George Durkee gedurkee@sonic.net • 209-591-8802
Columbia College: GIS & Emergency Services v 1.0 9/12/2016

Contents

Obtaining Cell Phone Locations for Search and Rescue

Cell phone forensics is increasingly important in locating a subject who is believed to have a cell phone. Common situations are:

I. Subject is reported overdue. SAR may or may not even have a good LKP. It is not known if the person has a cell phone. (*See Page 3*)
II. Subject is reported overdue and is known to have a cell phone. (*See Page 3*)
III. Subject calls a friend or SAR – but not 911 – and reports that he or she is lost or injured. (*See Page 5*)
IV. Subject calls 911 and reports that he or she needs help. (Workflow incorporated in III: *See Page 5*)

Each of these invokes a different workflow to follow to find the subject's location. It is critical that obtaining the subject's cell information be done very early in the search. Not only is the person's cell likely running out of battery, but some records are only kept by the cell carrier for a short period of time.

Sometimes SAR managers or law enforcement don't put a high priority on obtaining cell location data because too much time has passed for the cell phone to be active. In some cases, cell records are not sought because the subject is thought to be in a cell dead zone. While these concerns may be true, important location information, such as probability of area, can quite often be derived from data before the phone went dead. Coverage may not be enough for a text or voice call, but there may be areas where a brief tower to phone "ping" can take place – a potentially important clue. In addition, data history can indicate where a person might have visited enroute, suggesting the possibility of witnesses. There may also be text messages or contact with social media that might lead to other important clues.

If the search hasn't been started until several days after a LKP, the carrier may require a search warrant for data beyond the 48 hours often interpreted as the limit of an exigent circumstances request. This will take more time and is another critical reason to request cell carrier data immediately upon the report of a missing person.

Situation Types and Suggested Workflows

I. Subject is reported overdue. SAR may or may not have a relevant LKP. It is not known whether the person has a cell phone.

1. Contact friends and family for the person's cell phone number.
2. Determine the cell carrier the subject used (e.g. Verizon, AT&T etc.). If you have the cell number, there are online resources to find the carrier the number is assigned to. (See Resource Contacts AFRCC). Then follow the workflow outlined next:

II. Subject is reported overdue and is known to have a cell phone.

1. Determine the cell phone's carrier. This is who law enforcement will contact to obtain location information.
   a) This can be done in several ways. The best is using the carrier lookup tool provided by Justin Ogden's *Most Likely Area* websiste (https://mla.tools/). If you call the carrier(s) in your area of responsibility, it's likely they'll look it up for you and direct you to the owner's correct carrier if it's not them.
2. Call the subject's phone number. Log the call with time and the number of rings before voicemail comes on (this helps determine how long the cell has been off the cell network and establishes a time stamp for later cell forensics analysis). Leave a message to call 911 and be certain to state the name of your county in case the subject calls 911 and the call is routed to a PSAP in an adjoining county.
3. Send text to subject using location app at login.cellgps.org with text of: "*This is [County] Sheriff. A search has started for you. Tap link below and then tap "Allow" to send us your location. THEN call 911.*" The text will stay in queue and can be delivered even if voice contact is not possible. Delivery will also be registered on the network and likely provide a probability of area clue. See details for this app in *Section 2: Using login.cellgps.org.*
4. Request records from carrier. This can only be done by law enforcement. The carrier will immediately ask for your name and agency. Ideally you should know the subject's carrier, but if you call the one that handles towers in your area, they can look up subject's phone and direct you to right one (usually...).

   Although a non-LE SAR manager cannot directly make the request nor receive the subject's cell data, it's important that SAR people know the limitations of how a cell carrier interprets the location data they give you and the importance of requesting further analysis by AFRCC or other trained cell forensics analyst. An explanation of the process is described in *Section 3: Brief Introduction to Advanced Forensic Analysis* and resources to contact in *Resource Contacts).*

5. They'll fax you an Exigent Circumstances form to request the phone records.
   a. On the Exigent form (LE only) request two days prior to LKP and ask for text messages. Asking for days prior to LKP might show relevant texts on subject's intention or contact with social media (e.g. Facebook).
   b. Ask the carrier security tech if there's any cell activity shown. If so, ask for the records in the original.
   c. Carrier will send records only to an agency email address. **All files will be encrypted.** One of the files will be an html file that establishes a password with the encryption service, allowing the other files to be unencrypted and opened.
      i. The first thing the receiver has to do, then, is open the ***securedoc..... html*** (or similar) file, register with their service and create a password. Once registered, you can unencrypt the files with that password.

