THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 12 | Number 2 Article 7

6-30-2017

Forensic Cell Site Analysis: A Validation & Error Mitigation Methodology

John B. Minor
jminor@johnbminor.net

Follow this and additional works at: https://commons.erau.edu/jdfsl

 Part of the Computer Law Commons, and the Information Security Commons

Recommended Citation

Minor, John B. (2017) "Forensic Cell Site Analysis: A Validation & Error Mitigation Methodology," *Journal of Digital Forensics, Security and Law*: Vol. 12 : No. 2 , Article 7.
DOI: https://doi.org/10.15394/jdfsl.2017.1474
Available at: https://commons.erau.edu/jdfsl/vol12/iss2/7

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

(c)ADFSL

FORENSIC CELL SITE ANALYSIS: A VALIDATION & ERROR MITIGATION METHODOLOGY

John B. Minor
jminor@johnbminor.net
johnbminor.com

ABSTRACT

The E911 Initiative in the mid-1990s established an opportunity to obtain location specific digital evidence of subscriber activity from cellular carriers. Call Detail Records (CDR) containing Cell Site Location Information (CSLI) evidence production was made available from cellular carriers in response to the CALEA, 911 and ECPA acts. In the late 1990s, cellular carriers began to produce evidence for investigative and litigation purposes. CDR/CSLI evidence has become an important evidentiary focus in the courtroom. This research project resulted in the creation of a method of validating cellular carrier records accuracy and mitigating errors in forensic cell site analyst conclusions. The process establishes a scientific foundation critical to satisfying key Daubert requirements. The United States Patent and Trademark Office (USPTO) awarded a patent for this methodology.

Keywords: cellular carrier records, call detail records, signals analysis, forensic cell site analysis, error mitigation, validation, Daubert, CDR, CSLI, defendant location evidence, drive test, radio survey

1. INTRODUCTION

In 1996, the Federal Communications Commission (FCC) issued an order for the Enhanced 911 initiative. Phase 1 required that the location of the cell site to which a subscriber device was registered during communications be documented as part of the record keeping process (FCC, 2001). As early as 1999, cellular carriers began to produce Call Detail Records (CDR)/Cell Site Location Information (CSLI) evidence in response to subpoena, search warrants, and court orders. The primary focus of the analysis of this type of evidence is two-fold: 1) analysis of who was communicating with the subscriber and 2) where the subscriber device was located during communications. Forensic cell site analysis became a new forensic analysis discipline requiring knowledge of cellular carrier network infrastructure and operations as well as an ability to analyze and interpret CDR/CSLI evidence.

Cellular carrier evidence produced most often are Call Detail Records (CDR) which include location evidence, commonly called Cell Site Location Information (CSLI).

Most significantly, CSLI is frequently analyzed to determine the location of a subscriber device during active communications sessions. Forensic cell site analysts often create maps exhibiting cell site locations and estimate cell site coverage in the

© 2017 ADFSL

form of pie slices or Vs. Mapping produced by analysts have varying levels of accuracy, often providing an unreliable interpretation of the actual evidence.

Analysts typically plot the GPS coordinates of cell sites (which include Base Transceiver Station, NodeB, eNodeB, and future 5G Access Points) (5G PPP AWG, 2016; Freescale Semiconductor, 2009) provided by the cellular carrier and illustrate an estimate of coverage for communications sessions of interest without establishing any basis for the estimate. If challenged, and absent adequate analysis error mitigation or evidence validation, the resulting analysis fails to meet Daubert requirements.

In the United States, forensic cell site analysis has been utilized extensively in criminal cases. The United States Department of Justice stated that defendant location evidence is of utmost importance and that historical cell site analysis is a primary means of establishing such evidence (O'Malley, 2011). In civil cases, such as distracted driving litigation, cell site analysis of CDR/CSLI evidence is frequently used to determine driver fault. Chief Justice Roberts noted that "[m]odern cell phones ... are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy" (Riley v. California, 2014). A review and analysis of caselaw regarding the limitations and admissibility of historical cell site evidence resulted in publication of a law journal article in which several conclusions were offered including the statement that, "[h]opefully courts will preclude the admission of sub-par tracking testimony that is based on unreliable and unsubstantiated techniques" (Blank, 2011).

The National Institute of Standards and Technology (NIST) has published extensive forensic evidence guidance and standards documents for the acquisition, validation and analysis of computer and cell phone evidence (Ayers, Brothers, & Jansen, 2014). Curiously absent are standards for the handling, analysis, validation or error mitigation of CDR/CSLI evidence in NIST publications.

The United Kingdom is addressing the field of Digital Forensics – Cell Site Analysis by creating a code of practice and conduct through its Forensic Science Regulator Department (United Kingdom Forensic Science Regulator, 2016). The UK Accreditation Service for Laboratory Accreditation has also initiated an accreditation program for Forensic Cell Site Analysis. Validation is mentioned generally in the United Kingdom accreditation specifications and standards; however, no specific methodologies are delineated (United Kingdom Accreditation Service, 2016). This is the only state sponsored certification and standards development program for forensic cell site analysis discovered during research.

2. ERROR RATES

Live multilateration and trilateration device location calculation techniques, utilized during 911 calls, upon declaration of exigent circumstance, or during authorized wiretap intercepts include confidence and uncertainty (C/U) data (FCC, 2015). This type of evidence is produced in criminal cases and the C/U data is the only error rate information acknowledged or produced by cellular carriers in real time device tracking.

The absence of statistical data regarding CDR/CSLI evidence error rates coupled with the discovery of several types of errors encountered during research and analysis is the basis of a growing sense of fallibility in the cellular industry's record keeping process.

 © 2017 ADFSL

Errors have been discovered during CDR/CSLI evidence review and analysis in several distinct areas. Cellular carriers have documented neither error rates nor validation methodologies for the following:

1. Carrier cell site location database records.
2. CDR/CSLI records.
3. Documented network infrastructure and operational failures.

The FCC maintains Universal Licensing Filings which include cellular carrier transmitting cell site licensing (FCC, n.d). The FCC has documented neither error rates nor a validation methodology for the filings.

The Scientific Working Group on Digital Evidence (SWGDE, 2017) establishes that "a process for recognizing and describing both errors and limitations" (p. 8) should be utilized so "that confidence in digital forensic results is best achieved by using an error mitigation analysis approach that focuses on recognizing potential sources of error and then applying techniques used to mitigate them, including trained and competent personnel using tested and validated methods and practice" (p. 8).

3. RESEARCH METHODOLOGY

This study addresses three fundamental questions:

1. What are the methods for validating CDR/CSLI evidence and mitigating errors in forensic cell site analysis?
2. How often is evidence validation undertaken?
3. How effective is the error mitigation?

In sworn testimony and certified written responses, cellular carriers have stated that no error rate exists for their database repositories of subscriber activity records, carrier network infrastructure documentation, maintenance, and performance records. Thus, CDR/CSLI evidence production has historically been submitted as accurate by cellular carrier legal compliance departments and acknowledged as accurate by the courts without any validation or error mitigation.

For this research project, criminal and civil cases were reviewed in which historical CDR/CSLI evidence was produced and analyzed for subscriber device location. In every case selected for the control group, a preliminary analysis mapping of the CSLI was produced by the analyst (the first item in the Table 1 chart).

