

Civil Air Patrol



Forensics in Search and Rescue

03 June 2017

CITIZENS SERVING COMMUNITIES

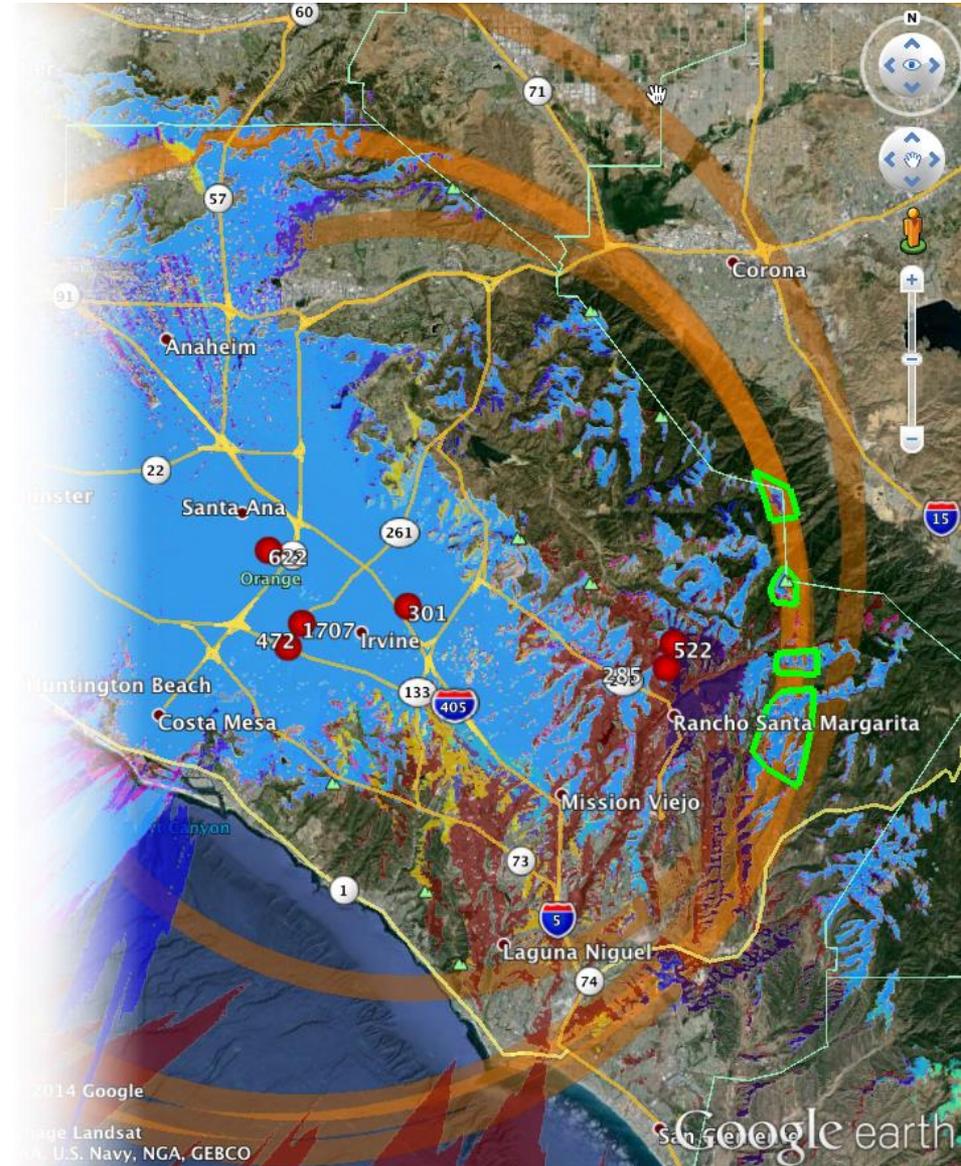


Topics

AFRCC/CAP Cellular/Radar Forensics

Understanding the raw data and analyzed data

Tips on what to do during a search







Air Force Rescue Coordination Center & Civil Air Patrol Cellular Forensics

- CAP has been carrying out the cellular forensics missions for AFRCC since 2006
- AFRCC/CAP provides cell forensics support on CONUS search and rescue missions similar to how they offer CAP air/ground teams and other military resources
- It started as a last resort tool for locating missing person and overdue aircraft, but is now a primary resource
- Some agencies are requesting cell forensics exclusively (no other federal assets requested)





Non Disclosure Letter



DEPARTMENT OF THE AIR FORCE
HEADQUARTERS FIRST AIR FORCE (AIR FORCES NORTHERN) (ACC)
AIR FORCE RESCUE COORDINATION CENTER (AFRCC)
650 FLORIDA AVE
TYNDALL AIR FORCE BASE, FLORIDA 32403-5017

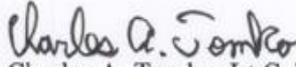
1 July 2010

MEMORANDUM FOR RECORD

FROM: AFRCC

SUBJECT: Non-Disclosure Cover Letter

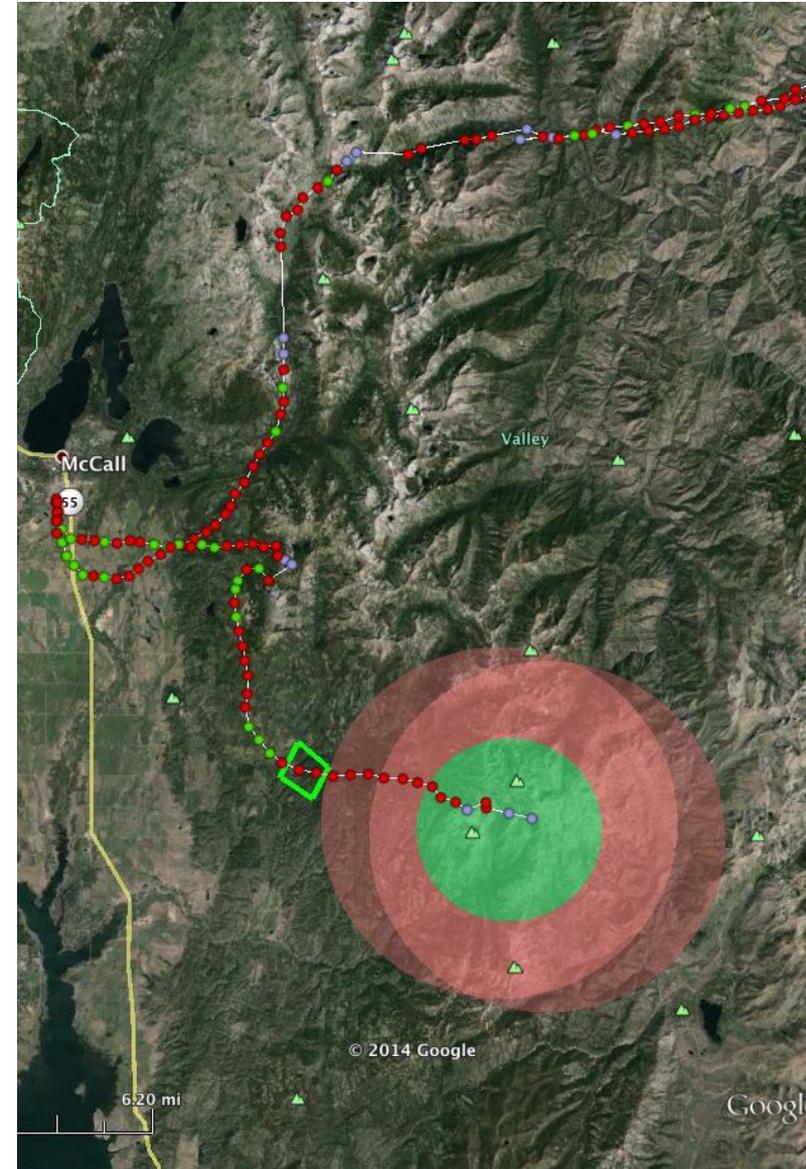
1. This Memo is a binding Non-Disclosure requirement for the purpose of preventing unauthorized disclosure of any and all Radar or Cell Phone Forensics information or data obtained during federal AFRCC mission investigation and prosecution.
2. The information contained in this email / fax is the expressed property of the AFRCC and may not be used, released or provided to any agency other than yourself without consent of the AFRCC Commander, Director of Operations or Chief of Operations. If another agency requests the information contained in this email / fax, please have them contact the AFRCC at 1-800-851-3051 and the SAR Duty Officer will prosecute their request.
3. The POC for this letter is Mr. Dan Conley, AFRCC Chief of Operations at (C) 850-283-5688 or danny.conley@tyndall.af.mil.

