THE PEOPLE OF THE STATE OF CALIFORNIA

-vs-

CHARLES RAY MERRITT

Geolocation of Calls

Vladan Jovanovic, Ph.D.

09/25/2018

Report Summary

This report presents the analysis of the calls made on the phone 909-374-1002 during the three intervals of interest in February of 2010, as defined by the Defense Counsel. We point at several false assumptions and misleading presentation of the data made by the Prosecution's geolocation expert. For each of the three periods we provide our own estimates of locations, and of the direction or travel when appropriate.

Contents

1 Introduction

The Cell Site Table file[1] provided by AT&T for the selected areas in San Bernardino, Riverside and San Diego counties is plagued with very serious problems in terms of the completeness, accuracy and consistency of the data, as described in the accompanying report[2]. These errors seriously impede the ability of any expert to provide geolocation estimates based on the data in Call Records file[3], which is based on and uses the data from AT&T's Cell Site Table.

In this report we first show that – even under the assumption that the unreliable cell locations and antenna pointing azimuth information in Call Records and Cell Site Table files are correct – the analysis provided by the Prosecution falls short of the normal scientific standards for the geolocation of calls. In particular, this analysis relays on an implicit assumption that the mobile phones always connect to the nearest cell site and an explicit assumption that the range of the cells that carried a call can be determined by the inter-cell distances. We will show here that neither of these assumptions necessarily holds true in the cellular networks.

In order to refute this approach, in the first part of this report we will present some necessary background information related to:

- RF propagation and received signal strengths in the field.
- Some characteristics of the phone Defendant used in early 2010.
- Directed Retry mechanisms, which can cause a mobile phone to connect with cells that did not have the strongest received signal.
- Network loading situations in AT&T networks in late 2009 and early 2010.
- Use of drive test data for verification of the signal strength estimates.

In the second part of this Report we provide our own analysis for 3 sets of calls as requested by the Defense Counsel:

1) 6PM-12PM on 02/04/2010.
2) Whole day of 02/06/2010.
3) 1:31PM-1:41PM on 02/08/2010.

Defense Counsel provided to me the following materials and data relevant for this report:

a) File "A1-09 (1).xlsx" from AT&T containing Cell Site Table in MS Excel format.
b) File "ATT Cells.pdf" from AT&T containing the same information in PDF format.
c) File "909-374-0102 - ReportAU_1497291.pdf" from AT&T containing the Call Records for Defendant's phone 909-374-0102 for period 01/02/2009-2/19/2010 in PDF format.
d) File "FVI1404194 ATT Mobility Records 2-4-10 to 2-8-10.pdf" providing the same information as in c) but for period 02/03/2010-02/09/2010 and with the phone type and model info added.

---

[1] Defense received several versions of the file, one referenced in here is in Excel format received under the name "A1-09 (1).xlsx".

[2] V. Jovanovic, "AT&T Cell Site Problems", 09/14/2018.

[3] Defense received several versions of the file, one referenced here is in a PDF format received under the name "909-374-0102 - ReportAU_1497291.pdf".

e) File “FVI1404194 ATT Records Key.pdf” from AT&T, with the explanation of the fields in the file “ReportAU_1497291.pdf”.

f) File “7298-7786 (SBSD Inv Rept Narratives) 2 of 4 (2).pdf” with analysis of Call Records file by Mr. Kevin Boles, pp.9-30.

g) File “7298-7786 (SBSD Inv Rept Narratives) 2 of 4 (2).pdf” with maps of Defendant’s calls from 02/01/2010 to 02/07/2010 made by a Prosecution’s expert for Preliminary Hearing.

h) File “7298-7786 (SBSD Inv Rept Narratives) 3 of 4 (2).pdf” as in g) but for the 02/08/2015 to 02/15/2010 period.

i) File “7298-7786 (SBSD Inv Rept Narratives) 3 of 4 (2).pdf” containing parts of the analysis from f) and some excerpts from the Call Records file.

j) File “FVI1404194 PLH Transcript 6-15-15. pdf” with transcript of the Mr. Boles’ testimony about his analysis of the Call Records from the Preliminary Hearing, pp.78-98.

k) File “ATT_DTP_RIVERSIDE_CA_DTRU_AGPS_2014-09-25_1411678097519.csv” with drive test data for the Riverside County in comma separated values (CSV) text format.

l) File “ATT_DTP_SAN BERNARDINO_CA_DTRU_AGPS_2014-09-25_1411679803237” with drive test data for San Bernardino County in CSV text format.

m) File “ATT_DTP_SAN DIEGO_CA_DTRU_AGPS_2014-06-18_1403073264387” with drive test data for San Diego County in CSV text format.

n) File “ATT Response to Reject SDT 2 for Phone Records 909-374-0102 - 6-29-2016.pdf” containing the original response from AT&T to the subpoena request; includes a copy of the subpoena request via fax by Defense Counsel.

2 RF Propagation Basics

In the course of their normal operation, mobile phones constantly search for and measure the strengths of all the signals transmitted from the neighboring cells that they can detect. When they need to connect to the network to initiate or receive a mobile call, they normally try to connect to the cell with the strongest detected signal. If during their continued operation they find a cell with a stronger signal, they execute a process called “hand-off”, in which the serving cell is switched from the old to the new stronger one. If performed during an active call, the hand-off process is directed by the network (based on mobile reported measurements), while in the phone’s idle mode it performs this switching autonomously.

According to the *Hata* model for RF propagation[4] widely used in RF Engineering, a signal received by a mobile from a cell over a “quasi smooth” terrain would vary depending on the following 4 factors, in order of their impact:

1) Distance – Received signal power reduces exponentially with distance (exponent around 3.5). Everything else being equal, signal from a cell at 1 mile would be received at about $2^{3.5}\approx 11$ times higher power level than the signal from a cell 2 miles away. This is the reason why mobiles often connect to the nearest cell.
2) “Clutter” – obstacles between cell and mobile at heights lower than cell antenna heights. Usually

[4] M. Hata, “empirical Model for Propagation Loss in Land Mobile Radio Services”, IEEE Transactions on Vehicular Technology, vol.VT-29, No.3, Aug.1980. Model is based on extensive set of field measurements. It is used in many theoretical studies and as a basis for signal strength predictions in the most RF Engineering tools.

the second largest factor. RF propagation path through flat open space gives about 100 times larger received power than paths through suburban areas, and often up to 1,000 times larger than through dense urban areas. Some versions of the *Hata* propagation models consider vegetation, which can have somewhat similar effects, not just the building densities.

3) Local phone environment – building penetration loss, car-penetration loss. These typically give about 3-10 and 10-100 attenuation factors respectively. Usually the third largest factor.
4) Cell's antenna height – received signal increases exponentially with antenna height (typical exponent is around 1.4, as long as antenna height is under 600 feet). Everything else being equal, antenna at 100 feet would give $2^{1.4} \approx 2.6$ times stronger signal than antenna at 200 feet.

"Quasi smooth" is a terrain with the "gentle" elevation variations within $\pm$10 yards. *Hata* model can be used in the "rolling hills" terrain by an "effective antenna height" concept. When bigger obstacles exist along the propagation path, especially those with heights approaching or exceeding the cell antenna height, diffraction effects over the edges have to be accounted for. In very mountainous areas, where hills and other obstacles can easily reach or exceed the cell antenna height, propagation is often limited to the locations with the "geographical line of sight" from the cell antenna.

While the mobile phones often connect to the geographically nearest cell, a combination of any of the factors enumerated above can cause it to receive a stronger signal from a geographically more distant cell.

3 Directed Retry

There are situations in cellular networks when mobile phones intentionally do not connect to the cell with the strongest signals. The most prominent such case is when a cell with the strongest signal has no radio resources available to serve the call request, a situation technically known as "blocking". Some level of blocking always exists in the cellular networks, but in the well-designed ones, it is kept in check by the various RF engineering techniques (adding new radios in the cells, tweaking cell parameters such as transmit power, antenna orientations and down-tilt angles to redistribute calls to the less congested cells nearby, building new cell sites in the congested areas to offload the busy ones, etc.)

In well designed and well-maintained cellular networks, the normal engineering objective is to block less than 2% of all calls in each cell during its busiest hour of the busiest day of the week. During the so-called "Cell Busy Hour", this translates into the busiest cells blocking some calls during a total of under 72sec. Individual instances of cell blocking are typically short, each lasting for a few seconds only.

A system-level technique to alleviate blocking problems is a *Directed Retry* mechanism. When Directed Retry is active, if a cell has no radio resources to serve a call request, the network can redirect that request to the cell nearby that has free radio resources. In this way the network intentionally instructs the mobile phone to connect not to the best cell, but to the one with the second or third strongest signal (which can often be in the adjacent sector to the blocking cell, but can be on a completely different cell site too). It is a technique routinely used in GSM (2.5G) technologies – all network equipment vendors provide an option to activate the Directed Retry mechanism in the GSM networks.

The way the most if not all the equipment vendors implement Directed Retry is to couple it with the so-called *call queuing* – if the cell that received the initial call request is blocking, the request would be first

put into a waiting queue and served if/when the radio resources in the cells get free. This waiting time is defined by a programmable timer on the network side, with a range of 1-15 sec. typically.

If no channel is available after this wait period, the mobile is to report the identities and signal levels of the neighboring cells. This process is controlled by another programmable timer of similar duration (typ. 10 sec.) to allow the mobile enough time to find the other candidate cells with sufficiently strong signals.

Directed Retry is effectively a mechanism to trade failed call attempts (due to blocking) for successful calls with extra set-up delay – while the calls in GSM networks are normally set-up within 5 sec (maybe up to 10 sec. if the network controllers are very busy and the corresponding messages have to be queued in there to), the calls with Directed Retries can easily take 20 sec or more to set-up.

4 "Target Phone" Characteristics

Inspection of the Call Records file[5] for the "target" phone number 909-374-0102 revealed that in February 2010, this phone number was assigned to a mobile unit made by "Samsung", model SGH-A167.

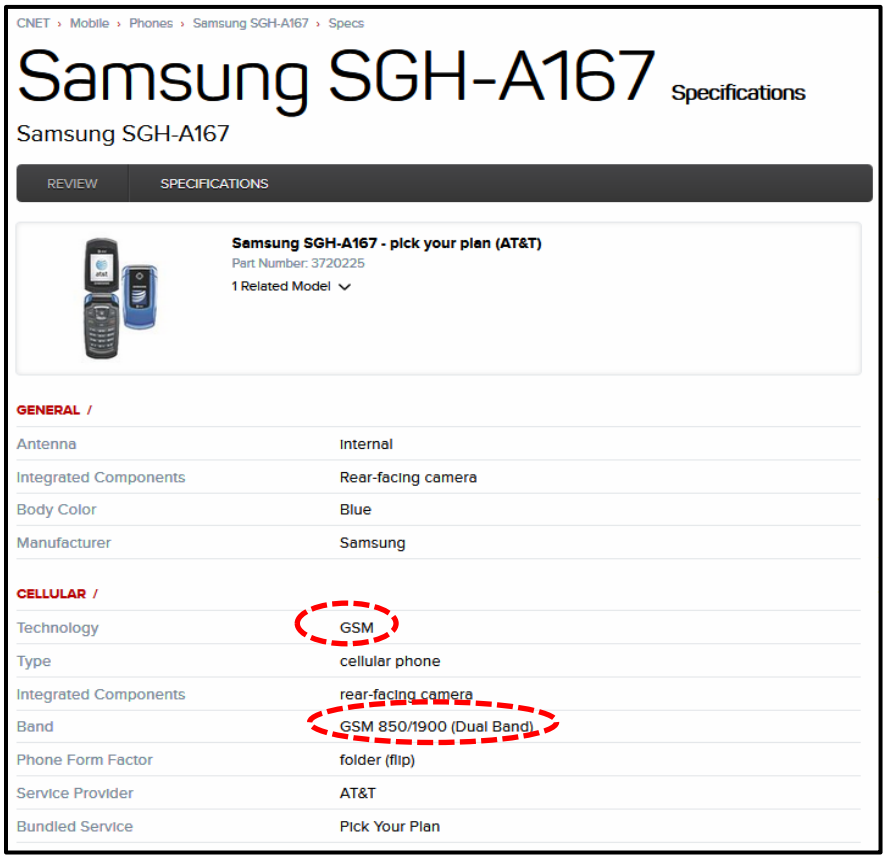

Figure 1: Samsung SGH-A167 phone specifications

Specifications for this mobile available on the Internet[6] (a snapshot is given in Figure 1) revealed that it is a GSM (2.5G) only phone (i.e. not a dual mode phone supporting 3G or 4G technologies too), capable of

[5] "FVI1404194 ATT Mobility Records 2-4-10 to 2-8-10.pdf".

[6] https://www.cnet.com/products/samsung-sgh-a167/specs/.

the so-called "dual band" operation in bands called 850 (MHz) and 1900 (MHz)[7]. This means this phone can connect only to GSM (2.5G) cells in 850 or 1900 bands, so that only the 2.5G cells in these two bands from the Cell Site Table are relevant for the analysis of the calls in the Call Records file.

Further inspection of the User Guide for this phone, available on the web[8], revealed that, although a rather simple model, and certainly not a modern smart phone, the SGH-A167 supports *Airplane* and *Silent* modes of operation. In the Silent mode this phone is actually active and able to receive the incoming calls, but does not give any audible alerts (only a vibrating one), while in the Airplane mode it switches off all the cellular radio circuitry inside. From the Call Records perspective, incoming calls while in Silent mode would appear as a normal mobile *termination* (technical term for an incoming call)[9], while those received in the Airplane mode would appear as if the phone was switched off (powered down).

5 AT&T Network Performance in 2009/2010

Inspection of the call records can reveal information not just about the "target" phone, but also about the performance of the network it operated on. Two of the very indicative fields for this that are available for each call are named *Seizure Time* and *Elapsed Time*. Per the legend file[10] provided by the AT&T, Seizure Time is a period "*it took from the 'Send' button was pressed to the time the call was connected to the network*", while the Elapsed Time is a "*number of minutes and second of the call between the connection time and the end of the call, also known as call duration. Does not include seizure time*".

In order to understand these entries, below we give a simplified version of the stages that a normal mobile originated call goes through (steps in the call processing mechanism, aka the *call protocol*)

1) When a user presses Send, the mobile sends a Channel Request message to the strongest cell.
2) After receiving the Channel Request, a cell sends a Channel Assignment message, informing the mobile about RF frequency and time slot to use for voice communication.
3) At the same time, the Cell turns on its RF transmission as defined in 2).
4) The mobile detects the signal from the cell as per 2), and sends an indication to the cell after it detects its incoming signal.
5) Cell detects the mobile's indication, call is now set up (established).
6) Mobile hears the ringing until calling party answers, conversation can start.
7) After either side hangs-up, cell or mobile send a Release message and stop the call.

If the mobile experiences a Directed Retry, in step 2) above, the Channel Assignment message would indicate a different cell for the mobile to tune to than the one that received the initial call request.

In the case of mobile termination (call received by the mobile), the protocol would be:

---

[7] Bands are separate ranges of radio frequencies on which phones can operate, a bit like AM and FM bands in the broadcast radio. Besides 850 and 1900 bands, AT&T has the right to operate their cells in 700 (MHz) and AWS bands (1,700-2,100MHz and around 2,300MHz), but the latter two are mostly used for the latest technology called LTE (or 4G), which AT&T started rolling out gradually in 2011.

[8] Can be downloaded from https://www.phonearena.com/phones/Samsung-SGH-A167_id3401/manual.

[9] Technical term for mobile initiated calls (when subscriber presses Send) is "mobile origination".

[10] "AT&T Key.pdf".

0) Page message directed to the mobile is sent from all cells in the area.

1)-7) Same sequence as for an Origination.

Measured times in Call Records are:

a) Seizure Time – interval from receiving message in 1) to 5).
b) Elapsed Time – interval from start of 6) to 7).

Depending on how AT&T set the rounding to the full second values for these timers, entries of 0 sec for Seizure Time in normal calls would be either impossible (if the rounding is to the nearest full second value, calls practically never setup in under 0.5 sec) or extremely rare (if rounded down). Elapsed Time of 0 sec would similarly mean that the call was released by one of the sides practically as the ringing started, which would be very rare but not impossible.

Further inspection of the Call Records file suggested that there are several scenarios in which Seizure Time = 0 and Elapsed Time > 0:

a) Mobile called to check its own mailbox (as per the entries in the "Description" field of Call Record).
b) Incoming call to a powered off mobile that went to the voice mail without attempting to page the mobile[11].

It is not completely clear based on the info in the Call Record file, but a scenario with Seizure Time = 0 and Elapsed Time > 0 appears also to be possible in some cases of 3-way calling[12] and maybe in call forwarding scenarios. Either way, a vast majority of calls that have both Seizure Time = 0 and Elapsed Time = 0 are incomplete calls that did not complete the whole procedure 1)-5) for originations, or 0)-5) for terminations, and were thus never established[13]. Possible scenarios for this are:

a) Connection Request was not granted because of blocking (no resources in cells).
b) Failed Attempt – somewhere between steps 1) and 5) cell and mobile stopped hearing each other.
c) Abandoned Attempt – during the call set-up, i.e. between steps 1) and 5) the calling party hung up (incoming call) or pressed End (outgoing call).
d) Mobile never responded to a page from step 0), despite network considering it powered up and able to receive the page – scenario applicable to terminations only.

Scenario d) is possible if the network failed to receive a message from the mobile indicating a forthcoming

[11] When powering down (or going into the Airplane mode), before turning off their RF circuitry the mobiles send a message to inform the network that they will be shutting down (and similarly they send another message when they get powered up). Network uses these messages to alleviate network congestion by routing all the incoming calls received between these two messages directly to the voice mail.

[12] E.g. calls 96-98 in the Call Records file "909-374-0102 - ReportAU_1497291.pdf". Call 96 is an originated call that started at 8:44AM and lasted for 7:24 minutes. Call 97 was an incoming at 8:44AM that lasted for 38sec and call 97 is a mobile originated one at 8:45AM that lasted for 31 sec. Both calls were made while the original call 96 was in progress, and both have Seizure Time = 0 since these 3-way calls did not go through the protocol for establishing calls in steps 0)-5), as the call was already established. There are no examples of forwarded calls in the whole Call Records file.

