When an individual or group of individuals is suspected of criminal activity, accessing the Call Detail Records (CDRs) of the suspects can provide powerful evidence of innocence or guilt. This paper discusses available analytical techniques that crime and other analysts can use within the SS8 Intellego™ solution to analyze CDRs as part of their investigations.

CALL DETAIL RECORDS (CDRs)

Every time someone places or receives a call using a cellular telephone, a Call Detail Record (CDR) is generated by the cellular provider. The amount of data in the CDR varies by carrier, but the record will almost always have the following fields: the phone number, IMSI and IMEI of the subscriber’s phone, the dialed number (along with any post-dialed digits), the duration of the call, and the cell tower or towers that the subscriber’s phone was connected to during the call. Investigators and analysts have been using this information for decades to track with whom an individual suspect may have communicated. But modern technology has enabled investigators to learn even more from the mountain of data that is generated in these communications.

Many people use their cellular phones dozens of times per day, and each call contains interesting data about the suspect’s activity on that day. SS8’s Intellego™ allows investigators and analysts to reconstruct and analyze this data to improve their understanding of a subject’s activities. When an individual or group of individuals is suspected of criminal activity, accessing the CDRs of the suspects can provide powerful evidence of innocence or guilt. For example, by plotting the cellular towers that the suspect accessed for each call (Figure 1), an investigator can obtain independent evidence of a suspect’s whereabouts at any date or time desired.

Many CDRs even contain the direction from the tower and an approximate distance of the target phone during the call, so a more precise location can be plotted (Figure 2). When several individuals are involved, the CDRs can provide evidence that they physically met at a specific date, time and location.
IDENTIFYING AND FINDING THE PATTERNS

Hierarchy
In addition to location, crime and other analysts can learn a lot by looking at the pattern of calls, both between suspects and to outside numbers as well. By visualizing the sent and received calls in a link chart, relevant patterns can become immediately apparent. For example, the hierarchy layout (Figure 3) in Intellego™ provides the investigator with an inferred hierarchy of the individuals involved based on the pattern of their phone calls back and forth. This is particularly useful when trying to identify key players who can be singled out for further investigation.

Centrality
Intellego™ also calculates centrality measures for the network of intercepted CDRs. There are three key metrics that help investigators understand the true nature of the network, both from a targeting perspective and from an intercept perspective.

Degree Centrality
An analyst may want to pare down the network to reflect only the individuals who have made or received more than a couple of calls to help focus the investigation on the key players. To do so, they would calculate a metric called degree centrality. Degree centrality assigns a score to each entity based on how many links originate from the entity. This is useful to pare down the network of phones in the CDR records. Numbers that have only been called once are likely not pertinent to the investigation and can be excluded from the chart, so that the investigator can focus on the important phone calls.

Closeness Centrality
To decide who in the network to target, an analyst would calculate closeness centrality. Closeness is a measure that describes how close to the center of the network an individual might be. Phones (and the subscribers to those phones) are given high closeness scores if they are connected to other highly connected nodes within the network. This means that someone who places many calls to other people who also themselves place many calls within the network are likely closer to the center of the network. From a targeting perspective, removing people with high closeness scores from the network by arresting them, for example, causes the most disruption to the communications structure of the network.

Betweenness Centrality
When attempting to gather more information about the network, an analyst may want to calculate the betweenness centrality of each node. Individuals with high betweenness scores are not necessarily the key players, but are more often the conduits of information. The phone that has the only calls between two separate groups who mostly call other members of the group will have a very high betweenness score. From an intercept perspective, intercepting the communications from that phone will gain the investigator the most information about the network, even if the person isn’t necessarily highly placed within the organization.
**CDR ANALYSIS ON LARGE DATA SETS**

In addition to looking at the Call Detail Records of targeted individuals, Intellego™ can work with extremely large volumes of CDRs, such as every call originating from one or more cellular providers’ networks. With a powerful ingestion engine, Intellego™ will consume hundreds of thousands of calls per second and make them available for analysis. Investigators working with this data may be looking for suspicious patterns in the data, for example which calls were made from phones connected to specific towers near the site of a terrorist attack.

The techniques described are technically infeasible when working with hundreds of millions of records, most of which are not criminally suspect. In order to provide the ability to drill down and identify the key calls that are relevant, Intellego provides two techniques, Smart Query and Grid Analysis.

**Smart Query**

Smart Query (Figure 4) allows an investigator to ask intelligent questions of the data and return with result sets that are more manageable in size and where the techniques of targeted analysis are useful. An investigator using the smart query tool may ask questions like “Show me all the phones with subscribers in post code M4C 1B5 who were connected to towers within 15 kilometers of the stadium between 5 and 6pm yesterday.”

The investigator or analyst can run these smart queries at time of analysis or schedule them to run automatically on a regular basis. An example of a scheduled query might be: “Every day, find and alert me to any new instance of two or more calls between prefixes assigned to town A and prefixes assigned to town B.” Those results are stored in a data set for analysis at any time.

**Grid Analysis**

Grid Analysis (Figure 5) is a technique that allows investigators or analysts to sort through the data by sorting and matching specific fields to pick out the relevant calls for a more detailed look. For example, an investigator or analyst may be interested in calls of 42 seconds in length and want to see those calls sorted by the date and time that they occurred. Grid analysis allows the analyst to filter or sort the result set based on any combination of parameters and see the results in a constantly updating grid.

![Figure 4: Smart Query interface](image)

![Figure 5: An analyst use of Grid Analysis to search specific fields based on any combination of parameters.](image)
CONCLUSION
Mobile phone use continues to grow and with it, the amount of data generated which can prove useful for investigations. Finding actionable data and patterns in this wealth of data takes good analytic skills and the right technology. Powerful analytics in Intellego™ enable analysts to find case-relevant Call Detail Records, understand the network of criminal activity and identify patterns helpful in investigations while improving the time to such meaningful analysis.

ABOUT INTELLEGO™
SS8’s Intellego™ is the world’s only web-based IP data monitoring and analytics platform. With advanced analytics such as Social Network Analysis (SNA), Intellego™ gives analysts and investigators the ability to monitor IP traffic from a variety of sources, index and search that data, and analyze and identify key patterns in the data, all in real time.

ABOUT SS8
SS8 is a leading worldwide provider of innovative regulatory compliant, communications compliance and high capacity end-to-end communications and cyber intelligence solutions. From access to mediation and monitoring to next generation criminal and national security intelligence analysis, SS8 can meet the data discovery and analysis needs for today’s fast and complex networks. SS8’s solutions enable telecommunications providers, law enforcement agencies (“LEAs”) and national governments communications compliance and cyber monitoring of both current- and next-generation voice and IP data communications in accordance with local laws and standards.

For more information about SS8 and SS8 solutions, please visit us on the web at http://www.ss8.com and follow us on Twitter at @SS8_Inc.