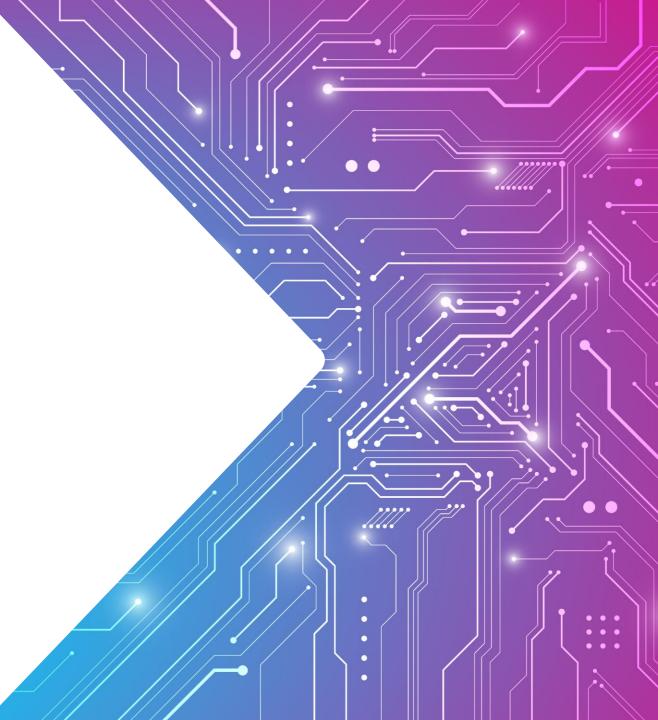


RF bugs and their detection

GS Days 2021

By Sébastien Dudek



About me

Founder of Penthertz

- Sébastien Dudek (<u>@FlUxluS</u>)
- > 10 years of experience in Software / Hardware security
 - Former Sogeti ESEC R&D as a researcher
 - and Synacktiv as a pentester + vulnerabilities researcher
- Specialized in Wireless communications
- Also, security researcher <u>@Trend Micro</u>
 - Industrial IoT
 - Mobile, and other RF/SDR things...





Penthertz

(((၀ု))

Main activities

Security assessments

- Wireless communications (RFID, Wi-Fi, Mobile communication, Bluetooth, etc.)
- Embedded devices
- Backend servers
- Red Team



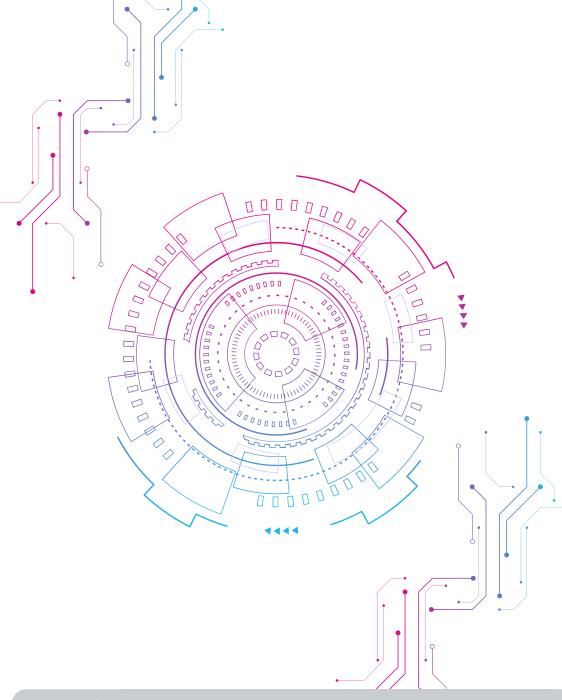
Trainings

- Software-Defined Radio
 Hacking
- Wi-Fi Red teaming
- RFID Hacking
- Mobile attacks (2G/3G/4G/5G)



Hardware security

- Firmware extraction
- Chip-off
- Secrets extraction
- Libraries analysis
- Vulnerability hunting



Summary

- **01** RF signal & use of SDR
- **02** Common bugs and ways to identify them
- **03** Unsuspected/Legit bugs

RF Signal & use of SDR



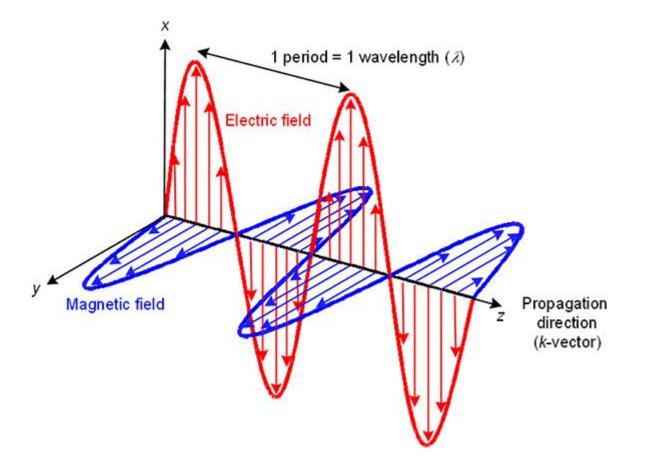
An invisible vector

E.g linearly polarized

sinusoidal EM wave:

- λ : wavelength in Meter
- c: celerity of light (3*10⁸ m.s-1)
- T: period in seconds (λ /c)
- f : frequency in Hz (1/T)

But can be observed somehow...



Spectrum analyzers

Example of a beast:

- R&S®FSV40
- 10 Hz to 40 GHz freq band
- 160 MHz signal analysis bandwidth
- costs > 43 000€

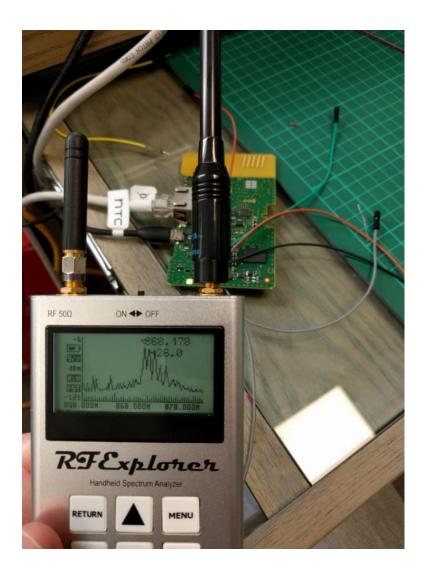




RF Explorer

A handy gadget for < 300€:

- Left SMA port (WSUB1G): 240-960MHz
- Right SMA port (WSUB3G): 15-2700 MHz
- Resolution bandwidth (RBW): automatic 3Khz to 600Khz



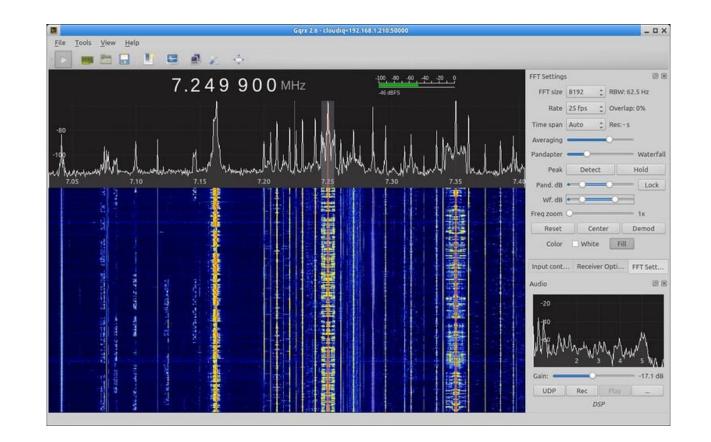
RF Signal

With SDR

Famous software:

- GQRX on Linux and Mac OS X
- HDSDR on Windows
- SDR# on Windows

But you can also build your own...



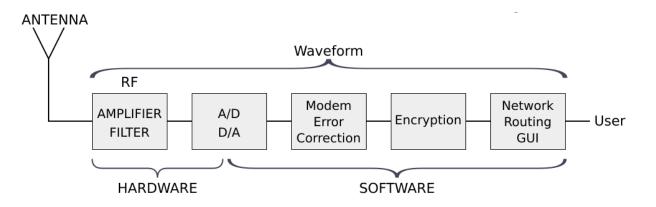
Software-Defined Radio

Before SDR \rightarrow difficult to get equipment without \$\$\$

- Made radio more accessible
- ADC/DAC conversion, RF Amp. and filtering performed on

RF equipment

• The rest is done in software, generally with a computer:



More than 100 SDR devices exist \rightarrow <u>https://en.wikipedia.org/wiki/List_of_software-defined_radios</u>

RF Signal

Cheap SDR: RTL-SDR

- Does only RX
- Different tuners/version:
 - e.g Elonics E4000 → 52-2200 MHz
- Costs from 15€
- RTL-SDR v3 is about 50€
- Good for a beginning





Part of our SDR lab

- Need to manage any type of transmission (2G-5G, Wi-Fi, Remotes, RFID, Bluetooth, ZigBee, RFID, etc).
- Able to get large bandwidth in some situation (sometimes > 100 Msps)



 Need adapted antennas for specific frequencies

Common bugs & identification

And the owner of the owner of the owner of the owner of the owner owner owner owner owner owner owner owner own

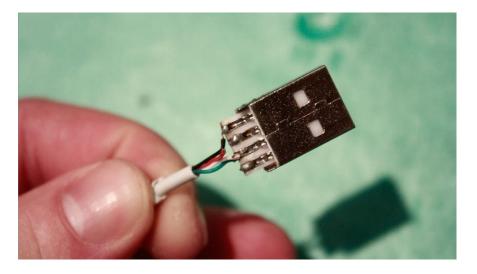
Some RF bugs

- Mobile mics (often GSM/GPRS)
- GPS tracking
- Fake cables (e.g. USB Ninja, or nRF product derivates)
- RF MITM keyboard devices
- etc.



