

# Spy vs. Spy

## A modern study of mic bugs operation and detection

ЗУС.  
БУШАГ!

Veronica Valeros

@verovaleros

Sebastian Garcia

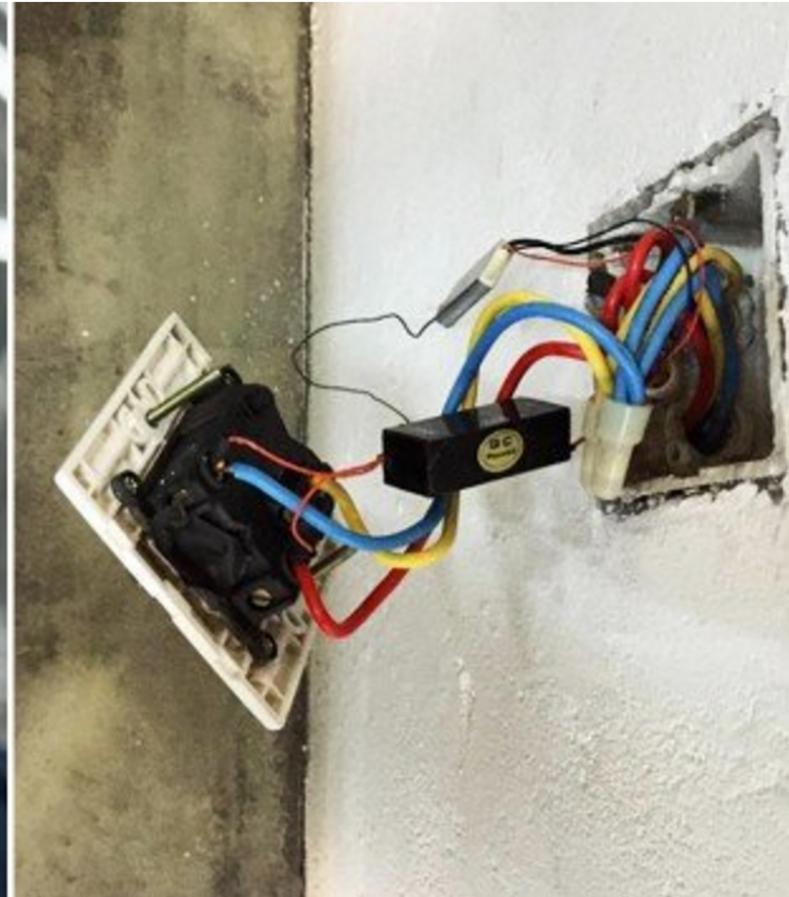
@eldracote

MatesLab Hackerspace

[bit.ly/Spy34c3](http://bit.ly/Spy34c3)



# Audio eavesdropping is a threat



BELJING - Dissident Chinese artist Ai Weiwei has posted photos on his Instagram account that suggest listening devices were planted in his Beijing studio.

# Audio eavesdropping is a threat

Ecuador

## Snowden row intensifies as hidden bug found in Ecuador's embassy

Ecuadorean minister threatens to reveal perpetrators after device discovered during meeting over Assange



This article is 4 years old

Nick Hopkins and Sam Jones

Wednesday 3 July 2013 21.14 BST



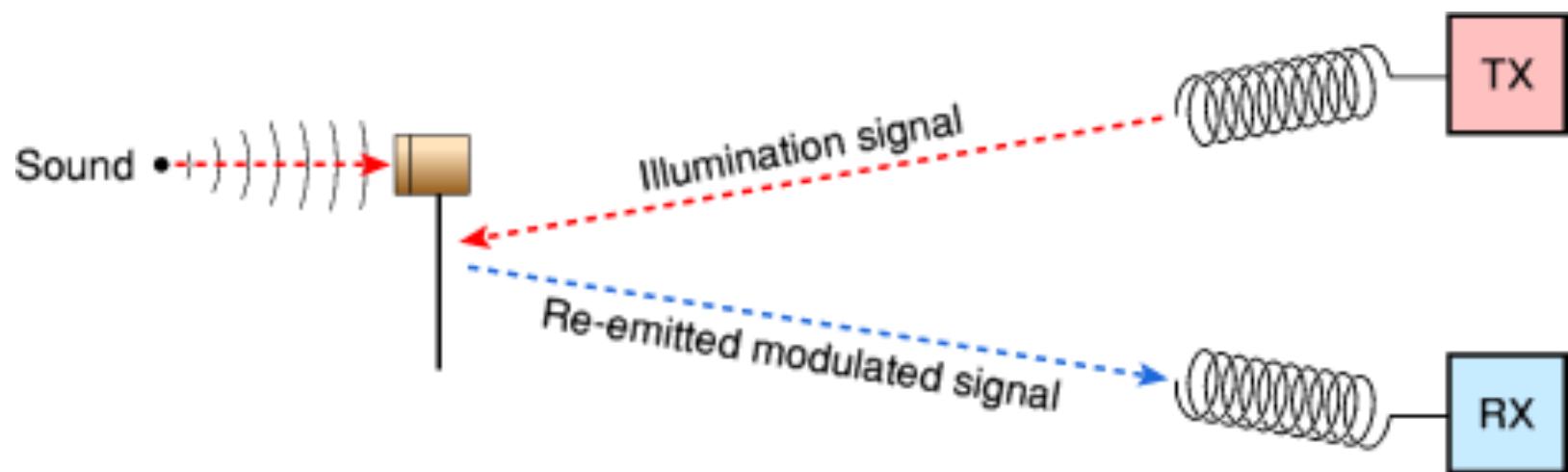
Ricardo Patiño, Ecuador's foreign minister, says the device was discovered a fortnight ago when he was in the UK to discuss Julian Assange. Photograph: Beretta/Sims/Rex Features

