Spooky Wireless







ALL YOUR RF ARE BELONG TO US! Your proximity to this device constitutes consent to

Your proximity to this device constitutes consent to be monitored on all applicable parts of the electromagnetic spectrum. You have no chance for privacy make your time.

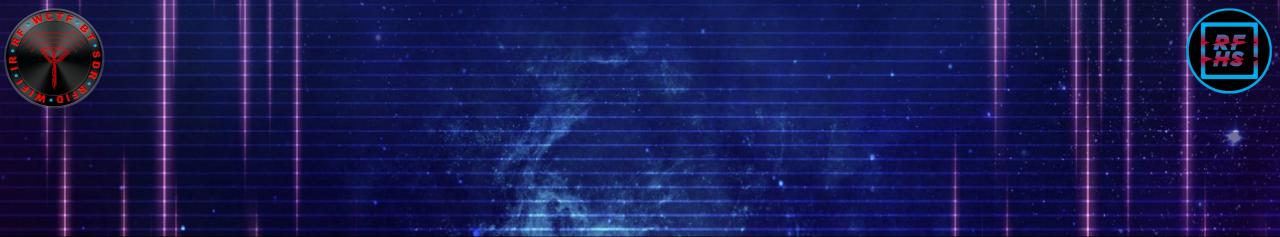


RF HS





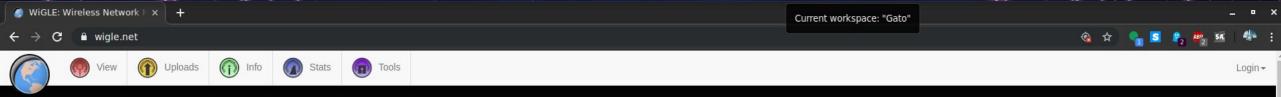




Apple devices scanner

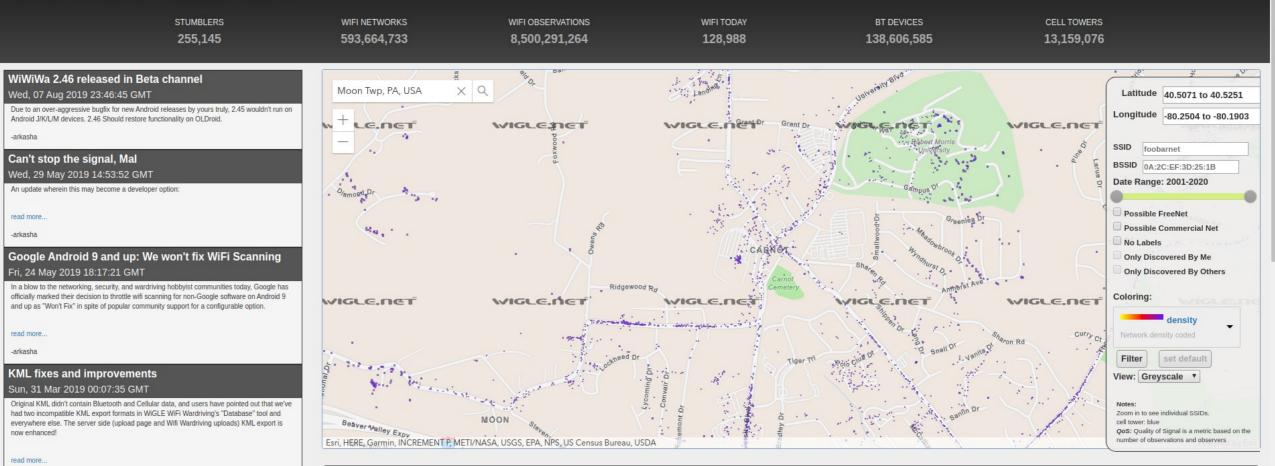
Мас	State	Device	WI-FI	OS	Phone	Time
50:2D:AC:99:12:94	Off	iPhone	0n	i0S12		1563353463
7E:B5:C1:97:E4:C9	Home screen	MacBook	On	Mac OS		1563353463
51:7B:B1:BB:E5:51	Lock screen	iPhone	On	i0S12		1563353463
56:E6:3F:CD:76:86	Off	Watch	On	WatchOS		1563353453
6B:54:70:E6:25:7D	Home screen	iPhone	On	i0S12		1563353463
49:5E:D2:98:47:47	Off	iPhone	On	i0S12		1563353463
41:CE:CF:85:21:B8	Off	Watch	0n	WatchOS		1563353463







All the networks. Found by Everyone.



