Civil Air Patrol

Cellular Forensics Training for Incident Staff Members

Brian Ready, Col CAP

Justin Ogden, Maj CAP

Webinar Presenters

John Desmarais
Director of Operations
National Headquarters

Col Brian Ready
Arizona Wing Commander
& Cellular Forensics Team

Maj Justin Ogden
Subject Matter Expert
Cellular Forensics Team

Webinar Rules of Engagement

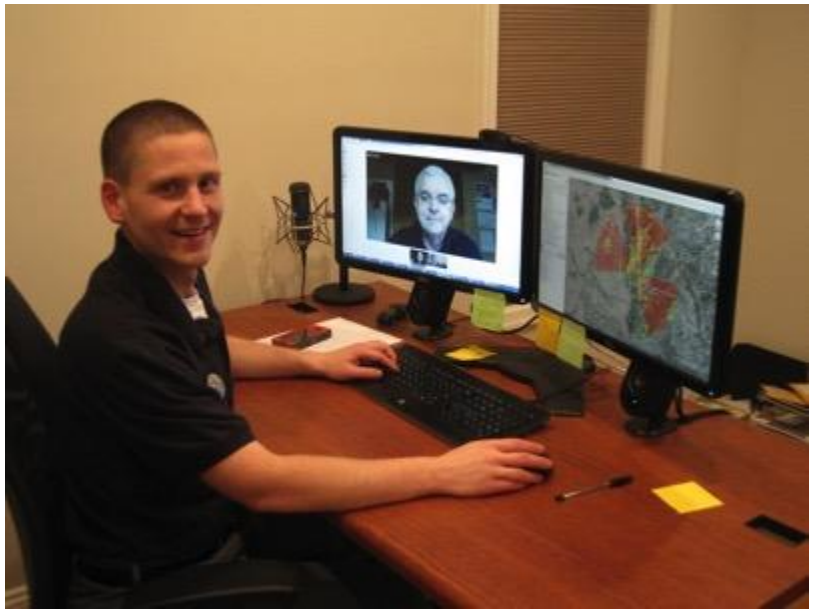
- Members in the field will be in listen only mode. We have several hundred members signed up, so having everyone with an open microphone is not supportable.
- We will try to answer questions throughout the webinar though. Just type your questions, and we will either answer you directly via text or provide a voice answer to your question.
- The webinar itself, questions, and chat log are being recorded, so please remain respectful.

Topics

- Cellular Forensics Team overview
  - Members
  - History
  - Capabilities vs other agencies
- Data Types
  - Raw Data
  - Likely Areas
- Mission Examples
- How you can help us

Members

- Primary members:
- Justin Ogden, Maj, CAP
  - Lives in Virginia
  - 22 years in CAP
  - Electrical Engineer
  - CAP GBD, GTL, UDF
  - Started with CAP cell forensics in 2006
- Brian Ready, Col, CAP
  - Lives in Arizona
  - 33 years in CAP
  - Professional pilot
  - CAP IC1, MP, MCP
  - Started with CAP cell forensics in 2009
- We work on 130+ missions per year



History

- 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 persons and overdue aircraft, but is now a primary resource
- Some agencies are requesting cell forensics exclusively (no other federal assets requested)

Capabilities

- **C**ollect, **A**nalyze, **P**resent
- Acts on behalf of AFRCC to **Collect** information from cellular providers and other data sources
- Performs **Analysis** on the data to extract clues that are useful to the mission
- **Present** the information to SAR resources through slide decks, Google Earth files, or teleconference

NHQC vs other agencies

- We collect exigent data in the same manner as other agencies
- We have experience reviewing records from all major carriers and have learned how to extract every bit of location detail from the available data
- We ensure that all sources are checked for data
- Roaming to another carrier, 911 information, etc
- We have access to analysis tools to rapidly visualize the data that are of the best in the cellular forensics industry
- We create coverage maps showing where cells sites do and do not have coverage
- We have access to a tool that allows for real-time location of the phone in some situations
- The volume of incidents we work (130+ per year) gives us incredible familiarity with the records and knowing exactly what the information means
  - Knowing what information can be trusted, and what can be misleading

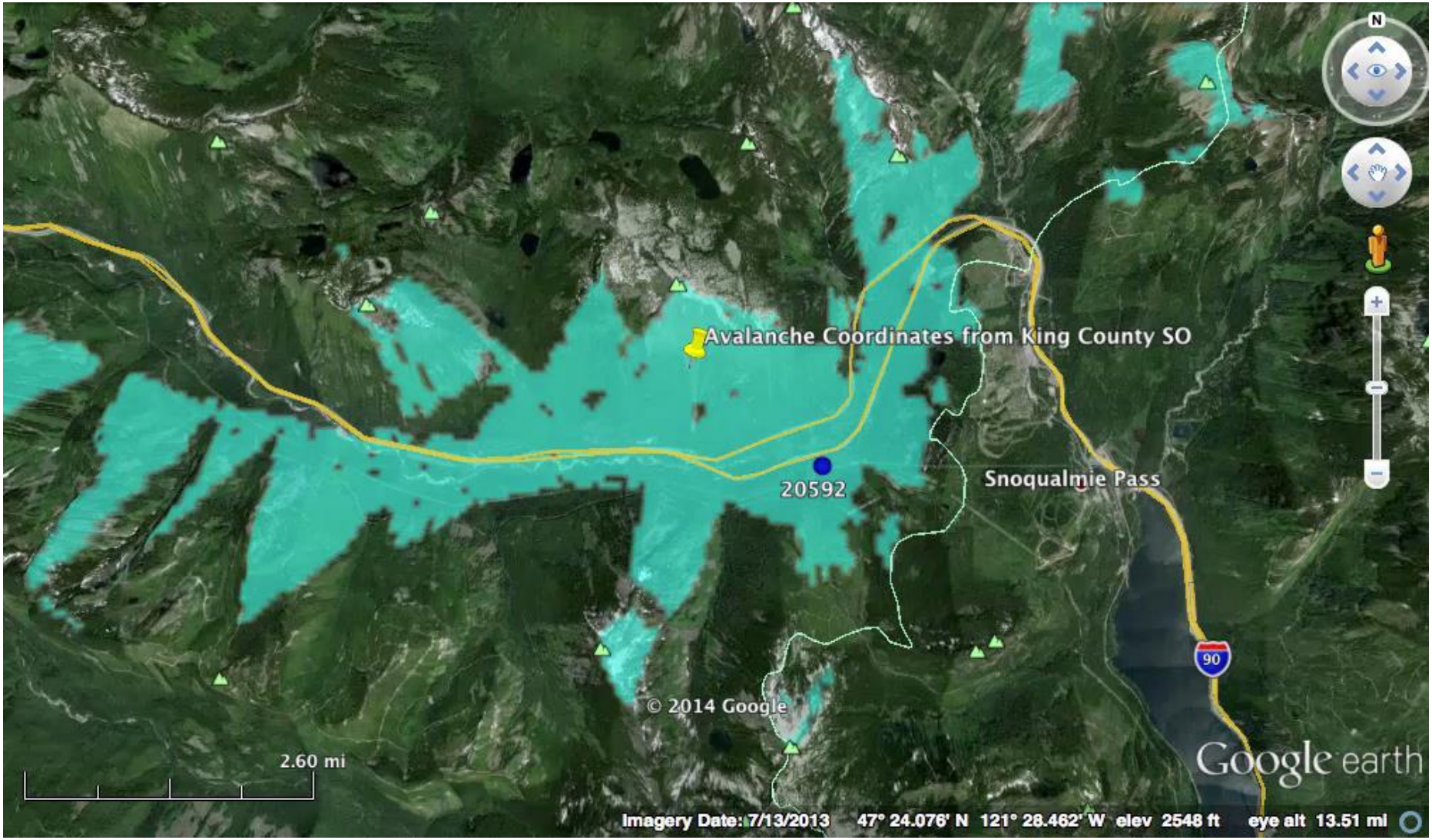
Data Types

- Raw Data
  - Obtained from various resources such as cell phone providers
  - Not distributed during a mission
- Analyzed Data
  - Raw data that has been scrubbed
    - To remove misleading information
    - To clarify ambiguous information
    - Focuses on data highlights pertinent to the mission (time line, locations, etc)
  - Time zone discrepancies are removed (or noted where ambiguity exists)
- Likely Areas
  - The “at a glance” look at where a phone was at a point in time

