Cell Phone Tracking Evidence

An excerpt from the upcoming book: Cellular Location Evidence for Legal Professionals.

By Larry E. Daniel, EnCE, DFCP, ACE, BCE, CTNS

Introduction:

We live in a world today where individuals' movements and locations are being recorded in many different ways. These movements and locations are commonly being used as evidence in civil, criminal and domestic litigation. It is of paramount importance that anyone who is involved in litigation that uses cellular location evidence understands the appropriate and inappropriate use of this type of location data.

Recent decisions by some courts have made it possible for government agencies to obtain real time tracking information using an individual's cellular phone or other cellular device without having to show probable cause or obtain a search warrant.

In most cases the government and courts continue to maintain the position that obtaining historical call detail records for an individual does not require probable cause or a warrant since the person holding the cell phone is voluntarily providing their location data to a third party, namely the cellular service provider.

However, in 2014, the U.S. Court of Appeals for the 11th circuit handed down a decision that would require law enforcement agencies to obtain a search warrant to get cell phone records that contain cell tower data.

Obtaining real time geo-location of a cell phone via the emergency 911 (E911) system may still require either a warrant or permission from the cellular carrier. Based on this author's experience, the threshold for carriers to provide this data in "exigent" circumstances is low.

What this book will cover is how the data for creating location maps for cellular phones and other cellular connected devices is collected, analyzed and presented in court.

What is Cellular Data Analysis?

Cellular data analysis is the process of collecting, analyzing and presenting the approximate location of a cell phone or other cellular device based on data obtained from the wireless company or in some rare cases, from the device itself.

There are several types of cell phone location data that can be collected and examined;

- Carrier based location data is collected by obtaining historical call detail records for a particular phone from the cellular carrier along with a listing of the cell tower locations for

that carrier. This data is then analyzed for the purpose of generally placing a cell phone in a location on a map based on cell towers used for calls and in some cases, text messages.

- Cellular data in the form of "pings", which is real time geo-location tracking of a cellular phone or other cellular device by activating the emergency 911 system (E911), which will then use either a network based or handset based method for locating the phone and will provide a location estimate generated via triangulation of the phone handset.
- Law enforcement may issue a warrant to get real-time call detail activity for a phone. This is the same type of data contained in a historical call detail record but is provided in real time.
- Cellular data may come from the device itself in the form of GPS location data either from an application running on the phone, a geo-tagged picture or some other data point.
- There is also real time location data or per call measurement data (PCMD) that can be obtained in CDMA networks. The accuracy of the GPS points for real time measurement data is not very good and should not be considered reliable for locating a phone with any precision.

What is important to understand about geo-location of a cellular phone or other cellular device is that the accuracy of the geo-location is dependent on a number of factors, not the least of which is the ability of the analyst to properly interpret and present the data and the methods used to present the information.

Throughout the remainder of this book, rather than typing out cellular phone or other cellular device, the author will use the term cell phone or handset unless there is a need to specifically describe a different type of cellular device such as an air card.

How does Cellular Data Analysis Work?

In a nutshell, cell phone location forensics involving historical call detail records generally progresses in the following way:

1. A phone number is identified as belonging to a person of interest.
2. The cellular phone company for the phone number is determined.
3. A warrant, subpoena or an administrative request is given to the cell phone company requesting the records for the phone.
4. An analyst then takes those records and plots them using mapping software such as Microsoft Street and Trips, Google Earth Professional, Microsoft Map Point, Arc GIS, or PenLink.
5. The maps will then be used to further an investigation or presented during litigation and potentially in a court of law.

The second type of data used in cellular data forensics is real time tracking of a cell phone. This is a different process from analyzing historical call detail records and has a different result since real time tracking uses the Emergency 911 (E911) system.

When the E911 system is used, the location of the phone is determined using various methods that will be described in detail later in this book. However, it is important to note that the E911 system is not infallible and does not always provide an accurate location of a cell phone.

An additional method that is sometimes used to attempt to locate a cell phone is geo-tagging of photos where the GPS location is recorded in the metadata of the image automatically by the phone. Geo-tagging is also a function of some digital cameras.

There are also applications on cell phones that can provide some information about the location of a phone based on the GPS location of wireless network routers that are recorded by the phone automatically. Again, the reliability and accuracy of this data is open to interpretation.

How is Cellular Data Analysis Used?

Cellular data analysis is used quite often in criminal cases to attempt locate a person of interest, either as they go about their criminal enterprises, or in relation to a particular incident or crime.

This type of analysis is also used in civil litigation involving vehicle accidents, property damage claims and other types of cases where the location of a particular cell phone at a particular time is of interest.

Cell phone location analysis is also used to locate missing persons who may have their phone with them when they go missing. This type of cell phone location is normally triggered through an exigent circumstances request to the cellular carrier to begin actively "pinging" the cell phone using the E911 location system to attempt to locate the phone.

What is the Basis for Cell Phone Tracking Using Call Detail Records?

The process of cell phone tracking using call detail records and tower locations is based on the concept of radio frequency reuse planning. This is the method that cellular companies use to determine when to add cell towers to an area to accommodate increases in user demand.

At the basic level a cell phone is just a two way radio. It requires one channel or frequency to transmit and one channel or frequency to receive. Cell phones can both send and receive at the same time, unlike a walkie-talkie that uses a single channel to send and receive where you have to wait your turn and push the button to send.

The reason that there is a requirement for radio frequency reuse planning is both simple and practical:

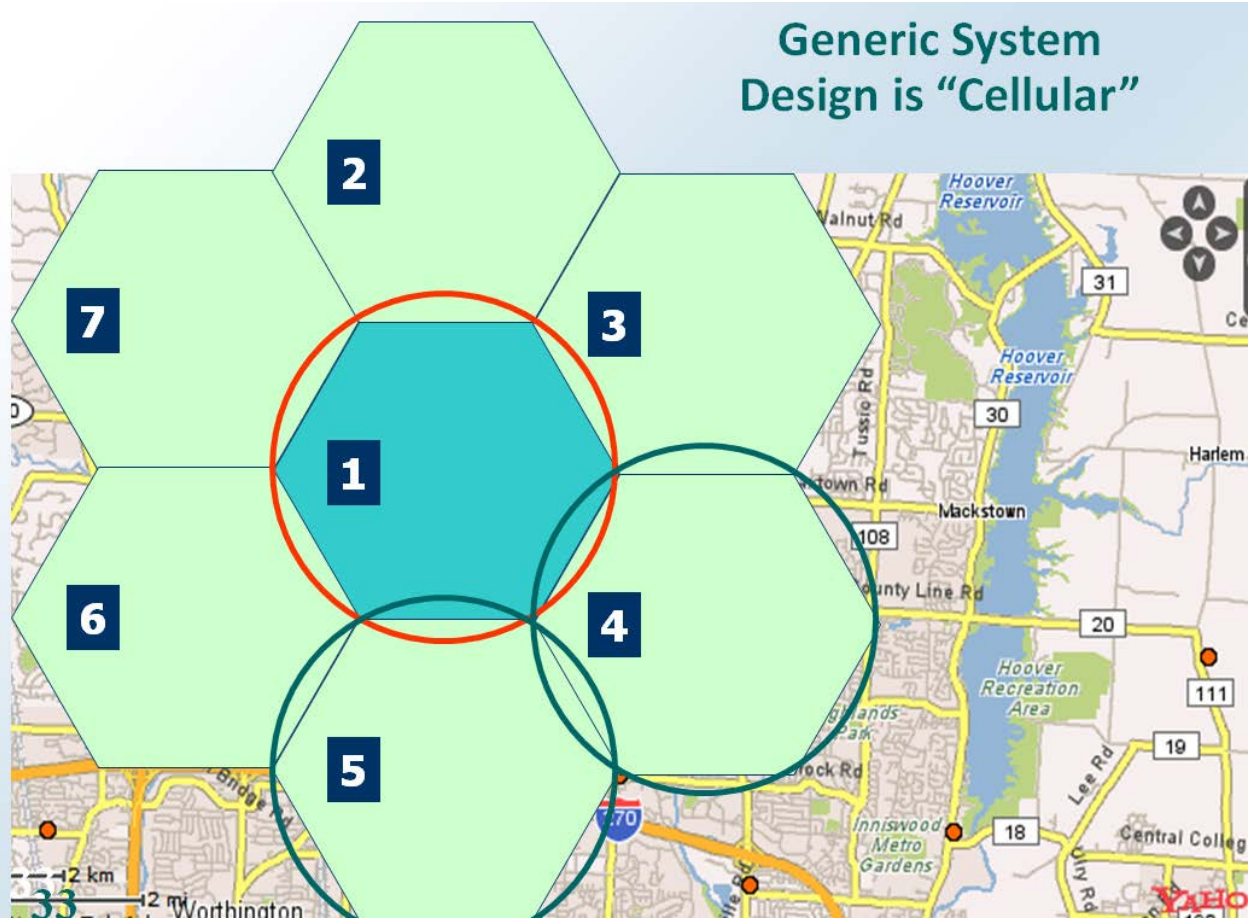
The Federal Communications Commission, (FCC) allots a limited number of radio frequencies to each wireless company. The number of frequencies available is far too small to accommodate millions of phone calls at the same time.