Statistics Over Time

WiFi Networks Over Time

600K

By popular demand, we are now vending bluetooth network data via the API and basic search pages. Please consider the detail results a non-final implementation, as bluetooth devices are

Bluetooth in API and Basic Search Fri, 22 Mar 2019 20:24:53 GMT

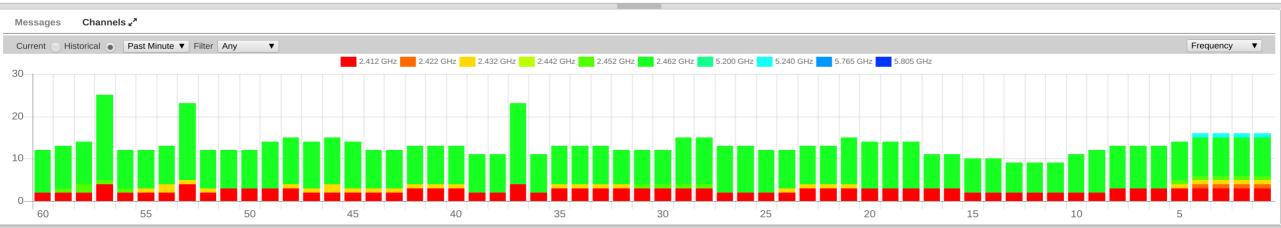
-arkasha

Google Play

≡ Kismet

									Search:		
Name	Туре	y Phy	Crypto	Signal	Channel	Last Seen	Data	Packets	Clients	BSSID	\$
UESC-N	Wi-Fi AP	IEEE802.11	WPA-CCMP	-35	11	Apr 05 2019 09:09:59	1.43 KB		5		•
	Wi-Fi AP	IEEE802.11	WPA-CCMP	-84	11	Apr 05 2019 09:09:32	0 B	II -I	0		
	Wi-Fi AP	IEEE802.11	WPA-TKIP	-35	1	Apr 05 2019 09:10:00	0 B	1_11_1111_11+1_11_1+	0		
and the second s	Wi-Fi AP	IEEE802.11	WPA-CCMP	-64	6	Apr 05 2019 09:09:49	0 B	1.111	0		
	Wi-Fi AP	IEEE802.11	WPA-CCMP	-34	11	Apr 05 2019 09:09:59	0 B	111. _11.1.111.	0		
	Wi-Fi AP	IEEE802.11	Open	-49	1	Apr 05 2019 09:10:00	0 B	1_11_11+1_11+1_11_1+	0		
Cat partay	Wi-Fi AP	IEEE802.11	WPA-CCMP	-35	11	Apr 05 2019 09:09:59	0 B		0		
	Wi-Fi AP	IEEE802.11	WPA-CCMP	-74	11	Apr 05 2019 09:09:59	0 B	1111.11.111.111.	0		
UESC	Wi-Fi AP	IEEE802.11	WPA-CCMP	-38	11	Apr 05 2019 09:09:59	22.95 KB		4		
UESC-N	Wi-Fi AP	IEEE802.11	WPA-CCMP	-74	11	Apr 05 2019 09:09:59	0 B		0		
Knappster	Wi-Fi AP	IEEE802.11	WPA-CCMP	-81	1	Apr 05 2019 09:09:56	0 B	 - -II	0		
UESC	Wi-Fi AP	IEEE802.11	WPA-CCMP	-75	11	Apr 05 2019 09:09:59	0 B	III_II_I+I+_III++I+_	0		
	Wi-Fi Bridged	IEEE802.11	n/a	-35	11	Apr 05 2019 09:09:12	740 B	- I	0		
	Wi-Fi Bridged	IEEE802.11	n/a	-38	11	Apr 05 2019 09:09:59	22.96 KB	l.h	0		-

