



Inquirix

Radio Wave OSINT using Software Defined Radio

AUTHOR: Abi Waddell

<http://www.inquirix.org>

VERSION 1.0

March 2022

This highlights what open-source intelligence (OSINT) can be gathered from radio waves using software defined radio (SDR) in the hope that this will be useful to red teamers and other infosec professionals who would not normally consider including radio transmissions (especially outside of the Bluetooth/Wi-Fi frequencies bands) in the scope of an engagement.

This will cover a bit on raw data capture and decoding, along with OSINT techniques, derived from advanced searches and technical exploration, to discover sensitive device and user data, and will also touch on the legalities of such radio interception.




Firstly, why should we focus on open-source intel? The main reasons include:

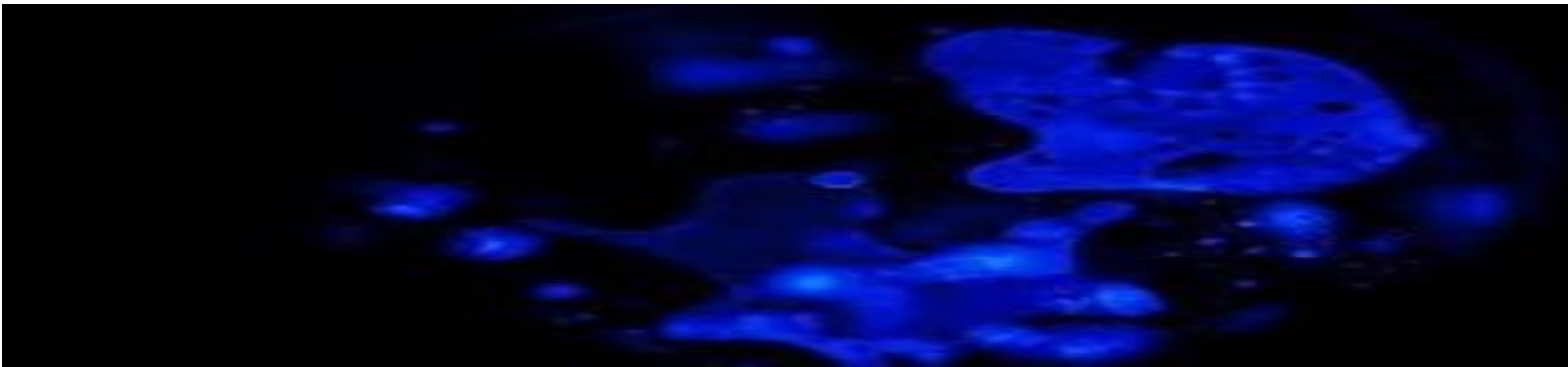
- To reduce the risk of fruitful pre-attack recon activity. In other words such activity could lead to a breach.
- The probability that intel from public sources will be discovered and exploited is high especially as this does not usually require a high level of skill.
- Leaks that are accessible to the wider public have a high potential of causing reputational damage.
- Breach recon activities are not usually captured by existing tools and methods either pre or post incident mainly because such activities occur away from the company network.

The good news is that open-source leaks can largely be remedied with a small effort but with a large impact on the reduction of risk, and finally, by considering public sources outside of the corporate network one has a greater visibility of the wider attack surface.

For those who are new to SDR, this is a very quick overview on getting started with some of the equipment used in radio scanning.

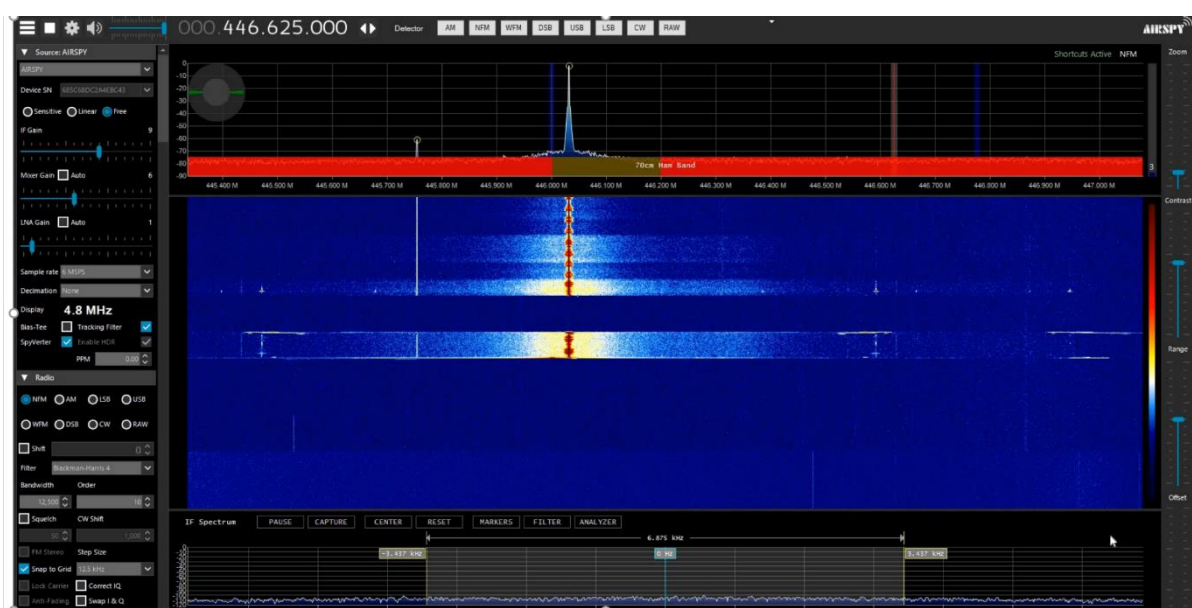
Scanner Equipment

<p>Traditional</p>  <ul style="list-style-type: none">• Expensive• Limited functions– but do it well• Less user input• Lack of customisation• May not have signal patterns displayed	<p>'Hobbyist'</p>  <ul style="list-style-type: none">• Plug & play• Runs on Android, Windows, Linux, RaspPi, Mac• 24 – 1700 MHz native RX range• Cost between £30£250	<p>Mobile scanner antenna</p> <ul style="list-style-type: none">• Frequency RX: 25-2000 MHz• Length: 650mm• Connection: BNC male 
--	--	--



Traditional hardware-based scanners look a bit like one on the left of the above image. They are expensive – usually costing between a few hundred to several thousand GBP; they have limited or dedicated functions – but do it well; and they require less user input – it’s usually a simple case of switching it on and turning some dials. However, there is little potential for user customisation, and it is not usually possible to see the visual signal patterns.