In order to compensate for this lack of radio frequencies, wireless companies use technology that allows them to split the frequencies into small sections so to speak, to allow more phones to use the frequencies than would be possible if a phone took up the entire radio channel.

The two primary methods for "sharing" radio channels are Time Division Multiple Access (TDMA) which is used in the Global System for Mobile Communications (GSM) network and Code Division Multiple Access (CDMA) which is used in the CDMA network. AT&T and T-Mobile use GSM wireless technology while Sprint, Verizon, Metro-PCS are use CDMA wireless technology.

For our purposes the methods used to split up radio channels is not important. What is important to understand is that the wireless system needs to support a huge amount of demand for radio channels at any given time and the wireless companies had to figure out a way to do that.

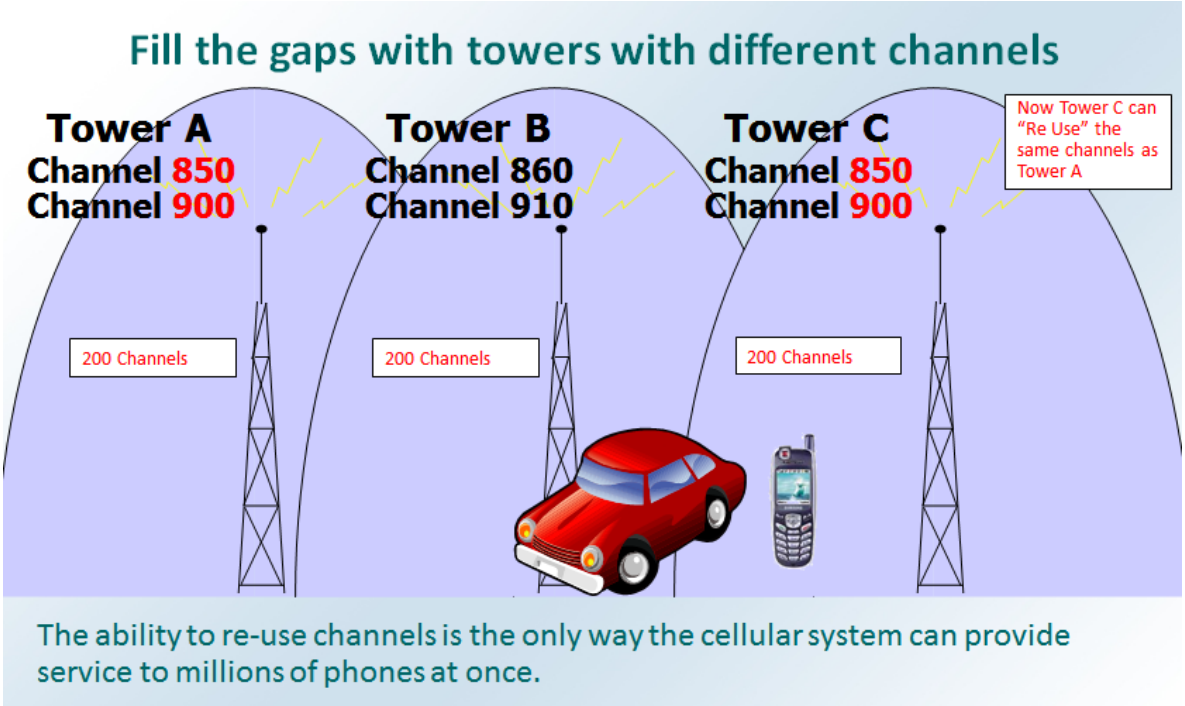
Even with the current technology for splitting up radio channels to handle more calls; that alone is not enough to cover a large number of cell phone users. To overcome that limitation, the wireless companies re-use those same radio frequencies over and over by putting them into clusters of cells, (hence the name cellular), and then separating sets of frequencies by distance so they will not interfere with each other.



The best way to be efficient and cover lots of cell phone users is to go small. In other words, each of the 7 cells shown in the image above is a cell tower or more properly a cell site. Each of the seven cell sites would have a set of radio frequencies that is different from all the other cell sites around it.

This is important since you can only have so many callers on a set of frequencies and on a single cell site due to capacity limitations.

As the number of cell phone users grows in an area, the wireless company has to figure out how to accommodate the new customers. The easiest way for the wireless company to do that is to add additional, smaller cell sites that cover a smaller geographic area. As shown in the figure above, rather than having one huge cell site represented by the red circle, it is more efficient to have seven smaller cell sites that cover more people.



It is this concept of radio frequency reuse planning that has been turned into a forensic method and is what is primarily used today in the United States for showing how a cell phone would be located in a particular area.

What about Triangulation?

The term triangulation is often misused and applied to the analysis of historical call detail records. Call detail records only contain information about a single cell tower that was used when a call was made. To triangulate the location of any phone or object you have to have a minimum of three points or more of reference.

Is There an Accurate Way to Track a Cell Phone Location?

Yes, but it can only be done in real time by using the cellular system or the cellular phone's GPS unit to track the phone.

There are basically three ways to locate a phone using technology: Handset based GPS, network based triangulation and hybrid location.

By law, cell phones are supposed to contain a GPS chip for the purpose of location the phone in an emergency. However, even today, not every phone has GPS capability.

The most accurate way to locate a phone is by activating the phone's GPS unit and allowing that to provide the phone's location back to the wireless company for transmittal to authorities. Handset based GPS location is supposed to be accurate within 50 feet.

The second way to locate a cell phone is by triangulating the phone using network based location services. What this does is calculate the position of the cell phone relative to three or more cell towers and provides that location information back to the wireless company.

The third way to locate a cell phone uses a combination of network based triangulation and local wireless router locations. However, this is not in common use at this time.

When a cell phone user calls 911 on their cell phone, the 911 operator will get a cell tower location, a sector and in some cases a GPS location for the phone.

However, these locations can be off up to several thousand feet from the actual location of the phone. In order to make sure that the GPS location is as accurate as possible, the PSAP (Public Safety Access Point) operator should manually update the location from their terminal. This manual update is called "re-bidding". Approximately 30 seconds after the 911 call connects to the PSAP, more accurate location information is available to the PSAP operator.

How Is Cellular Data Analysis Presented?

The location of a cell phone as evidence is typically presented using mapping software to plot the approximate location and movement of the phone. These maps will then show the location and times of any events of interest such as a bank robbery, shooting, arson or other type of crime or activity.

These maps may also be used to show the location of a person's phone relative to a traffic accident, or to show the movements of a person before or after a traffic accident, fire, or other property incident.

Here are some of the issues with the way cell tower tracking evidence is presented:

1. Cell phone tracking is based on an assumption that the location of the user of a cell phone can be determined merely by the location of the cell tower with which the cell phone connects when it is in use.

2. Many experts' reports are based upon the faulty assumption that a cell phone connects to the closest cell tower at the time a call is placed on a nearly 1 to 1 causal basis. While it is true that this is *normally* the case, it is not definitive enough to state that it occurs a particular percentage of the time, nor is there any way to determine this information from call detail records if the tower the phone connected to was in fact the closest tower to the phone at the time of the call. However, bear in mind that to use any cell tower, the phone must be within radio range of that tower.

3. The circles and sectors (pie wedges or centroids) drawn on maps to present this evidence are based on the idea that an "expert" can demonstrate the area covered by a cell phone by drawing circles or pie shapes on a map where the circles or pie shapes represent the approximate coverage area of a cell tower and that the cell phone will be in the area defined by the circle or pie shape. The idea is that the expert can determine the approximate coverage of a cell tower by comparing the distance between two cell towers, account for a theoretical overlap of tower coverage, and then draw a circle to represent the coverage area of each tower.