Showing 1 to 7 of 20 entries



Powered by many OSS components, see the **credits page**

Spooky Wireless: Hands-on Ghostbusting Labs





% whoami

Product Manager at Aruba Networks Board Member for RF Hackers Sanctuary Lead Developer Pentoo Linux Developer Aircrack-ng Extra Class Amateur Radio Operator Wireless Hobbiest







% whoami

Product Manager at Aruba Networks Board Member for RF Hackers Sanctuary Lead Developer Pentoo Linux Developer Aircrack-ng Extra Class Amateur Radio Operator Wireless Hobbiest Not a lawyer Not your lawyer





Legal disclaimer

https://www.fcc.gov/consumers/guides/interception-and-divulgence-radio-communications







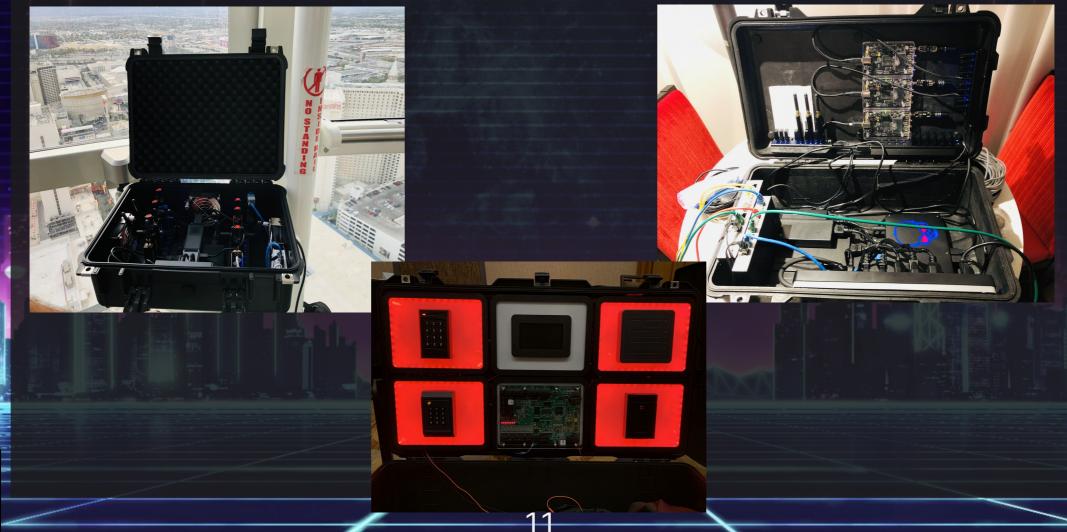
DefCon 27 Wireless Capture The Flag We were here!



10



DefCon 27 Wireless Capture The Flag Now we are here!



Why Linux?

Linux is an Open Source Operating System Free as in Beer Free as in Freedom Supports "most" computers Supports fun things that we want to do





Why Pentoo Linux?

Longest running "penetration testing" Linux distribution Lots of documented support Lots of wireless specific testing Me Truthfully, with a livecd it doesn't matter so long as it works https://pentoo.ch





Simple Stuff

Read a news article about new Apple issue called apple_bleee Google search gets us https://github.com/hexway/apple_bleee Contains a wonderful README, which you can...read. Follow the directions Report bugs







Kismet works with Wi-Fi interfaces Bluetooth interfaces some SDR (software defined radio) hardware like the RTLSDR and other specialized capture hardware

