Radio Wave Open Source Intel using SDR

- **Presented by Abi Waddell**
  March 2022

Introduction

- **Obtaining the raw data**
- **Decoding transmissions**
- **OSINT from publicly available sources and data leaks**
- **The law**

But why focus on OSINT?

- **Reduce the risk of fruitful pre-attack reconnaissance activity**
- **Probability that intel from public sources will be discovered and exploited is high. Often does not require a high level of skill**
- **Breach recon activities are not usually captured by existing tools and methods**
- **Open source leaks can largely be remedied with little effort but with a large impact on the reduction of risk**
- **Improved visibility of the wider attack surface**

Scanner Equipment

Traditional

- Expensive
- Limited functions – but do it well
- Less user input
- Lack of customisation
- May not have signal patterns displayed

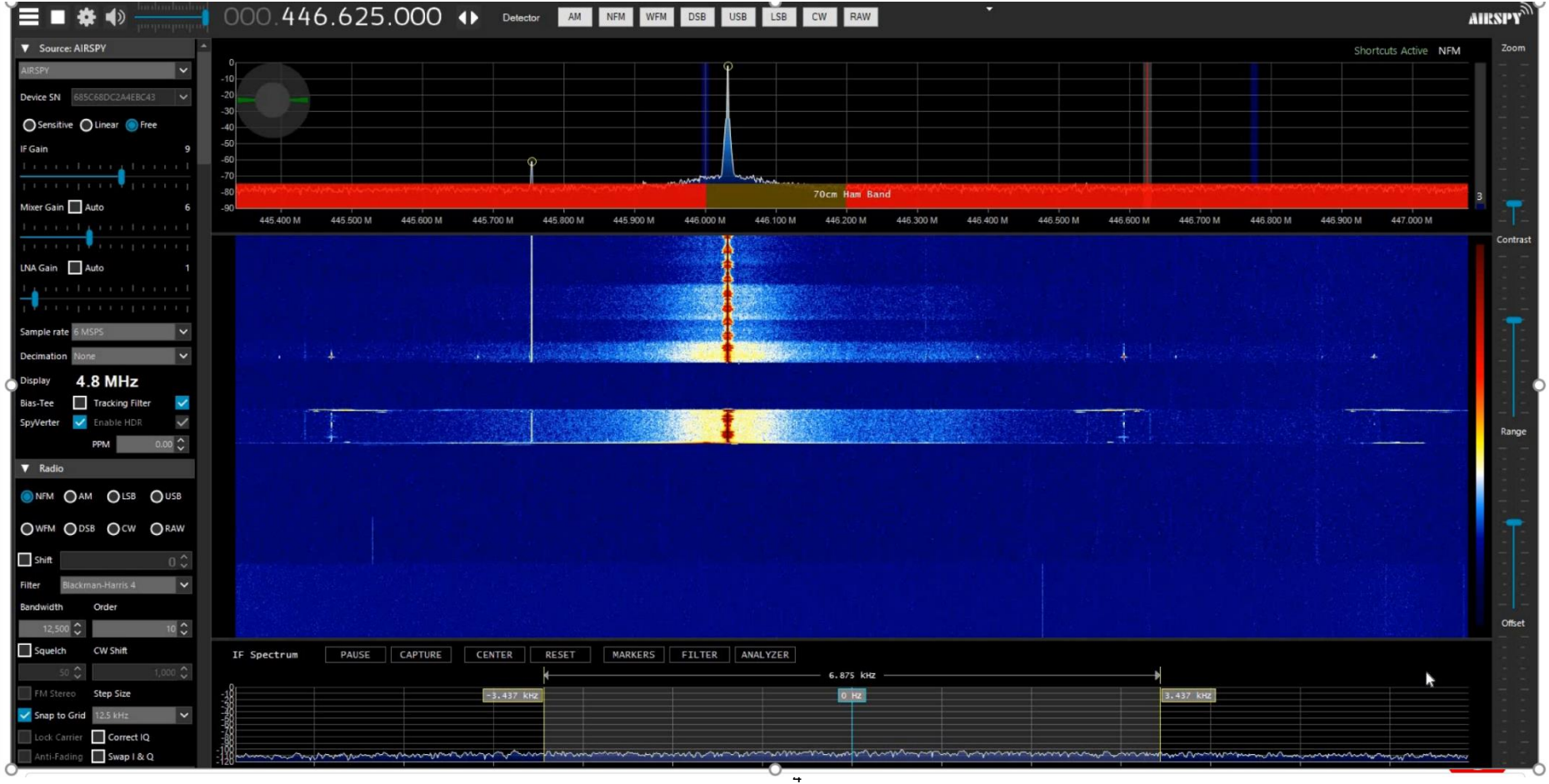
`Hobbyist’

- Plug & play
- Runs on Android, Windows, Linux, RaspPi, Mac
- 24 – 1700 MHz native RX range
- Cost between £30-£250

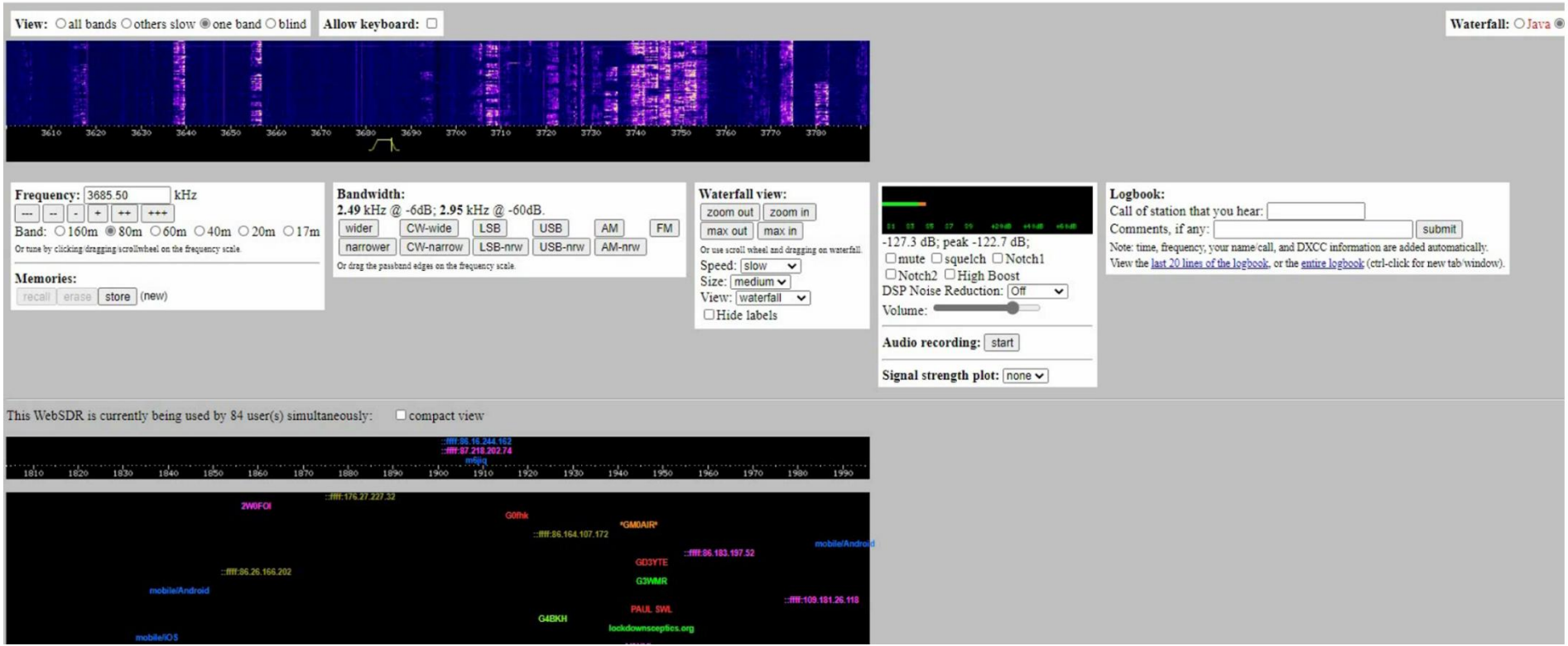
Mobile scanner antenna

- Frequency RX: 25-2000 MHz
- Length: 650mm
- Connection: BNC male

SDR Sharp – Basic Features



WebSDR


View: all bands others slow one band blind
Allow keyboard:
Waterfall: Java
3610 3620 3630 3640 3650 3660 3670 3680 3690 3700 3710 3720 3730 3740 3750 3760 3770 3780
Frequency: 3685.50 kHz
--- -- - + ++ +++
Band: 160m 80m 60m 40m 20m 17m
Or tune by clicking/dragging/scrollwheel on the frequency scale.
Memories:
recall erase store (new)
Bandwidth:
2.49 kHz @ -6dB; 2.95 kHz @ -60dB.
wider CW-wide LSB USB AM FM
narrower CW-narrow LSB-nrw USB-nrw AM-nrw
Or drag the passband edges on the frequency scale.
Waterfall view:
zoom out zoom in
max out max in
Or use scroll wheel and dragging on waterfall.
Speed: slow
Size: medium
View: waterfall
Hide labels
-127.3 dB; peak -122.7 dB;
mute squelch Notch1
Notch2 High Boost
DSP Noise Reduction: Off
Volume:
Audio recording: start
Signal strength plot: none
Logbook:
Call of station that you hear:
Comments, if any: submit
Note: time, frequency, your name/call, and DXCC information are added automatically.
View the last 20 lines of the logbook, or the entire logbook (ctrl-click for new tab/window).
This WebSDR is currently being used by 84 user(s) simultaneously:
compact view
1810 1820 1830 1840 1850 1860 1870 1880 1890 1900 1910 1920 1930 1940 1950 1960 1970 1980 1990
::ffff:86.16.244.162
::ffff:87.218.202.74
m6jrj
::ffff:176.27.227.32
2W0FOI
G0fhk
GM0AIR
::ffff:86.164.107.172
mobile/Android
::ffff:86.183.197.52
GD3YTE
::ffff:86.26.166.202
G3WMR
mobile/Android
::ffff:109.181.26.118
PAUL SWL
G4BKH
lockdownsceptics.org
mobile/iOS

Police messages over WebSDR

Frequently mention sensitive data such as names/criminal records/addresses/call signs/car licence plate numbers etc but…
*Note – personal/ sensitive info has been removed from this audio clip

Hams discussing buying guns & ammo

Radiolocation

Trilateration

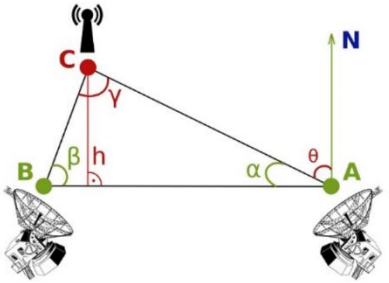
Each receiving station measures the length of time taken for the radio signal to reach their position, and when the times from three or more receiving stations are known, a position for the receiver can be calculated. Each receiving station is equipped with an omnidirectional antenna. Need multiple fixed receiving stations, and each station must be equipped with a very precise clock.

