Cellular Analysis for Legal Professionals

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

Copyright 2015, 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.

Channel (frequency) 610

Channel (Frequency) 1560
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.
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.

Base Transceiver Station (BTS)
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
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.

MSC - Mobile Switching Center
RNC - Radio Network Controller
Cell phones talk to towers.

Everything else talks to the standard telephone network over telephone cables.
Each Cellular Site may have 200 Channels (100 calls).

In rural areas with small populations this works fine.

Cell coverage range is determined by customer needs.
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.

As subscribers increase: Go Small to Serve More Customers
By repeating this pattern of 7 cell clusters, any size city can be fully covered by a cellular system by allowing frequencies to be used over and over again.
Example of expected 3 sector cell towers radio coverage using prediction software
CDMA Best Server Prediction Map using prediction software
GSM Best Server Prediction Map using prediction software
On power up your phone tunes to a known frequency and starts to listen.
Phone scans neighboring cells for best signal and will select a cell as needed for when a call connects.
When a call connects the phone will stay on the selected tower until it needs to change to a new tower. (hand off)
The Hook Up! – Choosing a Tower

Tower A

Pick me!

How does the phone choose a tower?

Pick me!

Tower B
Registration

On power up the cell phone connects to the Best Signal

The closest tower will *normally* have the best signal
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.

Sorry, all channels are busy!
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.
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)

<table>
<thead>
<tr>
<th>Network Element Name</th>
<th>Mobile Directory Number</th>
<th>Dialed Digit Number</th>
<th>Call Direction</th>
<th>Seizure Dt Tm</th>
<th>Seizure Duration</th>
<th>First Serving Cell Site</th>
<th>First Serving Cell Face</th>
<th>Last Serving Cell Site</th>
<th>Last Serving Cell Face</th>
<th>Calling Party Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Richmond</td>
<td>(434) 390-1234</td>
<td>6</td>
<td>7/24/2009 11:55</td>
<td>82</td>
<td>4</td>
<td>266</td>
<td>4</td>
<td>266</td>
<td>4</td>
<td>Richmond (434) 390-1234</td>
</tr>
<tr>
<td>Richmond</td>
<td>(434) 390-1234</td>
<td>3</td>
<td>7/24/2009 12:56</td>
<td>115</td>
<td>4</td>
<td>266</td>
<td>4</td>
<td>266</td>
<td>4</td>
<td>Richmond (434) 390-1234</td>
</tr>
<tr>
<td>Richmond</td>
<td>(434) 390-1234</td>
<td>3</td>
<td>7/24/2009 13:23</td>
<td>88</td>
<td>4</td>
<td>266</td>
<td>3</td>
<td>266</td>
<td>3</td>
<td>Richmond (434) 390-1234</td>
</tr>
<tr>
<td>Richmond</td>
<td>(434) 390-1234</td>
<td>6</td>
<td>7/24/2009 13:45</td>
<td>19</td>
<td>4</td>
<td>266</td>
<td>4</td>
<td>266</td>
<td>4</td>
<td>Richmond (434) 390-1234</td>
</tr>
<tr>
<td>Chantilly</td>
<td>(434) 390-1234</td>
<td>6</td>
<td>7/25/2009 9:02</td>
<td>90</td>
<td>4</td>
<td>209</td>
<td>3</td>
<td>209</td>
<td>3</td>
<td>Chantilly (434) 390-1234</td>
</tr>
<tr>
<td>Chantilly</td>
<td>(434) 390-1234</td>
<td>3</td>
<td>7/25/2009 19:52</td>
<td>6</td>
<td>3</td>
<td>209</td>
<td>3</td>
<td>209</td>
<td>3</td>
<td>Chantilly (434) 390-1234</td>
</tr>
<tr>
<td>Chantilly</td>
<td>(434) 390-1234</td>
<td>6</td>
<td>7/25/2009 20:45</td>
<td>48</td>
<td>3</td>
<td>209</td>
<td>3</td>
<td>209</td>
<td>3</td>
<td>Chantilly (434) 390-1234</td>
</tr>
<tr>
<td>Richmond</td>
<td>(434) 390-1234</td>
<td>6</td>
<td>7/25/2009 7:45</td>
<td>13</td>
<td>4</td>
<td>430</td>
<td>4</td>
<td>430</td>
<td>4</td>
<td>Richmond (434) 390-1234</td>
</tr>
<tr>
<td>Richmond</td>
<td>(434) 390-1234</td>
<td>3</td>
<td>7/25/2009 7:46</td>
<td>10</td>
<td>2</td>
<td>301</td>
<td>2</td>
<td>301</td>
<td>2</td>
<td>Richmond (434) 390-1234</td>
</tr>
<tr>
<td>Richmond</td>
<td>(434) 390-1234</td>
<td>5</td>
<td>7/25/2009 9:02</td>
<td>92</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Richmond (434) 390-1234</td>
</tr>
<tr>
<td>Richmond</td>
<td>(434) 390-1234</td>
<td>F</td>
<td>7/25/2009 11:03</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Richmond (434) 390-1234</td>
</tr>
<tr>
<td>Richmond</td>
<td>(434) 390-1234</td>
<td>F</td>
<td>7/25/2009 11:10</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Richmond (434) 390-1234</td>
</tr>
<tr>
<td>Richmond</td>
<td>(434) 390-1234</td>
<td>F</td>
<td>7/25/2009 11:25</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Richmond (434) 390-1234</td>
</tr>
</tbody>
</table>