The basis for this method is that cell towers are sectorized, meaning that a cell tower has more than one antenna, that each of the antennas points in a compass direction defined in degrees, and that the analyst can determine how far those signals reach based on comparing the locations of the adjacent cellular towers.

However, data regarding the actual coverage area of the any tower at the time of the incident is *not* provided by the cellular carrier and there is no method that can be used to determine the actual coverage of a cell tower at the time of the incident based on historical call detail records. It is not possible to reliably determine the coverage area of a cell tower antenna as it relates to a particular cell phone at the time of a call simply by comparing the distance between cell towers.

4. Cell phones attempt to connect with the tower emitting the strongest and highest quality signal at a given moment, not the closest. The actual determination of which cell tower is used is complex and hinges on a multitude of factors that are not memorialized in the call detail records. There is no data provided to determine **why** that particular tower was used for the call, only that a particular tower was recorded in the call detail records as having been used at the time for the call. Many factors come into play in the selection of a tower to handle a cellular phone call, and these factors are specific to the moment in time when the call is connected. Such factors include:

a. the loading of the towers in the area, which means, which tower has the available capacity at that moment in time to handle the call
b. the health of the towers in the area at the moment in time, which means, are all towers fully functioning at the time of the call
c. line of sight to the tower from the cellular phone itself
d. radio signal interference from other cell towers in the area
e. the make and model and condition of the particular cell phone being used

f. multi-pathing which is a function of the terrain as well as both natural and man-made clutter in the area such as trees, hills, buildings and signs that cause radios waves to be either reflected or absorbed, also referred to as Rayleigh fading.
g. the strength and quality of signal from the towers around the cell phone
h. whether the phone is inside a building or outside at the time the call was recorded, where structural materials may block the signal from one tower, forcing the cell phone to select a different tower than one it would be able to connect with if it were outdoors.

"1.3. Selection of a servicing cell

If a handset is directly in front of, and with line of site to, the antenna for a given cell and with no other cells of greater or equivalent power close by, it would be unlikely to select any other cell. This means that within the service area of a given cell, there will be regions where a phone could not be reasonably expected to initiate (or respond to) a call on any other cell. The location in question could be termed as the 'dominant' region of the cell. Elsewhere, the received signal strength of other cells will be closer to or supersede that of the cell in question. The effects of clutter (either by line of sight or the effects of localized interference, or 'fast fading') will mean that there may be marked differences of signal strength over very many small distances. If there are other cells serving the area with similar signal strengths, the cell selected as serving by the handset may change frequently. This (usually much larger) region is termed a 'non-dominant' area." (Source: Journal of Digital Investigation, Volume 8, 2012, "Historical cell site analysis – Overview of principles and survey methodologies", Matthew Tart, Iain Brodie, Nicholas Gleed, James Matthews.)

8. When preparing expert maps, analysts are trained to use the following methods for determining the approximate coverage area of a cell tower antenna sector:

a. Using a standard radius of 1 mile or 3 miles projected from the tower at the center, to the edge of the coverage area or,
b. Drawing the circles on the map after plotting the locations of cell towers where the circles are drawn to overlap each other based on the distance between the cell towers.
c. The compass direction of the tower sector antenna used for a phone call.
d. The beamwidth of the radio signal projected by the sector antenna, if known.

e. Using a percentage of the distance to the next nearest cell tower sector that would overlap with the antenna being used for the phone call.

There is no factual basis for drawing coverage circles or pie shapes on a map and the cellular company does not provide such data to experts in cases. The physical location of the cell tower masts is factual in basis because cellular carriers maintain the geo-location (GPS) coordinates of cell towers and provide those GPS locations to the expert for use in his plotting of the locations of the towers. However, there are no published set of principles or methods governing the estimation of cell tower coverage based on simply drawing circles on a map where the circles overlap based on the distance from one tower to other adjacent towers, the size of the circles being determined by the distance between cell towers. In fact, the distance between cell towers on a map have no real bearing on the coverage area of the cell tower at all for the following reasons:

a. Cell towers are placed based on anticipated load, which is the maximum number of cell phone calls anticipated at peak load times for the cell tower. Thus the expected coverage area can vary widely between cell towers.
b. Cell towers are not always configured to provide the same amount of antenna power output, which determines the maximum range of the signal produced by the antennas.
c. Cell towers are placed to cover specific areas by either mechanically or electronically tilting the antennas toward the ground and are not configured to cover an area shown as a perfect circle on a map.
d. Not all tower antennas have the same beamwidth. Beamwidth is the width of the antenna signal defined in degrees. The most widely used analogy to describe beamwidth is to think of the antenna as projecting a beam of light, in the same way that a flashlight beam projects. As the beam exits the flashlight it spreads out in a pattern. In the same say that some flashlights can adjust the width of the beam of light to become wider or narrower, the antennas on a cell tower can be adjusted to project a wider or narrower beam of radio signals. In the absence of the beamwidth being provided by the carrier for each sector, it is common to "assume" a beamwidth of 120 degrees. This is an assumption and should not be allowed to be used as evidence when such data is not provided by the cellular company.
e. Each cell tower that contains sector antennas can have 2 or more of these antennas pointing in different compass directions. Each of the antennas can be configured independent of the other antennas to suit the coverage need for that particular tower. In other words, the antennas can each have a different down tilt, beamwidth and a specified direction for the antenna. While the azimuth, which is the direction the antenna points, may be provided in

the tower locations records, the actual coverage area of the sector antenna can vary widely even between sector antennas on the same tower mast.

f. In today's cellular system environment, many cell towers contain more than a single set of antennas for a carrier, making it even more difficult to use the standard three sector antenna idea to estimate the coverage area.

9. There are no principles or methods to determine the coverage area of a cell tower or cell tower sector without applying complex engineering formulae to known parameters for each cell tower sector antenna. It is not possible for anyone to reliably determine the particular coverage area of a cell tower or cell tower antenna after the fact based solely on historical cell tower location data or historical call detail records. While some analysts will perform drive tests to attempt to make their presentations more "scientific", this is not a reliable method for determining the coverage of a cell tower or sector at the time of an incident. In order for a drive test to even be remotely accurate, it would have to be done within a few hours of the incident and every environmental and engineering factor would have to be exactly the same as it was at the time of the incident. This is rarely the case for drive testing in cell phone location cases. The drive test is normally done weeks, months and even years after the fact. Additionally, the drive test would have to be done at a minimum on the same day of the week, the same time of the year in areas that have large foliage variations, at the same time of day and under the same weather and cellular traffic conditions. It is simply not possible to exactly duplicate the conditions of the cellular system at some future time when the analyst gets involved in the case.

Bear in mind that it is a common "trick" to do a drive test to provide the "actual coverage area" of a cell tower at the time a call was made, no matter how distant in time it is between the drive test and the phone call. There is never any effort made to perform that drive test over a period of time to determine or confirm its accuracy from even one day to the next. In other words, even when drive testing is presented as evidence in court, the agency doing the drive test makes no effort to validate the drive test data.

10. Cell tower coverage does not fit into neatly drawn circles or pie shapes. The inherent issue with using maps with circles and pie shapes drawn in to illustrate the approximate location of a cell phone is that it gives **the incorrect impression, bolstered by expert testimony, that the cell phone location is limited to the area defined by the circle or pie shape**. Since it is impossible to determine the distance the phone is from a cell tower at any particular time, suggesting that the phone is within an arbitrary boundary drawn on a map is inherently false. While some analysts will attempt to use per call measurement (PCM) data to show the distance of

the phone from the tower at the time the call was made, in my experience, PCM data can be off as much as four miles when actually measured against the tower locations and the PCM global positioning (GPS) coordinates provided for that particular phone call.

The image below demonstrates the difference between an idealized layout of a cell network, and the theoretical service areas of 3 sectors within the network. (Source: Journal of Digital Investigation, Volume 8, 2012, "Historical cell site analysis – Overview of principles and survey methodologies", Matthew Tart, Iain Brodie, Nicholas Gleed, James Matthews.)

