



Brought to you by

**Forensic
Analytics**

Digital Forensic Experts



The need for an evolving Radio Frequency Propagation Survey (RFPS) methodology in law enforcement investigations - a hybrid concept

Martin Griffiths, Founder and RF Specialist, Forensic Analytics.

Peter Nuttall, EMEA Solution Architect, Gladiator Forensics.



CONTENTS

Executive Summary.....	3
Introduction and Background.....	4
RF Propagation Survey Equipment.....	5
SIM Based RF Propagation Survey Equipment.....	6
Equipment Comparisons.....	6
UK and US RFPS Considerations.....	8
Regulation and Compliance with Codes of Practice.....	8
Competent, capable and up to date RF experts.....	9
RF Training Curriculum.....	9
Accuracy of Survey Results.....	10
The Importance of CDR's.....	11
Usage of Survey Data for Intelligence Purposes.....	12
Speed of Response and Surveying.....	14
Considerations when selecting Surveying Equipment.....	15
Return on Investment.....	16
Conclusion.....	20

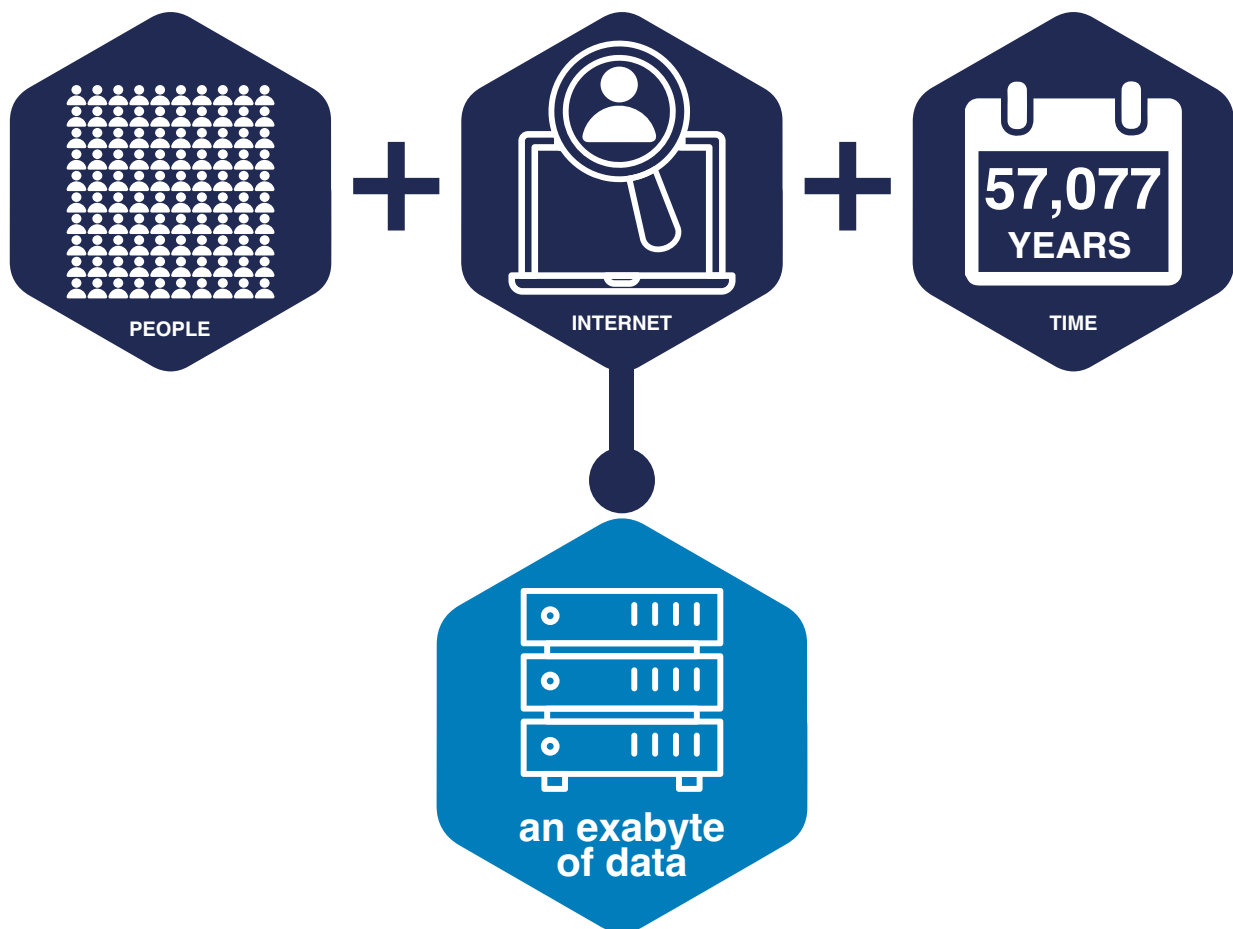
Executive Summary

The rise of digital forensic methodologies over the last 20 years, has been in response to an environment where the volume of data available to investigators has grown exponentially.

Criminals have weaponised technology taking advantage of both its availability and technology’s ubiquitous role in all our lives. For example, in 2007 - an iPhone 1 had a maximum memory capacity of 8 GB. In comparison, today - an iPhone 15 Pro Max has up to 1TB of data.

Written by two experienced criminal justice expert witnesses and Radio Frequency Propagation Survey (RFPS) practitioners, this paper will generate a discussion on multiple aspects of how data can be used in investigations. We explore the role of compliance and regulation, including the introduction in the UK of the Forensic Science Regulators Code of practice. We look specifically at the role of different methodologies available to law enforcement for RFPS surveys, we explore the different operating practices between the UK and US and finally, we recommend a fresh approach and methodology for conducting RF surveys. In addition, we have a call to arms for law enforcement generally and RF practitioners in particular, as we advocate the sharing of RF survey data and the creation of a UK national database

All this is against a background where by 2029 there will be 550 Exabytes of Fixed Wireless Access (FWA) and Cellular data generated every month. To put this into context, an office of 100 people would have to search the web for 57,077 years to reach an exabyte of data.



Stay awake, keep up and enjoy

Introduction and background

Radio Frequency Propagation Surveying (RFPS or RF for short) has been mainstream within UK Law Enforcement for many years, however in the US - although widely used at a Federal level – it remains uncommon at State and Local levels. This is starting to change.

