Brought to you by
Forensic Analytics

Communications Data Analysis & Cell Site Analysis Overview

Executive Summary

Communications data analysis is an investigatory discipline that attempts to gain useful intelligence and evidence from the records of communications – phone calls, text messages,social media chat sessions – between subject individuals.

An associated discipline, cell site analysis, employs a set of forensic techniques that attempt to provide evidence of where a mobile device may have been located when certain calls were made.

Mobile phone networks consist of a large number of radio 'cells' each of which covers a limited geographical area. Each cell is assigned a unique 'Cell ID', which is captured in the billing record when calls are made.

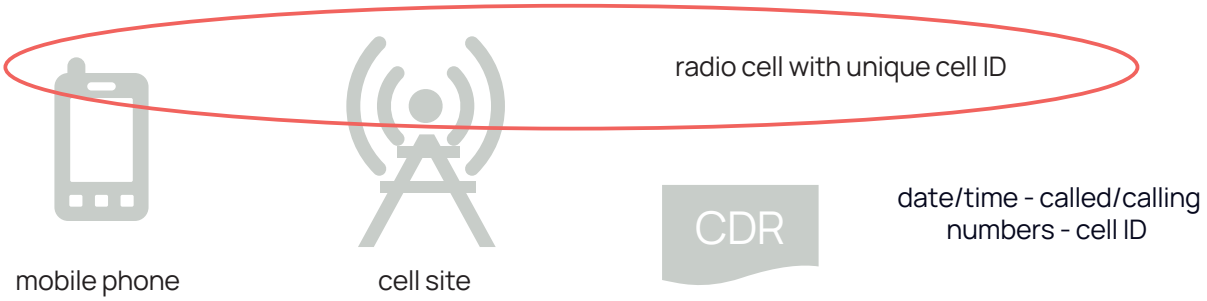
Network operators are able, under tight regulatory guidelines,to provide details of the calls made by 'subject' phones and can also provide details of the locations of the cells used by those phones.

Communications data analysis is used to discover information related to the exchange of communications between individuals.

If some of those communications events were carried by mobile networks, then cell site analysis can be used to enable an investigator to determine whether calls made at or around the time of an incident or offence used cells within a location of interest.

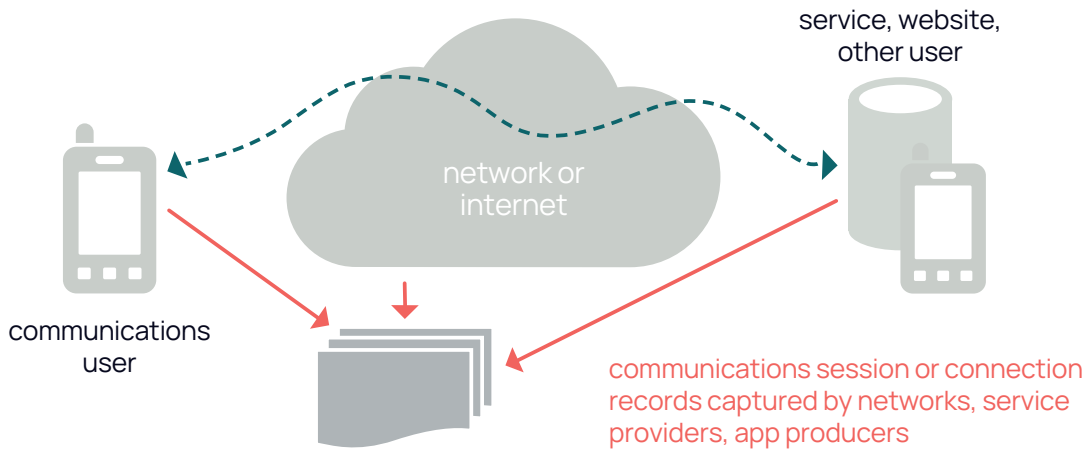
Additional evidence can be provided by undertaking a RFPS (Radio Frequency Propagation Survey) at each significant location. RFPS equipment captures details of the cells that can be detected at a location and can indicate which cells are most likely to be selected for use by a phone at those locations.

Based on a combination of communications data analysis of a phone's billing records and cell site analysis of the phone's potential cell location details and RFPS results, investigators can provide fact based testimony that can provide compelling evidence to compare against the contentions and allegations made in a case.



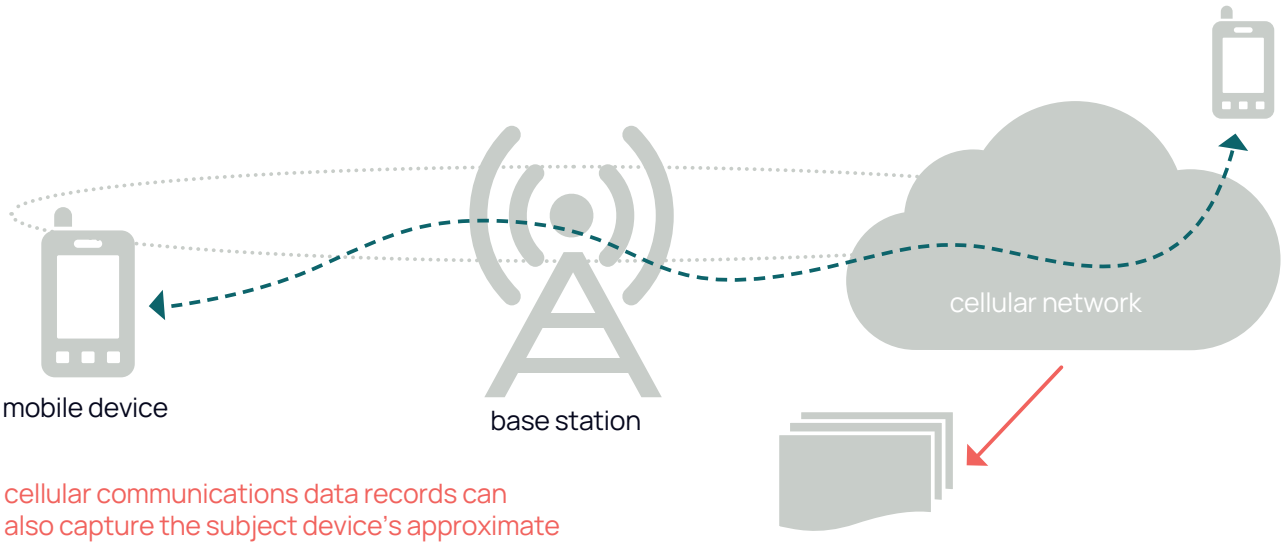
Communications Data Analysis

Communications data is captured by network operators, Internet Service Providers and even individual app providers every time a communications service user makes or receives a call, sends or receives a message or connects to a data service.