186 M. Tart et al. / Digital In

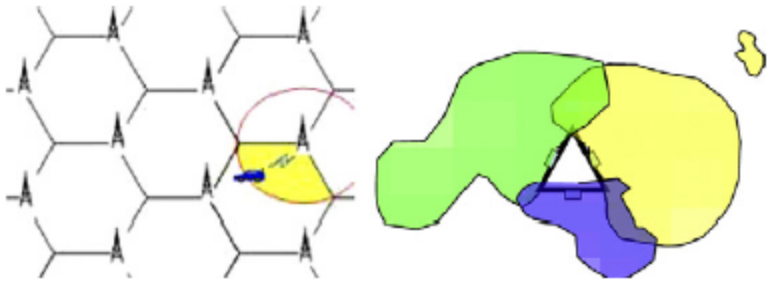


Fig. 1. Idealised layout of a network (a) and theoretical service areas of 3 sectors located on the same mast (b).

As shown in the Fig 1 above, cell sectors do not conform to a pie shape. Nor is the coverage area a circle.

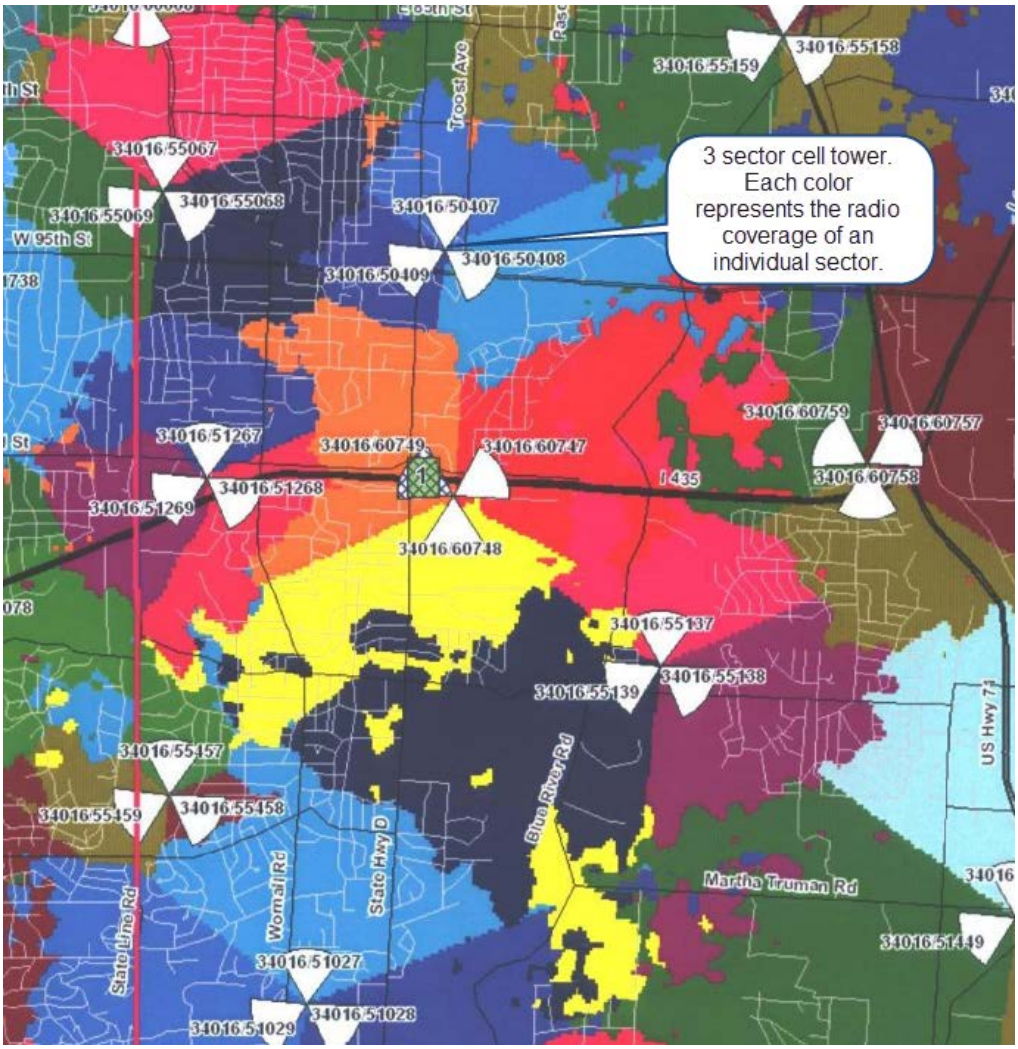
"A single cell site (usually a mast or building) can contain the hardware for several cells, which are then also known as sectors. Typically, there will be three sectors per cell site and each sector will usually point in a different direction (known as the azimuth) but this can vary, usually between one and six. The sectors will operate independently of each other, having unique Cell IDs usually related to each other and similar to the code for the covering cell site. Each sector will provide service over a particular geographical area, and this area will not be uniform (i.e. it will not be a circle, a triangle or any other regular shape); there may be many different shapes according to geography and the need of the network (e.g. long thin cells on motorways). There may also be disconnected areas of service known as hotspots." (Source: Journal of Digital Investigation, Volume 8, 2012, "Historical cell site analysis – Overview of principles and survey methodologies", Matthew Tart, Iain Brodie, Nicholas Gleed, James Matthews.)

The map below is a radio propagation prediction map from a GSM network carrier.

Note that a prediction map is based on using software to create a map of the radio coverate at ground level and takes into account ground clutter, and all of the engineering data for the cell towers.

These coverage maps are created as a normal function of the cellular companies' management of their cellular networks. Such maps can be generated either by entering the specific engineering data for all cell towers in the area and / or performing measurement tests in the field to determine the actual coverage of cellular towers in the carrier's market. Note that using propagation maps to show the coverage area of a cell phone in relation to a phone is not good science unless the propagation map is created and drive testing is performed to validate the coverage areas. And if that is to work, all the conditions mentioned above about drive testing would apply.

The purpose of including the prediction map is to show that the radio coverage of cell towers and sectors is not limited to a precise circle or pie shape and in fact, that the radio coverage varies a great deal from tower to tower and sector to sector and from day to day. While this particular area in Kansas is not going to be exactly the same as the conditions in another location, the principles of radio propagation are consistent no matter where you apply them.



The map illustrates the wide variation in radio coverage at ground level for cell tower sectors in an area.

Is cell tower tracking evidence junk science?

If your definition of junk science is presenting evidence that is supposed to be based on some scientific method or forensically sound practice, then I think it would qualify as such.

However, the reality is that generally locating a cell phone based on its historical call detail records for towers used at particular dates and times is an acceptable method for that purpose. ***From that standpoint, it is not junk science, however it is a science that is easily misinterpreted and misstated when prepared and or presented by persons not qualified to do this type of analysis.***

Is there a good use for cellular location evidence?

Properly applied and interpreted cell phone location evidence can be helpful in many cases. The issue is the overstatement of the accuracy of the phone's location.

For instance, if the phone is using a cell tower in a particular town where an incident occurred and the person who was in possession of the phone claims to have been in a different town, it is a simple presentation to dispute the person's claim.

Another good use is for tracking a phone across a distance based on cell tower usage. While the analyst cannot claim a particular road was used, the cellular evidence can certainly illustrate for a jury that the phone did in fact travel from one city to another or some area to another.

In a recent case cell tower evidence was used to show that a phone call was made near the location of the defendant's home and a subsequent call was located near his place of employment. At issue was whether or not it would be possible for the defendant to travel to another location, commit a burglary and still make it to the location near his work in the time span between the calls. By combining the cell phone locations, time estimates from Google Maps and the location of the burglary, the jury was convinced that the defendant could not have committed the burglary and still made it to the location of his work in rush hour traffic in Washington, DC.

Cellular evidence can also be used to show that a phone was near a particular area of interest with some reasonable confidence. And with more data points, this kind of analysis can be helpful in showing that even if the analyst cannot determine why the phone picked a particular tower, dozens of uses of the same tower in a short time would lend itself to showing that the phone was using that tower over other towers nearby on a consistent basis.

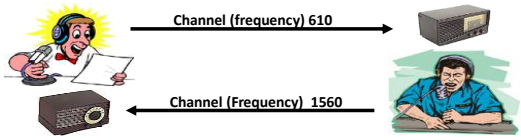
Cell Phone Location Evidence for Legal Professionals

•Larry E. Daniel
•Digital Forensic Examiner and Cellular Analyst
•EnCE, DFCP, BCE, ACE, CTNS

Copyright 2014, Guardian Digital Forensics

Cellular Telephone – Easy to Understand

- Just a two way radio
- (Talks) Sends on one channel
- (Listens) Receives on another channel
- But does both all the time.