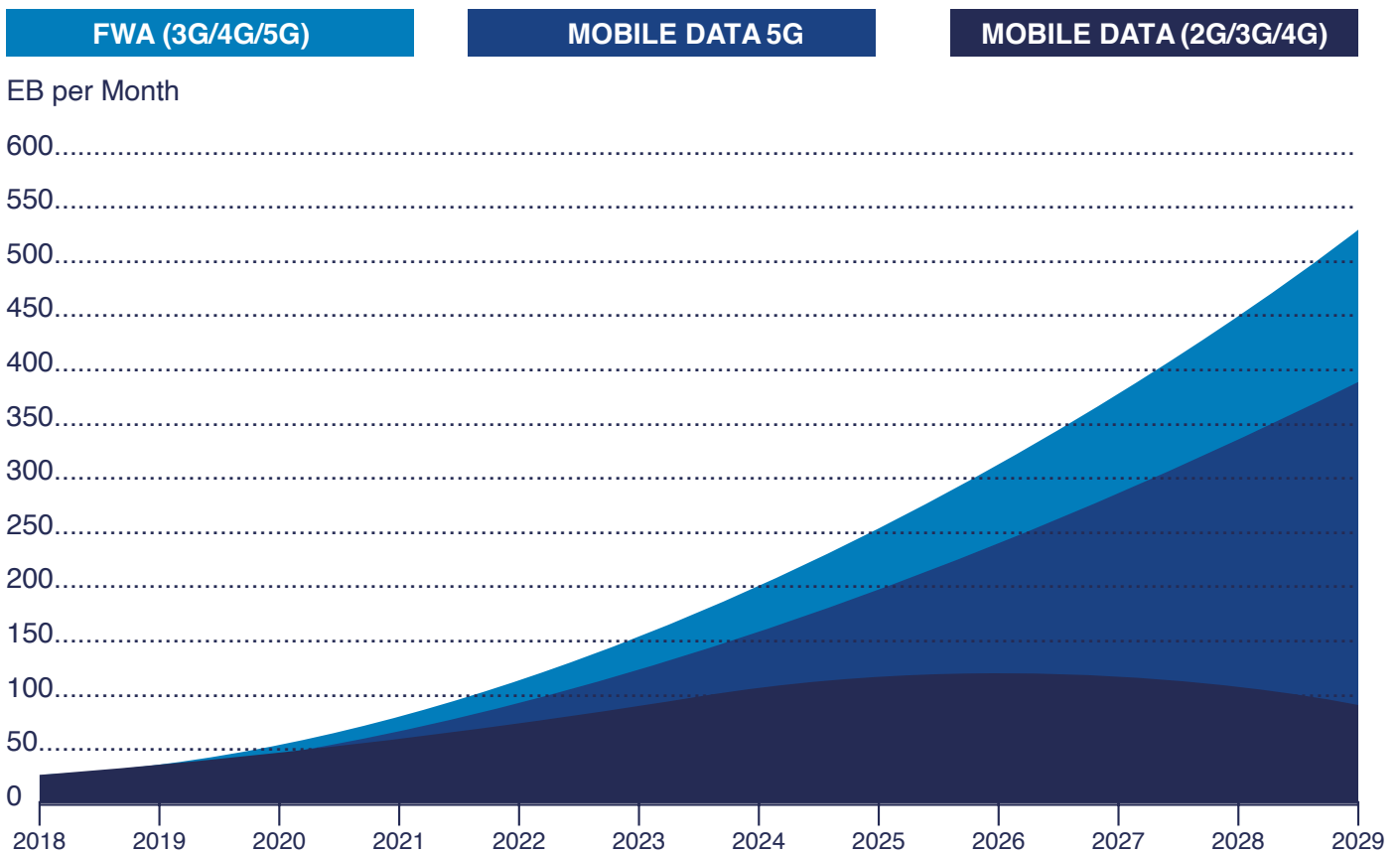
Cellular services including WiFi and collective radio technologies will continue to be the medium upon which we all rely on to communicate, entertain and transact business.

Radio Frequency (RF) Surveying involves recording the cellular and/or Wi-Fi coverage in an area, location, pattern of life and travel, scene preservation or other such use cases, critical to a law enforcement agency (LEA) investigation. This can be done in two ways:

- **Reactively** due to an event occurring.
- **Proactively** – to record data to assist with current or future investigations or as an intelligence resource.

The graph below demonstrates both actual and anticipated growth in data generation, measured in Exabytes (10¹⁸ or one billion bytes) for Fixed Wireless Access (FWA) and Cellular data generation.

To put this into context, the US Library of Congress contains 0.00001EB of data (1EB is 100,000 Libraries of Congress). Whilst data growth is exponential, so too will be the data available to an LEA investigation, which - to be of value – needs to be carefully **captured, curated, and managed**.



Source: <https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/mobile-traffic-forecast>

Societies dependence upon radio it can be argued, is – and will – continue to be an absolute.



The question we need to ask, is why should anyone particularly LEA's undertake RF surveys?

The benefits of RF surveying (a technique widely used throughout UK law enforcement for many years) allows an investigator to independently validate the cell coverage data that a cellular service provider supplies.

It also provides a picture of the RF environment and coverage at and around crime scenes, which can help determine investigative techniques and tactics within an operation. Importantly RF survey data can often be supportive and validate the investigators hypothesis.

RF also provides a dataset that can be repurposed again and again to provide evidence and insights for current and future investigations, such as missing persons or man hunts.

The rise of Cell Site analysis - or as is referred to by the UK Forensic Science Regulator - 'cell site analysis for geolocation', is a forensic science-based activity that seeks to model the utilisation of Cellular and Wi-Fi networks for criminal purposes. Although we live in a world where end to end encryption is becoming mainstream, very little radio communication can be undertaken without leaving some evidence. Typically, this is in the form of logfiles, Call Data Records (CDRs) or vehicle telemetry outputs. As a consequence, we expect this type of analysis to be a critical element in investigations for the foreseeable future.

Our capacity to be able to model and understand radio environments is - we contend - a critical capability, as it allows us to work through hypotheses and develop conclusions to aid an investigation. These typically relate to the utilisation patterns and common locations of target devices relevant to an investigation, or provide a confirmation of attribution.

With RF survey data, we add a whole layer of intelligence or evidence. When combined with other datasets and analysis, this can provide compelling insights for an investigation team and ultimately - a jury - in order to secure reliable convictions and help keep society safe.

RF Propagation Survey Equipment

Two types of survey tools have emerged and are in common use:

- **Software Defined Radio (SDR)**, which is scanner based
- **SIM card-based equipment** (or phone emulators as they are sometimes referred to).

SDR test equipment was initially created for the Telecom and Cellular industry to help with the design, deployment, and optimisation of services. These sophisticated tools have been repurposed by Law Enforcement (LE), and with appropriate training have produced impressive results. Each type of survey device has been proven to support valid survey methodologies, all of which have been shown to be evidentially robust enough to contribute to securing safe convictions.

Whether you have access to an SDR-based or a SIM-based solution, you are in a position to undertake RF surveys and assess whether phone activity featured within CDRs is supportive of a hypothesis as to the movements of that phone. Alternatively it is possible to proactively determine what the key serving cells are around locations of interest. Either of these tools are capable of a broad range of RF Survey capabilities, suitable for a standard historical investigation.

However, RF can do so much more. This paper argues that RF surveying should be used as a standard methodology like finger printing, and central to an LEA's investigation strategies.

This paper also considers the benefits of both SDR-based and SIM-based surveys, combined to create a hybrid RF Survey solution. Collectively, this achieves a significant Return on Investment (ROI) by providing both evidence and intelligence to speed up investigations, improve productivity and save lives and money. The value offered by a hybrid solution of developing a very granular view of RF coverage, cannot be overstated.

