Ataques SDR a Smart TVs: URL y channel injection

2018 March, Pedro Cabrera

@PCabreraCamara

/Rooted CON

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

2018 March, Pedro Cabrera

/Rooted®CON

Hybrid Broadcast Broadband Televison

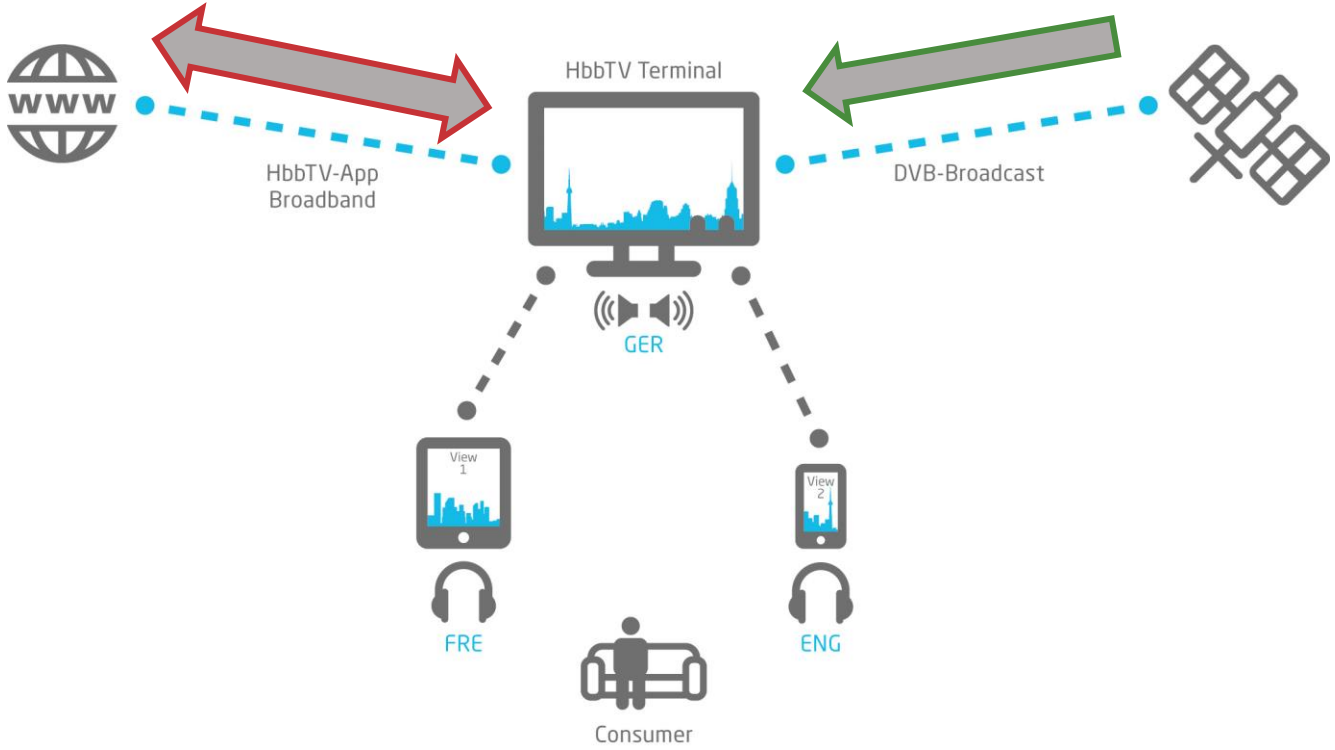
La especificación HbbTV amplía la TDT al introducir formatos de metadatos adicionales que mezclan contenido de Internet de banda ancha en el canal de televisión digital.

H4TV

HbbTV
(2009)

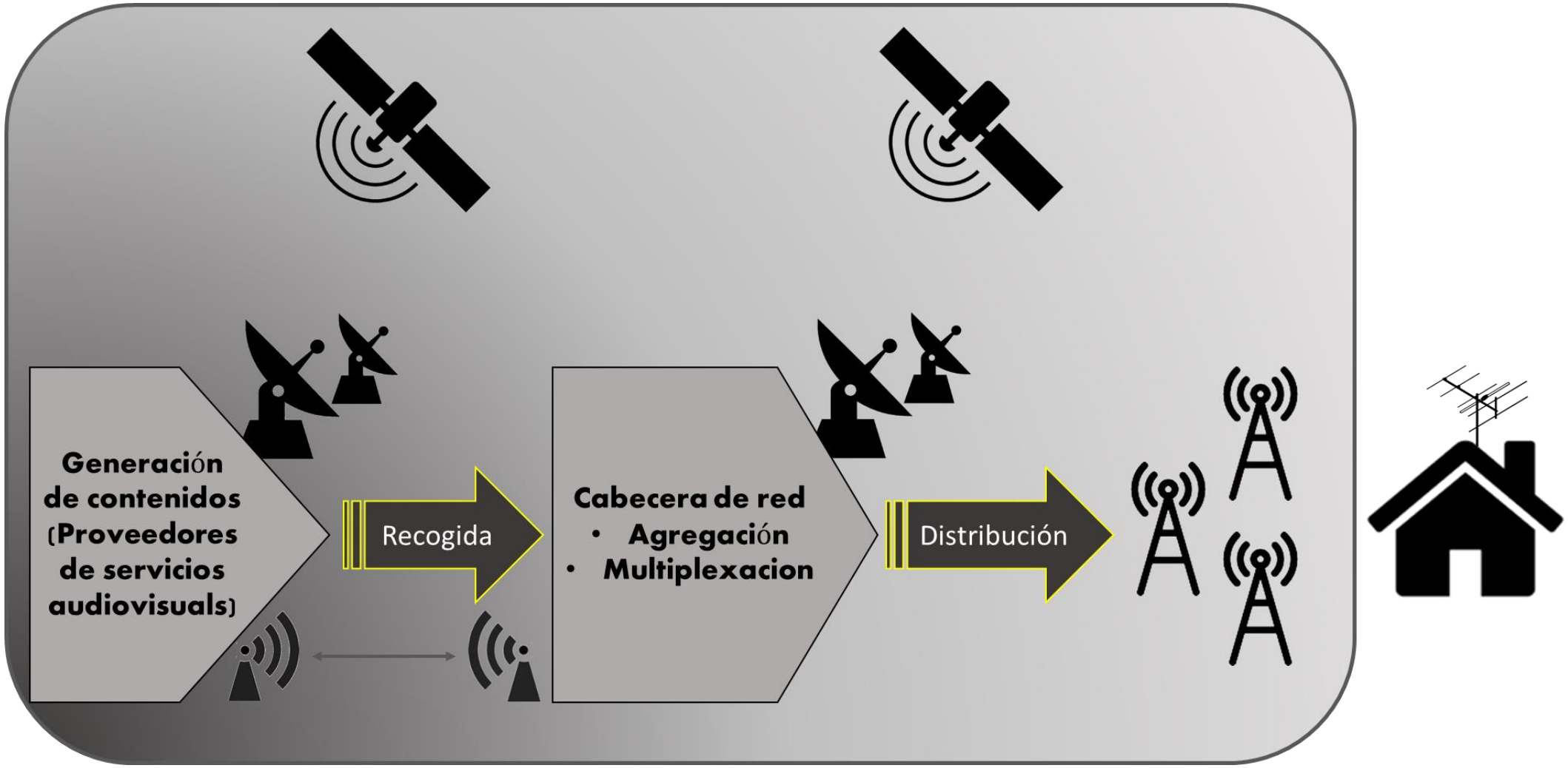
HTML Profit

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



2018 March, Pedro Cabrera

Red de distribución



Sobre TDT

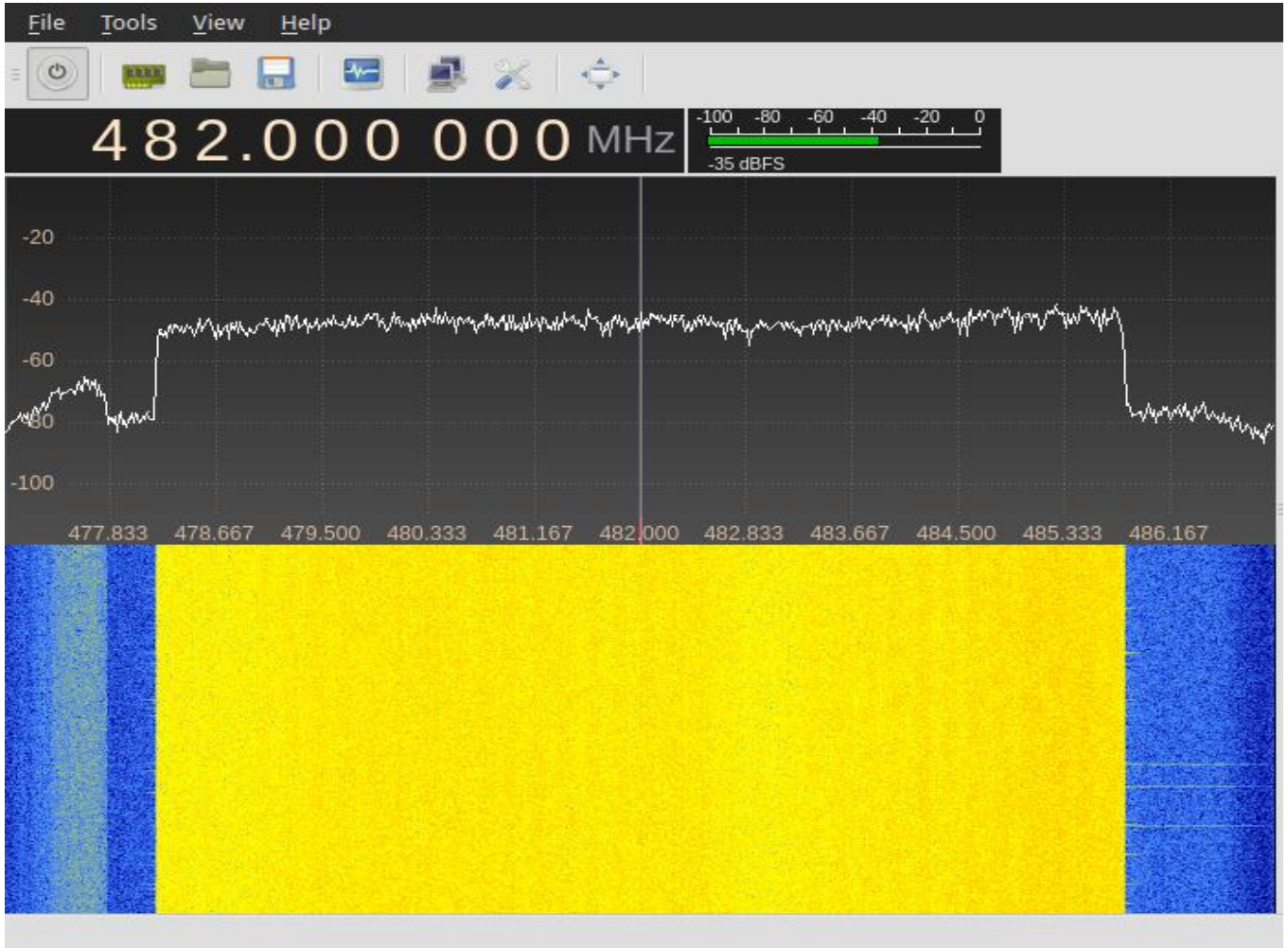
televisión digital terrestre

DVB S
DVB T
DVB C

DVB T2/C2/S2
DVB T2/C/S2
DVB T/C/S2

Modulación TDT:

