



Ataques SDR a Smart TVs: URL y channel injection

2018 March, Pedro Cabrera

/Rooted[®]CON

@PCabreraCamara



Sobre esta presentación

Esta presentación muestra nuevas herramientas -basadas en Software Defined Radio- para revisar la seguridad del sistema de televisión híbrido de broadcast y acceso de banda ancha (HbbTV) y su principal elemento; las SmartTV

Los objetivos de esta presentación son:

- Presentar el sistema HbbTV/TDT y desmitificar su complejidad
- Describir y demostrar los siguientes ataques a este sistema utilizando dispositivos SDR de bajo coste:
 - secuestro de canales TDT (channel injection)
 - servidor fake HbbTV (URL injection)
- Publicar este framework de herramientas Linux que permitirá a la comunidad investigar vulnerabilidades de las Smart TV utilizando estos dispositivos SDR

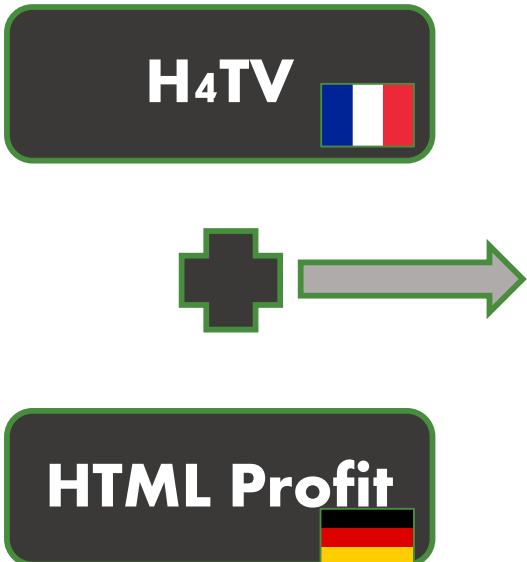
En ningún caso se describirán vulnerabilidades específicas de fabricantes o modelos concretos de Smart TV



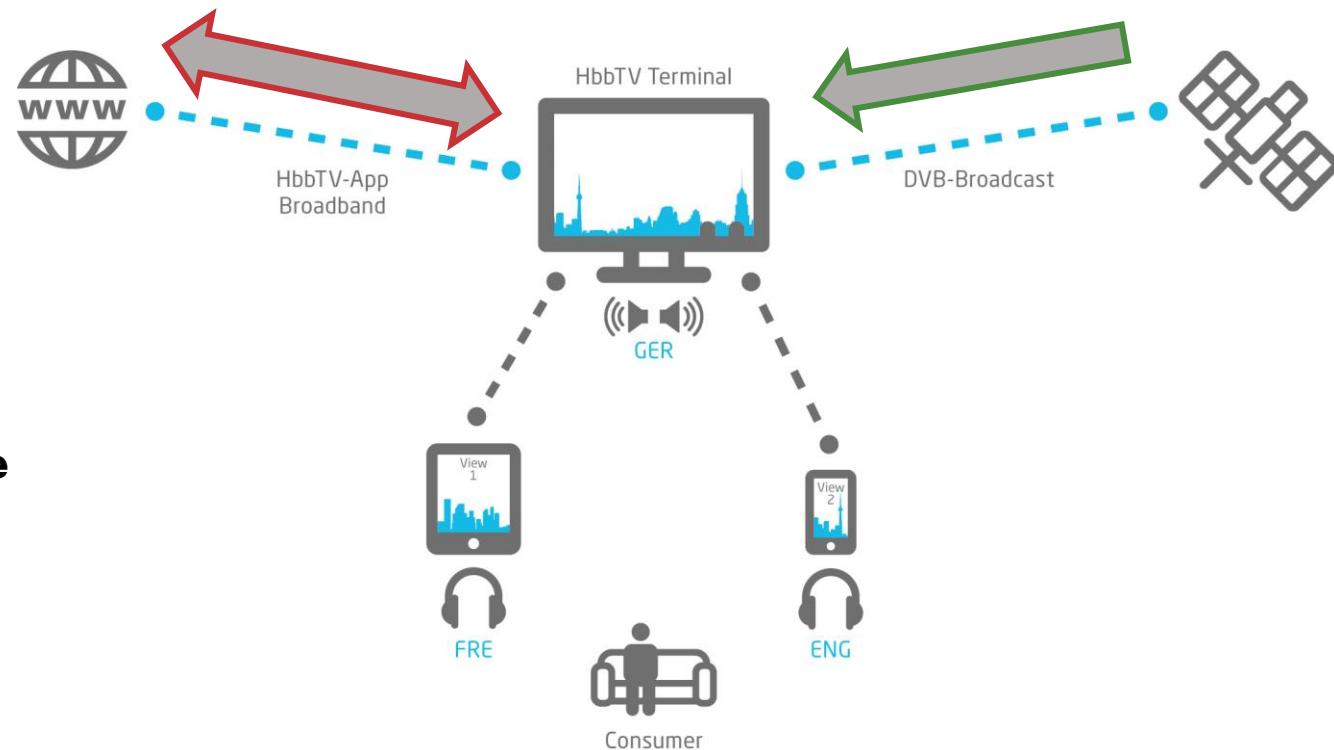
Hybrid Broadcast Broadband Television



La especificación HbbTV amplía la TDT al introducir formatos de metadatos adicionales que mezclan contenido de Internet de banda ancha en el canal de televisión digital.

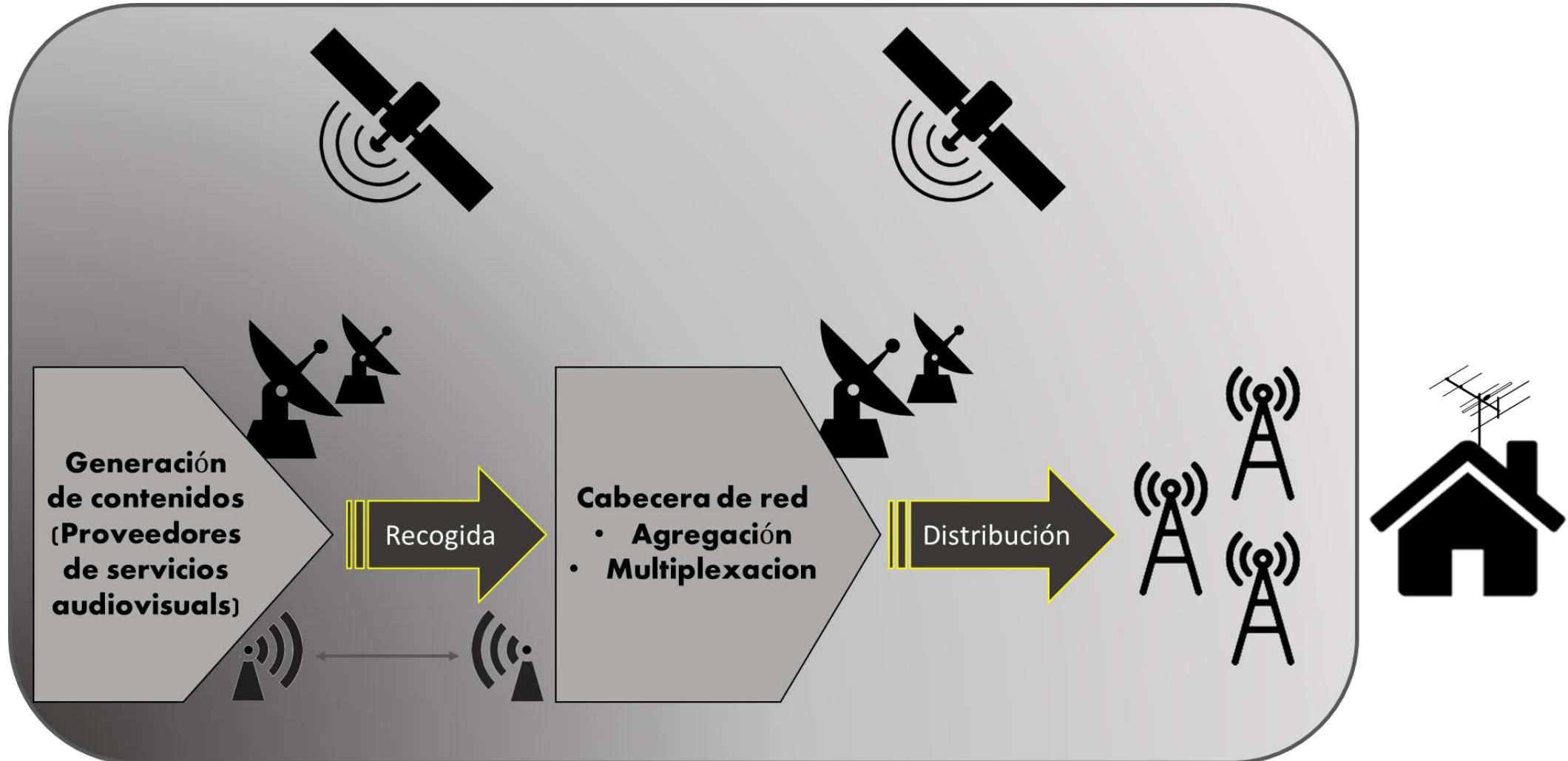


Televisión híbrida porque fusiona contenidos de televisión digital y contenidos web.





Red de distribución





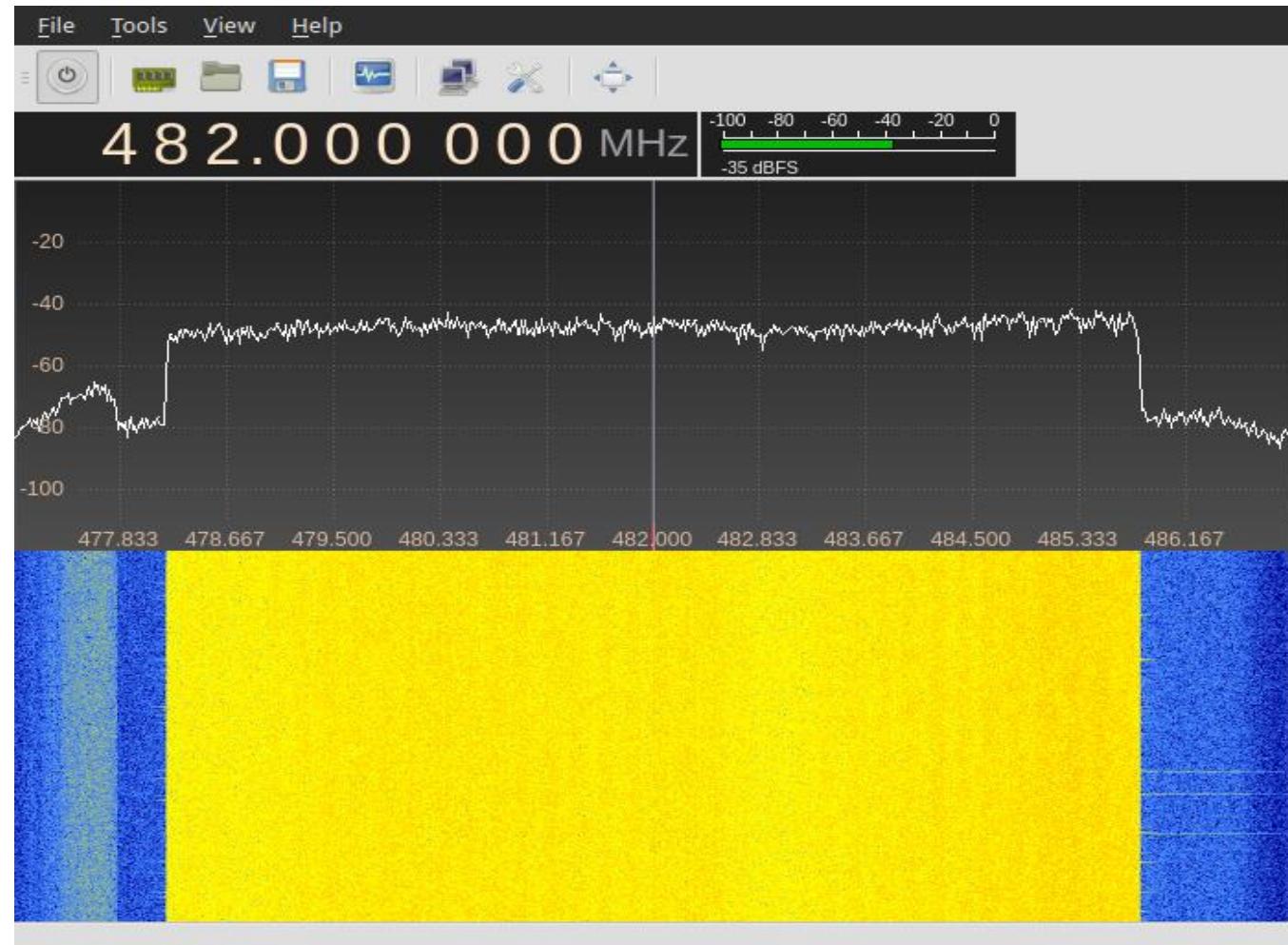
Sobre TDT



DVB_{T2/C2/S2}
DVB_{T2/C/S2}
DVB_{T/C/S2}

Modulación TDT:

- **Ancho de banda de 8 MHz**
- **Modos de transmisión: 8k (6.817 portadoras).**
- **Esquemas de modulación: 64 QAM**
- **Code Rate para protección interna de errores: 2/3.**
- **Longitud del intervalo de guarda: 1/4.**





Sobre TDT

Modulación TDT:

- **Ancho de banda de 8 MHz**
- WHAT THE FUCK**
- misión: 8k (6.817)**
- modulación: 64 QAM**
- AM I LOOKING AT**
- errores: 2/3**

Lengüeta



2018 March, Pedro Cabrera

GOOGLE

rtlsdr sample rate

All Images Videos Shopping News More Settings Tools

About 37,100 results (0.48 seconds)

The maximum sample rate is **3.2 MS/s** (mega samples per second). However, the RTL-SDR is unstable at this speed and may drop samples. The maximum sample rate that does not drop samples is **2.4 MS/s**, however some people have had luck with 2.8MS/s and **3.2 MS/s** working well on some USB 3.0 ports.

