/08/2020	15:55	Message sent	Hi there! I switched over.
	15:56	Message received	Awesome!
	15:57	Picture received	
		Message sent	The Osbourne!
	15:58	Picture sent	
	15:59	Incoming video call	(~1:10)
	16:01	Outgoing audio call	(1:10)
02/09/2020	13:00	Shared live location	Here I am!!
		Shared live location (ended at 13:04)	Here I am!!
	13:05	Shared static location	

Name: WeChat
Version Number: 7.0.10
Install Date: 01/29/2020
Install Time: 12:04

Note:

Date	Time	Action	Messages
02/13/2020	20:35	Uninstalled app	

Name: Wickr Me
Version Number: 5.45.4
Install Date: 01/29/2020
Install Time: 12:04

Username: ThisIsDFIR
Password: offing-ammo-railbird
Phone: +1 919-579-4674

Note:

Date	Time	Action	Messages
01/29/2020	13:47	Signed in	
01/31/2020	20:00	Added phone number to account	
02/09/2020	13:28	Shared static location	
	13:33	Shared live location (ended at 13:39)	
02/13/2020	20:08	Message sent	What's up?!
	20:09	Message received	Not much. Just trying to wrap up this image.
	20:10	Message sent	Word.
	20:11	Message received	Hey delete this message after you read it.
		Message sent	Ok.
	20:12	Deleted received message from 20:11	
	20:13	Outgoing audio call	(1:05)

Name: Wire
Version Number: 3.44.877
Install Date: 01/29/2020
Install Time: 12:04

Name: This Is DFIR
Username: thisisdfir@gmail.com
Password: abysmal-dress-pursue
Phone: 919-579-4674

Note:

Date	Time	Action	Messages
01/29/2020	13:28	Signed in	
01/31/2020	20:04	Updated phone number	
02/08/2020	15:39	Message sent	I am here. Have you switched over?
	15:40	Message received	Yep! I will send a picture in just a moment.
	15:42	Picture received	
		Message sent	Nice!
	15:43	Picture sent	
	15:44	Outgoing video call	(1:10)
	15:46	Incoming video call	(1:05)
02/09/2020	13:09	Shared static location	

STOCK APP INFORMATION

The stock apps that were tested are alphabetically listed below. Information about the app, including user interaction, is also listed. Please note that each app had previous data that was sync'd with the test device. Only the data that was populated during the testing will be show here. For information about the previously populated data, please see the documentation describing the Android 7.x, Android 8.x, and Android 9.x images, which can be found at https://thebinaryhick.blog.

Name: Android Auto
Version Number: 5.0.500224-release

Note: This app is a default app in Android 10.

Each time the device was connected to the vehicle also indicates a power event (on charge). Power event stops when device is disconnected. Messages that are read/dictated will appear in the Message section of the document. Each connection event also indicates a Bluetooth connection.

Date	Time	Action
01/30/2020	08:56	Connect to car & setup app
	08:58	Started "NPR Up First" podcast
	09:00	Invoked Google Assistant and asked for directions:
		"I need directions to 7629 Purfoy Road in Fuquay-Varina, North Carolina"
	09:01	Started navigation in Maps to location
	09:16	Disconnected from car
02/09/2020	13:44	Connect to car
	13:46	"Give me directions to Sir Walter Coffee in Holly Springs, North Carolina."
	13:47	Started "NPR Up First" podcast
	13:49	Got directions to Sir Walter Coffee in Holly Springs, NC
	13:51	Started "Digital Forensics Survival Podcast."
	13:59	Disconnect from car
	14:09	Connect to car
		Continued "Digital Forensics Survival Podcast."
	14:16	Disconnect from car

Name: Camera
Version Number: 7.2.018.281779528

Note: For information about the disposition of the picture listed below, see the entry for the Photos app.

Date	Time	Action
02/09/2020	13:23	Took picture

02/13/2020	19:20	Took picture

Name: Chrome
Version Number: 79.0.3945.136

Note:

Date	Time	Action
01/29/2020	11:33	Start Chrome
		Search “magisk”
		Traveled to “https://www.magiskmanager.com”
	11:34	Downloaded file “MagiskManager-V7.5.1.apk”
	11:35	Installed via Chrome

Name: Docs
Version Number: 1.20.022.05.40

Note: An action to move the document was taken within Drive. See that app’s entries for details.

