

\$atellite Hacking for Fun & Pr0fit!

Adam Laurie

adam@algroup.co.uk

<http://rfidiot.org>

Who Am I?

- Open Source developer / researcher
 - Bluetooth
 - RFID
 - Full Disclosure / White Hat!
- Freelance research / training / lecturing

Why Now?

- Jim Geovedi & Raditya Iryandi
 - Hacking a Bird in The Sky
- Old Skewl
 - Started doing this in late 90's.
 - So, err... why did it take so long to publish?

Feed Hunting

- Look for 'interesting' satellite feeds
 - Scan all satellites
 - Scan all frequencies
 - Report on mailing lists / forums

Poking in the dark

Applications Places System

Feedhunter Rini - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.feedhunter.com/en/

satellite feed hunter dx

satellite feed hunter dx

Slashdot: News for nerds, st... Enigma Web Interface - Drea... satellite feed hunter dx - Go... Feedhunter Rini

Home My Bookmarks Testcards 1 Funny 1 News 1

Links Feedhunters Testcards 2 Funny 2 News 2

About Me Picture Series Testcards 3 Sport 1 My other Site

Guestbook Testcards 4 Sport 2 Email

Welcome to my Web site!
Here you can find several links to websites in which I'm interested.

Satellite-feed-forums

Satellite-sites

Rini Feedhunter

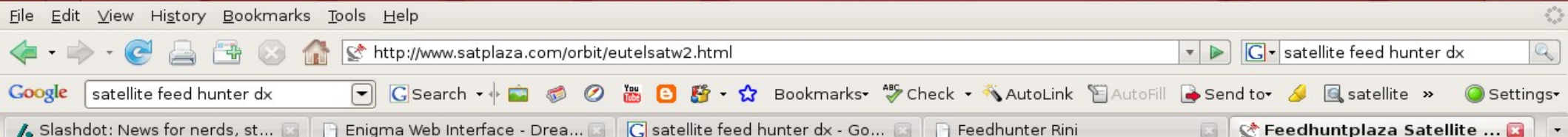
Sat-Benelux
Sat4fun
Sat4All
Satfeeds.eu
Feed Hunters Place
Chitchat
Sportfeeds
Satellite Tracker (info uitzendsatellieten)
Feedhuntplaza
Screenshots Feedhuntplaza
Satboard.nl
Feedhuntplaza
DXTV.de
DX-tv
King of Sat
Feed-Frequency
SatBox1All

BVD-sat
Worldwide webcam and Webcam TV
All digital sat-receivers
Online Satellite Calculations
Digi-television
Prog DVB
DVB-Dream
Flysat
Lyngsat
King of Sat
Satelliet-link-pagina
Satlinks-plaza
Football and other Sport on the Sat. 1
Football and other Sport on the Sat. 2
Football and other Sport on the Sat. 3
Football and other Sport on the Sat. 4
Football Live. 5
Free football on Sat 6

Done Tor Disabled

Feedhunter Rini - Mo... Starting Take Screen...

Poking in the dark



ENGLISH

FEED TRANSPONDERS

- 10.968 h 6400 3/4
- 10.976 h 5632 3/4
- 10.978 h 6400 3/4
- 10.989 h 6400 3/4
- 10.991 h 12800 7/8
- 10.997 h 5632 3/4
- 10.997 h 6400 3/4
- 10.997 v 6110 3/4
- 11.005 h 6400 3/4
- 11.008 h 5632 3/4
- 11.014 h 6400 3/4
- 11.016 h 3125 3/4
- 11.024 v 6110 3/4
- 11.043 h 4340 3/4
- 11.044 v 6400 3/4
- 11.051 h 5632 3/4

16 EAST - EUTELSAT W2

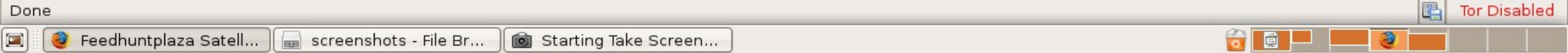
Date of Launch	05 - 10 - 1998
Launch Vehicle	Ariane 4 Flight 111
Time Of Life	approx. 12 year
Location	16 east
Inclined	no
Test Location	02 east
Graveyard Date	2010

Offering a total of twenty-four simultaneously-active transponders, the W2 satellite provides a fixed Widebeam coverage, spanning Europe, North Africa and the Middle East, and a Steerable coverage. Ten channels can be individually configured for operation via either of the two coverages. The remaining channels are connected to the Widebeam, which on the downlink is more concentrated than the Widebeam coverages of W1 and W3, offering enhanced capability for television and multimedia broadcasting. The Steerable coverage is positioned over the Indian Ocean for broadcasting digital television services to Mauritius and Reunion Island and includes a large part of south-eastern Africa.

At first the Eutelsat W2 satellite was called Eutelsat 3E2.

NEDERLANDS

FOOTPRINTS



Poking in the dark

The screenshot shows a Mozilla Firefox browser window with the address bar displaying `http://www.satplaza.com/feedhuntplaza/index.php/?cat=6`. The page title is "E 33 Eurobird 3 - Mozilla Firefox". The browser's address bar contains the text "satellite feed hunter dx". The page content includes a navigation menu with "Links" and "Screenshots" sections. The main content area features a "SATellite TRACKER" banner with the text "ALL INFORMATION ABOUT THE SATELLITES" and "POWERED BY FEEDHUNTPLAZA". Below the banner, the date "JULY 26TH, 2006" is displayed. The main article is titled "TV Spelletje" and contains the following text:

CHANNEL
Name: "RGS 2B" Provider: "Rosegarden"
TRANSPONDER
11185000, V, 8680000 QPSK
Satellite: 0330 - Eurobird 2
Signal Level:10% Quality:28%

IDs
NetworkID:1 TransponderID:2 SID:10
PIDs
Video:101 Audio:102 - dut PCR=101 PMT:100 Teletext:0
DATE/TIME
26-7-2006 11:26:54 (GMT +1)
REPORTER: Snuffer

Popularity: 6%

Posted by Snuffer as **E 33 Eurobird 3** at 11:27 AM PDT


No Comments »

The right sidebar contains a "Login/Register" section with a "Login" button and a "Satellites" section listing various satellite feeds:

- Algemeen / Main
- E 03 Telecom 2A
- E 04.8 Sirius 2
- E 05 Sirius 3
- E 05.2 Astra 1A
- E 07 Eutelsat W3A
- E 10 Eutelsat W1
- E 13 Hotbird
- E 16 Eutelsat W2
- E 19,2 Astra 1
- E 21.6 Eutelsat W6
- E 23.5 Astra 3A
- E 28.2 Astra 2
- E 28.5 Eurobird 1
- E 33 Eurobird 3
- E 36 Eutelsat sesat

The bottom of the browser window shows the taskbar with the system tray and the text "Tor Disabled".


Poking in the dark

Applications Places System  Wed 6 Feb, 9:53 AM 7 °C

» - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.satplaza.com/feedhuntplaza/index.php

Google Search  Bookmarks Check AutoLink AutoFill Send to satellite Settings


Slashdot: News for nerds, st... Enigma Web Interface - Drea... satellite feed hunter dx - Go... Feedhunter Rini