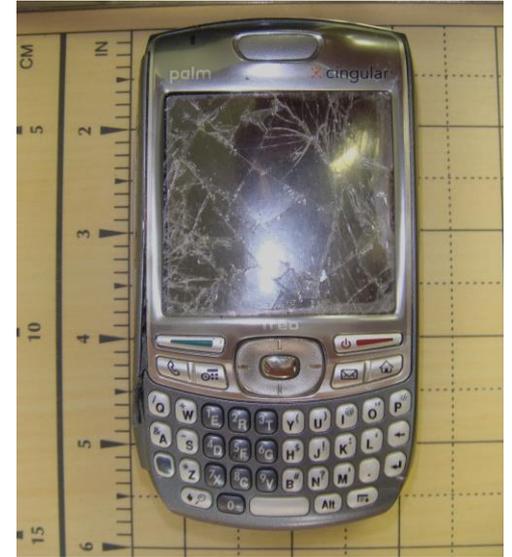

Charles A. Tomko, Lt Col
AFRCC Commander

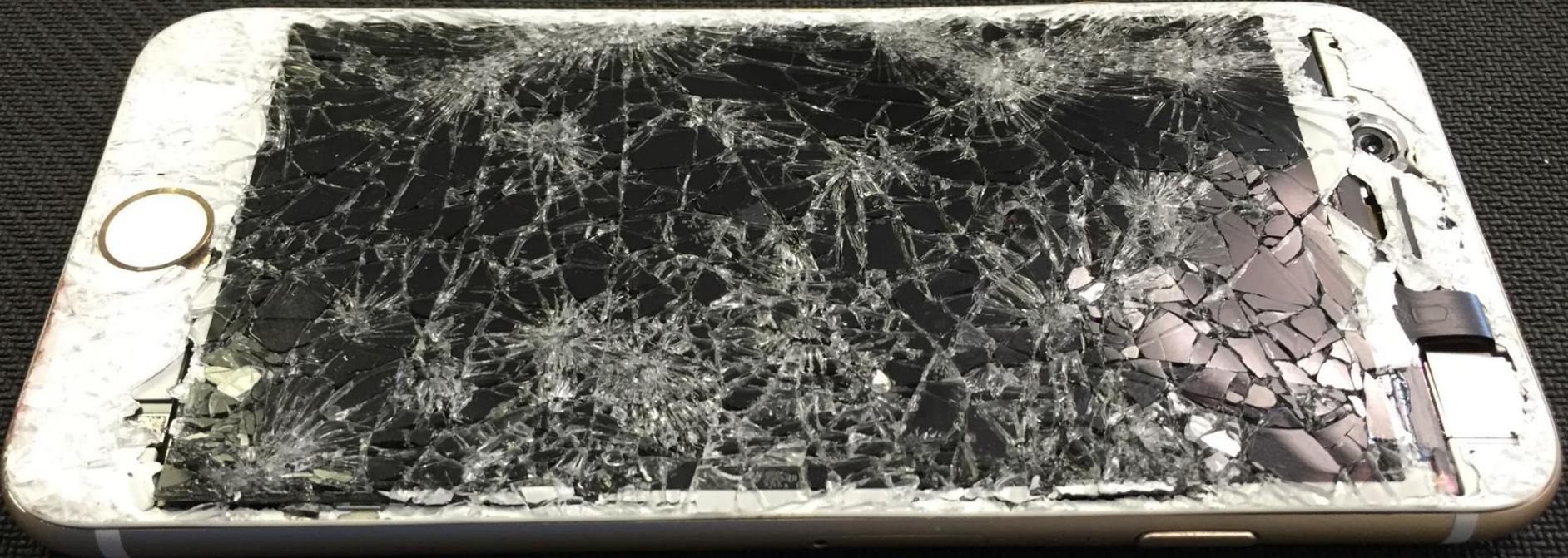


Cell phone analysis & other clues: ELTs, Radar, LKP, etc

- Cell phones can provide real time and historical data
- Phones are small and often survive harsh situations
- Phones are prevalent and highly likely to be on a missing aircraft or missing person









Likely Areas

- **Likely Areas are the result of analysis by a cellular forensics expert and represents the location(s) the phone may have been during a certain time frame**
- **Result of reviewing cell tower locations, sector information, coverage maps, distance data, and more**
- **Takes into account tolerances of supporting data**
- **Typically shown as a green outlined area - bounding the area in which the phone was most likely to be located during the given time stamp**
- **Likely Areas correspond to a time frame**
- **Gives the IC or Planning Section “at a glance” view of where a phone was located at a given time**