[13] Mathematically, if the call was not established, neither of the timer values exist as numerical values (they could not be measured) and should have been left as blanks instead of populated as zeros. The AT&T call records file, however, is not set to display zeros for either of the two timer values (none of the 9,688 calls recorded have blanks in either of these fields).

power-down (rare but possible) and certainly if the phone was in some sort of a coverage hole and could not hear the page. Case d) can be distinguished from other scenarios by the fact that there will be no information about starting cell populated in the Cell Location part of the call record (since the mobile never responded), while in cases a) to f) that information would be present.

Sorting of the call records in the file "909-374-0102 - ReportAU_1497291.pdf" shows that there were 9,688 voice calls recorded from Jan. 1, 2009 to Feb. 19, 2010, out of which 5,432 were the originations (mobile initiated calls) and 4,326 terminations (incoming calls). Out of 5,432 originations, 437 were found to be non-completed calls, or 8.0%. This is an extremely large number, in well-designed networks the percentage of incomplete calls averaged over busy and non-busy hours and various areas of the network are expected to be under 1% (and that includes blocking, failed attempts and abandoned attempts).

Furthermore, out of 4,326 terminations, 2,321 show both Seizure Time = 0 and Elapsed Time = 0. Out of these 2,321, total of 914 calls show no Cell Location indication, suggesting no page response (phone in the coverage hole, or network erroneously paging a powered-down mobile). This still leaves 2,321 – 914 = 1,291 non-completed incoming calls, none of which went to the voicemail. This amounts to a 30.5% noncompleted calls; an astonishing number for a cellular network.

Further insight can be gained by observing that for the originations, among 4,834 non-zero entries for the Seizure Time, 1,583 values are at or above 20 sec (33%), giving a strong indication that the Directed Retry mechanism was active. Among 1,915 terminations with non-zero Seizure Time, however, only 85 values are larger than or equal to 20 sec. Such low value (4.3%) indicates a significant probability that Directed Retry was not employed for the incoming calls at all.

This approach might be inspired by the customer surveys results, widely known within the cellular industry, which consistently show that the drop calls and then the failed attempts cause greatest dissatisfaction among subscribers, while incomplete termination attempts come as distant third (in large part because subscribers are usually not aware if an incoming call fails). In view of this, operators experiencing large network overloads could easily adopt a following strategy to prioritize call requests at the cells:

- Serve incoming hand-in calls (ignoring them during call in progress could cause call drops).
- New origination attempts (mobile initiated calls).
- New termination attempts (mobile received calls).

It should be also noted that the fact that AT&T network was extremely overloaded and experienced awful call performance in 2009 and 2010 was well known in the cellular industry. It was widely discussed in the various specialized publications for cellular industry professionals, as well as in the mainstream media[14]. It was even a subject of jokes in the late-night talk shows at the time[15].

---

[14] "Customers Angered as iPhones Overload AT&T", NYT, Sept. 2009 https://www.nytimes.com/2009/09/03/technology/companies/03att.html

"AT&T to Boost 3G Network in Six Cities", WSJ, Sep.9 2009 , https://www.wsj.com/articles/SB125252438005196727

"AT&T Ranked Last in Consumer Report's Best Cellphone Service Survey", All Thing Digital, Dec.1 2009 http://digitaldaily.allthingsd.com/20091201/att-ranked-last-in-consumer-reports-best-cell-phone-service-survey/

[15] "Late Show with D. Letterman", CBS, Jun 18,2010 https://www.youtube.com/watch?v=kP5xBQ9eAH8

The AT&T network problems were largely due to the launch of the Apple iPhone in the fall of 2008 (which remained the AT&T-exclusive in the USA until early 2011). It caused an unexpected and unprecedented increase in call volumes, especially in terms of data calls. Since the original iPhone was GSM (2.5G) only device, it caused enormous strain on the AT&T's GSM network, which was by then already being under a process of phasing out in favor of the newer, more efficient technology called UMTS (3G). Deployments of UMTS started in 2005 and required large portions of the original GSM bands to be converted to UMTS at one time, causing serious resource shortages on the GSM side and temporary outages (on both sides, during the equipment swaps).

6 Other Data Sources

Prosecution originally shared with the Defense only the Call Records file, which was insufficient for geo-location work as discussed in the accompanying report[16]. Facing this situation Defense Counsel issued a subpoena to AT&T for the following information from the area of interest:

1) Cell Site Tables as per Jan/Feb 2010 and June 2016.
2) Maintenance records for Jan/Feb 2010.
3) Propagation maps from Jan/Feb 2010 and June 2016.
4) Drive test data from Jan/Feb 2010 and June 2016.

Areas of interest were defined by a set of about 35 postal ZIP codes in the Riverside, San Bernardino and San Diego counties. They are listed in the companion report[16].

AT&T's response per request from 1) is discussed elsewhere[16]. Maintenance records from 2), which would have helped verify if some of cells that existed in the Cell Site Table in February 2010 were actually active, or taken off air for scheduled or unscheduled maintenance, were not received. Propagation maps from 3), usually coming from the operator's RF Propagation Prediction Tools were not received either. They are not perfectly accurate in terms of showing the actual RF coverage for each individual cell, but can be useful nevertheless.

AT&T did provide some drive test data from 4), which can be useful to assess the actual coverage of the cells. In general, drive test measurements give more accurate results for the cell coverage than the prediction maps, but provide much fewer data points (only along the streets driven). In addition, they usually provide data about the "on street" performance of the network only, with little or no information about the in-building coverage for instance.

Inspection of the received files indicated that they contain data from the drive tests performed in the summer of 2014, not from the intervals requested. In all calls the dialed number was 911, suggesting that these tests were performed to assess the AT&T compliance with the Federal Communication's Commission mandate for cellular operators to provide reasonably precise geolocation estimates for all emergency

"Late Show with J. Stewart", Comedy Central, 1/11/2011, http://www.cc.com/video-clips/gx0vcm/the-daily-show-with-jon-stewart-verizon-iphone-announcement

[16] V. Jovanovic, "AT&T Cell Site Problems", 09/14/2018, pp.5.

calls that dialed 911[17].

Supplied data covered quite extensive set of routes in the Riverside, San Bernardino and San Diego counties, as depicted in Figure 2 for the drives in Victorville/Apple Valley area. Besides the location of each individual point of measurement (mobile's GPS coordinates), data contains the cell ID information for the serving cell, enabling rather good estimates of which cell serves which areas along the routes. An example of this is shown in Figure 3.

Drive test data from 2014 cannot give an exact picture of the RF situation in 2010 because the cellular networks undergo constant changes. Cells and their configurations in 2014 are not necessarily the same as they were in 2010. In addition, even if the networks were exactly the same there will be seasonal differences – drive tests in June normally give different results than those in February because of the active foliage, which can have significant impact in some areas[18]. Furthermore, all 911 calls from the file where made using the UMTS (3G), not the GSM (2.5) technology that the Defendant's phone used. As such, this drive test data clearly cannot be used to definitely prove or disprove anything about the coverage on GSM technology in February 2010. After careful assessment of the GSM network in 2010 and the UMTS network in 2014, however, data can still be used to verify some basic assertions and conclusions about network coverage, especially those that are based on the terrain elevations and antenna heights.

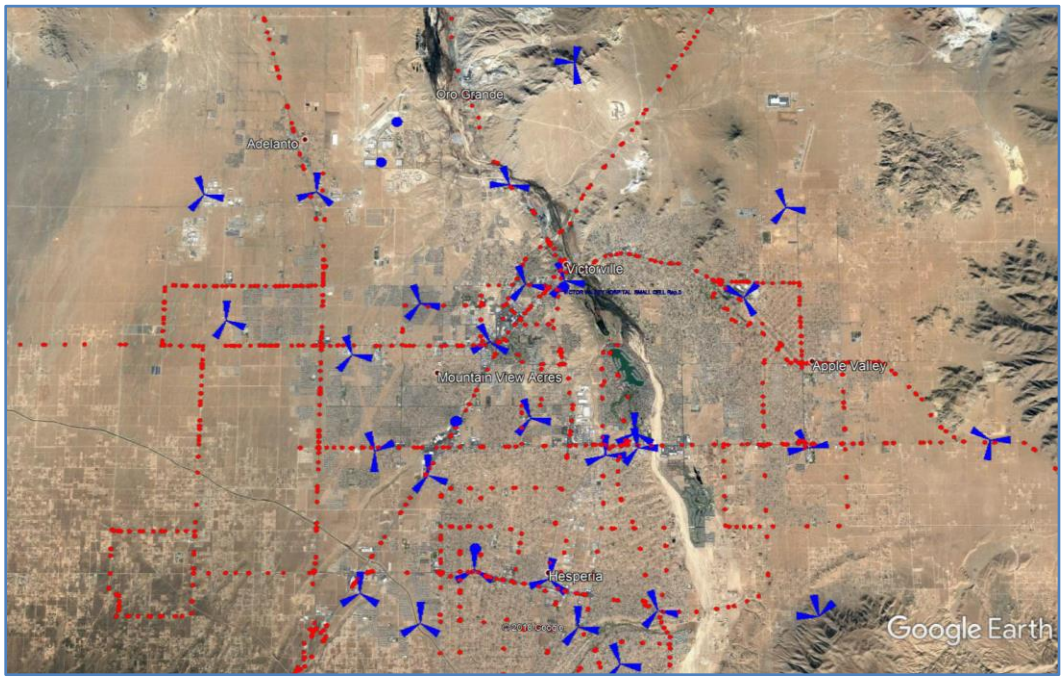

Figure 2: Drive test measurement points in Victorville/Apple Valley

[17] The so called "Enhanced 911, Phase 2" requirements that came into effect in the fall of 2012. Many operators were struggling to meet the requirements from both phases of the Enhanced 911, see for instance "Carriers push E-911 Lawsuit in Court Despite Winning Deadline Extension", RCR Wireless News, Mar. 14, 2008.

[18] Seasonal differences e.g. in the High Desert area are expected to be rather small, however.

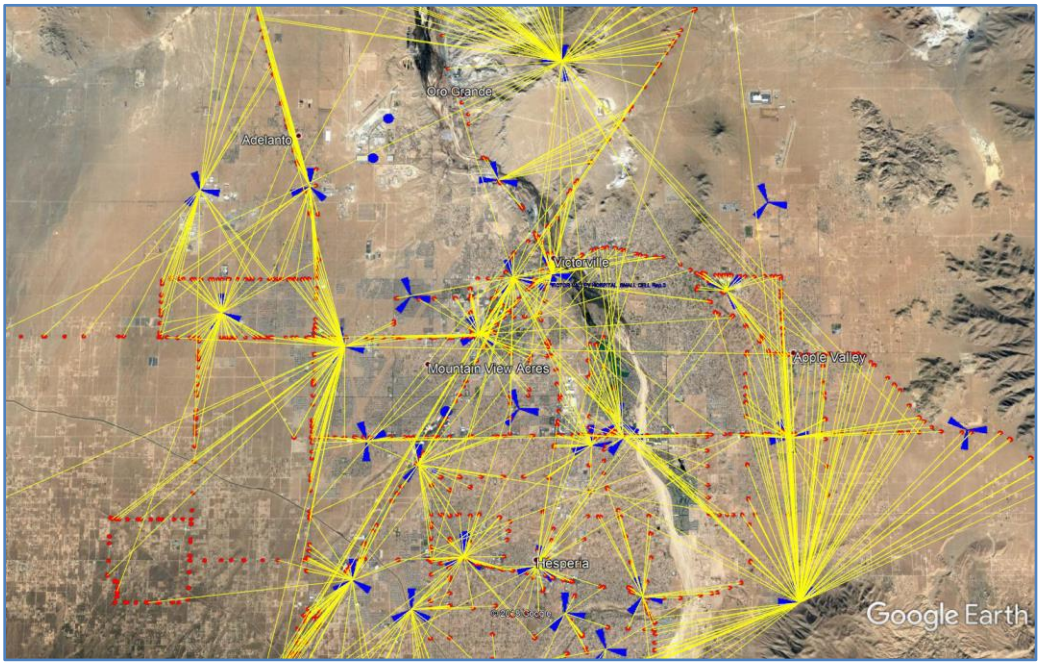

Figure 3: Plot as in Figure 2, but with the lines to the serving cell added

An example of network comparison that would be required to check the GSM (2.5G) and UMTS (3G) network in an area is shown in Figure 4. UMTS cells (blue) are superimposed on the GSM cell (red). Network differences in terms of the cell existing on UMTS that don't exist on GSM and vice versa are circled, as well as the differences in the sector antenna orientations on the sites that share the same location for both technologies.

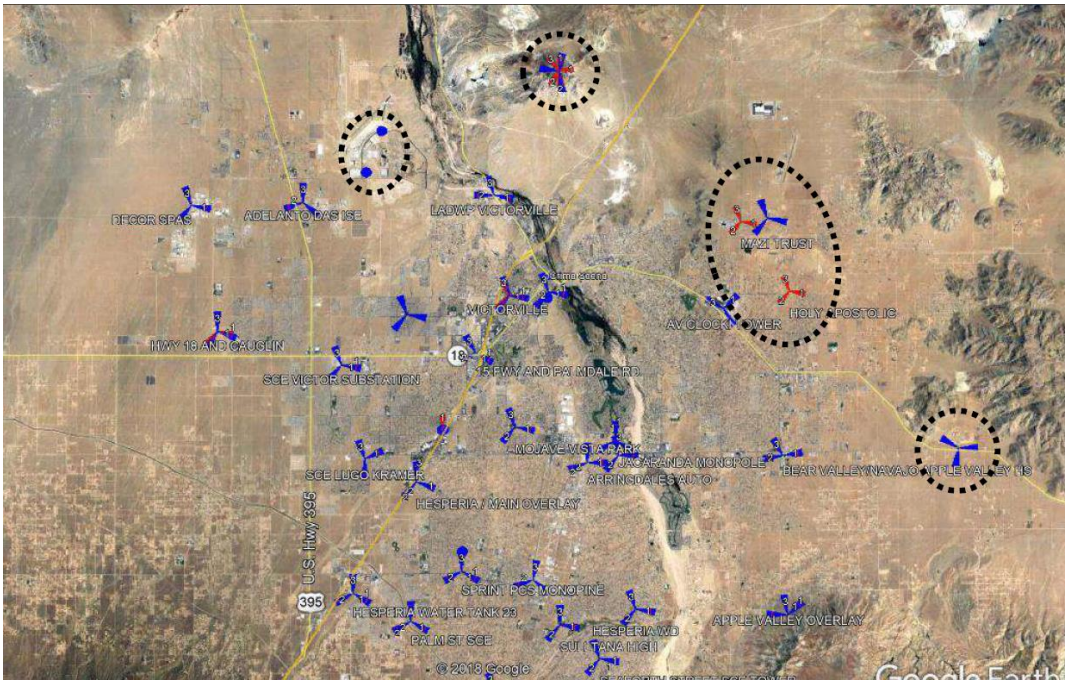

Figure 4: Plot of UMTS cells (blue) superimposed on GSM cells (red) in the same area

7 Analysis of calls 6PM-12PM on 02/04/2010

Excerpt from the Call Records file showing the calls made during this interval is given in Figure 5.

Item	ConnDateTime		Seizure Time	Originating Number	Terminating Number	Elapsed Time	Number Dialed	IMEI	IMSI	Description	CellLocation
9076	02/04/10	05:48PM	0:06	19492957451	19093740102	2:37	19093740102	1189700137274	310410208101679	m2M_DIR	[05267/16635:-117.55625:34.10839:100 05267/16631:-117.55625:34.10839:0]
9077	02/04/10	06:09PM	0:00	19092261197	19092132103	0:05	19093740102		310410208101679	M2M_VMB	[]
9078	02/04/10	06:10PM	0:00	19092261197	19092132103	0:04	19093740102		310410208101679	M2M_VMB	[]
9079	02/04/10	06:12PM	0:00	19093748951	19092132103	0:04	19093740102		310410208101679	M2M_VMB	[]
9080	02/04/10	06:17PM	0:00	19092261197	19092132103	0:05	19093740102		310410208101679	M2M_VMB	[]
9081	02/04/10	07:18PM	0:00	19092261197	19092132103	0:04	19093740102		310410208101679	M2m_VMB	[]
9082	02/04/10	09:04PM	0:00	19092261197	19092132103	0:04	19093740102		310410208101679	M2M_VMB	[]
9083	**02/04/10**	**09:32PM**	**0:10**	**19093740102**	**19092261197**	**3:12**	**19092261197**	**1189700137274**	**310410208101679**	**M2M_DIR**	**[55010/04469:-117.51056:34.00389:340 55010/15363:-117.4835:34.00211:320]**
9084	02/05/10	07:00AM	0:01	19093740102	19092132104	0:39	1119092132104	1189700137274	310410208101679	M2m_VMC	[05267/19605:-117.64371:34.13336:60 05267/19601:-117.64371:34.13336:60]

Figure 5: Calls between 6PM and 12PM on 02/04/2010 from the Call Records file

The six calls made between 6:09PM and 9:04PM were the unanswered incoming calls (terminations) that all went directly to voice mail because the mobile did not respond to the page message, as indicated by the empty Cell Location fields (phone in coverage hole, in Airplane mode etc.) They cannot be geolocated for this reason at all, so the only call in the whole period of interest that could be geolocated was the 9:32PM one, with the next recorded (and geolocatable) call at 7:00AM the next morning.

Experts for the Prosecution placed the 9:32PM call on the highway I-15, travelling northbound[19]. We note that the last geolocatable call before the 9:32PM one was made almost 4 hours earlier, while the next one was made more than 9 hours later. This means that any inference on the direction of travel could have only been made solely from the information related to the 9:32PM call itself (phone can travel a few hundred miles within 4 hours).

Inspection of the Call Records file reveals that the 9:32PM call on 02/04/2010 started on cell 55010/04469 and ended on 55010/15363. From the Cell Site Table file these two cells are the "Jurupa Valley Sport Park" and the "LAC526/Mira Loma Ovly – C536", both in the Mira Loma area, as shown in Figure 6.