6. Either ask for continued records to be sent to your dispatch center from the cell carrier or just phone in once or twice per day. They can verbally tell you if there's been activity. If there is, you might have to do another exigent circumstances form. Some carriers will just let you amend the existing form.
7. If there is cell activity in the time frame you're interested in, request a case with AFRCC *(See **Resource Contacts**)*. AFRCC works primarily with aircraft searches but will consider – and likely support – ground searches. AFRCC has the ability to carry out an analysis beyond what the cell carrier is able to provide (See Section 3: Brief Introduction to AFRCC Forensic Analysis techniques). They cannot, though, make the initial request for information from the cell carrier.
   a. Unzip and unencrypt all files, then send to AFRCC once they respond with direct contact information.
   b. Meanwhile, you can be looking at texts themselves, if there are any. AFRCC contact can guide you through what to look for or they'll just do it.
      i. Be checking cellgps.org occasionally to see if there's a reply. The same type of app on MLA Tools will automatically email you if a reply is made.
      ii. Continue to check for cell activity with the carrier. It may be that the subject comes out of a dead zone and establishes brief contact with the tower, perhaps even receiving text or voice ability (For instance, see Figure 6).

III. Subject calls a friend or SAR – but not 911 – and reports that he or she needs help.

Note: *The apps described below will not work with flip phones.*

1. Get their phone number – recontact if necessary – tell them to expect a text message from the *cellgps* app, to tap the link then then tap **Allow** to provide additional location information. Then tell the subject to hang up and immediately dial 911.
   a. Follow detailed instruction in *Section 2: Using login.cellgps.org* for details on how to do this.
2. Contact your 911 PSAP and tell them to expect the call. Also tell them if the call doesn't come through, to check with any adjoining PSAPs in case the call was mistakenly routed elsewhere.
3. After 911 is contacted by subject:
   a. From PSAP, obtain coordinate information AND accuracy estimate. Ask if the coordinate is "Phase 1" (cell tower location) or "Phase 2" (caller's possible location). If the accuracy value is over 200 meters, ask the PSAP to "re-bid" the 911 call in order to get a better position.
   b. Evaluate and prioritize the 911 clue: Map the location. It often happens that the first coordinate acquisition is on the cell tower being used.
      a. Practice and become familiar with several online or desktop mapping software. In addition to Google Earth, also try *GMap4*: *Online Mapping software that can search on any coordinate format.* **Double check your coordinate type!** (See *Mapping and Coordinate Exercise*).
   c. Does the mapped location make sense when considered with the other clues you have?
   d. Pass the phone number, location information and accuracy estimate verbally and by hardcopy to SAR IC. Identify the location and accuracy data as coming from the PSAP.
   e. Even when subject's location coordinates are provided by PSAP, a Best Practice includes double checking subject's location using text location app or by direct contact and talking the subject through using a coordinate app *(IV, step 4 directly below*).

IV. Subject calls 911 and reports that he or she is lost or injured.

Steps to verify subject's location continued from PSAP-obtained location.

4. **If the subject is in direct voice contact with SAR** or, after they've contacted 911 PSAP, voice or text contact should be reestablished by SAR, the following steps should be taken:
   a. As presented in detail in *Section 2: Using login.cellgps.org*, tell the subject to expect a text message and to tap the link in reply.

b. If you have a good connection with the subject, you can also ask the subject to read coordinates directly from their phone. Tell them to open their phone's browser and type ***findmesar.com*** in the address bar. (See the detailed workflow at *Section 1: Using findmesar.com (https://findmesar.com*).
c. After the app opens ask them to tap the **Next format** button until the screen appears that displays coordinates in the format preferred by your SAR team. Then have them read the coordinates shown, the accuracy value and the timestamp.
d. If the subject has provided coordinates from some other app or device, then it is important to try and get a 'second opinion' on the subject's location use one of the apps outline here, but make sure to tell them to also call 911 – that's the only recognized protocol for a subject in phone contact.