Every type of equipment comes with risk factors that any operator must be aware of. One of the risks associated with processing SDR Scanner's data that don't support decoding Broadcast Control Channel (BCCH) layer 3 information is the possibility of having false positives. It may determine that a cell provides service to an area, but without the BCCH layer 3 information it may produce an optimistic result in its assessment.

In summary, an SDR-based solution is essentially a radio receiver capable of capturing the full cellular radio spectrum occupied by 2G – 5G and Wi-Fi technologies in a matter of seconds. In the more advanced SDR systems, algorithms determine which of the measured cells had the potential to serve a location by examining the configuration data carried on each cells' BCCH. An SDR 'scanner' will therefore provide a comprehensive and detailed view of the complete cellular environment at a given location or whole area. A key point to consider, is that an SDR Scanner is not a phone and does not interact with the network in the same way that a phone does. It does however *"think"* like a phone, and the results it produces are based upon what a phone would see.

SIM Based RF Propagation Survey Equipment

The alternative to an SDR-based solution is a SIM-based solution, in which a number of phones can be combined in order to create a multi-cell survey solution, which may be tuned to a specific network or even an individual radio frequency band. As the name suggests, the SIM-based solutions are effectively multiple mobile phones working together and simultaneously measuring cellular coverage. As these are ultimately mobile/cell phones with SIM cards, these devices are also capable of generating mobile traffic, which is classed as being 'connected mode surveying', and will test whether a serving cell has the capability to carry traffic – which can be of critical importance in an investigation.

Unlike an SDR Scanner, which records the whole cellular environment - SIM-based surveying tends to be more focused on recording specific technologies, networks or radio channels. SIM based solutions can record the whole cellular estate, but this may require a survey to be undertaken in several sweeps of an area, or at least require a multiple modem set up that will capture all the bands that appear to be on air, as the radio environment becomes ever more complex. In comparison, an SDR Scanner can record everything simultaneously, whereas a SIM based solution records the serving cell, which can change and will do so frequently.

The main risk factor associated with SIM-based surveying, is that there is a danger of false negatives. This could be caused by a cell which is capable of serving, not being "seen" by the SIM based solution. There are often good reasons for this and mitigations are in place that one can follow, but this requires a degree of tradecraft.

As with any product solutions, each option has their own advantages and disadvantages, with both attempting to determine the same thing – *which cells have the potential to serve at a given location?* As the perceived risks of one solution are mitigated by the other, the combination of the two reduces those risks to **zero** and provides a cast iron, all-encompassing end-to-end solution.

Equipment Comparisons

A question which always arises is '**which solution is better?**' And this has split and tribalized the radio community for many years. There have been numerous instances of this debate over the past few years, and the general position within UK law enforcement is that **SIM-based surveying is effective, inexpensive and evidentially rigorous enough to provide reliable results.**

In the US, it is a slightly different situation. RF Surveying is not yet as mainstream as it is within the UK. Federal Agencies undertake this kind of activity, with organisations like the FBI Cellular Analysis Survey Team (CAST) holding a position of influence and knowledge for RFPS capability. Whilst the FBI CAST team provide a respected capability, the support they can provide across the full spectrum of US LEA's is limited.

At the same time, state and local LEA's are seeking to leverage RF survey capabilities, knowledge and standardization. A significant factor that creates both a supply and demand challenge together with a need for standardization, is that the US has more than 18,000 law enforcement agencies. As a consequence, achieving standard operating practices throughout US LEA's presents significant challenges. Unlike the UK, there is no Forensic Science Regulator setting standards and requiring compliance.

Other differentiating factors in the US, includes the access to more comprehensive datasets from the service providers. They allow the ability to access Timing Advance (Round Trip Time), Geofence and GPS data, all of which can provide reasonably accurate data about a phone's location. The need for an evidential RF survey is therefore not always required.

Similar to the UK, there is increased sensitivity within the US as to what could be construed to be 'mass surveillance', and the acquisition of what is considered to be 'en-masse' acquisition of personal data. As a result, the civil liberties implications of datasets such as *Google GeoFence** warrants, have been the source of debate and challenge. As a result, Google recently announced the withdrawal of this type of disclosure. By contrast, RF Survey data **does not** contain personally identifiable information, and can therefore be held indefinitely and will not be subject to the same kinds of civil liberties challenges.

[*Google GeoFence Policy Change](#)

In the future, the complexity of the radio environment will only increase and Scanners can play a part in it producing quick outcomes in spite of this.

Guess what? The future is now.

With the introduction of 5G SA (Stand Alone) networks in many countries, we have reached a point where the current survey methodology needs to be reviewed. This does not mean the equipment that you use today is not fit for purpose, it does however mean that a prudent, sensible and strategic approach should be taken in order to prepare for what is emerging.

Joe Hoy, one of the Founders of Forensic Analytics and Author of the seminal work '*Forensic Radio Survey Techniques for Cell Site Analysis*' mentioned in one of his blogs in 2018¹ "*the question for the future isn't 'what's best, scanners or test phones?' it is 'what's the best mix of scanners and test phones?' to achieve the optimum balance between time, cost and accuracy.*"

This paper's response to Joe's statement is in wholehearted agreement, which leads to the next question; How?

How do we create a balanced mix of Scanners and SIM based test phones?

In order to determine which approach, one might wish to adopt to address the exponential growth and ubiquity of RF data in the future. We should consider the current operational needs, together with what the anticipated changes are over the next few years. We can then determine the tools and techniques available to meet those needs, rather the doing things the other way around, where we continue use a tool or technique because "*that's what they taught us on the course*" or because "*it's what we've always done*". This is the difference between taking a strategic force-wide, or agency-wide view of RF Surveying, against where it is deployed in a piecemeal way and often inconsistently. The consequence of which, is missed opportunities to materially and positively impact investigative outcomes.

In a perfect world, without the external environmental, political and financial considerations playing a factor (which obviously they do), what are those needs?

¹ Joe Hoy (<https://www.forensicanalytics.co.uk/rfps-scanners-vs-test-phones>)

UK and US RFPS Considerations

The UK is not the only country to use mobile cellular technology, so how do other nations deal with their RF Survey requirements and what methodologies do they adopt? Could we all benefit from adopting similar responses to the same question?

The authors of this paper have been engaged as LEA and RF practitioners for the best part of a decade. We would define the UK Law Enforcement needs assessment, along with how we can evolve our methodologies to meet those needs as detailed below.

Forensic investigators working within the UK are required to obtain accreditation to prove their compliance with the Forensic Science Regulator (FSR) code of practice for geolocation analysis.

This is currently a UK-only issue, but similar quality and accreditation requirements are likely to be developed in other countries. In the US for example, there is an absence of clarity and guidance available from the forensic regulatory system and the lack of accredited standards can result in variability in the quality and consistency of forensic output. There are some moves towards common standards in cell site analysis in the US.