Multilateration

TDOA

Triangulation

Can be used with multiple fixed-position receiving stations, or with a single mobile receiving station. The station is equipped with a directional antenna and determines the angle which the signal is received from. When this angle is taken from three or more different locations, the location of the transmitter can be calculated. A single receiving station can be placed at each location in turn, and takes a bearing to the signal.



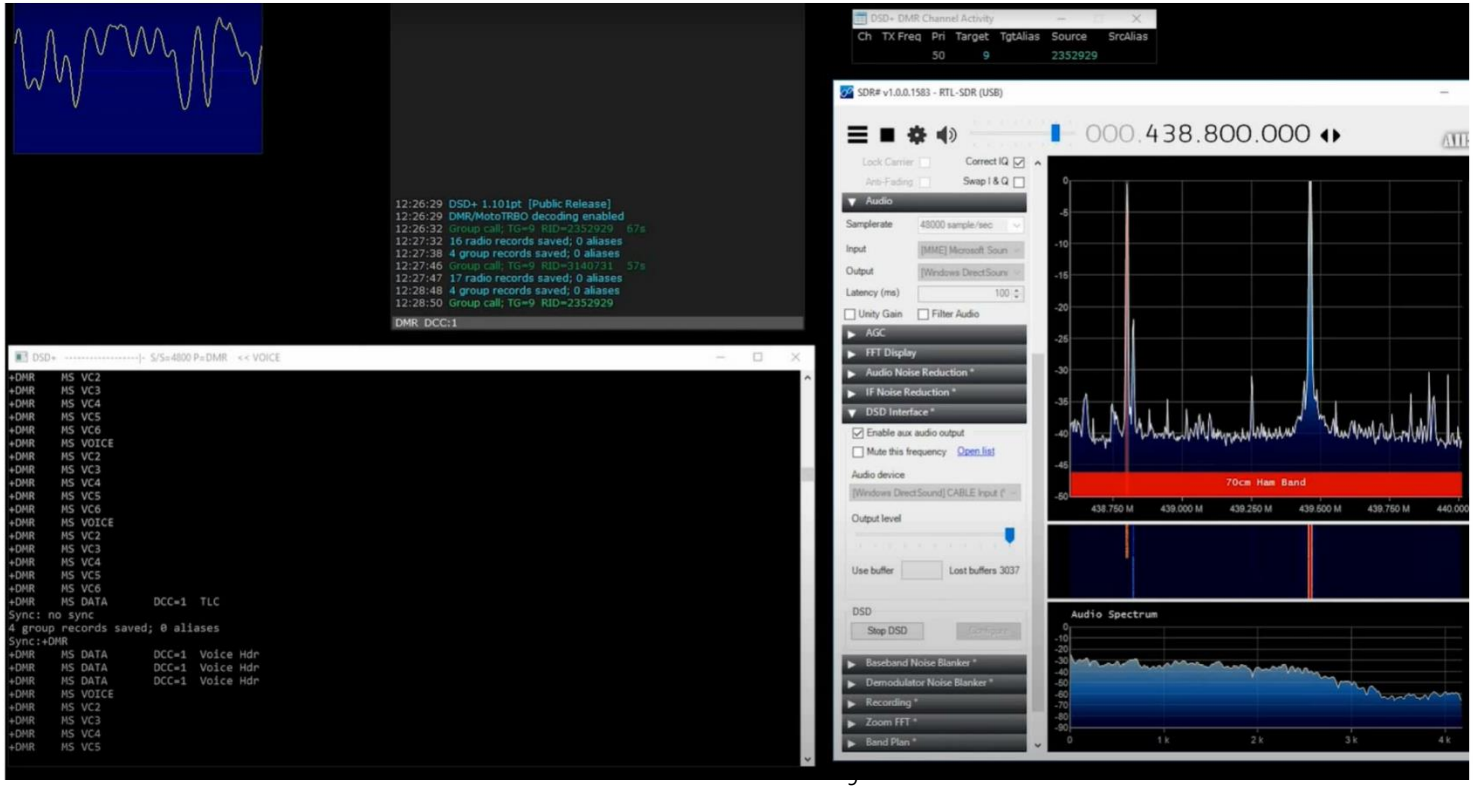
Direction Finding Systems

Doppler shift

Correlative interferometry

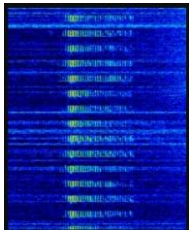
Decoding digital radio

Decoding process: capture raw encoded or encrypted data using SDR then decode using software on the fly OR capture raw data to a file (e.g pcap) for offline analysis including decryption



What can we listen to?

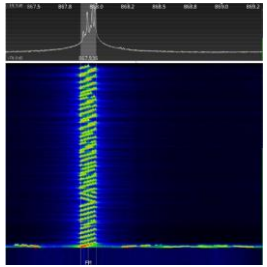
Illegal Fishing Buoys
Transmitting in the 28Mhz band – sometimes emit their ID in morse code



Numbers Stations
Shortwave radio stations that transmit encrypted messages in the form of numbers. The numbers are sent on pre-determined frequencies with the use of automated voice, Morse code, or even digital modes. Majority of numbers stations use a one-time pad encryption.
Each station is usually given a nickname depending on what is included in the broadcast. Many number stations are well known because of the music that they play.

Search for Extraterrestrial Intelligence (SETI)
Ongoing project that 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. Requirements are a dish 2.1 meters or larger, a motorized mount, and a feed, LNA and radio system able to receive 1 - 4.5 GHz. The collected audio is analysed using special software.

IoT Devices
For example: weather stations, doorbells, remotes, car tyre pressure readers. Europe: 433 MHz and 868 MHz; Australia and North America: 915 MHz; Asia: 923MHz.
LoRA (Long Range) is LPWAN (Low-Power Wide-Area Network) technology:
•2-3 Km wide coverage outdoor in urban areas;
•5-7 Km in rural areas;
•Can be up to 700 Km.



What can we listen to? (cont.)

DECT Cordless Phones
Use 1880 - 1900 MHz, and in the USA at 1920 - 1930 MHz. Can be unencrypted and usually has weak encryption if encryption is used.

Iridium/Inmarsat Satellites
Provides various services such as satellite phones, services for emergency operations too. Transmissions can be decoded.

Wireless Keyboards
Transmits radio frequency packets from the keyboard to a USB dongle plugged into a user's computer.

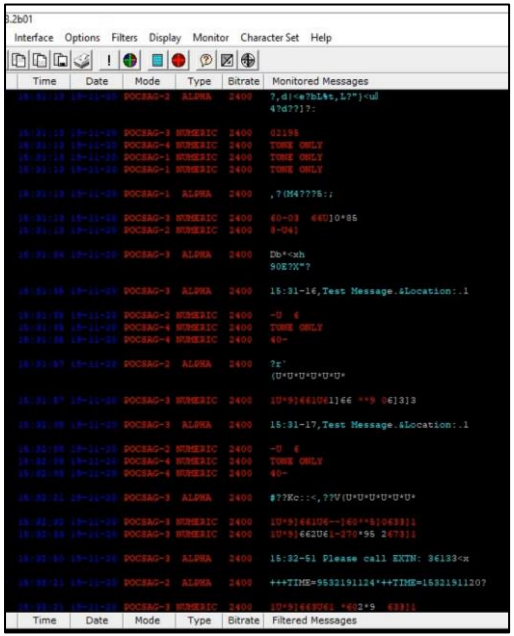
Military Radio Bands
Transmissions can be sent unencrypted particularly if commercial handsets are in use. Recently a set of bands for a particular country's alleged military were publicised on Twitter.

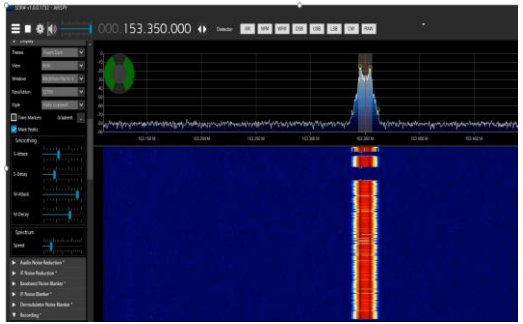
Fake 4G Base Station Detection
4G pre-authentication and downgrade vulnerabilities make this possible

WiFi Adapter Fingerprinting
Experiments in this area have shown 95% accuracy rate

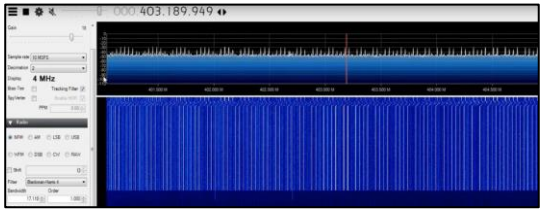
What can we listen to? (cont.)