Each case was next reviewed to determine if an analyst performed any type of validation of the evidence or error mitigation of the preliminary analysis mapping.

Research was conducted of the cellular carrier network infrastructure, subscriber communications flow through the network, subscriber authentication techniques and CDR/CSLI records creation methods. The fact that cellular carriers document all aspects of subscriber access and usage of the network infrastructure verifies that validation and error mitigation of this type of evidence can be accomplished by the forensic cell site analyst.

Further data was collected regarding how cellular carrier planned and unplanned maintenance logs are recorded. Ongoing maintenance of cellular carrier networks is accomplished by operations and maintenance personnel either contracted by or working directly for each cellular carrier. Each cellular carrier operates one or more Network Operations Centers (NOCs). Further research accompanied with evidence produced from compel proceedings revealed that maintenance records are kept for three or more years.

From this compilation arose a hypothesis resulting in several CDR/CSLI evidence

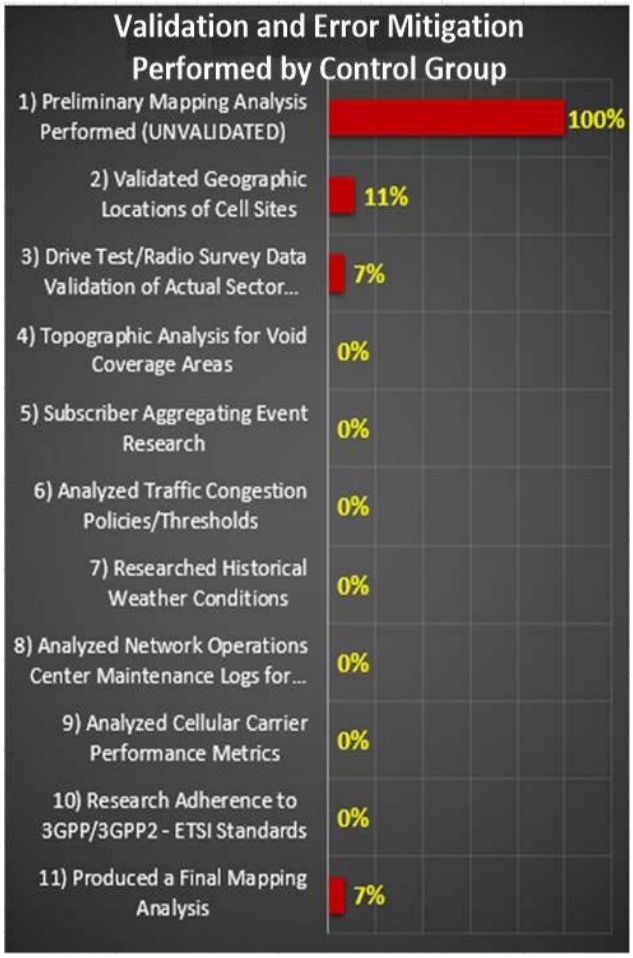
© 2017 ADFSL

validation and error mitigation steps listed as follows:

Evidence Validation & Error Mitigation Steps

1. Perform Preliminary Mapping
2. Validation of the Geographic Locations of Cell Sites
3. Drive Test / Radio Survey Validation of Actual Sector Coverage Extents
4. Topographic Analysis for Void Coverage Areas
5. Subscriber Aggregating Event Research
6. Analysis of Traffic Congestion Policies and Cellular Carrier Network Infrastructure Threshold Settings
7. Research of Historical Weather Conditions
8. Analysis of Network Operations Center Maintenance Logs for Planned/Unplanned Outages
9. Analysis of Cellular Carrier Performance Metrics
10. Research of Cellular Carrier Adherence to 3GPP, 3GPP2, ETSI, and IETF Operating Standards
11. Production of a Final Refined Accuracy Mapping Analysis

Table 1.
Rate of validation and error mitigation performed prior to application of methodology



The data in Table 1 was derived from approximately 100 criminal and civil cases in which a forensic cell site analyst created mapping exhibits during the interpretation of CDR/CSLI evidence and produced an analysis for use in litigation.

Table 1 shows the percentage of cases in which validation and error mitigation was performed.

Several observations were noted from the enquiry:

First, in only 11% of cases were any cell sites validated for geographic location. Neighboring or adjacent cell sites that would fall into the neighbor list, a list of cell sites

 © 2017 ADFSL

maintained within every subscriber device, were rarely validated for geographic location.

Second, in only 7% of the cases was drive testing/radio survey performed. Most of those radio surveys were performed using a single test phone rather than using multiple test phones sending/receiving voice calls, text messages, etc. The surveys also focused only on cell sites of interest rather than a geographic area that included cell sites utilized by the subscribe device and neighboring or adjacent cell sites in the neighbor list.

Third, the analyst's final analysis mapping was subjected to proper validation and error mitigation in only 7% of the cases.

Fourth, in the vast majority of cases no validation or error mitigation analysis steps were performed.

Application of the hypothesis to the control group tested the effectiveness and significance of utilizing the devised methodology.

4. OUTCOMES FROM APPLICATION OF VALIDATION & ERROR MITIGATION

Several validation and error mitigation steps, if applied prior to finalizing an analysis, ensure achievement of a reliable outcome.

4.1 Validation of the Geographic Locations of Cell Sites

Foremost, it is necessary for the analyst to compare the geographic cell site locations with the cellular carrier produced geographic cell site location records.

Performing this step comprises an onsite collection of the actual geographic cell site locations using a Global Positioning System (GPS) capable instrument, use of an internet search tool such as the FCC database repository of radio frequency transmitting sites, or utilization of an aerial image viewing tool such as Google Earth to validate the carrier records. When cell site locations are not validated the preliminary analysis mapping risks introduction of false positive indications of the general location of the cellular subscriber device. This fundamental first validation step eliminates a substantial percentage of errors.

An example of this validation step's impact on the cell site analysis outcome occurred when a cellular carrier produced records in response to a search warrant that erroneously identified more than 20 cell site locations within a radius of 2 miles. Many of the locations were identified as the same cell site scattered around the neighborhood. See figures 1 and 2 below. The records did not represent a Distributed Antenna System (DAS) under the ANSI/BICSI 006-2015 Distributed Antenna System (DAS) Design and Implementation Best Practices. The location data contained invalid location information, documented by contractors during initial installation or later equipment upgrades of the cell site (BICSI, 2015). Table 2 shows the error rate determined in the above example.