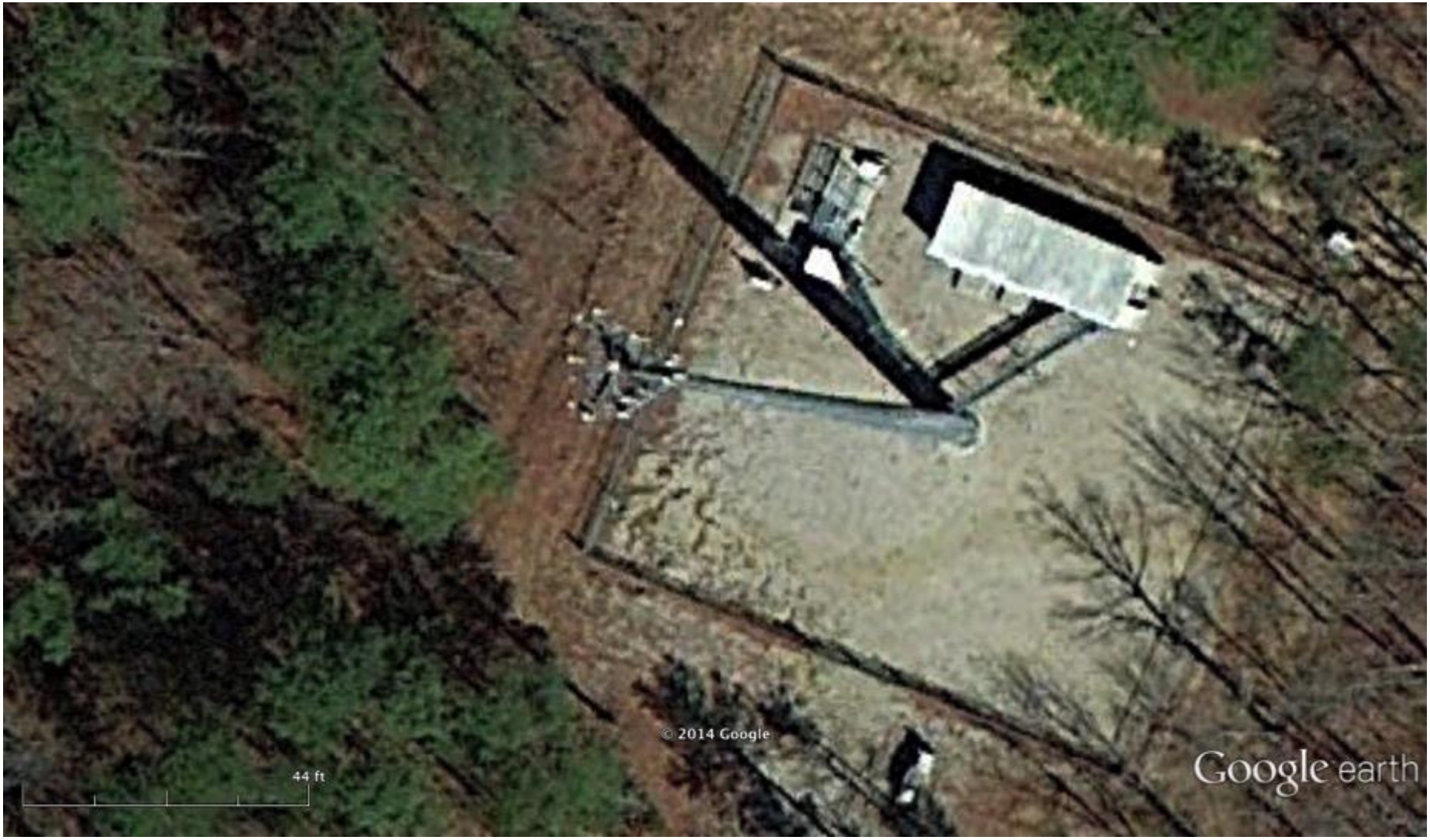
NHQC Analysis

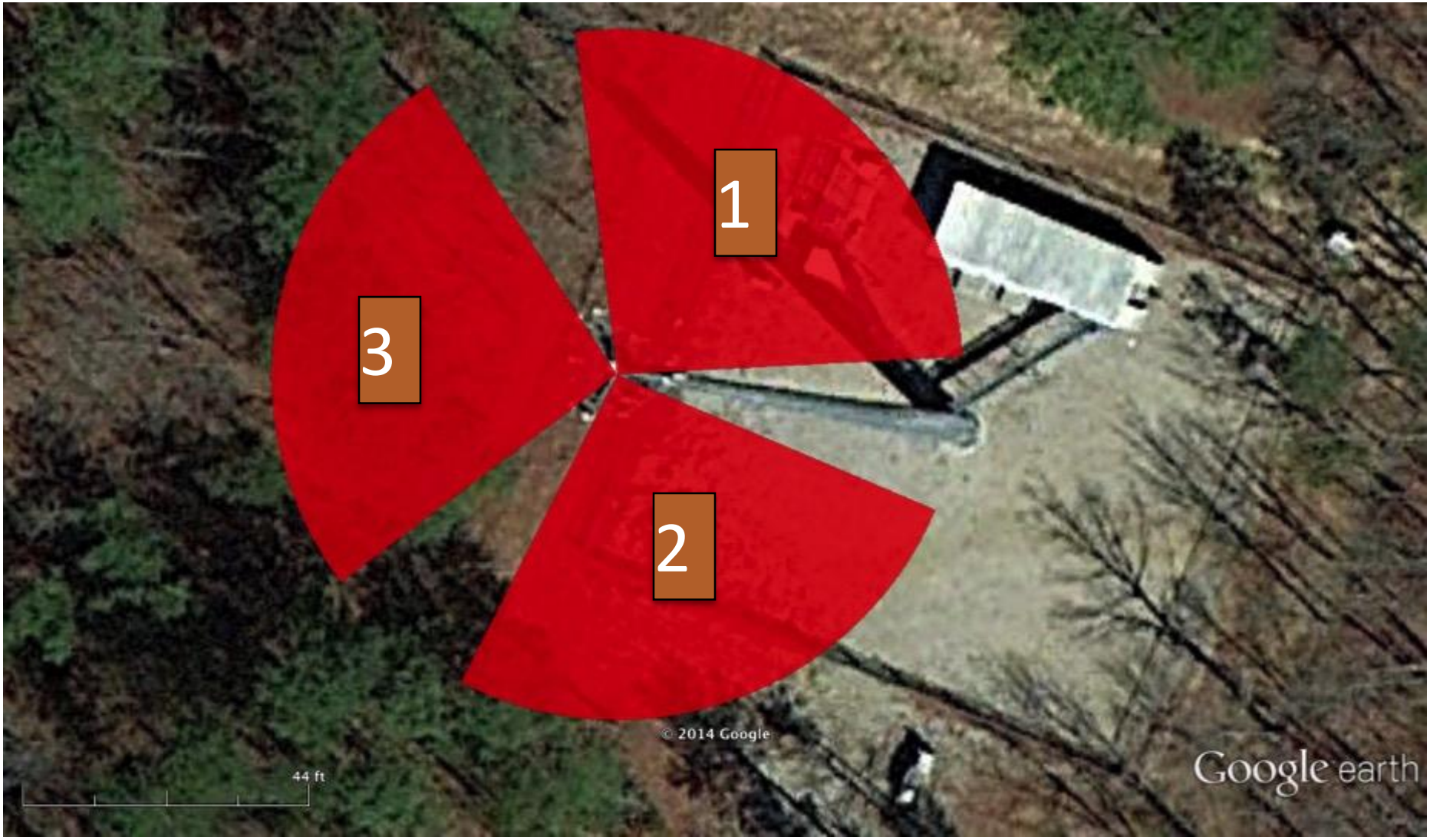
- Likely Areas
  - Likely Areas are the result of analysis and represents the location(s) of the phone during a specified time frame
  - Result of reviewing raw data
  - Takes into account tolerances of supporting data
  - Typically shown as an outlined area - bounding the area in which the phone was most likely to be located during the given time frame
  - Likely Areas correspond to a time frame
  - Gives the IC and Planning Section “at a glance” view of where a phone was located at a given time
  - Likely Areas are usually the only information provided for initial planning
- In Depth Analysis
  - We can go into more depth and explain how the Likely Areas were generated, answer questions specific to the cell data, etc
  - This is common for planning after the first operational period