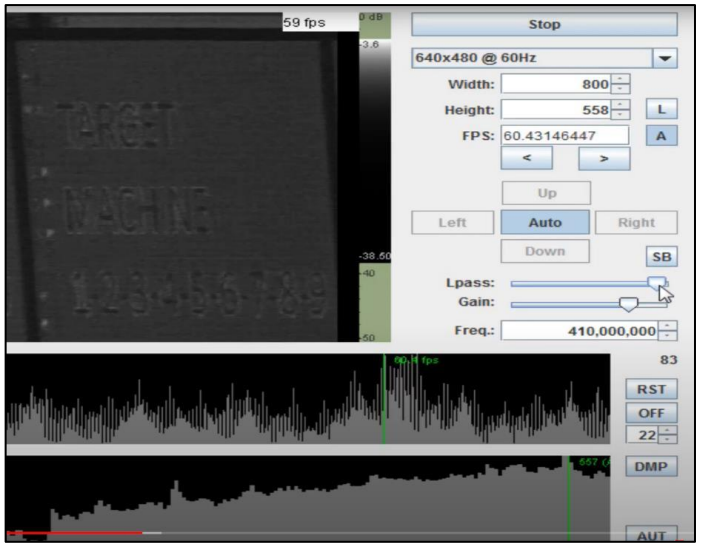
Pager interception





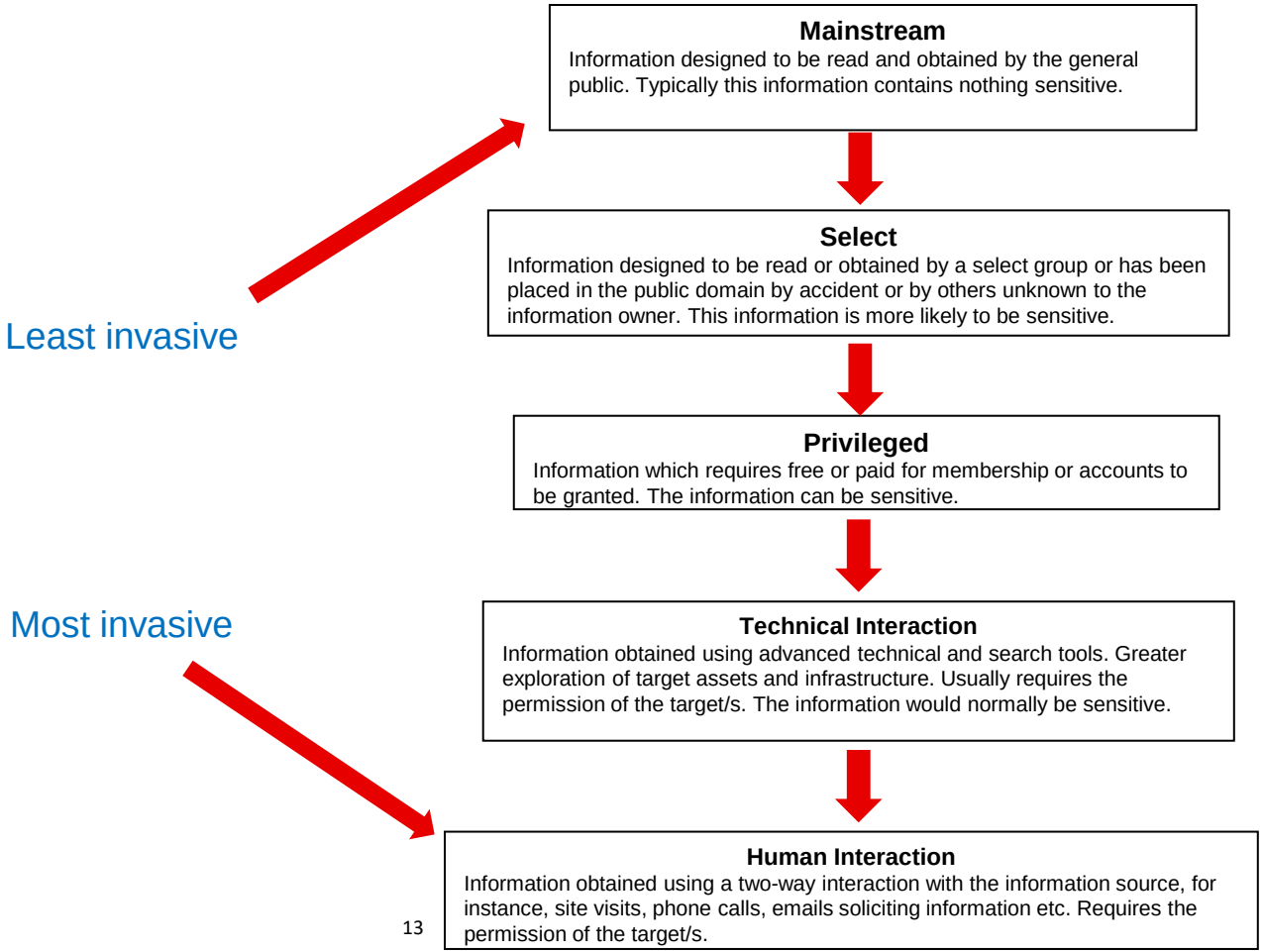
Capturing Monitor Emanations





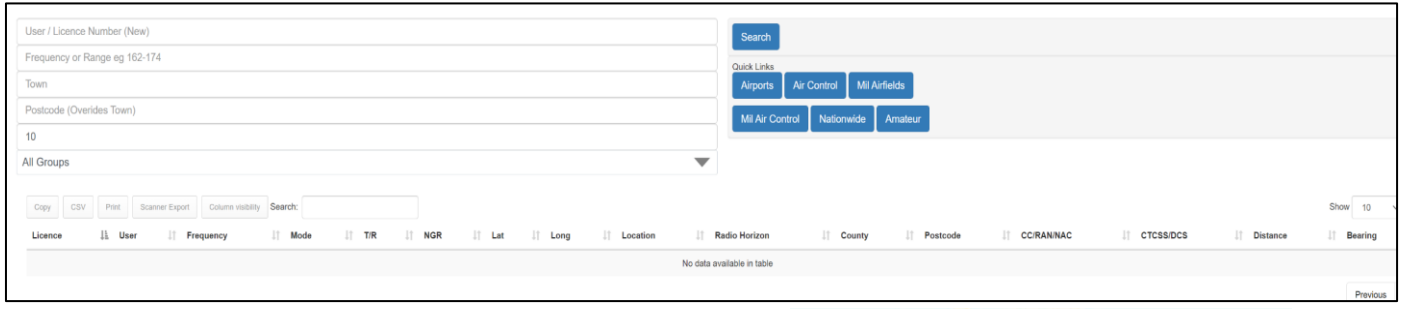
OSINT data retrieval model

OSINT gathering can be put into different categories according to the type of data repository, permission and sensitivity levels.



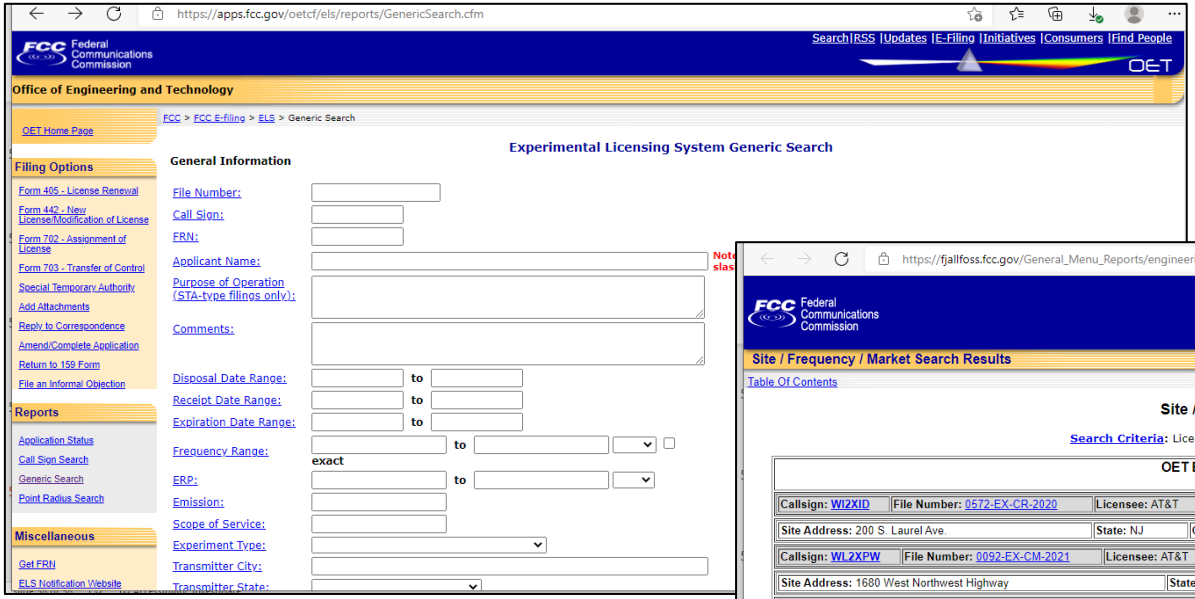
Search organisations' frequencies and transmitter locations

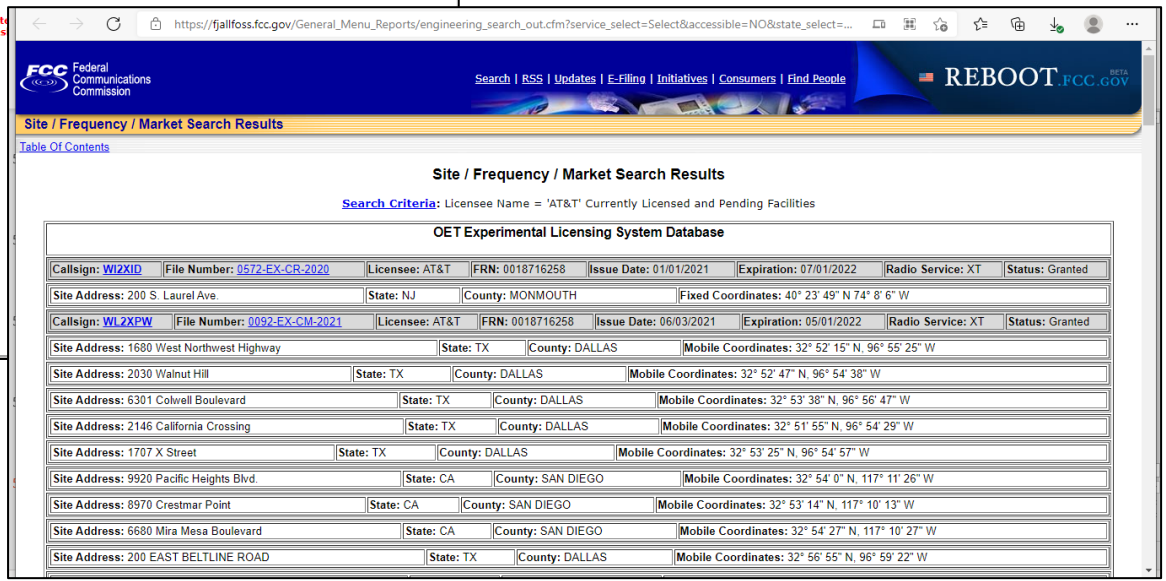
- radioreferenceuk.co.uk
- https://www.ofcom.org.uk /spectrum/information/spectrum-information-system-sis



