# SDR Against Smart TVs; URL and channel injection attacks

DefCON 27, Pedro Cabrera

@PCabreraCamara

# About Me

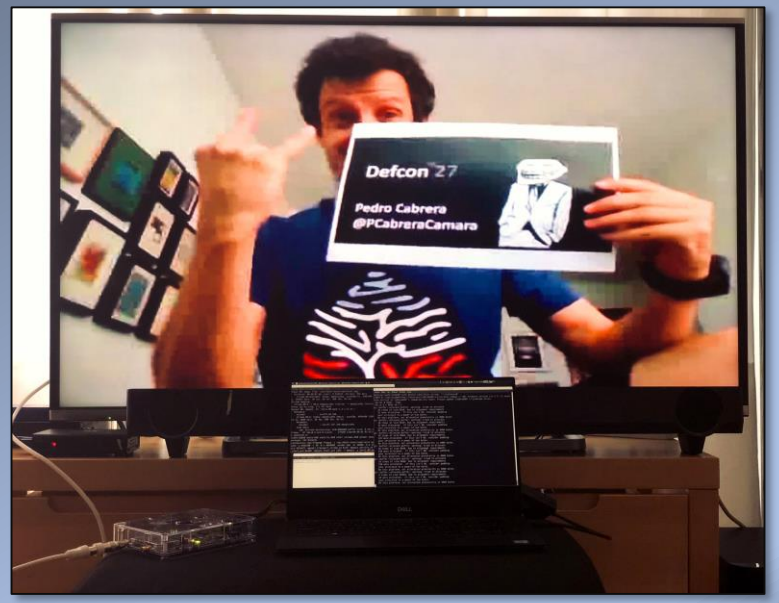
Industrial engineer, UAV professional pilot, Radio Ham (EA4HCF)

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 Televison

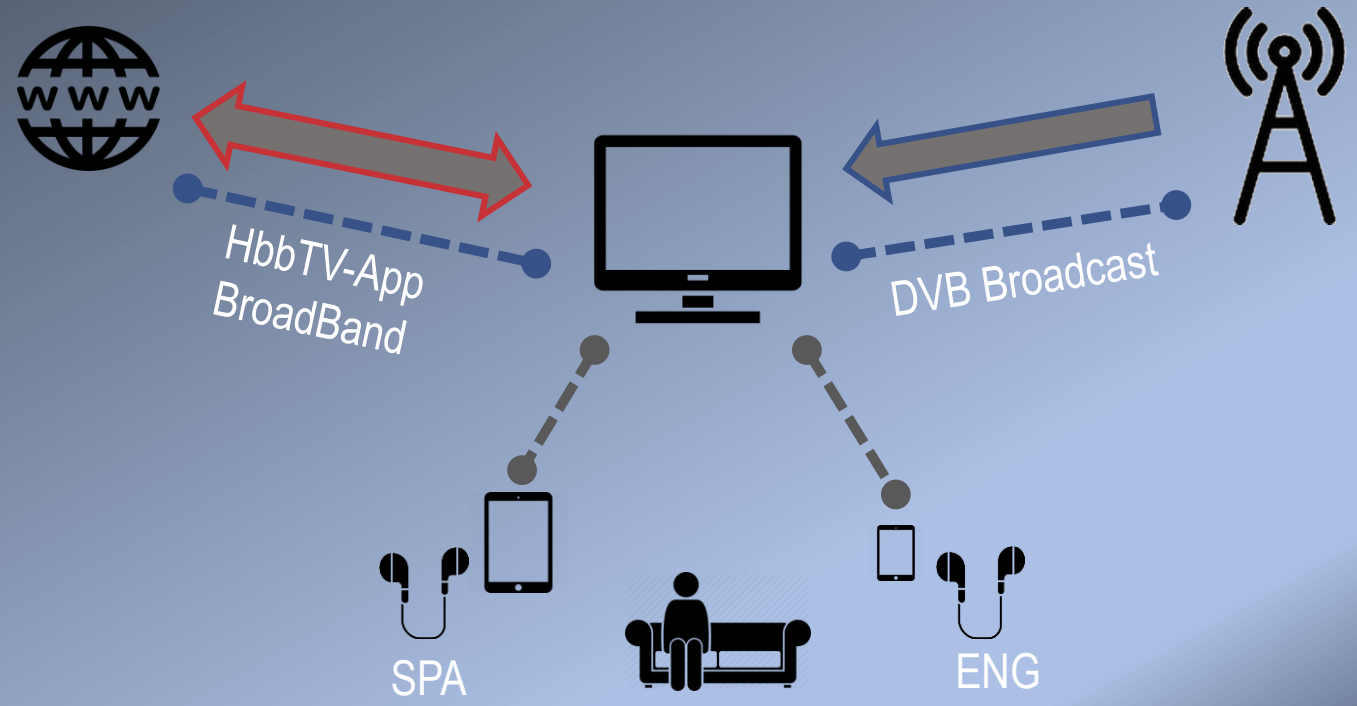
The HbbTV specification extends DVB-T by introducing additional metadata formats that mix broadband Internet content into the digital television channel.

H4TV project

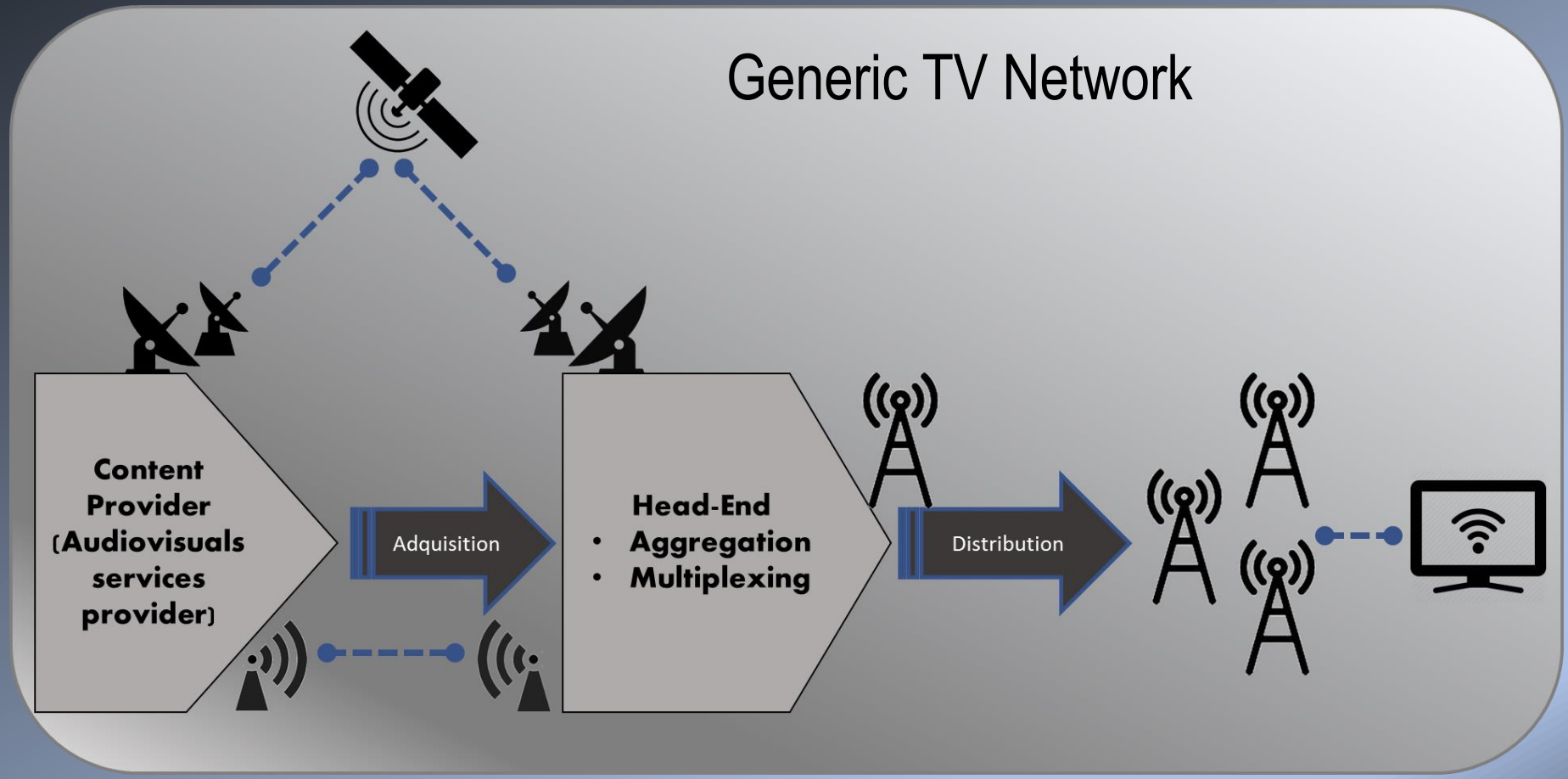
HTML profit project

HbbTV (2009)

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



# [I] TV Distribution Network



# [I] DVB-T

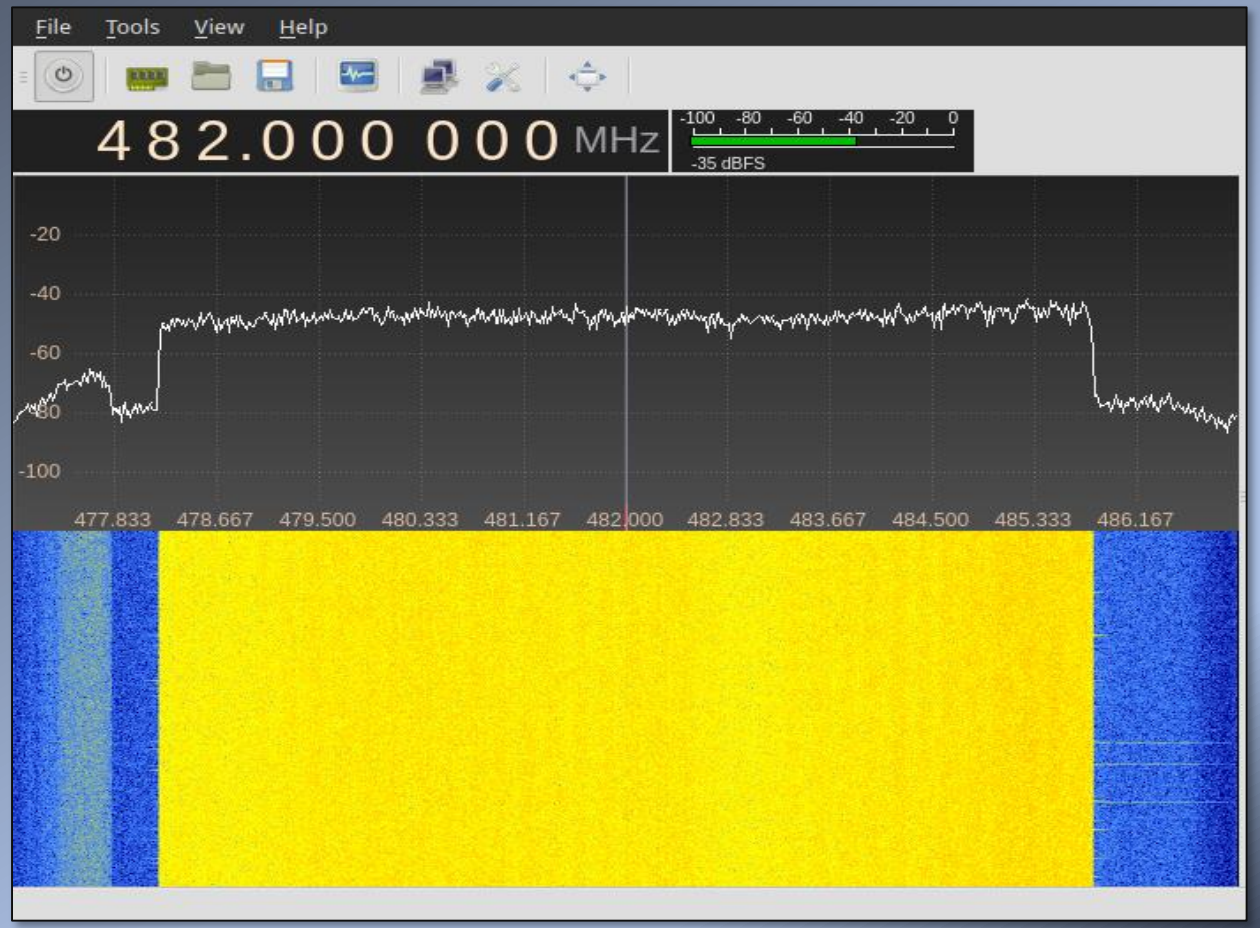
televisión digital terrestre

DVB S
DVB T
DVB C

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

*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.*

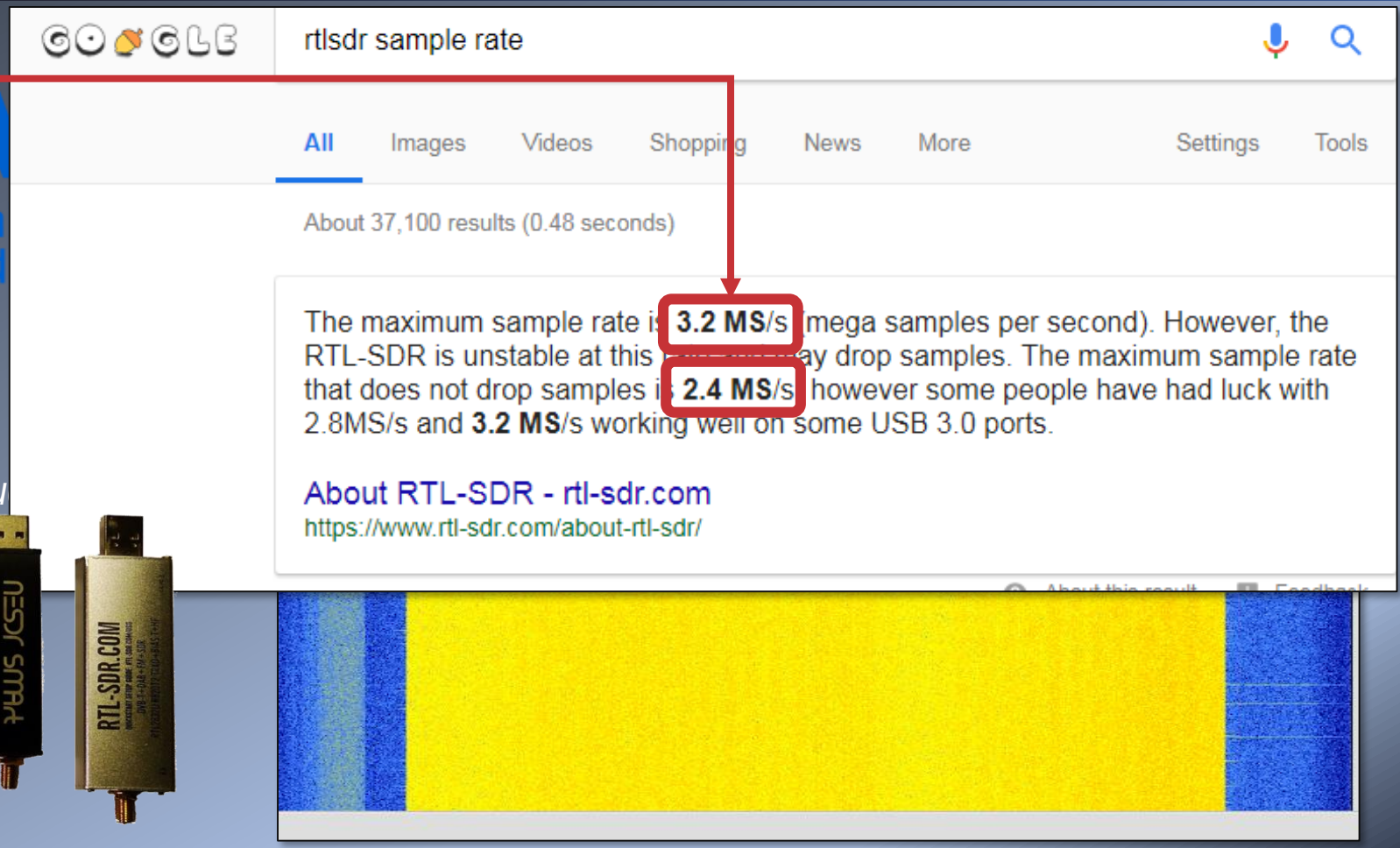


# [I] DVB-T


*Spain):*

- *8 MHz bandwidth*
- *Transmission mode: 8k (6,817 carriers).*
- *Modulation schemes: 64 Quadrature Amplitu*
  *OFDM*
- *le for al e ote 2/3*
- *gt uar va*