A brief tour through the  
last century FM mic bugs

# History: The Thing



# History: The Thing



# History: KGB bug

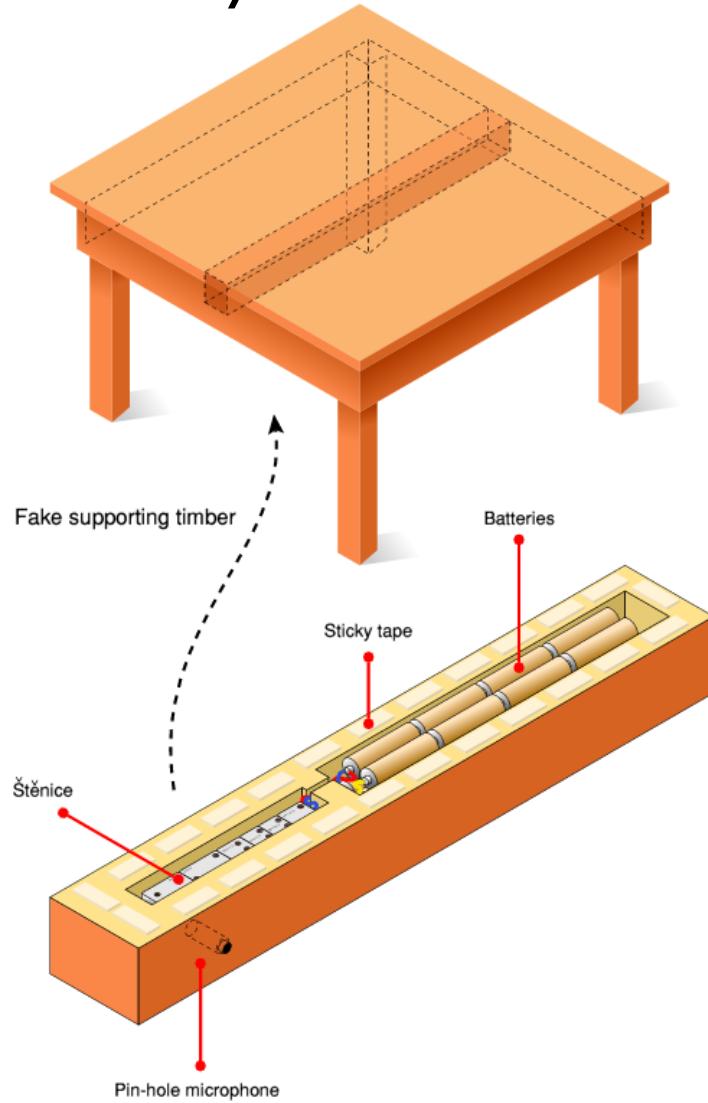


# History: TI-574A



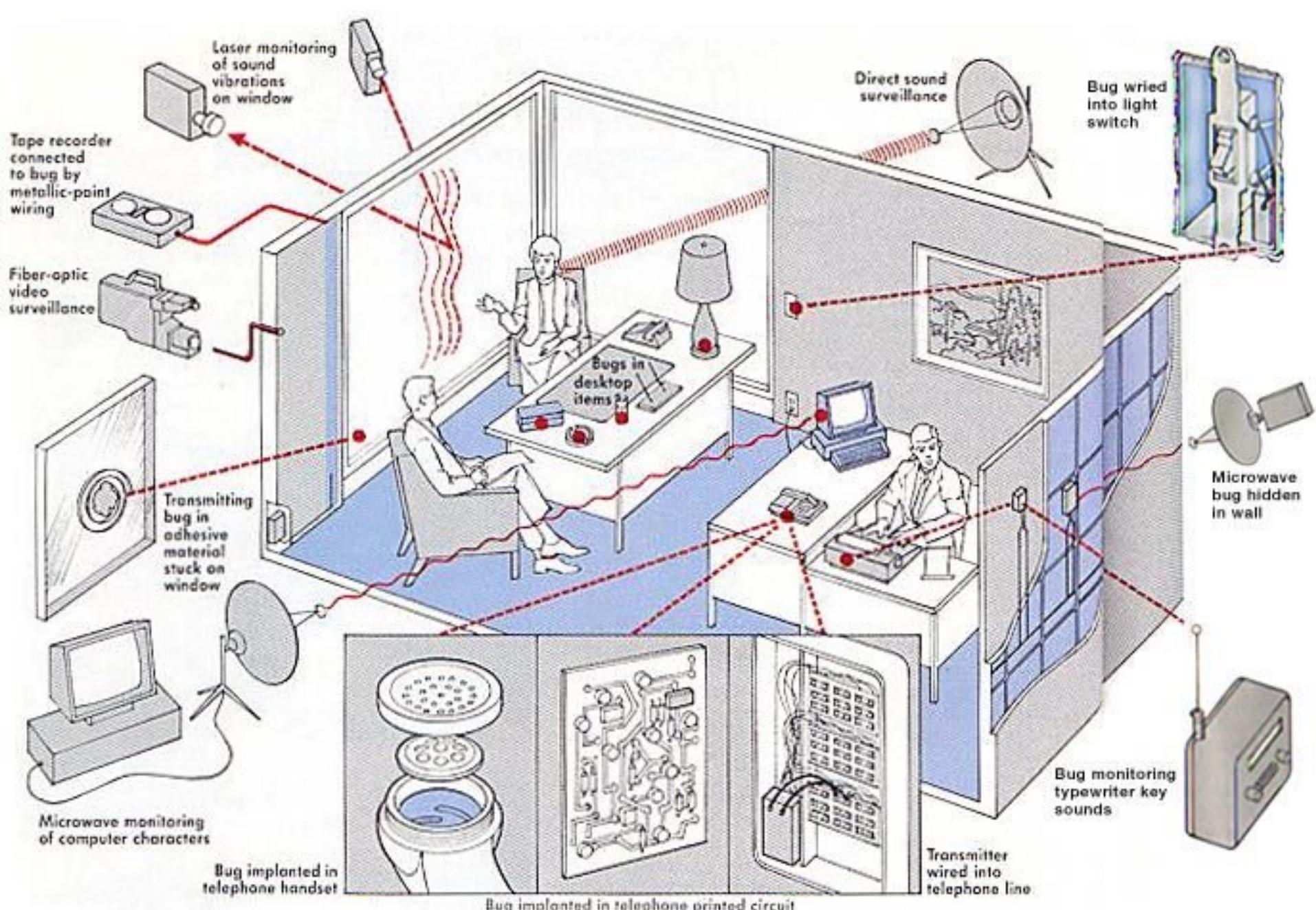
Cryptomuseum  
cryptomuseum.com

# History: TI-574A



# History: OPEC





The ordinary office is an information sieve for a good spy. Above are just some of the ways surveillance can take place.

# Mic Technology Advances

## From lasers in the air to malware



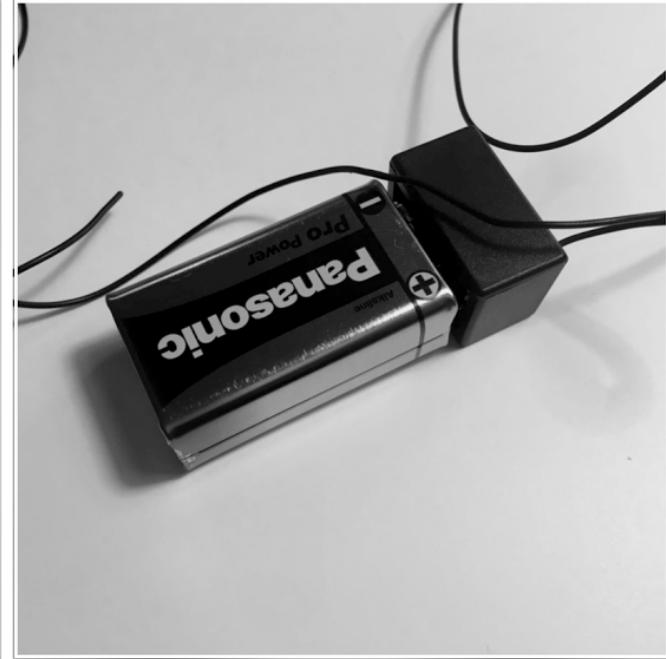
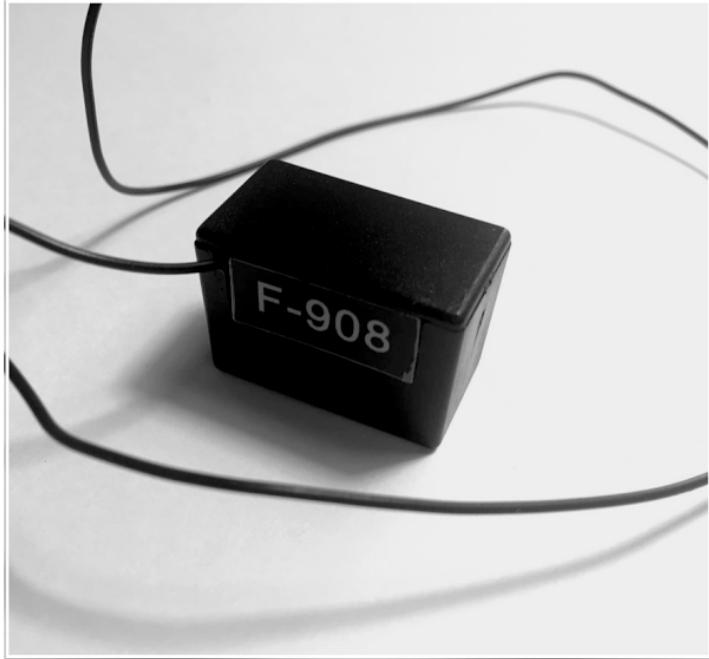
**FINFISHER SPYWARE**  
Suspected Government Users In 2015

Citizen Lab 2015  
Bill Marczak, John Scott-Railton,  
Adam Senft, Irene Poerntano & Sarah McKune