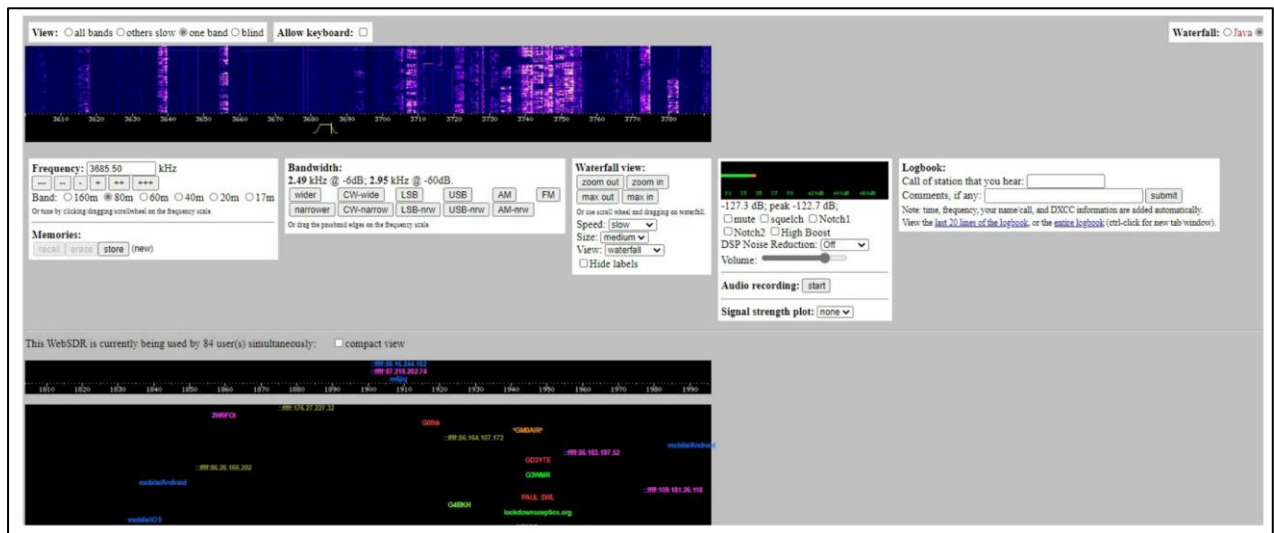
A typical hobbyist setup may involve using an SDR dongle which is about the size of a USB stick – perhaps a little larger. And then an antenna which can work on specific frequencies and may be able to transmit as well as receive. Some can be mounted on vehicles via a magnetised base. The SDR dongle will usually be plug and play, will work with most operating systems and may or may not be able to work as a transceiver. The above image gives a brief spec of the Airspy and a typical antenna. Most such SDR equipment comes to between £30 and £250 depending on what you want to use it for and how reliable you need it to be.



SDR sharp is a popular software app for SDR dongles. It is easy to use and has a multitude of modules that allows you to do some pretty interesting things. Many SDR programs share similar features – there is usually a screen showing the visual signal patterns, and an option to select the frequencies and filters. Frequencies in this app are shown clearly and it has some helpful labels for some of the bandwidth allocations – for instance military air, FM radio and other bands. The peaks represent the signal strength and time and are extremely helpful when discerning what the listen to. Specific frequencies can also be saved and communications recorded.

One of the most useful features is the automatic frequency scanner which saves you the trouble of manually searching for communications that you might want to listen to.

One other nifty module is the digital radio decoder which can decode various digital protocols such as P25, DMR and D-Star.



WebSDR allows one to listen in on others' SDR and antenna setup without having to get any special equipment yourself – only a web browser is needed. So it is possible to browse to various WebSDR servers in the world and tune in to whatever their antenna can pick up. The dashboard for each is very similar and is easy to use. There is the waterfall display and the option to fine tune the desired frequency and you can squelch background interference noise, alter the volume and make recordings.

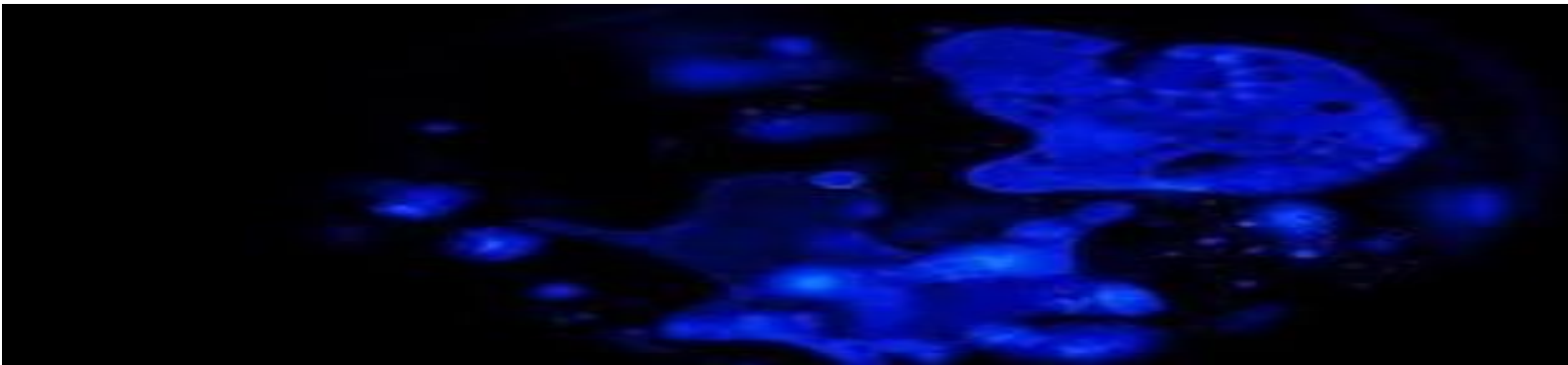
Down the bottom you can see who else is connected to the server. This sometimes helps to see which bands and frequencies are the most popular to listen to if you need any inspiration. The modulation such as USB, CW or AM can also be changed along with other settings.

It is quite surprising the sort of sensitive information that one can pick up over the air, such as usernames, criminal records, car licence plate numbers, physical and email addresses and passwords. Radio hams in particular will sometimes discuss sensitive details over the air.

It is usually very useful when radio scanning, to have the ability to physically locate the source of any transmission and this is just to summarise some methods of doing this.