Digita
Broad



# [I] Generic DVB-T receiver

**Radio Frequency**

DVB-T Tuner

DeModulator

**RTL-SDR: Rafael 820T2**

**RTL-SDR: Realtek RTL2832u**

**MPEG-2 Multiplex**

DeMultiplexer

Video Decoder

Audio Decoder

Metadata Decoder

# [I] DVB-T demodulator

**Radio Frequency**

RadioFreq Receiver

ADC

Synchronizer

Fast Fourier Transformer

Channel Estimator & Channel Equalizer

Inner Deinterleaver

Viterbi Decoder

Outer Deinterleaver

Reed Solomon Decoder

DeScrambler

**MPEG-2 MUX**

# [I] DVB-T linux demodulator

- *Bogdan Diaconescu (YO3IIU)*

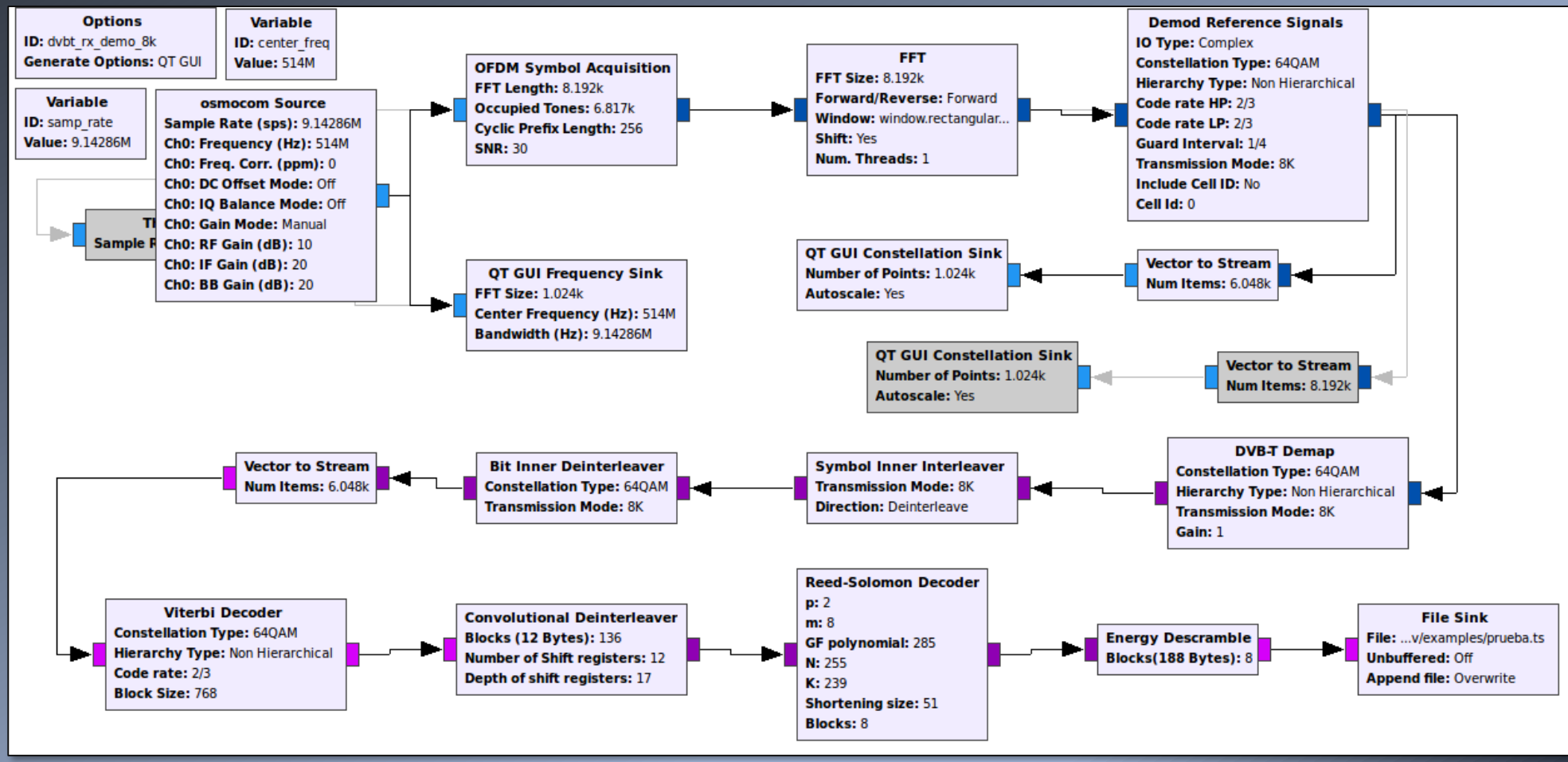
  *gr-dvbt (USRP N210)*

- *GNU Radio:*

  *gr-dtv (USRP)*

- *Ron Economos (W6RZ)*

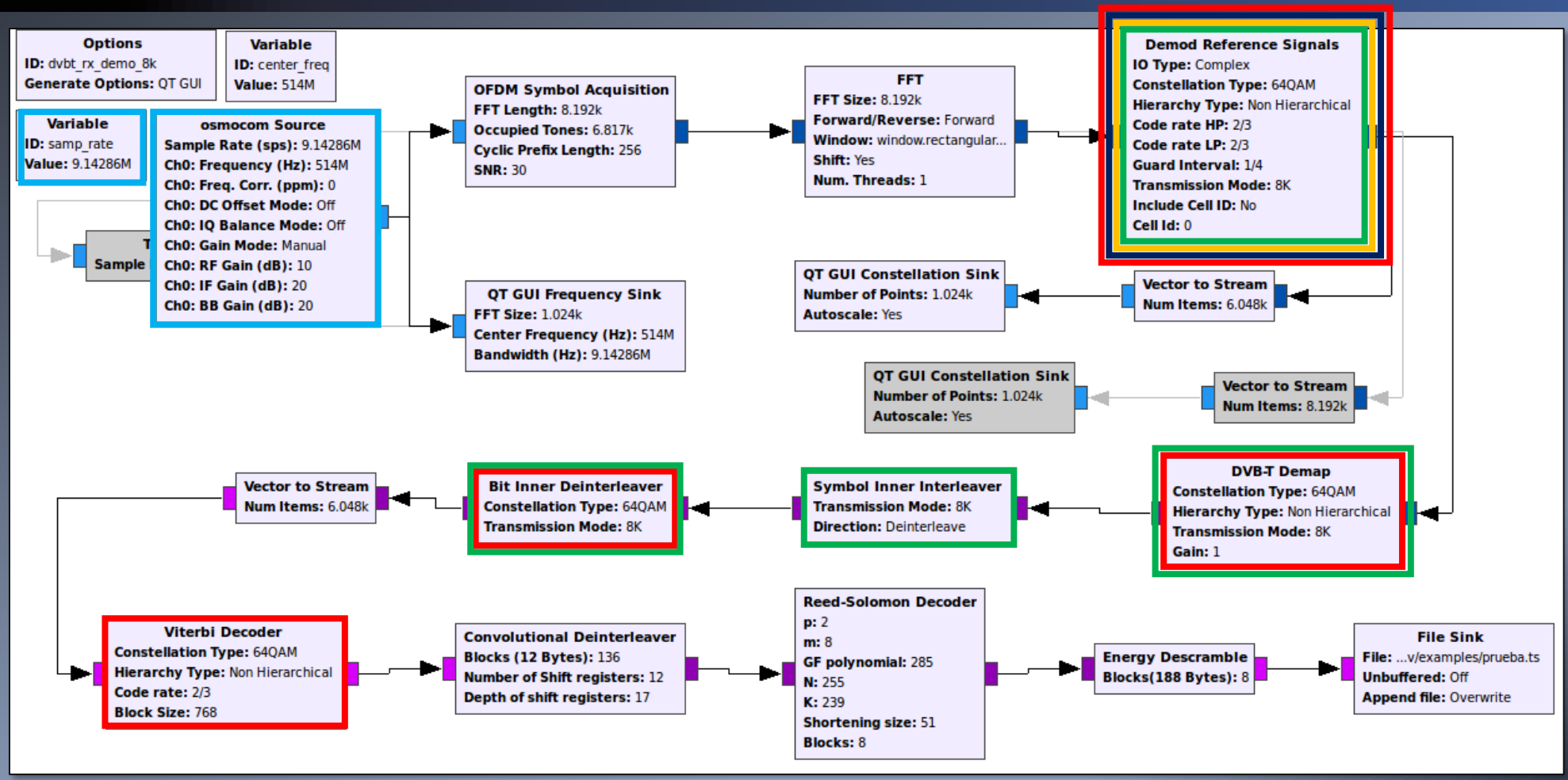
  *dtv-utils (BladeRF)*



# [I] DVB-T linux demodulator

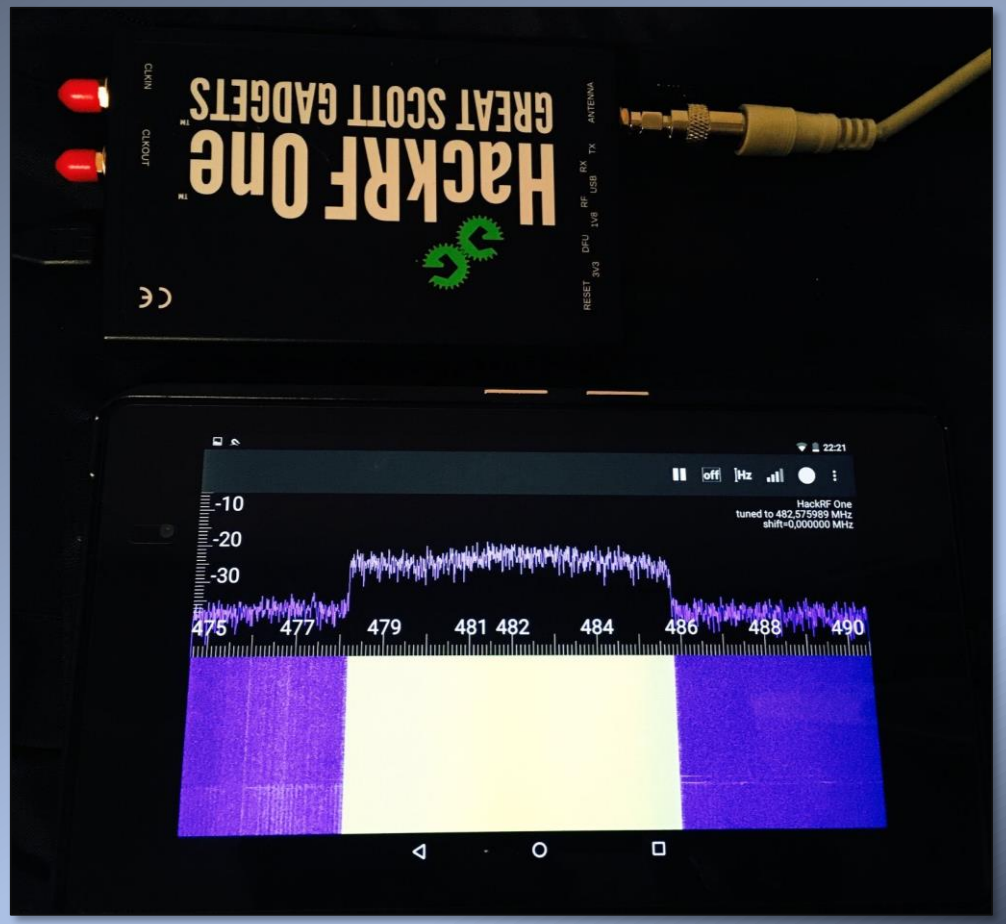
*DVB-T Modulation:*

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

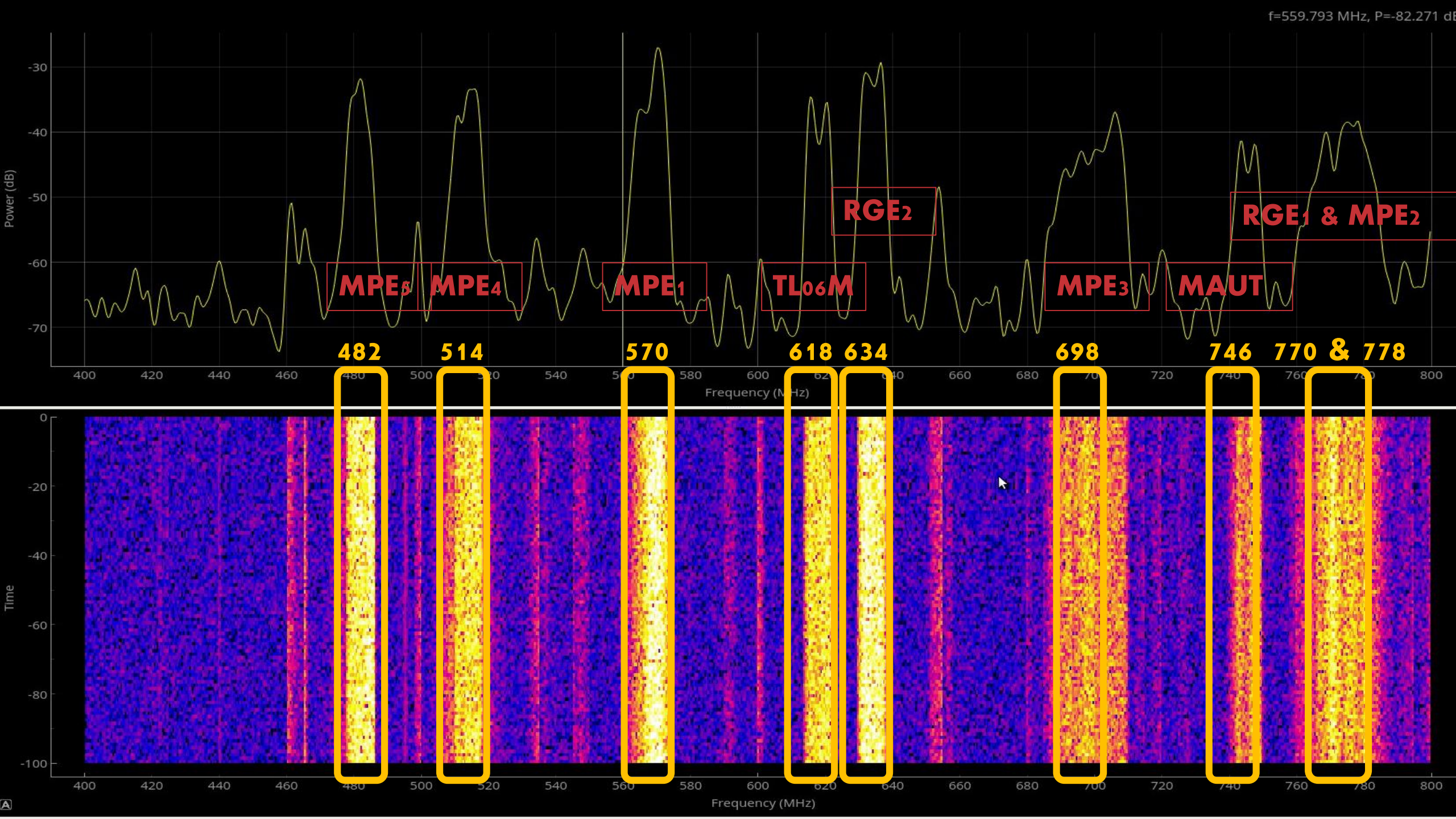


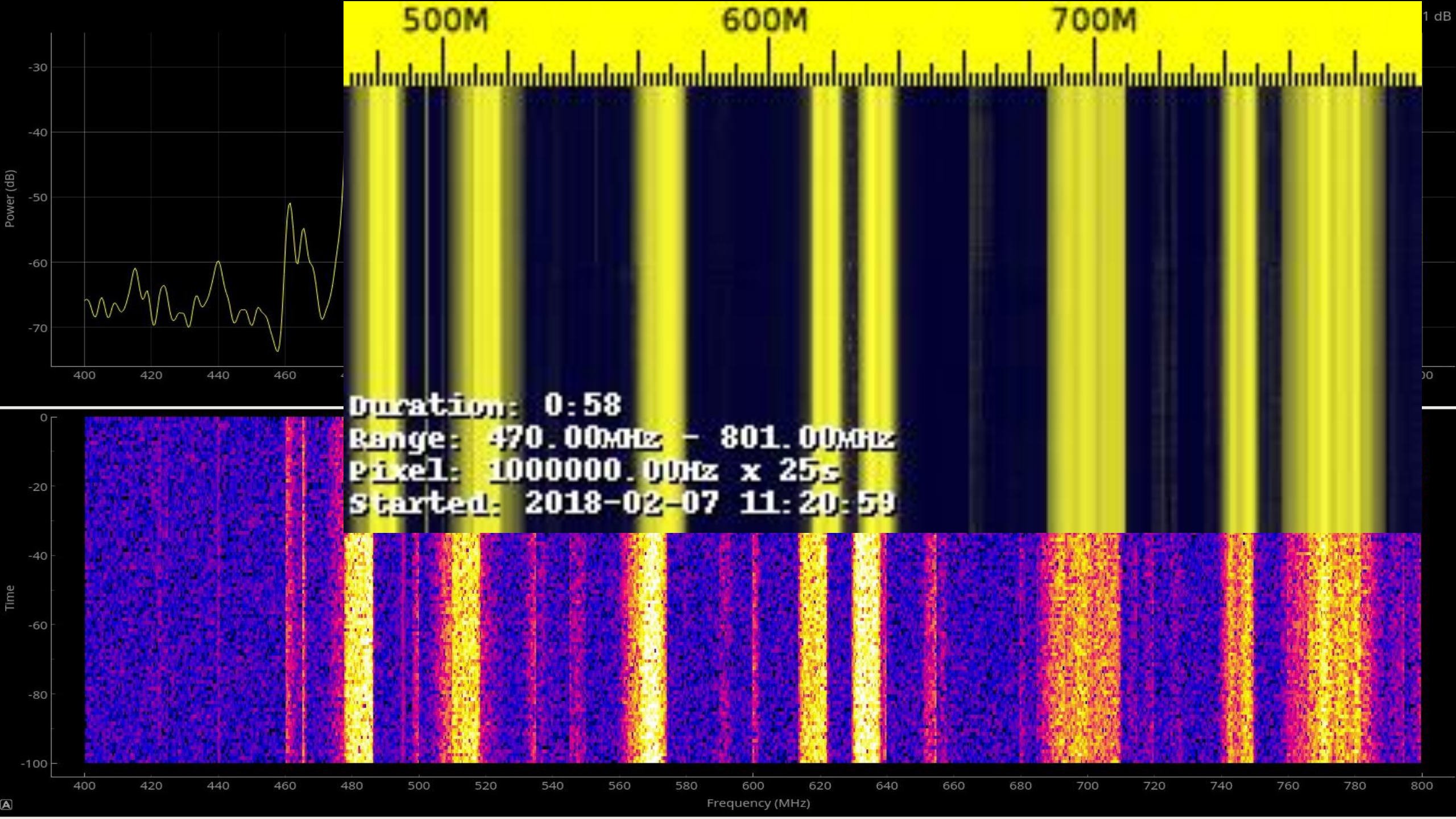
# [I] TV Channels & Frequencies

| Digital Mutiplex | Channel | Frequency | Digital Mutiplex | 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 |