# Lets Experiment!

FM and GSM commercially-available wireless stationary microphone bugs

# F908



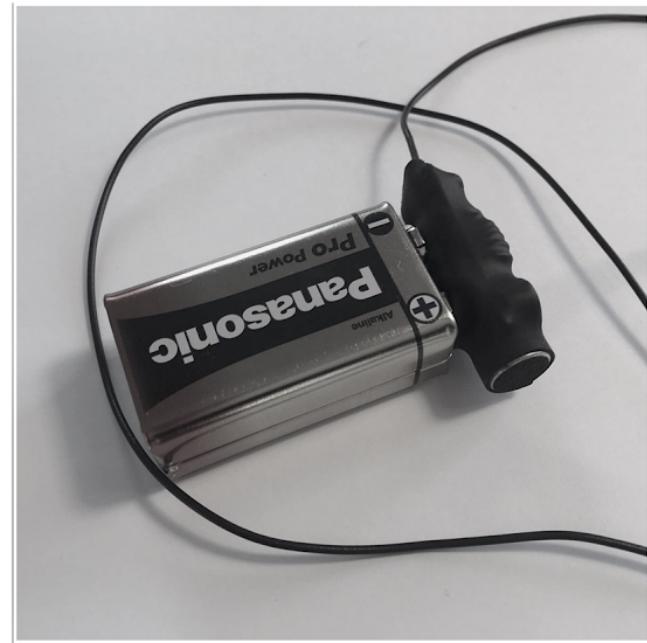
Frequency: 113.5MHz

Range: 500m

Battery: 9v

Price: 33 USD

# MicroSpy



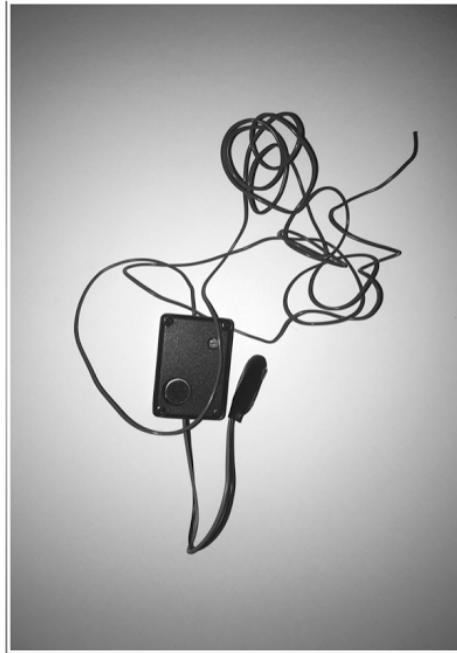
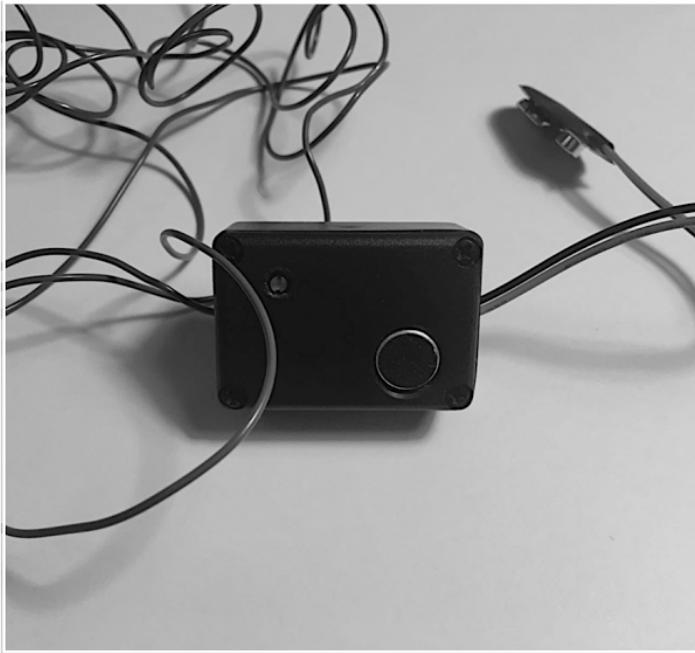
Frequency: 102MHz

Range: 500m

Battery: 9v

Price: 15 USD

# Ear-1



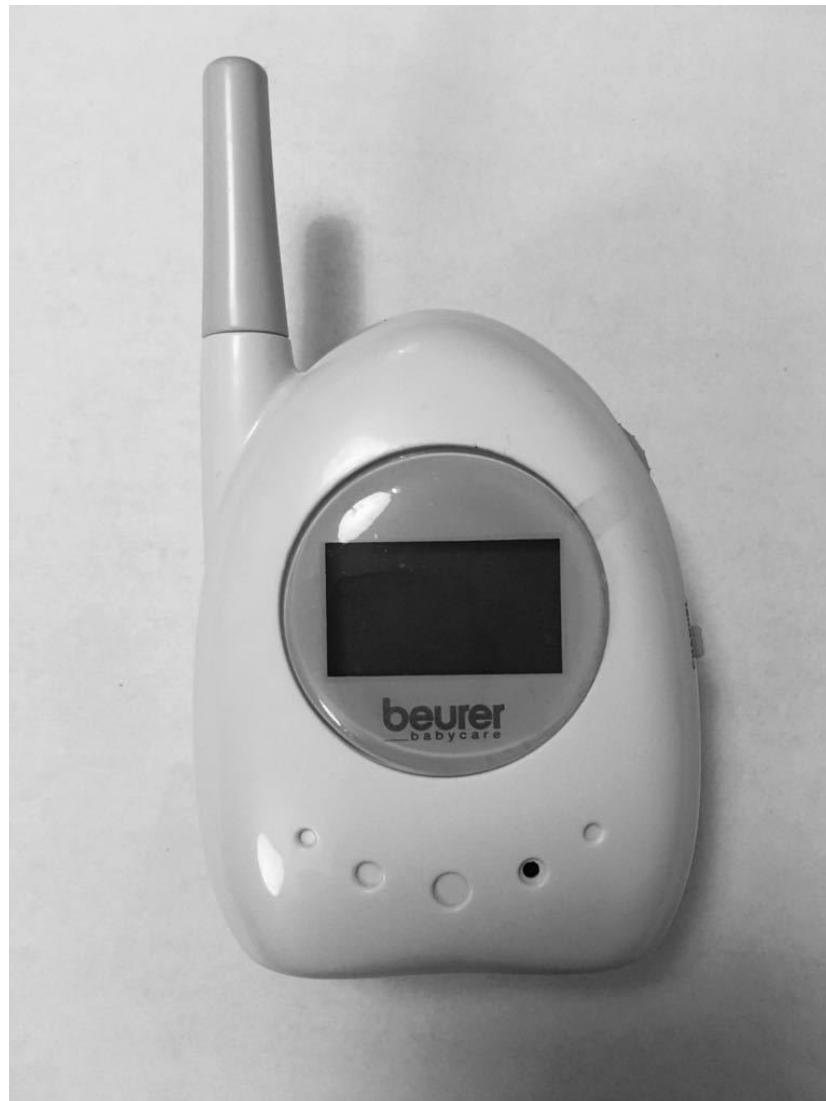
Frequency: 102.2MHz

Range: 500m

Battery: 9v

Price: 18 USD

# Beurer BY04



Frequency:

864MHz

Range:

800m

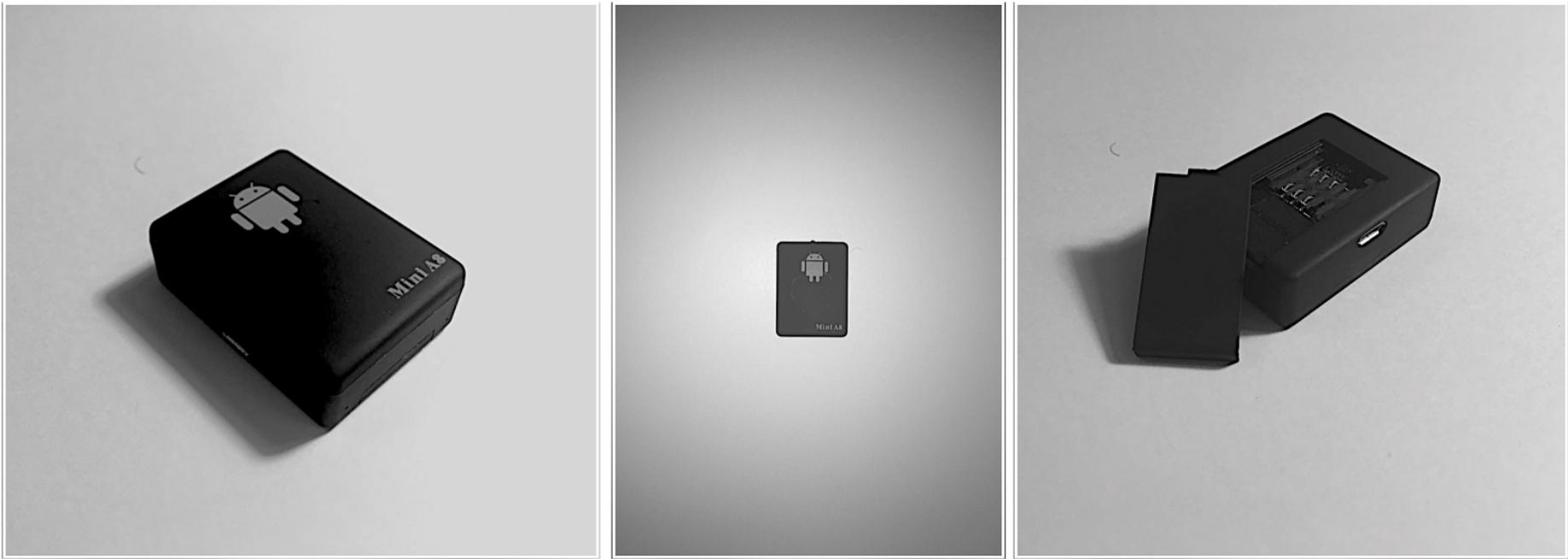
Battery:

3x AAA

Price:

65 USD

# Mini A8



Frequency: EU GSM

Range: world-wide

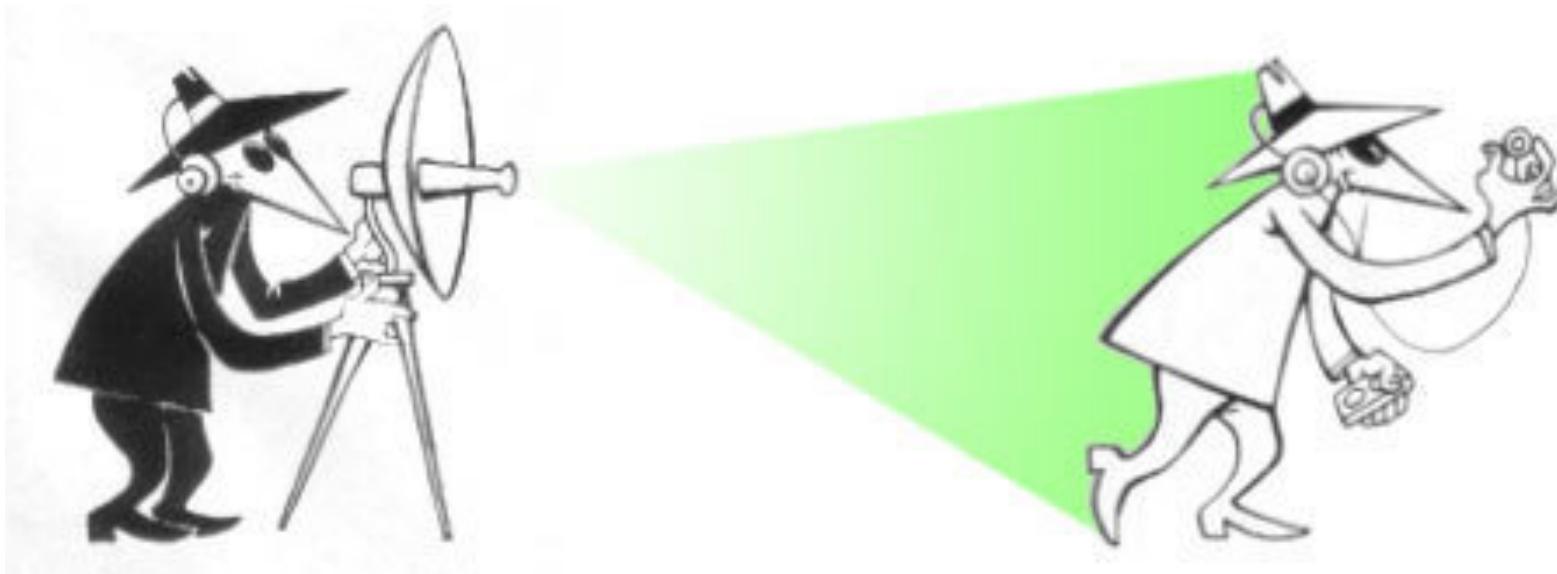
Battery: li-ion 3v

Price: 9.29 USD

# Comparison

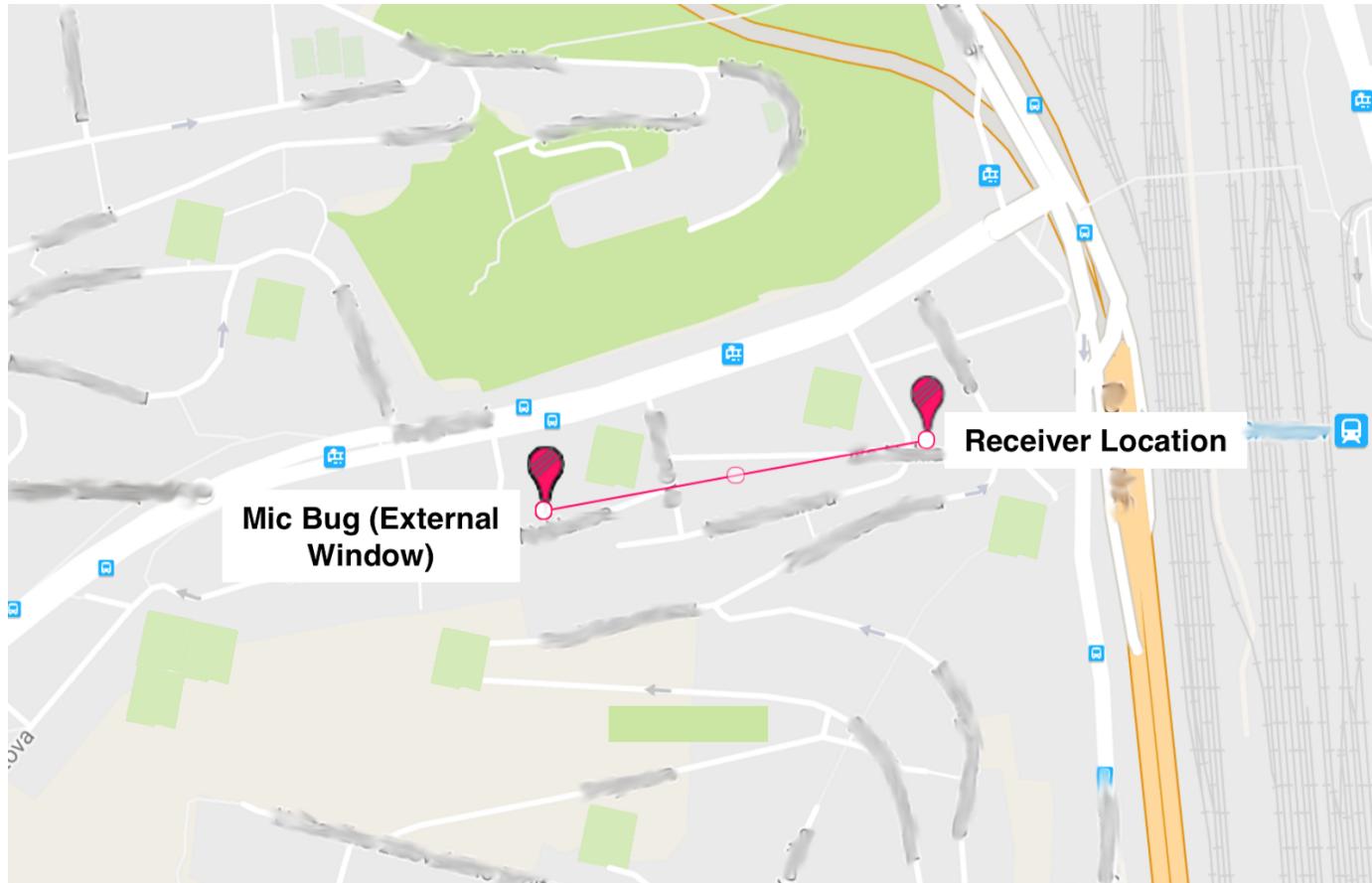
<b>Device</b>	<b>Type</b>	<b>Frequency</b>	<b>Range</b>	<b>Battery</b>	<b>Price</b>
MicroSpy	Mic Bug	102MHz	500m	9v battery	15 USD
F-908	Mic Bug	113.5MHz	500m	9v battery	33 USD
EAR-1	Mic Bug	102.2MHz	500m	9v battery	18 USD
Beurer BY 84	Baby Monitor	864MHz	800m	3x AAA	65 USD
MiniA8	GSM bug /tracker	EU GSM	worldwide	3.7V 500mAh Li-ion	9.29 USD