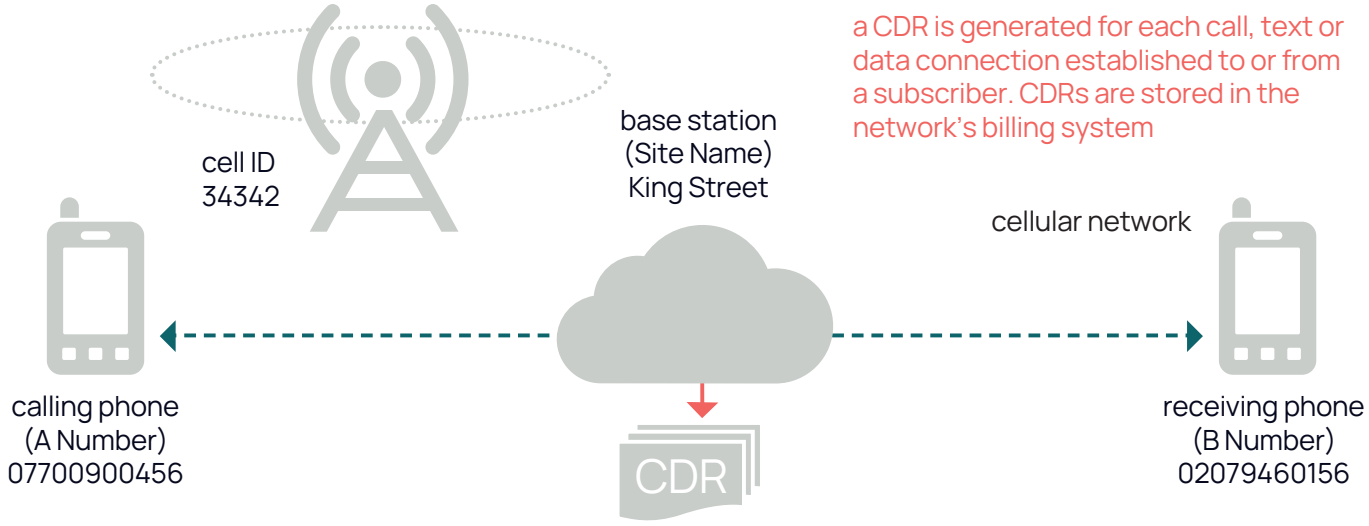
Analysis of communications data records can provide valuable intelligence and evidence of who has been in contact with whom, or of the websites or data services that individual users have accessed.

In cellular mobile phone systems these records are known as CDRs (Call Detail Records or Connection Detail Records) – cellular connection records provide the additional benefit of potentially being able to show approximately where a subject device was located when certain connections were made.



Cellular Call Detail Records

A new CDR is 'opened' each time a new connection is set up. Once a CDR is 'closed' (when the connection is released), it will be transmitted to the operator's billing system and stored in a centralised database. Ostensibly, CDR data is captured for billing and charging purposes, but can be disclosed to authorised agencies, such as the police, or obtained through a court order by solicitors, councils and other parties.



CDRs are provided by network operators in many different formats, with a variety of information, but generally each CDR contains the following:

- Date and time of call
- Originating phone number (also known as MSISDN or A-Number)
- Terminating phone number (B-Number)
- IMSI (identifies the subscriber) and IMEI (identifies the handset)
- Duration of call
- Type of service e.g. voice call, SMS, MMS, data, etc.
- First Cell ID (cell used at start of call)
- Last Cell ID (cell used at end of call) - not always provided

GPRS CDRs, also known as Mobile Data Events (MDE) or simply "Data", often use a different format but provide much the same level of information. The difference between 'voice' CDRs and 'data' CDRs however, is that a voice CDR will record each transaction (phone call, SMS) as a separate event, whereas for data the entire connectivity period is known as a Session and can last for several hours or even days. For billing purposes these Sessions are shown by one or more CDRs that collectively cover the whole session duration but won't provide details of individual connections (to a website, for example).

It is for this reason that, in terms of best practice for cell site analysis, current guidance indicates that Voice and Text CDRs should take precedence over Data CDRs if they are sufficient to prove the prosecution case.