| 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 | | | |




DefCON 27, Pedro Cabrera


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)


500M
600M
700M
Power (dB)
-30
-40
-50
-60
-70
400
420
440
460
Duration: 0:58
Range: 470.00MHz - 801.00MHz
Pixel: 1000000.00Hz x 25s
Started: 2018-02-07 11:20:59
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
Frequency (MHz)

# [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

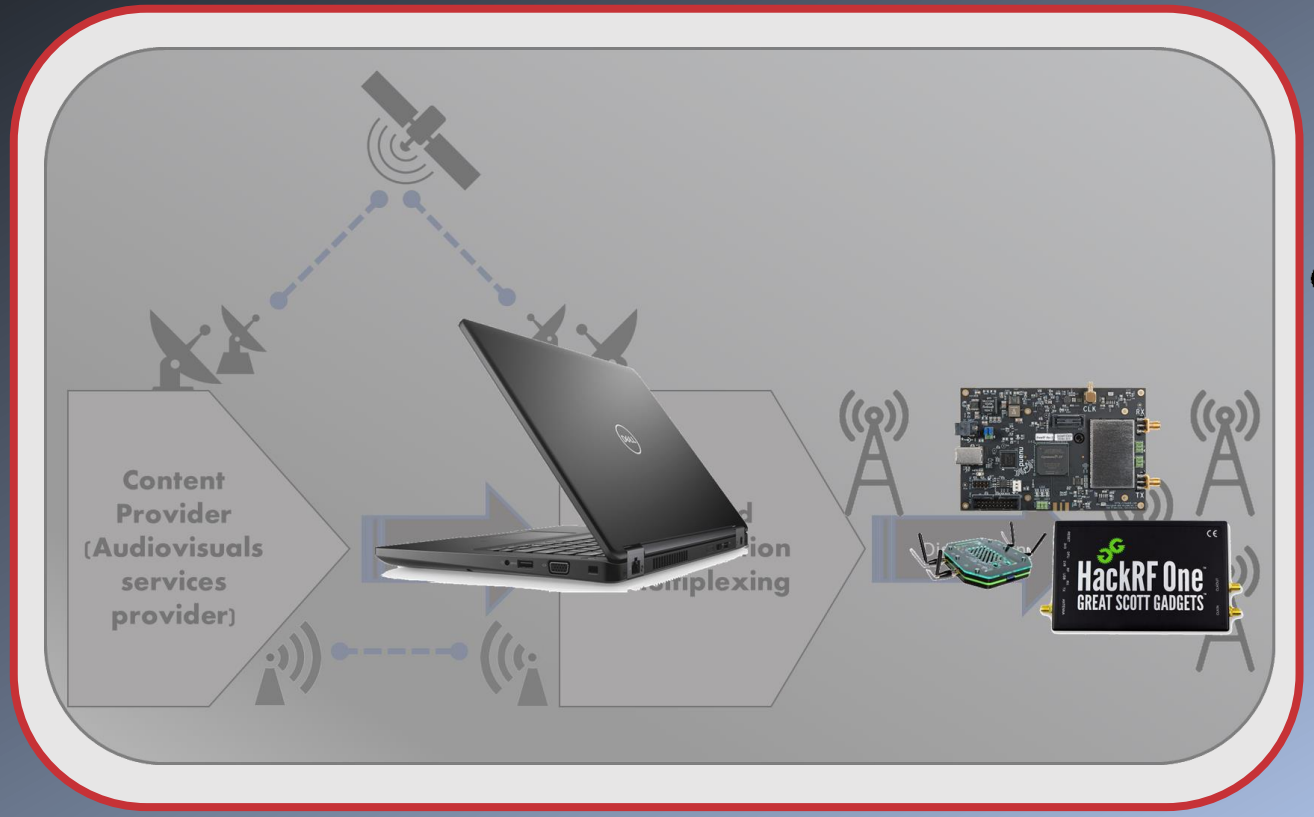
# [II] Smart TV attacks state of the art

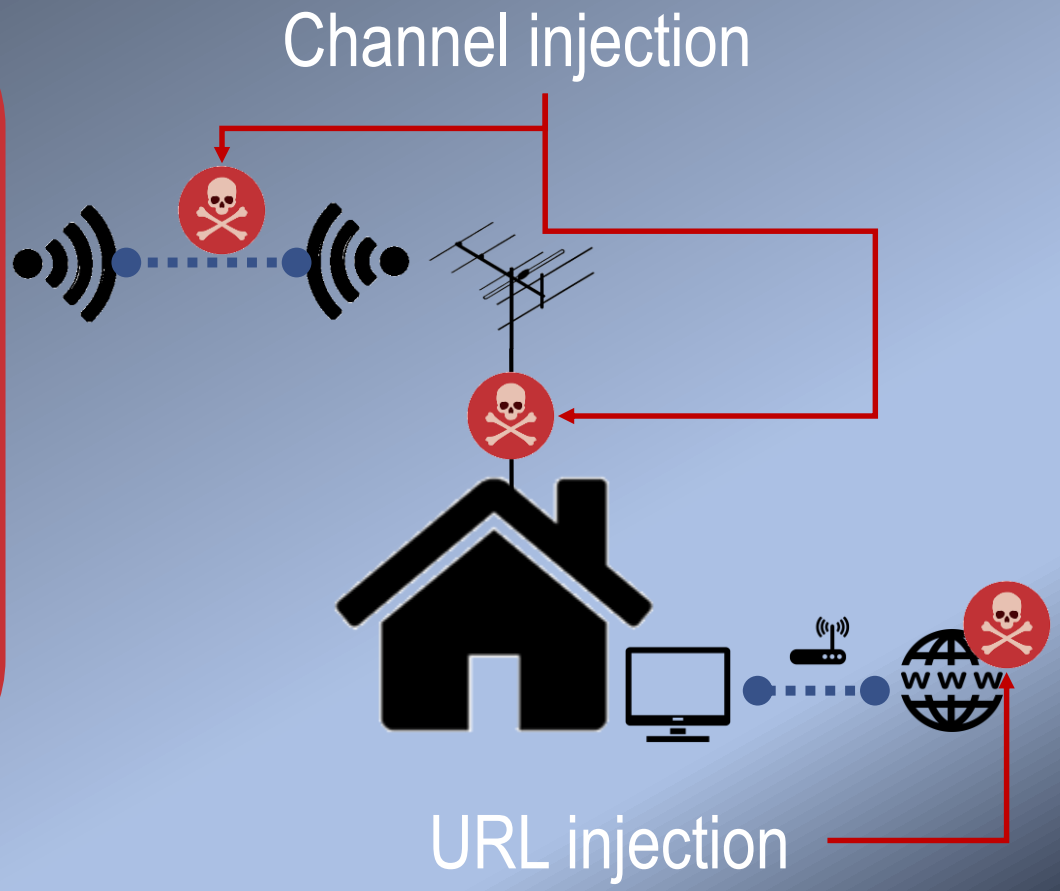
- June 2014 - Weeping Angel (CIA) - WikiLeaks. It shows exactly what an agent must do to turn a Samsung Smart TV into a microphone. Attack requires local access to the Smart TV.

- 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

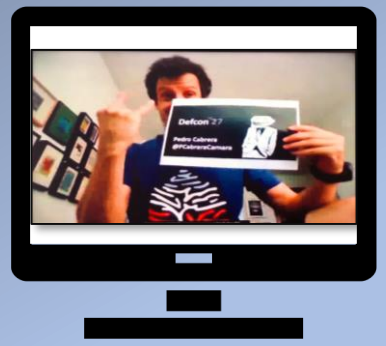
Using the same frequency and channel metadata as in the original channel, we will transmit our video file using BladeRF, HackRF or any capable SDR supported by GNURadio:

Video file

+

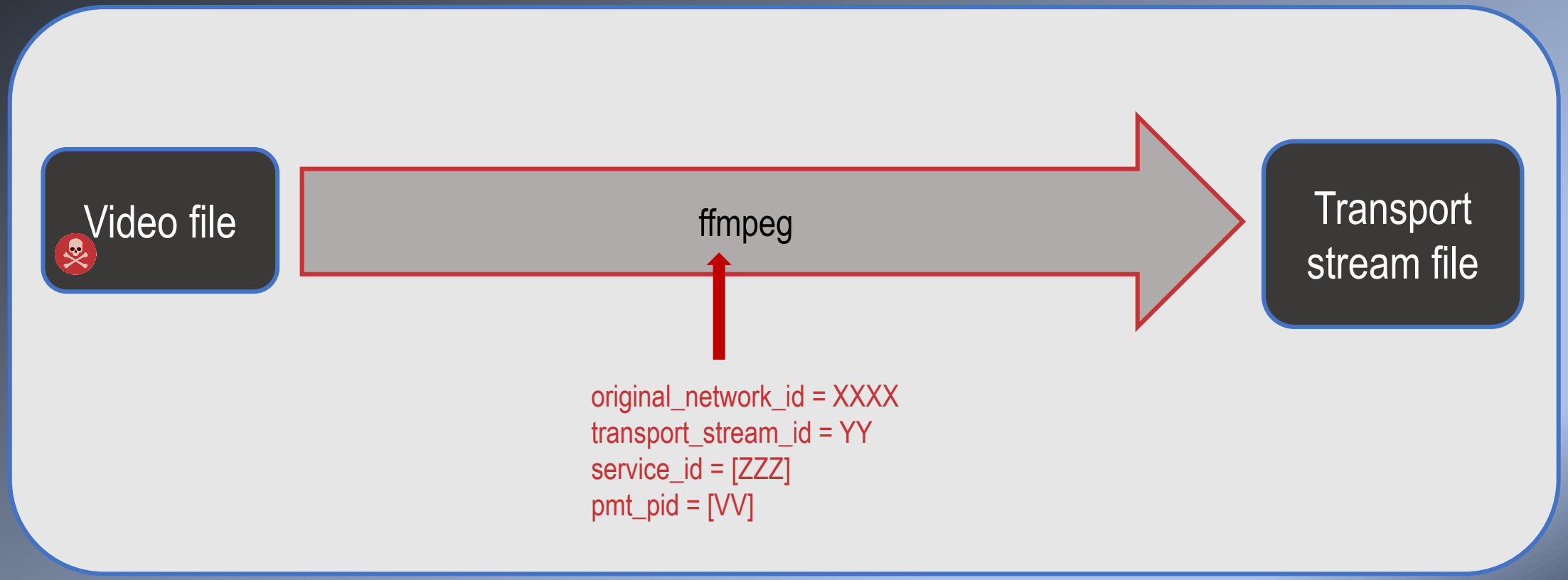
HbbTV Channel metada

gr-dtv (gr-dvbt)