Coverage Map



Sectors




1
2
3
© 2014 Google
44 ft
Google earth

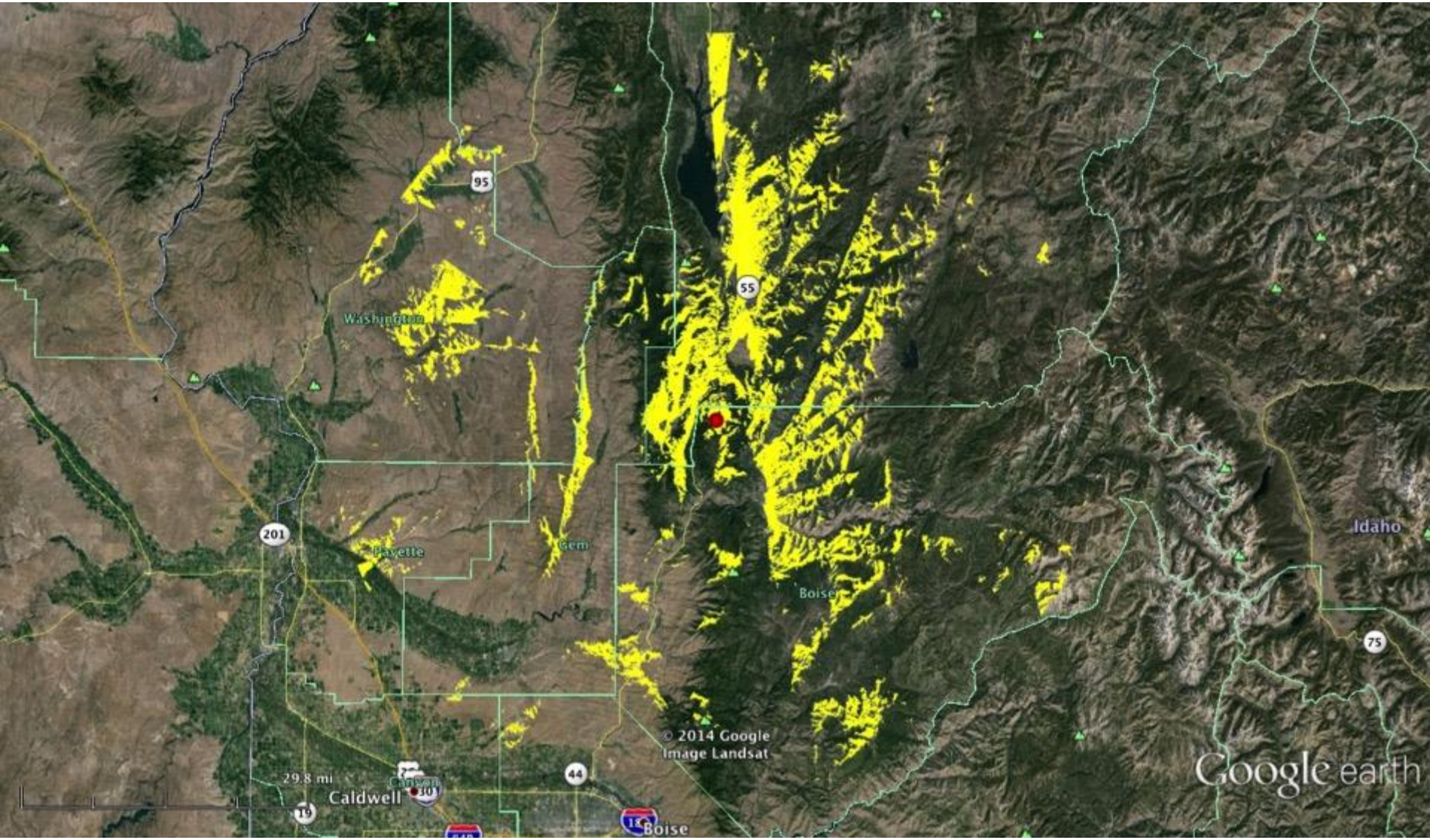
© 2014 Google
44 ft
Google earth

Likely Area Example

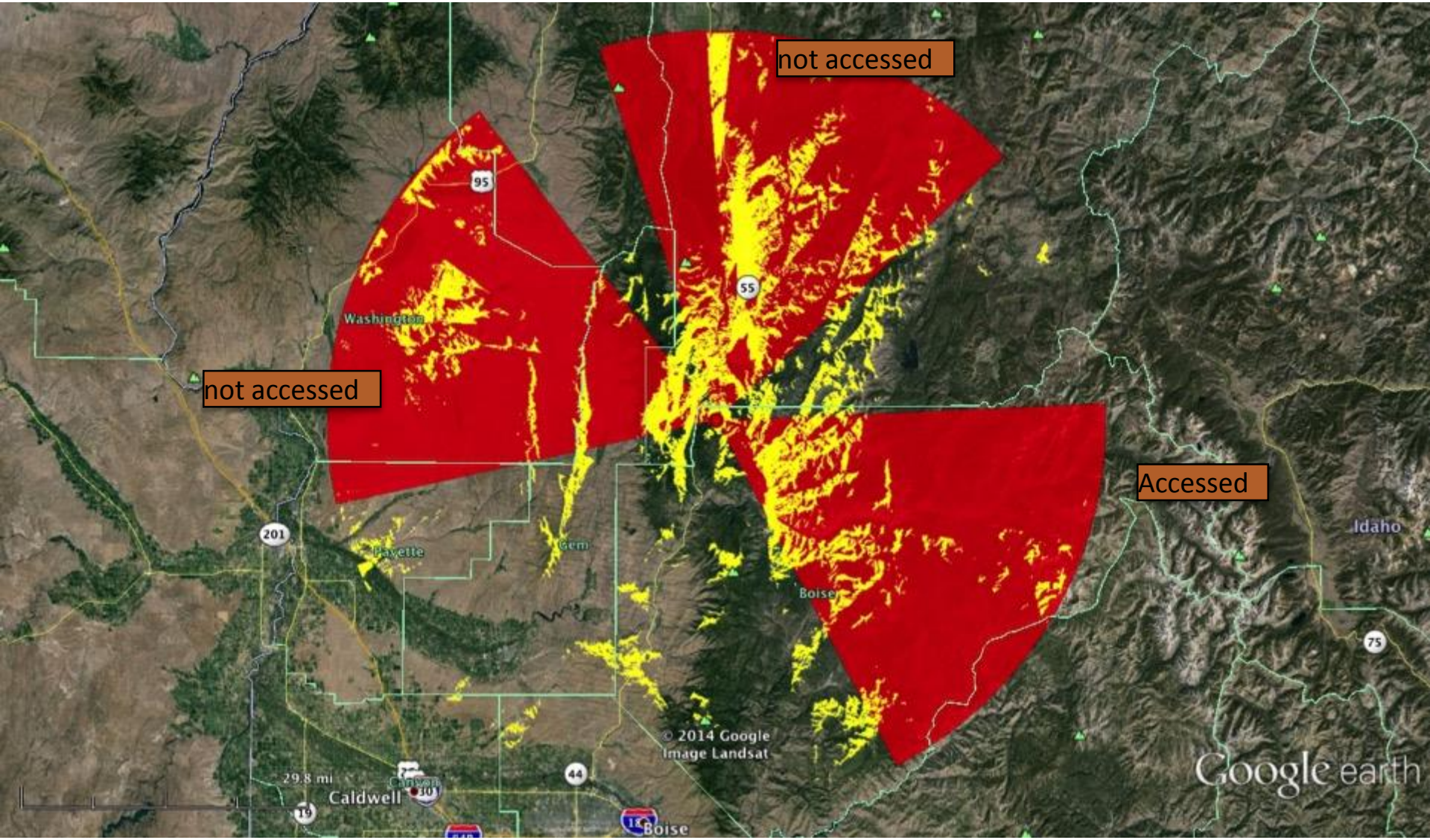
- Combining the raw data clues, we generate Likely Areas
- This is based on the available data and may include the tower location, coverage map, sector information, and more

