



**CELL PHONE RECORDS AND DATA RECOVERY
FACTUAL REPORT**

Mountain View, CA

HWY18FH011

(9 pages)



**NATIONAL TRANSPORTATION SAFETY BOARD
OFFICE OF HIGHWAY SAFETY
WASHINGTON, D.C.**

**CELL PHONE RECORDS AND DATA RECOVERY
FACTUAL REPORT**

A. CRASH INFORMATION

Location: Southbound US Highway 101 (US-101) south of North Shoreline Boulevard at the exit ramp transition to State Route 85 (SR-85), milepost 48.38, Santa Clara County, Mountain View, California.

Vehicle 1: 2017 Tesla Model X P100D

Vehicle 2: 2010 Mazda 3

Vehicle 3: 2017 Audi A4

Date: March 23, 2018

Time: Approximately 9:27 a.m. PDST

NTSB #: **HWY18FH011**

B. CRASH SUMMARY

For a summary of the crash, refer to the *Crash Summary Report* in the docket for this investigation.

C. DETAILS OF THE CELL PHONE RECORDS / DATA RECOVERY REPORT

- Section 1 of the report provides background information regarding the two cell phone devices found at the crash location.
- Section 2 of the report provides a summary of the AT&T cell phone records for the phone number assigned to the Tesla driver's phone.
- Section 3 of the report describes the inspection of the Apple iPhone and a description of the unencrypted log data recovered from the phone.
- Section 4 of the report provides a description of the game application found to be in the foreground of the phone during the Tesla driver's trip to work.

1. General Overview of Cell Phone Devices in Tesla Model X

Following the crash, the California Highway Patrol (CHP) recovered two cell phones from the crash scene. One phone, an Apple iPhone 8 Plus, was found among the debris on the highway. The iPhone 8 Plus was damaged and could not be powered on (see figure 1). The second phone, an Apple iPhone 10, was undamaged and found among the driver's personal belongings. The CHP inspected the phones and returned both phones to the Tesla driver's family prior to being inspected by the NTSB.



Figure 1 – Photo of the front and back of the Tesla driver's damaged iPhone 8 Plus
(Source: Apple)

The family returned both phones to Apple since they were initially supplied to the Tesla driver, an Apple employee, for business use. Apple was interested in obtaining custody of the phones out of concern that the phones may contain sensitive work data, including potential trade secret information.

Upon hearing that the cell phones were released by the CHP to Apple, NTSB contacted Apple and requested a hold be placed on the phones and no data be accessed or deleted. Apple advised the NTSB that the iPhone 8 Plus was a development fused model and was used primarily for business purposes. The iPhone 10 was also Apple-owned but was provided to the Tesla driver (Apple employee) for personal use. The Tesla driver was required to obtain his own wireless service for the phones.

2. AT&T Cell Phone Records

NTSB obtained information from the Tesla driver’s family and determined that the wireless and cell phone carrier was AT&T. A subpoena was issued to AT&T for all records related to the use of the cell phone(s) on the date of the crash (March 23, 2018 12:01:00 a.m. to March 23, 2018 11:59:00 p.m.) to determine if the driver was interacting with his personal electronic device in the moments leading up to the crash.¹

AT&T records were reviewed for the morning of the crash. The records showed that the Tesla driver was using the Apple-owned iPhone 8 Plus (Serial Number C39V20CAJ9LJ) cell phone on March 23, 2018.² The only record of incoming or outgoing calls or text messages made to or from the Tesla driver’s Apple iPhone 8 Plus cell phone was after the crash. Between about 11:34 a.m. to 11:56 a.m. (2 hours after the crash), there was a series of unanswered incoming phone calls and text messages that originated from the Tesla driver’s wife’s cell phone.

The records showed evidence of data usage while the vehicle was in motion, but the source of these transmissions could not be determined from the records alone.³ One data transmission showed a connection time of 9:26:48 – less than a minute before the crash.

To better understand the data activity, 12 hours of AT&T data usage was tabulated and plotted on a graph (Figure 2 below). In the table below the elapsed time reflects the number of minutes between connection times listed on the AT&T data usage records. Kilobytes (KB) Up refers to the number of KBs sent from the mobile station to the network. KB Down refers to the number of KBs sent from the network to the mobile station. The average Kilobytes per Minute reflects the average data rate usage for the given time period.

Time Period	ET	Kilobytes Up	Kilobytes Down	Kilobytes Total	Average Kilobytes/Minute
10:11:11 – 11:11:11 p.m.	60.00	25.290	17.093	42.383	0.71
11:11:11 – 12:11:11 a.m.	60.00	28.683	21.977	48.66	0.81
12:11:11 – 01:11:11 a.m.	60.00	23.033	19.152	42.185	0.70
01:11:11 – 02:11:11 a.m.	60.00	9.550	9.568	19.118	0.32

¹ The subpoena was later expanded to include all records from 3/19/18 12:00:00 a.m. UTC to 3/23/18 11:59:00 p.m. Cell phone tower locations were provided for March 23, 2018 only.

² Refer to Cell Phone Records Attachment 1 – AT&T Records.