Date	Time	Action
02/09/2020	14:51	Created a new test document “Untitled document.”
	14:52	Changed title to “Test Document 11.”

Name: Drive
Version Number: 2.20.035.04.40

Note:

Date	Time	Action
02/09/2020	14:54	Deleted “Test Document 7” from “Test Folder 1.”
	14:55	Created “Test Folder 2”
		Compressed “Test Document 11” to “Test Document 11.zip”
	14:56	Moved “Test Document 11” to “Test Folder 2.”

Name: Duo
Version Number: 71.0.290855224.DR71_RC06

Note:

Date	Time	Action
02/13/2020	20:20	Outgoing video call (~1:00)
	20:23	Outgoing audio call (1:05)
	20:24	Incoming video call (1:05)

Name: Gmail
Version Number: 2019.12.30.289507923.release

Note:

Date	Time	Action
02/13/2020	21:45	Sent an email with a picture attachment
	21:51	Sent an email with two picture attachments

Name: Google
Version Number: 10.93.13.21.arm64

Note: Some Google activity (Assistant) was conducted via Android Auto. See the entries for that app for details on that activity. This section will also include activity conducted in the Google Search Bar (GSB) from the home screen. Messages that were sent using Google Assistant will also be seen in the Messages app below.

Date	Time	Action
01/31/2020	21:14	Searched “famicom” from GSB
	21:16	Downloaded picture
02/09/2020	13:41	Used “Ok Google” to invoke Google Assistant:
		“Send a text message to Josh Hickman.”
		“I am on my way to the coffee shop. Do you want anything?”
		“Send it.”

Name: Google Home
Version Number: 2.16.1.10

Note: No action was taken with the app. However, a Google Home Speaker ("Office Speaker") and Google Home Hub ("Office Display") was seen in the app (those devices were setup by a different device).

Date	Time	Action
02/09/2020	15:05	Unlinked "Office Display"
	15:06	Setup Nest Hub (named "Office Display")
	15:07	Went through Voice Match process

Name: Maps
Version Number: 10.33.1

Note: Some Maps activity was conducted via Android Auto. See the entries for that app for details on that activity. Map usage via Android Auto should appear in the Maps area of the image.

Date	Time	Action

Name: Messages
Version Number: 5.2.062 (Pegasus_RC17_xxhdpi.arm64-v8a.phone)

Note: For a listing of messages, please see the Excel spreadsheets in the folder "Messages."

Date	Time	Action	Messages
02/01/2020	15:04	Message sent	Here's Signal
	15:06	Message received	It looks like the messaging is run through the Messages app. Strange
	15:07	Message sent	It might be an attempt at unified messaging…?
	15:08	Message received	Maybe?
	15:09	Message sent	It will be interesting to see where the messages are stored.

02/09/2020	13:41	Message sent	I am on my way to the coffee shop. Do you want anything?
	13:43	Message received	No, thank you.

Name: Phone
Version Number: 43.0.290782351

Note:

Date	Time	Action
01/31/2020	10:16	Missed phone call from "Private Number"
	13:07	Missed phone call from "Private Number"
	15:21	Missed phone call from "Private Number"
02/01/2020	14:28	Missed phone call from "Private Number"
02/03/2020	14:32	Missed phone call from "Private Number"
02/08/2020	15:14	Missed phone call from "+332629243087"
02/12/2020	10:37	Missed phone call from "+1 919-512-1037"
		Missed phone call from "+1 575-586-3247"
02/13/2020	20:29	Outgoing phone call (0:11)
	20:30	Incoming phone call (1:05)

Name: Photos
Version Number: 4.36.0.290828616

Note: Camera and other apps placed pictures in Photos. No actions were taken within the app. If a picture was saved via another app, the entry is documented in that app.

Date	Time	Action
01/31/2020	21:24	Saved IMG_20190917_082637.jpg to phone
	21:25	Saved 2ECED1BB-39FB-454D-8B63-E336F88A0E18.JPG to phone

POWER EVENTS

Below are the power events that occurred on the device.