Identification: the hard way

- Identification through accessible interface if any (UART, JTAG/SWD, SPI, I²C, etc.)
- We can teardown every cable or devices:



- But in some case \rightarrow destructive \rightarrow annoying if you want to use the product at the end
- Allow to identify one bug at a time for same family



E.g we want to avoid







E.g we want to avoid



Even if it could be a good exercise to identify components as seen in "Deux Ex Silicium" shows

penthertz.com

Identification: the RF way

- Scanning frequencies
- Identifying an interesting signal
- Further analysis:
 - Identify technology: modulation, encoding, etc.
 - Analyzing the communication
 - Interacting with RF devices
 - etc.

Isolation of devices

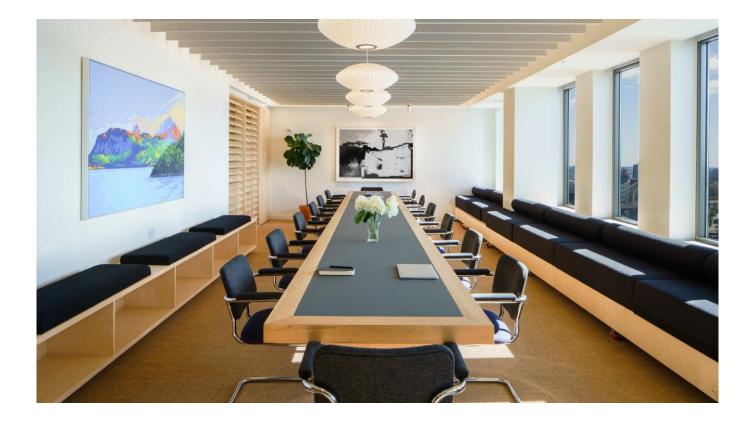
- Faraday room → enough to work with big targets
- Or a mobile faraday shield → useful to bring to a client





Inaccessible devices

- Some devices → simply accessible → hidden somewhere?
- Need to deal with legit transmissions:
 - Identifying legit transmission around → get RSSI level average ref
 - Spot freqs with high RSSI while moving the receiver → to analyze further





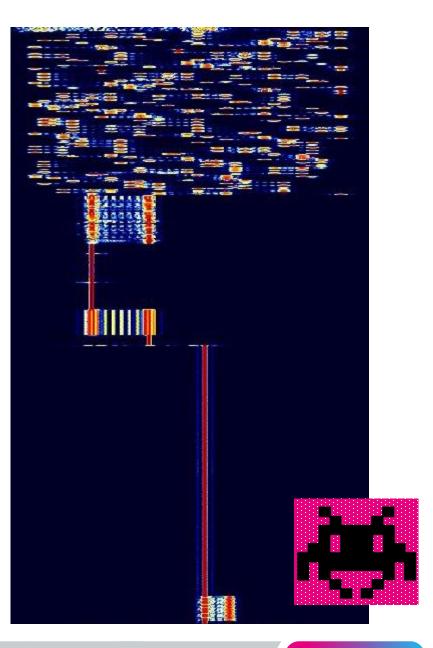
Analyze signal

- 1. Determine the frequency
- Look at the shape → which modulation does it use (ASK, FSK, GMSK...), or technique like OFDM, etc.
- Sometimes the shape is complicated to see → go deeper by look to the device's transmitter specs
- 4. Use the blocks you need to process the signa, etc.

In the end you'll have to decode it (NRZ, Manchester, PWM, Viterbi, etc.) \rightarrow and sometimes deal with encryption, etc.

Shape ID

- Elements to take into account:
 - Used frequency \rightarrow against databases like FCC ID
 - Harmonics of the signal \rightarrow DFT
 - Bandwidth
 - Signal
 - Modulation types
- Good tools:
 - Waterfall
 - Time & FFT sinks
- Ref DB: <u>https://www.sigidwiki.com/</u>



Cable bugs

Cable bugs

Wi-Fi based

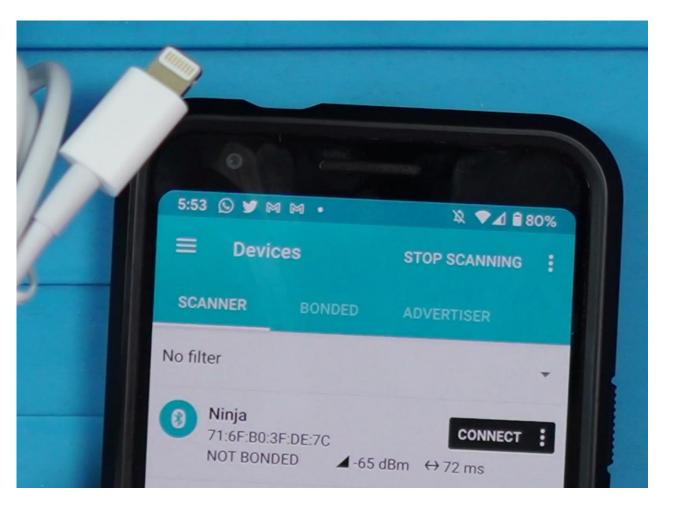
- 2.4GHz & 5 GHz to spot
- Mapping with SDR works → + analysis with WIME project
- But using dedicated dongles is even faster
- Generally expose a hotspot + management interface



Cable bugs

BLE based

- 2.4GHz to spot
- Mapping with SDR works → demod GFSK and decode
- But still: using dedicated dongles is even faster (e.g nRF52840)
- Can be spotted with a mobile APK like nRF connect → look at characteristics and play with services

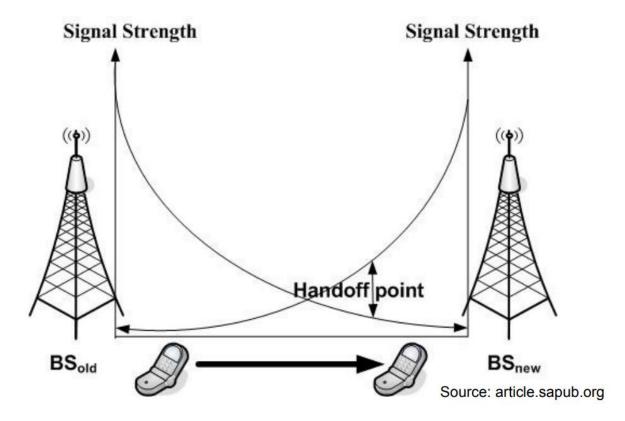


Micro spy bugs

- Uses the mobile network
- Identify \rightarrow attract them
 - But we need to map all legitimate UE =/



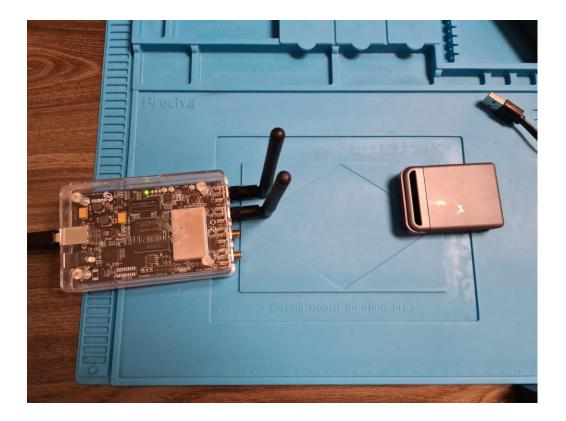
The old handover concept



• A stronger signal will likely attract targeted UEs

Fake 2G BTS

- In few steps
 - Bruteforce MCC/MNC
 - Strong GSM signal
 - Capture the communication in GSM/GPRS
- But what if the bug uses 3G or 4G?



2G - 5G targets

- 2G modules costs ~5€ min. (in AliExpress)
- 3G: ~15€ min.
- 4G: ~30 \in min. \rightarrow becoming expensive for part of a device
- 5G: ~151€ min. (and still have to be aware about NSA and SA caps)
- Further analysis from 3G:
 - Mutual authentication \rightarrow difficult to spawn a station at this level
 - We have to downgrade the communication to 2G → signaling or jamming attacks

Dumb&generic downgrade

- Jamming
- Several devices are available on the market
- But > 150€ → difficult to ship in France since July 2021 ⊗



