Review of Cell Phone Technology
Types of Cell Technology

- CDMA
- GSM
- iDen
- TDMA
CDMA

• Code Division Multiple Access (CDMA) – CDMA – Code Division Multiple Access. In reality it is cdmaone (2G) or CDMA2000 (3G); however, most times it is simply referred to as CDMA. Predominantly associated with Verizon, Alltel, U.S. Cellular, Cricket and Sprint
CDMA

• cdmaone – CDMA networks using the 2nd generation (2G) of CDMA technology.
• Cdma2000 – CDMA networks using the 3rd generation (3G) of CDMA technology.
• Note: It is important to remember that there are many more overlaying technologies, LTE, Wimax and so on, but for the purposes of forensics and tracking, the networks are still considered CDMA networks. (We will learn about a few of those later.)
CDMA

- CDMA networks do “soft handoffs” which means that a CDMA device can communicate with more than one cell, and therefore it can determine the strongest signal strength before completing the handoff.
## CDMA in the United States

<table>
<thead>
<tr>
<th>Rank</th>
<th>Operator</th>
<th>Services</th>
<th>Score</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Verizon Wireless</td>
<td>CdmaOne CDMA2000 1xRTT, EV-DO Rev 0, Rev A LTE</td>
<td>107.7</td>
<td>September 2011</td>
</tr>
<tr>
<td>2</td>
<td>AT&amp;T Mobility</td>
<td>GSM, GPRS, EDGE UMTS, HSDPA, HSUPA, HSPA, HSPA+ LTE</td>
<td>100.7</td>
<td>September 2011</td>
</tr>
<tr>
<td>3</td>
<td>Sprint Nextel</td>
<td>Sprint Network CdmaOne CDMA2000 1xRTT, EV-DO Rev 0, Rev A WiMAX LTE (Planned) Nextel Network iDEN, WiDEN</td>
<td>51.1</td>
<td>February 2011</td>
</tr>
<tr>
<td>4</td>
<td>T-Mobile USA</td>
<td>UMA GSM, GPRS, EDGE UMTS, HSDPA, HSUPA, HSPA, HSPA+</td>
<td>33.71</td>
<td>September 2011</td>
</tr>
<tr>
<td>5</td>
<td>TracFone Wireless</td>
<td>CdmaOne CDMA2000 1xRTT GSM, GPRS</td>
<td>19.269</td>
<td>September 2011</td>
</tr>
<tr>
<td>6</td>
<td>Clearwire</td>
<td>WiMAX LTE (Trials)</td>
<td>9.541</td>
<td>September 2011</td>
</tr>
<tr>
<td>7</td>
<td>MetroPCS</td>
<td>CdmaOne CDMA2000 1xRTT, EV-DO Rev 0, Rev A LTE</td>
<td>9.149</td>
<td>September 2011</td>
</tr>
<tr>
<td>8</td>
<td>U.S. Cellular</td>
<td>CdmaOne CDMA2000 1xRTT, EV-DO Rev 0, Rev A LTE (Planned)</td>
<td>5.932</td>
<td>September 2011</td>
</tr>
<tr>
<td>9</td>
<td>Cricket</td>
<td>CdmaOne CDMA2000 1xRTT, EV-DO Rev 0, Rev A LTE</td>
<td>5.755</td>
<td>September 2011</td>
</tr>
<tr>
<td>10</td>
<td>Qwest Wireless</td>
<td>CdmaOne CDMA2000 1xRTT, EV-DO Rev 0, Rev A LTE</td>
<td>0.982</td>
<td>June 2010</td>
</tr>
</tbody>
</table>
CDMA

• Electronic Serial Number (ESN) - The unique identification number embedded in a wireless phone by the manufacturer. Each time a call is placed, the ESN is automatically transmitted to the base station so the wireless carrier's mobile switching office can check the call's validity. MINs and ESNs can be electronically checked to help prevent fraud.
CDMA

- Mobile Equipment Identifier (MEID) - a globally unique 56-bit identification number for a physical piece of CDMA equipment. MEID’s replaced ESN’s after the original ESN scheme being depleted in 2008.
CDMA

Be Careful

• Don’t confuse the pESN with the actual ESN.
• pESN – pseudo ESN – It is calculated using a hash based on the MEID.
• The moral of the story, make sure and get the ESN or MEID.
CDMA

• Mobile Identification Number (MIN)-Unique identifier that can be used to identify a cellular phone by the network. The MIN and ESN are both transmitted to the network to assist with authentication.