a. If *cellgps.org* or *findmesar.com* produce location data with good accuracy that is significantly different than the location data provided by the PSAP then, once again, evaluate the clue as with all others. Evaluate the accuracy estimate of each and consider some of the accuracy limitations inherent if the wireless carrier is using any kind of triangulation technology to provide location data to the PSAP.
b. Both *cellgps.org* and *findmesar.com* require the GPS in the caller's phone to be turned on and may require the caller to give permission. See *Instructions to turn on/activate GPS function on several types of phones*. That section also has an important tip for Android users.
c. For the best GPS accuracy, the phone should have a reasonably good view of the sky, be held upright (portrait orientation) and with the subject's hand holding the lower part of the phone so the GPS antenna is not blocked.
d. In the unlikely event that the GPS is on and permission has been given but neither app displays the user's coordinates, then it may take 15-20 minutes for the phone to download some special data (GPS almanac) from the GPS satellites before the caller's coordinates are displayed.

Resources: Detailed Workflows

Practice with all these techniques and apps so you'll be familiar with them and able to choose the best one on an active incident.

Section 1: Using findmesar.com (https://findmesar.com)

This app can be used:

- When in direct voice or text contact with the subject.
- As a double-check on a PSAP location report or
- the subject's self-reporting of location using another gps app.

1. Tell the subject to open their phone's browser and type **findmesar.com** in the address bar.
2. If necessary, take the subject through the steps to turn on their GPS and give permission. See *Instructions to turn on/activate GPS function on several types of phones*.
3. Ask the subject to tap the **Next format** button until the coordinate format appears that is preferred by your SAR team. Four coordinate formats are supported and each is identified by a **unique screen color** and name:

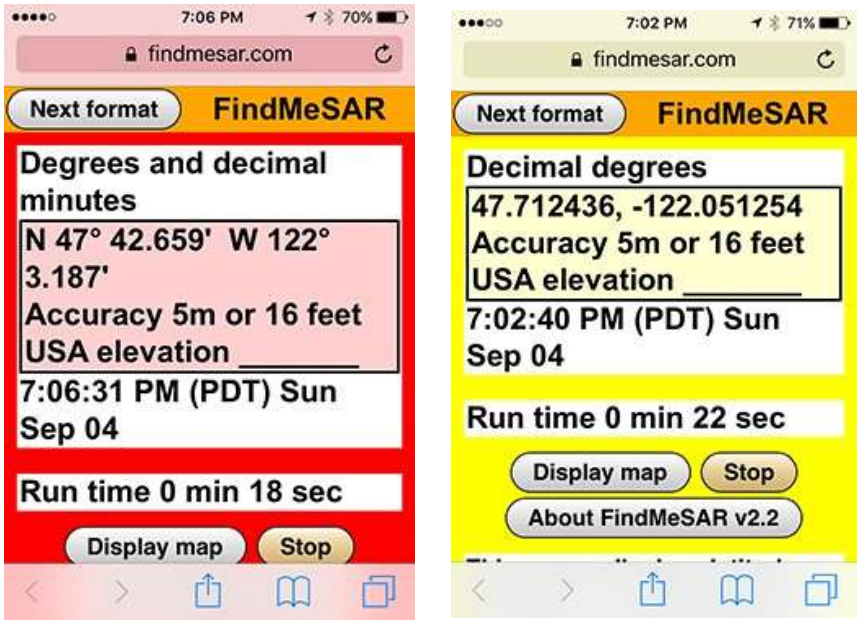


Figure 1: Examples of two coordinate types from *FindMeSAR* screenshots. Not shown are UTM (green background) and USNG (US National Grid, blue background).

4. The accuracy value will continue to improve (become smaller). Usually in 30 seconds or less the accuracy value will be 10m or smaller. Ask the subject to read off the

coordinates, accuracy value and timestamp. Remember, accuracy under about 100m is considered a Highly Reliable Clue and should be acted on immediately.