Last tower used

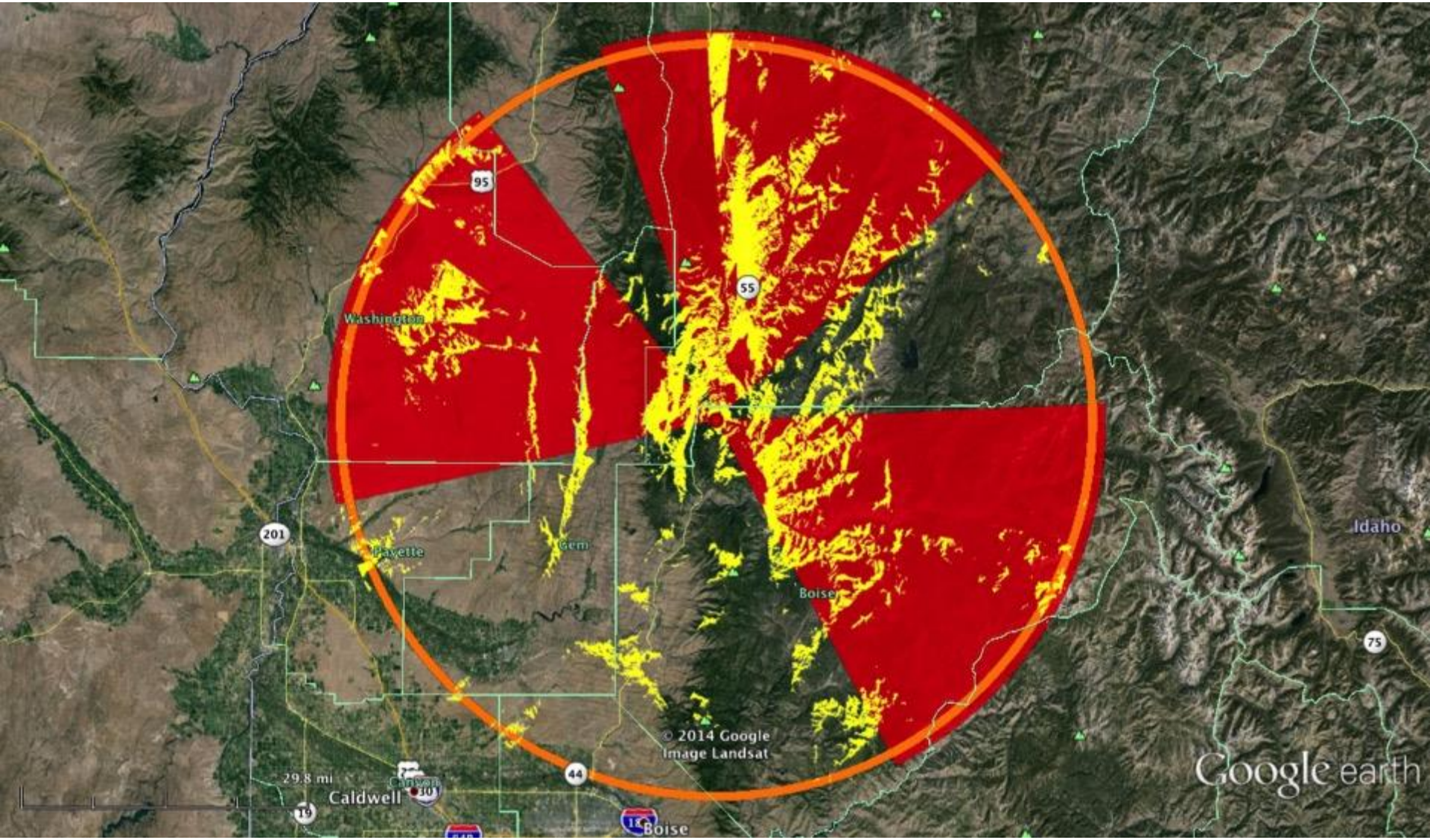
Coverage map for last tower used



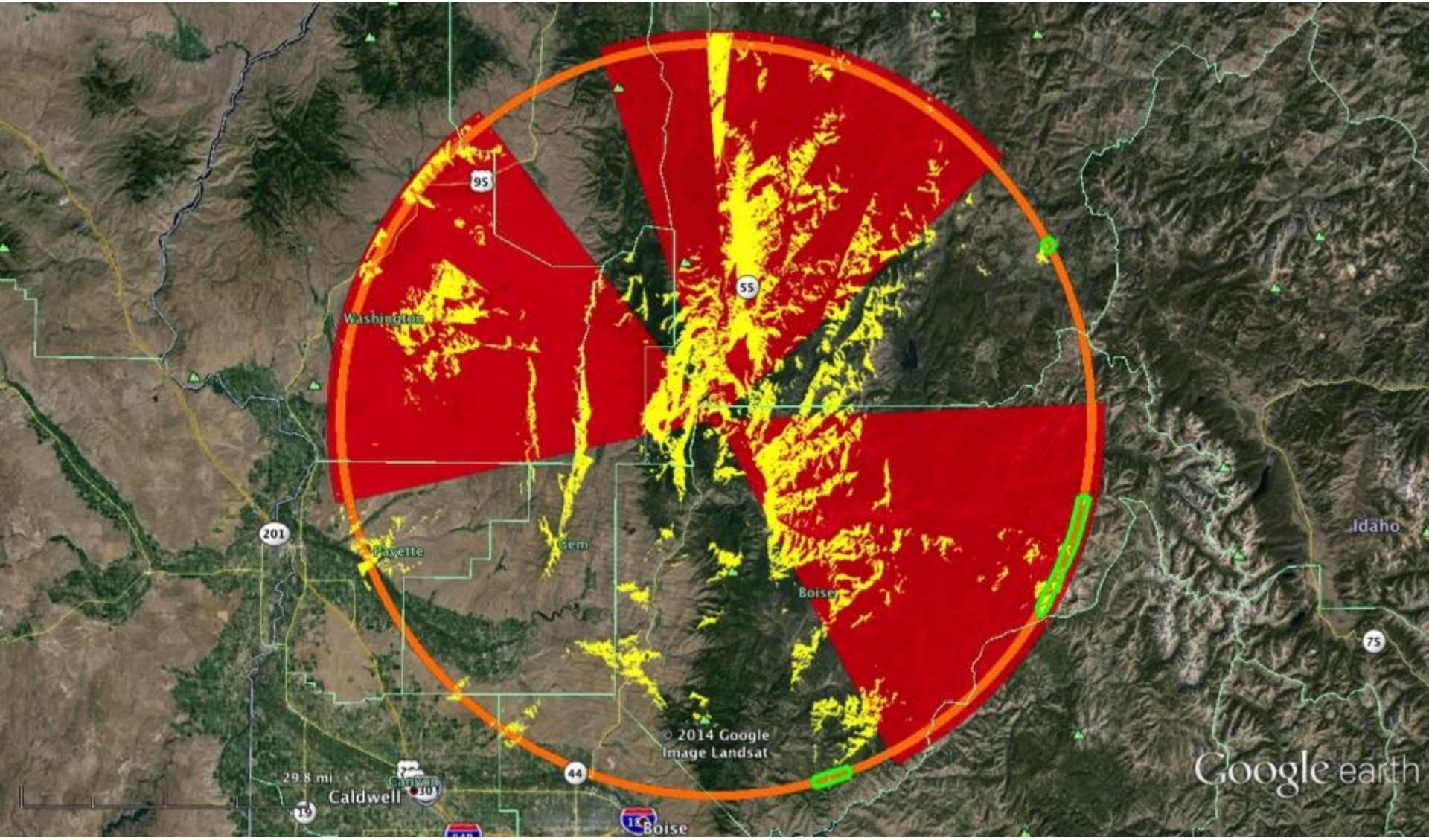
Last Sector Used



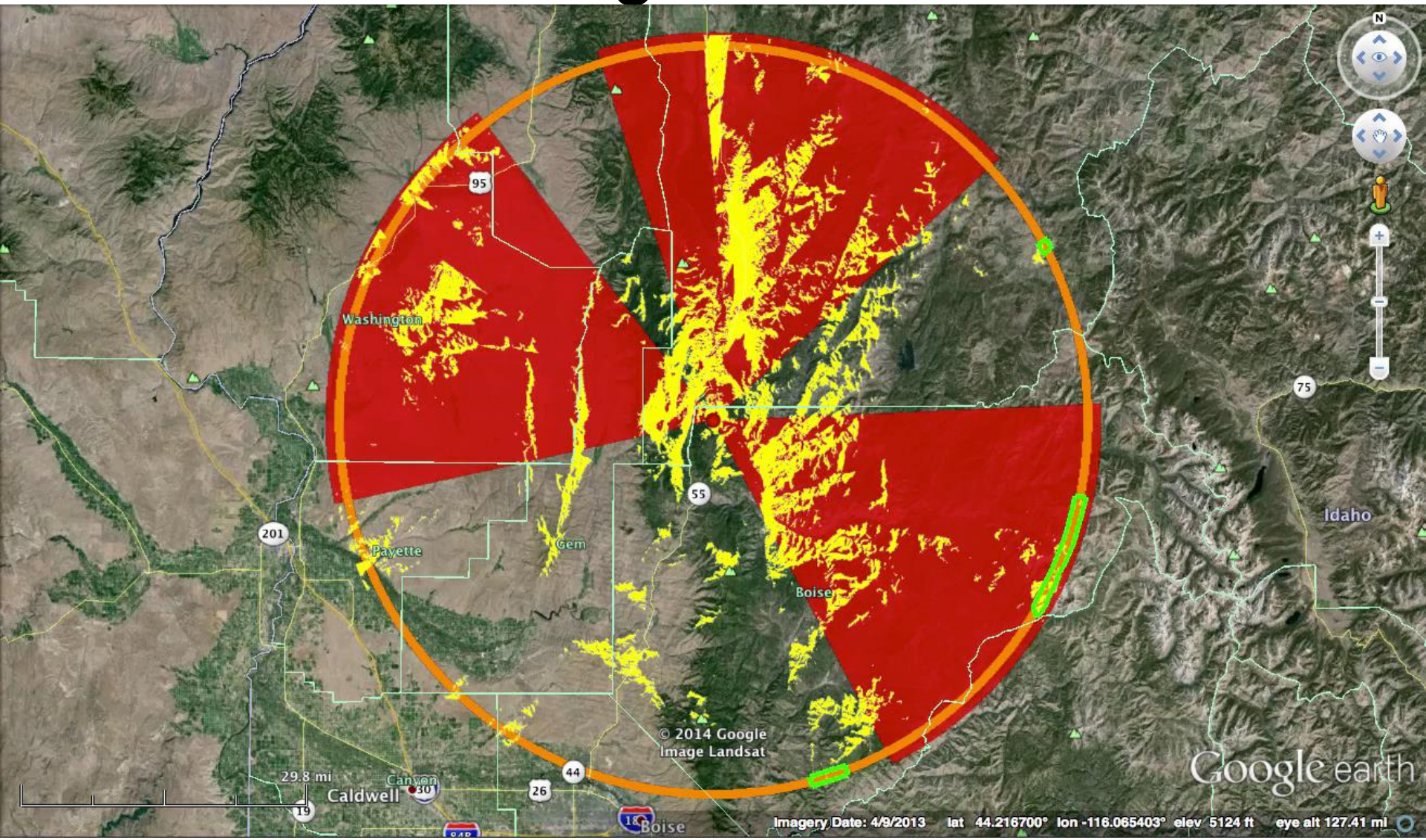
Distance information for last transaction



Likely Areas Defined



All the clues together leading to the find



The rescue!

Mission Examples

- The following slides are from actual missions
- They give a good sample of what to expect during a mission

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
Charles A. Tomko, Lt Col
AFRCC Commander

Cellular Forensics Data

Provided by

Air Force Rescue Coordination Center
Civil Air Patrol Cellular Forensics Team

AFRCC Mission Number: 15-M-xxxx

Mission Description: Missing horse back riders in ND

Presentation prepared by: Justin Ogden, Maj CAP

Brian Ready, Col CAP

Version 3

Version updates

- Version 1 – focused on coverage near the LKP only
- Version 2 – based on analysis of Carrier data
- Version 3 – Adds the 2035 Likely Area. Adds the 2119-2138 Likely Area. Removes the 2030-2119 Likely Area. Adjusted for MDT time zone.

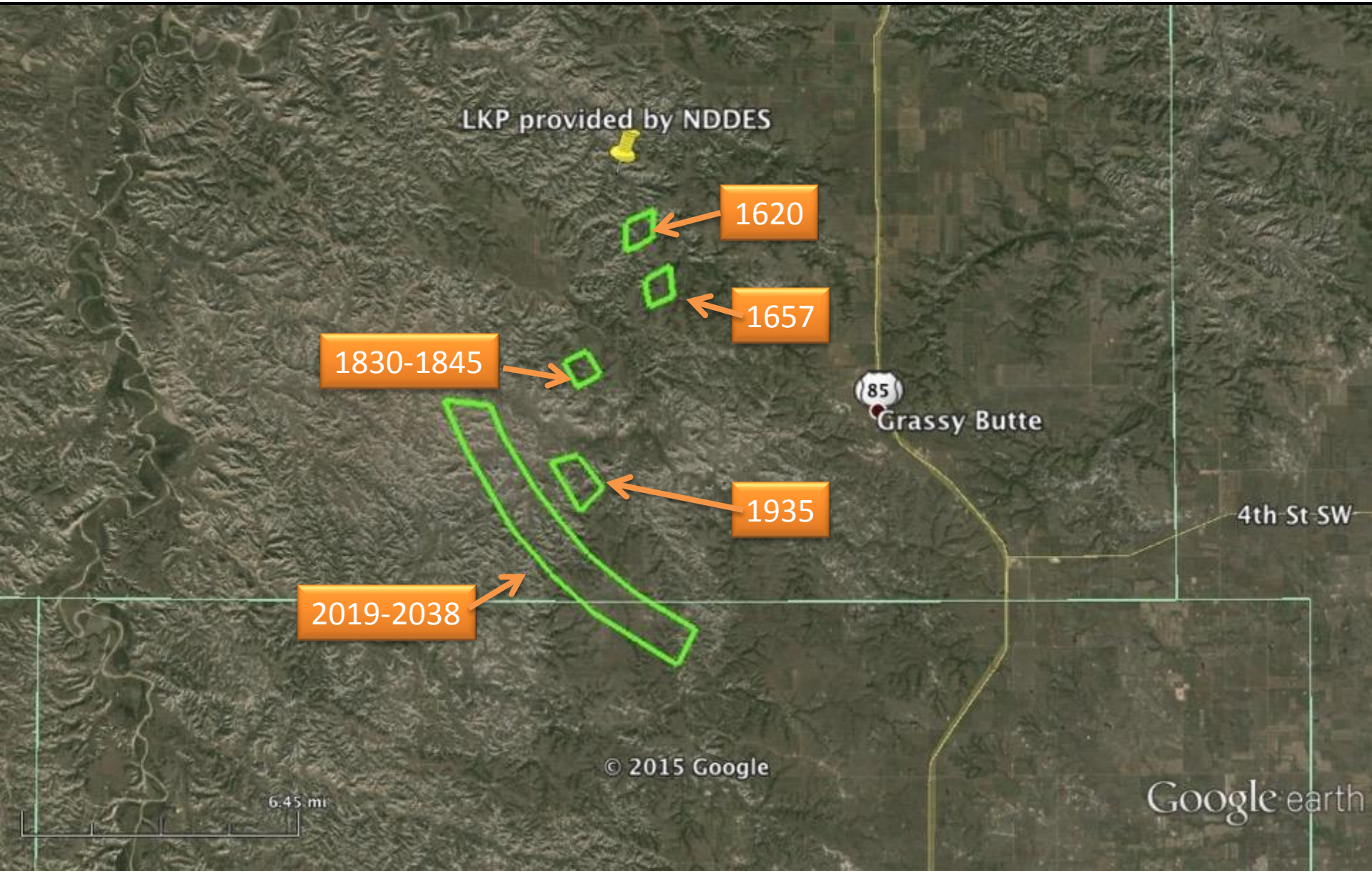
Overview

- 2 missing horse back riders (72 YOM and 50 YOF)
- One person has a phone ending in 2852
- (unknown 2nd phone number)
- LKP reported by NDDES is:
  - 47.47292° N 103.37793° W
  - (AFRCC Format: 47° 28.375' N, 103° 22.676' W)
- They started the ride at 1500 MDT (2100 Z)

