Work In Progress:
Cell Phone Forensics for Search and Rescue

George Durkee, NPS
What am I doing here? I can't play this thing! I'm a flutist, for crying-out-loud!
Cell Phone Forensics Guide for Search and Rescue

SCOPE
This operational guide is intended for use by law enforcement and associated SAR teams to understand the workflow, capabilities and limits of using cell phone technology in finding missing people. The goal has been to produce a document with enough information for effective and informed response but not too much to make it unwieldy. It is intended to be used in conjunction with the Law Enforcement Telephone Investigations Resource Guide, which gives contact numbers, procedures and exigent circumstances guidelines for law enforcement to contact cell phone carriers.

The guide will always be a work in progress. It is dependent on the input and needs of law enforcement and SAR teams and advances in technology. Send suggestions, further resource references and corrections to the correspondence author.

The latest version will be at www.napsg.org/wisar/docs
- Have him call 911 so we can get his location.
- Tell him to stay put.

Can you communicate with subject?
- Assume subject has cell phone with him
- Determine his phone number and cell provider
- Have law enforcement contact his cell provider

Call local PSAP to get his location
- Send him a text message
- Is his phone currently registered on any network?
- Call all the other carriers to determine if he's roaming on theirs

Did he make the call?
- Is his phone GPS enabled?
- PSAP can give you an accurate Lat/Long

Ask PSAP for:
- Lat/Long
- Confidence (e.g. 90%)
- Uncertainty (e.g. 1200 m)

Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he currently register (i.e., detected) on the network?
- Is his phone currently registered on any network?
- Get most recent registration data from all providers he was registered with

Still able to text him?
- Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he still talk?
- Can he tell you his Lat/Long?

Ask for his Lat/Long
- Ask all providers for:
  - Lat/long of the towers he hit
  - His nominal direction from the towers
  - If available, his distance from the tower
  - If available, his Lat/Long
  - Get data from the last several hours he was registered.

Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he tell you his Lat/Long?
- Ask for his Lat/Long

Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he still talk?
- Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he still talk?
- Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he still talk?
- Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he still talk?
- Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he still talk?
- Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he still talk?
- Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he still talk?
- Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he still talk?
- Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he still talk?
- Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he still talk?
- Can he turn on the GPS in his phone?
- Tell him to:
  - Go to http://gps.asrc.net/~admin/
  - Login using "Guest"
  - Say yes when asked if the app can turn on his GPS

Can he turn on the GPS in his phone?
Cell data from carrier is just another clue and must be carefully evaluated as to reliability. This requires knowledge of how cell phones work and how carriers analyze and derive location information.

Very likely requires working with a specialist.

Don’t be mislead by coordinates. They do not necessarily represent the accuracy of the clue.
Network based locations

Double-click to edit
Cell Phone Basics

Power On

- Turn on phone and it scans network available network sends signal to register with nearest tower (aka Ping). Phone is then registered on the network.
  - Ping is low level of data. Location potential is lower and storage varies with carrier.
  - Actual data exchange (aka Transaction) is higher level (e.g. Text, phone call or email). Better location information and retained in carrier’s records.
- Phone stays in constant contact with Tower(s). As many as 300 “I’m here” pulses per second.
- Two way feedback loop which constantly establishes ideal power level of phone for effective communication.
  - As distance from tower increases, phone uses more power.
  - When contact with tower is lost, phone goes to maximum power for about 10 minutes, then checks in every X minutes at maximum power. Rapid loss of battery.

Power Off Process

- Graceful Exit: power is purposely shut off. Phone unregisters from system; calls forwarded to Voice Mail.
  - This can even be true with battery failing.
- Sudden loss of contact with tower: calls will continue to try to contact phone for as long as 8 hours. After that, calls routed to Voice Mail.
Preplanning:
• What are the carriers in your area of responsibility?
• What are coverage areas in your area?
• Which company handles 911 source (Intrado or TCS)?

911 Contacted
• Did subject dial 911?
• Map coordinates received from e911 center. Make sure they’re not cell tower (Phase I).
• Wait for Phase II location or ask dispatch to rebid location.
  • Phase II derived from phone’s GPS and cell tower location data sent to phone to enhance speed of GPS response. If cell signal is spotty, that data may not be accurate.
  • Ask e911 what radius confidence of location is.
    • > 200 meters is likely not useful
    • If information incomplete or coordinates don’t make sense, call source: Intrado or TCS.
• Always ask for hard copy of data.