5. If it would be useful you can also ask the subject to read off their **elevation**. This value is displayed a few seconds after the user taps **Stop**.
6. Then ask the subject to turn off their GPS in order to conserve the phone's battery.
7. Relay the coordinates, accuracy, timestamp and (optionally) elevation to SAR IC.
8. For more information about *FindMeSAR*, you can open the app and tap the **About** button.
9. ***You should use, demonstrate and test this app as needed for training.***

Section 2: Using login.cellgps.org

This app can be used:

- Upon notification that a subject is missing and cell number is available;
- and/or when contact has been established with individual after a 911 call to double-check location;
- or when 911-provided coordinates are deemed unreliable (e.g. coordinates are location of cell tower).

1. Go to **http://login.cellgps.org**
2. Register as Guest (or, as pre-planning step, open a free account).
3. From the console (*See Figure 2)*, type in the cell phone number of the missing person.

Figure 2: Cell GPS Console. Phone number and message at top.

4. In text message box, type: "***This is [County] Sheriff. A search has started for you. Tap link below and then tap "Allow" to send us your location. THEN call 911.***"

gedurkee@sonic.net • 209-591-8802

5. The subject then receives *Figure 3* on his phone:

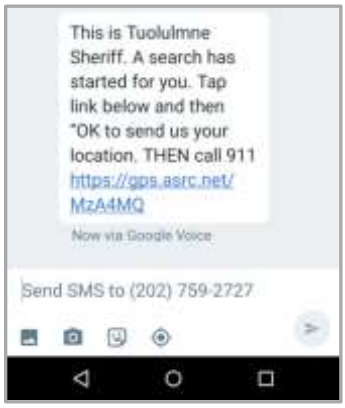


Figure 3: Message as it's received on phone.

6. After tapping the link, the subject sees *Figure 4* and must tap "Allow" to authorize the GPS feature to be activated and send the location:

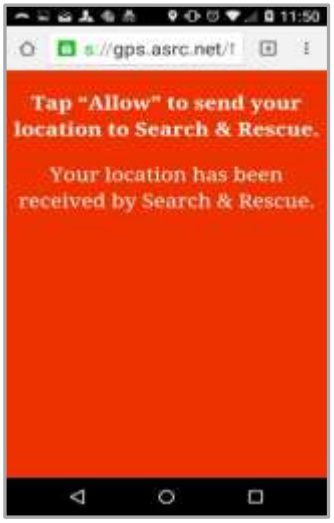


Figure 4: Return message on phone after permission granted.

7. From the Console, click on number in list for Details page. Then monitor and refresh page.

8. If successful, the Details Console will show as in *Figure 5*:

Figure 5: Details page showing response received from target cell. Note major inaccuracy of 13:19 hrs return making it unusable.

9. Note the Accuracy column estimate. If Accuracy > 100m, resend. If under 100m consider it a high reliability clue and should be acted on.
10. Click on the coordinates to show location in Google Maps.
11. Relay the coordinates and accuracy to SAR IC. Note coordinates are in Decimal Degrees (DD) and Accuracy in meters. Follow up with hardcopy screen shot to SAR.
12. Keep checking in and refreshing page throughout SAR. Individual may come within cell range at any time (*See example at Figure 6*).
13. ***You should use, demonstrate and test this app as needed for training.***

Keep in mind that the GPS and conversation with subject is draining their battery. Keep conversations short and advise them to turn off GPS once you have an accurate fix.

Section 3: Brief Introduction to AFRCC Forensic Analysis techniques

This section is intended to familiarize Incident Command with some of the techniques used by the AFRCC Cell Phone Forensics Team to take data provided by a cell phone's carrier and derive a better location probability than the carrier is often able to provide.

If only one tower is involved, as is often the case in Wilderness SAR, it often happens that the cell carrier tells SAR or LE that they can't give a very precise location. For instance, a "ping" is the most basic data exchange between tower and phone. It is much more limited than a voice call or text. The ping is a record kept only 48 hours or so by some carriers and usually doesn't contain direction information from the tower, only the time the signal took from tower to cell and back.