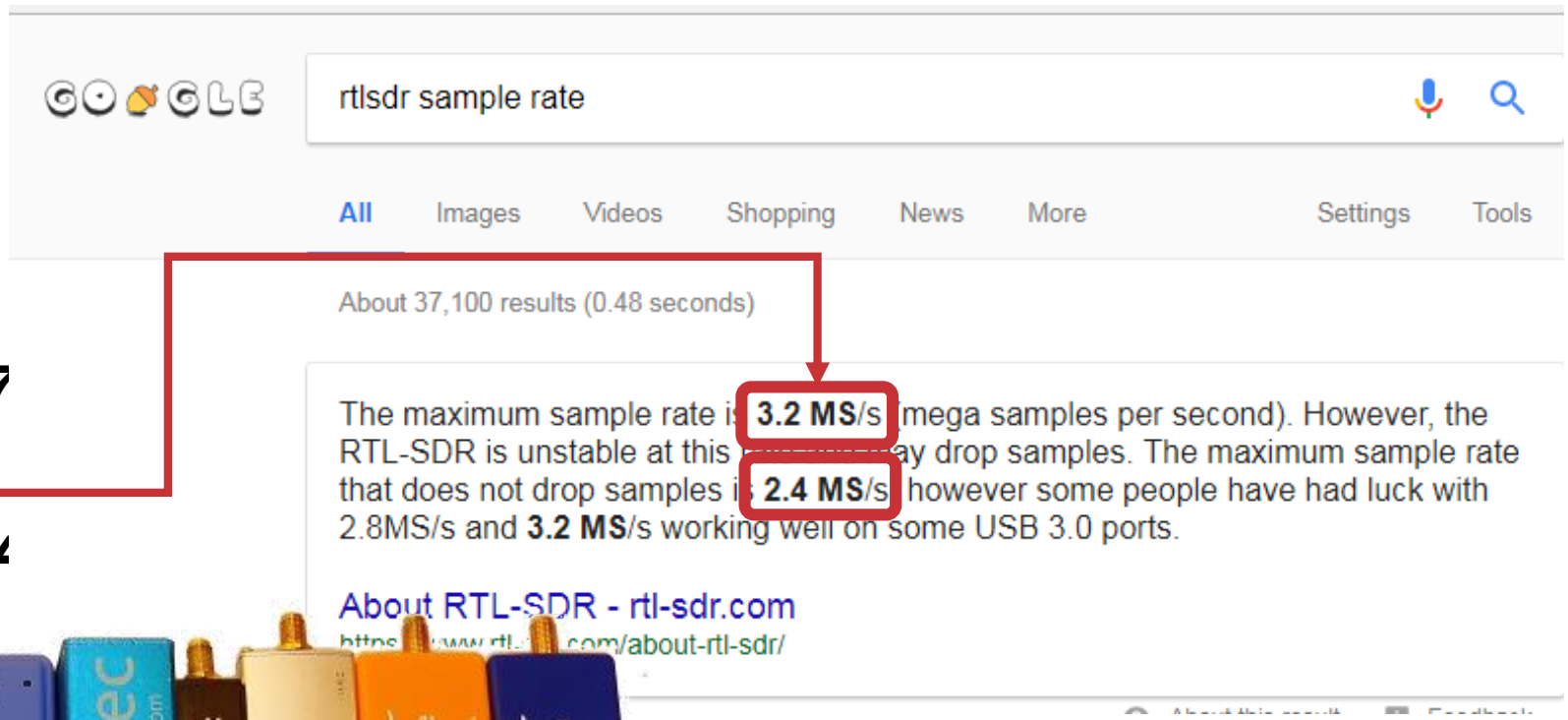
- ***Ancho de banda de 8 MHz***
- ***Modos de transmisión: 8k (6.817 portadoras).***
- ***Esquemas de modulación: 64 QAM***
- ***Code Rate para protección interna de errores: 2/3.***
- ***Longitud del intervalo de guarda: 1/4.***



Sobre TDT

Modulación TDT:

- ***Ancho de banda de 8 MHz***
- ***misión: 8k (6.817***
- ***odulación: 64 QA***
- ***errores: 2/3***
- ***Longit***

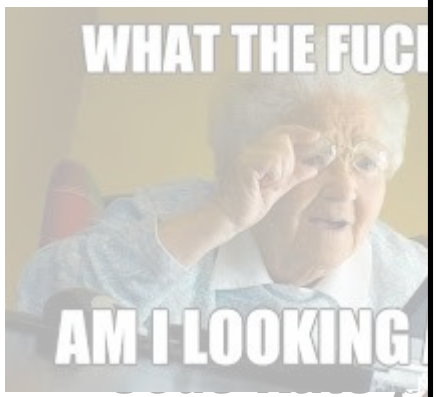


2018 March, Pedro Cabrera

Sobre TDT

Modulación TDT:

- *Ancho de ba*



errores: 2/3

- *Longit*

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 wI/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.

/Rooted CON

TDT en Linux – GNU Radio

- ***Bogdan (YO3IIU)***

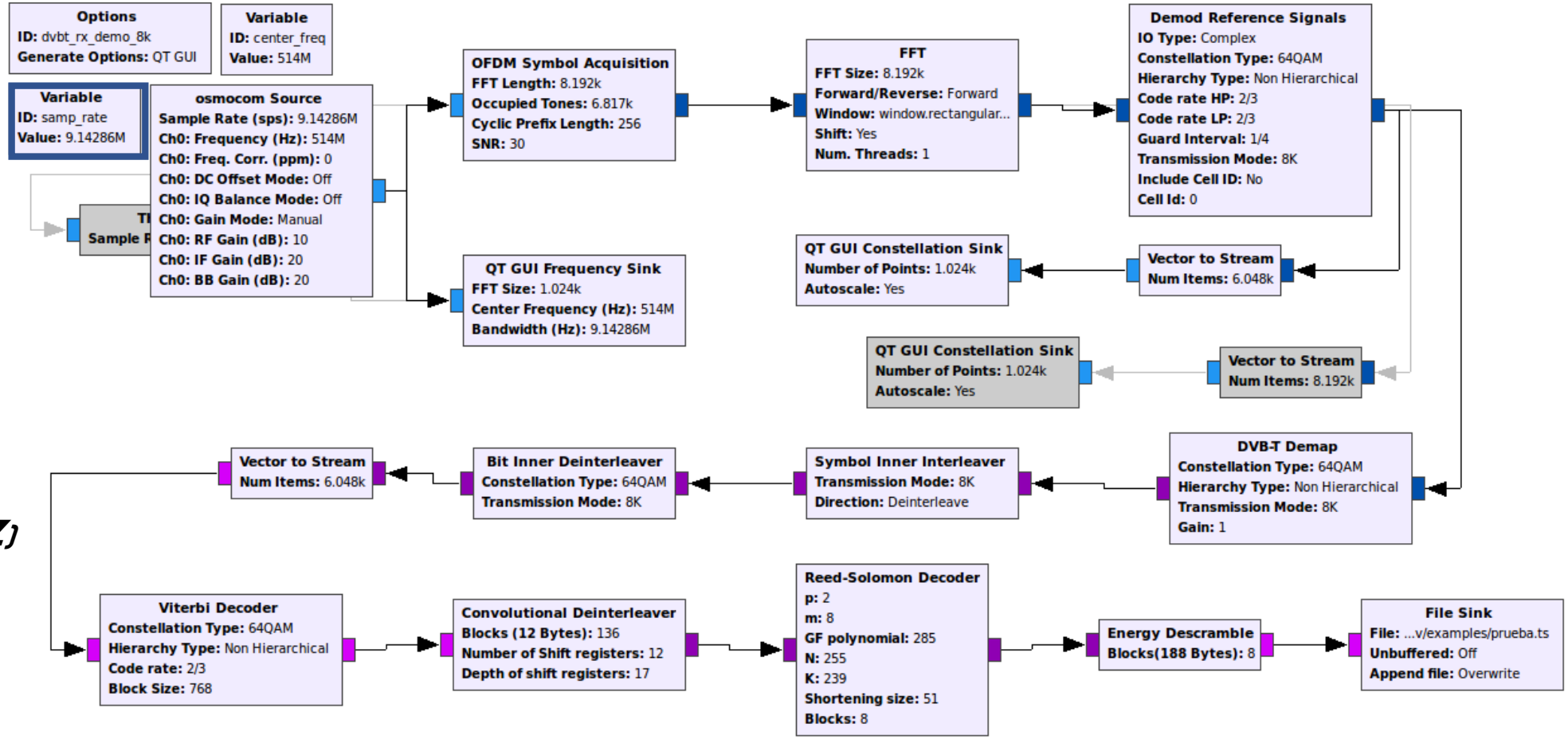
GR-DVBT
(USRP N210)

- ***GNU Radio:***

GR-DTV (USRP)

- ***Ron Economos (W6RZ)***

dtv-utils (BladeRF)



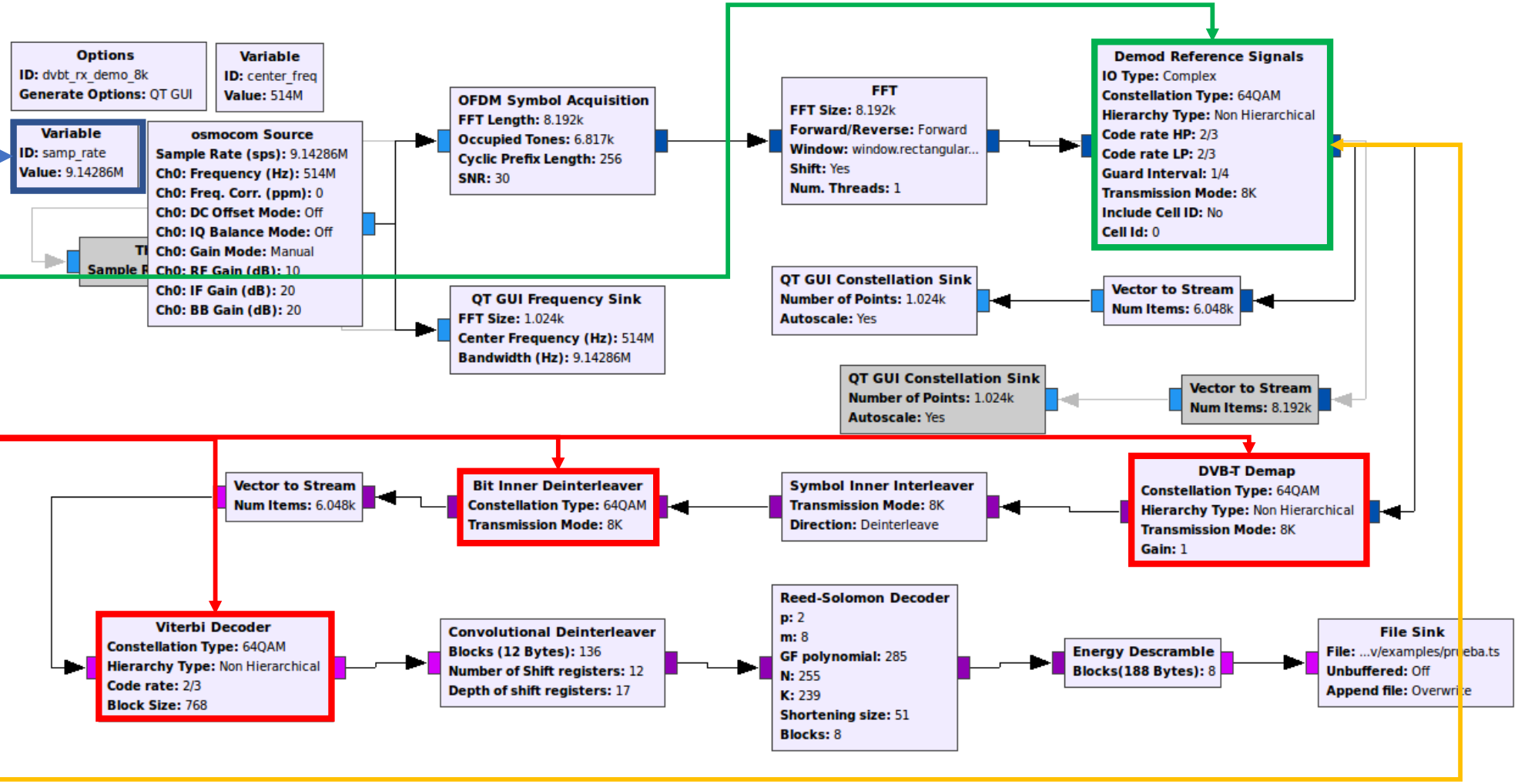
2018 March, Pedro Cabrera

/Rooted®CON

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.***



2018 March, Pedro Cabrera

/Rooted®CON

Canales TDT y Frecuencias

8 múltiples digitales:

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

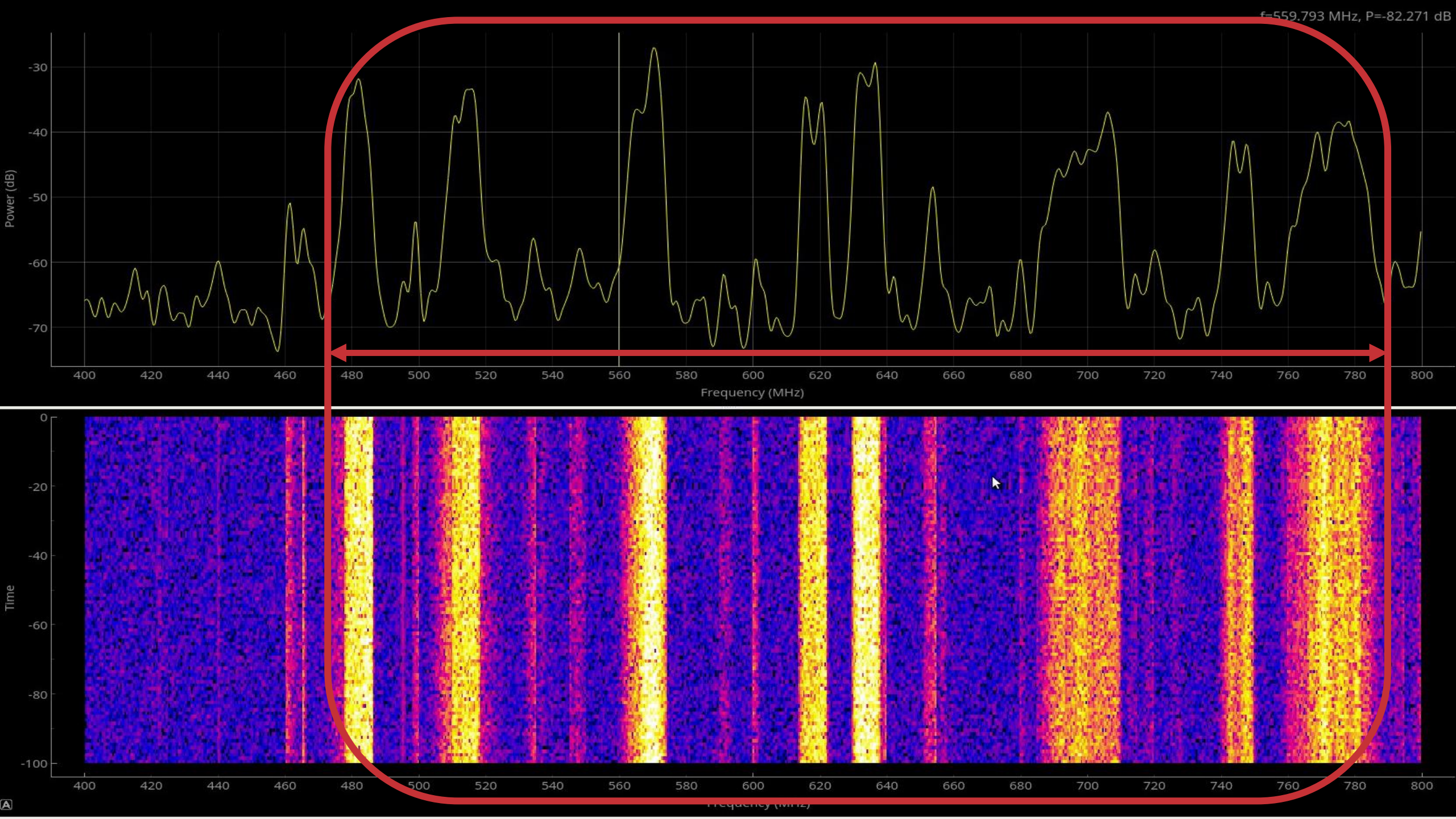
RGE: Red Global de Cobertura Estatal

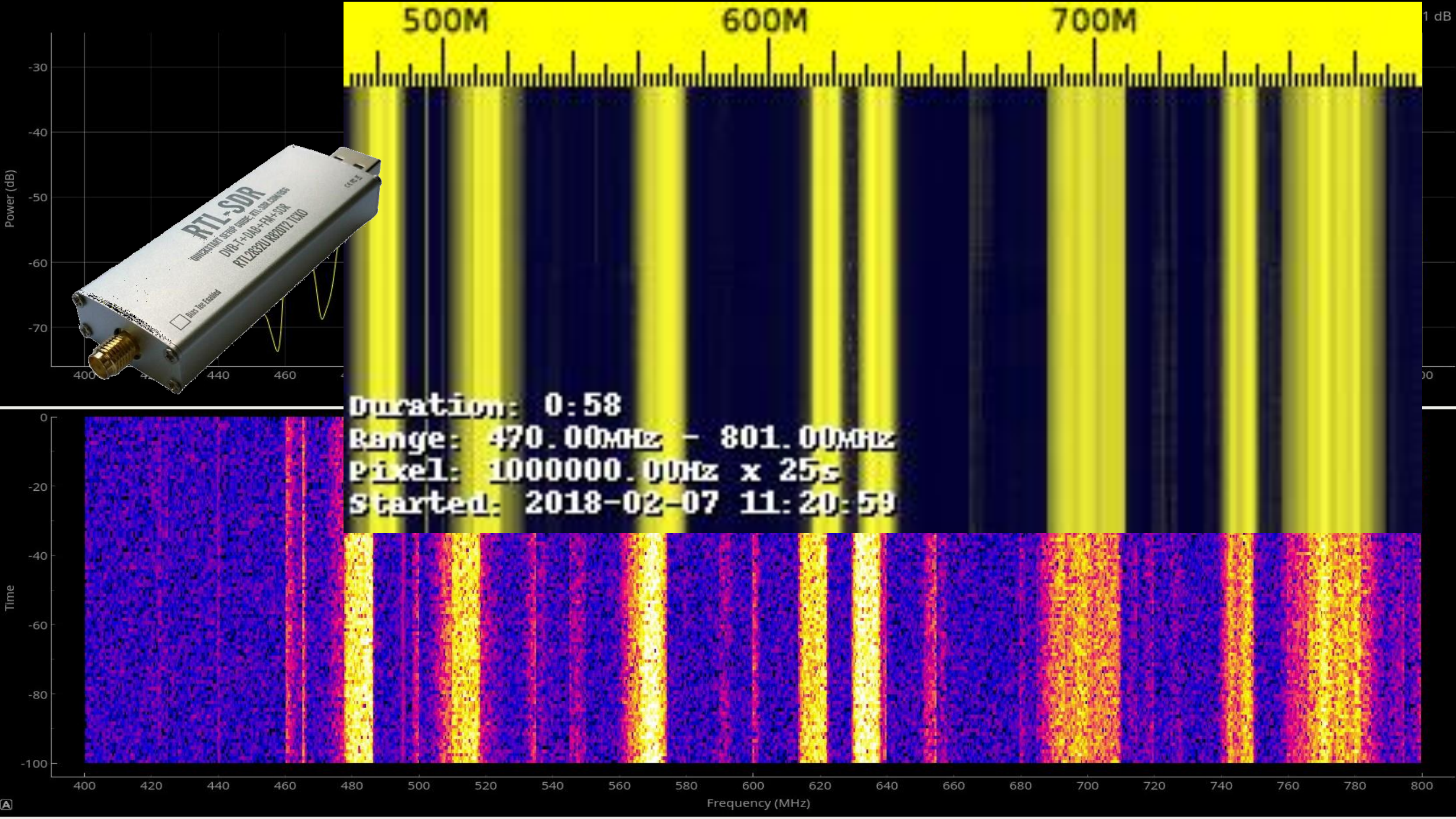
MPE: Múltiple Privado de Cobertura Estatal

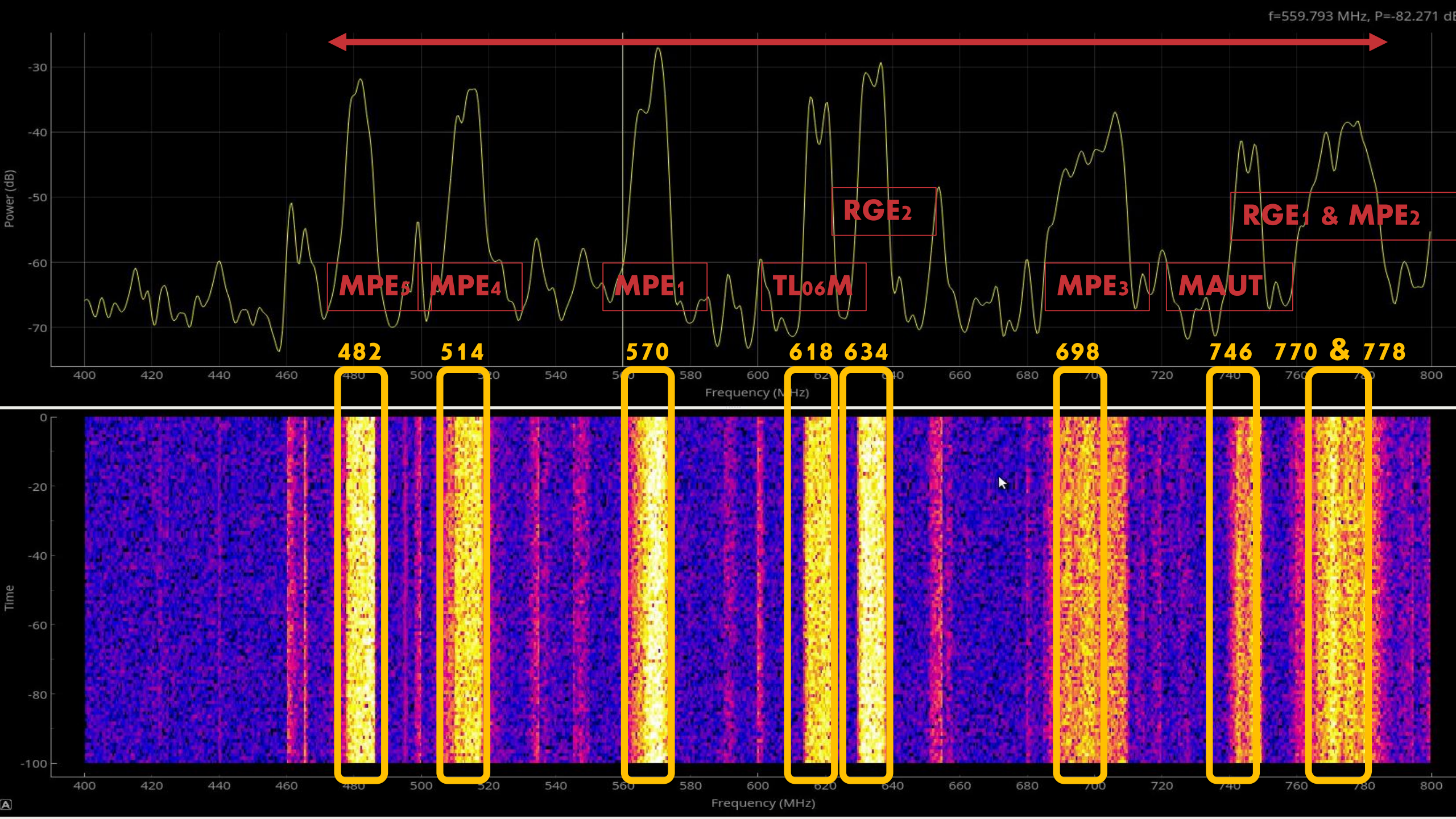
MAUT: Múltiple de Cobertura Autonómica

Múltiple digital	Canal	Frecuencia	Múltiple digital	Canal	Frecuencia
MPE5	*atreseries HD*	482.000.000	MPE3	*Telecinco*	698.000.000
MPE5	*BeMad tv HD*	482.000.000	MPE3	*Telecinco HD*	698.000.000
MPE5	*Realmadrid TV HD*	482.000.000	MPE3	*Cuatro*	698.000.000
MPE4	TRECE	514.000.000	MPE3	*Cuatro HD*	698.000.000
MPE4	Energy	514.000.000	MPE3	*FDF*	698.000.000
MPE4	mega	514.000.000	MPE3	*Divinity*	698.000.000
MPE4	Boing	514.000.000	MAUT	*Telemadrid HD*	746.000.000
MPE1	*PARAMOUNT CHANNEL*	570.000.000	MAUT	*Telemadrid*	746.000.000
MPE1	*GOL*	570.000.000	MAUT	*LA OTRA*	746.000.000
MPE1	*DMAX*	570.000.000	MAUT	*BOM*	746.000.000
MPE1	*Disney Channel*	570.000.000	RGE1	*La 2 HD*	770.000.000
TL06M	*TRECE*	618.000.000	RGE1	*La 2*	770.000.000
TL06M	*Intereconomia TV*	618.000.000	RGE1	*La 1 HD*	770.000.000
TL06M	*HIT TV*	618.000.000	RGE1	*La 1*	770.000.000
TL06M	*MegaStar*	618.000.000	RGE1	*Clan*	770.000.000
TL06M	*CGTN-Español*	618.000.000	RGE1	*24h*	770.000.000
TL06M	*Canal Galería*	618.000.000	MPE2	*nova*	778.000.000
TL06M	*Business TV*	618.000.000	MPE2	*neox*	778.000.000
TL06M	*8madrid*	618.000.000	MPE2	*laSexta HD*	778.000.000
RGE2	tdp HD	634.000.000	MPE2	*laSexta*	778.000.000
RGE2	TEN	634.000.000	MPE2	*antena3 HD*	778.000.000
RGE2	DKISS	634.000.000	MPE2	*antena3*	778.000.000
RGE2	tdp	634.000.000			
RGE2	Clan HD	634.000.000			