If 911 Not Contacted
• Send text to subject telling them to call 911
  • Establishes T0. Creates Transaction for better location information.
  • Consider sending link to VA SAR web location app: http://gps.asrc.net/~admin/
• Determine Carrier of subject’s phone
• Contact Carrier and start Exigent Circumstances request.
• Did phone roam onto another network?
CALL 911
e911 Call Routing
Carrier provides distance of ping based on RTD: Tower to Phone. Sometimes Segment is available. Buffered ring represents estimated confidence in distance of +/- 2,500 feet.
All the clues together leading to the find
The rescue!
Coverage Map
Avalanche in King County Washington
Cellular Forensics Team Workflow

- **Collect**
  - the *raw data* from cellular providers, PSAPs, etc

- **Analyze**
  - the *raw data* for meaningful content

- **Present**
  - the *analyzed data* in a way that can be immediately applied to the search
Three potential skill levels:

- **SAR Team Tech**
  - Understands basics of cell phones,
  - maintain coverage and tower maps,
  - can map incident information,
  - gathers necessary information during active incident.

- **Regional specialist:**
  - takes necessary information during active incident,
  - contacts cell carrier,
  - Analyzes results,
  - works with Plans to determine priority search area, additional information needed.
  - Only person who will contact cell carriers.

- **Super-geek Forensic Specialist** (e.g AFRCC, Justin Ogden).
  Others??
Basic Knowledge
Able to understand and, later, evaluate capabilities and limits of cell phone location technologies.

Team preplanning:
Develop tower and coverage maps and relationships with local cell carriers.
Know what information to gather from RP & subject’s family and friends. Have forms available to do so. (e.g. Contra Costa SAR Missing Person form).
Have a resource list of who to call and when to obtain additional technical assistance.
Familiarity with possibly helpful technologies and where to get them.
   Stingray (law enforcement only).
   SEG (Polish GSM phone locator).
   Portable cell sites.

Active Incident
Gather relevant information.
   Phone, carrier, ownership
   LKP – may need to go back several days
As soon as possible, send Text Message telling subject to contact 911.
Contact cell forensics specialist to evaluate information and talk directly with carrier.
Contact subject’s cell phone carrier and partners with towers in search area.
Work with results, cell specialist and other clues to plan segments.
Add coverage maps to IAP.
Resources

Cell Phone Forensics:
Justin Ogden, Maj CAP
Cellular Forensics Technical Specialist
Air Force Rescue Coordination Center
814-592-2340 (direct)
877-243-1215 (fax)
800-851-3051 (AFRCC console/supervisor)

PLBs:
Mike McDonald
mgmsar@comcast.net
Cell: 303-792-5256
Work: 720-847-5003

George Durkee
gedurkee@sonic.net
209-586-1651
Most Likely Area LLC

We specialize in
- analysis of historical records to determine location information
- displaying location data in easy to manage formats, such as Google Maps and Google Earth
- providing training on cellular forensics (data collection, analysis, and presentation)

MostLikelyArea.com
ASSA Mobile Sweep
GSM Only
Range: 3000 meters
Directional locator as well as voice or text communication.
Trying to Arrange Demo in fall in Yosemite
PLBs, ELTs and EPERBs
GEOSAR and LEOSAR Work Together

Path of LEO satellite.

Near instantaneous alerting BUT signal can be blocked by terrain. LEO sat provides coverage on the far side.
Doppler Derived Beacon Locations (con’t.)

- Doppler shift is also used to determine the probability of which of the two locations is more likely the “real” location. This location is designated the “A” solution and the lower probability “image” is designated the “B” solution.
- A higher “A” probability location (e.g., 90% vs. 55%) is usually more accurate.
- But even a high “A” probability (e.g., 95%) location may be incorrect.
- “Be aware that the Doppler location provided is not flawless.”
  - Direct from C/S G.007, page 1-7
Location of ELT
(It wasn’t moving)

The ELT was located inside the fuselage at about the number 4. No external antenna.

The 121.5 homing signal could not be received more than about a half mile away.
Batteries not kept in ELT/PLB DF unit.
Each unit requires 6 batteries.
20 fresh batteries stored in case.
Location Protocol Beacons

- Beacon gets its position from a Global Navigation Satellite System (GNSS) i.e. GPS, Galileo, GLONASS
- The beacon’s nav system may be internal to the beacon or an external nav device connected to the beacon
- As with all nav system devices, the calculated location is only as good as the nav signal being received
- Position accuracy is not the 10 meter or better accuracy users expect from handheld and mobile nav devices
  - Limitation of how the system processes the coordinates
- Location information is not provided in about 30% of the signals from location protocol beacons.
- Location protocol is an optional part of the C-S system
Distress Beacon Encoded Messages

- Contain information about the beacon and for location protocol beacons, the encoded position in latitude and longitude
  - Unique 15 digit hexadecimal identifier for every beacon
  - Encoded position comes from a global navigation device either internal to the beacon or an external one connected to the beacon
- Local User Terminals (LUT) decode the messages and compute Doppler locations for LEOSAR alerts
- LUTs send the data to the Mission Control Centers (MCC) which sort and match the data and check the beacon ID to a beacon registration database
  - The registration database contains beacon owner information
- The MCCs send alert messages with the data to the Rescue Coordination Centers (RCC)
Sample Alert (SIT) Message