Date	Time	Action
01/29/2020	10:36	On charger
	10:43	Off charger
01/31/2020	21:49	On charger
02/01/2020	07:27	Off charger
02/03/2020	10:13	On charger
	13:13	Off charger
02/06/2020	19:13	On charger
02/07/2020	08:15	Off charger
02/09/2020	19:14	On charger
02/10/2020	07:20	Off charger
02/12/2020	21:26	On charger
02/13/2020	18:00	Off charger
02/14/2020	09:49	On charger
	09:52	Off charger
	09:53	On charger
	09:56	Off charger
	09:57	On charger
	09:59	System re-start

WI-FI ACCESS POINTS

Below are the Wi-Fi access points the device connected to during the testing period.

SSID	Password
CcookiesDcastleR5	*No password is stored for this BSSID*

GOOGLE CASTING DEVICES

Data was casted to the following Google devices:

Google Home Speaker:

Name:	Office speaker
MAC Address:	D8:6C:63:4A:4F:5E
BSSID:	E0:1C:41:A9:67:94
Build Ver:	146679
Hotspot BSSID:	FA:8F:CA:94:32:BA
SSDP_UDN:	4c397772-95c6-314f-cbb2-877f671b25a5
UMA_Client_ID:	78abc8b3-e036-40bc-bf07-fbcb796e8446

Google Home Hub:

Name:	Office display
MAC Address:	1C:F2:9A:19:0F:03
BSSID:	e0:1c:41:a9:67:94
Build Ver:	146679
Hotspot BSSID:	FA:8F:CA:39:8A:51
SSDP_UDN:	f782d122-cd23-946e-20c5-770a5bab47e7
UMA_Client_ID:	3009b7c3-69cb-49f2-bde3-a07eaf48c03c

These devices should appear in the Google Home map.

BLUETOOTH PAIRED DEVICES

The following Bluetooth device was paired during the populating period:

Name:	Nissan
MAC:	b4:ec:02:73:ff:93

OTHER EVENTS

Below are other various events that occurred on the device.

Date	Time	Action
01/29/2020	10:39	Connect to CcookiesDcastleR5 WiFi network
	10:41	Sign into Google
	10:45	Changed wallpaper
	11:30	Changed to Dark Theme
		Set screen timeout to 5 minutes
02/13/2020	21:31	Took a screenshot
	21:32	Took a screenshot
	21:33	Took a screenshot
02/14/2020	07:51	Added second user account (User 2)
	07:56	Changed wallpaper (User 2)
	08:50	Set screen timeout to 5 minutes (User 2)
	09:37	Took a screenshot (User 2)

Home Screen Layout (User 1)

Screenshots of the home screens. Figure 3 contains a folder that is on screen 2.

Figure 1 – Home Screen 1.