SATELLITE TRACKER POWERED BY FEEDHUNTPLAZA
ALL INFORMATION ABOUT THE SATELLITES

FEBRUARY 14TH, 2007

7 E wrestling ECW in USA

7.0°E 11044,V,6666 F106WSHT (TandbergTV) 4:2:2



Done Tor Disabled

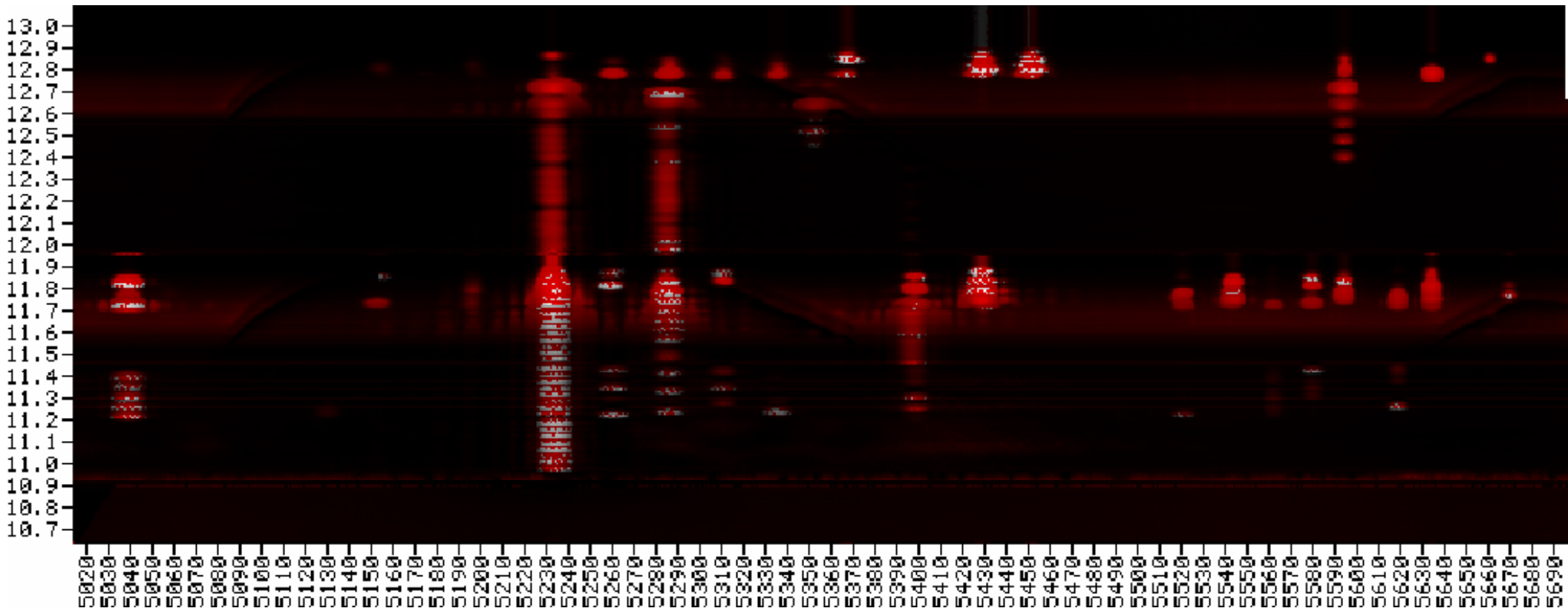
» - Mozilla Firefox screenshots - File Br... Starting Take Screen...

There must be a better way!

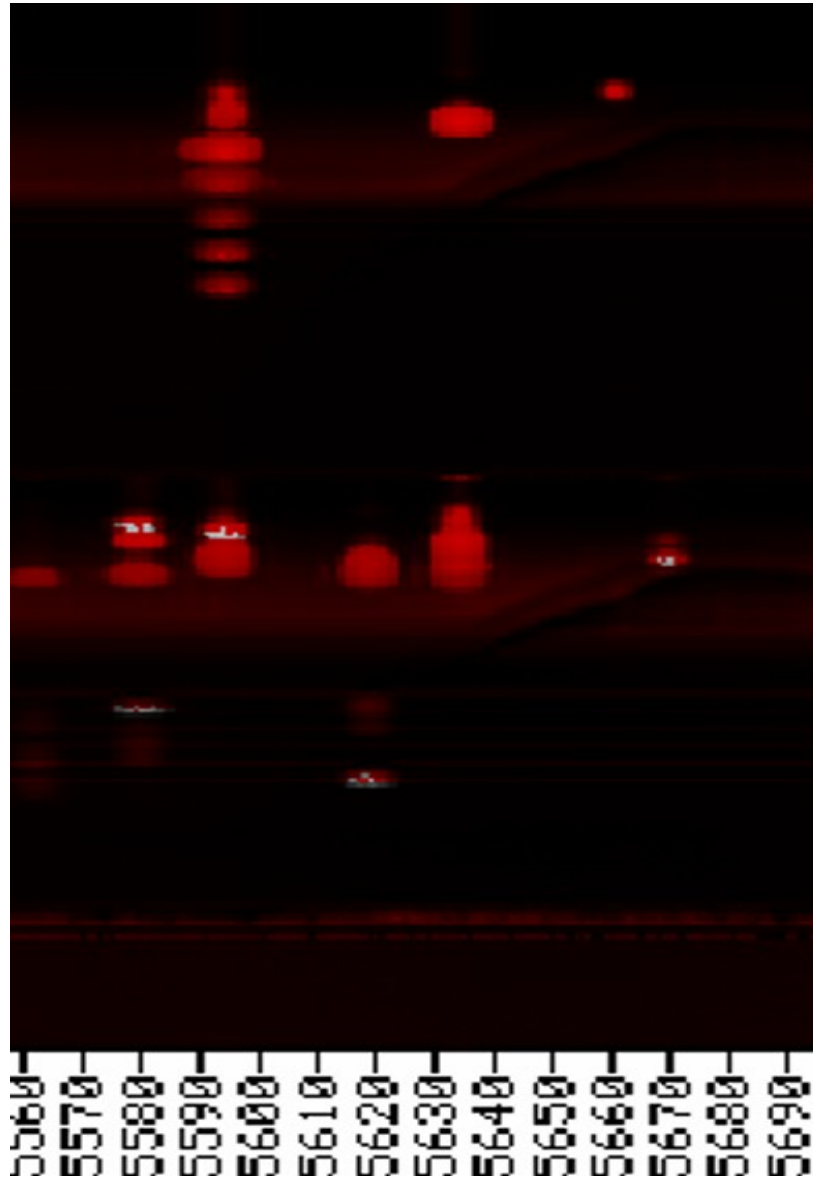
- Visualisation is your friend
 - Human Brain likes images
 - Recognise food
 - Recognise danger
 - Recognise friends
 - Recognise enemies

