

# DVB: Satellite Hacking For Dummies

**Wzz - Undercon 2004**



A satellite is shown in orbit above the Earth, with a blue beam of light directed towards the planet. The Earth is partially visible on the right side of the slide, showing continents and oceans.

# ¿Qué vamos a ver?

- § Introducción a los Satélites
- § Introducción a la interceptación de satélites
- § DVB
- § Equipo Básico recomendado
- § FTA y TV de Pago
- § Feeds
- § Datos: ISP satélite DVB/IP , DVB-RCS, etc.

# Introducción

A satellite is shown in orbit around the Earth. The satellite is a small, rectangular object with two long, thin solar panel arrays extending outwards. It is positioned in the upper right quadrant of the slide, with a blue orbital path leading towards the Earth. The Earth is shown as a curved horizon on the right side of the slide, with a bright light source (the sun) illuminating the top edge, creating a lens flare effect.

§ Satélites según su órbita

§ Órbita Baja (LEO)

§ Órbita Geoestacionaria (GEO)

§ Otras: Molniya, Alta (HEO), etc.

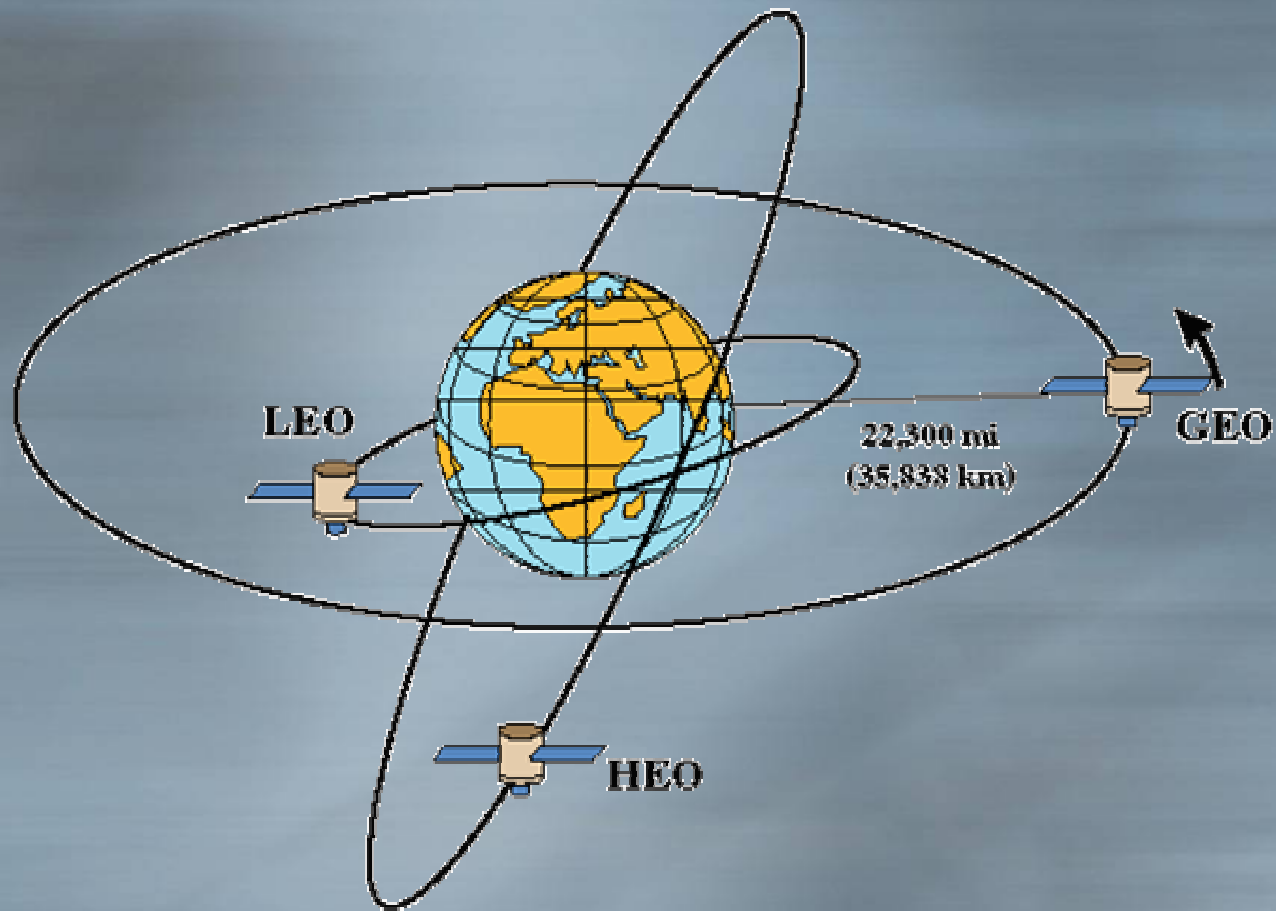
§ Satélites según su cometido

§ Comunicaciones

§ Observación de la tierra

§ Otros: Científicos, ISS, etc.

# Introducción



# Recepción de satélites

A satellite is shown in orbit above the Earth. The satellite is a small, rectangular object with a central body and two long, thin solar panel arrays extending outwards. It is positioned in the upper right quadrant of the slide, with a blue orbital path leading towards the Earth. The Earth is shown as a curved horizon with green and brown landmasses and blue oceans, set against a dark blue background representing space.

## § Satélites LEO

- § Meteorológicos (NOAA, 137 Mhz)

- § Radioaficionados (Voz y Packet) Ej. ISS.

## § Satélites GEO

- § UFO (UHF Follow On) Militares (250 mhz)

- § Inmarsat

- § Meteorológicos (Meteosat)

- § SCPC / Enlaces Telefonía FDMA

# Ej. Interceptación Inmarsat.



## § Inmarsat A

§ Teléfonos satélite analógicos

§ Banda L (1.5 Ghz), Narrow FM

§ Receptor (1000 Eur.), Fabricar Antena y LNA

## § Inmarsat C

§ Datos BPSK 1200 bps (NAVTEX, email, etc.)

§ Receptor (1000 Eur.), Antena, Software  
decodificador (4500 Eur.)

# Ej. Interceptación Inmarsat.



<http://ourworld.compuserve.com/homepages/pjmarsh/inmarsat.htm>

DVB



¡Por fin del cielo  
la señal que  
estaba esperando !



