Civil Air Patrol

2015 National Conference

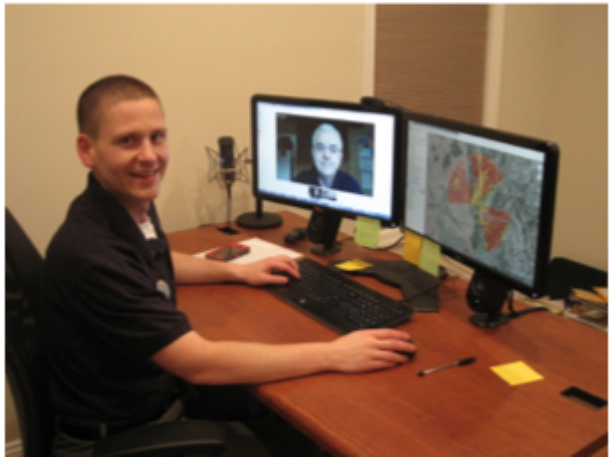
CAP Cellular Forensics

CIVIL AIR PATROL

Citizens Serving Communities

Who we are

- 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



What we offer

- **Collect**
  - the ***raw data*** from cellular providers, Public Safety Answering Points, and other data sources
- **Analyze**
  - the ***raw data*** for meaningful content
- **Present**
  - the ***analyzed data*** in a way that can be immediately applied to the search

How do we differ from what other agencies offer?

- 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 in-house 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 an in-house 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

Raw Data We Use

- Raw 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 reviewing cell phone data - ask yourself:
  - What time frame does this area represent?
    - Is it real-time, “post crash”, or historical before the incident that triggered the SAR.
  - How does this clue influence my search?

When is historical data recorded?

- Any interaction with the phone such as:
  - Calls
  - Text messages
  - Data usage
- GPS information is not recorded
  - The exception is calls to 911 which often have highly accurate coordinates, often derived from assisted GPS
- Apple iMessage, Facebook Messenger, Google Hangouts, etc show only as a data transaction

Products we produce

- 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 or 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

How to activate us

- CAP Cell Forensics only supports AFRCC missions. Tasking must come from AFRCC
- For missing aircraft searches, AFRCC will typically activate Radar and Cell Forensics 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
  - Request AFRCC provide a conference call for mission staff and CAP cell forensics

Things to do during a search

- Generate data
  - Get the victim to dial 911
  - Place calls and send text messages to the victim'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!

Questions?

Cellular Forensics Team Contacts

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

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