Jamming with Modmobjam

- Concept of "smart"-jamming:
 - Uses results from a scanner like Modmobmap
 - Then jam frequencies with adapted bandwidth



mple rate: 5M	o > (1 - sooo p)	cuon such clan_ib	enpy receto_	1528367496.json			B	dunta	adio-companion	jammer gen.grc 94x2	1
npie rate: SM										HTTP/1.1" 200 -	1
gain: 35							127.0.0.1 [27/Jul				
							127.0.0.1 [27/Jul	/2018 16:10:49			
ain: 35							127.0.0.1 [27/Jul	/2018 16:10:51] "POST /RPC2		
							127.0.0.1 [27/Jul	/2018 16:10:51			
							127.0.0.1 [27/Jul		<pre>3] "POST /RPC2</pre>		
a: 1.815G							127.0.0.1 [27/Jul				
							127.0.0.1 [27/Jul		i] "POST /RPC2		
ain: 10							127.0.0.1 [27/Jul				
							127.0.0.1 [27/Jul				
dwidth: 20M							127.0.0.1 [27/Jul				
awiden: [20M							127.0.0.1 [27/Jul				
		1					127.0.0.1 [27/Jul				
							127.0.0.1 · · [27/Jul				
							127.0.0.1 [27/Jul				
							127.0.0.1 [27/Jul				
							127.0.0.1 [27/Jul				
							127.0.0.1 [27/Jul				
							127.0.0.1 [27/Jul	/2018 16:11:05	5] "POST /RPC2		
							8	sudo puthop s	martiam mc nu	-f cells 1528367496.j	con 04×24
							[+] Jamming cell			it 2142.4 MHz with 1	
							[+] Jamming cell			it 2157.4 MHz with 1	
							[+] Jamming cell			15.0 MHz with 20 MH	
									requency at 26	45.8 MHz with 28 MH	z bandwidth
							[+] Jamming cell	0 central fr	requency at 26	45.0 MHz with 20 MH	z bandwidth
							<pre>[+] Jamming cell [+] Jamming cell</pre>	0 central fr 5 central fr			
le Edit View Bun To	ools Help						<pre>[+] Jamming cell [+] Jamming cell [+] Jamming cell</pre>	0 contral fr 5 central fr 0 central fr	requency at 26 requency at 18	62.5 MHz with 15 MH 70.0 MHz with 20 MH	lz bandwidth Iz bandwidth
							 [+] Jamming cell [+] Jamming cell [+] Jamming cell [+] Jamming cell 	0 central fr 5 central fr 0 central fr 00 central f	requency at 26 requency at 18 requency at 2	62.5 MHz with 15 MH 170.0 MHz with 20 MH 2645.0 MHz with 20 M	lz bandwidth Iz bandwidth Hz bandwidth
	ools Help		e 0 4	. ⊳ 8 (<pre>[+] Jamming cell [+] Jamming cell [+] Jamming cell [+] Jamming cell [+] Jamming cell</pre>	0 central fr 5 central fr 0 central fr 00 central f 10836 centra	requency at 26 requency at 18 requency at 2 al frequency a	62.5 MHz with 15 MH 70.0 MHz with 20 MH 645.0 MHz with 20 M 1 2167.2 MHz with 1	lz bandwidth lz bandwidth Hz bandwidth 0 MHz bandwidth
		0 🔒 🗐 🔌	0	; 🖻 🙁 🛛 🖨 🖨			<pre>[+] Jamming cell [+] Jamming cell</pre>	0 central fr 5 central fr 0 central fr 00 central f 10836 centra 00 central f	requency at 26 requency at 18 frequency at 2 al frequency at frequency at 8	62.5 MHz with 15 MH 170.0 MHz with 20 MH 1645.0 MHz with 20 M 1t 2167.2 MHz with 1 16.0 MHz with 10 MH	iz bandwidth iz bandwidth Hz bandwidth 0 MHz bandwidth iz bandwidth
		WX GUI Slider	🕐 🔵 🍕			v Core ▲	<pre>[+] Jamming cell [+] Jamming cell [+] Jamming cell [+] Jamming cell [+] Jamming cell</pre>	0 central fr 5 central fr 00 central fr 10836 central 10836 central 50 central f 50 central f	requency at 26 requency at 18 requency at 2 of frequency at 8 requency at 8 requency at 1	62.5 MHz with 15 MH 70.0 MHz with 20 MH 645.0 MHz with 20 M 1 2167.2 MHz with 1	iz bandwidth iz bandwidth Hz bandwidth 0 MHz bandwidth iz bandwidth Hz bandwidth
) • 🖻 • 🗐 🕷	WX GUI Slider			WX GUI Slider W			<pre>[+] Jamming cell [+] Jamming cell</pre>	0 central fr 5 central fr 0 central fr 00 central f 10836 centra 00 central f 50 central f 10712 centra	requency at 26 requency at 18 frequency at 2 il frequency at frequency at 8 frequency at 1 il frequency a	62.5 MHz with 15 MH 70.0 MHz with 20 MH 645.0 MHz with 20 M ot 2167.2 MHz with 10 MH 106.0 MHz with 10 MH 870.0 MHz with 20 M t 2142.4 MHz with 1	iz bandwidth iz bandwidth Hiz bandwidth 0 MHz bandwidth iz bandwidth Hiz bandwidth 0 MHz bandwidth
• 🖻 • 🔚 💥 Options	WX GUI Slider	WX GUI Slider	WX GUI Slider ID: rf_gain Label: RF gain	WX GUI Slider W ID: bb_gain ID: Label: 88 gain Lab	IX GUI Slider 1 sample_rate beli Sample rate	▼ Core ▶ Audio	<pre>(+) Jamming cell (+) Jamming cell</pre>	0 central fr 5 central fr 00 central fr 10836 central 10836 central 50 central f 10712 centra 10787 centra	requency at 26 requency at 18 requency at 2 l frequency at 2 requency at 8 frequency at 1 al frequency a al frequency a	62.5 MHz with 15 MH 170.0 MHz with 20 MH 1645.0 MHz with 20 MH 1645.0 MHz with 10 MH 16.0 MHz with 10 MH 1870.0 MHz with 10 MH 12.142.4 MHz with 11 12.157.4 MHz with 11	iz bandwidth iz bandwidth Hiz bandwidth 0 MHz bandwidth iz bandwidth Hiz bandwidth 0 MHz bandwidth 0 MHz bandwidth
Options D: jammar_gan ienerate Options: WX GU	WX GUI Slider Ibi //_gain Label: IF gain Default Value: 10	WX GUI Silder Di cent_freq abeli Freq efault Value: 1.87420	WX GUI Slider ID: rf_gain Label: RF gain Default Value: 10	WX GUI Slider W/ ID: bb_gain ID: Label: 88 gain Lab Default Value: 10 Def	rX GUI Slider 1 sample_rate beli Sample rate rfault Value: 5H	✓ Core Audio Boolean Opera	<pre>(+) Jamming coll (+) Jamming cell (+) Jamming cell (+) Jamming cell (+) Jamming cell (+) Jamming cell (+) Jamming cell</pre>	0 central fr 5 central fr 0 central fr 00 central f 10836 central 50 central f 10712 centra 10787 centra 0 central fr	requency at 26 requency at 18 frequency at 2 il frequency at 3 frequency at 8 frequency at 1 al frequency at al frequency at 18	62.5 MHz with 15 MH 70.0 MHz with 20 MH 645.0 MHz with 20 M t 2167.2 MHz with 10 MH 106.0 MHz with 10 MH 870.0 MHz with 20 M t 2142.4 MHz with 1	iz bandwidth iz bandwidth Hiz bandwidth 0 NHz bandwidth Hiz bandwidth 0 NHz bandwidth 0 NHz bandwidth 1 bandwidth
Options Dijammer_gen ienerate Options: WX GU Variable	WX GUI Slider IDi if_gain Label: IF gain Default Value: 10 Minimum: 10	WX GUI Slider Dr cent_freq abel: Freq efault Value: 1.87420 linimum: 900M	WX GUI Slider ID: rf_gain Label: RF gain Default Value: 10 Minimum: 10	WX GUI Slider W ID: bb_gain ID: Label: 88 gain Lab Default Value: 10 Def Minimum: 10 Min	IX GUI Silder sample_rate bels Sample rate fisault Values SM inimum: 2M	▼ Core ▶ Audio	<pre>++ Jamming cell ++ Jamming cell</pre>	0 contral fr 5 central fr 0 central fr 00 central f 10836 central 00 central f 10712 centra 10712 centra 0 central fr 0 central fr	requency at 26 requency at 12 frequency at 2 all frequency at frequency at 8 frequency at 1 al frequency a al frequency at 18 requency at 26	662.5 MHz with 15 MH (70.0 MHz with 20 MH (70.0 MHz with 20 MH 14 2167.2 MHz with 10 MH 16.0 MHz with 10 MH 1870.0 MHz with 20 MH 14 2157.4 MHz with 1 15.0 MHz with 20 MH	iz bandwidth Iz bandwidth HFL bandwidth 0 MHz bandwidth HEL bandwidth HEL bandwidth 0 MHZ bandwidth 2 bandwidth Iz bandwidth
Options Options WX GU Variable bisamg.rate	WX GUI Silder ID: If gain Label: IF gain Default Value: 10 Minimum: 10 Maximum: 60	WX GUI Slider Di cent_freq abeli Freq efault Valuei 1.87420 linkimum: 900M laximum: 2.26	WX GUI Slider ID: rf_gain Label: RF gain Default Value: 10 Minimum: 10 Maximum: 60	WX GUI Slider ID: ID: bb_gain ID: Label: 98 gain Lab Default Value: 10 Def Minimum: 10 Min Maximum: 60 Max	rX GUI Slider t sample_rate belt Sample rate rfault Value: SM inimum: 2M ssimum: 2M	✓ Core Audio Boolean Opera	<pre>(+) Jamming coll (+) Jamming coll</pre>	0 contral f 5 central f 0 central f 00 central f 10836 central f 10712 central f 10712 central f 10712 central f 0 central f 5 central f	requency at 26 requency at 18 frequency at 22 al frequency at 2 frequency at 1 al frequency at 1 al frequency at requency at 26 requency at 26	662.5 MHz with 15 MH 178.0 MHz with 20 MH 665.0 MHz with 20 MH to 2167.2 MHz with 1 16.0 MHz with 10 MH 1870.0 MHz with 20 MH to 2142.4 MHz with 1 to 2157.4 MHz with 1 15.6 MHz with 20 MH 45.0 MHz with 20 MH	iz bandwidth iz bandwidth Hiz bandwidth 00 MHz bandwidth Hiz bandwidth 00 MHz bandwidth 10 MHz bandwidth 12 bandwidth 12 bandwidth