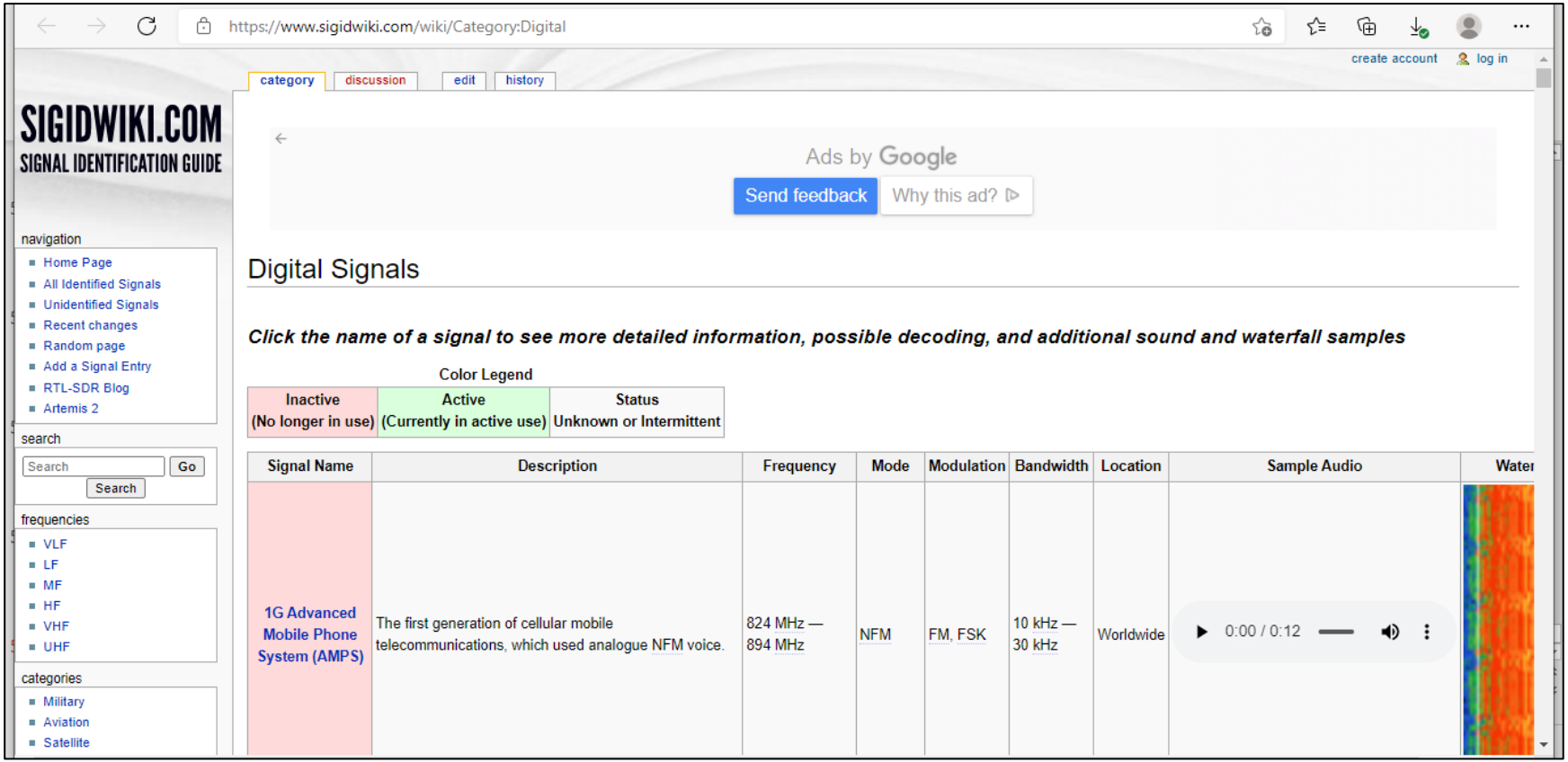
US FCC database

Shows call sign, frequencies in use, site addresses of licensees etc



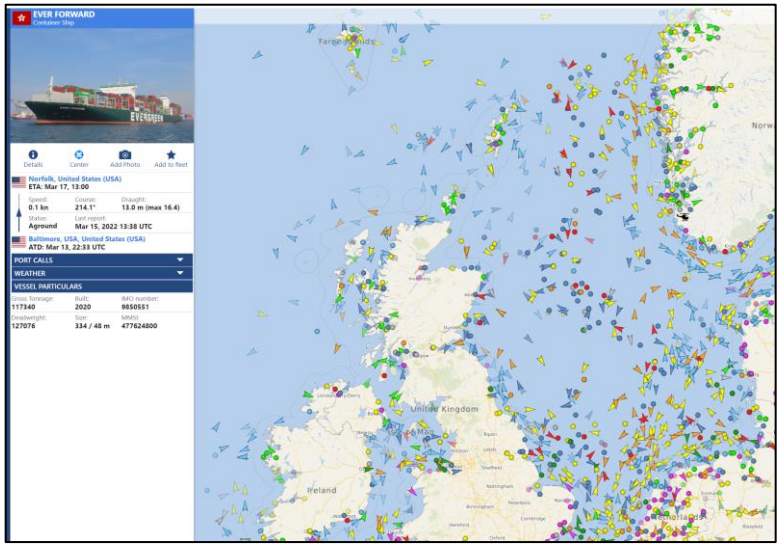


Signal Identification Guide

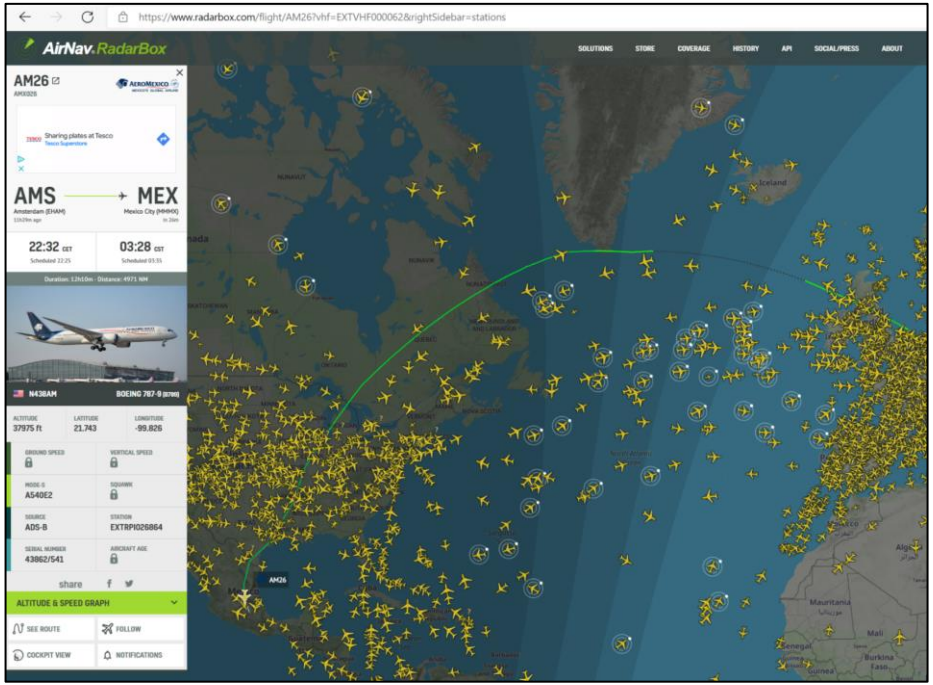


Transport Radar and WSPR

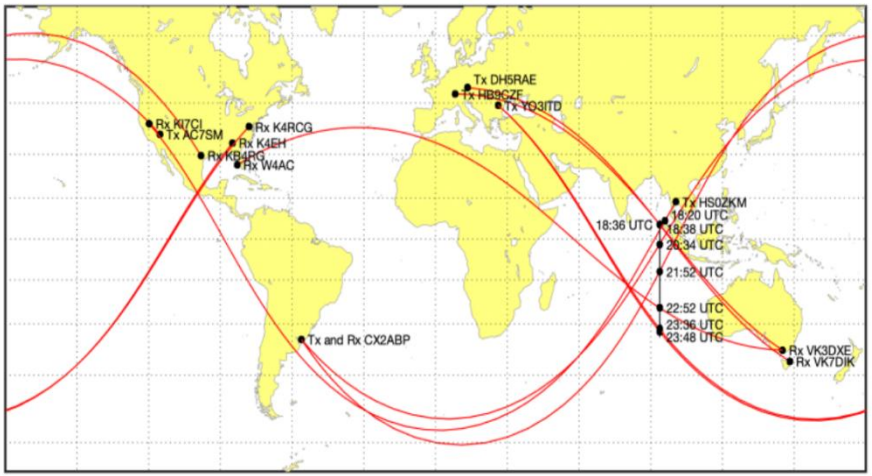
Marine Radar



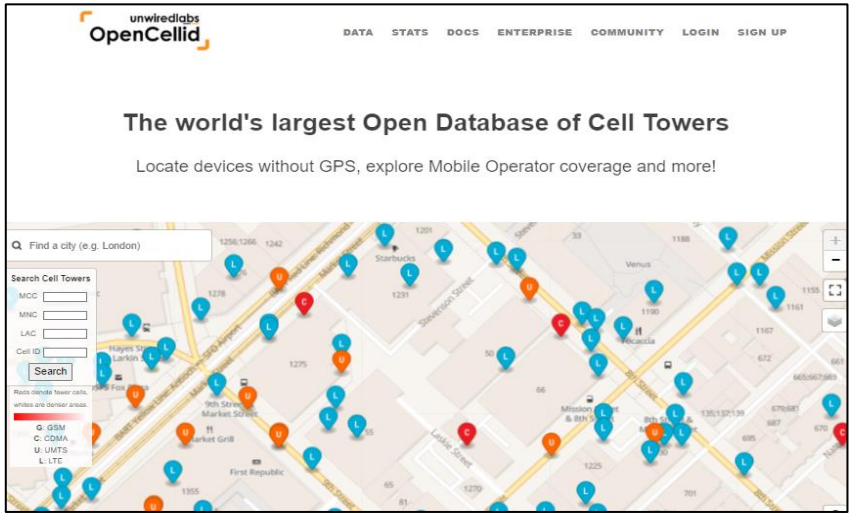
Flight Radar



WSPR



Maps of cryptocurrency miners and cell towers

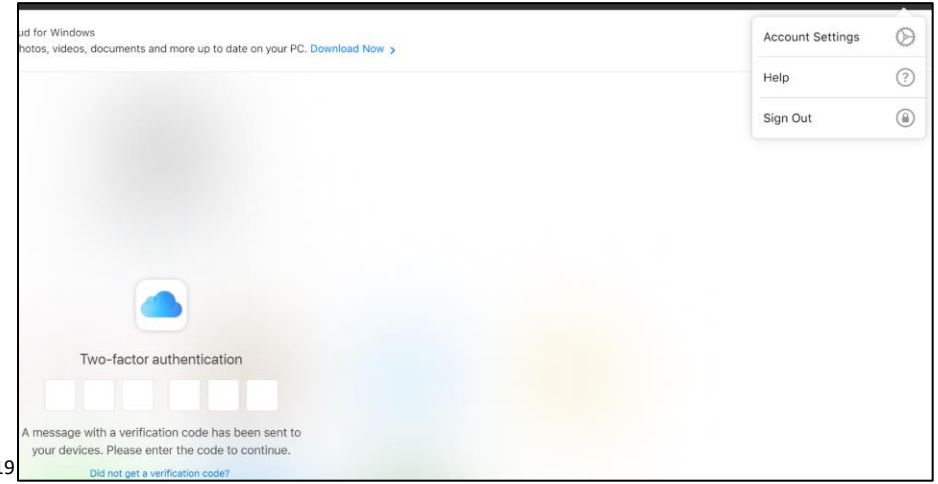


`Find my phone' iPhone verification bypass