Table 2
Cell Site Database Error Rate

Los Angeles Area Total Cell Sites	Errant Cell Site Locations Discovered	Error Rate
4979	95	1.91%

SWITCH	CELL	SECTOR	AZIMUTH	ADDRESS	CITY	COUNTY	STATE	ZIP	LAT	LONG
Sante Fe1(SW3)	409	1	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.9066	-118.19966
Sante Fe1(SW3)	409	2	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.9004	-118.19959
Sante Fe1(SW3)	409	3	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.89426	-118.20055
Sante Fe1(SW3)	409	4	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.91104	-118.22205
Sante Fe1(SW3)	409	5	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.90979	-118.21422
Sante Fe1(SW3)	409	6	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.91	-118.231352
Sante Fe1(SW3)	410	1	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.90483	-118.21
Sante Fe1(SW3)	410	2	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.89864	-118.20753
Sante Fe1(SW3)	410	3	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.89576	-118.21365
Sante Fe1(SW3)	412	1	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.903997	-118.230083
Sante Fe1(SW3)	412	2	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.89999	-118.22214
Sante Fe1(SW3)	412	3	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.89914	-118.23208
Sante Fe1(SW3)	412	4	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.90531	-118.22263
Sante Fe1(SW3)	412	5	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.90312	-118.21526
Sante Fe1(SW3)	412	6	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.89679	-118.23752
Sante Fe1(SW3)	440	1	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.89418	-118.22753
Sante Fe1(SW3)	440	2	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.88933	-118.22219
Sante Fe1(SW3)	440	3	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.87879	-118.21417
Sante Fe1(SW3)	440	4	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.88164	-118.17735
Sante Fe1(SW3)	440	5	0	127 N. Wilmington Ave.	Compton	Los Angeles	CA	90220	33.889	-118.18218

Figure 1. Example List of Erroneous Cell Sites Discovered

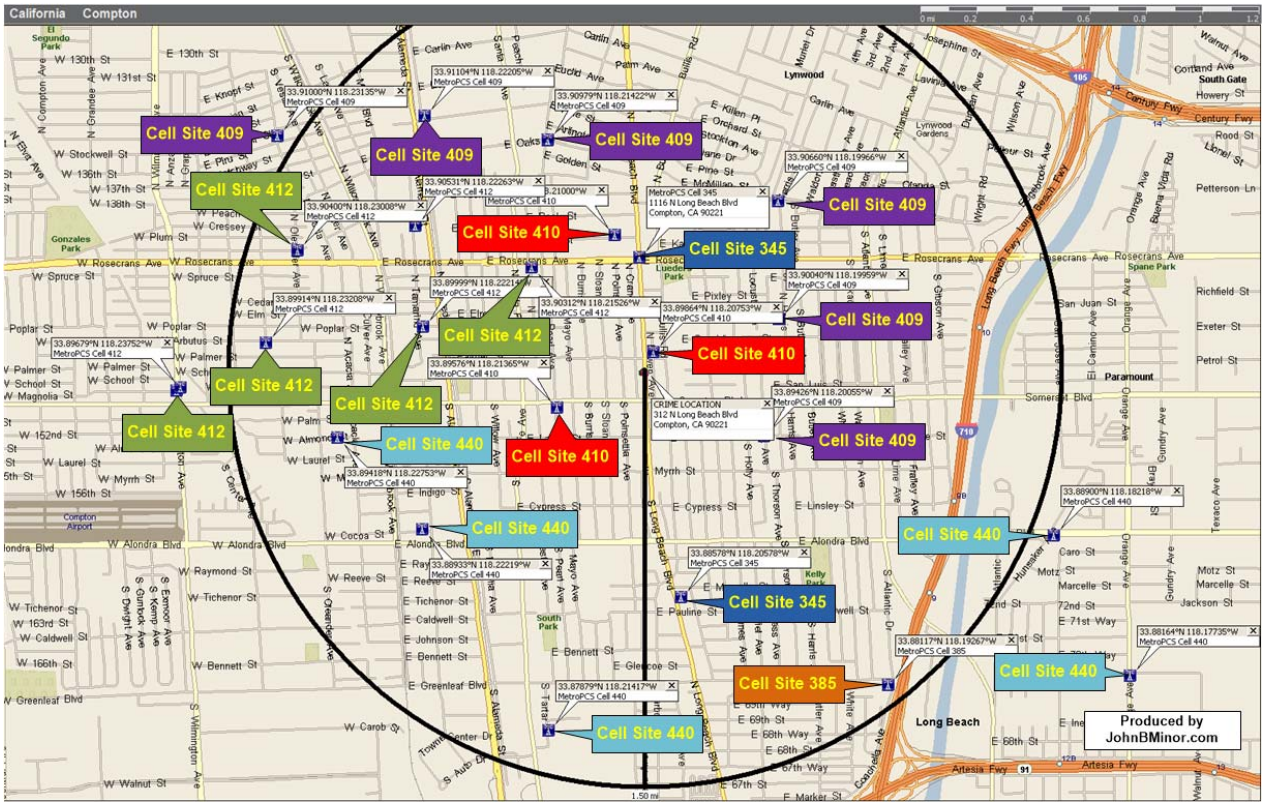


Figure 2. Depiction of the Mapped Coordinates of Erroneous Cell Sites Locations.

© 2017 ADFSL

4.2 Drive Test / Radio Survey Validation of Actual Sector Coverage Extents

The collection of on-site wireless cellular service test data, commonly called drive test or radio survey data, is important to the maintenance of cellular carrier networks. Radio surveys assist carrier engineering and operations departments in determining not only the coverage extents of each cell site but also hand over / hand off performance and other performance characteristics of the network (Hoy, 2015). The utilization of radio survey data, in the context of this study, is primarily to estimate the radio frequency propagation coverage extents for each validated cell site location as well as handover / handoff performance (Tart, Brodie, Gleed, & Matthews, 2012). Historic radio survey data acquired near the time of critical events will best depict network coverage during those critical events. Of paramount importance, the forensic cell site analyst must understand which generation (2G, 3G, 4G, LTE, 5G, etc.) of the cellular network was in use by the subscriber device to create the CSLI evidence and validate that radio survey data was sourced from the correct generation. Confirmation of any use of DAS or other relay nodes in the region under analysis is also critical to the validation and error mitigation process.