# Equipo recepción DVB



Antena 60 Cm + LNB  
25 Euros Aprox



Soporte, cable, etc.  
12 Euros Aprox



Tarjeta DVB  
SkyStar 2  
60 Euros Aprox.

Total: Menos de 100 Euros!

# DVB



§ Standard ETSI abierto para la transmisión de:

§ Video.

§ Múltiples portadoras de Audio

§ Radio.

§ Subtítulos, EPG, Teletexto.

§ Datos.

# DVB



## § DVB-C

§ TV por Cable Digital, 64-QAM

## § DVB-S

§ TV Satélite Digital, QPSK

## § DVB-T

§ TV Terrestre Digital , OFDM

§ DVB-H, DVB-S2, DVB sobre IP, etc.

# DVB-S



§ Transponder -> Portadora de Datos

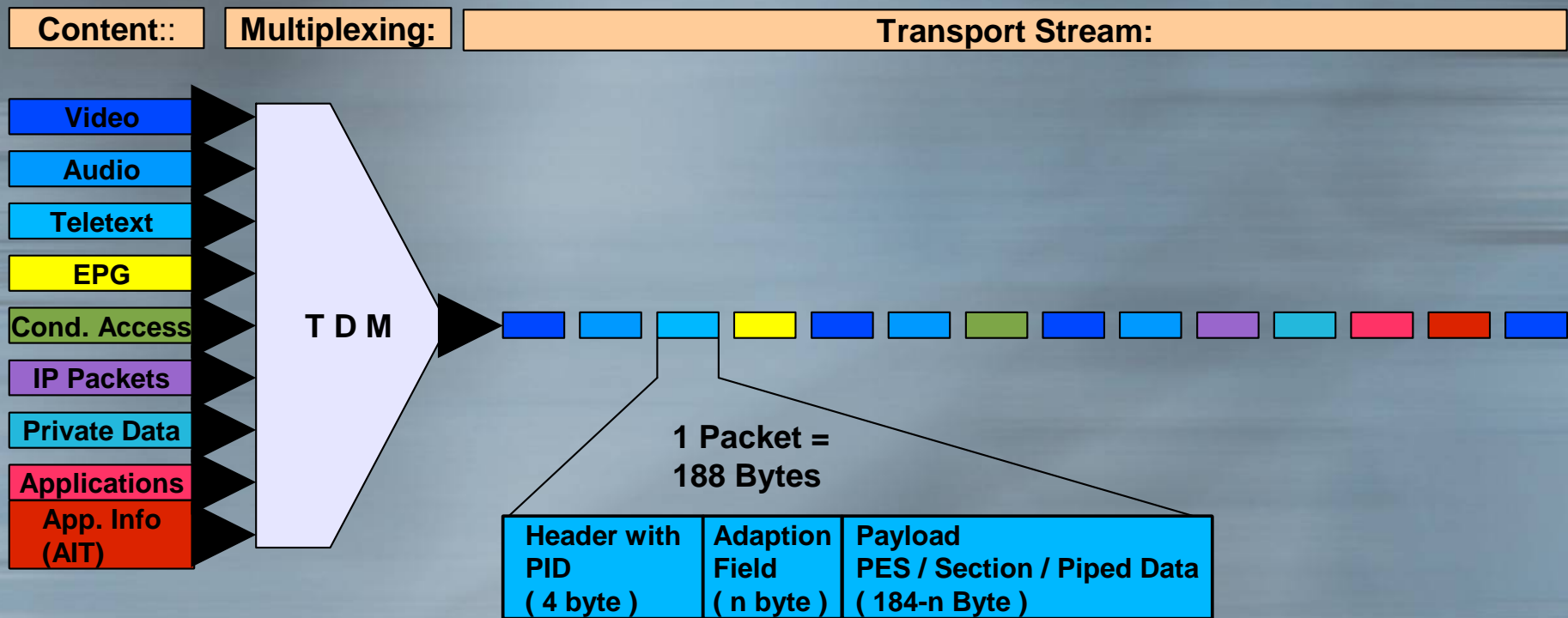
§ Frecuencia (banda C o Ku). Ej: 12.092 Ghz

§ Polarización. Vertical / Horizontal

§ Symbol Rate: Ej. 27500 Kbps

§ Tasa de FEC:  $\frac{3}{4}$ ,  $\frac{5}{6}$ , etc

# DVB-S



# DVB: TS (Transport Stream)



Header:

Body:



Header+Body = 188 bytes (184 Bytes de payload)

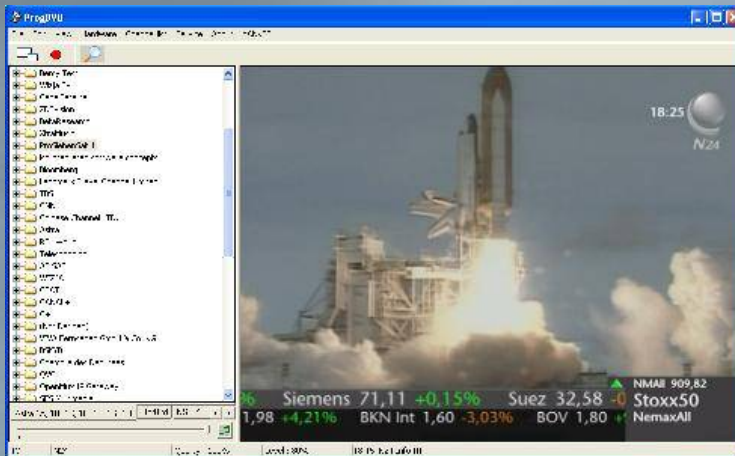
PID (Program ID): permite que varios programas sean multiplexados y distinguir entre sus componentes [Ej BBC1 PIDs: 600 (video), 601 (audio ingles), 603 (subtitulos), 4167 (teletexto)]

PIDs “Especiales”: NIT (Network Information Table), SDT (Service Description Table), PMT (Program Map Tables), PAT (Program Association Table).

# DVB-S Television

§ FTA (Free To Air)

§ Televisión de pago: Acceso condicional ,



**Software PC- SAT**



**Decodificador**

# DVB Televisión FTA



§ España: 24 Horas, Canal Internacional TVE, Telemadrid Satelite, ETB, Canales Senado y Congreso, etc.

§ Internacionales: CNN Intl, Sky News, CNBC, etc.