Options h jammar_pen enerate Options: WX GU Variable h samo_rate alue: SH	WX GUI Silder ID: If gain Label: IF gain Default Value: 10 Minimum: 10 Maximum: 60	WX GUI Slider Dr cent_freq abel: Freq efault Value: 1.87420 linimum: 900M	WX GUI Slider ID: rf_gain Label: RF gain Default Value: 10 Minimum: 10	WX GUI Slider ID: ID: bb_gain ID: Label: 98 gain Lab Default Value: 10 Def Minimum: 10 Min Maximum: 60 Max	IX GUI Silder sample_rate bels Sample rate fisault Values SM inimum: 2M	✓ Core Audio Boolean Opera Byte Operator Channelizers	<pre>++ Jamming coll ++ Jamming coll ++ Jamming coll (+) L (+) L</pre>	0 contral fr 5 central fr 0 central fr 00 central f 10836 central f 50 central f 10712 contra 10787 contra 0 central fr 0 central fr 0 central fr	requency at 26 requency at 18 frequency at 2 al frequency at 2 frequency at 8 frequency at 8 al frequency at 3 requency at 18 requency at 26 requency at 28	62.5 MHz with 15 MH (70.0 MHz with 20 MH 645.0 MHz with 20 MH 645.0 MHz with 20 MH (16.0 MHz with 20 MH (270.0 MHz with 20 MHz with 20 MH (270.0 MHz with 20 MHz with 20 MH (270.0 MHz with 20 MHz with 20 MHz with 20 MH (270.0 MHz with 20 MH	Iz bandwidth IIz bandwidth IIIz bandwidth 0 MHz bandwidth III bandwidth 0 MHz bandwidth 0 MHz bandwidth IZ bandwidth IZ bandwidth IZ bandwidth IZ bandwidth
Options Options Options WX GU Variable D: Samg_Xte suise: SM Variable Variable Variable	WX GUI Silder ID: If gain Label: IF gain Default Value: 10 Minimum: 10 Maximum: 60	WX GUI Slider Di cent_freq abeli Freq efault Valuei 1.87420 linkimum: 900M laximum: 2.26	WX GUI Slider ID: rf_gain Label: RF gain Default Value: 10 Minimum: 10 Maximum: 60	WX GUI Slider ID: ID: bb_gain ID: Label: 98 gain Lab Default Value: 10 Def Minimum: 10 Min Maximum: 60 Max	rX GUI Slider t sample_rate belt Sample rate rfault Value: SM inimum: 2M ssimum: 2M	Core Audio Boolean Opera Byte Operator Channelizers Channel Mode	<pre>(+) Jamming coll (+) Jamming coll (*) Jamming coll</pre>	0 contral fr 5 central fr 0 central fr 00 central fr 10836 central f 10712 central f 10712 central fr 0 central fr 0 central fr 0 central fr 0 central fr 0 central fr 10836 central fr	requency at 26 requency at 18 requency at 2 frequency at 2 frequency at 8 requency at 8 at frequency at 18 requency at 26 requency at 26 requency at 28 requency at 20 requency at 20 requ	62.5 MHz with 15 MHz 665.0 MHz with 20 MH 665.0 MHz with 20 M 16.0 MHz with 10 MH 870.0 MHz with 10 MH 870.0 MHz with 10 MH 870.0 MHz with 11 15.0 MHz with 20 MH 45.0 MHz with 20 MH 45.0 MHz with 20 MH 62.5 MHz with 15 MHZ 645.0 MHz with 20 MH 645.0 MHz with 20 MH	iz bandwidth Hz bandwidth HZ bandwidth O MHz bandwidth HZ bandwidth HZ bandwidth O MHz bandwidth Iz bandwidth Iz bandwidth HZ bandwidth HZ bandwidth HZ bandwidth
Coptions Di Jammer, gen enerate Options: WX GUE Variable Di samg, rate ahue: 3M Variable Variable N var, E, gan	WX GUI Silder ID: If gain Label: IF gain Default Value: 10 Minimum: 10 Maximum: 60	WX GUI Slider b: cart_freq beli Freq fault Value: 1.87420 linimum: 5004 laximum: 2.26 onverter: Float	WX GUI Slider ID: rf.gain Labelt RF.gain Default Value: 10 Minimum: 10 Maximum: 60 Converter: Float	WX CUI Slider 10: bb.gain Label: 88 gain Default Value: 30 Minimum: 50 Converter: Float	X GUI Silder XX GUI Silder	✓ Core Audio Boolean Opera Byte Operator Channelizers	 jamning cell 	0 contral fr 5 central fr 8 central fr 100 central f 10836 central 50 central f 50 central fr 10712 centra 10702 central 6 central fr 6 central fr 6 central f 60 central f 10836 central 10836 central f	requency at 26 requency at 18 requency at 2 l frequency at 2 requency at 2 al frequency at al frequency at requency at 18 requency at 26 requency at 26 requency at 26 requency at 20 requency at 20 requ	62.5 MHz with 15 MHz 663.6 MHz with 20 MH 6645.0 MHz with 20 MH 12167.2 MHz with 11 116.0 MHz with 11 116.0 MHz with 11 12157.4 MHz with 11 12157.4 MHz with 20 MH 45.0 MHz with 20 MH 45.0 MHz with 20 MHz 65.5 MHz with 15 MH 665.0 MHz with 15 MH 760.0 MHz with 10 MH 10.0 MHz with 10 MH 10.0 MHz with 10 MH 10.0 MHz with 10 MH	Iz bandwidth Iz bandwidth BR: bandwidth D MHz bandwidth Iz bandwidth MHz bandwidth Ø MHz bandwidth Iz bandwidth Iz bandwidth Iz bandwidth Iz bandwidth B bandwidth Ø MHZ bandwidth
Coptions Di Jammer, gen enerate Options: WX GUE Variable Di samg, rate ahue: 3M Variable Variable N var, E, gan	WX GUI Silder ID: If gain Label: IF gain Default Value: 10 Minimum: 10 Maximum: 60	WX GUI Slider Di cent_friq abeli Friq afault Value: 1.87420 lioitmum: 5000 anverter: Float	WX GUI Slider ID: rf_gain Labek RF gain Default Value: 10 Minimum: 10 Maximum: 60 Converter: Float	WX GUI Slider ID: bb.gain Label: 88 gain Default Vakes: 10 Minimum: 10 Maximum: 60 Converter i Fliat	K GUI Slider sample, rate bels Sample rate fault Values 188 nimume 2M aximume 20M moverters /Float MX GUI Slider teachwidth	Core Audio Boolean Opera Byte Operator Channelizers Channel Mode	 Jamning cell 	0 central fr 0 central fr 0 central fr 00 central fr 18836 central 18836 central 18712 central 18712 central 18712 central 5 central fr 0 central fr	requency at 26 requency at 21 requency at 22 of frequency at 2 requency at 2 requency at 1 frequency at 1 requency at 18 requency at 26 requency at 26 requency at 20 requency at 20 reque	$\begin{array}{c} 62.5 \ [\text{We}\ \text{with 15} \ \text{We}\ \text{with 20} \ \text{We}\ \text{with 21} \ \text{11} \ \text{10}\ \text{o}\ \text{We}\ \text{with 11} \ \text{11} \ \text{10}\ \text{o}\ \text{We}\ \text{with 11} \ \text{11} \ \text{o}\ \text{We}\ \text{with 11} \ \text{11} \ \text{o}\ \text{We}\ \text{with 12} \ \text{with 11} \ \text{11} \ \text{o}\ \text{We}\ \text{with 12} \ \text{with 12} \ \text{We}\ \text{with 10} \ \text{We}\ \text{We}\ \text{Wi}\ \text{We}\ \text{We}\ \text{We}\ \text{Wi}\ \text{We}\ We$	Iz bandwidth Iz bandwidth NHz bandwidth S bandwidth S bandwidth S bandwidth S bandwidth Iz bandwidth Iz bandwidth Iz bandwidth NHz bandwidth NHz bandwidth Iz bandwidth S bandwidth S bandwidth
Options tjarmar_gen enerate Options: WX GUE Variable tsamg_rate shute: 3M Variable tvar_d_gan	WX GUI Silder ID: If gain Label: IF gain Default Value: 10 Minimum: 10 Maximum: 60	WX GUI Silder br cert_freq abel: Freq abel: 5004 axfmum: 2.26 anværter: Fleat Chil Freq Oth Freq	WX GUI Slider ID: rf.gain Label: RF gain Default Value: 10 Minimum: 10 Maximum: 60 Converter: Float mocom Sink ate (spa): 5M server(HK): 1.8742G	WX GUI Slider ID: bl.gain Label: 88 gain Dafault Valuet 10 Minimum: 50 Converter: Float Will blue blue blue blue blue blue blue Garwetter: Float	XGUI Slider Sarrylk_rate bels Sandyle rate faction Values 358 infimume 254 asstroams 204 wrwerters if loat wrwerters if loat bandwidth	Core Audio Boolean Opera Byte Operator Channelizers Channel Mode Coding Control Port	 jamning cell 	B contral fr 0 contral fr 00 contral fr 10836 contral fr 10836 contral fr 10812 contral 10712 contral 10702 contral fr 00 contral fr 00 contral fr 10836 contral 10836 contral 10826 contral 10826 contral 10712 contral 10712 contral	requency at 26 requency at 21 requency at 2 requency at 2 requency at 3 requency at 8 requency at 8 requency at 8 requency at 26 requency at 26 requency at 2 requency at 2 requency at 2 requency at 3 requency at 8 requency at	62.5 MHz with 15 HH 645.0 MHz with 20 HH 645.0 MHz with 20 HH 71.0 MHz with 10 HH 72.0 MHz with 10 HH 72.0 MHz with 10 HH 72.1 MHz with 11 73.0 MHz with 20 HH 73.0 MHz with 20 HH 73.0 MHz with 21 HH 73.0 MHz with 21 HH 73.0 MHz with 20 HH 73.0 MHz w	Iz bandwidth Hz bandwidth Hz bandwidth Bz bandwidth Ez bandwidth Hz bandwidth Hz bandwidth Iz bandwidth Iz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth
Variabel Var	VX GUI Silder ID: (f_sain Labels IF gain Default Values 10 Minimums 10 Converters Flast Noise Source Noise Source	WX GUI Slider in cent_freq abel: Freq efault Value: 1.87420 ininieum: 5004 laximum: 2.26 anverter: Flaat 048 Sample Ra Chii Freq. Chii Freq.	WX GUI Slider ID: rf_gain Label: RF gain Default Values 10 Maximum: 60 Converter: Float nocom Sink ate (spa): 5M sency (Hz): 1.87420 . Corr. (spm): 0	WX GUI Slider (Dr) bit,gain Label 88 pain Default Waten 10 Minimum 10 Maximum 50 Canverter: Float Wi Kan Kan Kan Kan Kan Kan Kan Kan Kan Kan	IX GUI Slider sample_rate beht Sample rate beht Sample rate admenter Float www.eters Float	Core Audio Boolean Opera Byte Operator Channelizers Channel Mode Coding Control Port Debug Tools	 jamning cell 	B contral fr B central fr B0 central f 100 central f 10036 central 50 central f 10712 central 8 central fr B0 central fr B1836 central 10712 central 10712 central 10722 central	requency at 26 requency at 21 requency at 21 requency at 3 requency at 3 requency at 3 requency at 3 requency at 13 requency at 25 requency at 25 requency at 21 requency at 31 requency at 31 requency at 31 d requency 31 d requ	62.5 MHz with 15 MHz 663.6 MHz with 20 MH 6645.0 MHz with 20 MH 12167.2 MHz with 11 16.0 MHz with 12 MH 1216.0 MHz with 11 15.0 MHz with 20 MH 45.0 MHz with 20 MH 662.5 MHz with 20 MH 663.5 MHz with 20 MH 6645.0 MHz with 20 MH 6645.0 MHz with 20 MH 110.0 MHz with 20 MH 6645.0 MHz with 20 MH 1216.2 with 20 MHz 1217.2 MHz with 20 MH 124.2 with 20 MHz 1217.2 MHz with 20 MH 1214.2 with 20 MHz 1217.2 MHz with 20 MH 1214.2 with 20 MHz with 20 MH 20 MHz with 20 MHz	Iz bandwidth Iz bandwidth NH bandwidth S bandwidth Iz bandwidth Iz bandwidth S bandwidth Iz bandwidth Iz bandwidth Iz bandwidth NH bandwidth Iz bandwidth Iz bandwidth Iz bandwidth Iz bandwidth S bandwidth S bandwidth O MHIz bandwidth
Options Informacyon enerate Options WX GUI Variable Stamp atte share 38 Variable Variable Variable Variable Variable Variable	WX GUI Silder Ibr /f_pain Labeli /F pain Default Values 10 Mainimum 10 Convertient Plait Noise Source Noise Source Noise Source Noise Source	WX GUI Slider beit freq abelt freq afault Values 1.87420 (asomutes 2.00 answetter: Flast Oth Freq Chi Freq Chi Freq Chi Freq	WX GUI Slider ID: rf.gain Labek RF.gain Default Value: 10 Maximum: 10 Converter: Float nocom Sink tate (spa): 34 sency (Hz): 1.87420 Corr. (span): 0 ain (dB): 10	WX GUI Slider ID: bi.guin Labeli Bi guin Default Vaten: 10 Hinhmum: 10 Maxhumin: 0 Garverters Flast W Def Labeli Bi.guin Max Care	XGUI Slider Sarryla, rate bels Sarryla, rate bels Sarryla, rate bels Sarryla, rate XX GUI Slider bendswith bendswith bendswith bendswith bendswith bendswith realt Values 256	Core Audio Boolean Opera Byte Operator Channelizers Channel Mode Coding Control Port	 jamning cell 	<pre>B central fr 0 central fr 00 central fr 00 central fr 10836 centra 00 central fr 10712 centra 11722 central 10787 central fr 00 central fr 00 central fr 00 central fr 00 central fr 10836 central 10712 central 10712 central 0 central fr 20 central fr</pre>	requency at 26 requency at 21 requency at 2 requency at 2 requency at 3 requency at 8 requency at 8 requency at 8 requency at 26 requency at 26 requency at 26 requency at 26 requency at 20 requency at 8 requency at 8	62.5 MHz with 15 HHz 662.5 MHz with 20 HH 6645.0 MHz with 20 HH 12.67.2 MHz with 10 HHz with 10 HHz 11.6.0 MHz with 11 15.0 MHz with 20 HH 15.0 MHz with 20 HH 15.0 MHz with 20 HH 662.5 MHz with 20 HH 16.0 MHz with 20 HH 16.0 MHz with 10 HH 16.0 MHz with 10 HH 870.0 MHz with 10 HH 15.2 MHz with 10 HH 870.4 MHz with 10 HH 870.4 MHz with 10 HH 15.2 MHz with 20 HH 15.2 MHz with 20 HH 15.0 MHz with 20 HHz 15.0 MHz with 20 HH 15.0 MHz with 20 HHz 15.0 MHz with 20 HZ 15.0 MHz with 20 HZ 1	Iz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth D HHz bandwidth Iz bandwidth Hz bandwidth 0 MHz bandwidth 0 MHz bandwidth 0 MHz bandwidth
Variable to same standard to same standard to same standard Variable to var same standard Variable to var same standard Variable to var same standard Variable to var same standard var same st	VX GUI Silder ID: (f_sain Labels IF gain Default Values 10 Minimums 10 Converters Flast Noise Source Noise Source	WX GUI Silder br cart /raq abels Fraq effault Yabes 1.87420 linesuum: 900H sample Ra Chil Frag Chil Frag Chil Frag	WX GUI Slider ID: rf_gain Label: RF gain Default Values 10 Maximum: 60 Converter: Float nocom Sink ate (spa): 5M sency (Hz): 1.87420 . Corr. (spm): 0	WX GUI Silder 100 lb.gain Label 180 pin History 100 Madmum 60 Canverter Flaat We kinder flaat Kinder flaat Warder flaat With the second second second second Kinder flaat With the second second second second second Kinder flaat With the second seco	IX GUI Slider sample_rate beht Sample rate beht Sample rate admenter Float www.eters Float	Core Audio Boolean Opera Byte Operator Channelizers Channel Mode Coding Control Port Debug Tools	 jamning cell 	B contral fr B central fr B0 central f B0 central f B0 central f B0 central f B0 central f B0 central fr B0 central fr B0 central fr B0 central fr B0 central fr B0 central f B1836 central B1836 central f B1826 central f B1826 central f B0 central f B1826 central f B18272 central f B0 central f B0 central f B18272 central B1878 central B1878 central B1878 central f B0 central f	requency at 26 requency at 21 requency at 21 requency at 3 requency at 3 requency at 3 requency at 3 requency at 10 requency at 26 requency at 26 requency at 22 requency at 22 at requency at 2 at 1 requency at 2 at 1 at 1 requency at 2 at 1 at 1 requency at 2 at 1 at 1 at 1 at 1 at 1 at 1 at 1 at 1	62.5 MHz with 15 HHz 645.6 MHz with 20 HH 645.6 MHz with 20 HH 12.67.2 MHz with 10 11.6.0 MHz with 10 HHZ 11.6.0 MHz with 12.0 H 11.5.0 MHz with 12.0 HHZ 45.0 MHz with 20 HHZ 45.0 MHz with 20 HHZ 65.5 MHz with 20 HHZ 65.5 MHz with 20 HHZ 10.0 MHz with 21 H 11.6.0 MHz with 11 HHZ 11.6.0 MHz with 20 HHZ 11.6.0 MHz with 20 HHZ 11.6.0 MHz with 20 HHZ 12.57.4 HHZ with 11 11.5.0 MHz with 20 HHZ 12.5.7 HHZ with 11 11.5.0 MHz with 20 HHZ 12.5.7 HHZ with 11 15.0 MHz with 20 HHZ 15.0 MHZ 15.0 MH	Iz bandwidth Hz bandwidth Hz bandwidth Bz bandwidth Iz bandwidth Hz bandwidth Bz bandwidth D WHz bandwidth Iz bandwidth Iz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth Hz bandwidth Iz bandwidth Iz bandwidth
Voriable Voriable Voriable Voriable Voriable Voriable Voriable Voriable Voriable	WX GUI Silder Ibr /f_pain Labeli /F pain Default Values 10 Mainimum 10 Convertient Plait Noise Source Noise Source Noise Source Noise Source	WX GUI Silder br cart /raq abels Fraq effault Yabes 1.87420 linesuum: 900H sample Ra Chil Frag Chil Frag Chil Frag	WX GUI Slider ID rf.gain Labels PF pain Default Values 10 Maximum 60 Converters Flat nocom Sink tes (spa): 3M wency (Hz): 1.87426 Corr. (pp): 0 ain (dB): 10 ain (dB): 10	WX GUI Silder 100 lb.gain Label 180 pin History 100 Madmum 60 Canverter Flaat We kinder flaat Kinder flaat Warder flaat With the second second second second Kinder flaat With the second second second second second Kinder flaat With the second seco	DX GUI Slider sample, via beh Sample, via beh Sample, via dant Values 200 sakowa 200	Core Audio Boolean Opera Byte Operator Channelizers Control Port Control Port Debug Tools Deprecated Digital Televis	 Janning cell 	e contral fr 5 central fr 60 central f 18036 central f 18036 central f 18712 centra 18712 central 8 central fr 8 central fr 9 central f 9 central f 90 central f 18036 central 18712 centra 18712 centra 18712 central 6 central f 5 central f 5 central f 5 central f 5 central f 5 central f 6 central f 8 central f 7 central f 8 central f 8 central f 9 central f 8 central f 9 central f 8 central f	requency at 26 requency at 11 requency at 11 requency at 11 requency at 11 requency at 11 at frequency at 11 at frequency at 12 requency at 12 requency at 22 requency at 23 requency at 24 requency at 24 requency at 24 requency at 24 requency at 24 requency at 25 requency at 24 requency at 24 requency at 25 requency at 26 requency at 26 requency at 26 requency at 26 requency at 26	62.5 MHz with 15 HHz 645.0 MHz with 20 HH 645.0 MHz with 20 HH 7.10 MHz with 20 HH 7.10 MHz with 20 HH 870.0 MHz with 20 HH 870.0 MHz with 20 HH 7.10 MHz with 20 HH 45.0 MHz with 20 HH 45.0 MHz with 20 HH 7.10 MHz with 10 HH 7.10 MHz with 20 HHz 7.10 MHz with 20 HH 7.10 MHz with 20 HHZ	Iz bandwidth Ez bandwidth Hr bandwidth Hr bandwidth Hr bandwidth Hr bandwidth O MHz bandwidth O MHz bandwidth Iz bandwidth Hr bandwidth Hr bandwidth Hr bandwidth Hr bandwidth Hr bandwidth Hr bandwidth Hr bandwidth Hr bandwidth Iz bandwidth Hr bandwidth Iz bandwidth Iz bandwidth Iz bandwidth