# Listening Experiments



# Listening Experiments

No need for a van in front of your house



# Listening Experiments

Mic Bug Location	Receiver Location	Distance	Quality	Target
$T_1$	$R_1$	0.30Km	4/5	20cm from mic bug
$T_1$	$R_2$	0.32Km	4/5	20cm from mic bug
$T_1$	$R_3$	0.29Km	3/5	20cm from mic bug
$T_1$	$R_4$	0.23Km	4/5	20cm from mic bug
$T_1$	$R_5$	0.14Km	5/5	20cm from mic bug
$T_1$	$R_6$	0.07Km	5/5	20cm from mic bug
$T_1$	$R_7$	0.18Km	5/5	20cm from mic bug
$T_1$	$R_8$	0.31Km	3/5	20cm from mic bug
$T_1$	$R_9$	0.30Km	5/5	20cm from mic bug
$T_1$	$R_{10} = T_1$	15m	5/5	5m from mic bug

# Geolocation Remarks

- Attackers need to be close
  - Good for you, filters your attackers
  - Bad for them, they need to be close
  - Bad for you, they **are** close
- Nobody can help from the Internet
  - Bad for you

# Autonomy Validation

Device	Advertised Battery Autonomy	Autonomy Validation
MicroSpy	168 hours	Lower than advertised
F-908	-	Lower than the rest
EAR-1	100 hours	Accurate
Beurer BY 84	22 hours	Lower than advertised
MiniA8	2 hours	Accurate

# Comparison with Malware

- A successful malware infection is not guaranteed
- Malware leaves traces. Others can find the attack.
- People from the Internet can help with Malware

# Comparison with non commercial

- Battery vs. electricity
- Transmit vs. storage
- One-time conversation vs. all the time
- One time access vs. continuous access

Contact a company if you are  
in a life-threatening situation.