§ Futbol: Al Jazzera Sport (Nilesat)



# Acceso Condicional



**§ Decodificador**

**§ Decodificador + CAM + Tarjeta original abonado ;)**

**§ Tarjeta DVB**

**§ Software DVB + Plugin de Acceso + (Tarjeta )**

**§ Plugins: Yankse, S2EMU, Poor Man's CAM, etc**

**Es ilegal la visión de acceso condicional sin el correspondiente abono!**

# Televisión satélite en PC



§ **Tarjeta + PC + Salida TV = PVR**

§ **MPEG2 - > Divx (sin pasos analógicos)**

§ **Plugins de acceso condicional por software**

§ **Distribución en LAN (incluso Xbox)**

# DVB Feeds



- § Enlaces de transmisión de video.
- § Directos, eventos deportivos, imágenes sin editar, etc.
- § Temporales, solo se activan en el momento de la transmisión.
- § Normalmente en abierto (FTA)

# Feeds: Directos



**Feed Hispasat - Antena 3**

# Feeds: Directos



**Hispasat Feed Telecinco - FLY ATLAS - 20 Marzo 2004**

# Feeds: Agencias



**Hispasat – ATLAS Servicio Agencia – 29 Febrero 2004**

# Feeds: Varios



**Feeds Varios Hispasat**

# Feeds: OTAN

BBC NEWS | Programmes | Newsnight | Enthusiast watches Nato spy pictures - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

← Atrás → Búsqueda Favoritos Multimedia

Dirección <http://news.bbc.co.uk/1/hi/programmes/newsnight/2041754.stm>

BBC CATEGORIES TV RADIO COMMUNICATE WHERE I LIVE INDEX SEARCH  Go

## BBC NEWS

You are in: Programmes: Newsnight

News Front Page  
World  
UK  
England  
N Ireland  
Scotland  
Wales  
Politics  
Business  
Entertainment  
Science/Nature  
Technology  
Health  
Education  
Talking Point  
Country Profiles  
In Depth  
Programmes

### Newsnight

Thursday, 13 June, 2002, 00:28 GMT 01:28 UK

#### Enthusiast watches Nato spy pictures

By Mark Urban  
Newsnight's Diplomatic Editor

Nato surveillance flights in the Balkans are beaming their pictures over an insecure satellite link - and anyone can tune in and watch their operations live.

The discovery was made last November by John Locker, a satellite enthusiast in north west England.

He told Newsnight that he spent months e-mailing and faxing US and other Allied military officers to warn them of the dangers before finally deciding to go public.

Our investigation produced responses from Nato and American spokesmen



John Locker tried to alert

WATCH/LISTEN REAL MEDIA  
ON THIS STORY  
The BBC's Mark Urban  
"A serious threat to Nato continues"

### Newsnight

- Home
- Newsnight Review
- Latest programme
- Recent highlights
- About Newsnight
- Contact us

newsnight FORUM  
NATO security risk?

See also:

- 09 Mar 00 | Europe  
Nato spy 'leaked bombing secrets'
- 09 Mar 00 | Politics  
Nato spy revelations 'staggering'
- 23 Oct 01 | Americas  
Hacktivists take sides in war

Internet links:

- The Center for Public Integrity

The BBC is not responsible for the content of external

Listo Internet



# Feeds: OTAN



# Feeds



Hispasat 1C/1D at 30.0°W - LyngSat - Microsoft Internet Explorer

http://www.lyngsat.com/hispasat.html

11509 V tp B1	<a href="#">Retevisión</a>	A	DVB PowerVu	11000 - 3/4	1-100	Europe	R Toledano 040911
	(EFE feeds)			21 2160 2120			
	<a href="#">Net TV</a>	A	PowerVu	111 2260 2220 Sp			
11510 H tp B5	(feeds)		DVB	4444 - 3/4		Europe	8nce 040322
11521 H tp B6	(TSA feeds)		DVB	4500 - 3/4		Europe	FeedManiac 040302
11526 H tp B6	(TSA feeds)		DVB	4444 - 3/4		Europe	FeedManiac 040224
11533 H tp B6	(TSA feeds)		DVB	5632 - 3/4		Europe	8nce 040221
11535 V tp B1	<a href="#">Multicanal</a>	A	DVB Nagravision	24500 - 5/6	54-16		
	<a href="#">Canal Hollywood</a>	A	Nagravision	1 4132 4113 Sp 4113 P		Europe	W Zarembo 030730
	<a href="#">Odisea</a>	A	Nagravision	2 4160 4161 Sp 4161 P			
	<a href="#">Canal Panda</a>	A	Nagravision	3 4128 4129 P			
	<a href="#">Sol Música España</a>	A	Nagravision	4 4144 4145 Sp			
	<a href="#">Canal de Historia</a>	A	Nagravision	5 4176 4177 Sp 4177 P			
	<a href="#">Canal Hollywood Portugal</a>	A	Nagravision	7 4208 4209 P			
	<a href="#">Sol Música Portugal</a>	A T F		8 4192 4193 P			
11539 H tp B6	(TSA feeds)		DVB	3333 - 3/4		Europe	Reli 040908
11546 H tp B6	(Retevisión feeds)		DVB	4444 - 3/4		Europe	FeedManiac 040309
11551 H tp B6	(Retevisión feeds)		DVB	5632 - 3/4		Europe	James A 031221
11561 V tp B2	(feeds)		DVB	4500 - 3/4		Europe	Lytter 1 040312
11563 H tp B6	(feeds)		DVB	4500 - 3/4		Europe	FeedManiac 040309

Lyngsat

# Feeds Problemas de recepción



§ Lista de canales Vs “Blind Scan”

§ MPEG 4:2:2.

§ Bitrates Bajos

§ Nivel de señal reducido



# Para saber mas..

§ Dr HANS (Noticias: TV Pago, Feeds, etc)

§ <http://drhans.jinak.cz/news/index.php>

§ Zackyfiles (TV Pago, Foros)

§ <http://www.zackyfiles.info>

§ Feedlandia (Feeds)

§ <http://www.feedlandia.com>

# DVB Datos



## § DATAGRAMA DVB

§ DVB- MHP , etc.