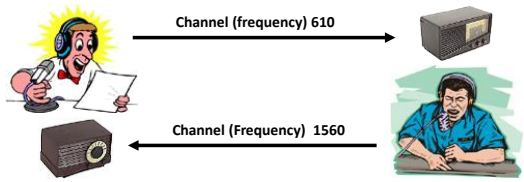


For cell phone to make or receive a call, it needs two radio channels

One channel to receive and on channel to transmit

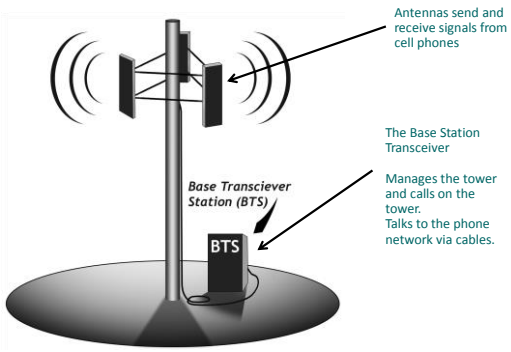
Each cellular company only has a limited number of channels to use.

Cellular Telephone – Easy to Understand



The Cellular System – Cell Towers

The Cellular System – A Cell Site



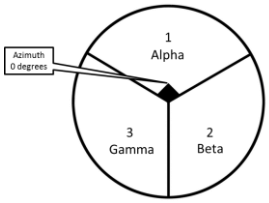
Antennas send and receive signals from cell phones

The Base Station Transceiver

Manages the tower and calls on the tower.
Talks to the phone network via cables.

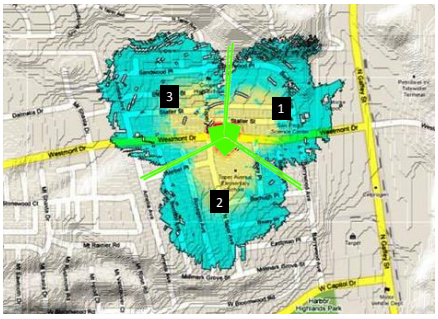
Cellular Tower Sectors

Sector Layout and Azimuth



Cell towers can have from 0 to 6 sectors.

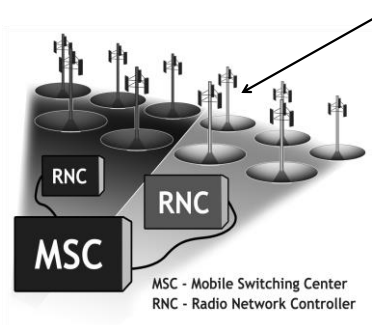
Most common is three sectors.



Example of expected 3 sector cell tower radio coverage using prediction software

Image Source: www.westsanpedro.org

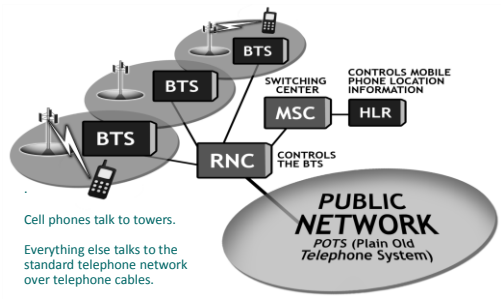
Anatomy of the Cellular System



Lots of cell sites are connected together to make up the cellular network.

Groups of cell sites talk to Radio Network Controllers via cables.

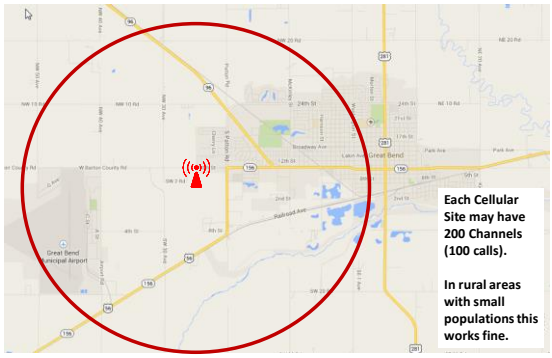
The Cellular System In a Nutshell



Cell phones talk to towers.

Everything else talks to the standard telephone network over telephone cables.

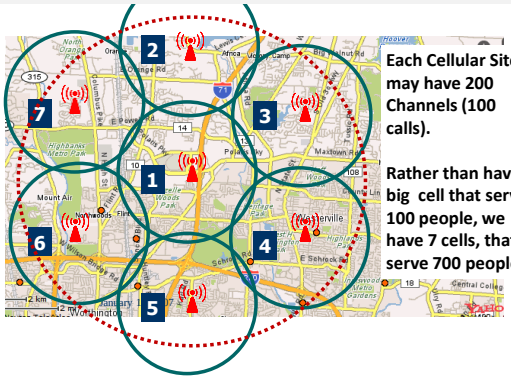
Cell coverage range is determined by customer needs.



Each Cellular Site may have 200 Channels (100 calls).

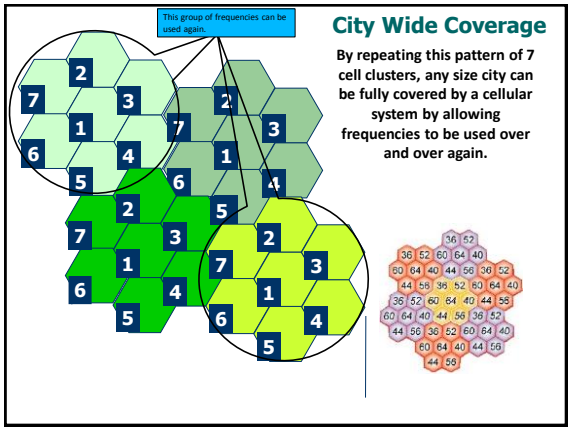
In rural areas with small populations this works fine.

As subscribers increase: Go Small to Serve More Customers

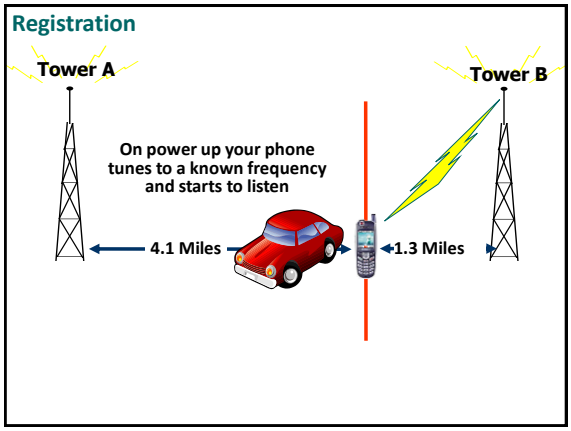


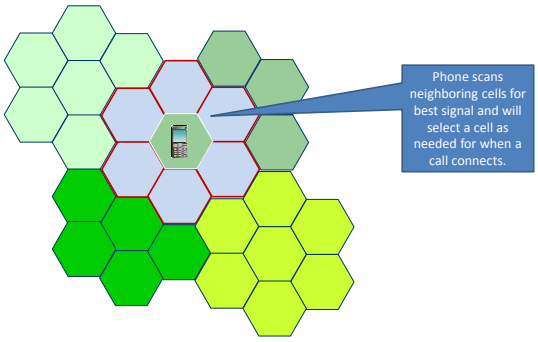
Each Cellular Site may have 200 Channels (100 calls).

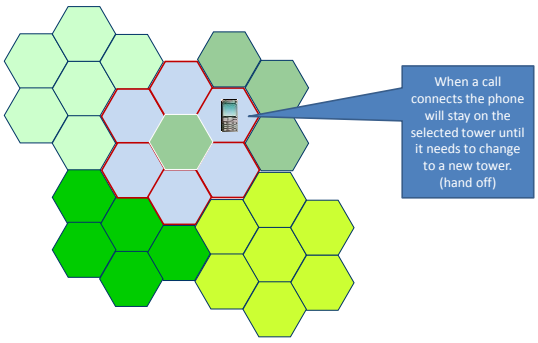
Rather than have 1 big cell that serves 100 people, we have 7 cells, that serve 700 people.