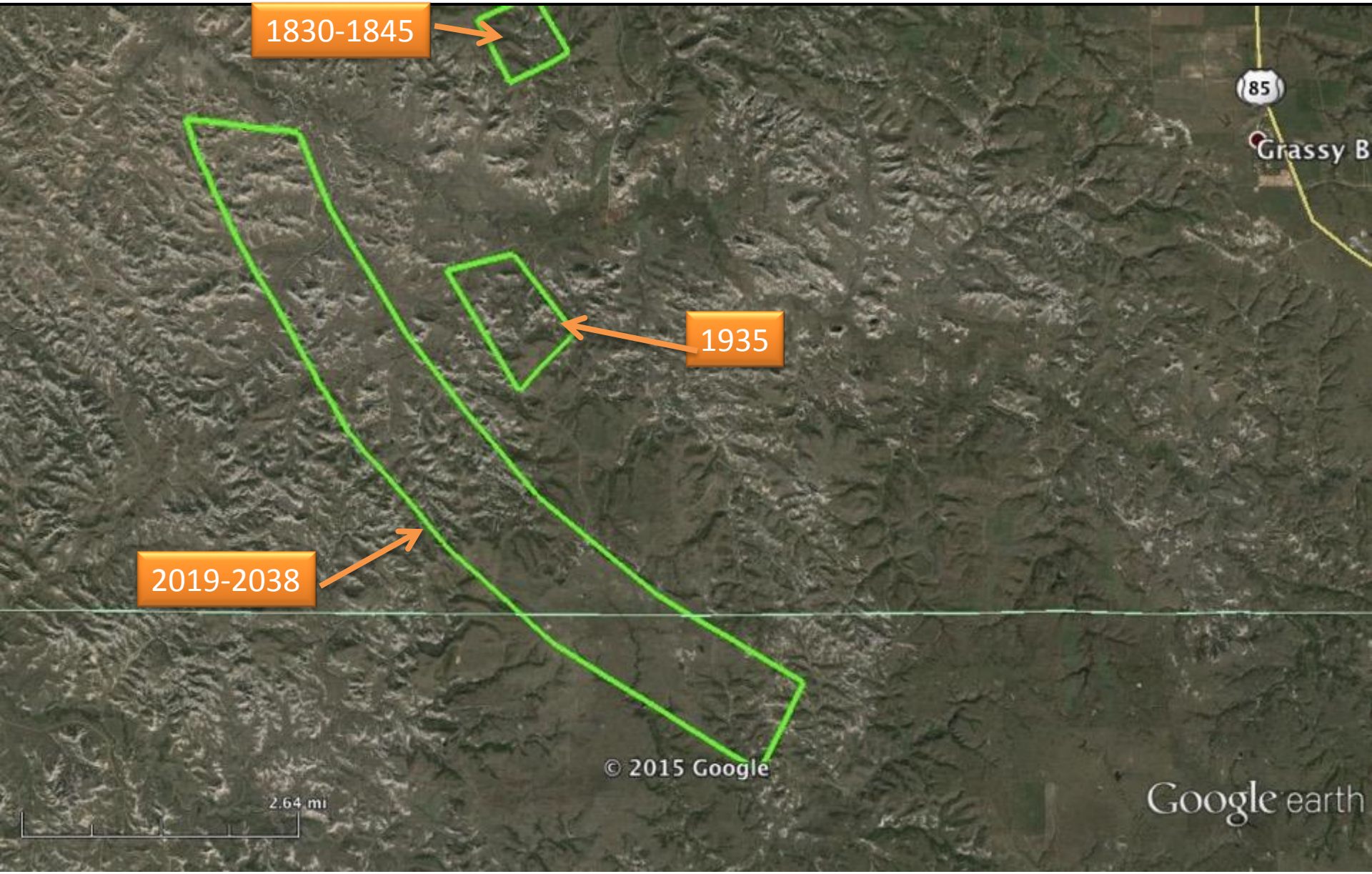
- Carrier has provided data
- The times in Version 3 of this presentation have been adjusted for MDT. (note that Version 2 presentation material was shown in CDT)
- We are showing Likely Areas the phone was in at
  - 1620
  - 1657
  - 1830-1845
  - 1935
  - 2019-2038
- The phone appears to be powered off or out of the coverage area at this time.

Likely Areas vs Time

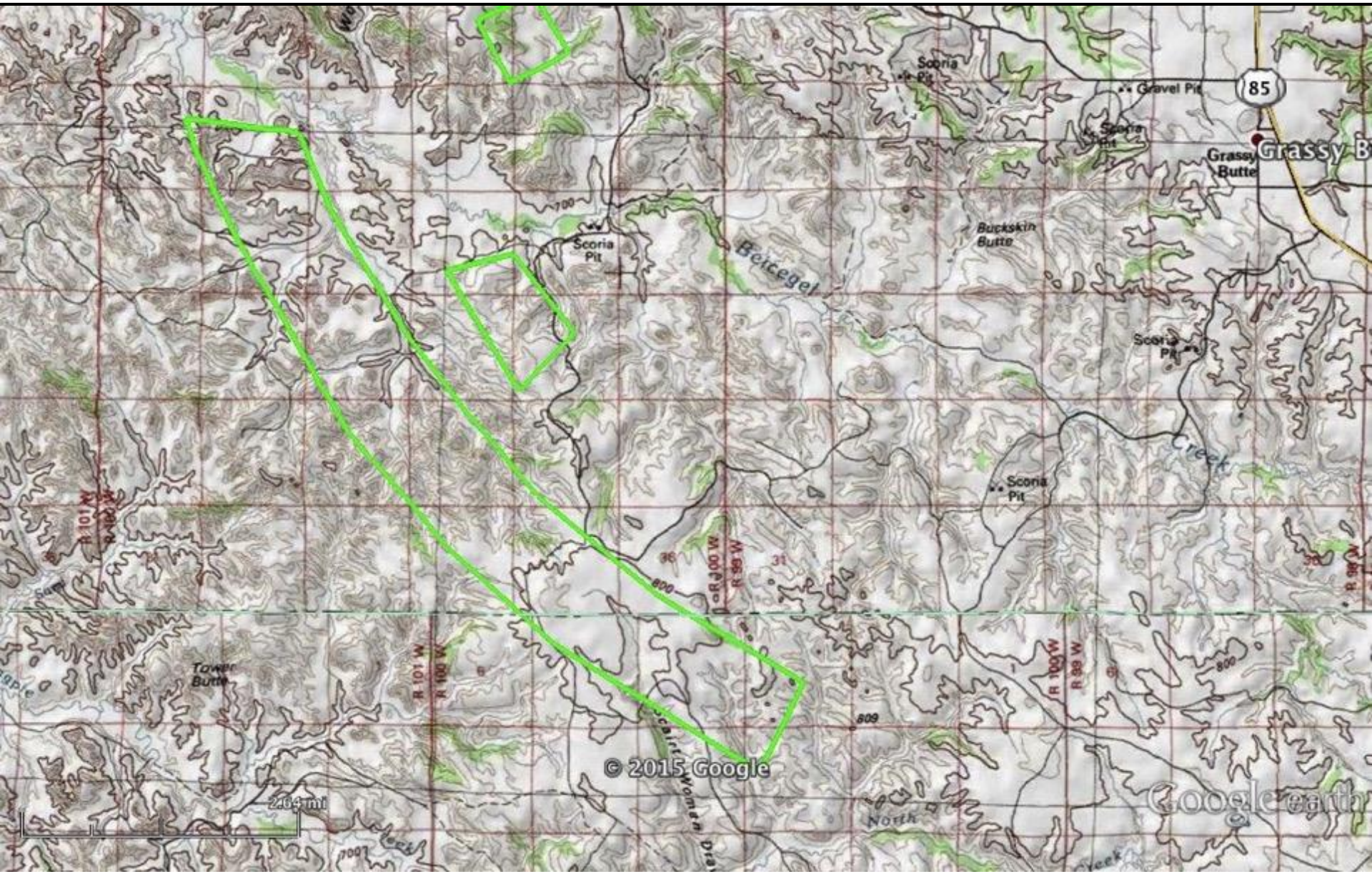
- All times are in MDT



Zoom to last three Likely Areas



Topo view


Scoria Pit
Gravel Pit
85
Grassy Butte
Grassy B
Buckskin Butte
Beiceget
Scoria Pit
Scoria Pit
Scoria Pit
Creek
Tower Butte
R 101 W
R 100 W
R 99 W
© 2015 Google
Google earth
North

Cellular Forensics Data

Provided by

Air Force Rescue Coordination Center
Civil Air Patrol Cellular Forensics Team

AFRCC Mission Number: 15-M-yyyy

Mission Description: Missing aircraft

Presentation prepared by: Justin Ogden, Maj CAP

Brian Ready, Col CAP

Version 2

Version info

- Version 1 – Initial data (goes to 2051 CDT)
- Version 2 – Updated with additional Carrier data that goes to 2057 CDT