Trilateration requires the distance between the receiver and transmitter to be measured. Each receiving station measures the length of time taken for the radio signal to reach their position, and when the times from three or more such stations are known, a position for the receiver can be calculated. Each receiving station has an omnidirectional antenna and a very precise clock in order to have any accuracy. A variant on this is time difference of arrival where you can locate a signal source from the different arrival times at the receivers.

Triangulation can be used with multiple fixed-position receiving stations, or it can be used with a single mobile station which has a directional antenna and determines the angle which the signal is received



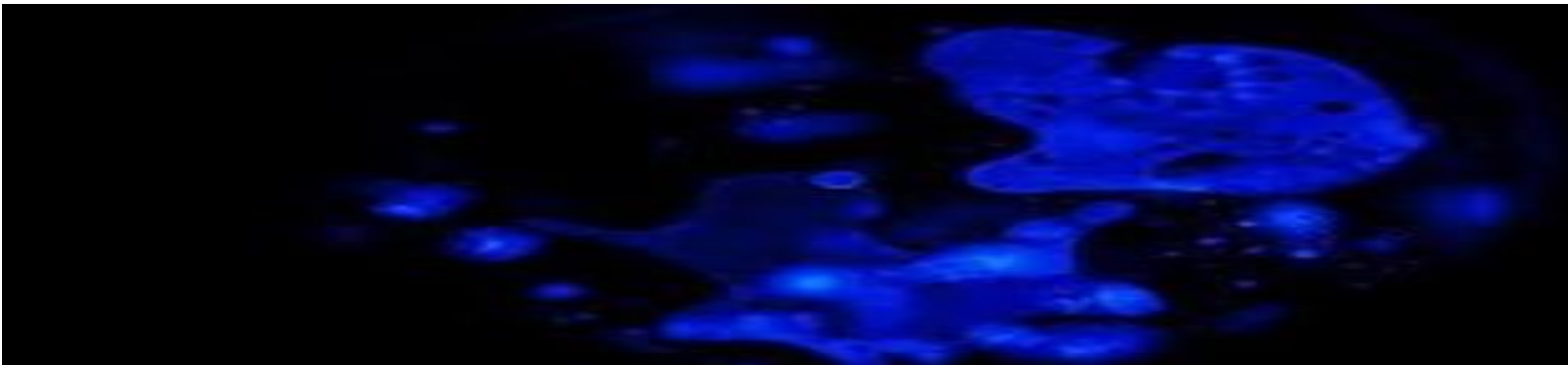
from, - keeping the same reference point such as magnetic north. When this angle is taken from three or more different positions, the location of the transmitter can be calculated. It's also possible to use a directional antenna to determine the position of a transmitter by using the antenna orientation producing the strongest signal to indicate the direction of the transmitter. You can then take two measurements from known transmitters in order to be able to apply triangulation.

Directional antennas show an increase or decrease of the received signal strength depending on the physical rotation. The doppler shift method analyses the received signals and determines a probable direction from which the signal originates. Correlative Interferometry is about moving receivers—perhaps in a vehicle, and how different measurements at different positions of the vehicle's trajectory are taken into account.

Transmissions sometimes have to be processed further in order to understand the content. Raw captured data which has been encoded or encrypted can either be processed on the fly at the time they are received by the SDR software using various modules, or this data could be saved to a file – usually a packet capture file for offline analysis.

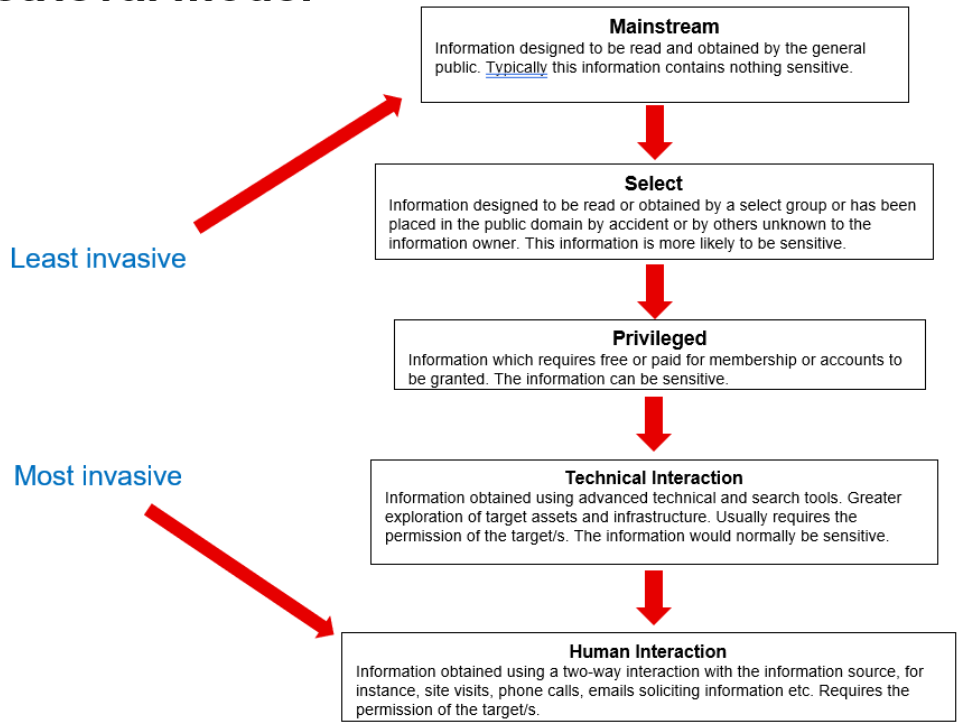
So what can be listened to? This is not meant to be an exhaustive list and note that I am not saying you should listen to these, but here are a few:

- Baby Monitors – not to listen to babies but other sounds in the physical vicinity of the monitor.
- Illegal Fishing Buoys can be detected especially as they often transmit in bands they are not authorised to use.
- Numbers Stations – these are shortwave radio stations that transmit encrypted secret messages in the form of numbers, thought to be used by government agents. The numbers are sent on pre-determined frequencies with the use of automated voice, Morse code, or digital modes. Most use a one-time pad encryption and so only the person who has a copy of the one-time pad would be able to decode the message. Stations are usually given a nickname and many are well known because of the music they play. Every transmission usually has an intro or end phrase.
- The SETI project aims to detect radio signals originating from intelligent species in space. Multiple stations around the world monitor stars for a period of time to collect data and the collected audio is analysed using special software.
- Long Range/low power wide area network IoT devices can be decoded and decrypted but this appears to be a work in progress.
- DECT cordless phones can be unencrypted and usually have weak encryption if encryption is used.
- Iridium/Inmarsat satellite transmissions can be decoded.