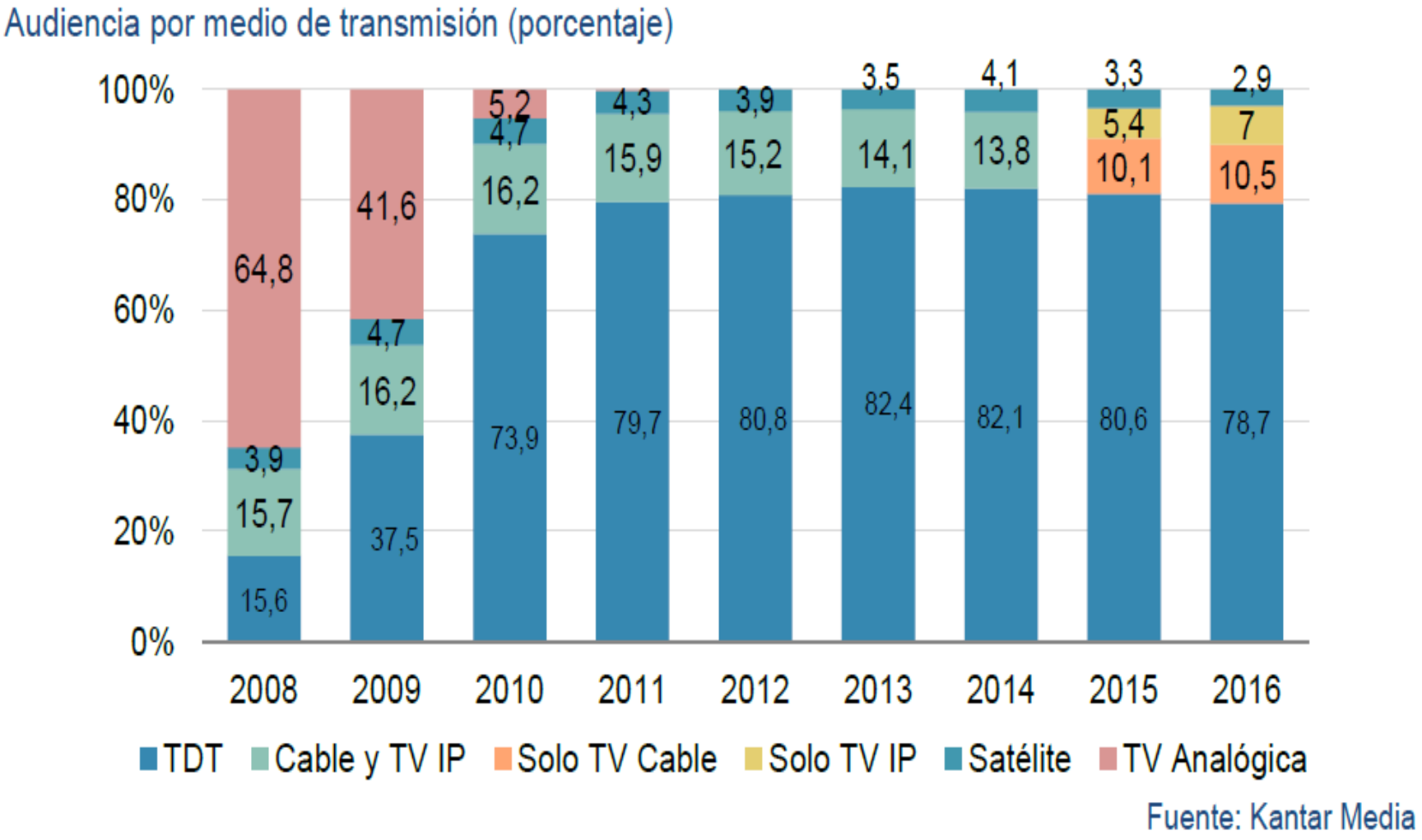
2018 **March, Pedro Cabrera**


f=559.793 MHz, P=-82.271 dB
Power (dB)
-30
-40
-50
-60
-70
400 420 440 460 480 500 520 540 560 580 600 620 640 660 680 700 720 740 760 780 800
Frequency (MHz)
Time
0
-20
-40
-60
-80
-100
400 420 440 460 480 500 520 540 560 580 600 620 640 660 680 700 720 740 760 780 800
A


500M
600M
700M
Duration: 0:58
Range: 470.00MHz - 801.00MHz
Pixel: 1000000.00Hz x 25s
Started: 2018-02-07 11:20:59
RTL-SDR
DVB-T+DAB+FM+SDR
Power (dB)
Time
Frequency (MHz)


f=559.793 MHz, P=-82.271 dB
Power (dB)
-30
-40
-50
-60
-70
MPE5
MPE4
MPE1
TL06M
RGE2
MPE3
MAUT
RGE1 & MPE2
482
514
570
618
634
698
746
770 & 778
400
420
440
460
480
500
520
540
560
580
600
620
640
660
680
700
720
740
760
780
800
Frequency (MHz)
Time
0
-20
-40
-60
-80
-100
Frequency (MHz)

Audiencia de la TDT



/Rooted®CON

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_intrusion

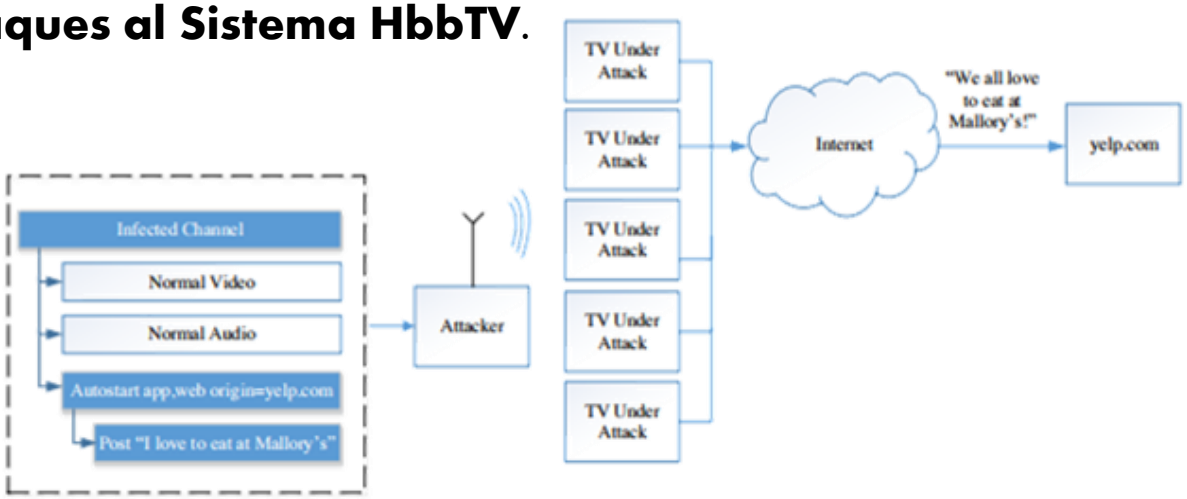
2018 March, Pedro Cabrera

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.

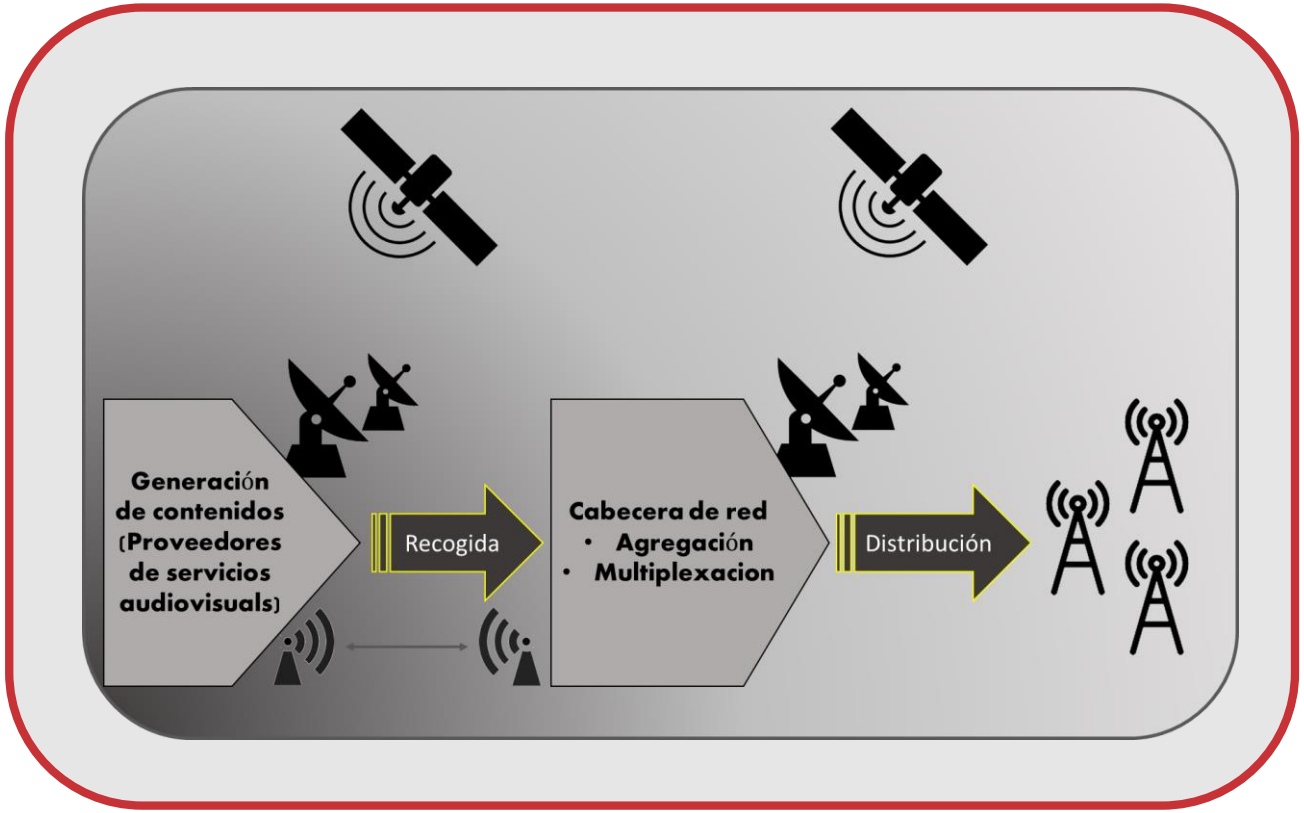
Junio 2014 – Weeping Angel (CIA) – Marzo 2017 WikiLeaks. Muestra exactamente lo que un agente debe hacer para convertir una Samsung Smart TV en un micrófono. Ataque requiere acceso local a la Smart TV.

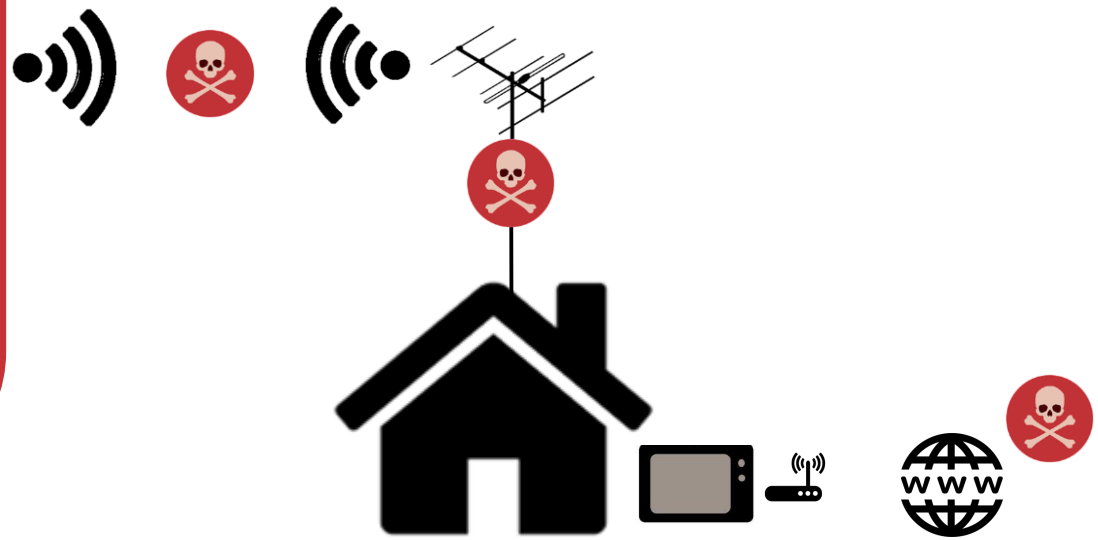


2018 March, Pedro Cabrera

/Rooted CON

Ataques SDR a las SmartTV

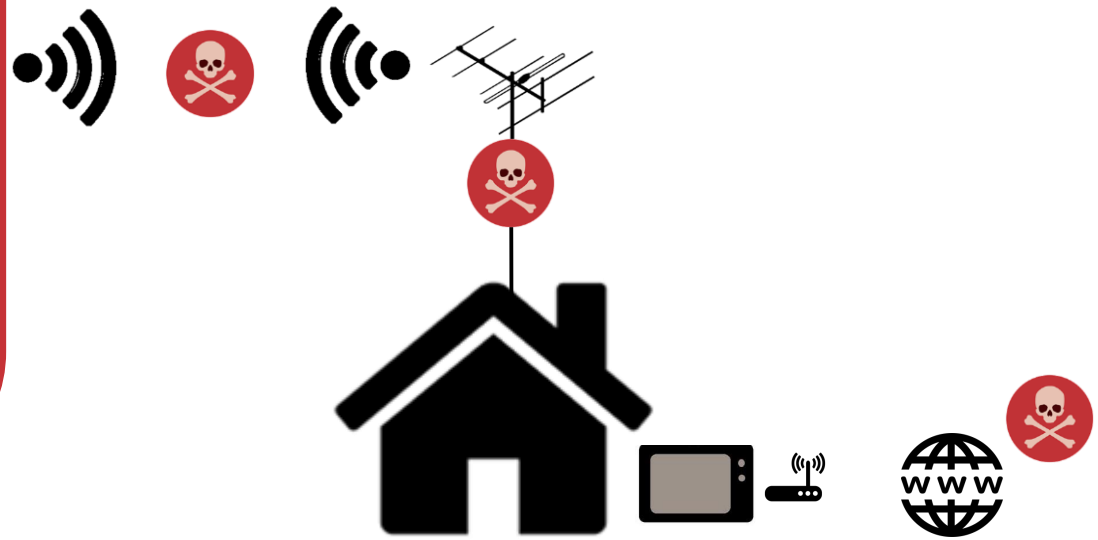




2018 March, Pedro Cabrera

/Rooted®CON

Ataques SDR a las SmartTV



2018 March, Pedro Cabrera

/Rooted®CON

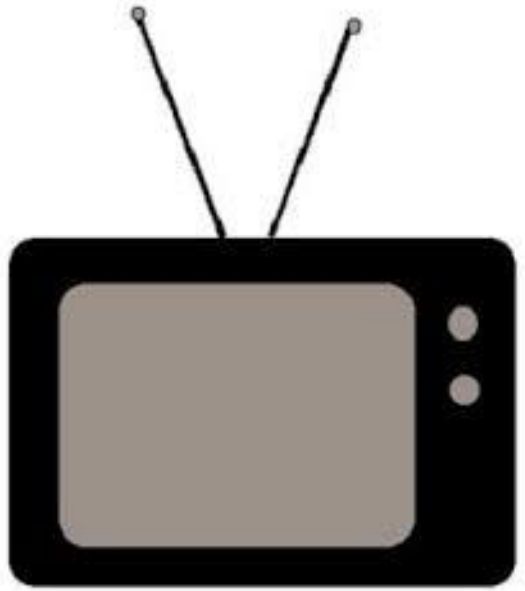
Ataque secuestro de canal TDT

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

Mpeg Video file

Metadatos HbbTV (solo AV)