The Scientific Working Group of Digital Evidence (SWGDE) for example, produce some excellent documentation, promoting best practice in this critically important area. Whilst forensic practitioners in the US are not currently required to adhere to the ISO17025 / 17020 forensic laboratory quality standards, there have been some significant recent rulings in the US Supreme Court, highlighting the importance of evidentially robust and validated methodologies. The findings of these rulings essentially match the pillars of ISO accreditation.

Digital forensics is still in its adolescence when compared to “wet forensics”, where fingerprint identification as an investigative methodology has been in use since the 1890’s. As discussed earlier in the UK, quality and accreditation requirements for all aspects of forensic science in criminal investigations are more formalised. With digital media in investigations growing as criminals weaponise technology, the UK has introduced a legislative requirement for digital evidence tools, practices and processes to be compliant with a common set of standards. This increases the professionalism of digital investigators and ensures predictability, reliability and a consistently high quality of evidence gathering, analysis and presentation.

Regulation and Compliance with Codes of Practice

In the UK, digital forensic practitioners are now compelled to be compliant within a 24-month grace period (starting from October 2023) to achieve accreditation to ISO17025 through United Kingdom Accreditation Service (UKAS). This assures the competence, impartiality, and integrity of tools and techniques used, data gathering and data curation together with the analysis of outputs.

This professionalisation of RF Survey work is welcomed; it ensures that high standards are maintained and is no different to what has already been implemented with other digital workstreams such as phone extractions.

As RF Survey practitioners, we have known that this necessary move to statutory regulation has been pending for several years. There has been some great work already undertaken by the body affiliated to the UK based College of Policing and the RF Development and User Group (RFDUG) - in relation to Standard Operating Procedures and liaison with the Forensic Capability Network (FCN) (a UK based, government funded organisation to support good science and promote quality to Law Enforcement organisations), to establish Ground Truth Data (GTD). It is vital that the different methodologies and equipment used by RF practitioners are all validated, calibrated and tested as part of these processes. Critically important, is to ensure that all equipment manufacturers are engaged in the process. The manufacturers have both a commercial and ethical imperative to support both the process and their users.

The direction of travel as the authors see it, is that standardisation of the methodologies and requirements are a given, and through a collaboration of the willing, RF practitioners should seek to ensure these principles are available to - and applied by - the entire RF survey community. The continued collaboration between Law Enforcement, equipment manufacturers, and training providers, is a good starting point to ensure the community speaks with one voice.

Competent, capable and up to date RF experts

Like it or not, the Forensic Science Regulator (FSR) in the UK considers RF survey evidence to be 'expert' evidence. This should not strike fear into the heart of any RF Practitioner. All it means is the practitioner is required to prove that they have a greater degree of knowledge related to RF surveying, than that of a lay person, which in turn can assist the Jury in making an informed decision at the end of a trial. If having knowledge on a subject and wishing to be competent in the topic is something that holds a fear for a practitioner, we are certainly in a dark place.

Competence, knowledge and skills ensure that Geolocation evidence can be delivered as *expert* opinion-based evidence to a Court, which can all be underpinned by adherence to the agreed workstreams in ways that are compliant with the FSR code. The natural outcome of this regime, is consistent - and high-quality evidence - that would increase the confidence in RF survey evidence across the Criminal Justice System. Accreditation of this kind, represents a standard or bar that every practitioner will have to reach in order to practice RF surveying – in the same way they would need to obtain a driving licence before operating a vehicle. Essentially, once the bar is reached, maintaining competence will come down to regular training and Continuing Professional Development (CPD), with ongoing competency assessments and recording all training and CPD type events which contribute to expert status.

The knowledge and expertise built up over several years as RF survey practitioners, also becomes interwoven with other digital disciplines. This allows professionalism to be infused by default in all other investigations, as sharing knowledge and expertise with colleagues helps to develop Digital Media Investigators (DMI) and digital investigative strategies. Law Enforcement RF Practitioners, can sit with an investigation team at the outset of each case and improve the quality of the investigative requests and evidential output, alongside managing the team's expectations of what is technically feasible. RF survey information can be provided quickly within collaborative teams of this kind, in the form of cell coverage data and serving cell tables, which can be dynamically adapted as an investigation unfolds.

All LE RF practitioners within the UK typically attend one of two courses for their initial training - the College of Policing course, or the Forensic Analytics equivalent. Upon completion of an initial course, CPD is achieved through attendance at organised events or online webinars (many of which are free). There is no mandated ongoing support, or further competence assessment as part of these frameworks and generally LE practitioners will keep up to date through briefing papers, conferences, experiential and peer learning. They will have to keep updated training and competence records, which can be requested by assessors as part of an accreditation assessment inspection.

RF Training Curriculum

In the US, LE have benefited by adapting a training pathway for their RF survey practitioners and undertake a series of courses and assessments over a period of time to prove their knowledge and competence. *Only* if they meet the competence threshold, are they accredited and as such they receive regular CPD update training and are deemed to be prosecution experts in the US courts. It must be stressed, that RF surveys are not currently a mainstream activity in the US and are not always necessary due to context such as macro movement or the availability of a reliable GPS fix (or 'ping') for a subject phone. At state and local level, it seems that many organisations are still figuring out their RF survey strategies in conjunction with national teams, to be prepared for potential challenges from defence attorneys in the cell site analysis field, which are starting to become more frequent following the recent rulings already outlined.

Within the US, there is an optional nationally recognised accreditation pathway. The UK should consider this to be a starting point for any practitioner before even considering the methodology to adopt. The UK LE RF Practitioners need to have better and more streamlined lines of communication with the mobile network operators. This would ensure the RF Practitioners have advanced notice of all upcoming changes to the data sources and easy access to new and emerging data sets such as Timing Advance (RTT arcs.) This will allow them to better manage the subsequent impact on their day-to-day analysis and ultimately the lives these technologies will save.

Some private sector digital forensics companies have already started using SDR Scanners to undertake RF surveys and as a result, LE may eventually find themselves on the back foot when providing evidence in cases when the radio environment becomes even more complex, especially if their current equipment becomes insufficient for the future. With the added pressures of private sector practitioners often being automatically considered to be 'Experts', and LE RF Practitioners generally regarded as being professional witnesses (witness of fact), any disparity between the equipment being used may compound the credibility problem further.

The introduction of ISO17025 will help add credibility to accredited LE RF Practitioners and allow them to present expert opinion evidence when suitably trained, competent and experienced; but the key point is that there needs to be a clearly defined and repeatable pathway for people to undertake this training journey and achieve this credibility over a period of time. Not simply to ensure they achieve a minimum standard to tick a box.

Accuracy of survey results

In any operational situation from intelligence product to serving cell tables for a cell dump, we want to know that we have gathered all the available information within the radio environment, not only the RF data appropriate to a case (which may reflect only a subset of the RF cellular coverage within an area). Given that this data can be repurposed for other investigations, we want to make sure we collect the whole cellular environment to give a comprehensive picture of cellular coverage. If a survey were undertaken in relation to a specific network around a crime hotspot, there is a possibility that also capturing the other networks' coverage data, could be very useful for other investigations down the line; or as investigations evolve and further handsets are discovered - which may utilise different networks.