Avalanche Coordinates from King County SO



Position Information

47.40405° N, 121.50015° W
47° 24.243' N, 121° 30.009' W
47° 24' 14.6" N, 121° 30' 14.6" W

Likely Area 4



Position Information

47.40769° N, 121.48964° W
47° 24.461' N, 121° 29.379' W
47° 24' 27.7" N, 121° 29' 27.7" W

Likely Area 3



Position Information

47.40223° N, 121.47846° W
47° 24.134' N, 121° 28.707' W
47° 24' 08.0" N, 121° 28' 08.0" W

Likely Area 1



Position Information

47.40466° N, 121.47112° W
47° 24.280' N, 121° 28.267' W
47° 24' 16.8" N, 121° 28' 16.8" W

Likely Area 2

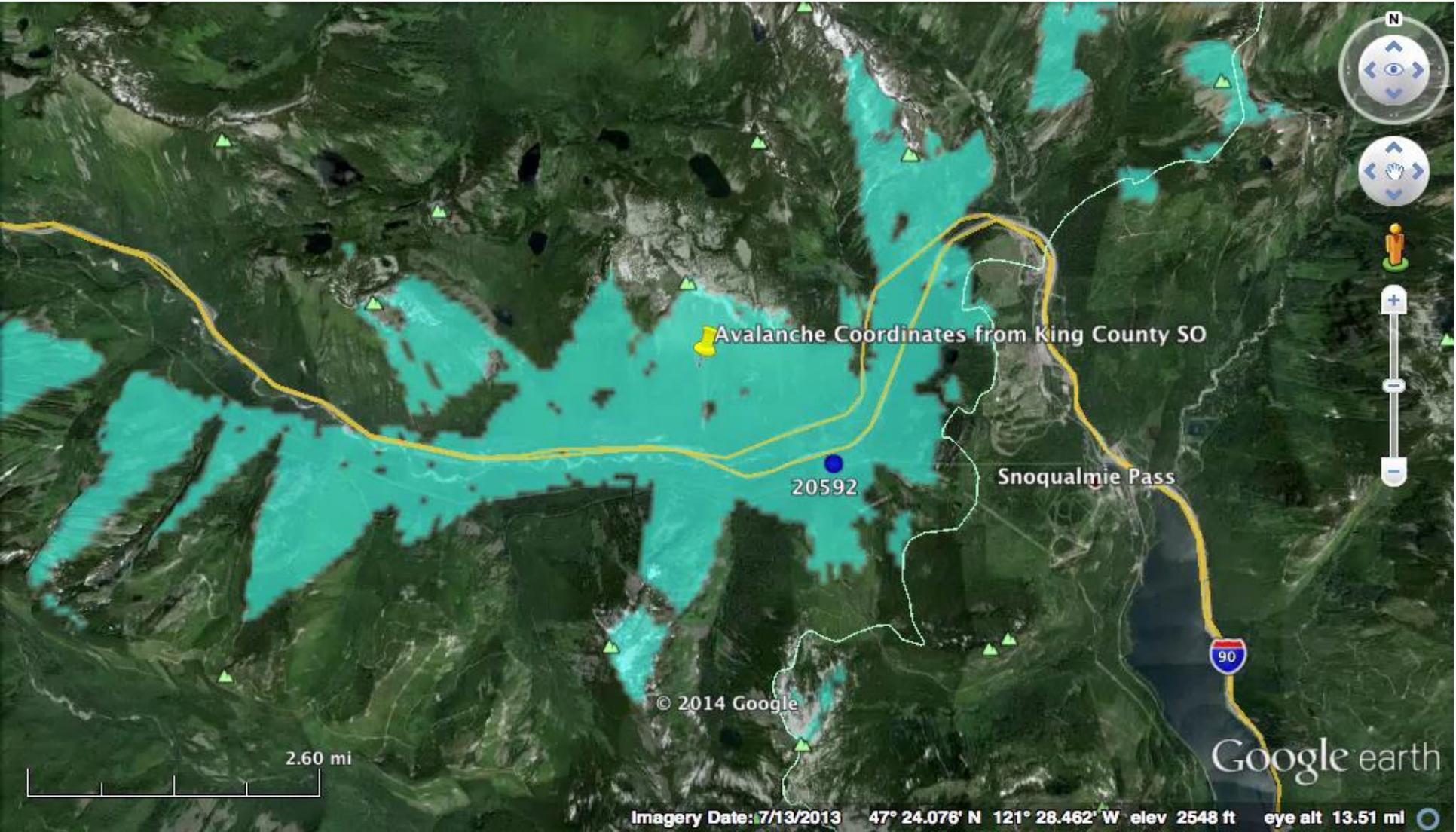


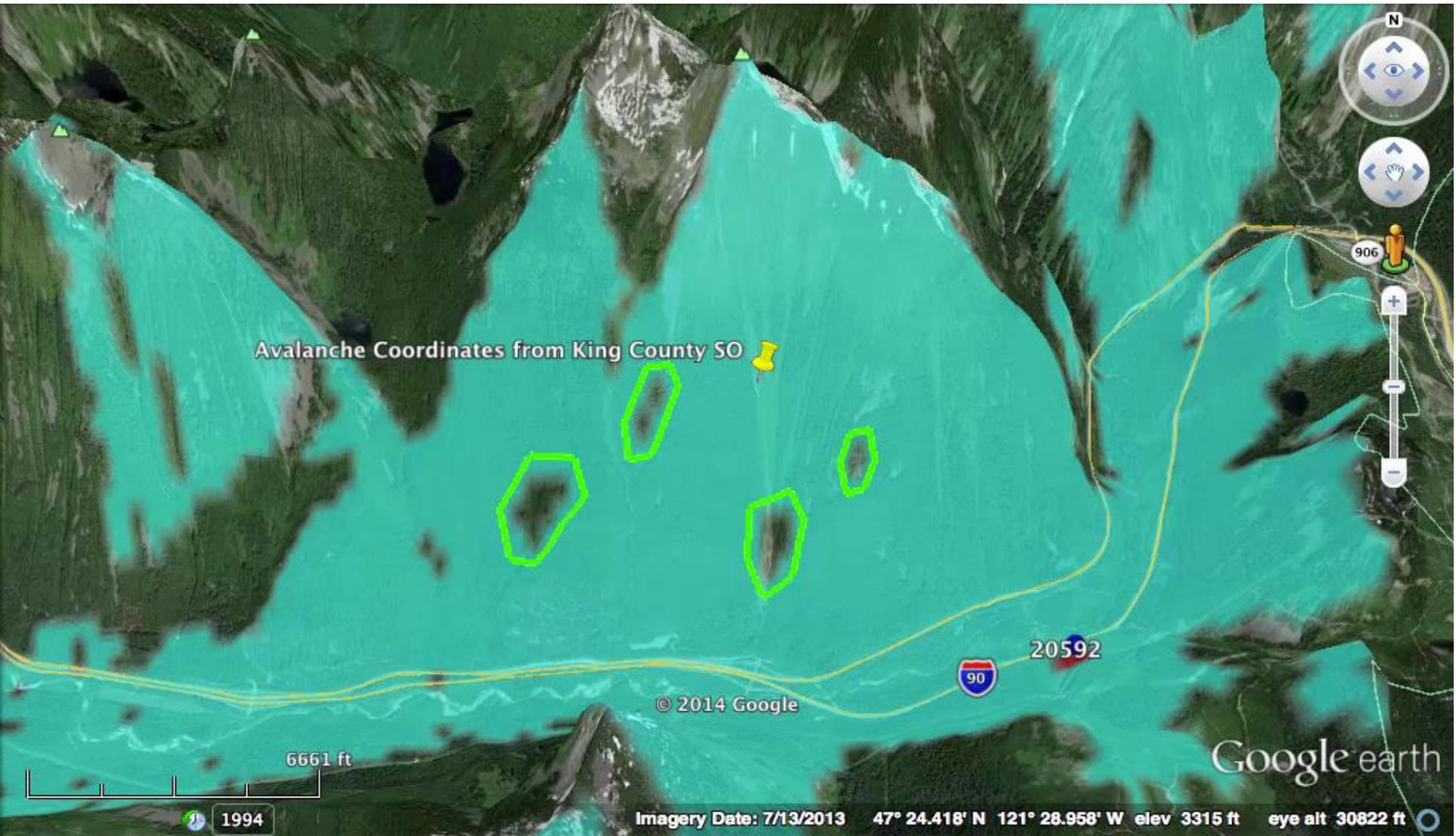
Propagation Analysis and Coverage Maps

- **Propagation Analysis uses computer models of terrain, tower height, antenna gain, transmitter power levels, and more to determine places on the ground that can communicate with a tower**
- **The result of Propagation Analysis is a Coverage Map**
- **Typical Coverage Maps show places that you can stand on the ground and communicate with a given cell phone tower**
- **Coverage Maps show places that also lack coverage, which may also be helpful**