- 
- Some wireless keyboards are vulnerable to being sniffed by measuring the Received Signal Strength (RSS) of the messages transmitted between the keyboard and the dongle attached to the computer, looking at the timings between different keystrokes, and also using machine learning to look at the likelihood of a particular word being entered by the target user.
 - Military radio transmissions can be picked up in the clear, particularly if commercial handsets are in use. Recently a set of bands for a particular country's alleged military were publicised on Twitter.
 - Fake 4G base stations can be detected using the Crocodile Hunter tool which essentially decodes the master information block and system information block for a group of cells, and detects anomalies in these results whilst determining the probable location of these cells using radiolocation techniques. Anomalies in the results include cells that move location or change signal strength, or have missing parameters, and cells being located in unexpected places. And experiments have been done to fingerprint Wi-Fi adaptors using radio frequency analysis with around 95% accuracy.
 - Pager messages can be intercepted and decoded on the fly using SDR Sharp and other software. Pagers are not so commonly used these days, but have a high likelihood of having their transmissions captured because the signal travels over long distances. Hospital staff and taxis still use pagers but such technology is being phased out. Pager transmissions have a very distinct waterfall view and sound.
 - SDR can also be used to detect emanations coming from electrical equipment – commonly known as a Tempest attack. This works by positioning the SDR and antenna close to the monitor of the victim computer and then picking up the live image being displayed on this device but on the attack computer, which is running the SDR software. Whilst it is easy and straightforward to run the tempest attack software, getting the technique to work effectively is a bit hit and miss and also requires being in very close proximity to the target device.

OSINT gathering can be put into different categories according to the type of repository of the data, the expected levels of permission to this data and the level of sensitivity of this data. This is an OSINT data retrieval model created by Inquirix:

OSINT data retrieval model



As the tiers go down, the data generally, but not always, is more sensitive and requires more permission to access. At the top, the mainstream category includes anything freely available to the public; the select category is data that is only meant to be shared with a specific group – this includes most free deep web sites; down to privileged, which requires an applied-for account in order to be accessed – such accounts require payment and, or further screening beyond a simple device verification. Examples include paid-for news or media subscription sites.

Down below, the more invasive methods usually result in obtaining more sensitive data but require greater permission levels. Any data out in the open from these methods is likely to be from unintentional leakage. An example could be that I am email a hotel reception about my room booking but they respond to me with an email that is intended for a different customer by mistake. Or a webpage is misconfigured and shows a list of hidden files and directories which anyone can access if they are technically able to find the misconfigured URL.

What follows are some of the ways of obtaining OSINT data relating to radio transmitters and users.

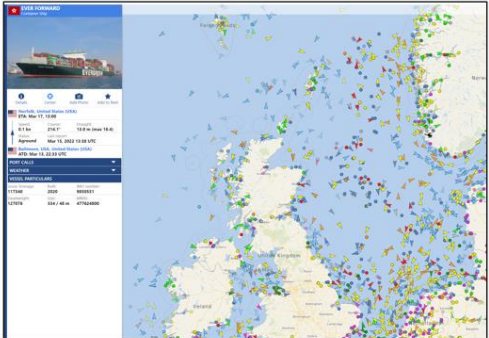
The radio reference site and this area on the Ofcom site allow one to search for organisations' owned licenced frequencies with location details of their transmitters.

In the USA the FCC site has a search facility to look up call sign, frequencies in use, site addresses of licensees and other information.

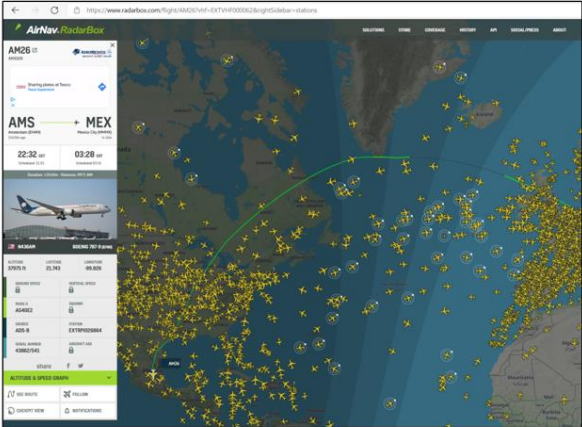
The Signal identification wiki site is useful for looking up the frequency bands, and includes samples of what these signals look like.

Transport Radar and WSPR


Marine Radar



Flight Radar



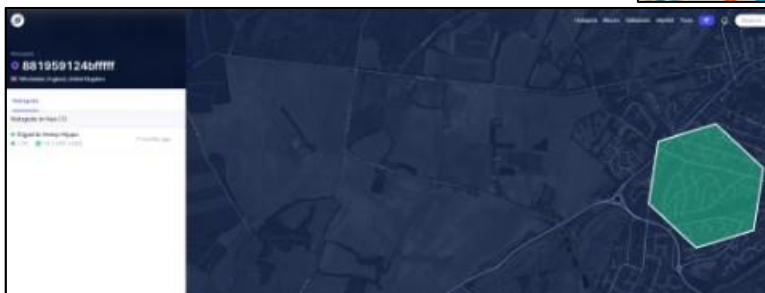
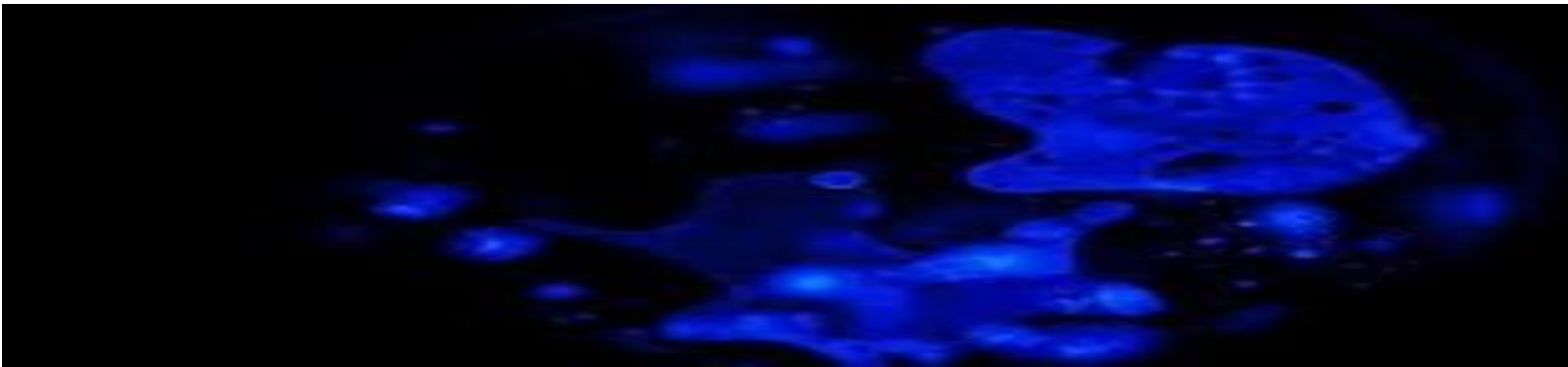
WSPR



