

Overview

Subject	LG's iPhone 6s forensic timeline and metadata analysis
Purpose	Reconstruct movement, app usage, and network activity from February 13–14, 2017
Key Tools	Cellebrite, GrayKey, Magnet AXIOM, ILEAP, CASTViz, Apple Health, knowledgeC
Lead Examiners	Bunner, Cecil, Eldridge

I. LG iPhone 6s Timeline

Date	Method & Tools Used	Examiner	Purpose / Notes
2/15/2017	Method 1 Cellebrite	Bunner	Initial logical extraction, battery dead on arrival
02/21/2017	Method 1 Cellebrite	Bunner	Network/iCloud data check
9/05/2017	Method 2 Cellebrite, ILEAP	Bunner	Software update analysis
10/05/2017	Method 3 Cellebrite, ILEAP	Homeland Security	Full file system extraction
6/2019	Method 3 Cellebrite, GrayKey	Bunner	Re-extraction
6/26/2019	Method 3 Cellebrite, Magnet AXIOM	Cecil	Pre 2:14 pm data search
2/17/2024	Method 3 Cellebrite, ILEAP, GrayKey, AXIOM	Cecil	Reprocessing 2019 data
5/18/2024	Method 3 Full re-extraction	Cecil	Metadata refinement

10/2024	Expert analysis Magnet AXIOM DB Browser, SQLite	Eldridge	Apple Health, network reconnection at 4:33 am
---------	---	----------	--

II. Digital Timeline

Feb 13, 2017 – Key Events

Date	Time (EST)	Event	App	Source
2/13/2017	12:01 pm	Start of movement segment #1		Apple Health
	1:31:40 pm	End of movement segment #1 (0 steps or movement)		Apple Health
	1:31:40 pm	Start of movement segment #2		Apple Health
	1:35 pm	Phone stops logging movement while Libby is in the car		Apple Health
	1:38 pm	Audio output route		knowledgeC
	1:38:49 pm	DG phone call starts	Phone	Call logs
	1:39:04 pm	DG phone call ends	Phone	Call logs
	1:39:08 pm	Phone charging		knowledgeC
	1:39:30 pm	Interaction with messaging app	Snapchat	knowledgeC
	1:39:45 pm	Snapchat viewing	Snapchat	knowledgeC
	1:40:56 pm	Unknown photo	Snapchat	knowledgeC
	1:41:44 pm	Unknown photo	Snapchat	knowledgeC
	1:43:59 pm	Libby selfie with Abby in the backseat	Snapchat	knowledgeC
	1:49 pm	Phone resumes logging movement after Libby gets out of the car		Apple Health
	2:05:10 pm	Photo of empty MHB	Snapchat	knowledgeC
	2:07:20 pm	Last screen unlock		Touch ID
	2:08:48 pm	End of movement segment #2		Apple Health

		(1682 steps)		
	2:08:48 pm	Start of movement segment #3		Apple Health
	2:13:51 pm	Start of "Bridge Guy" video	Camera	Camera metadata
	2:14:34 pm	End of "Bridge Guy" video	Camera	Camera metadata
	2:14:41 pm	Failed biometric unlock		Touch ID
	2:18:48 pm	End of movement segment #3 (414.38 meters)		Apple Health
	2:18:48 pm	Start of movement segment #4		Apple Health
	2:25:22 pm	End of movement segment #4 (0 steps or movement)		Apple Health
	2:25:22 pm	Start of movement segment #5		Apple Health
	2:31:22 pm	Two-floor elevation change detected (~20 feet or 32 steps)		Apple Health
	2:32:39 pm	End of movement segment #5 (50.64 meters)		Apple Health
	2:33 pm	Start of movement segment #6		Apple Health
	2:33 pm	Screen is off		knowledgeC
	3:11 pm	Phone call from DG	Phone	Call logs
	3:14 pm	Text message from DG	Messages	Text logs
	3:24 pm	Phone call from DG – straight to VM	Phone	Call logs
	3:32 pm	Phone call from DG – straight to VM	Phone	Call logs
	Approx 3:35 pm	Phone call from BP – straight to VM	Phone	Call logs
	Approx 3:35 pm	Phone call from TG – straight to VM	Phone	Call logs
	3:57 pm	Phone call from DG – straight to VM	Phone	Call logs
	4:06:46 pm	SMS received: "You need to call me now"	Messages	Text logs