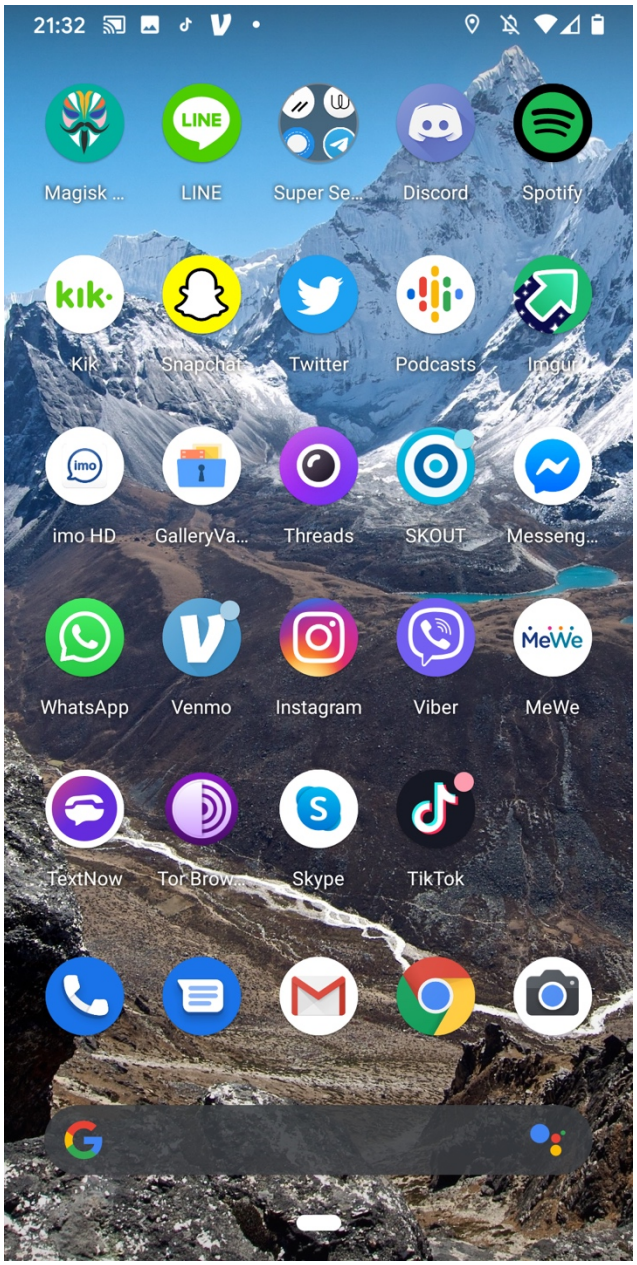

Figure 2 – Home Screen 2.

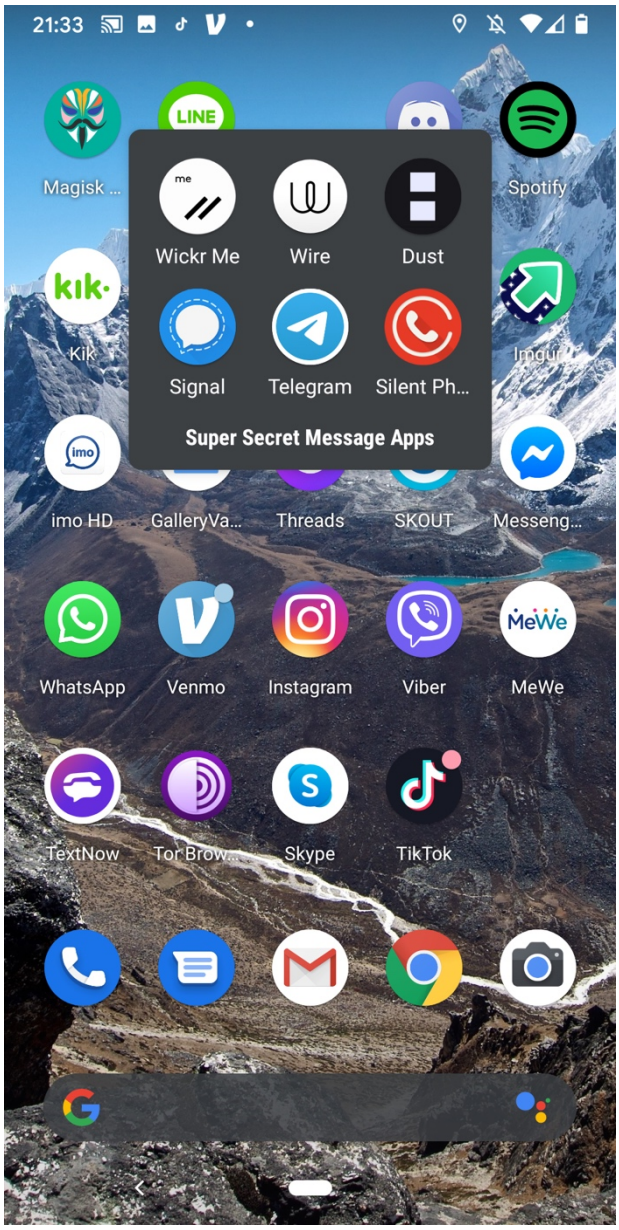

Figure 3 – Home Screen 2 with exposed folder.

USER 2 ACTIVITY

Name: Camera
Version Number: 7.2.018.281779528

Note: For information about the disposition of the picture listed below, see the entry for the Photos app.

Date	Time	Action
02/14/2020	09:16	Took picture

Name: Chrome
Version Number: 79.0.3945.136

Note:

Date	Time	Action
02/14/2020	08:38	Searched “how to hide my apps on android”
		Navigated to “androidpit.com”

Name: Google
Version Number: 10.93.13.21.arm64

Note:

Date	Time	Action
02/14/2020	08:40	Searched “best valentines day gifts” from Google Search Bar on home screen.
	08:41	Navigated to “esquire.com” address

Name: Google Play Store
Version Number: 18.6.43-all [0] [PR] 293212862
Install Date: 02/14/2020
Install Time: 08:45

Note:

Date	Time	Action
02/14/2020	08:44	Searched “snapchat”
	09:25	Searched “wickr”

Name: Gmail
Version Number: 2019.12.30.289507923.release

Note:

Date	Time	Action
02/14/2020	09:39	Sent email with attachment.