# Salamandra

SDR-based, free software detection  
and location of hidden microphones

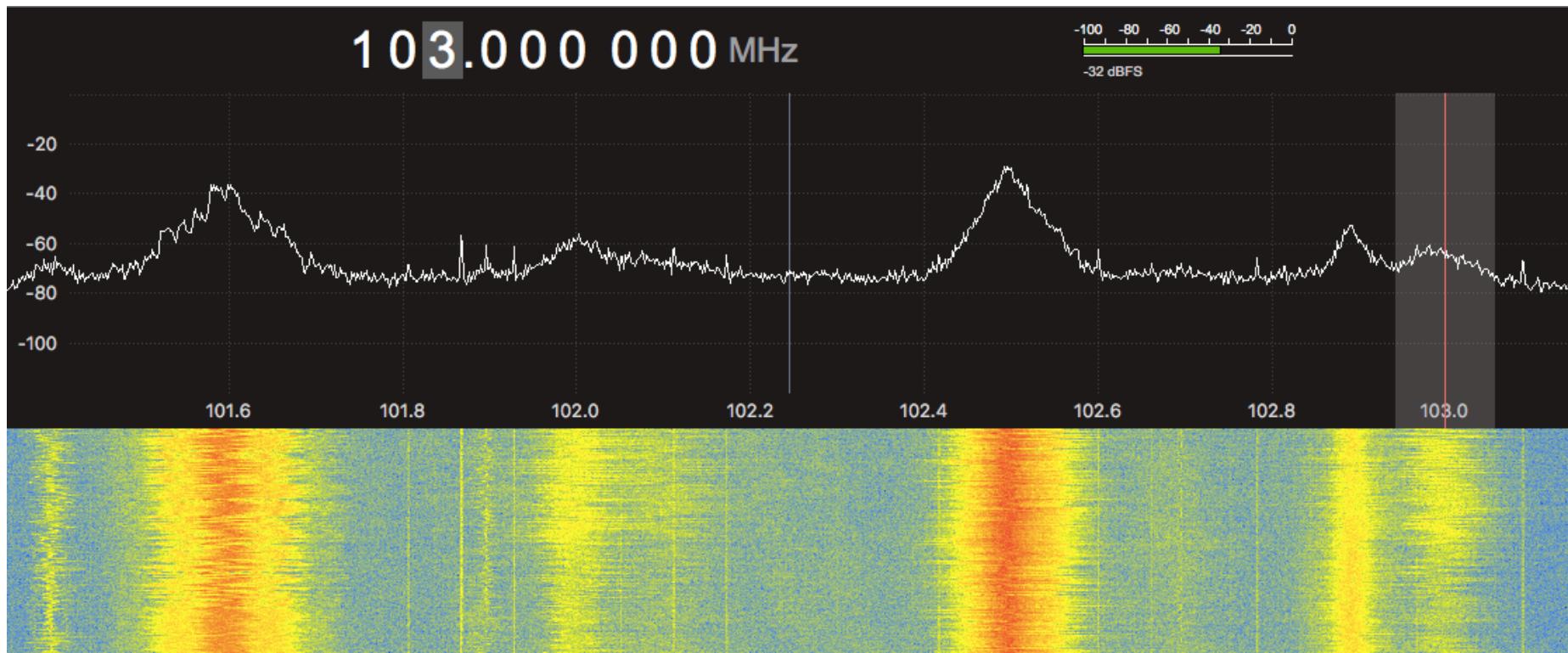
<https://github.com/eldraco/Salamandra>

# USB SDR device

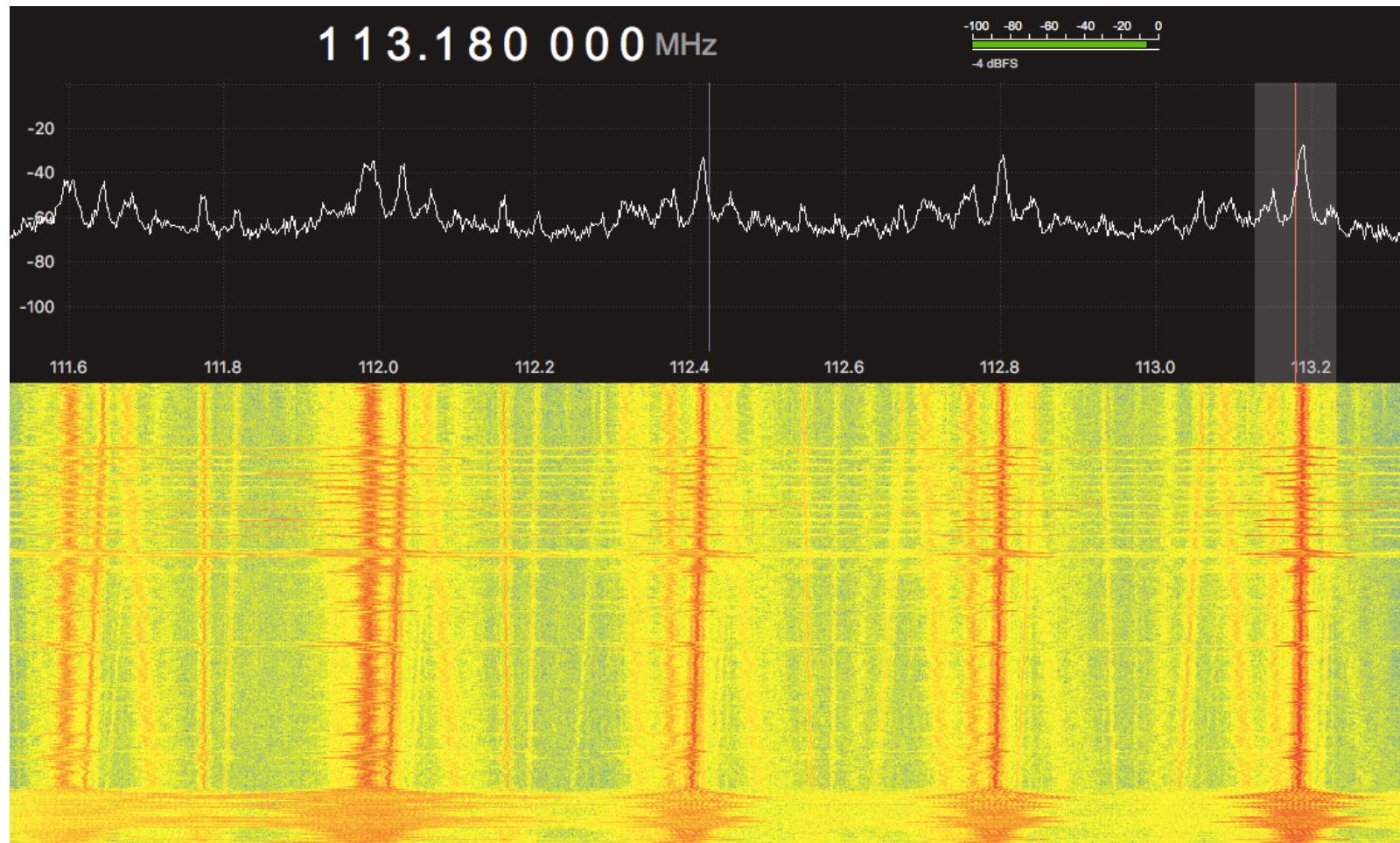


DVB-T+DAB+FM

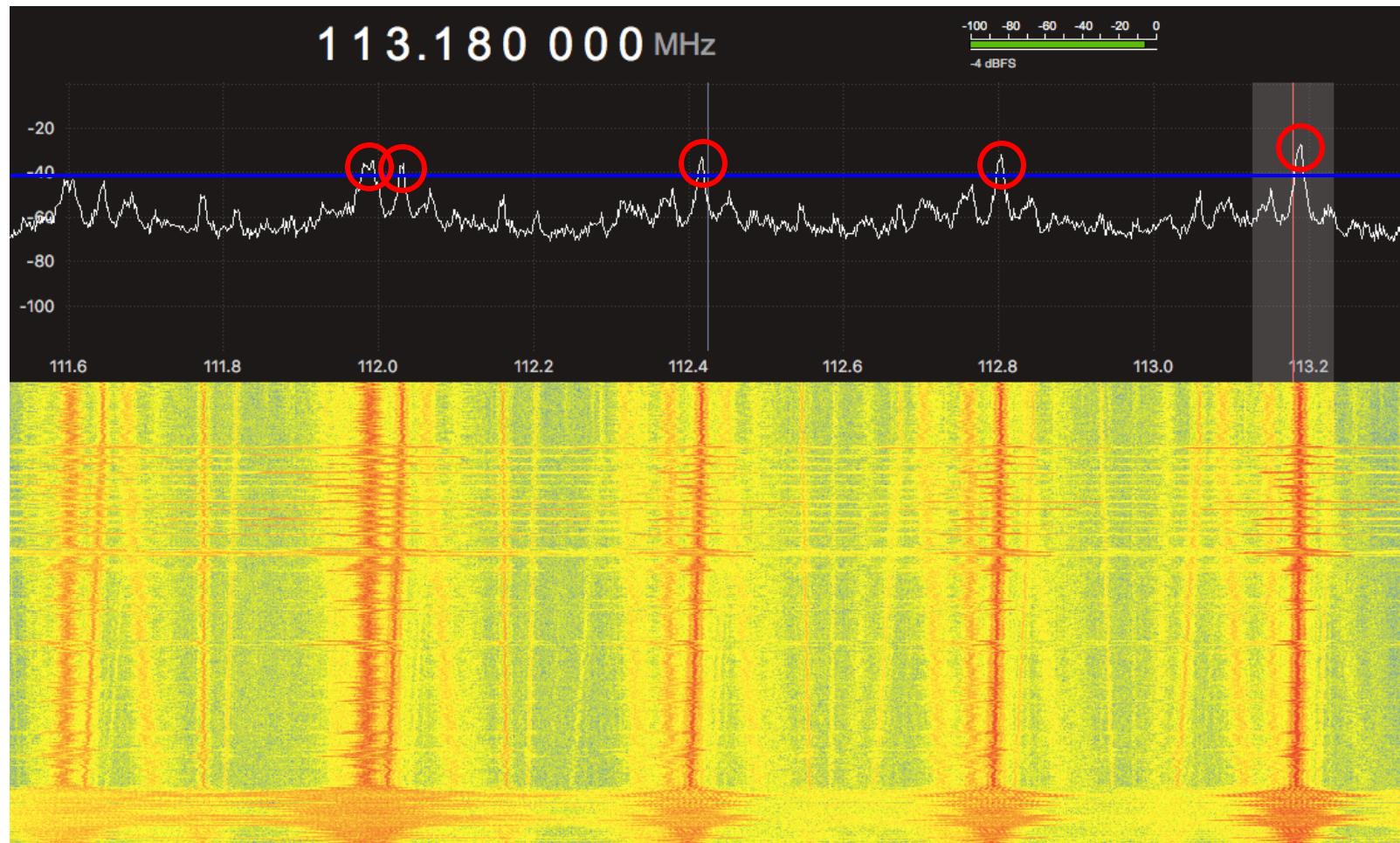
# Normal FM Radio Station



# Mic F908



# Mic F908



# Detection Feature

- Trained thresholds with ~85 experiments
- Fixed the thresholds for the best detection

<b>Th1</b>	<b>Th2</b>	<b>FM1</b>	<b>FPR</b>	<b>Acc</b>	<b>Prec</b>	<b>TPR</b>	<b>FP</b>	<b>TP</b>	<b>FN</b>	<b>TN</b>
15	2	0.551	0	0.67	0.38	0.38	0	16	26	37
<b>15.3</b>	<b>2</b>	<b>0.5</b>	<b>0</b>	<b>0.645</b>	<b>0.333</b>	<b>0.333</b>	<b>0</b>	<b>14</b>	<b>28</b>	<b>37</b>
13	3	0.472	0	0.632	0.309	0.309	0	13	29	37
15	1	0.676	0.02	0.734	0.523	0.523	1	22	20	36
10	5	0.436	0.02	0.607	0.285	0.285	1	12	30	36
10.8	3	0.53	0.05	0.645	0.38	0.38	2	16	26	35
<b>Ghost</b>	-	<b>0.727</b>	<b>0.08</b>	<b>0.756</b>	<b>0.888</b>	<b>0.651</b>	<b>3</b>	<b>24</b>	<b>15</b>	<b>32</b>
7	3	0.714	0.08	0.746	0.595	0.595	3	25	17	34
10	2	0.704	0.108	0.734	0.595	0.595	4	25	17	33
10.8	1	0.735	0.114	0.756	0.862	0.641	4	25	14	31

# Location Feature

Location Signal (the more, the closer)