³ The AT&T network constantly communicates with internet enabled devices when they are powered on. These communications are reported as data usage on customer records but do not necessarily indicate a customer initiated a transaction. AT&T does not retain records that can definitively show whether a transaction was customer initiated or AT&T’s network initiated the data transaction.

02:11:11 – 03:11:11 a.m..	60:00	7.996	8.449	16.445	0.27
03:11:11 – 04:11:11 a.m.	60:00	13.770	11.110	24.88	0.41
04:11:11 – 05:11:11 a.m.	60:00	7.433	6.922	14.355	0.24
05:11:11 – 06:11:11 a.m.	60:00	7.792	6.954	14.746	0.25
06:11:11 – 07:11:11 a.m.	60:00	8.217	7.890	16.107	0.27
07:11:11 – 08:11:11 a.m.	60:00	602.676	4200.917	4803.593	80.1
08:11:11 – 08:49:31 a.m.	38:20	349.622	1057.371	1406.993	36.7
08:49:31 – 09:02:43 a.m.	13:12	496.695	1607.030	2103.725	159.4
09:02:43 – 09:10:27 a.m.	7:44	145.860	416.504	562.364	72.7
09:10:27 – 09:15:21 a.m.	4:54	190.754	303.281	494.035	100.8
09:15:21 – 09:26:48 a.m.	11:27	371.911	1967.368	2339.279	204.3
09:27:27		Time	of	Crash	
09:26:48 – 09:49:52 a.m. ⁴	22:54	685.926	960.643	1646.569	71.9
09:49:52	0:00	0	0	0	0

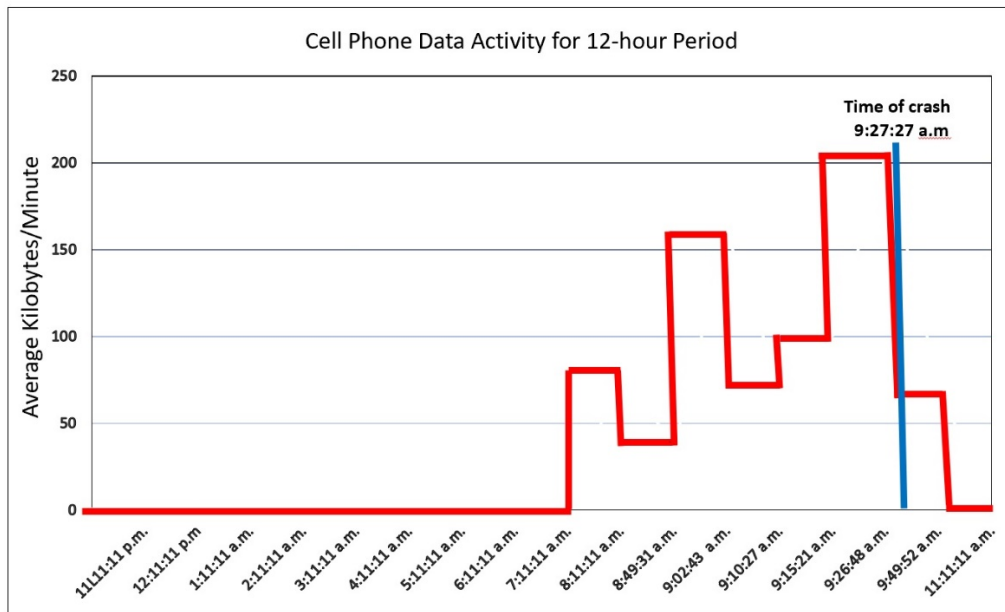


Figure 2 – Graph showing about 12 hours of data usage by Tesla driver from 10:11:11 p.m. March 22 to 9:49:52 a.m. on March 23.

⁴ The 4G Network Cell Site location reported for the data transmissions that occurred at about the time of the crash was recorded in AT&T records as 37.41263 N, 122.07655 W about 990 feet northwest of the crash attenuator.

Data activity being recorded in AT&T records can include the network updating software and phone applications, sending and receiving e-mails, internet usage, upload and download of photos, streaming of videos, and online game playing. AT&T provides general guidance for the amount of data for each activity.⁵ Examples of estimated data usage for each type of activity includes:

- 1 e-mail (no attachments) 20 KB
- 1 e-mail (with standard attachments) 300 KB
- 1 minute of “surfing” the web 250 KB (15 MB/hr.)
- 1 song download 4 MB
- 1 photo upload to social media 5 MB
- 1 min. of streaming standard-definition video 11.7 MB (700 MB/hr.)
- 1 min. of streaming high-definition video 41.0 MB (2500 MB/hr.)
- 1 min. of streaming 4K video 97.5 MB (5850 MB/hr.)
- 1 min. of online games 200 KB (12 MB/hr.)

In the 12 hours preceding the crash, the highest data usage was recorded in the minutes immediately leading up to the crash - a rate of 204 KB/minute. This level of data activity is consistent with online game activity. When the phone was not in use during the overnight hours when the Tesla driver was asleep, the average data usage was less than 1 KB/minute.