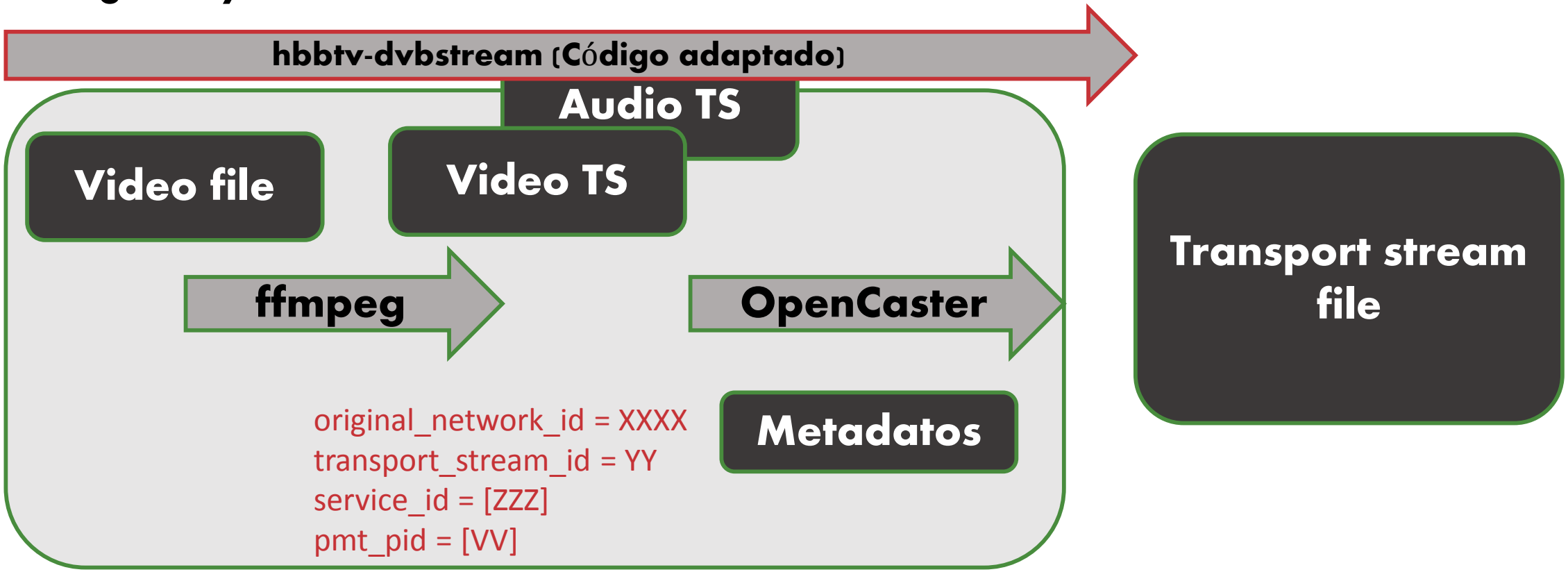
gr-dtv (gr-dvbt)



2018 **March, Pedro Cabrera**

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:



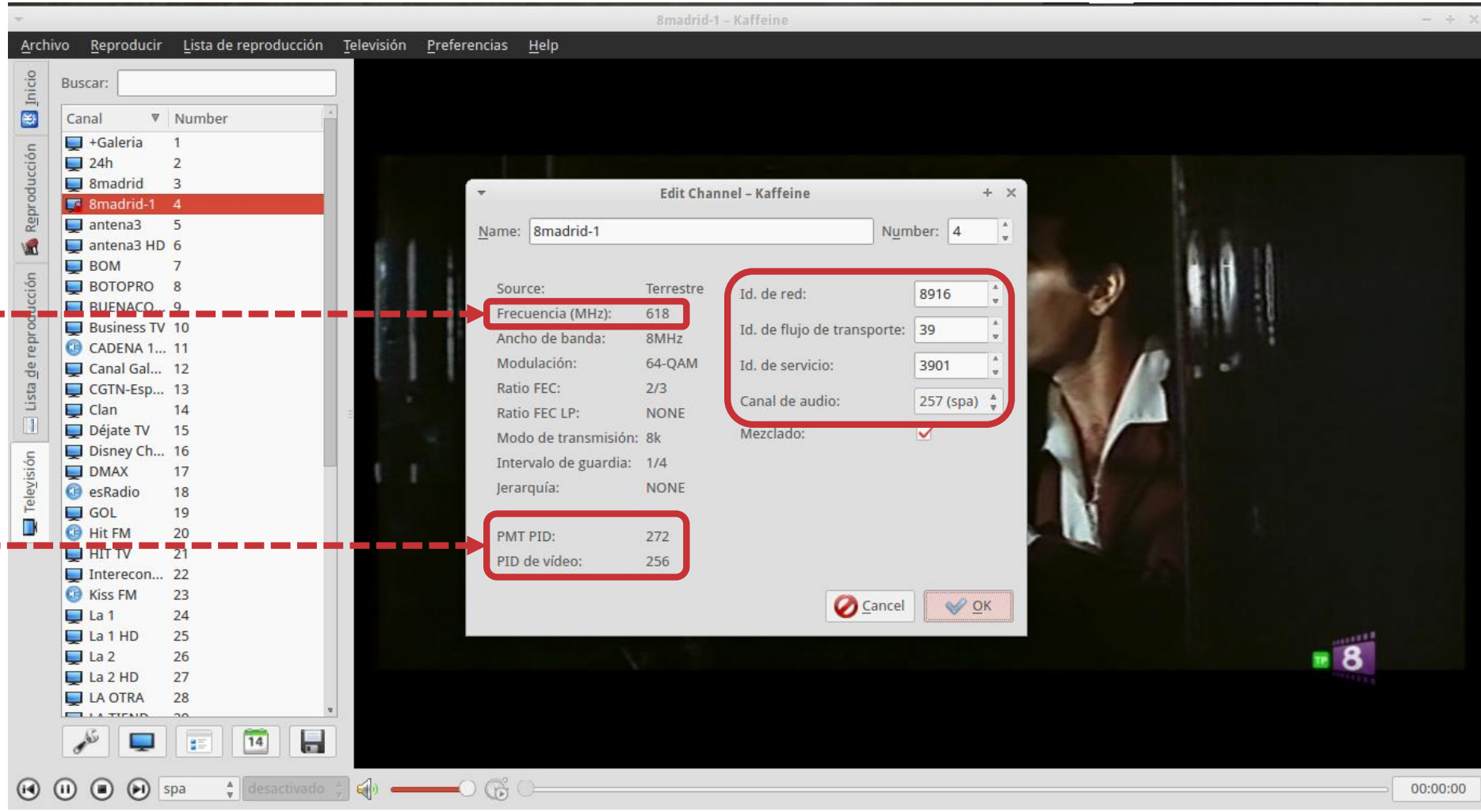
Parámetros canal TDT & HbbTV


```
{"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”

/Rooted®CON

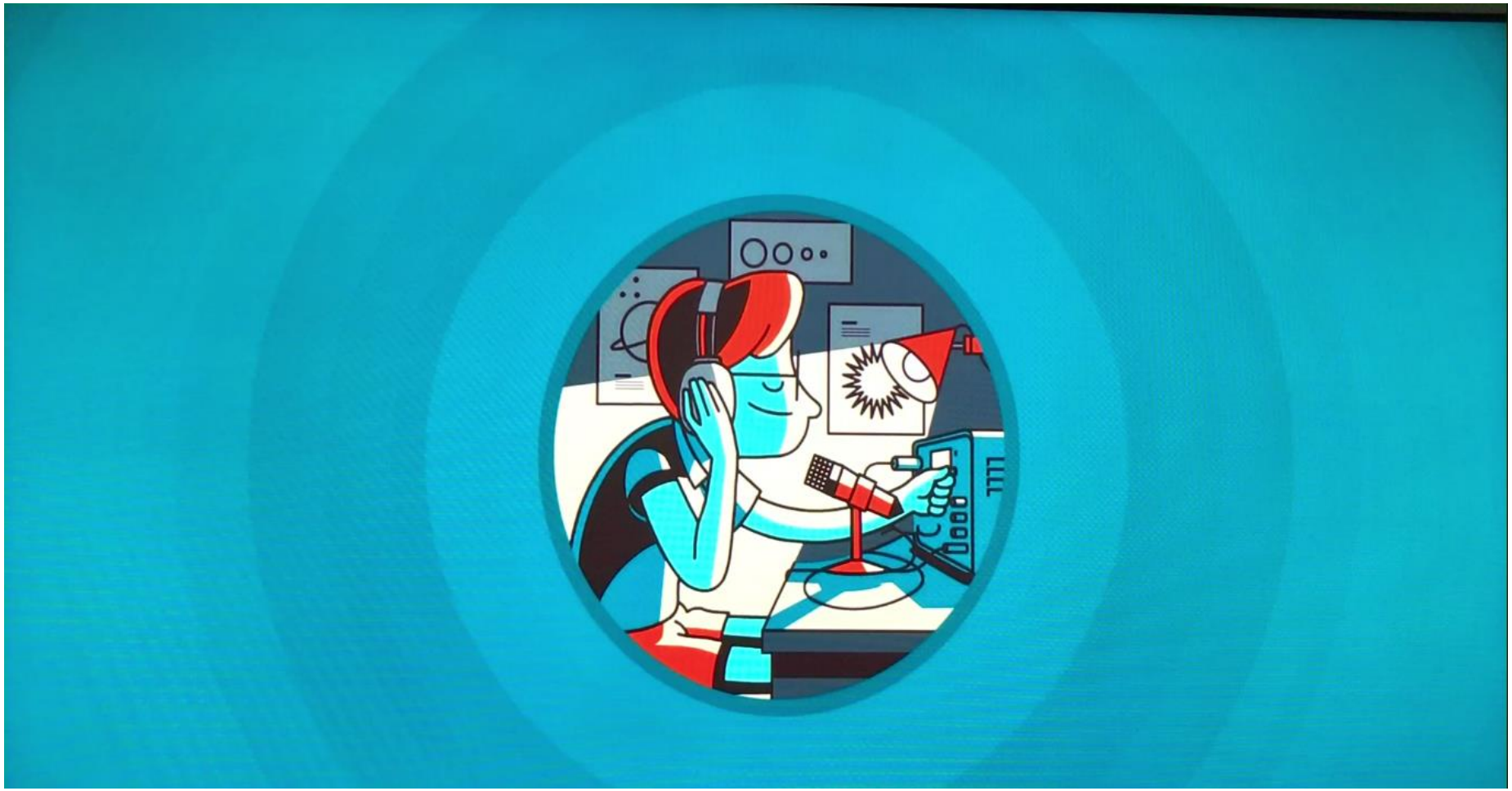
Parámetros canal TDT & HbbTV



kaffeine

/Rooted CON

Secuestro de canal – demo video

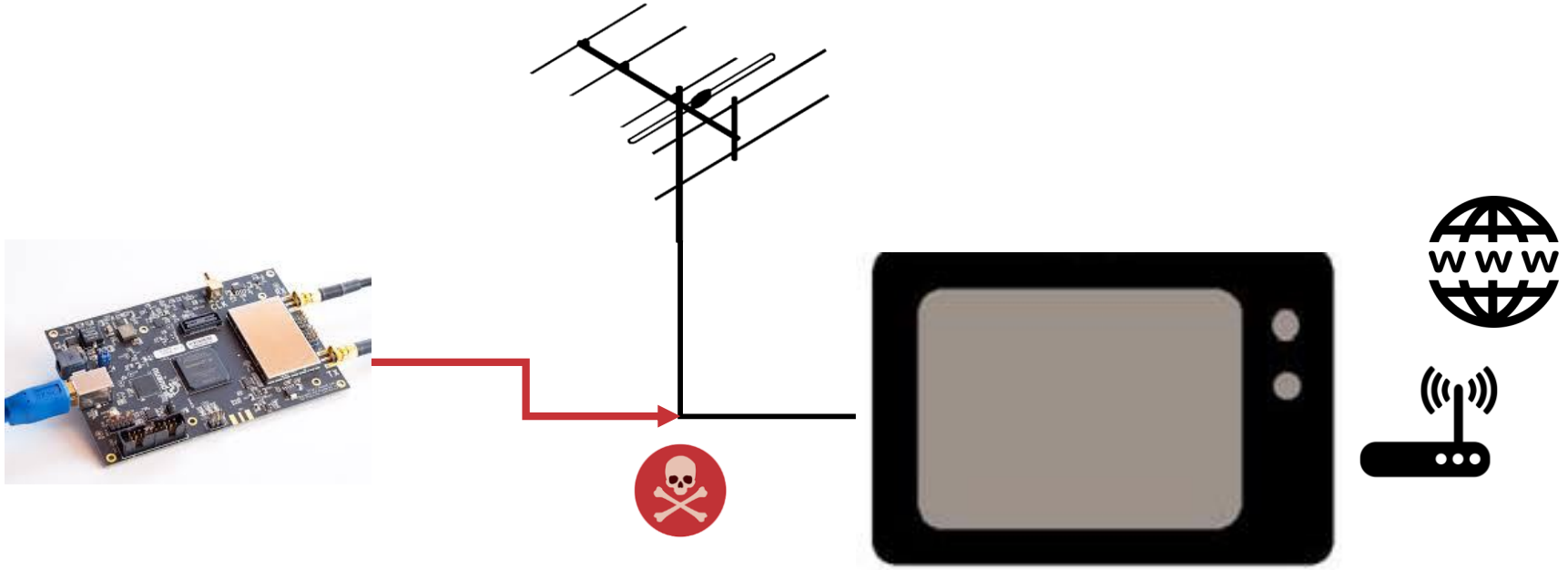


2018 March, Pedro Cabrera

/RootedCON

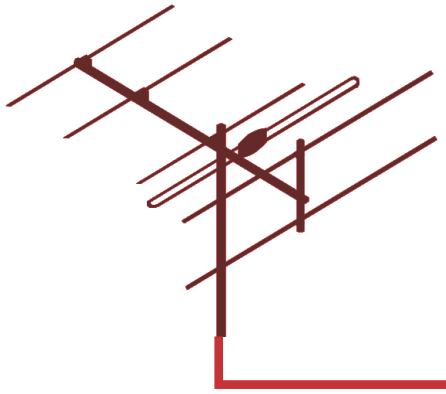
Ataques a instalaciones de antena

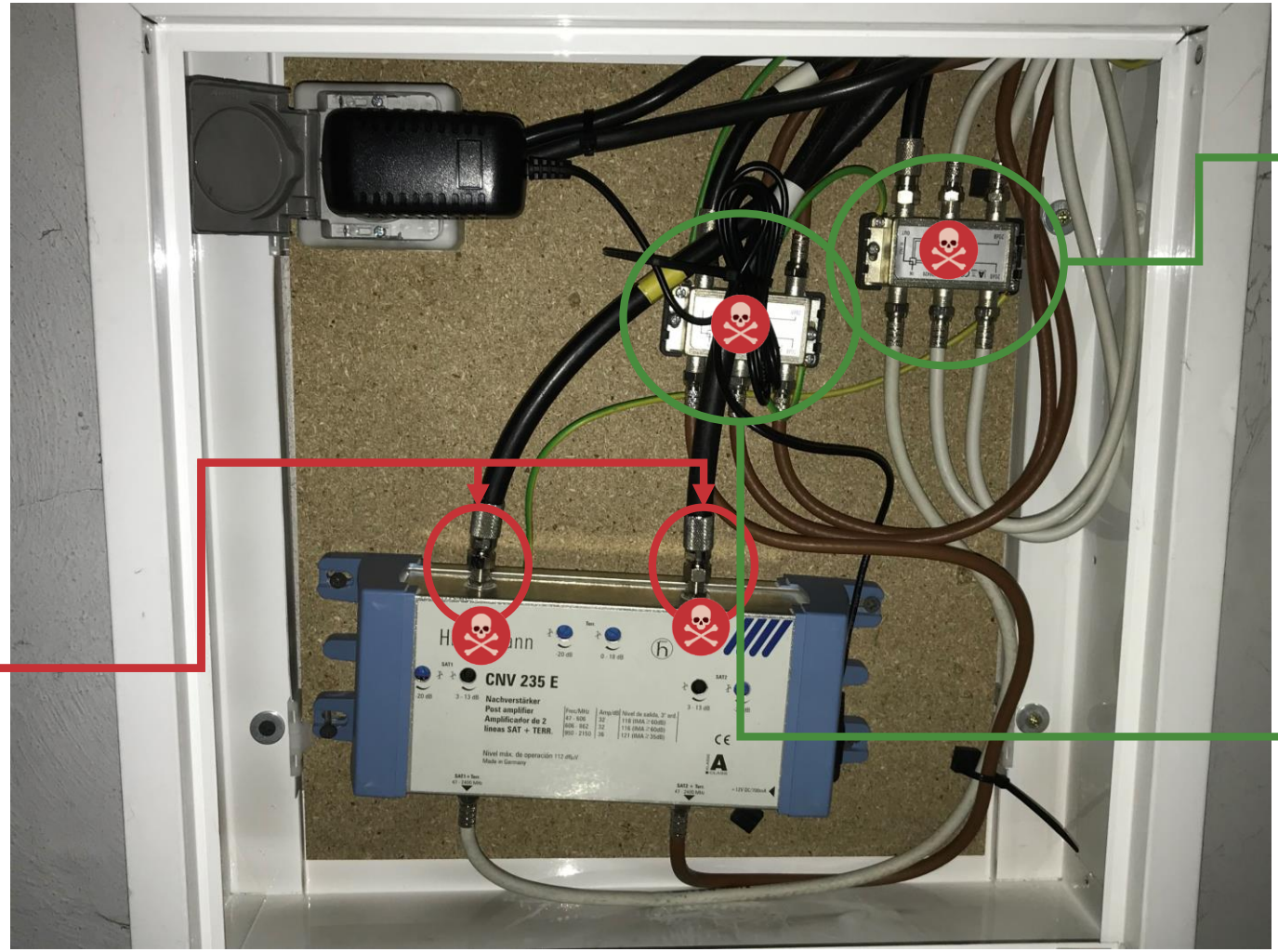
Podemos eliminar la etapa radio inyectando nuestra señal en la instalación de la antena.



/Rootəd CON

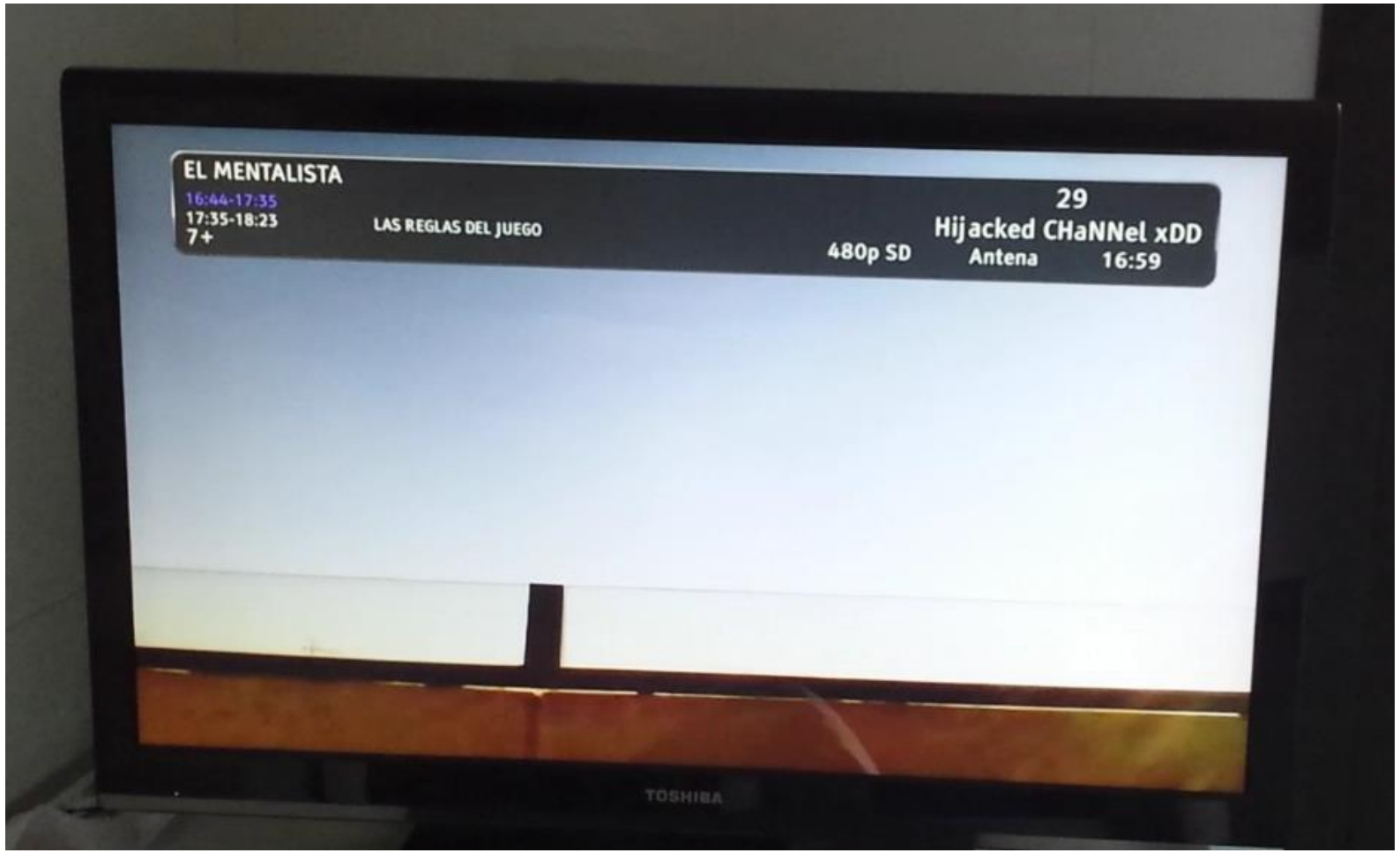
Ataques a instalaciones de antena





2018 March, Pedro Cabrera

Ataques instalaciones - Demo video



2018 March, Pedro Cabrera

SDR 2011/14

$ 30 300 400 1000 3000 $ $ $

* Año aparición 2011 2013 2013 2014

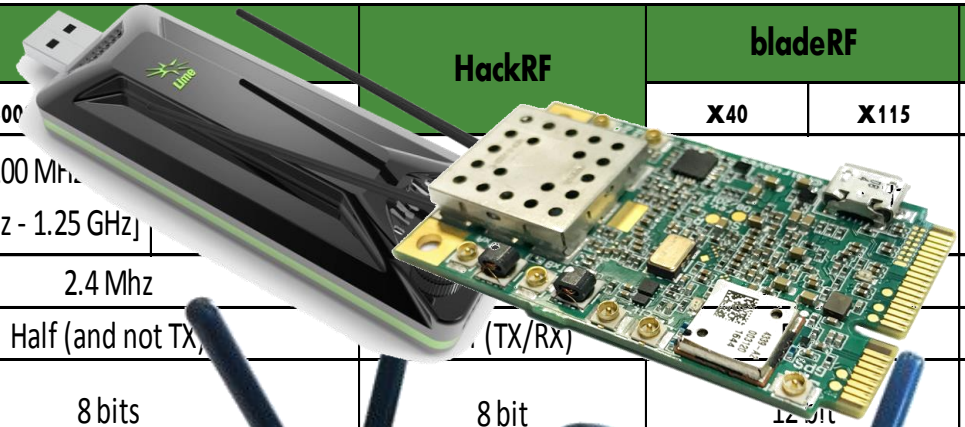
SDR Name	RTL-SDR		HackRF	bladeRF		USRP		
Model	E4000	R820T		x40	x115	B200	B210	N210
Radio Spectrum	52 – 2200 MHz ** [--1.1 GHz - 1.25 GHz]	24 – 1766 MHz	30 MHz – 6 GHz	300 MHz – 3.8 GHz		50MHz – 6 GHz		WBX: 50 MHz - 2.2 GHz SBX: 400 MHz - 4.4 GHz
Bandwidth	2.4 Mhz		20 MHz	28 MHz		61.44 MHz		40 MHz (SBX 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

$ 30 300 400 1000 3000 $ $ $

* Año aparición 2011 2013 2013 2014

SDR Name		HackRF	bladeRF		USRP		
Model	E400		x40	x115	B200	B210	N210
Radio Spectrum	52 – 2200 MH ** [--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/		(TX/RX)		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				61.44 Msps		100 Msps ADC 400 Msps DAC
Interface (Speed)	USB 2 HS (480 megabit)			abit)	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

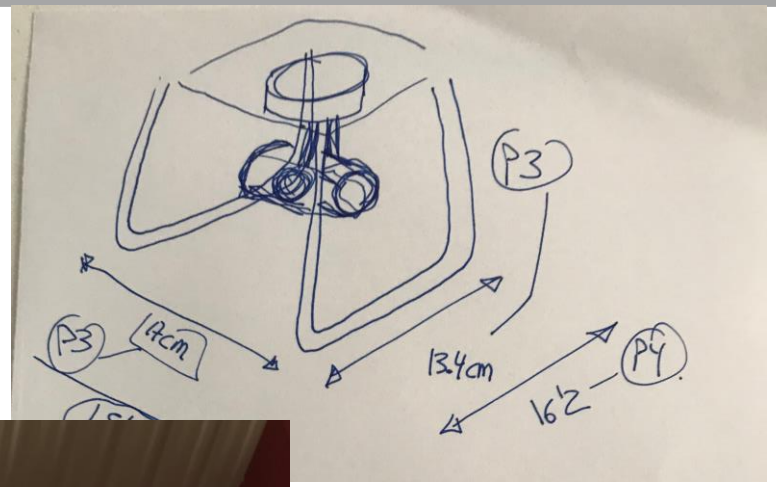
Fuente: https://www.uavsystemsinternational.com/how-much-weight-can-a-drone-lift/

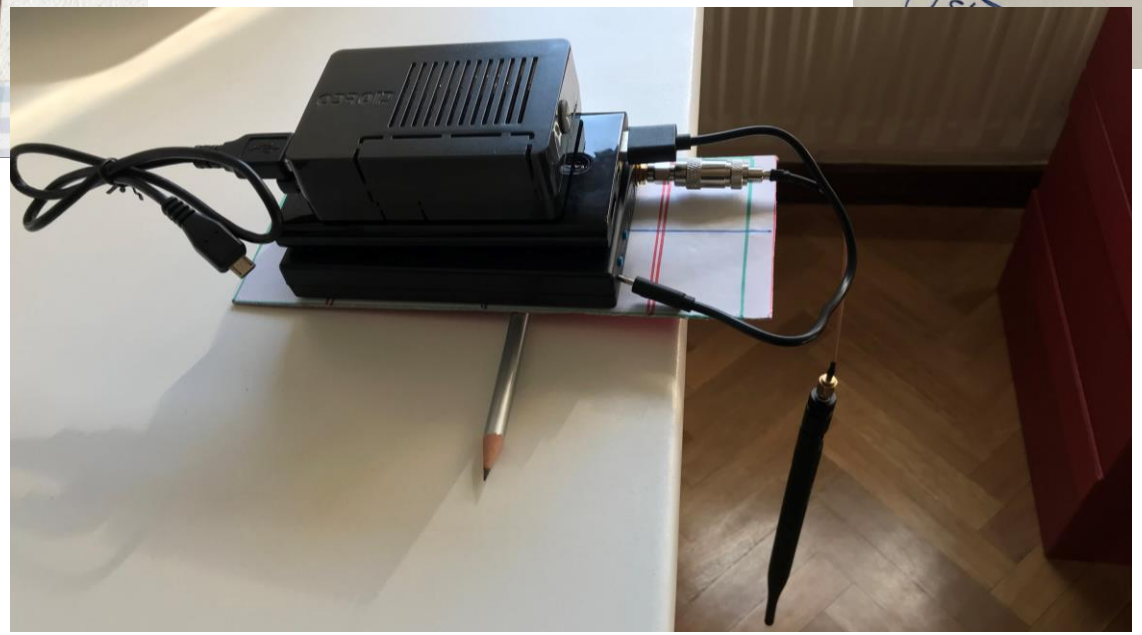
2018 March, Pedro Cabrera

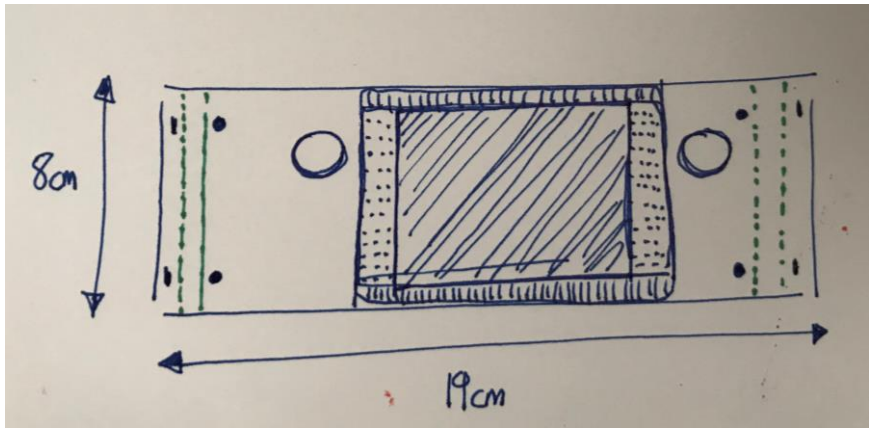
/Rooted®CON

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

2018 **March, Pedro Cabrera**

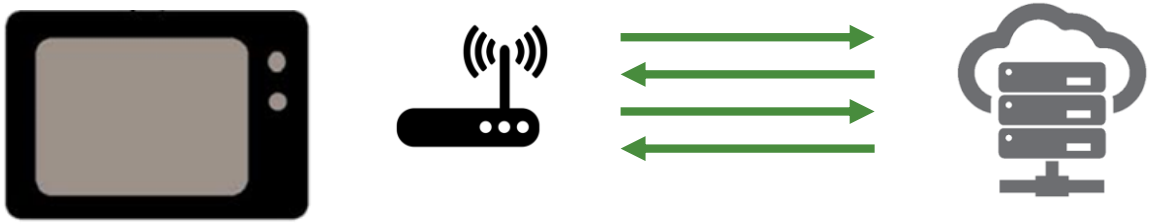
Drone attacks - Demo video

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-A655026
GET /api/channels/atreseries.hbbtv.x.es.smartclip/current_adstatus?format=jsonp&rnd=0B0A2F0A-5631-6559-0405-A655026
GET /api/channels/atreseries.hbbtv.x.es.smartclip/channel_config?rnd=64878329 HTTP/1.1
```