Visual Representations

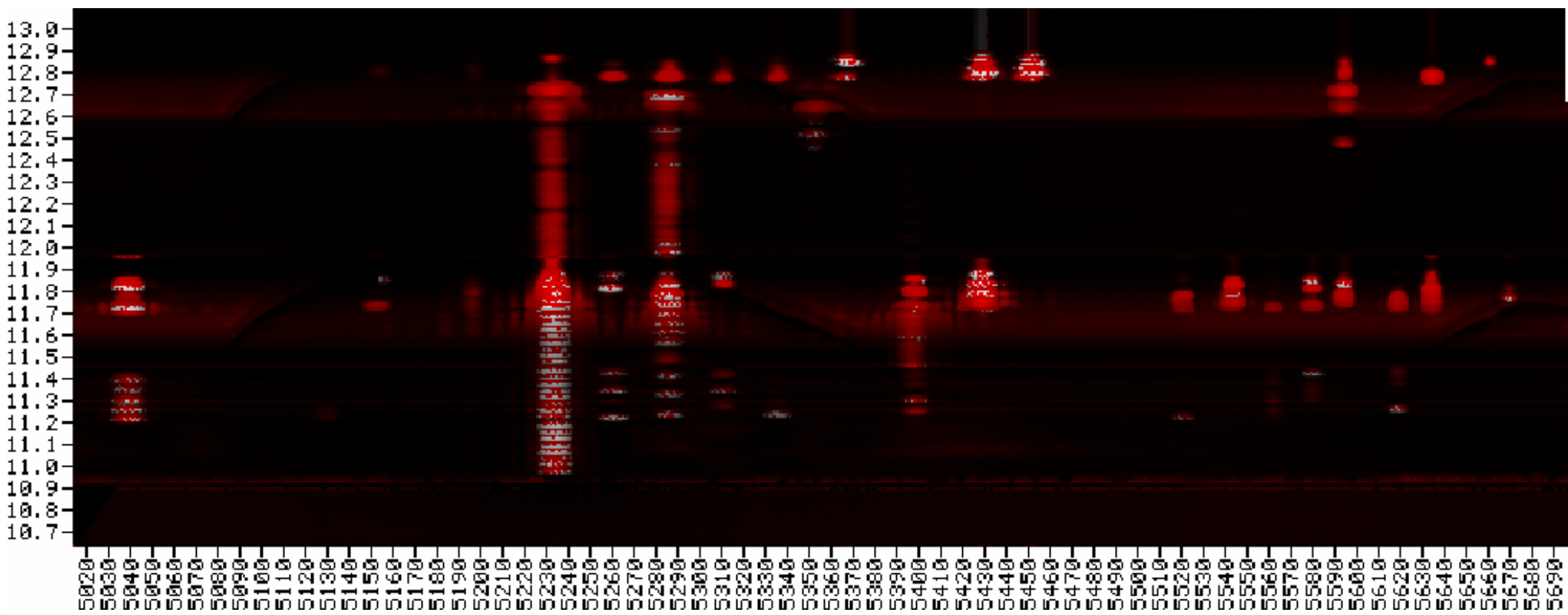
Visual Representations



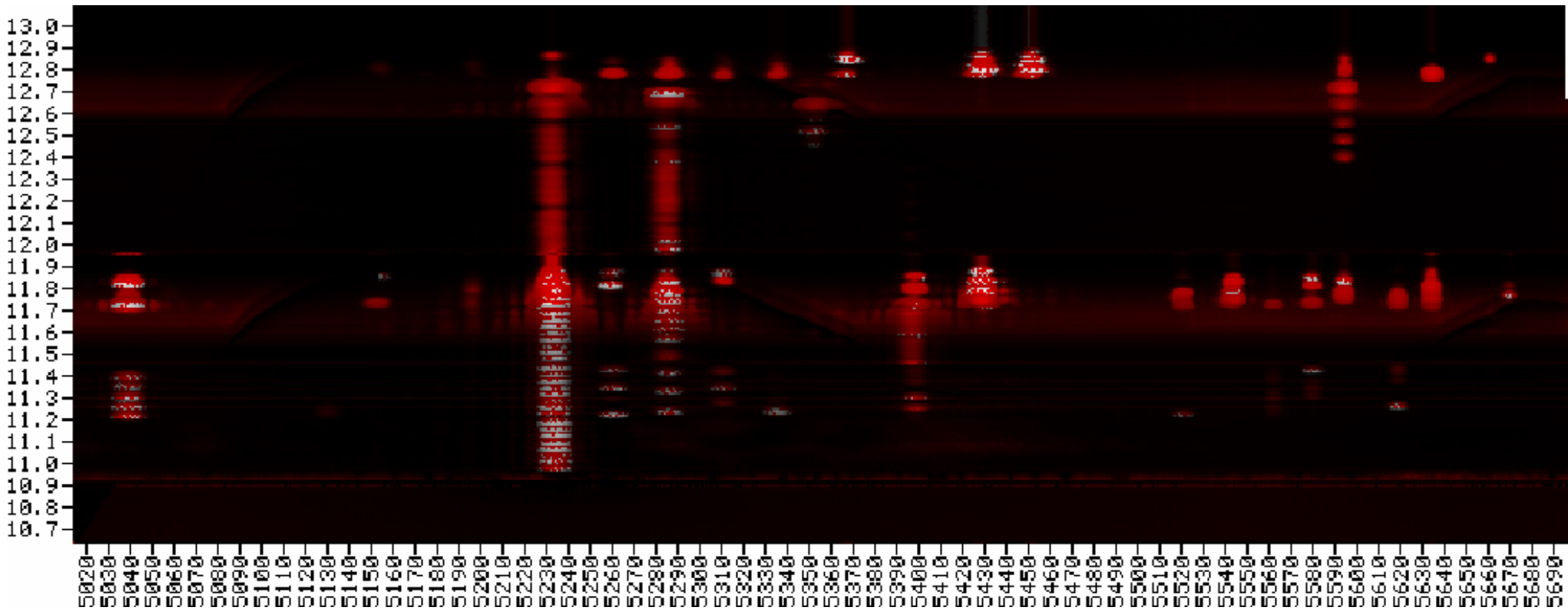
Visual Representations



Time travel – day 1



Time travel – day 2



That was then...

- Proprietary control systems
 - Undocumented
 - Reluctant manufacturers
 - Special hardware / interface converters
 - Motor Control
 - Signal Status
 - to RS232
 - Expensive receivers

This is now...

- Open standards
 - DVB Cards
 - Embedded Linux Receivers
 - Dreambox
 - Tuxbox based
 - GPL source code
 - Cross compilers
 - Alternative firmware
 - <http://www.i-have-a-dreambox.com>
 - <http://www.dream-multimedia-tv.de/>

This is now...

- Web Interface
 - Select programming
 - Steer dish
 - Examine feed properties

Web Interface

Applications Places System

Enigma Web Interface - Dreambox - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost:8888/?screenWidth=1280

Google

Slashdot: News for nerds, st... Enigma Web Interface - ...

100% Babes

DREAM
multimedia

SNR: 75% AGC: 89% BER: 26728 locked 223:21 h up 192.168.111.67 vpid: none apid: none

WEB-X-TV EPG Video Audio Info Stream Info VLC TEXT

0:00 n/a n/a

ZAP TIMERS CONTROL CONFIG HELP

ZAP: TV - Bouquets

TV Radio Data Movies Root Stream

All Services Satellites Providers Bouquets

Favourites (TV)
free
pr0n

- (0.0W) Premiere---Astra(19.2E)-----
- (0.0W) EASY.TV---Astra(19.2E)-----
- (0.0W) arena---Astra(19.2E)-----
- (0.0W) Premiere---Astra(23.5E)-----
- (0.0W) Hotbird---(13,0E)-----

Done Tor Disabled

Enigma Web Interfac... Starting Take Screen...

Stream Info

The screenshot shows a Linux desktop environment with a Mozilla Firefox browser window open. The browser window displays a page titled "Stream Information" for the URL "http://192.168.111.67". The page content is a table of stream parameters. The desktop background is a grid pattern. The system tray at the bottom shows the date and time as "Mon 4 Feb, 4:57 PM" and a temperature of "9 °C". The taskbar at the bottom contains several application icons, including "Enigma Web Interfac...", "http://192.168.111.6...", and "Starting Take Screen...".

Stream Information	
Service Name	Ladbrokes Blackjack
Service Provider	BSkyB
Service Reference	1:0:82:c754:96b:2:11c0000:0:0:0:
VPID	ffffffff (-1d)
APID	ffffffff (-1d)
PCRPID	ffffffff (-1d)
TPID	ffffffff (-1d)
TSID	096bh
ONID	0002h
SID	c754h
PMT	ffffffffh
Video Format	n/a
Namespace	11c0000h
Supported Crypto Systems	01xxh Seca/Mediaguard (Canal Plus), 05xxh Viaccess (France Telecom), 06xxh Irdeto, 0bxxh Conax (Norwegian Telekom), 17xxh Betacrypt (BetaTechnik), 18xxh Kudelski SA, 4a70h Dream Multimedia TV (DreamCrypt)
Used Crypto Systems	None
Satellite	orbit 284
Frequency	11661 MHz
Symbol Rate	27500 KSymbols/s
Polarisation	Horizontal
Inversion	No
FEC	2/3
SNR	93%
AGC	88%
BER	0
Lock	Yes
Sync	Yes

Stream Info

The screenshot shows a Linux desktop environment with a Mozilla Firefox browser window open. The browser window displays a page titled "Stream Information" for the URL "http://192.168.111.67". The page content is a table of stream parameters. The desktop background is a grid pattern. The taskbar at the bottom shows several open applications: "Enigma Web Interfac...", "http://192.168.111.6...", and "Starting Take Screen...". The system tray on the right shows the date and time as "Mon 4 Feb, 8:45 PM" and the temperature as "8 °C".

Stream Information	
Service Name	Data_01
Service Provider	OpenMux IP Gateway
Service Reference	1:0:c:22ca:238c:13e:820000:0:0:0:
VPID	ffffffff (-1d)
APID	ffffffff (-1d)
PCRPID	ffffffff (-1d)
TPID	ffffffff (-1d)
TSID	238ch
ONID	013eh
SID	22cah
PMT	ffffffffh
Video Format	n/a
Namespace	820000h
Supported Crypto Systems	01xxh Seca/Mediaguard (Canal Plus), 05xxh Viaccess (France Telecom), 06xxh Irdeto, 0bxxh Conax (Norwegian Telekom), 17xxh Betacrypt (BetaTechnik), 18xxh Kudelski SA, 4a70h Dream Multimedia TV (DreamCrypt)
Used Crypto Systems	None
Satellite	Hotbird (13.0E)
Frequency	12539 MHz
Symbol Rate	27500 KSymbols/s
Polarisation	Horizontal
Inversion	No
FEC	3/4
SNR	86%
AGC	88%
BER	0
Lock	Yes
Sync	Yes

You've got to know how to grab it...