Note the cell face numbers are 2,3,4.
<table>
<thead>
<tr>
<th>Switch Name</th>
<th>Cell Number</th>
<th>E-911 Latitude Degrees (NAD83)</th>
<th>E-911 Longitude Degrees (NAD83)</th>
<th>Street Address</th>
<th>City</th>
<th>State</th>
<th>Zip Code</th>
<th>Sector</th>
<th>Azimuth (deg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Richmond</td>
<td>256</td>
<td>37.3146</td>
<td>-78.3908</td>
<td>1025 West Osborne Rd.</td>
<td>Farmville</td>
<td>VA</td>
<td>23901</td>
<td>D1</td>
<td>50</td>
</tr>
<tr>
<td>Richmond</td>
<td>256</td>
<td>37.3146</td>
<td>-78.3908</td>
<td>1025 West Osborne Rd.</td>
<td>Farmville</td>
<td>VA</td>
<td>23901</td>
<td>D2</td>
<td>180</td>
</tr>
<tr>
<td>Richmond</td>
<td>256</td>
<td>37.3146</td>
<td>-78.3908</td>
<td>1025 West Osborne Rd.</td>
<td>Farmville</td>
<td>VA</td>
<td>23901</td>
<td>D3</td>
<td>290</td>
</tr>
<tr>
<td>Richmond</td>
<td>256</td>
<td>37.2633</td>
<td>-78.4555</td>
<td>5192 Back Hampden-Sydney Rd.</td>
<td>Prince Edward</td>
<td>VA</td>
<td>23901</td>
<td>D1</td>
<td>60</td>
</tr>
<tr>
<td>Richmond</td>
<td>256</td>
<td>37.2633</td>
<td>-78.4555</td>
<td>5192 Back Hampden-Sydney Rd.</td>
<td>Prince Edward</td>
<td>VA</td>
<td>23901</td>
<td>D2</td>
<td>180</td>
</tr>
<tr>
<td>Richmond</td>
<td>256</td>
<td>37.2633</td>
<td>-78.4555</td>
<td>5192 Back Hampden-Sydney Rd.</td>
<td>Prince Edward</td>
<td>VA</td>
<td>23901</td>
<td>D3</td>
<td>300</td>
</tr>
<tr>
<td>Richmond</td>
<td>520</td>
<td>37.287953</td>
<td>-78.356303</td>
<td>744 Persimmon Tree Fork Rd.</td>
<td>Farmville</td>
<td>VA</td>
<td>23901</td>
<td>D1</td>
<td>20</td>
</tr>
<tr>
<td>Richmond</td>
<td>520</td>
<td>37.287953</td>
<td>-78.356303</td>
<td>744 Persimmon Tree Fork Rd.</td>
<td>Farmville</td>
<td>VA</td>
<td>23901</td>
<td>D2</td>
<td>140</td>
</tr>
<tr>
<td>Richmond</td>
<td>520</td>
<td>37.287953</td>
<td>-78.356303</td>
<td>744 Persimmon Tree Fork Rd.</td>
<td>Farmville</td>
<td>VA</td>
<td>23901</td>
<td>D3</td>
<td>260</td>
</tr>
<tr>
<td>Richmond</td>
<td>384</td>
<td>37.4018</td>
<td>-77.6687</td>
<td>7201 Winterpock Rd.</td>
<td>Midlothian</td>
<td>VA</td>
<td>23224</td>
<td>D1</td>
<td>60</td>
</tr>
<tr>
<td>Richmond</td>
<td>384</td>
<td>37.4018</td>
<td>-77.6687</td>
<td>7201 Winterpock Rd.</td>
<td>Midlothian</td>
<td>VA</td>
<td>23224</td>
<td>D2</td>
<td>180</td>
</tr>
<tr>
<td>Richmond</td>
<td>384</td>
<td>37.4018</td>
<td>-77.6687</td>
<td>7201 Winterpock Rd.</td>
<td>Midlothian</td>
<td>VA</td>
<td>23224</td>
<td>D3</td>
<td>300</td>
</tr>
<tr>
<td>Richmond</td>