If asked by defence counsel or another expert, *'was there a better way for you to conduct your surveys and come to your conclusions?'*, we never want to have to respond with *"we could not have captured any more data as we did not have the right equipment /correct methodology / it was too expensive"*. These are simply not acceptable answers to give in a criminal prosecution, or even worse - to a Coroners Court. Of course, a worse scenario is to be giving evidence for the prosecution and have a defence attorney present you with an RF survey when you do not have one. This could seriously weaken your position, as your capacity to scrutinise the defence RF work may be limited and may not extend much beyond acknowledging that you agree with the methodology used.

Our survey methodologies - and the results generated - must be **evidentially sound**. We need to have the equipment to gather RF coverage information and the training to correctly interpret them.

We know that the only thing an SDR Scanner cannot do is make an active connection to the network (i.e. make a phone call) to obtain a connected mode reading, due to SDRs in general being passive, 'receive only' devices. By employing a hybrid RF solution - creating an SDR Scanner / SIM-based phone emulator dual methodology - practitioners can ensure that not only the details of all cells within the surveyed environment are captured, in addition, they can also make test calls and generate data pings where necessary. This offers the best of both worlds: the speed and efficiency of an SDR Scanner, with the empirical connected mode serving cell evidence provided by SIM-based phone emulators. The utilisation of multiple survey devices adds evidential rigor to an RF Survey and ensures that, if necessary, you get connected mode readings. More importantly, the survey devices can cross-validate each other, which counters any questions raised in court in relation to the reliability of the evidence created by the tools utilised on a case. This could be particularly important in the US when faced with Daubert and Frye hearings, which seek to test the validity of any forensic tools or techniques employed in a case.

The Importance of CDR's

A typical starting point for a survey (unless undertaking a scene preservation), is the case's CDR data. We need to ensure that our methodology meets the objectives of the survey so ultimately, we usually want to answer a simple question:

"The CDR shows that a device was using a particular cell, so where does that cell provide serving coverage? Can we use that information to determine if the phone could have been there or not?"

Instead of trying to determine *which* cell tower a phone would select if was at a particular location, we need to use the CDR data as a starting point. We already know that the phone used a particular cell as it's in the CDR, so what we need to do is use the survey equipment to identify the areas where the target phone could *possibly* have been whilst utilising that cell.

If our survey equipment and methodologies are not correct or robust enough, and no measurements for the target cell are captured (for which there could be many reasons), we may have to revert to expert opinion based on the CDR. We may alternatively have access to a central repository of RF survey data, where all survey data for a force or a region is stored.

Remember, RF survey data is not personal identifiable data and can safely be stored and reused or repurposed in other cases.

The timing of surveys matters – a repository of 'old' survey data may include surveys of the area within which an incident has occurred, but if the most recent survey data in our repository was undertaken several years before the incident occurred, it will be of questionable evidential value.

If we are proactive and comprehensive in our survey methodology, then we may find recent survey data that was captured around this area of interest. This data could be repurposed for a new case, especially if the survey captured data for all networks.

An additional benefit of using the SDR Scanner as part of a hybrid RF survey methodology, is that it detects cells regardless of any idle mode behaviour, offsets or service profiles that could be applied by a Cellular Service Provider to a SIM card. For example, some operators might force phones in idle mode to use cells in a specific radio band, meaning that idle mode SIM-based survey devices might not get the opportunity to detect serving cells in other radio bands. SDRs will also detect newer Frequency Bands that are not accessible to older devices, such as the latest smartphones having access to TDD Bands like Band 40 - which older phones could not access.

It is possible to have SIM-based tools that are future proofed to all emerging RF channels and technologies and to lock SIM-based equipment to specific radio bands, which can reveal hidden cells. But there is some tradecraft around this, rather than simply recording everything that is on air.

As the number of radio channels increases in a radio environment, then so does the required number of SIM-based modems required to capture them all. This in turn, may require the use of more than one survey device, or impose the requirement to make multiple surveys of the same area to capture the full cellular spectrum.

Usage of survey data for Intelligence purposes

The cost to LE for outsourcing RF survey work to external third-party companies can be expensive and is often charged for on an hourly rate. This results in an evidential report for Court. The raw data that sits behind such a report, is predominantly not delivered to LE by the third party and therefore cannot be stored by the Law Enforcement Agency (LEA) and reused for any other purpose. By owning these datasets themselves, LE can implement effective operational responses, repurpose the data and work through alternative hypothesis should the need arise.

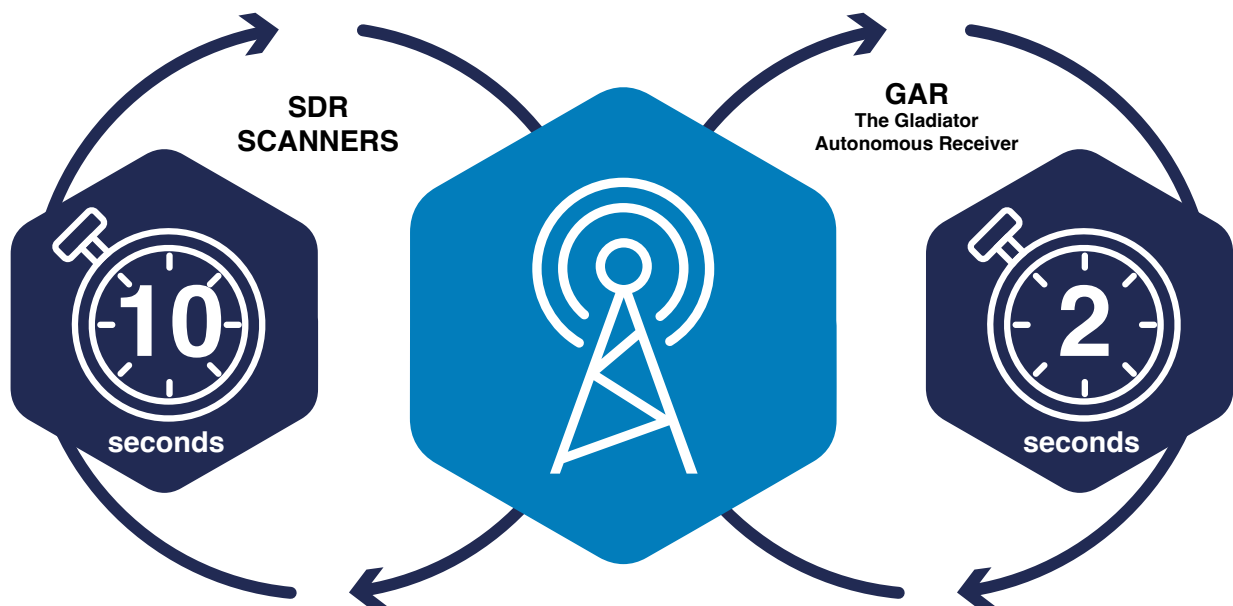
For intelligence purposes, an SDR Scanner can be deployed in isolation from the hybrid RF Solution. Some of the craftwork associated with SIM-based solutions (around connected mode readings / band locking / revisiting the same location / undertaking multiple surveys with different configurations) would be unnecessary when an SDR is used.

