Accident Case

Cellphone Forensic Analysis Report

Prepared by Richard Miletic

Introduction

This civil case involves an auto accident. I have been asked to evaluate the cell phone records and other information to provide my opinions as to driver distraction or lack thereof in this case.

I represented the defendant, an insurance company, in this case. The defendant driver was accused of using his cell phone prior to and during an accident that he caused.

Background and Experience

My CV is attached to this report and describes in detail my education, experience and training in wireless technology and forensics.

I have been involved with wireless technology since 1996 when I began work at Motorola headquarters in Schaumburg, IL. I participated in training classes in radio theory and applications that Motorola offered. As part of my work there I was involved in product development for analog and digital 2-way radio for private and public communication systems. I was also involved in the early development of Wi-Fi technology.

At SAFCO, ZK Celltest and ZK Services I was able to work closely with cellular and radio engineers at wireless operators AT&T, Verizon, and others as well as manufacturers such as Apple, Qualcomm, Nokia, Ericsson, and others. We licensed proprietary technology from some of these companies that allowed us to extract highly detailed and expansive amounts of data from the cell phones and tower equipment. We developed expertise in analyzing this data for the purpose of troubleshooting and improving the quality and coverage of cellular networks. The data we obtain for forensic studies are an exceedingly small subset of what we analyze for network performance analysis.

In 2016 I realized my experience in and knowledge of wireless technologies both theoretical and practical would help applying techniques used every day optimizing wireless networks to the legal field. By assisting prosecutors, plaintiffs, and defense attorneys in combing through the complexities of cell phone and cell tower records, I would help serve justice.

I have written articles that have been published in national publications and in several state bar associations educating attorneys about cell phone record analysis and cellular network design and functionality as well as how this is applied to legal cases.

My unique difference with most other experts in this field is that I bring both theoretical and practical knowledge of how wireless networks and technologies function. I have been trained on the theory of

analog, 2G, 3G, 4G and 5G technologies. I have performed in-field tests using high end test equipment to determine how these technologies perform in the field in the real world. By first understanding the theory then seeing how the technology works, provides a deep understanding of the technology itself and how it works when implemented with large numbers of users and varying environmental conditions.

I have served as an expert witness in both civil and criminal cases including vehicle accidents, murder cases, ATF bomb explosive case, FBI kidnapping case, etc. I have analyzed cell phone records, Cloud records, location data, tower records, etc. I am exceptionally good at explaining overly complex technical issues in layman's terms.

Call Records

Call Detail Record (CDR)

A CDR is provided by the wireless operator usually through a subpoena process. A subpoena is submitted to obtain records associated with a cell phone number or set of cell phone numbers. Each record indicates a voice call, SMS (i.e., short message or "text") or Data Session (e.g., Internet browsing).

The CDR typically includes the date/time, dialed number, terminating number, elapsed time, serving cell towers, etc. There may be additional information provided for an SMS or data call.

The records provided by AT&T in this case were Call Detail Records for dates XXXX.

Per Call Measurement Data (PCMD)

Network Operators may provide data that estimates the location of cell phone with a latitude/longitude value within a stated confidence. Also included in this data is phone number, connection date and time, call length, etc.

PCMD records were not provided in this case.

Cell Tower Data

The cell tower data includes location of tower in latitude/longitude coordinates, antenna azimuth (direction), beam width (angle at which the antenna transmits signal), maximum antenna range (max distance the cell site transmits signal), identification information that can be tied back to the phone call records (CDR and PCMD). With this data matched with the CDR or PCMD data we can typically identify the location of the serving cell for each call which allows us to assume the phone was in a certain general area within the coverage of the cell tower antenna.

A tower record file was not provided in this case however, there is tower location information provided in the AT&T CDR provided. The CDR file only lists the towers that were actively used during the voice, SMS, or data call. This is a subset of all the towers in the area. This may or may not be an issue in this case.

Data Analysis

I have been asked to review the information in this case and prepare a report on my analysis. The following documents were provided to me. Note that as of this writing I was not provided with the csv

version of the AT&T call records. This prevents me from importing the records into mapping, database, or spreadsheet software for additional analysis.

- Police Officer Crash Report
- Call Detail Records
- Deposition of Driver
- Deposition of Operations Manager

The time of the accident occurred at XXXX Central time as logged in the accident report. The following is an analysis of the AT&T call detail records prior to and during the time of the accident.

SMS (Text) Messages

According to the AT&T records there were no text messages sent or received on the day of or prior to or during the accident. The target' phone was not sending or receiving text message before or during the accident.

Voice Calls

There was one outgoing voice call for 5 minutes 50 seconds. This call ended at approximately 30 minutes prior to the accident. The next voice call initiated was approximately 20 minutes after the accident. There was no driver distraction due to a voice call.

Data Transmissions

There were two records associated with data transmissions during the accident.

Data Record #1

One lasting 60 minutes and zero seconds transmitted 1,467,448 bytes upload (or approximately 1.5 Megabytes (MB)) and 7,376,366 bytes download (or approximately 7.4 Megabytes (MB)). This is a total of approximately 8.84 MB in a 60-minute session as logged in the AT&T record.