<td>444</td>
<td>37.45415</td>
<td>-77.717867</td>
<td>16716 Genito Road</td>
<td>Moseley</td>
<td>VA</td>
<td>23120</td>
<td>D1</td>
<td>60</td>
</tr>
<tr>
<td>Richmond</td>
<td>444</td>
<td>37.45415</td>
<td>-77.717867</td>
<td>16716 Genito Road</td>
<td>Moseley</td>
<td>VA</td>
<td>23120</td>
<td>D2</td>
<td>180</td>
</tr>
<tr>
<td>Richmond</td>
<td>444</td>
<td>37.45415</td>
<td>-77.717867</td>
<td>16716 Genito Road</td>
<td>Moseley</td>
<td>VA</td>
<td>23120</td>
<td>D3</td>
<td>300</td>
</tr>
<tr>
<td>Richmond</td>
<td>316</td>
<td>37.6672</td>
<td>-77.5884</td>
<td>11303 TREXLER RD</td>
<td>Richmond</td>
<td>VA</td>
<td>23230</td>
<td>D1</td>
<td>30</td>
</tr>
<tr>
<td>Richmond</td>
<td>316</td>
<td>37.6672</td>
<td>-77.5884</td>
<td>11303 TREXLER RD</td>
<td>Richmond</td>
<td>VA</td>
<td>23230</td>
<td>D2</td>
<td>145</td>
</tr>
<tr>
<td>Richmond</td>
<td>316</td>
<td>37.6672</td>
<td>-77.5884</td>
<td>11303 TREXLER RD</td>
<td>Richmond</td>
<td>VA</td>
<td>23230</td>
<td>D3</td>
<td>270</td>
</tr>
<tr>
<td>Richmond</td>
<td>371</td>
<td>37.6659</td>
<td>-77.6524</td>
<td>1623 THREE CHOPT RD.</td>
<td>Richmond</td>
<td>VA</td>
<td>23233</td>
<td>D1</td>
<td>60</td>
</tr>
<tr>
<td>Richmond</td>
<td>371</td>
<td>37.6659</td>
<td>-77.6524</td>
<td>1623 THREE CHOPT RD.</td>
<td>Richmond</td>
<td>VA</td>
<td>23233</td>
<td>D2</td>
<td>180</td>
</tr>
<tr>
<td>Richmond</td>
<td>371</td>
<td>37.6659</td>
<td>-77.6524</td>
<td>1623 THREE CHOPT RD.</td>
<td>Richmond</td>
<td>VA</td>
<td>23233</td>
<td>D3</td>
<td>300</td>
</tr>
<tr>
<td>Richmond</td>
<td>301</td>
<td>37.506</td>
<td>-77.6992</td>
<td>15711 Midlothian Tumpike</td>
<td>Richmond</td>
<td>VA</td>
<td>23113</td>
<td>D1</td>
<td>50</td>
</tr>
<tr>
<td>Richmond</td>
<td>301</td>
<td>37.506</td>
<td>-77.6992</td>
<td>15711 Midlothian Tumpike</td>
<td>Richmond</td>
<td>VA</td>
<td>23113</td>
<td>D2</td>
<td>170</td>
</tr>
<tr>
<td>Richmond</td>
<td>301</td>
<td>37.506</td>
<td>-77.6992</td>
<td>15711 Midlothian Tumpike</td>
<td>Richmond</td>
<td>VA</td>
<td>23113</td>
<td>D3</td>
<td>290</td>
</tr>
<tr>
<td>Richmond</td>
<td>430</td>
<td>37.482869</td>
<td>-77.6585</td>
<td>101 Coalfield Road</td>
<td>Midlothian</td>
<td>VA</td>
<td>23114</td>
<td>D1</td>
<td>60</td>
</tr>
<tr>
<td>Richmond</td>
<td>430</td>
<td>37.482869</td>
<td>-77.6585</td>
<td>101 Coalfield Road</td>
<td>Midlothian</td>
<td>VA</td>
<td>23114</td>
<td>D2</td>
<td>180</td>
</tr>
<tr>
<td>Richmond</td>
<td>430</td>
<td>37.482869</td>
<td>-77.6585</td>
<td>101 Coalfield Road</td>
<td>Midlothian</td>