	4:17 pm	Phone call "Number 3" – straight to VM	Phone	Call logs
	4:47:33 pm	SMS sent to Libby's phone but not received	Messages	Text logs
	Approx 5:00 pm	Phone call from MP – straight to VM	Phone	Call logs
	Approx 5:15 pm	Phone call from MP – straight to VM	Phone	Call logs
	Approx 5:20 pm	Phone call from KG	Phone	Call logs
	5:28:25 pm	"01198: SENT TEXTTY TO LIBERTYS PHONE"	Messages	Text logs
	5:44:24 pm or 5:44:45 pm	"Wired headphones" inserted		knowledgeC
	5:44:49 pm	Phone call from BP	Phone	Call logs
	5:48 pm	Phone call – straight to VM	Phone	Call logs
	6:12:47 pm	"01190: ping sent 040 35 48.041N 1/086 40 48.353W hit on wells tower//"		AT&T
	6:29:23 pm	"01190: PING REC 040 35 48.041N 086 40 48.353W HIT AT WELLS"		AT&T
	7:01:34 pm	"01190 // PING SENT 086 40 48.353 W 040 35 48.041 N"		AT&T
	7:17 pm	"AT&T SENT PING ADV SAME LOCATION //"		AT&T
	7:25:23 pm	"01192 // ATTEMPTED TO TX CELL [REDACTED] // WENT TO VOICEMAIL //"	Phone	Call logs
	7:34:48 pm	"01190 // RCVD AT&T PING, ADV SAME LOCATION"		AT&T

	7:39:37 pm	"01192 // 8-6 ADV TX OF ATTEMPTED TX, WENT DIRECTLY TO VOICEMAIL //"	Phone	Call logs
	7:50:30 pm	"01192 // ATTEMPTED TX // RANG SEVERAL TIMES UNTIL VOICEMAIL CAME ON //"	Phone	Call logs
	7:52:43 pm	"01192 // 8-1 LEFT VOICEMAIL ON LIBERTY'S TX"	Phone	Call logs
	8:14:24 pm	"01190 // 040 35 48.041 N 086 40 48.353 W // HITTING ON WELLS"		AT&T
	8:30:20 pm	"01190 // PING SENT SAME LOCATION ON PING // D4 ADV NOTHING GOING ON AT THE HIGH SCHOOL // ENR TO THE ELEMENTARY // F-2 ADV NOTHING GOING ON AT THE ELEMENTARY"		AT&T
	8:42:43 pm	"01192 // ATTEMPTED TX, RANG DIRECTLY TO VOICEMAIL"	Phone	Call logs
	8:47:23 pm	"01190 // RCVD AT&T PING, ADV SAME LOCATION"		AT&T
	9:05:50 pm	"01190 // PING SENT SAME LOCATION //"		AT&T
	9:20 pm	"01190 // PING REC SAME LOCATION //"		AT&T
	9:25:10 pm	"01192 // D-1 SENT AT&T PING TO ISP"		AT&T
	9:30:55 pm	"CONTACT AT&T"		AT&T
	9:55:24 pm	"01192 // AT&T sent ping, same location"		AT&T

	10:32:26 pm	"Wired headphones" removed		AT&T
	10:36:50 pm	"01192 // AT&T sent ping, same location"		AT&T
	10:48:22 pm	SMS sent to Libby's phone but not received	Messages	Text logs
	11:17 pm	"PING REC 040 35 48.041 N 086 40 48.353 W"		AT&T
	11:51:58 pm	"01192 // rcvd AT&T ping, adv same location wells tower"		AT&T
	1:17:54 am	"RCVD AT&T PING, ADV SAME LOCATION"		AT&T
	2:27:00 am	"01192 // RCVD AT&T PING, ADV SAME LOCATION"		AT&T
	2:53:00 am	"01192 // RCVD AT&T PING, ADV SAME LOCATION"		AT&T
	3:26:53 am	"01192 // RCVD AT&T PING, ADV SAME LOCATION"		AT&T
	3:43:53 am	"01192 // RCVD AT&T PING, ADV SAME LOCATION"		AT&T
	3:59:34 am	"01192 // RCVD AT&T PING, ADV SAME LOCATION"		AT&T
	4:33:31 am	Burst of ~15 SMS messages received	Messages	Text logs
	4:33:56 am	"01192 // RCVD AT&T PING, ADV SAME LOCATION // LAT 040 35 48.041 / LONG 086 40 48.35"		AT&T
	4:34:21.909 am	com.apple.Music WiFi Bytes Sent: 0 WiFi Bytes Received: 0 Mobile Bytes Sent:	Music	knowledgeC