Sign in to iCloud with target's name & password

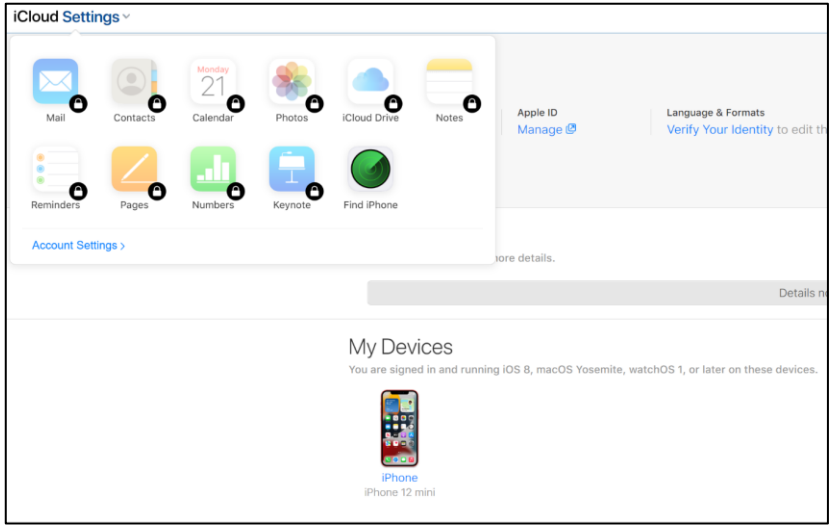
The verification 2FA is triggered

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

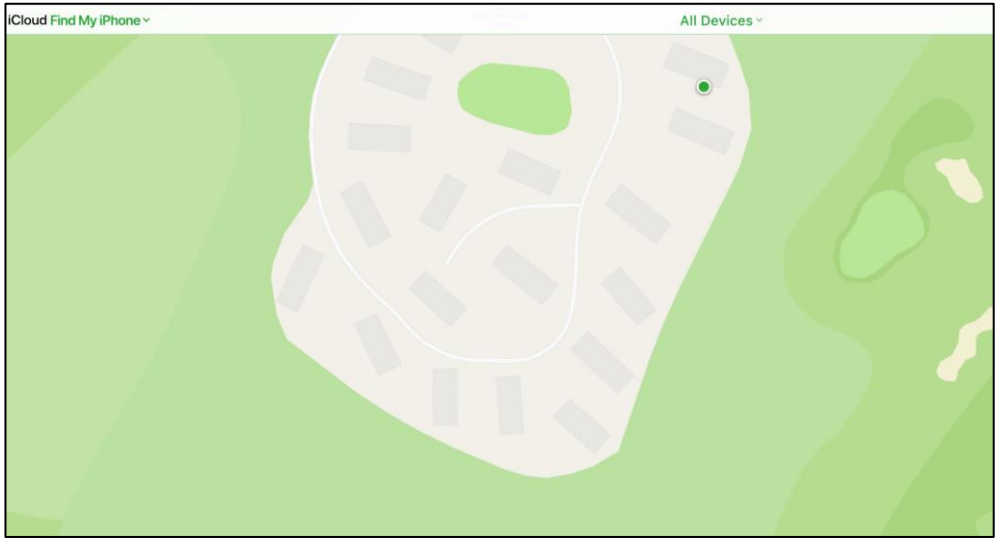


`Find my phone' iPhone verification bypass (cont.)

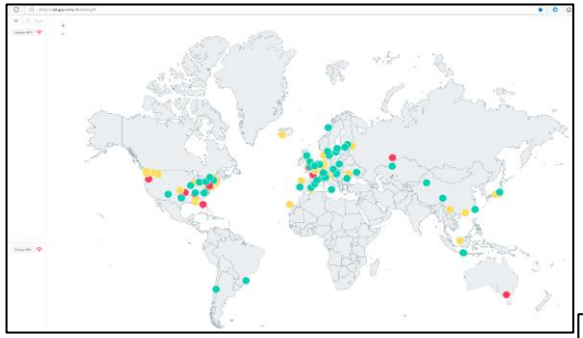
Device type can be seen. Click on `Find iPhone'



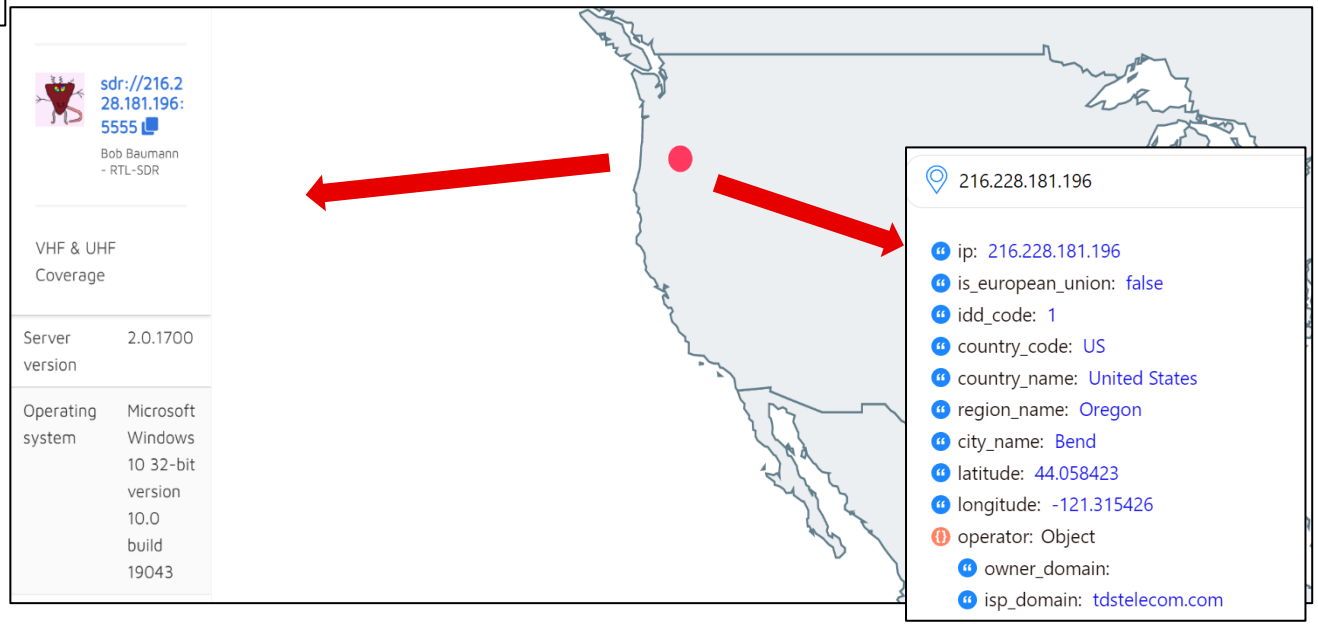
Location of device can be seen and further RF exploration can take place