About RTL-SDR - [rtl-sdr.com](https://www.rtl-sdr.com/about-rtl-sdr/)

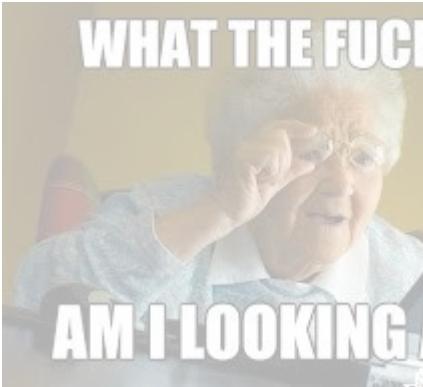
<https://www.rtl-sdr.com/about-rtl-sdr/>



Sobre TDT

Modulación TDT:

- *Ancho de ba*



2 MHZ SAMPLING RATE FROM AN 8 MHZ RECEIVER?

[POST REPLY](#)



Search this topic...



2 Mhz sampling rate from an 8 Mhz receiver?



by sdr dreams » Mon Jan 30, 2017 1:16 am

Recently I bought the miracle (extremely inexpensive) SDR capable, DVB receiver dongle (with RT820T2 silicon tuner and an RTL2832U chip) which is supposed to demodulate (in dongle hardware) and decode (possibly in PC cpu-gpu) digital terrestrial SDTV and HDTV signals which DO have 8 MHZ analog baseband signal bandwidth.

I'm sorry if this will be a dumb question as I didn't have time to search for the complete details but even at the first glance, to be able to decode an 8 Mhz baseband TV signal you could be sampling it at a minimum of 16 MSPS (from the basic sampling theorem). Now the question is: Then why is the software SDR# or alike do only provide a sampling rate of up to 3 Mhz with I/Q channels? Why is it not up to 8 Mhz w/I/Q separate channels supposedly available on the dongle?

I really cannot answer it by myself because the commercial purpose of the usb DVB-T congle implies the capability to receive, demodulate and decode TV signals with 8 Mhz baseband signal bandwidth? So what's the reason? What am I missing in this simple logic?

Re: 2 Mhz sampling rate from an 8 Mhz receiver?



by x3nus » Tue Jan 31, 2017 5:48 pm

Basically, the dongle has two modes: DVB-T mode and SDR mode. In DVB-T mode it can receive and decode DVB-T signals with up to 8 MHz bandwidth, but it require special (actually the original) drivers specially for DVB-T and therefore cannot be used as SDR. The SDR mode is actually the dongle's unspecified functionality discovered by the hackers who made the alternative rtl-sdr drivers and libraries, and the maximum sample rate you can get in SDR mode is 3,2 msps.



Settings Tools

cond). However, the maximum sample rate we have had luck with



TDT en Linux - GNU Radio

- **Bogdan (YO3IIU)**

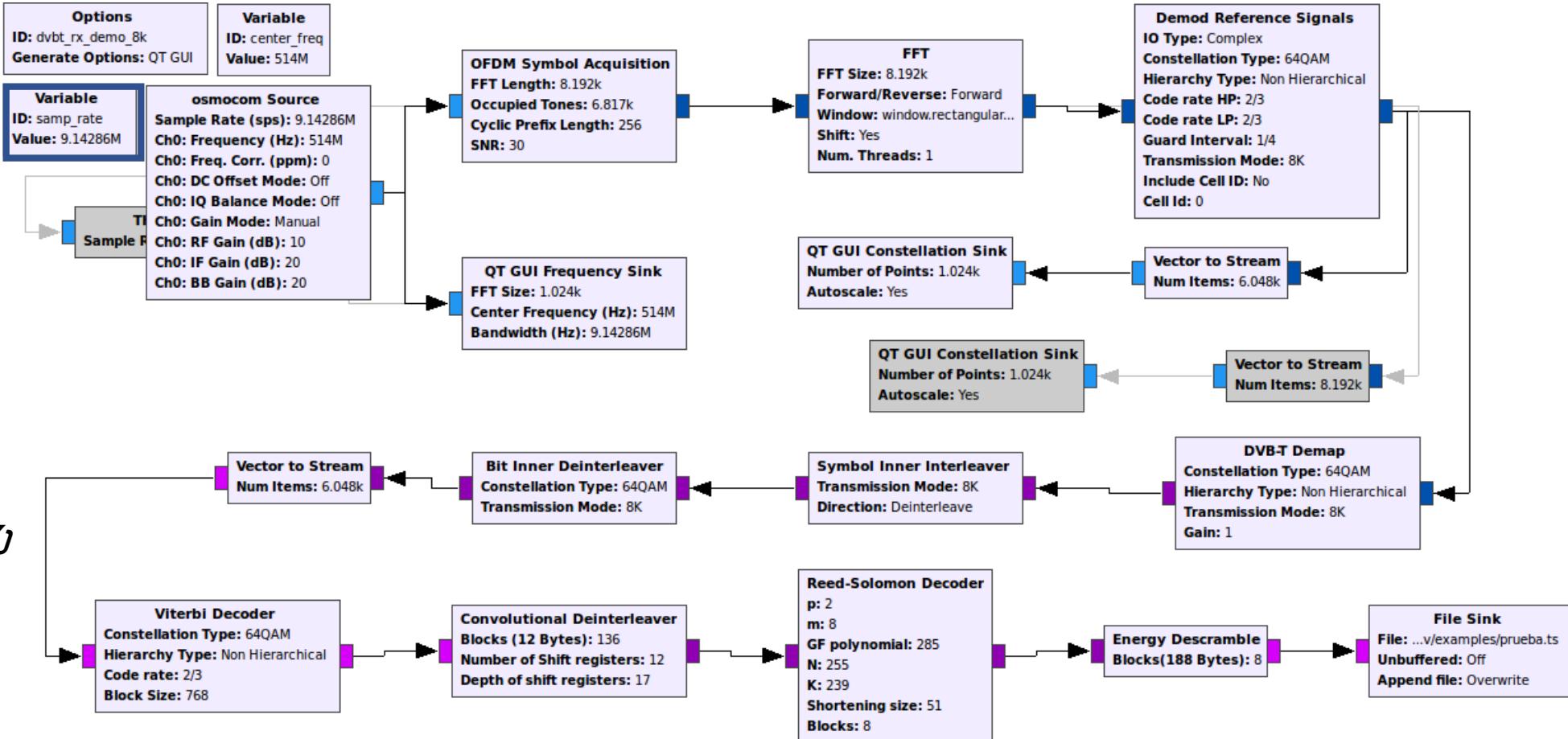
GR-DVBT
(USRP N210)

- **GNU Radio:**

GR-DTV (USRP)

- **Ron Economos (W6RZ)**

dtv-utils (BladeRF)

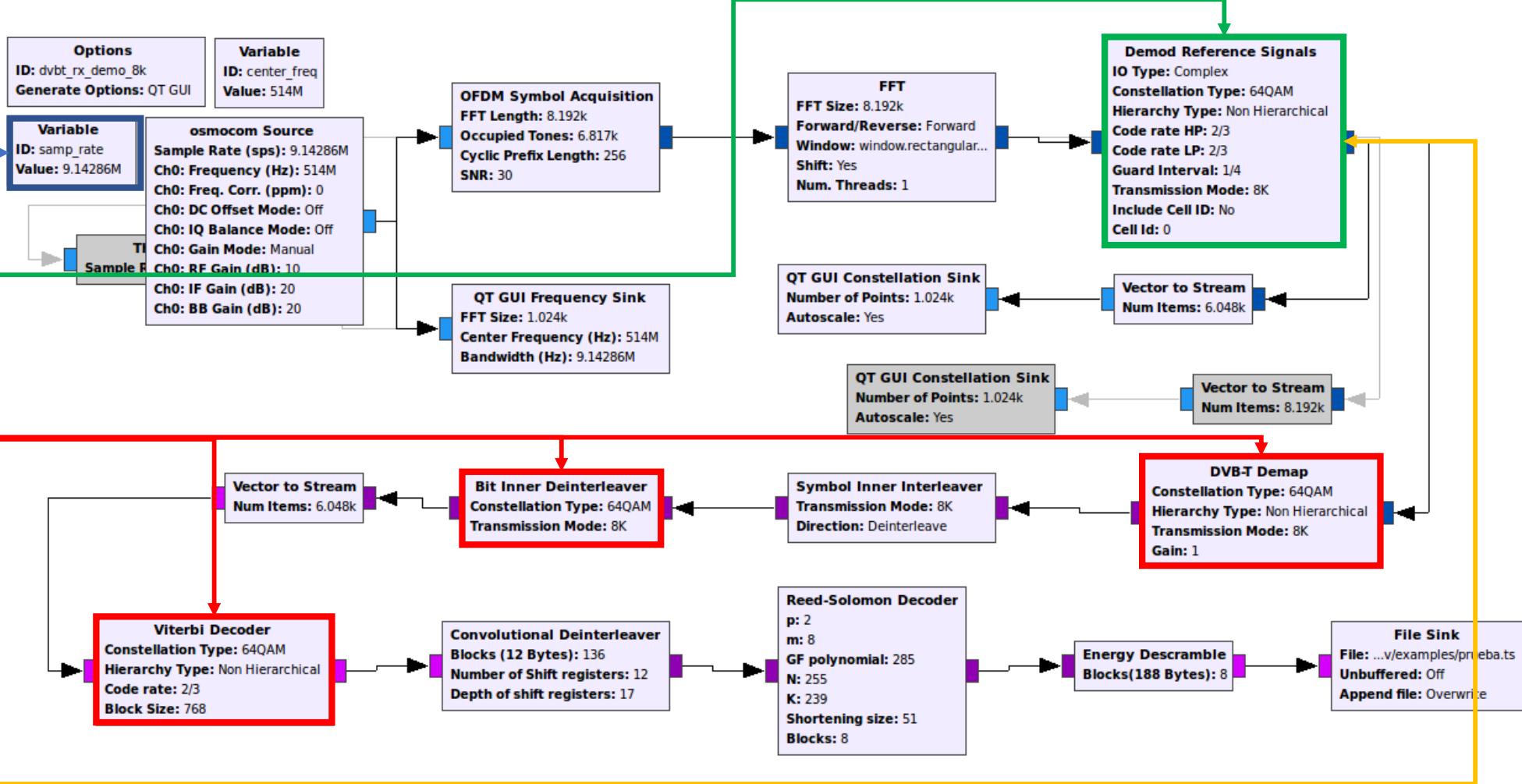




TDT en Linux - GNU Radio

Modulación TDT:

- **8 MHz**
- **Modos de transmisión: 8k**
- **Esquemas de modulación: 64 QAM**
- **Code Rate: 2/3.**
- **Longitud del intervalo de guarda: 1/4.**





Canales TDT y Frecuencias

8 múltiples digitales:

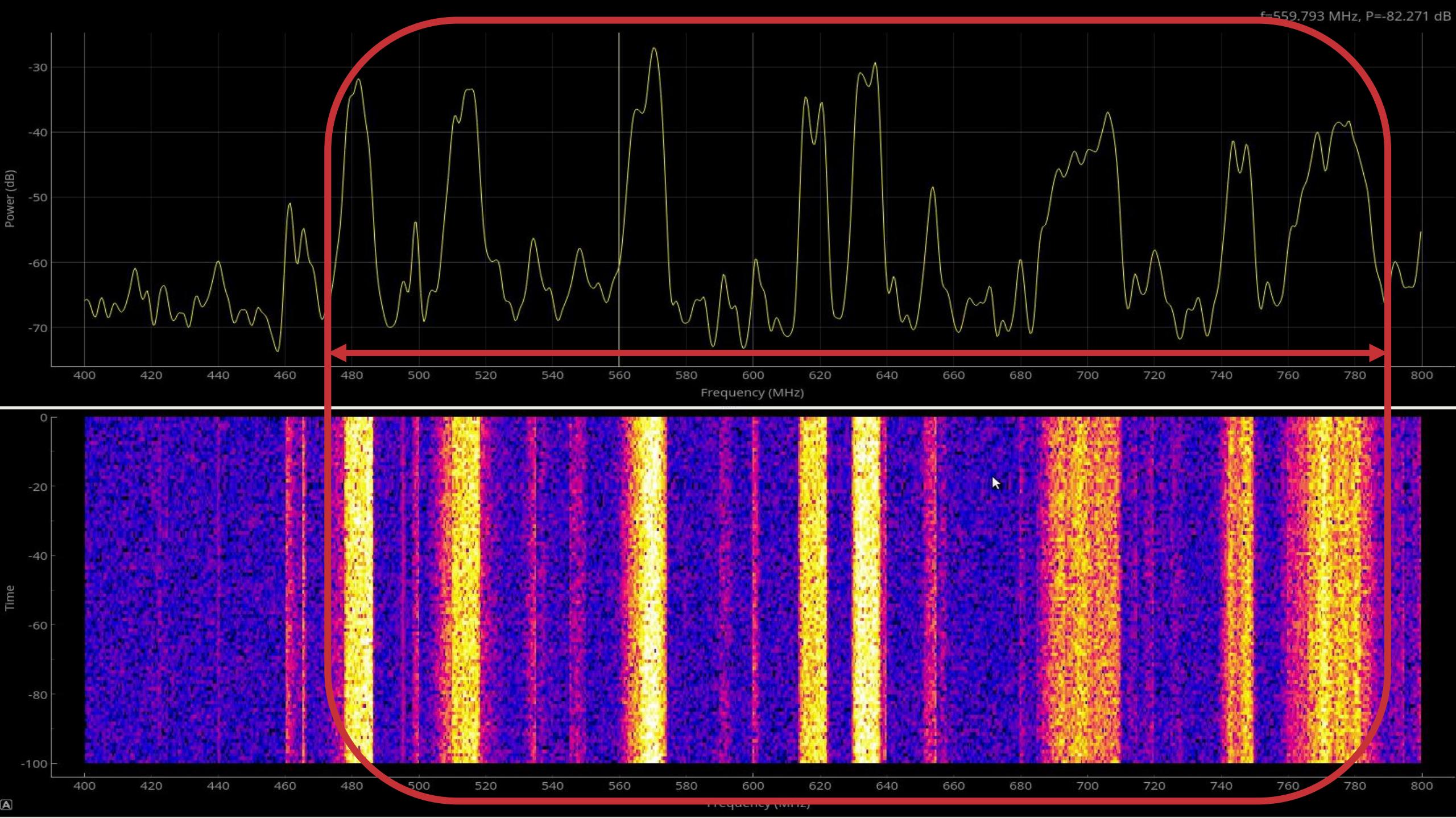
RGE₁, RGE₂, MPE₁, MPE₂, MPE₃, MPE₄, MPE₅ y MAUT