Stream Info

- dvbsnoop - DVB and MPEG stream analyzer
 - “WireShark for DVB”
 - Access to raw data from DVB card
 - Decode known PIDs

<http://dvbsnoop.sourceforge.net>

Stream Info

```
Applications Places System [Icons] [System Tray] Mon 4 Feb, 4:49 PM 9 °C
File Edit View Terminal Tabs Help
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~> dvbsnoop -s signal -n 1
dvbsnoop V1.4.48 -- http://dvbsnoop.sourceforge.net/

-----
Transponder/Frequency signal strength statistics...
max cycle count: 1
-----
cycle: 1 d_time: 0.001 s Sig: 56961 SNR: 62049 BER: 0 UBLK: 0 Stat: 0x7b [SIG LOCK ]
root@dm7020:~>
```


Stream Info

```
-----
Transponder/Frequency signal strength statistics...
max cycle count: 1
-----
cycle: 1 d_time: 0.001 s Sig: 56961 SNR: 62049 BER: 0 UBLK: 0 Stat: 0x7b [SIG LOCK ]
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~> dvbsnoop -s pidscan
dvbsnoop V1.4.48 -- http://dvbsnoop.sourceforge.net/
-----
Transponder PID-Scan...
-----
PID found: 0 (0x0000) [SECTION: Program Association Table (PAT)]
PID found: 1 (0x0001) [SECTION: Conditional Access Table (CAT)]
PID found: 17 (0x0011) [SECTION: Service Description Table (SDT) - other transport stream]
PID found: 18 (0x0012) [SECTION: Event Information Table (EIT) - actual transport stream, present/following]
PID found: 52 (0x0034) [SECTION: User private]
PID found: 89 (0x0059) [SECTION: ATSC reserved]
PID found: 96 (0x0060) [SECTION: User private]
PID found: 192 (0x00c0) [SECTION: DVB CA message section (EMM/ECM)]
PID found: 261 (0x0105) [SECTION: Program Map Table (PMT)]
PID found: 262 (0x0106) [SECTION: Program Map Table (PMT)]
PID found: 263 (0x0107) [SECTION: Program Map Table (PMT)]
PID found: 264 (0x0108) [SECTION: Program Map Table (PMT)]
PID found: 265 (0x0109) [SECTION: Program Map Table (PMT)]
PID found: 266 (0x010a) [SECTION: Program Map Table (PMT)]
PID found: 270 (0x010e) [SECTION: Program Map Table (PMT)]
PID found: 271 (0x010f) [SECTION: Program Map Table (PMT)]
```

Stream Info

```
descriptor_length: 7 (0x07)
country_availability_flag: 1 (0x01)
reserved: 127 (0x7f)
  country_code: GBR
  country_code: IRL

DVB-DescriptorTag: 95 (0x5f) [= private_data_specifier_descriptor]
descriptor_length: 4 (0x04)
PrivateDataSpecifier: 2 (0x00000002) [= BskyB 1]

DVB-DescriptorTag: 72 (0x48) [= service_descriptor]
descriptor_length: 18 (0x12)
service_type: 134 (0x86) [= User defined]
service_provider_name_length: 5 (0x05)
service_provider_name: "BSkyB" -- Charset: Latin alphabet
service_name_length: 10 (0x0a)
Service_name: "History HD" -- Charset: Latin alphabet

DVB-DescriptorTag: 178 (0xb2) [= User defined]
descriptor_length: 142 (0x8e)
Descriptor-data:
0000: 1d 01 b1 7f 2a ab 57 18 41 6a b8 75 55 63 be e3 .....*.W.Aj.uUc..
0010: fc 35 71 82 92 b2 d5 c6 0d 3b 81 55 c6 0a 51 86 .5q.....;.U..Q.
0020: b3 5b 93 ac 7f a5 2a e3 05 28 f3 15 bf aa e3 08 .[.....*(.....
0030: 1d 57 18 22 e9 23 b5 d3 aa e3 08 7d 57 18 52 74 .W.".#.....}W.Rt
0040: 6d 57 18 1b c9 2f 85 8c 93 e6 da b8 c0 e0 35 5c mW.../.....5\
0050: 60 49 aa e3 04 1f d4 f7 8d af 80 7f e5 66 81 b8 `I.....f..
0060: 15 5c 60 a5 1e ab 8c 13 aa e3 08 d2 47 4d 5c 60 .\`.....GM\`
0070: b9 db 0b aa a1 55 78 fa 2f 55 c6 10 fa 1b 5a d2 .....Ux./U....Z.
0080: fd 57 18 34 6a b8 c1 3a ae 30 8d 24 7b 55 .W.4j....0.$U
```

Stream Info

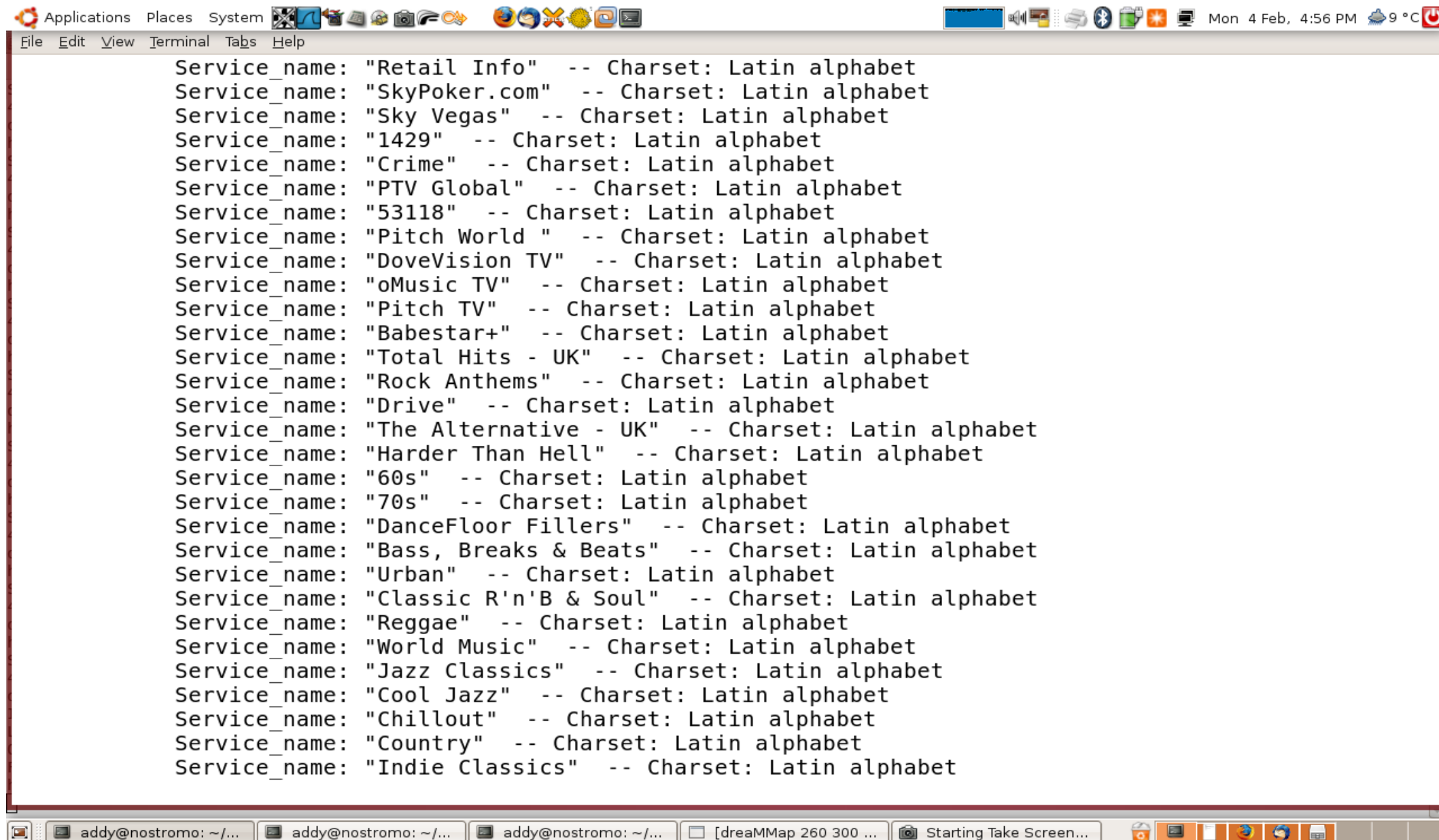
```
Event_ID: 21518 (0x540e)
Start_time: 0xd4e4170000 [= 2008-02-04 17:00:00 (UTC)]
Duration: 0x0002500 [= 00:25:00 (UTC)]
Running_status: 1 (0x01) [= not running]
Free_CA_mode: 0 (0x00) [= unscrambled]
Descriptors_loop_length: 395 (0x18b)

    DVB-DescriptorTag: 77 (0x4d) [= short_event_descriptor]
    descriptor_length: 154 (0x9a)
    ISO639_2_language_code: eng
    event_name_length: 9 (0x09)
    event_name: "<EM>MI High</EM>" -- Charset: Latin alphabet
    text_length: 140 (0x8c)
    text_char: "CBBC. Face Off: The team tackle a child crime-wave committed by allegedly well-beh
are baffled when Lenny is arrested too. [S]" -- Charset: Latin alphabet

    DVB-DescriptorTag: 80 (0x50) [= component_descriptor]
    descriptor_length: 11 (0x0b)
    reserved: 15 (0x0f)
    stream_content: 15 (0x0f)
    component_type: 5 (0x05)
    == Content&Component: (= user defined)
    component_tag: 255 (0xff)
    ISO639_language_code:
    component-description: "ETV 2" -- Charset: Latin alphabet

    DVB-DescriptorTag: 80 (0x50) [= component_descriptor]
    descriptor_length: 11 (0x0b)
    reserved: 15 (0x0f)
```