Coverage Map







Available Raw Data

- **Data is either real time or historical**
- **Real time data can be provided when a phone is powered on and with the coverage area**
- **Historical data is records of transactions with the phone that occurred sometime in the past, while the phone was on and in the network coverage area**
- **Each cell phone provider has different capabilities, which results in data that must be interpreted in different ways**



When is historical data recorded?

- Any interaction with the phone such as calls, text messages, or internet usage
- GPS information is not recorded
 - The exception is calls to 911 which often have highly accurate coordinates, often derived from assisted GPS

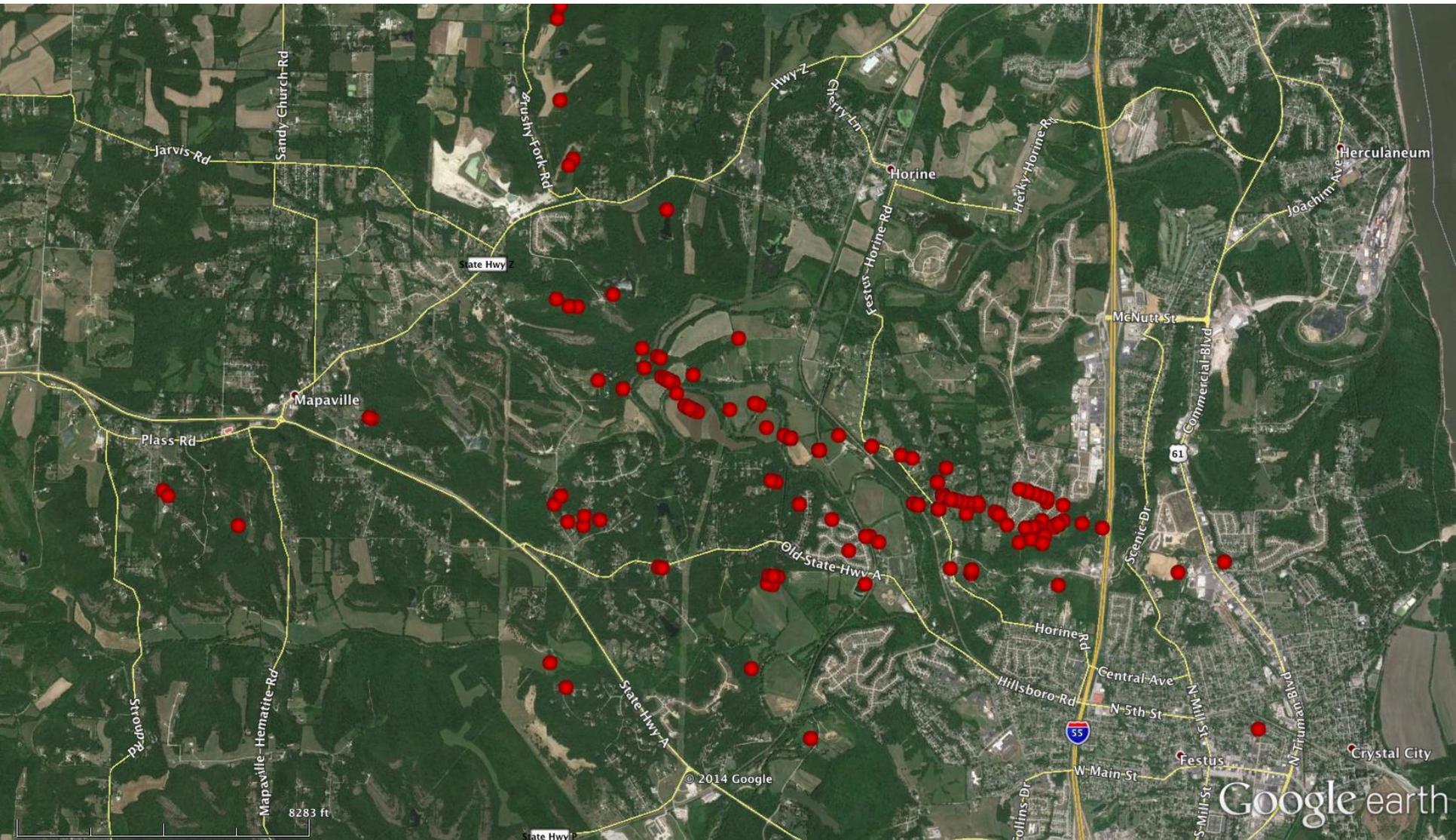


Raw Data: Network Based Locations

- **May be available in real time or as historical data**
- **Accuracy of each transaction is paramount to understanding it's 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**