<td>VA</td>
<td>23114</td>
<td>D3</td>
<td>300</td>
</tr>
<tr>
<td>Chan</td>
<td>151</td>
<td>38.426111</td>
<td>-77.606839</td>
<td>88 STORk RD</td>
<td>FREDERICKSBURG</td>
<td>VA</td>
<td>22406</td>
<td>D1</td>
<td>4</td>
</tr>
<tr>
<td>Chan</td>
<td>151</td>
<td>38.426111</td>
<td>-77.606839</td>
<td>88 STORk RD</td>
<td>FREDERICKSBURG</td>
<td>VA</td>
<td>22406</td>
<td>D2</td>
<td>124</td>
</tr>
<tr>
<td>Chan</td>
<td>206</td>
<td>38.47229</td>
<td>-77.69791</td>
<td>ST ROUTE 631</td>
<td>SUMMER DUCK</td>
<td>VA</td>
<td>22742</td>
<td>D1</td>
<td>4</td>
</tr>
<tr>
<td>Chan</td>
<td>206</td>
<td>38.47229</td>
<td>-77.69791</td>
<td>ST ROUTE 631</td>
<td>SUMMER DUCK</td>
<td>VA</td>
<td>22742</td>
<td>D2</td>
<td>124</td>
</tr>
<tr>
<td>Chan</td>
<td>206</td>
<td>38.47229</td>
<td>-77.69791</td>
<td>ST ROUTE 631</td>
<td>SUMMER DUCK</td>
<td>VA</td>
<td>22742</td>
<td>D3</td>
<td>244</td>
</tr>
<tr>
<td>Va10</td>
<td>209</td>
<td>39.199278</td>
<td>-78.169222</td>
<td>799 Fairmont Avenue</td>
<td>Winchester</td>
<td>VA</td>
<td>22601</td>
<td>D1</td>
<td>4</td>
</tr>
<tr>
<td>Va10</td>
<td>209</td>
<td>39.199278</td>
<td>-78.169222</td>
<td>799 Fairmont Avenue</td>
<td>Winchester</td>
<td>VA</td>
<td>22601</td>
<td>D2</td>
<td>124</td>
</tr>
<tr>
<td>Va10</td>
<td>209</td>
<td>39.199278</td>
<td>-78.169222</td>
<td>799 Fairmont Avenue</td>
<td>Winchester</td>
<td>VA</td>
<td>22601</td>
<td>D3</td>
<td>244</td>
</tr>
<tr>
<td>Va10</td>
<td>101</td>
<td>39.165625</td>
<td>-78.153636</td>
<td>1460 University Drive</td>
<td>Winchester</td>
<td>VA</td>
<td>22601</td>
<td>D1</td>
<td>4</td>
</tr>
<tr>
<td>Va10</td>
<td>101</td>
<td>39.165625</td>
<td>-78.153636</td>
<td>1460 University Drive</td>
<td>Winchester</td>
<td>VA</td>
<td>22601</td>
<td>D2</td>
<td>124</td>
</tr>
<tr>
<td>Va10</td>
<td>101</td>
<td>39.165625</td>
<td>-78.153636</td>
<td>1460 University Drive</td>
<td>Winchester</td>
<td>VA</td>
<td>22601</td>
<td>D3</td>
<td>244</td>
</tr>
<tr>
<td>Va10</td>
<td>120</td>
<td>39.179306</td>
<td>-78.081111</td>
<td>191 Eddys Lane</td>
<td>Winchester</td>
<td>VA</td>
<td>22602</td>
<td>D1</td>
<td>70</td>
</tr>
<tr>
<td>Va10</td>
<td>120</td>
<td>39.179306</td>
<td>-78.081111</td>
<td>191 Eddys Lane</td>
<td>Winchester</td>
<td>VA</td>
<td>22602</td>
<td>D2</td>
<td>190</td>
</tr>
<tr>
<td>Va10</td>
<td>120</td>
<td>39.179306</td>
<td>-78.081111</td>
<td>191 Eddys Lane</td>
<td>Winchester</td>
<td>VA</td>
<td>22602</td>
<td>D3</td>
<td>310</td>
</tr>
</tbody>
</table>
Cell Towers Are Divided Into Sectors