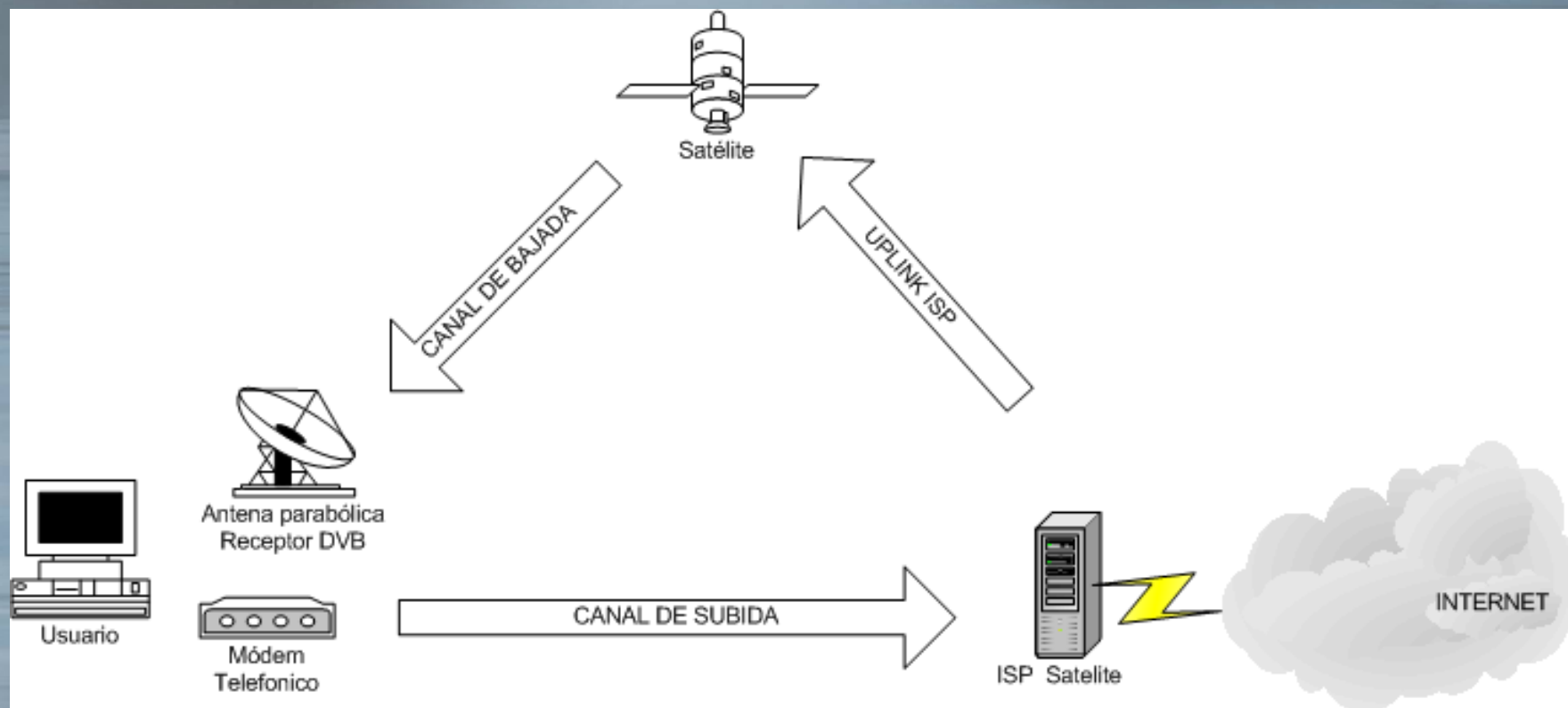
§ Datos propietarios

§ Encapsulado de IP

§ Encapsulado de Datos propietarios  
en IP sobre DVB

(Eumetsat, Casablanca, etc.)

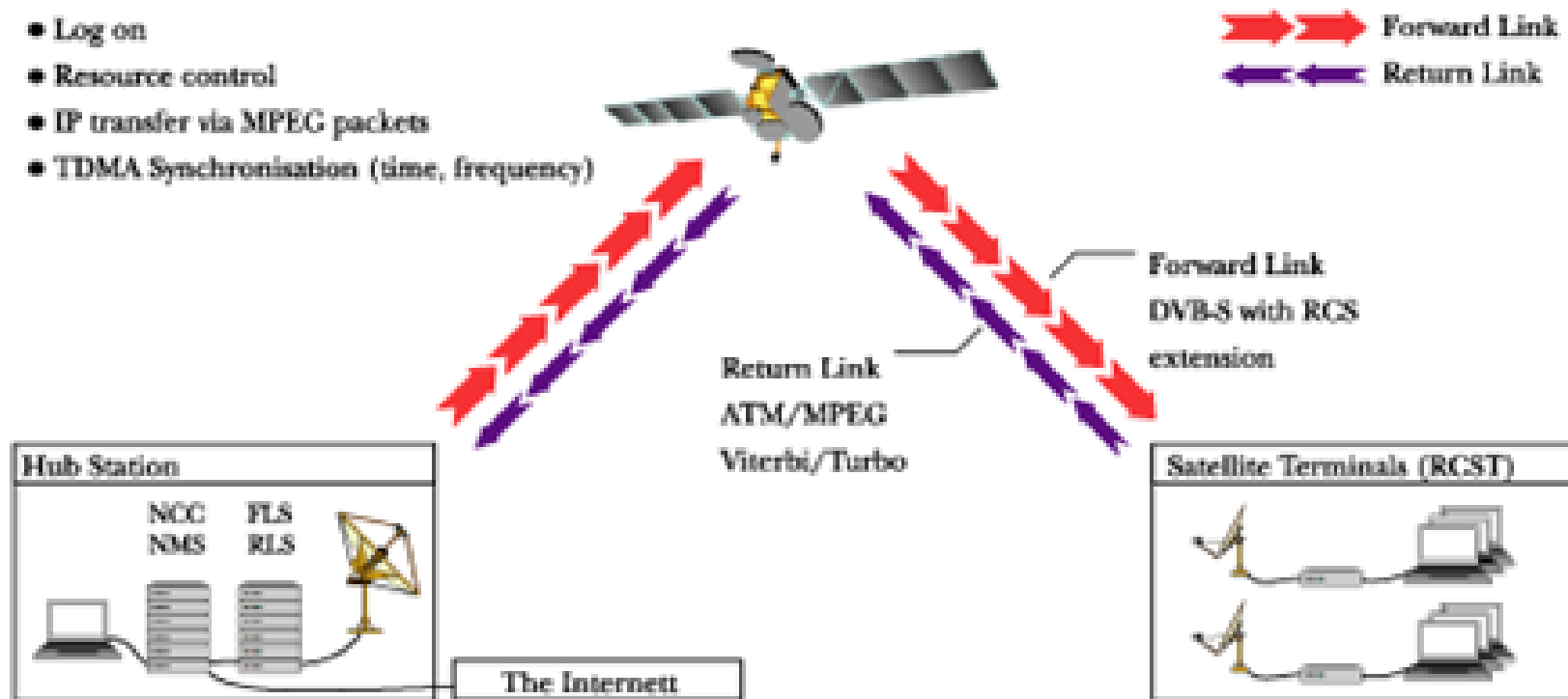
# DVB ISP Satellite



# DVB-RCS

## DVB-RCS

- Log on
- Resource control
- IP transfer via MPEG packets
- TDMA Synchronisation (time, frequency)



