# 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: O all bands O others slow () one band O blind	Allow keyboard: 🗆			Waterfall: OJava @
3610 3620 3630 3640 3659 3660 367	0 3650 3650 3710 3710 3750 3760 376	27 27 28 29 20 20 20 20 20 20 20 20 20 20 20 20 20		
Frequency:       3685.50       kHz              Band:       160m          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-nnw USB-nnw AM-nnw Or drag the passband edges on the frequency scale.	Waterfall view: [zoom out] [zoom in max out] [max in] Or use screll 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:
This WebSDR is currently being used by 84 user(s) simulta	neously: Compact view			
	······································			



# **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

Clevel H	and Police lousing Au	e and Metro ithority	0
Feed St	atus: Online	Listeners: 1	056
	03:0	7	
	Stop	<b>4</b> 3)	
Volume:	-		-
Abrie	ef 15-30 sec a	ad will play at	
	the start of t	his feed.	
No ads	for Premiu	m Subscribers	

### 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

M		OSD- DMR Channel Activity → ×     Ch TX Freq Pri Target TgtAlias Source SrcAlias     S0 9 2352929     SDR# v1.0.0.1583 - RTL-SDR (USB)	-
Image: DSD+	12:26:29 DSD+ 1.101pt [Publi: Release] 12:26:29 DMR/MotoTRBO decoding enabled 12:26:32 Group call; TG=9 RID=3235929 67x 12:27:33 4 group records saved; 0 aliases 12:27:46 Group call; TG=9 RID=310711 57x 12:28:30 Group call; TG=9 RID=3252929 DMR DCC:1	Oco 438.800.000	
August and a second a		DSD         Audio Spectrum           Stop DSD         0           > Baseband Noise Banker*         0           > Demodulator Noise Banker*         0           > Recording*         0           > Band Plan*         0           1 k         2 k	4 k

### 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**

3.2i	o01 nterface	Options F	ilters Displ	ay Monit	or Chara	acter Set Help
		131				
	Time	Date	Mode	Туре	Bitrate	Monitored Messages
		112101	pocaad-2	ALPEA	2400	?,d) <e?bl%t,l?")<ul 42d??}?:</e?bl%t,l?")<ul 
			POC8AG-3	NUMBERIC		02195
			POCSAG-4	NUMBER IS		TORE OF Y
			POCSAC-1	NUMBERIC	2400	TONE ONLY
			POCBAG-2	DISTRICT		
						Db*<#h 902?%*?
						15:31-16,Test Message.&Location:.1
						TORE ORLY
						(U+U+U+U+U+U+U+
						15:31-17,Test Message.&Location:.1
						+++TIME=9532191124*++TIME=1532191120?
	H 98 7	10-11-28	POCSNO-3	NUMBER OF	2400	10-91669061 *692*9 63311
	Time	Date	Mode	Туре	Bitrate	Filtered Messages



### Capturing Monitor Emanations





# OSINT data retrieval model



Mainstream Information designed to be read and obtained by the general

permission of the target/s.

### Search organisations' frequencies and transmitter locations

### • radioreferenceuk.co.uk

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

User / Licence Number (New)	Search
Frequency or Range eg 162-174	Quick Links
Томп	Airports Air Control Mil Airfields
Postcode (Overides Town)	Mil Air Control Nationwide Amateur
10	
All Groups	
Capy CSV Prest Scanner Export Column valiably Search:	Show 10
Licence	Radio Horizon County Postcode CCIRANNAC CCCSIDCS Distance Bearing
No dat	a available in table
	Previous