If the survey tool is suitably autonomous, then there is no requirement for a trained RF survey technician to conduct surveys for intelligence purposes. Other - less expensive & untrained resources - could be deployed to undertake drive surveys in an area, leaving specialist expert resources to be utilised when and where they are needed rather than spending their time surveying.

The sample rate employed by a survey device - for example how frequently the device captures each new set of RF measurements - is really important in this context, as it is a factor in determining the granularity of the resultant intelligence. A sufficiently frequent sample rate, where a new set of measurements are captured every few seconds, means that a drive survey can be conducted at normal road speeds with the certainty that data isn't being missed. Both UK and US LE are short on manpower and time, so if an 'intel' survey product is never going to be shown inside of a Court room, there is no point tying up a highly trained RF surveyor to capture the data, meaning less highly trained resources can share the burden.

With the ever-expanding set of radio bands used for cellular services – from the 700 MHz band, up in to the 3.5 GHz band and on into the mm Wave GHz bands and beyond, it is necessary to ensure that the sampling rate employed by a survey device is sufficient.

It has been demonstrated in the past that it can take some SDR scanners up to **10 seconds** to scan the entire spectrum which is obviously inadequate in a fast-moving vehicle. The Gladiator Autonomous Receiver (GAR) has an average sampling rate of **2 seconds**, meaning that every 2 seconds it reads everything between 350 MHz and 6 GHz (to capture the upper Wi-Fi band too). This granularity of data capture is *vital* for effective intelligence and evidential surveys.



SIM-based equipment such as the Lima Cell Monitor has a sample rate of 1 second, however each modem is tuned in to a specific service provider, technology or radio channel. As such, a full scan of all frequencies to capture the cellular environment is not the objective of this type of equipment. Despite the fact that scans of the whole frequency spectrum are possible, they will take much longer than the 2 seconds performed by the GAR.

The issues that LE generally encounter when using RF survey data for intelligence purposes, revolve around making the data accessible to other investigators and analysts. RF survey teams are generally small and multi-purpose and are therefore not available to interrogate their survey data 24/7, followed by interpreting the data for others.

Most LE investigative teams will deal with RF survey data on a case-by-case basis. Once a survey is complete, they will secure a master and working copy, hash it to protect it, and then file away with the case papers never to be seen again, until further review or defence work requires completion. Some teams have taken an extra step, and place all of their RF survey data into some form of database, which can then be interrogated for intelligence purposes. This is an excellent and progressive step to take, however it still has limiting factors in that the RF survey practitioners have to be present to access and share this intelligence with relevant teams. Historical data collected and stored prior to the implementation of standardised processes and methodologies required under the UK FSR Code (and previously commended in this paper) adds another level of risk to the utilisation of historical data outside accredited standard operating practices.

The true value in using RF survey data for intelligence purposes lies with having the correct management system to consolidate all the data within one central repository.

Modern day policing in the UK is no longer defined by county boundaries, and neither should our RF survey data be. We need to have **a common and sharable** database for RF survey data that not only allows all participants to utilise it in day-to-day policing, but also helps and expedites knowledge transfer.

An example of where this is critical is where one network records the Cell IDs with a bespoke numbering format which doesn't reflect the Cell Global Identifier (CGI) number transmitted by a base station over the air.

If the cell ID format presented in the CDRs *does not* match up to the cell ID format captured in RF survey data, it is difficult to link those two forms of data together. These records would need to be correlated, meaning that knowledge, understanding and expertise are critical components of any solution in the geolocation space.

Additionally, one of the biggest impacts on government organisations is the turnover of skilled staff, leaving a gap in the organisation's knowledge. The implementation of searchable, historical RF survey database with all the required domain knowledge, help and correctly formatted data within it - would help to mitigate capability gaps.

By creating such a system as suggested above, it would allow all survey data to be used more intelligently and more frequently, with greater impact - but this is only as good as the data that is entered into it. There are two considerations with this;

- If a location has never been surveyed, then how can the database be used for intelligence purposes in relation to that location as the cellular coverage is unknown?
- What if the location has been surveyed, but it did not capture the entire radio environment (which could be the case should an environment have been surveyed for only one network), what about the others?

The future survey methodology needs to address both of these points and could be achieved by conducting proactive drive surveys on known high impact areas using a surveying solution that captures everything.

Speed of response and surveying

Capturing the RF environment as close as possible to the date of an offence provides best evidence. This is to ensure that the networks have the least opportunity to have changed between the date of the offence and survey, particularly so in periods of high network change. For example, with 5G being rolled out and 2G/3G being retired, network architectures fluctuate, meaning some of the cells that are broadcasting today may not be there tomorrow.

It has also been demonstrated to great effect, that LE can react in real time to events that unfold during a trial. It has been known for defendants to wait until the prosecution case has ended, before getting into the witness box themselves and providing a version of events that the prosecution then has no time to react to. In this instance, if an unexpected defence statement is provided in a case, suitably equipped LE RF survey practitioners can go out **the same day**, survey new locations and then provide an evidential report back to the Court as rebuttal evidence, thereby potentially negating the defence testimony.

In terms of how fast LE are able to respond, this would only pose an issue to LE who outsource their RF survey work, as they are dependent upon a third party's availability which they are not in control of. LE who have their own RF survey capability and equipment, can react as soon as their operational commitments allow. LE who outsource, must go through established protocols and service level agreements with vendors, and often due to the onerous nature of these forensic submissions, this gets left as a lower priority task to complete. As a result, outsourced surveys are sometimes not undertaken until many months after the incident took place. In the current extremely dynamic RF environment, this can have a significant impact on a case.

The time taken to complete the full survey including, ensuring that all desired cells have been captured, handling issues associated with missing cells, having to make repeat visits to a site adding delay to the process will resonate with the LE RF Community. Having to repeatedly return to the same location to find missing cells or spending days surveying multiple locations is not only frustrating, but wastes hours of a trained RF survey technicians' time. Repeat visits could be due to a result of new information which is brought forward in a case, involving different networks for example. By deploying the hybrid RF methodology, all networks and scenarios can be captured on the first visit, reducing the need to return.

What about the opposite end of this speed argument?

What if the survey request relates to a cold case or one that has taken many years to come to fruition?

Our hybrid RF methodology needs to have a better response to handling cold cases, other than reverting to CDR analysis and opinion. LE can store RF survey data indefinitely as it doesn't contain any personal information.

As mentioned previously, by gathering, collating, analysing and storing our RF data in a suitable management system, it would be possible to use that historical data to provide insights to the cell coverage found at locations at points in the past.

Interoperability between forces and regions

In the UK, the debate on whether we should maintain a national RF survey intelligence database to allow law enforcement agencies to pool and access survey data for intelligence purposes has rumbled on for many years. RF survey practitioners provide mutual aid to each other in this area of business, by sharing survey data if asked, but each LE team is usually very small and has little operational resilience.