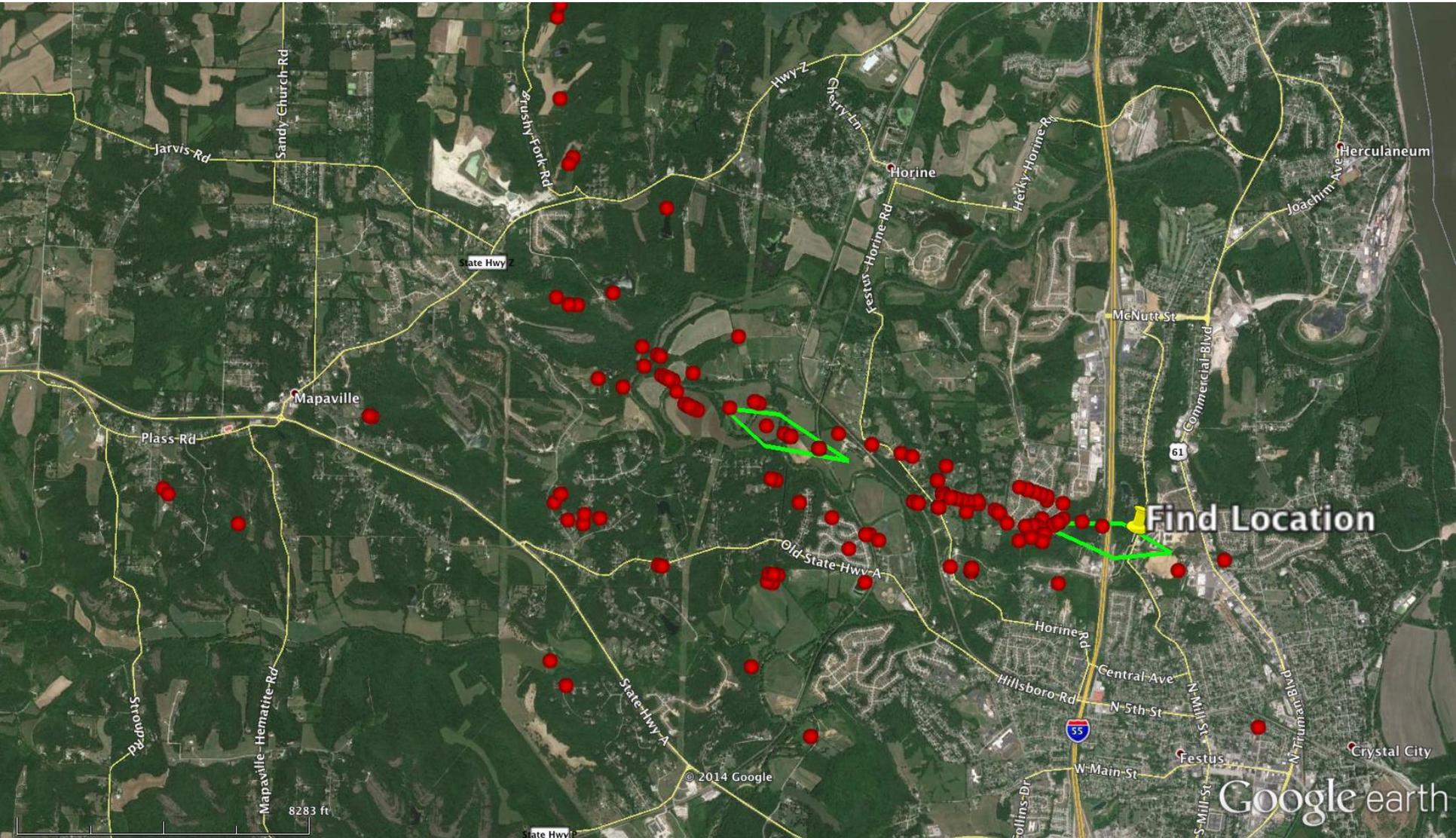


Network Based Locations





Find Location





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





All Sectors **3** Shown



© 2014 Google

Google earth





Raw Data: Distance Information

- Sometime carriers can report the distance a phone was from a tower during a transaction
- This distance is derived from timing information (not signal strength)
- Multiple distance rings from multiple cell sites can allow for very good historical locations





Combining pieces of data results in Likely Areas

- **Combining distance, sector, coverage and other clues are often helpful in a search**
- **Example the follows is from a search for a missing family who were overdue from a hunting trip**
- **Family members reported they were unsure where the missing family was going hunting - expressed interest in places spanning 150 miles**
- **Cell phone data (coverage, sector, distance) and knowledge of the areas they expressed interest in, lead to the find**