### **US FCC database**

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

$\leftarrow \rightarrow C$	https://apps.fcc.gov/oe	tcf/els/reports/GenericSearch.cfm	G C= G 4 🔍 ···
FCC Communications Commission	\$		SearchIRSS  Updates IE-Filino IInitiatives  Consumers  Find People
Office of Engineering ar	nd Technology		
OET Home Page	FCC > FCC E-filing > ELS > Ge	neric Search	
iling Options	General Information	Experimental Licensing System (	Jenenc Search
Form 405 - License Renewal	File Number:		
Form 442 - New License/Modification of License	Call Sign:		
Form 702 - Assignment of	ERN:		
Form 703 - Transfer of Control	Applicant Name:	Not	🗧 🗧 🗁 🖸 🗅 https://fjallfoss.fcc.gov/General_Menu_Reports/engineering_search_out.cfm?service_select=Select&accessible=NO&state_select= 🖽 🏦 🏠 🎓 👍 🔹 …
Special Temporary Authority Add Attachments	Purpose of Operation (STA-type filings only):		
Reply to Correspondence	Comments:		Commission Search ISS 1 Updates 1 E-min 1 initiatives 1 Consumers 1 Hill resource Conversions
Amend/Complete Application			Site / Eranuency / Market Search Results
Return to 159 Form	Disposal Date Range:	to	Table Of Contents
	Receipt Date Range:	to	Cite / Engranda Vierket Source Booute
Reports	Expiration Date Range:	to	Sile / Frequency / Market Search Results
Application Status	Frequency Range:	to 🔽 🗸	Search Criteria: Licensee Name = 'AT&T' Currently Licensed and Pending Facilities
Call Sign Search Generic Search	EPD-	exact to V	OET Experimental Licensing System Database
Point Radius Search	Emission:		Callaion: WIXID Elia Number: 0572 EV.CP. 2020   Iconsee: 478 T EDN: 0018716258   Issue Date: 01/01/2021   Evolution: 07/01/2022   Dadio Service: VT Status: Granted
Minnellaneous	Scope of Service:		Site Address: 200 S. Laurel Ave. State: NJ County: MONMOUTH Fixed Coordinates: 40° 23' 49' N 74' 8' 6" W
inscendieous	Experiment Type:	<b>~</b>	Calision: WL2XPW File Number: 0092-EX-CM-2021 Licensee: AT&T FRN: 0018716258 Issue Date: 06/03/2021 Expiration: 05/01/2022 Radio Service: XT Status: Granted
Get FRN FLS Notification Website	Transmitter City:		Site Address: 1880 West Northwest Hiphway State: TX County: DALLAS Mobile Coordinates: 32° 52′ 15° N 96° 55° 25° W
	ranspiller State:	, i i i i i i i i i i i i i i i i i i i	State: TV County Dall 45 Mobile Coordinates: 375 57 47: N 665 54: 38: W
			[construction] [const
			Inter-Autress. Our Commer Joureana Instance Andreas (CALLAS International Instance) (CALLAS International Instance (CALLAS International Instance) (CALLAS I
			Iste Address: 214b California Crossing Istate: 1.A IL-County: DALLAS [Mobile Coordinates: 32"51"55" N, 96"54"29"W
			Site Address: 1707 X Street State: TX County: DALLAS Mobile Coordinates: 32° 53' 25' N. 96' 54' 57' W
			Site Address: 9920 Pacific Heights Blvd.   State: CA   County: SAN DIEGO   Mobile Coordinates: 32° 54' 0" N, 117° 11' 26' W
			Site Address: 8970 Crestmar Point State: CA County: SAN DIEGO Mobile Coordinates: 32° 53' 14" N, 117° 10' 13" W
			Site Address: 6680 Mira Mesa Boulevard    State: CA    County: SAN DIEGO    Mobile Coordinates: 32° 54° 27" N, 117" 10° 27" W
			[Site Address: 200 EAST BELTLINE ROAD         [State: TX         [County: DALLAS         [Mobile Coordinates: 32" 56" 55" N, 96" 55" X         96" 25" W

# **Signal Identification Guide**

	https://www.sigidwil	ki.com/wiki/Category:Dig	ital						2 <b>0</b>	£^≡	ſ <u>⊕</u> <u>∔</u> ₀	• • •
	category discu	ussion edit history									create account	🤱 log in 🔺
SIGIDWIKI.COM SIGNAL IDENTIFICATION GUIDE	÷			Ads Send feedba	by <b>Goo</b> ck Wh	o <b>gle</b> y this ad?	⊳					
navigation  Home Page All Identified Signals	Digital Sig	nals										
Unidentified Signals     Recent changes     Random page     Add a Signal Entry	Click the nam	ne of a signal to see	e more detailed infor	mation, pos	sible de	coding, a	nd additi	onal sou	ind and wate	rfall sa	mples	
RTL-SDR Blog     Artemis 2     search	Inactive (No longer in use	Active (Currently in active use)	Status Unknown or Intermittent									
Search Go	Signal Name	Des	cription	Frequency	Mode	Modulation	Bandwidth	Location	Sa	mple Aud	io	Water
Search frequencies = VLF = LF = MF = HF = VHF = UHF categories = Military = Aviation = Satellite	1G Advanced Mobile Phone System (AMPS)	The first generation of cellu telecommunications, which	ular mobile nused analogue <u>NFM</u> voice.	824 MHz — 894 MHz	NFM	FM, FSK	10 kHz — 30 kHz	Worldwide	▶ 0:00 / 0:	12 —	• •) :	

### **Transport Radar and WSPR**

#### Marine Radar

#### Flight Radar





WSPR



# Maps of cryptocurrency miners and cell towers





## **`Find my phone' iPhone verification bypass**



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

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

Cloud Setti	ngs ~						
Mail	Contacts	Monday 21 Calendar	Photos	iCloud Drive	Notes	Apple ID Manage 🕑	Language & Formats Verify Your Identity to edit th
Account Sett	ings >		,			ore details.	
							Details n
				My De You are sign iPhor iPhor 12	vices red in and runn of the second s	ning iOS 8, macOS Yosen	hite, watchOS 1, or later on these devices.