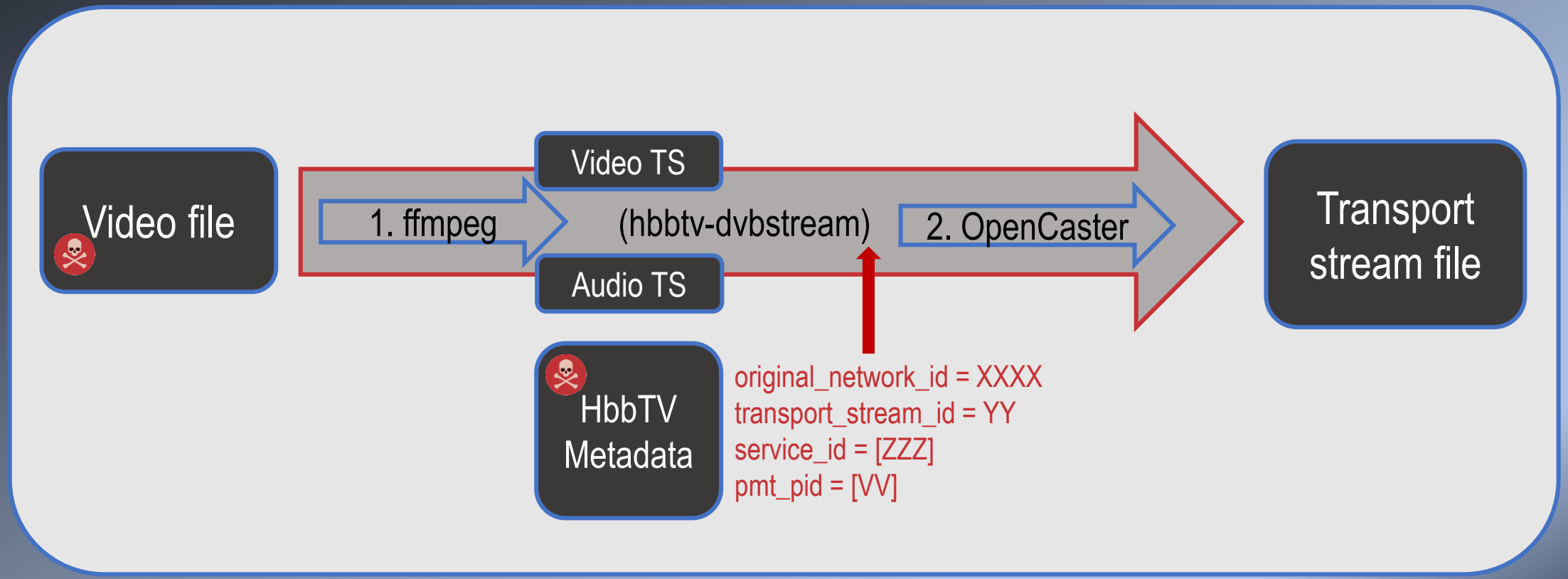
# [II] DVB-T Channel Hijacking

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

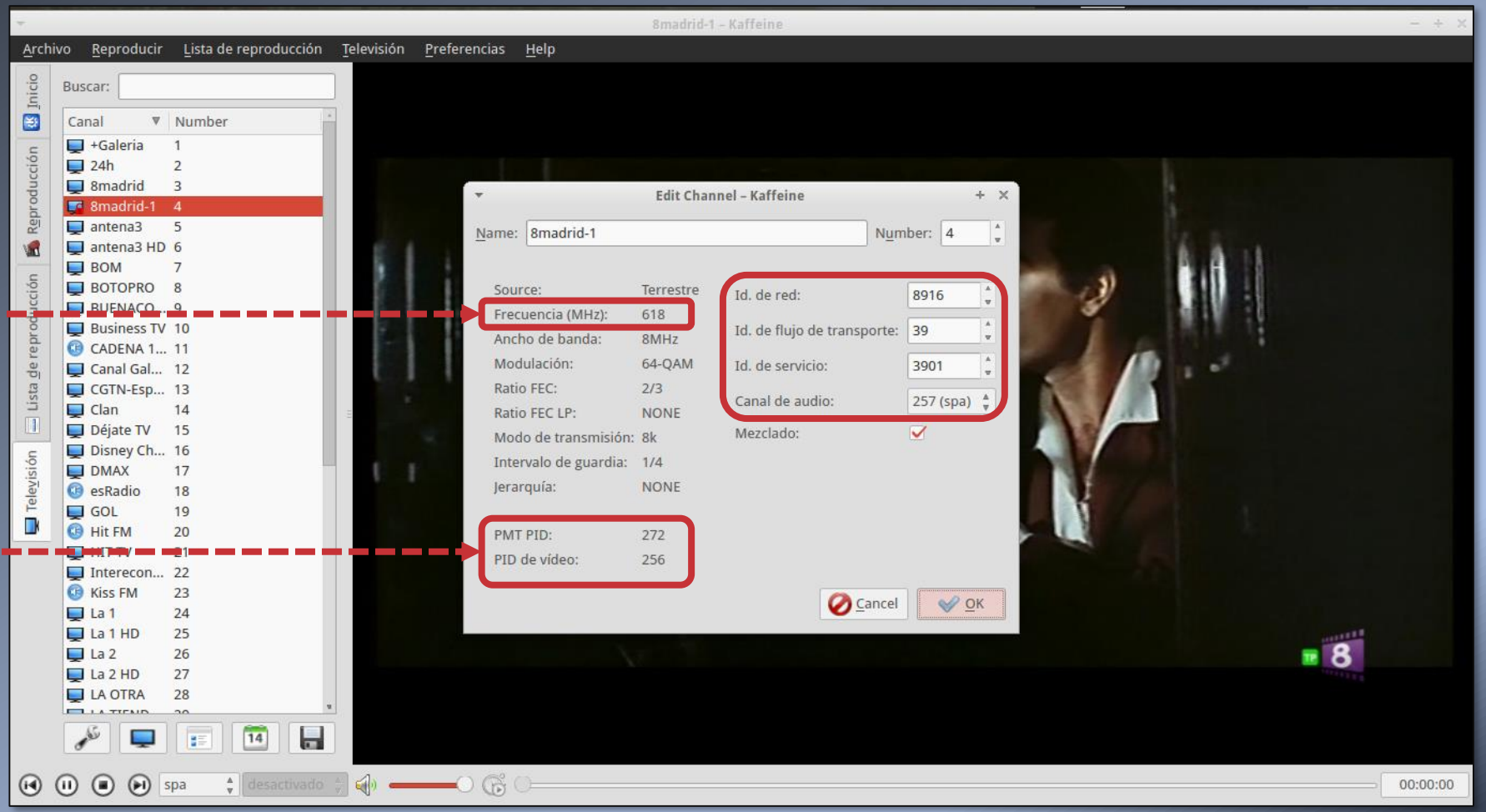


# [II] DVB-T Channel Hijacking

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

# [II] DVB-T Channel Parameters

Linux command line:
dvbv5-scan (DVBv5 Tools)

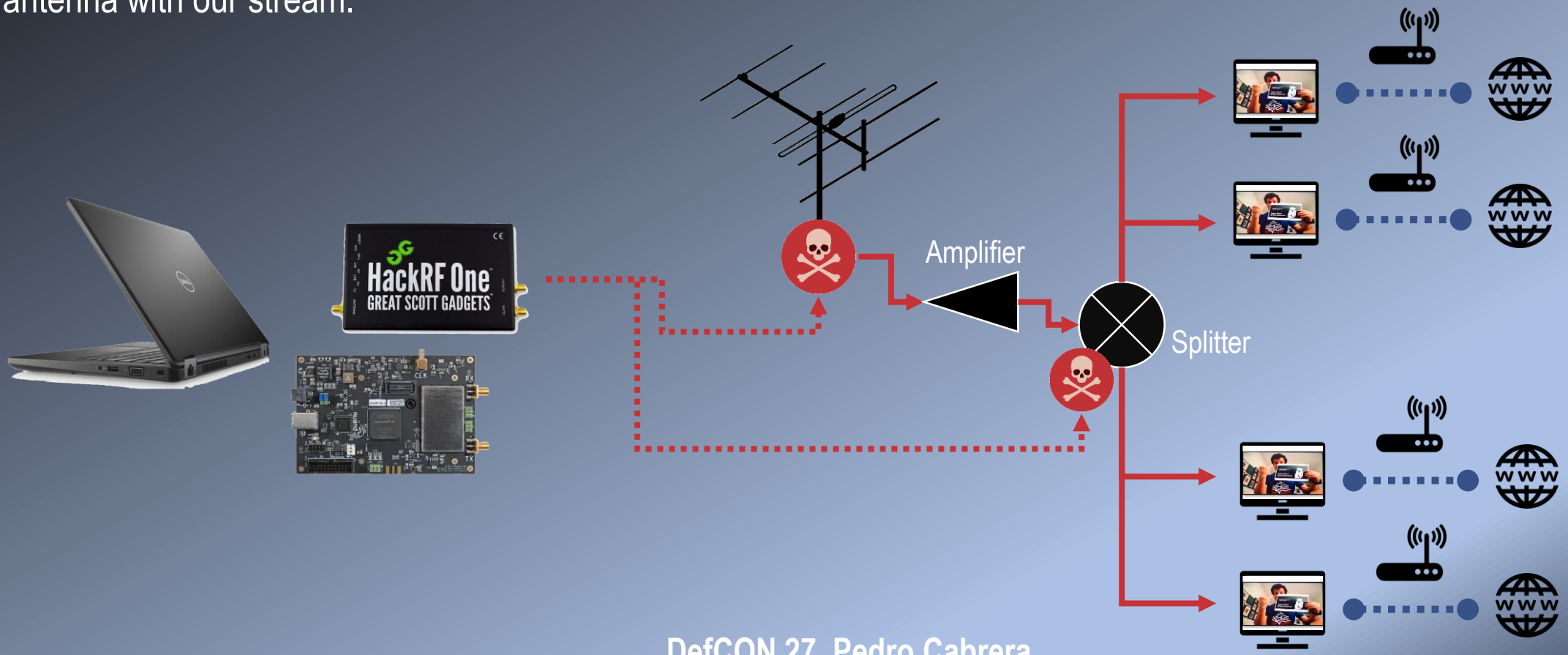
```
Terminal - root@icarus: /home/pedro
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
[nova]
        SERVICE_ID = 154
        NETWORK_ID = 8916
        TRANSPORT_ID = 15
        VIDEO_PID = 601
        AUDIO_PID = 603 604 605
        PID_0c = 625
        PID_06 = 611 202
        PID_05 = 615
        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#
```

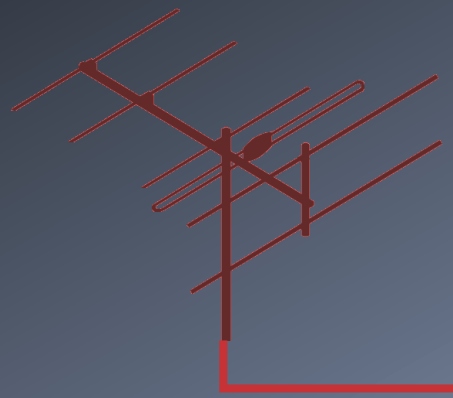
# [II] DVB-T Channel Hijacking

# [III] TV antenna facility attack

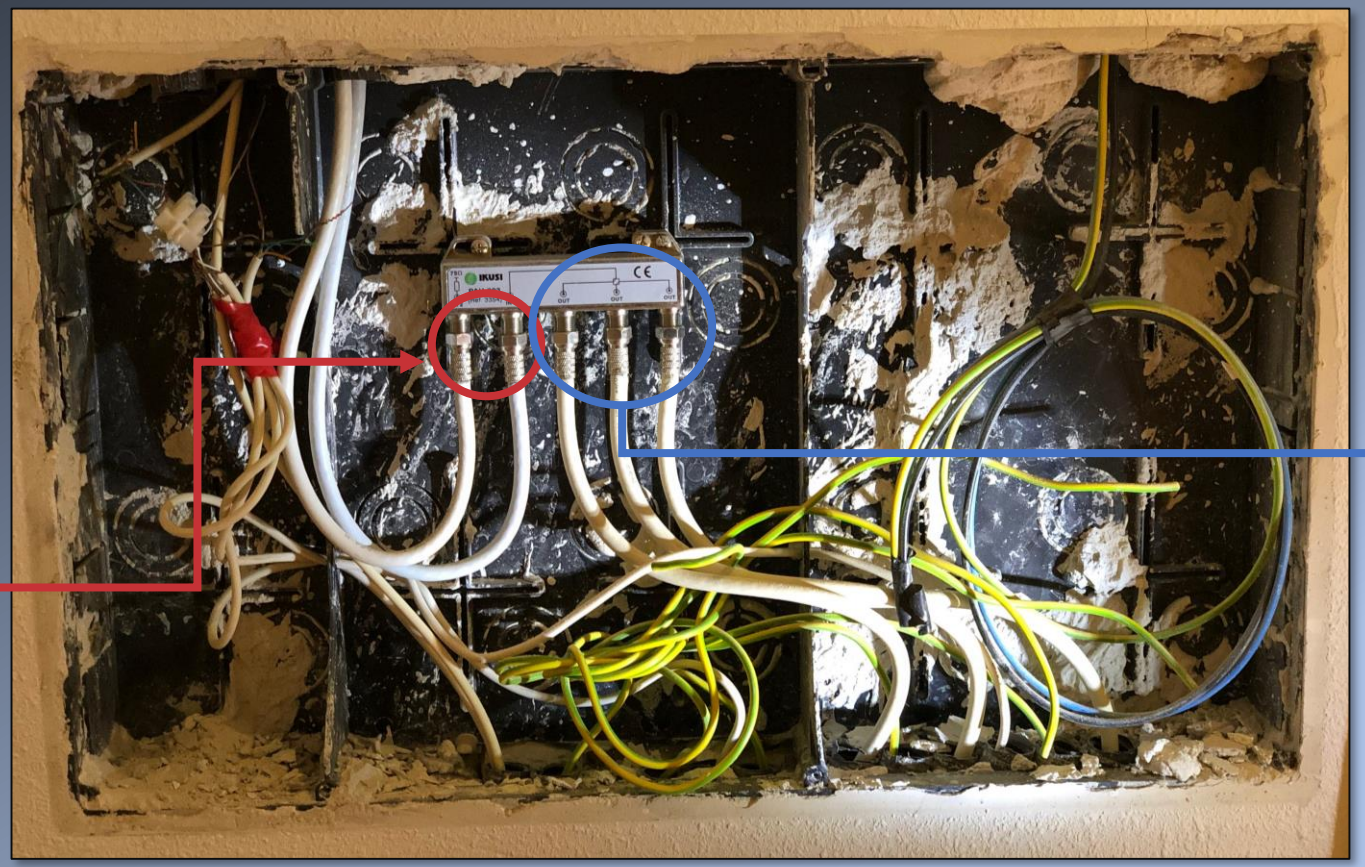
We can eliminate the radio phase by injecting our signal into the antenna facility, replacing the main TV stream from the antenna with our stream.