© 2017 ADFSL

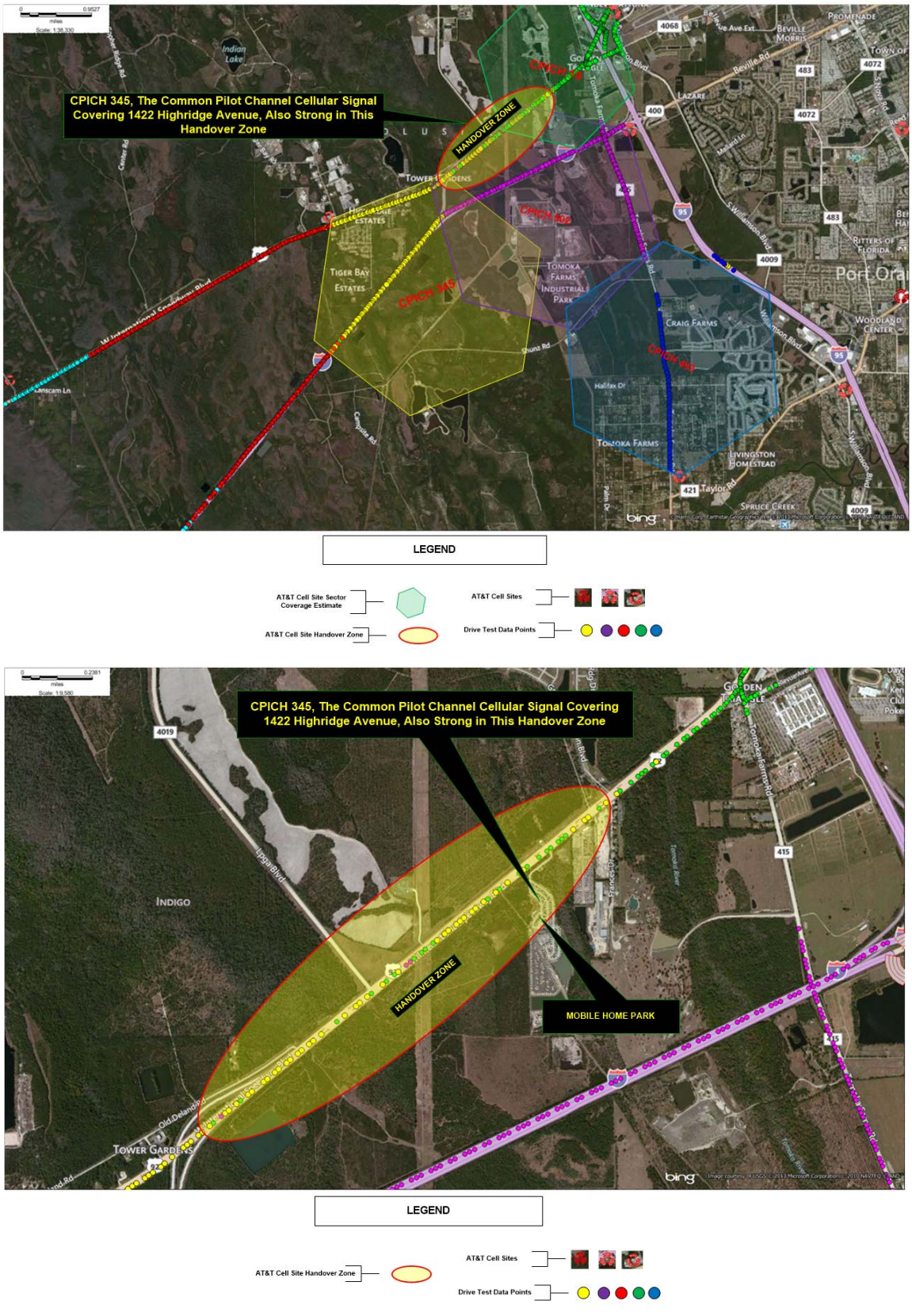


Figure 3. Graphic Examples of Drive Test/Radio Survey Data Filtered for Cell Sites of Interest.

 © 2017 ADFSL

Cellular carriers maintain drive test/radio survey data; however, subpoenas or court orders are currently required to obtain the data. Figure 3 exhibits the use of cellular carrier produced drive test / radio survey data to depict sector coverage and hand over zones. Private entities conduct radio surveys for a variety of purposes, including the fulfillment of contracts with carriers (MobileComm Professionals, 2015) and, upon request, for use in forensic cell site analysis. The FBI Cellular Analysis Survey Team (CAST) performs radio surveys in some cases, though often not adequate to map the neighbor list cell site coverage extents in a proper manner. In some instances, this data may not be available to an analyst. If not, then other analysis steps will assist in further refining the potential coverage area of a cell site.

An alternate method is to obtain and analyze the technical configuration characteristics of each cell site and corresponding adjacent cell sites with a predictive cellular coverage application. The FCC Code of Federal Regulations defines a Cellular Geographic Service Area (CGSA) and Service Area Boundary (SAB) (FCC, 2013). Furthermore, a review of the Service Area Boundary (SAB) for each analyzed cell site will assist in performing an analysis based upon planned or unplanned adjacent cell site outages (Figure 4). Such analysis would expand the coverage area of any analyzed cell site if outage of any adjacent cell site is discovered during the analysis timeframe.

Location 10 (Fixed - A)			
140 Merrick Avenue (97374) STATEN ISLAND, NY RICHMOND County			
Site Elevation (AMSL)	116.1m		
ASR #/File #	N/A		
Support Structure Type	B - Building		
NEPA Required	No		
Quiet Zone Notification Date			
Is coordination with Canada required?			
Is coordination with Mexico required?			
Location Buildout Deadline			
Special Conditions	None		
Antenna 1			
Height to Tip AGL	21.0m		
Maximum Transmitting ERP			
• Radials		**0°**	**45°**
	Radiation Center HAAT	139.9	143.1
	Transmitting ERP	278.600	129.600
	Distance to SAB	35.4	31.3
	Distance to CGSA	0.0	0.0

Figure 4. Example of Federal Communications Commission Universal Licensing System Research Results Indicating the Service Area Boundary (SAB)
Source:http://wireless2.fcc.gov/UlsApp/UlsSearch/licenseLocDetail.jsp?pageNumToReturn=1&keyLoc=5015381&licKey=13092

4.3 Topographic Analysis for Void Coverage Areas

A topographic analysis tool should be utilized to determine the presence or absence of radio frequency propagation coverage due to morphologies that introduce absorption, refraction, diffraction, scatter or reflection of the cell site signal (NASA, 2016). The analysis may result in a preclusive or inclusive finding that the cellular subscriber device was located within an area near the location of critical events.

Other examples of radio frequency propagation coverage adjustment factors, including waterways, roadways, forestation, and high-rise buildings, should also be investigated for modification of signal coverage (Hamid & Kostanic, 2013; Hata, 1980; Lee, 1995, 2005; Okamura, Ohmori, Kawano, & Fukuda, 1968).

4.4 Subscriber Aggregating Event Research

The analyst should undertake additional research for subscriber aggregating events occurring in the general vicinity of key cell sites and near the time of critical events. Examples of subscriber aggregating events that cause a clustering of cellular subscribers would be traffic congestion, traffic accidents, and sporting or other public events. Subscriber communications traffic congestion may result in the registration of a cellular subscriber device to a cell site that is not the nearest cell site to the cellular subscriber device nor is the strongest signal detected by the device (Ali, 2009).

4.5 Analysis of Traffic Congestion Policies and Network Infrastructure Threshold Settings

A thorough review of the technical configuration characteristics and traffic congestion policies should be performed to determine a traffic loading threshold for the analyzed cell sites. The traffic loading threshold is the maximum number of cellular subscribers that may be concurrently registered to the analyzed cell sites (Bahl, Hajiaghayi, Jain, Mirrokni, Qiu, & Saberi, 2007). Subscriber communications traffic congestion may result in the registration of a cellular subscriber device to a cell site that is not the nearest cell site to the cellular subscriber device nor is the strongest signal detected by the cellular subscriber device (Ali, 2009).

This analytical step would determine whether the estimated radio signal coverage of an analyzed cell site should be expanded to include a greater geographic area. Expanded coverage areas would alter the area within which the cellular subscriber device was located.

4.6 Research of Historical Weather Conditions

Analysis should be undertaken of the historical weather records for certain weather events that may have resulted in disrupting cellular service provided by the analyzed cell sites. This step determines whether the radio signal coverage of an analyzed cell site should be expanded during mapping to include a greater geographic area.

The impact of weather on cellular communications, an example of which the graphic (figure 5) below depicts, demonstrates that the network is susceptible to rain fade or may suffer cell site outages caused by lightning strikes on or near cell sites (FCC, 2016).