	D	E	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	frequency	technology	sitename	address	city	state	county	zip	latitude	longitude	lac	cid	height	sectorid	beamwidth	sectororientation
5156	850	25G	JURUPA VALLEY SPORTS PARK	10400-10500 BELLEGRAVE AVENUE	MIRA LOMA	CA		91752	34.00389	-117.51056	55010	4461	72	A	0	0
5157	850	25G	JURUPA VALLEY SPORTS PARK	10400-10500 BELLEGRAVE AVENUE	MIRA LOMA	CA		91752	34.00389	-117.51056	55010	4462	72	B	0	120
5158	850	25G	JURUPA VALLEY SPORTS PARK	10400-10500 BELLEGRAVE AVENUE	MIRA LOMA	CA		91752	34.00389	-117.51056	55010	4463	72	C	0	240
5159	1900	25G	JURUPA VALLEY SPORTS PARK	10400-10500 BELLEGRAVE AVENUE	MIRA LOMA	CA		91752	34.00389	-117.51056	55010	4467	72	A	68	100
5160	1900	25G	JURUPA VALLEY SPORTS PARK	10400-10500 BELLEGRAVE AVENUE	MIRA LOMA	CA		91752	34.00389	-117.51056	55010	4468	72	B	68	220
5161	**1900**	**25G**	**JURUPA VALLEY SPORTS PARK**	**10400-10500 BELLEGRAVE AVENUE**	**MIRA LOMA**	**CA**		**91752**	**34.00389**	**-117.51056**	**55010**	**4469**	**72**	**C**	**68**	**340**
5162	850	25G	ONTARIO CA-0197	1206 NORTH GROVE AVENUE	ONTARIO	CA		91764	34.08	-117.62833	55010	8101	80	A	85	100

	D	E	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	frequency	technology	sitename	address	city	state	county	zip	latitude	longitude	lac	cid	height	sectorid	beamwidth	sectororientation
5211	850	25G	LAC536/MIRA LOMA OVLY - C536	4752 FELSPAR STREET	RIVERSIDE	CA		92509	34.00211	-117.4835	55010	15361	92	A	65	30
5212	850	25G	LAC536/MIRA LOMA OVLY - C536	4752 FELSPAR STREET	RIVERSIDE	CA		92509	34.00211	-117.4835	55010	15362	92	B	65	220
5213	**850**	**25G**	**LAC536/MIRA LOMA OVLY - C536**	**4752 FELSPAR STREET**	**RIVERSIDE**	**CA**		**92509**	**34.00211**	**-117.4835**	**55010**	**15363**	**92**	**C**	**65**	**320**
5214	1900	25G	LAC536/MIRA LOMA OVLY - C536	4752 FELSPAR STREET	RIVERSIDE	CA		92509	34.00211	-117.4835	55010	15367	92	A	65	30
5215	1900	25G	LAC536/MIRA LOMA OVLY - C536	4752 FELSPAR STREET	RIVERSIDE	CA		92509	34.00211	-117.4835	55010	15368	92	B	65	220
5216	1900	25G	LAC536/MIRA LOMA OVLY - C536	4752 FELSPAR STREET	RIVERSIDE	CA		92509	34.00211	-117.4835	55010	15369	92	C	65	320

Figure 6: Cell Site Table excerpts for cell sites "Jurupa Valley Sport Park" and "LAC526/Mira Loma Ovly – C536"

[19] File "7298-7786 (SBSD Inv Rept Narratives) 1 of 4 (2).pdf", p.13 (Bates #007533).

Due diligence exercise on the Cell Site Table as reported in the accompanying report suggested that the entries for the end cell are reasonable and probably correct, while the entries for the "Jurupa Valley Sports Park" show serious inconsistencies with azimuths, although the value of 340° as reported here is likely to be the correct one[20]. The area of these two sites is depicted in Figure 7.

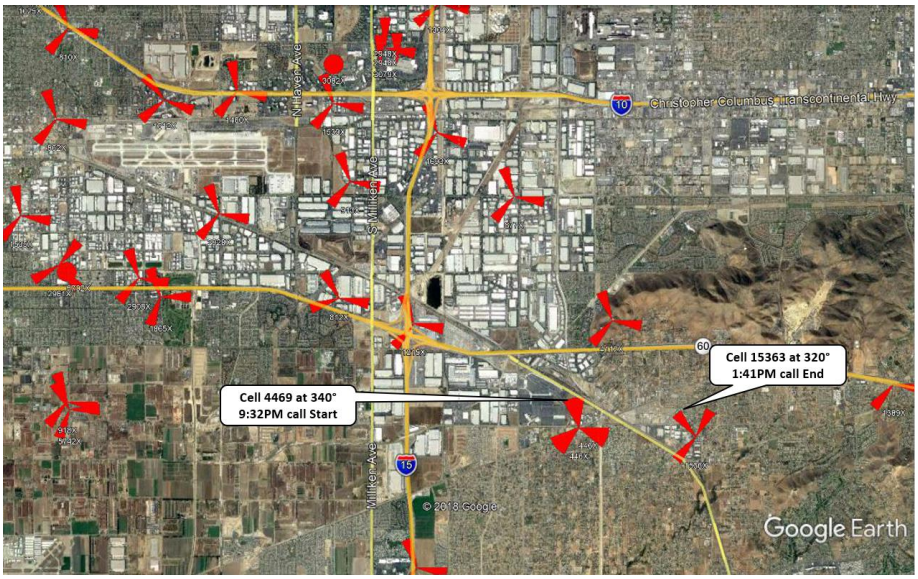

Figure 7: Network in Mira Loma area – 9:32PM call on 02/04/2010

Prosecution's assertion that phone was on I-15 during 9:32PM call is impossible to corroborate because:

- Both cells that carried the call are pointed towards North/Northwest.
- There are 5 cells in that direction, near or on I-15, that are more likely to carry the calls on I-15 based on their proximity.
- Terrain along I-15 elevates slowly, from about 820 feet around Rte. 60 to about 1,000 feet near I-10.
- Both cells that carried the call are at approx. 730 feet elevation, with the antenna heights of 72 and 90 feet per the Cell Site Table.
- Call Seizure Time of 10 sec. is not indicative of a Directed Retry.

While the claim that cells 55010/04469 and 55010/15363 can reach I-15 while shooting below the elevation levels of I-15 to the North does not seem justifiable, inferences about the northbound direction of travel is clearly unfounded. The more likely directions of travel were:

- Moving Eastbound on Mission Blvd.
- Moving Southbound along Van Buren Blvd.

Check of the drive test data available from this region shows that on the UMTS the areas covered by these two sites do not include I-15 either, as depicted in Figure 8. Again, results from the UMTS cannot be used as a definitive proof for anything on the GSM (e.g. sector orientation on both cells was somewhat changed in the UMTS cells), but they strongly suggest that our conclusions based on the terrain elevation and the antenna heights (which are the same for both technologies) are valid.

[20] V. Jovanovic, "AT&T Cell Site Problems", 09/14/2018, pp.25-27.

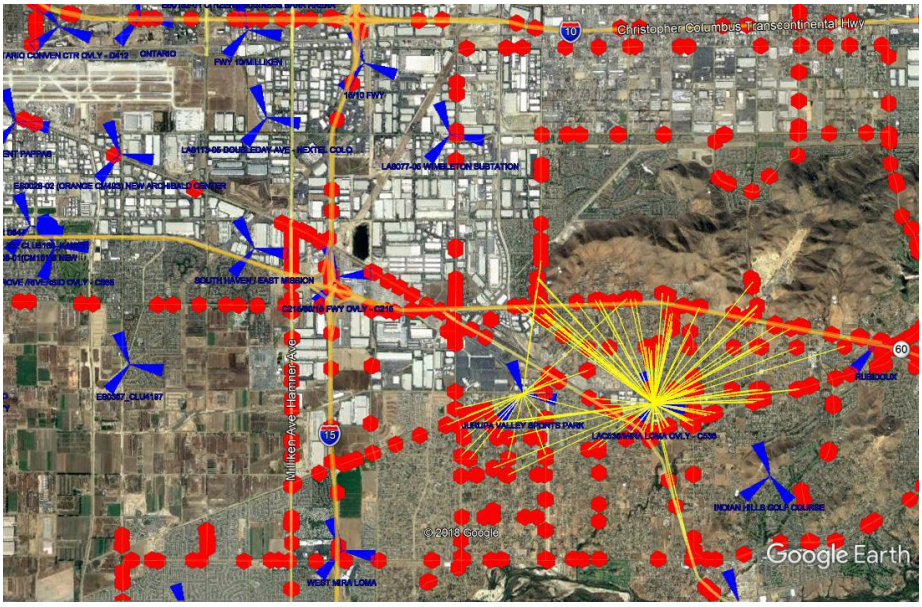

Figure 8: Drive test data indicating coverage of cells 55010/04469 and 55010/15363

8 Analysis of Calls on 02/06/2010

Excerpt from the Call Records file that cover calls made on this day is presented in Figure 9.

Item	ConnDateTime		Seizure Time	Originating Number	Terminating Number	Elapsed Time	Number Dialed	IMEI	IMSI	Description	CellLocation
9105	02/05/10	09:25PM	0:21	19093740102	19092261197	1:35	2261197	1189700137274	310410208101679	M2M_DIR	[05267/13047:-117.54278:34.08472:350 05267/29412:-117.49992:34.12117:]
9106	02/06/10	10:46AM	0:27	19093740102	19092261197	0:03	2261197	1189700137274	310410208101679	M2M_DIR	[05262/15777:-117.31157:34.52922:340 05262/15772:-117.31157:34.52922:220]
9107	02/06/10	11:30AM	0:00	18003952274	19093740102	0:00	19093740102	1189700137274	310410208101679	O2M	[05262/11095:-117.28944:34.61111:85 05262/11091:-117.28944:34.61111:10]
9108	02/06/10	11:31AM	0:26	19093740102	19092261197	0:03	2261197	1189700137274	310410208101679	M2M_DIR	[05262/11095:-117.28944:34.61111:85 05262/11091:-117.28944:34.61111:10]
9109	02/06/10	11:32AM	0:10	19093740102	19093748951	0:02	19093748951	1189700137274	310410208101679	M2M_DIR	[05262/11091:-117.28944:34.61111:10]
9110	02/06/10	11:33AM	0:27	19093740102	19093748951	0:04	19093748951	1189700137274	310410208101679	M2M_DIR	[05262/11095:-117.28944:34.61111:85 05262/11091:-117.28944:34.61111:10]
9111	02/06/10	11:34AM	0:26	19093740102	19092261197	0:02	2261197	1189700137274	310410208101679	M2M_DIR	[05262/11095:-117.28944:34.61111:85 05262/11091:-117.28944:34.61111:10]
9112	02/06/10	11:52AM	0:26	19093740102	19092261197	0:09	2261197	1189700137274	310410208101679	M2M_DIR	[05262/11095:-117.28944:34.61111:85 05262/03483:-117.32611:34.50806:330]
9113	02/06/10	11:53AM	0:26	19093740102	19093748951	0:10	19093748951	1189700137274	310410208101679	M2M_DIR	[05262/03483:-117.32611:34.50806:330 05262/15403:-117.187:34.41181:350]
9114	02/06/10	12:49PM	0:08	19093740102	19092261197	3:45	2261197	1189700137274	310410208101679	M2M_DIR	[05262/29186:-117.29347:34.53044:220 05262/03481:-117.32611:34.50806:120]
9115	02/06/10	01:30PM	0:09	19093740102	19092261197	0:44	2261197	1189700137274	310410208101679	M2M_DIR	[05262/11092:-117.28944:34.61111:170 05262/18613:-117.3525:34.46056:360]
9116	02/06/10	02:22PM	0:00	18003952274	19093740102	0:00	19093740102	1189700137274	310410208101679	O2M	[05267/16636:-117.55625:34.10839:220 05267/16632:-117.55625:34.10839:0]
9117	02/06/10	02:40PM	0:00	18003952274	19093740102	0:00	19093740102	1189700137274	310410208101679	O2M	[05267/16636:-117.55625:34.10839:220 05267/16632:-117.55625:34.10839:0]
9118	02/06/10	03:14PM	0:12	19093740102	19092261197	0:55	2261197	1189700137274	310410208101679	M2M_DIR	[05267/16635:-117.55625:34.10839:100 05267/16631:-117.55625:34.10839:0]
9119	02/07/10	10:35AM	0:00	18003952274	19093740102	0:00	19093740102	1189700137274	310410208101679	O2M	[05267/16635:-117.55625:34.10839:100 05267/16631:-117.55625:34.10839:0]

Figure 9: Calls on 02/06/2010

Defendant's phone was involved in 13 calls on this day, between 10:46AM and 3:14PM. All but 3 were outgoing calls (3 incoming were at 11:30AM, 2:22PM and 2:40PM). Seizure times of 26 and 27 sec for all the calls but one before 12:49PM are indicative of possible Directed Retries (an exception was the call at 11:32AM; 11:30AM was a non-completed call and could have gone either way).

8.1 Call at 10:46AM on 02/06/2010

Inspection of the Cell Site Table shows that both the start and the end cell for this call were on the cell site called "Victorville". Based on the mapping tools we utilized, the reported location and antenna height (80 feet) appear to be correct. General area of this site is shown in Figure 10.

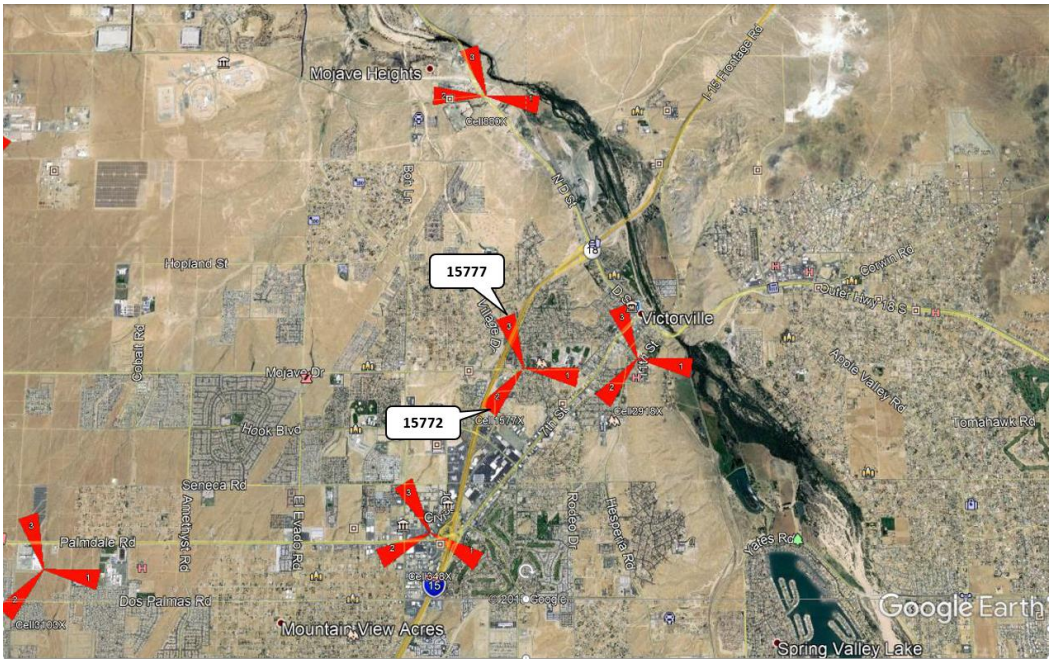

Figure 10: Area around cell site "Victorville"

From the figure it is easy to conclude that this call was made from West side of Victorville, possibly on I-15. The fact that call started on the cell 15777 and ended on the cell 15772 would further suggest the southbound travel on I-15, but since the Seizure Time of 27 sec indicates a likely Directed Retry scenario, no such conclusion should be made. The sequence of cells during this call would depend on which cell was free of blocking, not just on the direction of travel.

8.2 Calls from 11:30 to 11:34AM on 02/06/2010

There were 5 calls made in this period. Prosecution's expert indicated a double-shaded area in Figure 11 as the likely zone from which these calls were made (as well as the 11:52AM call; that point will be addressed later). We note that the double-shaded area is questionable in two ways:

- segment's angular boundaries (pie segment "width").
- radius of the "pie segment" (will be addressed later too).

Pie segment in Figure 11 spans from approximately 20° to 90° from North. These boundaries appear to have been drawn assuming a nominal 120° sector width[21], in which case the overlap region would have been from 25° to 70°, i.e. considerably further North and away from the "Location of Crime Scene" then indicated[22].

[21] "FVI1404194 PLH Transcript 6-15-15. pdf", pp.88.

[22] Cell pointing at 10° would cover azimuths from 310° (10°-60°=-50°, 360°-50°-310°), to 70° (10°+60°). The cell at 85° would cover from 25° (85°-60°) to 145° (85°+60°), resulting in the overlap area between 25°and 70°.