There is nothing in the call record that identifies what phone application was running, if any, during this transmission. There is nothing in the data record that identifies that a user was actively interacting with the phone during this transmission.

There are nearly 2,000,000 apps in the Apple Store many of which do not require user intervention at all. In the following paragraphs we show data rates for video, music, mapping, and social media apps.

The following table shows three of the most popular video applications Zoom, Netflix and YouTube. Data Record #1 was launched 12 minutes before the crash and the AT&T record shows the length of the data session as 60 minutes. The amount of data that would typically have been downloaded in both time periods is shown in the following table.

As you can see all the values are significantly higher than the 8.84MB that was in the AT&T record. Therefore, the amount of data transmitted does not correlate to a video session even at the lowest possible resolution.

Video					
Zoom	Low (one-to-one)	108	MB/12min	540	MB/60min
	High (one-to-one)	324	MB/12min	1620	MB/60min
	Low (Group)	162	MB/12min	810	MB/60min
	High (Group)	480	MB/12min	2400	MB/60min
Source:	How Much Data Does Zoom Use? | WhistleOut				
Netflix	Low	60	MB/12min	300	MB/60min
	Medium	140	MB/12min	700	MB/60min
	HD	600	MB/12min	3000	MB/60min
	UHD	1400	MB/12min	7000	MB/60min
Source:	How Much Data Does Netflix Use On Cell Phones? | Wirefly				
Youtube	240p	40	MB/12min	200	MB/60min
	360p	60	MB/12min	300	MB/60min
	480p	100	MB/12min	500	MB/60min
	720p	300	MB/12min	1500	MB/60min
	1080p	600	MB/12min	3000	MB/60min
Source:	How Much Data Does YouTube Use? | WhistleOut				

The following table shows 4 of the most popular music apps and the typical data transferred over a 12-minute and 60-minute period. The values in yellow are comparable to the actual data transferred during the session from the target phone. It is possible that the phone could have been playing a music application if we assume the music stopped playing at the time of the crash which was 12 minutes after the session started.

Music					
Spotify	Normal	8.64	MB/12min	43.2	MB/hr
	High	14.4	MB/12min	72	MB/hr
	Extreme	28.8	MB/12min	144	MB/hr
Apple Music		23.04	MB/12min	115.2	MB/hr
Google Music	Low	8.64	MB/12min	43.2	MB/hr
	Normal	23.04	MB/12min	115.2	MB/hr
	High	28.8	MB/12min	144	MB/hr
Youtube Music	240p	13.5	MB/12min	67.5	MB/hr
	480p	33.3	MB/12min	166.5	MB/hr
	720p	60.3	MB/12min	301.5	MB/hr
	1080p	99	MB/12min	495	MB/hr
Source:	Music Streaming Data Usages Compared | finder.com				

The following table shows 3 of the most popular mapping applications. These apps provided turn-by-turn directions and are legal in most states. The values in yellow are comparable to the actual data transferred during the session from the target phone. It is possible that the phone could have been running a mapping application.

It is also interesting to note that two separate tests were conducted for the Apple mapping app with vastly different results. This goes to show that data transfer results vary greatly based on other variables.

Maps					
Google		1.00	MB/12min	5	MB/hr
Source:	How Much Data Does Google Maps Use				
Apple		1.08	MB/12min	5.4	MB/hr
Source:	Apple Maps Data Usage Explained – Canstar Blue				
Apple		1.86	MB/12min	9.3	MB/hr
Apple		5.42	MB/12min	27.12	MB/hr
Source:	How Much Data Does Apple Maps Use? - Connected Car Life				

The following table shows typical data transfer amounts for 12-minute and 60-minute time periods. As you can see, even at the lowest value of 18MB, it is double the amount of data that was transferred in the AT&T call record. This does not correlate to the data transferred during this session on the target phone.

Social Media					
	Scroll/Read	18	MB/12min	90	MB/hr
	Interact	31.2	MB/12min	156	MB/hr
Source:	How much data does social media apps use				