 © 2017 ADFSL

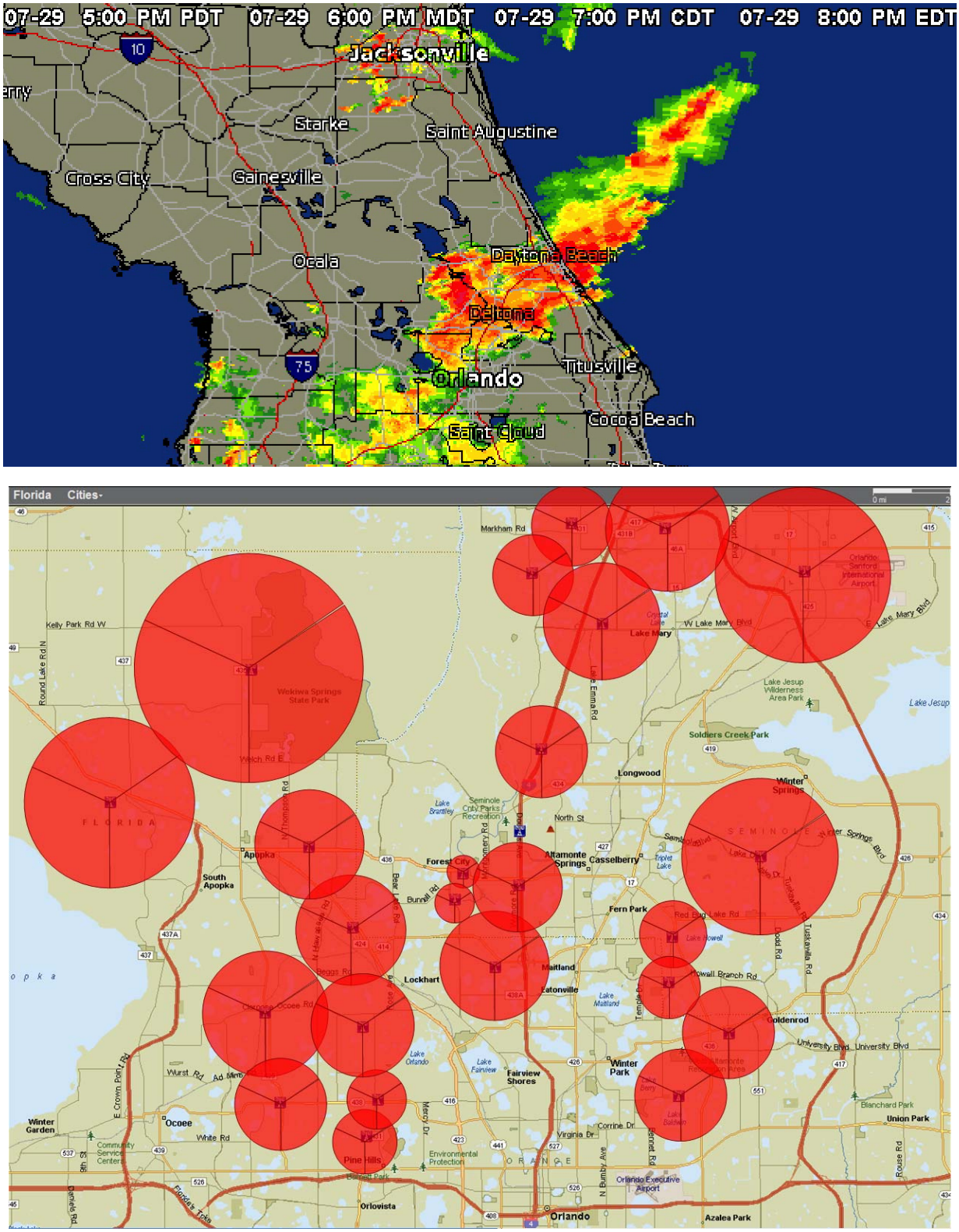
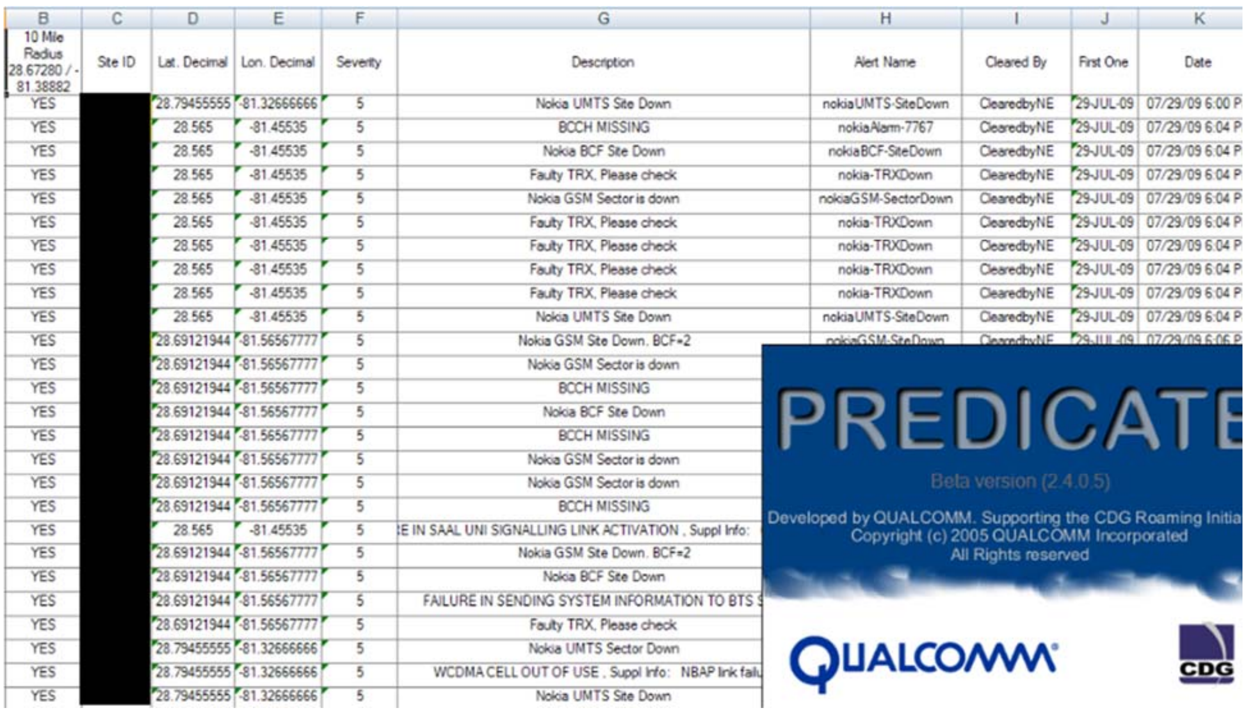


Figure 5. Historical weather radar exhibiting severe weather during critical event times and resulting cellular network outages

4.7 Analysis of Network Operations Center Maintenance Logs for Planned or Unplanned Outages

Analysis of the operation and maintenance logs for an equipment disruption or other service disruption during critical event times is also important. An outage of neighboring cell sites will affect the radio frequency coverage area, thereby expanding the coverage of one or more cell sites. Figure 6 is an example of maintenance logging exhibiting sector and cell site outages (Xu, Broustis, Ge, Govindan, Mahimkar, Shankaranarayanan, & Wang, 2015).