Well documented at https://kismetwireless.net/docs/ Report bugs







Software Defined Radio

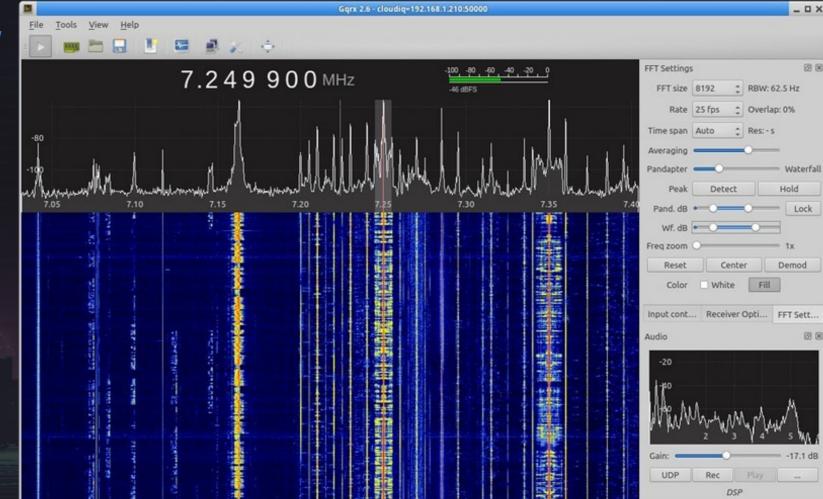
a radio communication system where components that have been traditionally implemented in hardware (e.g. mixers, filters, amplifiers, modulators/demodulators, detectors) are instead implemented by means of software on a personal computer or embedded system.* Flexible Hardest way to do one thing well Only way to do everything

*paraphrased from wikipedia sdr entry



GQRX

http://gqrx.dk/





http://gqrx.dk/doc/practical-tricks-and-tips

Universal Radio Hacker

18

https://github.com/jopohl/urh

Reverse Engineering Toolkit





Universal Radio Hacker

N O S





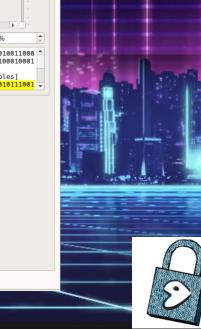
Interpretation Analysis Generator Name Size anlernen3x3.t. 9.3 MB 1: Complex Signal Image: Backup.URHP. 10 KB 303 KB Boeser14er.c... steckdose_anlernen decodings.txt 458 bytes 38,6 MB fernbedienun. Noise: 0,0111 fernbedienun.. 16.6 MB fernbedienun... 18,4 MB -0,0539 Center: 86,4 MB gen.complex 4 KB info.txt Bit Length: 104 19,9 MB old tar bz2 profile.fuzz 13 KB Error Tolerance: 5 27 KB protocol ke.txt Modulation: FSK -8 KB protocol.proto + 2002 samples selected | 2,00 ms 9 KB protocol.txt 98,0 MB steckdose a. Signal View: analog adadadado/000/001037111390101 1Fause, 33231 Samples aaaaaaaa67686768ecc16de20f0c2844d97ad239735619b455caf2955bf9f [Pause: 13176 samples] steckdose_a... 48,2 MB 14.2 MB steckdose_anl. Autodetect parameters aaaaaaaa67686768ebc16d818db64bc6637ade5b6104c4baaa47132c6c3ba38 [Pause: 13602 samples] tuersensor an.. 19,1 MB aaaaaaaa67686768e8816de20f0c2844d97ad2397408e1f8f88d77c5466c5c8ca37e7 [Pause: 12133 samples] 14,9 MB tuersensor an... ✓ Show Signal as Hex aaaaaaaa67686768fcfa7da910d20 [Pause: 1049346 samples] 30,4 MB tuersensor_an.. 421 KB tuersensor-an... tuersensor-an... 273 KB 2: Complex Signal 🕞 🚯 🙆 tuersensor-an... 2,5 MB 156 KB tuersensor-an.. steckdose anlernen2 5 KB URHProject.x... 2,9 MB versch_tage.t... Noise: 0,0111 Center: 0,0000 \$ Bit Length: 100 4 Error Tolerance: Modulation: FSK -+ 0 samples selected | 0,00 ns Signal View: analog Autodetect parameters