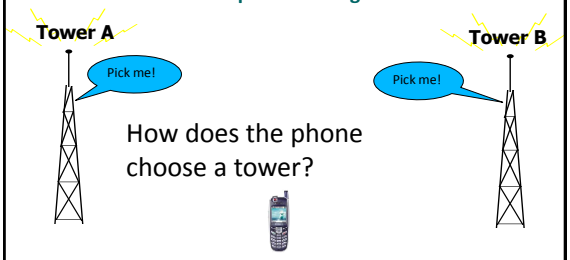
Example of expected 3 sector cell towers radio coverage using prediction software







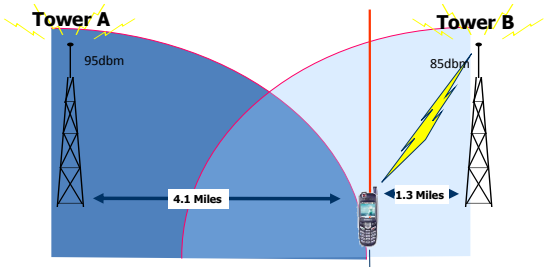
The Hook Up! – Choosing a Tower



How does the phone choose a tower?

Registration

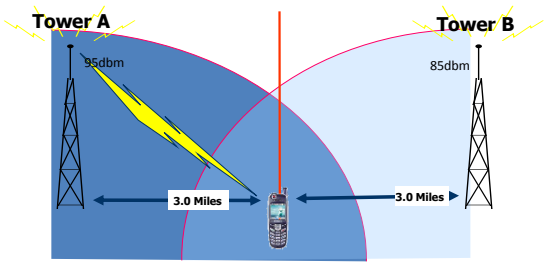
On power up the cell phone connects to the Best Signal



The closest tower will *normally* have the best signal

Registration

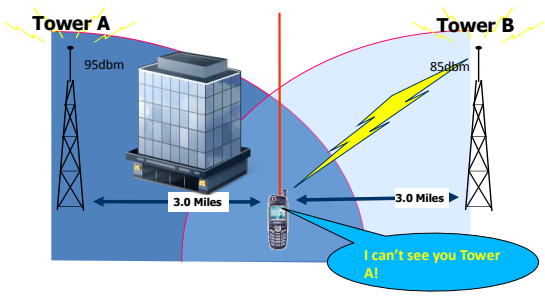
On power up the cell phone connects to the Best Signal



When equally distant from both towers,
the power output from the antennas may come into play.

Registration

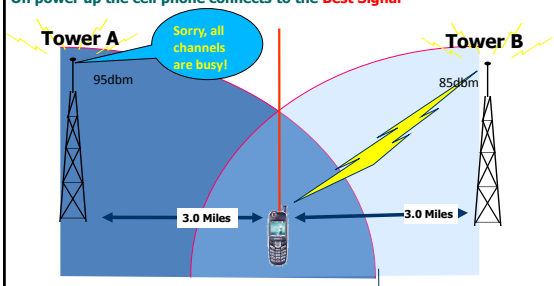
On power up the cell phone connects to the Best Signal



When equally distant from both towers, clutter may be the deciding factor.

Registration

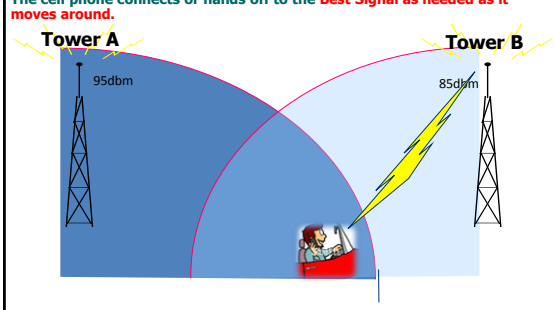
On power up the cell phone connects to the Best Signal



Channels must be available for the phone to use.

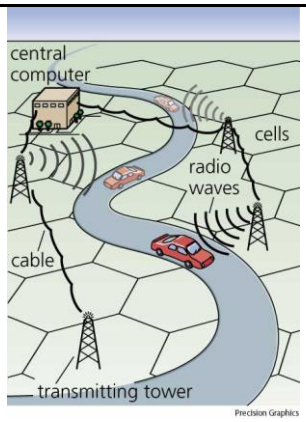
Operation

The cell phone connects or hands off to the Best Signal as needed as it moves around.



As the cell phone moves around, it will change to a new cell tower as needed to maintain the call.

This is called a hand off.



Source : images.yourdictionary.com

Call Detail Records (CDRs)

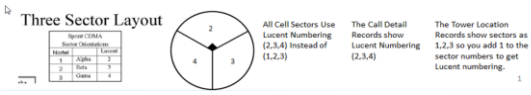
- Legal Proof of a Service Provided
- A Technical Road Map of a Call
- A Financial Transaction Record

•Used to determine the cell tower used by a phone.
•Tower Locations are then plotted on a map.

Call Detail Records (CDRs)

Network Element Name	Mobile Directory Number	Dialed Digit Number	Call Direction	Seizure DTTM	Seizure Duration	First Serving Cell Site	First Serving Cell Face	Last Serving Cell Site	Last Serving Cell Face	Calling Party Number
Richmond	(434) 390-1254		1	7/24/2008 11:55	82	266	4	266	4	
Richmond	(434) 390-1254		1	7/24/2008 12:00	115	266	4	266	4	
Richmond	(434) 390-1254		1	7/24/2008 12:23	38	266	4	266	4	
Richmond	(434) 390-1254		1	7/24/2008 12:27	58	266	4	266	4	
Chantilly	(434) 390-1254		1	7/25/2008 10:03	65	209	2	209	2	
Chantilly	(434) 390-1254		1	7/25/2008 12:08	661	209	2	209	2	
Chantilly	(434) 390-1254		1	7/25/2008 16:41	12	209	2	209	2	
Chantilly	(434) 390-1254		1	7/25/2008 16:51	3	209	2	209	2	
Chantilly	(434) 390-1254		1	7/25/2008 16:52	5	209	2	209	2	
Chantilly	(434) 390-1254		1	7/25/2008 16:54	305	209	2	209	2	
Chantilly	(434) 390-1254		1	7/25/2008 20:41	6	209	2	209	2	
Chantilly	(434) 390-1254		1	7/25/2008 20:45	5	209	2	209	2	
Chantilly	(434) 390-1254		1	7/25/2008 20:55	21	209	2	209	2	
Chantilly	(434) 390-1254		1	7/25/2008 20:58	237	209	2	209	2	
Richmond	(434) 390-1254		1	7/26/2008 7:45	13	430	4	430	4	
Richmond	(434) 390-1254		1	7/26/2008 7:46	15	301	2	301	2	
Richmond	(434) 390-1254		1	7/26/2008 9:02	92	0	0	0	0	
Richmond	(434) 390-1254		2	7/26/2008 10:10	4	0	0	0	0	
Richmond	(434) 390-1254		2	7/26/2008 10:10	4	0	0	0	0	
Richmond	(434) 390-1254		2	7/26/2008 11:11	10	0	0	0	0	
Richmond	(434) 390-1254		2	7/26/2008 11:21	4	0	0	0	0	

Note the cell face numbers are 2,3,4.



All Cell Sectors Use Lucent Numbering (2,3,4) Instead of (1,2,3)

The Call Detail Records show Lucent Numbering (2,3,4)

The Tower Location Records show sectors as 1,2,3 so you add 1 to the sector numbers to get Lucent numbering.