The Round Trip Distance (RTD) between cell and tower is then calculated. With no direction, a ring with the tower at its center then represents the probability that the subject is somewhere at

that calculated distance from the tower (*Figures 6 and 7*). The width of that ring represents the accuracy estimate of the RTD. Though, a direction is not likely part of that data AFRCC will create a map of the projected cell coverage from the tower. In uneven terrain, the coverage is not continuous and will show dead zones and areas where cell to tower contact is possible. As such, a ping is likely to have occurred where there's coverage, narrowing the search area. If a subject's general direction and travel route is known or suspected from other clues (e.g. known intent, a trail, road or other travel corridor) the search area can be further narrowed where those travel corridors intersect a mapped transmit area.

Similarly, dead zones should be considered to help narrow a search area. If a subject was pinging a tower and those pings cease, it might be because the person is in a dead zone (or, of course, the cell phone died)

In addition to pings, cell records include transactions. These are voice calls, texts or contact with voice mail and are retained by the cell carrier for a very long time. They can provide better location information. Transaction data will include not only RTD but the segment from the tower that handled the exchange. This gives a cone of direction (*Figure 6*) from that cell tower antenna. Also recorded are the phone numbers or web sites contacted. Follow-up to these clues can provide further direction to investigators on possible trip plans or intent.

In most incidents where you use AFRCC, you'll be able to talk directly to Justin or one of his colleagues as they develops a clue probability map based on what the IC knows of the subject and what likely areas are indicated by the cell data. You'll be sent a KML or KMZ (Google Earth) file to project the Most Likely Area for your team to act on. In many situations, AFRCC will also send a narrated Google Earth view of the search area and the reasoning behind the MLA choice.

gedurkee@sonic.net • 209-591-8802

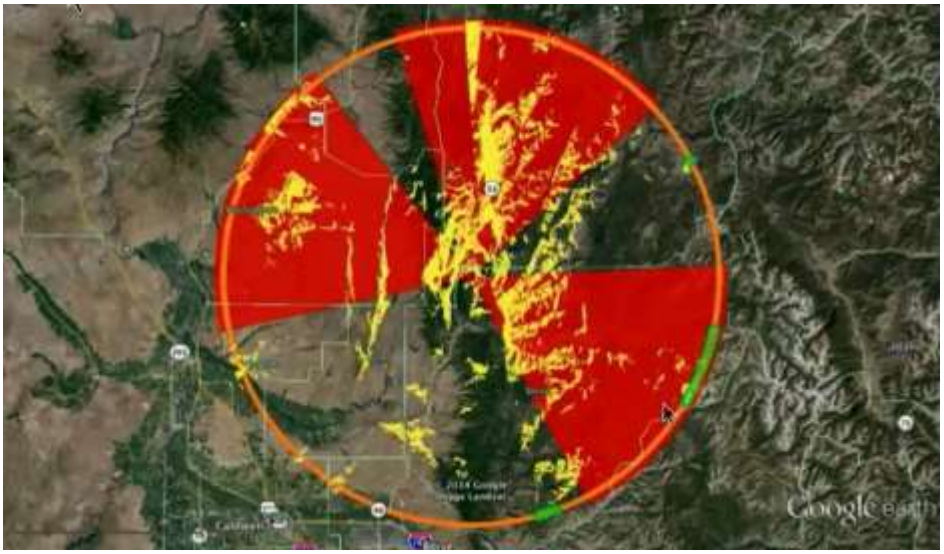


Figure 6: Cell tower coverage showing conic sections of antennae coverage (red). Yellow is actual coverage of tower out to orange probability ring (calculated from RTD and buffered at 2,500 meters to represent confidence level). Subject was believed to be in a vehicle driving south so green is for areas in that POA where subject direction of travel, ring and coverage occur.