Airspy SDR server map

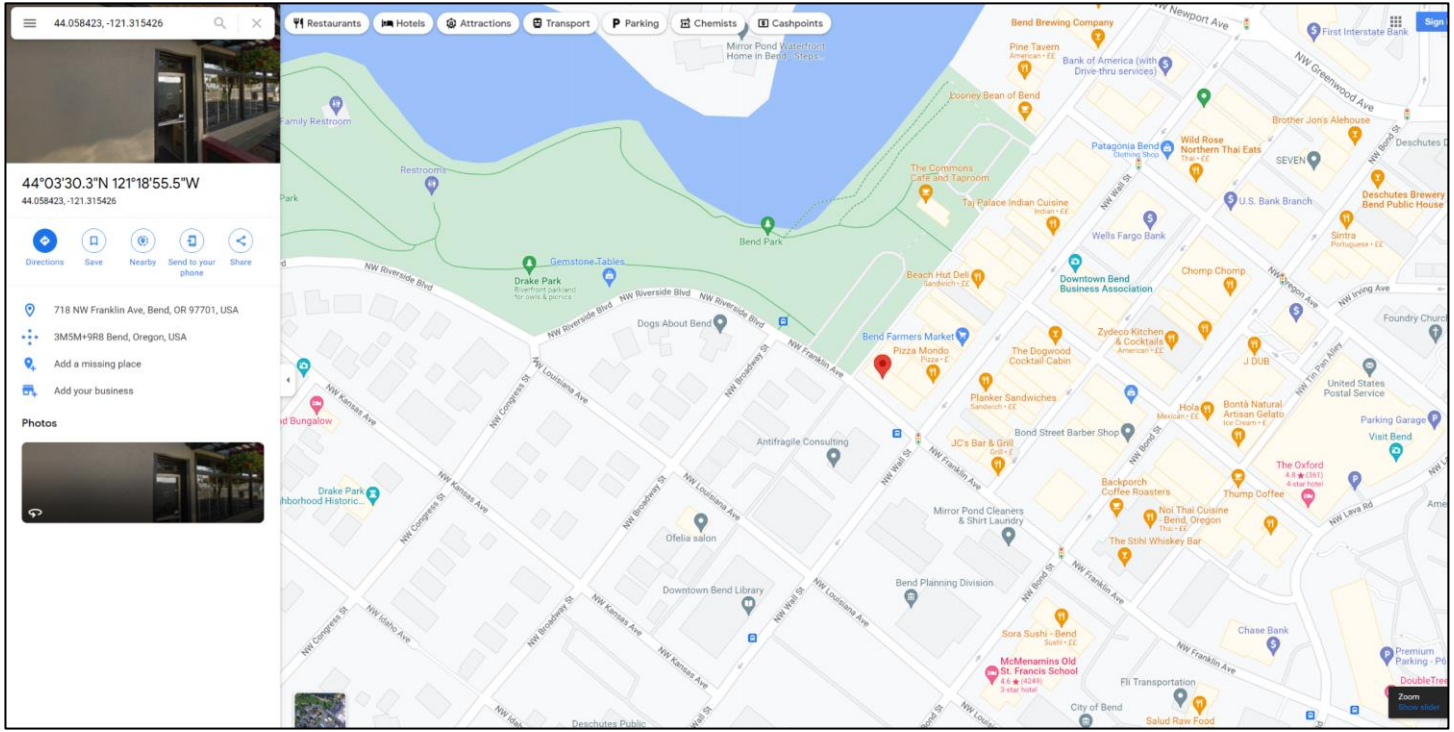


Reveals IP address, coordinates and sometimes OS and user details



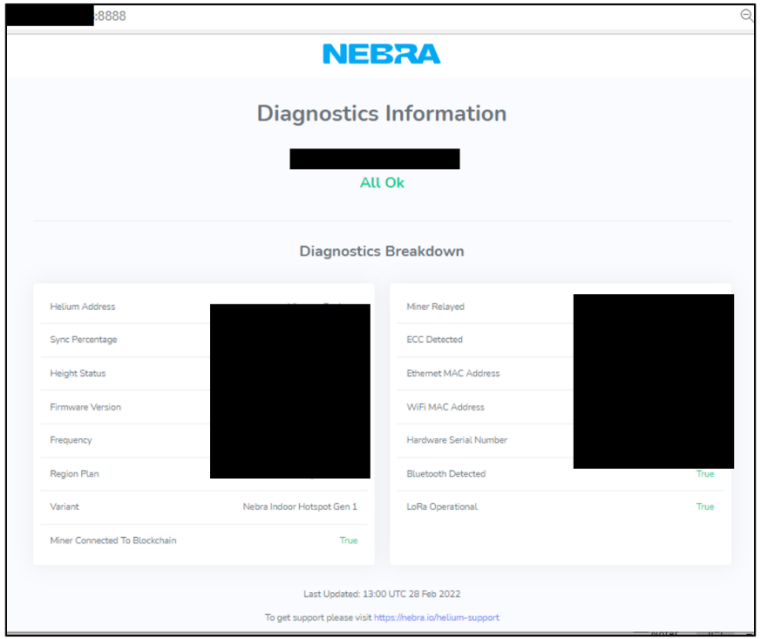
Location of SDR servers

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

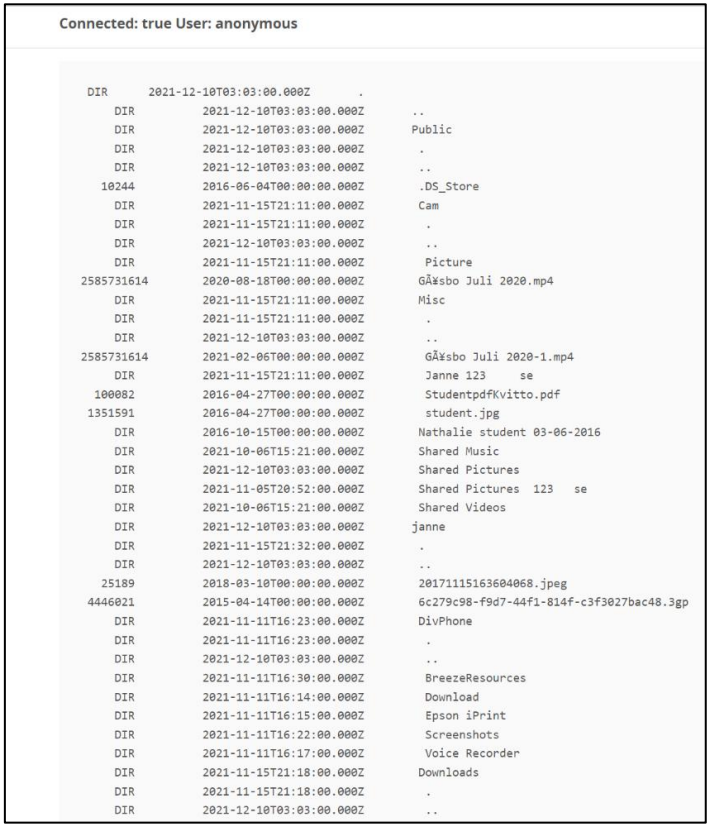


Accessible IoT ports and anonymous access to data

Nebra IoT device data over port 8888

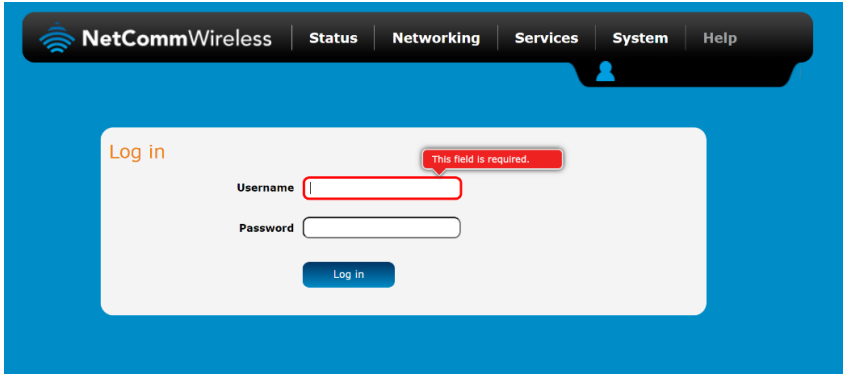


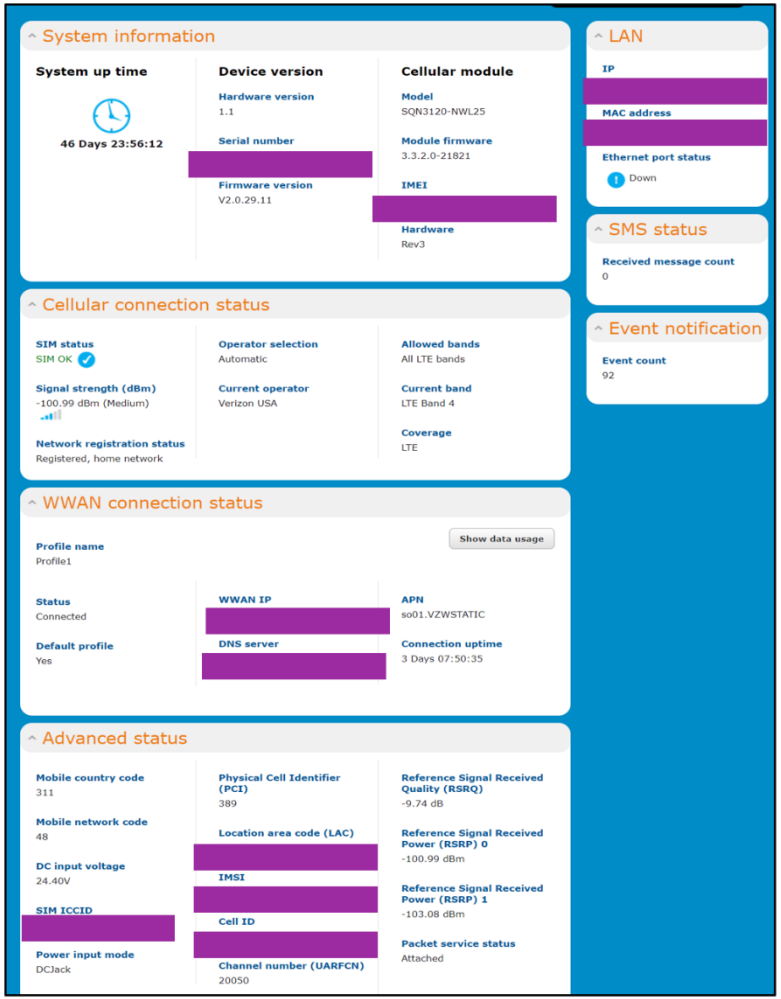
Samsung DVR files accessible over anonymous login on port 21



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

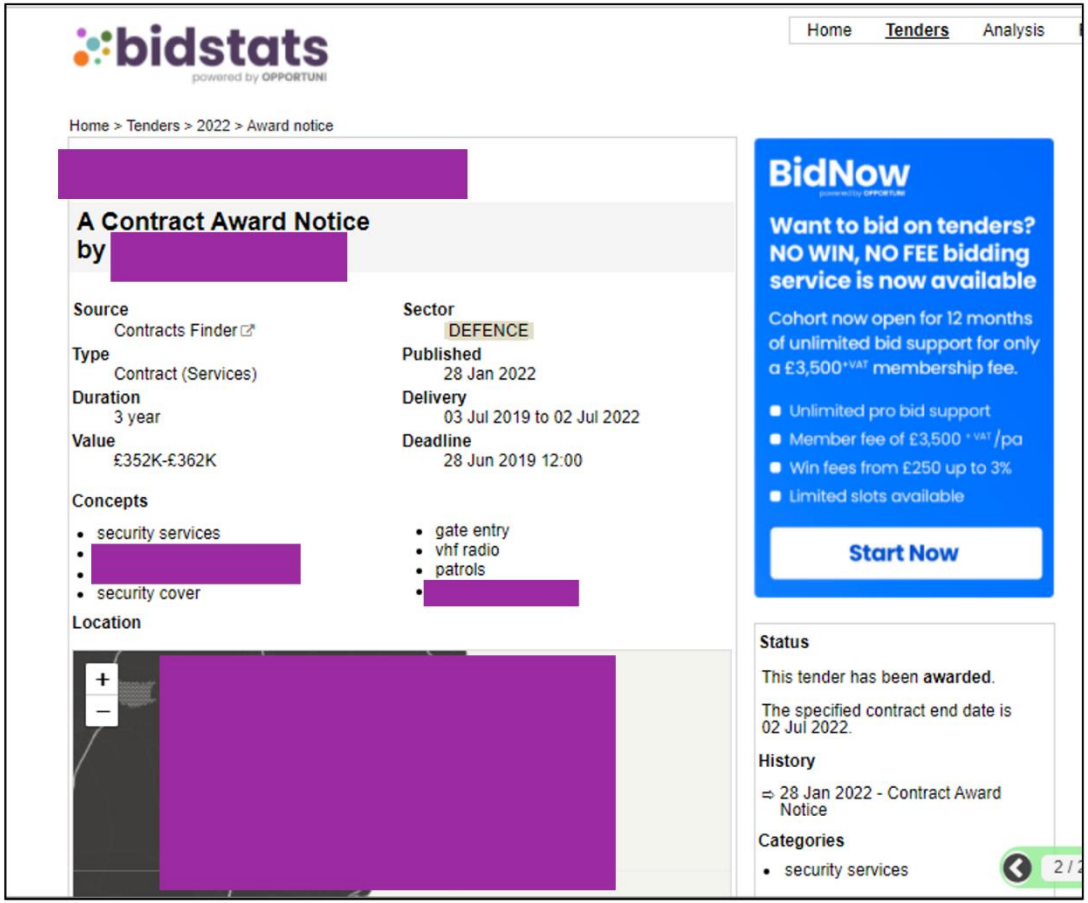




Data on radio suppliers

If the target radio model is known then there is a greater likelihood of finding frequency and type of transmission used.