# DVB Datos



§ LinuxTV ([www.linuxtv.org](http://www.linuxtv.org))

§ Soporte en el kernel tarjetas DVB-S/C/T

§ Utilidades (linuxtv-apps): sintonizador, test, soporte DVB/IP, etc.

§ DVBSnoop ([dvbsnoop.sourceforge.net](http://dvbsnoop.sourceforge.net))

§ Analizador de protocolo DVB para consola

§ Para DVB/IP

§ Ethereal, Tcpdump, etc.



# DVB/IP: Tune



```
root@localhost:~/tmp/linuxtv-dvb-apps-1.1.0/util/szap
File Edit View Terminal Tabs Help
[root@localhost szap]# ./szap -c channels.conf-dvbs-astra ALICESAT
reading channels from file 'channels.conf-dvbs-astra'
zapping to 230 'ALICESAT':
sat 1, frequency = 11875 MHz H, symbolrate 27500000, vpid = 0x0123, apid = 0x0124
using '/dev/dvb/adapter0/frontend0' and '/dev/dvb/adapter0/demux0'
status 03 | signal b4f5 | snr b7cf | ber 00000154 | unc 00000000 |
status 1f | signal b392 | snr bb0b | ber 00000175 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b338 | snr ba39 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b458 | snr b99d | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b3bc | snr ba60 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b429 | snr bb02 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b518 | snr bc8b | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b3de | snr bbb6 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b416 | snr bbc8 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b5e8 | snr bcd3 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b63d | snr bc46 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b5f7 | snr bc46 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b43f | snr bc55 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b2d6 | snr bbf5 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b461 | snr bbaa | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b3bb | snr bc55 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b412 | snr bac9 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b6a9 | snr bab7 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
```

# Dvbsnoop: PID Scan

```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost root]# dvbsnoop -s pidscan  
dvbsnoop V1.3.35 -- http://dvbsnoop.sourceforge.net/  
  
-----  
Transponder PID-Scan...  
-----  
PID found:    0 (0x0000) [SECTION: Program Association Table (PAT)]  
PID found:   16 (0x0010) [SECTION: Network Information Table (NIT) - actual network]  
PID found:   17 (0x0011) [SECTION: Service Description Table (SDT) - actual transport stream]  
PID found: 1451 (0x05ab) [SECTION: DSM-CC - private data section // DVB datagram]  
PID found: 7451 (0x1d1b) [SECTION: Program Map Table (PMT)]  
[root@localhost root]#
```

# Dvbsnoop



```
root@localhost:tmp/linuxtv-dvb-apps-1.1.0/util/dvbnet
File Edit View Terminal Tabs Help
[root@localhost dvbnet]# dvbsnoop 17 -n 3 | more
dvbsnoop V1.3.35 -- http://dvbsnoop.sourceforge.net/

-----
SECT-Packet: 00000001  PID: 17 (0x0011), Length: 303 (0x012f)
Time received: Sat 2004-09-11 15:23:38.362
-----
0000: 42 f1 2c 04 f9 c5 00 00 00 01 ff 1d 1b fc 80 18 B.,.....
0010: 48 16 0c 09 4e 65 74 73 79 73 74 65 6d 0a 4e 65 H...Netsystem.Ne
0020: 74 20 73 79 73 20 30 31 1d 1c fc 80 16 48 14 0c t sys 01....H..
0030: 09 4e 65 74 73 79 73 74 65 6d 08 41 6c 69 63 65 .Netsystem.Alice
0040: 53 61 74 1d 1d fc 80 18 48 16 0c 09 4e 65 74 73 Sat....H...Nets
0050: 79 73 74 65 6d 0a 4e 65 74 20 73 79 73 20 30 33 ystem.Net sys 03
0060: 1d 1e fc 80 18 48 16 0c 09 4e 65 74 73 79 73 74 ....H...Netsyst
0070: 65 6d 0a 4e 65 74 20 73 79 73 20 30 34 1d 1f fc em.Net sys 04...
0080: 80 18 48 16 0c 09 4e 65 74 73 79 73 74 65 6d 0a ..H...Netsystem.
0090: 4e 65 74 20 73 79 73 20 30 35 1d 20 fc 80 18 48 Net sys 05. ...H
00a0: 16 0c 09 4e 65 74 73 79 73 74 65 6d 0a 4e 65 74 ...Netsystem.Net
00b0: 20 73 79 73 20 30 36 1d 21 fc 80 18 48 16 0c 09 sys 06.!...H...
00c0: 4e 65 74 73 79 73 74 65 6d 0a 4e 65 74 20 73 79 Netsystem.Net sy
00d0: 73 20 30 37 1d 22 fc 80 18 48 16 0c 09 4e 65 74 s 07."...H...Net
00e0: 73 79 73 74 65 6d 0a 4e 65 74 20 73 79 73 20 30 system.Net sys 0
00f0: 38 1d 23 fc 80 18 48 16 0c 09 4e 65 74 73 79 73 8.#...H...Netsys
0100: 74 65 6d 0a 4e 65 74 20 73 79 73 20 30 39 1d 24 tem.Net sys 09.$
0110: fc 80 18 48 16 0c 09 4e 65 74 73 79 73 74 65 6d ...H...Netsystem
0120: 0a 4e 65 74 20 73 79 73 20 31 30 e8 e9 ff 11 .Net sys 10....

PID: 17 (0x0011)
SDT-decoding....
--More--
```