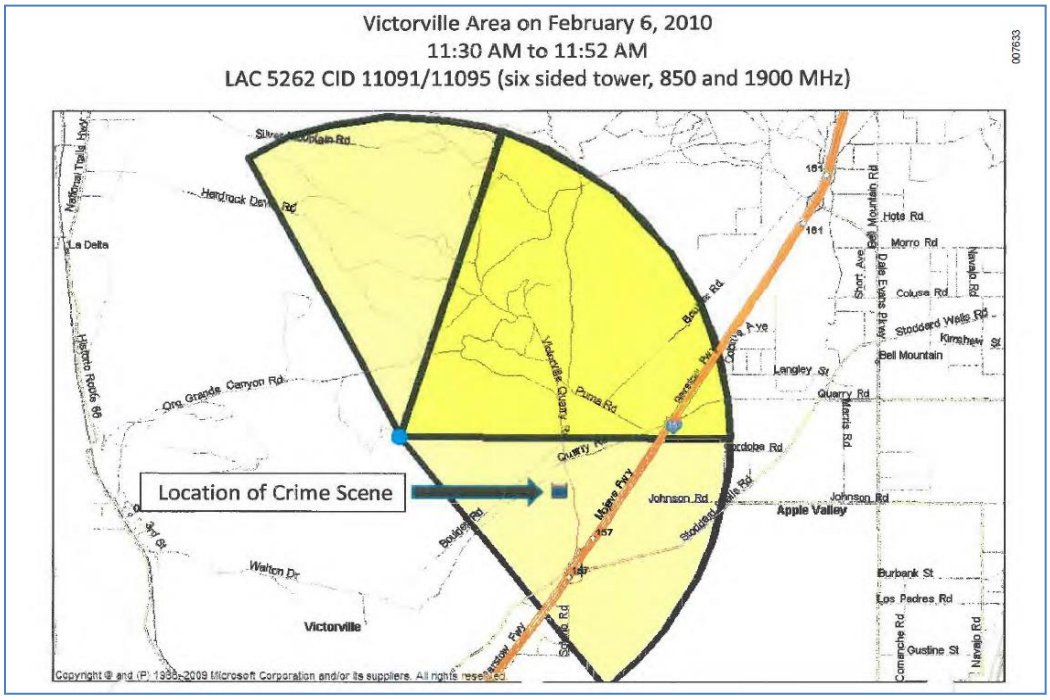

Figure 11: Likely area for the 11:30-11:34AM calls as presented by the Prosecution's experts[23]

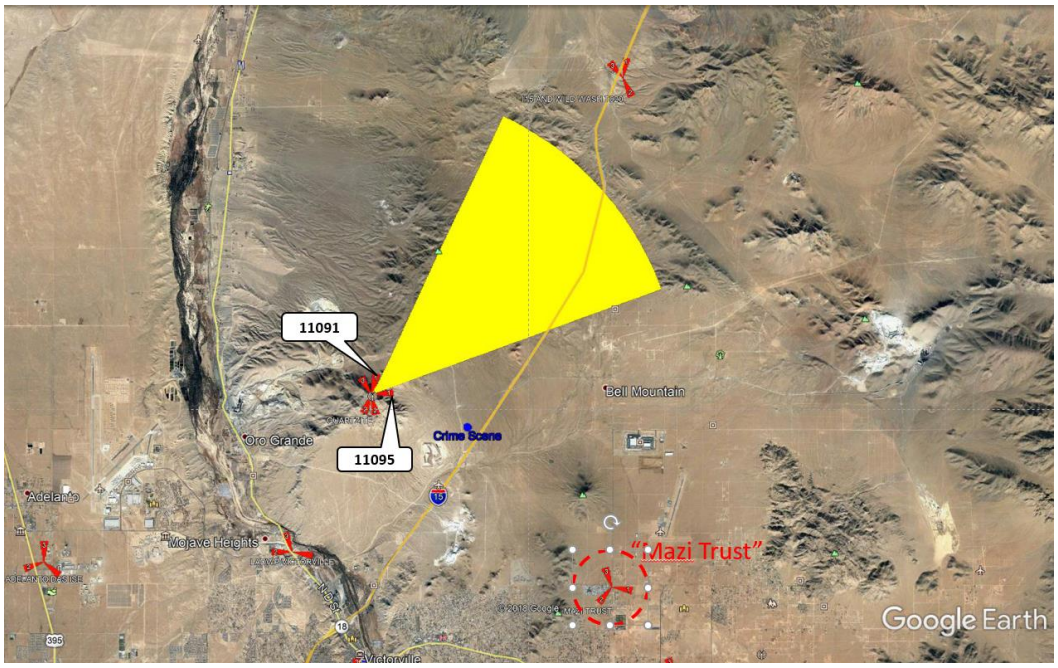

Figure 12: Our estimate area of the hand-ff overlap area between cells 11091 and 11095[24]

The correct depiction of the overlap area from 25 to 70° is shown in Figure 12. We note that the crime

[23] File "7298-7786 (SBSD Inv Rept Narratives) 4 of 4 (2).pdf", p.4.

[24] This graph is obtained analytically, as an area in which signals from 2 antennas are within a 9:1 range (9.5dB) of each other, which also gives boundaries at 25° and 70° (±0.5°). This range is chosen to account for hand-off hysteresis of 2-3dB and signal measurement errors of up to 6dB. Standard parabolic approximation for the radiation pattern of 65° antennas was used, per the beamwidth entries from the Cell Site Table for the two cells involved.

scene is not in the area of overlap in either of the two plots.

Going back to the original call records from Figure 5, however, the following observations can be made regarding the 5 calls in the 11:30-11:34AM period:

- All calls but one started on cell 05262/11095 pointing almost straight to the East (azimuth 85°) and then handed-off to the cell 05262/11091 shooting almost straight to the North (azimuth 10°).
- Call at 11:32AM did not hand-off, but started and ended on cell 05262/11091 (shooting North).
- Seizure time of 10 sec for the same 11:32AM call is not indicative of a Directed Retry. All other calls either very likely endured a Directed Retry (Seizure Times of 26 and 27 sec) or might have done so (11:30AM, incomplete call, impossible to tell).

The series of hand-offs back and forth between cells 11095 and 11091 is rather unusual. Such bouncing between serving cells is undesirable in cellular networks because it taxes the call processing resources within the system. To prevent it, cellular networks normally employ two mechanisms:

- *Hand-off Hysteresis* requires the new cell to be typically 1.6 to 2 times (2-3dB) stronger than the old one for the cell swap to occur (it delays the handoff until new cell is sufficiently stronger so that bounce back is less likely)[25].
- *Hand-off Timer* mandates a wait period of typically 2-5 sec after a handoff before a new one would be serviced.

For this sequence of hand-offs to occur, the call records suggest that the phone must have spent 4 minutes in an area where both cells are of very comparable but variable signal strengths. Furthermore, both of these cells are on different sectors of the same cell site ("Quartzite", per the excerpt from the Cell Site Table shown in Figure 13), which makes the bouncing even more unusual[26].

	D	E	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	frequency	technology	sitename	address	city	state	county	zip	latitude	longitude	lac	cid	height	sectorid	beamwidth	sectororientation
59	1900	25G	QUARTZITE	1 ORO GRANDE ROAD	ORO GRANDE	CA	SAN BERNARDINO	92368	34.611111	-117.28944	5262	11091	117	A	65	49
60	1900	25G	QUARTZITE	1 ORO GRANDE ROAD	ORO GRANDE	CA	SAN BERNARDINO	92368	34.611111	-117.28944	5262	11092	117	B	65	49
61	1900	25G	QUARTZITE	1 ORO GRANDE ROAD	ORO GRANDE	CA	SAN BERNARDINO	92368	34.611111	-117.28944	5262	11093	117	C	-1	-1
62	850	25G	QUARTZITE	1 ORO GRANDE ROAD	ORO GRANDE	CA	SAN BERNARDINO	92368	34.611111	-117.28944	5262	11095	117	A	65	49
63	850	25G	QUARTZITE	1 ORO GRANDE ROAD	ORO GRANDE	CA	SAN BERNARDINO	92368	34.611111	-117.28944	5262	11096	117	B	65	49
64	850	25G	QUARTZITE	1 ORO GRANDE ROAD	ORO GRANDE	CA	SAN BERNARDINO	92368	34.611111	-117.28944	5262	11097	117	C	65	49
4276	**1900**	**25G**	**QUARTZITE**	**1 ORO GRANDE ROAD**	**ORO GRANDE**	**CA**		**92368**	**34.61111**	**-117.28944**	**5262**	**11091**	**117**	**A**	**65**	**10**
4277	1900	25G	QUARTZITE	1 ORO GRANDE ROAD	ORO GRANDE	CA		92368	34.61111	-117.28944	5262	11092	117	B	65	170
4278	1900	25G	QUARTZITE	1 ORO GRANDE ROAD	ORO GRANDE	CA		92368	34.61111	-117.28944	5262	11093	117	C	-1	-1
4279	**850**	**25G**	**QUARTZITE**	**1 ORO GRANDE ROAD**	**ORO GRANDE**	**CA**		**92368**	**34.61111**	**-117.28944**	**5262**	**11095**	**117**	**A**	**65**	**85**
4280	850	25G	QUARTZITE	1 ORO GRANDE ROAD	ORO GRANDE	CA		92368	34.61111	-117.28944	5262	11096	117	B	65	205
4281	850	25G	QUARTZITE	1 ORO GRANDE ROAD	ORO GRANDE	CA		92368	34.61111	-117.28944	5262	11097	117	C	65	325

Figure 13: Entries for 2.5G technology cell on site "Quartzite" from Cell Site Table

One possible explanation for these hand-off patterns is that azimuths for the cell 11095 and 11091 were not populated correctly in the Cell Site Table. Looking at the excerpt in Figure 13, we find the obviously

[25] Note that the hysteresis creates an area of overlap where a phone can be served on either of the two cells, depending on the direction of travel, i.e. the history of past signal changes.

[26] Antennas on the neighboring sectors of the same tower are spatially very close, usually within a yard or two. Any obstacles along the propagation path between these antennas and the phone antenna normally affect both signals in the same way. Boundaries between the sectors in such a case are defined almost exclusively by the antenna radiation patterns, which are very precisely defined and steady.

erroneous entries for this cell site (all 3 sectors on the azimuths of 49° in the first block of entries, rows 58-64), incomplete data (missing azimuth for the sector C in 1900 band in both blocks of entries, rows 61 and 4278) or rather suspect entries (different sector orientations in 1900 and 850 band in the second block[27]). The Companion report[28] goes into more detail about these and other problems with all blocks of entries for the "Quartzite" and for many other cell sites, indicating a very disorderly data entry and the Cell Site Table audit process in AT&T at the time.

A comparison with the Call Records shows that the second block of entries for "Quartzite" (rows 4276-4281) was the one in use in February 2010 (otherwise cells 11095 and 11091 would have been listed at 49°). Now, if the entries for one of the bands were wrongly populated in this block, and in reality, the sectors on both bands had the same azimuths as is usually the case, then both cells 11091 and 11095 would have been on the same azimuth since they are both in sector A (either 10° or 85°). Hand-offs between two cells on different bands within the same sector would then be a rather routine procedure in cellular operations (Inter-band, intra-sector hand-offs, often used for to balance the traffic load between bands)[29].

Yet another possible explanation for the chaotic hand-off patterns could be related to antenna down-tilts. Inspection of the terrain elevation data (e.g. in Google Earth) reveals that the site "Quartzite" is on top of a 4,500-foot-high mountain, while the High Desert area to the East and Northeast is at about 3,000-3,100 feet, as depicted in Figure 14. Elementary trigonometry then shows that the locations 2 miles away from the site (i.e. points along I-15 nearby) would be seen at a vertical angle of 9°, while the locations at say, 6 miles away along the same highway, would be seen at an angle of 3°.

In Figure 15, which depicts the radiation patterns of a typical cellular antenna[30], we see that in this range of vertical angles the antenna transmits largely outside of its main radiation lobe. Gain in the sidelobes is much smaller, very irregular and prone to deformations when the antenna is mounted on a tower (due to the signal reflections from the support structure). If in an area covered by the side lobes, mobile phones

[27] Having the same sector on different azimuths in different bands is not impossible, but is rather unusual. It precludes the use of the so-called *dual-band* antennas, causes more call processing than necessary, more inherently less reliable inter-band handoffs, etc. In addition, it would cause various problems in the optimization and performance engineering (with Neighbor List maintenance, interpretation of drive test data, etc).

RF engineering tool *Truecall™* by *Newfield Wireless* (now *Netscout*), used by cellular operators for visual presentation of the network data based on the call records, on which author worked for about 7 years, did not have an option to handle or display different azimuths for different bands on the same sector. During that period Cell Site Tables from at least 20 different operators from the USA and abroad were imported into this tool and no single instance of a problem due to this limitation was ever reported.

[28] V. Jovanovic, "AT&T Cell Site Problems", 09/14/2018; problems with entries for cell site "Quartzite" are addressed on pp.16-18 and pp.21-22.

[29] It is further worth noticing here that – even if these entries were correct and sector A indeed had cells pointing in different directions in different bands – the missing entry for cell in sector C in 1900 band would still be a problem. Any discussion of the potential handoff areas between cells at pointing angles of 10° and 85° would be predicated on the assumption that the cell with the missing entry is pointing far away from the area of their overlap. Azimuths of the adjacent cells in 1900 band suggests that the missing azimuth might be somewhere around 270°, which would have little impact on the overlap area if true, but we would never know for sure.

[30] This particular data is from antenna CX063X19x00 by "Amphenol".

could receive unpredictable and very variable signals even in the case of the very small phone movements.

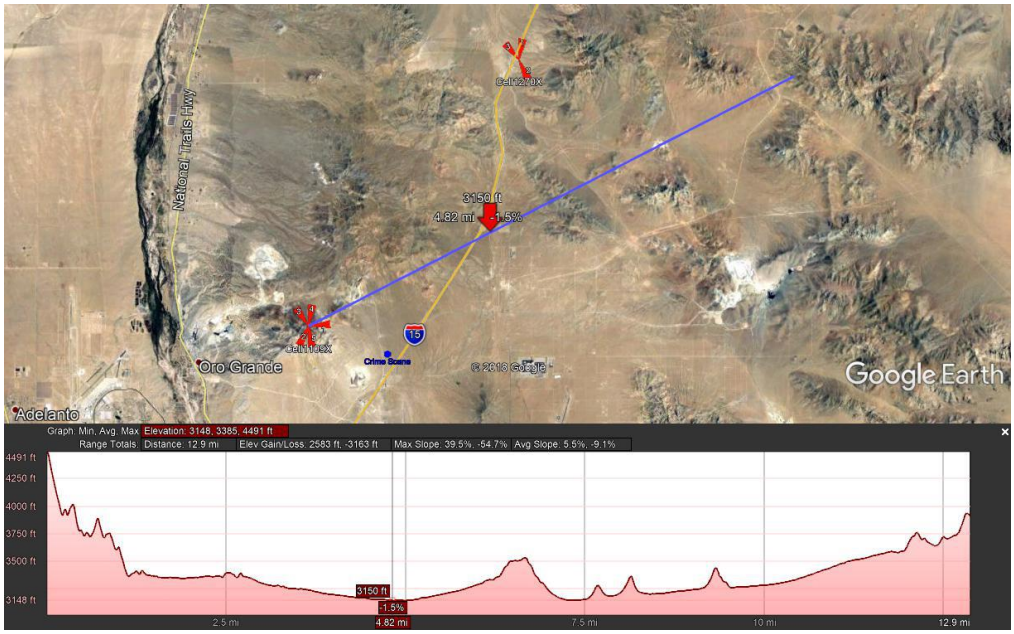

Figure 14: Elevation profile for a path in High Desert area to the Northeast of cell site "Quartzite" (Terrain profile is a standard feature in Google Earth software)

Good RF engineering practices in this scenario would require the cell antennas to be down-tilted by about 6°. This would ensure that even the locations nearby are illuminated by the main antenna lobe and would remove all the unpredictability and variability due to the sidelobes. These good engineering practices are not always followed by the RF Engineering teams in the field, however. Some of reasons are that antennas with large electrical down-tilts were not available until roughly 10 years ago, while the effects of the alternative – the mechanical down-tilt of the antennas – are a bit complicated to calculate and often not properly understood

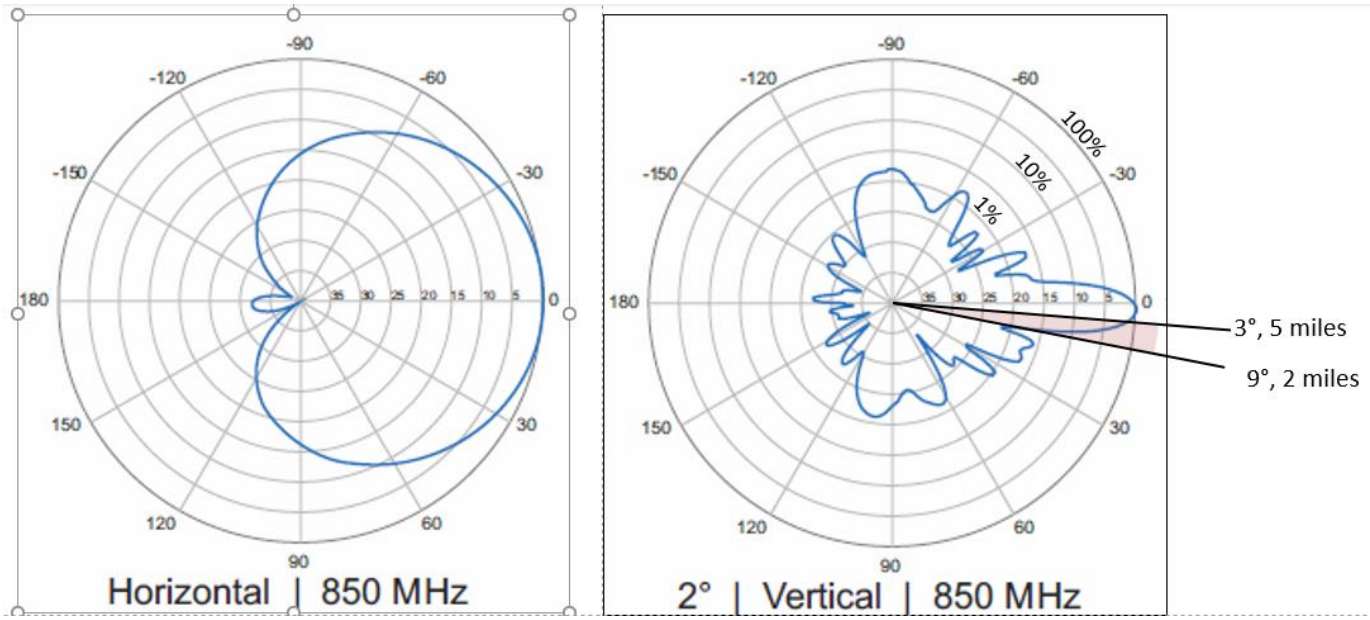

Figure 15: Radiation patterns in horizontal and vertical plane for the antenna CX063X19x00 by "Amphenol"

Since AT&T did not furnish the requested down-tilt information for the cells, we cannot confirm if the antennas on site "Quartzite" were properly down-tilted. If they were not, the chaotic hand-off patterns observed in calls from 11:30-11:34AM could have been caused by the unpredictable variations in the vertical side lobe radiation patterns, but we cannot know for sure one way or another.