		292918.0 Mobile Bytes Received: 1253201.0		
	4:34:21.911 am	Music/com.apple.Music WiFi Bytes Sent: 7504.0 WiFi Bytes Received: 69704.0 Mobile Bytes Sent: 274011.0 Mobile Bytes Received: 1709631.0	Music	knowledgeC
	4:51:35 am	"// REC PING SAME LOCATION"		AT&T
	5:08:41 pm	"revd ping, same location"		AT&T
	5:25:38 am	"01192 // revd ping, same location"		AT&T
	5:41:18 am	"01192 // revd ping, same location"		AT&T
	7:16 am	First ping on 2/14 sent to Libby's phone by AT&T. Result: no response.		AT&T
	3:06 pm	Device powered on/off by Bunner		knowledgeC
		Voicemails left between 5:45 pm on 2/13/2017 and 4:33 am on 2/14/2017 are finally recorded on LG's phone	Phone	Extraction

Feb 14, 2017 – Key Events

Date	Time	Event	Source
2/14/2017	4:33:31.909 am	Burst of ~15 SMS messages received	Text logs
	4:34:21.911 am	Music app mobile data burst	knowledgeC

III. Metadata and App Artifacts

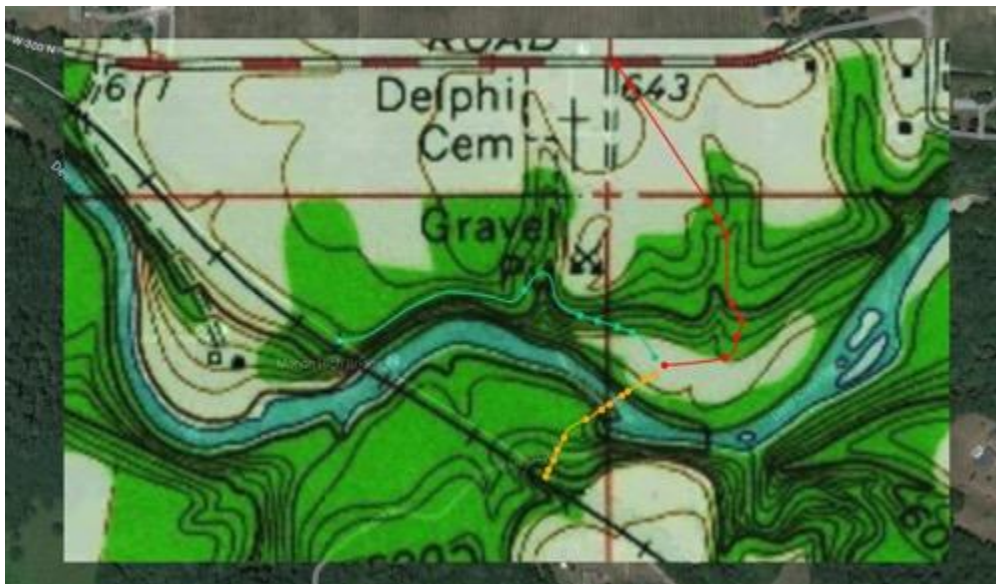
DETAILS	DETAILS
ARTIFACT INFORMATION	ARTIFACT INFORMATION
Process Name Music/com.apple.Music	Process Name com.apple.Music
Type Process	Type App
First Used Date/Time 2/4/2017 11:52:57.915 AM	First Used Date/Time 2/4/2017 11:52:58.549 AM
Last Used Date/Time 2/14/2017 4:34:21.909 AM	Last Used Date/Time 2/14/2017 4:34:21.911 AM
Last Connected Date/Time 2/14/2017 4:33:38.916 AM	Last Connected Date/Time 2/4/2017 11:52:58.549 AM
WiFi Bytes Sent 0.0	WiFi Bytes Sent 7504.0
WiFi Bytes Received 0.0	WiFi Bytes Received 69704.0
Mobile Bytes Sent 292918.0	Mobile Bytes Sent 274011.0
Mobile Bytes Received 1253201.0	Mobile Bytes Received 1709631.0
Artifact type Network Usage - Application Data	Wired Bytes Sent 0.0
Item ID 15963	Wired Bytes Received 0.0

Apple Music App Activity (Feb 14 @ 4:34 am)



GPS and Metadata Anomalies

Artifact/Event	Location Conflict	Resolution / Insight
GPS for “Bridge Guy” video @ 2:14 pm	Initially Delphi High School (~1 mi off) 40°34'54.8"N 86°39'59.4"W	Corrected within 4 seconds
AW bridge photo @ 2:07 pm	Verified online, not on device	Possibly cloud-only or alternate device
Apple Health movement	Ends at 2:32 pm	No movement, but phone still active
Messages app activity @ 4:33 am	Cellular sync detected	Refutes phone inactivity theory
Music app activity @ 4:34 am	Cellular sync detected	Refutes phone inactivity theory