# DVB-IP

```
root@localhost:/tmp/linuxtv-dvb-apps-1.1.0/util/dvbnet
File Edit View Terminal Tabs Help
[root@localhost dvbnet]# ./dvbnet -p 1451

DVB Network Interface Manager
Version 1.1.0-TVF (Build Fri Aug 06 12:16:12 PM 2004)
Copyright (C) 2003, TV Files S.p.A

Device: /dev/dvb/adapter0/net0
Status: device dvb0_0 for pid 1451 created successfully.
[root@localhost dvbnet]# ifconfig dvb0_0
dvb0_0    Link encap:Ethernet  HWaddr 00:00:00:00:00:00
          BROADCAST NOARP MULTICAST  MTU:4096  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Base address:0x5ab

[root@localhost dvbnet]# █
```

# DVB/IP



(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	130.88.193.193	172.30.25.135	TCP	1145 > 4625 [ACK] Seq=0 Ack=0 Win=65190 Len=1348 TSV=143
2	0.000108	66.28.205.175	172.30.9.118	HTTP	Continuation
3	0.000181	69.64.38.140	172.23.29.7	TCP	[TCP ZeroWindow] ircd > 51123 [RST] Seq=0 Ack=0 Win=0 Le
4	0.000253	151.37.23.144	172.30.49.116	TCP	6699 > 1263 [PSH, ACK] Seq=0 Ack=0 Win=65455 Len=498
5	0.000325	204.118.73.215	172.30.47.142	TCP	6699 > 1424 [ACK] Seq=0 Ack=0 Win=63952 Len=498
6	0.000400	216.231.124.243	172.23.29.4	HTTP	Continuation
7	0.000698	69.31.87.154	172.30.22.249	HTTP	Continuation
8	0.000770	213.19.160.190	172.30.16.28	HTTP	Continuation
9	0.000842	213.19.160.190	172.30.16.28	HTTP	Continuation
10	0.000916	212.177.107.133	172.30.14.143	HTTP	Continuation
11	0.001043	216.164.17.205	172.30.30.114	TCP	6699 > 3259 [ACK] Seq=0 Ack=0 Win=64174 Len=1360
12	0.001120	82.48.41.98	172.30.33.75	TCP	7041 > 1166 [ACK] Seq=0 Ack=0 Win=17271 Len=1348 TSV=575
13	0.001194	64.62.194.20	172.30.8.144	HTTP	Continuation
14	0.001313	82.52.59.27	172.30.18.225	TCP	6699 > 3480 [PSH, ACK] Seq=0 Ack=0 Win=64991 Len=160
15	0.001382	216.155.193.182	172.23.7.102	YMSG	YAHOO_SERVICE_CHATJOIN, YAHOO_STATUS_BRB
16	0.001450	68.142.233.20	172.23.28.87	TCP	5100 > 31599 [ACK] Seq=0 Ack=0 Win=27494 Len=0

▶ Frame 1 (1414 bytes on wire, 1414 bytes captured)

▶ Ethernet II, Src: 00:00:00:00:00:00, Dst: 00:d0:d7:30:79:b2

▶ Internet Protocol, Src Addr: 130.88.193.193 (130.88.193.193), Dst Addr: 172.30.25.135 (172.30.25.135)

▶ Transmission Control Protocol, Src Port: 1145 (1145), Dst Port: 4625 (4625), Seq: 0, Ack: 0, Len: 1348  
Data (1348 bytes)

```
0000 00 d0 d7 30 79 b2 00 00 00 00 08 00 45 00  ...0y... ..E.
0010 05 78 11 07 40 00 73 06 e7 b9 82 58 c1 c1 ac 1e  .x..@.s. ...X...
0020 19 87 04 79 12 11 eb 07 c5 af 52 a6 89 94 80 10  ...y.... ..R.....
0030 fe a6 f8 de 00 00 01 01 08 0a 00 da a6 ca 00 09  ....G.....
0040 be 7a 53 8a a2 72 8a 36 b9 00 47 df f0 56 0e 72  .zS..r.6 ..G..V.r
```

Filter:  + Expression...   File: (Untitled) 8092 KB P: 8808 D: 8808 M: 0

# DVB/IP



```
root@localhost:~  
File Edit View Terminal Tabs Help  
IPtraf  
- Statistics for dvb0_0 -  


|                  | Total<br>Packets | Total<br>Bytes | Incoming<br>Packets | Incoming<br>Bytes | Outgoing<br>Packets | Outgoing<br>Bytes |
|------------------|------------------|----------------|---------------------|-------------------|---------------------|-------------------|
| <b>Total:</b>    | <b>121026</b>    | <b>107992K</b> | <b>121026</b>       | <b>107992K</b>    | <b>0</b>            | <b>0</b>          |
| <b>IP:</b>       | <b>121026</b>    | <b>106228K</b> | <b>121026</b>       | <b>106228K</b>    | <b>0</b>            | <b>0</b>          |
| <b>TCP:</b>      | <b>117999</b>    | <b>105809K</b> | <b>117999</b>       | <b>105809K</b>    | <b>0</b>            | <b>0</b>          |
| <b>UDP:</b>      | <b>2838</b>      | <b>407748</b>  | <b>2838</b>         | <b>407748</b>     | <b>0</b>            | <b>0</b>          |
| <b>ICMP:</b>     | <b>189</b>       | <b>11227</b>   | <b>189</b>          | <b>11227</b>      | <b>0</b>            | <b>0</b>          |
| <b>Other IP:</b> | <b>0</b>         | <b>0</b>       | <b>0</b>            | <b>0</b>          | <b>0</b>            | <b>0</b>          |
| <b>Non-IP:</b>   | <b>0</b>         | <b>0</b>       | <b>0</b>            | <b>0</b>          | <b>0</b>            | <b>0</b>          |


|                        |                           |                            |          |
|------------------------|---------------------------|----------------------------|----------|
| <b>Total rates:</b>    | <b>23462.6 kbits/sec</b>  | <b>Broadcast packets:</b>  | <b>0</b> |
|                        | <b>3228.8 packets/sec</b> | <b>Broadcast bytes:</b>    | <b>0</b> |
| <b>Incoming rates:</b> | <b>23462.6 kbits/sec</b>  |                            |          |
|                        | <b>3228.8 packets/sec</b> |                            |          |
| <b>Outgoing rates:</b> | <b>0.0 kbits/sec</b>      | <b>IP checksum errors:</b> | <b>0</b> |
|                        | <b>0.0 packets/sec</b>    |                            |          |

  
- Elapsed time: 0:00 -  
X-exit
```

# DVB/IP: Driftnet



# DVB/IP: LIVE Inet Stream Filter

**LIVE Internet Stream Filter 9.03 (LiveINET903) by CBArts**

The FIRST live internet filter for the DVB-PC-CARD from TechnoTrend/Siemens ...  
The program uses the WorkShop-Interface from DVinGena (DVinGena@yahoo.de) for TT-DVB cards:  
For B2C2 (e.g. SkyStar2) cards the new B2C2-Interface from Marfi (marfi@bb.onet.pl) is used.