17

There are various sites that show the live movements of flights and ships such as Radarbox and vessel finder. The WSPR or whisper network which stands for Weak Signal Propagation Reporter is a global set of transmitting and receiving whisper radio stations that document any “spots” or detections of specific radio transmissions. A single whisper link can provide detection of an aircraft along its propagation path using high frequency transmissions over several thousand kilometres. Multiple whisper links synchronised at the same time, can provide more specific data and it’s possible to track an aircraft as it will produce a scatter of radio signals. It was possible to track some of the journey of the doomed missing Malaysian flight MH370 using this method as all search efforts had not met with any success.

Opencellid is a useful site to see the location and details of cell towers. And the Helium explorer map shows the location of all the active Helium cryptocurrency mining devices:



If a particular device of interest is suspected, either because of its owner, or its possible geographical location, it is possible to find out more about this device if it's an iPhone and has the find my iPhone service enabled and you know the user's iCloud credentials, because one can skip the two-factor authentication in order to use the app via a browser. Obviously, this is a feature which is there by design as it allows users who have lost their phone to find it, and they only need to login to iCloud to do this.

'Find my phone' iPhone verification bypass

Sign in to iCloud with target's name & password



The verification 2FA is triggered



Ignore the 2FA and go to Account Settings at the top



Device type can be seen. Click on 'Find iPhone'



Location of device can be seen and further RF exploration can take place



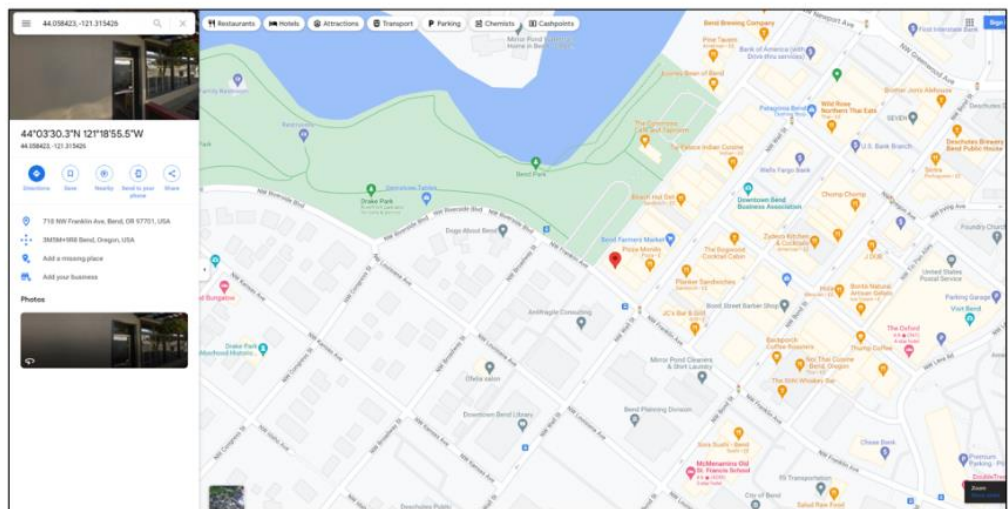
So, if an unauthorised user has possession of the victim's iCloud credentials, they can go right in and see the phone model they use and also their geographical location. Knowing that the user here has an iPhone 12 we can assume that ultrawide band may be in use and this information may be useful if conducting further assessments in the locality. Ultrawide band is a radio technology that can use a

very low energy level for short-range, high-bandwidth communications, and is particularly suited to precision location activities. Apple was the first to introduce this in smartphones and the advantage of this over Wi-Fi and Bluetooth is that it uses less power and has greater location accuracy. Some of the ultra-wide band applications for phones include the Apple car key, improved seamless media file transfers and connection with home IoT device.

The Airspy server map shows users who have registered their SDRs as servers on this site and this show which are live, their location, and other details like the operating system, the type of device in use, IP address and username.

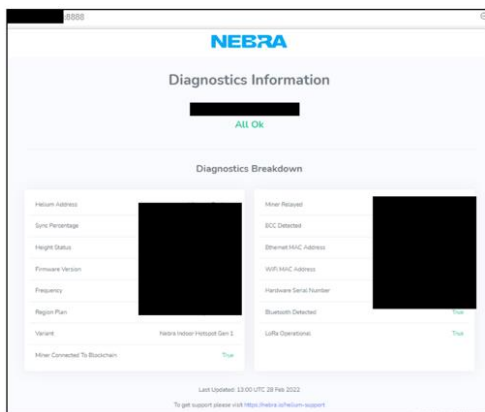
With the location coordinates given in the previous step or even with the IP address from which one can discover a related map location, it is then possible to target surrounding radio frequency transmitters including Wi-Fi hotspots by using the advertised SDR server to scan for signals in the locality. This is still within the bounds of open source as the SDR server is meant to be accessed by the public.