# [III] TV antenna facility attack

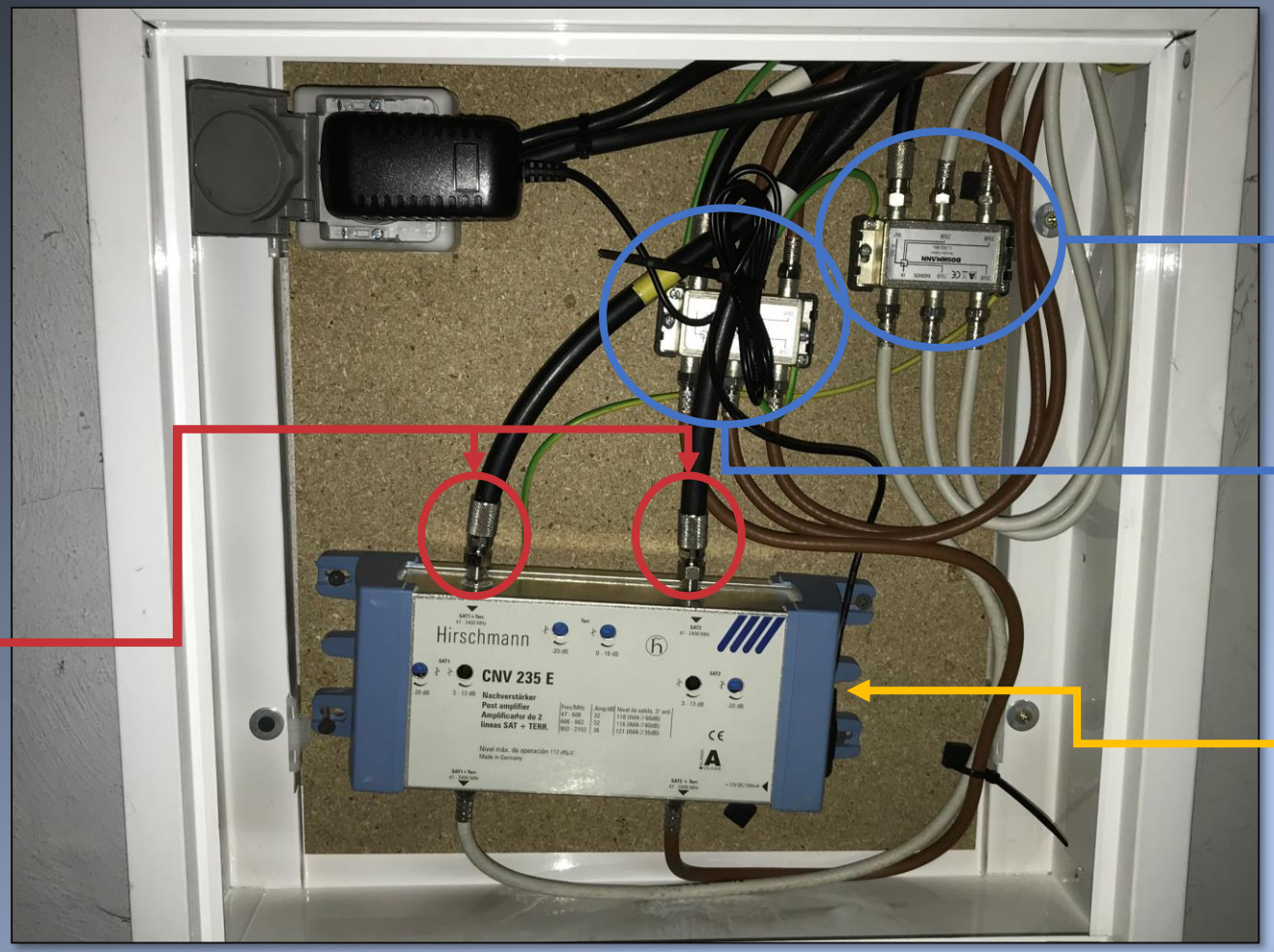


TV antenna facility



TV splitters (1/3)

# [III] TV antenna facility attack (II)

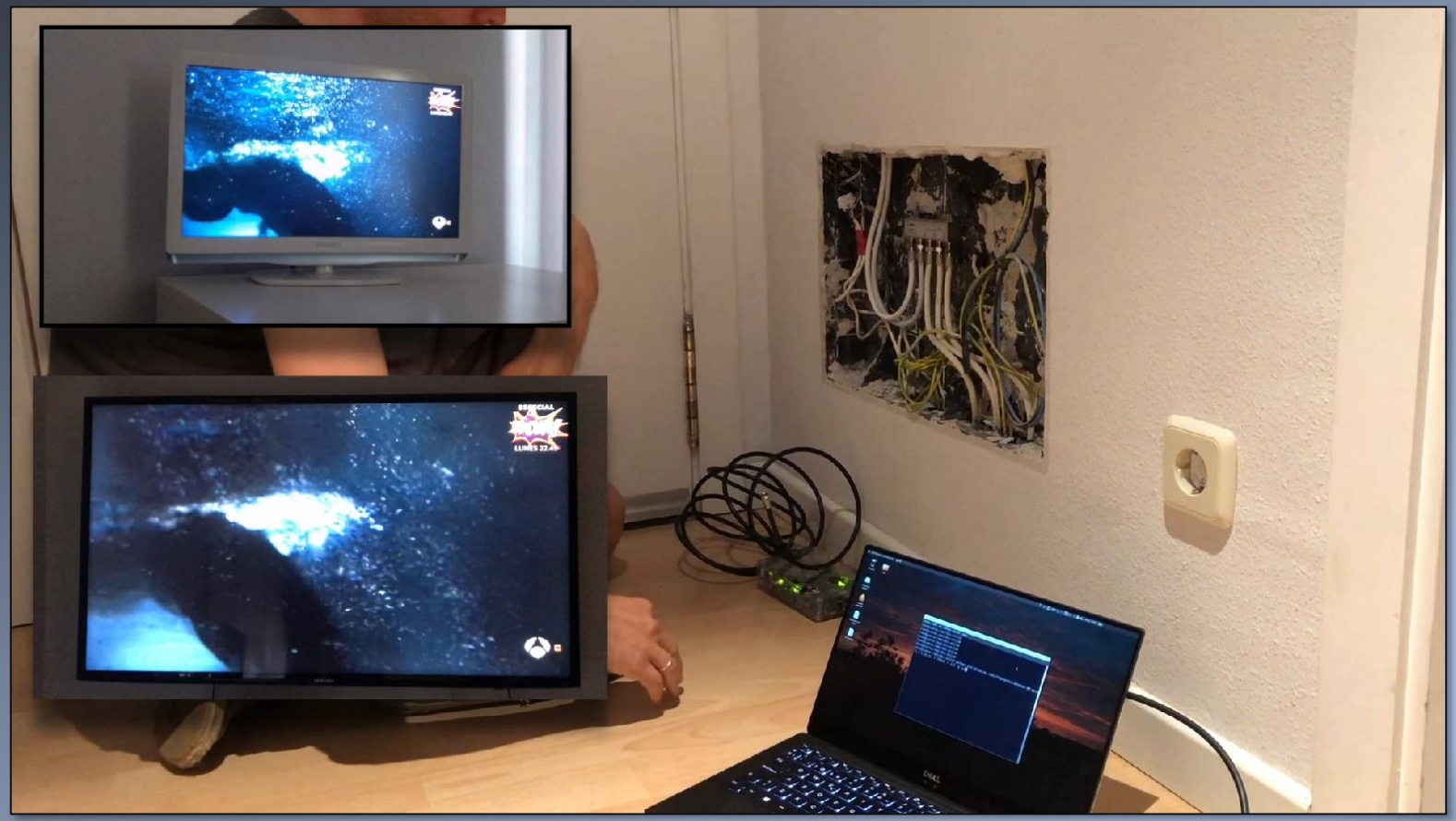



TV splitters (1/4)

TV antenna facility

TV Amplifier

# [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

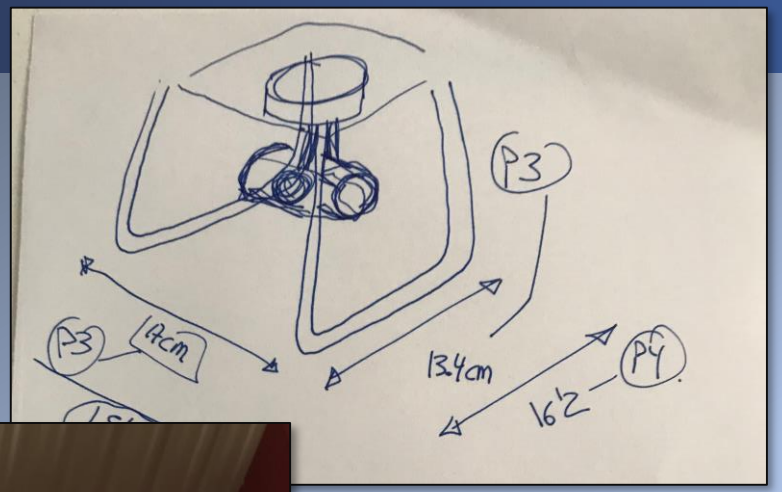
Reservar

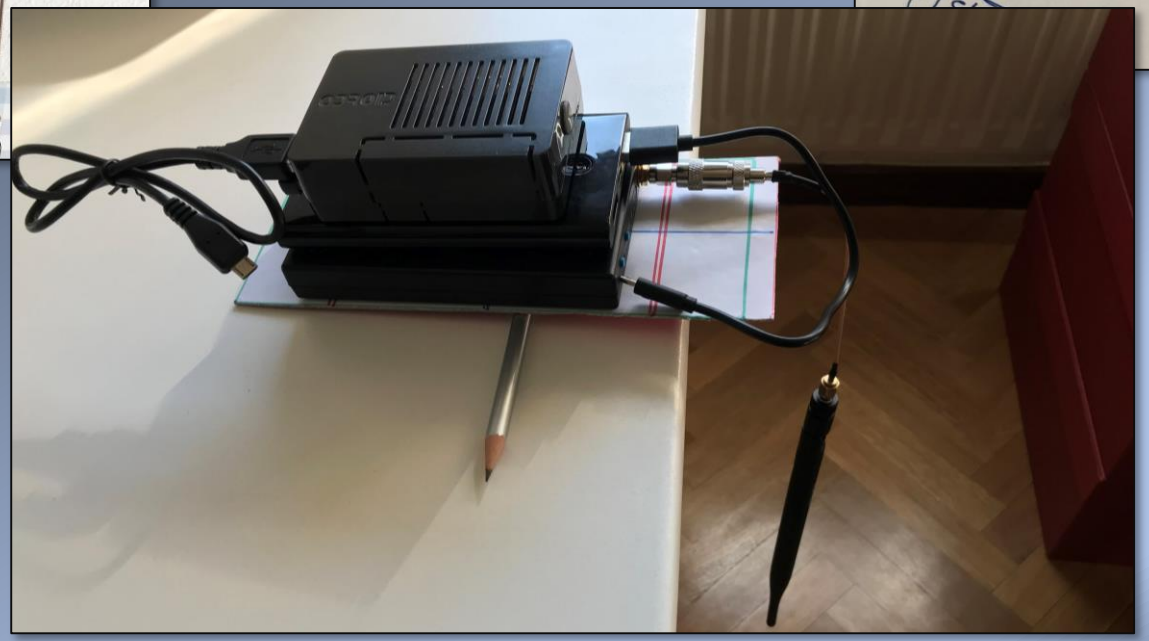
The DJI Phantom 3 Standard is among the most popular drones of all time to date. Despite its design geared towards aerial photography, this does not stop it from being able to lift an additional payload. The DJI Phantom 3 Standard can lift around an additional 300 grams, or

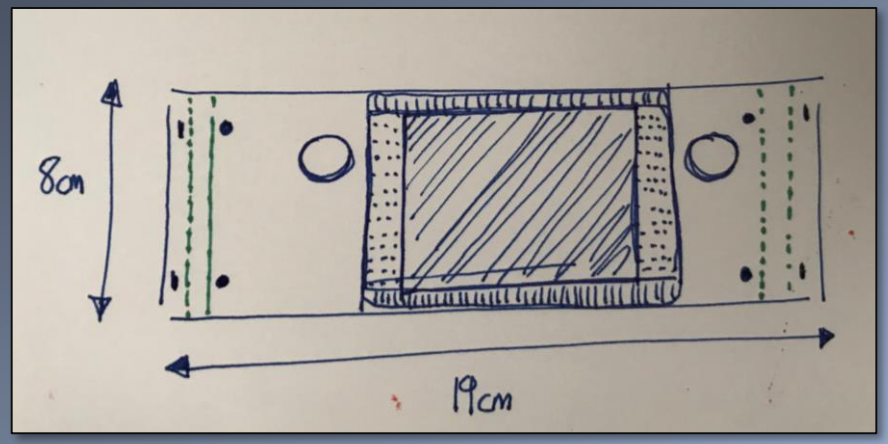
https://www.uavsystemsinternational.com/how-much-weight-can-a-drone-lift/