Stream Info



The image shows a terminal window with a list of service names and their character sets. The window title is "Applications Places System" and the menu bar includes "File Edit View Terminal Tabs Help". The system tray shows the date "Mon 4 Feb, 4:56 PM" and the temperature "9 °C". The terminal output is as follows:

```
Service_name: "Retail Info" -- Charset: Latin alphabet
Service_name: "SkyPoker.com" -- Charset: Latin alphabet
Service_name: "Sky Vegas" -- Charset: Latin alphabet
Service_name: "1429" -- Charset: Latin alphabet
Service_name: "Crime" -- Charset: Latin alphabet
Service_name: "PTV Global" -- Charset: Latin alphabet
Service_name: "53118" -- Charset: Latin alphabet
Service_name: "Pitch World " -- Charset: Latin alphabet
Service_name: "DoveVision TV" -- Charset: Latin alphabet
Service_name: "oMusic TV" -- Charset: Latin alphabet
Service_name: "Pitch TV" -- Charset: Latin alphabet
Service_name: "Babestar+" -- Charset: Latin alphabet
Service_name: "Total Hits - UK" -- Charset: Latin alphabet
Service_name: "Rock Anthems" -- Charset: Latin alphabet
Service_name: "Drive" -- Charset: Latin alphabet
Service_name: "The Alternative - UK" -- Charset: Latin alphabet
Service_name: "Harder Than Hell" -- Charset: Latin alphabet
Service_name: "60s" -- Charset: Latin alphabet
Service_name: "70s" -- Charset: Latin alphabet
Service_name: "DanceFloor Fillers" -- Charset: Latin alphabet
Service_name: "Bass, Breaks & Beats" -- Charset: Latin alphabet
Service_name: "Urban" -- Charset: Latin alphabet
Service_name: "Classic R'n'B & Soul" -- Charset: Latin alphabet
Service_name: "Reggae" -- Charset: Latin alphabet
Service_name: "World Music" -- Charset: Latin alphabet
Service_name: "Jazz Classics" -- Charset: Latin alphabet
Service_name: "Cool Jazz" -- Charset: Latin alphabet
Service_name: "Chillout" -- Charset: Latin alphabet
Service_name: "Country" -- Charset: Latin alphabet
Service_name: "Indie Classics" -- Charset: Latin alphabet
```

The terminal window also shows a taskbar at the bottom with several open windows: "addy@nostromo: ~/...", "[dreaMMap 260 300 ...", and "Starting Take Screen...".

Stream Info

```
Applications Places System [System Icons] [Network Icons] [System Icons] Mon 4 Feb, 5:18 PM 9 °C
File Edit View Terminal Tabs Help
PID found: 160 (0x00a0) [PS/PES: ITU-T Rec. H.262 | ISO/IEC 13818-2 or ISO/IEC 11172-2 video stream]
PID found: 161 (0x00a1) [PS/PES: ISO/IEC 13818-3 or ISO/IEC 11172-3 audio stream]
PID found: 176 (0x00b0) [PS/PES: ITU-T Rec. H.262 | ISO/IEC 13818-2 or ISO/IEC 11172-2 video stream]
PID found: 177 (0x00b1) [PS/PES: ISO/IEC 13818-3 or ISO/IEC 11172-3 audio stream]
PID found: 191 (0x00bf) [unknown]
PID found: 192 (0x00c0) [PS/PES: ITU-T Rec. H.262 | ISO/IEC 13818-2 or ISO/IEC 11172-2 video stream]
PID found: 193 (0x00c1) [PS/PES: ISO/IEC 13818-3 or ISO/IEC 11172-3 audio stream]
PID found: 194 (0x00c2) [PS/PES: ISO/IEC 13818-3 or ISO/IEC 11172-3 audio stream]
PID found: 208 (0x00d0) [PS/PES: ITU-T Rec. H.262 | ISO/IEC 13818-2 or ISO/IEC 11172-2 video stream]
PID found: 209 (0x00d1) [PS/PES: ISO/IEC 13818-3 or ISO/IEC 11172-3 audio stream]
PID found: 211 (0x00d3) [SECTION: DSM-CC - private data section // DVB datagram]
PID found: 223 (0x00df) [unknown]
PID found: 224 (0x00e0) [PS/PES: ITU-T Rec. H.262 | ISO/IEC 13818-2 or ISO/IEC 11172-2 video stream]
PID found: 225 (0x00e1) [PS/PES: ISO/IEC 13818-3 or ISO/IEC 11172-3 audio stream]
PID found: 239 (0x00ef) [unknown]
PID found: 240 (0x00f0) [PS/PES: ITU-T Rec. H.262 | ISO/IEC 13818-2 or ISO/IEC 11172-2 video stream]
PID found: 241 (0x00f1) [PS/PES: ISO/IEC 13818-3 or ISO/IEC 11172-3 audio stream]
PID found: 257 (0x0101) [PS/PES: ISO/IEC 13818-3 or ISO/IEC 11172-3 audio stream]
PID found: 258 (0x0102) [PS/PES: ISO/IEC 13818-3 or ISO/IEC 11172-3 audio stream]
PID found: 259 (0x0103) [PS/PES: ISO/IEC 13818-3 or ISO/IEC 11172-3 audio stream]
PID found: 260 (0x0104) [PS/PES: ISO/IEC 13818-3 or ISO/IEC 11172-3 audio stream]
PID found: 272 (0x0110) [PS/PES: ITU-T Rec. H.262 | ISO/IEC 13818-2 or ISO/IEC 11172-2 video stream]
PID found: 273 (0x0111) [PS/PES: ISO/IEC 13818-3 or ISO/IEC 11172-3 audio stream]
PID found: 288 (0x0120) [PS/PES: ITU-T Rec. H.262 | ISO/IEC 13818-2 or ISO/IEC 11172-2 video stream]
PID found: 289 (0x0121) [PS/PES: ISO/IEC 13818-3 or ISO/IEC 11172-3 audio stream]
PID found: 304 (0x0130) [PS/PES: ITU-T Rec. H.262 | ISO/IEC 13818-2 or ISO/IEC 11172-2 video stream]
PID found: 305 (0x0131) [PS/PES: ISO/IEC 13818-3 or ISO/IEC 11172-3 audio stream]
PID found: 320 (0x0140) [PS/PES: ITU-T Rec. H.262 | ISO/IEC 13818-2 or ISO/IEC 11172-2 video stream]
PID found: 321 (0x0141) [PS/PES: ISO/IEC 13818-3 or ISO/IEC 11172-3 audio stream]
root@dm7020:~>
```

Stream Info

```
Applications Places System
File Edit View Terminal Tabs Help
Section_length: 1513 (0x05e9)
MACaddrbyte/DeviceID 6: 24 (0x18)
MACaddrbyte/DeviceID 5: 127 (0x7f)
reserved_2: 3 (0x03)
payload_scrambling_control: 0 (0x00) [= unscrambled]
address_scrambling_control: 0 (0x00) [= unscrambled]
LLC_SNAP_flag: 0 (0x00)
current_next_indicator: 1 (0x01) [= valid now]
Section_number: 0 (0x00)
Last_Section_number: 0 (0x00)
MACaddrbyte/DeviceID 4: 64 (0x40)
MACaddrbyte/DeviceID 3: 94 (0x5e)
MACaddrbyte/DeviceID 2: 0 (0x00)
MACaddrbyte/DeviceID 1: 1 (0x01) => MAC-Address/DeviceID: 01:00:5e:40:7f:18

IP_datagram_bytes:
  Version: 4 (0x04)
  IP header length: 5 (0x05)
  Type of service: 0 (0x00)
  Total length: 1500 (0x05dc)
  Identification: 6070 (0x17b6)
  Reserved: 0 (0x00)
  DF: 0 (0x00)
  MF: 1 (0x01)
  Fragment offset: 185 (0x00b9)
  Time to live: 7 (0x07)
  Protocol: 17 (0x11) [= UDP]
  Header checksum: 61042 (0xee72)
  Source address: 0a290e2e [= 10.41.14.46]
  Destination address: efc07f18 [= 239.192.127.24]
--More--

addy@nostromo: ~/... [addy@nostromo: ~/... addy@nostromo: ~/... Starting Take Screen...
```