Name: Messages
Version Number: 5.2.062 (Pegasus_RC17_xxhdpi.arm64-v8a.phone)

Note: For a full listing of messages, please see the Excel spreadsheets in the folder “Messages.”

Date	Time	Action	Messages
02/14/2020	08:09	Message sent	Wow, the messages sync over between accounts.
	08:10	Message received	That is interesting.

Name: Phone
Version Number: 43.0.290782351

Note:

Date	Time	Action
02/14/2020	08:06	Outgoing phone call to (1:25)
	09:41	Incoming phone call (1:30)

Name: Snapchat
Version Number: 10.75.5.0
Install Date: 02/14/2020
Install Time: 08:45

Username: tdfirtwo
Name: This Is DFIR Two
Email Address: thisisdfirtw0@gmail.com
Password: crease-acts-cra

Note: Chat settings were changed from the default (delete after viewing) to delete after 24 hours.

Date	Time	Action	Messages
02/14/2020	08:47	Signed in	
	08:52	Message received	Hi there second account!
	08:58	Message sent	Hey, I hope no one finds this account!
	08:59	Message received	I won't tell anyone. Promise.
	09:01	Message sent	Good. Keep it on the low.
	09:03	Picture received	
	09:06	Changed chat settings (delete after 24 hours)	
	09:13	Snap sent	

Name: Wickr Me
Version Number: 5.46.1
Install Date: 02/14/2020
Install Time: 09:27

Username: thisisdfirtwo
Password: warren-foreleg-ambient
Phone: none

Note:

Date	Time	Action	Messages
02/142020	09:29	Signed in	
	09:32	Message received	Test message 1
	09:33	Message sent	Message received.
	09:34	Message sent	I hope no one finds this account either!
		Message received	They won't.

HOME SCREEN LAYOUT (USER 2)

Screenshot of the home screen for account User 2.

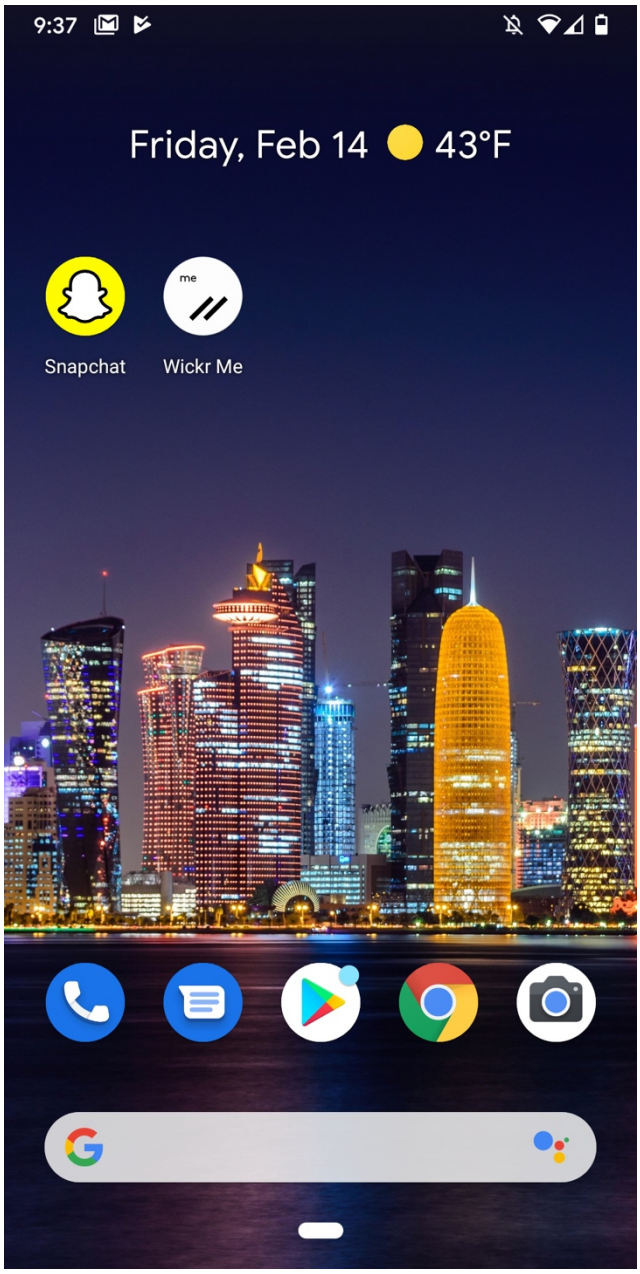

Figure 4 – Home screen for User 2.