Overview

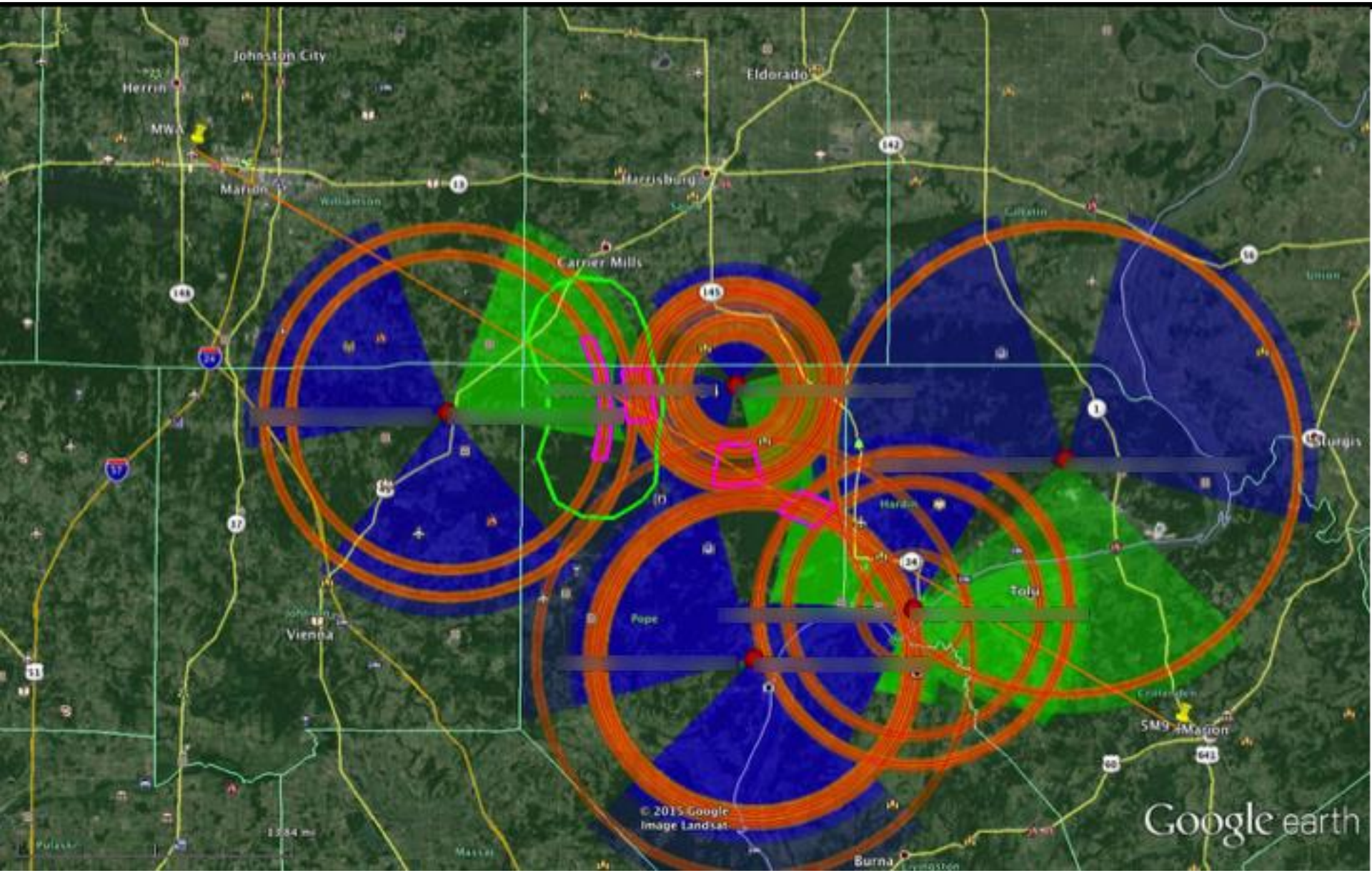
- Aircraft departed 5M9 around 2030 CDT (0130 Z) en route to MWA
- Pilot has a Carrier cell phone (ending 0486) and iPad (ending 5197)
  - There was activity on the pilot's phone, detailed in this presentation
  - **The iPad does show a time of departure from 5M9 around 2040 CDT (0140 Z)**
- Passenger has an Carrier phone (ending 3973)
  - Last contact with the Carrier phone was at 1529 CDT (2029 Z) on 9-Aug near MWA. It is *assumed* that this phone was left at MWA or at home. At any rate, it appears to not have flown on the trip.

Notes

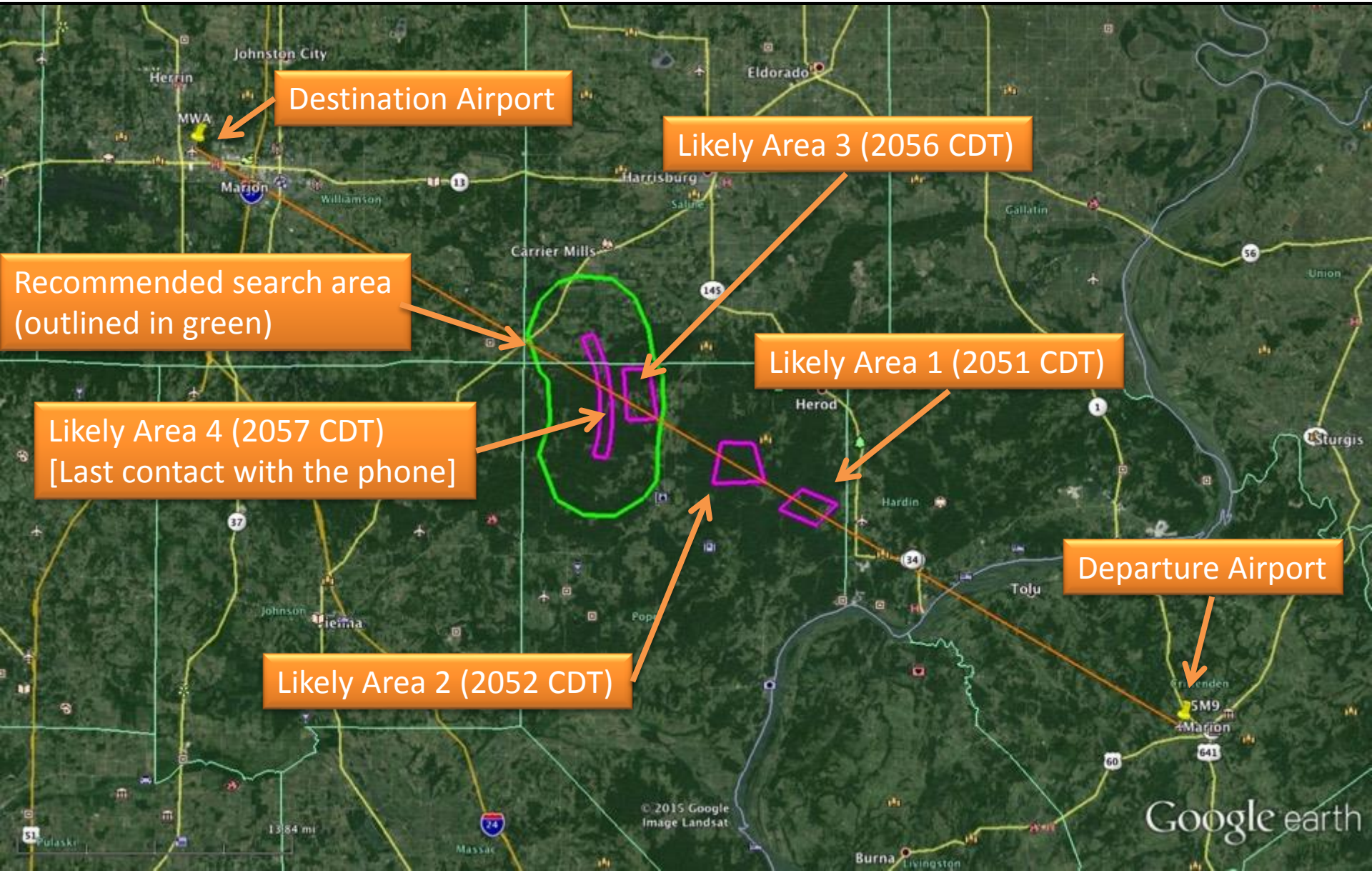
- Last contact with the pilot's phone was at 2057 CDT 9-Aug (0151 Z 10-Aug)
- Locations for the phone between 2051-2057 CDT are shown as Likely Areas outlined in purple
- An attempt to reach the phone at 2058 CDT failed, meaning the phone was turned off, out of range, or was damaged between 2057-2058 CDT
  - (an earlier report said that the attempted contact was at 2055, that was incorrect)