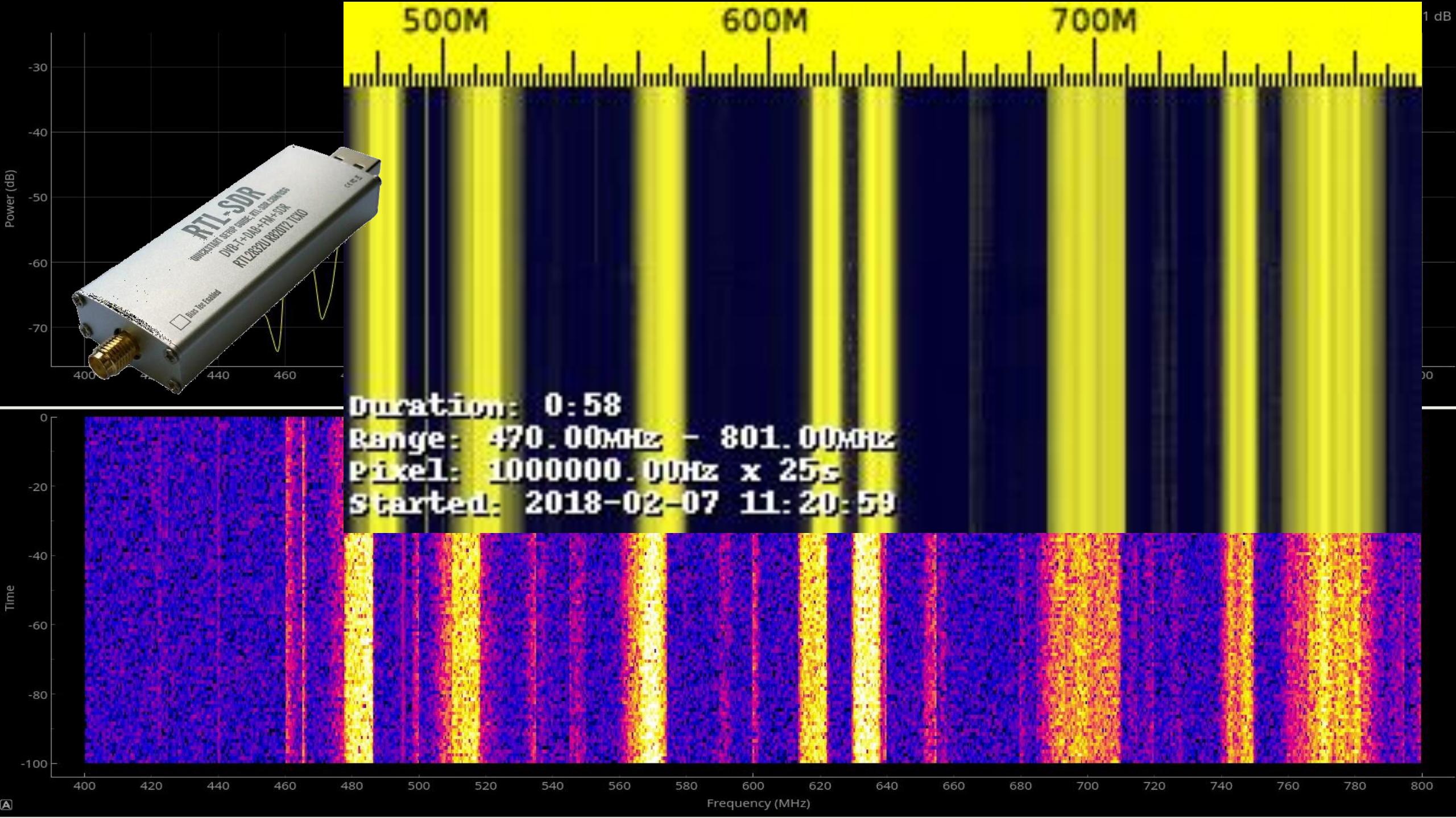
RGE: Red Global de Cobertura Estatal

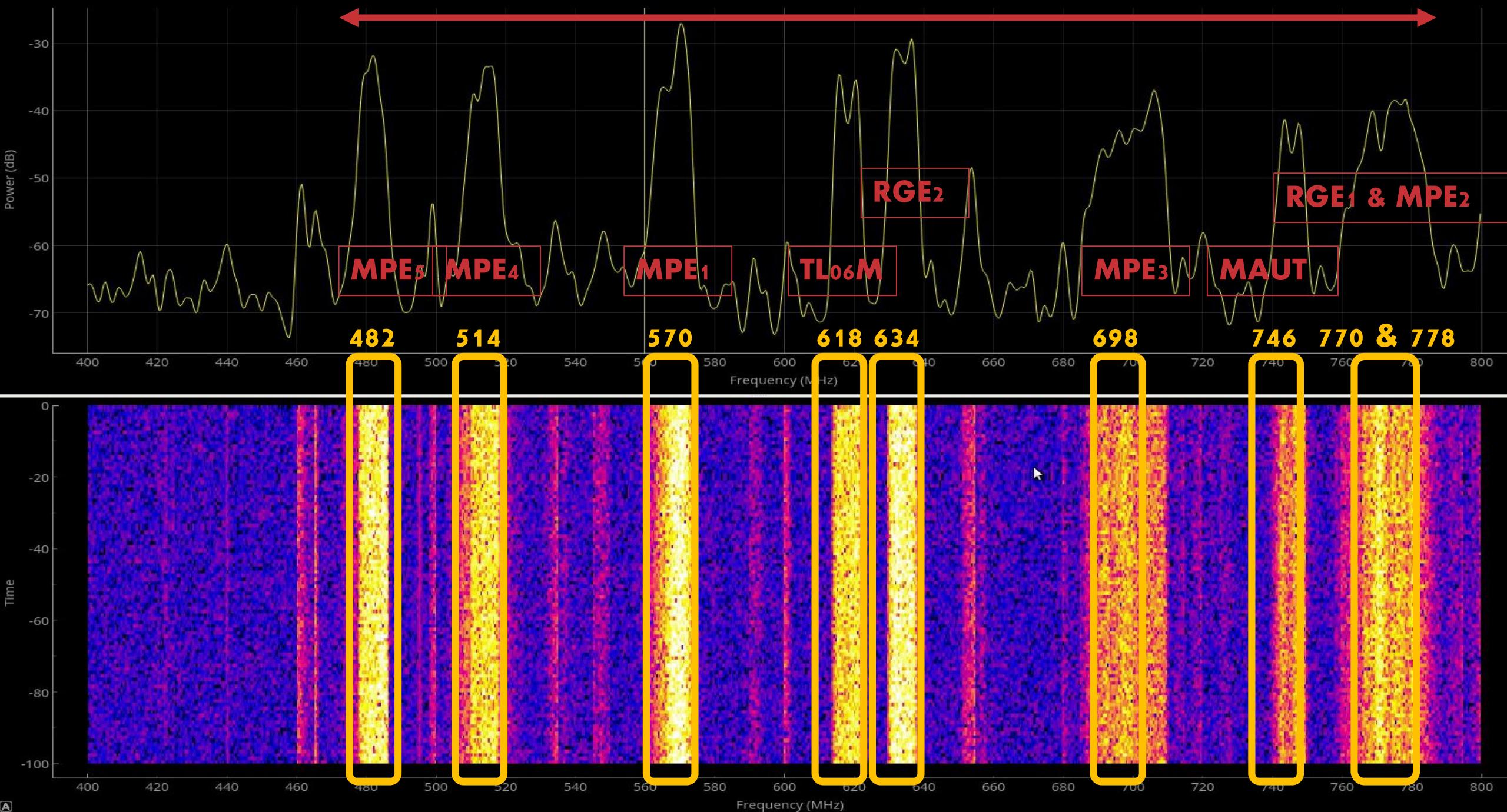
MPE: Múltiple Privado de Cobertura Estatal

MAUT: Múltiple de Cobertura Autonómica

Múltiple digital	Canal	Frecuencia	Múltiple digital	Canal	Frecuencia
MPE₅	<i>atreseries HD</i>	482.000.000	MPE₃	<i>Telecinco</i>	698.000.000
MPE₅	<i>BeMad tv HD</i>	482.000.000	MPE₃	<i>Telecinco HD</i>	698.000.000
MPE₅	<i>Realmadrid TV HD</i>	482.000.000	MPE₃	<i>Cuatro</i>	698.000.000
MPE₄	<i>TRECE</i>	514.000.000	MPE₃	<i>Cuatro HD</i>	698.000.000
MPE₄	<i>Energy</i>	514.000.000	MPE₃	<i>FDF</i>	698.000.000
MPE₄	<i>mega</i>	514.000.000	MPE₃	<i>Divinity</i>	698.000.000
MPE₄	<i>Boing</i>	514.000.000	MAUT	<i>Telemadrid HD</i>	746.000.000
MPE₁	<i>PARAMOUNT CHANNEL</i>	570.000.000	MAUT	<i>Telemadrid</i>	746.000.000
MPE₁	<i>GOL</i>	570.000.000	MAUT	<i>LA OTRA</i>	746.000.000
MPE₁	<i>DMAX</i>	570.000.000	MAUT	<i>BOM</i>	746.000.000
MPE₁	<i>Disney Channel</i>	570.000.000	RGE₁	<i>La 2 HD</i>	770.000.000
TL_{06M}	<i>TRECE</i>	618.000.000	RGE₁	<i>La 2</i>	770.000.000
TL_{06M}	<i>Intereconomia TV</i>	618.000.000	RGE₁	<i>La 1 HD</i>	770.000.000
TL_{06M}	<i>HIT TV</i>	618.000.000	RGE₁	<i>La 1</i>	770.000.000
TL_{06M}	<i>MegaStar</i>	618.000.000	RGE₁	<i>Clan</i>	770.000.000
TL_{06M}	<i>CGTN-Español</i>	618.000.000	RGE₁	<i>24h</i>	770.000.000
TL_{06M}	<i>Canal Galería</i>	618.000.000	MPE₂	<i>nova</i>	778.000.000
TL_{06M}	<i>Business TV</i>	618.000.000	MPE₂	<i>neox</i>	778.000.000
TL_{06M}	<i>8madrid</i>	618.000.000	MPE₂	<i>laSexta HD</i>	778.000.000
RGE₂	<i>tdp HD</i>	634.000.000	MPE₂	<i>laSexta</i>	778.000.000
RGE₂	<i>TEN</i>	634.000.000	MPE₂	<i>antena3 HD</i>	778.000.000
RGE₂	<i>DKISS</i>	634.000.000	MPE₂	<i>antena3</i>	778.000.000
RGE₂	<i>tdp</i>	634.000.000			
RGE₂	<i>Clan HD</i>	634.000.000			



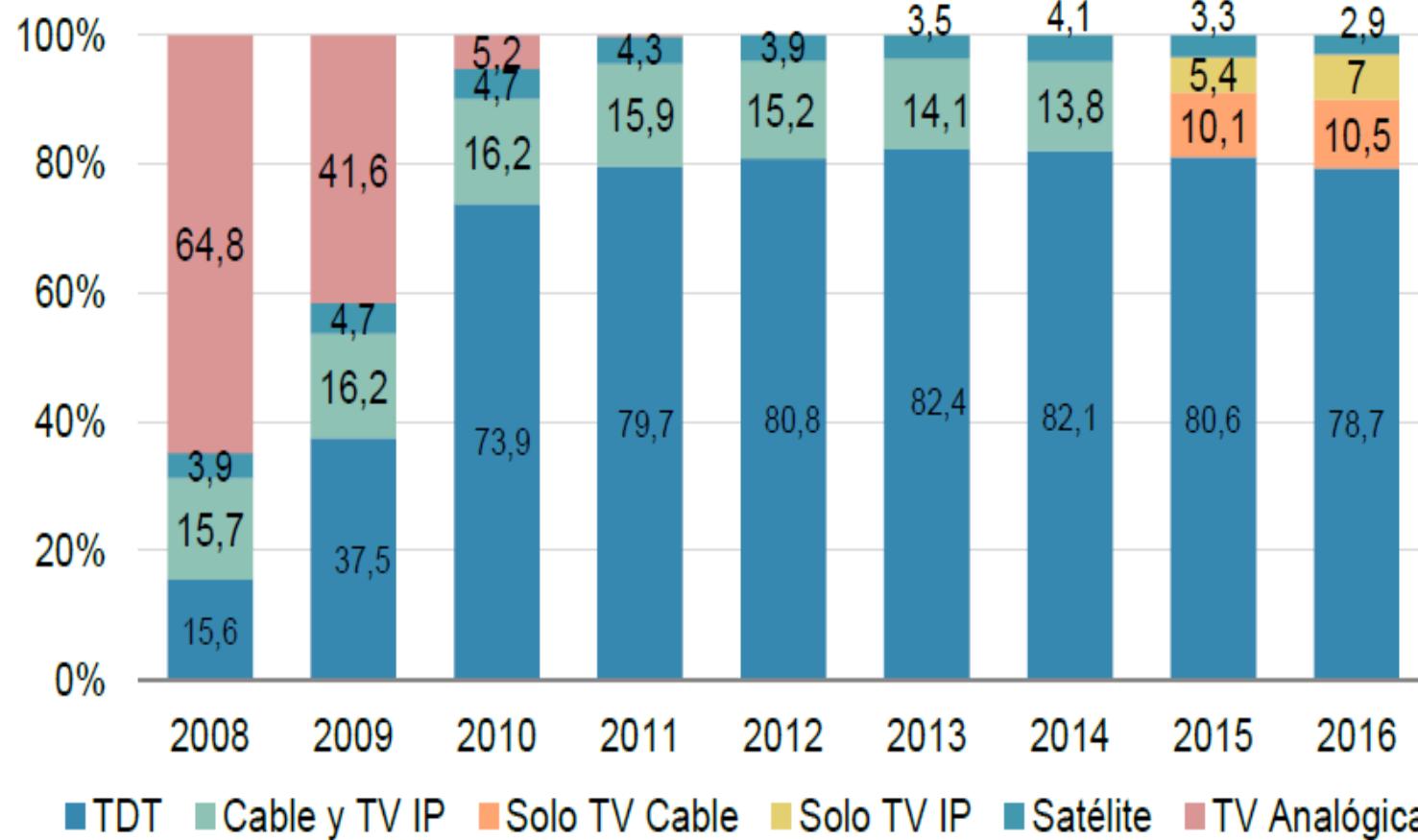






Audiencia de la TDT

Audiencia por medio de transmisión (porcentaje)



Fuente: Kantar Media

Ataques previos secuestro de canal



CHICAGO 1987 . WGN (Channel 9) sportscast es secuestrado a las 21:14 del 22 de Noviembre. Alguien luciendo una máscara Max Headroom y usando un blazer amarillo interrumpió un segmento grabado de los "Chicago Bears" durante unos 25 segundos. A las 23:15 la emisión de un episodio del "Dr. Who" en la cadena WTTW fue interrumpida por el mismo personaje, esta vez con audio extraño, una aparición de otra persona y un tiempo más largo en el aire.