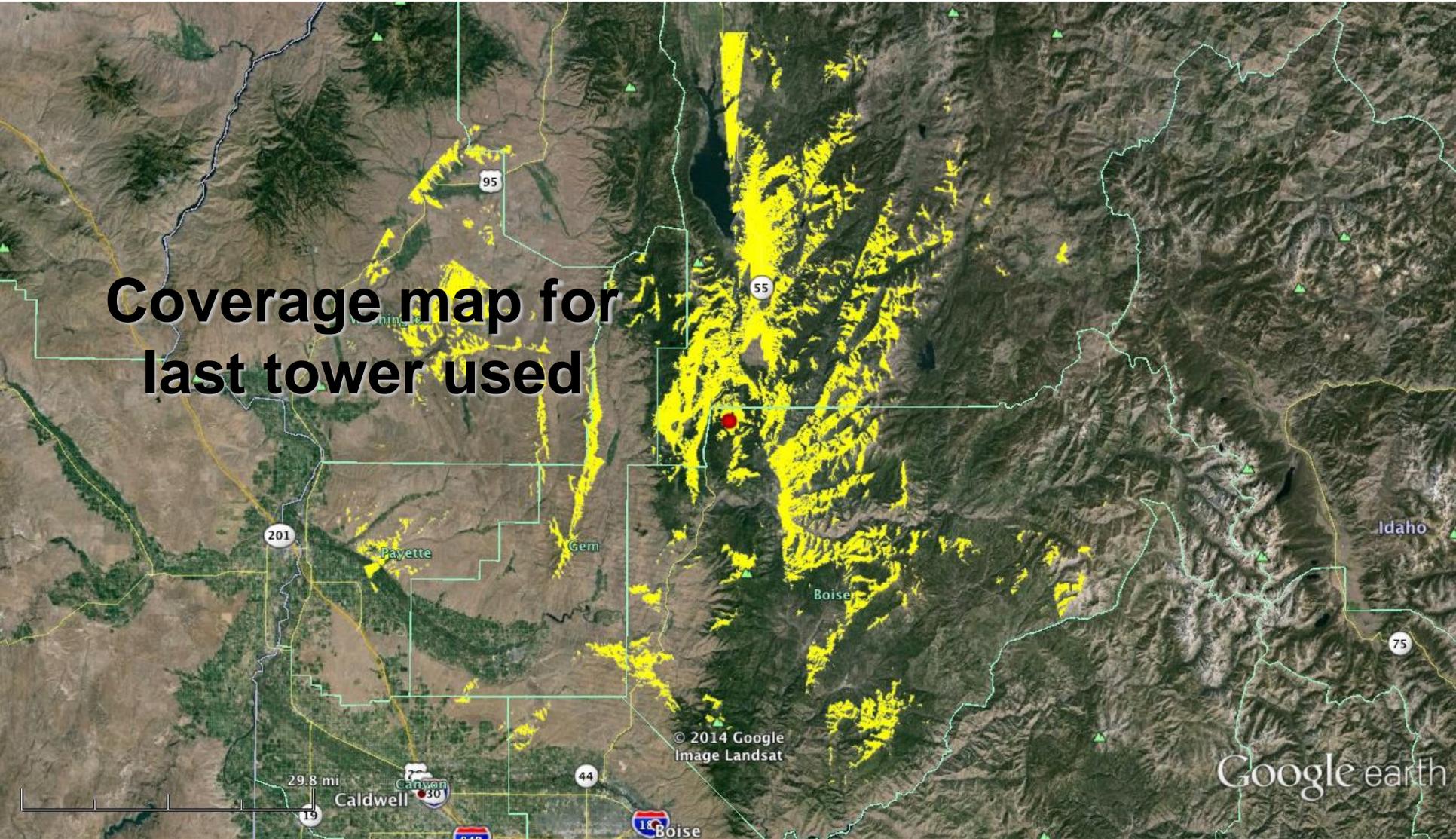


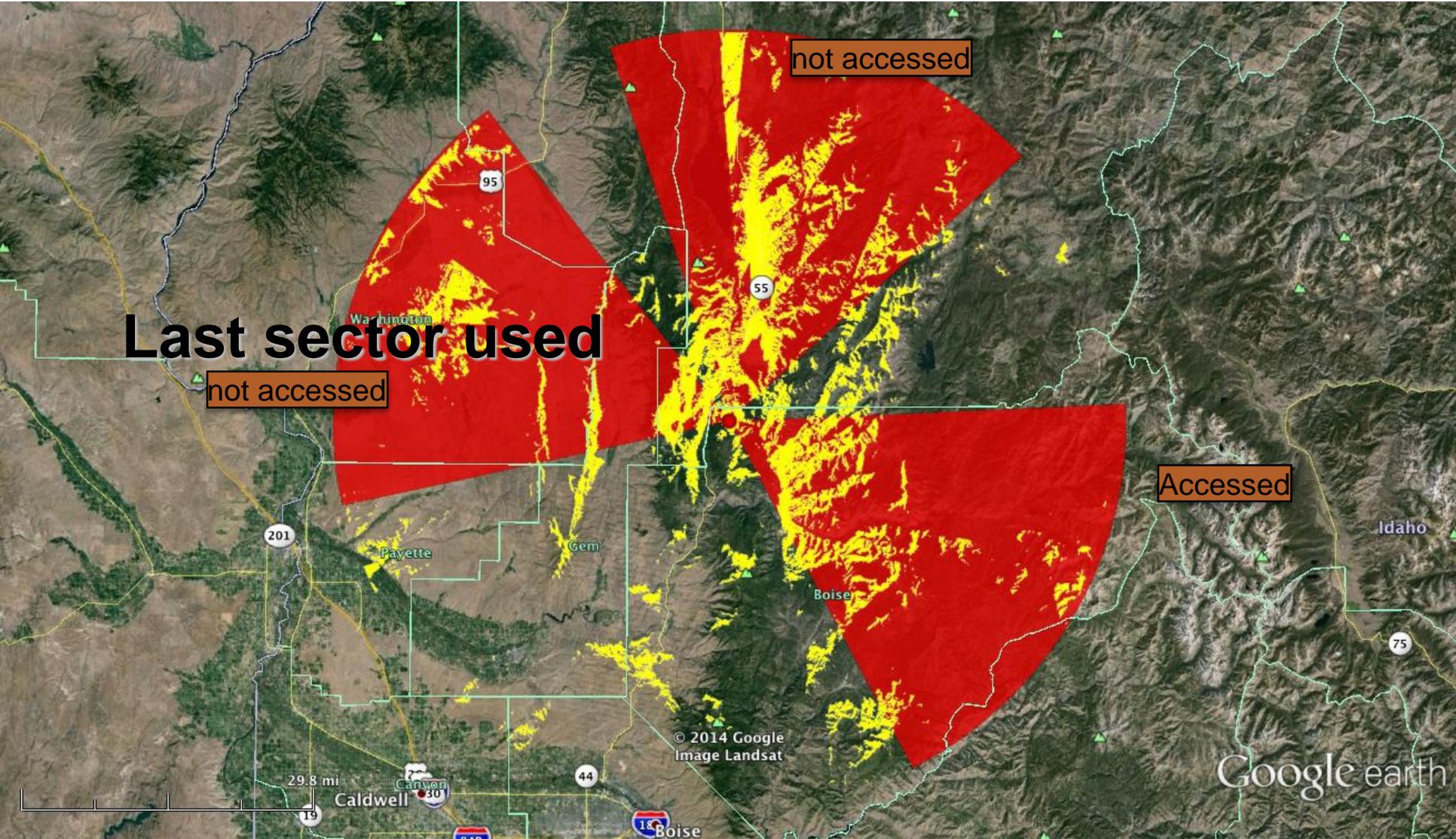
Last tower used





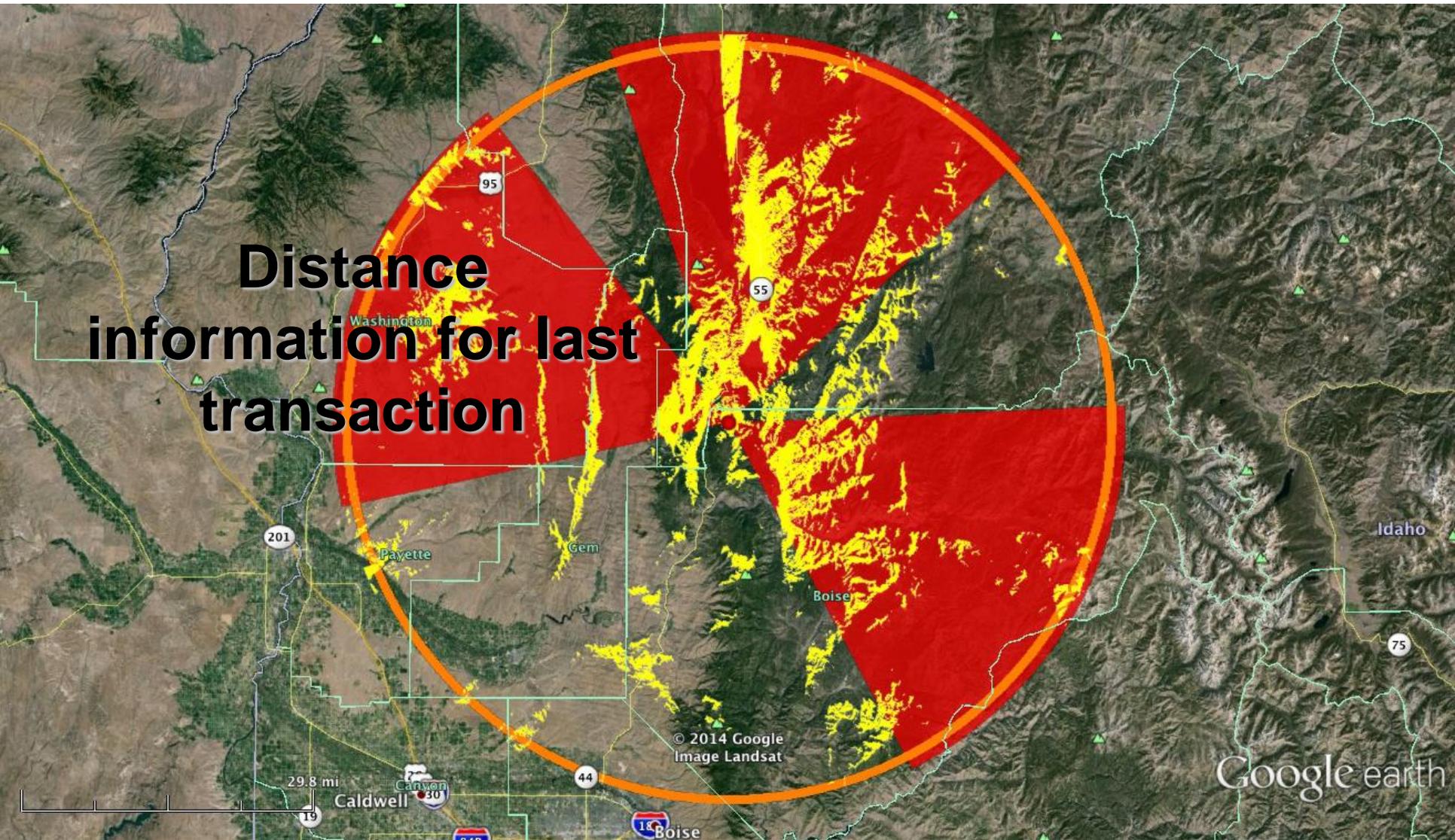
Coverage map for last tower used





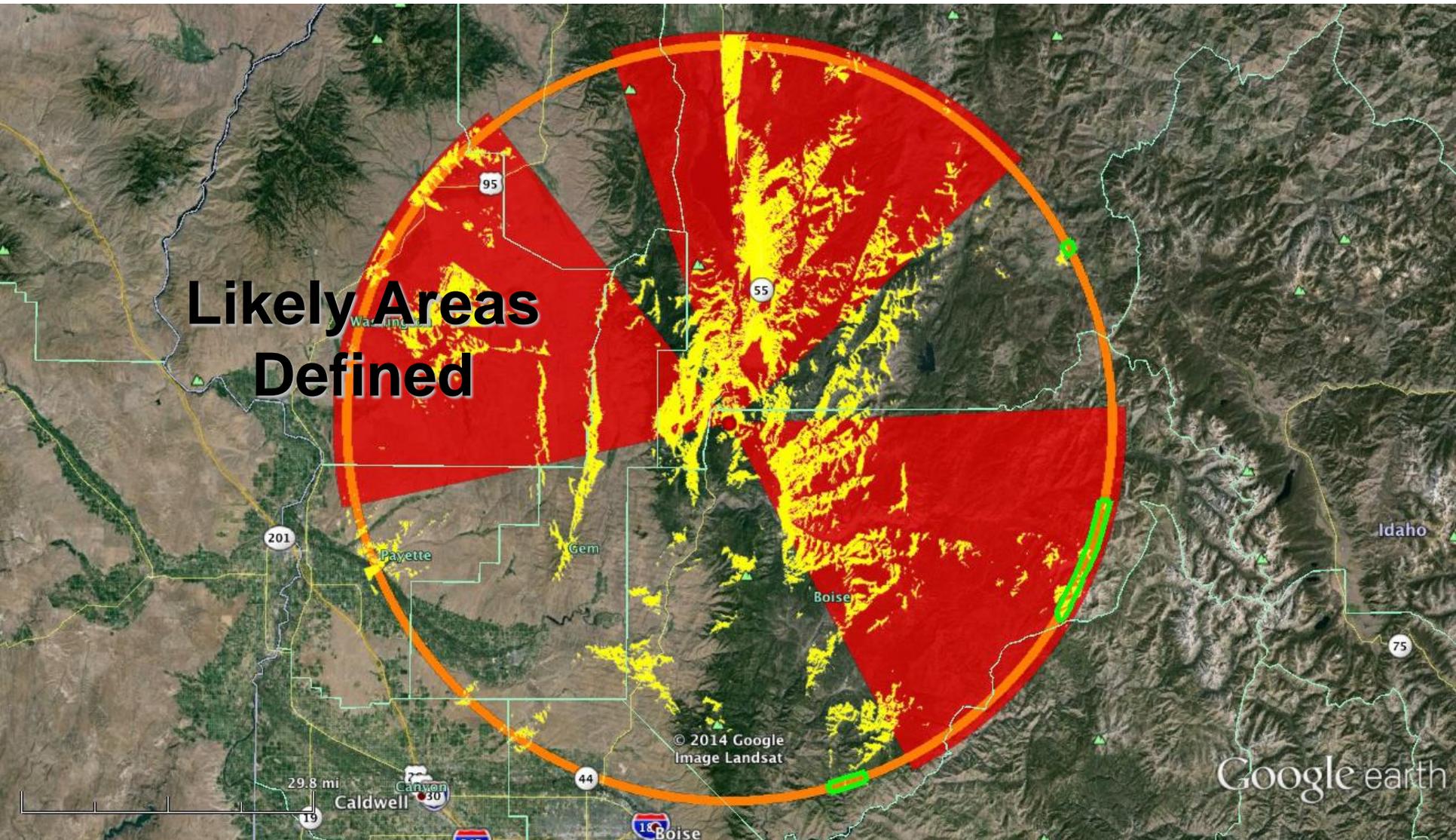


Distance information for last transaction



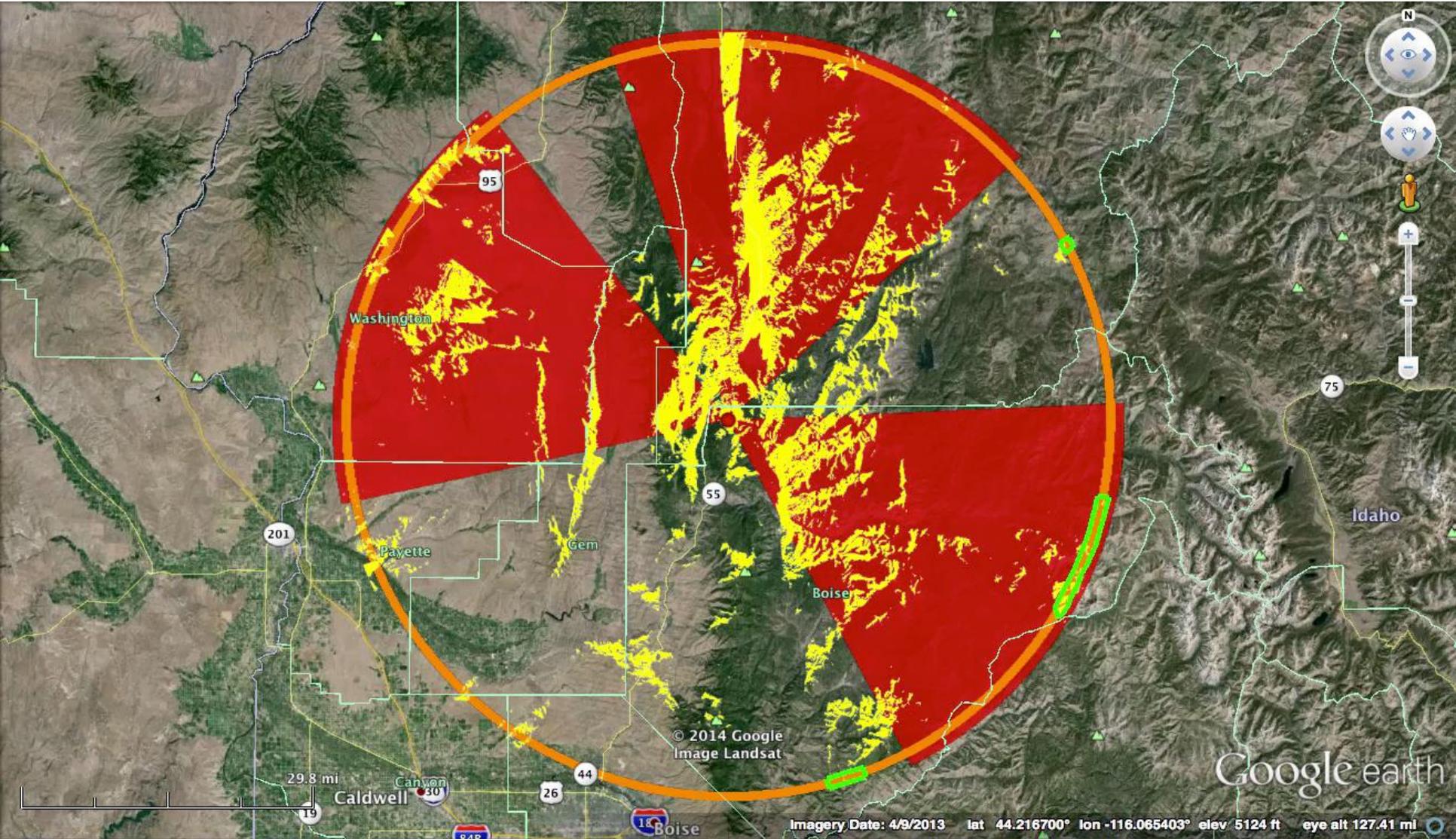


Likely Areas Defined



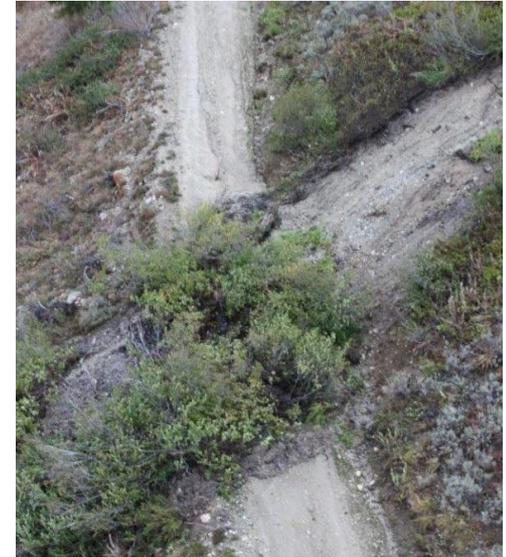


All the clues together leading to the find





The rescue!





Things to do during a search

- **Generate data**
 - **Get the victim to dial 911**
 - **Place a call and send a text message to the victim's phone (log it!) - note the number of rings until the phone picks up**