Raw Data

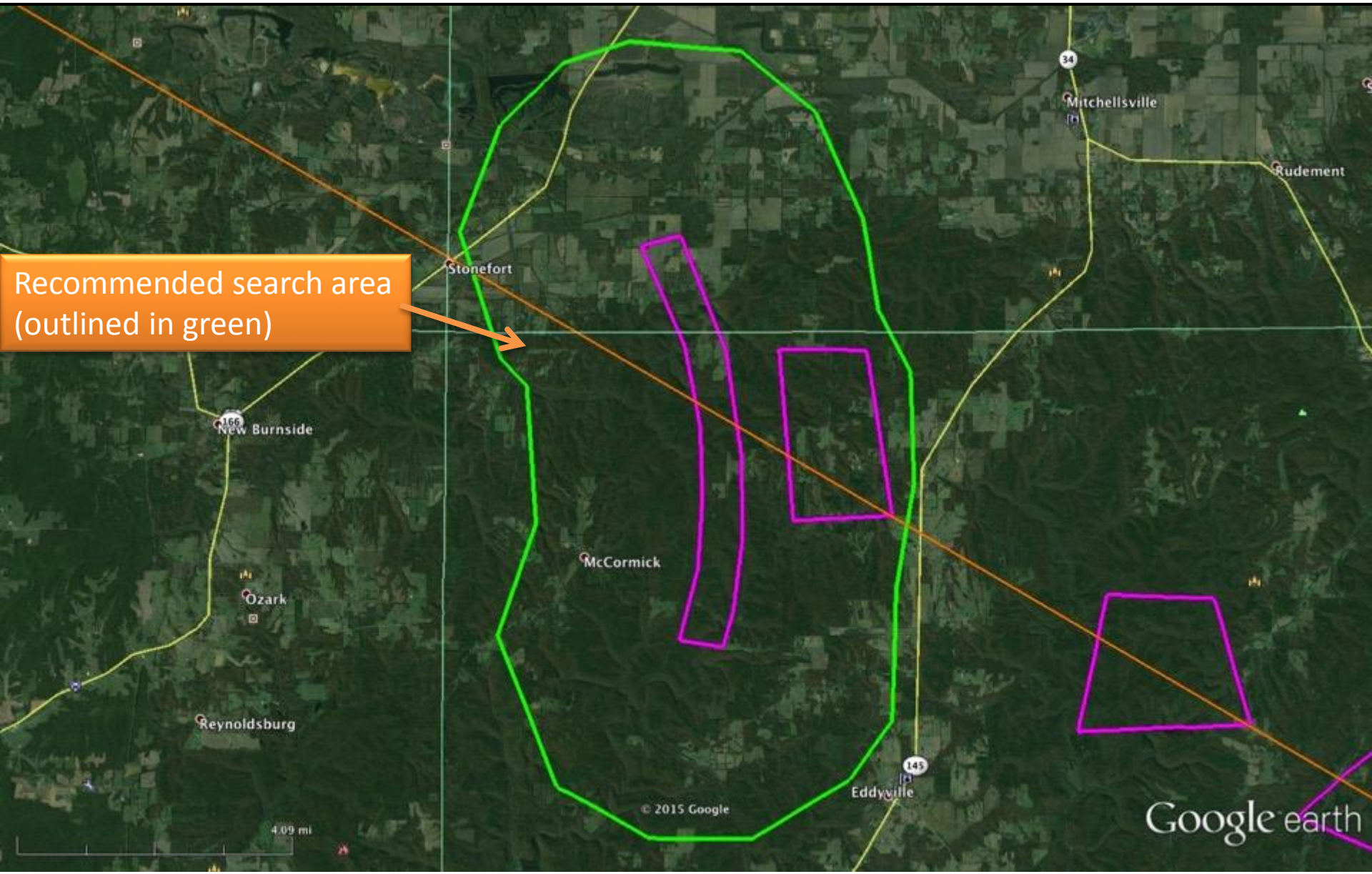
- All Carrier data for time of flight



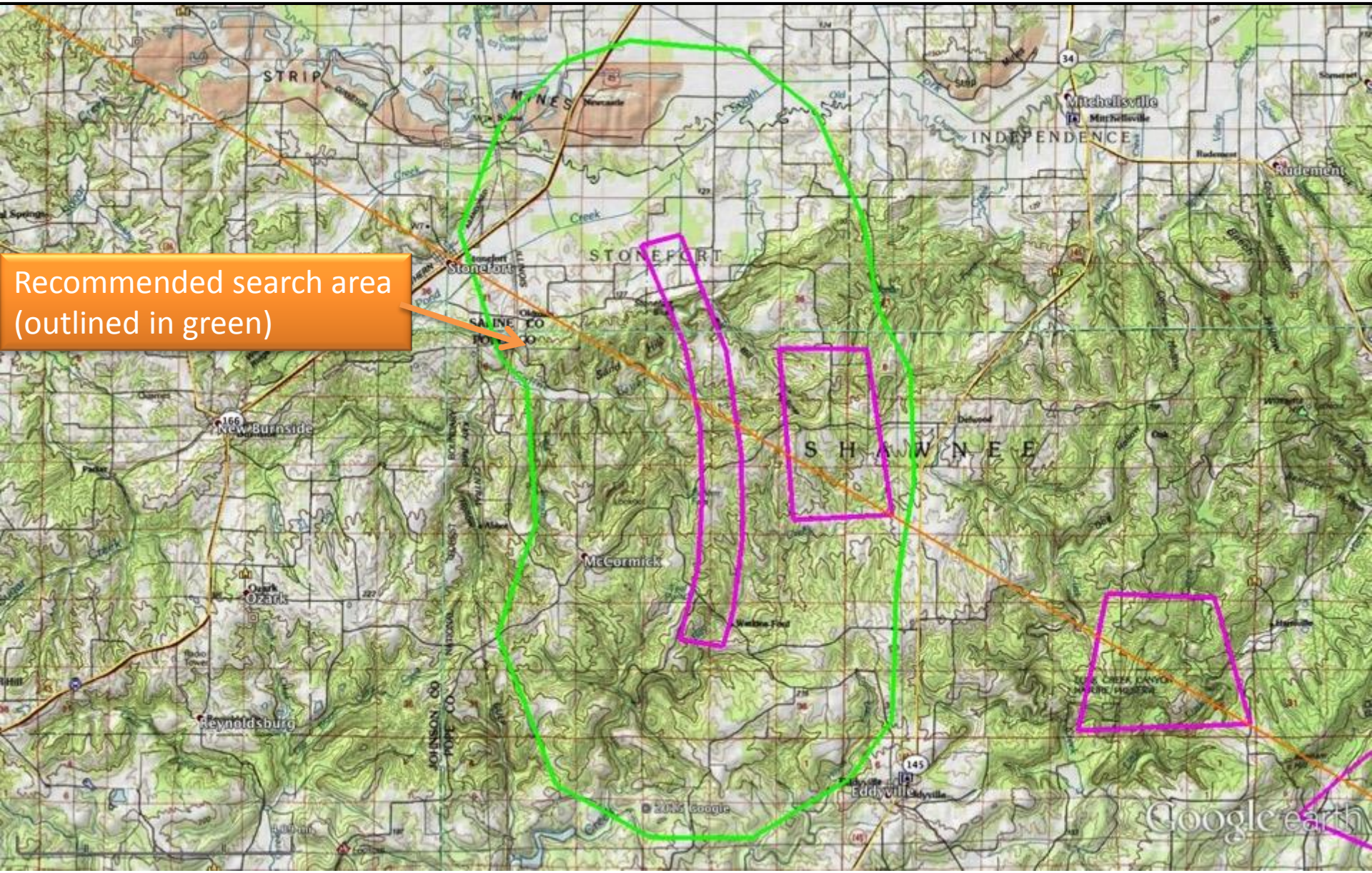
Route of Flight & 2051-2057 CDT Likely Area for the Pilot's Phone