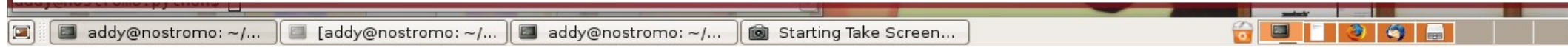
Stream Info



```
IP_datagram_bytes:
  Version: 4 (0x04)
  IP header length: 5 (0x05)
  Type of service: 0 (0x00)
  Total length: 1500 (0x05dc)
  Identification: 6070 (0x17b6)
  Reserved: 0 (0x00)
  DF: 0 (0x00)
  MF: 1 (0x01)
  Fragment offset: 185 (0x00b9)
  Time to live: 7 (0x07)
  Protocol: 17 (0x11) [= UDP]
  Header checksum: 61042 (0xee72)
  Source address: 0a290e2e [= 10.41.14.46]
  Destination address: efc07f18 [= 239.192.127.24]

UDP_datagram:
  Source port: 14299 (0x37db)
  Destination port: 59913 (0xea09)
  Length: 37795 (0x93a3)
  Checksum: 30137 (0x75b9)
  Data
    0000:  a4 33 82 05 92 f8 eb ca  8c 79 e8 16 b6 fd a9 b6  .3.....y.....
    0010:  9f 6f a0 7a 5b ca bc c5  b5 17 cb 8a 5a 29 b4 a2  .o.z[.....Z)..
    0020:  17 fe df cf a1 a7 2a 0d  aa 3a 1c e6 34 9a b7 a9  .....*.....4...
    0030:  b9 5f 48 5e 95 84 5b f4  2f d1 b4 0c 45 68 2a 56  ._H^..[./...Eh*V
    0040:  75 20 14 f5 08 44 10 57  c1 2d 96 b3 9d fa 1f 3b  u ...D.W.-.....;
    0050:  8c ff 10 5a c5 7b a8 64  13 95 f8 b4 05 e6 61 34  ...Z.{.d.....a4
    0060:  a6 f6 f1 84 71 4d 97 1a  1a cc be ad b0 50 eb 38  ....qM.....P.8

--More--
```



Stream Info

```
Applications Places System [system tray icons] Mon 4 Feb, 8:35 PM 8 °C
addy@nstromo: ~/work/suppose-addy-talks/research/dreambox/python
File Edit View Terminal Tabs Help
reserved_2: 0 (0x00)
payload_scrambling_control: 0 (0x00) [= unscrambled]
address_scrambling_control: 0 (0x00) [= unscrambled]
LLC_SNAP_flag: 0 (0x00)
current_next_indicator: 1 (0x01) [= valid now]
Section_number: 0 (0x00)
Last_Section_number: 0 (0x00)
MACaddrbyte/DeviceID 4: 224 (0xe0)
MACaddrbyte/DeviceID 3: 0 (0x00)
MACaddrbyte/DeviceID 2: 0 (0x00)
MACaddrbyte/DeviceID 1: 0 (0x00) => MAC-Address/DeviceID: 00:00:00:e0:00:00

IP_datagram_bytes:
  Version: 0 (0x00)
  Unknown Data / Padding
    0000: 00 15 0a 59 01 00 0e 01 08 58 63 6f 6d 44 77 6e ...Y.....XcomDwn
    0010: 4c 02 02 23 8a 00 00 00 6e 01 11 00 00 51 c1 08 L..#....n....Q..
    0020: 0a 58 0a 58 0a 58 00 01 00 00 00 00 00 23 00 11 .X.X.X.....#..
    0030: 44 53 38 31 30 58 45 5f 31 2e 34 30 38 2e 32 2e DS810XE_1.408.2.
    0040: 31 00 1c 00 16 88 b8 05 0a 00 01 44 0a 00 01 25 1.....D...%
    0050: 0b 00 00 44 0a 00 01 00 0b 00 00 29 0c 00 23 00 ...D.....)..#.
    0060: 24 01 04 00 00 00 01 02 16 01 00 00 12 52 65 63 $......Rec
    0070: 6f 6d 6d 65 6e 64 65 64 20 55 70 64 61 74 65 03 ommended Update.
    0080: 04 9f 00 00 14 00 00 .....

CRC: 3040108318 (0xb5345f1e)
=====
-----
addy@nstromo: ~/... addy@nstromo: ~/... Starting Take Screen...
```


Taking over the Dreambox

- Avoid programming
 - Analyse config files
 - Tools to tweak and update
 - Use existing Web Interface URLs
 - Use remote tools via IP
 - ssh / scp
 - dvbsnoop
 - tun/tap

Taking over the Dreambox

The screenshot shows a Mozilla Firefox browser window displaying the Enigma Web Interface. The address bar shows the URL `http://localhost:8888/?screenWidth=1280`. The page title is "Enigma Web Interface - Dreambox - Mozilla Firefox". The browser's search bar contains "satellite feed hunter dx".

The main content area displays the "Enigma Web Interface" logo and a status bar with the following information: SNR: 92% AGC: 87% BER: 0 locked 224:07 h up 192.168.111.67 vpid: none apid: none. Below the status bar are navigation tabs: WEB-X-TV, EPG, Video, Audio, Info, Stream Info, VLC, and TEXT. A media player interface shows a progress bar at 0:00 and playback controls. Below the media player are tabs for ZAP, TIMERS, CONTROL, CONFIG, and HELP.

The "ZAP: TV - Satellites" section is active, showing a list of satellite services and providers. The list is organized into columns: All Services, Satellites, Providers, and Bouquets. The "Satellites" column lists various satellite services, including Astra (19.2E) - new found, Astra (19.2E) - services, Astra/Eurobird (28.2E) - services, Astra/Eurobird (28.2E) - services, Eutelsat W2 (16.0E) - new found, Eutelsat W2 (16.0E) - services, Hotbird (13.0E) - new found, Hotbird (13.0E) - services, and current transponder. The "Providers" column lists various providers, including (19.2E) AXN (a/P), (19.2E) AbsolutSexy.TV, (19.2E) Alpenglühn TVX, (19.2E) BABY FIRST, (19.2E) BELSAT TV, (19.2E) BOOMERANG (a/P), (19.2E) BiB, (19.2E) Biography Channel, (19.2E) CANAL CLUB, (19.2E) CANAL EVENEMENT, (19.2E) CANAL+ FAMILY, (19.2E) CARACOL TV, (19.2E) CE SOIR, (19.2E) CINE FX, (19.2E) DISNEY MAGIC HD, (19.2E) DISNEY PLAYHOUSE (P), (19.2E) DISNEY TOON (P), (19.2E) E.CLIPS (P), (19.2E) ECUAVISA INT, and (19.2E) ENCYCLOPEDIA.

The browser's taskbar at the bottom shows the system tray with the date and time "Wed 6 Feb, 9:59 AM" and a temperature of "7 °C". The system tray also includes icons for Applications, Places, System, and various system utilities. The browser's status bar at the bottom shows "Done" and "Tor Disabled".

Taking over the Dreambox

Applications Places System Wed 6 Feb, 8:32 AM 0°F

Enigma Web Interface - Dreambox - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost:8888/?screenWidth=1280

Google

Slashdot: News for nerds, st... Enigma Web Interface - ...