✓ Show Signal as Bits

X-Zoom: 100%

Participants: not assigned





Y-Scale

\$

Y-Scale

X-Zoom: 424195%

Universal Radio Hacker

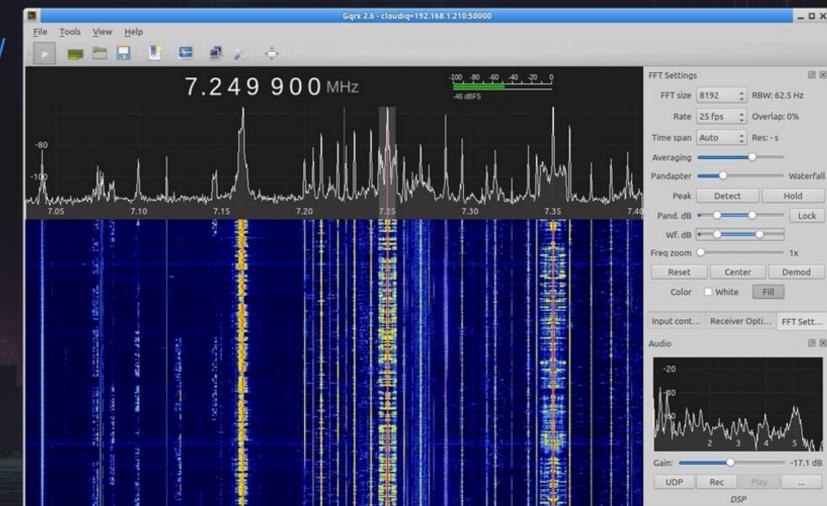
S D R

Compare your protocols here		Search	n Patte	rn				S	earch	•	2	- /	-									RS	SI: 0	0,12								Time	estam	np: 9	,20 s	(+9	,12 s)				
🔻 🗹 🚞 New Group			1 2	З	4 5	5 6	78	9	10 1	1 12	13 1	4 15	16	17 18	8 19	20	21 22	23 2	24 2	5 26	27	28 2	9 30	31	32 3	3 34	35	36 3	7 38	39	40 4	1 42	43 4	4 45	5 46	47	48 4	9 50	51	52 53	3 54 [*]	
 ✓ steckdose_anlernen ✓ steckdose_anlernen2 		1 (A)	a a	а	a a	a a	a a	9	a 7	7d	9	a 7	d	2 d	8	0	70	e	0 0	0	0	з 1	L b	6	0	з з	0	0 (0 1	0	0 4	1 O	з	0 1	4	f	7 4	1 8	9	c 5	9	-
		2 (B)	a a	а	a a	a a	a a	6	76	58	6	76	8	0 6	1	b	60	з	з 7	8	e	28	3 9	0	0	0 0																
		3 (B)	a a	а	aa	аа	a a	9	a 7	7 d	9	a 7	d	3 2	0	0	70	1	b e	5 0	3	3 7	78	е	2	89	с	0 (0 1	0	4 0) 2	0	67	2	4	9 0	97	f	a a	0	
		4 (A)	a a	2						7 d	0	. 7		0 3			e 2		9 (0													-								
				a	d	a a	a a	9	a /	u u	9	a /	-			-			-					-	-	_																
		5 (A)	a a	а	aa	a a	a a	6	/ 6	5 8	6	/ 6	8	1 3	2	0	70	/	8 €	2	8	9 1	Lb	6	0	3 3	0	0 (0 0	0	0 0	0	a 4	4 3		а	6 2	25	9	b 8	6	
		6 (B)	a a	а	a a	a a	a a	6	76	58	6	76	8	0 3	1	b	60	3	3 (0 (0	0					_															-
Hex	-	7 (B)	a a	а	a a	a a	a a	6	76	58	6	76	8	1 a	2	0	70	1	b 6	5 O	З	3 7	8 7	е	2	B 9	0	0 (D C	6	2 0	e	66	6 a	4	8	c 6	6 d	0	c 7	с	+
DeWhitening Special	•	8 (A)	a a	а	a a	a a	a a	6	76	58	6	76	8	0З	7	8	e 2	8	9 (0	0	0																				-
Decoding errors for block: 0 (0,00%)		9 (A)	a a	а	a a	a a	a a	6	76	58	6	76	8	1 3	2	0	70	7	8 €	2	8	9 1	LЬ	6	0	з з	0	0 (0 0	0	0 0	1	5 k	b 4	e	2	4 4	45	а	b 5	з	-
Analyze	Ţ	10 (B)	a a	а	a a	a a	a a	6	7 6	5 8	6	76	8	0 3	1	b	60	3	з (0	0	0																				+
Show these participants:	_0	11 (B)	a a	a	a		a =	6	7 6	5 8	6	7 6	8	1 a	2	0	70	1	be	i 0	3	3 7	7 8	e	2	89	0	0 (0 6	6	2 0	f	3 2	a 1	8	a	9 1	5 8	4	6 9	0	
✓ not assigned				-	a		aa	6	7 6		č .	76	-	0 3		-			9 (0			-	-		Ŭ			Ŭ					Ŭ	u	5				Ĭ	