Tender/contracts' sites reveal radio/security companies and suppliers. The redacted contract award here shows the supplier



Data on radio suppliers (cont.)

Spreadsheet on public spending and website showing site stats/visitors. Web stats searches and backlinks/referrer apps may show possible suppliers.

www.[redacted]/webalizer/usage_201408.html

9	19	0.06%	18	0.07%	2720	0.35%	0	0.00%	101.85.202.3
10	121	0.39%	92	0.37%	2400	0.31%	2	0.05%	82.178.136.8

Top 30 of 1016 Total Referrers

#	Hits		Referrer
1	7964	25.37%	- (Direct Request)
2	114	0.36%	https://www.google.com/
3	73	0.23%	http://cellphone-spy-on-wife.soup.io/
4	71	0.23%	http://www.google.com/url
5	48	0.15%	https://www.google.co.in/
6	47	0.15%	http://162.215.248.63/
7	44	0.14%	http://www.baidu.com/s
8	31	0.10%	http://www.google.co.in/url
9	17	0.05%	http://www.google.ae/url
10	16	0.05%	http://ngolobal.wordpress.com/2012/11/14/download-official-redhat-linux-iso-image/
11	16	0.05%	http://www.bing.com/images/search
12	15	0.05%	https://www.google.ae/
13	14	0.04%	http://android-call-spy-full-apk.soup.io/
14	13	0.04%	http://www.baidu.com/search/spider.htm
15	13	0.04%	http://www.google.com.om/url
16	12	0.04%	http://best-android-spy-apps-2014.soup.io/
17	12	0.04%	http://best-spy-tracking-app-for-android.soup.io/
18	12	0.04%	http://kino.moukrest.ru
19	12	0.04%	http://nglobalinc.blogspot.com/2012/10/pc-tools-registry-mechanic-v1101716.html
20	11	0.04%	http://best-catch-a-cheater-android-spyware.soup.io/
21	11	0.04%	http://hotel.qunar.com/
22	11	0.04%	http://semalt.semalt.com/crawler.php
23	10	0.03%	http://android-mobile-spy-apps-download-apk.soup.io/
24	10	0.03%	http://ngolobal.wordpress.com/2012/10/03/free-mp3-download-of-maithili-song/
25	9	0.03%	http://best-android-spy-security-app.soup.io/
26	9	0.03%	http://best-pof-spy-apps-on-android.soup.io/
27	9	0.03%	http://best-rated-sms-spy-for-android.soup.io/
28	9	0.03%	http://cell-phone-spy-for-android-2015.soup.io/
29	9	0.03%	http://spy-on-android-to-iphone.soup.io/
30	9	0.03%	http://top-spying-software-for-android-2014.soup.io/

58	[redacted]	824.36	785.2	œ39.16	œ824.36	[redacted]
59		5170.66	4308.92	œ861.74	œ5,170.66	
60		719.48	685.32	œ34.16	œ719.48	
61		3896.07	3246.74	œ649.33	œ3,896.07	
62		204.35	194.63	œ9.72	œ204.35	
63		1855.37	1546.15	œ309.22	œ1,855.37	
64		113.73	108.33	œ5.40	œ113.73	
65		-688.48	-573.73	#NAME?	#NAME?	
66		32.71	31.16	œ1.55	œ32.71	
67		2545.81	2121.52	œ424.29	œ2,545.81	
68		414.82	345.69	œ69.13	œ414.82	
69		32.69	31.15	œ1.54	œ32.69	
70		694.53	578.78	œ115.75	œ694.53	
71		647.88	617.06	œ30.82	œ647.88	
72		2930.18	2441.82	œ488.36	œ2,930.18	
73		773.5	736.74	œ36.76	œ773.50	
74		2062.74	1718.97	œ343.77	œ2,062.74	
75		54600	45500	œ9,100.0(	œ54,600.(	
76		54600	45500	œ9,100.0(	œ54,600.(	
77	[redacted] ENGLAI Facilities ######## [redacted] Security	28340.62	23617.18	œ4,723.44	œ28,340.€	SECURITY P274495 SECURITY AND STEWARDING FOR [redacted]

Corporate manned building security

Site A

Analogue two-way radios used 24hrs a day, 7 days a week. Easily scanned and listened to.

Site B

Digital and analogue two-way radios used 24hrs a day, 7 days a week. Open source search shows high probability that Hytera radios are used. Thus likely to use frequencies 400-440MHz and 430-470MHz with DMR.

Try different search terms to find better images, potentially showing device makes

Blurry

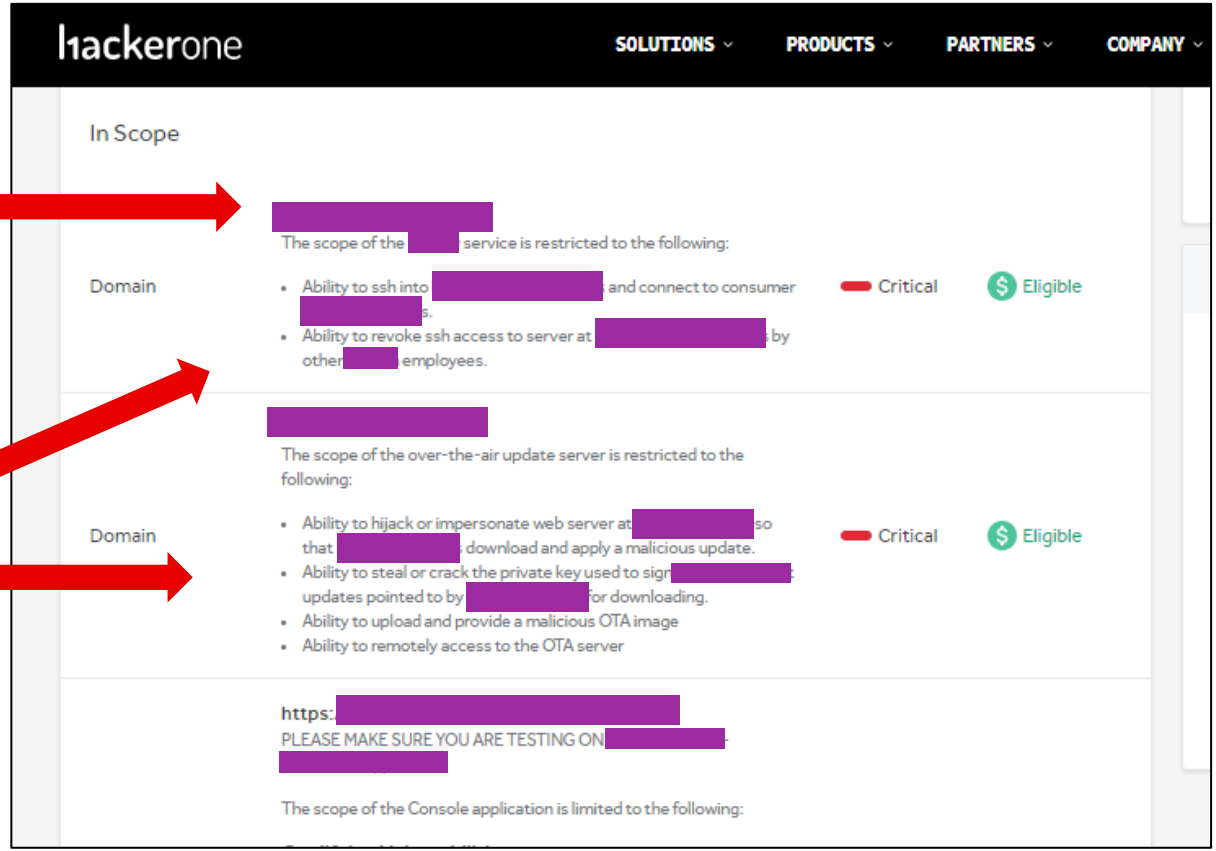
Same photo but different sources

Sharp

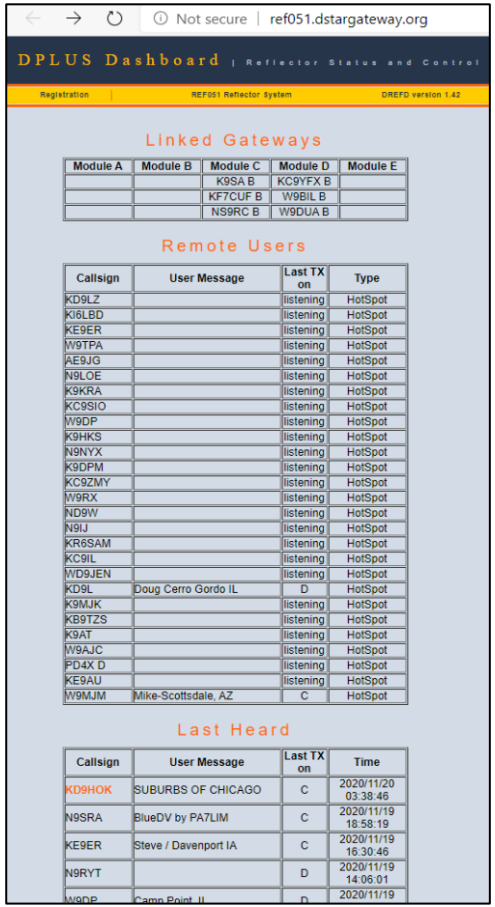
Bug Bounty Sites – leak data and vulnerabilities

This site address is not publicly advertised

Potential security vulnerabilities as noted by the site owners



Radio user and equipment OSINT



Not secure | ref051.dstargateway.org

DPLUS Dashboard | Reflector Status and Control

Registration | REF051 Reflector System | DREFD version 1.42

Linked Gateways

Module A	Module B	Module C	Module D	Module E
		K9SA B	KC9YFX B	
		KF7CUF B	W9BIL B	
		NS9RC B	W9DUA B	