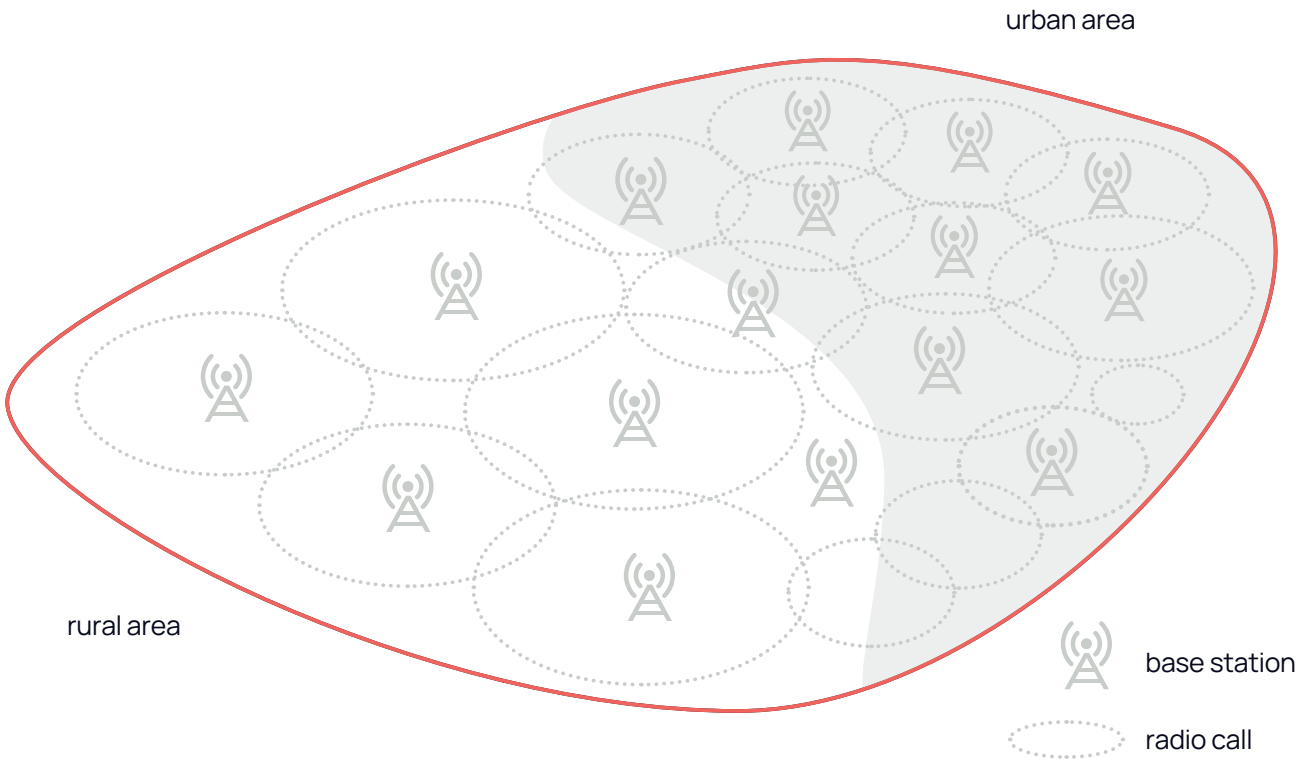
Cellular Mobile Networks

The original radiotelephone networks, which went into service from the 1920s onwards, employed a single radio transmitter to provide the service over a wide geographical area. The main limiting factor of these networks was the lack of capacity caused as a consequence of the large radio transmission areas used. If a network operator employed just one very powerful transmitter to provide coverage for a city or a region, they would only ever be able to serve a tiny fraction of the potential market in that area. In the early 1960s, a concept known as Cellular Mobile Communications was developed to address this capacity problem.

Cellular network architecture provides not just one transmitter for each region but uses hundreds or even thousands of much smaller and less powerful radio transmitters to cover the same geographical area.

These smaller transmitters are known as Base Stations and the small geographical areas covered by their radio signals are known as Cells. In the same area previously covered by just one large transmitter, a cellular operator might site hundreds of Base Stations, each supporting several radio channels, which would increase the availability of radio connections by a similar factor.

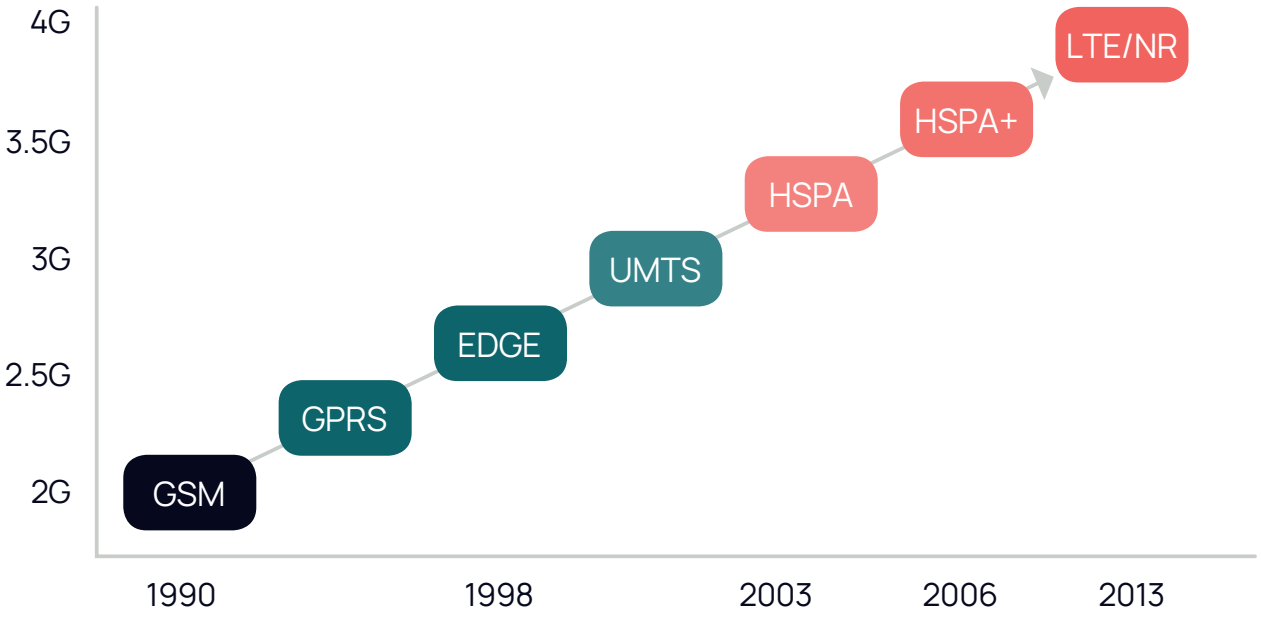
The size of the cells used in a network can vary according to factors like geography and demand. Base stations serving rural locations with low demand for service might be configured with cells that cover a large area. Base Stations covering high-demand areas such as city centres, business areas and airports might be configured to provide coverage using very small cells.



Network Generations

The earliest type of mobile communication provided by radiotelephone networks offered a very expensive service to a very limited number of users. The first truly 'cellular' mobile networks began to appear in the late 1970s and are now collectively known as 1G (1st Generation) systems.

The modern era of digital mobile communications began in the early 1990s with the release of 2G (2nd Generation) networks. Several competing versions of 2G networks were developed in different regions, but the system developed in Europe – known as GSM (Global System for Mobile communications) – eventually came to be the dominant global 2G technology.



2G GSM networks offered access to a limited range of services – voice calls, text messaging, dial-up data services – but provided them in a secure, high capacity and high-quality fashion. In the late 1990s two updates to GSM were released, known as GPRS (General Packet Radio Service) and EDGE (Enhanced Data rates for Global Evolution), which offered more efficient data and Internet connectivity.

GPRS/EDGE formed what became known as a 2.5G system. In the early 2000s networks started to launch 3G (3rd Generation) services, beginning with a technology known as UMTS (Universal Mobile Telecommunications System), which offered voice, text and picture messaging and faster Internet connections.

3.5G upgrades to UMTS were developed later in the decade, known as HSPA/HSPA+ (High Speed Packet Access), which offered increasing fast mobile broadband data rates. In the early 2010s, 4th Generation (4G) networks began to be launched known as Long Term Evolution (LTE) offering even faster and lower latency Internet connectivity. In late 2010s 5th Generation (5G) emerged known as New Radio (NR) with even lower latency and faster connections.

The diagram reflects the progression of European brands of mobile technologies and, although these are the dominant network types around the world, other technologies are used in some countries and regions. Whichever mix of technologies they use, most countries now support a mix of 2G, 3G, 4G and 5G services.