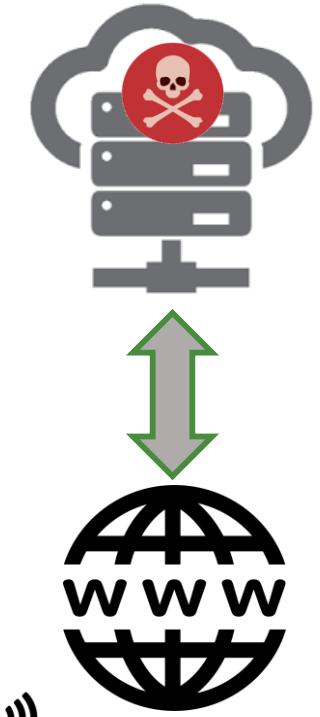


2018 March, Pedro Cabrera

/Rooted®CON

Ataque fake servidor HbbTV

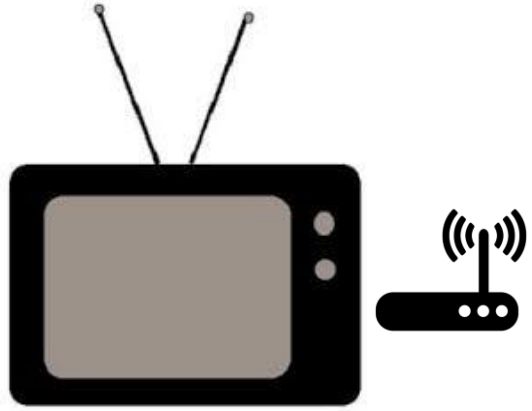
Añadimos la URL de nuestro servidor fake en los metadatos HbbTV: nombre de aplicación, URL base, web page, organisationId y applicationId



Mpeg Video file

gr-dtv (gr-dvbt)

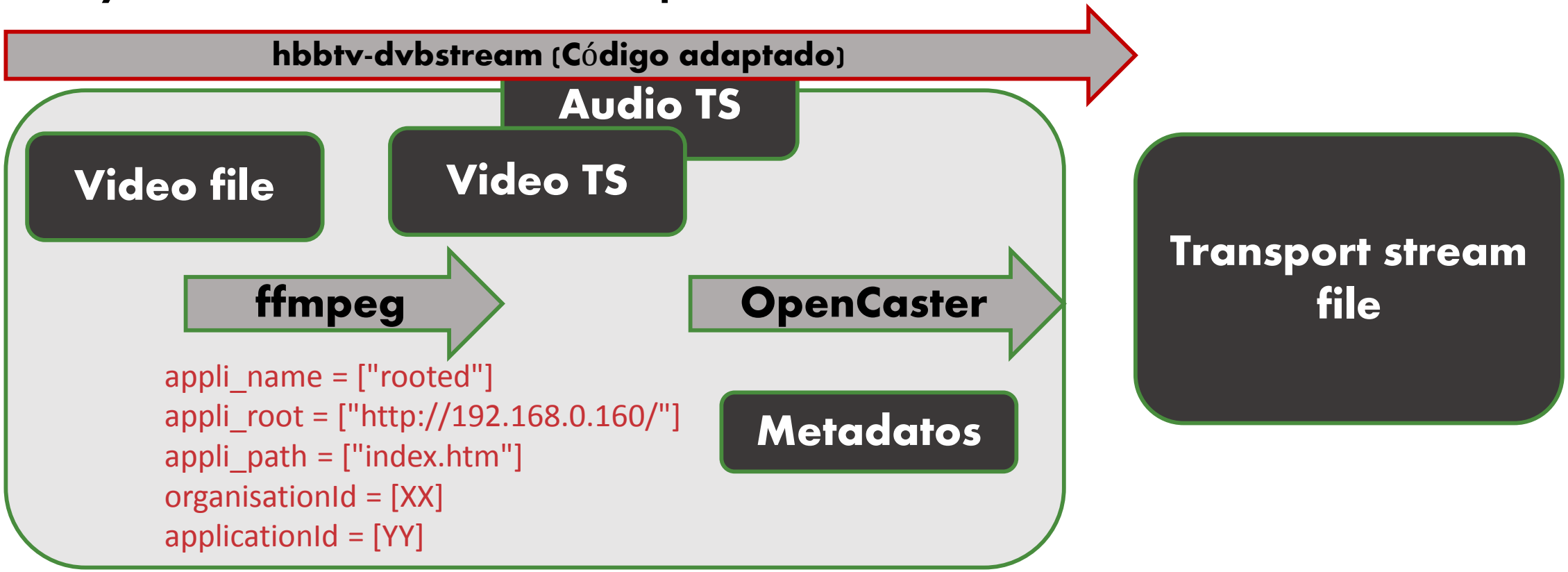
Metadatos HbbTV (AV + fake APP)



2018 **March, Pedro Cabrera**

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:



/Rooted®CON

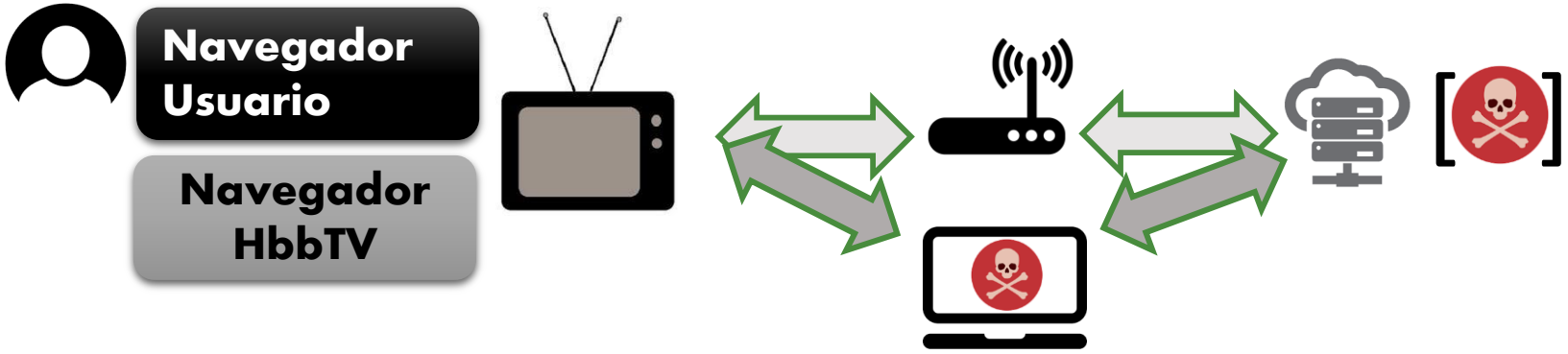
1 SmartTV - 2 navegadores web

Ataque fake server SDR

Navegador web HbbTV

Ataque fake server MITM ARP Poison/DNS Hijacking

Navegador web Usuario (SO) & HbbTV



2018 **March, Pedro Cabrera**

/Rooted®CON

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
```

2018 March, Pedro Cabrera

/Rooted®CON

Smart (TV) scanning

Apache Log files:

- Dirección IP pública
- Busqueda de modelos/marcas (UA)
- Análisis audiciencias 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;)"
```

2018 March, Pedro Cabrera

/Rooted CON

Ingeniería social

/Rooted CON

Ataque fake servidor HbbTV

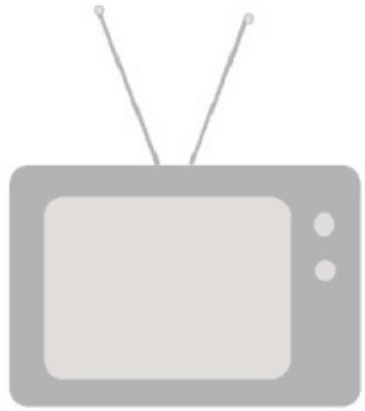
Añadimos la URL de nuestro servidor fake en los metadatos HbbTV

