Work In Progress:
Cell Phone Forensics for Search and Rescue
What am I doing here? I can't play this thing! I'm a flutist, for crying-out-loud!
Cell Phone Docs

SAR_GIS10 Folder on Google Drive:

https://drive.google.com/drive/folders/12Ah_2IqueKt-TSiAa-uAXcb9VQX_fpOP?usp=sharing

- Operational Guide to Cell Phones for SAR_DurkeeG_20160213_v2-7.docx
- CellForensicsWorkflow_20180418__DurkeeG.docx
- PLB SEKI_DurkeeG.docx
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. Tower sets 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.
Cell data from a 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.

There are limitations inherent in the data and locations that a cell carrier provides. Understanding these limitations are critical to evaluating such clues.

Analysis is best done in two stages:
• Initial contact with subject’s cell phone carrier
• Further analysis by Cell Forensics team at AFRCC.

Don’t be mislead by coordinates. They do not necessarily represent the accuracy of the clue.
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!
- 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

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)

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 tell you his Lat/Long?

Ask for his Lat/Long

His Lat/Long will be embedded in the metadata

Have him take a photo of the sole of his shoe and send it to you

Get most recent registration data from all providers he was registered with

Can he currently register (i.e., detected) on the network?

Is his phone currently registered on any network?

Call all the other carriers to determine if he's roaming on theirs

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.

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 (i.e., detected) on the network?

Determine his phone number and cell provider

Call law enforcement to contact his cell provider

Is his phone currently registered (i.e., detected) on the network?

Get most recent registration data from all providers he was registered with

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?
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

Link to Article on AFRCC/CAP Cell Forensics Team

October 04, 2018
CAP Sets Modern Saves Record -- 155 -- for Fiscal 2018; 95% Credited to Cell Phone Team
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
Future
(~2015)

• Common reporting app useful for multiple emergencies and incidents (e.g. take geotagged photo, send to agency to show downed poles, house damage etc.

• Receiver capable of finding phone signal, either by targeted phone # (preferred) or find active phones in area (car over side).

• Google maps w/better base maps and symbology
A Good Day for SAR: Yosemite Ranger Dave Pope with Child, Merced River, Yosemite National Park
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
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
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)
Map of ELT Example

- 10 km radius
- 5 km radius
- Actual
- Comp-2-3
- Comp-1-2
- Hit-1A
- Hit-2A
- Hit-4A
- Hit-3B

See NOTAMs/Directory for Class D/E (sfc) off hrs

CASSE
Z60/2P

CAUTION
HIGH-PERFORMANCE MILITARY AIRCRAFT OPERATING AT ALTITUDES BELOW 7500' MSL
Take Home message with PLB’s & Cell Phones:

Do NOT commit resources – especially in dangerous conditions – based only on Cell Phone or PLB clues!