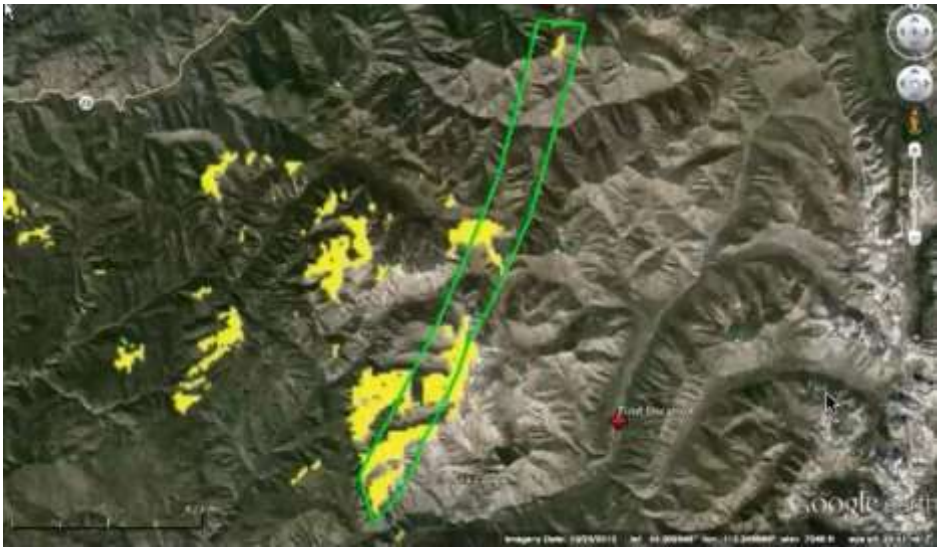


Figure 7: Close up of Most Likely area where both coverage and probability ring intersect. Subject was driving in a dead zone, came up a ridge and entered a coverage area where his cell phone pinged the tower, then dropped into a dead zone on the other side of the ridge. SAR followed the road and found the subject on the other side of a rock slide which had blocked his return.

Justin Ogden, one of the Cell Forensic Team at AFRCC, has cautioned:

- Accuracy of each transaction or ping 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 and the coordinates are passed on with a decimal string indicating high accuracy.
- Based on Round Trip Distance between phone and tower, large potential errors can occur in determining distance and direction.

It often happens that further analysis is needed on a 911 call. Location information for those is derived in two ways: Network Based Location and GPS based location. Both are very complex and can have sources of error inherent in the underlying technology. The PSAP or phone carrier reporting to you can only do so much in interpreting the location.

Remember, this is not an NCIS TV show. A computer screen does not immediately zoom onto a blinking light indicating the subject's location. What you can get, though, is a Most Likely Area with accuracy estimates that accompany the data. As with any other clue, LE and SAR IC must evaluate this information along with other clues to determine the subject's location. Also keep in mind that this is an estimate of where the phone *was* at a given time. As such, it may indicate a direction of travel and not necessarily a current location.

Instructions to turn on/activate GPS function on several types of phones

When in direct contact with a subject and the phone is not showing coordinates using the above apps, you can talk them through turning on their GPS function and/or giving the required permissions.

Turn on Location Services for Apple IOS 7,8,9; Android & Samsung Galaxy

You can turn Location Services on or off at Settings ➔ Privacy ➔ Location Services. You can turn Location Services on either during the Setup Assistant process or later through the Location Services setting. You can individually control which apps and system services have access to Location Services data. When Location Services are off, apps can't use your location in the foreground or background. This will limit the performance of various Apple and third-party apps.

Turn on Location Services from iPhone

1. Turn location on using above directions.
2. While in the location services settings menu, make sure the setting for Safari says "While using". If the subject uses a different browser, then make sure that setting is "While using".
3. Also, while in the location services settings menu, slide button next to "Compass" on to allow compass to use the phone's location. The slider button will turn from grey to green when it is turned on.
4. Start the compass app by tapping the "Utilities" app and then the compass icon. The lat/lon in degrees minutes seconds will be displayed at the bottom of the screen. Since the compass app does not display an accuracy value it should be considered a backup in case neither of the browser apps discussed above will work.
   For example, they will see: 39° 11′ 18″ N 120° 7′ 12″ W. To ensure correct transmitting and understanding of coordinates, specify location is in "Degrees Minutes Seconds" and

read or record as: "39 degrees, 11 minutes, 18 seconds North by 120 deg, 7 min, 12 sec West."