Language: Standard(English) (+)  
(Language:)

Use Card:  TT-DVB  B2C2 (SkyStar2)

Start DVB-Server Save config Remove config Information

Source-Box  
Providers: NetSystem119 Add Remove Edit

Provider: NetSystem119 Freq.: 12722000 kHz Pol.: H Symb.: 22000000  
DiSEqC: Off Options: n/a FEC: 5/6 PID: 451  
LOF settings Format: Normal Set Provider Cut-Val: B8

Stream-Box  
 Use MAC-Filter Start Streaming Stop Streaming  
MAC-Settings  
 Use support filter (TT 1.23b)

SpeedUp-Box  
 Don't update form display  
 Switch statusdisplay off

Directories/Output-Box  
Work-Directory: C:\LiveNet\Work\ Browse workdirectory  
Data-Out-Dir: C:\LiveNet\Out\ Browse outdirectory  
 Save Timeout-Files: C:\LiveNet\Inc\  
 Sort files into MAC-Directories (yout\????????????\...)  
 Write "yout\FileInfo.txt" (Informations about original filesizes, MACs, source-IPs, destination IPs...)  
 Write "yout\FileInfo.CSV" (same as above but in MSExcels CSV-format)

File-Box  
 Write files bigger than 64384 bytes  
 Write files smaller than 100000 bytes  
 Don't write files with unknown size  
 File-Timeout (global) min. 20 300 sec

Accept Filetypes:  
13  Unknown types  
93  text/html  
115  image/jpeg  
0  image/pipeg  
159  image/gif  
0  application/zip  
0  application/x-tar  
1  video/mpeg  
0  video/quicktime  
0  video/x-msvideo  
0  video/avi  
0  video/vnd.m-realvideo  
1  audio/mpeg  
0  audio/vnd.m-realaudio  
0  application/pdf  
ETC Select all Clear all

EXPERT-Box  
 Limit Filelist to x entries:  
x= 1000  
 Chksum off  
 Server kill off  
 Auto-WorkDir-Cleanup off  
 Use NetSys repair(only TTDVB)  
 Use debug Chksum

Status-Box  
Packets count/used/fail/lost: 5780/392/868(10)/4520  
HTTP Header defect: 13  
Filelist count: current/max: 157/x  
Files count/started/done/timeout/sizeerr: 276/157/119/0/0

Exit





# DVB Data: Análisis

```
root@localhost:/tmp/linuxtv-dvb-apps-1.1.0/test
File Edit View Terminal Tabs Help
ABCDEFGHIJKLMN
OPQRSTUVWXYZ
ABCDEFGHIJKLMN
OPQRSTUVWXYZ
DIGITAL+
Ingenier
a de Servicios de Valor A
adido - V
a Digital
11:47:44
Sep 1 2004
Versi
n %s Build %s %s %s
viadigital
908210134
mero de tel
fono %s, entorno de Producci
viapruebas
mero de tel
fono %s, entorno de Calidad
mero de tel
fono %s, entorno desconocido
Assert failed: result != AUTOLOAD_FAILED. File ../src/module.c, line 42.
Assert failed: current_handle != ILLEGAL_HANDLE. File ../src/module.c, line 75.
Assert failed: this->info.handle != MODULE_ILLEGAL_HANDLE. File ../src/module.c, line 80.
Assert failed: this -> info.data. File ../src/module.c, line 94.
Assert failed: current_handle != ILLEGAL_HANDLE. File ../src/module.c, line 108.
No es para el module
:
```

# DVB/IP Aplicación financiera

The screenshot displays the Wireshark interface with a list of captured packets. The selected packet (No. 11) is expanded to show its structure:

- Frame 11 (1381 bytes on wire, 1381 bytes captured)
- Ethernet II, Src: 00:00:00:00:00:00, Dst: 01:00:5e:48:48:01
- Internet Protocol, Src Addr: 10.16.200.128 (10.16.200.128), Dst Addr: 234.72.72.1 (234.72.72.1)
- User Datagram Protocol, Src Port: 4001 (4001), Dst Port: 4001 (4001)
- Data (1339 bytes)

The data section shows a hex dump and ASCII representation of the payload:

Offset	Hex	ASCII
0210	4c 2e 44 55 4e 49 50 41 50 45 4c 20 43 55 50 55	L.DUNIPA PEL CUPU
0220	4e 49 50 41 50 45 4c 20 43 55 50 53 2e 20 20 20	NIPAPEL CUPS.
0230	20 20 20 20 20 20 20 20 20 20 20 30 30 30	000
0240	30 30 30 30 2b 30 2a 03 93 14 02 78 48 44 44 2a	0000+0*...xHDD*
0250	30 30 34 30 36 30 39 32 30 34 30 32 30 45 53 30	00406092 04020ES0
0260	31 35 35 39 37 35 30 33 32 42 31 42 43 4e 30 f2	15597503 2B1BCNO.
0270	f2 30 f2 30 30 30 30 30 30 30 2a 03 c0 0c 02	.0.00000 000*....
0280	79 48 44 45 2a 33 30 34 30 39 31 39 31 34 34 38	uHDE*304 09191448
0290	34 34 43 4c 50 33 37 31 30 4d 31 30 39 30 56 30	44CLP371 0M1090V0
02a0	4d 43 4f 58 45 4f 43 20 45 4e 44 45 53 41 20 43	MCDXECC ENDESA C
02b0	48 49 4c 45 45 4e 44 45 53 41 20 43 48 49 4c 45	HILEENDE SA CHILE
02c0	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
02d0	20 20 30 30 30 30 30 30 30 2b 30 2a 03 0b 14 02	000000 0+0*....