Remote Users

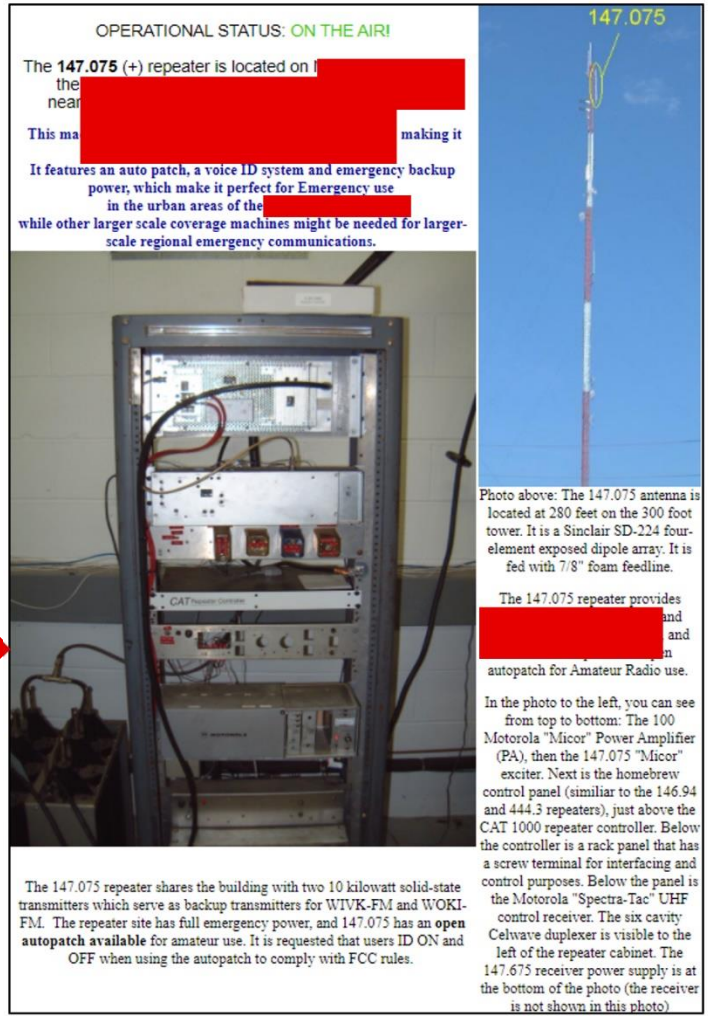
Callsign	User Message	Last TX on	Type
KD9LZ		listening	HotSpot
Ki6LBD		listening	HotSpot
KE9ER		listening	HotSpot
W9TPA		listening	HotSpot
AE9JG		listening	HotSpot
N9LOE		listening	HotSpot
K9KRA		listening	HotSpot
KC9SIO		listening	HotSpot
W9DP		listening	HotSpot
K9HKS		listening	HotSpot
N9NYX		listening	HotSpot
K9DPM		listening	HotSpot
KC9ZMY		listening	HotSpot
W9RX		listening	HotSpot
ND9W		listening	HotSpot
N9IJ		listening	HotSpot
KR6SAM		listening	HotSpot
KC9IL		listening	HotSpot
WD9JEN		listening	HotSpot
KD9L	Doug Cerro Gordo IL	D	HotSpot
K9MJK		listening	HotSpot
KB9TZS		listening	HotSpot
K9AT		listening	HotSpot
W9AJC		listening	HotSpot
PD4X D		listening	HotSpot
KE9AU		listening	HotSpot
W9MJM	Mike-Scottsdale, AZ	C	HotSpot

Last Heard

Callsign	User Message	Last TX on	Time
KD9HOK	SUBURBS OF CHICAGO	C	2020/11/20 03:38:46
N9SRA	BlueDV by PA7LIM	C	2020/11/19 18:58:19
KE9ER	Steve / Davenport IA	C	2020/11/19 16:30:46
N9RYT		D	2020/11/19 14:06:01
W9DP	Camp Point, IL	D	2020/11/19

D-Star radio gateway/users database

Active radio hardware technical details often available



OPERATIONAL STATUS: ON THE AIR!

The **147.075** (+) repeater is located on [redacted]

This ma[redacted] making it

It features an auto patch, a voice ID system and emergency backup power, which make it perfect for Emergency use in the urban areas of the [redacted] while other larger scale coverage machines might be needed for larger-scale regional emergency communications.

147.075

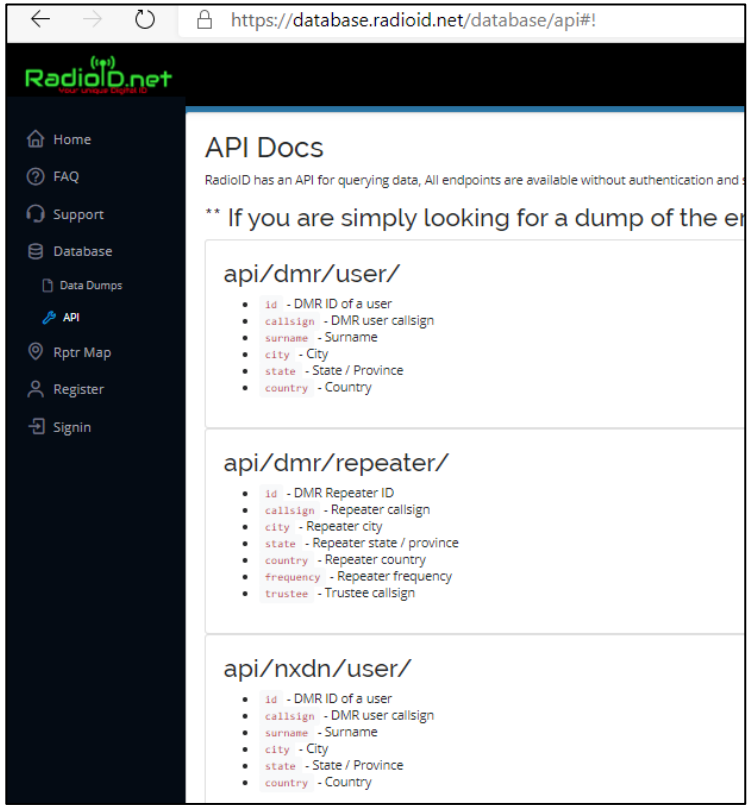
Photo above: The 147.075 antenna is located at 280 feet on the 300 foot tower. It is a Sinclair SD-224 four-element exposed dipole array. It is fed with 7/8" foam feedline.

The 147.075 repeater provides [redacted] and autopatch for Amateur Radio use.

The 147.075 repeater shares the building with two 10 kilowatt solid-state transmitters which serve as backup transmitters for WIVK-FM and WOKI-FM. The repeater site has full emergency power, and 147.075 has an **open autopatch available** for amateur use. It is requested that users ID ON and OFF when using the autopatch to comply with FCC rules.

In the photo to the left, you can see from top to bottom: The 100 Motorola "Micor" Power Amplifier (PA), then the 147.075 "Micor" exciter. Next is the homebrew control panel (similiar to the 146.94 and 444.3 repeaters), just above the CAT 1000 repeater controller. Below the controller is a rack panel that has a screw terminal for interfacing and control purposes. Below the panel is the Motorola "Spectra-Tac" UHF control receiver. The six cavity Celwave duplexer is visible to the left of the repeater cabinet. The 147.675 receiver power supply is at the bottom of the photo (the receiver is not shown in this photo).

D-Star DMR/NXDN OSINT



DMR/NXDN users and repeater details

	RADIO_ID	CALLSIGN	FIRST_NAME	LAST_NAM	CITY	STATE	COUNTRY	REMARKS
2	1023001	VE3THW	Wayne	Edward	Toronto	Ontario	Canada	DMR
3	1023002	VA3ECM	Mathieu	Goulet	Ottawa Hull	Quebec	Canada	CCS7
4	1023003	VE3QC	Guy	Charron	Gloucester	Ontario	Canada	CCS7
5	1023006	VA3UZ	Allan Timothy	Harvey	Sparta	Ontario	Canada	DMR
6	1023007	VA3BOC	Hans Juergen	Bockholt	Cornwall	Ontario	Canada	
7	1023008	VE3JMR	Mark		Niagara Falls	Ontario	Canada	DMR
8	1023009	VA3AMO	Rolando	Parto	Scarborough	Ontario	Canada	DMR
9	1023010	VA3AMO	Rolando	Parto	Scarborough	Ontario	Canada	DMR
10	1023013	VE3SLD	Barry	Brousseau	Guelph	Ontario	Canada	DMR
11	1023014	VA3DB	Diane	Bruce	Nepean	Ontario	Canada	DMR
12	1023016	VE3IAO	John Christensen	Christense	Almonte	Ontario	Canada	DMR
13	1023017	VA3MSV	John	Visser	London	Ontario	Canada	DMR
14	1023018	VA3BTQ	Jacqualine May	Norman	Nestleton Station	Ontario	Canada	DMR
15	1023019	VA3BTQ	Jacqualine May	Norman	Nestleton Station	Ontario	Canada	DMR
16	1023020	VE3ZXN	Denis	Jakac	Bradford	Ontario	Canada	DMR
17	1023021	VE3ZXN	Denis	Jakac	Bradford	Ontario	Canada	DMR
18	1023023	VA3TDG	Doug	Baxter	Sudbury	Ontario	Canada	DMR
19	1023024	VA3MRJ	David S	Johnson	Kitchener	Ontario	Canada	DMR
20	1023025	VA3ZDX	Gregory K	Green	Ailsa Craig	Ontario	Canada	DMR
21	1023026	VE3ELX	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	VE3OZT	Alexander	Blais	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

The Legal Stuff

Every jurisdiction has different laws but in doubt:

- Don’t have the scanner in your car
- Don’t use your scanner to transmit
- Don’t use the scanner to facilitate a crime
- Don’t gain material benefit from any radio interception
- Don’t use the scanner to decrypt communications
- Don’t scan cellular and aviation frequencies
- Don’t make public private communications
- Don’t possess a scanner if you have been convicted of a crime in the last 5 years
- Get a licence from your national communications regulatory body

UK Law

Section 48 of the Wireless Telegraphy Act 2006

- Must be ***no intent to obtain information*** as to the contents, sender or addressee of any message whether sent by means of wireless telegraphy or not, of which neither the person using the apparatus nor a person on whose behalf he is acting is an intended recipient.
- Must not disclose any information as to the contents, sender or addressee of any message
- It does not apply where the information would have come to the person's knowledge without the use of wireless telegraphy apparatus by the person or by anyone else
- The use of radio receivers is exempt from requiring a licence unless it is also capable of transmission.
- Ofcom only investigated 3 offences under this section between 2016 and 2021

US law

Varies considerably between jurisdictions

FCC and the Communications Act does not forbid:

- Interception of `overhearing your neighbor's conversation over a cordless telephone', or listening to emergency service reports, such as over-the-air radio and television broadcasts, broadcasts related to ships, aircraft, vehicles or persons in distress, transmissions by amateur radio or citizen band radio operators.
- Intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is ***readily accessible to the general public***

But FCC cannot authorize radio scanning equipment that:

- Can receive transmissions in the frequencies allocated to domestic cellular services.
- Can readily be altered by the user to intercept cellular communications.
- May be modified to convert digital transmissions to analog voice audio.

It is illegal to manufacture, import, sell or lease such unauthorized equipment in the United States.

Thanks!