• Mobile Directory Number (MDN)- The actual number a person would dial to reach a specific phone. (This is your phone number!!)
GSM

- Global System for Mobile Communications (GSM) - GSM is a digital cellular phone technology based on TDMA that is the predominant system in Europe, the Middle East, Africa, Asia and in parts of America and Canada. First introduced in 1991, the GSM standard has been deployed at three different frequency bands: 900 MHz, 1800 MHz and 1900 MHz. GSM 1900 is primarily deployed in North America. Named after its frequency band around 900 MHz, GSM-900 has provided the basis for several other networks using GSM technology. GSM uses narrowband TDMA which allows eight simultaneous calls on the same radio frequency. Along with CDMA and TDMA it represents the second generation of wireless networks.
GSM

• GSM technology is used by
  – AT&T
  – T-Mobile
GSM

• GSM – Global System for Mobile Communication.
• Most popular in the world. Extremely popular everywhere but the United States.
• The phones contain a SIM card
• SIM – Subscriber Identity
• Module
GSM

• Subscriber Identity Module (SIM)-A small card inserted into a GSM cellular phone that contains subscriber-related data.

• Note: Some CDMA phones (Verizon, Sprint, etc) can have SIM cards. This is becoming more popular as those carriers are making world phones. However, when in the US, these phones use CDMA technology.
GSM
SIM Cards
GSM

• What can a SIM card contain?
  – Phonebook
  – Call logs
  – Speed dial
  – SMS messages
GSM

• What must a SIM card contain?
  – The IMSI

• (We will learn exactly what the IMSI is in a few minutes.)
GSM

• Integrated Circuit Card ID (ICCID) – a 19 to 20 digit serial number for a SIM card used to securely store the IMSI number for a subscriber.

• The ICCID is also called the SIM Serial Number.

• It is stamped on the SIM card.
GSM
GSM

• International Mobile Equipment Identifier (IMEI)- A unique 15-digit number that serves as the serial number of the GSM handset. The IMEI appears on the label located on the back of the phone. The IMEI is automatically transmitted by the phone when the network asks for it. A network operator might request the IMEI to determine if a device is in disrepair, stolen or to gather statistics on fraud or faults.

• Here is a good thing to know. Take your GSM phone, go to the dial pad and dial *# 06 #
GSM

• International Mobile Subscriber Identifier (IMSI)-A unique 15-digit number which designates the subscriber. This number is used for provisioning in network elements.

• It is stored on the SIM card.
GSM

IMSI

• The first 3 numbers identify the country code, for example the US is code 310.
• The next 3 number will identify the carrier code, for example AT&T code is 410. T-Mobile is code 026.
• Therefore an AT&T IMSI will begin with 310410
GSM

• Can AT&T identify the IMEI and IMSI?
  – Let’s take a look and find out:
GSM

IMEI and IMSI from an AT&T record
GSM

Note

• When the IMSI and IMEI are dependent upon each other to work properly, it is called being “locked”.

• So how do people in Europe have iPhones? They get an “unlocked” iPhone:
iDEN

• Integrated Digital Enhanced Network (IDEN) – technology developed by Motorola which uses compression and TDMA on the 25KHz frequency channel. Currently allocated by the Nextel cellular network. Source – Mobiledia.com