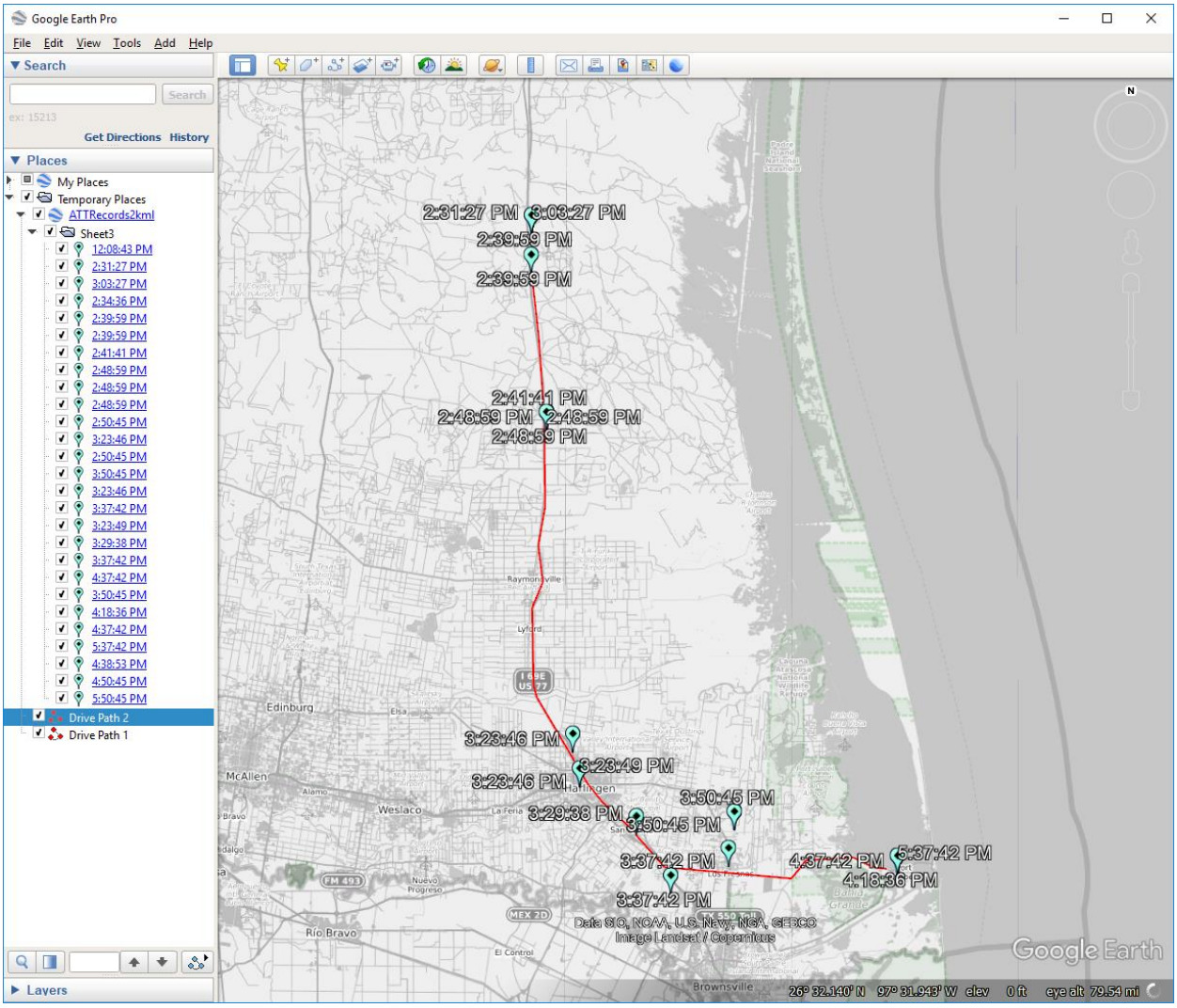
Data Record #2

This session lasted 60 minutes and zero seconds and transmitted 20,916 bytes upload (or approximately 20.9 kilobytes (kB)) and 18,376 bytes download (or approximately 18.4 kilobytes (kB)).

In terms of the amount of data transmitted during this session it is insignificant. It is less than 0.25% of the amount of data downloaded in data record #1. Assuming an average 4G connection speed of 5 MB of data per second it would take less than one second to download 18.4 kB of data. This would have occurred many minutes before the accident and if the user were actively interacting with the phone there would be a magnitude larger amount of data transmitted. Due to the insignificant amount of data transmitted that there was no user interaction in relation to this call record causing the accident.

Location Mapping

Below is a map of the assumed drive route based on the AT&T records. The highlighted points are cell towers that the target phone accessed along the route. Nothing unusual is identified by the data and it looks like the vehicle was moving according to the speed limits based on the times and locations in the records.



Conclusions

The target phone was not on a voice call just prior or during the accident and was not distracted by being on a voice call.

The target phone was not texting on the day of the accident until approximately 6pm that evening long after the accident. Thus, he was not distracted by texting in relation to the accident.

There were two data transmissions prior to and during the time of the accident. The log files do not list what application was running, if any. They do not list that the user was actively interacting with the phone. The amount of data transmitted in first data record is consistent with a mapping, a turn-by-turn real time mapping program and a music playing app. Both apps run without user intervention.

Data transferred in data record #1 is not consistent with video or social media application usage.

The amount of data transmitted in the second data session is insignificant and would have taken less than one second to transmit, long before the accident occurred.

There is no evidence in the records that the driver was distracted using his phone in causing the accident. In fact, there is evidence to the contrary in that the phone may have been running a music or mapping app, both of which do not require user intervention.

Certification

I certify under penalty of perjury that I prepared this report truthfully and to the best of my ability.

Richard Miletic
Expert Witness
ZK Services
650-279-2403
www.zkservices.net
rich@zkservices.net