 - **Understand what the accuracy of information is when handling raw data**
 - **Request AFRCC/CAP support**



Tools and Skills Needed

To get the most out of interacting with AFRCC/CAP Forensics teams

- **Internet connection at Incident Command Post**
- **Google Earth expertise**
- **Google Hangouts (not required, but helpful)**
- **Go To Meeting**
- **Slack**



New CAP Cellular Forensics Tools

CAP's new tools to assist in missions:

- **Determine objective's phone vendor**
- **Can determine if the phone is on or off/out of service area**
- **Will monitor and alert if the phone is turned back on or travels into a service area**
- **Send and receive messages to the objective's phone as needed**
- **Automated Google Earth data plotting tools**
- **Enhanced coverage plotting capabilities**



Cellular Forensics Team Contacts

Justin Ogden, Maj, CAP

justin.ogden@forensics.cap.gov

Brian Ready, Col, CAP

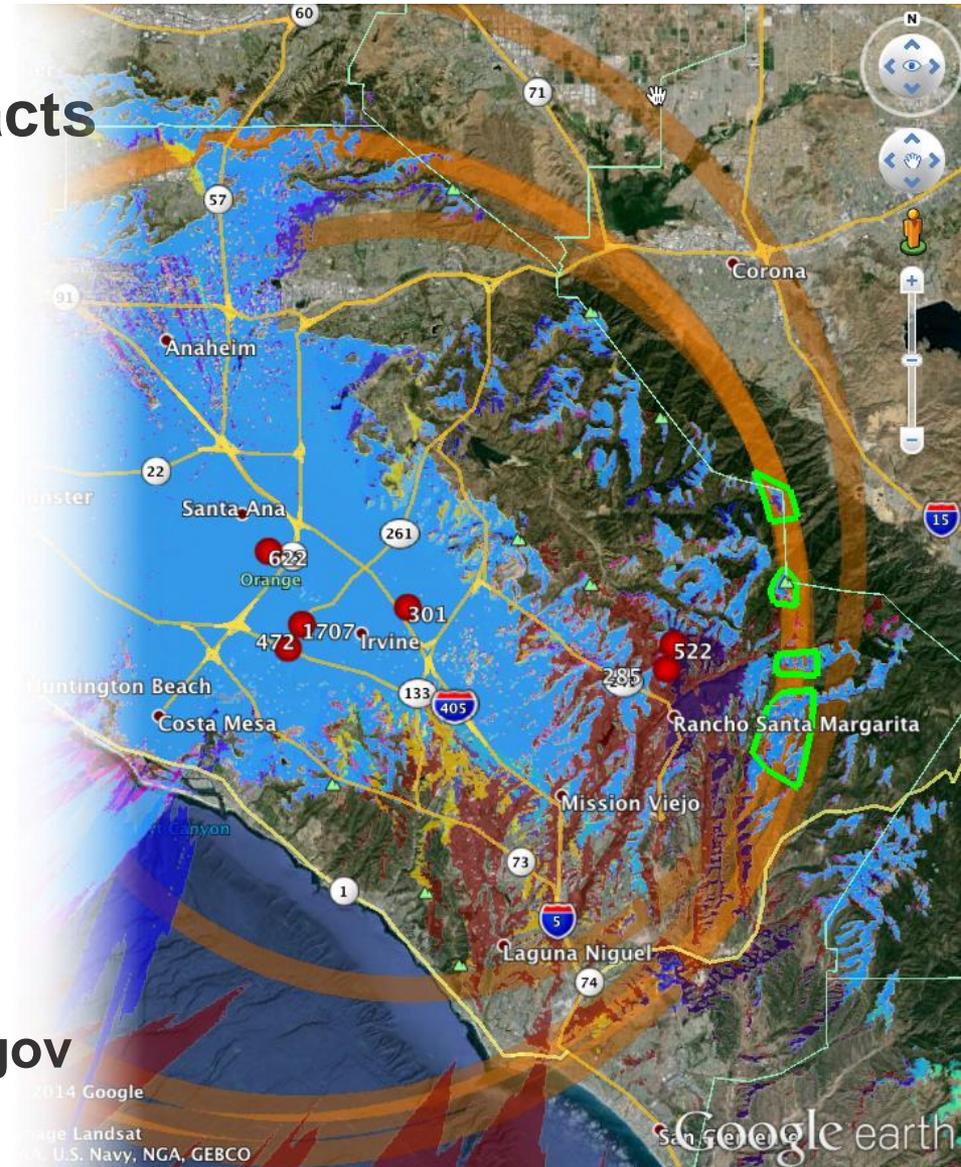
brian.ready@forensics.cap.gov

Jerad Hoff, Maj, CAP

jerad.hoff@forensics.cap.gov

Paul Combellick

paul.combellick@forensics.cap.gov



Civil Air Patrol



...Citizens Serving Communities!