At this point ask yourself;

Do the points laid out above, summarise the needs associated with your RF surveying activities and does your existing RF survey methodology meet those needs?

If your RF surveying needs are not being met, then what do we need to do now? What do we also need to do to future proof ourselves against the ever-developing complexity of the radio environment, shifting accreditation landscape and diminishing financial budgets?

As long as RF survey data continues to be stored in silos within individual RF teams, then the ambitions of data sharing, mutual support and searchable historical coverage data are never going to be truly achieved. A nationally accessible cloud-based solution that interacts with all RF survey devices and allows the survey data to be uploaded automatically in real time, should be the **true** objective. This can then allow appropriate personnel both inside **and** outside of the RF survey teams, to access this valuable intelligence regardless of agency, location or time of day. This would truly add value to all areas of policing, from low level functions such as missing and wanted persons that may not reach the threshold for higher end techniques, all the way through to a full covert response for a crime in action.



Considerations when selecting surveying equipment

Any RF Survey equipment can only measure what is there at the time a survey is conducted. Often, an RF survey has a clear objective to be achieved – whether that is to find the service area of specific cells and/or to see what cells serve at a specific location. When purchasing RF survey equipment, careful consideration should be given with regards to how it will be used:

Do you want to gather the whole spectrum in a single pass, rather than band locking and re-driving the same route repeatedly? We need to consider each of the below areas to ensure we meet our needs:

- **Strategy (proactive versus reactive)**
- **Futureproofing**
- **Ease of use**
- **Affordability (ROI)**
- **Training and accreditation**
- **Operational costs**
- **Support**

The complexity of the radio environment determines what equipment you need to capture it.

We have more than **doubled** the spectrum allocation for cellular communication in the past 10 years - this fact alone adds enormous complexity. The deployment of new technologies, such as 4G/5G Dynamic Spectrum Sharing ([DSS Technical Paper](#))*, adds another level of complexity, whereby on the same frequency, it is possible to have more than one technology co-resident within a single radio channel.

Whilst the deployment of an SDR scanner will achieve the same result in a matter of minutes or hours in comparison to what a SIM based solution may take, at first it may seem difficult for the limited budgets of LE to stretch to more than £100k for a single piece of SDR scanner equipment.

However, when using RF survey data acquired by such a device to address **threats to life** in real time cases, this cost pales in significance when compared to reductions in **threat, harm, risk, collateral intrusion, exposure of covert assets and the reduction of staff hours deployed.**



Return on investment


In order to quantify this return on investment, we need to look at our current methodology for a crime in action, such as a manhunt or a Missing Person enquiry.



One of the authors of this paper spent over a decade involved in these types of incidents and is well versed in the implemented procedures.

When a life is at risk - every minute counts and involves the deployment of every available resource and capability. An average force in the UK has 12 Missing Person (MISPERS) enquiries per day. In turn, a person goes missing every 90 seconds across the UK. The Metropolitan Police alone spend around **£77 million** on Medium Risk MISPERS every year (as shown below).

This is calculated by showing the number of medium risk MISPERS multiplied by the investigative cost per case, which currently sits at £3228.00³ Based on the following:

 METROPOLITAN POLICE		METROPOLITAN POLICE - MISSING PERSONS Investigations - 2020/2021(COVID) - Risk Level				
		High Risk	Medium Risk	Low Risk	No Apparent Risk	TOTAL
		3,969	24,050	7,732	3,505	39,256 107.55 Per Day
		24,050 x £3,228 (Medium Risk) = £77,633,400				

It is not uncommon to spend hours and days searching for phones using traditional methodologies and the staff welfare, asset exposure and cost associated with this are all additional factors. Reducing this time is mission critical, which can be measured in successful outcomes with saved lives and saved time. Time is money.

The respected UK research organisation - The Police Foundation - in their final report as part of 'The Strategic review of Policing' in England and Wales stated:

“Similarly missing persons calls are a regular occurrence. Almost half of all young people in care go missing at least once and for some it is much more common. Of course, it is important to track down missing persons, but it is striking that the police spend three million investigation hours per year on these cases.

That is equivalent of 1,562 full time officers, all day and every day; incredibly that is more police officer time than we currently allocate to police the whole of North Yorkshire”.³

As discussed previously, introducing RF survey data to reduce search areas and more accurately directing resources not only recovers the target more quickly, but also reduces threat, harm, risk and collateral intrusion. In addition, it is more efficient, saving thousands of £ or \$ in the process, by reducing lengthy deployments to a couple of hours.

Resourcing an “incident control room” on a rest day, can cost in the region of a thousand pounds an hour. To reduce a 12 hour deployment down to 2 hours, (which one of the authors has personally been involved in), would reduce the overtime expenditure by £10k or \$12.6k on a single event.

If RF survey data was utilised on as few as 10% of these types of events, this would still amount to savings far greater than the procurement costs of the RF survey solutions every year.

³ A NEW MODE OF PROTECTION Redesigning policing and public safety for the 21st century March 2022.

RF survey practitioners are trained with SIM-based surveying solutions, meaning they will understand the arguments in support of using this methodology. SIM-based survey devices (which are lower cost than SDR Scanners) emulate the actions of the subject phone and provide an indication of the ‘usability’ of cells as well as their ‘detectability’, allowing practitioners to make calls to test that usability.

This has always been the “best we can do in the circumstances”, however we know operationally that we can have two identical devices, with the same chipset, same operating system, antennas, firmware and SIM’s, that occasionally measure different serving cells at the same location. This was backed up by a recent ground truth data survey witnessed by one of the writers, whereby two SIM-based survey devices sitting next to each other on the front passenger seat of a vehicle - reported *different* serving Cell IDs to each other **at the same point** in time, despite both having the same configuration. There are obviously various factors that can affect the choice of serving cell by a phone or phone emulator, including direction of travel, usage of the device, the type of SIM and/or handset and other radio environmental factors, but even then - is a SIM based solution alone really gathering all the cellular data that is there?

For the more technical readers, the following information may be useful, however if technical papers don’t rock your world, feel free to skip the following paragraph.