# 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

Connected:	true User: anonymous	
DIR	2021-12-10T03:03:00.000Z .	
DIR	2021-12-10T03:03:00.000Z	
DIR	2021-12-10T03:03:00.000Z	Public
DIR	2021-12-10T03:03:00.000Z	3.4.
DIR	2021-12-10T03:03:00.000Z	
10244	2016-06-04T00:00:00.000Z	.DS_Store
DIR	2021-11-15T21:11:00.000Z	Cam
DIR	2021-11-15T21:11:00.000Z	
DIR	2021-12-10T03:03:00.000Z	••
DIR	2021-11-15T21:11:00.000Z	Picture
2585731614	2020-08-18T00:00:00.000Z	GÃ¥sbo Juli 2020.mp4
DIR	2021-11-15T21:11:00.000Z	Misc
DIR	2021-11-15T21:11:00.000Z	
DIR	2021-12-10T03:03:00.000Z	
2585731614	2021-02-06T00:00:00.000Z	GÃ¥sbo Juli 2020-1.mp4
DIR	2021-11-15T21:11:00.000Z	Janne 123 se
100082	2016-04-27T00:00:00.000Z	StudentpdfKvitto.pdf
1351591	2016-04-27T00:00:00.000Z	student.jpg
DIR	2016-10-15T00:00:00.000Z	Nathalie student 03-06-2016
DIR	2021-10-06T15:21:00.000Z	Shared Music
DIR	2021-12-10T03:03:00.000Z	Shared Pictures
DIR	2021-11-05T20:52:00.000Z	Shared Pictures 123 se
DIR	2021-10-06T15:21:00.000Z	Shared Videos
DIR	2021-12-10T03:03:00.000Z	janne
DIR	2021-11-15T21:32:00.000Z	
DIR	2021-12-10T03:03:00.000Z	
25189	2018-03-10T00:00:00.000Z	20171115163604068.jpeg
4446021	2015-04-14T00:00:00.000Z	6c279c98-f9d7-44f1-814f-c3f3027bac48.3gp
DIR	2021-11-11T16:23:00.000Z	DivPhone
DIR	2021-11-11T16:23:00.000Z	
DIR	2021-12-10T03:03:00.000Z	
DIR	2021-11-11T16:30:00.000Z	BreezeResources
DIR	2021-11-11T16:14:00.000Z	Download
DIR	2021-11-11T16:15:00.000Z	Epson iPrint
DIR	2021-11-11T16:22:00.000Z	Screenshots
DIR	2021-11-11T16:17:00.000Z	Voice Recorder
DIR	2021-11-15T21:18:00.000Z	Downloads
DIR	2021-11-15T21:18:00.000Z	
DIR	2021-12-10T03:03:00.000Z	

### 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

🚖 NetCommWireless 🛛	Status Networking Services	System Help
		<b>1</b>
Log in	This field is required.	
Username		
Password		
	Log in	

<ul> <li>System informati</li> </ul>	on		^ LAN
System up time	Device version	Cellular module	IP
	Hardware version	Model	
(4)	1.1	SQN3120-NWL25	MAC address
46 Days 23:56:12	Serial number	Module firmware	
		3.3.2.0-21821	Ethernet port status
	Firmware version	IMEI	Down
	¥2.0.23.11		
		Hardware Rev3	<ul> <li>SMS status</li> </ul>
			Received message count
			0
<ul> <li>Cellular connection</li> </ul>	on status		
SIM status	Operator selection	Allowed bands	<ul> <li>Event notification</li> </ul>
SIM OK 🧭	Automatic	All LTE bands	Event count
Signal strength (dBm)	Current operator	Current band	92
-100.99 dBm (Medium)	Verizon USA	LTE Band 4	
Network registration status		Coverage	
Registered, home network		LTE	
<ul> <li>WWAN connectio</li> </ul>	n status		
		Show data usage	
Profile name Profile1			
Status	WWAN IP	APN soot VZWSTATIC	
Connected		SUT ALWSTATE	
Default profile Yes	DNS server	3 Days 07:50:35	
Advanced status			
Auvanceu status			
Mobile country code	Physical Cell Identifier	Reference Signal Received	
311	(PCI) 389	Quality (RSRQ) -9.74 dB	
Mobile network code	Location area code (LAC)	Reference Signal Received	
40	(1R0)	Power (RSRP) 0	
DC input voltage 24.40V	IMSI	200.99 UBIII	
		Reference Signal Received Power (RSRP) 1	
SIM ICCID	Cell ID	-103.08 dBm	
Power input mode		Packet service status	
DCJack	Channel number (UARFCN)	Attachéd	
	20030		