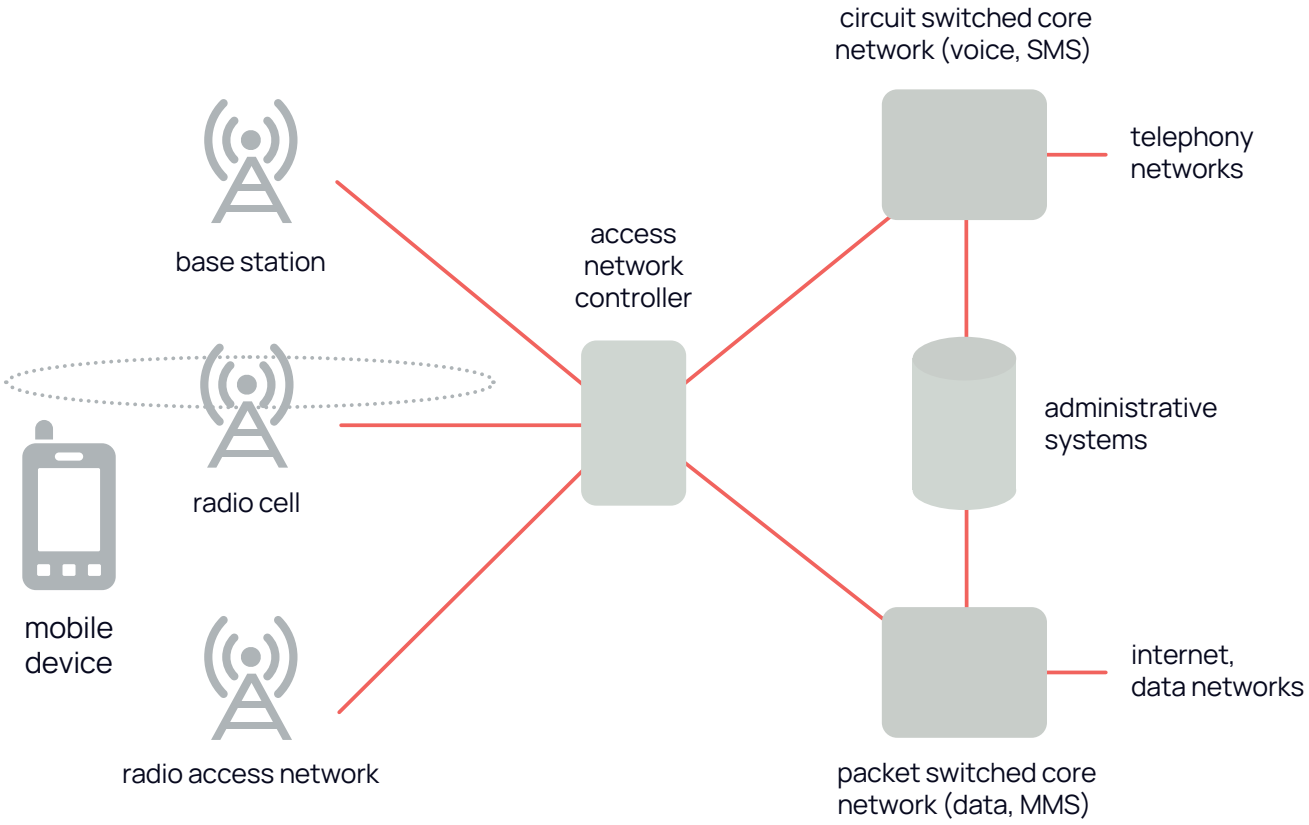
Network Architecture

Cellular networks are generally divided into two main areas:

- The Radio Access Network – which is home to the cells, base stations and other radio elements
- The Core Network – which is home to the network's central administrative and interconnection services

2G and 3G core networks are divided into three main areas:

- The CS (Circuit Switched) core, which deals with 'real time' services such as voice and video telephony and also typically deals with SMS text messaging
- The PS (Packet Switched) core network, which deals with 'non real time' data services such as Internet connections, email, instant messaging and MMS



4G LTE and 5G NR networks only have a PS core network, as they only provide data services - voice connections are supported, but they are carried using data techniques. All generations of network share a common administrative area that hosts subscriber databases, the billing system and other key services.

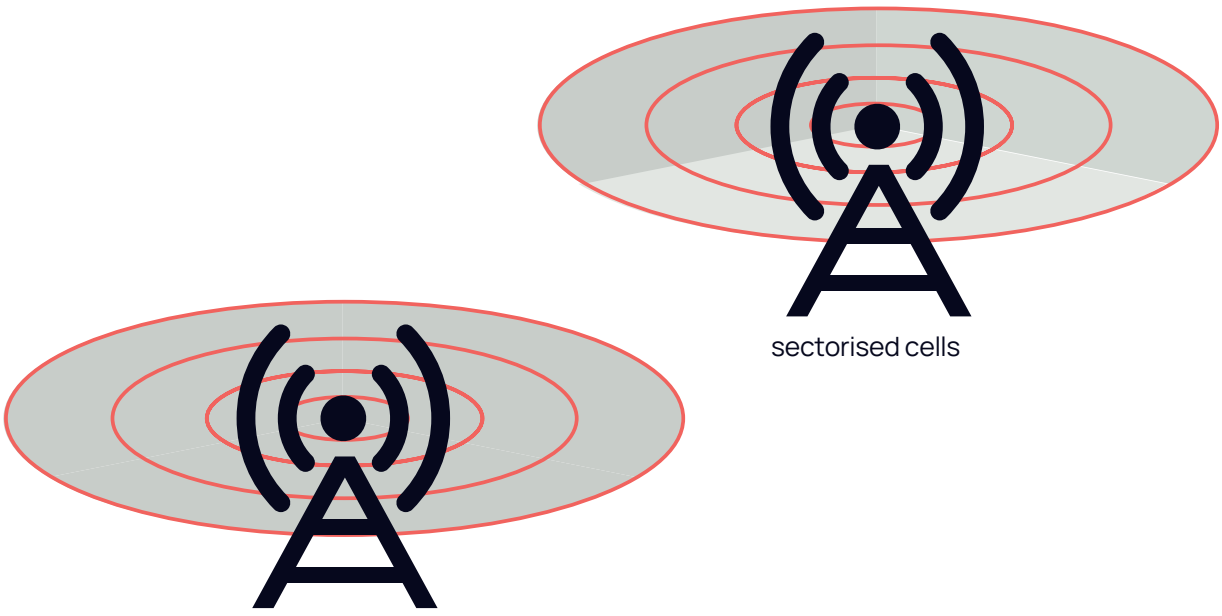
Cells & Base Stations

A cellular base station is designed to generate radio cells that allow it to transmit and receive users and control traffic over the radio path or 'air interface' radio channels that connect to users' mobile phones.

A base station contains sets of radio transmitter/receiver units which each cover a certain geographical area of the operator's network. The base station may generate one cell or several cells and maybe operate across one or more radio channels.