# [III] Miniaturization – Drone attacks

300 gr

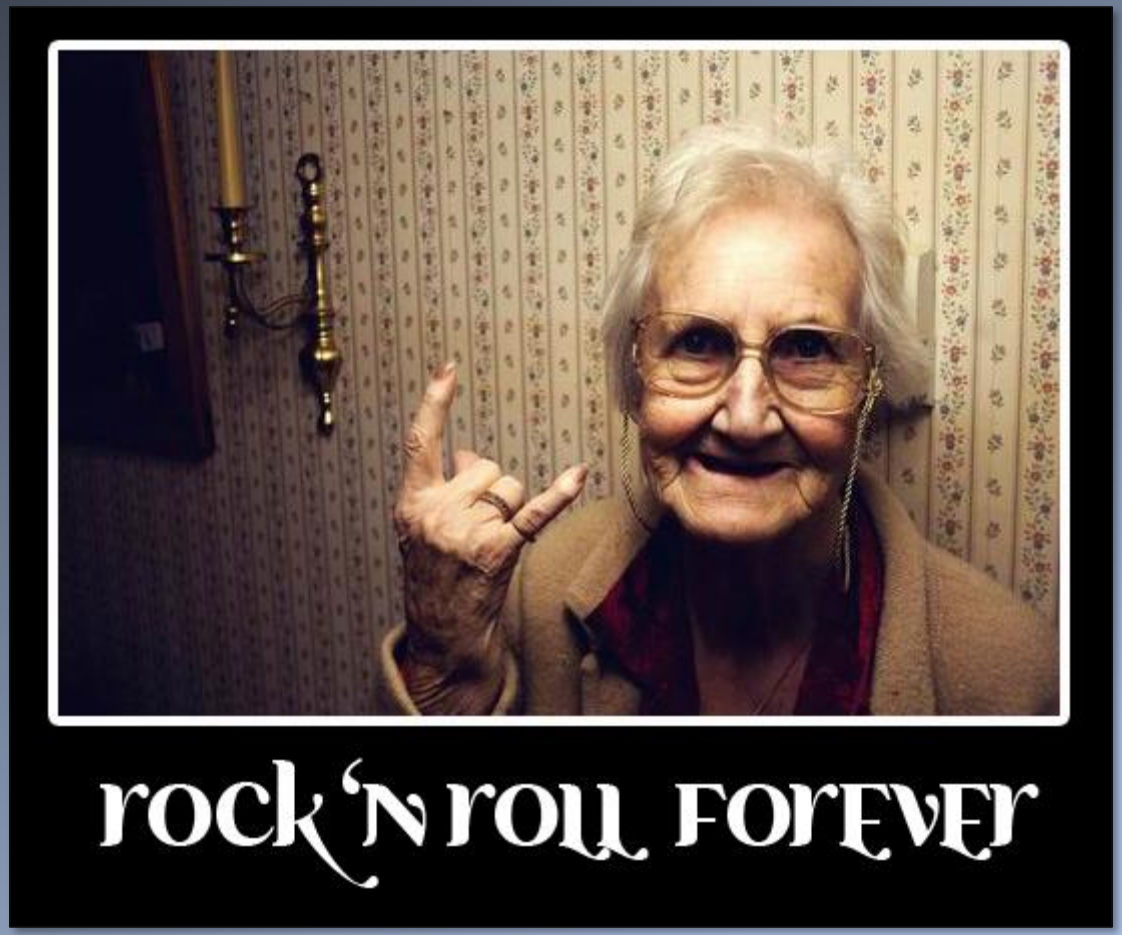


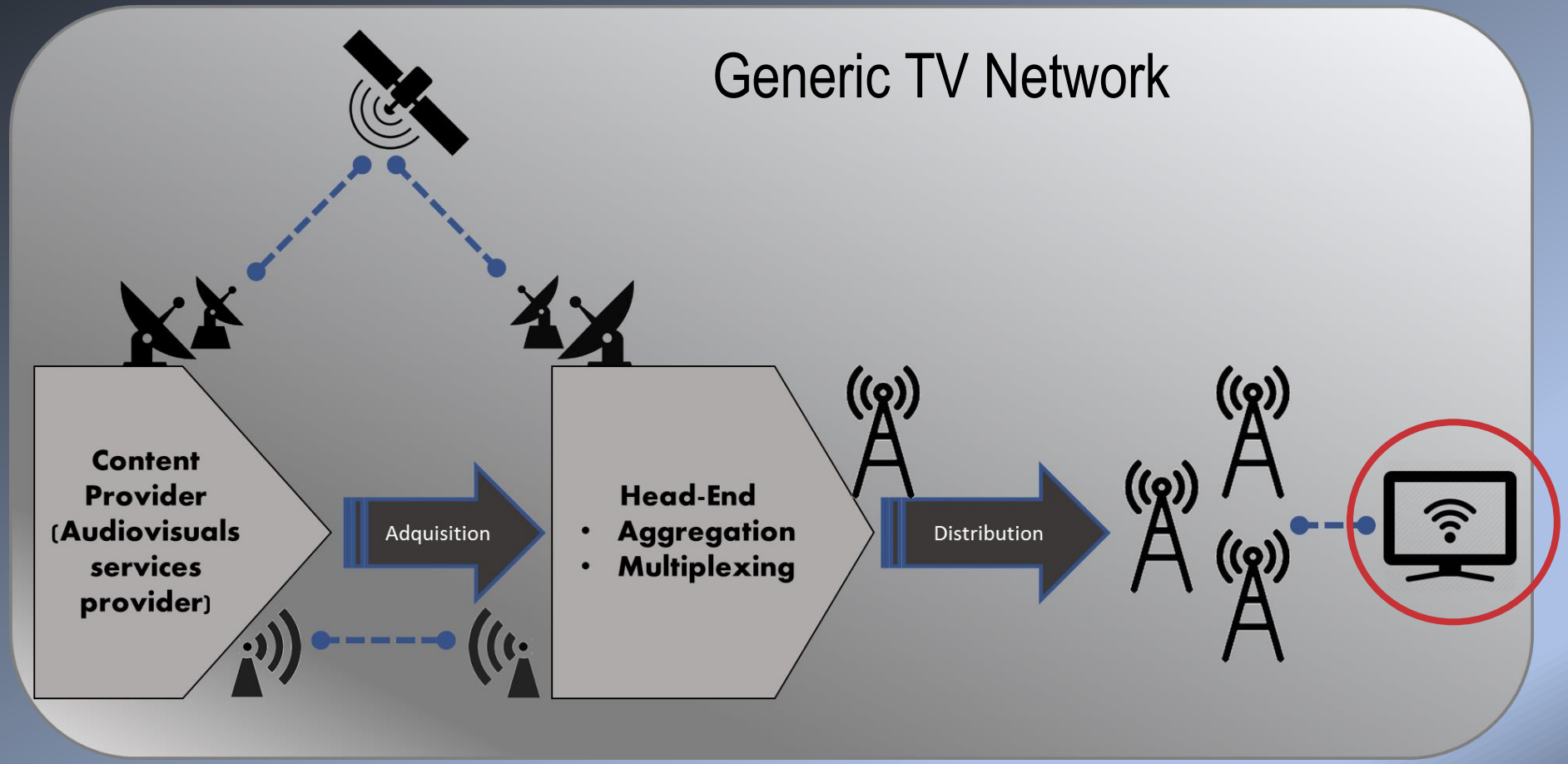



| | |
|---|---|
| GPD | 480gr |
| BladeRF | 170gr |
| | |
| HackRF | 100gr |
| Bateria iPhone 10.000mA | 280gr |
| Bateria Solar 24.000mA | 350gr |
| Bateria NeoXeo 6.000mA | 100gr |
| | |
| Odroid C2 | 68gr |
| Carcasa Odroid | 32gr |

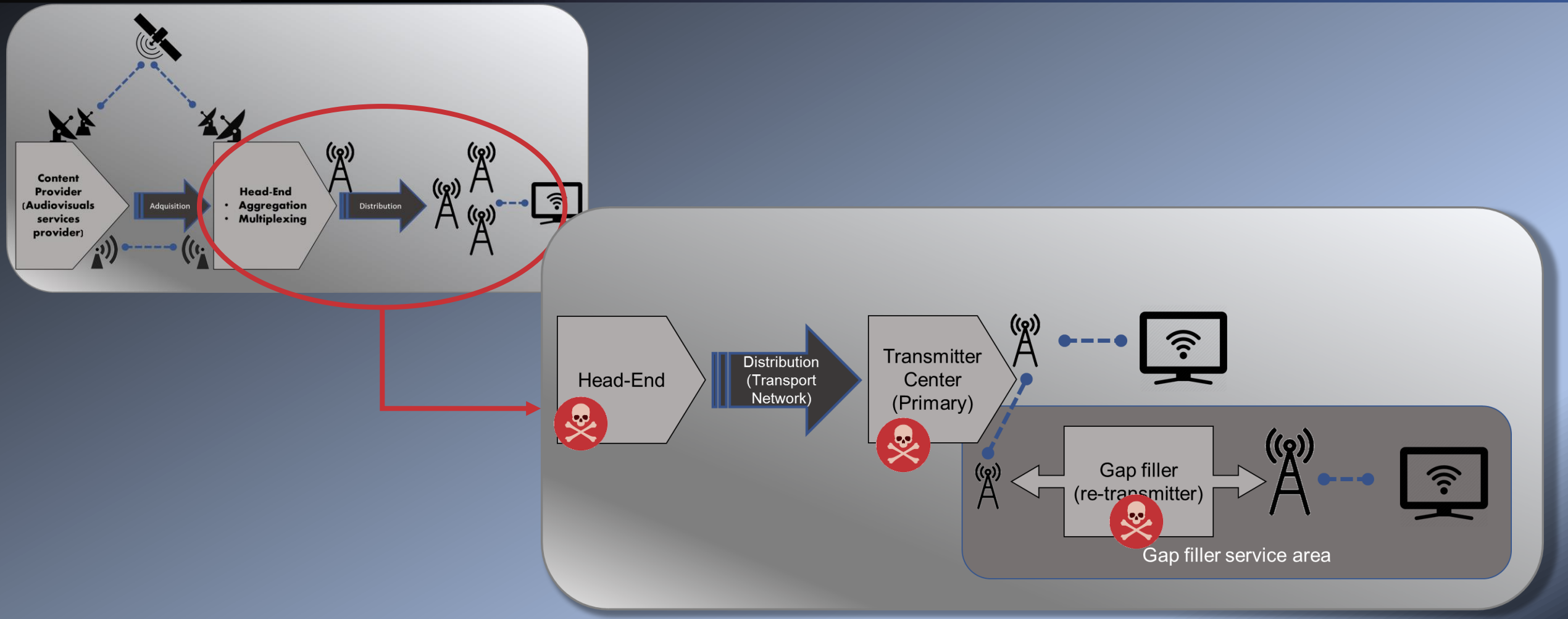
# [III] Drone attack



# [III] DVB-T Channel Hijacking: Impact

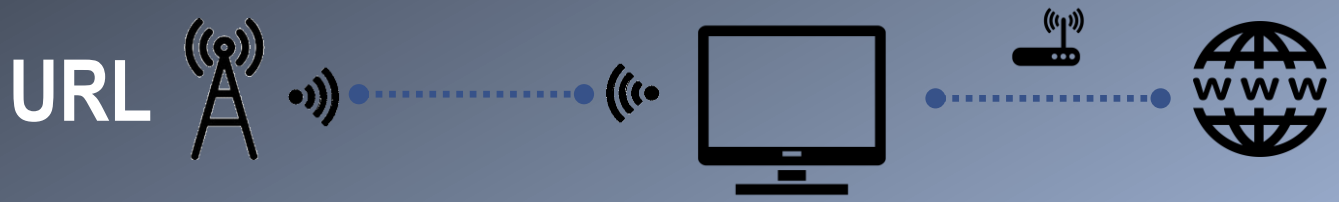


# [III] DVB-T Channel Hijacking: Impact



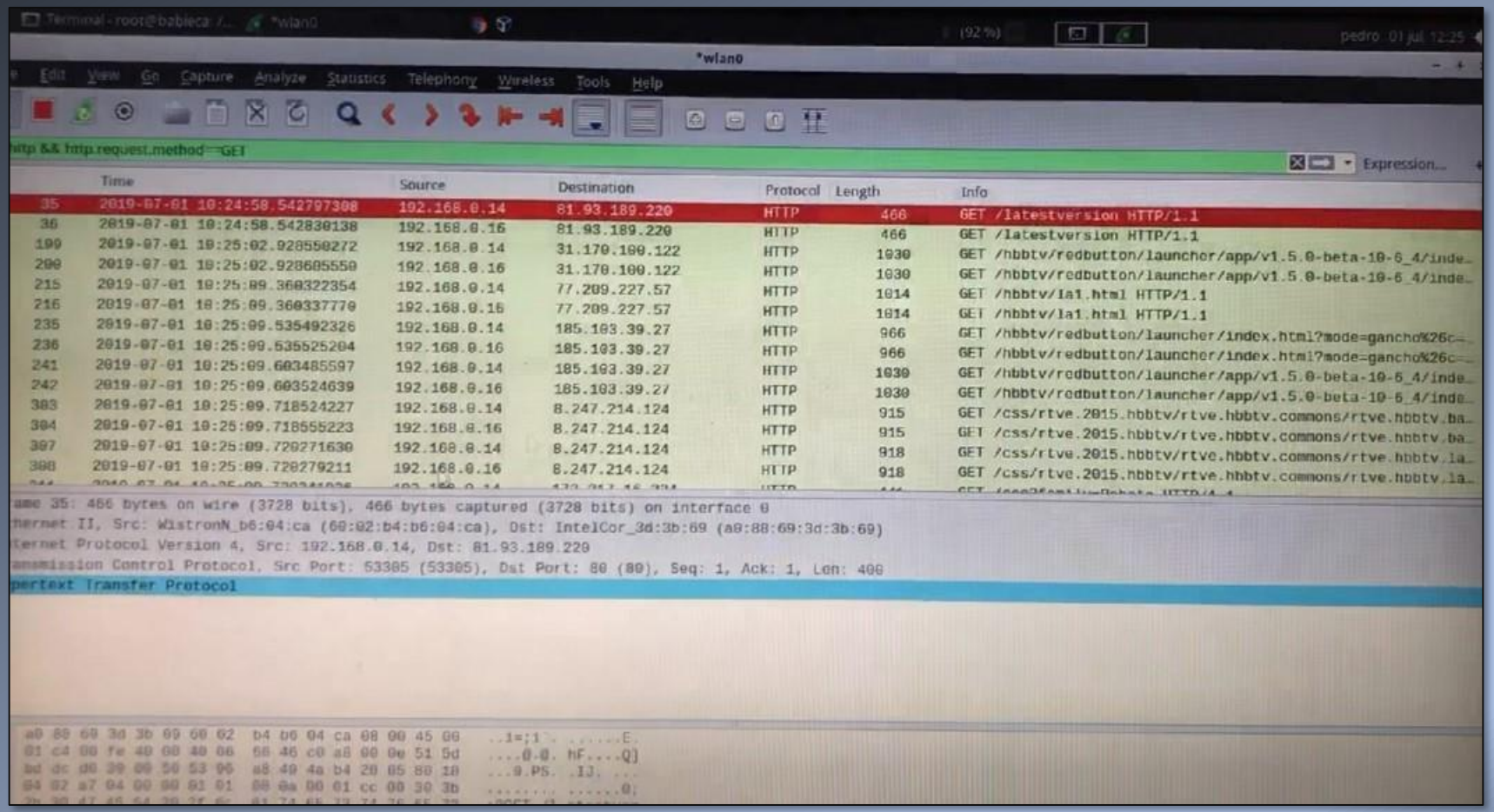
# [IV] URL Injection attack

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



# [IV] URL Injection attack: Basic

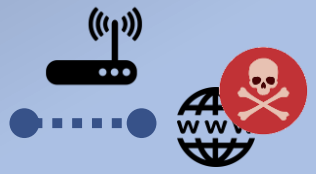
We add the URL of our fake server in the HbbTV metadata: application name, base URL, web page, organizationId and applicationId

Video file

+

HbbTV Channel Metada (URL)

→ gr-dtv (gr-dvbt)

# [IV] URL Injection attack: Video Replay

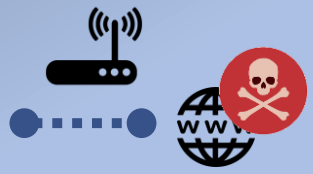

DVBv5 Tools
dvbsnoop

Channel video
& audio

gr-dtv
(gr-dvbt)