Costa Este EEUU 1986. A las 12:32, HBO (Home Box Office) recibió su señal satelital desde su centro de operaciones en Long Island en Nueva York interrumpida por un hombre que se hace llamar "Capitán Midnight". La interrupción ocurrió durante una presentación de The Falcon and the Snowman.



Guerra de Libano 2006. Durante la Guerra del Líbano de 2006, Israel sobrecargó la transmisión satelital de Al Manar TV de Hezbollah para transmitir propaganda anti-Hezbollah.

https://en.wikipedia.org/wiki/Broadcast_signal_intusion

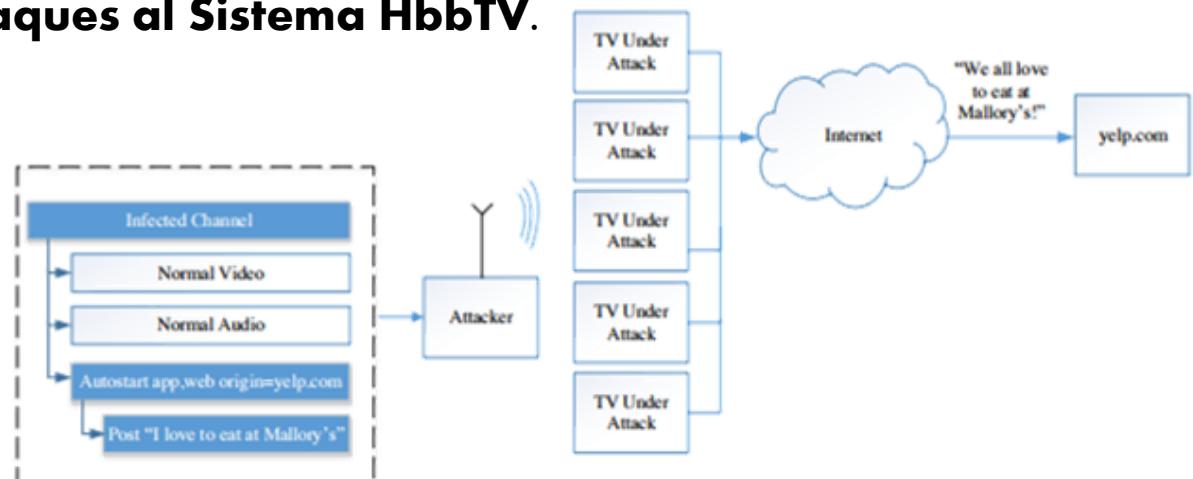


Ataques previos a HbbTV/Smart TV

Febrero 2017 – Rafael Scheel “Hacking a Smart TV”. Presenta dos vulnerabilidades a dos navegadores web de Smart TV de Samsung: Flash y Javascript, que explota creando su propia aplicación HbbTV, emitiéndola a través de su propio canal de TDT. Para ello utiliza un dispositivo propietario de bajo coste y un SW no publicado. En ningún caso utiliza SDR o herramientas OpenSource.

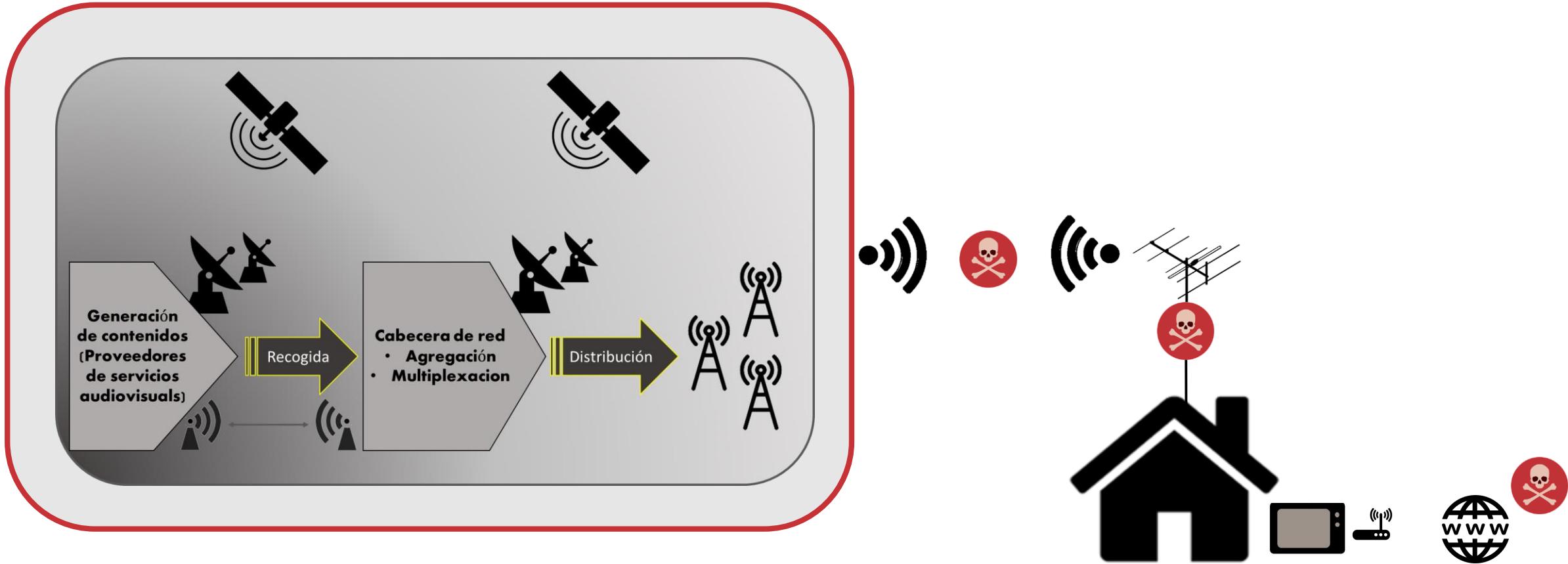
Abril 2015 - Yossef Oren and Angelos D. Keromytis “Attacking the Internet using Broadcast Digital Television”. Estudio teórico sobre los potenciales ataques al Sistema HbbTV.

Junio 2014 – Weeping Angel (CIA) – Marzo 2017 WikiLeaks. Muestra exactamente lo que un agente debe hacer para convertir una Samsung Smart TV en un micrófono. Ataque requiere acceso local a la Smart TV.



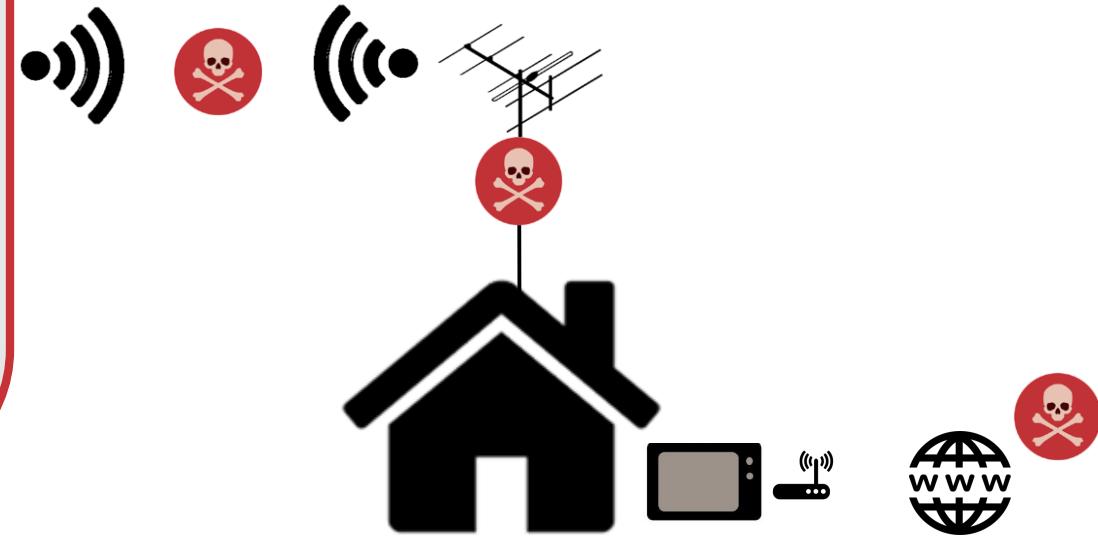


Ataques SDR a las SmartTV





Ataques SDR a las SmartTV





Ataque secuestro de canal TDT

Utilizaremos la misma frecuencia que el canal original para suplantar la emisión de contenidos, utilizando BladeRF o HackRF:

Mpeg
Video file



gr-dtv
(gr-dvbt)



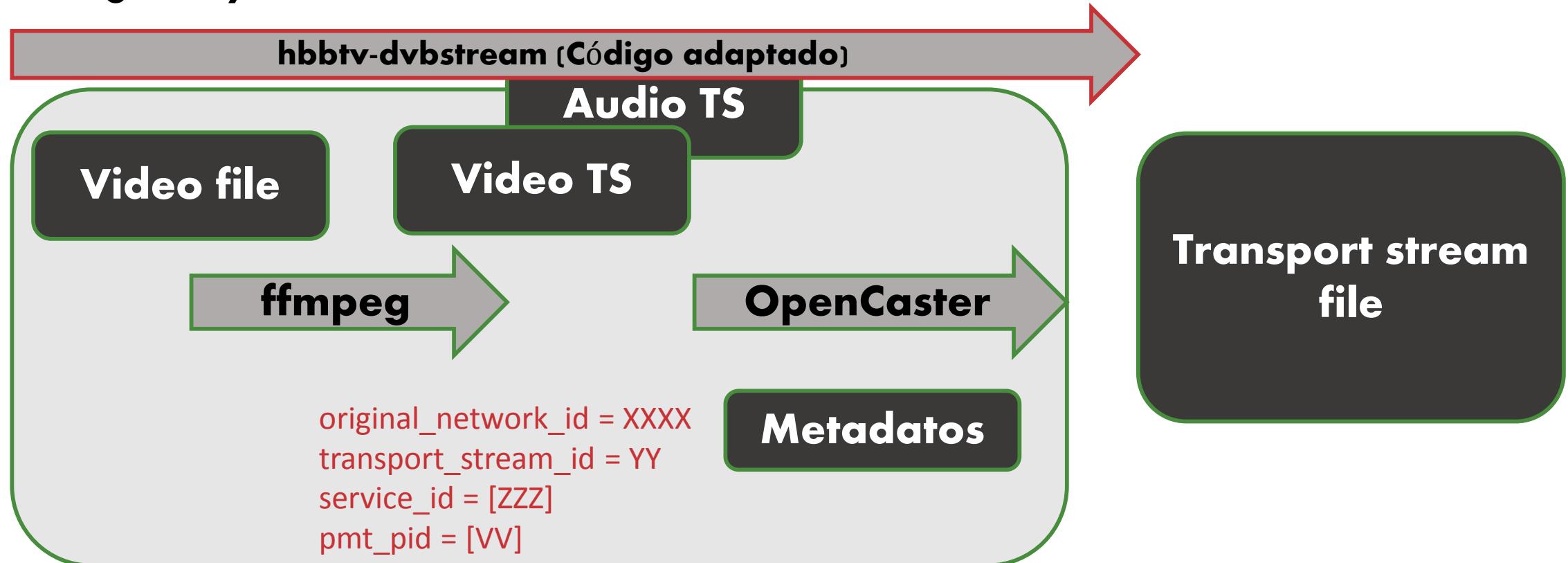
Metadatos
HbbTV
(solo AV)





Ataque secuestro de canal TDT

Antes de emitir, debemos generar un fichero “Transport Stream” TS con los parámetros del canal legítimo y el nuevo contenido A/V:





Parámetros canal TDT & HbbTV

```

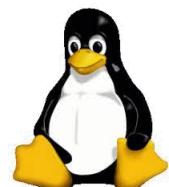
{
  "service": {
    "transportStreamId": 1012,
    "serviceId": 531,
    "providerName": "RTVE",
    "serviceName": "La 2",
    "status": "RUNNING",
    "type": "TV"
  },
  "mux": {"freq": 770000000, "bandwidth": 8000000, "deliverySystem": "DVBT"},
  "pids": [{"rawPid": 201, "type": "PCR_PID"}, {"rawPid": 200, "type": "PMET_PID"}, {"rawPid": 0, "type": "PAT_PID"}, {"rawPid": 17, "type": "SDT_PID"}, {"rawPid": 201, "type": "H262_VIDEO"}, {"rawPid": 202, "type": "DOLBY_DIGITAL_PLUS_AUDIO"}, {"rawPid": 203, "type": "MPEG_1_AUDIO"}]
}
...
  