# 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

	Home	Tenders	Analysis	Register	Log in
tome > Tenders					
UK – Public Sector Contracts					
Town 2,071 notices in past week. Wed 02 Mar 2022	new			C Liv	e tender:
Hyndsun Bonogh Council Environmental Services Replacement of the Existing Welfare Depict Replaces and Accomption Cerellety, Acctington, Logial Services - Procurement were: 4 supplier	t Solicitors Par	Northum Debt C award: -	brian Water Gro ollection Ager I suppliers	ncy Framewo	ork
South Tymeside Council London Borough of Bexley Patient Invite/Recall Service for Health ewerd: 8 uppliers £208K tender o	E175K	taffordshire Cou amily Suppor award: 2 supplier	nty Council t and Outread s	ch Service E3.4M	
UK Hydrographic Office McGanes & Lancashire CSU Translink MFG Sandbox Operational Support Bast Track General Property L award: Rowe IT £75K award: Deta Care £2K tender ⊙	Maintenance F	ramework £10M	Cumbria Count Physical Dis award: Combe	ty Council ability) Domiciliary Ca	are £506
NHS England & NHS Improvement North East & Yorks Whitby and Robin Hood's Bay General Dental Services tender ⊙ £10M	Midlands & Lan Care Home V Life - 65+ award: Orrell G	cashire CSU Vith Nursing - range Nursing H	Fast Track/Er	nd of £3.9K	
Borough Council of Kings Lynn & West Nortolik Athletic Hammer Cage award: Sport & Play £48.4K	tes £40K	fence Science & tial Analysis o EO) Data Fro ryload rard: Surrey Univ	Technology Lab the Medium m the DSX/Cl ersity	oratory Earth Orbit REDANCE	:42.5K

		BidNow
A Contract Award No by	tice	Want to bid on tenders NO WIN, NO FEE bidding service is now availabl
Source Contracts Finder 2* Type Contract (Services)	Sector DEFENCE Published 28 Jan 2022	Cohort now open for 12 month of unlimited bid support for on a £3,500 <sup>+VAT</sup> membership fee.
Duration 3 year Value	Delivery 03 Jul 2019 to 02 Jul 2022 Deadline	<ul> <li>Unlimited pro bid support</li> <li>Member fee of £3.500 * VAT / pa</li> </ul>
£352K-£362K	28 Jun 2019 12:00	<ul> <li>Win fees from £250 up to 3%</li> <li>Limited slots available</li> </ul>
security services	<ul> <li>gate entry</li> <li>vhf radio</li> <li>patrols</li> </ul>	Start Now
Location		Status
+ manut		This tender has been awarded.
_		The specified contract end date is 02 Jul 2022.
		History

### 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.

	824.36 5170.66	785.2 œ39.16	œ824.36	
	5170.66			
		4308.92 02861.74	œ5,170.66	
	719.48	685.32 œ34.16	œ719.48	
	3896.07	3246.74 œ649.33	œ3,896.07	
	204.35	194.63 œ9.72	œ204.35	
	1855.37	1546.15 œ309.22	œ1,855.37	
	113.73	108.33 ce5.40	œ113.73	
	-688.48	-573.73 #NAME	#NAME?	
	32.71	31.16 œ1.55	œ32.71	
	2545.81	2121.52 œ424.29	œ2,545.81	
	414.82	345.69 œ69.13	œ414.82	
	32.69	31.15 œ1.54	œ32.69	
	694.53	578.78 œ115.75	œ694.53	
	647.88	617.06 œ30.82	œ647.88	
	2930.18	2441.82 œ488.36	œ2,930.18	
	773.5	736.74 œ36.76	œ773.50	
	2062.74	1718.97 œ343.77	œ2.062.74	
	54600	45500 œ9.100.	œ54.600.0	
	54600	45500 œ9.100.	œ54.600.0	
ENGLAL Facilities	28340.62	23617.18 094.723	028 340 6 SECURITY P274495 SECU	RITY AND STEWARDING FOR