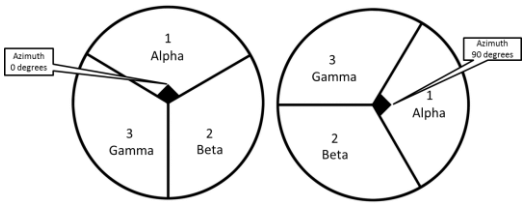
1

Cell Site Listing

Switch Name	Cell Number	% 911 Latitude Decimal (NAD83)	% 911 Longitude Decimal (NAD83)	Street Address	City	State	Zip Code	Sector	Azimuth (deg)
Richmond	266	37.3490	-78.9808	1005 West Dabourne Rd.	Farmville	VA	23901	01	50
Richmond	266	37.3490	-78.9808	1005 West Dabourne Rd.	Farmville	VA	23901	02	180
Richmond	266	37.3490	-78.9808	1005 West Dabourne Rd.	Farmville	VA	23901	03	290
Richmond	256	37.2603	-78.4955	5186 Back Hampden-Sydney Rd.	Prince Edward	VA	23901	01	60
Richmond	256	37.2603	-78.4955	5186 Back Hampden-Sydney Rd.	Prince Edward	VA	23901	02	180
Richmond	256	37.2603	-78.4955	5186 Back Hampden-Sydney Rd.	Prince Edward	VA	23901	03	300
Richmond	520	37.267663	-78.356833	798 Persimmon Tree Fork Rd.	Farmville	VA	23901	01	20
Richmond	520	37.267663	-78.356833	798 Persimmon Tree Fork Rd.	Farmville	VA	23901	02	140
Richmond	520	37.267663	-78.356833	798 Persimmon Tree Fork Rd.	Farmville	VA	23901	03	240
Richmond	520	37.267663	-78.356833	798 Persimmon Tree Fork Rd.	Farmville	VA	23901	03	260
Richmond	384	37.4543	-77.6687	7001 Winterpock Rd.	Midlothian	VA	23004	01	40
Richmond	384	37.4543	-77.6687	7001 Winterpock Rd.	Midlothian	VA	23004	02	160
Richmond	384	37.4543	-77.6687	7001 Winterpock Rd.	Midlothian	VA	23004	03	300
Richmond	444	37.45415	-77.717667	16756 Genito Road	Moseley	VA	23120	01	60
Richmond	444	37.45415	-77.717667	16756 Genito Road	Moseley	VA	23120	02	180
Richmond	444	37.45415	-77.717667	16756 Genito Road	Moseley	VA	23120	03	300
Richmond	358	37.4872	-77.5884	15201 TRUEA EA RD.	Richmond	VA	23235	01	40
Richmond	358	37.4872	-77.5884	15201 TRUEA EA RD.	Richmond	VA	23235	02	170
Richmond	358	37.4872	-77.5884	15201 TRUEA EA RD.	Richmond	VA	23235	03	300
Richmond	371	37.6658	-77.6924	1623 THRSE CHOPT RD.	Richmond	VA	23220	01	40
Richmond	371	37.6658	-77.6924	1623 THRSE CHOPT RD.	Richmond	VA	23220	02	180
Richmond	371	37.6658	-77.6924	1623 THRSE CHOPT RD.	Richmond	VA	23220	03	300
Richmond	301	37.304	-77.6862	15711 Midlothian Turnpike	Richmond	VA	23113	01	50
Richmond	301	37.304	-77.6862	15711 Midlothian Turnpike	Richmond	VA	23113	02	170
Richmond	301	37.304	-77.6862	15711 Midlothian Turnpike	Richmond	VA	23113	03	290
Richmond	430	37.463889	-77.6985	101 Coalfield Road	Midlothian	VA	23114	01	60
Richmond	430	37.463889	-77.6985	101 Coalfield Road	Midlothian	VA	23114	02	180
Richmond	430	37.463889	-77.6985	101 Coalfield Road	Midlothian	VA	23114	03	300
CHAN	151	36.435211	-77.605889	66 STORK RD.	FREDERICKSBURG	VA	22405	01	40
CHAN	151	36.435211	-77.605889	66 STORK RD.	FREDERICKSBURG	VA	22405	02	124
CHAN	151	36.435211	-77.605889	66 STORK RD.	FREDERICKSBURG	VA	22405	03	264
CHAN	206	36.47529	-77.69791	67 ROUTE 615	SUMMER DUCK	VA	23750	01	4
CHAN	206	36.47529	-77.69791	67 ROUTE 615	SUMMER DUCK	VA	23750	02	124
CHAN	206	36.47529	-77.69791	67 ROUTE 615	SUMMER DUCK	VA	23750	03	244
VNXI	209	39.199278	-78.168972	799 Fairmont Avenue	Winchester	VA	22601	01	4
VNXI	209	39.199278	-78.168972	799 Fairmont Avenue	Winchester	VA	22601	02	124
VNXI	209	39.199278	-78.168972	799 Fairmont Avenue	Winchester	VA	22601	03	244
VNXI	101	39.165825	-78.153616	1882 University Drive	Winchester	VA	22601	01	4
VNXI	101	39.165825	-78.153616	1882 University Drive	Winchester	VA	22601	02	124
VNXI	101	39.165825	-78.153616	1882 University Drive	Winchester	VA	22601	03	244
VNXI	120	39.179806	-78.085611	181 Esther Lane	Winchester	VA	22603	01	50
VNXI	120	39.179806	-78.085611	181 Esther Lane	Winchester	VA	22603	02	190
VNXI	120	39.179806	-78.085611	181 Esther Lane	Winchester	VA	22603	03	310

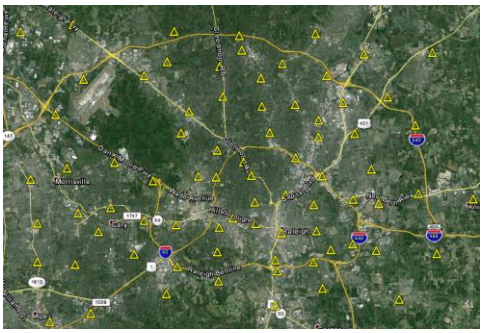
Cell Towers Are Divided Into Sectors

Some towers have no sectors and some have 2, 3, 4 or 6 sectors



Sector	Azimuth (deg)
D1	50
D2	180
D3	290
D4	60

Tower locations can be plotted on a map using the information from tower lists.



How far can a cell phone be from a tower and still make or receive a phone call?

- Assuming a perfectly flat earth, with a very tall cell tower.
- And the cell tower must be at maximum legal allowable power.
- And no other cell towers in the area…

GSM (AT&T or T-Mobile) the maximum theoretical distance is 22 miles.

CDMA (Sprint, Verizon, etc.) the maximum theoretical distance is about 35 miles.

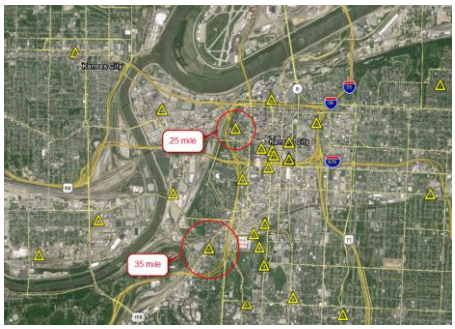
- What Limits the Distance?
  - Terrain
  - Ground clutter
  - Proximity of other cell towers. (Signal Interference)
  - Signal strength at the tower
  - The cell phone being used

How far can a cell phone be from a tower and still make or receive a phone call?

The practical connection distance for a cell phone is determined by the distance and density of other cell towers in the area for that carrier.

How far can a cell phone be from a tower and still make or receive a phone call?

The practical connection distance for a cell phone is determined by the distance and density of other cell towers in the area for that carrier.



Locating Phones – The Methods

Call Detail Records

This is the most common type of location analysis perform for cell phones.

Call detail records record the cell site that was used to connect a phone call, and in some cases, a text message.

ATT (GSM) – Provides the cell tower used for voice calls and text messages and data transmissions.
Data transmission locations is considered unreliable and should not be plotted for the analysis of a cell phone's location.

Sprint, Verizon, Metro PCS (CDMA) – Provides the cell tower used for voice calls only. They send all text messages through gateways.

Locating Phones – The Methods

Call Detail Records

Call detail records record the cell site that was used to connect a phone call, and in some cases, a text message.

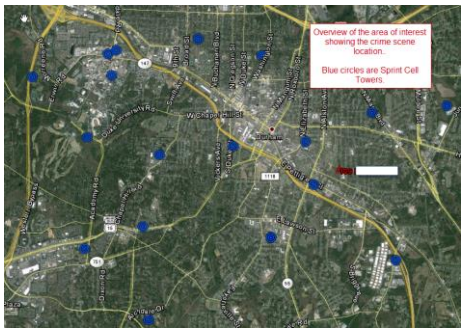
You cannot "triangulate" the location of a phone using call detail records.

The cell tower and sector (side) of the tower used by a phone can be determined in most cases (Not for Cricket)

At most you can determine the cell tower location and a general area where a phone could be, you cannot pinpoint a phone using call detail records.