100% Babes

SNR: 77% AGC: 86% BER: 5140 locked 223:20 h up 192.168.111.67 vpid: none apid: none

WEB-X-TV EPG Video Audio Info Stream Info VLC TEXT

0:00 n/a n/a

ZAP TIMERS CONTROL CONFIG HELP

CONTROL: Satfinder

Shutdown	orbit 260	10770 / 22000 / H
Restart	orbit 261	10770 / 22000 / V
Reboot	orbit 262	10771 / 22000 / H
Standby	orbit 263	10771 / 22000 / V
Wakeup	orbit 264	10772 / 22000 / H
OSDshot	orbit 265	10772 / 22000 / V
LCDshot	orbit 266	10773 / 22000 / H
Screenshot	orbit 267	10773 / 22000 / V
Message	orbit 268	10774 / 22000 / H
Satfinder	orbit 269	10774 / 22000 / V
Remote Control	orbit 270	10775 / 22000 / H
	orbit 271	10775 / 22000 / V
	orbit 272	10776 / 22000 / H
	orbit 273	10776 / 22000 / V
	orbit 274	10777 / 22000 / H
	orbit 275	10777 / 22000 / V
	orbit 276	10778 / 22000 / H
	orbit 277	10778 / 22000 / V
	orbit 278	10779 / 22000 / H
	orbit 279	10779 / 22000 / V
	orbit 280	10780 / 22000 / H

Done

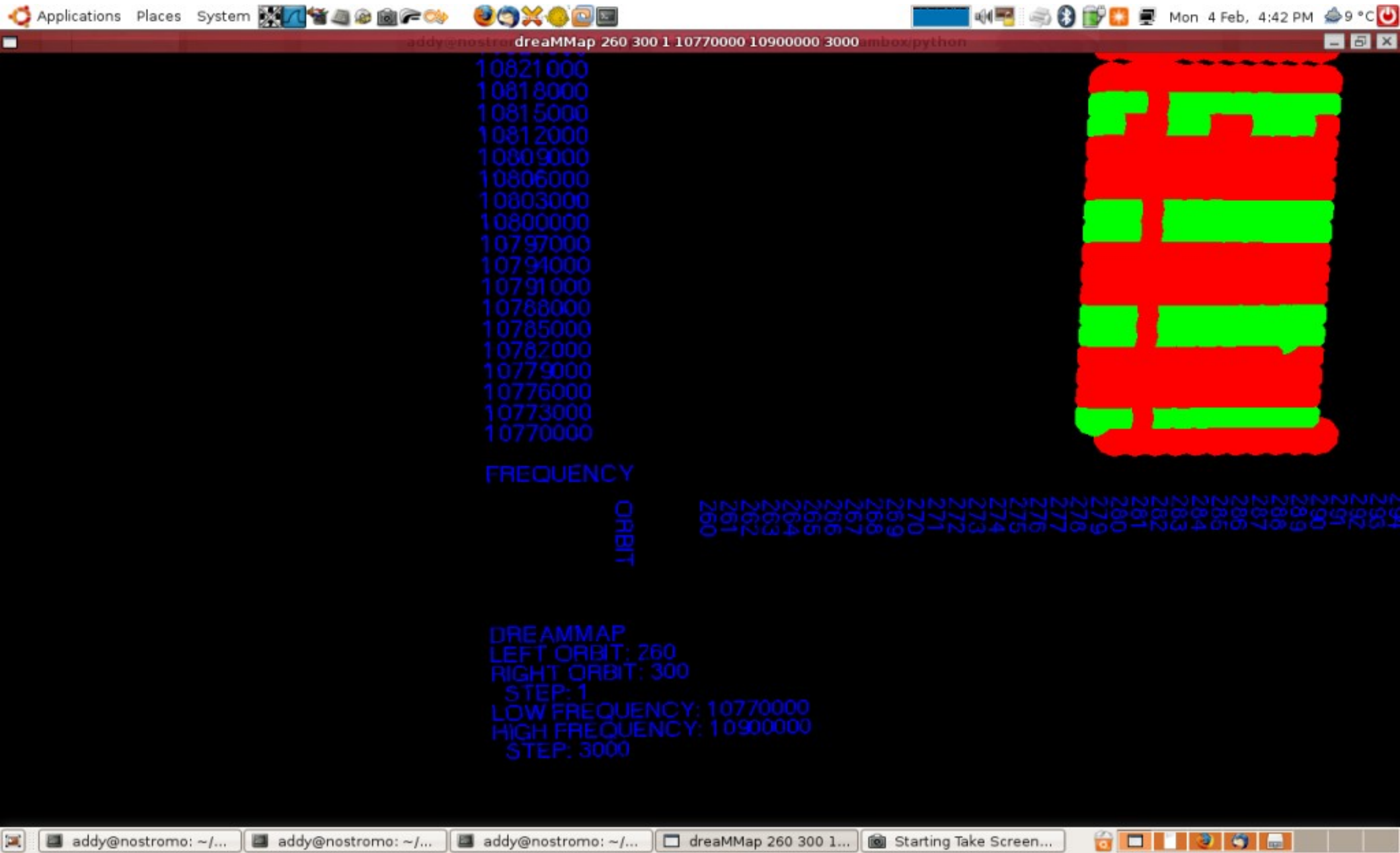
Enigma Web Interfac... Starting Take Screen...

Tor Disabled

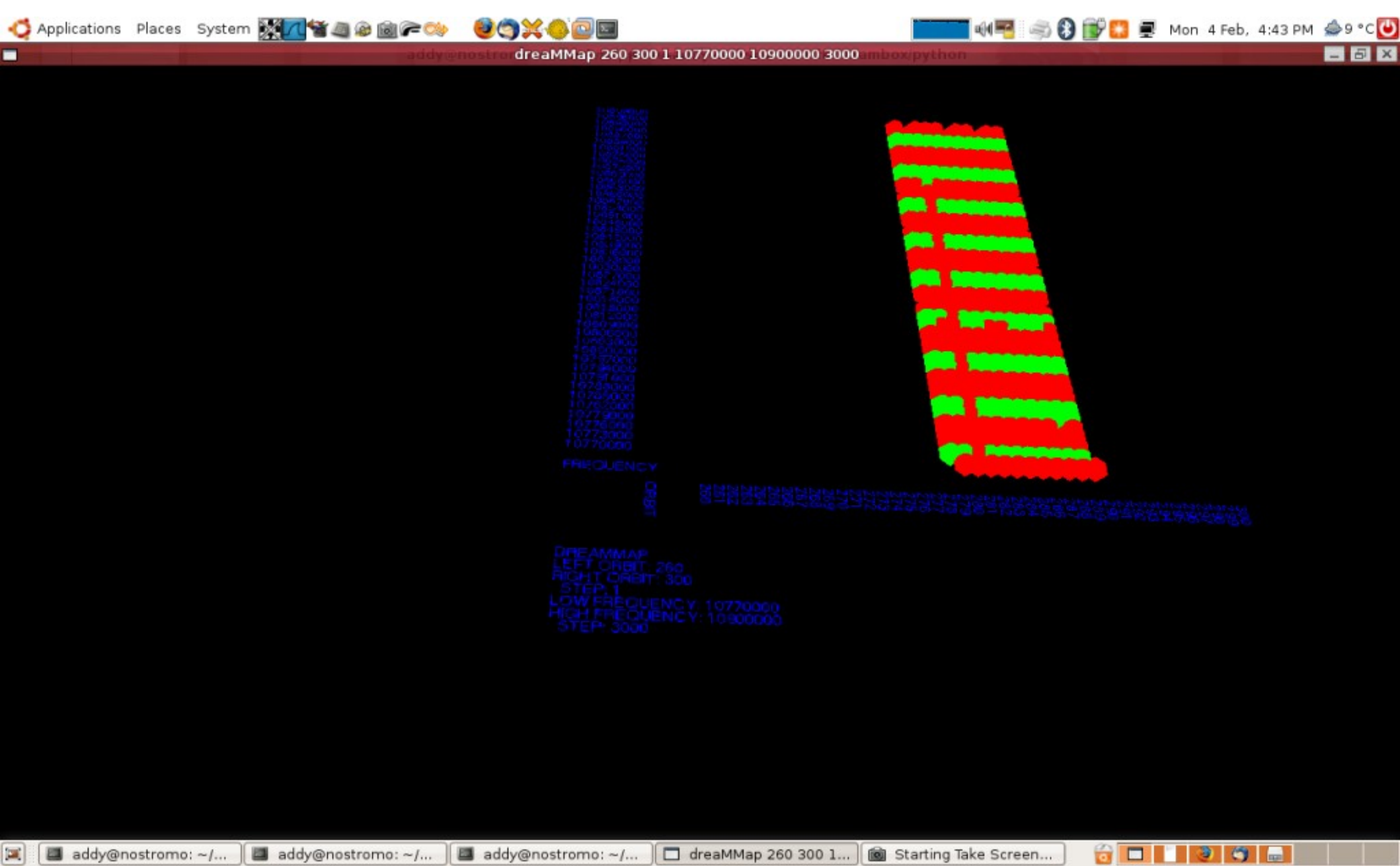
dreaMMap

- python (yay!) script
 - Grab URL
 - Read status from returned webpage
 - Create 3D model

This is now...



This is now...