Options It jammar, gan enerate Options WX GUI Variable It sam, state share 30 Variable It sar, state hare 30 Variable It sar, state hare 30 Variable	WX GUI Silder Ibr /f_pain Labeli /F pain Default Values 10 Mainimum 10 Convertient Plait Noise Source Noise Source Noise Source Noise Source	WX GUI Silder icent/req bebl: Freq feall Waker: 127420 linkiwams 2004 laskforman 2.26 anverter: Flast Cho: Freq Cho: Freq C	WX GUI Slider ID rf.gain Labels PF pain Default Values 10 Maximum 60 Converters Flat nocom Sink tes (spa): 3M wency (Hz): 1.87426 Corr. (pp): 0 ain (dB): 10 ain (dB): 10	WX GUI Silder 100 lb.gain Label 180 pin History 100 Madmum 60 Canverter Flaat We kinder flaat Kinder flaat Warder flaat With the second second second second Kinder flaat With the second second second second second Kinder flaat With the second seco	DX GUI Slider sample, via beh Sample, via beh Sample, via dant Values 200 sakowa 200	Core Audio Boolean Opera Byte Operator Channel Mode Coding Control Port Debug Tools Deprecated Digital Televis Equalizers	 Jamaing cell 	e central fr 5 central fr 60 central f 10836 central f 10836 central f 10712 central 10712 central 6 central fr 8 central fr 9 central fr 9 central f 1000 central 1000 central 1000 central 1072 central 1072 central 6 central f 10712 central 6 central f 6 central f 6 central f 8 central f 9 central f	requency at 26 requency at 18 requency at 18 requency at 11 requency at 11 requency at 11 requency at 11 requency at 11 requency at 26 requency at 26 requency at 26 requency at 21 requency at 20 requency at 20 requency at 20 requency at 26 requency at 26 requen	62.5 MHz with 15 MH 64.5 MHz with 20 MH 64.6 MHz with 20 MH 64.6 MHz with 20 MH 64.6 MHz with 20 MH 10.6 MHz with 20 MH 10.6 MHz with 20 MH 11.5 MHz with 20 MH 64.5 MHz with 20 MH 64.5 MHz with 20 MHZ with 20 MH 64.5 MHz with 20 MHZ with 20 MHZ 10.6 MHZ with 20 MHZ with 20 MHZ 10.5 MHZ with 20 MHZ with 20 MHZ 10.5 MHZ with 20 MHZ with 20 MHZ 10.5 MHZ with 20 MHZ with 20 MHZ 10.7 M	Ir bandwidth Bre bandwidth Bre bandwidth D Mrt bandwidth D Mrt bandwidth Ir bandwidth D Mrt bandwidth D Mrt bandwidth Ir bandwidth Ir bandwidth Bre bandwidth Bre bandwidth Bre bandwidth Ir bandwidth
Options h) Jaromez,gen encrete Options. WX OUI Variable have: 30 Norse, fyren have: 187420 Variable have: 187420 Variable have: 187420 Variable	WX GUI Silder Ibr /f_pain Labeli /F pain Default Values 10 Mainimum 10 Convertient Plait Noise Source Noise Source Noise Source Noise Source	WX GUI Silder icent/req bebl: Freq feall Waker: 127420 linkiwams 2004 laskforman 2.26 anverter: Flast Cho: Freq Cho: Freq C	WX GUI Slider ID: rf_gain Labels PF pain Default Value: 10 Minisum: 10 Maximum: 50 Converter: Flaat moccom Sink tet (spa): 2M moccom Sink tet (spa): 2M moccom Sink tet (spa): 2M moccom Sink id (dB): 10 ain (dB): 10 ain (dB): 10 ma: 1 Minisum: 10 Minisum: 10	WX GUI Silder 100 lb.gain Label 180 pin History 100 Madmum 60 Canverter Flaat We kinder flaat Kinder flaat Warder flaat With the second second second second Kinder flaat With the second second second second second Kinder flaat With the second second second second second second second second seco	DX GUI Slider sample, via beh Sample, via beh Sample, via dant Values 200 sakowa 200	Core Audio Boolean Opera Byte Operator Channelizers Control Port Control Port Debug Tools Deprecated Digital Televis	 Jamning cell 	e contral fr 5 central fr 60 central f 18836 central 1972 central 1972 central 8 central f 8 central fr 8 central fr 9 central 9 central 19836 central 9 central 19836 central 1972 central 1972 central 1972 central 1972 central 1973 central 6 central 1973 central 9 central 7 central 7 central 9 central 9 central 7 central 9 c	requency at 26 requency at 11 requency at 11 requency at 11 requency at 11 requency at 11 requency at 12 requency at 12 requency at 26 requency at 26 requency at 26 requency at 20 requency at 21 requency at 25 requency at 25 requen	$\begin{array}{c} 62.5 \ \mathrm{ME} \ \mathrm{virth} \ 15 \ \mathrm{MH} \ \mathrm{virth} \ 10 \ \mathrm{MH} \ 10 \ 10 \ \mathrm{MH} \ 10 \ 10 \ 10 \ 10 \ 10 \ 10 \ 10 \ 1$	Ir bandwidth Bre Dandwidth Bre Dandwidth Bre Dandwidth Bre Dandwidth Bre Dandwidth B MRC bandwidth B MRC bandwidth Ir bandwidth Ir bandwidth Ir bandwidth B MRC bandwidth B MRC bandwidth B MRC bandwidth Ir bandwidth B MRC bandwidth B MRC bandwidth Ir bandwidth B MRC bandwidth Ir bandwidth B MRC bandwidth Ir bandwidth Ir bandwidth Ir bandwidth Ir bandwidth Ir bandwidth
Options Diplement gen Diplement gen Market State Variable Disang zete Disang	WX GUI Silder Ibr /f_pain Labeli /F pain Default Values 10 Mainimum 10 Convertient Plait Noise Source Noise Source Noise Source Noise Source	VX GUI Slider h carf Jon bah Trop efruit Valen 1.8740 inimum 500 bahman 2.26 anverter Flast Colo Free Colo IF G Colo IF G	WX GUI Slider ID: rf_gin Label: RF gain Label: RF gain Default Value: 10 Mainsum: 10 Maximum: 00 Converter: Flaat nocom Sink te (spa): 34 ency (Hz) 1.87420 .corr. (gpm): 0 ain (dB): 10 ain (dB): 10 mm: 1 heidth (Hz): 10H	WX GUI Silder 100 lb.gain Label 180 pin History 100 Madmum 60 Canverter Flaat We kinder flaat Kinder flaat Warder flaat With the second second second second Kinder flaat With the second second second second second Kinder flaat With the second second second second second second second second seco	DX GUI Slider sample, via beh Sample, via beh Sample, via dant Values 200 sakowa 200	Core Audia Audia Bolean Oper Byte Operator Channel Mode Control Port Debug Tools Deprecated Digital Televis Equalizers Error Coding	 Jamning cell 	e central fr 5 central fr 60 central f 10836 central f 10836 central f 10712 central 10712 central 10712 central fr 8 central fr 8 central fr 9 central f 90 central f 10836 central 10712 centra 1072 central 1072 central 1072 central 1072 central 1072 central 1073 central 6 central f 8 central f 9 central f 8 central f 9 central f 9 central f 9 central f 9 central f 9 central f 9 central f	requency at 26 requency at 21 requency at 21 requency at 21 requency at 21 requency at 11 requency at 21 requency at 21 requency at 26 requency at 26 requency at 21 requency at 26 requency at 26 requen	$ \begin{array}{c} 62.5 & \text{Mix} \text{ with } 15 & \text{Mix} \\ 70.0 & \text{Mix} \text{ with } 20 & \text{Mix} \\ 70.0 & \text{Mix} \text{ with } 20 & \text{Mix} \\ 70.0 & \text{Mix} \text{ with } 20 & \text{Mix} \\ 70.0 & \text{Mix} \text{ with } 10 & \text{Mix} \\ 70.0 & \text{Mix} \text{ Wix} \\ 70.0 & \text{Mix} \text{ Wix} \\ 70.0 & \text{Mix} \\ 70.0 &$	Iz bandudth Ez bandudth He bandudth He bandudth Brekadauth Brekadauth Brekadauth Brekadauth B Web bandudth He bandudth He bandudth He bandudth B Web bandudth B Web bandudth B Web bandudth B Web bandudth B Web bandudth Iz bandudth B Web bandudth Iz bandudth He bandudth