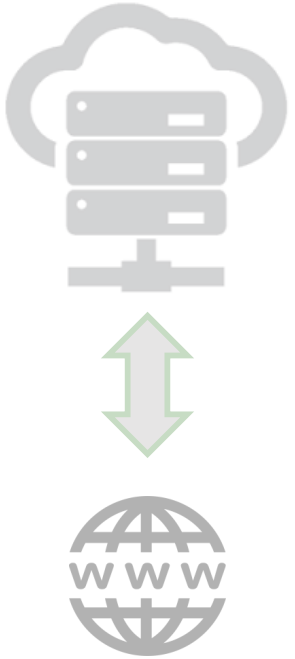
Mpeg Video file

gr-dtv (gr-dvbt)

Metadatos HbbTV (AV + fake APP)

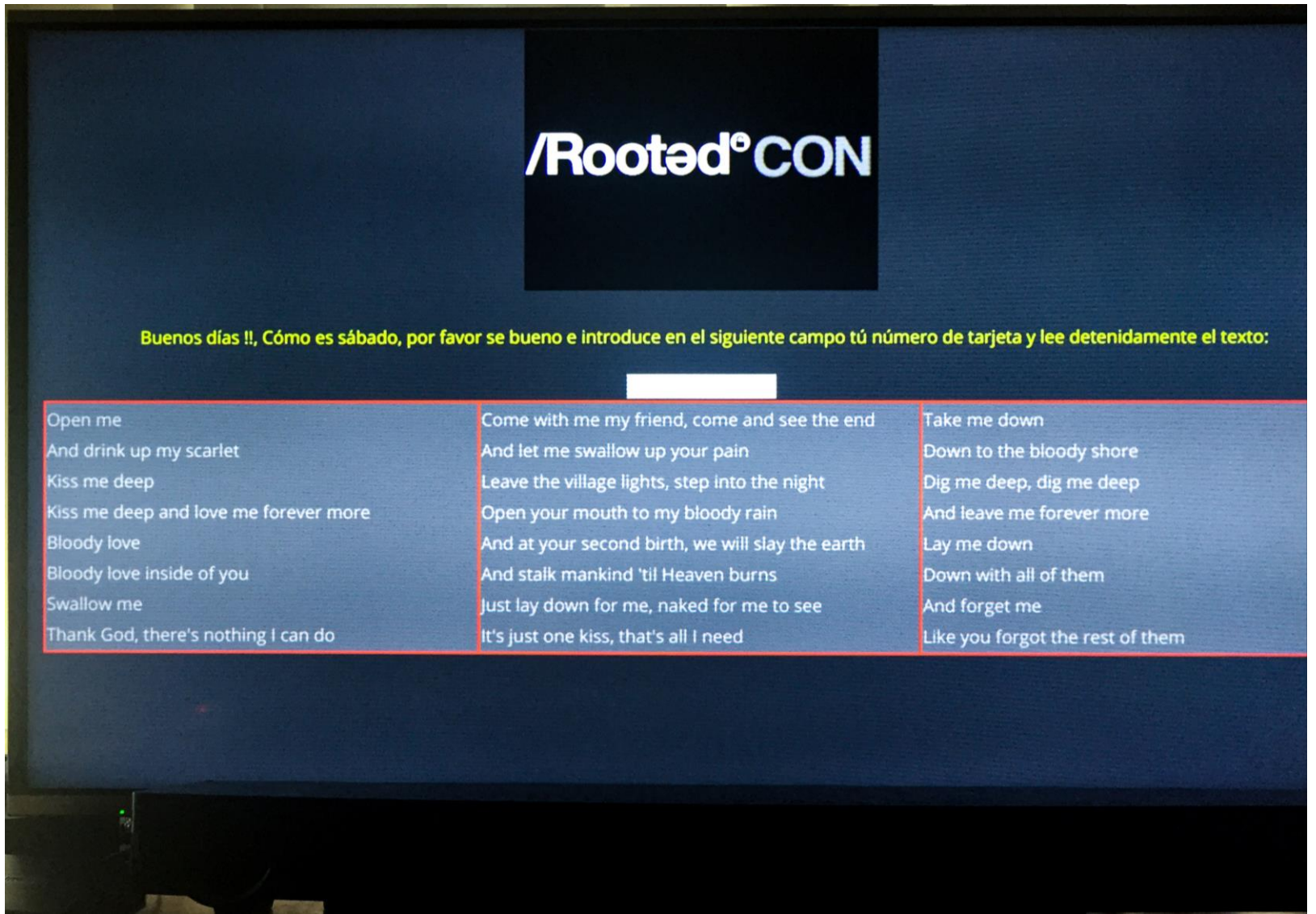
Demo Time





2018 March, Pedro Cabrera

Keylogger Javascript



/Rooted®CON

Minado de criptomonedas

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

Fuente:
https://www.xataka.com/seguridad/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.

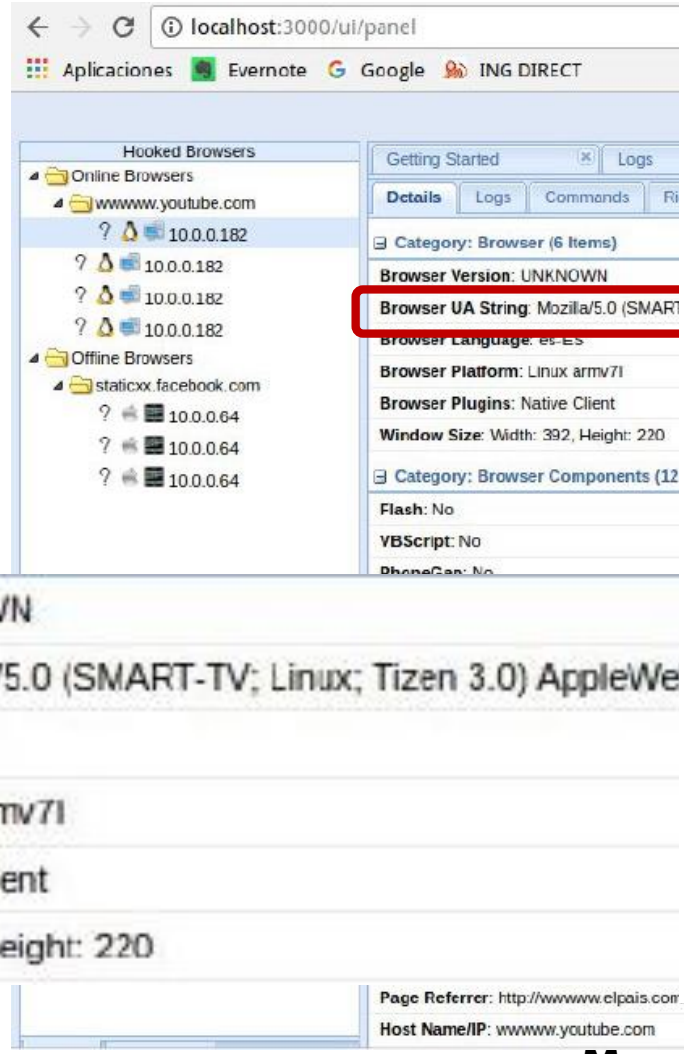
Fuente:
https://www.elespectador.com/tecnologia/hackers-contaminan-miles-de-paginas-web-para-minar-criptomonedas-articulo-738718

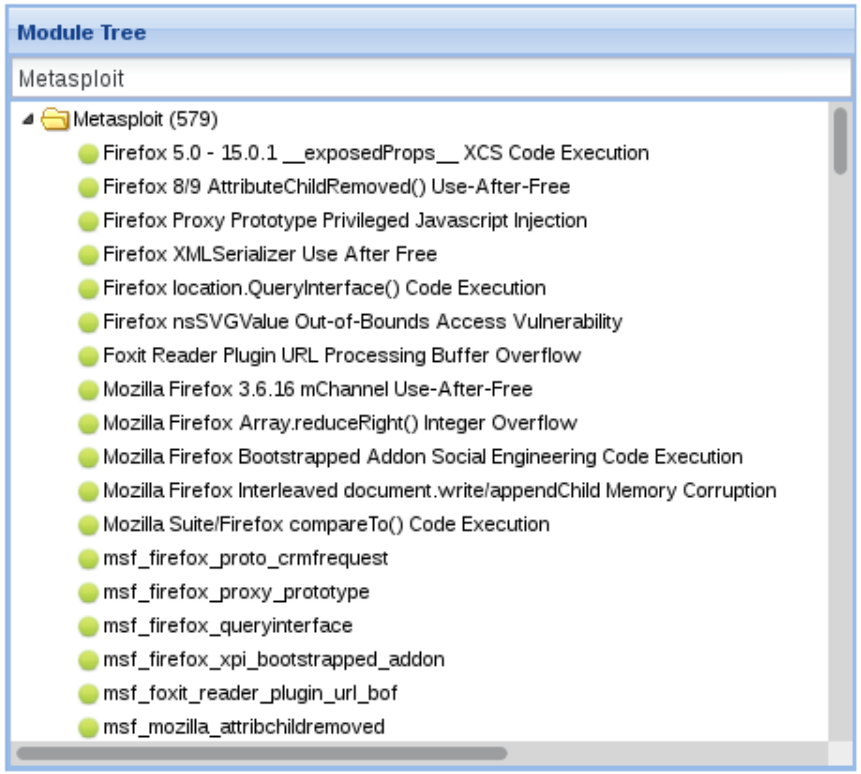
2018 **March, Pedro Cabrera**

Minado de criptomonedas

/Rooted®CON

Hook.js navegador de usuario





2018 **March, Pedro Cabrera**

/Rooted CON

Ataque fake servidor HbbTV

android tv

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 Inyect	✓	✓

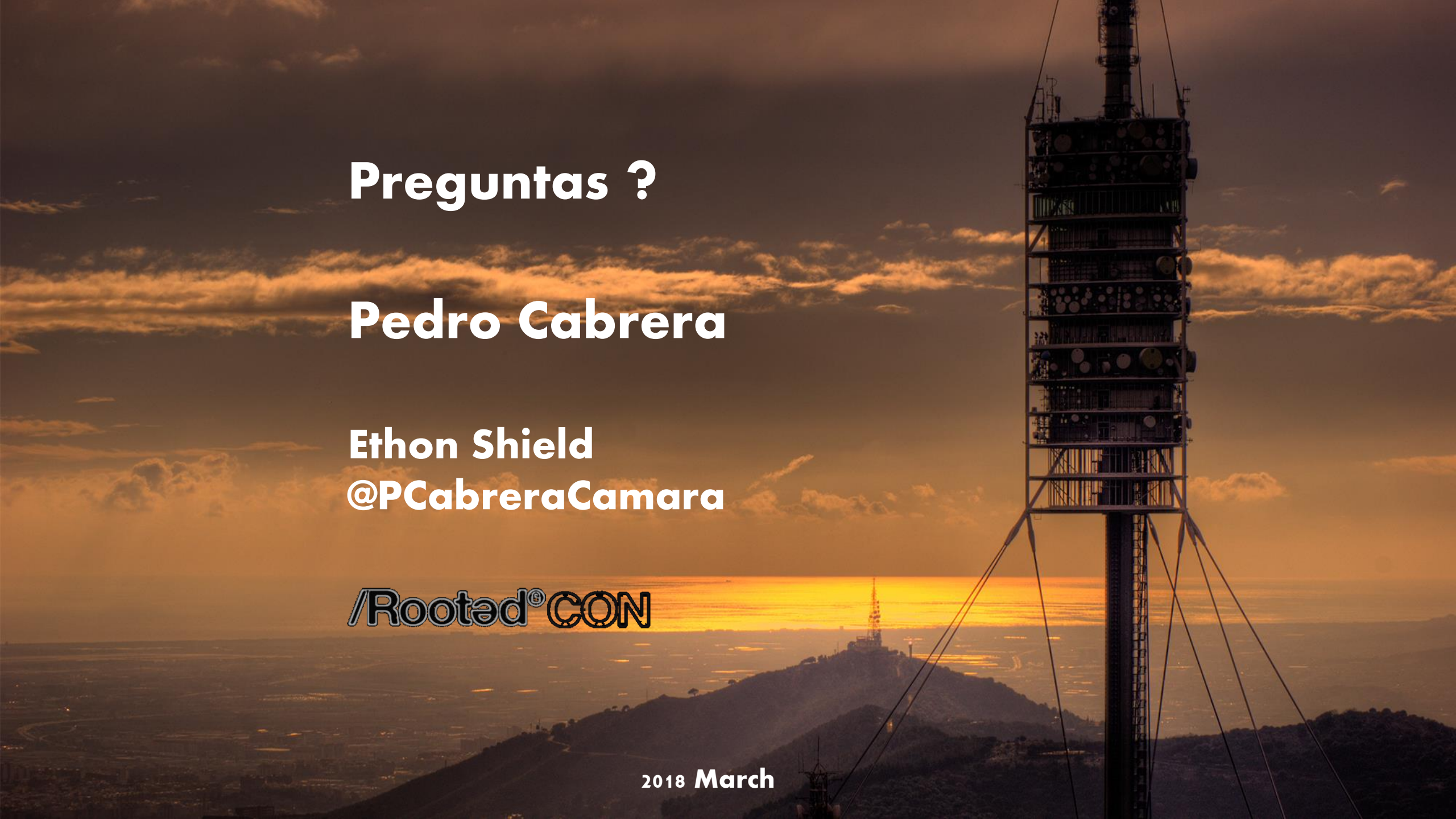
2018 March, Pedro Cabrera

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


Preguntas ?
Pedro Cabrera
Ethon Shield
@PCabreraCamara
/Rooted®CON
2018 March