Base station configurations fall into two basic categories:

- Omni-directional Sites (covering one cell) that transmit their radio signal in all directions from one antenna like a ring doughnut of radio energy.
- Sectorised Sites that transmit their radio signals in sectors, with each sector being generated by a different, directional antenna. This method resembles a torch beam shining focused radio energy over a specific area. The traditional sectorised cell configuration uses three antennas to create three different cells that between them provide 360° coverage around the site.



sectorised cells

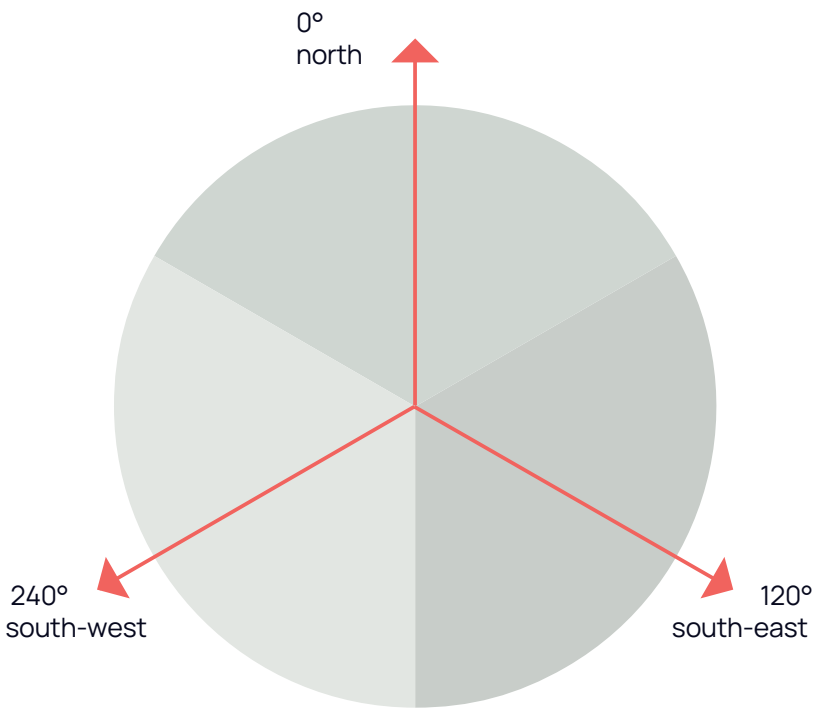
omni-directional cells

A sectorised site employs directional antennas, which limit transmission of each radio channel to a specific part of the base station coverage area. Sectorised sites can be configured in a variety of ways, but typically have either three or six sectors.

Sectorised Cells

Cell sectors will point in a certain direction. In cellular parlance, this is described using the word 'azimuth', an ancient navigational term which identifies the compass angle along which the centre of a cell's radio beam is pointing in relation to Due North.

For example, with a three sectored cell site, if one of the antennas had an azimuth of 0° (North) then the other sectors would normally be 120° (South East) and 240° (South West).



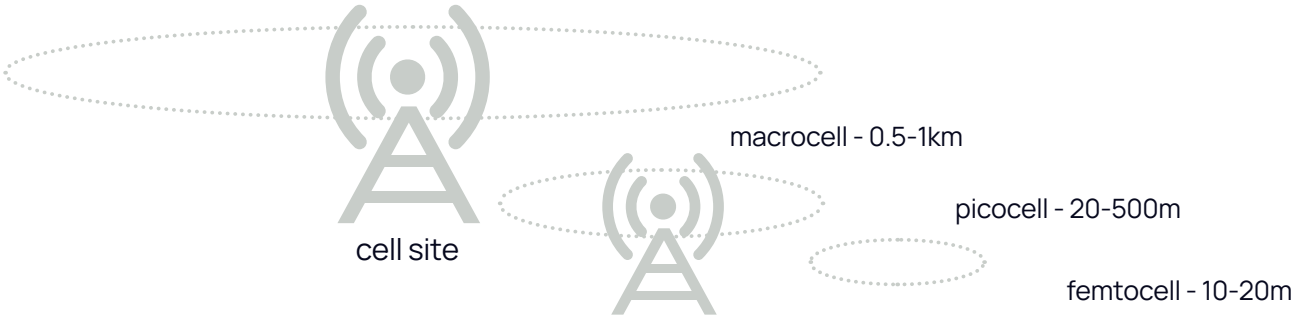
Each cell is assigned a unique Cell ID, which will be unique within its network.

The Cell ID is advertised on a 'broadcast' channel in each cell, allowing mobile devices to determine the identity of the cell they are currently connected to. If the location of a cell site and the azimuth of its cells are known, then simple inferences about the approximate location of phones using that cell/sector can be drawn.

Cell Types & Sizes

A typical radio cell, of any generation, has a finite capacity limit.

For large cells this finite capacity is spread across a wide area and might need to be shared by many users. This has implications for the density of coverage (in terms of numbers of concurrent connections that can be supported vs. the population of the area served by the cell) and may also limit the data rates that might be available to individual users. With small cells this finite capacity is focused on a small area, which implies high density of coverage and potentially high data rates per user.



However, a few large cells can cover a wide area, lowering the cost of providing service to that area, while a large number of small cells would be required to cover the same area, which would increase the cost of service. Cellular operators are therefore very careful about planning the size and number of cells they deploy to match the expected customer demand in each area.

The range of cell types that operators can choose from is generally categorised as follows:

- **Macrocells** – outdoor sites that provide wide area coverage with typical cell radius measurements of 1km up to 20km or more
- **Microcells** – outdoor sites that provide more focused hotspot coverage with typical cell radius measurements of 0.5-1km
- **Picocells** – can be deployed as outdoor sites, in which case the cell radius can be up to 500m, or as indoor sites in offices, shopping centres or airports with a typical cell radius of 20-30m
- **Femtocells** – can be deployed as outdoor sites or indoor sites with a typical cell radius of 10-20m

There are no rigidly defined standards for cell descriptions and so the descriptions provided above should be viewed as guidelines rather than rules.

In general, the cells in a mobile network provide coverage over a limited area. Overall network coverage is therefore based on a 'patchwork' of coverage provided by deploying large numbers of closely spaced base stations.

It should be noted that cellular network coverage is very deliberately planned and well-engineered.

User & Network Identifiers

PLMN ID
Mobile networks are technically known as PLMNs (Public Land Mobile Networks) and each authorised network is assigned a unique 'PLMN ID'. This consists of a three digit MCC (Mobile Country Code), which indicates the country the network operates in, and a two or three digit MNC (Mobile Network Code), which identifies the network within their country. Examples include: 234 (UK), 208 (France), 505 (Australia), 310 (USA). The MCC/MNC pair is used as a prefix on values such as Cell IDs and IMSIs.

IMEI
The IMEI (International Mobile Equipment Identity) is a number unique to every GSM, UMTS, LTE and NR mobile device. Today this could even be applied to a modern vehicle. It is usually found printed on the phone and can also be displayed by dialling *#06# into the phone.

The IMEI is 14 digits long but is usually transmitted and captured with extra digits on the end. In voice/SMS CDRs the 14 digit IMEI is supplemented by a check digit to create a 15-digit IMEI and in GPRS/data CDRs the 14 digit 'stem' has a two digit 'software version' added to create a 16 digit IMEI. Both the 15 and 16 digit versions of the IMEI share the same 14 digit stem and are therefore functionally identical.