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

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 performed 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

Overview of the area of interest showing the crime scene location.

Blue circles are Sprint Cell Towers.
Locating Phones – The Methods

Call Detail Records

The angled shape indicates the direction and of the cell tower antenna used for the call.
Locating Phones – The Methods

Call Detail Records

- 6/18/2013 10:49:49
- 6/18/2013 10:56:03
- 6/18/2013 10:58:32

8501 phone activity uses two towers from 10:49 to 10:58
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

Each point displays the PCMD distance in miles.

Per Call Measurement Data Analysis of Points for:
Tower 209 Sector 1 (2)
Red circle is 1.5 miles from tower.

Green dots are PCMD for Voice Calls.

Note voice calls plotted behind the tower antenna.
Locating Phones – The Methods

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

Note that the calculated distance for all text messages is 0

Per Call Measurement Data Analysis of Points for:
Tower 209 Sector 1 (2)
Red circle is 1.5 miles from tower.

Green dots are PCMD for Text Messages

Note text messages plotted behind the tower antenna face.
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.


“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

Tricking GSM Phones

3G network has mended the vulnerability of GSM Users and base stations must authenticate each other.

• However, we may selectively ‘jam’ 3G phones When 3G network fails, phones will fall back to GSM mode.
Locating Phones – The Methods

IMSI Catchers

StringRay and Other IMSI catchers

Can work in Active or Passive Mode

Can intercept voice and text content.

Can localize (locate) a cellular device.

PASSIVE MODE:

Simulates the behavior of a cell tower, but does not act as a cell tower.

The activity of base station surveys allows extracting information on cell sites that includes identification numbers, signal strength, and signal coverage areas.

StingRay operates as a mobile phone and collects signals sent by cell stations near the equipment.
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

StringRay and Other IMSI catchers

ACTIVE MODE

The principal operations made by the StingRay are:

• Data Extraction from cellular devices – StingRay collects information that identifies a cellular device (i.e. IMSI, ESN) directly from it by using radio waves.
• Run Man In The Middle attacks to eavesdrop on Communications Content
• Writing metadata to the cellular device
• Denial of Service, preventing the cellular device user from placing a call or accessing data services.
• Forcing an increase in signal transmission power
• Forcing an abundance of signal transmissions
• Tracking and locating
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

**OW STINGRAY WORKS**
A Stingray is a mobile device that masquerades as a cellphone tower. It’s usually mounted in a police surveillance vehicle.

**STINGRAY SYSTEM**
Antennas on the police vehicle determine the distance and direction of the phone in relation to the Stingray and other cell towers, telling police where the phone is in real-time.

The intercepting device, known as Stingray, with related antenna and gear is sold under the names Amberjack, KingFish, Harpoon and RayFish.

**WHO HAS IT?**
The FBI and most other investigative bodies in the federal government, as do at least 25 different local and state police departments. Even more have access through sharing agreements with federal, state and regional task forces.
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

Now
- A-GPS
- 50m
- 67% of all 911 Calls

Proposed
- 3m
- 50m
- 67% of indoor 911 calls within 2 years
- 80% within 5 years

Network
- 150m

Source: FCC
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