Last but certainly not the least cause for chaotic hand-offs could have been the Directed Retry mechanism, probably invoked in 3, if not in 4 of the 5 calls attempted in this interval. With enough blocking in cells on "Quartzite", almost any handoff pattern could have been observed in the general area to the Northeast of the site, depending on which cell was blocking at which particular instance. We note, however, that even with Directed Retry there is no basis to believe that these calls could have been made from any areas to the South of "Quartzite", including the crime scene:

- Measurement in Google Earth shows that the crime scene is at azimuth of 109° relative to the site "Quartzite". Even if the cell 11095 pointing East (85°) was blocking, calls from that direction would have been served by the cell 11092 at azimuth of 170°, not by the cell 11091 at 10° azimuth[31].
- The call at 11:32AM, the only one that did not experience any hand-offs during the call, and the only one not likely to have experienced a Directed Retry, was carried on the cell 11091 only, shooting almost straight North (azimuth 10°), suggesting most clearly that the phone was in that direction.

Careful comparison of the plot for the overlap and the possible hand-off area prepared by the Prosecution from Figure 11, with our estimate for the same from Figure 12 reveals that their "pie shaped" pattern in the former was about 3 miles, while our "pie" was 6 miles long. The explanation given at the Preliminary Hearing for the Prosecution's estimate is based on the inter-cell distance – Prosecution's expert testified that the hand-offs usually occur "*at the 50% distance mark*" towards the adjacent cell, but that in their estimation they "*typically go out to 70% to be on the safe side*"[32].

The fundamental problem with this methodology is that it does not account for the terrain elevations. "Quartzite" site is on a tower mast 117 feet tall and is located on a mountain peak with an elevation of 4,500 feet above sea level. Within less than a mile towards I-15, the elevation quickly falls to 3,000-3,100 feet levels, and – with the exceptions of a few small hills – then slowly slopes upwards toward the Stoddard Ridge area (Figure 14). Similar elevation profiles appear further to the Northeast and North, and even to the Southeast and South, with "Quartzite" site being by far the highest point in the whole area[33].

What this means effectively is that in this whole area, the site "Quartzite" behaves like a 1,500 tall cell site (4500+117-3100). This height is so extreme that the standard *Hata* model cannot be used in such a case

[31] Calculations based on the parabolic approximation of the radiation patterns (see footnote[24]) show that cell 11092 would be received at ≈50 times stronger level than cell 11091 in the direction of the crime scene. For a call from there to be served by cell 11091, both cells 11092 and 11095 would have to block. Even with the blocking rate of 10% (which is higher than 8% rate calculated in Section 5, and that number includes blocked, failed and abandoned calls), probability of joint blocking is 1%, and for 3 calls to be blocked it is 0.0001%, or literally 1 in a million.

[32] "FVI1404194 PLH Transcript 6-15-15. pdf", pp.96-97.

[33] Closer inspection of that mountain top revealed at least 2 radio and 1 tower for TV broadcast, as well as 3 more towers some of which could belong to the AT&T's cellular competitors. Such high locations are sought by broadcasters and cell operators because they offer the so-called line-of site propagation conditions, ensuring a good signal reception over a very large surrounding area.

(it is applicable only to cells with the antenna heights under 200m, or about 650 feet – vast majority of the operational cellular towers are well below these heights).

While the theoretical analysis of such tall sites is possible[34], it is far from straightforward. Cellular experience, however, shows that very tall GSM sites in desert areas can carry the calls well over 22 miles away. A system related limitation restricting the range to 22 miles was actually discovered in the desert areas in the Australian Outback when the GSM system with unusually tall cell towers (1000-1300 feet[35]) was first deployed there in the early 1990s[36], in conditions that seem similar to the situation here. Our initial estimate thus was that cell site "Quartzite" could cover:

- At least 10 miles, possibly up to 20 towards North and East (except where obstructed by Turtle Mnt., Black Mnt., Blake Jade Hill, but easily still up to 8 miles).
- Coverage to the East could easily extend beyond these ranges, especially on higher grounds – site can overshoot these obstacles farther away, maybe all the way to some portions of the Rte. 247[37].
- Coverage to the South and Southeast would most likely be limited by other cells in Victor and Apple Valley and towards Adelanto (without these cells, similar ranges as to the North and East would be expected).
- Coverage to the Northeast and along I-15 would be likely limited by the site "I15 and Wild Wash", located very near I-15.

The Northeast direction is of special interest because of the cells that carried the calls between 11:30-11:34AM and because of the I-15, the only major thoroughfare in this area. The cell "I15 and Wild Wash" is about 8 miles away in a straight line, but our estimate of the range of "Quartzite" site in that direction would not be anywhere close to 3 miles as the Prosecution's plot from Figure 12 suggests (and not even 4 miles, which would be a 50% distance mid-point). Reasons for this are:

- Site "I15 and Wild Wash" is rather short (71 feet).
- Its ground elevation is approx. 3,000 feet.
- Sector antennas on "I15 and Wild Wash" are pointed away from the Southwest direction (sectors are at 10°, 155° and 320° degrees, shooting roughly to the N, SSE and NW).
- "I15 and Wild Wash" is in a valley, with terrain gradually sloping up in the S and SW direction.

---

[34] In particular see Y. Okumura et al., "Field Strength and its Variability in UHF and VHF Land-Mobile Radio Service", Rev.Elec.Comun.Lab, vol.16, 1968. Authors gave the curves for estimation of the signal strengths for antennas up to 3,000 feet above the average ground level, based on the extensive field measurements. However, the curves are not easy to use, and the results are a bit questionable because of the limited number of measurements available for such extreme cases. Hata devised his model by fitting numerical expressions that approximate the curves obtained experimentally by Okumura, but only for antenna heights under approximately 650 feet (200m).

[35] Author's memory suggests that sites were between 300 and 400m tall (1000-1,300 feet), but the internet search done for this report did not yield any information to confirm these heights.

[36] Limitation was due to the maximum value of the "Time Advance" parameter in the original GSM standard. Based on these results from Australia, GSM standard was amended and an "Extended Range" feature was introduced, which allows for GSM cells to cover up to 33 miles away.

[37] Note that the site "Mazi Trust", and to a lesser extent the site "Holy Apostolic", both to the Southeast of the "Quartzite" could have limited its coverage towards East (see Figure 12Due diligence, however, suggests that neither of these sites were ever deployed, although they are listed in the Cell Site Table, see V. Jovanovic, "AT&T Cell Site Table Problems", pp.11-15.

– There is a ridge around the cell about 2 miles to the S and SW, at elevation of about 3,250 feet (antenna is at less than 3,100 feet), see Figure 16 for details.

Based on these factors, we estimated that the covered range of the site “Quartzite” in the Northeast direction would be about 6 miles, leaving the remaining 2 miles for site “I-15 and Wild Wash” to cover.

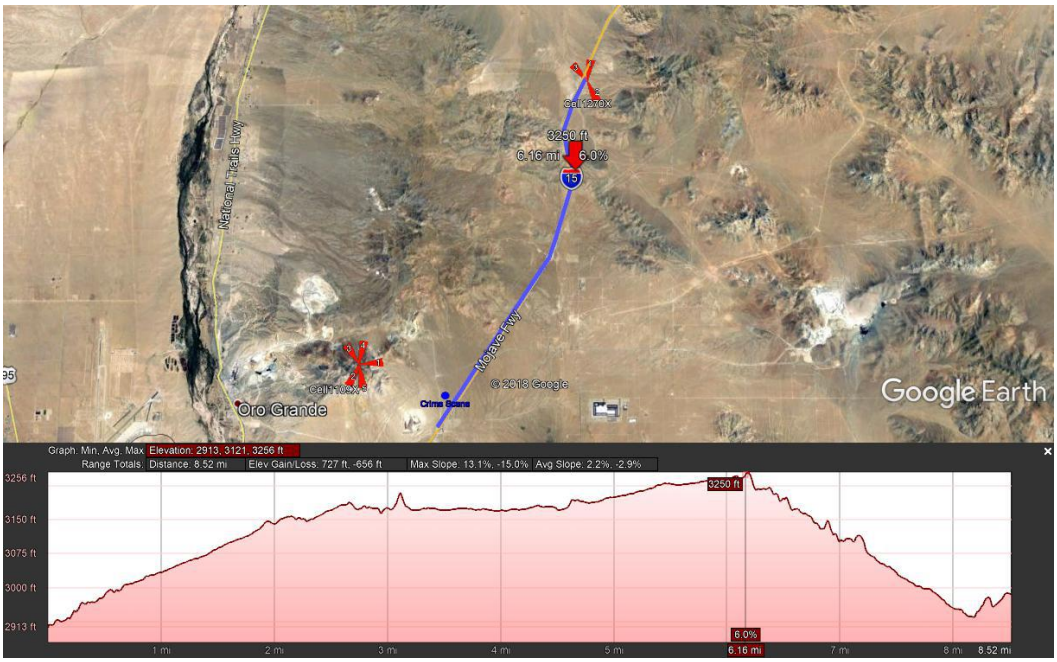

Figure 16: Elevation profile along I-15 from “Quartzite” to “I15 and Wild Wash”

To check these conclusions, in Figure 17 the drive test data points where “Quartzite” was the server are presented.

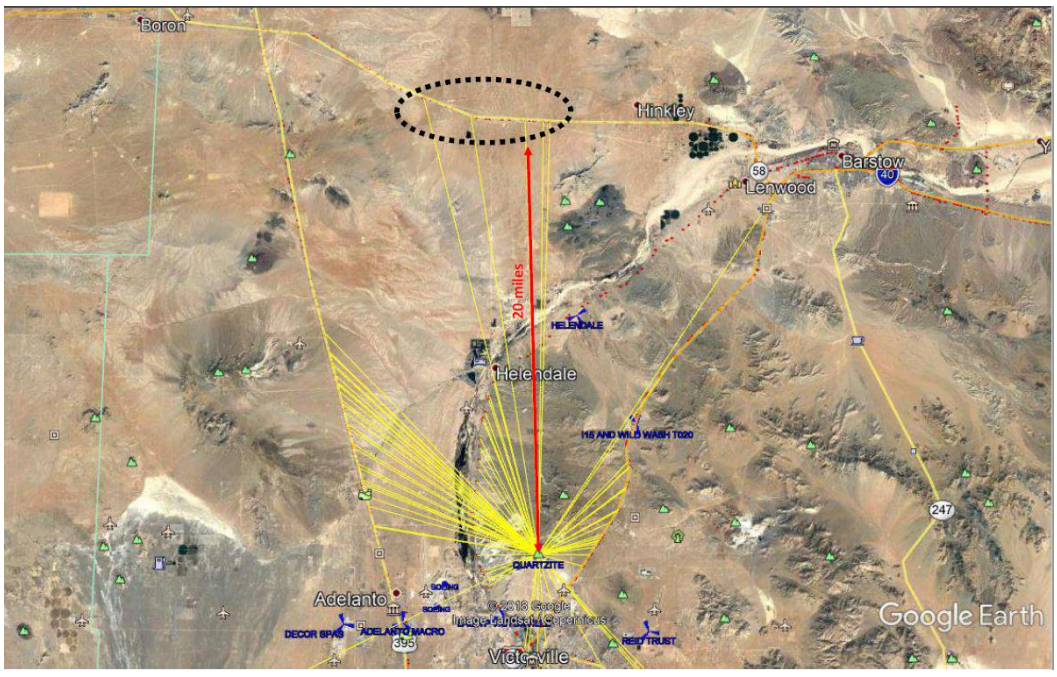

Figure 17: Drive test data point with “Quartzite site as a server

From the plot we see that the "Quartzite" site can really cover about 20 miles (on Route 58 to the North, where it is unconstrained by any other sites, and even in one point in West Barstow). Similar results could be expected towards the East, except in the areas where it would have been shadowed by the local hills as described earlier, but no drive test routes covered this area).

A magnified detail of Figure 17 of the area between the "Quartzite" and the "I15 Wild Wash" is further shown in Figure 18. We see that that the hand-off boundary on UMTS appears to be very close to our prediction, standard disclaimer about the conclusions based on UMTS drive test withstanding.

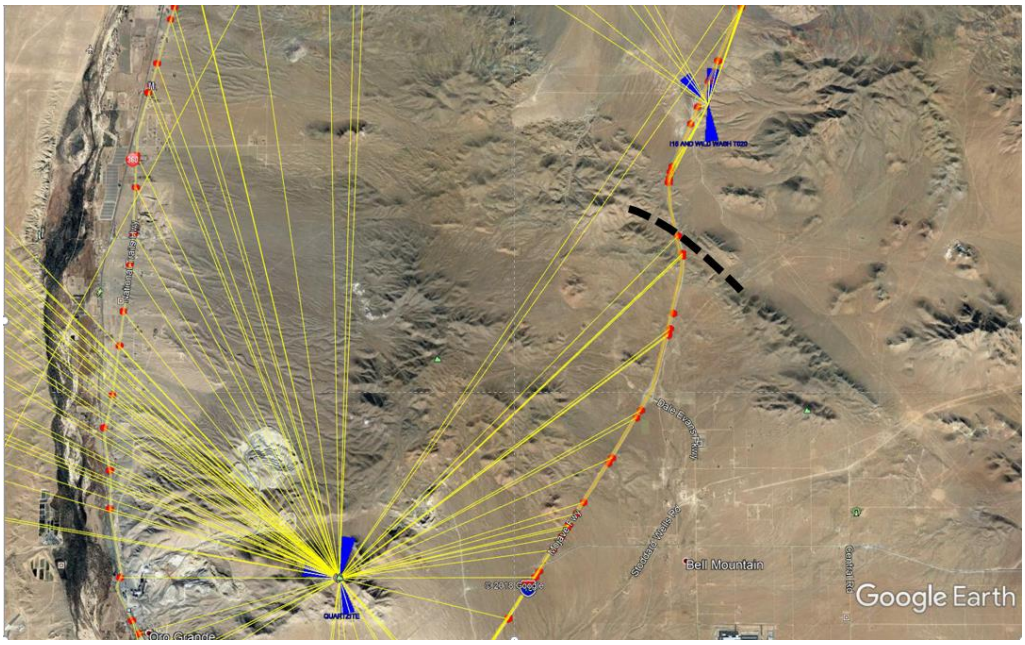

Figure 18: Hand-off area between "Quartzite" and "I15 and Wild Wash"

In summary, we can state the following about the location of calls from 11:30 to 11:34AM on 02/06/2010:

- There is no evidence whatsoever that these 5 calls could have been made from the "crime scene".
- Due to the Directed Retry being likely invoked in majority of the calls, they could have been made anywhere up to about 20 miles distance to the North and East, or up to about 6 miles to the Northeast along I-15.
- At least some of the unusual handoff patterns reported during these calls could have been due to the inadequate down-tilts, but AT&T did not provide any antenna down-tilt data that could prove or disprove this hypothesis.

8.3 Call at 11:52AM on 02/06/2010

Per the call record from Figure 9 the call at 11:52 started at cell 05262/11095 and ended on cell 05262/03483. The starting cell is on the "Quartzite" site pointing at 85° that was already discussed, while the ending cell is on the site "15 Fwy and Palmdale Rd", which points at the azimuth 330°. Inspection of the Cell Site Table for this site did not expose anything unusual or controversial, and mapping tools suggest that the location (to the West of I-15, near the intersection with Palmdale Rd.) and the reported height of 55 feet are both reasonable.

From Figure 19, which depicts the area where these two cells are located, it is tempting to conclude that

the record corresponds to the phone moving southbound along I-15, but the problem is that the call lasted for 35 sec (Seizure Time = 26 sec and Elapsed Time = 9 sec). Assuming the speed of 60 mph, a mobile phone can traverse a path only 0.6 miles long, as also depicted in Figure 19 by a blue line segment.

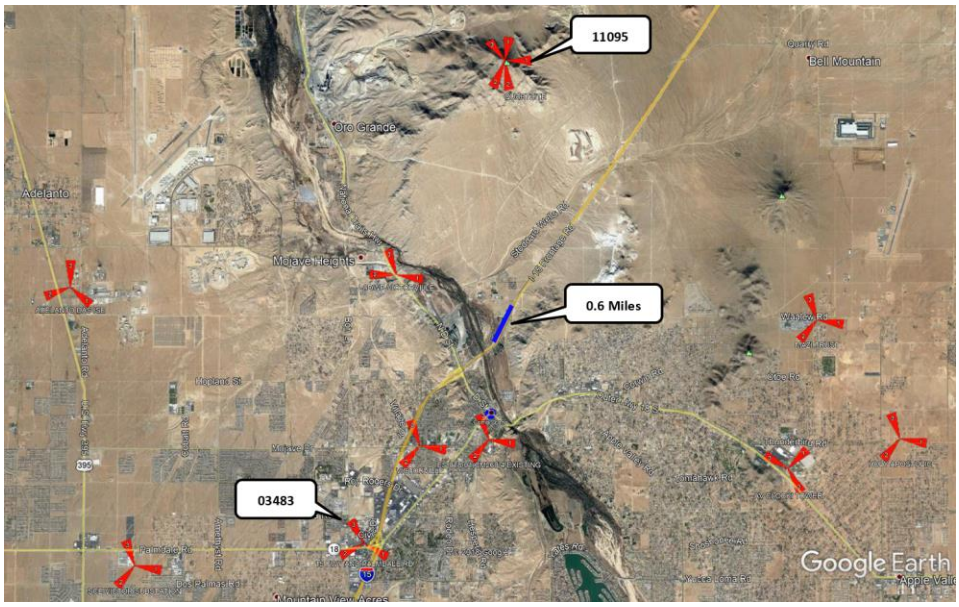

Figure 19: Area of interest for the 11:52AM call that lasted for 35 sec
Blue line segment indicates maximum distance phone could have travelled during the call

It should be fairly obvious that it is impossible to find a section of this length on I-15, or any other road in this area, where the phone could have been to start the call on cell 11095 and end it on cell 03483 based on the proximity criteria only.

