Cellular Records Review and Analysis
Part 1: AT&T
PATCtech

Glenn K Bard, Chief Technology Officer
Jim Alsup, Director – PATC
Scott Lucas, Instructor and Examiner
Steve Dempsey, Instructor
Kathy Enriquez, Instructor
Brian Sprinkle, Case Manager and Software consultant
Keenan Dolan, Webinar Manager
Stefani Lucas, Marketing Director
Glenn K. Bard
Public Agency Training Council tech
Chief Technical Officer
PA State Trooper – Retired
NCMEC – Project ALERT
CISSP, EnCE, CFCE, CHFI, A+, Network+, Security+, ACE, AME
For Starters

• What can we get from AT&T?
Cell phone technology

• What can AT&T provide with appropriate legal process?

  • Call detail logs
  • Cell Sites accessed
  • Cell site sector Azimuth
  • Beam Width
  • Direction of call (incoming or outgoing)
  • Calling number
  • Dialed number
  • Call Time and duration (UTC)
  • Data usage location information
  • Location of cell tower
Cell phone technology

• Subscriber information (Name, address, etc)
• SMS location information
• IMEI, IMSI of target phone.
• Phone Model
• Tower dump
• Definitions page (Key Codes)
• Reports of Lost / stolen phone
• If prepaid, where purchased?
• Other phones on the same account
• Cell sites at the time of the incident (Not current)
• Historical Handset Location (Nelos)
• Contents of the Cloud
Some important definitions

• IMEI – International Mobile Equipment Identifier
• IMSI – International Mobile Subscriber Identifier
• MSISDN - Mobile Station International Subscriber Directory Number (It means your phone number)
Some important definitions

- **LAC / CID** – This is the switch (LAC – Location Area Code) and tower along with side (CID – Cell ID) accessed
- **CGI** – Cell Global Identifier
- **Azimuth** – The median of the sector accessed
- **Beam Width** – The width of the sector accessed
- **MCC** – Mobile Country Code
- **MNC** – Mobile Network Code
Some important definitions

- **Seizure** – The time it takes for the call to connect to the network. NOT the elapsed time.
- **ET** – Elapsed Time
- **CT** – Call Type
- **UTC** – Universal Time, also known as GMT
Some important tips

• The location is Longitude then Latitude
  – This is the opposite of all other companies

• MSISDN - Mobile Station International Subscriber Directory Number (It means your phone number including country code)

• The records will come in both PDF and TXT
  – If you want Excel, we will learn how to import TXT into Excel in a bit.
Some important tips

• AT&T can provide locations for Voice, SMS and Data for a very long time. (Which is not common.)

• Tower Dumps also include Voice, SMS and Data. (Which is not common.)

• AT&T does not use the terms Lucent or Nortel when describing the tower sides. They simply give the Azimuth. (Which is not common.)
Some important tips

- **NELOS**
  - AKA: “historical GPS Locations”, “Historical Handset Location data”, and “Handset triangulation data”
  - Technically: Network Event Location System
  - What it means is an estimate of the location of the handset itself at the initiation of the event.
  - How accurate can it be:
Some important tips

• NELOS

<table>
<thead>
<tr>
<th>Location Accuracy:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>11</td>
</tr>
<tr>
<td>12</td>
</tr>
<tr>
<td>13</td>
</tr>
</tbody>
</table>
Contact information (updated)

AT&T Wireless
208 South Akard, 10th Floor
Dallas, Texas  75202

Phone Number:  800-291-4952
Fax Number:    888-938-4715
E-mail Address: compsent@att.com
Note(s):        AT&T will now accept service by email at: compsent@att.com
Contact information

Two Hints:

AT&T now owns Cricket.

TracFone sells phones that use the AT&T towers, so the records must come from AT&T.

We will get into both of those in Part 4 of this series.
Warrant language

• Subscriber information for the number ______________ including name, date of birth, mailing address, alternate phone number, and other numbers on the same account.

• All communication for the wireless number ______________ for the time period of ______________ to include cellular calls, SMS messages and Data communications, tower locations (LAC / CID) and azimuth for the sectors accessed during the communication. Also, identify the existence of any AT&T cloud services associated with the wireless number of ______________ and provide any data held within the cloud to include SMS, MMS, and emails communications. Additionally, supply “historical GPS Locations”, “Historical Handset Location data”, “Handset triangulation data”, aka NELOS (Network Event Location System). Also provide any IP (Internet Protocol Addresses) assigned to the device for the time period of ______________. Lastly, provide a detailed definitions page which identifies all information in the records.

• Please provide this information to Detective ______________ in digital format on a compact disc in Excel, PDF or TXT format.
Retention periods

Subscriber information: 7 years
Call History: 7 years
Tower Locations: 7 years
SMS Content: Not available
Tower Dumps: 7 years
NELOS: 90 days
Now let’s see some examples of what you can get:
Follow PATCtech!

- PATCtech
- @PATCtech
- Forensic Digital Evidence Investigators (LinkedIn Group)

- Updates & PATCtech Research
- Public Safety News
- Training Opportunities