The check digit is not part of the digits transmitted at IMEI check occasions, which means that the IMEI printed on a handset often differs from the IMEI captured in call records, with a different last digit.

IMEI
International Mobile
Equipment Identity

MS-ISDN
Mobile
ISDN Number
(phone number)

IMSI
International
Mobile
Subscriber
Identity

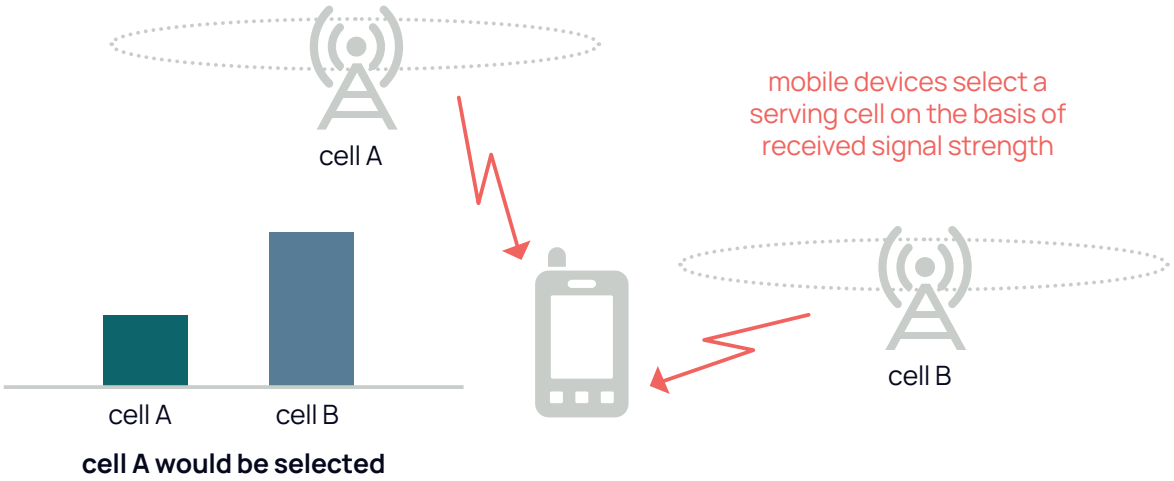
IMSI
The IMSI (International Mobile Subscriber Identity) number is used for registering and identifying a subscriber within the PLMN. The HLR (Home Location Register) uses the IMSI to uniquely identify each mobile subscriber. A mobile device identifies its user/subscriber using the IMSI number that is stored on the SIM card.

An IMSI is always 15 digits long and consists of the following format: MCC – MNC – MSIN (Mobile Subscriber ID Number, unique within PLMN)

MSISDN
The MSISDN is a phone number uniquely identifying a subscription in a GSM, UMTS, LTE and NR mobile network. It is the number allocated to the SIM card and the number normally dialled to connect a call to the mobile phone.

Mobile Phone Operation

Mobile devices try to ensure that they are able to offer the best quality connection.



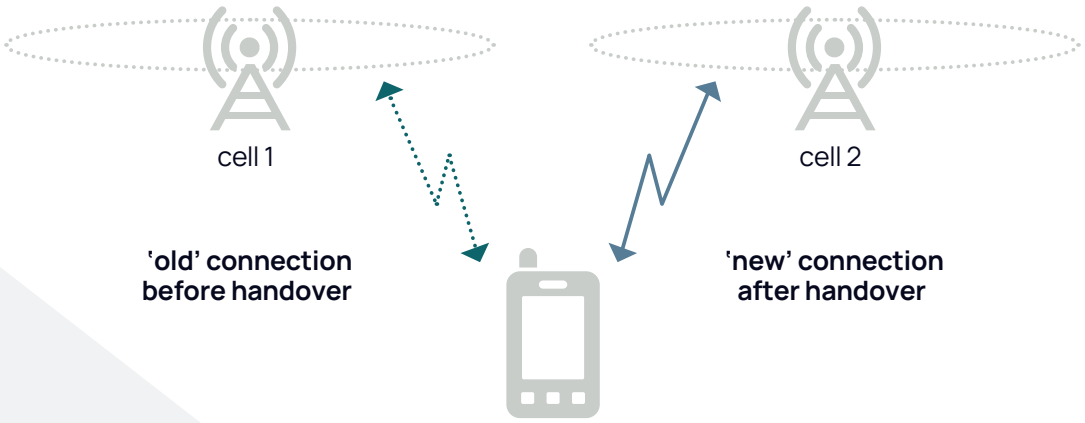
They do this by taking measurements of the strength of the signals being received from local base stations and compiling a list of cells ordered by signal strength.

When a mobile device is in 'idle mode' – meaning that it's switched on but not currently engaged in a call – the phone manages this process for itself by 'reselecting' to the strongest local cell when one is detected.

The cell that a phone currently chooses to monitor is known as the 'serving' cell.

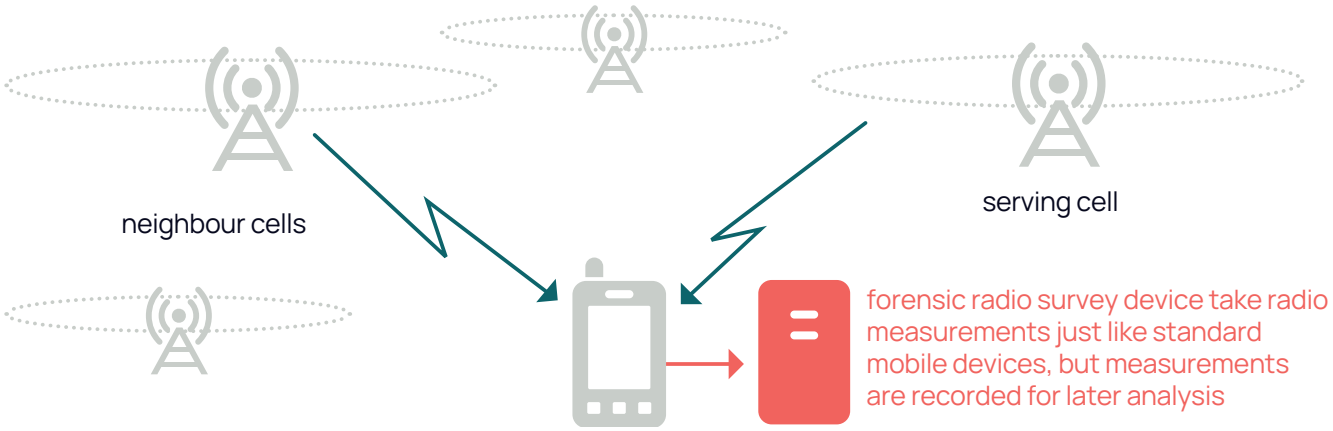
During a call, when the phone is in 'connected mode' it passes its signal strength measurements to the network and lets it decide if a change of serving cell is required.