See surrounding addresses/business to piggyback into their hotspots, remotely from the SDR on the map



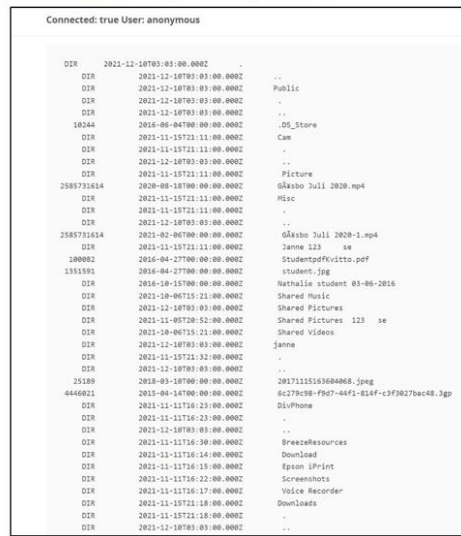
Another way of looking for IoT device information is to access their enabled and open ports and services. Routers which also run cellular and RF services are often accessible this way. This Nebra hotspot miner device was accessible over this specific port and showed the device's version, the MAC address, Helium address and frequency. The other example on the right shows the files accessible over anonymous FTP access on port 21 on a Samsung DVR device.

Nebra IoT device data over port 8888



23

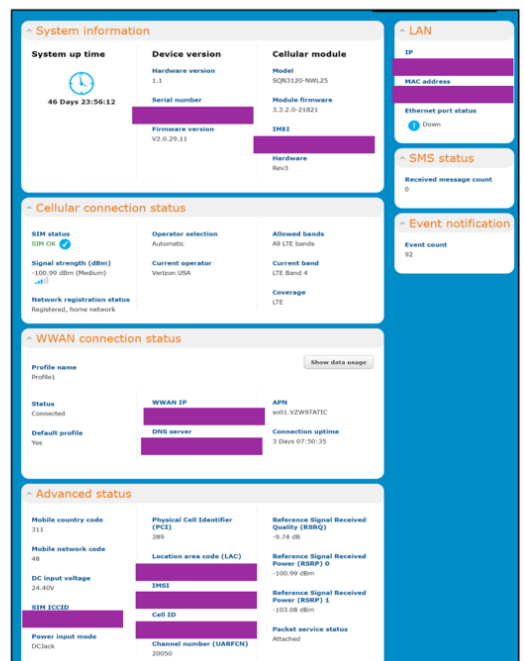
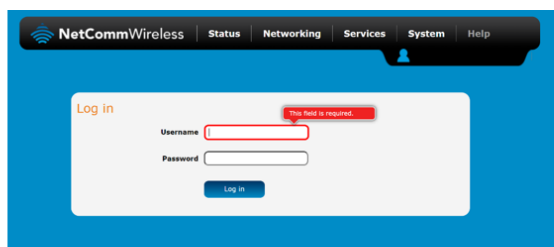
Samsung DVR files accessible over anonymous login on port 21



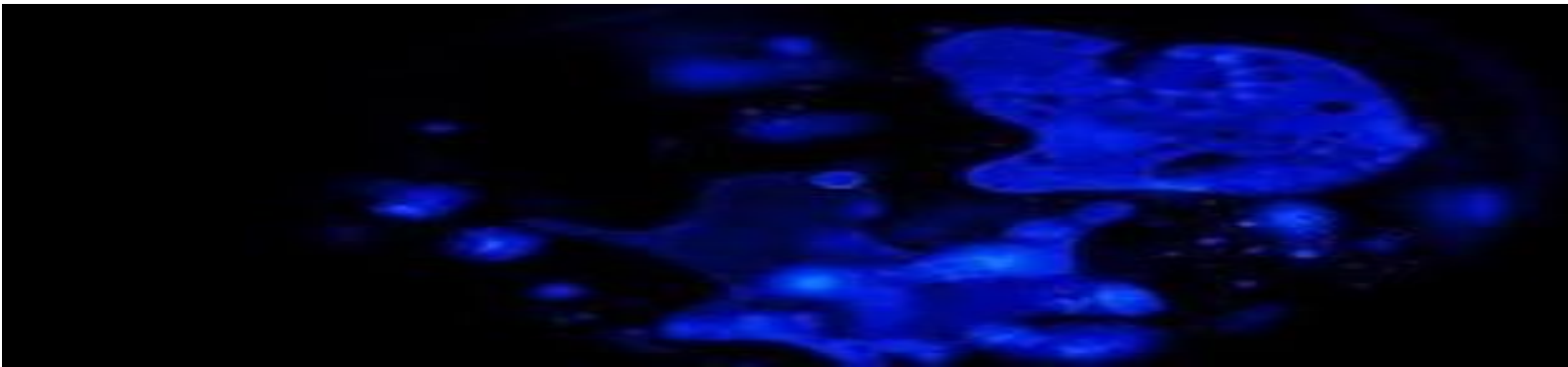
This 4G IoT Netcomm device login screen was accessed over a browser in the same way. It was not necessary to login in order to see the status details which showed the IMEI, IMSI, firmware, and other details.

NetComm login bypass to see device info

4G industrial IoT router login not needed in order to see the `status` which shows IMEI, IMSI, firmware, and other details



24



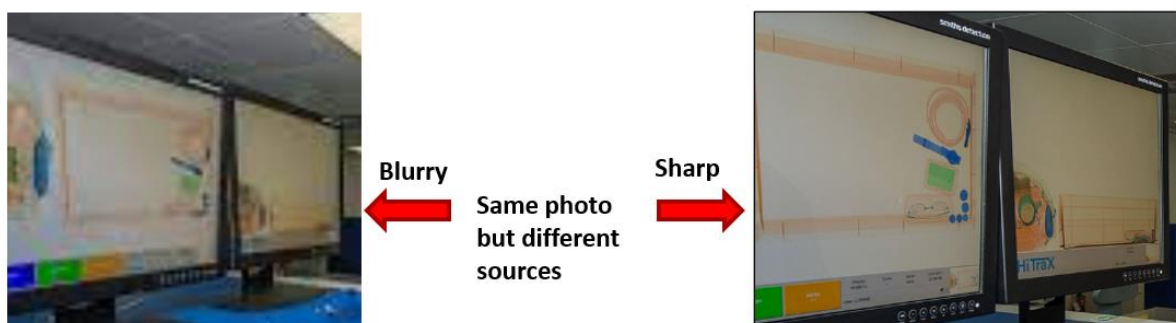
One way of discovering the two-way radio frequencies in use by a target company is to discover the handset models in use. Different radio models usually have their own default frequencies which may not be changed by the users. And one particular way of establishing this is to use tender or contract award databases and websites, as these may reveal the radio supplier and or security company the target has engaged to work with. In the UK, Bidstats is an example of such a site, and this is freely accessible. The redacted contract award here shows the supplier which is a manned security company.