Locating Phones – The Methods

Call Detail Records



Locating Phones – The Methods

Call Detail Records

Locating Phones – The Methods

Per Call Measurement Data or Reveal Records – Sprint and Verizon Only

PCMD is NOT a call detail record. Call detail records have been in use for many years and are widely accepted as being an accurate record of phone call activity.

Per Call Measurement data is used for load balancing, to determine system health and optimizing the cellular system over time. It is not used as a method for locating cell phones.

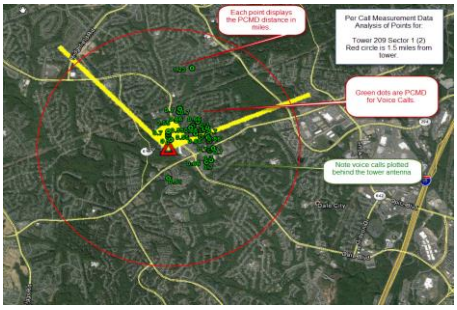
PCMD is a measurement of the distance of the phone from the tower using Round Trip Delay (RTD)

The accuracy is affected by several factors:

- Multi Pathing
- Repeaters in the network
- A phone in a multiple hand off situation.

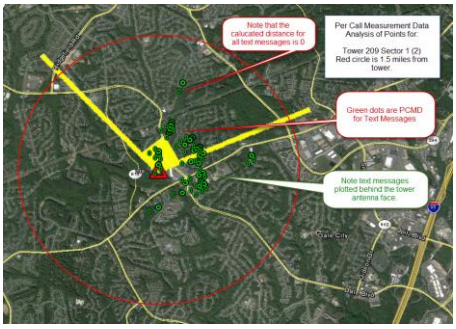
Locating Phones – The Methods

Per Call Measurement Data or Reveal Records – Sprint and Verizon Only



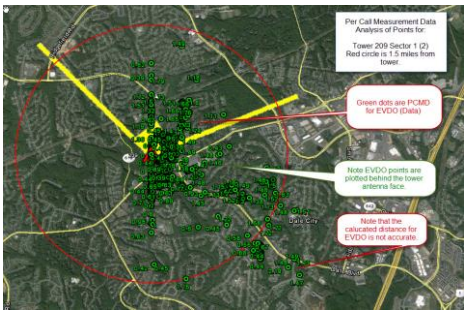
Locating Phones – The Methods

Per Call Measurement Data or Reveal Records – Sprint and Verizon Only



Locating Phones – The Methods

Per Call Measurement Data or Reveal Records – Sprint and Verizon Only



Locating Phones – The Methods

IMSI Catchers

IMSI Catchers basically trick phones into either sharing information with them or by forcing a phone to connect to them.

They can work because the encryption for 2G and 3G has been compromised for a long time.

By bypassing the encryption, an IMSI catcher can trick a phone into making a connection without authenticating properly with the cellular network.

Locating Phones – The Methods

IMSI Catchers

GSM (2G cell network) Identifiers

IMEI: International Mobile Equipment Identifier
Identifies a handset. Easily changed, illegal to do so.

IMSI: International Mobile Subscriber Identifier
Secret? Kind of.
Identifies an account - stored in SIM (Subscriber Identification Module) card.

TMSI: Temporary Mobile Subscriber Identifier
Assigned by network to prevent IMSI transmission.

Auth with IMSI, use TMSI from then on Unless, of course, the BTS asks for it.

Locating Phones – The Methods

IMSI Catchers

Tricking GSM Phones

We want to trick GSM phones into thinking that our fake base station is a genuine and better one Then he will handover to our base station

"Better" Stronger signals. Will trigger handover

"Genuine" Consistent with nearby base station information
Nearby base station will provide handover candidate base stations and frequencies. Copy that information into our fake station.

Locating Phones – The Methods

IMSI Catchers

StringRay and Other IMSI catchers

ACTIVE MODE

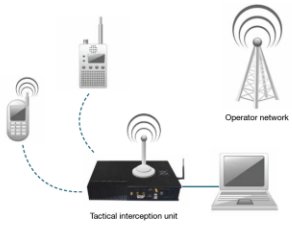
StingRay equipment operating in "active mode" will force each cellular device in a predetermined area to disconnect from its legitimate service provider cell site and establish a new connection with the attacker's StingRay system.

StingRay broadcasts a pilot signal that is stronger than the signals sent by legitimate cell sites operating in the same area, forcing connections from the cellular device in the area covered by the equipment.

Locating Phones – The Methods

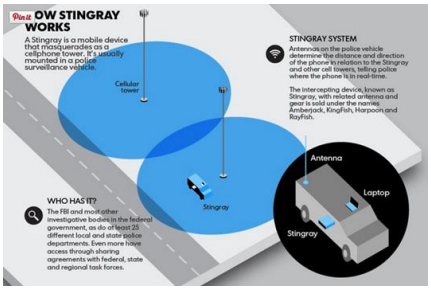
IMSI Catchers

- Embedded power amplifier
- Multi-bands and multicells (GSM, DCS and UMTS)
- Fast 2G/3G scanner
- Target identification, target localization, SMS interception, SMS sending, mobile ringing for localization purpose, 3G -> 2G switch, mobile disabling, interception of called numbers, listening of environmental sounds
- Data mining with a on-line and off-line exploitation



Locating Phones – The Methods

IMSI Catchers



Locating Phones – The Methods

Emergency 911 System

Police can activate the E911 system to actively track a phone's location in near real time.

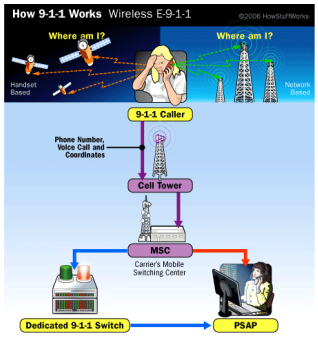
Supposed to only occur in the case of an exigent circumstance.

Threat to national security
Immediate threat to a person or persons

In reality, phone companies will start the system even without the proper paperwork.

The phone companies charge for this service.

E-911 Location



E-911 Location

- E-911 System Consists of 2 Phases
- Phase 1 and Phase 2
- Phase 2 is the best location
- Phase 2 is not always available

E-911 Location

- E-911 System Consists of 2 Phases
- Phase 1 requirement is:
  - Calling Number
  - Sector of a cell tower (hundreds of acres)

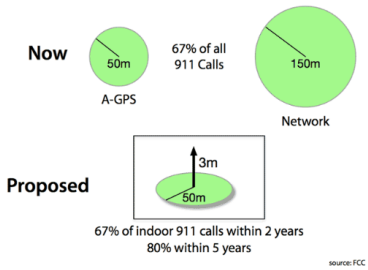
E-911 Location

- **E-911 System Consists of 2 Phases**
- **Phase 2 requirement is:**
  - **Calling Number**
  - **GPS location with 150 feet accuracy.**
    - **Must be manually updated by 911 operator to get best accuracy. This is called a "bid."**

Locating Phones – The Methods

Emergency 911 System

Wireless 911 Accuracy Requirements



Case Development

- When did the incident occur?
  - Time factor for deciding which calls to include.
- What phones were involved.
  - Defendant, co-defendants, victim or possible witnesses.
- Where did the incident occur?
  - For plotting calls versus location.

Correct Case Analysis Steps

- Perform an independent analysis of the telephony facts of the matter.
- Build a timeline
- Place calls along timeline
- Develop Map of towers for correct date of incident (Radio Frequency Plan aka Coverage Map)
- Show location and path of phones based on discovery
- Get original data sources
- AFTER analysis of phones, THEN review incident in light of facts to form opinion, rather than unscientifically using cell phone evidence to fit the desired facts of the incident.

Key Takeaways

- The analysis is only as good as the analyst
- While this seems simple, it is very complex:
  - Not just drawing towers on a map.
  - Must understand the cellular system.
  - Must understand the different carriers technology.
  - Must be able to properly interpret call detail records.
  - Must be able to explain in plain language to juries.

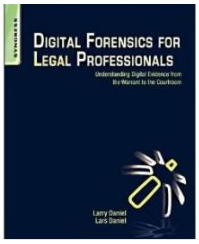
Questions?

Contact Information:

Email: larry@guardiandf.com

Web: www.guardiandf.com

Blog: www.exforensis.com

Phone: 919-868-6281

Digital Forensics for Legal Professionals
By Larry E. Daniel and Lars E. Daniel