DateTime (Amount of peaks) [Top Freq Detected MHz] Histogram

```
2017-08-23 18:43:05 ( 34) [113.89]: #####
2017-08-23 18:43:05 ( 37) [113.89]: #####
2017-08-23 18:43:05 ( 44) [113.89]: #####
2017-08-23 18:43:05 ( 36) [113.89]: #####
2017-08-23 18:43:05 ( 42) [113.89]: #####
2017-08-23 18:43:05 ( 36) [113.89]: #####
2017-08-23 18:43:05 ( 36) [112.59]: #####
2017-08-23 18:43:05 ( 40) [113.89]: #####
2017-08-23 18:43:05 ( 32) [113.89]: #####
2017-08-23 18:43:05 ( 36) [113.89]: #####
2017-08-23 18:43:05 ( 37) [112.59]: #####
2017-08-23 18:43:05 ( 40) [113.89]: #####
2017-08-23 18:43:05 ( 33) [112.59]: #####
2017-08-23 18:43:05 ( 36) [113.89]: #####
2017-08-23 18:43:05 ( 41) [113.89]: #####
2017-08-23 18:43:05 ( 51) [113.89]: #####
2017-08-23 18:43:05 ( 36) [112.59]: #####
2017-08-23 18:43:05 ( 33) [112.59]: #####
2017-08-23 18:43:05 ( 34) [112.59]: #####
2017-08-23 18:43:05 ( 49) [113.89]: #####
2017-08-23 18:43:05 ( 30) [112.60]: #####
2017-08-23 18:43:05 ( 30) [112.60]: #####
2017-08-23 18:43:05 ( 35) [112.59]: #####
2017-08-23 18:43:05 ( 45) [113.89]: #####
2017-08-23 18:43:05 ( 48) [113.89]: #####
2017-08-23 18:43:05 ( 37) [113.89]: #####
2017-08-23 18:43:05 ( 40) [113.89]: #####
2017-08-23 18:43:05 ( 45) [113.89]: #####
2017-08-23 18:43:05 ( 39) [113.89]: #####
2017-08-23 18:43:05 ( 45) [113.89]: #####
2017-08-23 18:43:05 ( 37) [112.60]: #####
2017-08-23 18:43:05 ( 44) [112.58]: #####
2017-08-23 18:43:05 ( 12) [113.58]: #####
2017-08-23 18:43:05 ( 11) [113.57]: #####
2017-08-23 18:43:05 ( 9) [113.56]: #####
2017-08-23 18:43:05 ( 9) [113.56]: #####
2017-08-23 18:43:06 ( 8) [113.57]: #####
2017-08-23 18:43:06 ( 9) [113.56]: #####
2017-08-23 18:43:06 ( 8) [113.56]: #####
2017-08-23 18:43:06 ( 9) [113.56]: #####
```

Status: Reading      Threshold: 5.0      Sound: False

Press 's' to increase the threshold (less sensitivity), 'S' to decrease the threshold (more sensitivity), 'm' to toggle sound, or 'q' to quit. Current Time: 2017-08-23 18:43:20.193848

# Salamandra new features

- Detect and **locate** microphones
- You can use **rtl\_power** to record and send the signal to others with Salamandra
- Profile your environment in different times and compare

# Real Life Experiments



# Experiments Methodology

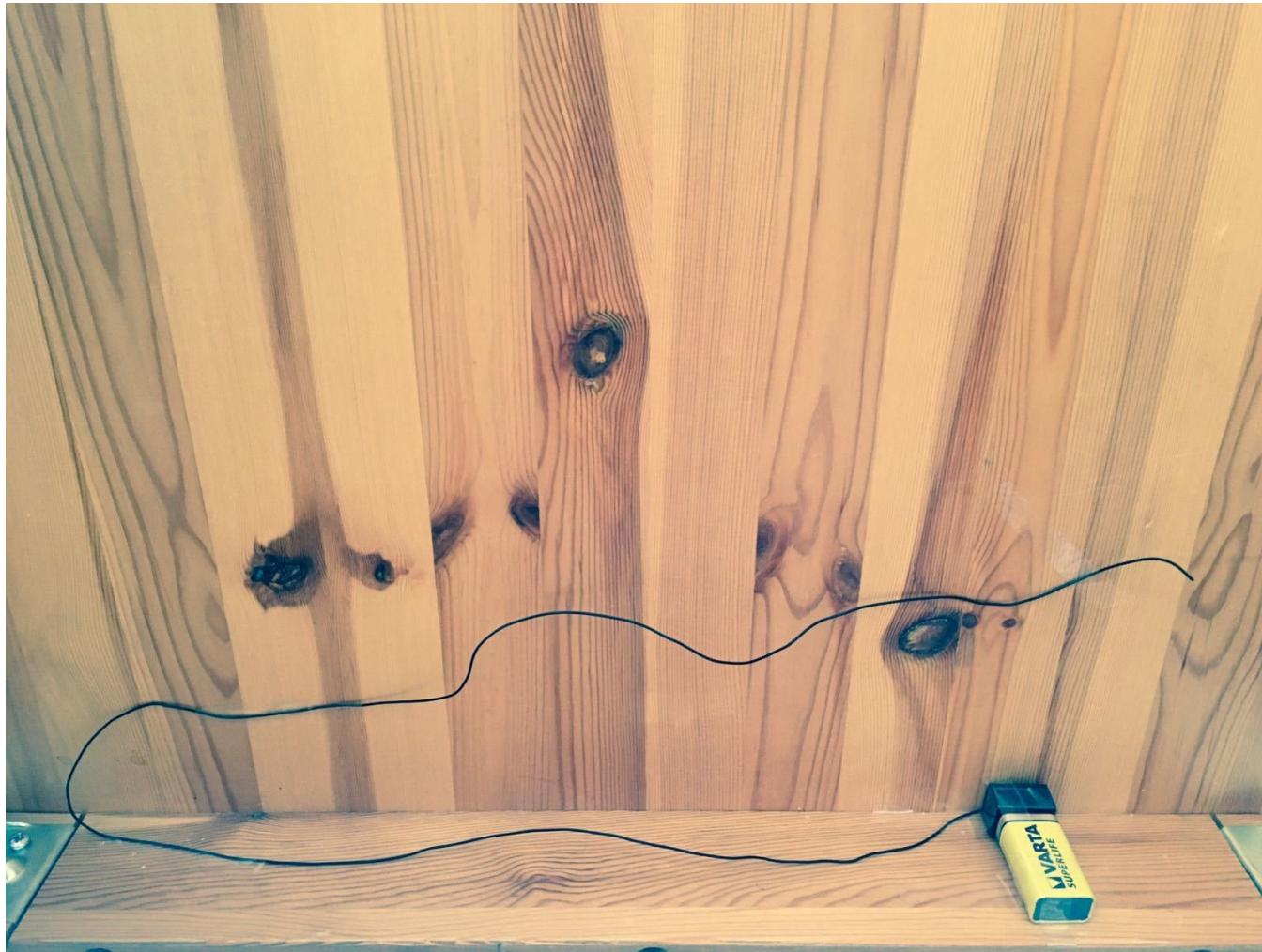
1. Seeker goes out. Hider hides mic (or **not**)
2. Seeker gets in. Speaks passwords. Hider tries to catch them
3. Measure time to detection
4. Measure time to location
5. Measure recall: (passwords heard / total passwords)