• Six tips:
  • Designed by Motorola
  • Used by Nextel (And other smaller companies in the US.)
  • First all Digital
  • Uses Simplex and Duplex
  • Allows for Push to talk
  • Also use SIM cards
<table>
<thead>
<tr>
<th>Company Name</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airtel Wireless Ltd.</td>
<td>Canada Calgary, Alberta, Ca</td>
</tr>
<tr>
<td>Airpeak</td>
<td>United States</td>
</tr>
<tr>
<td>ARINC</td>
<td>United States</td>
</tr>
<tr>
<td>Avantel</td>
<td>Colombia</td>
</tr>
<tr>
<td>Boost Mobile</td>
<td>United States</td>
</tr>
<tr>
<td>Bravo Telecom</td>
<td>Saudi Arabia</td>
</tr>
<tr>
<td>Procall Pvt. Ltd.</td>
<td>India</td>
</tr>
<tr>
<td>China Satcom Guomai Comm Co. Ltd.</td>
<td>China</td>
</tr>
<tr>
<td>Iconnect</td>
<td>China Hong Kong(SAR)</td>
</tr>
<tr>
<td>Connect Net</td>
<td>United States</td>
</tr>
<tr>
<td>GRID Communications</td>
<td>Singapore</td>
</tr>
<tr>
<td>Iconnect</td>
<td>Guam</td>
</tr>
<tr>
<td>Intelfon</td>
<td>El Salvador</td>
</tr>
<tr>
<td>Intelfon</td>
<td>Guatemala</td>
</tr>
<tr>
<td>Mirs</td>
<td>Israel</td>
</tr>
<tr>
<td>Monttcashire</td>
<td>Ecuador</td>
</tr>
<tr>
<td>NEXNET</td>
<td>Japan</td>
</tr>
<tr>
<td>Spacedata</td>
<td>United States</td>
</tr>
<tr>
<td>Sprint Nextel</td>
<td>United States</td>
</tr>
<tr>
<td>Nextel Argentina</td>
<td>Argentina</td>
</tr>
<tr>
<td>Nextel Brazil</td>
<td>Brazil</td>
</tr>
<tr>
<td>Nextel Chile</td>
<td>Chile</td>
</tr>
<tr>
<td>Nextel Mexico</td>
<td>Mexico</td>
</tr>
<tr>
<td>Nextel Peru</td>
<td>Peru</td>
</tr>
<tr>
<td>Vona</td>
<td>Brazil</td>
</tr>
<tr>
<td>Next Mobile</td>
<td>Philippines</td>
</tr>
<tr>
<td>Proxtel Wireless</td>
<td>Puerto Rico</td>
</tr>
<tr>
<td>Shenzhen Yunliantong Comm Service</td>
<td>China</td>
</tr>
<tr>
<td>KT Powertel</td>
<td>South Korea</td>
</tr>
<tr>
<td>SouthernLINC Wireless</td>
<td>United States</td>
</tr>
<tr>
<td>Telus</td>
<td>Canada</td>
</tr>
<tr>
<td>Inquam Telecom</td>
<td>Morocco</td>
</tr>
<tr>
<td>XPress</td>
<td>Jordan</td>
</tr>
</tbody>
</table>
TDMA

• Time Division Multiple Access (TDMA) – a technology that allows for shared access to a Frequency band. Used in cellular networks such as GSM (2G) and iDEN in the United States.

• Very important for 1 reason – It started it all. It was the first in America, used by AMPS.

• Also used in Satellite and wired communication.
TDMA

• Advanced Mobile Phone Service- An analog cellular radio standard that serves as the foundation for the U.S. cellular industry. AMPS represents the first generation of wireless networks.

• AMPS eventually became Cingular, which ultimately became AT&T.

• AMPS migrated to GSM technology.
QUICK REFERENCE TO TECHNOLOGIES USED BY MOST POPULAR CELLULAR PROVIDERS

CDMA
- Alltel
- Sprint PCS
- U.S. Cellular
- Verizon
- Cricket
- Metro PCS

GSM
- AT&T
- T-Mobile

iDEN
Nextel

(These are just guidelines. There are special circumstances where a given provider may use a different technology for certain phones)
Definitions

• Multiple Band-(To include Dual, Tri and Quad band) The ability for a cellular phone to work on more than one frequency. (IE two, three or four frequencies.)

• Cellular frequencies- The cellular frequencies can include 850, 900, 1800 and 1900 Mhz. Due to expansion, frequencies such as 750 (LTE), 2100 (WCDMA) and 2500 (WiMAX) are also being used.