When we consider the topography, it would not be surprising if the "Quartzite" site can reach the areas in the Victor Valley with considerable signal strengths, due to its extreme height – whole area in and around Victorville is at the elevation of about 3,000 feet. But the site "15 Fwy and Palmdale Rd", being at that elevation and with antenna heights of 55 feet only, cannot be expected to propagate much to the North, in part because it propagates through an urban area (although from the *Hata* perspective, most of the Victorville city area would be classified as a suburban RF clutter). In particular, site "15 Fwy and Palmdale Rd" is not very likely to overshoot the site "Victorville" (the one that carried the 10:46AM call), which is at height of about 2920 feet with antennas 80 feet tall. Even a careful search in Google Map's Street view along the I-15 from the vicinity of the "Quartzite" site all the way to the Palmdale Rd did not reveal any peculiar features that could have given such hand-off pattern (like tall overpasses that would rise above the antenna levels of the sites in the valley, or ravines/underpasses in which the nearby short sites would be blocked but a tall site far away still could be seen).

The drive test data for these two sites, presented in Figure 20, proved to be of limited help. It did show two areas, one in Victorville and the other in the Apple Valley, where the "15 Fwy and Palmdale Rd" and the "Quartzite" are of a comparable strength, but neither of these areas is likely to be served by a combination of a cell pointed at 85° on the "Quartzite" site and a cell pointed at 340° from the "15 Fwy and Palmdale Rd" site (likely servers would be the cell at 170° on the former, and the cell at 243° on the latter).

Since the 11:42AM call likely endured the Directed Retry (Seizure Time was 26 sec), the most likely

scenario for the observed pattern is that the phone was reasonably close to the "15 Fwy and Palmdale Rd" site in the West Victorville, but was redirected to a cell on the "Quartzite" site which was a second or third strongest server there (a situation that would not be revealed by drive tests, which show best server information), and then went back to the "15 Fwy and Palmdale Rd" when it stopped blocking. Another possibility is that some cells in Victorville area experienced outage in this period and "Quartzite" had to take over instead, but that hypothesis cannot be proved or disproved without the maintenance logs from AT&T for this period.

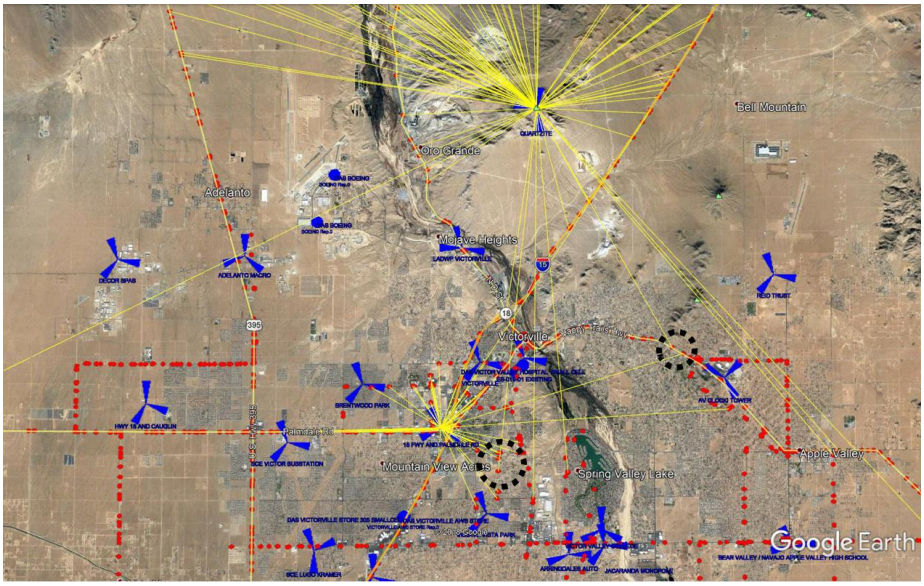

Figure 20: Drive test data for cells "Quartzite" and "15 Fwy and Palmdale Rd"

In summary, the call record for 11:52 AM is quite mind boggling. Our best estimate is that it was made from the West Victorville area, but other options cannot be excluded. Based solely on the call record data, technically the safest thing would be to characterize it as unlocatable.

8.4 Call at 11:53AM on 02/06/2010

The 11:53AM call was initiated within a minute of the 11:52AM call and started on the same cell on "15 Fwy and Palmdale Rd" site where the previous call ended (05262/03483), which is not unusual. The 11:53AM call ended on the cell 05262/15403 that points at 350°, which is, however, unusual. From Figure 21 we see that it is more than 10 miles away, and since the 11:53AM call lasted for 36 sec (Seizure Time=26 sec once again, Elapsed Time=10 sec) the mobile phone could have traversed only 0.6 miles, just like in the previous call.

Compared to the 11:52AM call this one is a bit less mind-boggling given that the cell 05262/15403 shoots almost straight to the North. Furthermore, the cell is on site "Apple Valley Overlay" which is at an elevation of approximately 3,600 feet and has a tower mast 183 feet tall, giving it an effective height of 600-700 feet in the Apple and Victor Valleys to the North. Collocated on the same mast are antennas for the radio station "KZXY FM Apple Valley", suggesting a location domineering over the areas to the North, although not to the same extent as "Quartzite" domineers to the South.

Like in the previous case, cell 05262/03483 is expected to cover a much smaller range, due to height and elevation profiles, and the fact that it is embedded in the area within the suburban RF clutter.

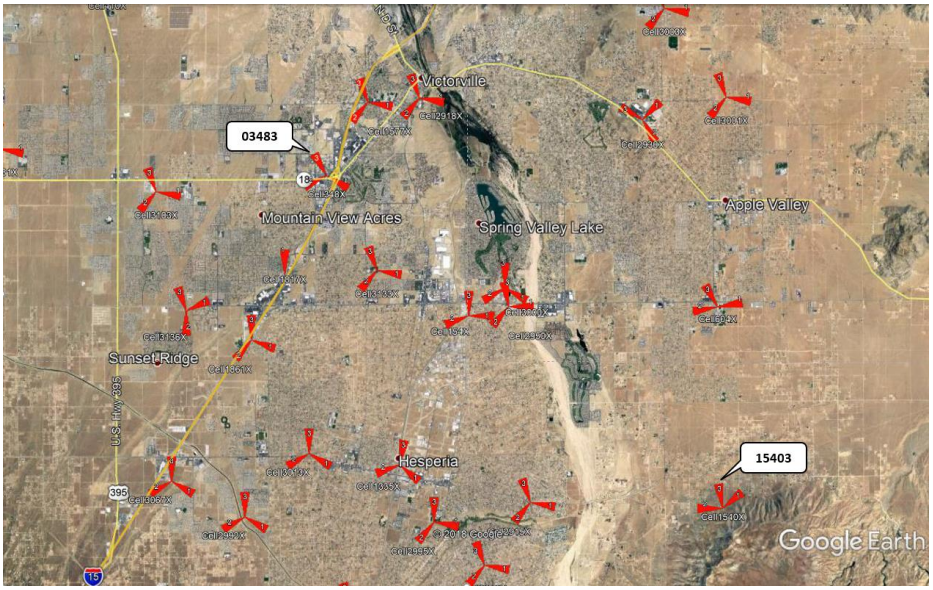

Figure 21: Area of interest for the 11:53AM call that lasted for 35 sec

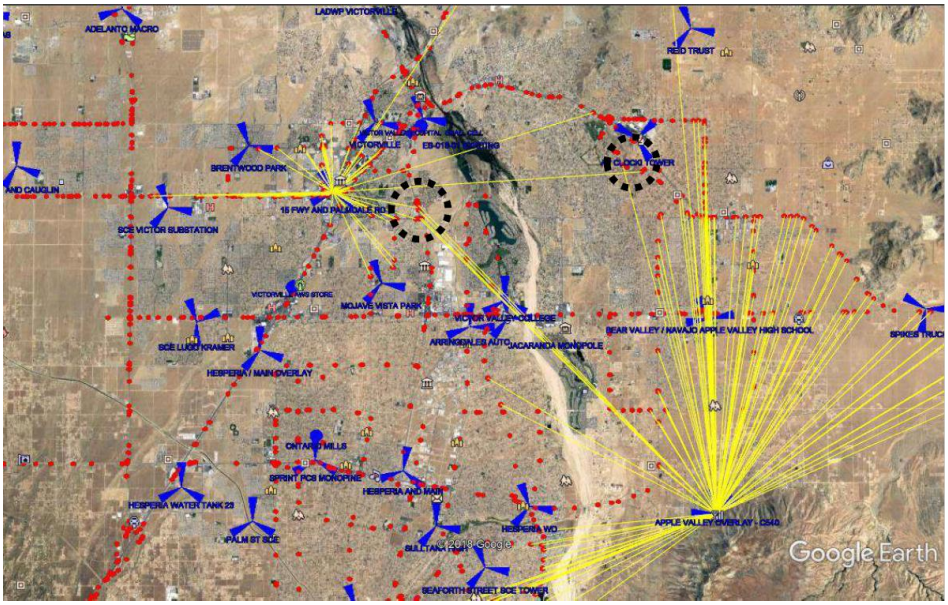

Figure 22: Drive test data for cells ""Apple Valley Overlay" and "15 Fwy and Palmdale Rd"

Based on the drive test data we were again able to identify two areas where these two sites come at comparable strength, indicating the potential locations for a hand-off (Figure 22). The area in Victorville is actually quite close to the one where cells from "Quartzite" and "15 Fwy and Palmdale Rd" sites were found to be in a similar hand-off situation. It is tempting to conclude that both calls were made from that area, except for the fact that cell 03483, shooting to the NW, is not the natural sever in this area[38].

[38] At this point one cannot but start wondering if the cell 03483 was indeed pointing to the NW and not more towards East. This could have easily been another Cell Site Table data entry error that no due diligence in the mapping tools would detect. But the same effect can also be caused by cross-connecting the antenna cables at the cell site. This is an unusual but not extremely rare error in practice – author's former company *Newfield Wireless* has been approached by several operators for a feature that would identify such a problem with the *TrueCall*™ tool.

Very similar to the previous call, taken on its own the call at 11:53AM is best characterized as unlocatable. Taken together with the 11:52AM call however, and considering that the phone could not have travelled for more than 2 miles in this whole period, as well as the likely coverage patterns of the 3 cells involved based on the elevations and RF clutter, South Victorville and the areas further to the East towards Apple Valley seem the most likely. The area in South Victorville between the I-15 and Spring Valley Lake, where all 3 cells come strong based on the drive test data, is one specific candidate, but others in that general area cannot be excluded – there might be other such areas that drive tests did not cover, and outages on some of the cells in Victorville could have caused similar patterns, etc.

8.5 Call at 12:49PM on 02/06/2010

The call record shows that it started on the cell 05262/29186 pointing to 220° at the site "ES-018-01(CM260)4 Existing" and ended on the cell 05262/03481 pointing at 120° at the site "15 Fwy and Palmdale Rd", the same site that was involved in the previous two cases (but on a different sector).

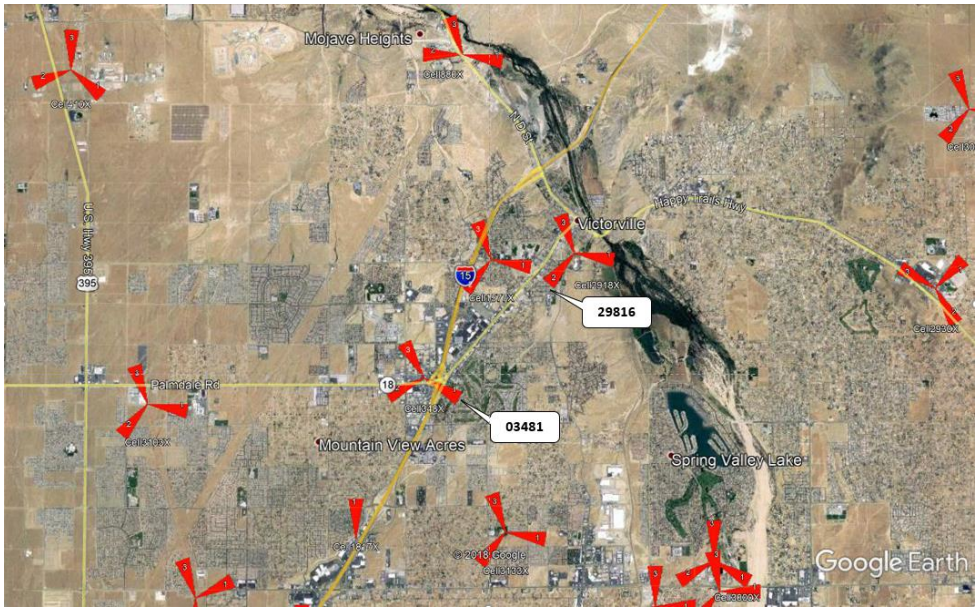

Figure 23: Area for the 12:49PM call

The call records further reveal that no Directed Retry was likely (Seizure Time = 9 sec). Given the elevations and heights of the cells in the area, it is practically certain that the call has been made from South Victorville, possibly even from the same area as calls at 11:52AM and 11:53AM (which does not mean that the mobile was in that area throughout the whole period – it could have moved out and came back within almost an hour with no recorded calls, between 11:53AM and 12:49PM).

8.6 Call at 1:30PM on 02/06/2010

Call records show that this call started on the cell 05262/11092, again on the site "Quartzite" but on the sector pointing at 170° almost straight South. It ended on the cell 05262/18613 pointing at 360°, straight to the North. Cell Site Table shows that the end cell is on the site "Hesperia/Main Overlay", for which due diligence did not reveal any suspicious or erroneous entries. Its antenna height is 77 feet and the ground elevation is around 3,200 feet (terrain at this point start sloping upwards in the southbound direction, towards the Cajon Pass at about 4,000 feet). Its coverage is likely to be relatively small on that side

because of the antennas shooting into the hill, while on the North side it is expected to be constrained by the site "15 Fwy and Palmdale Rd" as discussed already.

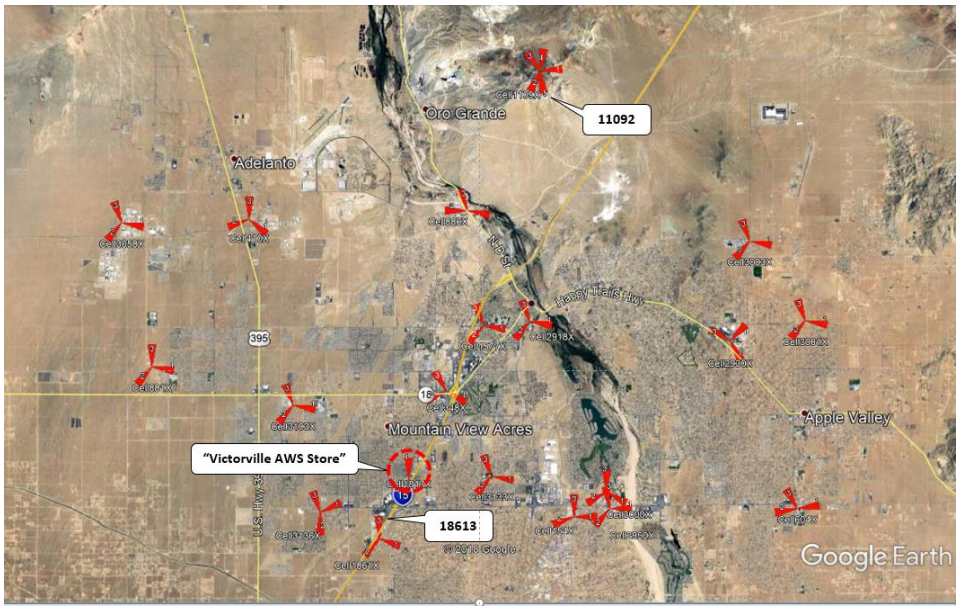

Figure 24: Area for the 1:30PM call

This call is puzzling because the start and end cell are more than 10 miles apart again, with a slew of cells in between them, especially along I-15. The total call length is 53 sec, during which the phone could not have traveled more than 1 mile, making the situation similar to that for the calls at 11:52 and 11:53AM.

The big difference here, however, is that reported Seizure Time = 9sec does not indicate a likely Directed Retry. This would suggest that the cell 05262/11092 on "Quartzite" was the best server somewhere reasonably close to the "Hesperia/Main Overlay". This is not impossible based on the antenna heights and RF clutter, but the drive test data shows no such areas along I-15 in the Mountain View Acres/Hesperia region (although it confirms a fairly short range of for the site "Hesperia/Main Overlay" towards North). Based on the information for this call only, it should probably be considered as unlocatable too. In view of the fact that the subsequent calls (starting at 2:22PM, from the next Section) were most certainly made from the Rancho Cucamonga to the South, about 40 min drive along the I-15 (according to Google Maps Directions feature), the most likely location for this call was on I-15 itself, probably in the Mountain View Acres area around the intersections of I-15 with Luna or La Mesa Road[39].

8.7 Calls from 2:22 to 3:14PM on 02/06/2010

Three calls were made in this period and are the last calls made on 02/06/2010 (after the 3:14PM call, the next one was recorded the 10:35AM the following day). The first two, at 2:22PM and 2:40 PM, are the non-completed calls that started on the cell 05267/16636 pointing at 220° and ended on the cell

[39] Site "Victorville AWS Store" in this area per the Cell Site Table would be expected to cover this stretch of the road (see the map in Figure 24). Due diligence, however, suggests that it is an indoor micro-cell inside of the AT&T's store, which would have no or extremely small coverage outside. Drive test data corroborates no outdoors coverage on UMTS. Further details about likely errors in the entries for this site are available in the companion report (V. Jovanovic, "AT&T Cell Site Problems", 09/14/2018, pp. 15-16).

05267/16632 pointing at 0° per the call record. Third call, at 3:14PM, was a completed call that started on the cell 05267/16635 shooting at 100° and ended on the cell 05267/16631 shooting at 0°. All 4 cells involved in these 3 calls happen to be on the cell site named "S Rancho Cucamo Ovly-C663", located near the Defendant's residence at Church St. This area is depicted in Figure 25, and shows very dense cells, with a typical inter-cell distance of about 1 mile only.