IMAGE CREATION

Application: Cellebrite UFED 4PC
Version: 7.28.2.8
Date: 02/14/2020
Time: 18:43

File Name: *Google_G013A Pixel 3*

Note: All files are included in the zip file **Android 10 Image with Documentation.zip**. Once extracted, multiple files are present. The document **Android10-ImageCreation.pdf** along with the file folder **FileSystem ADB 02.** The extraction is segmented across several files; a .ufd file is included.

Hash Values:

Google_G013A Pixel 3.ufd

MD5: c6f52d360b8024ba218050d50fd3fc4e
SHA-1: 7b742df7cdc9527d1a87516308f350935554f589
SHA-256: cbcc2624170347515cd1d0daac2c0d5d49fb2ee8bec08ff57e1b4f13d0c1a641

Google_G013A Pixel 3.z01

MD5: e9e3be16594e65a90fc712795d72de42
SHA-1: bb91c934c3fe5977428e2ec8b3d11b9aa5fb4542
SHA-256: d1b6a233d67ba1022feab914796ee0864f14868e4b1adfffeab31bb04e887f1e

Google_G013A Pixel 3.z02

MD5: d3430253650c4686b32855b3ed1e96e3
SHA-1: c11f9e0e6d2e572fa02957a2c5511d7b28eaeb32
SHA-256: 82e59a968ef3cc51e61e0ebaf3cbbce11827b12a92b8abf30a68d5b591e02a0d

Google_G013A Pixel 3.z03

MD5: b68dfd27113c9498b616a57d302ec939
SHA-1: a8518c3f550266485b372076b59242ddecaab389
SHA-256: 5dc14cbd8d7745361816404680b8a3f9ce9d934318ea092712308f2f6936cf06

Google_G013A Pixel 3.z04

MD5: e8935c29acdf3152f2e7fa8b49f4717f
SHA-1: 020c6368faf717f83cb9ffecb74d6c36e11f9c67
SHA-256: a0d51333f3f2775647b08fa9e08551d7daa27d223a53dcf95f6a789646f1586b

Google_G013A Pixel 3.z05

MD5: 9686ec3068351a6f30e8369a437c9600
SHA-1: ee573b2a28da8966e7d3e484d73a53af9681a87e
SHA-256: 395db9eac18d868482e98b7d0e313f726ce0f6c16bf71b341df70b50a1671563

Google_G013A Pixel 3.z06

MD5: 82212a983140cf27f644ac083b2c2bad
SHA-1: 0adad282ffd85e62ad47f7b0bb476ae5bfe900ec
SHA-256: 5d1c3bf9c95923cc2f4ea98921f720f32510aae1753a132ee4867426f8e49730

Google_G013A Pixel 3.z07

MD5: 37a9419354d8e71aedad051bd3283de8
SHA-1: d2b00c95f9bc31ce250d061492aa2ca69a163813
SHA-256: 3dba6d8083d5d7f56044a60bcfcb820b7edf4027a7b0acfbd4e29ea3cb18b78a

Google_G013A Pixel 3.z08

MD5: 214ed9c81144dd4a9ca55c5fc11d945c
SHA-1: 63fa898492aa6f6453686ff3ba7ca948ea5a3fc7
SHA-256: 721c65557617004a9846817432ee210eade34659e5c617869b59b3fc08619675

Google_G013A Pixel 3.zip

MD5: 286da85cf63eb5027a77b03792bd216b
SHA-1: 6732d2e9607409510afac080717b7cdd7eaa17ef
SHA-256: ba74bdb0074348ab9d9305319bd0140c468bfe3c077a44911c31c8555a0b83be

SMS-Messages.xlsx

MD5: e0d08e10d6084077293220a03289008e
SHA-1: 9817705daa3ae687ec824738d90e60c67a75c5c2
SHA-256: e5f158d6560b5458039728424e4390a8182a578e919617442d326c5591861310