Another useful source are spreadsheets and other databases on public spending. In one example, a security company was paid several thousand pounds to provide stewarding services to an event being held by the organisation listed. Also useful, for finding a company's suppliers are the web statistics functionality that is sometimes accessible on some company websites. Such stats show site visitors which may include suppliers, and there are also paid-for site search engine analytic services that can show much more detailed site backlinks and referrers. So once the radio or security supplier is found, one can look further into the likely radio device models in use.

An assessment was made of the likely frequencies that the manned security guards of a blue big organisation were using for their two-way radio communications. By just talking to the guards, it was discovered that they used analogue two-way radios at one of their sites and so this would have been easy to pick up with a scanner. They also said that at the head office site, they used a mixture of digital and analogue radios.

A search of their suppliers and equipment showed that there was a high probability that Hytera radios were in use, which would have been set on a specific set of frequencies, if left on the default settings.

Images of devices in use can sometimes be found on public sources and it is often useful to get creative with the search terms in use if a particular image is of a poor quality. This example shows the Xray scanner in an airport on a military base – the first search term used the words 'xray scanner' and the name of the base and this showed the image on the left. A search for 'screening device' plus the name of this base, however, shows the device make. Whilst this isn't a typical IoT device the same principal applies.



Another place to pick up open-source data on IoT websites are bug bounty sites, which allow organisations to make freely accessible, details of their servers and applications, and pointers to where they believe vulnerabilities are. This information can then be used for further exploitation. Obviously, this is not to discourage companies from seeking help and wanting to improve their security, but to make one aware of how someone with little scruples could make use of this data.

In this example we can see a well-known Crypto miner development site details showing URL that isn't in public sources and a description of possible ways it could be exploited.

This site address is not publicly advertised

Potential security vulnerabilities as noted by the site owners

hackerone SOLUTIONS PRODUCTS PARTNERS COMPANY

In Scope

The scope of the [redacted] service is restricted to the following:

Domain

- Ability to ssh into [redacted] and connect to consumer [redacted]
- Ability to revoke ssh access to server at [redacted] by other [redacted] employees.

Domain

The scope of the over-the-air update server is restricted to the following:

- Ability to hijack or impersonate web server at [redacted] so that [redacted] download and apply a malicious update.
- Ability to steal or crack the private key used to sign updates pointed to by [redacted] for downloading.
- Ability to upload and provide a malicious OTA image
- Ability to remotely access to the OTA server

https://[redacted]
PLEASE MAKE SURE YOU ARE TESTING ON [redacted]

The scope of the Console application is limited to the following:

It is possible to pick up quite a bit of OSINT from the DSTAR, DMR and other common standards gateways and servers using such sites as dstargateway.org, where information can be found on the last known callers and their location. Very often one sees the gateway or server owners publicising a lot of the details of the configuration of their hardware, with photos too, and with the admin console readily accessible. Likewise, the radioid.net database shows DMR/NXDN users and repeater details:

DPLUS Dashboard | Reflector Status and Control

Registration: [redacted] | Reflector System: [redacted] | DPLUS version: 1.42

Linked Gateways

Module A	Module B	Module C	Module D	Module E
		KBSA B	KCSVFX B	
		KF7CUP B	WRBL B	
		NS9RC B	WWDUA B	

Remote Users

Callsign	User Message	Last TX on	Type
KDLZ		listening	HotSpot
KULBD		listening	HotSpot
KEWER		listening	HotSpot
W9TFA		listening	HotSpot
AE9JG		listening	HotSpot
NK9OE		listening	HotSpot
K9KRA		listening	HotSpot
KC9SIO		listening	HotSpot
W9GFP		listening	HotSpot
K9HKS		listening	HotSpot
NS9YX		listening	HotSpot
K9CPLP		listening	HotSpot
KC9ZMY		listening	HotSpot
W9RX		listening	HotSpot
ND9W		listening	HotSpot
NS9J		listening	HotSpot
K9S9AM		listening	HotSpot
KC9IL		listening	HotSpot
W0BJEN		listening	HotSpot
KD9L	Doug Cerro Gordo IL	D	HotSpot
NS9LJK		listening	HotSpot
K9TFS		listening	HotSpot
NS9AT		listening	HotSpot
W9JUC		listening	HotSpot
PD4X D		listening	HotSpot
KE9AU		listening	HotSpot
W9MJM	Mike-Scottsdale, AZ	C	HotSpot

Last Heard

Callsign	User Message	Last TX on	Time
K9BHOK	SUBURBS OF CHICAGO	C	2020/11/20 03:38:46
NS9RA	BlueDV by PA7LJM	C	2020/11/19 18:58:19
KEWER	Steve / Davenport IA	C	2020/11/19 18:30:46
NS9YT		D	2020/11/19 14:08:01
NS9OE	Cerro Point, IL	D	2020/11/19

The screenshot shows the Radioid.net API documentation page. The left sidebar contains navigation links: Home, FAQ, Support, Database, API, Rpt/ Map, Register, and Signin. The main content area is titled 'API Docs' and includes a note: 'Radioid has an API for querying data. All endpoints are available without authentication and... ** If you are simply looking for a dump of the en...'. Three API endpoints are listed:

- api/dmr/user/**
 - id - DMR ID of a user
 - callsign - DMR user callsign
 - surname - Surname
 - city - City
 - state - State / Province
 - country - Country
- api/dmr/repeater/**
 - id - DMR Repeater ID
 - callsign - Repeater callsign
 - city - Repeater city
 - state - Repeater state / province
 - country - Repeater country
 - frequency - Repeater frequency
 - trustee - Trustee callsign
- api/nxdn/user/**
 - id - DMR ID of a user
 - callsign - DMR user callsign
 - surname - Surname
 - city - City
 - state - State / Province
 - country - Country

To the right of the documentation is a table titled 'DMR/NXDN users and repeater details' with the following data:

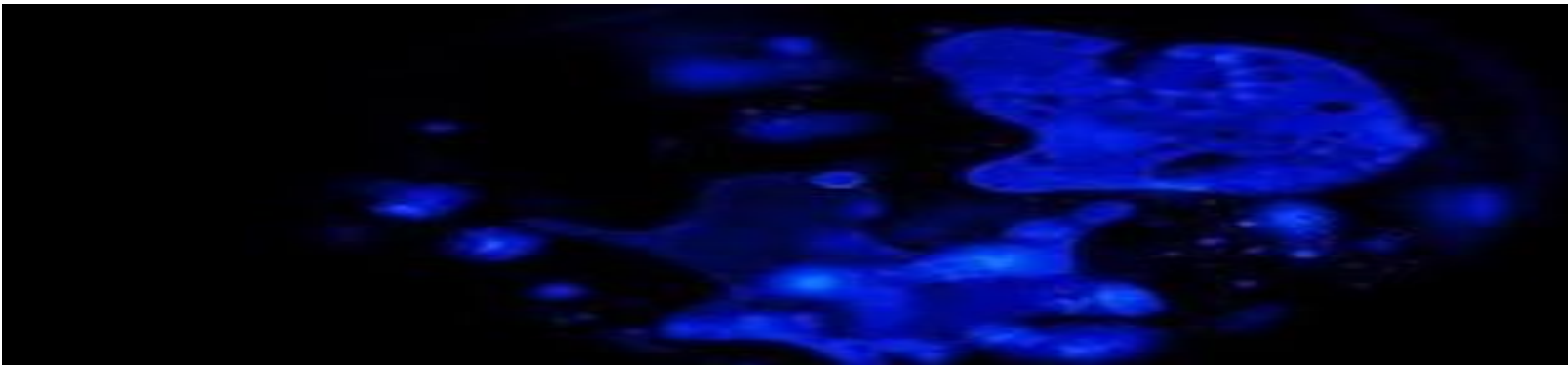
RADIO_ID	CALLSIGN	FIRST_NAME	LAST_NAM	CITY	STATE	COUNTRY	REMARKS
1	1023001	VE3THW	Wayne	Edward	Toronto	Ontario	Canada DMR
2	1023002	VA3ECM	Mathieu	Goulet	Ottawa Hull	Quebec	Canada CCS7
3	1023003	VE3JCZ	Guy	Charon	Gloucester	Ontario	Canada CCS7
4	1023006	VA3UZ	Allan Timothy	Harvey	Sparta	Ontario	Canada DMR
5	1023007	VA3BOC	Hans Juergen	Bockholt	Cornwall	Ontario	Canada
6	1023008	VE3MR	Mark		Niagara Falls	Ontario	Canada DMR
7	1023009	VA3AMO	Rolando	Parto	Scarborough	Ontario	Canada DMR
8	1023010	VA3AMO	Rolando	Parto	Scarborough	Ontario	Canada DMR
9	1023013	VE3SLD	Barry	Brousseau	Guelph	Ontario	Canada DMR
10	1023014	VA3DB	Diane	Bruce	Nepean	Ontario	Canada DMR
11	1023016	VE3AD	John Christensen	Christens	Almonte	Ontario	Canada DMR
12	1023017	VA3MSV	John	Visser	London	Ontario	Canada DMR
13	1023018	VA3BTQ	Jacqueline May	Norman	Nestleton Station	Ontario	Canada DMR
14	1023019	VA3BTQ	Jacqueline May	Norman	Nestleton Station	Ontario	Canada DMR
15	1023020	VE3ZN	Denis	Jakac	Bradford	Ontario	Canada DMR
16	1023021	VE3XN	Denis	Jakac	Bradford	Ontario	Canada DMR
17	1023022	VE3DK	Doug	Baxter	Sudbury	Ontario	Canada DMR
18	1023023	VA3TDG	Doug	Baxter	Sudbury	Ontario	Canada DMR
19	1023024	VA3MRJ	David S	Johnson	Kitchener	Ontario	Canada DMR
20	1023025	VA3ZDK	Gregory K	Green	Ailsa Craig	Ontario	Canada DMR
21	1023026	VE3ELK	David B	Bohan	London	Ontario	Canada DMR
22	1023028	VA3API	Kevin	Bousquet	Burlington	Ontario	Canada DMR
23	1023029	VA3NSC	David B	Sangwin	Port Perry	Ontario	Canada DMR
24	1023030	VE3DZT	Alexander	Blaiss	Kitchener	Ontario	Canada DMR
25	1023031	VA3PMR	Perry Marvin	Rubin	Thornhill	Ontario	Canada DMR
26	1023032	VE3TJD	Tedd	Doda	Petersburg	Ontario	Canada DMR
27	1023033	VE3YES	Andrew James	Moss	Caledon	Ontario	Canada DMR
28	1023034	VE3KPB	Paul	Becker	Oshawa	Ontario	Canada DMR

It is easy to forget or not worry too much about whether you may be breaking the law owning and using an SDR – the laws are often different in each country or even in different jurisdictions within the same country and the likelihood of getting caught is fairly low.

Here are some general rules to abide by if in doubt however:

- Don't have a scanner in your car – not just actively working, but just physically in your car switched on or off, don't use your scanner to transmit.
- An obvious one but don't use your scanner to commit a crime
- Don't obtain material benefit from your scanning activities
- Don't use your scanner to decrypt communications
- Don't scan cellular frequencies
- Don't possess a scanner if you have been convicted of a crime in the last 5 years
- Look into whether you need to get a licence from your national communications regulatory body

In the UK the main law of interest is section 48 of the Wireless Telegraphy Act. This says there must be no intent to obtain or disclose information from any private message except where the information would have come to the person's knowledge via non-RF sources from others. So, the journalist who shows up at the site of a burning building to report on it, as a result of hearing a fire service emergency transmission via a scanner would be acting illegally.



You don't need a licence to use a scanner unless it is capable of transmission. In practice it is difficult to police anyone contravening these laws. Ofcom only investigated three offences under this section between 2016 and 2021 so that's an average of one every 18 months or so.

It is a plausible defence to say that certain frequencies were stumbled on by accident and the onus should be on the people transmitting confidential transmissions to encrypt or encode them.

In the USA, the law here varies considerably between the different states. In general though, the FCC and the Communications Act does not forbid the interception of 'overhearing your neighbour's conversation over a cordless telephone', or listening to emergency service reports, media broadcasts and transmissions by amateur radio operators.

Now this bit is interesting – it is legal to intercept communication that is readily accessible to the general public. This may be open to interpretation. Clearly a cordless phone conversation is not meant to be heard by the general public but they can be readily accessed by the public. Emergency service communications in the UK are encrypted by default, as opposed to in the United States where most are unencrypted by default. Some police forces there have made the deliberate decision to leave their transmissions unencrypted to enable different police forces and emergency services in other jurisdictions to be able to communicate with them effectively and to also provide a level of accountability to the general public who may be listening to their communications.

In the USA, it is illegal to manufacture, import, sell or lease equipment that can intercept or disrupt the cellular service.

To conclude, it is hoped that this report has highlighted the benefits and principal methods of obtaining and using radio wave OSINT data for security and other assessments.