Performing this step reveals any functionality issues within network elements including cell sites and communications traffic routing elements. Malfunctioning network elements in a cellular carrier network often modifies signal coverage and pathing/routing of communications sessions.



B	C	D	E	F	G	H	I	J	K
10 Mile Radius 28.67280 / -81.38882	Site ID	Lat. Decimal	Lon. Decimal	Severity	Description	Alert Name	Cleared By	First One	Date
YES	[redacted]	28.79455555	-81.32666666	5	Nokia UMTS Site Down	nokiaUMTS-SiteDown	ClearedbyNE	29-JUL-09	07/29/09 6:00 P
YES		28.565	-81.45535	5	BCCH MISSING	nokiaAlarm-7767	ClearedbyNE	29-JUL-09	07/29/09 6:04 P
YES		28.565	-81.45535	5	Nokia BCF Site Down	nokiaBCF-SiteDown	ClearedbyNE	29-JUL-09	07/29/09 6:04 P
YES		28.565	-81.45535	5	Faulty TRX, Please check	nokia-TRXDown	ClearedbyNE	29-JUL-09	07/29/09 6:04 P
YES		28.565	-81.45535	5	Nokia GSM Sector is down	nokiaGSM-SectorDown	ClearedbyNE	29-JUL-09	07/29/09 6:04 P
YES		28.565	-81.45535	5	Faulty TRX, Please check	nokia-TRXDown	ClearedbyNE	29-JUL-09	07/29/09 6:04 P
YES		28.565	-81.45535	5	Faulty TRX, Please check	nokia-TRXDown	ClearedbyNE	29-JUL-09	07/29/09 6:04 P
YES		28.565	-81.45535	5	Faulty TRX, Please check	nokia-TRXDown	ClearedbyNE	29-JUL-09	07/29/09 6:04 P
YES		28.565	-81.45535	5	Faulty TRX, Please check	nokia-TRXDown	ClearedbyNE	29-JUL-09	07/29/09 6:04 P
YES		28.565	-81.45535	5	Nokia UMTS Site Down	nokiaUMTS-SiteDown	ClearedbyNE	29-JUL-09	07/29/09 6:04 P
YES		28.69121944	-81.56567777	5	Nokia GSM Site Down. BCF=2	nokiaGSM-SiteDown	ClearedbyNE	29-JUL-09	07/29/09 6:06 P
YES		28.69121944	-81.56567777	5	Nokia GSM Sector is down				
YES		28.69121944	-81.56567777	5	BCCH MISSING				
YES		28.69121944	-81.56567777	5	Nokia BCF Site Down				
YES		28.69121944	-81.56567777	5	BCCH MISSING				
YES		28.69121944	-81.56567777	5	Nokia GSM Sector is down				
YES		28.69121944	-81.56567777	5	Nokia GSM Sector is down				
YES		28.69121944	-81.56567777	5	BCCH MISSING				
YES		28.565	-81.45535	5	:E IN SAAL UNI SIGNALLING LINK ACTIVATION , Suppl Info:				
YES		28.69121944	-81.56567777	5	Nokia GSM Site Down. BCF=2				
YES		28.69121944	-81.56567777	5	Nokia BCF Site Down				
YES		28.69121944	-81.56567777	5	FAILURE IN SENDING SYSTEM INFORMATION TO BTS S				
YES		28.69121944	-81.56567777	5	Faulty TRX, Please check				
YES		28.79455555	-81.32666666	5	Nokia UMTS Sector Down				
YES		28.79455555	-81.32666666	5	WCDMA CELL OUT OF USE , Suppl Info: NBAP link failu				
YES		28.79455555	-81.32666666	5	Nokia UMTS Site Down				

Figure 6. Carrier maintenance logging documenting equipment failures.

4.8 Analysis of Cellular Carrier Performance Metrics

Performance metrics are utilized by cellular carrier engineering teams to determine the overall regional health of the network. Review of the cellular carrier performance metrics for the 90 days prior to critical events in the region surrounding the vicinity of the subscriber device communications sessions under analysis will aid in determining whether the cellular network was functioning nominally (Ouyang & Falla, 2010).

Key Performance Indicators (KPI) such as Session Defect Ratio, Drop Call Rate, Hand Over Success Rate, Standalone Dedicated Control Channel Success Rate, Traffic Channel Traffic Carried, and Uplink Interference help determine the Quality of Service (QoS) in a cellular carrier network. These and other factors are important to understanding the

 © 2017 ADFSL

general condition of the network within the geographic region of analysis (Andleeb & Ali, 2015). This review will aid in validating the impact of planned and unplanned maintenance events on the state of network functionality.

4.9 Research of Cellular Carrier Adherence to 3GPP/ 3GPP2/ ETSI/ IETF Operating Standards

A review should be performed of the cellular carrier's historical network infrastructure buildout and adherence to 3rd Generation Partnership Project (3GPP), 3rd Generation Partnership Project 2 (3GPP2), European Telecommunications Standards Institute (ETSI) and Internet Engineering Task Force (IETF) standards. Cellular networks are heavily integrated into the network of networks known as the Internet and utilize packet switched networking almost exclusively. Cell site to core cellular network element backhaul connectivity uses segments of the photonic backbone networks of the Internet.

The complexity of and inter-reliance upon multiple network operators necessitate that the forensic cell site analyst gains an advanced understanding of the complexity of roaming procedures between cellular carriers. Analysts should also obtain deep insight into peering and transit procedures between member networks of the Internet, the photonic backbones and packet switched network operations within the Internet, and the potential latency or failure points that arise when implementations do not comply with standards (Hussain, 2005).

Signaling System 7 (SS7) is the foundation set of telephony communication protocols developed in the 1970s. SS7 is a packet data network, used to set up and tear down phone calls, among other telephony network functions (including the transport of text messages). Signaling transport (SIGTRAN) denotes a family of protocols that improve the reliability of cellular communications delivery over packet switched networks (IETF, n.d.b), and deterministic networking (DETNET) protocols continue the reliable transport paradigm (IETF, n.d.a). The SIGTRAN and DETNET Working Groups of the IETF encompass a collection of standards that, when properly adhered to, assure delivery of control and user plane communications and content via cellular carrier network backhaul, fronthaul and crosshaul transports.

Conformance testing is addressed in multiple standards. An analyst must develop insight into how conformance testing is undertaken by a cellular carrier to ensure compliance with standards and optimization of control channel and subscriber communications flow (ETSI, 2017).

This step requires that an analyst acquire a substantial understanding of each cellular carrier's historic operational adherence to standards as well as deep insight into each carrier's design tactics, capital expenditure (CapEx) and operational expenditure (OpEx) investment, and adherence to the carrier's own network design and construction philosophy, including engineering work plan detail adherence policy enforcement. This knowledge is available through training.

4.10 Outcomes

After applying the validation and error mitigation methodology to each case, the final analysis mapping resulted in a confirmation that the analysis of the CDR/CSLI evidence was as accurate as possible, eliminating innuendo or allusion in the analytical result.