IV. Environmental Context

- Terrain: Wooded, uneven, creek nearby
- Phone recovered under shoe and body
- No forensic test for water/dirt contamination
- Headphone metadata suggests human interaction, not environmental trigger

Signal Reconnection:

Date	Time	Event	Location	Implication
2/14/2017	4:33 am	Burst of ~15 SMS messages	Likely same recovery zone	Phone reconnected to tower, active app sync
	4:34 am	Music app mobile data burst	Likely same recovery zone	Phone reconnected to tower, active app sync



V. Location and Geofence Analysis

Time	Device	Approx location	Owner
12:39 pm	1	~60 to 100 yds from crime scene	Not RA or LG
3:02 pm	2	~60 to 100 yds from crime scene	Not RA or LG
3:27 pm	3	~60 to 100 yds from crime scene	Not RA or LG
5:49 pm	4	~60 to 100 yds from crime scene	Not RA or LG

Google Geofence Warrant

CASTViz	Used for mapping on 11/4/2019
Target Radius	~60 to 100 yards
Response	18,632 rows of geolocation data

Missing	Phase 3 subscriber mapping
---------	----------------------------

Known Artifacts

Artifact	Time	Source Tool(s)	Extraction Date(s)	Examiner(s)	Validation Status	Notes / Contradictions
Movement segments (Apple Health)	12:01 pm to 2:32 pm	Apple Health, Magnet AXIOM	Multiple (2017-2024)	Bunner, Cecil	✅ Confirmed	Key for reconstructing movement and pauses
Geofence device hits (not RA or LG)	12:39 pm to 5:49 pm	CASTViz, Google Geofence	11/4/2019	Homeland Security	⚠️ Unattributed	Devices near scene not linked to users—missing Phase 3 subscriber mapping
Unknown photo (Snapchat)	1:40 pm	knowledgeC, Magnet AXIOM	6/26/2019 2/17/2024		⚠️ Unattributed	Mentioned at trial but not known to/seen by the public
Unknown photo (Snapchat)	1:41 pm	knowledgeC, Magnet AXIOM	6/26/2019 2/17/2024		⚠️ Unattributed	Mentioned at trial but not known to/seen by the public
Libby selfie with Abby in the backseat (Snapchat)	1:43 pm	knowledgeC, Magnet AXIOM	6/26/2019 2/17/2024	Cecil	✅ Confirmed	Matches witness accounts; confirms presence in car
Empty MHB photo (Snapchat)	2:05 pm	knowledgeC	6/26/2019	Cecil	✅ Confirmed	Key timestamp for bridge location
Last screen unlock (Touch ID)	2:07 pm	knowledgeC	6/26/2019	Cecil	✅ Confirmed	—
AW bridge photo (online)	~2:07 pm	—	—	—	❌ Missing	Not found on LG's device—possible alternate device or cloud-only upload
AW bridge photo (online)	~2:07 pm	—	—	—	❌ Missing	Verified online but not found on device—possible cloud-only or alternate device
"Bridge Guy" video (Camera)	2:13 pm to 2:14 pm	Camera metadata, Magnet AXIOM	6/2019 2/17/2024	Bunner, Cecil, Eldridge	✅ Confirmed	GPS initially mislocated; corrected within seconds

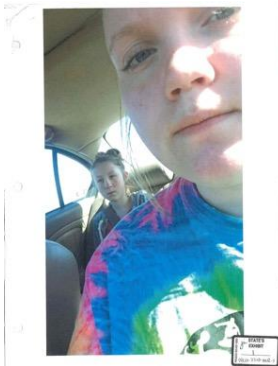
Failed biometric unlock	2:14 pm	Touch ID logs	6/26/2019	Cecil, Eldridge	✓ Confirmed	Last known user interaction
Headphones inserted	5:45 pm	knowledgeC	10/5/2024	Eldridge	✓ Confirmed	Suggests human interaction—contradicts environmental damage theory
Headphones removed	10:32 pm	knowledgeC	10/5/2024	Eldridge	✓ Confirmed	Indicates phone was handled
SMS burst	4:33 am	Text logs	10/5/2024	Eldridge	✓ Confirmed	Indicates tower reconnection
Music app data burst	4:34 am	Magnet AXIOM, knowledgeC	10/5/2024	Eldridge	✓ Confirmed	Refutes theory of phone being dead or damaged
Boot log (device power-on)	3:06 pm	Cellebrite	2/15/2017	Bunner	✓ Confirmed	Confirms device was powered on for extraction
Voicemail delivery delay	2/17/2017	Phone logs	2/17/2017	Eldridge	⚠ Delayed	Voicemails left on 2/13, not recorded until 2/17—timeline distortion
Axiom software (initially unavailable to defense)	—	Magnet AXIOM, DB Browser	—	—	✗ Inaccessible	Defense lacked licensed software—prevents independent review