```



App: Aerial TV
"channels.json"



Parámetros canal TDT & HbbTV



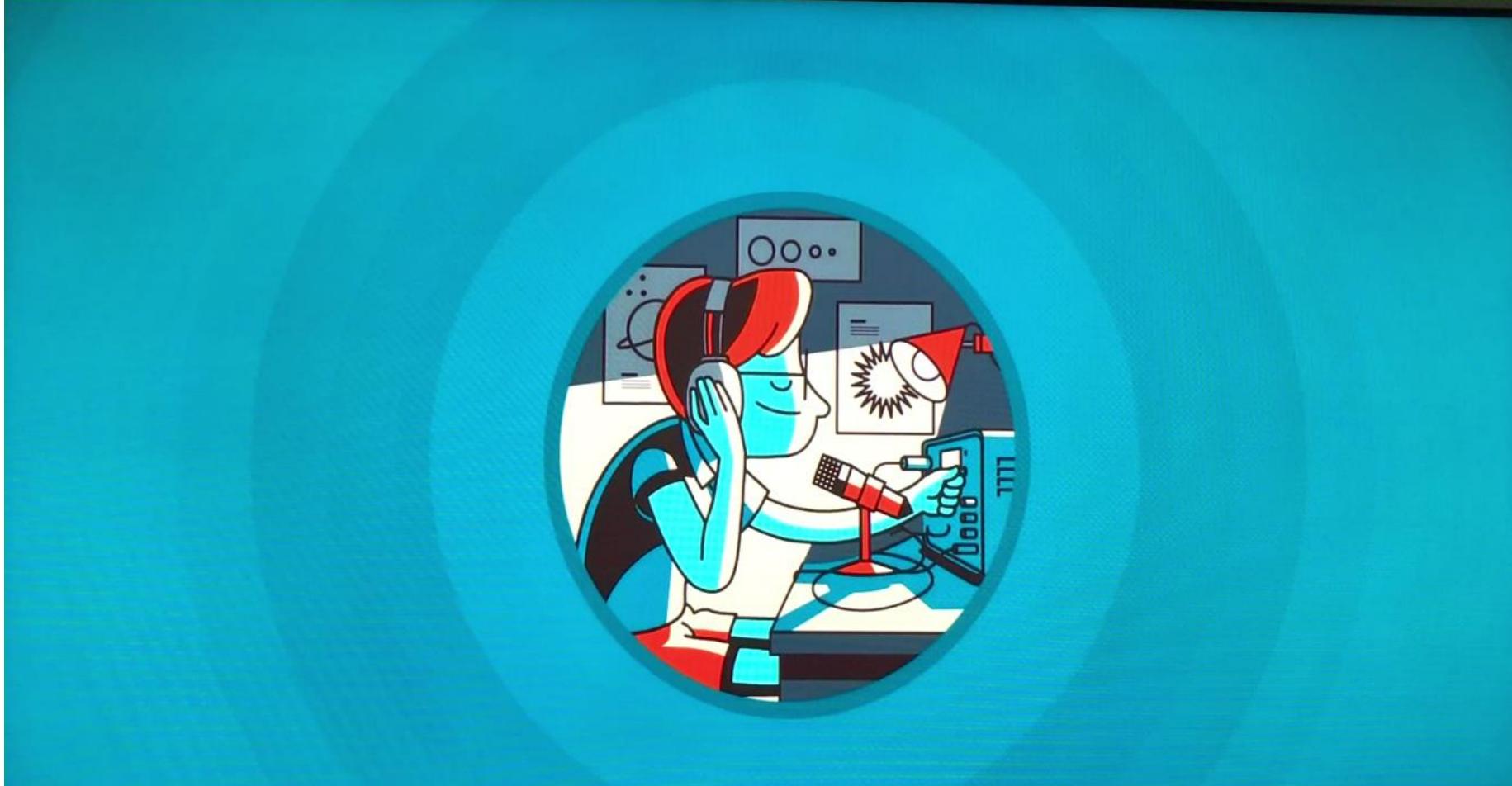
kaffeine

The screenshot shows the Kaffeine application interface. On the left is a sidebar with tabs for Inicio, Reproducción, Lista de reproducción, and Televisión. The 'Televisión' tab is selected, showing a list of channels. The channel '8madrid-1' is selected and highlighted with a red box. A red dashed line connects this selection to the 'Edit Channel - Kaffeine' dialog box on the right. The dialog box has fields for Name (8madrid-1), Number (4), Source (Terrestre), and various parameters like Frecuencia (MHz) set to 618, Id. de red set to 8916, and PMT PID set to 272. Another red dashed line connects the 'PMT PID' field in the dialog to the 'PMT PID' field in the list on the left. The background shows a video player window displaying a scene from a movie.



/Rooted® CON

Secuestro de canal - demo video



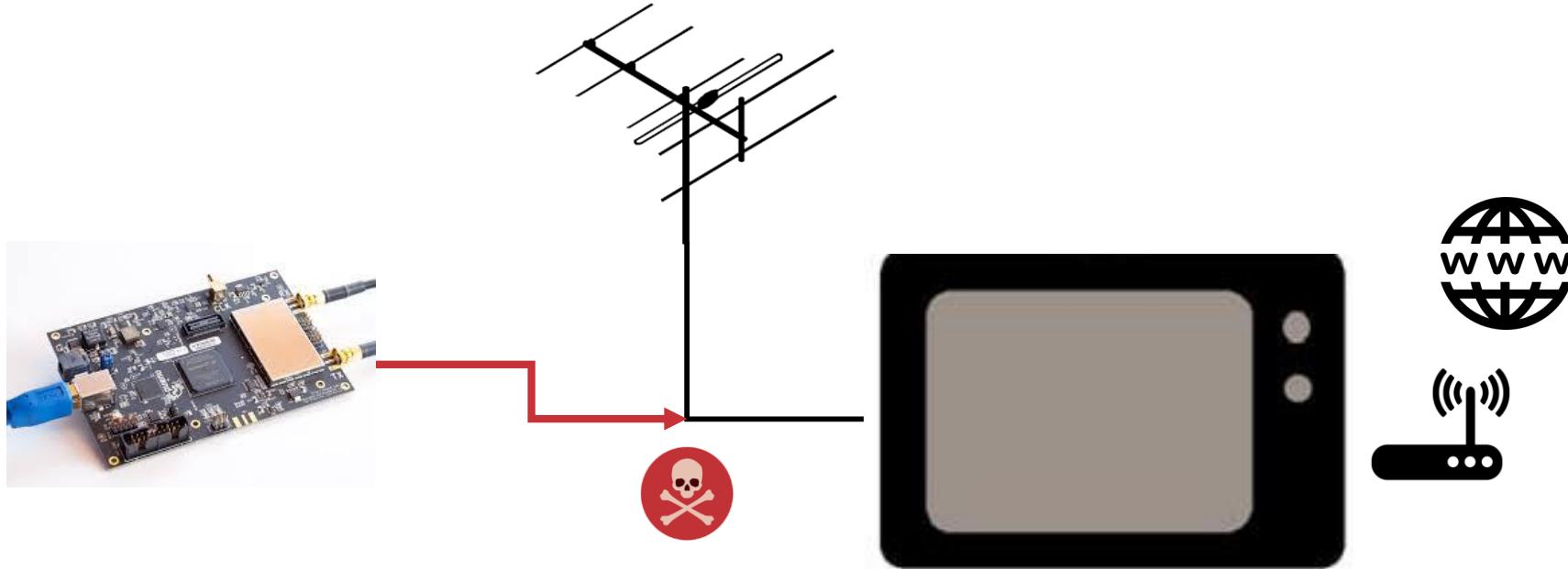
2018 March, Pedro Cabrera



Ataques a instalaciones de antena

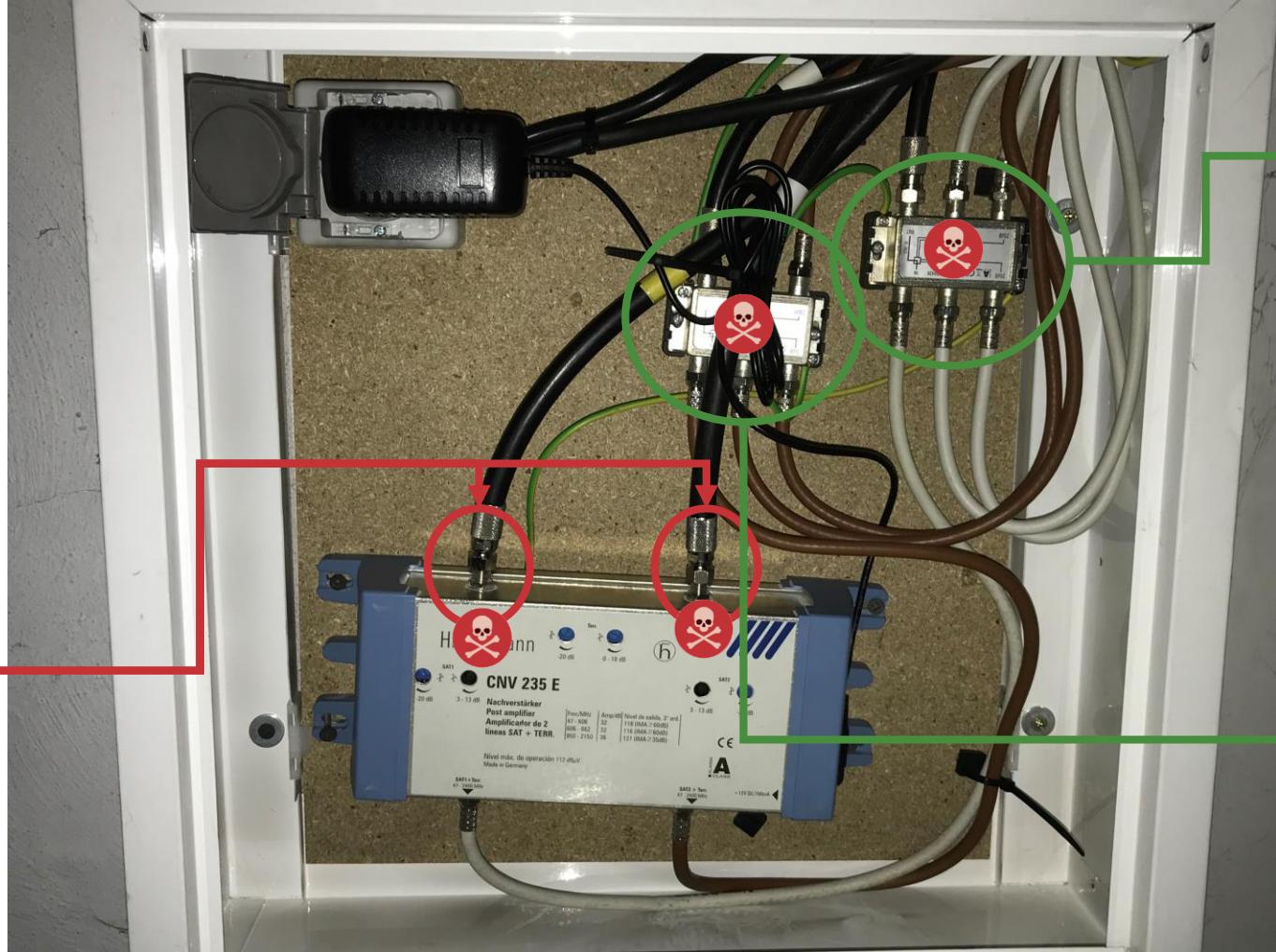
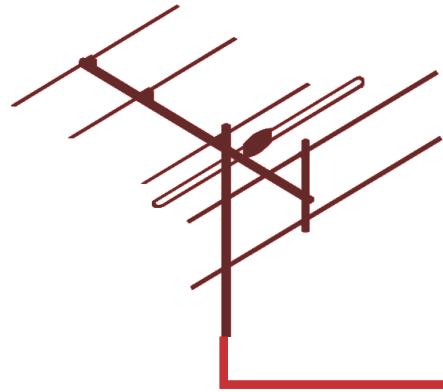


Podemos eliminar la etapa radio inyectando nuestra señal en la instalación de la antena.





Ataques a instalaciones de antena



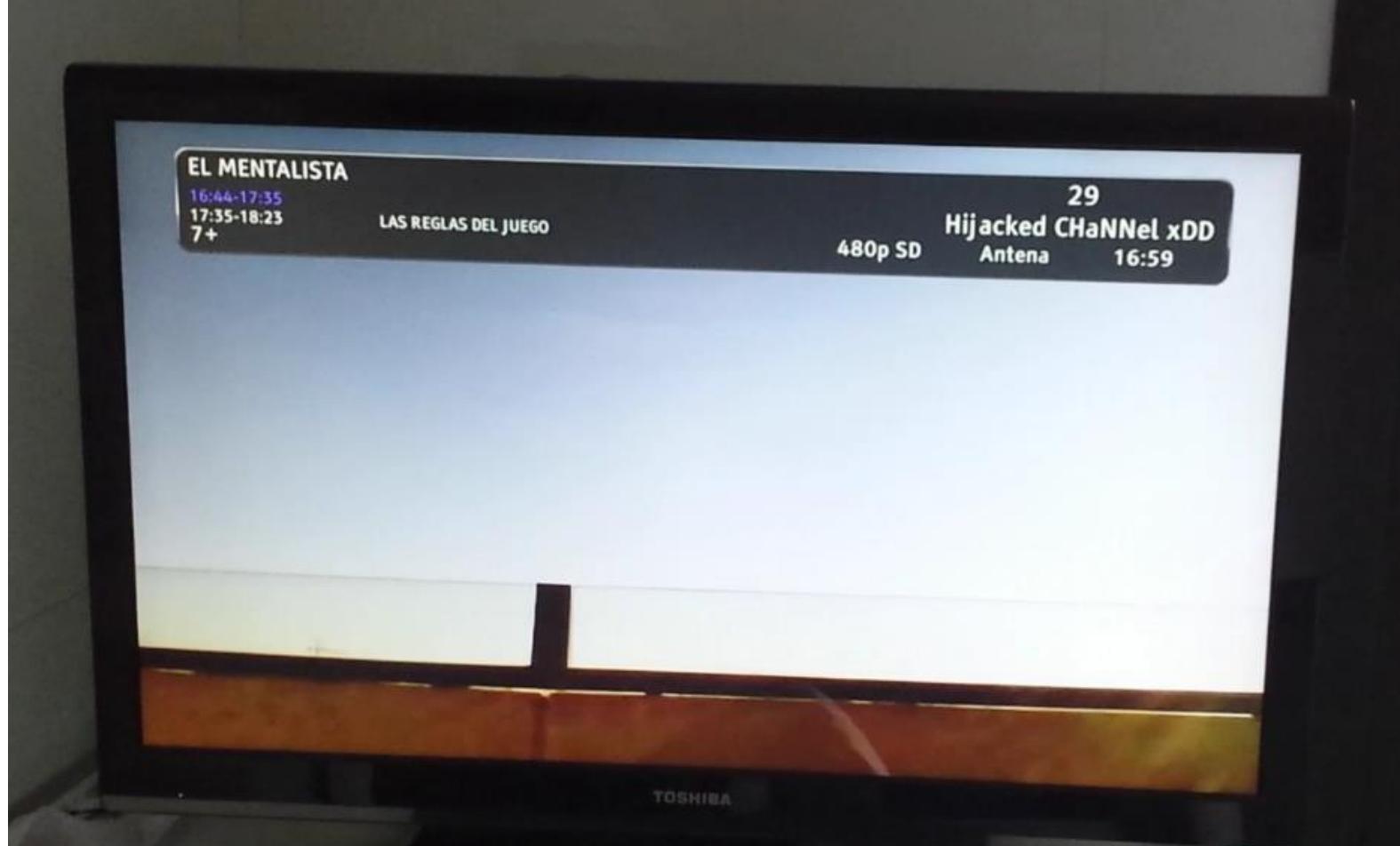
x4

x4



/Rooted® CON

Ataques instalaciones - Demo video



2018 March, Pedro Cabrera



SDR 2011/14



* Año aparición

2011

2013

2013

2014

SDR Name	RTL-SDR		HackRF	bladeRF		USRP		
Model	E4000	R820T		X40	X115	B200	B210	N210
Radio Spectrum	52–2200 MHz ** [-1.1 GHz - 1.25 GHz]		24–1766 MHz	30 MHz – 6 GHz	300 MHz – 3.8 GHz	50MHz – 6 GHz		WBX: 50 MHz - 2.2 GHz SBX: 400 MHz - 4.4 GHz
Bandwidth	2.4 Mhz		20 MHz	28 MHz		61.44 MHz		40 MHz (SBX and WBX)
Duplex	Half (and not TX)		Half (TX/RX)	Full		Full	2x2 MIMO	Full
Sample Size (ADC/DAC)	8 bits		8 bit	12 bit		12 bit		14-bit ADC 16-bit DAC
Sample Rate (ADC/DAC)	2.4 Msps		20 Msps	40 Msps		61.44 Msps		100 Msps ADC 400 Msps DAC
Interface (Speed)	USB 2 HS (480 megabit)		USB 2 HS (480 megabit)	USB 3 (5 gigabit)		USB 3 (5 gigabit)		Gigabit Ethernet
FPGA Logic Elements	NA		NA	40k	115k	75k	150k	3400k
Microcontroller	NA		LPC43XX	Cypress FX3		Cypress FX3		Spartan 3A-DSP 3400 FPGA