Use of the methodology in the same group of criminal and civil cases resulted in a modified final mapping analysis in approximately 40% of the cases.

The most significant outcome was that in 6% of the cases, use of the validation and error

mitigation process resulted in a modified final mapping analysis that impacted the outcome of the case in terms of the verdict of guilt or innocence in criminal cases or damages award in civil litigation.

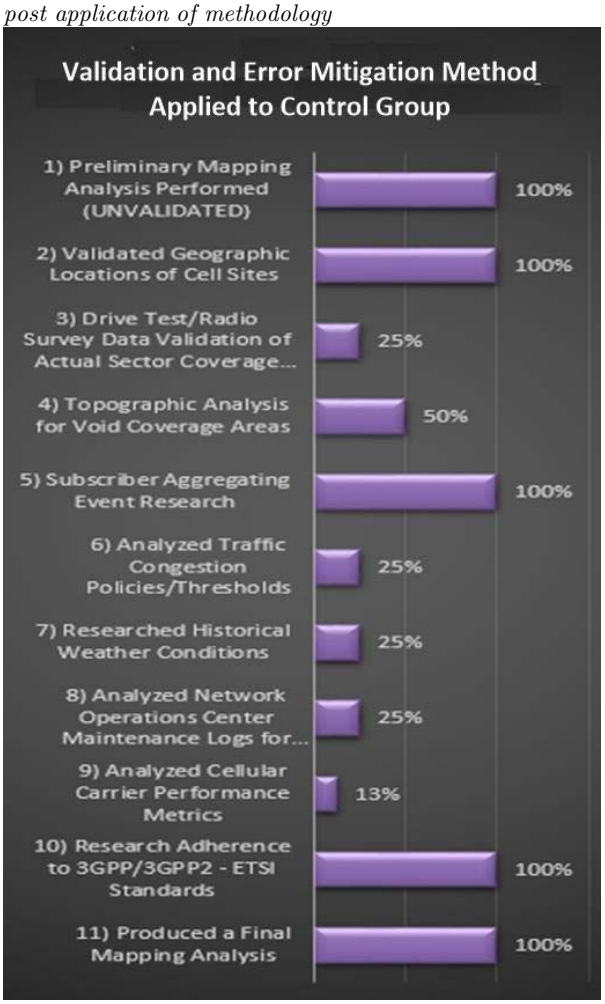
Table 3
Outcomes from application of the methodology to the Control Group

Percentage of Cases Resulting in Modified Final Mapping Analysis	40%
Percentage of Cases Verdict Impacted by Modified Final Mapping Analysis	6%

Table 4 depicts the percentage of steps completed when CDR/CSLI evidence validation and analysis error mitigation was applied to the control group of criminal and civil cases reviewed in Table 1.

Each case had a unique set of conditions and those factors, coupled with the age of the case, determined what percentage of steps were completed.

Table 4.
Rate of validation and error mitigation performed post application of methodology



 © 2017 ADFSL

5. CONCLUSIONS

This study determined the significance of performing validation of CDR/CSLI evidence and, furthermore, the importance of applying error mitigation when analyzing CDR/CSLI evidence.

Evidence validation and analysis error mitigation are critical to assuring reliable, repeatable analysis results when performing forensic cell site analysis in criminal and civil cases.

Properly applied, the discovered methodology advances the forensic cell site analysis protocol to a scientific level of certainty commensurate with key Daubert requirements. Use of the methodology was found to bring a significantly more reliable outcome to forensic cell site analysis.

The method for performing the discovered Evidence Validation and Analysis Error Mitigation Process (EVAEMP Method) may utilize the discovered steps in an either/or fashion after step 2, independently from or in addition to each other step in the process, as additional evidence (e.g., data, logging, test results, etc.) is available. The forensic cell site analysis should pursue execution of all steps whenever possible.

Although the described methodology may appear to some to be overkill, one only needs to consider that a wrongful conviction in criminal cases has a profound impact on lives of the accused or that civil case parties may be deeply affected by skewed financial awards. In 2015, the United States Patent and Trademark Office (USPTO) awarded a patent for this methodology (Minor, 2015).

Note that while analysis tools are not delineated in this paper, it should be understood that the analysis utilizes one or a combination of more than one currently known tools and methods for performing the evidence validation and analysis error mitigation process described herein, including, but not limited to: human notation, a software database tool such as spreadsheet, Sequential Query Language or Structured Query Language, signals analysis software, radio frequency propagation analysis software or other specialty database software application, mapping software, and/or topographical mapping software. One example of the use of this process was in the "Cannibal Cop" case (United States v. Valle, 2014) (Atticus, 2014).

Although several specialty software tools purport to produce accurate analysis results, including mapping generated from CDR/CSLI evidence, none of the software tools currently perform the discovered evidence validation and analysis error mitigation methodology.

The conclusion from this study is that the discovered evidence validation and analysis error mitigation process will improve the reliability and precision of forensic cell site analysis by empowering analysts to offer conclusions that qualify as scientific knowledge derived from scientific methodology, using techniques generally accepted by the scientific community that can be tested.

AUTHOR BIOGRAPHY

John B. Minor is an independent consultant with over 30 years of experience in the technology and communications field. He designed and marketed an early wireless router product under the RadlinQ corporate brand. Mr. Minor's experience and research focus has been primarily on real-time and historical cellular network subscriber records as evidence, cellular network subscriber device location services, photonic network design and implementation, and communications interception and disruption tradecraft. John was awarded patent US9113307 for the methodology conceived during this research

project. See John B. Minor, Qalypsis, and Signals Analyst.

 © 2017 ADFSL

REFERENCES

5G PPP Architecture Working Group. (2016, July). View on 5G architecture, Version 1.0. Retrieved from https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-5G-Architecture-WP-July-2016.pdf

Ali, K.A.A. (2009) Directional cell breathing – A framework for congestion control and load balancing in broadband wireless networks. Retrieved on January 30, 2017, from http://www.collectionscanada.gc.ca/obj/thesescanada/vol2/OKQ/TC-OKQ-1813.pdf

Andleeb, M., & Ali, S.A. (2015). A study on the hourly behavior of key performance indicators of global system for mobile communications, Journal of Emerging Trends in Computing and Information Sciences, 6(3). Retrieved from http://www.cisjournal.org/journalofcomputing/archive/vol6no3/vol6no3_6.pdf

Atticus, Volume 26 Number 2 (2014, Summer), Privacy on the Line, New York State Association of Criminal Defense Lawyers, pp24-35. Retrieved from https://issuu.com/nysacdl/docs/atticuswcc

Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics. National Institute of Standards and Technology (NIST) Special Publication 800-101, Revision 1. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

Bahl, P. (V.), Hajiaghayi, M.T., Jain, K., Mirrokni, S.V., Qiu, L., & Saberi, A. (2007, February). Cell breathing in wireless LANs: Algorithms and evaluation. IEEE Transactions on Mobile Computingˆ, 6(2). Retrieved from https://www.cs.utexas.edu/~lili/papers/pub/TMC2006.pdf

Blank, Aaron (2011) The Limitations and Admissibility of Using Historical Cellular Site Data to Track the

Location of a Cellular Phone, XVIII RICH. J.L. & TECH. 3. Retrieved from

http://jolt.richmond.edu/v18i1/article3.pdf.