✓ Bob (B) ✓ Alice (A)		12 (A)	a a		u .		u .	0	/ (0	0		-			Ŭ		-	-	-	-	-																				
		13 (A)	a a	а	a a	a a	a a	6	76	58	6	76	8	1 3	2	0	70	7	8 €	2	8	9 1	l b	6	0	33	0	0 (0 0	0	0 0) 2	a t	fb	a	b	0 4	17	0	c 1	e	
		14 (B)	a a	а	a a	a a	a a	6	76	58	6	76	8	0 3	1	b	60	3	3 (0 (0	0					_															
		15 (B)	a a	а	a a	a a	a a	6	76	58	6	76	8	1 4	2	0	70	1	b 6	5 O	З	3 7	78	е	2	B 9	0	0 (D C	6	2 1	. 0	9 (c 8	2	9	8 5	50	З	c d	2	
		16 (A)	a a	а	a a	a a	a a	6	76	58	6	76	8	0З	7	8	e 2	8	9 (0	0	0																				
1-		17 (A)	a a	а	a a	a a	a a	6	76	58	6	76	8	1 3	2	0	70	7	8 €	2	8	9 1	L b	6	0	33	0	0 (0 0	0	0 0	3	c I	14	е	b	e () 1	b	7 d	f	
	_	18 (B)	a a	а	a a	a a	a a	6	7 6	58	6	76	8	0 З	1	b	60	з	з (0	0	0																				L N
Mark diffs in protocol		19 (B)	a a	а	aa	аа	a a	6	7 6	58	6	76	8	1 4	2	0	70	1	b é	5 0	з	3 7	78	e	2	89	0	0 () c	6	2 1	1	9 3	39	з	b	0 f	fe	з	а 3	e	
Show only diffs in protocol		20 (A)	a a					6	7 6	5 8	6	76	8	1 7	6	0	7 0	7	8 6	2	8	0 1	l h	6	0	3 3	0	0 (0 0	0	0 0) 4	0	f b	6	f	2	-	f	0 5		$\sim \Gamma$
Show only labels in protocol					a c		a a				с .	, ,						1			, The second sec			Ŭ	· ·		Ŭ	0		Ŭ	0 0			1 0	•		- 0	i c		0 5		
		21 (B) ∢	a a	а	a a	аа	a a	6	76	58	0	76	8	0 3	1	D	60	3	3 (0	0	0																			• •	
	E.	Bit: 00	00011	0011:	1001	0			н	ex: 0	672							De	cima	al: 16	650															4	4	Col	umn(s) sel	ected	1
Show these protocol labels:																		Labe	el va	lues	for l	bloc	k #3																			
default 👻	+	Nam	ne	Val	lue T	ype																	Va	alue																		
Preamble Sync	P	reambl	e	Hex			aaaaa	aaaa																																		
✓ Length	s	Sync		Hex			9a7d	9a7d																																		
 ✓ Type ✓ DST Address 	L	ength		Deci	mal		50																																			
SRC Address	т	уре		Hex			0070																																			
	C	DST Add	Iress	Hex			1b60	33																																		
		RC Add					78e2																																			
	s	equenc	e						24																																	
		lumber		Deci	mai		3221	29203	54																																	