At the bottom, the filter bar shows an empty filter and the status bar indicates "Data (data), 1339 bytes P: 68 D: 68 M: 0".

DVB



AB(USANDO) DVB

# Hidden Channels

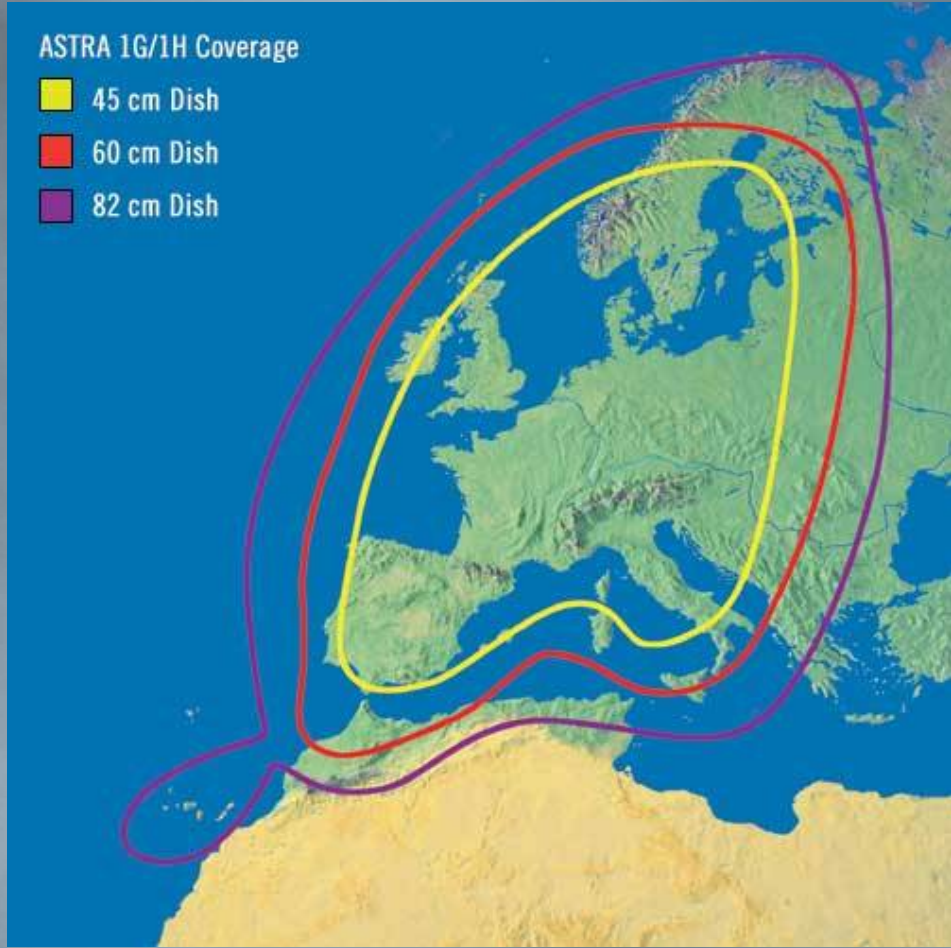


```
root@kali:~#  
[root@kali root]# hping 212.212.212.137 -E mensaje.txt --spoof 212.212.212.212 -d 17 -c 10  
HPING 212.212.212.137 (eth0 212.212.212.8.137): NO FLAGS are set, 40 headers + 17 data bytes  
  
--- 212.212.212.137 hping statistic ---  
10 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
[root@kali root]#
```

# Hidden Channels

```
root@localhost:/tmp/pak/src
File Edit View Terminal Tabs Help
[root@localhost src]# tcpdump -p -i dvb0_0 -A src 212.212.212.212 -c 3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on dvb0_0, link-type EN10MB (Ethernet), capture size 96 bytes
22:39:17.883129 IP 212.212.212.212.2400 > 212.██████████: . 109728130:10972814
7(17) win 512
E..9.Z..5.Z.....8..  `....Q.S2z.P.....
.
.....
22:39:18.877836 IP 212.212.212.212.cvspserver ██████████.137.0: . 1149380235:1
149380252(17) win 512
E..9r...5..r.....8..  a..D.&..D..P...'...TENEMOS UN IBERIA
22:39:19.880497 IP 212.212.212.212.2402 > 212.██████████.0: . 1471598608:1471598
625(17) win 512
E..95v..5.....8..  b..W...S.F.P...k...
.
.....
3 packets captured
21 packets received by filter
0 packets dropped by kernel
[root@localhost src]#
```

# Hidden Channels



# Escaneo de puertos anónimo

```
root@ [redacted] :-  
[root@ [redacted] root]# ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:08:02:[redacted]  
          inet addr:[redacted]  Bcast:[redacted]  Mask:255.255.255.252  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:641372 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:1421315 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:100  
          RX bytes:74467221 (71.0 Mb)  TX bytes:95332490 (90.9 Mb)  
          Interrupt:11  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:17761 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:17761 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:1567207 (1.4 Mb)  TX bytes:1567207 (1.4 Mb)  
  
[root@ [redacted] root]# scanrand www.nsa.gov -d eth0 -i 212.[redacted].137 -S -s hackthis  
[root@ [redacted] root]# █
```



# Escaneo de puertos anónimo

```
root@localhost:/tmp/pak/src
File Edit View Terminal Tabs Help
[root@localhost src]# ifconfig
dvb0_0  Link encap:Ethernet  HWaddr 00:40:11:11:11:11
        inet addr:212.111.111.137  Bcast:212.56.238.255  Mask:255.255.255.0
        inet6 addr: fe80::200:11:11:11:0/64 Scope:Link
        UP BROADCAST RUNNING NOARP MULTICAST  MTU:4096  Metric:1
        RX packets:143215 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:117475557 (112.0 Mb)  TX bytes:0 (0.0 b)
        Base address:0xc25

[root@localhost src]# ./scanrand -t0 -L -s hackthis
UP:  12.110.110.204:80    [17]  26.633s
UP:  12.110.110.204:443 [17]  26.634s
```

# Otras ideas



- § Echelon “Amateur”
- § ¿Conexión satélite anónima y gratuita?
- § Protocolo de envío de ficheros multicast.
- § “Offensive use of IDS”.
  - § Localización de “zombies”
  - § Escaneo pasivo de vulnerabilidades.  
Ej. Banner grabbing

Fin

Gracias!



¿Alguna pregunta?