Turn On Location Services from Android and Galaxy S

Go to Settings icon:

Choose Location ➔ Move slider to ON ➔ Choose Mode ➔ Select "GPS only"

Samsung Galaxy S: Apps ➔ Settings➔ Location.

If the subject is using an Android device and the browser apps described above are not able to easily report coordinates with an accuracy of 30m or better, then ask the subject to make sure their location mode (aka method) is set to "GPS only". The "Power saving" setting ignores the GPS in the phone and the "High accuracy" setting actually allows data from cell towers to degrade the more accurate location data from the GPS satellites.

GMAP4: Online Mapping software that can search for any coordinate format

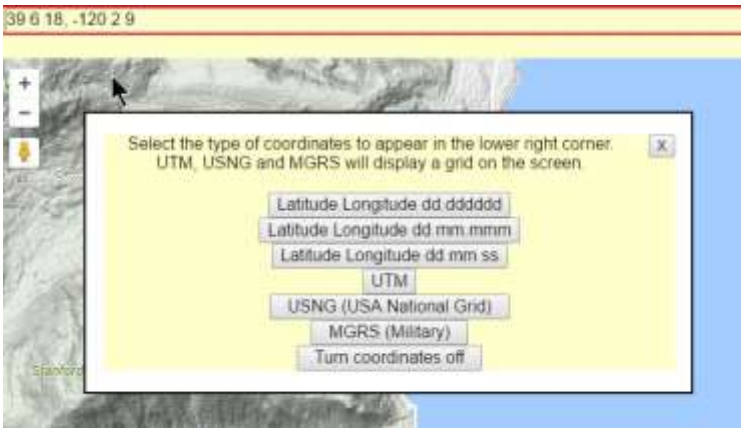
Gmap4 is an enhanced Google map viewer that can display high resolution USGS topo maps in addition to the standard Google basemaps. The software automatically detects the type of coordinate that you enter in the search bar. It has an added advantage over other online mapping software in that it can use USNG (US National Grid, now the standard for all emergency response) and MGRS (Military Grid Reference System). To search using any coordinate format:

1. Your browser needs to be online. Go to: https://mappingsupport.com/p/gmap4.php
2. Choose Menu ➔ Search

3. Enter the coordinates in the search bar above the map, check the coordinates on the Results popup and click either **Map Selected Items** or **Search and Mark**.

You can search on all three versions of latitude longitude (DD, DDM and DMS) as well as UTM, USNG and MGRS. **In the western hemisphere, longitude must have a minus sign**. South of the equator, latitude must have a minus sign. For instance, if you have: 39° 6′ 18″ N 120° 2′ 9″ W you must enter that without the "N", "S" or degree symbols: 39 6 18, **-**120 2 9 (Center of Lake Tahoe). All letters and special symbols in latitude longitude coordinates will be ignored. If the search does not work, make sure all letters and special symbols are stripped from the coordinate string.

You can also convert coordinates by entering the coordinate type you received, click on the coordinate types at the bottom of the Menu dropdown (**UTM – USNG – LatLng**) and choose from the popup menu the coordinate type you want.



You can then convert from the type you entered by right clicking on the point, which gives you a popup of all coordinate types for that point. For the GMap4 cell phone app, tap the < symbol on the left of the screen ➔ DRAG the marker popup to the position you want the coordinates of ➔ tap **DRAG**:

Gmap4 also has the following functions:

- To turn on a UTM or USNG grid go to **Menu ➔ UTM - USNG - Lat/Lng.** Then select UTM or USNG.
- To display a high resolution USGS topo map, click the basemap button (next to the **Menu** button) and select **t4 CalTopo Hi-res**. You may need to zoom in.
- To display the weather radar, click the basemap button and then under the "Overlays" heading select **USA_weather radar**.
- You can also display KML or KMZ files on a high resolution USGS topo map. See the Gmap4 homepage: https://mappingsupport.com/p/gmap4.html

Practice! An active incident is not the time to become familiar with these – or any other – apps.

Mapping and Coordinate Exercise

Here's some coordinates to practice locating with GMap4 or any other software.