21

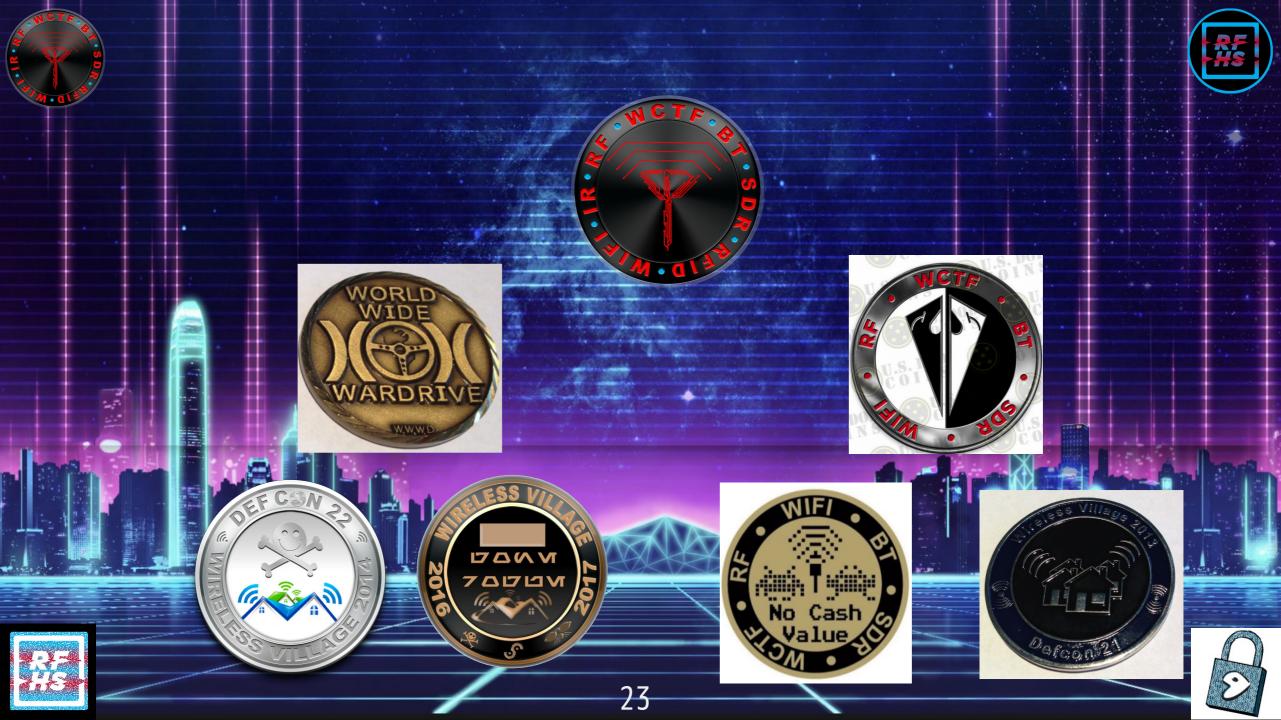
GQRX

http://gqrx.dk/





http://gqrx.dk/doc/practical-tricks-and-tips 22 Re



Links



https://wirelessvillage.ninja/ https://wctf.us/

24