SDR en 2018



* Año aparición

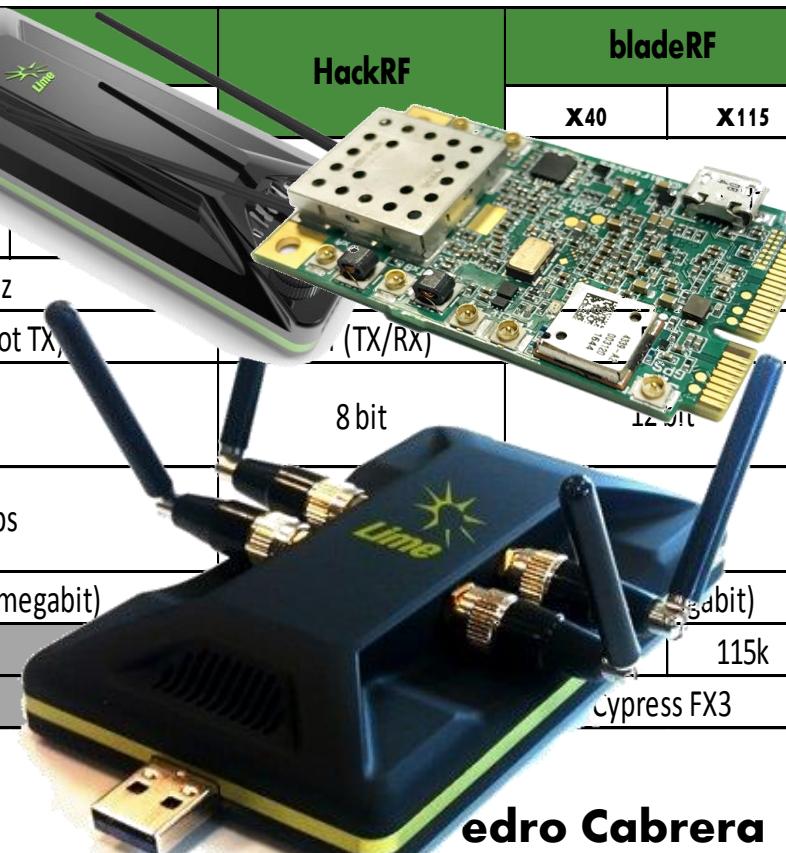
2011

2013

2013

2014

SDR Name	HackRF	bladeRF	USRP		
Model	E400	X40	B200	B210	N210
Radio Spectrum	52 – 2200 MHz ** [-1.1 GHz - 1.25 GHz]		50MHz – 6 GHz	WBX: 50 MHz - 2.2 GHz SBX: 400 MHz - 4.4 GHz	
Bandwidth	2.4 Mhz		61.44 MHz	40 MHz (SBX and WBX)	
Duplex	Half (and not TX)		Full	2x2 MIMO	Full
Sample Size (ADC/DAC)	8 bits	8 bit	12 bit	14-bit ADC 16-bit DAC	
Sample Rate (ADC/DAC)	2.4 Msps		61.44 Msps	100 Msps ADC 400 Msps DAC	
Interface (Speed)	USB 2 HS (480 megabit)	(5 gigabit)	USB 3 (5 gigabit)	Gigabit Ethernet	
FPGA Logic Elements	NA	115k	75k	150k	3400k
Microcontroller	NA	Cypress FX3	Cypress FX3	Spartan 3A-DSP 3400 FPGA	



edro Cabrera



XTRX

#**Miniaturización**

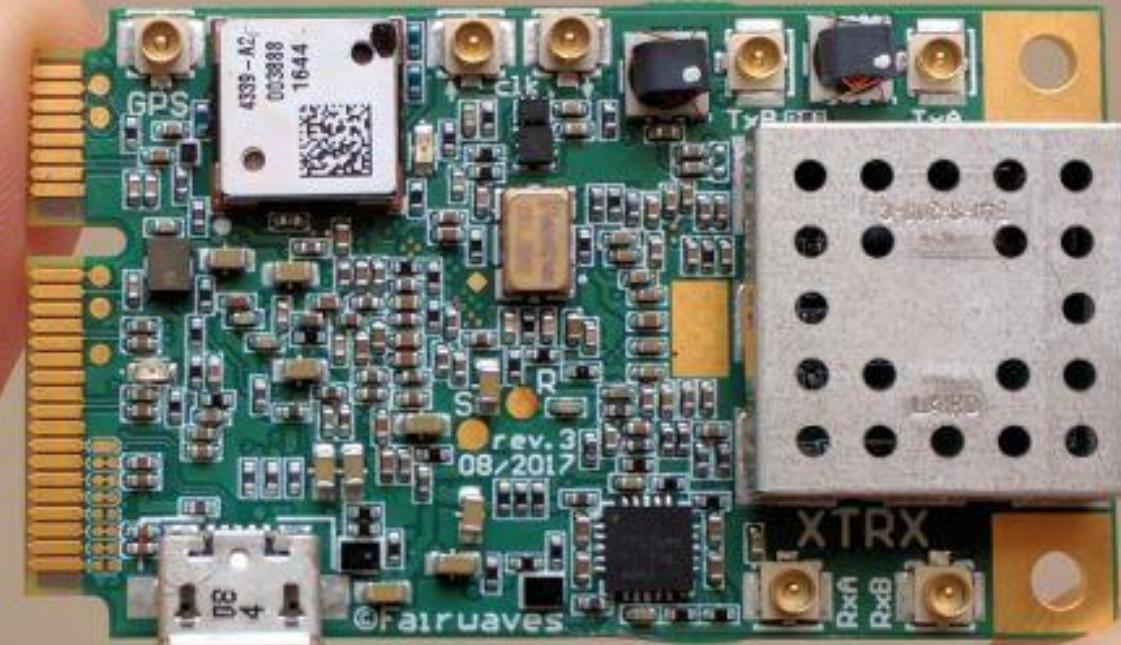
miniPCIe

2×2 MIMO

LMS7002M

100kHz – 3.8Ghz

120MHz BW



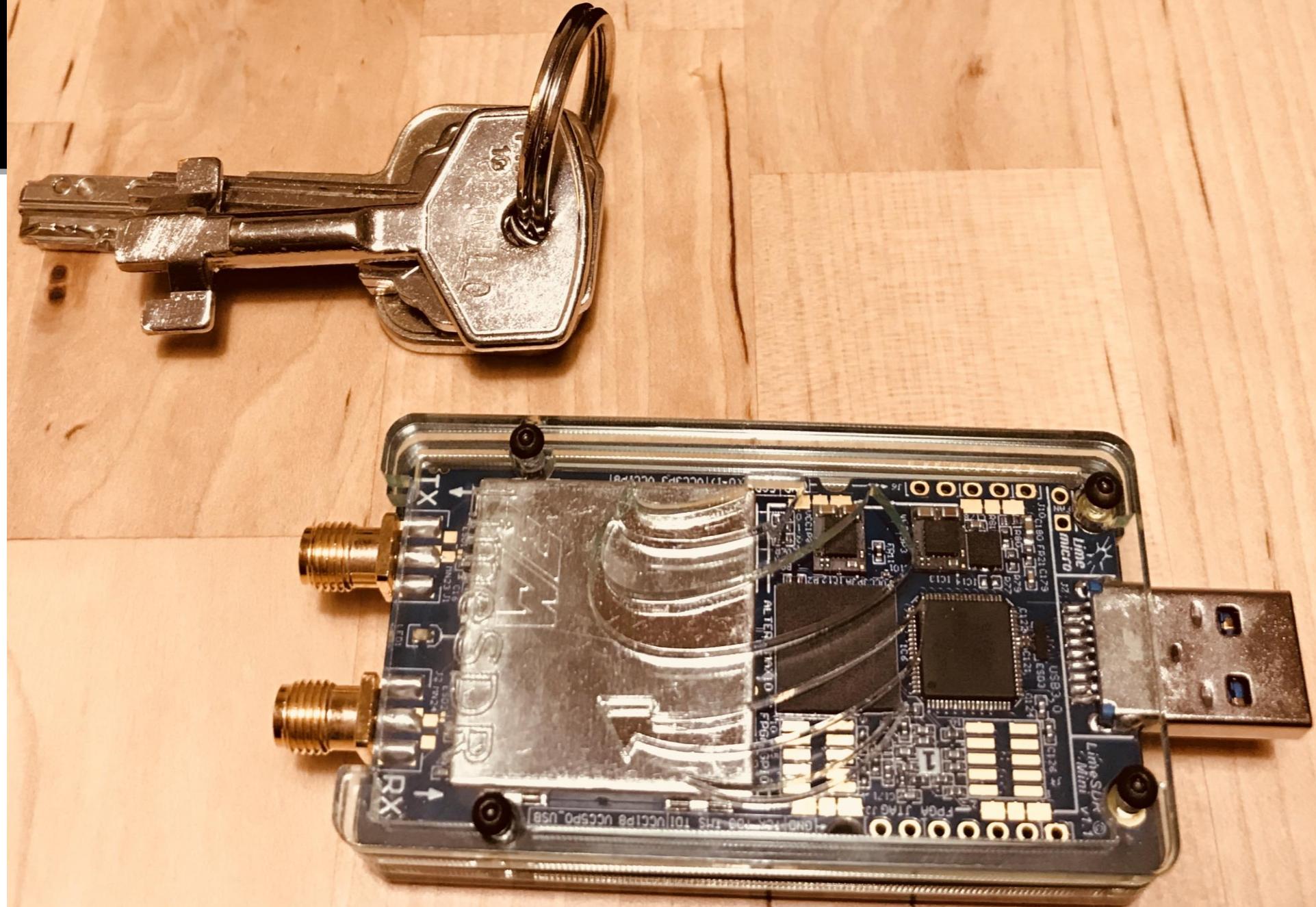


LimeSDR mini

#Miniaturización

USB 3.0

LMS7002M
100kHz – 3.8Ghz
120MHz BW





Miniaturización ?

Madrid > Fotografía y vídeo > Drones > Alquiler Dron Phantom 3 st

Alquiler de Dron Phantom 3 st

100.00 € por día

Carlos hace descuentos en función de la duración del alquiler.

Fin de semana (3 días): **250,00 €**

Semana (7 días): **450,00 €**

Desde el

dd/mm/aaaa

Hasta el

dd/mm/aaaa

Reservar



The DJI Phantom 3 Standard is among the most popular drones of all time to date. Despite its design geared towards aerial photography, this does not stop it from being able to lift an additional payload. The DJI Phantom 3 Standard can lift around an additional 300 grams, or

Fuente: <https://www.uavsystemsinternational.com/how-much-weight-can-a-drone-lift/>

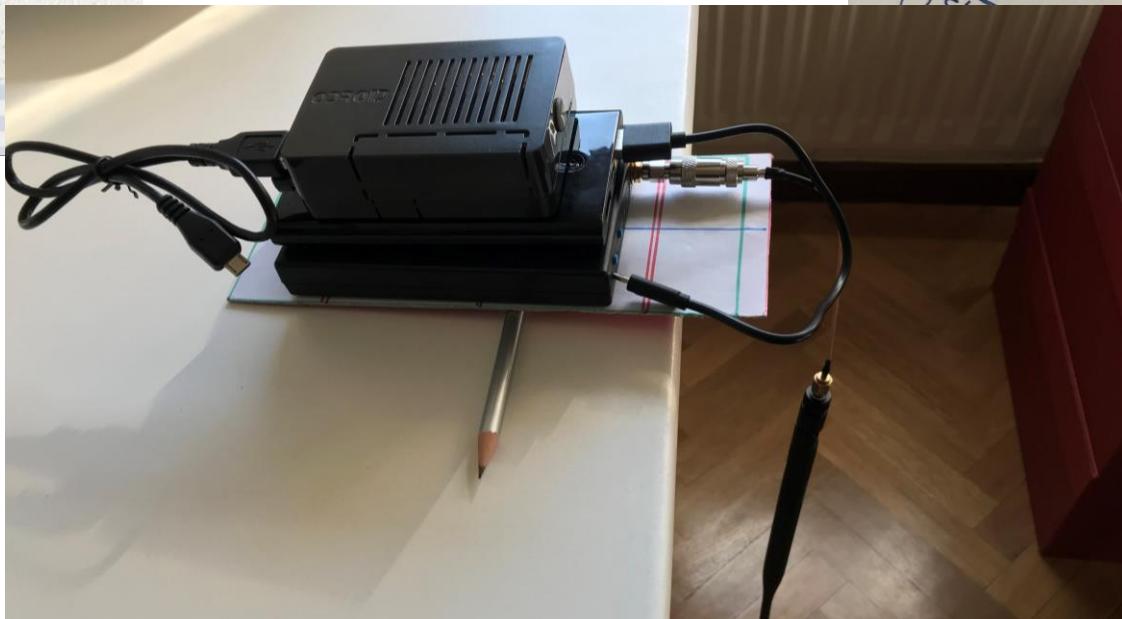
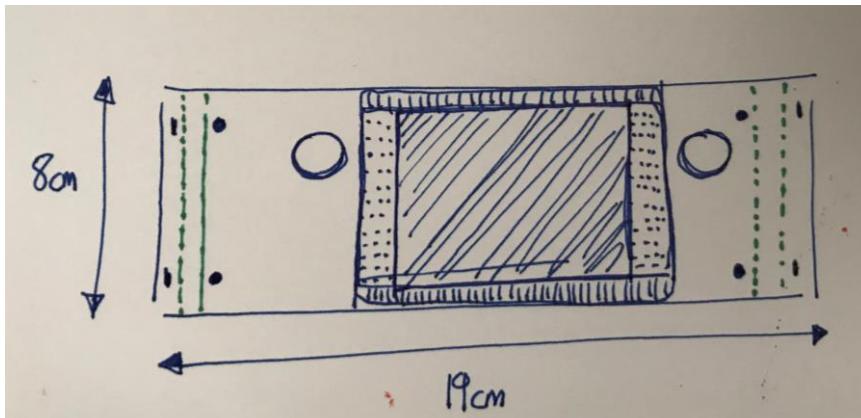
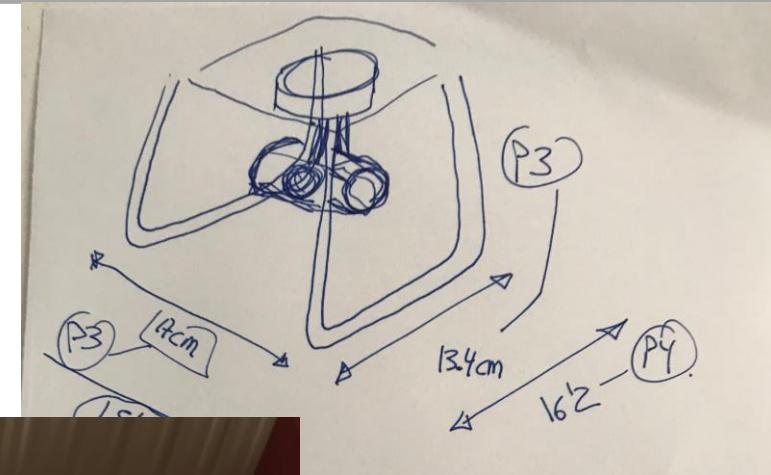
2018 March, Pedro Cabrera