# Real Life Experiments

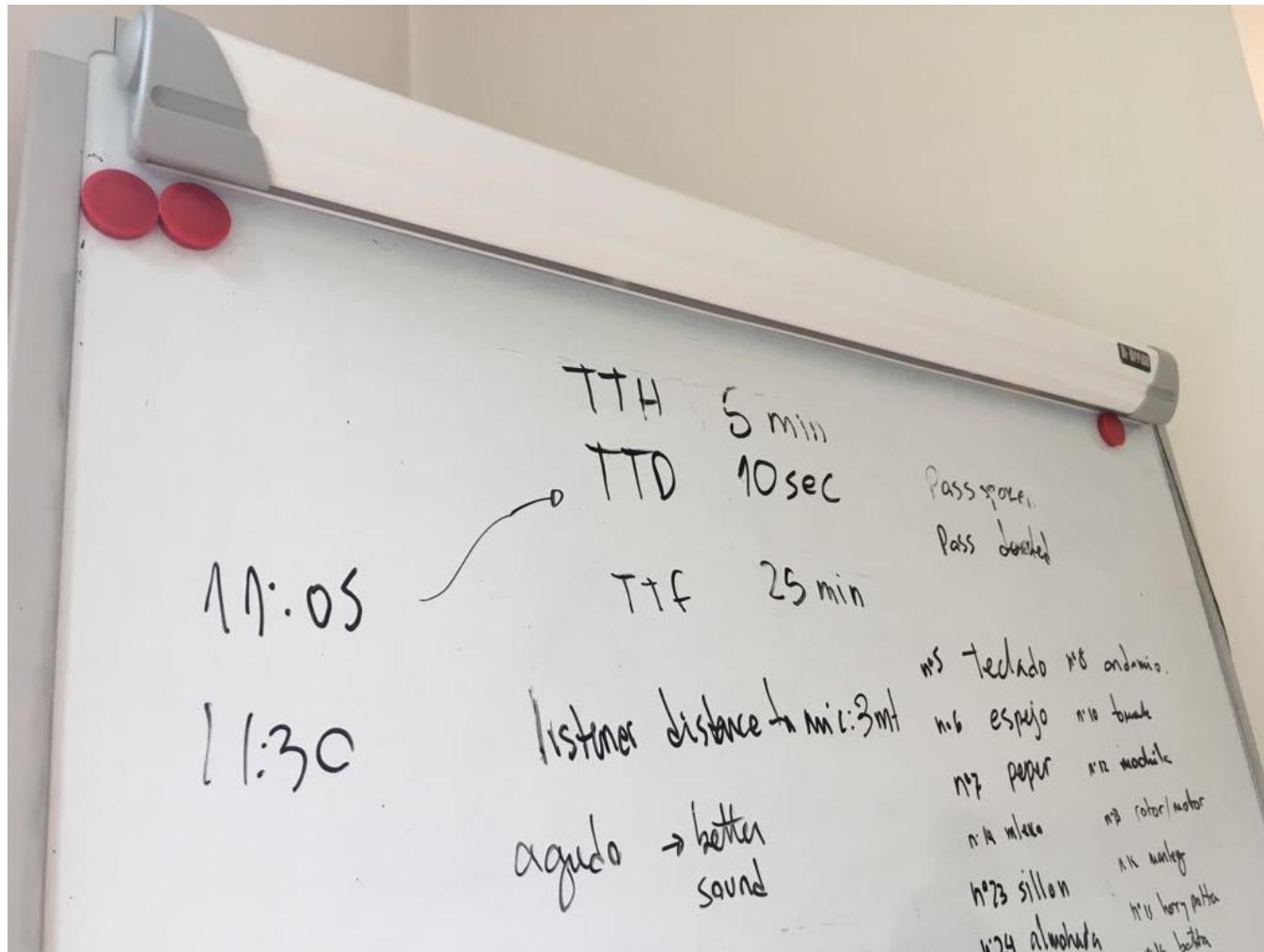
Exp. Id	# Mics Hidden	# Mics found	TTD	TTF
1	1	1	3s	40min
2	1	1	7s	40min
3	1	1	10s	25min
4	1	1	25min	-
5	1	1	3min	20min

Exp. Id	Passwords spoken	Passwords listened	Distance of the Hider	Ghost
1	10	10	5m	Yes
2	-	-	4m	Yes
3	16	13	2m	Yes
4	10	0	4m	No
5	10	5	6m	Yes

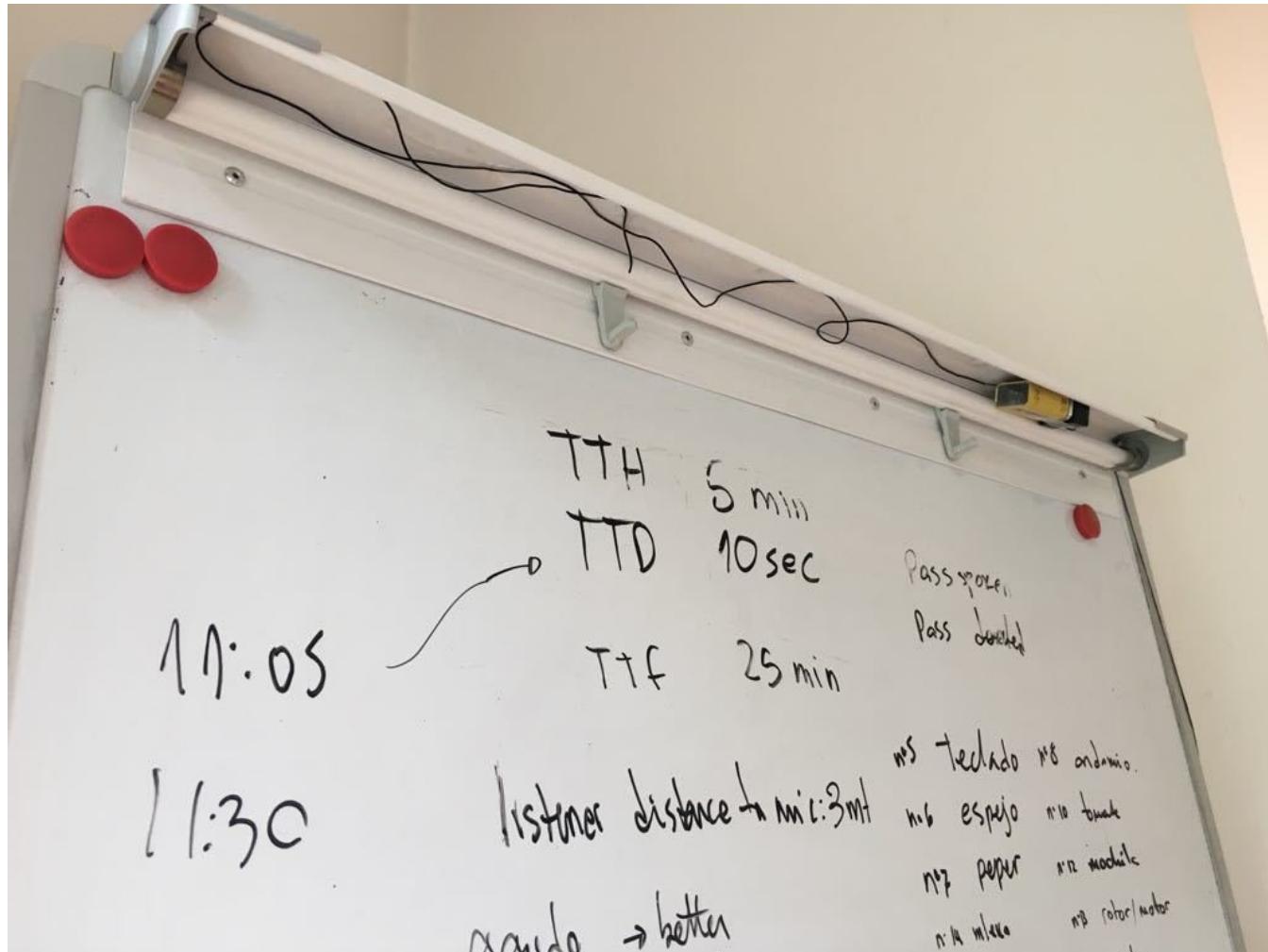
# Real Life Experiments



# Real Life Experiments



# Real Life Experiments



# Experiments Conclusions

- Hiding is **hard**
  - Power, behavior, know your target, physical access
- Location is **hard**
- Listening is **hard**
- Detection is **fast** (w/Salamandra)

# Audio Improvements

Original

Improved

Music doesn't help so much these days. Be  
more creative!

# Contributions

- Systematic research on mic usage and performance
- First sdr-based mic detection tool
- First real-life experiments for comparison

# Conclusions

- Audio eavesdropping is a real threat. Don't be fooled.
- Now you know how it works.
- Now you know how to protect yourself.

Try Salamandra, find mics.

Advance the field. Help others.

# Questions?

Veronica Valeros

@verovaleros

vero.valeros@gmail.com



Sebastian Garcia

@eldracote

eldraco@gmail.com