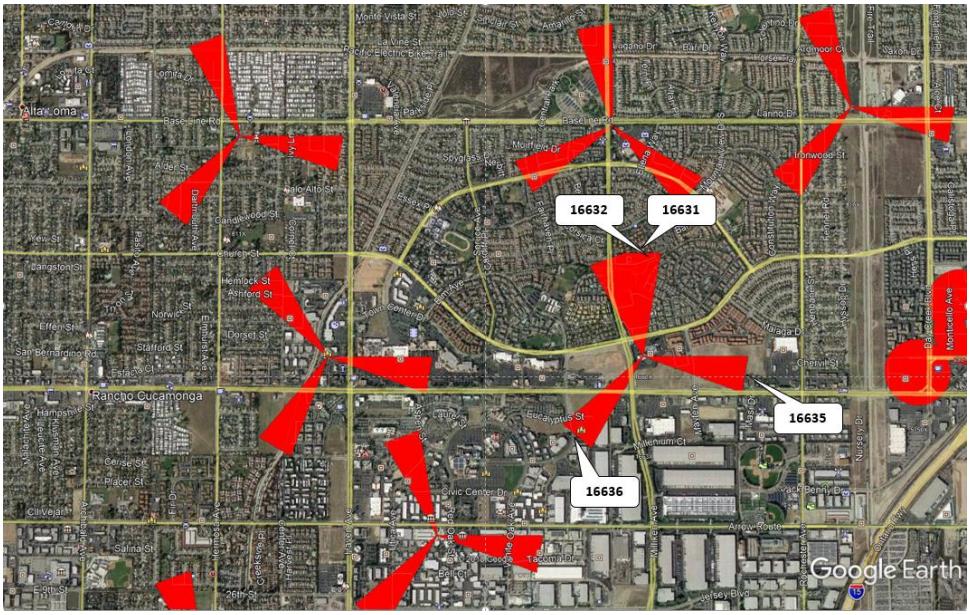

Figure 25: Area for 2:22-3:14PM calls

Given the density of the network and the urban RF clutter, we can be sure that all 3 calls were made from Rancho Cucamonga, most likely from within 1 mile or so from the intersection of the E. Foothill Blvd. and Milliken Ave. What is somewhat unusual is that in each case the call started on a cell shooting at least somewhat towards South (220° and 100°), and ended on cells shooting straight North (0°), as if the phone was constantly circling around the site "S Rancho Cucamo Ovly-C663".

	4	5	7	8	9	13	14	15	16	17	18	19	20
1	frequency	technology	sitename	address	city	latitude	longitude	lac	cid	height	sector id	beam-width	sector orientation
4819	1900	25G	S RANCHO CUCAMO OVLY - C663	7777 MILLIKEN AVENUE	RANCHO CUCAMONGA	34.108389	-117.55625	5267	16631	64	A	90	0
4820	1900	25G	S RANCHO CUCAMO OVLY - C663	7777 MILLIKEN AVENUE	RANCHO CUCAMONGA	34.108389	-117.55625	5267	16632	64	B	90	0
4821	1900	25G	S RANCHO CUCAMO OVLY - C663	7777 MILLIKEN AVENUE	RANCHO CUCAMONGA	34.108389	-117.55625	5267	16633	64	C	90	0
4822	850	25G	S RANCHO CUCAMO OVLY - C663	7777 MILLIKEN AVENUE	RANCHO CUCAMONGA	34.10839	-117.55625	5267	16635	64	A	68	100
4823	850	25G	S RANCHO CUCAMO OVLY - C663	7777 MILLIKEN AVENUE	RANCHO CUCAMONGA	34.10839	-117.55625	5267	16636	64	B	68	220
4824	850	25G	S RANCHO CUCAMO OVLY - C663	7777 MILLIKEN AVENUE	RANCHO CUCAMONGA	34.10839	-117.55625	5267	16637	64	C	68	340

Figure 26: Cell Site Table Entries for the site "S Rancho Cucamo Ovly-C663"

Inspection of the Cell Site Table for this site revealed that this must be another data entry error, since cells on all 3 sectors in the 1900 band are listed as pointing to 0° azimuth, which is impossible by definition. If the cells in the band 1900, however, followed the usual cellular practice and were aligned with the corresponding sectors in the 850 band, all of these would have been rather normal and quite frequent inter-band, intra-sector hand-offs (i.e. hand-offs from a cell in the 850 band to another cell on the same sector B in the 1900 band during the first two calls, and on the same sector C during the third one). No circular movement around this cell site would be necessary to explain the reported hand-offs, in that case.

8.8 Summary of Analysis for Calls on 02/06/2010

The call records from this period included some of the most perplexing examples that this author has ever encountered. Besides the recurring problems with the AT&T's Cell Site Table accuracy, these calls were especially difficult to interpret because:

a) The area has extremely large geographic elevation variations.
b) Many calls endured very probable Direct Retries.
c) Following of the good RF engineering practices regarding down-tilts could not be verified.
d) Possible cell outages could not be verified.
e) Drive test data was of limited use because of the temporal and technological differences.

Problems c) to e) were largely due to AT&T's inability to comply with the Defense's subpoena request.

Out best geolocation estimates for the calls in this period are as follows:

- **10:46AM call**
  - West Victorville, possibly on the Hwy I-15.
  - Southbound direction of travel doubtful because of the likely Directed Retry.
- **11:30-11:34AM calls**
  - No evidence that any of these calls could have been made from the "crime scene".
  - Calls could have been made from up to 20 miles to the North (including Route 58), many areas up to 20 miles to the East (possibly up to Route 247) and to about 6 miles away in the Northeast direction.
  - Besides Directed Retries, rather unusual hand-off patterns could have been caused by the inadequate antenna down-tilts on the site "Quartzite".
- **11:52 and 11:53AM calls**
  - Individually, both calls should be classified as unlocatable.
  - As a pair of calls in quick succession, they were probably made from the Southwest Victorville; area between I-15 and Spring Value Lake is one specific possibility.
  - Other areas to the East of this location in the Victor and even Apple Value cannot be excluded.
- **12:49PM call**
  - Made from Southwest Victorville, near the possible location for 11:52 and 11:53AM calls.
- **1:30PM call**
  - Unlocatable call per se.
  - Given the location of subsequent 2:22PM call, most likely location is on I-15 driving southbound, around intersections with Luna Rd. or La Mesa Rd. in the Mountain View Acres area.
- **2:22-3:14PM calls**
  - Undoubtedly made in Rancho Cucamonga, most likely within 1 mile from the E. Foothill Blvd. and the Milliken Ave intersection.

At this point, we would also like to show how some of the Prosecution's exhibits, although not necessarily incorrect technically, could be misleading because of what they omit. In Figure 27 we are reproducing the Prosecution's depiction of the calls from 10:46AM to 1:30PM on 02/06/2010. Based on the full data for these calls from Call Records file, it is obvious that this exhibit shows only the cell sites that the corresponding calls were started on. Based on this plot, most people would probably tend to conclude that the phone was in Victorville at 10:46AM, near the crime scene from 11:30AM to 11:52AM, and back in

Victorville for calls at 11:53AM and 12:49PM, and then back near the crime scene at 1:30PM.

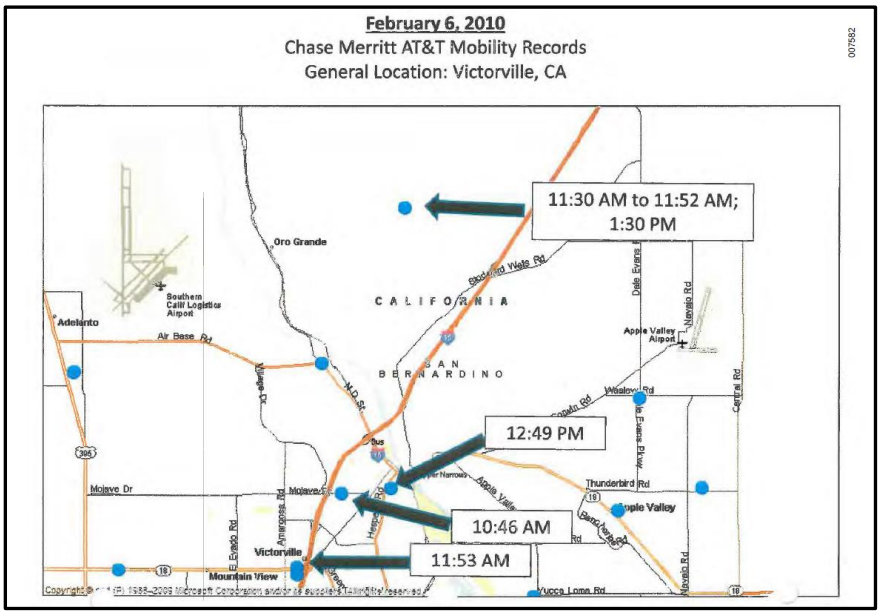

Figure 27: Prosecution's depiction of the call events from 10:46AM to 1:30PM on 02/06/2010[40]

When both start and end cells are taken into account, calls at 10:46AM and 11:30AM-11:34AM would still be in the general vicinity of the cells indicated in Figure 27, but calls at 11:52AM and 1:30PM would be nowhere near the site that arrow points to (which happens to be "Quartzite), and by the extension nowhere near the crime scene. Note that for this presentation to make sense, phone would have had to travel for more than 7 miles southbound between 11:52AM and 11:53AM, probably along I-15, which is just impossible – phone would have to move at about 200 mph in between these two calls for this to happen.

9 Calls from 1:31PM to1:41PM on 02/08/2010

Another example of the potentially misleading and partially incorrect/incomplete geolocation work by Prosecution is depicted in Figure 28[41], which shows two calls, at 1:31PM and 1:41PM on 02/08/2010. Inspection of the Call Records file per Figure 29, however, suggests that there were 4 calls made within this interval. Our annotated map for this area is given in Figure 30.

Comparing Figure 29 and Figure 30 we see that, except for the two missing calls and apparently showing the starting cells only, Prosecution's map seems to have marked the "1:41PM" call at the point which does not correspond to either the start or the end cell for this call (location shown is on, or very near the I-15, in between 1st and the 2nd St.; the real call start and call end locations are both farther North)[42].

[40] File "7298-7786 (SBSD Inv Rept Narratives) 2 of 4 (2).pdf"; pagination in the top right corner reads 007582.

[41] "7298-7786 (SBSD Inv Rept Narratives) 3 of 4 (2).pdf", p.3; pagination in top right corner shows 00758.

[42] Note that the start cell for the 1:41PM call does not exist in the Cell Site Table that AT&T provided to the Defense – its location was marked manually in Google Earth, using the coordinates from the Call Records file. This information is missing due to an oversight by Defense: when the Cell Site Table information was subpoenaed, ZIP code 92860 for Norco, CA was omitted in the list of ZIPs from which the cell site information was requested.

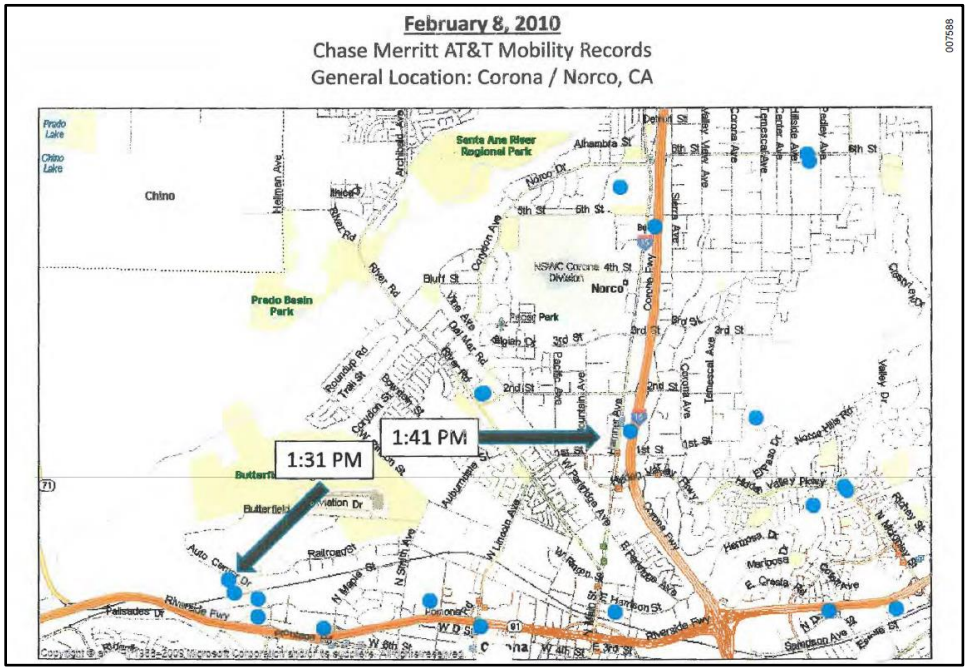

Figure 28: Prosecution's depiction of the call events from 10:46AM to 1:30PM on 02/06/2010

	A	B	C	D	E	F	G	H	I	J	K	L
1	Item	ConnDateTime		Seizure Time	Originating Number	Terminating Number	Elapsed Time	Number Dialed	IMEI	IMSI	Description	CellLocation
9139	9138	02/08/10	12:34PM	0:00	19092261197	19092132103	0:19	19093740102		310410208101679	M2m_VMB	[]
9140	9139	02/08/10	01:31PM	0:01	19093740102	19092132104	0:48	1119092132104	1189700137274	310410208101679	M2m_VMC	[05264/14596:-117.61889:33.88694:245 05264/14591:-117.61889:33.88694:0]
9141	9140	02/08/10	01:33PM	0:22	19093740102	19092261197	0:04	2261197	1189700137274	310410208101679	M2M_DIR	[05264/14591:-117.61889:33.88694:0]
9142	9141	02/08/10	01:33PM	0:04	19092261197	19093740102	0:38	19093740102	1189700137274	310410208101679	M2M_DIR	[05264/14591:-117.61889:33.88694:0 05264/15811:-117.58222:33.88139:95]
9143	9142	02/08/10	01:41PM	0:28	19093740102	19092261197	0:02	19092261197	1189700137274	310410208101679	M2M_DIR	[05264/10137:-117.56194:33.93458:340 05264/16922:-117.54797:33.97706:220]
9144	9143	02/08/10	01:42PM	0:00	19092261197	19093740102	0:00	19093740102		310410208101679	M2M	[]

Figure 29: Excerpt from Call Records file showing calls from 1:31PM to 1:41PM om 02/08/2010

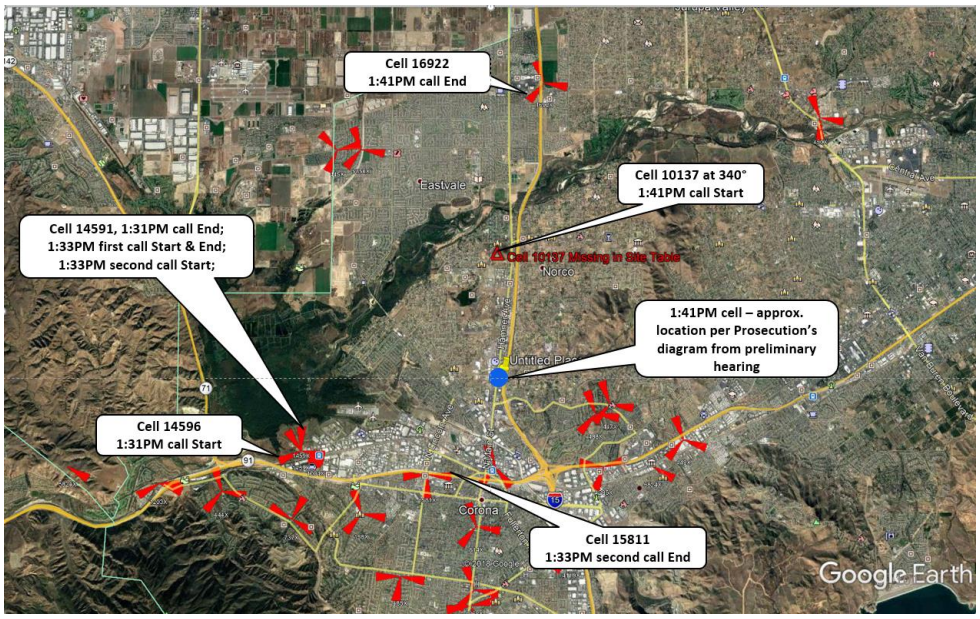

Figure 30: Area for calls from 1:31PM to 1:41PM on 02/08/2010

Now what is puzzling in our complete depiction of all 4 calls, with both start and end cell information included, is that the phone started a call at 1:31PM on the cell 05264/14596 pointing to of 245° on the site "91 Fwy/Corona Expw". This places the phone location somewhere near the Hwy 91 and Hwy 71 intersection. The phone then jumps to the North in order to end for that call to end on the cell 05264/14591 on the same site that shoots straight North at 0°. This places the phone in a largely unpopulated area with virtually no roads, where it spends next about 2 minutes, starting and finishing the first 1:33PM call on the same cell. It then starts another call at 1:33PM from there, but within the 42 sec duration of the 1:33PM call jumps about 2 miles to the East, to end the call on the cell 05264/15811. This cell, based on its orientation (95°) and the proximity of the first adjacent cell farther to the East, and seems to be covering very little apart from a short stretch of Hwy 91 in Corona.

A jump of about 2 miles within the 42 sec duration of the second 1:33PM call is clearly impossible (would have required mobile to move at about 160 mph). The situation becomes clearer after inspecting the Cell Site Table for the site "91 Fwy/Corona Expw", however.

	4	5	7	8	9	13	14	15	16	17	18	19	20
1	frequency	technology	sitename	address	city	latitude	longitude	lac	cid	height	sector id	beamwidth	sector orientation
4560	1900	2G	91FWY/CORONA EXPW	2385 AUTO CENTER DRIVE	CORONA	33.88694	-117.61889	5264	14591	101	A	90	0
4561	1900	2G	91FWY/CORONA EXPW	2385 AUTO CENTER DRIVE	CORONA	33.88694	-117.61889	5264	14592	101	B	90	0
4562	1900	2G	91FWY/CORONA EXPW	2385 AUTO CENTER DRIVE	CORONA	33.88694	-117.61889	5264	14593	101	C	90	0
4563	850	2G	91FWY/CORONA EXPW	2385 AUTO CENTER DRIVE	CORONA	33.88694	-117.61889	5264	14595	101	A	70	100
4564	850	2G	91FWY/CORONA EXPW	2385 AUTO CENTER DRIVE	CORONA	33.88694	-117.61889	5264	14596	101	B	70	245
4565	850	2G	91FWY/CORONA EXPW	2385 AUTO CENTER DRIVE	CORONA	33.88694	-117.61889	5264	14597	101	C	70	325

Figure 31: Excerpt from Cell Site Table showing cells on site "91Fwy/Corona Expw"

We readily recognize another error in populating the 1900 band entries – all sectors shown as zero degrees – which then propagated into the call records. If AT&T followed the normal practice of orienting all cells in same sector the same way, azimuth for cell 14591 would have been 100°, shooting almost straight East. In that case the sequence of call records would indicate a smooth drive Eastbound on Hwy 91 from 1:31 to about 1:34PM and then a turn onto I-15 Northbound, where it was at 1:41PM.