• Dual Mode-The ability for some cell phones to work on both analog and digital networks.

• Attenuation-The breakdown of cellular signal due to absorption, reflection or diffusion.

• Foliage Attenuation- The breakdown of the cellular signal due to trees, shrubs and plants.
Definitions

- **North American Numbering Council (NANC)** - The FCC advisory group formerly responsible for administering the North American Numbering Plan that oversees assignment of area codes, central office codes and other numbering issues in the United States, Canada, Bermuda and part of the Caribbean. NANC administration responsibility was transferred to Lockheed Martin. Source – Mobiledia.com

- **Number Portability** - The ability to take a cellular phone number from one wireless carrier to another, even though you have to change phones and networks.

- **Communications Assistance to Law Enforcement Act (CALEA)** - A 1994 law that gave Law Enforcement the right to wiretap digital transmissions, and use surveillance technology.

- **Federal Communications Commission (FCC)** - The governing body of cellular communication in the United States.
Definitions

• Microcell-A cell having a very small coverage area, which could be as small as one floor of an office building, one part of an airline terminal, or one corner of a busy intersection. These cells are typically used when coverage and/or capacity is strained and the use of a normal sized cell would cause interference or would be impractical to install. These cells transmit with extremely low power outputs.

• Mobile Telephone Switching Office (MTSO)-The central switch that controls the entire operation of a cellular system. It is a sophisticated computer that monitors all cellular calls, tracks the location of all cellular-equipped vehicles traveling in the system, arranges handoffs, keeps track of billing information, etc.
Definitions

- **Base Station** - The central radio transmitter/receiver that maintains communications with mobile radiotelephone sets within a given range (typically a cell site).

- **Base Station Controller (BSC)** - The part of the wireless system's infrastructure that controls one or multiple cell sites' radio signals, thus reducing the load on the switch. Performs radio signal management functions for base transceiver stations, managing functions such as frequency assignment and handoff.

- **Base Transceiver Station (BTS)** - The name for the antenna and radio equipment necessary to provide wireless service in an area. Also called a base station or cell site.

- **Cell Site** - The location where the wireless antenna and network communications equipment is placed. A cell site consists of a transmitter/receiver, antenna tower, transmission radios and radio controllers. A cell site is operated by a Wireless Service Provider (WSP).
Cell Phone Signals

• And most importantly, how does the cell signal actually work?
  – Omni directional?
Cell Phone Signals

- Hexagonal?
- And the tower is not in the center of the hexagon, it is in between three hexagons.
Cell Phone Signals

• A few things to remember:
  – The coverage is NEVER perfect.
  – Range depends on:
    – Population
    – Terrain
    – Number of towers
  – And other variables.
Cell Phone Technology

• Now that we have an understanding of cell phone technology, what can we obtain from the providers
Cell Phone Technology

- Now that we have a good understanding of cell phone technology, what can we get from the Wireless Services Provider?
- Call detail logs
- Originating cell site (Latitude and Longitude)
- Terminating cell site
- Cell site sector Azimuth
- Direction of call (incoming or outgoing)
- Calling number
- Dialed number
- Call duration
- Data usage
- Location of cell towers
Cell Phone Technology

- Subscriber information (Name, address, etc)
- SMS information (Text or just sender and receiver?)
- ESN / MEID, MIN, MDN, IMEI, IMSI of target phone.
- Tower dump
- Definitions
- Reports of Lost / stolen phone
- Type of phone
- If prepaid, where purchased?
- Status
- Other phones on the same account
- Cell sites at the time of the incident (Not current)
- PCMD (Per Call Measurement Data) Maybe?
Cell Phone Technology

• When we ask for the cell site towers, what time frame do we use?
  – The time of the incident!!!!
Cell Phone Technology

• It is important to remember one thing about obtaining locations from cellular providers:
• If you are looking for Real Time, you can get locations of the phone.
• If you are asking for information in the past, Historical data, you will get Cell site and sector information. (Getting a little blurry due to PCMD)
Azimuth

- Azimuth – Angular measurement in a spherical coordinate system.