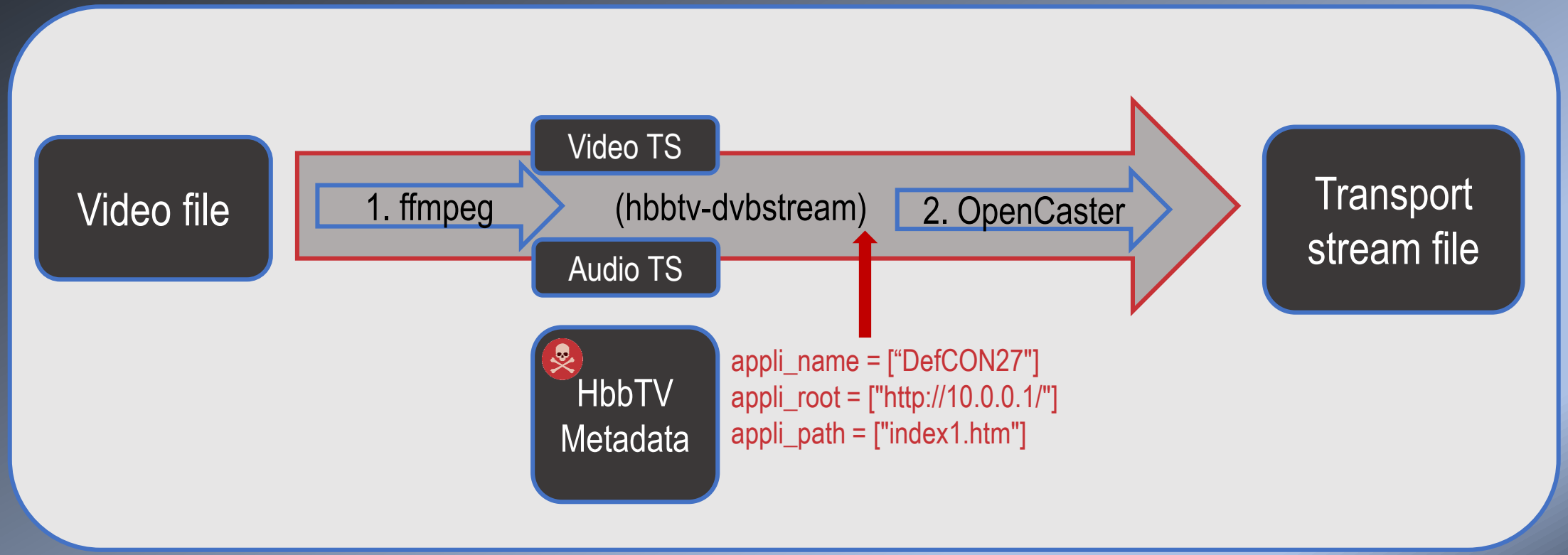
HbbTV
Channel
Metada (URL)





# [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:



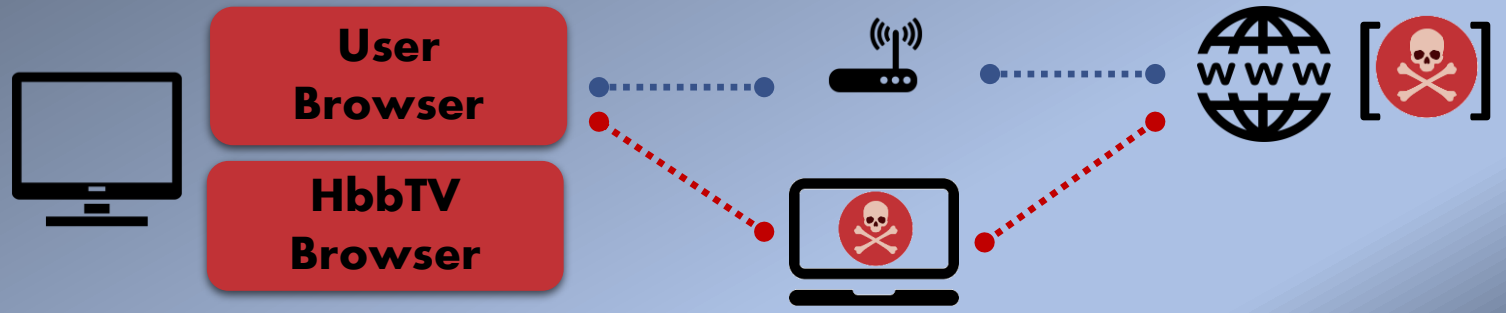
# [IV] One SmartTV, two browsers

**SDR URL injection attack**

· HbbTV Browser (remote)


**ARP Poison/DNS Hijacking URL injection attack**

· 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:

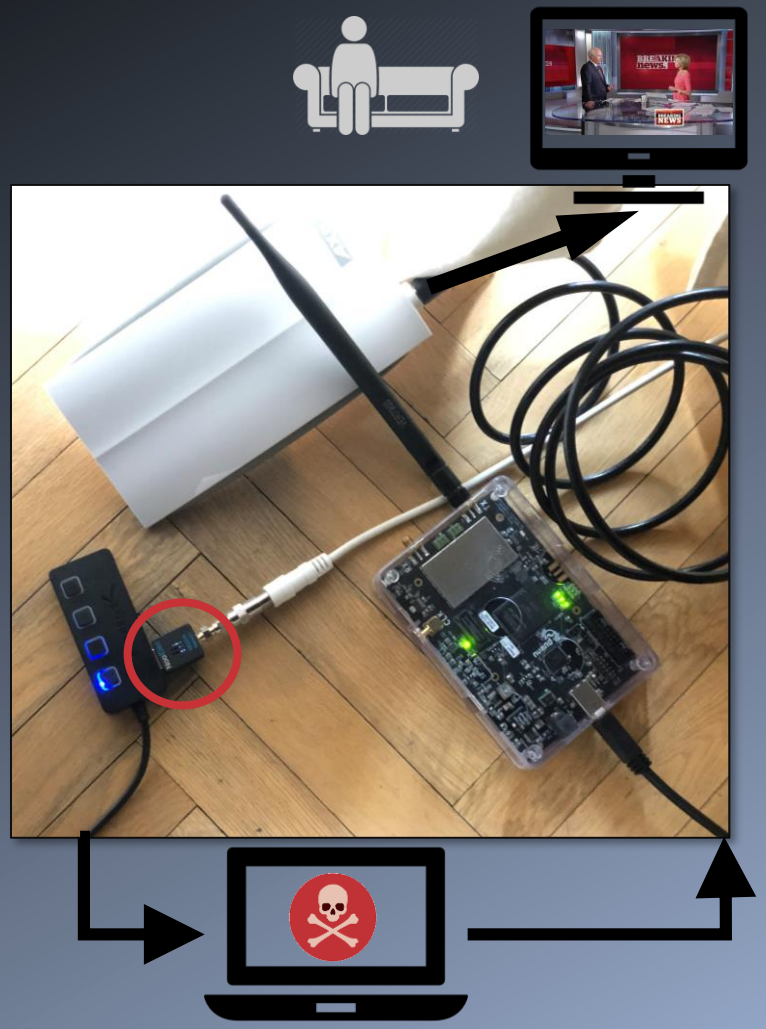
- Public IP address
- Models/Manufacturers (UA)
- DVB-T Channels/Audience analysis

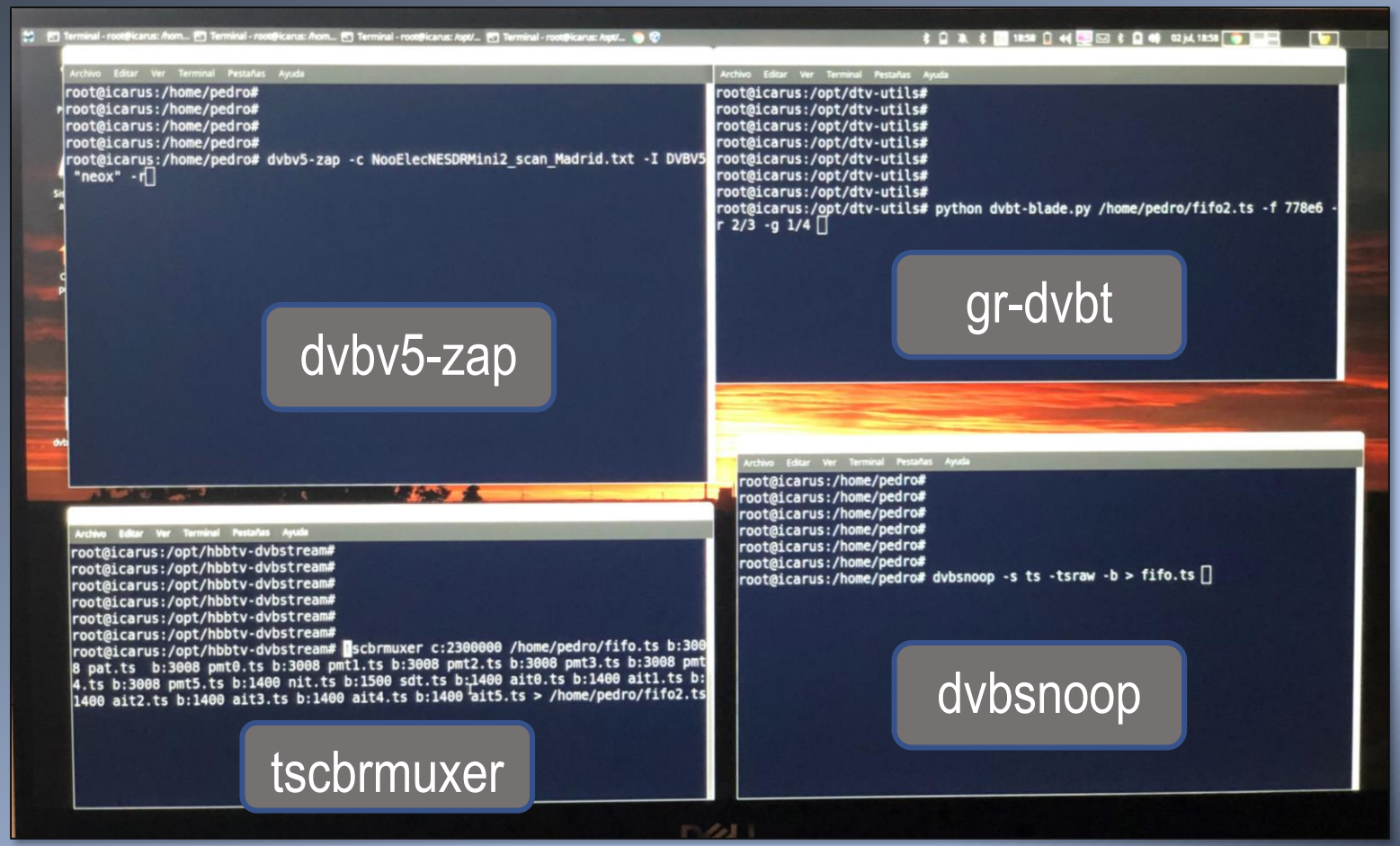
Terminal - root@babieca: /var/log/apache2