When a change is made the network triggers a process called 'handover' which moves responsibility for the phone's connections to a new cell or base station.



Forensic Radio Surveys

Cell Site Analysis can make use of a forensic technique known as RFPS (Radio Frequency Propagation Surveys) to capture information about the coverage at a location or in an area.



Radio Frequency Propagation Surveys can be undertaken for several reasons:

- To determine the set of cells that provide coverage at a location
- To determine the extent of coverage of a given cell
- To determine serving coverage along a given route

Surveys are usually undertaken in support of historical cell site analysis but may also be performed to gather intelligence as part of 'live' events such as kidnaps. There are three main RFPS techniques employed:

Spot/Location Surveys
Location Surveys provide details of the set of serving and non-serving cells that provide coverage at a given location. Generally the location chosen is the address where an incident has occurred or where a person of interest lives or works.

Cell Coverage Surveys
Cell coverage surveys are intended to determine the extent of serving coverage of a particular cell. The survey is generally performed as a drive survey and the results provide a snapshot of cell coverage at the time the survey was undertaken.

Route Profiles
A route profile employs similar methods as a coverage profile, but whereas a coverage profile seeks to determine the area served by a single cell, a route profile attempts to represent the set of cells that serve along a given route.

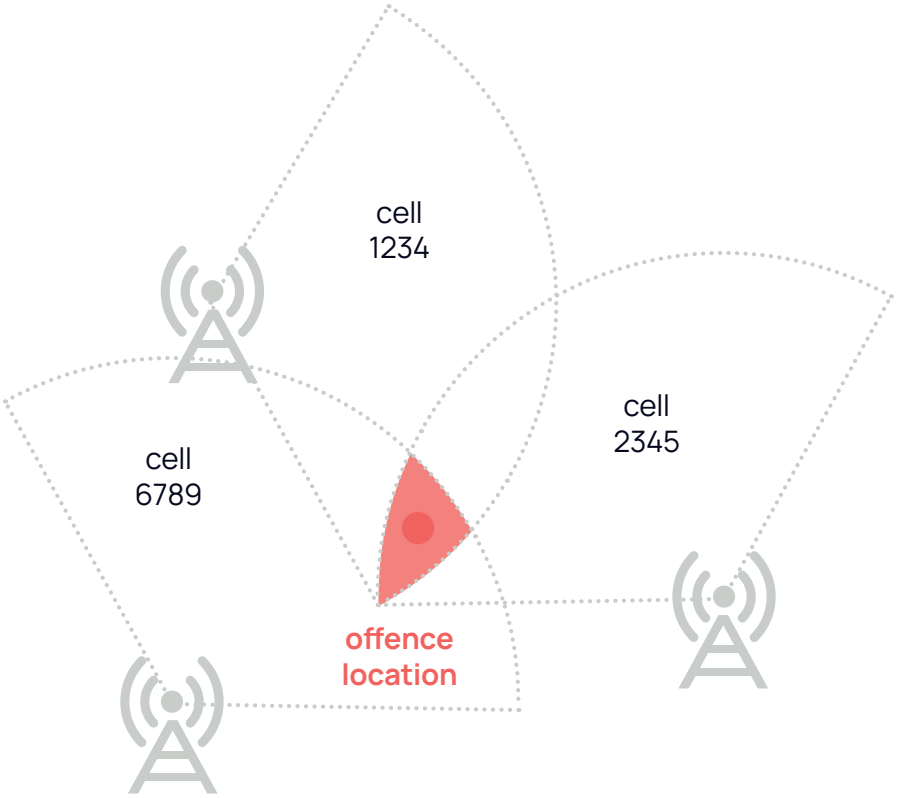
Cell Site Analysis

Communications data analysis is concerned with processing communications data records and determining the set of contacts and events that have taken place. It can be performed on connection records from all kinds of communications network and service.

Cell site analysis provides a further set of techniques that can be applied specifically to calls, text messages and data sessions carried by cellular networks. This form of analysis attempts to determine whether calls of interest could be linked to a location of interest and uses the 'serving cell' information captured in cellular CDRs to assist with this.

Knowledge of the locations of the cell or cells that carried a call or series of calls can help to identify the general area within which those calls had to have been made.

RFPS survey data can help to prove whether any of those calls could have been made from a specific location by checking to see if the cell used to carry a call is a cell that serves at the location of interest. If the used cell is detected as serving at or near that location then it is possible to conclude that the call could have been from there.



Cell Site Analysis Reports

The process of compiling a cell site analysis report is largely an iterative one:

- Divide calls into batches that match the times of the allegations being made
- Check each batch of a suspects calls against the allegations being made
- Were any calls made at around the time of a significant event?
- If so, did those calls use cell sites near to the event location?
- If yes, do the RFPS results from that location indicate that the cells used for the calls are 'serving' cells at the location?
- If the cells do serve, then the report can conclude that the calls 'could have been made at or in the vicinity of the location'
- If the cells provide non-serving coverage, then the report can conclude that the calls 'could have been made in the general area of the location'
- If the cells were not detected during the RFPS survey, the report can conclude that the calls 'are unlikely to have been in the general area of the location'

Cell site reports are often used to provide support for, or confirmation of, other forms of evidence.

For example, a 'significant event' in a case may have been 'the suspect was captured on CCTV making a phone call'. Cell site evidence would then be used to show whether any call details were recorded for the suspects phone at that time and if so, whether the cell used serves at the observed location.

Cell site reports are sometimes required to show whether calls could have been made from a car during a specific journey; for example, if a call was made during a period when the suspect was alleged to have been in a getaway car fleeing a robbery scene. In this case the cell site analyst might request an RFPS 'route profile' to be performed following the route of the getaway vehicle. If the cells used by the target phone serve at points along the route, then this supports the allegation that the user of the phone could have been in the vehicle at the time the calls were made.

Cell site reports are often used to show 'association' between individuals, so reports might be required to focus on calls made between target phones or to highlight instances of 'co-location' where target phones might be using cells that cover the same areas.

In cases where the attribution of a mobile phone to a suspect is not solid, especially where there is a suspicion that 'clean' and 'dirty' handsets are being used interchangeably, cell site analysis can be used to provide additional attribution evidence.

What Cell Site Analysis Can (and Can't) Prove

As cell site evidence is generally considered to be too open to interpretation to be used as the sole or the primary evidence in a case, it works best as supporting evidence.

The simplest thing that cell site evidence can prove is that a subject phone used a specific cell to make a call at a certain time. The subject device must therefore have been somewhere within the coverage footprint of that cell when it was used.

If the coverage area of a cell can be measured (by undertaking an RFPS cell coverage survey, for example), then a reasonably exact area in which the phone must have been located can be determined.