Miniaturización ? - Drone attacks



300 gr



GPD	480gr
BladeRF	170gr
HackRF	100gr
Bateria iPhone 10.000mA	280gr
Bateria Solar 24.000mA	350gr
Bateria NeoXeo 6.000mA	100gr
Odroid C2	68gr
Carcasa Odroid	32gr



/Rooted® CON

Drone attacks - Demo video



2018 March, Pedro Cabrera

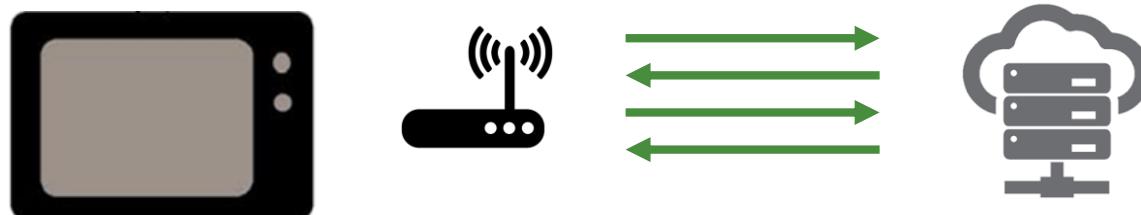


Ataque fake servidor HbbTV



Como hemos visto, el estándar HbbTV permite que las Smart TV envíen peticiones de descarga a la URL emitida por el canal (estación) cada cierto tiempo:

```
GET /api/channels/atreseries.hbbtv.x.es.smartclip/channel_config?rnd=82575690 HTTP/1.1
GET /api/channels/atreseries.hbbtv.x.es.smartclip/channel_config?rnd=82575690 HTTP/1.1
GET /api/channels/atreseries.hbbtv.x.es.smartclip/channel_config?format=jsonp&rnd=87488938&callback=smartns_channel_
GET /api/channels/atreseries.hbbtv.x.es.smartclip/channel_config?format=jsonp&rnd=87488938&callback=smartns_channel_
GET /api/channels/atreseries.hbbtv.x.es.smartclip/channel_config?rnd=71453005 HTTP/1.1
GET /api/channels/atreseries.hbbtv.x.es.smartclip/channel_config?rnd=71453005 HTTP/1.1
GET /api/channels/atreseries.hbbtv.x.es.smartclip/channel_config?format=jsonp&rnd=43032479&callback=smartns_channel_
GET /api/channels/atreseries.hbbtv.x.es.smartclip/channel_config?format=jsonp&rnd=43032479&callback=smartns_channel_
GET /api/channels/atreseries.hbbtv.x.es.smartclip/current_adstatus?rnd=0B0A2F0A-5631-6559-0405-A65502695E8F.1825499
GET /api/channels/atreseries.hbbtv.x.es.smartclip/current_adstatus?rnd=0B0A2F0A-5631-6559-0405-A65502695E8F.1825499
GET /api/channels/atreseries.hbbtv.x.es.smartclip/current_adstatus?format=jsonp&rnd=0B0A2F0A-5631-6559-0405-A65502695E8F.1825499
GET /api/channels/atreseries.hbbtv.x.es.smartclip/current_adstatus?format=jsonp&rnd=0B0A2F0A-5631-6559-0405-A65502695E8F.1825499
GET /api/channels/atreseries.hbbtv.x.es.smartclip/channel_config?rnd=64878329 HTTP/1.1
```

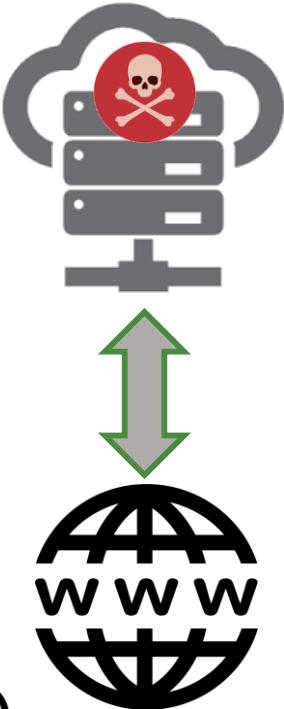
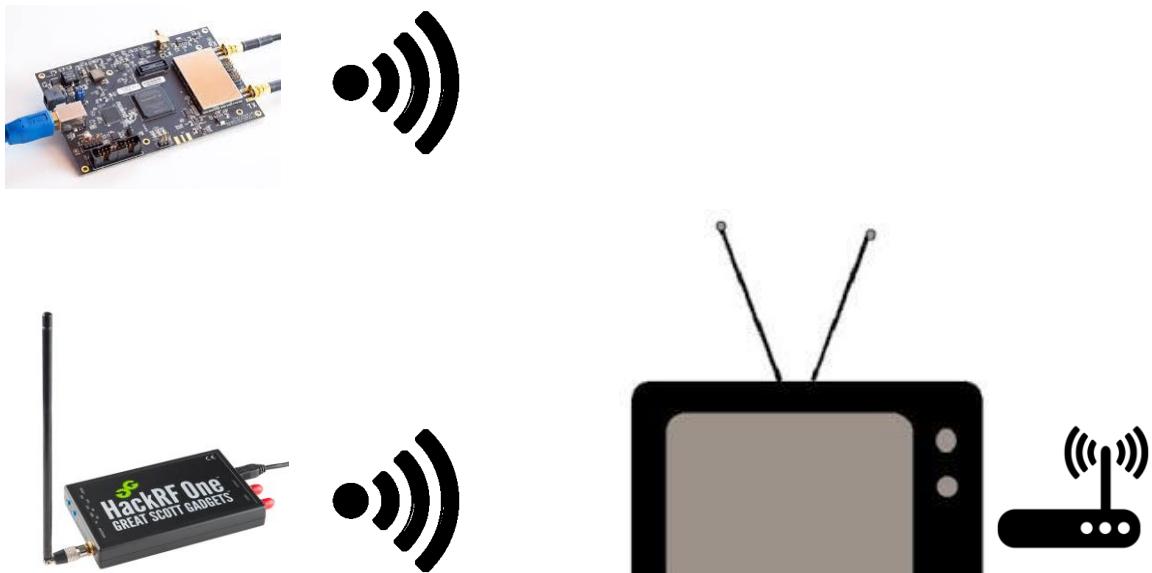




Ataque fake servidor HbbTV



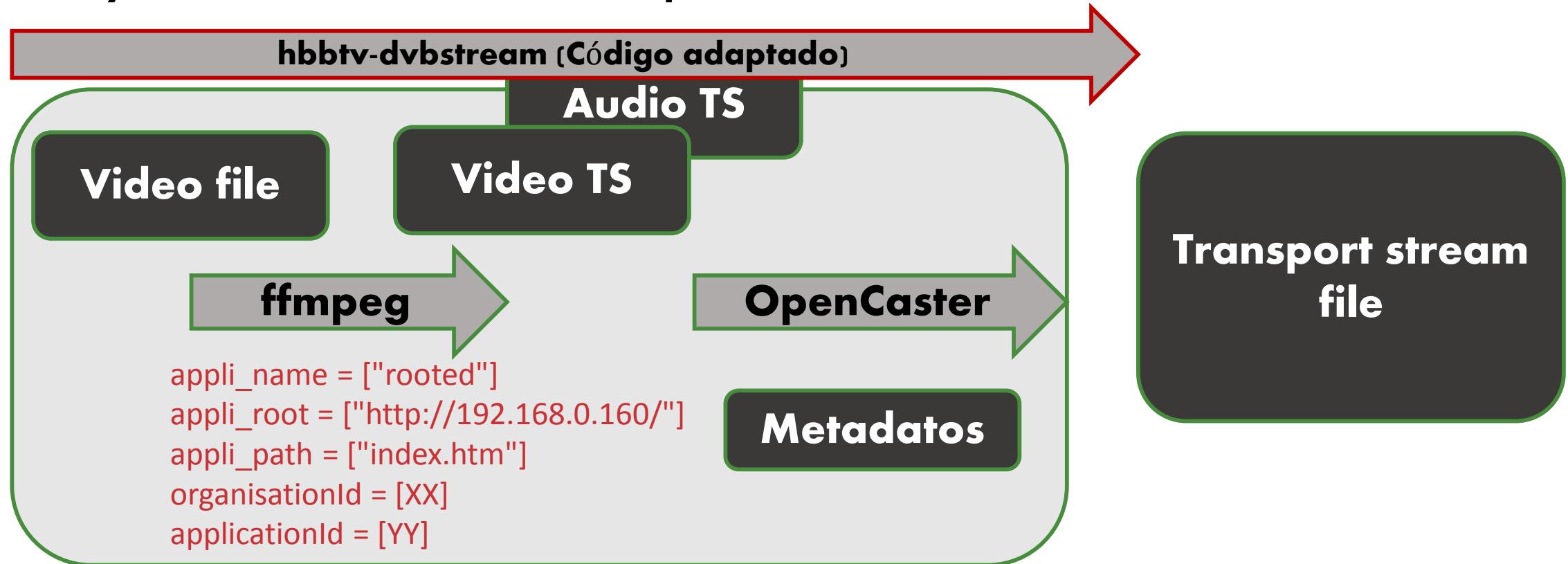
Añadimos la URL de nuestro servidor fake en los metadatos HbbTV: nombre de aplicación, URL base, web page, organisationId y applicationId





Ataque fake servidor HbbTV

Antes de emitir, debemos generar un fichero “Transport Stream” TS con los parámetros del canal inyectando la URL de nuestro ataque:





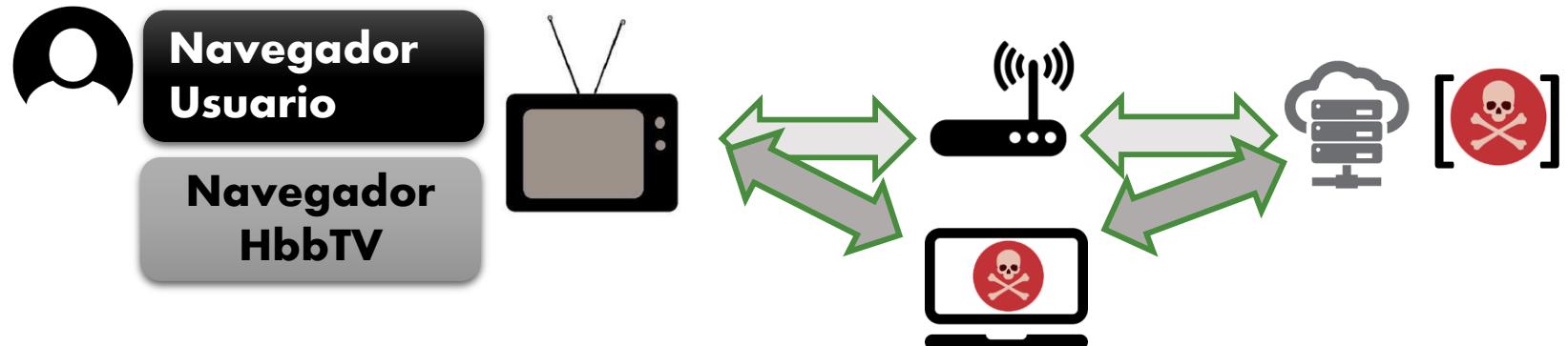
1 SmartTV - 2 navegadores web



**Navegador
web HbbTV**



**Navegador web
Usuario (SO) &
HbbTV**





UA de los navegadores web

Ej. Samsung:

HbbTV/1.2.1 (+DRM+TVPLUS;Samsung;SmartTV2017;T-KTMDEUC-1106.2;;)

**Mozilla/5.0 (SMART-TV; Linux; Tizen 3.0) AppleWebKit/537.36 (KHTML, like Gecko)
SamsungBrowser/2.0 Chrome/47.0.2526.69 TV safari/537.36**

Ej. Panasonic:

HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)

**Mozilla/5.0 (X11; FreeBSD; U; Viera; es-ES) AppleWebKit/537.11 (KHTML, like Gecko)
Viera/3.10.14 Chrome/23.0.1271.97 Safari/537.11**



Smart (TV) scanning

Apache Log files:

- Dirección IP pública
- Busqueda de modelos/marcas (UA)
- Análisis audiencias TDT/canales

```
Terminal - root@babieca:/var/log/apache2
Archivo Editar Ver Terminal Pestañas Ayuda
10.0.0.60 - - [20/Feb/2018:13:03:02 +0100] "GET /lasexta/app/scenes/Score.js HTTP/1.1" 200 794 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:03:02 +0100] "GET /lasexta/app/scenes/ShortcutToScene.js HTTP/1.1" 200 498 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:03:02 +0100] "GET /lasexta/resources/language/langConfig.js HTTP/1.1" 200 358 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:03:02 +0100] "GET /lasexta/resources/language/eng.js HTTP/1.1" 200 441 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:03:02 +0100] "GET /lasexta/app/javascripts/phaser.js HTTP/1.1" 200 432897 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:04:40 +0100] "GET /lasexta/index.html HTTP/1.1" 200 806 "-" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:04:40 +0100] "GET /lasexta/app/javascripts/head_min.js HTTP/1.1" 200 3849 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:04:40 +0100] "GET /lasexta/app/loader.js HTTP/1.1" 200 811 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:04:40 +0100] "GET /lasexta/app/stylesheets/styleSheet.css HTTP/1.1" 200 600 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:04:40 +0100] "GET /lasexta/app/stylesheets>Loading.css HTTP/1.1" 200 420 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:04:40 +0100] "GET /lasexta/app/stylesheets/MainMenu.css HTTP/1.1" 200 584 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:04:40 +0100] "GET /lasexta/app/stylesheets/GameState.css HTTP/1.1" 200 726 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:04:40 +0100] "GET /lasexta/app/stylesheets/Score.css HTTP/1.1" 200 416 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:04:40 +0100] "GET /lasexta/app/javascripts/jquery.js HTTP/1.1" 200 72895 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:04:40 +0100] "GET /lasexta/app/javascripts/state_machine.js HTTP/1.1" 200 2796 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:04:40 +0100] "GET /lasexta/app/javascripts/srtObjects.js HTTP/1.1" 200 5240 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:04:40 +0100] "GET /lasexta/app/common.js HTTP/1.1" 200 2906 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:04:40 +0100] "GET /lasexta/app/javascripts/soundPlayer.js HTTP/1.1" 200 9130 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
```