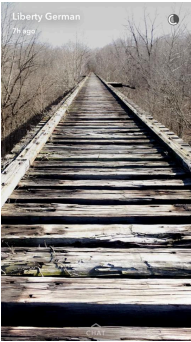

Apple Health Data

Time (EST)	Event	Source
1:31:40 pm	Start of movement segment #1	Apple Health
2:05:10 pm	Snapchat photo (bridge)	knowledgeC
2:07:20 pm	Last screen unlock	knowledgeC
2:08:48 pm	End of movement segment #1 (1682 steps)	Apple Health
2:08:48 pm	Start of movement segment #2	Apple Health
2:13:51 pm	Start of “Bridge Guy” video	Camera metadata
2:14:34 pm	End of “Bridge Guy” video	Camera metadata
2:14:41 pm	Failed biometric unlock	Touch ID

2:18:48 pm	End of movement segment #2 (414.38 meters)	Apple Health
2:18:48 pm	Start of movement segment #3	Apple Health
2:25:22 pm	End of movement segment #3 (0 steps or movement recorded)	Apple Health
2:25:22 pm	Start of movement segment #4	Apple Health
2:31:22 pm	Two-floor elevation change detected (~20 feet, or 32 steps)	Apple Health
2:32:39 pm	End of movement segment #4 (50.64 meters)	Apple Health

Where did the Snapchat pic of AW on the bridge at 2:07 pm go?

Snapchat Story	Time	Event	Found in Snapchat Cache?	Source
	1:39:30 pm	Interaction with messaging app		knowledgeC
	1:39:45 pm	Snapchat viewing		knowledgeC
	1:40:56 pm	Unknown photo	✓ Yes	knowledgeC
	1:41:44 pm	Unknown photo	✓ Yes	knowledgeC
	1:43:59 pm	Libby Snapchat with Abby in the backseat	✓ Yes	knowledgeC
	1:49 pm	Phone resumes logging steps		Apple Health

	2:05:10 pm	Snapchat of empty MHB	✓ Yes	knowledgeC
	2:07:20 pm	Last screen unlock		knowledgeC
	2:07 pm	Snapchat of Abby on MHB	✗ No	
	2:08:48 pm	End of movement segment #2 (1682 steps)		Apple Health

VI. Expert Testimony Summary

Expert	Role / Tools Used	Key Contributions / Issues
Bunner	ISP Cyber Crime Unit / Cellebrite expert	Initial extractions, missed metadata
Cecil	ICAC Task Force / Magnet AXIOM	Google search in court
Eldridge	Retired FBI CART / forensic analyst	Clarified headphone metadata, timeline
Chapman	AV technician / Axon 5, Adobe Audition	Enhanced video/audio of suspect

VII. Legal and Investigative Gaps

Issue	Description	Implication
-------	-------------	-------------

Missing subscriber mapping	No device-to-user linkage from Google	Blocks suspect attribution
AXIOM file inaccessible	Defense lacked licensed software	Prevents independent review
Selective device disclosure	Only 3 phones disclosed from CAST	Possible cherry-picking
Interview documentation	Claimed by prosecution, not produced	Undermines transparency

VIII. Observations and Next Steps

- Cloud-only artifacts (e.g. AW 2:07 pm bridge photo) may reveal alternate device(s) or iCloud access analysis.
- Unattributed geofence hits could identify proximity overlaps if overlaid.
- Voicemail delay and headphone metadata are high-value contradiction points.

Issue	Conflict / Curiosity	Implication
Headphone metadata	Inserted at 5:45 pm, removed at 10:32 pm	Suggests human interaction
Movement halt vs. phone alive	No steps after 2:32 pm, but metadata active	Phone stationary but powered
GPS for “Bridge Guy” video	Initially mislocated, corrected within seconds	GPS triangulation lag
AW 2:07 pm bridge photo	Verified online, not found on device	Possible cloud-only upload
Voicemail timestamps	Recorded 2/13, delivered 2/17	Misleading timeline
App activity at 4:34 am	Music app active	Refutes phone inactivity theory