Options Instructure Deptions Instructure Deptions Instructure Deptions Instructure Deptions Instructure Deptions	Victor State Victor	VX GUI Slider h card_ha bell Fel fedri Vaker 1.87420 loknown 2001 audmmit 250 noverter Field Ohi Fea Choi Rea Choi Rea Choi Rea Choi Rea Choi Rea	WX GUI Slider 10 rf_pin Label RF pin Label RF pin Molecum 10 Molecum 10 Genverter: Flux noc com Sink tei (spal: 34 wenry (Net) 1.8740 .corr. (span): 34 wenry (Net) 1.8740 .corr. (span): 34 wenry (Net) 1.8740 .corr. (span): 34 .corr. (span): 34	WX GUI Silder 100 lb.gain Label 180 pin History 100 Madmum 60 Canverter Flaat We kinder flaat Kinder flaat Warder flaat With the second second second second Kinder flaat With the second second second second second Kinder flaat With the second second second second second second second second seco	DX GUI Slider sample, via beh Sample, via beh Sample, via dant Values 200 sakowa 200		<pre>c Jamming cell Jamming cell</pre>	e central fr 5 central fr 60 central f 10836 central 10712 central 10712 central 10712 central 60 central fr 60 central 10836 central 10712 central 10712 central 10712 central 10712 central 10712 central 10712 central 10712 central 10712 central 6 central 10712 central 10712 central 6 central 10712 central 10720 central 10730 central 10730 central 10730 central 10730 central 10836 central 10836 central 10836 central 10836 central 10836 central 10836 central 10836 central 10830 central 108300 central 108300 central 108300 central 108300 centra	requency at 26 requency at 10 requency at 11 requency at 11 requency at 11 requency at 11 requency at 11 requency at 12 requency at 12 requency at 26 requency at 26 requen	$\begin{array}{c} 62.5 & \text{Mex} with 15 & \text{Me} \\ 62.5 & \text{Mex} with 2 & \text{oth} 30 \\ 63.6 & \text{gell the stath 20 & \text{me} \\ 64.6 & \text{gell the stath 20 & \text{me} \\ 64.6 & \text{gell the stath 20 & \text{me} \\ 10.6 & \text{me} & \text{stath 10 & \text{me} \\ 10.6 & \text{me} & \text{stath 11 & \text{me} \\ 10.5 & \text{me} & \text{stath 11 & \text{me} \\ 10.5 & \text{me} & \text{stath 11 & \text{me} \\ 10.5 & \text{me} & \text{stath 12 & \text{me} \\ 10.5 & \text{me} & \text{me} \\ 10.5 & me$	Iz bandudith Iz bandudith Iz bandudith Iz bandudith Iz bandudith Iz bandudith Iz bandudith Iz bandudith I Iz bandudith Iz bandudith
Options Options Options Options Options Options Options Options Options Option	Vic Cut Slider Wic Cut Slider Wic Cut Slider Wic Cut Slider Wic Cut Slider Wich States Works Struct Annumer Moles Struct Anglinules: 30 Seed: 0 XULERC Server	VX GUI Slider h (art/jok shch irros efruit Vaden: 1.87400 inimums 5004 ladmam: 2.26 anverter: Fiast Ch0: Free, Ch0: Free, Ch0: FG Ch0:	WX GUI Slider ID: rf_gain Label: RF gain Label: RF gain Default Value: 10 Mainsum: 10 Maximum: 00 Converter: Flaat nocom Sink te (spa): 34 ency (Hz) 1.87420 .corr. (gpm): 0 ain (dB): 10 ain (dB): 10 mma: 1 heidth (Hz): 10H	WX GUI Silder 100 lb.gain Label 180 pin History 100 Madmum 60 Canverter Flaat We kinder flaat Kinder flaat Warder flaat With the second second second second Kinder flaat With the second second second second second Kinder flaat With the second second second second second second second second seco	DX GUI Slider sample, via beh Sample, via beh Sample, via dant Values 200 sakowa 200	Core Audia Audia Bolean Oper Byte Operator Channel Mode Control Port Debug Tools Deprecated Digital Televis Equalizers Error Coding	 Jamning cell 	e contral fr 5 contral fr 60 contral f 10836 contral 500 contral f 10836 contral 60 contral f 10787 contra 8 contral fr 80 contral fr 80 contral fr 80 contral f 10836 contral 110836 contral 110836 contral 10712 contra 10712 contra 10725 contral 5 contral f 8 contral f 9 contral f	requency at 26 requency at 18 requency at 18 requency at 18 requency at 18 requency at 10 requency at 11 requency at 11 requency at 26 requency at 26 requen	$ \begin{array}{c} 62.5 & \text{Mez} \text{ with } 15 & \text{Mez} \text{ with } 201 & \text{Mez} \text{ with } 101 & \text{Mez} \text{ Mez} \text{ with } 101 & \text{Mez} \text{ with } 101 & $	Iz bandudith Iz bandudith Bandudith B WEb bandudith B WEb bandudith B WE bandudith B WE bandudith Iz bandudith Iz bandudith Iz bandudith B WEb bandudith
Options Options Options Options Options Options Options Options Options Option	VX CUI Slider Wirk CUI Slider Wir	VX GUI Slider h (art/jok shch irros efruit Vaden: 1.87400 inimums 5004 ladmam: 2.26 anverter: Fiast Ch0: Free, Ch0: Free, Ch0: FG Ch0:	WX GUI Silder 10 r (r jain Lokeli 87 pain Lokeli 87 pain Lokeli 87 pain Lokeli 10 Maximum 50 Converters Flast ency (Hz) 1.8720 corr. (apn): 0 ain (dB): 10 ain	WX GUI Silder 100 lb.gain Label 180 pin History 100 Madmum 60 Canverter Flaat We kinder flaat Kinder flaat Warder flaat With the second second second second Kinder flaat With the second second second second second Kinder flaat With the second second second second second second second second seco	DX GUI Slider sample, via beh Sample, via beh Sample, via dant Values 200 sakowa 200		<pre>c Jamming cell Jamming cell</pre>	<pre>0 contral fr 9 contral fr 0 contral fr 0 contral fr 00 contral fr 10035 contral fr 10032 contral fr 9 contral fr 9 contral fr 9 contral fr 0 contral fr</pre>	requency at 26 enquency at 26 frequency at 21 frequency at 21 (1) frequency at 27 (1) frequency at 28 frequency at 28 enquency at 28 enquency at 28 enquency at 26 enquency	62.5 Mez with 15 MeV 70.6 Mez with 20 MeV 64.5 MeV with 20 MeV 64.5 MeV with 20 MeV 16.6 MeV with 10 MeV 1870.6 MeV with 10 MeV 1870.6 MeV with 11 MeV 1870.6 MeV with 11 MeV 42.5 MeV with 20 MeV 42.6 MeV with 20 MeV 42.6 MeV 42.6 MeV with 20 MeV 42.6 MeV with 20 MeV 42.6 MeV 42.6 MeV 42.6 MeV 42.6 MeV 42.6 MeV 42.6 MeV 42.6 MeV 42.6 MeV 42.6 MeV 42.6	Iz bandudith Iz bandudith He bandudith He bandudith He bandudith He bandudith He bandudith He bandudith He bandudith Iz bandudith Iz bandudith He bandudith Iz bandudith He bandudith
Options Definitions Definitions Definitions	VC CUI Slider Wire and a state of the state of t	VX GUI Silder h cert/ing beh/h res fruit Vehrer: 187420 landmann: 5004 landmann: 225 moverter 1818 Chi Free Chi Free	WX GUI Silder 10 r (r jain Lokeli 87 pain Lokeli 87 pain Lokeli 87 pain Lokeli 10 Maximum 50 Converters Flast ency (Hz) 1.8720 corr. (apn): 0 ain (dB): 10 ain	WX GUI Silder 100 lb.gain Label 180 pin History 100 Madmum 60 Canverter Flaat We kinder flaat Kinder flaat Warder flaat With the second second second second Kinder flaat With the second second second second second Kinder flaat With the second second second second second second second second seco	DX GUI Slider sample, via beh Sample, via beh Sample, via dant Values 200 sakowa 200	✓ Core	<pre>c Jamming cell Jamming cell</pre>	<pre>0 contral fr 0 contral fr</pre>	requency at 26 requency at 26 requency at 21 11 frequency at 21 frequency at 2	$ \begin{array}{c} 62.5 & \text{Mez} \text{ with } 15 & \text{Mez} \text{ with } 20 & \text{Mez} \text{ with } 10 & \text{Mez} $	Iz bandudith Iz bandudith Brandudith Brandudith Brandudith Brandudith Brandudith Brandudith Iz bandudith Iz bandudith Iz bandudith Iz bandudith Iz bandudith Brandudith Brandudith Brandudith Iz bandudith Brandudith Iz bandudith Iz bandudith
Options Diplamente que Diplamente de la construction Variable Nancy de la construction Variable Di sang de la construction Variable Variab	XX CUI Slider W. Cui S	VX GUI Silder h cert/ing beh/h res fruit Vehrer: 187420 landmann: 5004 landmann: 225 moverter 1818 Chi Free Chi Free	WX GUI Silder 10 r (r jain Lokeli 87 pain Lokeli 87 pain Lokeli 87 pain Lokeli 10 Maximum 50 Converters Flast ency (Hz) 1.8720 corr. (apn): 0 ain (dB): 10 ain	WX GUI Silder 100 lb.gain Label 180 pin History 100 Madmum 60 Canverter Flaat We kinder flaat Kinder flaat Warder flaat With the second second second second Kinder flaat With the second second second second second Kinder flaat With the second second second second second second second second seco	DX GUI Slider sample, via beh Sample, via beh Sample, via dant Values 200 sakowa 200	Core Audio Boolean Operi Byte Operator Control Port Control Port Debug Tools Deprecated Digital Televis Deprecated Digital Televis Equalizers Error Coding FiCe Operators	<pre>c Jamming cell Jamming cell</pre>	<pre>0 contral fr 0 contral fr</pre>	requency at 26 requency at 26 requency at 21 11 frequency at 21 frequency at 2	62.5 MEZ with 15 MEM 42.5 MEZ with 20 MEM 24.5 A 20 MEM	Iz bandudith Iz bandudith Brandudith Brandudith Brandudith Brandudith Brandudith Brandudith Iz bandudith Iz bandudith Iz bandudith Iz bandudith Iz bandudith Brandudith Brandudith Brandudith Iz bandudith Brandudith Iz bandudith Iz bandudith