10 Conclusions

As explained in more detail in our accompanying report, the AT&T Cell Site Table is plagued with omissions, errors and highly suspect entries. As such, it does not meet the essential requirements in terms of the completeness, accuracy and consistency of evidentiary material. This jeopardizes possible conclusions about the locations and the direction of travel, making most of them suspect. Indeed, missing, erroneous or highly dubious entries were found in the cells covering all areas where phone 909-374-0102 was making calls in the evening of February 4th, whole day on February 6th and in the early afternoon on February 8th, 2010, the three intervals that Defense Counsel asked the author to investigate.

Apart from assuming that all the Cell Site Table information as presented in the Call Records is accurate and not subjecting it to a proper checking and verification, the approach of the Prosecution's expert was flawed because:

- Calls were assumed to connect to the serving cells based on the proximity criterion.
- All cell range estimates were based exclusively on the inter-cell distances.

- Only start cell information is used in the analyses (end cell information mostly or completely ignored).
- Numerical errors were made in calculations of sectors overlap, location of some cells, etc.

Analysis by the Prosecution's expert generally failed to account for:

– Complex topography in the area (extremely large geographical altitude variations).
– RF "clutter" – the morphology of the terrain as it impacts the RF propagation.
– The high probability that many calls endured Directed Retry; this was not recognized.
– Geolocation consequences of Directed Retries were not addressed.
– Problems due to unknown antenna tilts were not recognized and addressed.
– Possibility of cell outages was not recognized and addressed.

In particular, in the 3 intervals of interest we found:

- Wrong estimates of the potential location and direction of travel for the only call in the evening on 02/04/2010.
- Wrong estimate of the width and serious underestimate of the range for the "pie" shaped area where 11:30-11:34M calls could have been made on 02/06/2010.
- Failure to indicate the end of call cell locations gave very misleading location inferences for calls at 11:52AM, 11:53AM and 1:30PM on 02/06/2010.
- Presentation of the incomplete call data and a failure to recognize a possibility of Directed Retries and the erroneous entries in the Cell Site Table gave the misleading ideas about the locations and direction of travel during the calls from 1:31PM to 1:41PM on 02/08/2010.

Appendix

In the course of this investigation we performed an analysis of the area of the potential overlap between the signals from the cells 11095, 11091 and 11092. It was made in the early stages of the project, before the author became aware of the likelihood of the Directed Retries and the availability of the drive test data. After this data confirmed the hypothesis that the calls from 11:30AM to 11:34AM could have been made from large areas to the North and East of the site, the question of the possible area for these calls in the NE direction (along I-15) became less relevant, so we are including it as an Appendix.

Regarding the cells 11095, 11091 and 11092 on the cell site "Quartzite", Cell Site Table gives the azimuths as 10°, 85° and 170° respectively, while beamwidths for all three are 65°. Although the antenna models are not specified, and the actual radiation patterns are thus unknown, in the RF engineering theory it is well known that radiation pattern of any antenna (when expressed in units of decibels, dB for short) can be very well approximated by the so-called parabolic curve. This parabolic approximation can be calculated whenever the antenna beamwidth is known, and in Figure 32 we show an example of the actual antenna pattern vs. its parabolic approximation. The agreement is obviously quite good, especially in the main antenna lobe which is of primary interest anyway.

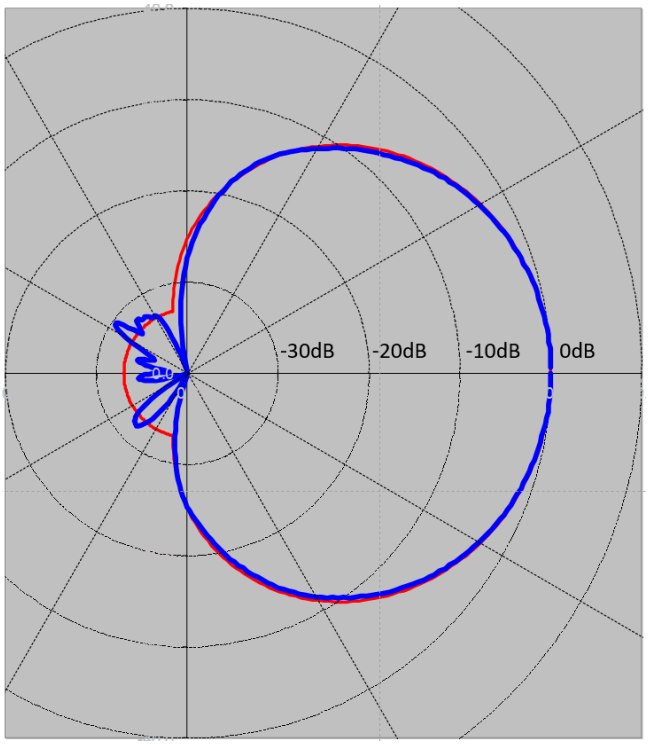

Figure 32: Radiation Pattern (blue) and parabolic approximation (red) for antenna CSS-XS4-65-R1

Based on this approximation and the known antenna azimuths from the Cell Site Table, we can plot the radiation patterns of the cell antennas that are next to each other on a cell site. Such a depiction is shown in Figure 32 for the two antennas with 65° beamwidths pointing at 10° and 85°, which are the azimuths for the cells 11091 and 11095 per the Cell Site Table. Picture is given in the normal Cartesian coordinates (x-y), not in the polar coordinates used in Figure 32, because the rest of the material seems easier to understand that way. Note that the curves of the radiation power in solid lines are drawn in the linear scale (on the left), while the radiation powers in dB units are drawn in dashed lines against the scale in dB units on the right. Dashed curves follow the parabolic (quadratic) shape that the approximation is named after and the linear curves are shown in % points scaled to the maximum radiation level at antenna boresight. Radiated powers are shown in the azimuth range from 0° to 180°, i.e. for any angle of the received antenna starting from North direction to the South.

Hand-offs in a cellular network are based on the received power measurements from all cell sites that mobile can detect. The decision for executing the hand-off, however, are made based on the ratios of the measured signals – when the hand-off hysteresis is e.g. 3dB, hand-off would be executed when the newly detected cell site power level is 3dB above the old one, which – translated back into linear instead of the dB domain – means when the power from the new cell is 2 times larger than from the old one.

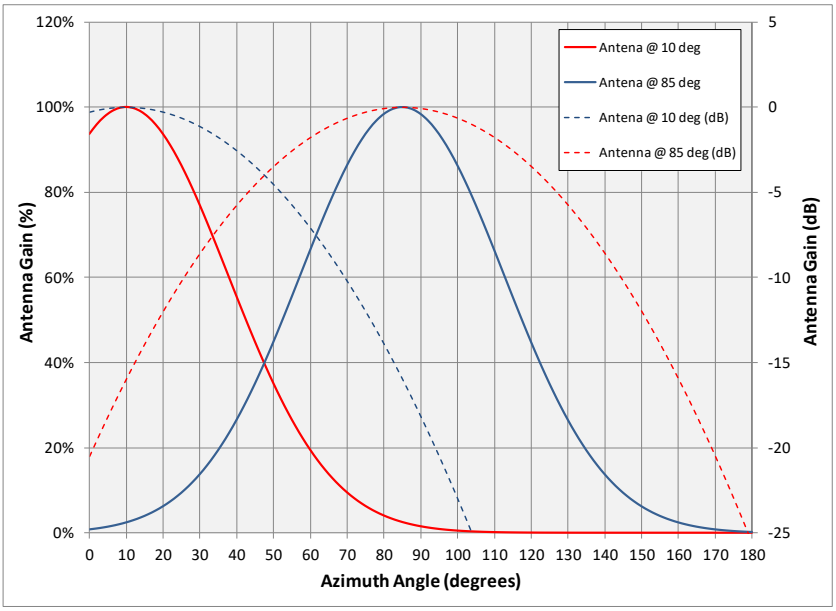

Figure 33: Radiation patterns for two antennas with 65° beamwidths pointing at 10° and 85° In linear (solid lines) and dB scale (dashed)

Since we can calculate the individual powers of the two antennas as in Figure 33, we can also calculate their ratios. A plot of such a calculation is presented in Figure 34. Note that the azimuths of the two cells involved is marked on the X-axis, as well as the azimuth for the "crime scene" ("gravesite" location) as seen from the cell site "Quartzite". Only a range from 0° (N) to 120° (ESE) is shown because the ratio for larger azimuths increases very sharply (e.g. power ratio of cells 11095/11091 at the 109° azimuth for the gravesite direction is at 459.56).

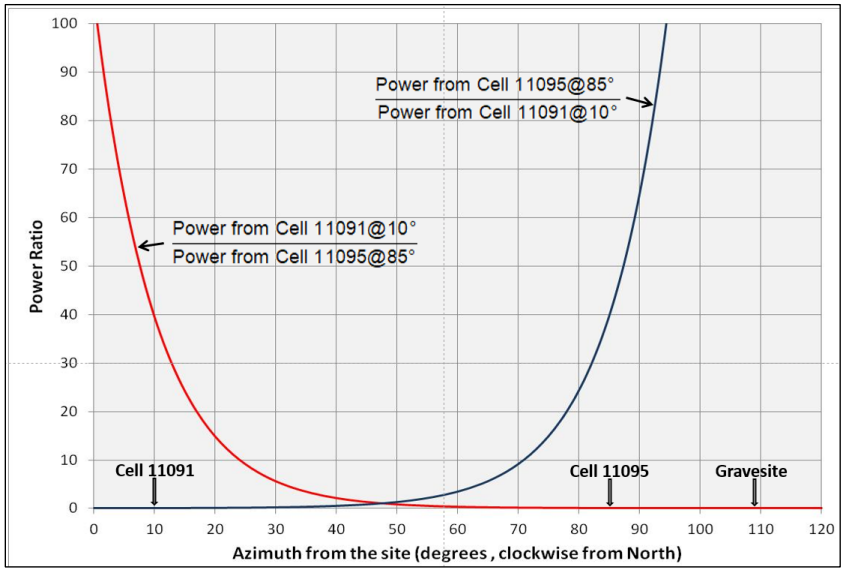

Figure 34: Ratio of the cell powers for various azimuths from N to ESE

If the signal power measurements were perfect, areas of potential hand-offs would be determined solely by the hand-off hysteresis value. If there is no hysteresis (0dB, or factor of 1), hand-off would be executed in the mid-point, which is 47.5°. When the hysteresis is 3dB (factor of 2), the hand-off points can be determined by finding the azimuth points on the X-axis where the power ratio is equal to 2 on the Y-axis.

In this picture they turn out to be at 40° for the red line and about 55° for the blue one. This means that a mobile going from right to left (northbound) would be served on cell on the right (at 85°) until the red line reaches 2, i.e. it would hand-off at 40°. Similarly, a mobile moving from left to right (southbound) would stay on the cell pointing at 10° until the blue line reaches the value of 2, i.e. until it reaches the azimuth of 55°, when it would hand-off to the cell pointing at 85°. Region from 40° to 55° would then be the hand-off uncertainty region, i.e. the range of azimuths were mobile can be on either of the cells, depending on the past history.

Signal power measurements made by the mobiles are never perfect – they always have some systematic errors. Since the signal powers at the time of hand-off are of comparable strength, however, the errors are going to be very similar for both and the ratio of the measured powers would practically be unaffected.

The mechanism that makes measurements much more inexact is a mechanism called "fast fading" (or "small scale" fading). It describes the variations of the received signal power over the short distances. Depending on the RF frequency, received signal can change form a few times *above* the average to theoretically up to 100 times *below* the average level over the distances of just 6 to 12 inches (on cellular networks frequencies). This is due to a phenomenon called *multipath* propagation – the fact that mobile antennas receive multiple rays of RF signals that bounce of neighboring objects (ground, buildings, hills, etc.). These rays sometimes combine constructively to increase the received level above the average, but sometimes work against each other and deep fade can be experienced as a result.

Now, somewhat paradoxically, when a mobile phone is moving fast it tends to go through many ups and downs of the received waveform (at 30mph, it traverses about 15 yards each second) during the measurement interval and the averaging gives a pretty good estimate of the mean signal value. When the mobile is strictly stationary, however, then there is very little to average and radically different measurement results can be obtained when it moves by as little as a couple of inches. This is enough to cause a hand-off from one site to the other, depending on how each of the two signals changed, and can be easily demonstrated with real phones in practical situations.

There seems to be no results in the open literature about the real values of phone's signal measurements variations under various conditions of speed and multipath[43]. Under the "Quartzite" cell, whose height would ensure the line-of-sight conditions, there will also not be too many at least man-made objects for signals to bounce of, so the fading is likely to be *Rician* (as opposed to more severe *Rayleigh* type) and the literature[44] suggest that dips with GSM signals would be less than 15-30 times (12-15dB) below the average value with very small movements. For mobiles moving at the vehicular speeds (say 10-60 mph), practical experience suggests that variations in such conditions are rather small, of the order of 2-3dB (or 1.6 to 2 times in power), maybe going up to 6dB (factor of 4) in some extreme cases[45].

In Figure 35 we now show basically the same picture as in Figure 34, but with lines for several different values of the hand-off hysteresis and uncertainties in the measurements due to fast fading combined.

[43] Phone manufacturers certainly have such results, but keep them proprietary for competitive reasons.

[44] F.D. Cardoso, L.M. Correia, "Fading Depth Dependence on System Bandwidth in Mobile Communications—An Analytical Approximation", IEEE Trans. Vehic. Techn., vol. VT-52, No.3, May 2003

[45] Mostly from hand-offs observed during drive testing – locations of hand-offs along the same path are quite repeatable, which would not be happening if the measurement errors due to fast fading are large.

Line marked “2:1” would correspond to uncertainty due to hand-off hysteresis only (typ. 2-3dB, factor of 2 or less), line “9:1” would correspond to the uncertainty due to hysteresis plus another uncertainty range of all the way up to 6dB for a phone moving at vehicular speed, and the line “60:1” would correspond to the additional uncertainty of 12-15dB for a stationary mobile swaying back and forth by a bit.

The resulting uncertainty region with these uncertainties now increases to an arc from about 25° to 70° with mobile speeds, which is what was actually depicted in Figure 12 in the main part of the report, while with a stationary mobile the area would be wider and would span azimuths from about 5° to about 91°. Given that the hand-off area to the NE of “Quartzite” seems to be empty except for the I-15 and a few secondary roads, one can probably argue that the former set of boundaries is more realistic, but the wider area corresponding to the stationary conditions could have been applicable too, for instance in a case of traffic jam and “stop-and-go” traffic conditions on the I-15.

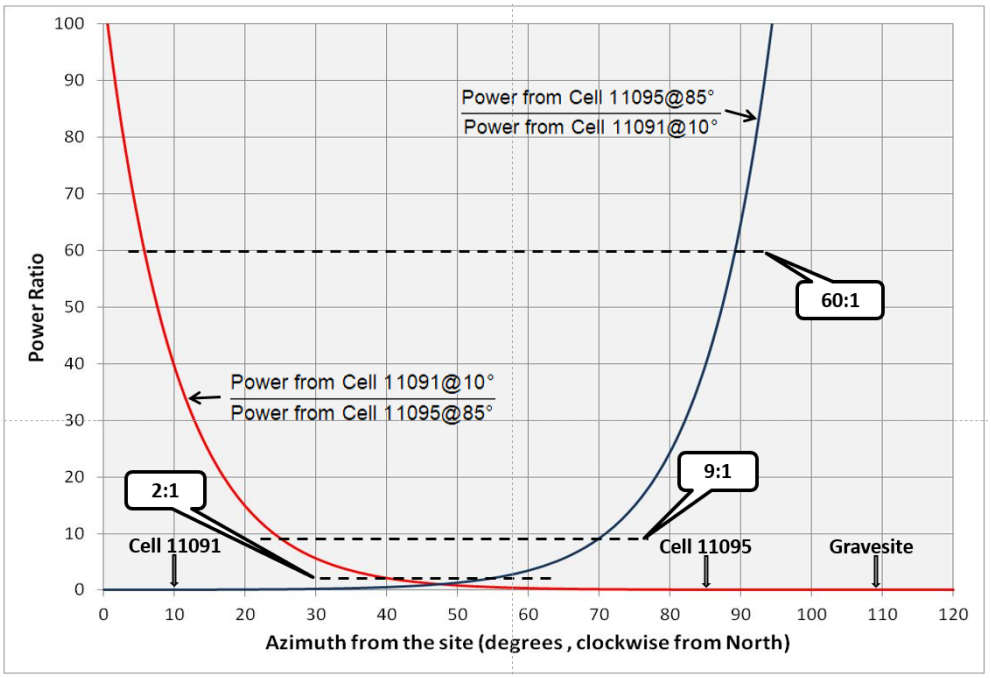

Figure 35: Estimating the hand-off uncertainty region

Although the hand-off area now becomes closer to the gravesite (at the azimuth 109°), there is still no possibility that the calls with hand-offs bouncing between cells at 10° and at 85° could have been made from the gravesite – cell 11095 is about 450 times stronger than cell 11091 in that direction, and no combination of fading and mobile’s speeds could have caused the mobile to hand-off to cell 11091.

Similar plots can also show that – in the case that the cell 11095 was blocking – Directed Retry would have sent the call to the cell 11092 (pointing at 170°, almost straight to the South) rather than to the cell 10091 (pointing at 10°, almost straight to the North), because the signal from cell 10092 is more than 50 times stronger than the signal from cell 10091 in the direction of the gravesite.