/Rooted® CON

Ingeniería social



The central digital overlay contains the following text and interface elements:

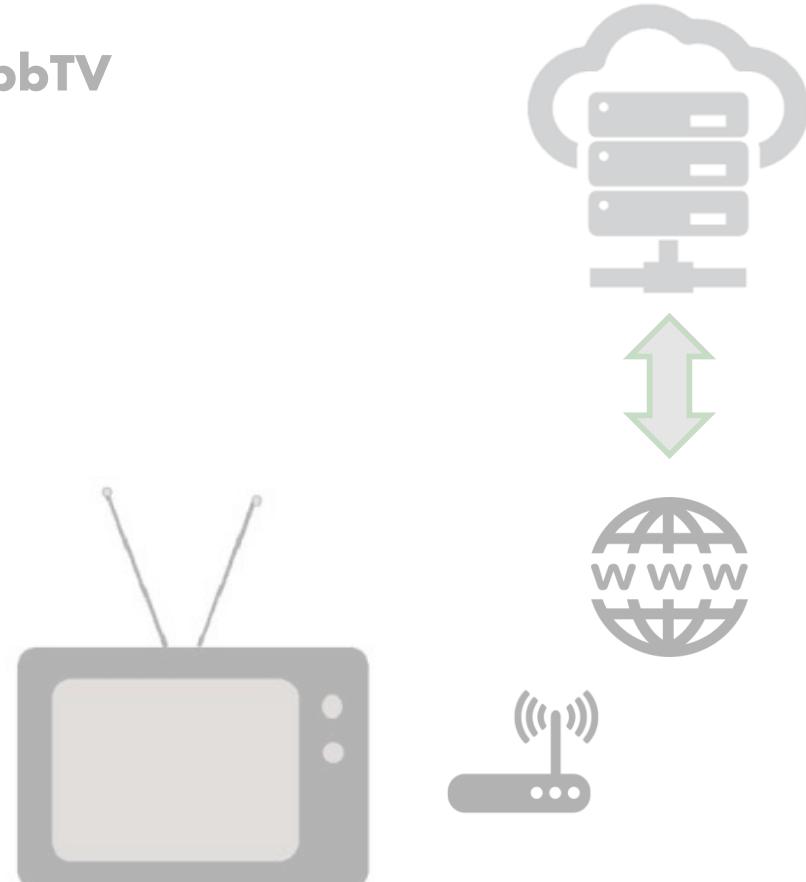
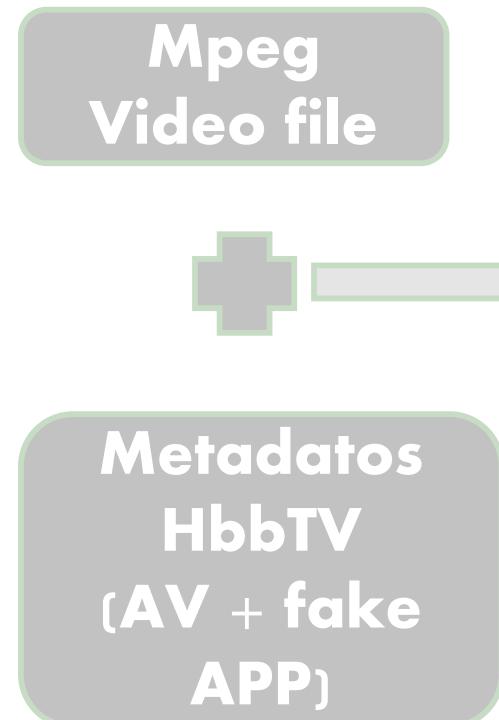
- A large black rectangle with the text "/Rooted® CON" in white.
- Below it, a smaller box displays the message "Wifi ESSID (name) confirmation needed:" followed by the text "Home-Wifi".
- A blue QWERTY keyboard is shown below the text input field.
- At the bottom of the keyboard area are two buttons: "Aceptar" (Accept) and "Borrar" (Delete).
- To the right of the keyboard, there is a blue banner with the text "aegon.es" and the phone number "900 303 903".
- At the bottom left of the screen, there is small text: "Precio final/mes/asegurado, para nuevas contrataciones de p... y contratando cuadro médico nacional. No incluida tasa de liquidación de entidades aseguradoras. Sujeto a resto normas de suscripción. Más información en aegon.es".
- At the bottom right, there is additional small text: "44 años, residentes en zona geográfica incluida en promoción".



Ataque fake servidor HbbTV



Añadimos la URL de nuestro servidor fake en los metadatos HbbTV





Keylogger Javascript



Buenos días !!, Cómo es sábado, por favor se bueno e introduce en el siguiente campo tú número de tarjeta y lee detenidamente el texto:

[Redacted]

Open me And drink up my scarlet Kiss me deep Kiss me deep and love me forever more Bloody love Bloody love inside of you Swallow me Thank God, there's nothing I can do	Come with me my friend, come and see the end And let me swallow up your pain Leave the village lights, step into the night Open your mouth to my bloody rain And at your second birth, we will slay the earth And stalk mankind 'till Heaven burns Just lay down for me, naked for me to see It's just one kiss, that's all I need	Take me down Down to the bloody shore Dig me deep, dig me deep And leave me forever more Lay me down Down with all of them And forget me Like you forgot the rest of them
--	---	--



Minado de criptomonedas



Cuidado con los anuncios de YouTube, algunos aprovechan tu CPU para hacer minería de criptomonedas

Fuente:

<https://www.xataka.com/seuridad/cuidado-con-los-anuncios-de-youtube-algunos-aprovechan-tu-cpu-para-hacer-mineria-de-criptomonedas>

La Controversia Alrededor de los Mineros
JavaScript

Fuente:

<https://blog.sucuri.net/espanol/2017/09/sitios-web-hackeados-minan-criptomonedas.html>

Hackers contaminan miles de páginas web para minar criptomonedas

Tecnología 12 Feb 2018 - 3:24 PM

Por: Redacción tecnología con información de AFP

Los ataques afectaron a más de 4.000 sitios web, incluidos los de la agencia británica de protección de datos y privacidad y el del sistema de tribunales federales de Estados Unidos.

Fuente:

<https://www.elespectador.com/tecnologia/hackers-contaminan-miles-de-paginas-web-para-minar-criptomonedas-articulo-738718>

Minado de criptomonedas





Hook.js navegador de usuario



Browser Version: UNKNOWN

Browser UA String: Mozilla/5.0 (SMART-TV; Linux; Tizen 3.0) AppleWebKit/537.36 (KHTML, like Gecko) Goolge/Chrome/51.0.2371.93 Mobile Safari/537.36

Browser Language: es-ES

Browser Platform: Linux armv7l

Browser Plugins: Native Client

Window Size: Width: 392, Height: 220

The screenshot shows the BeEF user interface at localhost:3000/ui/panel. On the left, there's a sidebar titled "Hooked Browsers" with sections for "Online Browsers" (listing www.youtube.com with four entries) and "Offline Browsers" (listing staticxx.facebook.com with three entries). On the right, a detailed view for www.youtube.com shows the following information:

- Category: Browser (6 Items)
- Browser Version: UNKNOWN
- Browser UA String: Mozilla/5.0 (SMART-TV; Linux; Tizen 3.0) AppleWebKit/537.36 (KHTML, like Gecko) Goolge/Chrome/51.0.2371.93 Mobile Safari/537.36
- Browser Language: es-ES
- Browser Platform: Linux armv7l
- Browser Plugins: Native Client
- Window Size: Width: 392, Height: 220
- Category: Browser Components (12)
- Flash: No
- VBScript: No
- PhoneGap: No

Below this, the "Details" tab is selected in the top navigation bar.

Metasploit Modules

Once Metasploit has been [configured](#) and launched, Metasploit modules are directly included in the BeEF command modules tree:

The screenshot shows the Metasploit module tree. The root node is "Metasploit (579)" which contains the following modules:

- Firefox 5.0 - 15.0.1 __exposedProps__ XCS Code Execution
- Firefox 8/9 AttributeChildRemoved() Use-After-Free
- Firefox Proxy Prototype Privileged Javascript Injection
- Firefox XMLSerializer Use After Free
- Firefox location.QueryInterface() Code Execution
- Firefox nsSVGValue Out-of-Bounds Access Vulnerability
- Foxit Reader Plugin URL Processing Buffer Overflow
- Mozilla Firefox 3.6.16 mChannel Use-After-Free
- Mozilla Firefox Array.reduceRight() Integer Overflow
- Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
- Mozilla Firefox Interleaved document.write/appendChild Memory Corruption
- Mozilla Suite/Firefox compareTo() Code Execution
- msf_firefox_proto_crmfreuest
- msf_firefox_proxy_prototype
- msf_firefox_queryinterface
- msf_firefox_xpi_bootstrapped_addon
- msf_foxit_reader_plugin_url_bof
- msf_mozilla_attribchildremoved



Ataque fake servidor HbbTV

androidtv

TIZEN™

webOS

Ataque inyección URL	Objetivo navegador	Base de ataque	Smart TV 1	Smart TV 2
Smart TV scanning	HbbTV	(SDR)	✓	✓
Ingeniería Social	HbbTV	(SDR)	✓	FAIL
	Usuario	DNS Hijack	✓	FAIL
KeyLogger	HbbTV	(SDR)		
	Usuario	DNS Hijack	✓	FAIL
Minado Criptomonedas	HbbTV	(SDR)	FAIL	FAIL
	Usuario	DNS Hijack	FAIL	
Beef	HbbTV	(SDR)		
	Usuario	JS Inject	✓	✓

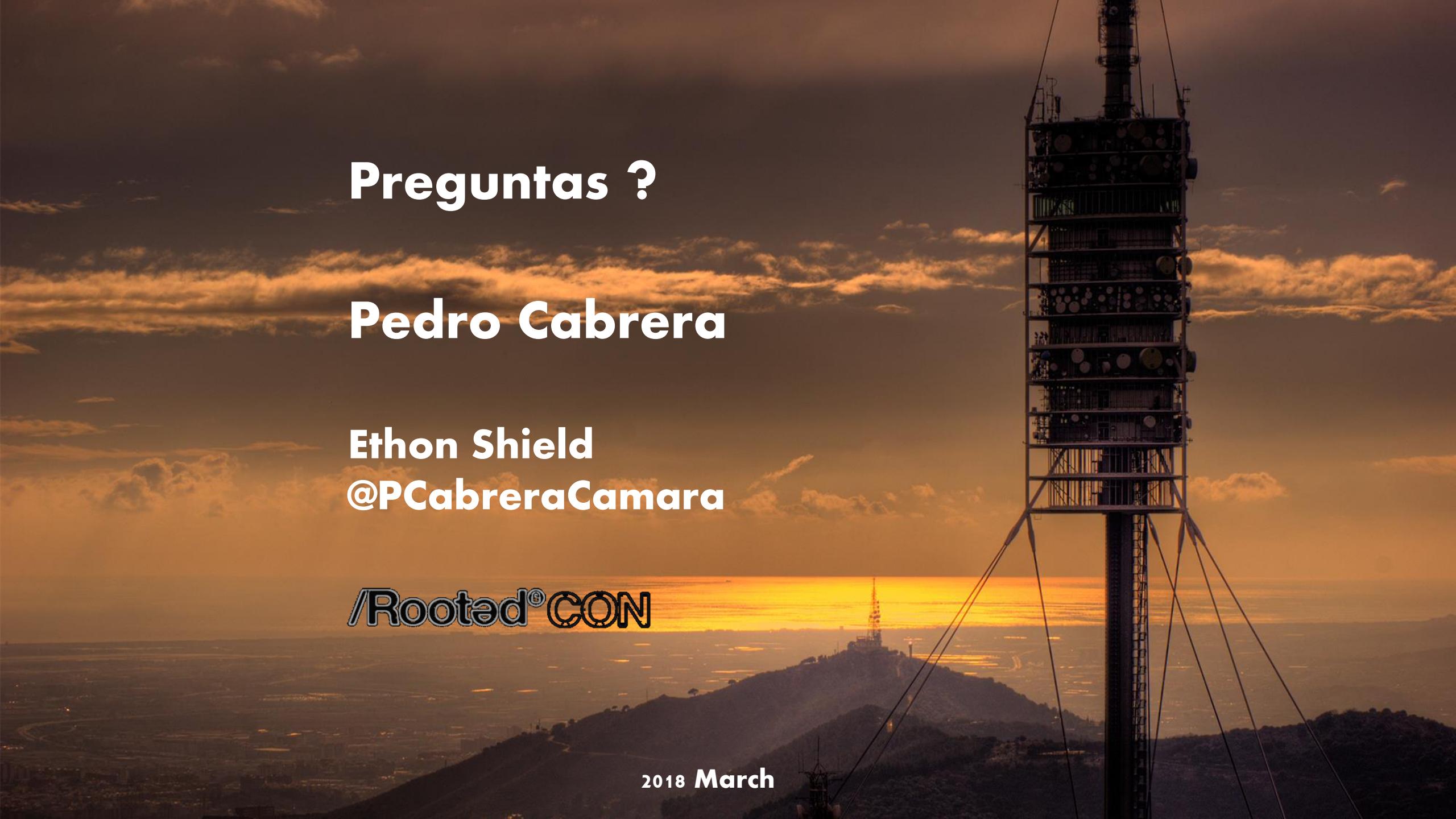
PUSH CODE

Code & Github

- S.O Linux
- GNU Radio 3.7
- Dispositivo SDR compatible con GR-OsmoSDR y capaz de emitir 8 MHZ de ancho de banda entre 470 y 790 MHz:
HackRF & BladeRF

[github.com/pcabreraCamara/
rootedCON2018](https://github.com/pcabreraCamara/rootedCON2018)

TO GITHUB



Preguntas ?

Pedro Cabrera

**Ethon Shield
@PCabreraCamara**

/Rooted®CON

2018 March