Recommended Search Area

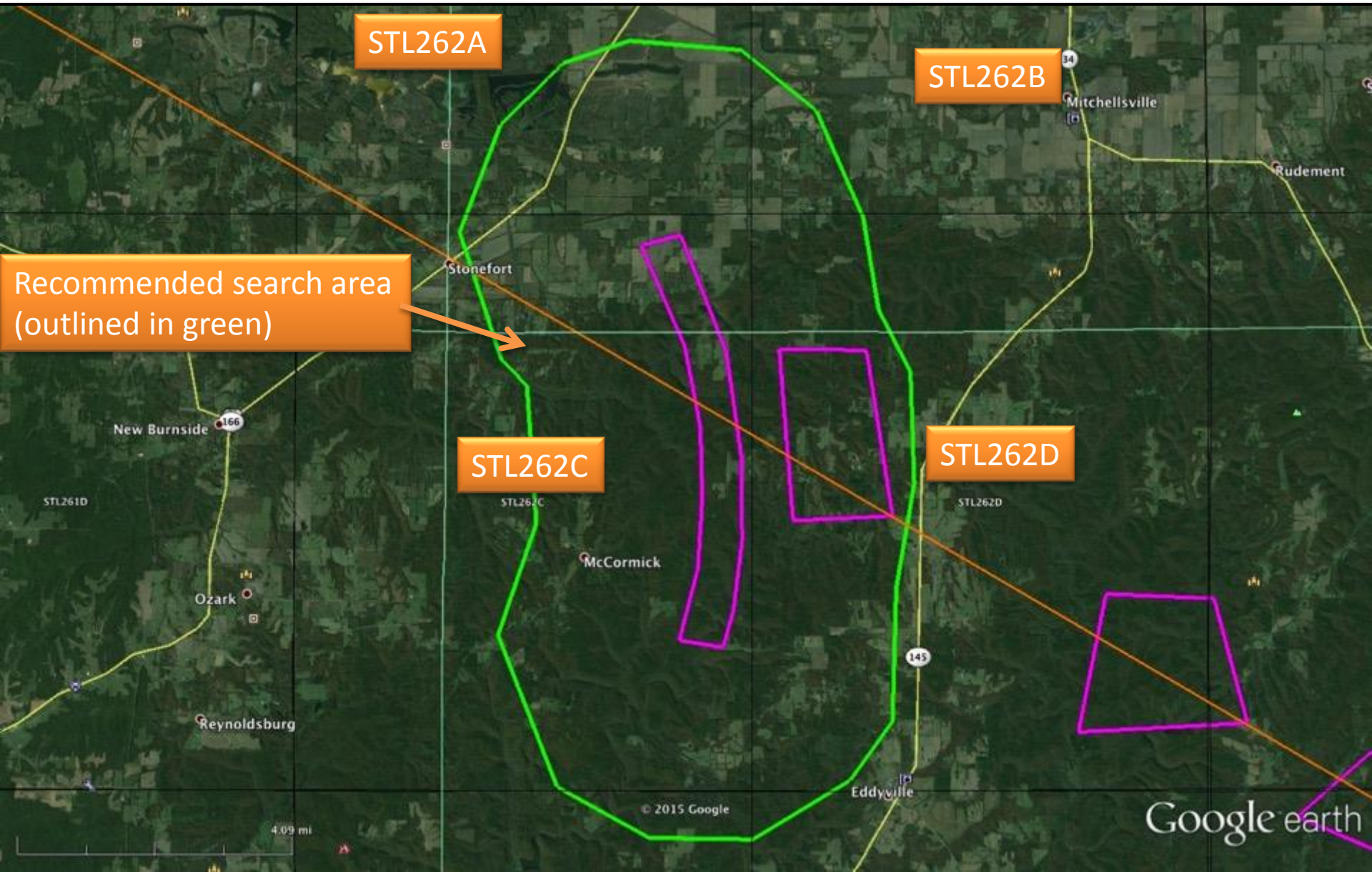


Recommended Search Area



CAP Search Grids

- STL262A, B, C, D
- Favors 262A & 262C



Cellular Forensics Data

Provided by

Air Force Rescue Coordination Center
Civil Air Patrol Cellular Forensics Team

AFRCC Mission Number: 15-M-zzzz

Mission Description: Missing boaters on Lake Michigan

Presentation prepared by: Justin Ogden, Maj CAP

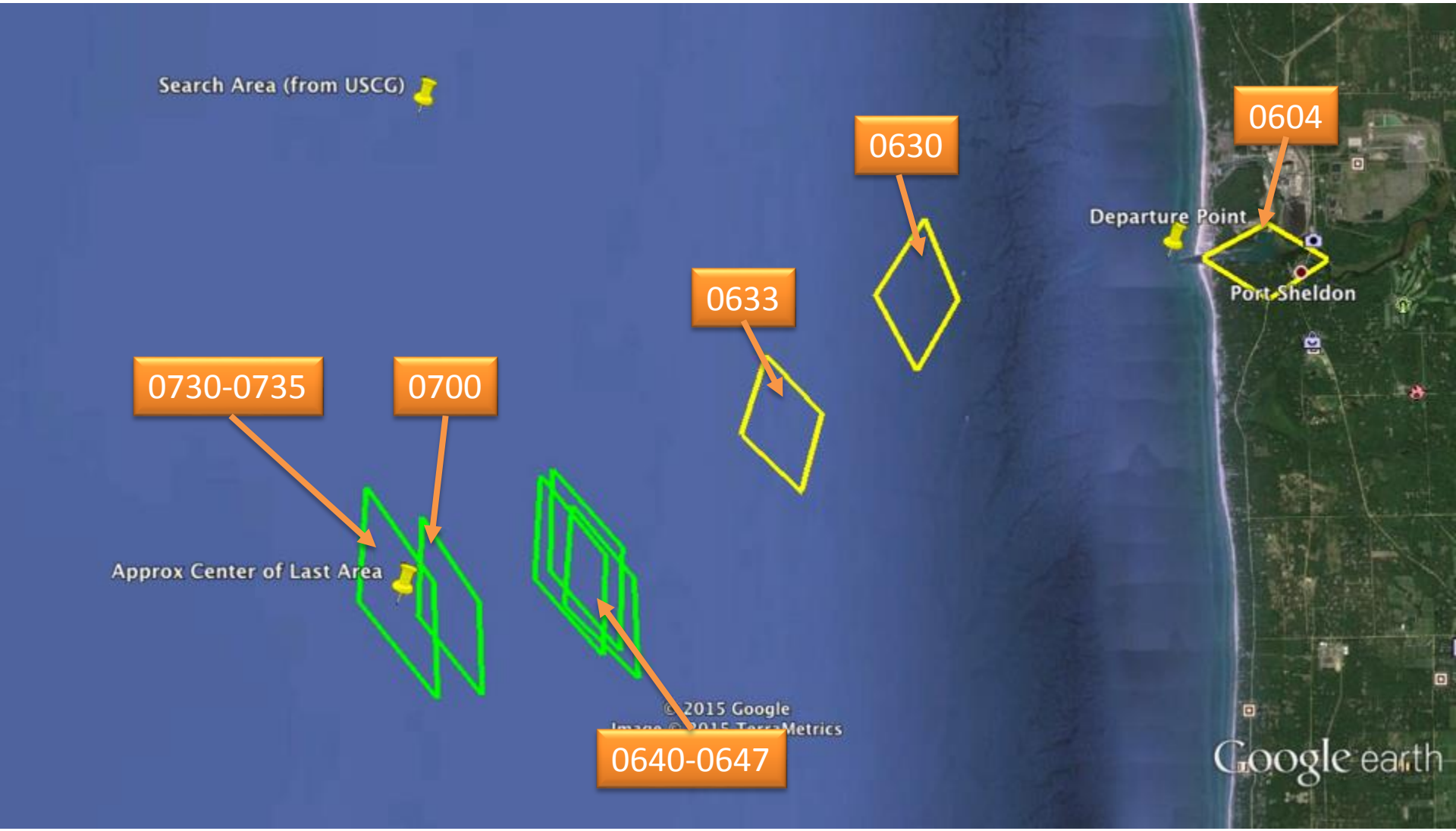
Brian Ready, Col CAP

Version 2

Version info

- Version 1 – Email after screen sharing session with AFRCC, District 9, and Sector Lake Michigan
- Version 2 – This document, that includes location information from records EVDO and LTE activity on the phone ending in 4107

Likely Areas vs Time (EDT on 26-Sep)



Cellular Forensics Data

Provided by

Air Force Rescue Coordination Center
Civil Air Patrol Cellular Forensics Team

AFRCC Mission Number: 15-M-aaaa

Mission Description: Missing boater in ND

Presentation prepared by: Justin Ogden, Maj CAP

Brian Ready, Col CAP

Version 1

Version info

- Version 1 – Initial data (there were some preliminary emails sent before this)

- The find was announced while generating the last few slides of this presentation.

Overview

- Missing boater in North Dakota
- Reported overdue 11-Oct
- Carrier phone ending in 7694
- The phone was very chatty with the network on 10 and 11 Oct until 1302 CDT.
  - We believe something happened at or around 1302 CDT on 11-Oct-2015 (such as the battery died, the phone was destroyed by water, the phone was turned off, etc)
- The following pages show location data leading up to the last activity.
- The outlined areas indicate the uncertainty in the measurement. The phone may be located anywhere inside the shape at the given time.
- All times are CDT on 11-Oct

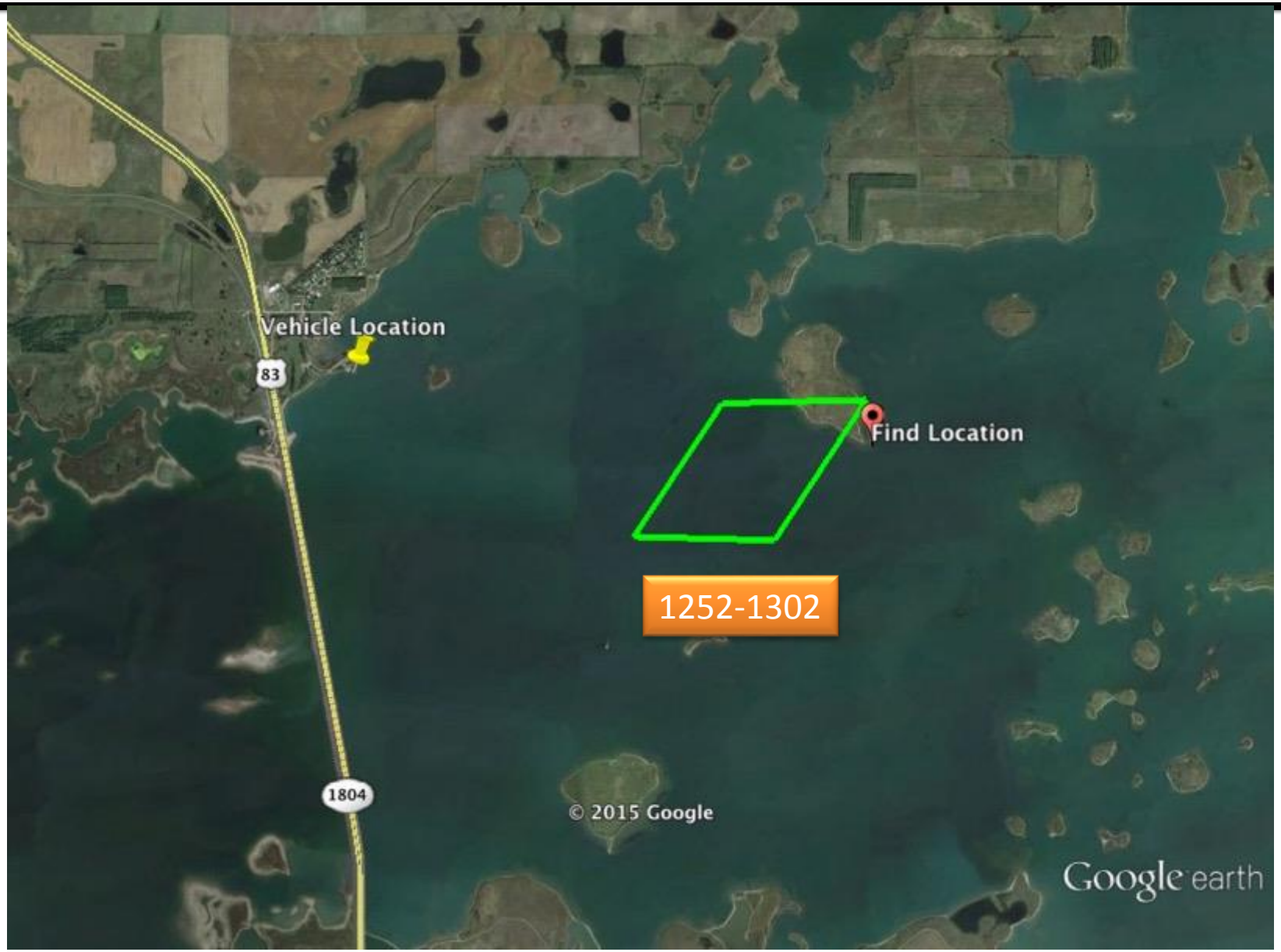
Likely Areas vs time

Likely Areas vs time

Likely Areas vs time

Find Location

- The Find was announced while generating this slide presentation



Tools and skills needed

- Tools & skills needed to get the most out of NHQC
  - Internet connection at Incident Command Post
  - Google Earth expertise
  - Google Hangouts (not required, but helpful)
  - Go To Meeting

How to activate us

- CAP Cell Forensics only supports AFRCC missions. Tasking must come from AFRCC.
- For missing aircraft searches, AFRCC will typically activate us immediately (many times before the local Wing)
- For missing person searches, it depends on the agreements between AFRCC & your state

How you can help us

- Ensure the data we provide is applied to the search correctly
  - For instance, if we have a real time location of a phone, it is imperative to investigate that location immediately
- Ask questions about the cell data if there is ambiguity
  - You can request AFRCC provide a conference call for mission staff and CAP cell forensics

Things to do during a search

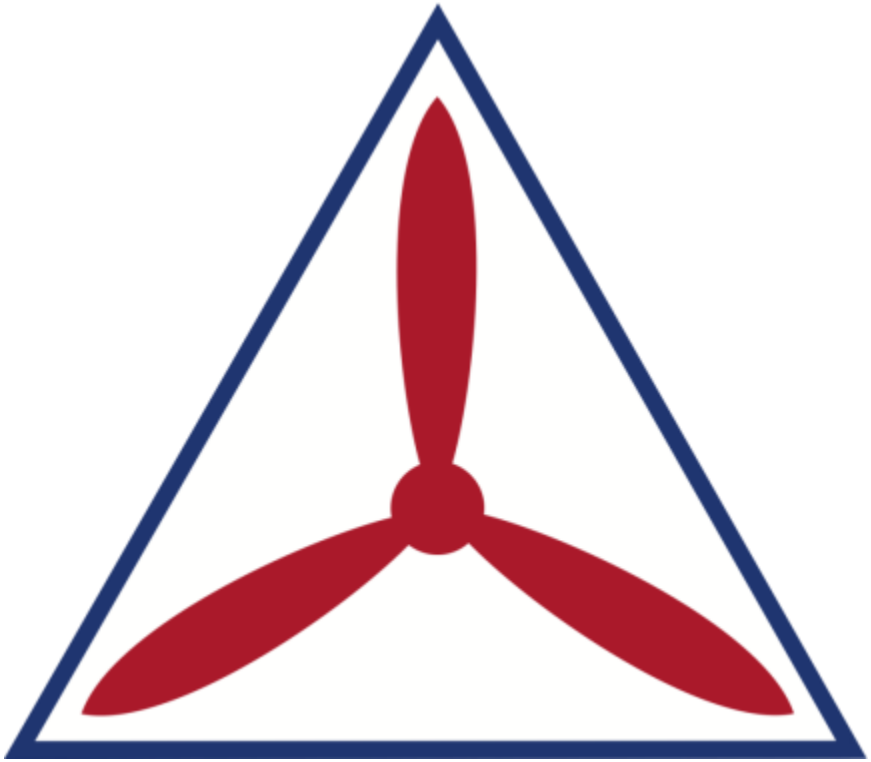
- Generate data
  - Get the objective to dial 911
  - Place calls and send text messages to the objective's phone regularly (log it!) - note the number of rings until the phone or voicemail answers
- Request AFRCC/CAP support
- **Trust the data produced by NHQC and NHQR - history has shown radar and cell phone data works!**

Cellular Forensics Team Contacts

- Justin Ogden, Maj CAP
- justin.ogden@forensics.cap.gov

- Brian Ready, Col CAP
- brian.ready@forensics.cap.gov

Civil Air Patrol



…Citizens Serving Communities!