Coordinates for center of Lake Tahoe, CA

DMS: W39° 6′ 28″, N120° 2′ 4″ (remember to enter as 39 6 28, -120 2 4).

DD: 39.1072, -120.03524 (This is the coordinate type most often used by satellite devices such as SPOT, PLBs and InReach).

DDM: 39° 6.445, -120° 2.218 (This is the coordinate type most often used by marine vessels and aircraft)

USNG: 10SGJ56423292 (US National Grid. This is the standard for all SAR and emergency response, though adoption is slow. For more information go to: http://usngcenter.org/).

Coordiantes for Mt. Whitney Summit, CA

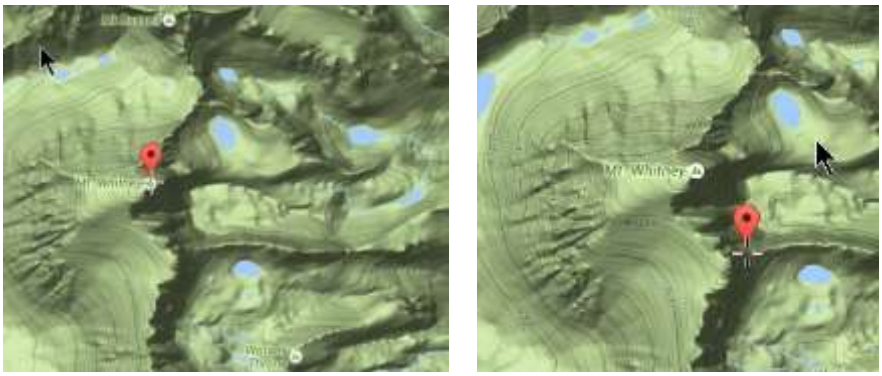
UTM: 11S 384389, 4048905 (This coordinate type is often used by goernment agencies: NPS and USFS).

DMS: N36° 34′ 43″, W118 17 32

DDM: 36 34.717, -118 17.533

It is very common to misinterpret coordinates if they are not clearly identified when being relayed verbally. When doing so, make sure to clearly identify the coordinate type and identify each number with the appropritate identifier ("degrees", "minutes" "seconds" or "point".

See what the error can be by entering the above DMS as DD: 36 34.43, -118 17.32:



Example of misunderstanding coordinates. On left are coordinates in Degrees Minutes Seconds (36° 34′ 43″, -118 17 32) on right are same numerical string, but entered as Degrees Decimal Minutes (36 34.43, -118 17.32). A difference of about 0.5 miles.

Finally, see what happens if you plot as DD: 36.3443, -118.1732.

Resource Contacts

AFRCC
Justin Ogden, Maj CAP
Cellular Forensics Technical Specialist
Air Force Rescue Coordination Center
814-592-2340 (direct)
877-243-1215 (fax)
800-851-3051 (console/supervisor)
For both downed aircraft and ground searches, Justin should be requested through AFRCC. If it's a non-aircraft search, it's not an AFRCC incident and assistance is at their team's discretion.

Justin has also created a web site with a number of tools to automate many of the tasks necessary for location analysis: number lookup for the phone's carrier; text location app similar to *login.cellgps.org*; create coverage maps of individual towers; and create location map from cell carrier's data files. The site is intended for LE only, however some tools might be made available for SAR professionals. Go to https://mla.tools to contact Justin and get further information.

Don Ferguson
Appalachian Search and Rescue Conference
Don has experience mapping cell coverage areas and estimating locations from RTD off the involved tower. He might especially be used to map coverage areas and dead zones either during an active incident or as part of a preplanning effort.
304-290-9118 (cell phone)
Don Ferguson dferguson002@gmail.com

George Durkee
Adjunct Instructor, GIS & Emergency Services
Columbia College
gedurkee@sonic.net
209-591-8802

Acknowledgments

Thanks to Joseph Elfelt, Justin Ogden (AFRCC), Paul Long (Placer County, CA SO), John Dill (YOSAR), Paul Doherty, Arnold Gaffrey (SMSR), Art Fortini (SMSR) and the always-helpful gang at Using GIS in SAR and Emergency Services discussion group.