An SDR Scanner - like the Gladiator GAR - provides the expected wide-spectrum capture capability, but **backs that up** by capturing cell selection parameters from the detected cells and performing the same selection calculations that a phone emulator would undertake. It decodes all the broadcast channel network information which is within the master information block (MIB) and system information blocks (SIBs). The way in which this system information is deployed is evolving with 5G SA. A snapshot of the types of information that these blocks hold is shown in the below table;

BLOCK	4G	5G
MIB	Carries physical layer information of LTE cell which in turn help receive further SIs, i.e. system bandwidth	SFN, critical information for the reception of SIB1, Cell barred flag, Intra frequency reselection allowed flag
SIB1	Cell Access Related Information - PLMN Identity List, PLMN Identity, Cell selection / barring, radio resource config, scheduling of other SIBs TA Code, Cell identity & Cell Status	Cell selection / barring, radio resource configuration, scheduling of other SIB’s
SIB2	Access Barring Information - Access Probability factor, Access Class Baring List, Access Class Baring Time, Random Access Parameter, PRACH Configuration	Cell reselection (intra freq, inter freq, IRAT) common
SIB3	Cell-reselection parameters for INTRA-Frequency, INTER-Frequency Information about the serving frequency and intra-frequency neighbouring and Inter-RAT	Information about the serving frequency and INTRA-frequency neighbouring cells relevant for cell re-selection
SIB4	Cell-reselection parameters for Neighbouring INTRA-Frequency	Information about Inter-frequencies neighbouring cells relevant for cell re- selection
SIB5	Cell-reselection parameters for INTER-Frequency	Information about E-UTRA frequencies and E-UTRA neighbouring cells relevant for cell re-selection
SIB6	Cell-reselection parameters for INTER-Frequency	Used for Earthquake and Tsunami warning system – Primary. This is SIB10 on LTE
SIB7	Cell-reselection parameters INTER RAT Frequency (GERAN)	Used for Earthquake and Tsunami warning system – Secondary. This is SIB11 on LTE
SIB8	Information for reselection to CDMA2000 systems	Commercial Mobile Alert System. This is SIB 12 on LTE
SIB9	Home eNodeB name - for future LTE femtocell applications	Information related to GPS time and Coordinated Universal Time (UTC). This is SIB16 on LTE

The table shown does not show all the SIBs, however one additional important block of note is System Information Block 24 (SIB24). This is configured on the 4G side to broadcast all the cell reselection info for 5G neighbours, so a phone can perform cell reselection from 4G towards 5G.

On a recent high-profile murder case, where it was crucial to ensure that the entire radio environment was captured, no suspect device was initially known, meaning that no CDRs were available to the investigation. The investigators requested an RF 'preservation survey', which captures details of all networks and all technologies at a location for later use in the investigation when suspects and their devices have been identified. Both SDR-based and SIM-based types of equipment were utilised as outlined above as a hybrid RF solution.

This is not a complete breakdown / assessment, but for example purposes the resultant data showed;

- On 900 MHz on Vodafone, the SIM-based surveying equipment detected 4 cells with reported dBm values all in excess of -86. These were all really strong readings and obviously a GSM phone always uses the strongest signal;
 - C1 select the strongest available permitted cell,
 - C2 if a neighbour cell is strong enough, for long enough then the device must reselect to the stronger cell.

But were the SIM based solutions blinkered – were they seeing everything they needed to?

If a suspect had been using a burner phone with a PAYG SIM on an MVNO with no credit, would it have camped on these cells?

The SDR-based device at the same time and location reported that there were 38 cells detected on 900 MHz on Vodafone, which all had a signal strength in excess of -104 dBm. Obviously, a GSM phone is not going to choose to use a signal as weak as -104dBm when much stronger ones are available, however if the circumstances had been different, *aren't these still usable cells?*

Even disregarding the lower end of the cell detections, the survey devices corroborated each other as to the strongest signals detected bar one. The four cells detected on the SIM based solutions, were in the top 5 on the set detected by the SDR equipment - however the second strongest cell on a different channel, was not detected on the SIM-based equipment. Undoubtedly, if the SIM based solution had been band locked to each Vodafone radio channel, this cell would have been detected, but in a situation where you need to capture everything regardless, this is only viable if you have the time and the tradecraft knowledge to potentially do multiple sweeps

- On LTE with EE, the SIM-based equipment detected 11 cells across bands 3 & 7 (both FDD) and all within the same tracking area code (No band locking was applied as this was a preservation survey). The Reference Signal Received Quality (RSRQ) on all 11 cells was between -11 dB and -18.25 dB (which is quite low powered) and the average Reference Signal Received Power (RSRP) levels were all above -120 dBm. The scanner detected 19 cells with an RSRQ better than -20 dB across 3 different tracking area codes. These were detected on Bands 1, 3, 7, 20 and 40 (FDD and TDD) and again the average RSRP was above -120 dBm.

By assessing these results against the needs assessment above, we can see that using only SIM-based surveying equipment would not have provided such a comprehensive view and hence may not have met the survey requirements. If a serving cell table was provided to an investigator based on SIM-based survey equipment alone, it is possible that their survey may have missed some important cells. If any of those 'missed' cells were later found to be significant, once a suspect was identified and once their CDRs were obtained, the fact that the cell was missing from the RF survey summary, may have led investigators to believe that the cell didn't cover the crime scene.

So, what's best – SDR-based surveying or SIM-based surveying?

There is no simple answer, but one option that has been proven to work and achieves everything on our 'methodology needs list', is to deploy a hybrid SIM / SDR scanner RF survey model. In addition to improving the depth and detail of survey data, this hybrid model can break the separate silos of RF survey data open, and make it more accessible for use by front line and specialist policing. This in turn provides significant operational savings through reducing unnecessary deployment time and freeing up officers to work on different tasks - but more importantly - reduces threat, harm and risk to both the public and LE officers by reducing their exposure time.

By utilising RF survey data at the outset of an investigation, it can also help to reduce collateral intrusion by speeding up or even entirely preventing the deployment of covert assets, which in turn reduces liability towards LE. By providing a 24/7/365 actionable intelligence product to a wider set of internal data 'customers', LE teams could secure separate funding streams, rather than being solely reliant on their limited RF survey budgets.

Conclusion

To meet the current and future needs of LE RF surveying, we can sum up our evolved methodology as:

- Move from entirely SIM-based surveying techniques to a hybrid RF survey solution, using both SIM-based and SDR-based survey devices to ensure data breadth and accuracy in a constantly evolving radio environment.
- Use RF survey data in much more productive ways to benefit all areas of Policing, such as PoLSA's, County Lines, Wanted / Fugitive units, Analysts, Covert Units, telecom SPoC's and even front-line response teams.
- Share RF survey data, methodologies and knowledge more widely within the LE community through an appropriate data management system that is secure, accessible and available.
- Define an accreditation pathway from end to end, with continuous ongoing CPD assessment and support that gives the judiciary confidence in the expert status of LE RF practitioners.

An example of this more forward-thinking approach, and one that ultimately will result in financial and operational savings within just over a year of initial investment, is the "invest to save" model, adopted by Greater Manchester Police. GMP deploy a hybrid RF survey methodology that achieves all the needs outlined in this paper.

Gladiator Forensics and Forensic Analytics would like to invite you to an event for you to come and see this hybrid RF survey model in action. GMP and the authors will host you for a day of workshops, case studies and presentations on Tuesday 30th April 2024. If you're interested in attending, please register [here](#)

The hybrid RF survey methodology combines the speed and breadth of SDR-based surveys with the connected mode detail of SIM based solutions. It offers a path to a more efficient method of conducting surveys, coupled with a scalable and searchable RF survey data management systems that can unlock the investigative benefits of RF survey data for a far wider pool of law enforcement purposes. Join us to find out more.