Building Industry Consulting Service International (BICSI). (2015). Distributed antenna system (DAS) design and implementation best practices. American National Standards Institute (ANSI)/BICSI 006-2015. Retrieved on December 5, 2016, from http://www.bicsi.org/book_details.aspx?Book=BICSI-006-CM-15-v5&d=0

European Telecommunications Standards Institute (ETSI). (2017). ETSI Conformance Testing Web page. Retrieved on March 2, 2017, from http://www.etsi.org/technologies-clusters/technologies/testing

Federal Communications Commission (FCC). (n.d.). Universal licensing system Web site. Retrieved on December 5, 2016, from http://wireless.fcc.gov/uls/index.htm

Federal Communications Commission (FCC). (2001, January). Fact sheet: FCC wireless 911 requirements. Retrieved on January 25, 2017, from https://transition.fcc.gov/pshs/services/911-services/enhanced911/archives/factsheet_requirements_012001.pdf

Federal Communications Commission (FCC). (2013, October 1). Cellular Geographic

Service Area (CGSA). CFR 22.911. Retrieved from https://www.gpo.gov/fdsys/pkg/CFR-2013-title47-vol2/pdf/CFR-2013-title47-vol2-sec22-911.pdf

Federal Communications Commission (FCC). (2015, January 29). Wireless E911 location accuracy requirements. PS Docket No. 07-114. Retrieved on December 5, 2016, from https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-9A1.pdf

Federal Communications Commission (FCC). (2016, October 25). Understanding wireless telephone coverage areas. Retrieved on December 14, 2016, from https://www.fcc.gov/consumers/guides/understanding-wireless-telephone-coverage-areas

Freescale Semiconductor. (2009, February). Wireless Base Station Evolution. Networking and Multimedia Group, Document Number: WBSEVOLWP Rev. 1. Retrieved from http://www.nxp.com/assets/documents/data/en/white-papers/WBSEVOLWP.pdf

Hamid, M., & Kostanic, I. (2013). Path Loss Models for LTE and LTE-A Relay Stations. Universal Journal of Communications and Network, 1, 119-126. DOI: 10.13189/ujcn.2013.010401.

Hata, M. (1980, August). Empirical formula for propagation loss in land mobile radio services. IEEE Transactions on Vehicular Technology, 29(3), 317-325. DOI: 10.1109/T-VT.1980.23859.

Hoy, J. (2015). Forensic Radio Survey Techniques for Cell Site Analysis. Chichester, West Sussex, UK: John Wiley & Sons.

Hussain, I. (2005). Understanding high availability of IP and MPLS networks, network and service outages. Cisco Press. Retrieved on December 5, 2016, from http://www.ciscopress.com/articles/article.asp?p=361409&seqNum=4

Internet Engineering Task Force (IETF). (n.d.a). Deterministic networking Networking (detnet) Working groupGroup. (ND). Internet Engineering Task Force. Retrieved on January 15, 2017, from https://datatracker.ietf.org/wg/detnet/documents

Internet Engineering Task Force (IETF). (n.d.b)., Signaling Transport (sigtran) Working Group. Retrieved on December 14, 2016, from https://datatracker.ietf.org/wg/sigtran/documents/

Lee, William W.C. Y. (1995). cell coverage for signal and traffic In S. S. Chapman Second Edition, Mobile Cellular Telecommunications: Analog and Digital Systems, 2nd. ed. (pp.103-156). New York, NY: McGraw-Hill.

Lee, William W.C. Y. (2005). Cell coverage and antennas in Third Edition, Wireless and Cellular Telecommunications, 3rd. ed. (pp.349-424). New York, NY: McGraw-Hill.

MobileComm Professionals, Inc. (2015). Integrated approach to wireless engineering. Retrieved on February 2, 2017, from http://www.mcpsinc.com/downloads/MobileComm_Corporate_Profile.pdf

Minor, J. B. (2015). A method of validating cellular carrier records accuracy, U.S. Patent No. 9,113,307. Washington, DC: U.S. Patent and Trademark Office. Retrieved on December 5, 2016, from http://patft.uspto.gov/netacgi/nph-Parser?Sect2=PTO1&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN/9113307

 © 2017 ADFSL

National Aeronautics and Space Administration (NASA). (2016, August 10). Wave behaviors. Science Mission Directorate. Retrieved on March 2, 2017, from http://science.nasa.gov/ems/03_behaviors

O'Malley, T.A. (2011, November). Using historical cell site analysis evidence in criminal trials, The United States Attorney's Bulletin, 59(6), 16. Retrieved on December 5, 2016, from https://www.justice.gov/sites/default/files/usao/legacy/2011/11/30/usab5906.pdf

Okamura, Y., Ohmori, E., Kawano, T., & Fukuda, K. (1968, September-October). Field Strength and its Variability in VHF and UHF Land-Mobile Radio Service. Review of the Electrical Communication Laboratory, 16(9-10), 825-873.

Ouyang, Y. & Falla, M.H. (2010, March). A performance analysis for UMTS packet switched network based of multivariate KPIs., International Journal of Next-Generation Networks (IJNGN), 2(1), 80-94. Retrieved on December 5, 2016, from https://arxiv.org/ftp/arxiv/papers/1003/1003.5438.pdf

Riley v. California (2014), 134 S. Ct. 2473, 2484 (2014)

SWGDE (2017, February 21). Establishing confidence in digital forensic results by error mitigation analysis, Version 1.6, Retrieved on March 1, 2017, from https://www.swgde.org/documents/Current%20Documents/SWGDE%20Establishing%20Confidence%20in%20Digital%20Forensic%20Results%20by%20Error%20Mitigation%20Analysis

Tart, M., Brodie, I., Gleed, N., & Matthews, J. (2012). Historic cell site analysis - Overview of principles and survey methodologies. Digital Investigation, 8(3-4), 185-193. Retrieved on December 5, 2016, from https://viewfromll2.files.wordpress.com/2015/07/tart-et-al-2012.pdf

United Kingdom Accreditation Service. (2016, May). Accreditation for Forensic Cell Site Analysis – Pilot Update, ISO/IEC 17025. Retrieved on December 5, 2016, from https://www.ukas.com/news/isoiec-17025-accreditation-for-forensic-cell-site-analysis-pilot-update-may-2016/

United Kingdom Forensic Science Regulator. (2016, June 9). Codes of Practice and Conduct - Appendix: Digital Forensics - Cell Site Analysis. Retrieved on December 5, 2016, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/528197/FSR-C-135_Cell_Site_Analysis_Issue_1.pdf

United States v. Valle (2014), No. 12 Cr. 847 (PGG), 2014 WL 2980256 (S.D.N.Y. Jun. 30, 2014)

Xu, X., Broustis, I., Ge, Z., Govindan, R., Mahimkar, A., Shankaranarayanan, N.K., & Wang, J. (2015). Magus: Minimizing Cellular Service Disruption during Network Upgrades, In Proceeding of the UCLA Engineering SIGCOMM 2015 Conference Presentation. doi:10.1145/2716281.2836106

© 2017 ADFSL

 © 2017 ADFSL