IMSI catching on 4G via registration failures

When an unknown user tries to register

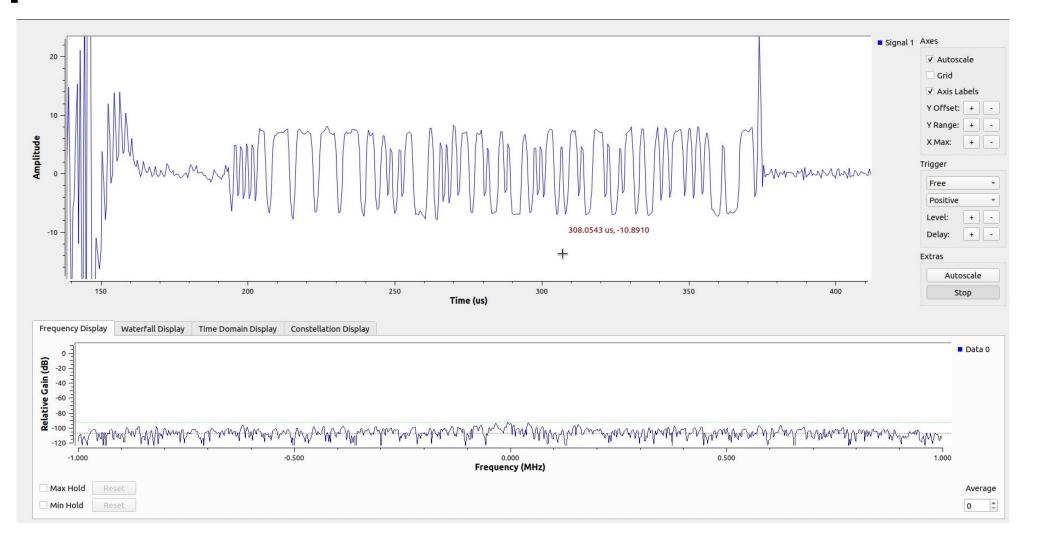
```
Received Initial UE message -- Attach Request
Attach request -- M-TMSI: 0xf1e003d0
Attach request -- eNB-UE S1AP Id: 1
Attach request -- Attach type: 2
Attach Request -- UE Network Capabilities EEA: 11110000
Attach Request -- UE Network Capabilities EIA: 01110000
Attach Request -- MS Network Capabilities Present: true
PDN Connectivity Request -- EPS Bearer Identity requested: 0
PDN Connectivity Request -- Procedure Transaction Id: 3
PDN Connectivity Request -- ESM Information Transfer requested: true
UL NAS: Received Identity Response
```

IMSI catching on 4G via registration failures

- Several RF devices are
- vulnerable to keystroke injection:
 - Mouse, Keyboard, Presenters
 - etc.
- Cause:
 - No confidentiality when sending keystrokes
 - Or no anti-replay
 - Or pairing key sent in clear
 - etc.



RF pattern after FSK demod

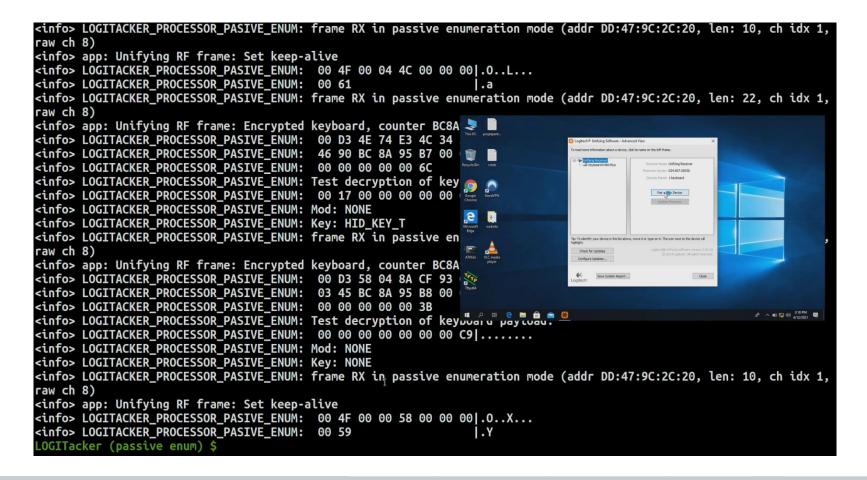


Publications and tools

- MouseJack: <u>https://www.mousejack.com/</u>
- LOGITacker: <u>https://github.com/RoganDawes/LOGITacker</u>
- Research paper on mouses and keyboards by Matthias Deeg and Gerhard Klostermeier: <u>https://www.syss.de/fileadmin/dokumente/Publikationen/2017/2017_06_01_of-mice-and-keyboards_paper.pdf</u>
- And lot of other researches...

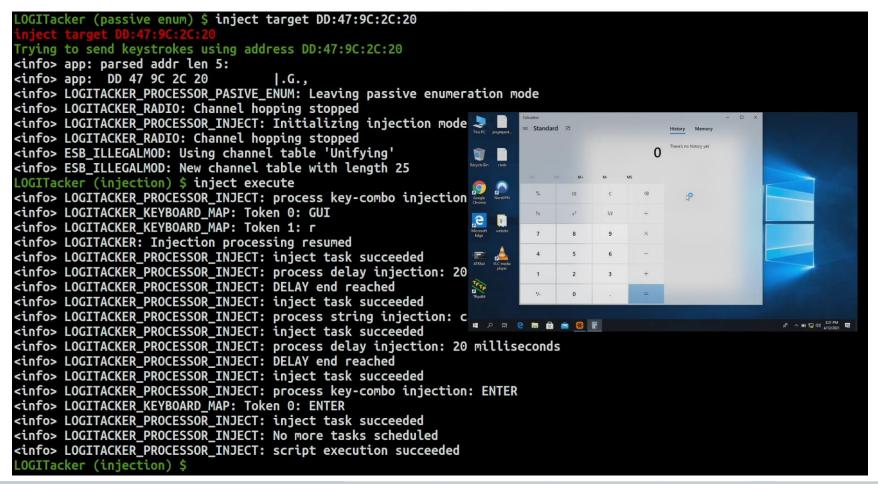
Hijacking a keyboard

Sniffing keystrokes



Hijacking a keyboard

Popping a shell



Conclusion

Conclusion

To conclude

- Sometimes same techniques as offensive ones
- Wireless RF spy bugs are difficult to track
- A strict mapping of all RF devices is mandatory to spot them
- Introducing RF legit devices \rightarrow turned against us
- Further work \rightarrow identification of RF signal using Machine Learning \rightarrow incoming in our next offers
- If you want to know more about our detection, or other products, or trainings:





Thank You

Please contact us:

•••

- ⊠ contact@penthertz.com
- 🕸 +33 1 88 33 94 15
- penthertz.com

Watch us on You Tube