-----------

Date: 10/09/2011 23:29
To: KROGCTEY
From: KZDZSLA
Subject: /00642 00000/3660/11 282 2323 /160/3668

406 BEACON
-----------

DD KROGCTEY
092323 KZDZSLA
/00642 00000/3660/11 282 2323 /160/3668

406 BEACON UNLOCATED FIRST ALERT
-----------

BEACON ID: 2DC6E E2166 9FBFF  SITE ID: 20234
-----------

DETECTION TIME AND POSITIONS FOR THE BEACON
-----------

PROB SOL LATITUDE LONGITUDE DETECT TIME SAT SOURCE SRR /BUFFER
N/A N/A N/A 03 2322 OCT 013 SMCC AFNOC
-----------

BEACON ID CONTAINS THE FOLLOWING ENCODED INFORMATION
-----------

COUNTRY: USA  CRAFT ID:
MID CODE: 366  MOUNTING: 121.5 MHz
MANUFACTURER: CSTA# 156  MODEL:
SERIAL NUM: 4276  BEACON TYPE: FLB SERIAL (STANDARD)
-----------

USMCC REGISTRATION DATABASE INFORMATION  -----------

OWNER:  USA  TEL 1:  
  TEL 2:  
  TEL 3:  
  TEL 4:  
EMAIL:  

CONTACTS:
  TEL 1:  
  TEL 2:  
  TEL 3:  
  TEL 4:  

-----------

Message sections will be explained in slides that follow.
Alert Message Header

Header information - format is the same for all SIT messages

Message date
Date: 10/09/2011 23:23
To: KRCCYCYX
From: KZDCZSZA
Subject: /00642 00000/3660/11 282 2323 /160/366S

------------- 406 BEACON
Julian day  SIT number

Sequential message number for all messages, not just this beacon

Information is repeated in this area

Full SIT message title

------------- 406 BEACON UNLOCATED FIRST ALERT
Raw Data:

**Network based locations**

- May be available in real time or as historical data.
- Accuracy of each transaction is paramount to understanding its importance to the search.
- If someone can’t give you the accuracy data - proceed with caution!
- These locations are *tempting* to use because they plot so easily in Google Earth.

- Based on Round Trip Distance (RTD) between phone and tower. Large potential error in determining distance and direction.
Raw Data:

**Sector information**

- Sectors utilize directional antennas to maximize coverage in a given direction from a tower.
- 3 sectors per tower are common, but can vary from 1 to more than 6.
- Sectors provide a way to help understand what side of a tower a phone was for a given transaction.
What carrier does the phone number belong to?

Step 1: Check with Neustar at 571-434-5781. My agency’s PIN: ____________________________

(request a PIN here http://www.npac.com/the-npac/access/law-enforcement-agencies-psaps/ivr-system)

Step 2: If Neustar says “Not Ported”, check NPA-NXX: https://www.telcodata.us/search-area-code-exchange-detail

Did the objective dial 911?

<table>
<thead>
<tr>
<th>What PSAP took the original call?</th>
<th>What 911 information did they provide? (Phase 1 or 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remember, a Phase 2 location should have a latitude, longitude and a confidence factor (or radius)</td>
<td></td>
</tr>
</tbody>
</table>

If information is missing, call Intrado (800-514-1851) or TCS (800-959-3749)

<table>
<thead>
<tr>
<th>Carrier</th>
<th>Intrado</th>
<th>TCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT&amp;T</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sprint</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T-Mobile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>US Cellular</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verizon</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Carriers that may roam on each other’s network

<table>
<thead>
<tr>
<th>GSM</th>
<th>AT&amp;T, T-Mobile, International Phones</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDMA</td>
<td>Sprint, Verizon, US Cellular</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Carrier</th>
<th>Phone Number</th>
<th>Records to request (request all records be emailed instead of faxed)</th>
</tr>
</thead>
</table>
| AT&T    | 800-635-6840 | • Call detail records with cell site location for Voice, Data and SMS
|         |              | • NELOS Report
|         |              | • Real time location and location updates |
| T-Mobile| 973-292-8911 | • Call detail records with cell sites for Voice, SMS, and Data
|         |              | • Real time location and location updates |
| Sprint  | 888-877-7330 | • Call detail records with cell sites for Voice, SMS, and Data
|         |              | • Per Call Measurement Data (PCMD) |
|         |              | • Real time location and location updates |
| US Cellular | 630-875-8270 | • Call detail records with cell sites for Voice, SMS, and Data |
| Verizon | 800-451-5242 | • Call Detail Records
|         |              | • SMS Detail Records
|         |              | • Tower, Sector, Distance information |