3. Apple iPhone 8 Plus Inspection and Data Recovery

The Tesla driver’s Apple iPhone 8 Plus was damaged during the crash and could not be powered on. Apple assisted the NTSB with powering on the iPhone which was a development fused model of the iPhone 8 Plus. Because the device was an Apple-owned development fused model, after the iPhone was powered on, Apple was able to recover certain diagnostic logs that it located on the device. These diagnostic logs would not have been available if the phone was a consumer release model iPhone.⁶

The diagnostic logs that were able to be recovered consisted of unencrypted cell phone application CrashReporter logs.⁷ CrashReporter logs are available to application developers for diagnostic purposes. When an application on a phone crashes, an application crash report is created and stored on the device. Application Crash reports generally describe the conditions under which the application terminated and contain a limited amount of

⁵ Refer to <https://www.att.com/esupport/data-calculator/index.jsp> accessed July 5, 2019.

⁶ For a consumer release model, a PIN is required to access system logs. NTSB contacted the family of the deceased Tesla driver who advised that they did not know the PIN for the phone.

⁷ Refer to Cell Phone Records Attachment 2 – Apple CrashReporter logs

information that can be used for a timeline analysis. In a review of the CrashReporter logs for the Tesla driver's iPhone 8 Plus, two types of logs of interest were recorded:

- Jetsam logs: Dropped whenever a process exceeds its memory limit. Apple uses this telemetry data to quantify and drive down memory related to possible software bugs. It is also used to improve the quality of software.
- Wakeup resource logs: Dropped when phone processes are using an excessive amount of power. Apple uses these logs to improve device battery life.

On Friday, March 23, 2018, the following logs were dropped on the Tesla driver's iPhone 8 Plus:⁸

9:06:50 a.m.: A jetsam log was dropped that showed process "sgz" to be the application in use and in the foreground of the phone. The process was running for approximately 6 minutes prior to the log being dropped because of excessive memory use.

9:10:25 a.m.: A wakeups resource log was dropped that showed process "sgz" to be extremely active for a 5-minute window. The log was dropped due to excessive power usage.

9:49:51 a.m.: A jetsam log was dropped that showed process "sgz" to be foreground visible on the phone. This log was dropped because process "com.apple.siri.embeddedspeech" exceeded its memory limit while holding an active transaction. This means that Siri was engaged and listening for audio. The log also shows that Siri was launched about 2 minutes and 43 seconds prior to this log being dropped at about 9:47:8 a.m. Apple advised NTSB that Siri could have been engaged by someone holding the home button, or a damaged button could have kept Siri engaged and listening from 9:47:8 to 9:49:51 a.m.⁹

⁸ Phone logs listed the product identification as an iPhone 10. It is likely that the driver was using the SIM (subscriber identity module) card from his iPhone 10 within the iPhone 8 Plus device.

⁹ This log was dropped after the crash which occurred at 9:27:27, 22 minutes and 24 seconds after the crash. It is possible that one of the first responders recovered the phone and hit the home button of the Apple iPhone 8 Plus activating the Siri process. NTSB checked with the California Highway Patrol and they queried on scene officers and nobody could recall who recovered the cell phone at the scene.

4. Game Application Active During Trip

NTSB reviewed the logs and identified the “sgz” process to be a gaming application known as “Three Kingdoms” mobile edition, with a build version of 1.4.0.¹⁰ The game was released on November 15, 2017, by Hong Kong based Black Beard Games Limited and its content is in Chinese. Build version 1.4.0 was released on March 21, 2018, two days before the crash.

The game is a world building, strategy game with multi-player capability. In the game, players from around the world are placed together on a map grid of more than 1 million tiles, and players recruit generals, develop cities, create squads, and develop alliances with other players to compete against others. When playing the game on a mobile device such as an iPhone 8 Plus, most players have both hands on the phone to support the device and manipulate game actions. The log data does not provide enough information to ascertain whether the Tesla driver was holding the phone or how interactive he was with the game at the time of the crash.

A look at historic CrashReporter logs from the driver’s device shows a pattern of active game play, every day from Monday, March 19, 2018 to Friday, March 23, 2018, between the hours of 9:00 a.m. to 10:00 a.m. Wakeup resource logs were dropped each day showing that the driver was using the “Three Kingdoms” game during his trip to work:

- March 19, 2018 at 09:03:21
- March 20, 2018 at 09:18:53
- March 21, 2018 at 09:37:53
- March 22, 2018 at 09:21:31

NTSB queried the wife of the Tesla driver (through the family attorney) whether she was aware of her husband playing the game “Three Kingdoms” on his phone. The wife responded that her husband loved to play games on his phone, but he never did so while driving. Additionally, the wife advised that she did not recognize the game “Three Kingdoms” as something her husband was interested in.

¹⁰ The process was referred to as com.bbgame.sgz2017.tw in the wakeup resource log dropped at 9:10:26.11.

D. DOCKET MATERIAL

The following attachments are included in the docket for this investigation:

LIST OF ATTACHMENTS

Cell Phone Records Attachment 1 – AT&T Records

Cell Phone Records Attachment 2 – Apple CrashReporter logs

END OF REPORT

Donald F. Karol
National Resource Specialist