	9 10 1	19 0.00 21 0.30	Mi         18         0.07%         2720         0.35%         0         0.00%         101.85.202.3           Mi         92         0.37%         2400         0.31%         2         0.00%         82.178.136.8
Ē	-		Top 30 of 1016 Total Referrers
#	H	lits	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
1	16	0.05%	http://ngolobal.wordpress.com/2012/11/14/download-official-redhat-linux-iso-imag
1	1 16	0.05%	http://www.bing.com/images/search
1	2 15	0.05%	https://www.google.ae/
1.	3 14	0.04%	http://android-call-spy-full-apk.soup.io/
1.	4 13	0.04%	http://www.baidu.com/search/spider.htm
1	5 13	0.04%	http://www.google.com.om/url
1	5 12	0.04%	http://best-android-spy-apps-2014.soup.io/
1	7 12	0.04%	http://best-spy-tracking-app-for-android.soup.io/
1	8 12	0.04%	http://kino.moukrest.ru
19	12	0.04%	http://nglobalinc.blogspot.com/2012/10/pc-tools-registry-mechanic-v1101716.html
20	0 11	0.04%	http://best-catch-a-cheater-android-spyware.soup.io/
21	1 11	0.04%	http://hotel.qunar.com/
22	2 11	0.04%	http://semalt.semalt.com/crawler.php
2.	3 10	0.03%	http://android-mobile-spy-apps-download-apk.soup.io/
24	4 10	0.03%	http://ngolobal.wordpress.com/2012/10/03/free-mp3-download-of-maithili-song/
2	5 9	0.03%	http://best-android-spy-security-app.soup.io/
20	5 9	0.03%	http://best-pof-spy-apps-on-android.soup.io/
2	7 9	0.03%	http://best-rated-sms-spy-for-android.soup.io/
23	9	0.03%	http://cell-phone-spy-for-android-2015.soup.io/
29	9 9	0.03%	http://spy-on-android-to-iphone.soup.io/
3	9 9	0.03%	http://top-spying-software-for-android-2014.soup.io/

www.

### **Corporate manned building security**



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

Sharp

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 Sa bu

Same photo but different sources



### **Bug Bounty Sites – leak data and vulnerabilities**



# **Radio user and equipment OSINT**

$\rightarrow$ $\bigcirc$	Not secure   ref051.dstargateway.org							
LUS Da	shboar	d I Ref	lector S	tatus and	Contro			
egletration	REI	F051 Reflector S	ystem	DREFD	version 1.42			
	Linke	d Gate	ways					
Module A	Module B	Module C	Module D	Module E				
		K9SA B	KC9YFX B					
		KF7CUF B	W9BIL B					
		NS9RC B	W9DUA B					
	Rem	ote Us	ers					
Callsign	User N	User Message		Туре				
KD9LZ			listening	HotSpot				
KI6LBD			listening	HotSpot				
KE9ER			listening	HotSpot				
W9TPA			listening	HotSpot				
AE9JG			listening	HotSpot				
N9LOE			listening	HotSpot				
K9KRA	<u> </u>		listening	HotSpot				
KC9SIO	<u> </u>		listening	HotSpot				
W9DP			listening	HotSpot				
K9HKS			listening	HotSpot				
N9NYX			listening	HotSpot				
K9DPM	<u> </u>		listening	HotSpot				
KC9ZMY			listening	HotSpot				
W9RX			listening	HotSpot				
ND9W			listening	HotSpot				
N9IJ	<u> </u>		listening	HotSpot				
KR6SAM			listening	HotSpot				
KC9IL			listening	HotSpot				
WD9JEN	<u> </u>		listening	HotSpot				
KD9L	Doug Cerro G	ordo IL	D	HotSpot				
K9MJK			listening	HotSpot				
KB9TZS			listening	HotSpot				
K9AT			listening	HotSpot				
W9AJC			listening	HotSpot				
PD4X D			listening	HotSpot				
KE9AU			listening	HotSpot				
M9MJM	Mike-Scottsda	le, AZ	C	HotSpot				

#### Last Heard

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

**D-Star radio** gateway/users database

Active radio hardware technical details often available



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.

(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)

and

## **D-Star DMR/NXDN OSINT**

A https://database.radioid.net/database/api#!  $\odot$  $\leftarrow$ RadioD.net 斺 Home API Docs ⑦ FAQ RadioID has an API for querying data, All endpoints are available without authentication and Support \*\* If you are simply looking for a dump of the er Database api/dmr/user/ 🗋 Data Dumps Id - DMR ID of a user 🔑 api callsign - DMR user callsign surname - Surname Rptr Map
 Revenue
 city - City state - State / Province 8 Register country - Country 🕣 Signin 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

### DMR/NXDN users and repeater details

1	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	Christens	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

### <u>US law</u>

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!