Archivo Editar Ver Terminal Pestañas Ayuda

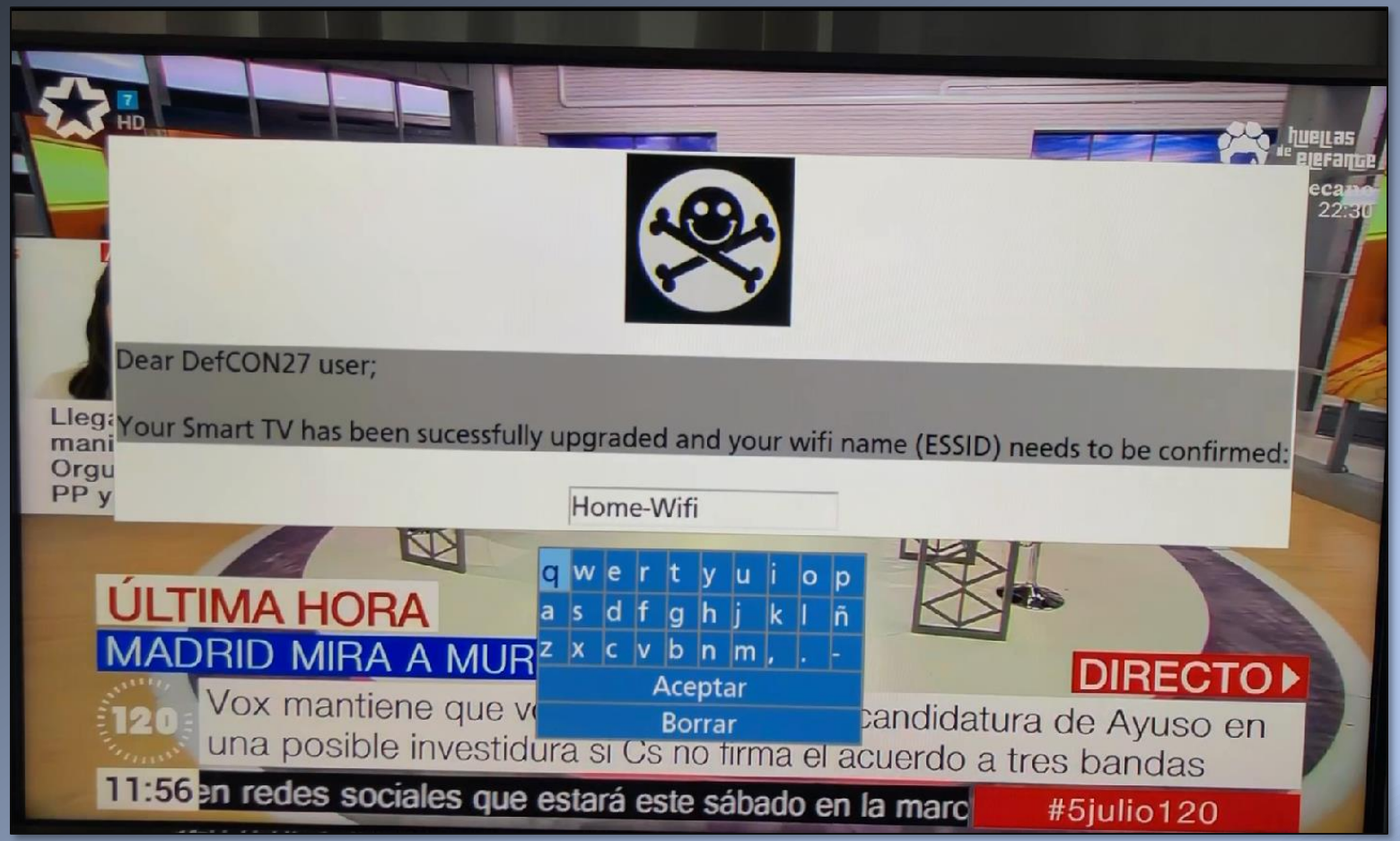
```
10.0.0.60 - - [20/Feb/2018:13:03:02 +0100] "GET /lasexta/app/scenes/Score.js HTTP/1.1" 200 794 "http://hbbtv.atresmedia.com/lasexta/index.html" "HbbTV/1.2.1 (;Panasonic;VIERA 2014;3.101;6101-0003 0010-0000;)"
10.0.0.60 - - [20/Feb/2018:13:03:02 +0100] "GET /lasexta/app/scenes/ShortcutToScene.js HTTP/1.1" 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

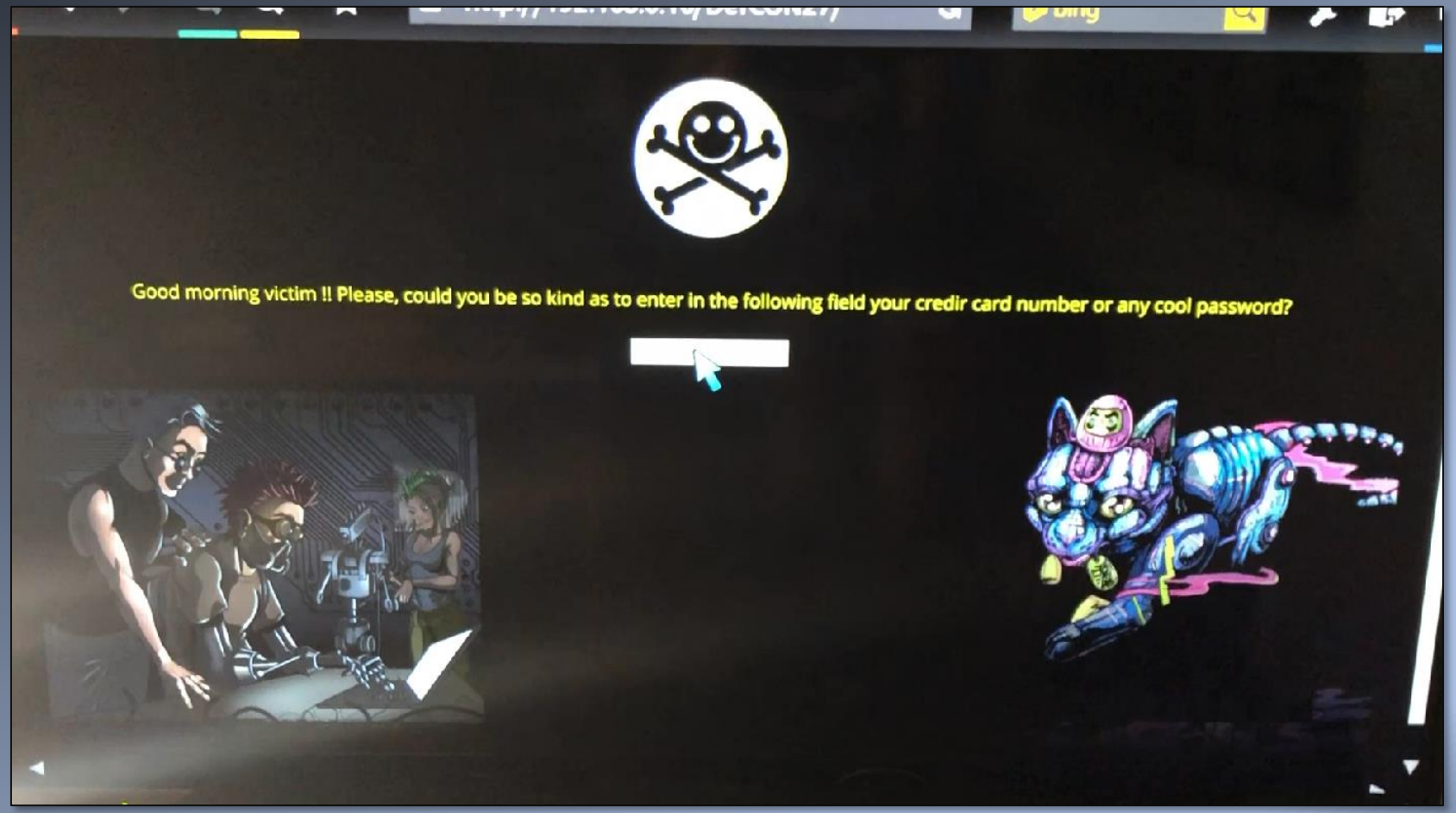




# [IV] Social engineering (SE) attacks



# [IV] Keylogger attack



# [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

**Cryptojacking: Hackers Just Want to Borrow your CPU**

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

**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.

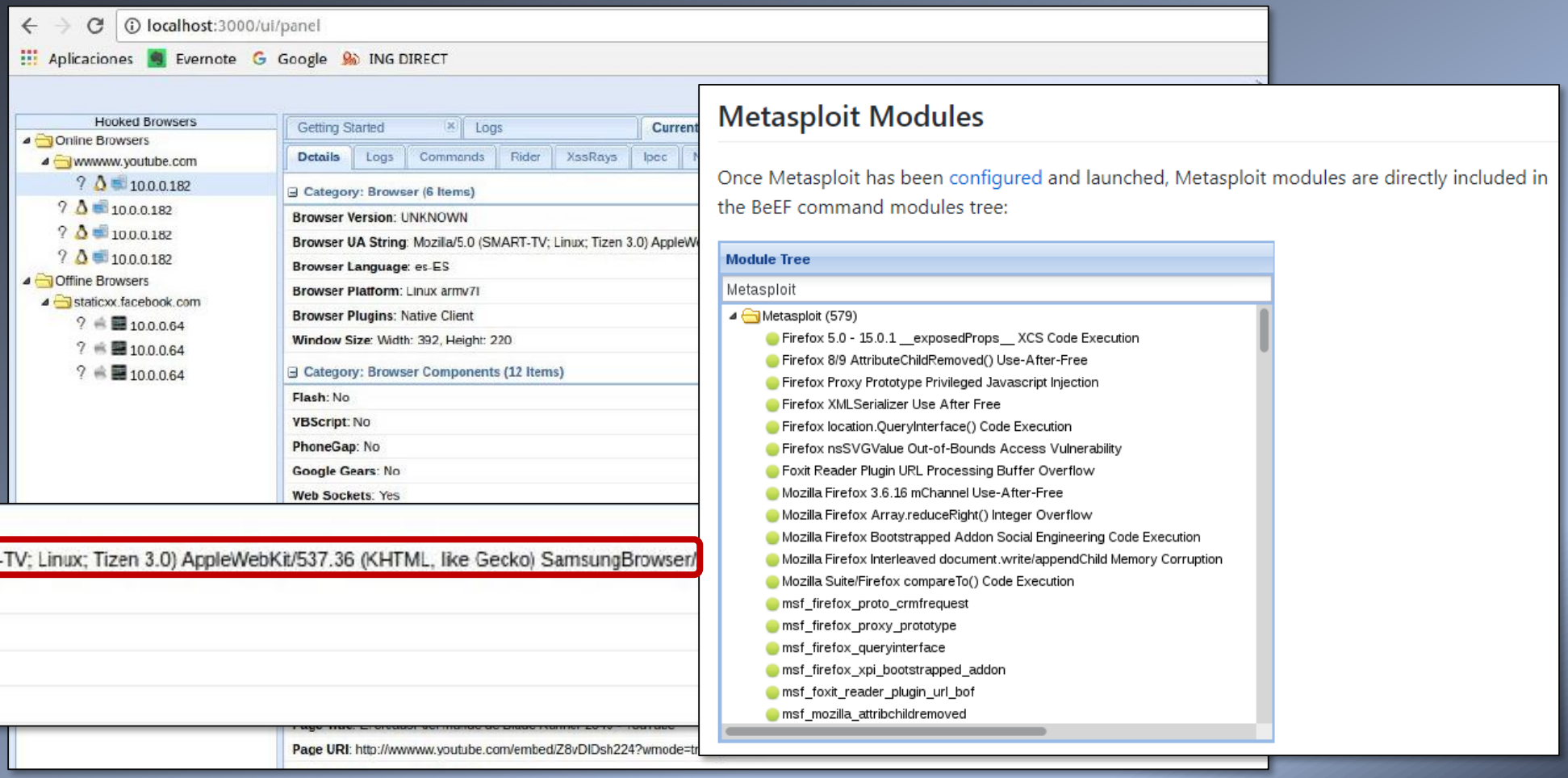
https://www.express.co.uk/finance/city/911278/cryptocurrency-hacking-bitcoin-ripple-ethereum-mining-youtube-adverts

**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/

# [IV] Crypto Mining attack


# [IV] Hooking user browser

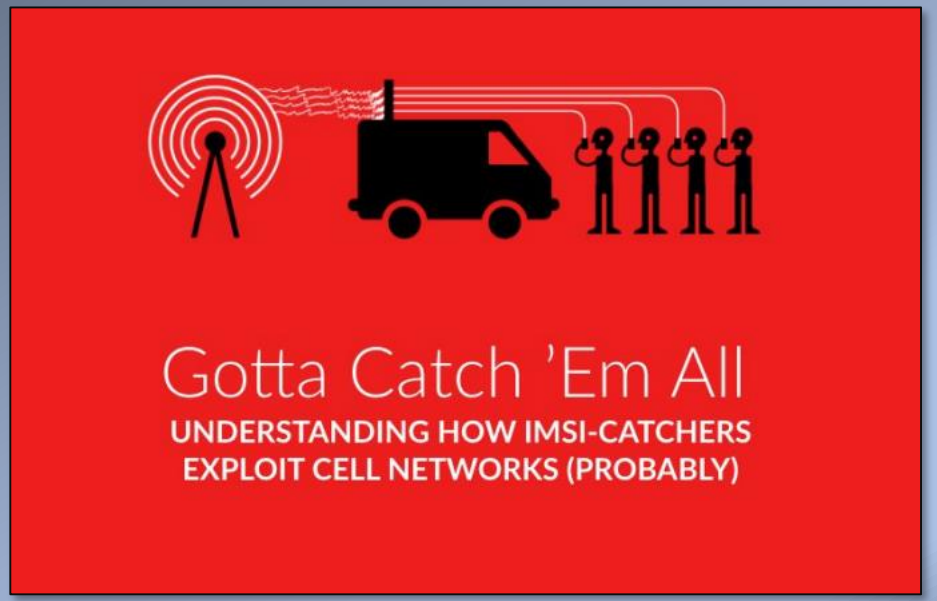


# [IV] User browser attack

# [V] Conclusions

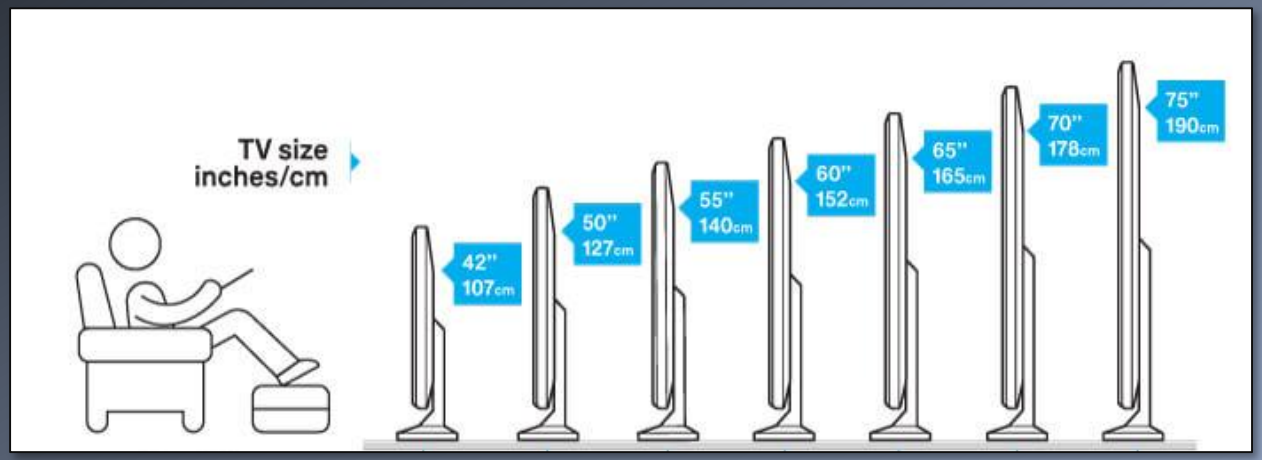
## Mass GPS Spoofing Attack in Black Sea?

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

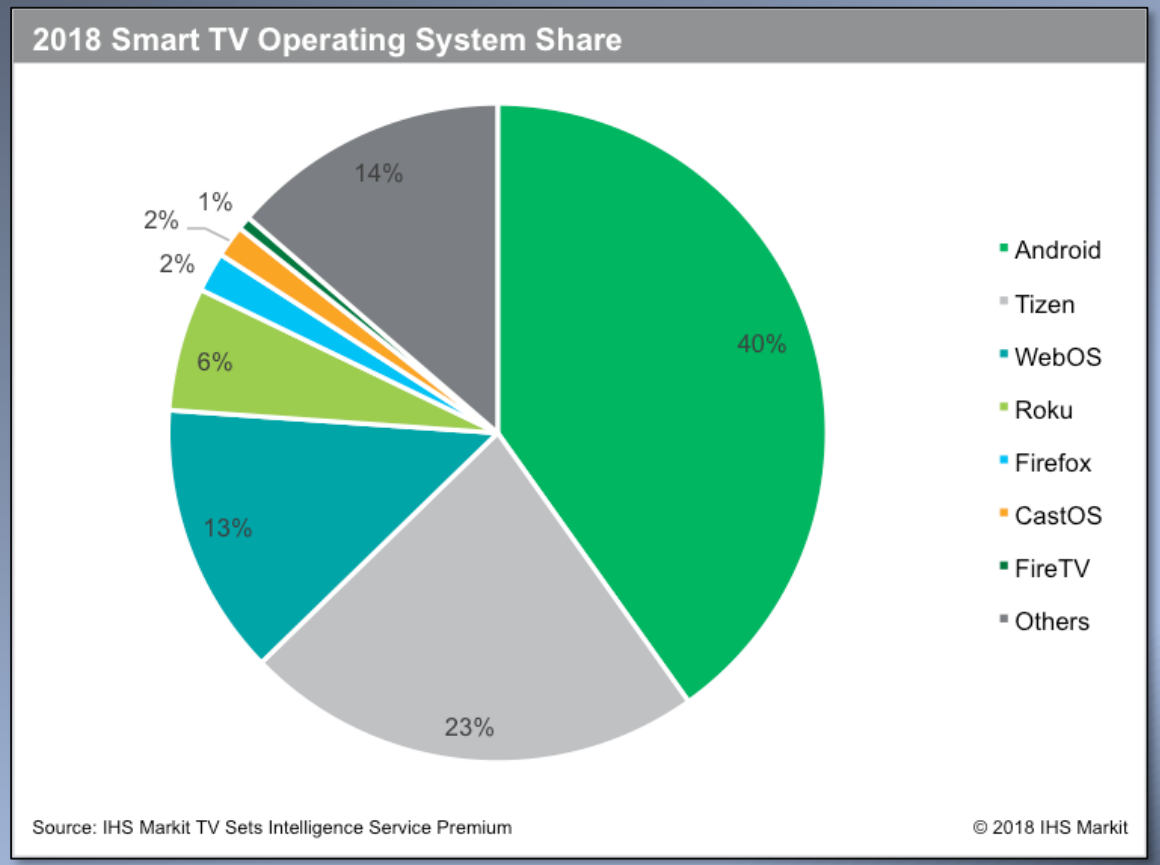



https://www.eff.org/files/2019/07/09/whitepaper_imsicatchers_eff_0.pdf

# [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-alexa-and-google-assistant/


Thank You
Gonzalo Manera
Pepe Cámara
Alvaro Castellanos
Luis Bernal (aka n0p)
github.com/pcabreracamara/DC27
2019 August, DefCON 27