This level of evidence is commonly used to help prove or disprove an alibi. For example, with cell site analysis it is possible to prove where a handset 'wasn't' located. If someone states that they were in Birmingham at the time of an incident and the cell site evidence points to the handset being in London, then that alibi can be shown to be potentially false.

RFPS surveys may be undertaken to provide details of the 'serving' cells at a specific address or location. If one of the cells used by a target phone at around the time of a significant event used one of those cells, it possible to conclude that the user of the target phone could have been at that location at that time.

Note the use of the words 'could have been' in the previous paragraph. Unless a cell can be shown to provide coverage only to the surveyed address, the fact that a cell used by the target phone serves at that location doesn't necessarily prove that the phone was actually there. The target phone may alternatively have been anywhere else in the cell's coverage area at that time.

If there is other evidence available – eyewitnesses, CCTV images, ANPR hits, credit card usage records – that helps to place the alleged user of the target phone at the significant location, then the cell site evidence can provide very compelling reinforcement of that evidence.

If the cell site evidence is all that the investigator has to tie the suspect to a location, then a level of uncertainty must be accepted.

In general, except in very specific and unusual circumstances, cell site evidence cannot be used to prove that the user of a phone was definitely at a particular location and nowhere else. At best, cell site evidence can be used to show only that it is possible for the user of the phone to have been at a location.

Additionally, cell site evidence typically provides evidence of where the user of a mobile phone may or may not have been when calls were made. Cell site evidence generally does not provide proof of the identity of that 'user' - cell site analysis is used to identify the potential location of a handset, not the hand holding the handset - so it is recommended that cell site analysis is only undertaken once a solid attribution for the target phone(s) relevant to a case is made.

CSAS

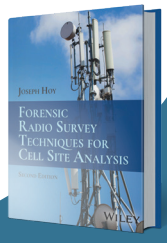
CSAS is a powerful and secure investigative platform which has become a staple in criminal investigations UK wide.

CSAS empowers investigations by enabling Investigators and Analysts to advance investigations at pace by rapidly cleansing voluminous data sets.

This includes the enhanced processing of call data, phone handset downloads, automatic number plate recognition, vehicle telemetry, wearable technology, social media take out and more.

"**Over 90% of all crime has a digital component** and the need for innovation in tackling the ingenuity of the criminal world has never been greater. Since 2013, **CSAS has played a pivotal role in this fight**."

Joe Hoy,
Founder, Forensic Analytics



- **Rapid processing of large complex disparate digital data sets**
- **Powerful analytical queries**
- **Data visualisation**
- **Fast easy extraction and production of evidence/ intelligence products**
- **Evidential standard reporting and auditing**
- **Integration with other solutions i.e. NMPR, CellView, i2 and others**
- **Radio Frequency Propagation survey case management**
- **Reveal links between operations, investigations, people, locations and devices**

CSAS produces actionable intelligence to robust evidential standard - in seconds. Not only does this help apprehend criminals faster, it also helps secure early guilty pleas and lighten the burden on the courts.

Following 'Op Orochi', the Metropolitan Police Serious and Organised Crime team have achieved the following by using CSAS:

Arrest to charge ratio

Guilty plea at first court hearing

Conviction rate

Making a real difference

CSAS has recently helped police forces across the UK analyse complex communications data and other digital media to deliver a string of convictions and lengthy prison sentences for county lines drugs, homicides, fraud and human trafficking.

- Reducing the timeline of investigations
- Intelligence led policing
- Saving Lives & improved safeguarding of vulnerable people
- Delivering on control strategy & local priorities
- Improving identification of suspects leading to early intervention/disruption
- Increasing victim satisfaction
- Reduce demand and costs
- Increasing trust & confidence
- Improving efficiency & effectiveness
- Delivering capabilities at the front line to respond to the changing landscape of investigations and calls for service

CSAS now works even more effectively with CellViewTM thanks to advancements in displaying 4G cells in the eCGI format. This significantly improve the results of CellView queries, adding accuracy and precision to coverage areas which can be hugely important in threat to life situations.

CellView

Working In Partnership

Many of our team served as sworn police officers and our proven track record is the reason law enforcement and the criminal justice system trust CSAS. Quite simply, we are here to empower your team to swiftly bring to justice to those that cause communities most harm and protect those that are most vulnerable while maintaining public confidence and building upon trust within law enforcement.

Deploying CSAS

CSAS V3 can be deployed on premise for a single user or as a networked solution for hundreds of users. It's compact enough to run on a standard laptop, but powerful enough to crunch all the data you can throw at it. CSAS V3 is also available via browser in your own cloud environment. Whichever way you want to deploy CSAS, we will have a dedicated team of experts on hand to support you and an accredited training programme to accelerate your use of CSAS.

Glossary

2G	2nd Generation mobile technologies
3G	3rd Generation mobile technologies
4G	4th Generation mobile technologies
ANPR	Automatic Number Plate Recognition
Azimuth	Compass angle an antenna points towards
CCTV	Closed Circuit TV
CDR	Call Detail Record
CI	Cell ID
CSA	Cell Site Analysis
CSAS	Cell Site Analysis Suite - Forensic Analytics software
CSP	Communication Service Provider
dB	decibel
dBm	decibel milliwatts
EDGE	Enhanced Data rate for Global Evolution - 2.5G
EE	Everything Everywhere - UK mobile operator
GHz	Gigahertz
GPRS	General Packet Radio Service - 2.5G technology
GSM	Global System for Mobile - 2G technology
Hex	Hexadecimal (base 16 number system)
HLR	Home Location Register
HSPA/HSPA+	High Speed Packet Access - 3.5G technology
Hz	Hertz
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber
IPA	Identity Investigatory Powers Act 2016
kHz	kilohertz
LAC	Location Area Code
Log	Logarithm
LTE	Long Term Evolution - 4G technology
MCC	Mobile Country Code
MHz	Megahertz
MMS	Multimedia Messaging Service (photo messages)
MNC	Mobile Network Code
MS-ISDN	Mobile Station ISDN Number (mobile phone number)
MSIN	Mobile Subscriber Identity Number
mW	milliwatts
Ofcom	Office of the Communications Regulator
NR	New Radio - 5G technology
PLMN	Public Land Mobile Network
RF	Radio Frequency
RFPS	Radio Frequency Propagation Survey
RIPA	Regulation of Investigatory Powers Act 2000
SAC	Service Area Code
SIM	Subscriber Identity Module
SMS	Short Message Service (text messages)
UMTS	Universal Mobile Telecommunications System - 3G

Brought to you by
Forensic Analytics

Forensic Analytics Ltd | Registered in England and Wales. Company No: 08606475
Pixmore Centre, Pixmore Avenue, Letchworth, SG6 1JG
+44 800 158 3830 | www.forensicanalytics.io