3D model capabilities

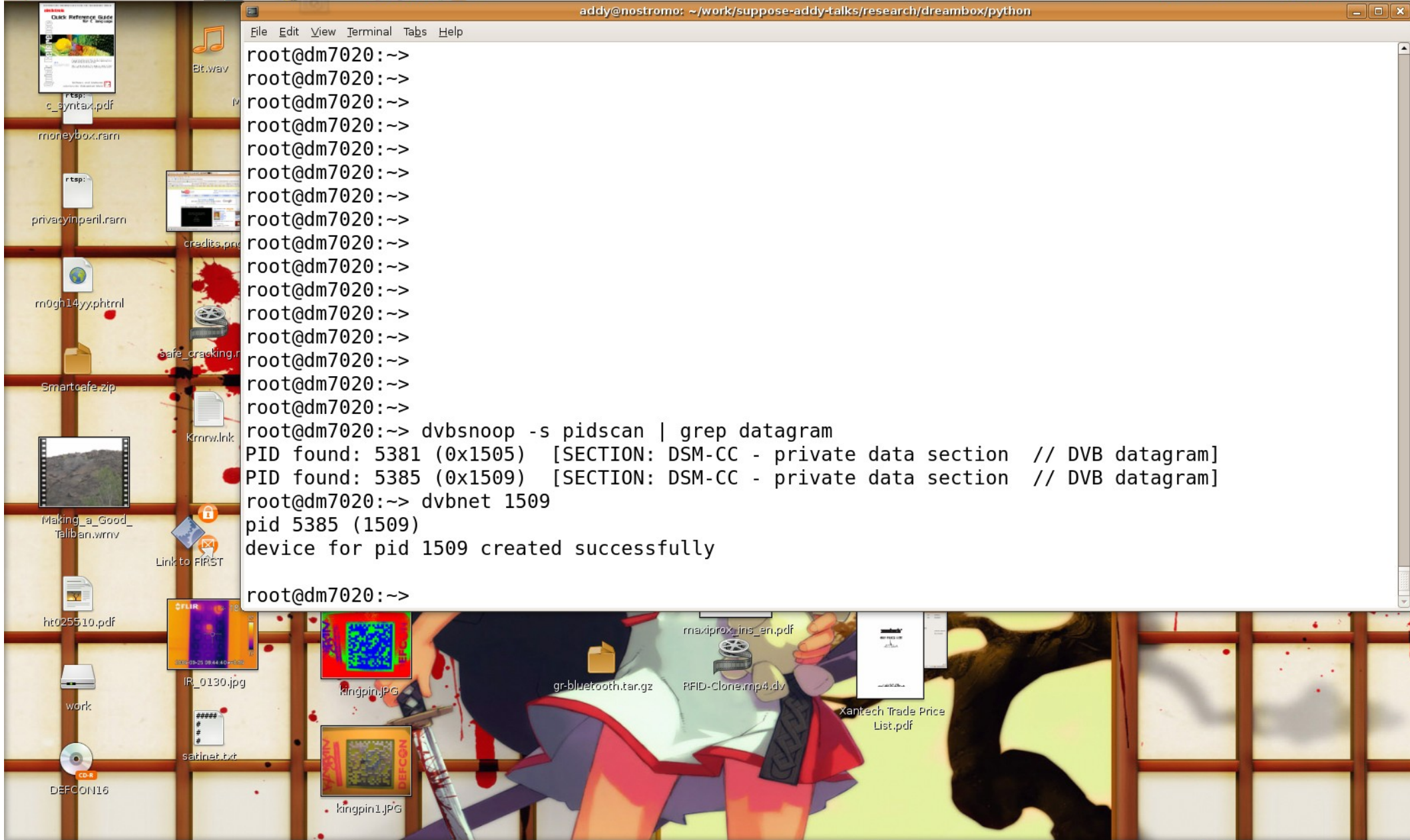
- Point & Click
 - Steer to sat/freq
 - Decode DVB/Audio within model
 - Read Text / EPG
 - Pipe datagrams to Wireshark

Demonstration

File Edit View Terminal Tabs Help

```
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~>
root@dm7020:~> dvbsnoop -s pidscan | grep datagram
PID found: 5381 (0x1505) [SECTION: DSM-CC - private data section // DVB datagram]
PID found: 5385 (0x1509) [SECTION: DSM-CC - private data section // DVB datagram]
root@dm7020:~> dvbnet 1509
pid 5385 (1509)
device for pid 1509 created successfully

root@dm7020:~>
```




```
File Edit View Terminal Tabs Help
root@dm7020:~> dvbnet 1509
pid 5385 (1509)
device for pid 1509 created successfully

root@dm7020:~> ifconfig -a
dvb0_0  Link encap:Ethernet  HWaddr 00:09:34:BA:DA:DD
        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:0x1509

eth0    Link encap:Ethernet  HWaddr 00:09:34:14:BA:07
        inet addr:192.168.111.67  Bcast:192.168.111.255  Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:1615 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1834 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:133285 (130.1 KiB)  TX bytes:350560 (342.3 KiB)
        Interrupt:29

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
```



```

addy@nostromo: ~/work/suppose-addy-talks/research/dreambox/python
File Edit View Terminal Tabs Help
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:116 errors:0 dropped:0 overruns:0 frame:0
TX packets:116 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:8446 (8.2 KiB) TX bytes:8446 (8.2 KiB)

root@dm7020:~> ifconfig dvb0_0 up
root@dm7020:~> ifconfig
dvb0_0 Link encap:Ethernet HWaddr 00:09:34:BA:DA:DD
UP BROADCAST RUNNING NOARP MULTICAST MTU:4096 Metric:1
RX packets:1019 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:363018 (354.5 KiB) TX bytes:0 (0.0 B)
Base address:0x1509

eth0 Link encap:Ethernet HWaddr 00:09:34:14:BA:07
inet addr:192.168.111.67 Bcast:192.168.111.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1659 errors:0 dropped:0 overruns:0 frame:0
TX packets:1860 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:137103 (133.8 KiB) TX bytes:355694 (347.3 KiB)

```




```

File Edit View Terminal Tabs Help

root@dm7020:~> tcpdump -lni dvb0_0 | more
tcpdump: WARNING: dvb0_0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on dvb0_0, link-type EN10MB (Ethernet), capture size 68 bytes
16:45:04.493883 IP 10.190.10.110.1549 > 236.8.8.21.3420: UDP, length: 189
16:45:04.495151 IP 10.190.10.110.1539 > 236.8.8.23.3420: UDP, length: 44
16:45:04.506835 IP 10.190.10.121.1163 > 236.8.8.13.6000: UDP, length: 1162
16:45:04.511748 IP 10.190.10.110.1550 > 236.8.8.17.3420: UDP, length: 772
16:45:04.513942 IP 10.190.10.110.1547 > 236.8.8.22.3420: UDP, length: 263
16:45:04.519625 IP 10.190.10.110.1549 > 236.8.8.21.3420: UDP, length: 859
16:45:04.520495 IP 10.190.10.110.1539 > 236.8.8.23.3420: UDP, length: 79
16:45:04.521769 IP 10.190.10.117.3069 > 236.8.8.8.6001: UDP, length: 146
16:45:04.529671 IP 10.190.10.121.1163 > 236.8.8.13.6000: UDP, length: 1168
16:45:04.536046 IP 10.190.10.121.1163 > 236.8.8.13.6000: UDP, length: 1175
16:45:04.538852 IP 10.190.10.110.1550 > 236.8.8.17.3420: UDP, length: 312
16:45:04.540319 IP 10.190.10.110.1547 > 236.8.8.22.3420: UDP, length: 280
16:45:04.543185 IP 10.190.10.110.1549 > 236.8.8.21.3420: UDP, length: 328
16:45:04.543819 IP 10.190.10.110.1537 > 236.8.8.27.3420: UDP, length: 85
16:45:04.554539 IP 10.190.10.110.1539 > 236.8.8.23.3420: UDP, length: 664
16:45:04.568045 IP 10.190.10.110.1550 > 236.8.8.17.3420: UDP, length: 318
16:45:04.570913 IP 10.190.10.110.1547 > 236.8.8.22.3420: UDP, length: 338
16:45:04.572326 IP 10.190.10.117.3069 > 236.8.8.8.6001: UDP, length: 93
16:45:04.587298 IP 10.190.10.110.1549 > 236.8.8.21.3420: UDP, length: 661

```



Equipment List

- Dreambox 7020
 - £250 (\$350)
- Dish
 - £50 - £200
- Motor & Mount
 - £100
- Total = £550 (\$785)

Questions?

<http://rfidiot.org>

adam@algroup.co.uk